RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 55 02 80 70
http://www.ifri-uac.bj Courriel : secretariat@ifri.uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Sécurité Informatique

Présenté par :
Clarisse **ADJIBA**

Déploiement d'un VPN site-à-site au travers de Fortigate: cas des filiales de MAPCOM TECHNOLOGIES

Sous la supervision :
Dr Pierre Jérôme **ZOHOU**

Membres du jury :

AGOSSOU Carlos	Docteur	Président
TOBOSSI Agossou Olivier	Ingénieur	Examinateur
ZOHOU Pierre Jérôme	Docteur	Rapporteur

Année Académique : **2023-2024**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux viii

Liste des acronymes ix

Introduction 1

1 Etat de l'art 3

2 Analyse, choix techniques et déploiement de la solution 12

3 Résultats et discussion 22

Conclusion 38

Bibliographie 39

Webographie 40

Table des matières 42

Dédicace

Je dédie ce mémoire à :
- ma mère Elisabeth DINHOUNDJO ;
- mon père Hodonou ADJIBA ;
- à toute ma famille et mes proches ;

Remerciements

Nous exprimons notre profonde gratitude à l'Eternel, Dieu Créateur, pour son amour infini, pour l'inspiration et la protection dont il nous comble tous les jours. Nous tenons également à remercier :
• Le Professeur Eugène C. EZIN, le Directeur de l'institut de formation et de recherche en informatique (IFRI) pour nous avoir assuré cette formation ;
• Le Professeur Gaston EDAH, le Directeur Ajoint de l'institut de formation et de recherche en informatique ;
• Docteur Pierre Jerôme ZOHOU, notre encadreur et enseignant à l'institut de formation et de recherche en informatique ;
• Monsieur Zahim DAOUDA, Technicien réseau et système et responsable du service intégration et sécurité à MAPCOM TECHNOLOGIES en son temps, pour son soutien et ses précieux conseils ;
• Tous les enseignants de notre institut en particulier ceux de la filière sécurité informatique pour avoir accepté de partager une partie de leurs connaissances avec nous ;
Tout ceci n'aurait été possible sans la bienveillance de mes parents surtout celle de ma mère. Qu'ils et tous ceux qui ont aidés d'une manière ou d'une autre, trouvent ici l'expression de ma profonde gratitude.

Résumé

Dans un contexte où la connectivité entre sites distants est essentielle, MAPCOM TECHNOLOGIES doit garantir un échange sécurisé et fiable de ses données entre ses filiales du Bénin et du Togo. Cette étude porte sur la mise en place d'un VPN site-à-site, une technologie permettant de créer un lien sécurisé entre deux réseaux situés à des endroits différents, comme s'ils faisaient partie d'un même environnement interne. Pour répondre à ce besoin, nous avons choisi la solution FortiGate de Fortinet, qui utilise le protocole IPSec pour chiffrer les communications entre les sites. Cette approche garantit la confidentialité, l'intégrité et la disponibilité des informations échangées, tout en offrant un accès fluide et sécurisé aux ressources de l'entreprise, notamment aux données hébergées sur le serveur de la direction générale du Bénin. Elle assure également une protection avancée contre les cybermenaces et une meilleure gestion des ressources informatiques de l'entreprise. Avant de procéder au déploiement réel, nous avons réalisé une simulation du réseau dans un environnement virtuel à l'aide de machines EVE-NG sous VMware. Cette étape a permis de tester et d'optimiser la configuration du VPN, afin d'assurer son bon fonctionnement et d'anticiper d'éventuels défis techniques. Ce projet s'inscrit dans une démarche globale d'optimisation de l'infrastructure informatique de MAPCOM TECHNOLOGIES, avec pour objectif de soutenir sa croissance et d'améliorer son efficacité opérationnelle de manière plus économique.

Mots clés : Chiffrement IPSec, VPN site-à-site, Fortigate, accès sécurisé, interconnexion.

Abstract

In a context where connectivity between remote sites is essential, MAPCOM TECHNOLOGIES must ensure secure and reliable data exchange between its branches in Benin and Togo. This study focuses on the implementation of a site-to-site VPN, a technology that creates a secure link between two networks located in different places, as if they were part of the same internal environment. To meet this need, we have chosen the FortiGate solution from Fortinet, which uses the IPSec protocol to encrypt communications between sites. This approach ensures the confidentiality, integrity, and availability of exchanged information while providing smooth and secure access to the company's resources, particularly the data hosted on the server of the general management in Benin. It also provides advanced protection against cyber threats and enhances the management of the company's IT resources. Before proceeding with the actual deployment, we conducted a network simulation in a virtual environment using EVE-NG machines on VMware. This step allowed us to test and optimize the VPN configuration, ensuring its proper functioning and anticipating potential technical challenges. This project is part of a broader initiative to optimize the IT infrastructure of MAPCOM TECHNOLOGIES, aiming to support its growth and improve its operational efficiency in a more cost-effective manner.

Key words: IPSec encryption, site-to-site VPN, Fortigate, secure access, interconnexion.

Table des figures

1.1 Fonctionnement d'un pare-feu [6] . . . 5
1.2 Illustration du Virtual Private Network [8] . . . 7
1.3 Fonctionnement du Virtual Private Network[7] . . . 8
1.4 Illustration d'un VPN d'accès distant [7] . . . 8
1.5 Illustration d'un VPN site-à-site [7] . . . 9
1.6 Comparaison des protocoles VPN [7] . . . 11

2.1 Logo EVE-NG [15] . . . 17
2.2 Logo WinSCP [16] . . . 18
2.3 Logo VMware [17] . . . 18
2.4 Caractéristiques de la machine virtuelle EVE-NG . . . 19
2.5 Interface EVE-NG . . . 19
2.6 Configuration de base de EVE-NG . . . 20
2.7 Accueil EVE-NG . . . 20
2.8 Accès à l'interface graphique de la machine EVE-NG . . . 21

3.1 Architecture réseau . . . 24
3.2 Configuration de l'interface "Management" et "WAN" en ligne de commande(CLI) . . . 25
3.3 Page web d'authentification du Fortigate . . . 26
3.4 Tableau de bord Fortigate . . . 26
3.5 Configuration port2(DMZ) . . . 27
3.6 Configuration port1(LAN) . . . 27
3.7 Configuration de l'interface "Management" et "WAN" en ligne de commande(CLI) . . . 28
3.8 Configuration port1(LAN) . . . 28
3.9 Avant de commencer . . . 29
3.10 Choix du type d'installation . . . 29
3.11 Choix du serveur de destination . . . 30
3.12 Choix des rôles de serveurs . . . 30
3.13 Confirmation des rôles choisis . . . 31
3.14 Serveur IIS installé . . . 31
3.15 Création du tunnel IPSEC(Bénin vers Togo) sur le FGB . . . 32
3.16 Créaton des règles de pare-feu pour autoriser le trafic au travers du tunnel VPN . . . 33
3.17 Créaton de la route statique pour autoriser le trafic au travers du tunnel VPN . . . 33
3.18 Création du tunnel IPSEC(Togo vers Bénin) sur le FGT . . . 34
3.19 Créaton des règles de pare-feu pour autoriser le trafic au travers du tunnel VPN . . . 35
3.20 Créaton de la route statique pour autoriser le trafic au travers du tunnel VPN . . . 35
3.21 VPN en mode UP après configuration . . . 36

3.22 Vérification de la connexion par ping 36
3.23 Autorisation du trafic ICMPv4 entrant sur le serveur 36
3.24 Ping du LAN du Togo vers le serveur 37

Liste des tableaux

1.1 Tableau comparatif des différents types de VPN 9

2.1 Tableau récapitulatif des besoins de MAPCOM TECHNOLOGIES 13
2.2 Comparaison des solutions d'interconnexions de sites 16

3.1 Légende des équipements du réseau 23
3.2 Plan d'adressage 25

Liste des acronymes

ACL :

Access Control List. 5,

Cisco ASA :

Cisco Adaptive Security Appliance. 13, 14, 16,

DMZ :

Demilitarised Zone.

DPI :

Deep Packet Inspection. 14,

EVE-NG :

Emulated Virtual Environment-Next Generation. vi, 17–21, 43,

FAI :

Fournisseur d'Accès à Internet. 7,

FTP :

File Transfer Protocol. 17,

FWaaS :

Firewall as a Servicz. 15,

HIDS :

Host-based Intrusion Detection System. 6,

ICMP :

Internet Control Message Protocol.

IDS :

Intrusion Detection System. 6, 42,

IKEv2 :

Internet Key Exchange version 2.

IP :

Internet Protocol. 4, 7, 10, 14, 22–24, 28, 30,

IPS :

Intrusion prevention System. 6, 42,

IPSEC :

Internet Protocol Seurity. 13, 15, 31, 34,

ISP :

Internet Service provider

L2TP/IPSEC :

Layer 2 Tunneling Protocol/ IP Security.

LAN :

Local Area Network.

MFA :

Multi-Factor Authentication. 5,

NAC :

Network Access Control. 5,

NAT :

Network Address Translation. 14,

NGFW :

Next Generation Firewall. 14, 16, 21,

NIDS :

Network Intrusion Detection System. 6,

PPTP :

Point-to-Point Tunneling Protocol.

PSK :

Pre-Shared Key.

QoS :

Quality of Service. 15,

RED :

Remote Ethernet Device. 15,

S3 :

Simple Storage Service. 17,

SASE :

Secure Access Service Edge. 15,

SCP :

Secure Copy Protocol. 17,

SD-WAN :

Software Defined- World Area Network. 14, 15,

SFTP :

SSH File Transfer Protocol. 17,

SHA1 :

Secure Hash Algorithm 1.

SHA256 :

Secure Hash Algorithm 256 bits.

SSH :

Secure Shell.

SSL :

Secure Socket Layer.

SSTP :

Secure Socket Tunneling Protocol.

UTM :

Unified Threat Management.

VPN :

Virtual Private Network. vi, viii, 3, 7–12, 14, 15, 21–24, 31, 42, 43,

WAN :

World Area Network.

WebDAV :

Web Distributed Authoring and Versioning. 17,

Introduction Générale

Dans un monde de plus en plus connecté, la sécurité des données devient un paramètre cruciale pour toute organisation compte tenu des échanges d'informations qui se font au quotidien. A cet effet, pour toute entreprise surtout celles géographiquement dispersés, il devient important de déployer des solutions qui garantissent une communication sécurisée entre ces différents sites et un accès sécurisé aux ressources internes. C'est dans cette dynamique que s'inscrit notre travail de déploiement d'un VPN au sein de MAPCOM TECHNOLOGIES.

Problématique :

Avec son expansion au Togo, MAPCOM TECHNOLOGIES doit relever un défi stratégique : assurer une connectivité sécurisée, fiable et performante entre ses filiales tout en optimisant les ressources existantes. Actuellement, les données et applications critiques de l'entreprise sont hébergées sur un serveur centralisé au Bénin. Cependant, les employés de la filiale togolaise doivent pouvoir y accéder en toute sécurité et sans interruption, afin de garantir la continuité des opérations et la productivité des équipes.

Deux solutions pourraient être envisagées : l'installation d'un serveur dédié au Togo ou la mise en place d'une connexion sécurisée entre les deux sites. La première option, bien que possible, engendrerait des coûts élevés liés à l'acquisition, l'installation et la maintenance d'un serveur supplémentaire, ainsi qu'aux infrastructures réseaux nécessaires. De plus, elle complexifierait la gestion des ressources informatiques en dispersant les données sur plusieurs sites. Cette étude propose la mise en place d'un VPN site-à-site basé sur la solution FortiGate de Fortinet, utilisant le protocole IPSec. Cette technologie permettra de créer un tunnel sécurisé entre les deux filiales, garantissant un échange fluide et protégé des données sans nécessiter l'installation d'un serveur supplémentaire au Togo. Ce qui offre une solution optimale et économique à MAPCOM TECHNOLOGIES.

Objectifs :

L'objectif principal de notre travail est de garantir une interconnexion sécurisée et efficace entre les filiales béninoise et togolaise de MAPCOM TECHNOLOGIES tout en optimisant les coûts liés à l'infrastructure informatique. De façon spécifique, notre travail vise à :

- créer un tunnel VPN sécurisé basé sur le pare-feu Fortigate et le protocole IPsec pour assurer

une communication privée entre les deux site ;

- centraliser les données et les applications critiques sur le serveur de la filiale béninoise afin d'éviter l'investissement dans un serveur dédié pour le Togo ;
- assurer une gestion efficace et économique du VPN en mettant en place des politiques de sécurité adaptées, un suivi des performances et une maintenance proactive.

Présentation du lieu de stage :

MAPCOM TECHNOLOGIES est un prestataire de services en conception, développement et intégration de solutions en Technologies de l'Information et de la Communication (TIC). Il est spécialisé en systèmes réseautiques convergents, applications informatiques et applications VoIP. Il exerce ses activités sur le territoire béninois depuis 2004. MAPCOM TECHNOLOGIES est une société immatriculée au registre commercial No BB/COT/07B 2208 portant identification fiscale sur le No 3201002013519. La société a pour objectif d'implémenter des technologies afin qu'elles deviennent des solutions intégrées dans les processus métier des entreprises et répondent aux solutions organisationnelles en ressources métier humaines. Sa mission est d'aider les entreprises à maintenir le cap au travers des évolutions technologiques qu'elles vivent. Pour y parvenir elle fournit les services suivants :
- intégration de réseaux et systèmes ;
- virtualisation des données ;
- stockage des données ;
- interconnexion des sites ;
- location d'équipements informatiques ;
- construction de Datacenter ;
- audit informatique ;
- mise en place de cloud privés ;
- maintenance d'infrastructures ;

Organisation du mémoire :

Ce présent travail de recherche est organisé en trois chapitres. Le premier est une revue de la littérature consacrée à l'état de l'art. Le deuxième chapitre analyse et explique les choix techniques effectués et le déploiement de la solution. Enfin, le troisième chapitre présente et analyse les résultats obtenus lors des tests effectués.

Chapitre 1

Etat de l'art

Introduction

La sécurité informatique est devenue un enjeu majeur dans notre société actuelle. Les cyberattaques se multiplient et les conséquences peuvent être désastreuses, tant pour les individus que pour les entreprises. Ce chapitre aborde les concepts fondamentaux de la sécurité informatique, les enjeux associés, ainsi que les mécanismes de protection des réseaux informatiques. Nous avons également abordé les réseaux privés virtuels (VPN), une solution essentielle pour sécuriser les communications et interconnecter les différents sites d'une entreprise.

1.1 La sécurité informatique

La sécurité informatique couvre l'ensemble des moyens, outils, techniques et méthodes pour garantir que seules les personnes ou autres systèmes autorisés interviennent sur le système d'information d'une organisation ou d'une personne, et l'utilisent dans le cadre prévu. Pour garantir la sécurité d'un système, cinq (05) principaux objectifs sont visés :

- **l'intégrité** : permet de garantir que les données n'ont subi aucune altération ;
- **la confidentialité** : consiste à assurer que seules les personnes autorisées ont accès aux ressources échangées.
- **la disponibilité** : permet de garantir un fonctionnement continu et sans faille du système et d'assurer l'accès aux services et ressources avec le meilleur temps de réponse.
- **la non-répudiation** : représente la garantie qu'aucune action ou transaction sur le système ne peut être niée par son commanditaire.
- **l'authentification** : vise à assurer que la personne demandant l'accès aux ressources est bien celle qu'elle prétend être.

Dans le cadre de ce document, les aspects de la sécurité mis en avant sont la disponibilité, l'intégrité et la confidentialité.

1.1.1 Les enjeux de la sécurité informatique

Le risque en termes de sécurité informatique, est la probabilité qu'une attaque survienne. Il est généralement caractérisé par l'équation suivante :

$$Risque = \frac{menace \times vulnrabilits}{contre - mesure}$$

.

La menace (ou « *threat* » en anglais) est toute cause potentielle d'incident. Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque, tandis que la vulnérabilité (« *vulnerability* » en anglais), appelée parfois faille ou brèche, représente le niveau d'exposition face à la menace. Elle peut être une erreur de conception (*bug*) pouvant altérer la sécurité du système. On peut trouver des vulnérabilités au niveau du système d'exploitation, au niveau applicatif ou bien au niveau du réseau.

Enfin, la contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace. Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies. Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi.

Une attaque informatique est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables. Les attaques touchent généralement trois composantes du système à savoir la couche réseau, le système d'exploitation et la couche applicative.

1.1.2 Les mécanismes de protection d'un réseau informatique

Les failles de sécurité peuvent entraîner le vol de données, des interruptions de service, une perte de confiance des clients et des partenaires, ainsi que des coûts élevés pour la réparation et la mise en place de mesures de sécurité. Les entreprises, afin d'éviter ces problèmes, adoptent des mécanismes de protection que sont :

1.1.2.1 Pare-feu(Firewall)

Un pare-feu, également connu sous le nom de firewall, est un dispositif de sécurité réseau qui contrôle le trafic entrant et sortant d'un réseau. Son rôle principal est de filtrer le trafic en fonction de règles prédéfinies, ce qui permet de protéger le réseau contre les menaces et les attaques potentielles.
Le fonctionnement d'un pare-feu repose sur un ensemble de règles définies qui déterminent quelles connexions réseau sont autorisées ou bloquées. Ces règles sont généralement basées sur des critères tels que :

- l'adresse IP source et de destination ;
- le port utilisé pour la communication ;
- le protocole de communication (par exemple, TCP, UDP) ;
- et d'autres paramètres spécifiques.

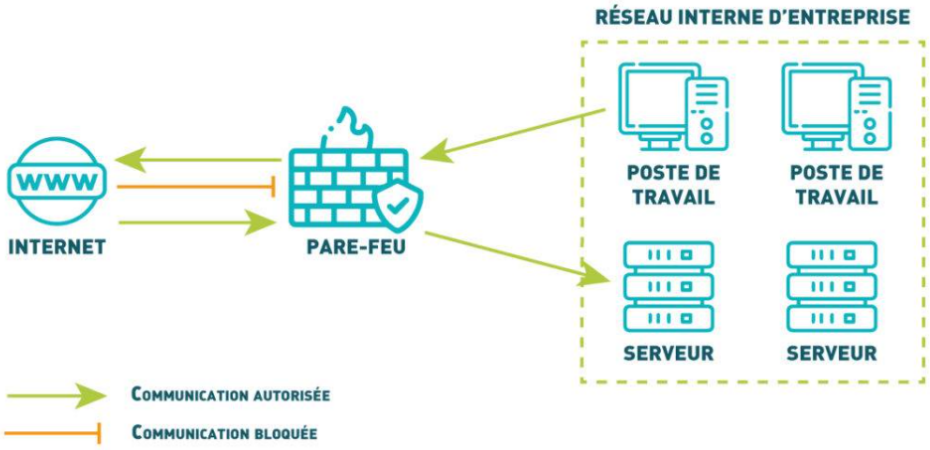


FIGURE 1.1 : Fonctionnement d'un pare-feu [6]

Il existe de nombreux types de pare-feu, souvent classés par format, emplacement sur le réseau, méthode de filtrage des données et catégorie de systèmes protégés. En se référant au classement par format, nous distinguons deux types de pare-feu :

- le **pare-feu matériel :** c'est un boîtier physique placé entre le réseau interne et internet. Grâce à l'analyse active des paquets de données, ce pare-feu peut identifier et bloquer les menaces, assurant ainsi une défense efficace contre d'éventuelles intrusions.
- le **pare-feu logiciel :** fourni sous forme d'application installable sur un serveur et/ou un ordinateur, il embarque la même technologie que le matériel tout en offrant diverses options de déploiement adaptées aux besoins des environnements virtualisés ou multi-cloud.

1.1.2.2 Contrôle d'accès(Access Control)

Le contrôle d'accès au réseau (NAC), également connu sous le nom de contrôle d'admission au réseau, est le processus consistant à empêcher les utilisateurs et appareils non autorisés d'accéder à un réseau d'entreprise ou privé. Le NAC garantit que seuls les utilisateurs authentifiés et les dispositifs autorisés et conformes aux politiques de sécurité peuvent pénétrer dans le réseau. Il inclut des mécanismes comme les listes de contrôle d'accès (ACL) et l'authentification multi-facteurs (MFA). Les solutions NAC peuvent être configurées pour détecter toute activité inhabituelle ou suspecte du réseau et réagir avec une action immédiate, telle que l'isolation du dispositif du réseau pour empêcher la propagation potentielle de l'attaque.

1.1.2.3 Chiffrement(Encryption)

C'est l'ensemble des techniques permettant de chiffrer des messages, c'est- à-dire de les rendre incompréhensibles sans une action spécifique. Le message initial est appelé message en claire et, après chiffrement, message chiffré ou cryptogramme. Le chiffrement et le déchiffrement sont réalisés principalement à partir d'algorithmes, en utilisant des clés secrètes ou publiques. Les techniques de chiffrement sont essentiellement scindées en deux, notamment :

- le chiffrement symétrique : il utilise une seule clé pour le chiffrement et déchiffrement d'un message. Il est le moins sécurisé, du fait que c'est la même clé qui est échangée entre les deux entités communicantes.

- le chiffrement asymétrique : plus sécurisé que le chiffrement symétrique du fait qu'on utilise une paire de clés, une clé publique pour chiffrer le message une clé privée que seul le destinataire possède pour pouvoir déchiffrer le message.

1.1.2.4 Segmentation du réseau (Network segmentation)

La segmentation consiste à diviser le réseau en plusieurs parties. Chaque partie, ou segment, contient un groupe spécifique d'ordinateurs ou de dispositifs qui ont quelque chose en commun, comme l'appartenance à un même service ou la nécessité de mesures de sécurité similaires. Cette segmentation empêche les accès non autorisés et limite la propagation des menaces potentielles au sein du réseau. En d'autres termes, même si un segment du réseau est compromis, l'impact est contenu dans ce segment spécifique, ce qui empêche l'attaquant de se déplacer facilement vers d'autres parties du réseau.

1.1.2.5 Système de détection et de prévention des intrusions (IDS/IPS)

a- IDS :
La détection d'intrusions est le processus de surveillance des événements se trouvant dans un système d'ordinateurs ou de réseau et les analysant pour détecter les signes des intrusions, défini comme des tentatives pour compromettre la confidentialité, l'intégrité, la disponibilité ou éviter des mécanismes de sécurité de l'ordinateur ou du réseau. Le système de détection des intrusions est un logiciel ou un matériel qui automatise des surveillances et les processus analysés. Nous avons plusieurs types d'IDS disponibles de nos jours, caractérisés par des surveillances différentes et des approches d'analyse. On cite essentiellement trois types d'IDS, comme suit :

1. **Network Intrusion Detection System (NIDS)** : surrveille le trafic réseau pour détecter des comportements suspects ou des attaques.
2. **Host-based Intrusion Detection System (HIDS)** : surveille les activités spécifiques d'un hôte (ordinateur ou serveur) pour identifier des intrusions.
3. **Intrusion Detection System hybride** : combine les fonctionnalités des NIDS et HIDS pour une meilleure détection.

b- IPS :
Un système de prévention des intrusions est une forme de sécurité de réseau qui sert à détecter et prévenir les menaces identifiées. Les systèmes de prévention des intrusions surveillent en permanence votre réseau, recherchant les éventuels actes de malveillance et capturent des informations à leur sujet. L'IPS signale ces événements aux administrateurs du système et prend des mesures préventives, telles que la fermeture des points d'accès et la reconfiguration des firewalls pour empêcher de futures attaques. Les solutions IPS peuvent également être utilisées pour identifier les problèmes liés aux politiques de sécurité de l'entreprise, afin de dissuader les employés et les invités du réseau d'enfreindre les règles incluses dans ces politiques. Un réseau d'entreprise typique ayant une multitude de points d'accès, il est essentiel que vous disposiez d'un moyen de surveiller les signes d'effractions potentielles, d'incidents et de menaces imminentes. Les menaces réseau actuelles sont de plus en plus sophistiquées et capables d'infiltrer toutes les solutions de sécurité, même les plus robustes.

1.2 Virtual Private Network(VPN)

Un Virtual Private Network (VPN) est un réseau privé virtuel qui permet de créer une connexion sécurisée et chiffrée entre un utilisateur (ou un réseau local) et Internet. Il crée un tunnel sécurisé à travers un réseau public, tel que l'Internet, pour protéger les données de l'utilisateur. Lorsqu'un utilisateur se connecte à un VPN, toutes les données envoyées et reçues sont chiffrées, ce qui rend difficile leur interception et leur accès non autorisé.

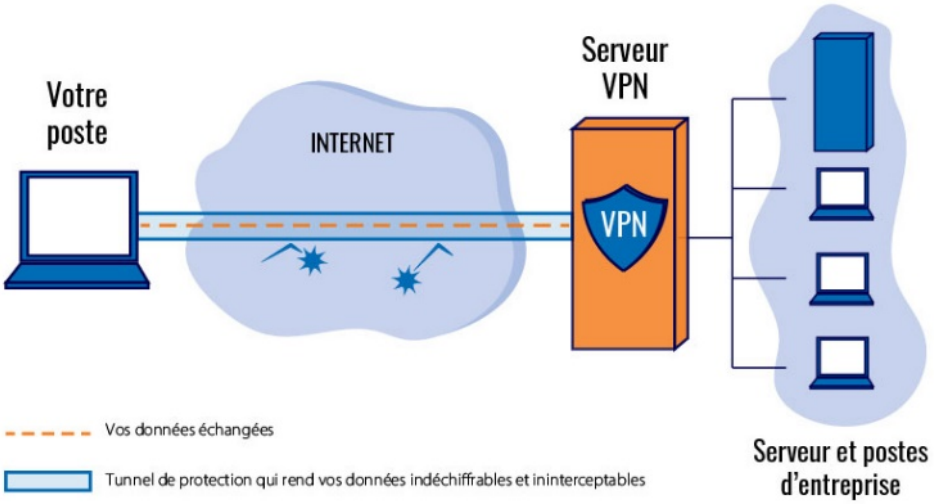


FIGURE 1.2 : Illustration du Virtual Private Network [8]

1.2.1 Fonctionnement d'un VPN

Le réseau privé virtuel a été développé par Microsoft en 1996 pour permettre aux employés travaillant à distance d'accéder au réseau interne de l'entreprise en toute sécurité. Constatant qu'il avait permis de doubler la productivité de l'entreprise, d'autres compagnies ont commencé à adopter cette pratique. Les VPN d'entreprise permettant le travail à distance sont devenus une caractéristique standard dans le monde entier. Les développeurs se sont alors rendus compte que ce « tunnel » sécurisé pouvait être utilisé par les particuliers voulant se connecter en toute sécurité au plus grand réseau de la planète, le World Wide Web ou Internet. Les VPN sont désormais la pierre angulaire de la protection de la confidentialité en ligne pour les consommateurs.

Plutôt que d'envoyer votre trafic Internet (recherches en ligne, chargements, téléchargements...) directement à votre FAI, le VPN achemine d'abord votre trafic via son serveur VPN. Ainsi, lorsque vos données sont finalement transmises sur Internet, elles semblent provenir du serveur VPN et non de votre appareil personnel. Sans VPN, votre adresse IP (Internet Protocol address), un numéro spécial propre à votre réseau domestique, est visible sur le web. Un VPN masque votre adresse IP en agissant comme un intermédiaire et en réorientant votre trafic. Il ajoute également un système de chiffrement, ou un tunnel autour de votre identité, lorsque vous vous connectez. L'association du serveur VPN et du tunnel de chiffrement empêche votre FAI, les gouvernements, les pirates ou qui que ce soit d'espionner votre navigation sur le web.

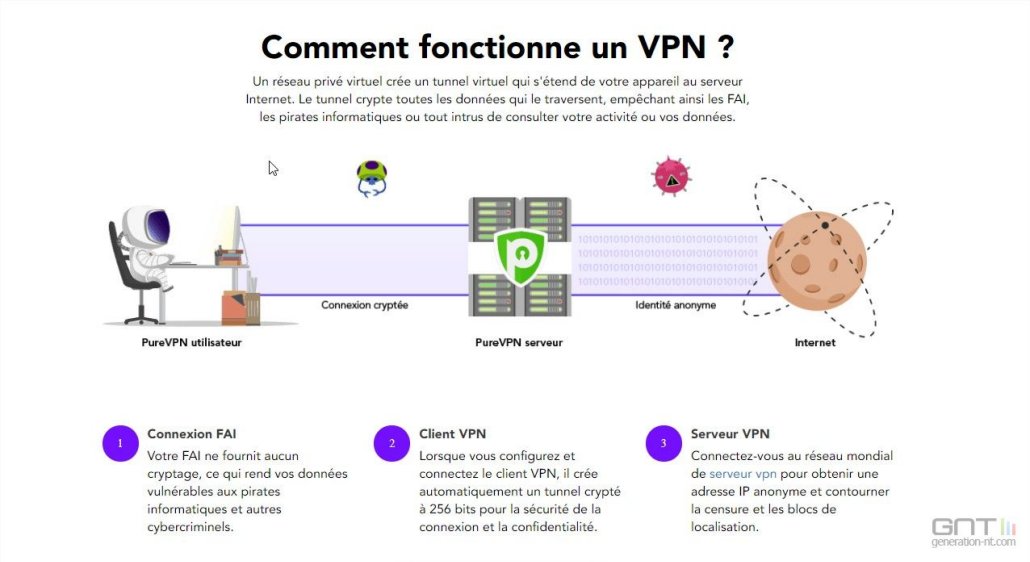


FIGURE 1.3 : Fonctionnement du Virtual Private Network[7]

1.2.2 Différents types de VPN

Il existe deux types de VPN : le VPN d'accès à distance et le VPN site-à-site.

1.2.2.1 VPN d'accès à distance

Un VPN d'accès à distance permet aux utilisateurs de se connecter à un autre réseau via un tunnel privé et chiffré, qu'il s'agisse d'Internet ou du système interne de leur entreprise.

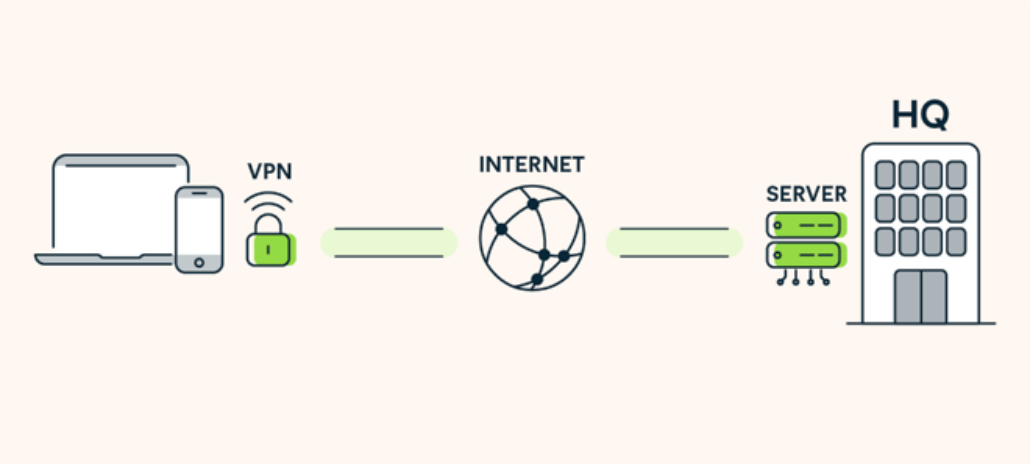


FIGURE 1.4 : Illustration d'un VPN d'accès distant [7]

1.2.2.2 VPN site-à-site

L'autre type de VPN, un VPN site-à-site, est également appelé VPN routeur-à-routeur. Ce type de VPN est principalement utilisé dans le monde professionnel, en particulier lorsqu'une entreprise possède des bureaux à différents emplacements. Le VPN site-à-site crée un réseau interne fermé auquel les différents sites peuvent se connecter les uns aux autres. Ce modèle est appelé intranet.

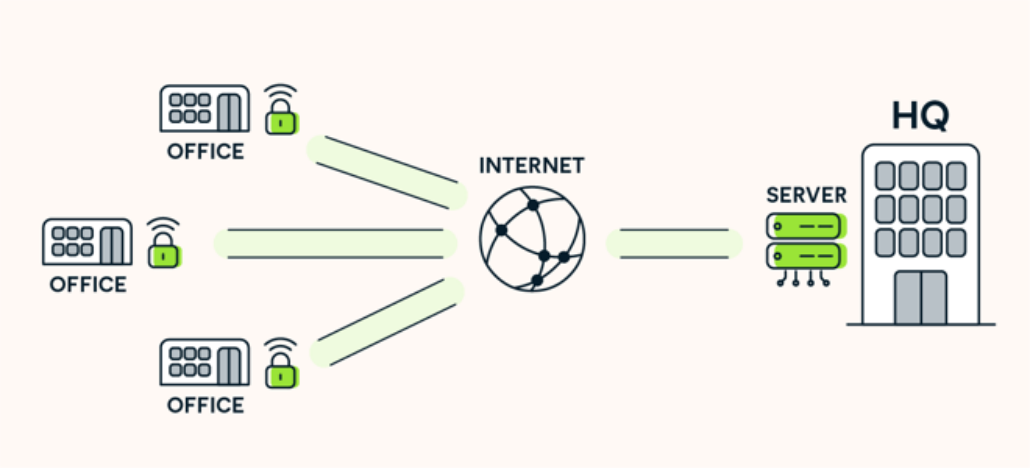


FIGURE 1.5 : Illustration d'un VPN site-à-site [7]

TABLE 1.1 : Tableau comparatif des différents types de VPN

Solution	VPN site à site (site to site VPN)	VPN d'accès à distance (Remote Access VPN)
Fonctionnement	Établit une connexion sécurisée entre deux réseaux distants	Permet aux utilisateurs distants de se connecter au réseau d'entreprise
Connectivité	Connecte des réseaux locaux de différents sites géographiques	Connecte des utilisateurs individuels à distance au réseau d'entreprise
Configuration	Configuration requise au niveau des équipements réseau (routeurs, firewalls, etc.)	Configuration requise au niveau du serveur VPN et des clients VPN
Sécurité	Authentification et chiffrement des données entre les réseaux distants	Authentification et chiffrement des données entre le client et le réseau
Gestion des trafics	Routage du trafic entre les réseaux distants	Routage du trafic depuis les utilisateurs distants vers le réseau
Coûts	Généralement plus coûteux en raison des équipements réseau requis	Coûts plus bas, nécessitant principalement un serveur VPN et des clients
Configuration	Plus complexe en raison de la configuration des équipements réseau	Configuration plus simple au niveau du serveur VPN et des clients
Evolutivité	Possibilité d'ajouter de nouveaux sites distants au réseau	Possibilité d'ajouter de nouveaux utilisateurs distants

1.2.3 Avantages du VPN

Une connexion VPN protège vos données en ligne en les chiffrant, rendant leur interception impossible pour les pirates ou cybercriminels grâce aux fonctionnalités suivantes :

- **chiffrement sécurisé** : un VPN utilise des clés de chiffrement pour protéger vos données. Sans ces clés, il est quasiment impossible de déchiffrer vos informations, même en cas d'attaque par force brute. Cela garantit la confidentialité de vos activités, même sur des réseaux publics.
- **anonymat et dissimulation de localisation** : en redirigeant votre trafic via un serveur distant, un VPN masque votre position réelle. Cela empêche quiconque de déterminer votre emplacement exact. Par ailleurs, la plupart des fournisseurs de VPN n'enregistrent pas vos activités, bien que certains conservent des journaux limités à des fins internes. Il est donc essentiel de vérifier leur politique de confidentialité avant de choisir un service.
- **accès aux contenus régionaux** : les VPN permettent de contourner les restrictions géographiques en changeant virtuellement votre localisation. Cela vous donne accès à des contenus ou services disponibles uniquement dans certains pays, même lorsque vous êtes en déplacement.
- **transfert sécurisé de données** : pour les professionnels travaillant à distance, un VPN est souvent requis pour accéder aux fichiers sensibles d'une entreprise. En utilisant des serveurs privés et des méthodes de chiffrement avancées, les VPN réduisent considérablement le risque de fuite ou d'interception des données.

1.2.4 Protocoles VPN

Un protocole VPN définit comment vos données sont transmises entre votre appareil et un serveur VPN. Les applications VPN utilisent ces protocoles pour créer un tunnel stable et crypté vers le serveur de votre choix, masquant ainsi votre adresse IP et votre activité de navigation. C'est pourquoi on parle aussi de « protocoles de tunnelisation ». Chaque protocole VPN utilise une technologie différente, offrant des niveaux variés de vitesse, de sécurité et de compatibilité.

Voici les principaux protocoles VPN :

- **PPTP (Point-to-Point Tunneling Protocol)** : l'un des plus anciens protocoles, facile à configurer mais considéré comme peu sécurisé aujourd'hui.
- **IKEv2 (Internet Key Exchange version 2)** : rapide et particulièrement adapté aux appareils mobiles grâce à sa capacité à maintenir une connexion stable même lors de changements de réseau.
- **L2TP/IPSec (Layer 2 Tunneling Protocol avec Internet Protocol Security)** : combine la sécurité d'IPSec avec les fonctionnalités de tunnelisation de L2TP. Sécurisé mais parfois plus lent en raison du double encapsulage.
- **SSTP (Secure Socket Tunneling Protocol)** : développé par Microsoft, il fonctionne bien sous Windows et utilise le port HTTPS (443), ce qui le rend efficace pour contourner les pare-feu.
- **WireGuard** : un protocole moderne, axé sur la rapidité et l'efficacité. Il est plus léger et plus facile à auditer que les autres.

- **SoftEther** : flexible et multiplateforme, il prend en charge plusieurs protocoles et est souvent utilisé pour ses performances élevées.
- **OpenVPN** : considéré comme l'un des plus sécurisés et flexibles. Il est open source et utilise des protocoles de chiffrement robustes, adapté à de nombreux cas d'utilisation.

Protocole	Vitesse	Sécurité	Utilisation des données
WireGuard	Très rapide	Très élevée	Très faible
OpenVPN	Moyenne	Très élevée	Élevée
IKEv2/IPSec	Très rapide	Élevée	Moyenne
SoftEther	Très rapide	Élevée	Faible
L2TP/IPSec	Moyenne	Moyenne	Élevée
SSTP	Lente	Moyenne	Élevée
PPTP	Lente	Faible	Moyenne

FIGURE 1.6 : Comparaison des protocoles VPN [7]

Conclusion

En conclusion, la sécurité informatique est indispensable pour protéger les données et les systèmes contre les menaces croissantes. Les mécanismes de protection des réseaux, tels que les contrôles d'accès, la cryptographie et les pare-feu, jouent un rôle crucial dans la défense contre les cyberattaques. Les VPN, en particulier, offrent une solution efficace pour sécuriser les communications et interconnecter les différents sites d'une entreprise, garantissant ainsi la confidentialité et l'intégrité des données transmises.

Chapitre 2

Analyse, choix techniques et déploiement de la solution

Introduction

Dans ce chapitre, nous avons exposé les solutions existantes sur le marché afin d'en choisir une pour répondre aux besoins actuels de l'entreprise cliente. Nous avons également abordé un aperçu des différents outils et technologies utilisés pour l'implémentation de notre solution.

2.1 Analyse des besoins

Le déploiement d'un VPN site-à-site entre les filiales de MAPCOM TECHNOLOGIES, situées au Bénin et au Togo, nécessite une étude approfondie des besoins en termes d'infrastructure, de sécurité, de performances et de conformité. L'objectif principal est de permettre un partage sécurisé des données hébergées sur le serveur de la filiale du Bénin avec celle du Togo. Le VPN doit fournir une interconnexion transparente entre les deux sites, permettant une collaboration fluide, comme s'ils étaient sur le même réseau local (LAN).

TABLE 2.1 : Tableau récapitulatif des besoins de MAPCOM TECHNOLOGIES

Catégorie	Description des besoins
Infrastructure réseau	Chaque site doit disposer d'une connexion Internet stable et rapide pour supporter le trafic du VPN, en particulier pour le transfert de grandes quantités de données. L'équipement réseau, tel que des routeurs ou pare-feu supportant le VPN (comme FortiGate, Cisco ASA ou Palo Alto), est nécessaire pour sécuriser et gérer les connexions. De plus, des adresses IP publiques statiques sont requises pour établir le tunnel VPN entre les deux sites.
Sécurité	Le VPN doit garantir la confidentialité et l'intégrité des données grâce à des protocoles de chiffrement sécurisés, comme IPSEC. Une authentification forte, utilisant des certificats ou des clés pré-partagées (PSK), est essentielle pour assurer que seuls les sites autorisés peuvent établir la connexion. Des politiques de pare-feu strictes doivent être mises en place pour filtrer le trafic et protéger les ressources partagées.
Performances	Le VPN doit être configuré de manière à minimiser l'impact sur la bande passante, en particulier si des fichiers volumineux sont régulièrement transférés. La latence doit également être réduite au maximum pour assurer des échanges rapides et une stabilité des connexions entre les deux sites.
Maintenance et gestion	Il est important de mettre en place des outils de surveillance pour superviser l'état du VPN et garantir qu'il reste opérationnel en tout temps. Un support technique doit être disponible pour résoudre rapidement tout problème de connectivité ou de configuration, et les équipements doivent être régulièrement mis à jour pour maintenir la sécurité et les performances.
Conformité et réglementation	Le déploiement du VPN doit respecter les réglementations locales en matière de gestion des données et de réseaux privés dans les pays concernés (Bénin et Togo).
Évolutivité	La solution VPN doit être évolutive, permettant d'ajouter de nouveaux sites ou de gérer une augmentation du volume de données sans compromettre les performances ou la sécurité.

2.2 Les solutions d'interconnexion de sites distants existants

Dans le cadre de l'interconnexion de sites distants, plusieurs solutions sont disponibles sur le marché, chacune offrant des fonctionnalités spécifiques pour répondre aux besoins variés des entreprises. Voici quelques unes de ces solutions :

- FortiGate Next Generation Firewall(NGFW) :
  Le FortiGate NGFW est le pare-feu réseau le plus déployé au monde, offrant une gamme complète de fonctionnalités pour assurer la sécurité et la performance des réseaux. Il intègre des fonctions telles que le VPN, la prévention d'intrusion, le filtrage web, ainsi que la protection anti-malware et anti-spam. Le FortiGate peut fonctionner en mode transparent, s'installant entre le réseau interne et le routeur sans nécessiter de modifications, ou en mode Network Address Translation(NAT)/Route, où il agit comme une passerelle, masquant les adresses IP privées. Grâce à ses processeurs de sécurité performants, il optimise les performances réseau tout en assurant une protection robuste contre les attaques. Bien que son interface en ligne de commande puisse être complexe pour les débutants, il reste une solution recommandée pour les entreprises sans personnel de sécurité dédié.

- Cisco ASA(Adaptive Security Appliance) :
  Le logiciel Cisco Adaptive Security Appliance (ASA) est le système d'exploitation principal de la gamme Cisco ASA, offrant des fonctionnalités de pare-feu de classe entreprise pour divers formats de périphériques. Il intègre des technologies de sécurité critiques comme IPS, VPN et communications unifiées, et permet un clustering hautes performances pour améliorer la capacité et les performances. Le logiciel assure une haute disponibilité, facilite la collaboration entre périphériques physiques et virtuels, et répond aux besoins spécifiques des réseaux et centres de données. Il fournit également une connaissance contextuelle avancée et facilite le routage dynamique et les VPN site à site.

- Palo Alto Networks :
  Palo Alto Networks est une entreprise leader dans le domaine de la cybersécurité, reconnue pour ses solutions innovantes. Entre elles on peut citer le NGFW et Prisma SD-WAN. Le NGFW de Palo Alto Networks offre plusieurs fonctions avancées, comme un VPN pour des connexions sécurisées, la détection et prévention des menaces avancées pour protéger contre les attaques sophistiquées, l'inspection approfondies des paquets(DPI pour Deep Packet Inspection), le déchiffrement SSL pour analyser le traffic chiffré, et le contrôle basésur les applications et les utilisateurs pour une gestion granulaire des politiques de sécurité. Prisma SD-WAN, de son côté, optimise la gestiondes réseauxdistribués en utilisant l'intelligence artificielle et l'automatisation pour améliorer la performance du réseau, tout en intégrant la sécurité native et une gestion centralisée pour une connectivité fiable et sécurisée, particulièrement adapté aux environnements cloud et hybrides. L'intégration fluide entre le NGFW et Prisma SD-WAN permet aux entreprises, toute taille y compris, de bénéficier d'une protection renforcée et d'une gestionsimplifiée de leurs réseaux, tout en optimisant les performances et en réduisant les coûts d'exploitation.

- Sophos XG Firewall :
  Le Sophos XG Firewall est une solution de sécurité réseau de nouvelle génération qui offre une protection complète et une gestion simplifiée pour les entreprises de toutes tailles. IL combine des fonctionnalités avancées telles que la prévention des intrusions, le contrôle des applications, le filtrage web, et la détection des menaces avancées pour protéger contre une large gamme de cybermenaces. Le XG Firewall intègre également les capacités VPN et SD-WAN pour l'interconnexion sécurisée des sites distants, ainsi que des dispositifs RED pour faciliter cette connectivité. Géré via la plateforme cloud Sophos Central, il permet une gestion centralisée et active la Synchronized Security, où les produits Sophos communiquent pour détecter et répondre automatiquement aux incidents de sécurité. Le XG Firewall offre une visibilité approfondie sur le réseau grâce à des rapports détaillés et personnalisables, faisant de lui une solution idéale pour renforcer la sécurité et améliorer la performance des réseaux d'entreprise.

- pfSense :
  pfSense est une solution open-source de pare-feu et de retour qui excelle dans l'interconnexion des sites distants grâce à ses fonctionnalités robustes. Elle prend en charge divers types de VPN, y compris IPSEC, OpenVPN et L2TP,permettant de créer des connexions sécurisées et cryptées entre différents sites. pfSense offre également des capacités SD-WAN telles que la répartitionde charge, le basculement et la gestion de la qualité de service(QoS), optimisant ainsi la performance et la disponibilité du réseau. Sa flexibilité et sa scalabilité en font une solution adaptée auxpetites et grandes entreprises, tout en étant économiquement avantageuse. Entant que solutionopen-source, pfSense bénéficie d'une large communauté et permet une personnalisation poussée,offrant ainsi une connectivité sécurisée et adaptable pour les besoins variés des organisations.

- Zscaler Cloud Firewall :
  Zscaler Cloud Firewall ets une solution idéale pour l'interconnexion des sites distants, offrant une sécurité réseau avancée sans nécessiter du matériel sur site. En tant que pare-feu en tant que service (FWaaS pour Firewall as a Service) dans une architecture SASE(Secure Access Service Edge), il sécurise et optimise le trafic entre les sites distants en inspectant tout le trafic réseau directement dans le cloud. Cette approche élimine la complexité des infrastructures locales et permet une gestion centralisée des politiques de sécurité à travers tous les sites. Cette solution inclut des fonctionnalités clés telles que le filtrage des paquets, la détectiondes intrusions, et le contrôle des applications, assurant une protection complète contre les menaces tout en permettant une connectivité fluide et sécurisée. Il supporte également les principes du Zero Trust, authentifiant et sécurisant chaque connexion entre les sites pour minimiser les risques liés aux menaces internes et externes. De plus,la solution offre un routage intelligent et une gestion de la qualité de service(QoS), optimisant ainsi le trafic et améliorant l'expérience utilisateur. Avec Zscaler Cloud Fireall,les entreprises bénéficient d'une interconnexion des sites distants performante,sécurisée, et évolutive, tout en simplifiant la gestion et en réduisant la latence.

2.2.1 Etude comparatif des solutions d'interconnexion existantes

Avant de choisir la solution la plus adaptée aux besoins de l'entreprise, il convient d'effectuer une analyse comparative des différentes options présentées précédemment. La comparaison est synthétisée dans le tableau suivant, qui confronte les principales caractéristiques techniques, sécuritaires et économiques des solutions étudiées.

TABLE 2.2 : Comparaison des solutions d'interconnexions de sites

Critère	**FortiGate NGFW**	**Cisco ASA**	**Palo Alto Networks**	**Sophos XG**	**pfSense**	**Zscaler Cloud FW**
Type	NGFW/UTM	Pare-feu avec NGFW	NGFW/SD-WAN	NGFW/UTM	Open Source FW	Cloud Firewall
Facilité d'intégration	Haute	Haute	Haute/Très haute	Moyenne	Personnalisable	Très haute
Protection avancée	Oui	Moyenne	Très haute/Oui (via Prisma)	Moyenne	Moyenne	Très haute
Performances SSL	Haute	Moyenne	Très haute/N/A	Moyenne	Moyenne	Haute
Coût	Modéré	Modéré à élevé	Élevé	Modéré	Faible	Basé sur l'usage
Type d'architecture	Sur site	Sur site	Sur site/-Cloud	Sur site	Sur site	Cloud native
Taille d'entreprise	Moyenne à grande	Moyenne à grande	Moyenne à grande	Petite à moyenne	Petite à moyenne	Grande

2.2.2 Choix de la solution adéquate

Le choix de FortiGate pour le déploiement du VPN site-à-site de MAPCOM TECHNOLOGIES repose sur sa sécurité avancée, son coût optimisé et sa facilité de gestion. Contrairement à d'autres solutions comme Cisco ASA ou Palo Alto, FortiGate intègre plusieurs fonctionnalités essentielles (pare-feu, VPN, protection contre les intrusions) en un seul appareil, réduisant ainsi les coûts d'investissement et de maintenance. Grâce à son chiffrement IPSEC, il garantit la confidentialité et l'intégrité des échanges entre les filiales du Bénin et du Togo.

En plus de sa sécurité, FortiGate se distingue par son excellent rapport qualité/prix. Son interface intuitive permet une gestion simplifiée du réseau sans nécessiter d'expertise technique avancée, réduisant ainsi les coûts opérationnels. Contrairement à d'autres solutions nécessitant des abonnements ou des mises à niveau fréquentes, FortiGate permet d'ajouter de nouveaux sites sans frais excessifs, ce qui en fait une solution évolutive et adaptée à la croissance de l'entreprise.

Enfin, FortiGate assure une conformité aux normes de cybersécurité en vigueur au Bénin selon [19], évitant ainsi les risques liés aux audits ou aux failles de sécurité. Son support technique 24/7 garantit une stabilité et une assistance rapide en cas de problème, contrairement aux solutions open-source comme pfSense qui ne bénéficient pas d'un accompagnement officiel. Ainsi, FortiGate offre à MAPCOM TECHNOLOGIES une solution fiable, sécurisée et rentable pour son interconnexion entre sites distants.

2.3 Déploiement de la solution

2.3.1 Logiciels et outils utilisés

EVE-NG(Emulated Virtual Environnement - Next Generation : est un logiciel de simulation réseau par virtualisation qui permet de créer des topologies réseaux complexes en utilisant divers équipements virtuels comme des routeurs, des commutateurs et des pare-feu. Elle offre une interface graphique conviviale pour concevoir et gérer facilement ces topologies dans des environnements virtuels comme Docker et VMware. De plus, elle offre des fonctionnalités avancées comme la gestion des snapshots et l'intégration avec des outils de monitoring et de gestion réseau tels que Wireshark, GNS3 et Nagios.Dans le cadre de notre projet, il nous a permis de concevoir l'architecture réseau utilisée.



FIGURE 2.1 : Logo EVE-NG [15]

WinSCP : WinSCP est un client SFTP, FTP, WebDAV, S3 et SCP open source et gratuit pour Windows. Il permet de transférer des fichiers entre un ordinateur local et un serveur distant de manière sécurisée à travers une interface graphique conviviale. WinSCP prend également en charge des fonctionnalités avancées telles que la synchronisation de dossiers, l'édition de fichiers à distance et l'automatisation via des scripts. Nous l'avions utilisé pour transférer des fichiers de notre PC directement sur notre machine EVE-NG de manière rapide et sécurisé.



FIGURE 2.2 : Logo WinSCP [16]

VMware Workstation Pro 17 : VMware Workstation est un outil de virtualisation de poste de travail créé par la société VMware. Il peut être utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation. Cette solution de virtualisation est disponible pour Windows et Linux. Nous l'avions utilisé pour créer un environnement adéquat pour le déploiement de notre VPN.



FIGURE 2.3 : Logo VMware [17]

2.3.2 Installation et configuration de EVE-NG

Pour installer notre machine virtuelle EVE-NG, après avoir ouvert VMware Workstation, nous avons choisir l'option **Créer une machine virtuelle**. Nous avons ensuite suivi les instructions afin de personnaliser notre machine et de lui attribuer les ressources nécessaires en tenant compte des indications données dans la figure suivante :

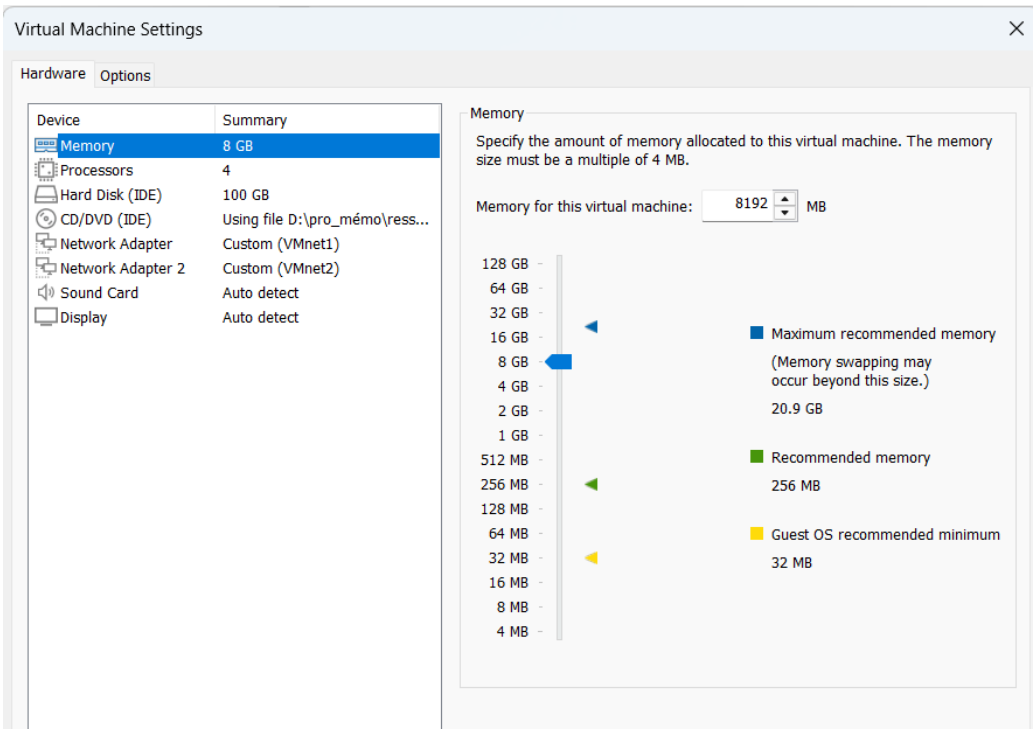


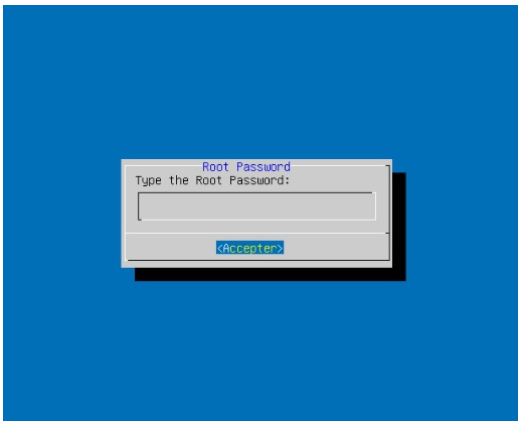
FIGURE 2.4 : Caractéristiques de la machine virtuelle EVE-NG

Après la création de la machine, nous l'avions lancé avec notre fichier .iso de EVE-NG puis procéder à l'installation du système d'exploitation. Lors de l'installation de notre solution, nous accédons à l'interface que voici :



FIGURE 2.5 : Interface EVE-NG

Après avoir saisi le nom d'utilisateur(**root**) et le mot de passe(**eve**) comme définis dans la documentation de EVE-NG dans l'interface de la figure 2.5, nous obtenons l'interface de configuration de base de EVE-NG.



(a) Configuration du mot de passe de la machine EVE-NG



(b) Configuration de l'adresse IP de la machine EVE-NG

FIGURE 2.6 : Configuration de base de EVE-NG

Comme l'indique la figure 2.6, nous pouvons maintenir le mot de passe "eve" ou le changer. Dans notre cas nous l'avions maintenir et choisir le mode pour finaliser l'installation de notre machine. La capture suivante nous montre la fin du processus d'installation.

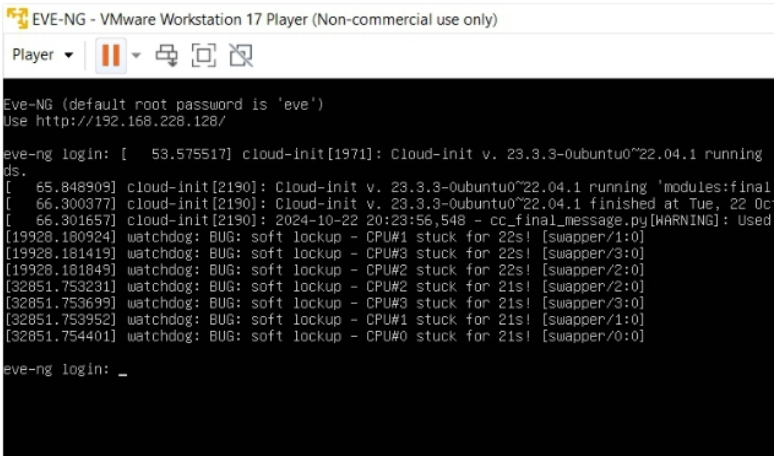
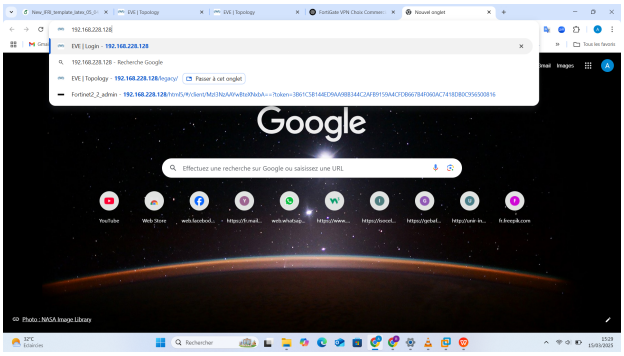


FIGURE 2.7 : Accueil EVE-NG

La figure 2.7 nous montre que nous pouvons accéder à l'interface graphique de EVE-NG en saisissant l'adresse http ://192.168.228.128 dans le navigateur web.



(a) Entrée de l'adresse IP dans le navigateur



(b) Interface web EVE-NG

FIGURE 2.8 : Accès à l'interface graphique de la machine EVE-NG

Une fois que l'adresse IP est insérée dans le navigateur comme l'indique la figure 2.8a, nous accédons à l'interface de la figure 2.8b où nous devons fournir les identifiants de l'administrateur EVE-NG en utilisant **admin** comme username, **eve** comme mot de passe et en choisissant **HTML5 console** pour la troisième option.

Conclusion

En se basant sur l'analyse des besoins et la comparaison des solutions, FortiGate NGFW est le choix idéal pour le déploiement de notre VPN. Il combine sécurité avancée, performances optimisées, gestion centralisée et flexibilité, tout en restant conforme aux exigences locales et en étant évolutif pour s'adapter aux futures extensions de l'entreprise. Le déploiement de notre solution nécessite l'utilisation EVE-NG, un puissant outil virtuel de simulation des environnements réseau complexes.

Chapitre 3

Résultats et discussion

Introduction

Dans ce chapitre, nous avons basé notre travail sur l'architecture réseau proposé pour réaliser des tests afin de mesurer l'efficacité et l'efficience de la solution Fortigate que nous avons choisi.

3.1 Prérequis et architecture réseau

3.1.1 Prérequis

Basés sur les recommandations générales de Fortinet, la mise en place d'un VPN site à site avec les appareils Fortigate nécessite plusieurs principaux prérequis :

- **connectivité réseau :** s'assurer que les deux Fortigate sont connectés à des réseaux fonctionnels et que les adresses IP sont correctement configurées.
- **licence VPN :** vérifier que l'on dispose de licences appropriées et valides pour les deux Fortigate afin d'activer les fonctionnalités VPN.
- **adresses IP publiques ou statiques :** en cas d'utilisation d'adresses IP publiques, chaque Fortigate doit disposer d'une adresse IP publique unique. Dans le cas où ce sont des adresses IP privées, s'assurer qu'elles sont uniques et qu'elles ne se chevauchent pas avec d'autres réseaux.
- **version du firmware :** s'assurer que les deux Fortigate exécutent une même version de firmware, prise en charge et recommandée par Fortinet. Il faut aussi garder ce firmware à jour pour pouvoir bénéficier des derniers correctifs et fonctionnalités.
- **authentification :** choisir une méthode d'authentification pour le VPN, telle que les clés prépartagées (SHA256/SHA1) ou les certificats. S'assurer que les paramètres d'authentification sur les deux Fortigate soient les mêmes.
- **la configuration de base :** configurer les paramètres de base pour chacun des Fortigate, y compris les adresses IP, les sous-réseaux, les interfaces, les routes statiques, etc.

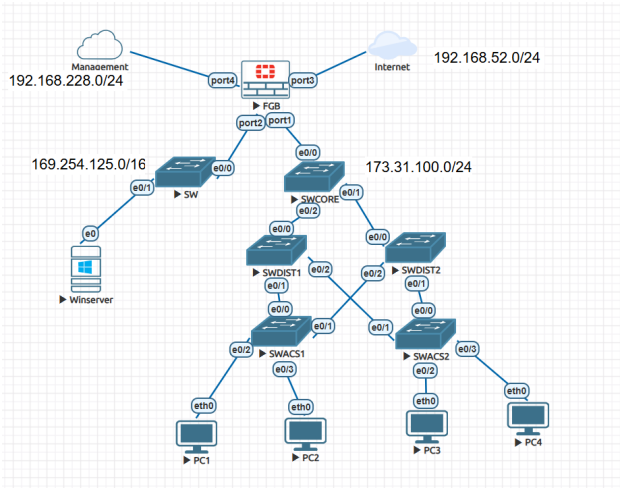
- **configuration du tunnel VPN :** configurer sur chacun des Fortigate le tunnel VPN en spécifiant les paramètres tels que l'adresse IP distante du Fortigate distant, les protocoles de chiffrement, les algorithmes d'authentification, les modes de négociation, etc. S'assurer que les configurations soient les mêmes des deux côtés.
- **politiques de sécurité :** définir les politiques de sécurité de chaque côté pour le trafic VPN, notamment les règles de pare-feu et les restrictions d'accès.
- **mode routeur et transparent :** choisir le mode de fonctionnement souhaité, soit le mode routeur (route-based) où le trafic est acheminé via le VPN, soit le mode transparent (policy-based) où le trafic est filtré en fonction des politiques de sécurité.
- **test et débogage :** une fois la configuration terminée, effectuer des tests pour vous assurer que le tunnel VPN fonctionne correctement. Vérifier les journaux systèmes et utiliser les outils de débogage pour diagnostiquer et résoudre les éventuels problèmes.

3.1.2 Architecture de réseau

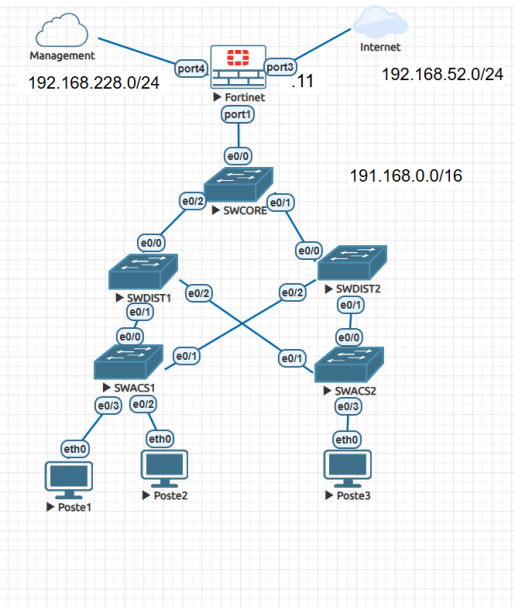
Dans le but de répondre aux besoins en terme de sécurité de MAPCOM TECHNOLOGIES, il s'avère nécessaire de bien disposer les équipements du réseau afin d'offrir un niveau de sécurité élevé. Ainsi l'architecture du réseau que nous proposons dans le cadre de notre projet se présente comme suit :

TABLE 3.1 : Légende des équipements du réseau

Équipement	**Rôle**	**Site**
Routeur FortiGate (FGB)	Routeur principal	Bénin
Routeur FortiGate (FGT)	Routeur principal	Togo
Switch Core (SWCORE)	Distribution centrale	Bénin, Togo
Switch Distribution (SWDIST1, SWDIST2)	Répartition réseau	Bénin, Togo
Switch Accès (SWACC1, SWACC2)	Connexion des utilisateurs	Bénin, Togo
Serveur Windows (Winserver)	Hébergement de services	Bénin
Stations Utilisateurs	Postes de travail (PC1-4, Poste1-3)	Bénin, Togo



(a) Architecture du réseau du Bénin



(b) Architecture du réseau du Bénin

FIGURE 3.1 : Architecture réseau

Pour le déploiement de notre solution, nous avons utilisé deux machines virtuels EVE-NG, représentant les deux sites. Comme on peut le voir sur la figure 3.1, une architecture à trois niveaux (core, distribution et accès) a été retenue pour les deux réseaux. Cette architecture est conçue pour les petites et moyennes entreprises, permettant une interconnexion sécurisée entre deux sites distants. Elle se compose des éléments suivants :

- **le réseau interne (LAN ou zone verte)** : ce réseau inclut les ordinateurs locaux du personnel sur chaque site. Ici, on retrouve les postes de travail des utilisateurs sur les réseaux du site du Bénin et du site du Togo. Au niveau des réseaux locaux, les switches sont disposés de sorte à assurer la redondance et renforcer la sécurité du réseau, maintenant ainsi la disponibilité même en cas de panne d'un composant.

- **les pare-feu Fortigate (FGB et FGT)** : chaque site est équipé d'un pare-feu Fortigate, qui joue un rôle central dans la sécurisation des échanges entre les deux réseaux locaux. Les pare-feu gèrent le tunnel VPN site-à-site, permettant aux réseaux internes de communiquer de manière sécurisée. Ces pare-feu sont connectés aux adresses IP publiques fournies par l'ISP, facilitant l'interconnexion sécurisée entre les deux sites.

- **DMZ(Zone démilitarisée)** : cette zone abrite les serveurs qui peuvent être exposés, tels que les serveurs web, DNS, ou de messagerie. Dans notre cas, cette zone n'héberge qu'un serveur IIS(Internet Information Services) qui héberge des applications métiers, des informations clients etc

Pour faciliter l'administration, des liens de management sont reliés aux pare-feu Fortigate, permettant de les connecter à une carte réseau virtuelle et d'accéder à leur interface graphique. Nous avons également relié nos réseaux à un cloud qui à son tour a été relié à l'un des réseaux de notre carte virtuelle (vmnet2) qui a servi de routeur pour l'interconnexion des deux machines. Cette configuration permet un accès direct et sécurisé aux pare-feu pour la gestion et la surveillance du réseau.

3.1.3 Tableau du plan d'adressage

TABLE 3.2 : Plan d'adressage

Nom	Adresse
Réseau LAN Bénin	191.168.0.0/16
Réseau LAN Togo	192.168.10.0/24
Réseau DMZ	169.254.162.0/16
Réseau WAN Bénin et Togo	192.168.52.0/24
Réseau Management	192.168.228.0/24

3.2 Configuration des équipements de notre réseau

3.2.1 Configuration de bases des pare-feux Fortigate

Dans notre architecture, les pare-feux Fortigate jouent un rôle central dans les transmissions entre les différents réseaux (LAN, DMZ, VPN et WAN). Ils assurent la sécurité des communications en filtrant le trafic, en appliquant des règles de sécurité, et en gérant les connexions entre les sites distants. Nous allons donc débuté notre travail par la configuration de ces deux équipements.

3.2.1.1 Configuration du pare-feu FGB(Fortigate Benin)

Nous allons commencer par configurer les identifiants d'accès à notre FGB en utilisant **admin** comme username et **Passw0rd** comme password. Nous allons ensuite configurer l'interface management relié au port4 et le WAN relié au port3 de notre FGB en mode afin de connecter l'équipement à la carte réseau de notre machine pour pouvoir accéder à l'interface graphique du Fortigate.

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port4
FortiGate-VM64-KVM (port4) # set mode dhcp
FortiGate-VM64-KVM (port4) # set allowaccess ping http https ssh
FortiGate-VM64-KVM (port4) # set alias "Management"
FortiGate-VM64-KVM (port4) # next
FortiGate-VM64-KVM (interface) # edit port3
FortiGate-VM64-KVM (port3) # set  mode dhcp
FortiGate-VM64-KVM (port3) # set allowaccess ping http https ssh
FortiGate-VM64-KVM (port3) # set alias "WAN"
FortiGate-VM64-KVM (port3) # set role wan
FortiGate-VM64-KVM (port3) # next
FortiGate-VM64-KVM (interface) # end
```

```
FortiGate-VM64-KVM # diagnose ip address list
IP=192.168.52.10->192.168.52.10/255.255.255.0 index=5 devname=port3
IP=192.168.228.133->192.168.228.133/255.255.255.0 index=6 devname=port4
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=7 devname=root
IP=10.255.1.1->10.255.1.1/255.255.255.0 index=11 devname=fortilink
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=12 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=14 devname=vsys_fgfm
```

FIGURE 3.2 : Configuration de l'interface "Management" et "WAN" en ligne de commande(CLI)

En se référant à la figure 3.2, l'adresse IP (192.168.228.133) permet d'accéder à la page d'authentification du Fortigate et l'interface WAN est configuré sur 192.168.52.10.

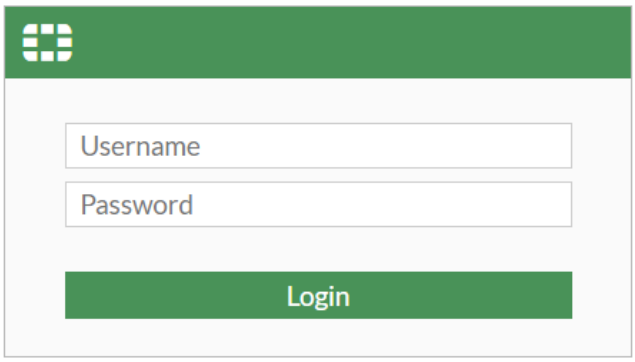


FIGURE 3.3 : Page web d'authentification du Fortigate

Après avoir entré cette adresse dans le navigateur web nous accédons à l'interface de la figure 3.3 où nous devrons entrer les identifiants configurer précedemment dans la CLI.

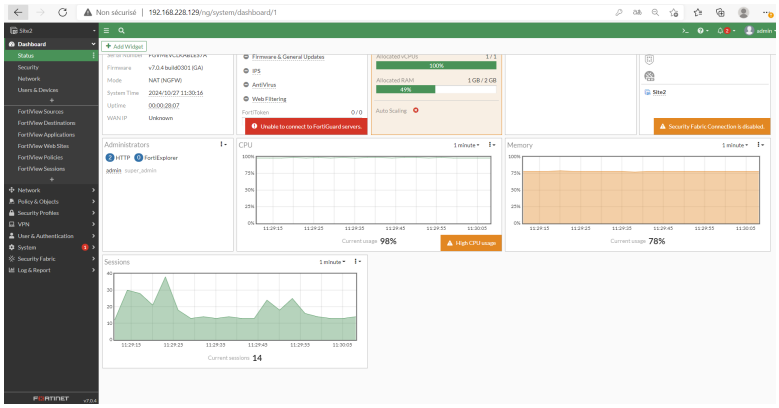


FIGURE 3.4 : Tableau de bord Fortigate

Une fois ces étapes passées, nous accédons au tableau de bord Fortigate comme sur la figure 3.4. Sur ce tableau de bord, nous avons sur notre gauche en noir le menu qui va nous permettre de naviguer sur la page. En haut en vert nous avons l'en-tête qui contient la barre de recherche, le console, l'aide, les notifications et le profil admin. Et au milieu de tout ça se trouve des widgets qui présente le résumé des performances et les statiques du trafic.

Maintenant que nous pouvons naviguer facilement sur l'interface graphique de notre fortigate, il est tant de passer à la configuration des autres ports de notre pare-feu.

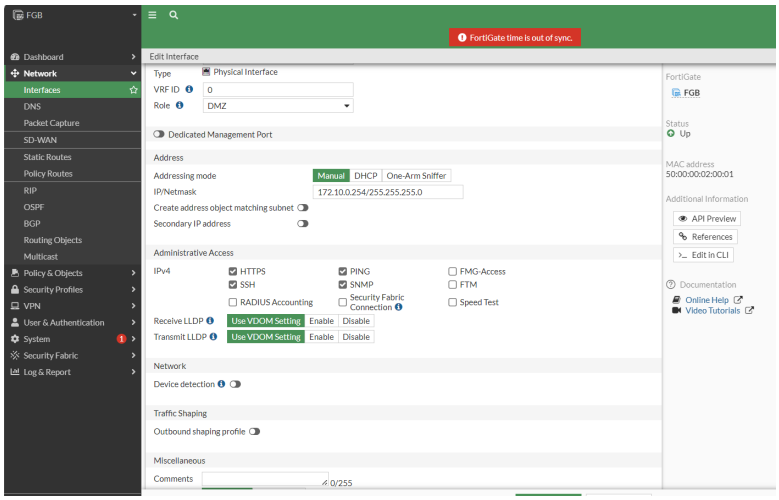


FIGURE 3.5 : Configuration port2(DMZ)

Ensuite nous avons configuré le port2 du Fortigate relié à la zone démilitarisé où se trouve le serveur sur l'adresse IP 169.254.162.254/16 comme indiqué dans la figure **??**.

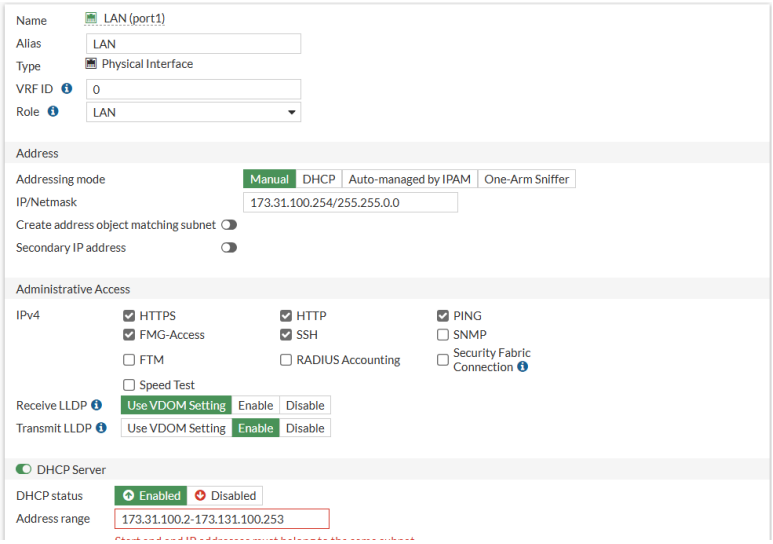


FIGURE 3.6 : Configuration port1(LAN)

Enfin nous avons configuré le port1 relié au réseau local LAN du site du Bénin avec l'adresse IP 173.31.100.254/24 comme indiqué sur la figure 3.6 pour finaliser les configurations de bases de notre pare-feu FGB.

3.2.1.2 Configuration du pare-feu FGT(Fortigate Togo)

Comme nous l'avions faire le pare-feu précédent, nous allons reprendre le même processus sur celui-ci aussi. Nous allons commencer par configurer les identifiants d'accès à notre FGB en utilisant **admin** comme username et **Passw0rd** comme password ; il est recommandé par Fortinet que les deux Fortigates soient configurés de la même façon pour faciliter l'interconnexion. Nous allons ensuite configurer l'interface management relié au port4 et le WAN relié au port3 de notre FGT en mode afin de connecter l'équipement à la carte réseau de notre machine pour pouvoir accéder à l'interface graphique du Fortigate.

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port4
FortiGate-VM64-KVM (port4) # set mode dhcp
FortiGate-VM64-KVM (port4) # set allowaccess ping http https ssh
FortiGate-VM64-KVM (port4) # set alias "Management"
FortiGate-VM64-KVM (port4) # next
FortiGate-VM64-KVM (interface) # edit port3
FortiGate-VM64-KVM (port3) # set  mode dhcp
FortiGate-VM64-KVM (port3) # set allowaccess ping http https ssh
FortiGate-VM64-KVM (port3) # set alias "WAN"
FortiGate-VM64-KVM (port3) # set role wan
FortiGate-VM64-KVM (port3) # next
FortiGate-VM64-KVM (interface) # end
```

```
FortiGate-VM64-KVM # diagnose ip address list
IP=192.168.228.136->192.168.228.136/255.255.255.0 index=5 devname=port3
IP=192.168.228.134->192.168.228.134/255.255.255.0 index=6 devname=port4
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=7 devname=root
IP=10.255.1.1->10.255.1.1/255.255.255.0 index=11 devname=fortilink
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=12 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=14 devname=vsys_fgfm
```

FIGURE 3.7 : Configuration de l'interface "Management" et "WAN" en ligne de commande(CLI)

Comme le montre la figure 3.7, l'adresse IP pour accéder à l'interface web du Fortigate est le 192.168.228.134. En entrant cette adresse dans notre navigateur, nous pouvons accéder à permettant d'accéder à la page d'authentification du Fortigate, entrez les identifiants pour accéder au tableau afin de démarrer les configurations des autres interfaces de notre fortigate comme fait précedemment.

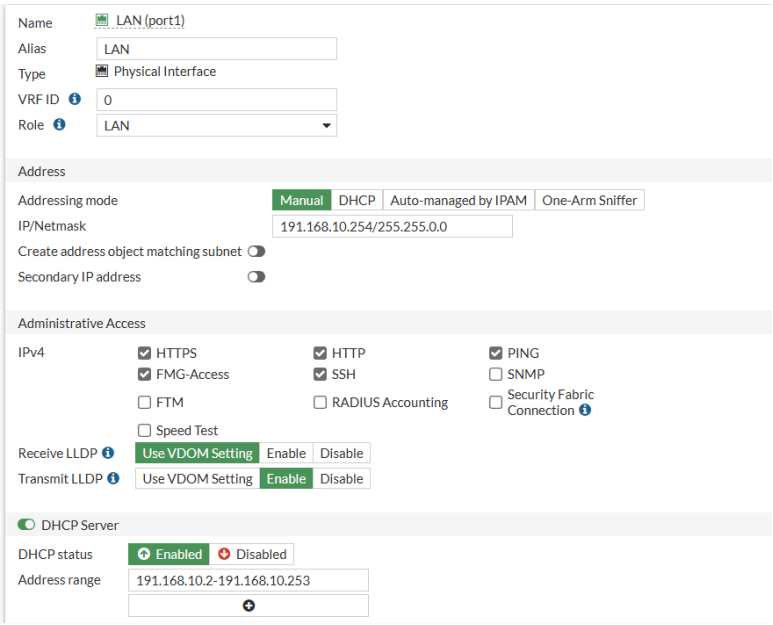


FIGURE 3.8 : Configuration port1(LAN)

Nous passons maintenant à la configuration du port1 relié au réseau local LAN du site de Togo avec l'adresse IP 191.168.0.0.254/16 comme indiqué sur la figure 3.8 pour finaliser les configurations de bases de notre pare-feu FGT.

3.2.2 Installation et configuration du server IIS

Danz le cadre de ce travail, nous allons installé un serveur IIS pour stocker les informations clients, les applications métiers et toutes les données importantes de l'entreprise.

Nous avons opté pour Windows Server 2022 parce que c'est la version la plus récente, offrant des améliorations en sécurité (TLS 1.3, Defender ATP), en performance (HTTP/3, TCP optimisé) et en haute disponibilité (Failover Clustering, Load Balancing). Il est donc plus adapté pour un serveur IIS sécurisé et performant.

Pour commencer, nous allons installé le serveur Windows dans EVE-NG en suivant les étapes de la vidéo [11] avant de lancer le **Gestionnaire de serveur** pour l'installation du service IIS.

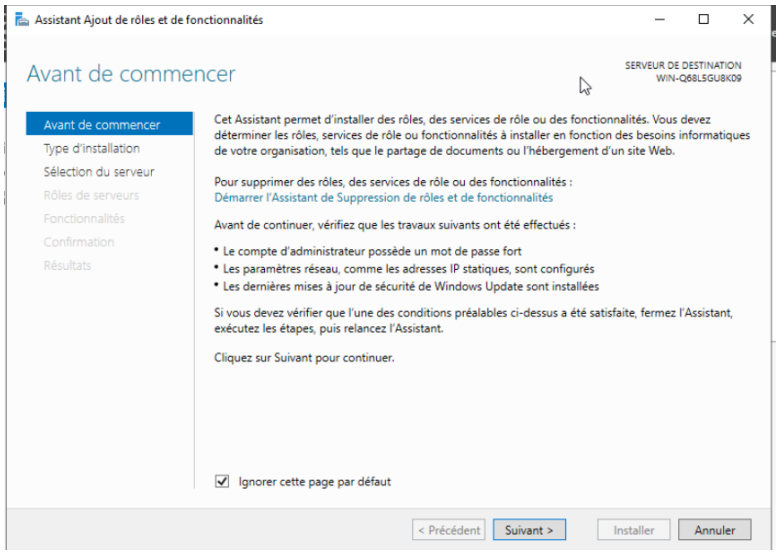


FIGURE 3.9 : Avant de commencer

Ensuite, nous allons choisir l'option **Ajouter des rôles et des fonctionnalités** qui nous renvoie vers la page de la figure 3.9 où l'assistant explique les vérifications à effectuer avant l'installation (mot de passe administrateur, configuration réseau et mises à jour).

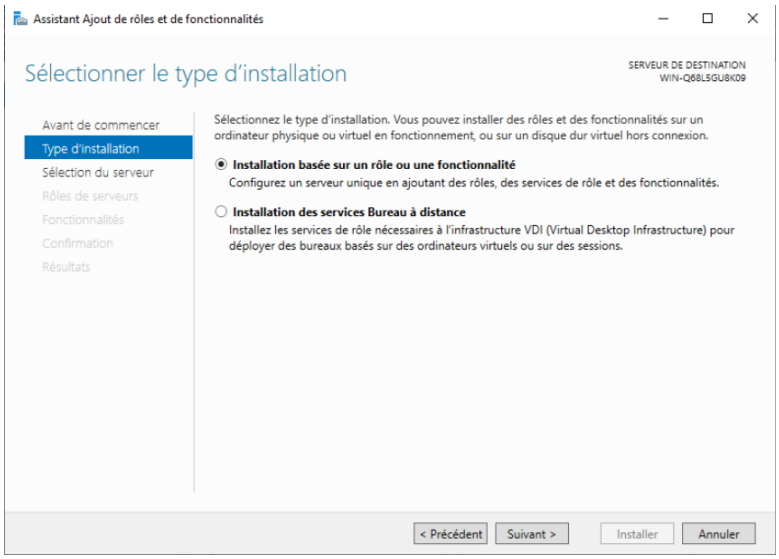


FIGURE 3.10 : Choix du type d'installation

Passer cette étape, nous avons sélectionné l'installation basée sur un rôle ou une fonctionnalité pour configurer un serveur unique, comme sur la figure 3.10. Cliquez sur Suivant pour poursuivre.

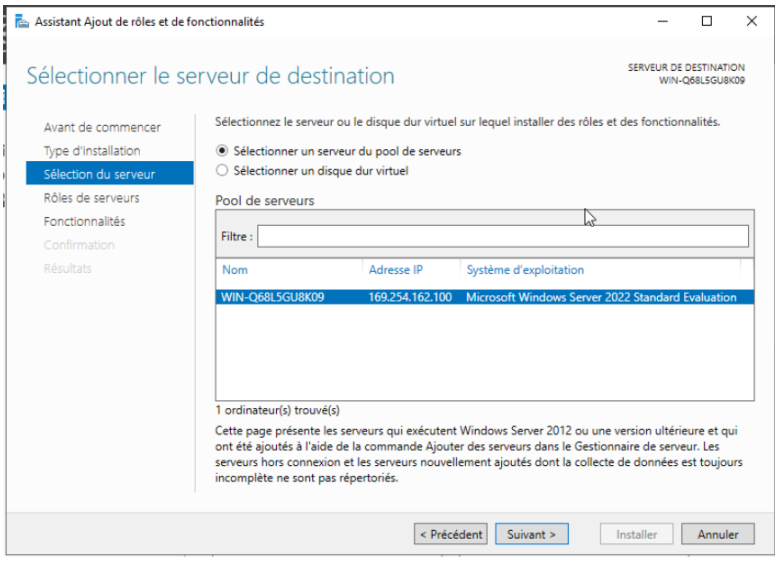


FIGURE 3.11 : Choix du serveur de destination

Ici, il faut choisir le serveur de destination identifié par son adresse IP et son système d'exploitation pour installer les rôles comme sur la figure 3.11. Cliquez sur Suivant pour continuer.

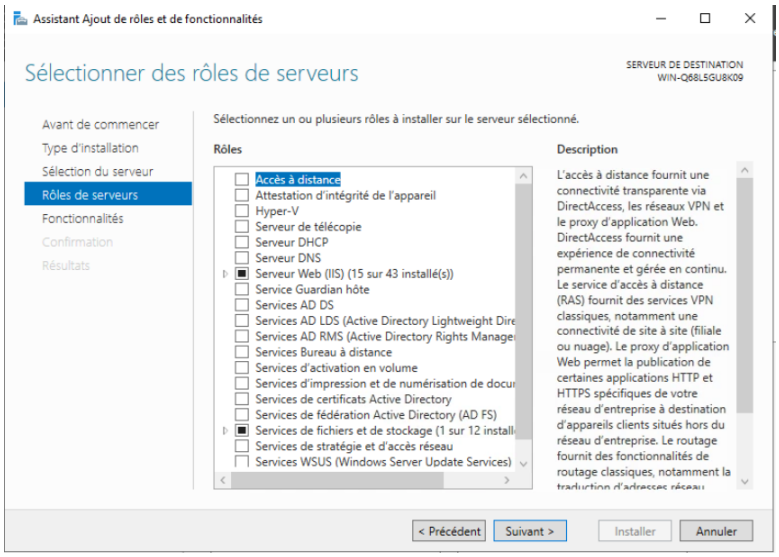


FIGURE 3.12 : Choix des rôles de serveurs

La figure 3.12 présente une liste des rôles de serveur disponibles, comme les Services Bureau à distance, le serveur Web (IIS) et les Services de fichiers et de stockage, ainsi que leurs descriptions. Nous allons choisir ceux qui conviennent pour le serveur IIS, les installer et cliquer sur suivant pour aller à l'étape suivante.

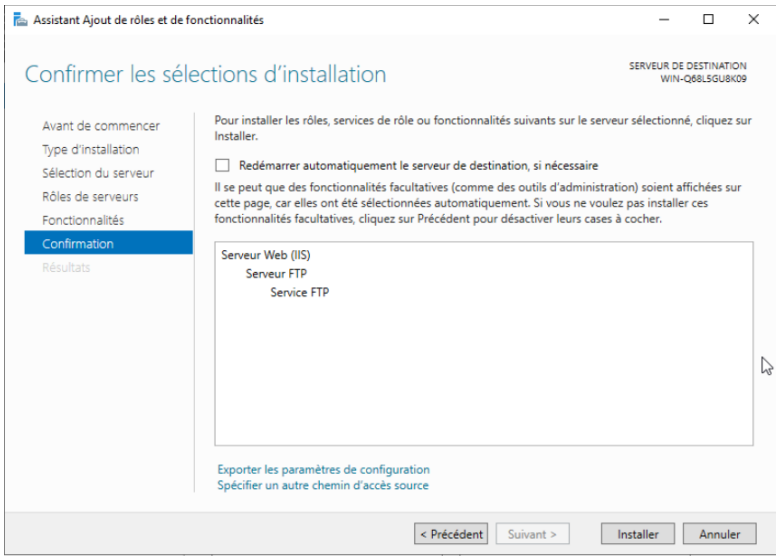


FIGURE 3.13 : Confirmation des rôles choisis

Enfin, c'est le moment de confirmer l'installation des rôles, services ou fonctionnalités sur notre serveur comme sur la figure 3.13. Si par mégarde, des erreurs avaient été commises durant le processus, c'est le moment de les corriger avant d'installer le service.

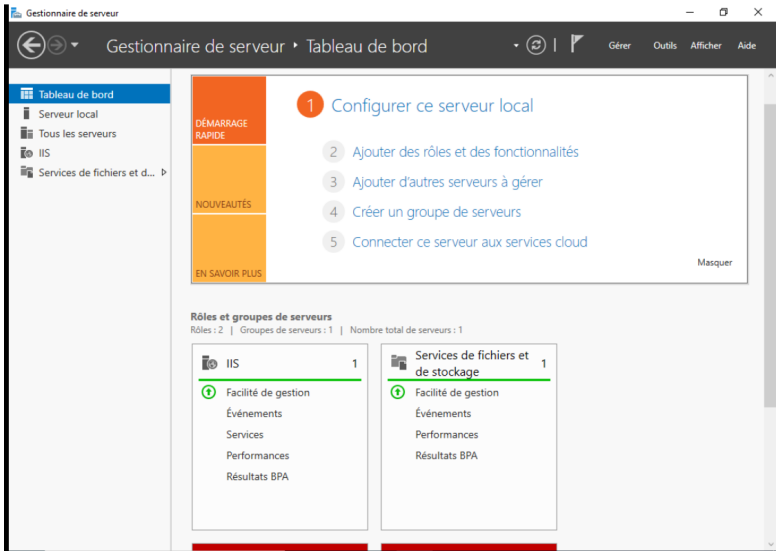


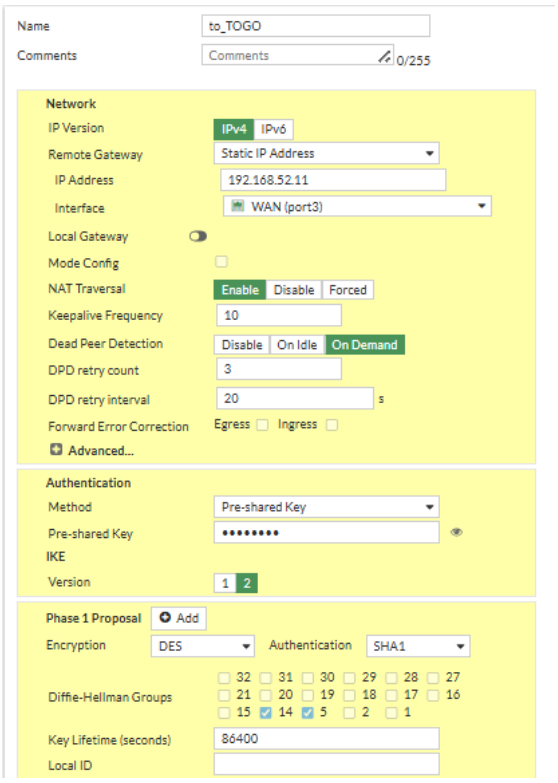
FIGURE 3.14 : Serveur IIS installé

Sur la figure 3.14, notre serveur a été bien installé.

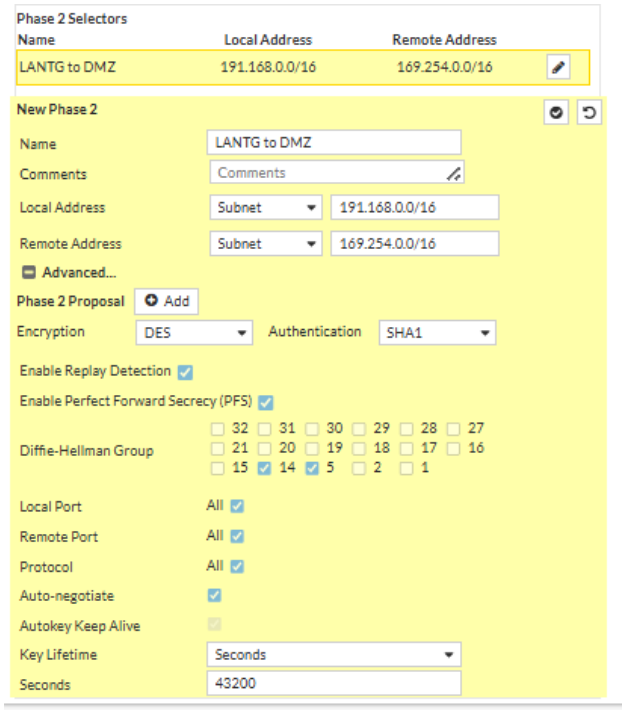
3.2.3 Création du VPN site à site

3.2.3.1 Sur le site du Bénin

- Création du tunnel IPSEC
  Ce tunnel va gérer le trafic réseau de la Direction Générale (Bénin) vers l'agence de TOGO.



(a) Phase1 de la configuration du tunnel VPN

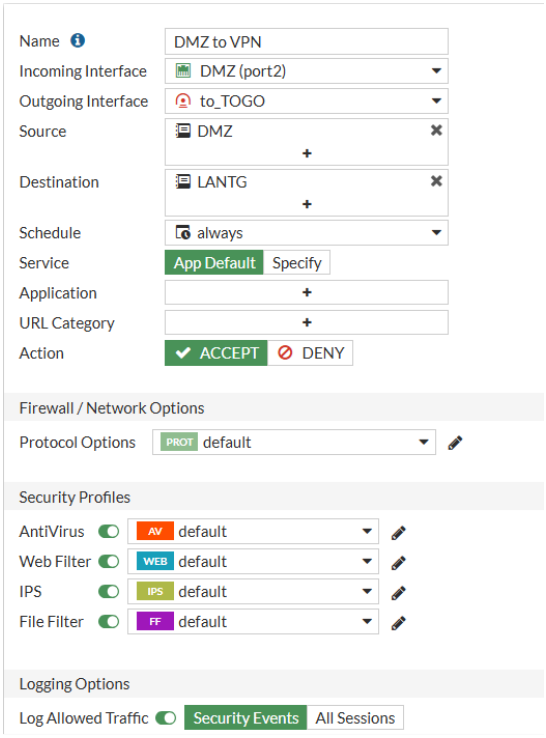


(b) Phase1 de la configuration du tunnel VPN

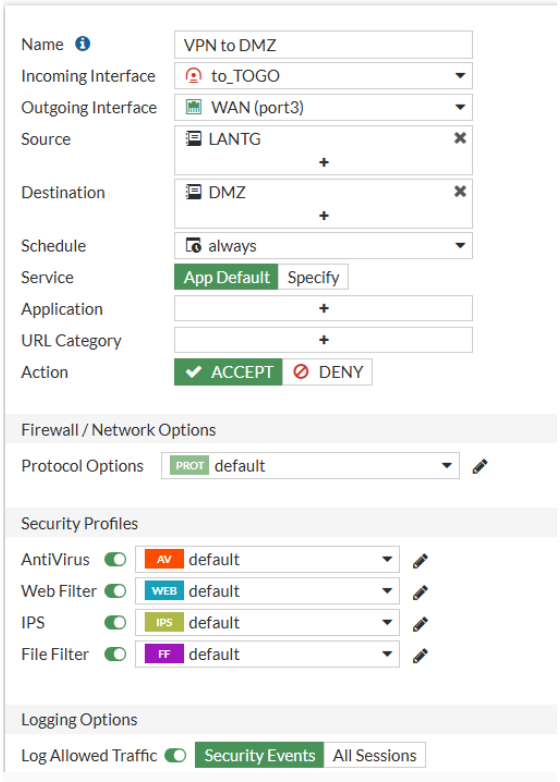
FIGURE 3.15 : Création du tunnel IPSEC(Bénin vers Togo) sur le FGB

Comme l'indique la figure 3.15, nous avons configuré le tunnel IPSEC entre les deux réseaux DMZ(169.254.0.0/16) et le LAN du site de TOGO(191.168.0.0/16) sortant parle port3(WAN) du fortigate et utilisant le 192.168.52.11(adresse IP publique du Fortigate distant).

- Création de la politique du pare-feu pour autoriser le trafic du DMZ vers internet



(a) Autorisation du trafic de la DMZ vers le VPN



(b) Autorisation du trafic de la VPN vers le DMZ

FIGURE 3.16 : Créaton des règles de pare-feu pour autoriser le trafic au travers du tunnel VPN

Sur la figure 3.16, nous pouvons voir que le trafic du réseau DMZ(169.254.0.0/16) contenant le serveur vers le réseau local du site de Togo(191.168.0.0/16) au travers du tunnel VPN, a été autorisé ainsi que d'autres services comme le filtrage web, le système de prévention des intrusions(IPS), l'antivirus et le filtrage des fichiers pour plus de sécurité.

- Création de la route statique du DMZ vers le VPN

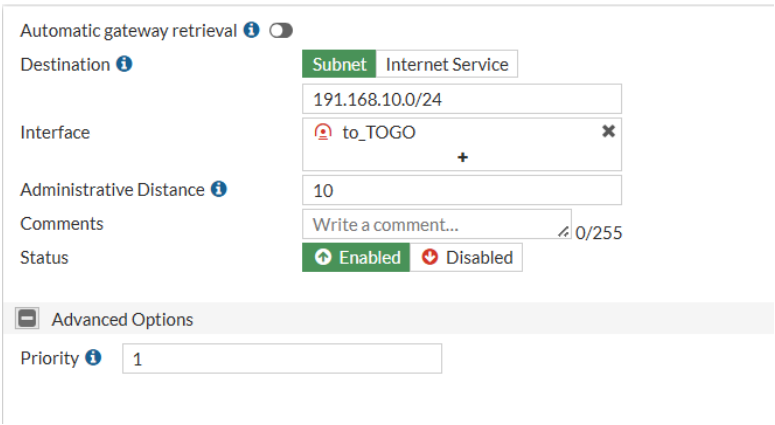
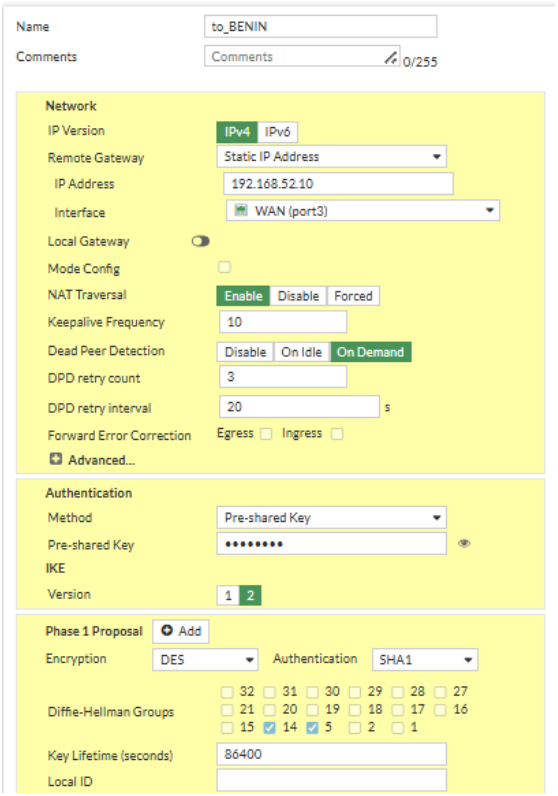


FIGURE 3.17 : Créaton de la route statique pour autoriser le trafic au travers du tunnel VPN

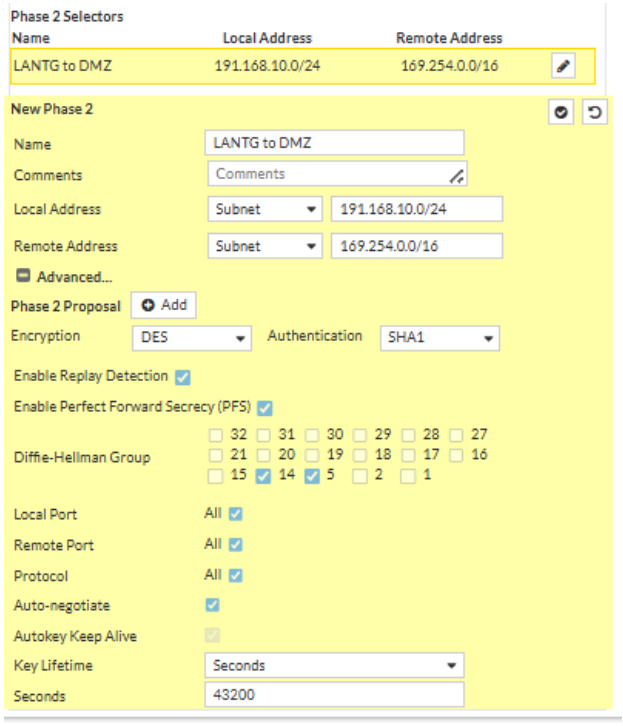
La route de la figure 3.17 permet d'acheminer le trafic vers le réseau LAN du Togo à travers le tunnel VPN avec une priorité de 1.

3.2.3.2 Sur le site du Togo

- Création du tunnel IPSEC
  Ce tunnel va gérer le trafic réseau de l'agence de Togo vers la Direction générale (Bénin).



(a) Phase1 de la configuration du tunnel VPN

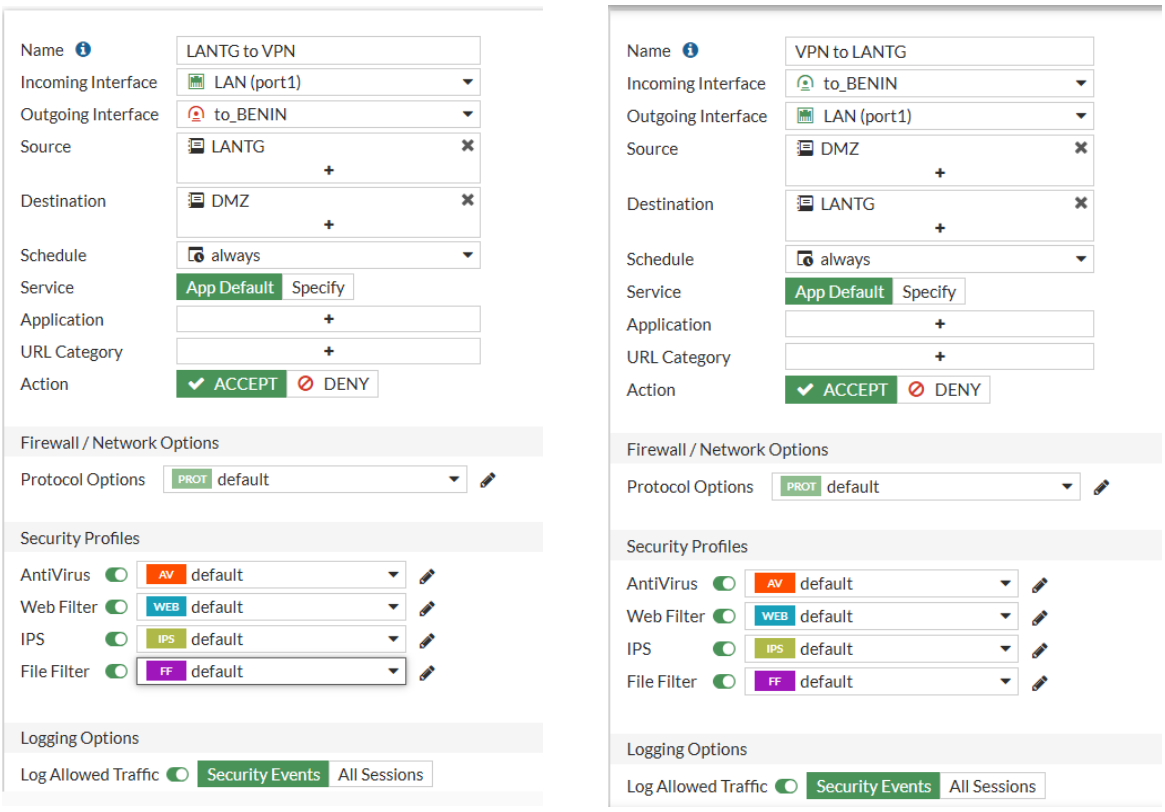


(b) Phase1 de la configuration du tunnel VPN

FIGURE 3.18 : Création du tunnel IPSEC(Togo vers Bénin) sur le FGT

Comme l'indique la figure 3.18, nous avons configuré le tunnel IPSEC entre les deux réseaux le LAN du site de TOGO(191.168.0.0/24) et DMZ(169.254.0.0/16) sortant parle port1(WAN) du fortigate et utilisant le 192.168.52.10(adresse IP publique du Fortigate distant).

- Création de la politique du pare-feu pour autoriser le trafic du LAN vers internet



(a) Autorisation du trafic du LAN vers le VPN (b) Autorisation du trafic du VPN vers le LAN

FIGURE 3.19 : Créaton des règles de pare-feu pour autoriser le trafic au travers du tunnel VPN

Sur la figure 3.16, nous pouvons voir que le trafic du réseau local du site de Togo(191.168.0.0/24) vers la DMZ(169.254.0.0/16) du site du Bénin au travers du tunnel VPN, a été autorisé ainsi que d'autre services comme le filtrage web, le système de prévention des intrusions(IPS), l'antivirus et le filtrage des fichiers pour plus de sécurité.

- Création de la route statique du LAN du site de TOGO vers le VPN

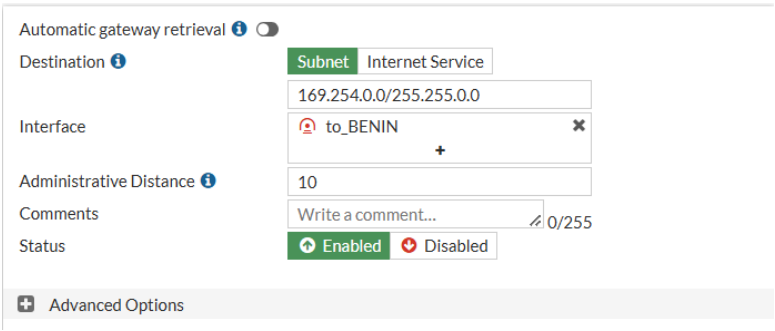
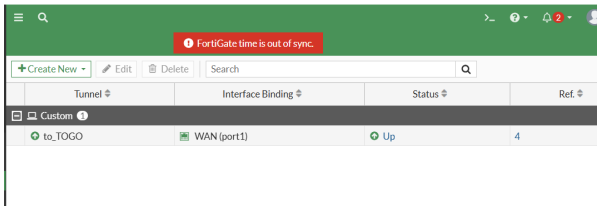


FIGURE 3.20 : Créaton de la route statique pour autoriser le trafic au travers du tunnel VPN

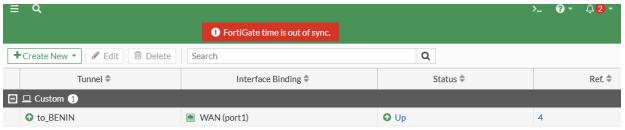
La route de la figure 3.20 permet d'acheminer le trafic vers le serveur du Bénin à travers le tunnel VPN avec une priorité de 1.

3.3 Résultats obtenus

Avant de terminer ce travail, nous allons montrer quelques constats faits après les configurations faites.



(a) VPN vers Togo en mode UP

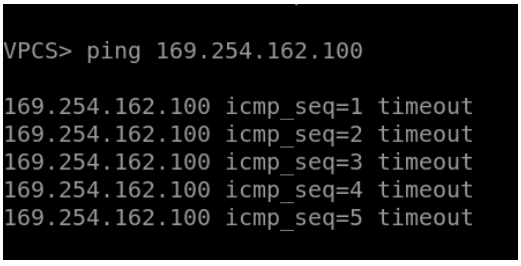


(b) VPN vers Bénin en mode UP

FIGURE 3.21 : VPN en mode UP après configuration

Après toutes les configurations, le statut du VPN sur chacun des Fortigate change de Down à UP comme dans la figure 3.21.

Maintenant, nous allons passer à l'étape des tests pour s'assurer que les deux réseaux communiquent normalement. Pour ça, nous allons faire des tests de ping entre les deux réseaux.



(a) Ping vers le serveur depuis l'un des postes du LAN Togo



(b) Ping du serveur vers l'un des postes du LAN Togo

FIGURE 3.22 : Vérification de la connexion par ping

Sur la figure 3.22, nous pouvons voir que le ping du serveur IIS vers le LAN de Togo passe normalement mais celui vers le serveur ne passe pas comme souhaité ; surement dûe à un problème de politique de sécurité. Jetons donc un coup d'oeil au serveur.

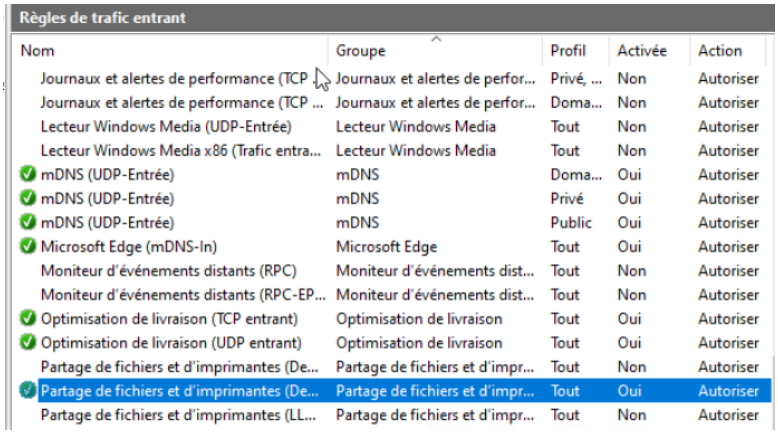


FIGURE 3.23 : Autorisation du trafic ICMPv4 entrant sur le serveur

La règle autorisant le trafic ICMPv4 entrant sur le serveur n'est pas activé. Nous l'avons donc activé comme sur la figure 3.23. Allons maintenant vérifier si nos pings passent comme cela se doit.

```
VPCS> ip dhcp
DDORA IP 192.168.10.3/24 GW 192.168.10.254

VPCS> ping 169.254.162.254

84 bytes from 169.254.162.254 icmp_seq=1 ttl=254 time=57.511 ms
84 bytes from 169.254.162.254 icmp_seq=2 ttl=254 time=27.773 ms
84 bytes from 169.254.162.254 icmp_seq=3 ttl=254 time=29.140 ms
84 bytes from 169.254.162.254 icmp_seq=4 ttl=254 time=26.702 ms
84 bytes from 169.254.162.254 icmp_seq=5 ttl=254 time=22.882 ms
```

FIGURE 3.24 : Ping du LAN du Togo vers le serveur

Sur la figure 3.24, nous pouvons voir que le ping vers le serveur IIS passe désormais sans problème.

3.4 Discussion

Le déploiement du VPN site-à-site entre les filiales béninoise et togolaise de MAPCOM Technologies a permis d'établir une communication sécurisée entre les deux sites. Grâce au protocole IPSec et aux équipements FortiGate, les échanges de données sensibles sont protégés, et les employés peuvent accéder aux ressources hébergées sur le serveur IIS de la direction générale. Toutefois, bien que cette solution réponde aux besoins actuels, elle présente des limites qui pourraient impacter la croissance de l'entreprise.

Tout d'abord, le VPN site-à-site est limité à la connexion entre deux sites à la fois. Or, MAPCOM Technologies possède plusieurs filiales et pourrait en ouvrir d'autres à l'avenir. Cette architecture deviendra rapidement difficile à gérer, car chaque nouvelle interconnexion nécessiterait un tunnel VPN distinct. De plus, FortiGate ne permet le déploiement que d'un seul VPN, ce qui rend la solution peu évolutive. Actuellement, l'entreprise ne peut pas interconnecter directement tous ses sites, ce qui freine la fluidité des échanges et la centralisation des ressources.

Ensuite, la fiabilité du VPN dépend fortement de la qualité des connexions Internet locales. Une panne ou une dégradation de la bande passante chez l'un des fournisseurs impacte directement la communication entre les sites entrainant une latence.

Enfin, une transition vers un **VPN centralisé évolutif** ou une solution **SD-WAN** avancée permettrait à MAPCOM Technologies d'assurer une connectivité plus flexible et adaptée à sa croissance.

Conclusion

Notre solution VPN site-à-site a permis de répondre efficacement aux besoins de l'entreprise MAPCOM TECHNOLOGIES en interconnectant les filiales du Bénin et du Togo et en garantissant un transfert sécurisé des données sensibles hébergées sur le serveur IIS de la direction générale du Bénin. Cela permet à MAPCOM TECHNOLOGIES de bénéficier d'une communication intersite fiable et confidentielle, favorisant ainsi une meilleure collaboration et un accès optimisé aux ressources critiques.

Conclusion Générale

Le déploiement d'un VPN site-à-site entre les filiales de MAPCOM TECHNOLOGIES au Bénin et au Togo représente une solution technique efficace et sécurisée pour résoudre les défis liés au partage des données sensibles hébergées sur le serveur IIS de la direction générale du Bénin. Face aux contraintes budgétaires, notamment l'acquisition d'un second serveur pour le site du Togo, cette solution permet de centraliser les ressources tout en évitant des investissements supplémentaires conséquents.

L'adoption de la solution FortiGate de Fortinet, appuyée par le protocole IPsec, s'est imposée grâce à ses atouts en matière de sécurité, de fiabilité et de performance. Le chiffrement des communications garantit la confidentialité et l'intégrité des données échangées, tandis que la solution elle-même se distingue par sa facilité de gestion et sa capacité à évoluer avec les besoins futurs de l'entreprise.

Le processus de déploiement, allant de l'analyse des besoins à la configuration des équipements et aux tests de validation, a permis d'obtenir une interconnexion stable, sécurisée et transparente pour les utilisateurs finaux. Ce projet nous a permis de développer des compétences techniques approfondies, renforçant notre expertise en cybersécurité et en gestion des réseaux.

Perspectives

Bien que le déploiement du VPN ait été un succès, certains défis restent à anticiper. Il est essentiel de garantir la pérennité du réseau ainsi qu'une évolutivité avec les besoins de l'entreprise. Nous proposons donc aux entreprises disposant plus de deux sites de :

- mettre en place un VPN multi-sites basé sur une architecture hub-and-spoke pour faciliter l'interconnexion des filiales ;
- ou d'intégrer une solution SD-WAN pour une gestion plus intelligente du trafic et une meilleure résilience en cas de panne ;
- et d'optimiser les performances du trafic en utilisant le QoS afin de réduire la latence et d'améliorer l'expérience utilisateur.

Bibliographie

[1] Jean-Paul ARCHIER *Les VPN fonctionnement, mise en œuvre et la maintenance des Réseaux privés virtuel*, Juin 2010.

[2] Whitman, M. E. and Mattord, H. J *Principles of Information Security*, 2017.

[3] Guy PUJOLLE *Les réseaux*, 2014.

[4] Guillaume Desgeorge, La sécurité des réseaux, Cour, 2000.

[5] Ofer Shmueli, Fortigate Firewall Admin Pocket Guide, janvier 2021.

Webographie

[6] https://www.axis-solutions.fr/quest-ce-quun-pare-feu-et-quel-est-son-role/, Consulté dernièrement en août 2024

[7] https://www.generation-nt.com/actualites/vpn-securite-internet-1967963 https://www.avast.com/fr-fr/c-what-is-a-vpn https://surfshark.com/fr/blog/vpn-protocols, Consulté dernièrement en août 2024

[8] https://www.alliance-informatique.fr/revue-blog/qu-est-ce-qu-un-vpn-et-comment-ca-fonctionne/, Consulté dernièrement en août 2024

[9] https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/913287/basic-site-to-site-vpn-with-pre-shared-key, Consulté dernièrement en septembre 2024

[10] https://www.it-connect.fr/creation-dune-regle-de-pare-feu-avec-un-fortigate/, Consulté dernièrement en septembre 2024

[11] https://youtu.be/JGhAAvl3WAA, Consulté dernièrement en septembre 2024

[12] https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html, Consulté dernièrement en septembre 2024

[13] https://www.paloaltonetworks.com/network-security/next-generation-firewall, Consulté dernièrement en septembre 2024

[14] https://www.sophos.com/en-us/products/next-gen-firewall, Consulté dernièrement en septembre 2024

[15] https://www.eve-ng.net/index.php/documentation/howtos/, Consulté dernièrement en novembre 2024

[16] https://winscp.net/eng/docs/lang:fr#google_vignette, Consulté dernièrement en novembre 2024

[17] https://en.m.wikipedia.org/wiki/File:Vmware_workstation_16_icon.svg, Consulté dernièrement en novembre 2024

[18] https://www.securiteinfo.com/cryptographie/IPSec.shtml, Consulté dernièrement en novembre 2024

[19] https://www.afapdp.org/wp-content/uploads/2018/06/Benin-Loi-2017-20-Portant-code-du-numerique-en-Republique-du-Benin.pdf, Consulté dernièrement en novembre 2024

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

. iv

Abstract v

. v

Table des figures vi

Liste des tableaux viii

Liste des acronymes ix

Introduction 1

1 Etat de l'art 3

Introduction 3

1.1 La sécurité informatique 3

1.1.1 Les enjeux de la sécurité informatique 4

1.1.2 Les mécanismes de protection d'un réseau informatique 4

1.1.2.1 Pare-feu(Firewall) 4

1.1.2.2 Contrôle d'accès(Access Control) 5

1.1.2.3 Chiffrement(Encryption) 5

1.1.2.4 Segmentation du réseau (Network segmentation) 6

1.1.2.5 Système de détection et de prévention des intrusions (IDS/IPS) 6

1.2 Virtual Private Network(VPN) 7

1.2.1 Fonctionnement d'un VPN 7

1.2.2 Différents types de VPN 8

1.2.2.1 VPN d'accès à distance 8

1.2.2.2 VPN site-à-site 8

1.2.3 Avantages du VPN 10

1.2.4 Protocoles VPN 10

Conclusion 11

2 Analyse, choix techniques et déploiement de la solution 12

Introduction . . . 12
2.1 Analyse des besoins . . . 12
2.2 Les solutions d'interconnexion de sites distants existants . . . 14
2.2.1 Etude comparatif des solutions d'interconnexion existantes . . . 16
2.2.2 Choix de la solution adéquate . . . 16
2.3 Déploiement de la solution . . . 17
2.3.1 Logiciels et outils utilisés . . . 17
2.3.2 Installation et configuration de EVE-NG . . . 18
Conclusion . . . 21

3 Résultats et discussion **22**
Introduction . . . 22
3.1 Prérequis et architecture réseau . . . 22
3.1.1 Prérequis . . . 22
3.1.2 Architecture de réseau . . . 23
3.1.3 Tableau du plan d'adressage . . . 25
3.2 Configuration des équipements de notre réseau . . . 25
3.2.1 Configuration de bases des pare-feux Fortigate . . . 25
3.2.1.1 Configuration du pare-feu FGB(Fortigate Benin) . . . 25
3.2.1.2 Configuration du pare-feu FGT(Fortigate Togo) . . . 27
3.2.2 Installation et configuration du server IIS . . . 28
3.2.3 Création du VPN site à site . . . 31
3.2.3.1 Sur le site du Bénin . . . 31
3.2.3.2 Sur le site du Togo . . . 34
3.3 Résultats obtenus . . . 36
3.4 Discussion . . . 37
Conclusion . . . 37

Conclusion **38**

Bibliographie **39**

Webographie **40**

Table des matières **42**