République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira. Bejaïa
Faculté des Sciences Exactes
Département Informatique

Mémoire de Fin d'études

En vue de l'obtention du diplôme Master professionnel en Informatique
Spécialité : Administration et sécurité des réseaux

Thème :

Interconnexion de deux sites par une liaison VPN
Cas d'étude : Entreprise Spa TMF AKBOU

Présenté par :
M^elle^ Azoula Djamila

M^elle^ Meziani Sabrina

Encadré par :

M^me^ Khaled Hayette

Devant le jury composé de :
Présidente : M^me^ Ghanem Souhila
Examinatrice : M^me^ Bouadem Nassima

Promotion : 2021/2022

REMERCIEMENTS

Grâce à Dieu ce mémoire a été réalisé, Dieu merci pour le courage et la volonté sans lesquelles notre travail n'aurait jamais pu voir la lumière de ce jour.

Nous exprimons toute notre gratitude à notre promotrice Madame KHALED HAYETTE, pour l'effort fourni, les conseils prodigués, sa patience, son aide précieuse et sa persévérance dans le suivi. Son optimisme inébranlable nous a permis d'avancer sereinement. Qu'elle trouve dans ce travail un hommage vit à sa haute personnalité.

Nous tenons à remercier l'organisme d'accueil de l'entreprise «Spa TMF Logistics-Akbou », qui nous accepté comme stagiaires et qui nous a donné une chance pour découvrir le domaine professionnel. Nous remercions particulièrement notre promoteur de stage Mr BADJADJ YOUSEF pour son accueil, le temps consacré et le partage de son expertise au quotidien, Ainsi, que pour tous les membres et les travailleurs, pour leur accueil et leur sympathie.

Nos vifs remerciements vont également aux membres du jury d'avoir accepté à d'examiner et de juger notre travail.

Nous tenons à remercier également tous les enseignants qui ont contribués de près ou de loin à notre formation universitaire, sans oublier tous les personnes qui nous a aidés à mener à terme notre projet.

Nous remercions fortement tous les membres de nos familles qui nous ont toujours encouragés et soutenus durant toutes nos études.

Enfin, un grand merci à nos parents, pour leur soutien constant, leur présence et la confiance dont ils ont fait preuve.

Dédicaces

Avec un énorme plaisir, un cœur ouvert et une immense joie, que je dédie ce modeste travail :

- à mes très chers et respectueux parents dont je ne saurai comment leur exprimer mes remerciements pour leur encouragement, leur aide, le soutien qu'ils m'ont apporté et Le sacrifice qu'ils ont fait pour moi, durant toutes les années de mes études que Dieu les protège et les entoures de sa bénédiction.

- à tous ceux qui m'aiment et que j'aime autant, mes sœurs et mes frères qui m'ont toujours soutenu et qui étaient présents à mes côtés aux moments difficiles.

- à tous mes ami(es) qui m'ont aidé de près ou de loin, et plus précisément à kahina, et à toute personne m'ayant fait part de son savoir.

Djamila

Dédicaces

Je dédie ce travail à :
A celle qui a toujours attendu ma réussite, à mon vaste abri d'amour et de tendresse, à ma chère mère.
A celui qui a était toujours présent pour m'encourager à aller vers le mieux et le meilleur, à mon père.
A mes chères sœurs et mes chers frères qui m'ont toujours soutenu et qui étaient présents à mes côtés aux moments difficiles.
A ma grand-mère et tous les membres de ma famille.
A tous mes ami(es) qui m'ont aidé de près ou de loin.
A tous qui ont marqué leurs existences dans ma mémoire et que mon stylo n'a pas cité.

Sabrina

TABLE DES MATIÈRES

Remerciements **II**

Liste d'abréviations **XI**

Introduction générale **1**

1 Description de l'organisme d'accueil **3**
1.1 Introduction 3
1.2 Présentation de Spa TMF 3
1.3 Structure de Spa TMF 4
1.4 Présentation du centre informatique 4
1.5 Etude du système informatique existant 4
1.5.1 État des ressources du système informatique 5
1.5.2 Aspect positif du système 8
1.6 Problématique 8
1.7 Solution proposée 9

2 Généralités sur les réseaux informatiques et leur système de sécurité **10**
2.1 Introduction 10
2.2 Définition 10
2.3 Classification des réseaux informatiques 11
2.3.1 Selon l'étendu 11
2.3.2 Selon la topologie 14
2.4 Architecture des réseaux 15
2.4.1 Le modèle OSI 15
2.4.2 Le modèle TCP/IP 16

2.5 Les équipements d'interconnexion 16
2.6 Définition 18
2.7 Principaux concepts de la sécurité informatique 18
2.8 Objectifs de la sécurité 18
2.9 Les attaques 19
2.9.1 Catégories d'attaques 19
2.9.2 Scénarios d'attaques 20
2.9.3 Quelques attaques courantes 20
2.10 Mécanismes de défense 21
2.10.1 Zone Démilitarisée 21
2.10.2 Contrôle d'accès 21
2.10.3 Proxys 22
2.10.4 Chiffrement 22
2.10.5 Pare-feu 22
2.10.6 Antivirus 23
2.10.7 virtual Private Network (VPN) 23
2.11 Conclusion 24

3 Les réseaux privés virtuels 25
3.1 Introduction 25
3.2 Définition d'un réseau privé virtuel (VPN) 26
3.3 Principe de fonctionnement d'un VPN 26
3.4 Objectifs et caractéristiques fondamentaux d'un VPN 26
3.4.1 Authentification d'utilisation 26
3.4.2 Confidentialité de données 27
3.4.3 Gestion de clés 27
3.4.4 Intégrité des données 27
3.4.5 Prise charge multi-protocole 27
3.5 Les types et les catégories d'un VPN 27
3.5.1 VPN d'accès (poste à site) 27
3.5.2 L'intranet VPN (site à site) 28
3.5.3 L'extranet VPN (poste à poste) 29
3.6 Protocoles utilisés pour réaliser une connexion VPN 29
3.6.1 Niveau 2 29
3.6.2 Niveau 3 31
3.6.3 Niveau 4 36
3.7 Conclusion 36

4 Implémentation et réalisation 37

4.1 Introduction 37
4.2 Les logiciels et équipements utilisés 37
4.2.1 Logiciels 37
4.2.2 Équipement requis 40
4.3 La réalisation des deux architectures 40
4.3.1 L'architecture réseau 40
4.3.2 La plage d'adresse 41
4.3.3 Configuration de serveur et de dhcp 42
4.3.4 Configuration de base du Fortigate Spa TMF 46
4.3.5 Création et configuration du VPN IPsec 47
4.3.6 Création et configuration des routes statiques 55
4.3.7 Définition des régles 56
4.3.8 Tests de ping pour la vérification des règles 58
4.4 Vérification du cryptage des données au niveau du tunnel avec Wireshark 59
4.5 Conclusion 62

Conclusion générale 65

Bibliographie 67
Résumé 68

TABLE DES FIGURES

1.1 Organisme de Spa TMF 5
1.2 Réseau local du site Spa TMF-d'AKBOU. 7
1.3 Réseau local du site Spa TMF-d'ALGER. 8

2.1 Classification des réseaux informatique selon leur étendu. 11
2.2 Réseau PAN. 12
2.3 Réseau LAN. 12
2.4 Réseau MAN. 13
2.5 Réseau WAN. 13
2.6 Déférence entre le modèle OSI et le modèle TCP/IP 16

3.1 Le VPN d'accès poste à site. 28
3.2 L'intranet VPN site à site. 29
3.3 L'extranet VPN poste à poste. 29
3.4 En-tête AH. 32
3.5 En-tête ESP 33

4.1 L'interface Gns3. 38
4.2 L'interface Vmware workstation. 39
4.3 L'interface Wireshark. 40
4.4 Architecture réseaux réaliser 41
4.5 Tableau de la plage d'adressage. 41
4.6 Configuration static de serveur d'AKBOU. 42
4.7 Spécification du nom pour l'étendu. 43
4.8 La plage d'adresse IP de distribution du Serveur 43
4.9 La plage d'adresse IP d'exclusion de Serveur 44
4.10 La durée du bail 44
4.11 Ajout de l'adresse de la passerelle. 45
4.12 L'ajout de l'adresse de Serveur DNS et le nom de domaine. 46

4.13 La configuration basique des deux sites. 46
4.14 L'étape VPN setup. 48
4.15 L'étape d'authentification. 48
4.16 L'étape de plicy et routing. 49
4.17 Configuration de la phase une de site Spa TMF-AKBOU. 50
4.18 Configuration de la phase deux de site Spa TMF-AKBOU. 51
4.19 L'étape vpn setup. 52
4.20 L'étape d'authentification. 52
4.21 L'étape Policy et Routing. 53
4.22 Configuration de la phase une de site Spa TMF-ALGER. 54
4.23 Configuration de la phase deux de site Spa TMF-ALGER. 55
4.24 La création de la route statique site Spa TMF-AKBOU. 56
4.25 La création de la route statique site Spa TMF-ALGER. 56
4.26 Les règles coté Spa TMF-AKBOU. 57
4.27 Les règles coté Spa TMF-ALGER. 57
4.28 Test de ping vers le site Spa TMF-AKBOU. 58
4.29 Test de ping vers le site Spa TMF-ALGER. 59
4.30 Les données cryptés au niveau tunnel. 60
4.31 L'affichage du protocole ESP. 61
4.32 La phase une du Protocole ISAKMP 61
4.33 La phase deux du Protocole ISAKMP 62

LISTE D'ABRÉVIATIONS

AES	Advanced Encryption Standard
AH	Authentification Header
ASP	Application service provider
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	demilitarized zone
DNS	Domain Name Server
FDDI	Fiber Distributed Data Interface
GNS3	Graphical Network System 3
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
ISAKMP	Internet Sécurité Association and Key Management protocol
ISO	International Organization for Standardization
ISP	In-System Programming
L2F	Layer Two Forwarding
L2TP	Layer two Tunneling Protocol
Lac	L2TP Access Concentrator
LAN	Local Area Network
MAN	Métropolitain Area Network
MAU	Multistation Access Unit
MD5	Message Digest 5
MPLS	Multi-Protocol Label Switching
NAS	Network Access Server

NAT	Network Address Translation
OSI	Open Systems Interconnexion
PAN	Personale Area Network
PKI	Public Key Infrastructure
PPP	Point-To-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RFC	Request For Comments
SA	Security Association
SAD	Security Association Database
SADB	Security Associations Database
SHA	Secure Hash Algorithm
SP	Security Policy
Spa	Section par action
SPD	Security Policy Database
SSL	Secure Socket Layer
SSH	Secure SHell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMF	Transport Marchandise Frigorifiques
URL	uniform Resource Locator
VPC	virtual personnel computer
VPN	Virtual Privat Network
VM	Virtual Machine
WAN	Wide Area Network

INTRODUCTION GÉNÉRALE

Aujourd'hui, les entreprises crées sont de plus en plus partout dans le monde, et donc leurs besoins de communiquer, d'échanger des données et des informations, est devenus une nécessité cependant toutes les entreprises possédant un réseau local qui dispose d'un accès à Internet.

L'internet assure la communication entre les différents sites d'une même entreprise. Malheureusement, cette solution n'est pas sans risque, car elle présente des menaces et des vulnérabilités sur les données échangées qui sont confidentielles, ce qui engendre un risque de pénétration de réseau local, et d'accéder à des informations sensibles dans le but de les intercepter, les modifier ou les détruire, qui peut causer de grands problèmes à l'entreprise sois au bon fonctionnement du système ou au développement de l'entreprise.

Dès que ces réseaux sont apparus comme des cibles d'attaques une architecture sécurisée est devenue un enjeu incontournable pour les différentes institutions, de ce fait les entreprises se trouvent dans l'obligation de sécuriser leur réseau et mettre en place des politiques de sécurité informatique pour assurer la confidentialité des données et les garder en toute sécurité. Parmi les outils et moyens qui sont disponibles, en trouve les systèmes de détection d'intrusions (IDS), les antivirus, les firewalls (pare-feux) et les réseaux privés virtuels (VPN).

Une telle architecture doit être basée sur un firewall. Cet outil a pour objectif de sécuriser au maximum le réseau local de l'entreprise et de détecter les tentatives d'intrusion. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur internet beaucoup plus sûr, il permet d'analyser, de sécuriser, de gérer le trafic des services, de ce fait le pare-feu propose un véritable contrôle sur le trafic réseau de l'entreprise, et la restreindre l'accès interne vers l'extérieur.

En plaçant un pare-feu limitant accès à ces services, ainsi de limiter et d'empêcher les personnes sans autorisation d'accéder au réseau de données, l'entreprise peut donc bénéficie d'un contrôle sur les activités se déroulant dans son établissement. Ce dernier permis de crée un VPN, qui repose sur un protocole appeler tunnel ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée entre deux extrémité du tunnel. Le principe de tunnel consiste à construire un chemin virtuel via Internet après avoir identifié l'émetteur et le destinataire qui proposent d'échanger des données en toute sécurité en les encapsulant et les transmettant à travers le tunnel.

L'objectif principal de notre travail consiste alors à mettre en place une architecture VPN afin d'établir une communication sécurisée entre « Spa TMF Logistics AKBOU» et « Spa TMF Logistics ALGER». Celle-ci est assurée avec un fortigate on utilisant un VPN IPsec et afin de réaliser les objectifs visés, nous avons structuré ce travail en trois chapitres :

- Le premier chapitre est dédié à la présentation de l'organisme d'accueil ou nous avons effectué notre stage.
- Le deuxième chapitre est consacré aux généralités sur les réseaux et la sécurité informatique, nous allons aborder quelques notions sur les réseaux informatiques et nous présentons les menaces et les différentes attaques auxquelles un réseau peut être exposé.
- Le troisième chapitre est focalisé sur les réseaux Privés Virtuels : leurs principes et fonctionnement, leurs différents types et les différents protocoles utilisés pour leur réalisation. plus précisément le protocole IPsec qui consiste la majeure partie de notre projet.
- Le dernier chapitre sera consacré à la réalisation de l'architecture réseau sécurisé proposée pour l'entreprise Spa TMF d'AKBOU, nous définirons les outils utilisés et nous présentons la simulation d'une connexion VPN entre deux sites distants, pour cela nous avons utilisé le router-firewall (fortigate) Le simulateur GNS3, et VMware et quelque capture de la configuration réalisée.
- Enfin, nous conclurons ce travail en résumant les connaissances acquises durant la réalisation du projet.

CHAPITRE 1

DESCRIPTION DE L'ORGANISME D'ACCUEIL

1.1 Introduction

Dans ce chapitre, nous allons présenter le groupe SPA TMF (Transport de Marchandises et Frigorifiques) ainsi que sa structure hiérarchique, ensuite nous exposerons la problématique suivie de la solution proposée.

1.2 Présentation de Spa TMF

Spa TMF est une société implantée stratégiquement à l'est de payé, à Taharacheth d'Akbou wilaya de Béjaïa avec un capital de 509 803 000.00 DA, à proximité donnant accès directe sur l'autoroute est ouest, spécialisée dans le domaine de transport routier de marchandise et Frigorifiques à travers le territoire national et international.

La société TMF fut créés par son fondateur, Mr BATOUCHE Mohand, pour répondre à un besoin de transport pour le compte d'une de ses sociétés.

A partir de cette date, l'évolution de cette société fut exceptionnelle, et son activité n'a cessé de progresser. Aujourd'hui SPA TMF est l'un des acteurs majeur de la logistique en Algérie, son champ d'activité couvre l'ensemble de prestations logistique en commençant par le transport, le stockage, la manutention jusqu'à la mise à disposition du matériel des travaux publics. Elle dispose aujourd'hui d'une flotte de plus de 240 camions de différents types, et différents tonnages dont une partie est basée à Sétif Pour répondre à la demande de ses clients de la région.

La société SPA TMF dispose d'un effectif jeune de près de 400 employés qui tend à augmenter et qui pourrait dépasser les 500 employés d'ici la fin de l'année en cours.

1.3 Structure de Spa TMF

L'organisation de TMF spa est structurée en trois directions : la direction transport et logistique, la direction maintenance et la direction administration et ressources humaines. Et en trois départements : le département commercial, le département finance et le département comptabilité, achat et approvisionnement.

Le service système d'information de gestion et l'informatique est rattachée directement au directeur général. Son rôle est de piloter et encadrer le processus et les opérations d'acquisition, d'essai, de mise en service, d'entretien et de maintenance des équipements et applications informatiques, y compris la formation des utilisateurs. Mais aussi garantit. L'harmonisation et la cohérence des équipements, système et application informatique de TME spa, Organisme de Spa TMF est présenté par la figure ci-dessous.

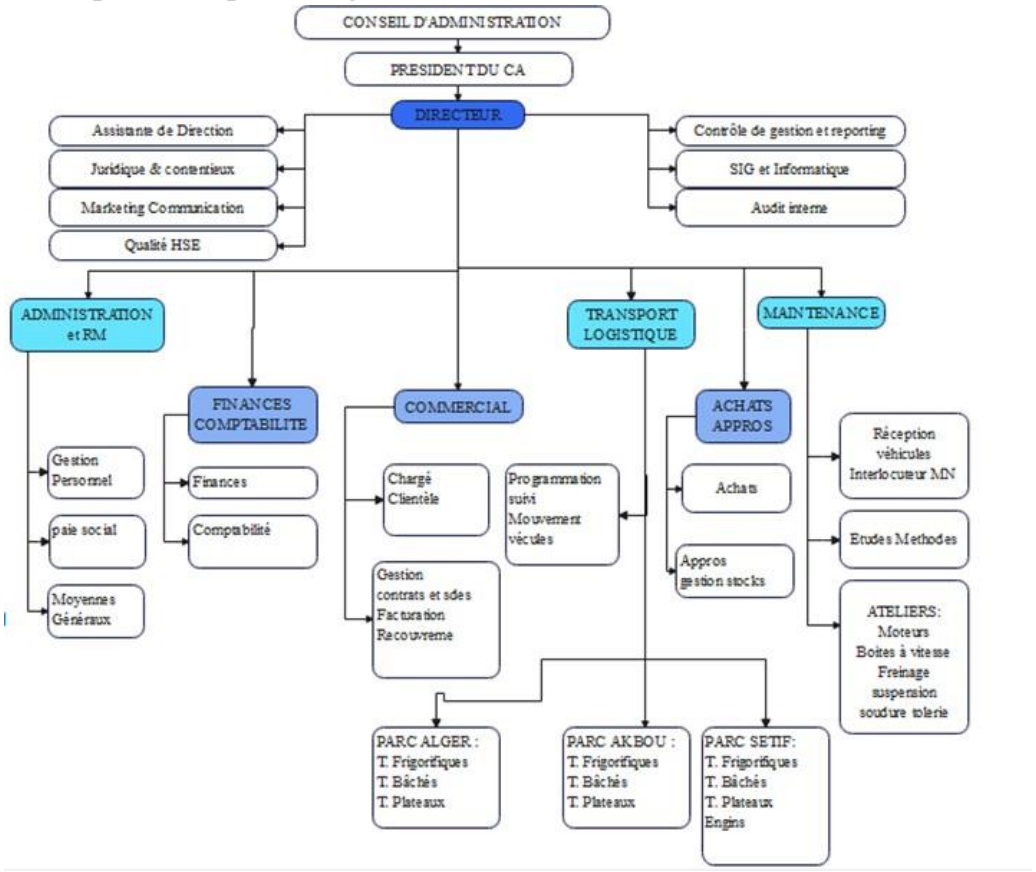

FIGURE 1.1 – Organisme de Spa TMF.

1.4 Présentation du centre informatique

C'est le service qui gère le système d'information et le parc informatique de l'entreprise, son rôle est d'assurer le bon fonctionnement des infrastructures et d'intervenir en cas de défaillance des systèmes.

1.5 Etude du système informatique existant

Toute révision, modification réaction visant à apporter des améliorations au système informatique du TMF doit passer par une connaissance préalable de l'ensemble des différents éléments constituant l'architecture de son système informatique existant.

L'analyse de l'existant a pour but à la fois d'évaluer le niveau de performance et de disponibilité de l'infrastructure réseau et de déterminer quelles améliorations peuvent être apportées afin de la rendre plus performante tout en facilitant sa gestion.

1.5.1 État des ressources du système informatique

- **Les ressources matérielles :** C'est le matériel qui constitue le système informatique du spa TMF, il se présente comme suit :

  - Serveur : TMF dispose d'un seul serveur physique HP Poliant 8ème génération avec un processeur Xeon, et une capacité de mémoire de 24 GO. Partagée sur plusieurs machines virtuelles.

  - Station de travail : Une cinquantaine de pc entre ordinateurs du Bureau et lap-tops, La plupart sont sous Microsoft Windows 7, et on trouve 15 imprimantes de type canon partagées dans les différents services. Plus deux imprimantes photocopieuses installées dans le réseau local (Une pour chaque étage).

- Pour la communication : TMF bénéficier de deux service de communication la téléphoner et l'internet, pour la ligne téléphonique TMF utilise un PBX pour relier les lignes internes de l'entreprise au réseau téléphonique publique, chaque bureau dispose d'une ligne de téléphone interne pour communiquer. Elle utilise aussi internet, cette dernière est fournie par deux opérateurs, Algérie Télécom via son service Djaweb pour l'entreprise (2mb/s). Et deux autres raccordements au réseau mondial par l'entreprise privée ICOSNET. Une dans chacun des sites de l'entreprise.

- **Ressources logicielles :** La société utilise un pack de logiciels indépendants pour le bon déroulement des différents processus et activités reliéesà l'entreprise, les logiciels et systèmes installés sont :

  - Logiciels de métier :

    Logiciel de géolocalisation Fleetcenter : Est une application web basé sur la technologie GPS qui permet la géolocalisation de la flotte de l'entreprise en temps réel, elle fornit des rapports journa- lier sur l'activité de transporter de la logistique.

    Logiciel de gestion de facturation et de vente : Une application client-serveur utilisée par le service facturation, de plus, elle analyse les informations relatives aux clients et aux prospects, dans le but de les fidéliser en leur offrant le meilleur service.

    PC Compta : Est un logiciel de comptabilité générale, auxiliaire et analytique, il est multi dossiers, multi-exercices, le volume des données n'est limité que par la taille du disque dur.

    PC Pai : Est un logiciel de paie, multi-dossiers,le volume des données n'est limité que par la taille du disque dur.

    Application de gestion de temps : Kelio bodet Le logiciel de gestion des temps Kelio intègrent toutes les fonctionnalités nécessaires à un suivi fiable et efficace des temps de travail : fiche individuelle du salarié, horaires multiples, gestion des entrées/sortie, badgeages, pauses, absences, primes.

    GMAO : gestion de la maintenance assistée par ordinateur

OPTIMAINT est un logiciel utilisé par la section maintenance pour l'aider dans son activité.

- Système et autre : La plupart des postes de travails son sous Windows 7, les serveurs (physique et virtuels) utilisent Microsoft Windows serveur 2008 R2. Un de ces serveurs est dédié à la gestion du réseau local : DNS (tmf-logistics.net), DHCP (192.168.1.0/24), l'annuaire active directory et port la messagerie interne TMF utilise l'outil Microsoft Exchange 2010, le serveur web de l'entreprise gère la messagerie externe (tmf-logistics.com).

- **Le réseau interne**

L'entreprise TMF est composée de deux sites distants, Éloigné par une distance de 1km environ. Chaque site est doté d'un réseau local. Et les deux sont connectés à internet par le fournisseur d'accès ICOSNET.
La figure ci-dessous nous montre l'architecture du réseau local de spa TMF-AKBOU.

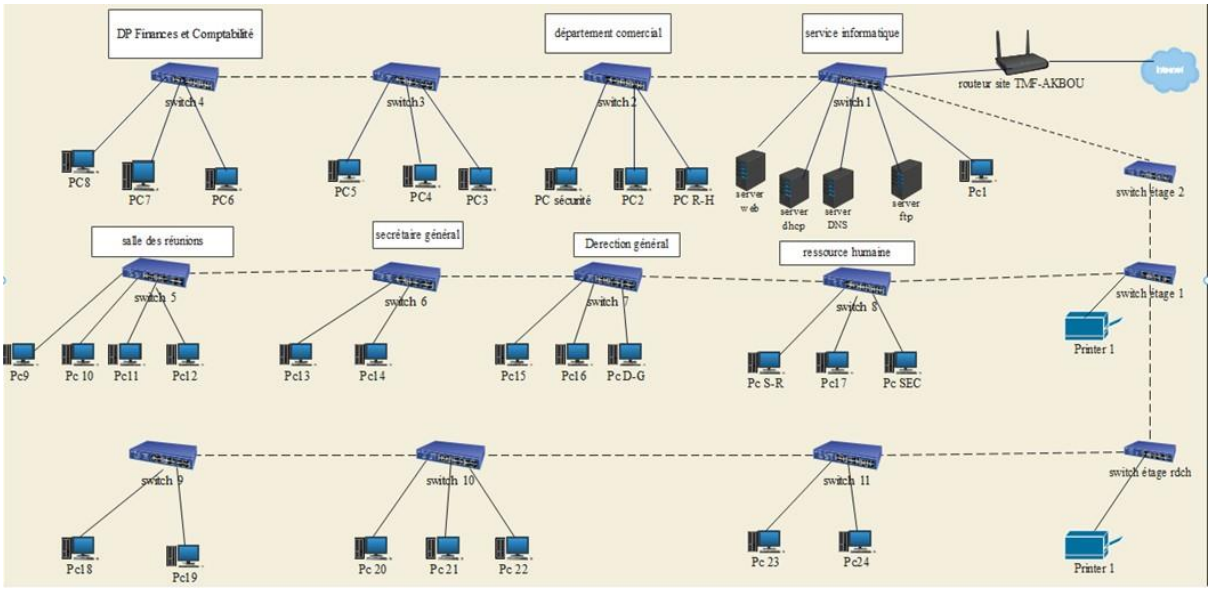

FIGURE 1.2 – Réseau local du site Spa TMF-d'AKBOU.

L'illustration de l'architecture du site spa TMF-ALGER est montrée sur la figure suivante :

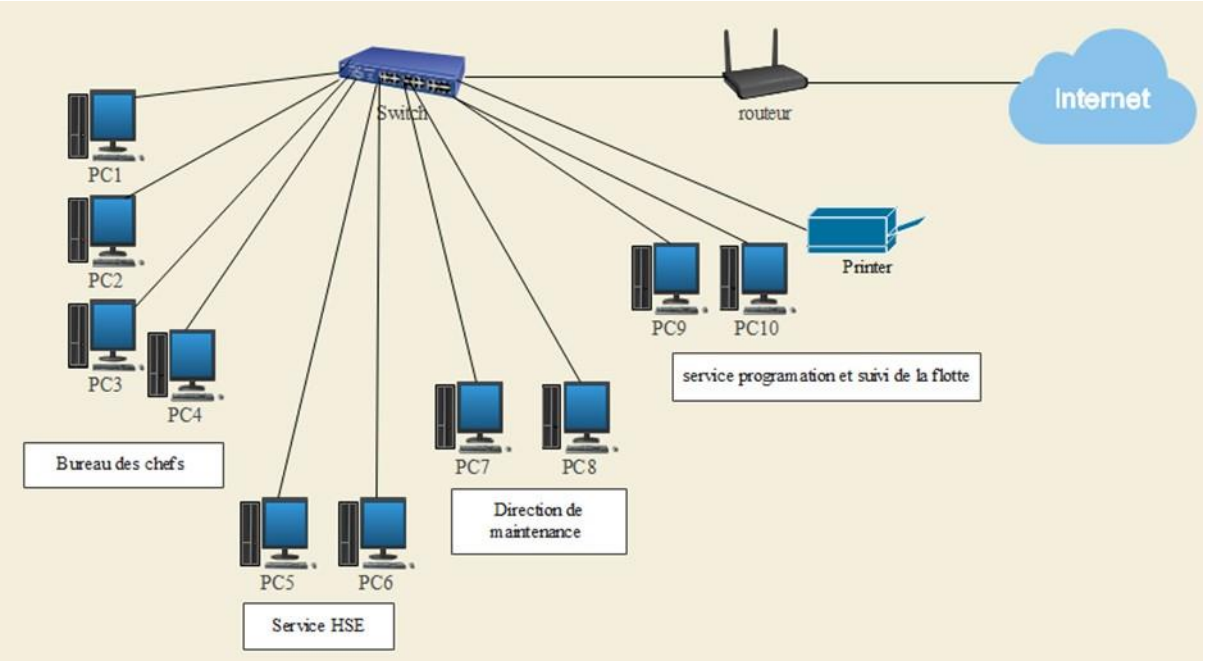

FIGURE 1.3 – Réseau local du site Spa TMF-d'ALGER.

1.5.2 Aspect positif du système

Les points appréciables sur le plan physique du système informatique du TMF sont :

- Installation électrique : des prises de terre et des onduleurs permettant la protection des équipements informatiques contre les pics du courant, les surtensions.
- deux abonnements Internet Djaweb et COSNET en cas de panne de l'une l'autre, prend le relais afin d'assurer la continuité de service Internet.
- une version d'antivirus KaspersKy Sécurity est installée sur les serveurs Windows ainsi que sur la plupart des postes de travail.
- l'existence d'un serveur de fichier : permet une centralisation des fichiers d'utilisateur et le partage de fichiers en réseau.

1.6 Problématique

Les réseaux informatiques sont de plus en plus répandus et complexes. L'implantation d'un réseau complexe doit être sûre pour diminuer les risques.

L'entreprise Spa TMF Logistics dans laquelle nous avons effectué notre stage est composé de trois sites distants (Alger, Sétif et Akbou) et qui souhaite en

tirer les avantages d'une liaison Internet entre ses sites pour des taches de gestion d'administration à distances, et parmi ces dernies on distingue le site de Spa TMF d'AKBOU et Spa TMF d'ALGER ce qui est demandé est de pouvoir interconnecter ces deux sites en intégrants une connexion site à site. La question qui se pose alors est :

Comment peut-on relier les deux sites de l'entreprise Spa TMF d'AKBOU et Spa TMF d'ALGER toute en assurant la sécurité et l'intégrité des échanges des données ?

1.7 Solution proposée

L'objectif de notre projet est l'interconnexion de deux sites distants. Pour la solution nous avons opté VPN site à site qui basé sur deux réseaux locaux qui ont connecté grâce à une liaison Internet sécurisée au niveau de deux sites distants de Spa TMF.

Un VPN est le mieux adapté à l'interconnexion de différents sites car il permet un partage sécurisé des données et protège la confidentialité et l'intégritédes informations et des données échangées via un tunnel. Nous allons effectuer différentes applications sur le pare-feu (FortiGate) afin d'exploiter les fonctionnalités fournies par ce dernier.

Pour protéger les communications réseau à l'aide de techniques de cryptage on peut utiliser IPSec. Ce dernier permet à une entreprise ou à l'administrationde réaliser une extension de son périmètre de sécurité grâce à un tunnel VPN et de pouvoir exercer les tâches administratives à distance.

CHAPITRE 2

GÉNÉRALITÉS SUR LES RÉSEAUX INFORMATIQUES ET LEUR SYSTÈME DE SÉCURITÉ

2.1 Introduction

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que des stations de travail ou des serveurs. La sécurité des réseaux informatiques est un sujet essentiel qui favorise le développement des échanges d'information dans tous les domaines.

Pour mener à bien notre projet qui est l'interconnexion de deux sites, nous présentons dans ce premier chapitre les réseaux informatiques dans la première partie puis nous abordons différent concepts de la sécurité informatique dans la deuxième partie.

Partie I : Les réseaux informatiques

2.2 Définition

Un réseau informatique est un groupe d'équipements qui permet l'interconnexion de l'ensemble des ressources de communication logicielle et matérielle afin d'échanger des information grâce à des équipement d'interconnexions (ordinateurs, concentrateur, commutateur, router, imprimante..). Un réseau possède un équipement appelé nœud qui assure l'intersection de plusieurs connexions [1].

2.3 Classification des réseaux informatiques

On peut classer les réseaux selon deux critère à savoir l'étendu et la topologie :

2.3.1 Selon l'étendu

Les réseaux peuvent être classés en fonction de l'éloignement maximal entre stations. On peut alors distinguer déférents types de réseau : le réseau personnel (PAN), le réseau local (LAN), le réseau métropolitain (MAN) et le réseau étendu (WAN) (voir figure 2.1).

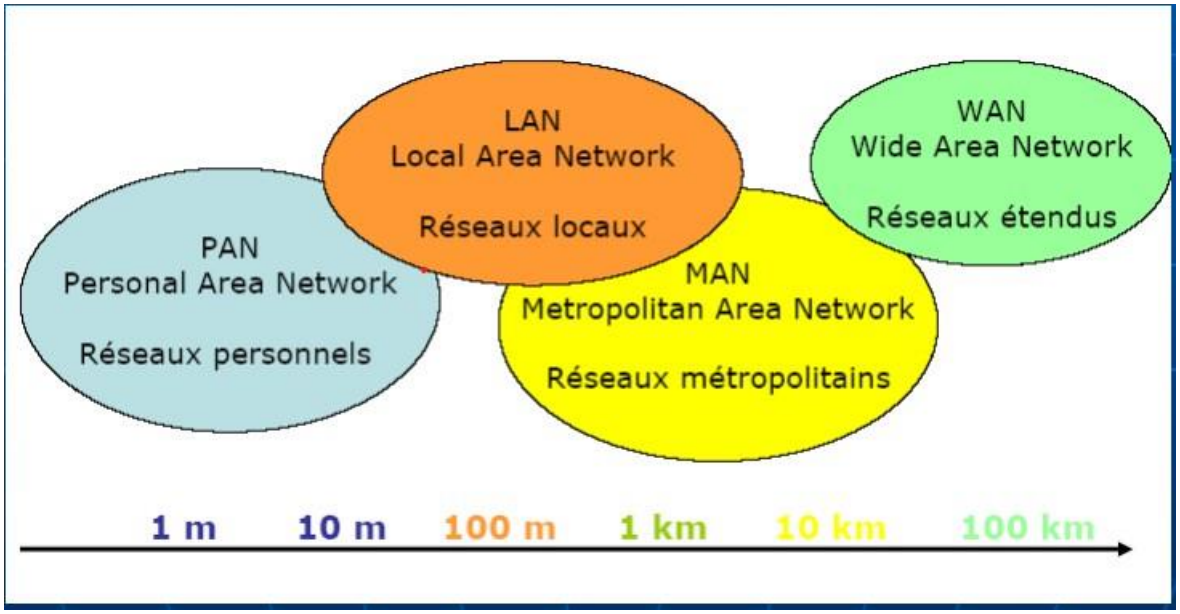

FIGURE 2.1 – Classification des réseaux informatique selon leur étendu.

- **Réseau personnel(PAN) :** Un réseau personnel est un réseau domestique ou un réseau individuel pour une seule personne (même utilisateur) qui permet d'interconnecter des équipements sur quelques mètres autour d'un utilisateur. La liaison avec ces périphériques peut être câblée ou sans fil (figure 2.2) :

FIGURE 2.2 – Réseau PAN.

- **Réseau local(LAN) :** Un LAN (figure 2.3) Est un réseau situé généralement dans la même entité géographique (entreprise, compus,..). Les LANs peuvent être interconnecté pour former des réseaux plus grands (WAN, MAN,..). On dit alors que le LAN est un sous-réseau du réseau auquel il est connecté[2] :

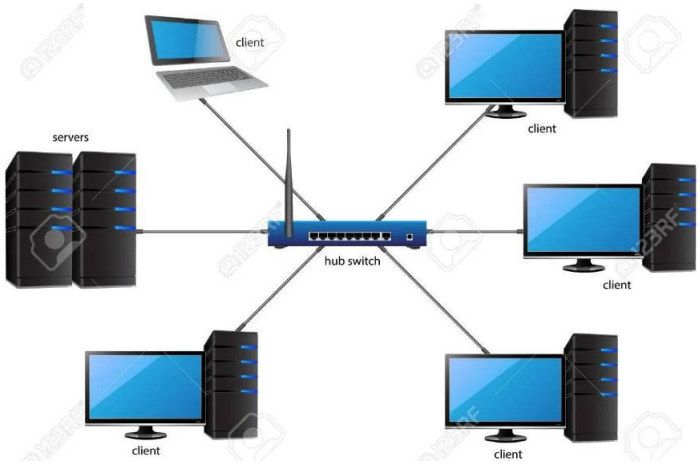

FIGURE 2.3 – Réseau LAN.

- **Réseau métropolitain(MAN) :** Les réseaux MAN (voir la figure 2.4) Nommé également réseau fédérateur assure des communications sur de plus grandes distances (quelques dizaines de kilomètres), interconnectant souvent plusieurs réseaux LAN [3].
  Ce type de réseaux est récent et garde les avantages des LAN sur de plus

longues distances de l'ordre de la ville [02].

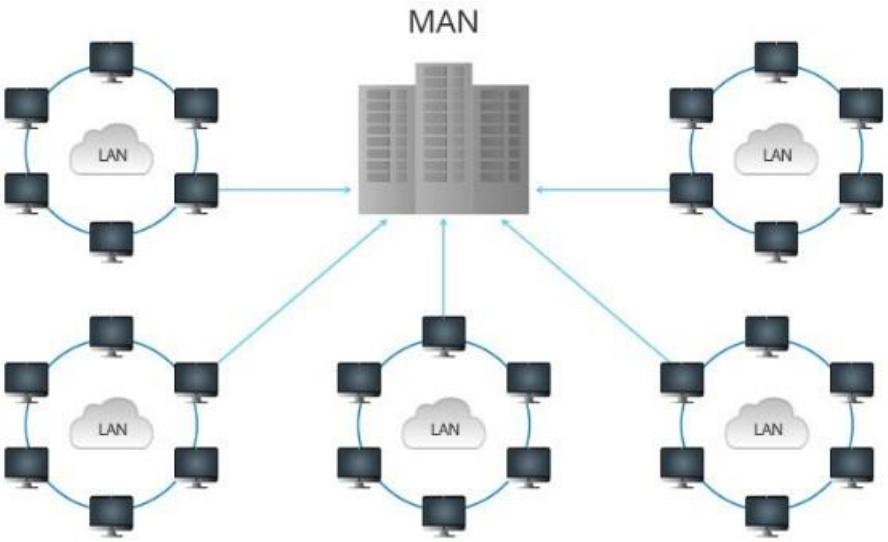

FIGURE 2.4 – Réseau MAN.

- **Réseau étendu (WAN) :**

  Le WAN (voir la figure 2.5) est un réseau de communication étendu capable de couvrir une grande zone géographique, il se distingue des réseaux de type LAN et/ou MAN.

  Aujourd'hui, internet est le réseau étendu le plus connu dans le monde.

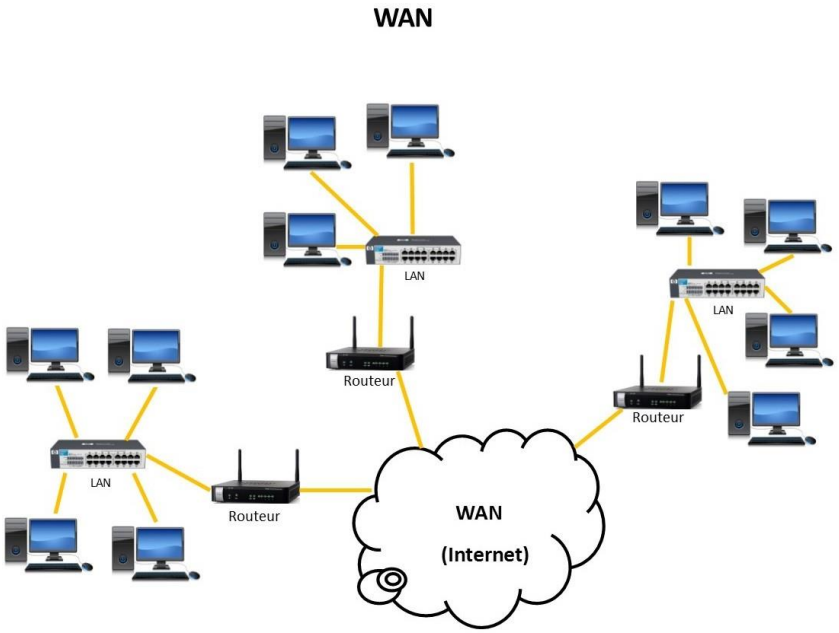

FIGURE 2.5 – Réseau WAN.

2.3.2 Selon la topologie

La topologie est la manière d'interconnecter les machines grâce à des lignes de communication (câbles réseaux) et des éléments matériels (cartes réseau,...) ainsi que d'autres équipement permettant d'assurer la bonne circulation des données, on distingue deux aspects :
La topologie logique : qui est la manière de faire circuler le signale ou les données transitent dans les lignes de communication (exemples : Ethernet, Token Ring et FDDI).
La topologie physique : qui est l'arrangement physique, autrement dit la configuration spatiale du réseau, on peut désigner trois topologies en bus, on anneauet en étoile).

- **Topologie en Bus :** La topologie en bus su réseau est une architecture de communication où la connexion des matériels est assurée par un bus partagé par tous les utilisateurs, c'est l'organisation la plus simple d'un réseau, tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial, il est très facile de relier plusieurs postes d'une même salle.
  Aujourd'hui cette topologie n'est plus adaptée aux réseaux importants.

- **Topologie en Anneau :** Dans un réseau possédant une topologie en anneau, les ordinateurs sont situé sur une boucle et communiquent chacunson tour. En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur appelé MAU (Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en accordant à chacun d'entre-eux un temps de parole [1].

  La méthode d'accès à ce type de câblage est celle du passage de «jeton». Pour pouvoir transmettre, un ordinateur doit être en possession du jeton libre ce qui évite toute collision sur le réseau [4].

- **Topologie en étoile :** Dans une topologie en étoile le système repose sur un équipement central appelé concentrateur, il s'agit d'une boite comprenant un certain nombre de jonctions auxquelles les connexions peuventêtre effectuées via des câbles à paire torsadée ou des câbles coaxiaux.

2.4 Architecture des réseaux

Pour que les données transmises entre l'émetteur et le récepteur arrivent correctement avec la qualité de service exigée, il faut une architecture logicielle, dans ce qui suit on présente les deux architectures existantes :

2.4.1 Le modèle OSI

Le modèle OSI a été créé par l'organisme ISO (international Organization for Standardization), il écrit les fonctionnalités nécessaires à la communication entre ordinateurs et assure l'organisation de ces fonctions.
Ce modèle est formé de sept couches, ayant chacune des applications bien distinctes. Les déférentes couches sont [5] :

- **La couche physique :** Elle s'occupe de la transmission effective des signaux entre les interlocuteurs. Elle assure un transfert de bits sur le support.
- **La couche liaison de données :** Gère les communications entre deux machines adjacentes connectées entre elles (physiquement connectées par un canal) et permet d'échanger des données sous forme de bits regroupés en trames de façon fiable et efficace.
- **La couche réseau :** Elle assure l'acheminement des données et des paquets de bout en bout de la source vers la destination via plusieurs réseaux, routeurs et adressage des paquets.
- **La couche transport :** Gère les communications de bout en bout entre processus et assure un transport fiable des données de bout en bout entre les deux extrémités.
  Cette couche s'occupe de la fragmentation des données en petits paquets et vérifie éventuellement qu'elles ont été transmises correctement.
- **La couche session :** Gère la synchronisation des échanges, elle permet principalement d'ouvrir, de gérer et de clore une session entre deux machines communicantes.
- **La couche présentation :** Permet la conversion et la présentation des données dans un format standard compréhensible par la toutes les machines,les applications et les utilisateurs.
  Elle assure le cryptage, le décryptage et la compression de données.

- **La couche application :** C'est le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme [6].

2.4.2 Le modèle TCP/IP

Contrairement au modèle OSI, le modèle TCP/IP est un protocole de transport fiable, en mode connecté. Il permet une interconnexion des réseaux et l'établissement d'une session de communication entre deux parties qui veulent échanger des données. Il reprend l'approche modulaire (utilisation de couche ou module) mais en contient uniquement quatre : la couche d'accès au réseau, la couche internet, la couche transport, et la couche application.
La figure suivante représente la différence entre le modèle OSI et le modèle TCP/IP :

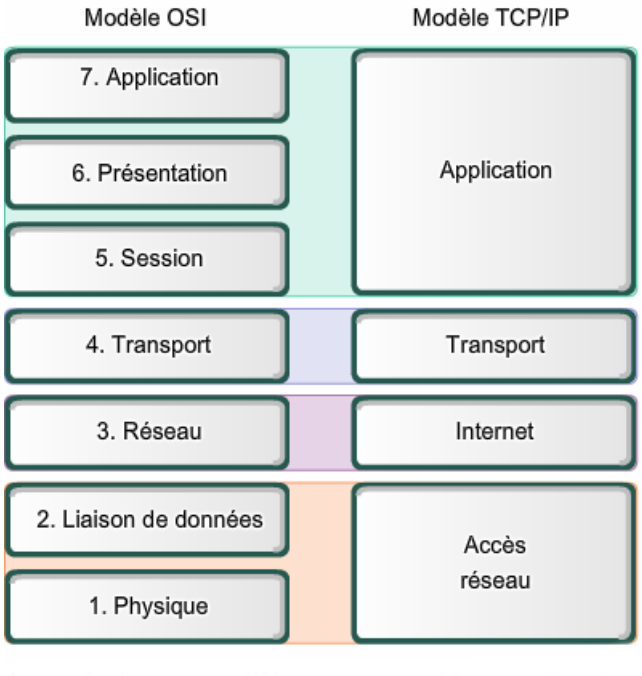

FIGURE 2.6 – Déférence entre le modèle OSI et le modèle TCP/IP.

2.5 Les équipements d'interconnexion

Un réseau utilise plusieurs équipements d'interconnexion afin de faire interconnecter plusieurs sous réseaux et avoir la possibilité dialogué entre eux.

- **Le répéteur :** Est le composant le plus simple de la couche physique du réseau. C'est un organe non intelligent, qui répète automatiquement tous les signaux qu'il reçoit et transitent d'un support vers un autre support [07].

- **Concentrateur(Hub) :** Un concentrateur permet de concentrer le trafic provenant de différents équipements terminaux, il peut être actif ou passif.
- **Commutateur(Switch) :** Le commutateur est un pont multiport qui assure la connexion entre les ordinateurs du réseau. Il s'agit le plus souvent d'un boitier disposant de plusieurs ports, il a donc la même apparence qu'un concentrateur la seule différence est sa capacité de connaitre l'adresse physique des machines.
- **Le pont (bridges) :** Au contraire d'un répéteur, un pont est un organe intelligent capable de reconnaître les adresses de blocs d'information qui transitent sur les supports physiques.
- **Le routeur :** Un routeur est un élément intermédiaire dans un réseau informatique dont la fonction principale consiste à orienter et circuler les données à travers un réseau.
- **La passerelle(Gateway) :** Une passerelle est un nœud de réseau utilisé dans les télécommunications qui relie entre deux réseaux ayant des protocoles de transmission différents (par exemple un réseau local et le réseau internet).
- **Adaptateurs(Transmetteur) :** C'est un composant qui se trouve sur la carte qui gère l'interface entre l'équipement et le support physique. Il est responsable de la connexion physique.
- **Le coupleur (carte réseau ou encore carte d'accès) :** Elle se charge de contrôler les transmissions sur le câble. Le coupleur assure le formatage et le dé-formatage de données de blocs de données à transmettre et la détection d'erreur.

Partie II : Sécurité informatique

2.6 Définition

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire à la mise en place de moyens à empêcher les entités non autorisées à accéder au réseau et aux données numériques.

2.7 Principaux concepts de la sécurité informatique

- **Les vulnérabilités :** Ce sont les failles de sécurité dans un ou plusieurs systèmes, qui peuvent être exploitable ou non.
- **Les attaques :** Représentent les moyens d'exploiter une vulnérabilité, il peut y avoir plusieurs attaques pour une même vulnérabilité.
- **Les contre-mesures :** Sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.
- **Les menaces :** Ce sont des adversaires déterminés et capable de monter une attaque on exploitant une vulnérabilité.

2.8 Objectifs de la sécurité

Assurer la sécurité d'un système informatique revient à atteindre un ensemble d'objectifs en vue de garantir la protection des informations contre toute divulgation, altération ou destruction. L'accès à ces information doit être également contrôlé par un accès protégé. Dans cette section, un ensemble d'objectifs sont présentés [8] :

- **Authentification :** Il existe deux type d'authentification en trouve authentification d'une information c'est de prouver qu'une information provientde la source annoncé (auteur, émetteur). Et authentification d'une entité elle consiste à prouver que l'identité est bien celle annoncé.

- **Non-répudiation :** Empêcher les entités de nier leurs actions précédentes ou leurs engagements.

- **confidentialité :** Empêcher la divulgation d'information à des entités non autorisées à les connaitre. Les entités peuvent être des sites, organisations, personnes.

- **Intégrité :** Assure que les informations n'ont pas été modifié (ou altérées) par des entités non autorisées ou inconnues. Généralement, l'intégrité est appliquée sur des données en transmission.

- **Signature :** Lier une information à une entité.

- **Contrôle d'accès :** Limiter l'accès des ressources aux entités autorisées selon différents privilège. En pratique, on trouve plusieurs modèles d'accès.

- **Certification :** L'approbation de l'information par une entité de confiance.

- **Réception :** Approuver la réception de l'information.

- **Anonymat :** Cacher l'identité d'une entité impliquée dans un processus pour des fins de protection.

2.9 Les attaques

Une attaque est l'exploitation d'une vulnérabilité au niveau d'un système informatique à des fins non connues par le l'exploitant du système et généralement préjudiciable.

2.9.1 Catégories d'attaques

Il existe plusieurs catégories d'attaque à savoir [9] :

- **Interception :** C'est une attaque portée à la confidentialité. Il peut s'agir d'une personne, d'une personne, d'un programme ou d'un ordinateur. Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes.

- **Interruption :** C'est une attaque porté à la disponibilité, elle consiste à rendre les données d'un système inaccessible. Cela implique par exemple la suppression des données, rendre l'accès à un serveur indisponible par une attaque de déni de service, la destruction d'une pièce matérielle (tel un disque dur), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers.

- **Modification :** Il s'agit d'une attaque portée à l'intégrité. Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmissur un réseau.

- **Fabrication :** C'est une attaque portée à l'authenticité. Il peut s'agir de l'insertion de faux message dans un réseau ou l'ajout d'enregistrements à un fichier par une tierce partie non autorisée.

2.9.2 Scénarios d'attaques

Il existe deux scénarios d'attaque à savoir :

- **Attaque passive :** L'intrus va tenter de dérober les informations par audit ou intrusion, ce qui rend sa détection relativement difficile. En effet, ses actions ne modifient pas le comportement du système [08].

- **Attaque active :** L'intrus modifie volontairement le comportement ou le contenu du système. La détection de ce type d'action est facile, mais il peut être trop tard lorsque l'attaque a déjà eu lieu.
  Les menaces actives peuvent être des interceptions, des interruptions, des fabrications ou des modifications.

2.9.3 Quelques attaques courantes

- **Attaque par déni de service :** Cette attaque cherche à rendre un serveur hors service en le submergeant de trafic inutile [10].

- **Attaque de l'homme du milieu :** Le hacher se fait place entre deux ordinateurs et se fait passer pour l'un de ses victimes afin d'obtenir le mot

de passe de l'autre victime, il peut alors se retourner contre le premier avecun mot de passe valide pour l'attaquer.

- **Programme malveillant (malware) :** Il s'agit d'un logiciel crées dans le but de nuire à un système informatique, Plusieurs méthode sont utilisées par les hackeur pour infecter un ordinateur parmi ces méthode en trouve Porte dérobé, Virus et Bombe logique [10].

- **Cassage de mot-de-passe :** Le cassage de mot de passe est un type d'attaque informatique ayant pour but de prendre connaissance des mots de passe des clients, des utilisateurs d'un site internet ou d'une application web. Ce genre d'attaque consiste pour le pirate ou logiciel utilisé à essayer différentes combinaisons possible jusqu'à trouver la bonne. Des attaques de pirates sur le net, le cassage de mot de passe, aussi désigné par «password cracking» en anglais, est le plus classique. Il n'est d'ailleurs pas uniquement lié au web, mais à l'ensemble des domaines informatique [11].

2.10 Mécanismes de défense

2.10.1 Zone Démilitarisée

La DMZ, est une partie d'un réseau d'entreprise qui se trouve derrière un pare-feu mais en dehors ou segmentée du réseau interne. La DMZ héberge généralement des services publics, tels que des serveurs Web, de messagerie et de domaine [13].

2.10.2 Contrôle d'accès

Est la gestion des autorisations d'accès à des ressources. Une autorisation consiste à gérer et à vérifier les droits d'accès, en fonction des règles spécifiées dans la politique de sécurité. On dit qu'un sujet (entité qui demande l'accès, dite aussi entité active) si et seulement s'il est autorisé à effectuer la fonction d'accès correspondante sur cet objet [9].

2.10.3 Proxys

Un proxy, parfois appelé mandataire, c'est composant logiciel qui se place entre deux autre pour faciliter ou surveiller leur échanges. Dans le cadre plus précis des réseaux informatique, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement internet. Par extension, on appelle aussi proxy un matériel (un serveur par exemple) mise en place pour assurer le fonctionnement de tels services [8].

2.10.4 Chiffrement

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 son réalisés principalement à partir d'algorithmes, en utilisant des clés secrètes ou publiques. Les techniques de chiffrement sont essentiellement scindées en deux, notamment [9] :

- **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 chiffrerle message. Et une clé privée pour le déchiffrer, et seul le destinataire possède la clé secrète pour déchiffrer le message.

2.10.5 Pare-feu

Il peut être considéré comme une approche standard qui protège les ressources informatiques locales contre les menaces externes. Il est conçu pour filtrer les paquets IP provenant du réseau externe vers le réseau local. C'estaussi un moyen efficace de protéger le système local ainsi que le réseau, et vous pouvez accéder simultanément à internet ou à un réseau étendu. Il n'empêchepas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ilne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas) [9].

2.10.6 Antivirus

Sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Il ne protége pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisée à le faire [12].

2.10.7 virtual Private Network (VPN)

Ce réseau est dit virtuel car il relie deux réseaux locaux par internet, et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données. Le VPN est une technique permettant à un ou plusieurs postes distants de communiquer de manière sûre. C'est un environnement de communication, dans lequel l'accès est contrôlé, afin de permettre des connexions entre une communauté d'intérêt seulement [12].

Le trafic VPN est chiffre pour garantir la confidentialité des transferts de données pendant la durée de la connexion. Le principe du VPN consiste à établirun chemin virtuel unique avec l'identification de l'émetteur et du récepteur. Ce chemin est aussi appelé tunnel. Le VPN établit une connexion sécurisé vers un réseau à distance en utilisant la technique de tunnelling à travers Internet. Cette technique consiste en l'encapsulation, la transmission, la desencapsulation d'un paquet de données sous forme de message à l'intérieur d'un paquet IP. Le transfert de ces données est réalisé à travers Internet.

- **Avantage du VPN**

  - La possibilité de réaliser des réseaux privés à moindre coût par rapport à tout autre type de connexion, l'entreprise ne paye que l'accès à Internet, il n'est pas nécessaire de payer une communication nationale ou internationale.
  - La mise en œuvre d'un Intranet étendu et homogène permettant à tous les utilisateurs d'accéder à distance à des ressources partagées ou des services de types ASP (application service provider), quelle que soit leur localisation.
  - L'utilisation de tunnels de communication cryptés pour l'extension des réseaux locaux.
  - La possibilité de communiquer entre vos partenaires ou vos clients en toute sécurité.

2.11 Conclusion

Ce chapitre nous a permis en premier lieu de découvrir et de mieux comprendre les notions et les aspects élémentaire des réseaux informatiques, oùnous avons décrit leur définitions, types, topologies ainsi que les modèles OSIet TCP/IP, et en deuxième lieu de comprendre les concepts et les objectifs dela sécurité informatique, et plus particulièrement la sécurité des réseaux oùnous avons présenté brièvement les différentes politiques sécuritaires, commeles pare-feu, les proxys ainsi que les VPNs qu'on abordera en détails dans le chapitre suivant.

CHAPITRE 3

LES RÉSEAUX PRIVÉS VIRTUELS

3.1 Introduction

Les réseaux locaux type LAN permettent de faire communiquer les ordinateur d'un site d'une société ensemble. Ces réseaux sont relativement sûr car ils sont quasiment toujours derrière une série de pare-feu ou coupés d'Internet etque le chemin emprunté par les données ne quitte pas l'entreprise et est connu. Ils peuvent toutefois être soumis à des attaques dites du «man-in-the-middle»qui sera l'objet d'un autre document. Sur Internet, on ne sait pas par où passent les données car les chemins changent. Ces données peuvent être écoutées ou interceptées. Il n'est donc pas envisageable de faire connecter deux LAN entre eux par internet sans moyen de sécuriser le cheminement des données échangées.

Pour sécuriser les échanges de données entre deux LAN, on utilise deux solutions opposées :
-relier les deux sites par une ligne spécialisée mais hors de prix.
-créé un réseau privé virtuel sécurisé autrement dit VPN qui encapsule les données dans un tunnel crypté.

Au cours de ce chapitre, nous nous intéresserons à la deuxième alternative. Nous allons commencer notre chapitre par une définition d'un VPN et parler de son principe de fonctionnement. Puis nous allons citer quelques objectif, types de VPN et définir les principaux protocoles réseaux associés et nous donnerons quelques indication qui nous aiderons dans notre choix de la mise en place du VPN.

3.2 Définition d'un réseau privé virtuel (VPN)

Un VPN est un réseau virtuel ou un tunnel sécurisé à l'intérieur d'un réseau permettant à un ou plusieurs postes distants de communiquer de manière sûre et d'échanger des informations de manière sécurisée, tout en empruntant les infrastructures publiques. Les VPN sont très utilisés par les multinationales et grandes sociétés de relier les différents sites. VPN garantie la sécurité et la confidentialité des données, qui circulent de manière cryptée par Internet, afin que personne de malintentionné ne puisse intercepter les informations.

3.3 Principe de fonctionnement d'un VPN

Un réseau VPN repose sur un protocole de tunnelisation qui permet de chiffrer les données par un algorithme cryptographique entre les deux réseaux autrement dit c'est un protocole qui encapsule dans son datagramme un autre paquet de données complet utilisant un protocole de communication différent etqui permet le passage de données cryptées d'une extrémité du VPN (machine client) à l'autre (machine serveur) grâce à des algorithmes cryptographiques.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu couteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagés, comme internet.

3.4 Objectifs et caractéristiques fondamentaux d'un VPN

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes [14] :

3.4.1 Authentification d'utilisation

Afin de garantir qu'un message provient d'une source authentique, que la personne avec qui la communication est établie est effectivement le destinataire escompté. Les réseaux privés virtuels peuvent utiliser des mots de passe, des

certificats numériques et des cartes à puce pour vérifier l'identité des parties à l'autre extrémité du réseau.

3.4.2 Confidentialité de données

Les VPNs visent à protéger le contenu des messages contre toute interception par des sources non authentifiées ou non autorisées. La confidentialité est garantie grâce à l'encapsulation et au chiffrement effectués.

3.4.3 Gestion de clés

Les VPNs assurent la génération, la distribution, le stockage et la suppression des clés de cryptage pour le client et le serveur avec différents mécanisme et protocoles.
Les clés de cryptage pour le client et le serveur doivent pouvoir être générés et régénérées.

3.4.4 Intégrité des données

Pour garantir qu'aucune altération ou modification n'a été apportée aux données lors de leurs parcours être la source et la destination, les VPN utilisentdes hachages. Un hachage ressemble à une somme de contrôle ou à un seau garantissant que personne n'a lu le contenu, tout en étant plus robuste.

3.4.5 Prise charge multi-protocole

La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

3.5 Les types et les catégories d'un VPN

Suivant les besoins, on peut distinguer trois types standards d'utilisation des VPNs selon leur mode d'utilisation :

3.5.1 VPN d'accès (poste à site)

Le VPN d'accès ou VPN poste à site est utilisé pour permettre à des utilisateurs distants d'accéder au réseau privé ou au réseau de leurs entreprises viaun VPN. L'utilisateur se sert d'une connexion internet pour établir une liaison sécurisé.

Afin de réalisée cette solution nous distinguons deux cas :

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexioncryptée.
- L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise [15]. la figure suivante illustre le VPN poste à site.

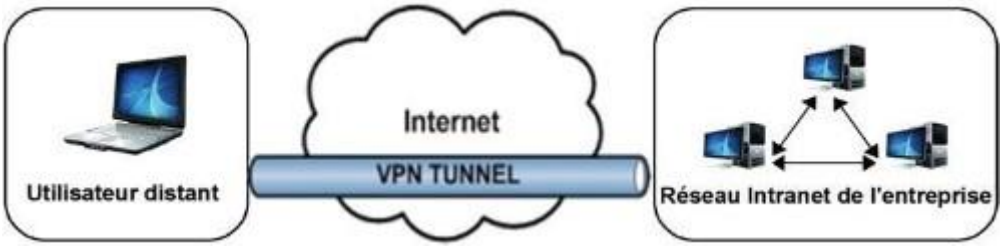

FIGURE 3.1 – Le VPN d'accès poste à site.

3.5.2 L'intranet VPN (site à site)

Il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseaux est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressource, exploitation de serveur distant, etc.) [15].
Le VPN site à site est illustré dans la figure suivante.

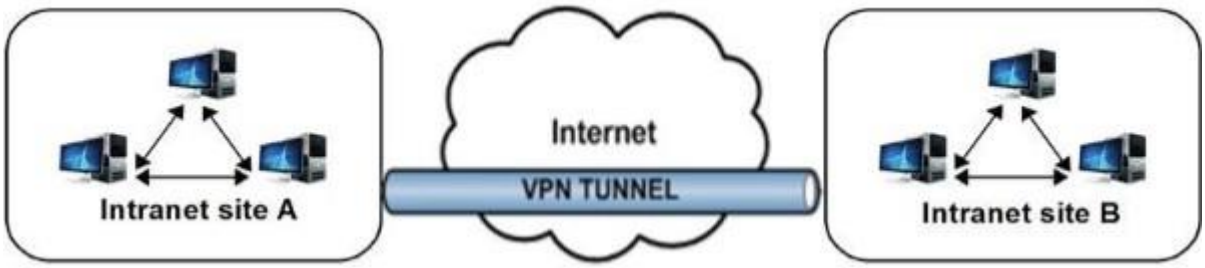

FIGURE 3.2 – L'intranet VPN site à site.

3.5.3 L'extranet VPN (poste à poste)

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et partenaires. Elle ouvre alors son réseau local à ces derniers, dans ce cas il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus en plus, seule une partie des ressources sera partagée, ce qui signifie une gestion rigoureuse des espaces d'échange [15].
La figure si dessous illustre le VPN poste à poste.

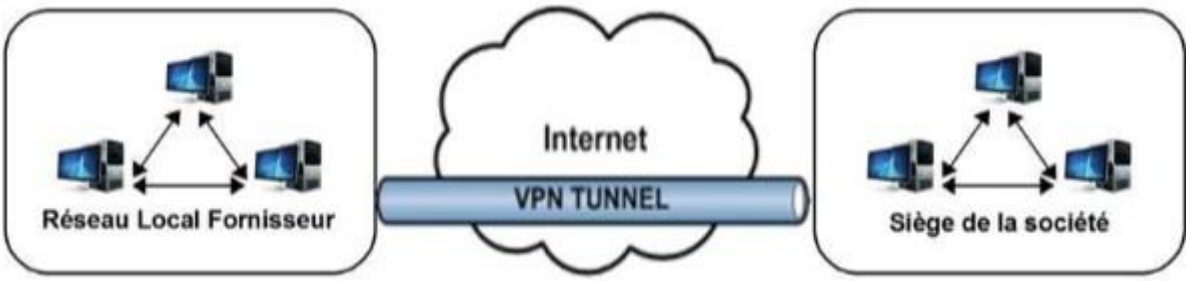

FIGURE 3.3 – L'extranet VPN poste à poste.

3.6 Protocoles utilisés pour réaliser une connexion VPN

Il existe trois niveau de protocole le niveau 2 (travail au niveau de la couche Liaison de données), le niveau 3(travail niveau de la couche IP) et niveau 4(travail niveau de la couche Transport) :

3.6.1 Niveau 2

Dans ce niveau nous trouvons quatre protocoles qui sont :

Point-To-Point Protocol (PPP) : Est un protocole de transfert des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule le paquet IP, IPX et Netbeuidans des trames point à point, puis il transmet ces paquets encapsulés au travers de la liaison point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau(NAS) [15].

Point-to-Point Tunneling Protocol (PPTP) : Un VPN PPTP crée un tunnel qui capture les données. Les VPN PPTP sont utilisés par des utilisateurs distants pour se connecter à leur réseau VPN en utilisant leur connexion internet existante. Les utilisateurs s'y enregistrent en utilisant un mot de passe pré-approuvé dans ce VPN. Les VPN PPTP sont aussi les plus courants grâce à leur compatibilité avec tous les serveurs (Windows, Mac et Linux) [16].

Layer two tunneling protocol (L2TP) : Est issu de la convergence des protocoles PPTP et L2F. IL est actuellement développé et évalué par cisco system, Microsoft, ascend, 3Com ainsi que d'autre acteur clés du marché des réseaux. Il permet l'encapsulation des paquets PPP au niveau des couches 2 et couche 3. Lors de sa configuration pour le transporte des données sur ip, L2tp peut être utilisé pour faire du tunnelling sur internet. Il repose sur deux concepts : les concentrateurs d'accès LTP (Lac Access Concentrator) et les serveurs réseau L2tp (Lns : Network Server). L2TP n'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi L'IETF préconise l'utilisation conjointe d'IPSec et L2TP [15].

Layer Two Forwarding (L2F) : Est un protocole de qui travaille au niveau de la couche 2 conçu par la société cisco. Il est implémenté dans le système d'exploitation IOS (Internetworking Operating System) équipant les équipements de la marque. L2F permet de crée un tunnel, par exemple, entre un serveur d'accès à distance NAS et un routeur, et fonctionne uniquement en mode tunnel.

Les trames PPP sont encapsulées par l'équipement de départ et désencapsulées par l'équipement d'arrivée qui les achemine sur le réseau local de destination.

Dans ce cas dysfonctionnement, le client se connecte à l'ISP par une liaison PPP classique et emprunte le tunnel créé entre le serveur d'accès à

distance et le routeur d'extrémité. Il est noté que le protocole L2F n'a pas de client définit et que plusieurs client peuvent emprunter le même tunnel. Ce protocole est remplacé naturellement pas L2TP qui est plus souple [17].

3.6.2 Niveau 3

Dans ce niveau on trouve deux protocoles qui sont :

Protocole de commutation d'étiquettes (MPLS) : Ce protocole est utilisé pour des connexions de type Site-à-Site. C'est principalement dû aufait que les MPLS sont très flexibles et adaptables. Le MPLS est une ressource normalisée pour accélérer le processus de distribution de paquetsde réseau avec de multiples protocoles. Les VPN MPLS sont des systèmesbasés sur fournisseurs d'accès. On dit çà quand un site ou plusieurs sontconnectés pour former un VPN avec le même fournisseur d'accès ISP. L'inconvénient des VPN MPLS c'est que le réseau n'est pas facile à mettreen place, par rapport aux autre VPN. Il est aussi très difficile à modifier.De plus, les VPN MPLS sont souvent trop chers [16].

Internet Protocol Secuity (IPsec) : IPsec est un protocole VPN utilisé pour sécuriser les échanges de données sur un réseau IP. Un tunnel est mis en place dans entre les deux extrémités et vous permet d'accéder à votre site central. Un IPsec Sécurise le protocole de communication internet en vérifiant chaque session et avec un cryptage individuel des paquets de données pendant toutes la connexion. Il y deux modes distincts d'opération dans un VPN IPsec : le mode de transport et le mode tunnel. Les deux modes servent à protéger le transfert des données entre deux réseaux différents. Avec le mode transport, le message dans les paquets de données est crypté y a pas d'entête IP supplémentaire. Avec le mode tunnel, le paquet de données entier est crypté, un nouveau entête IP est rajouté [16].
La protection IPsec implique six composants principaux :

- **Protocoles de sécurité :**
  - **Authentification Header (AH) :** AH permet d'assurer l'intégrité et l'authentification de la source des paquets IP mais pas la confidentialité des données(ne possède pas de cryptage). Un en-tête AH ajouté au paquet IP contient un hachage des données, permettantde vérifier l'authenticité des données. un numéro de séquence, qui permet la protection contre le rejeu ainsi permet

d'éviter les attaques par inondation. Que des informations qui assurer l'intégrité des données et empêcher la redondance des attaques. Dansce mode on utilise MD5 et SHA-1 comme méthode de cryptage.La Figure 3.4 illustre l'en-tête AH [18].

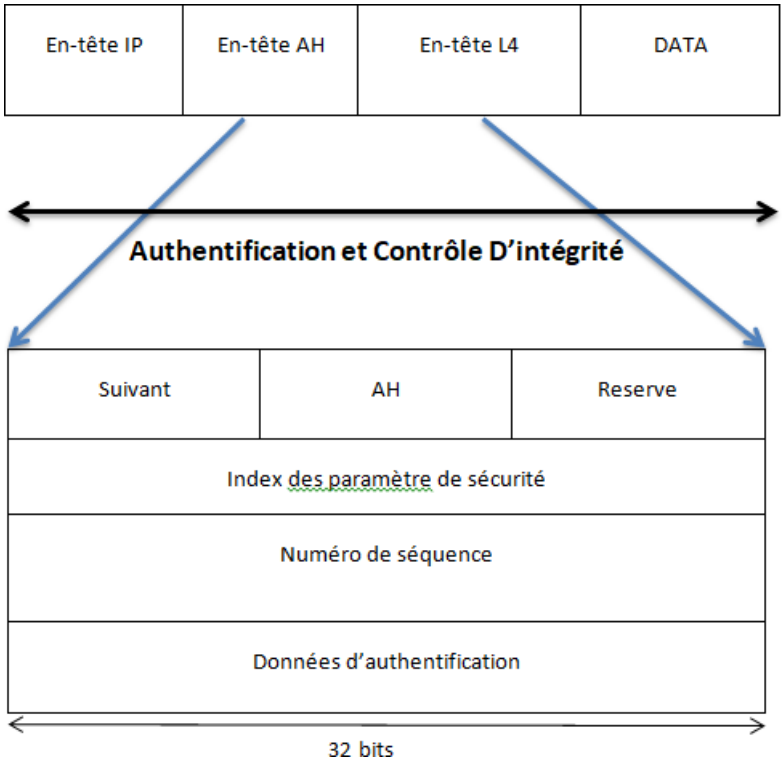

FIGURE 3.4 – En-tête AH.

- **Encapsulation Security Payload (ESP) :** Définie dans RFC 2406, ESP utilise une combinaison de plusieurs services de sécurité,ajout des vérifications d'intégrité pour assurer l'authentification et l'unicité des paquets, et que ces données ne sont pas modifiées au cours du transfère. Il permet aussi la confidentialité des données en utilisant l'algorithme de chiffrement [19]. en trouve deux méthodes de cryptage utilisé par ESP qui sont DES et 3DES.
  La Figure 3.5 illustre l'en-tête ESP.

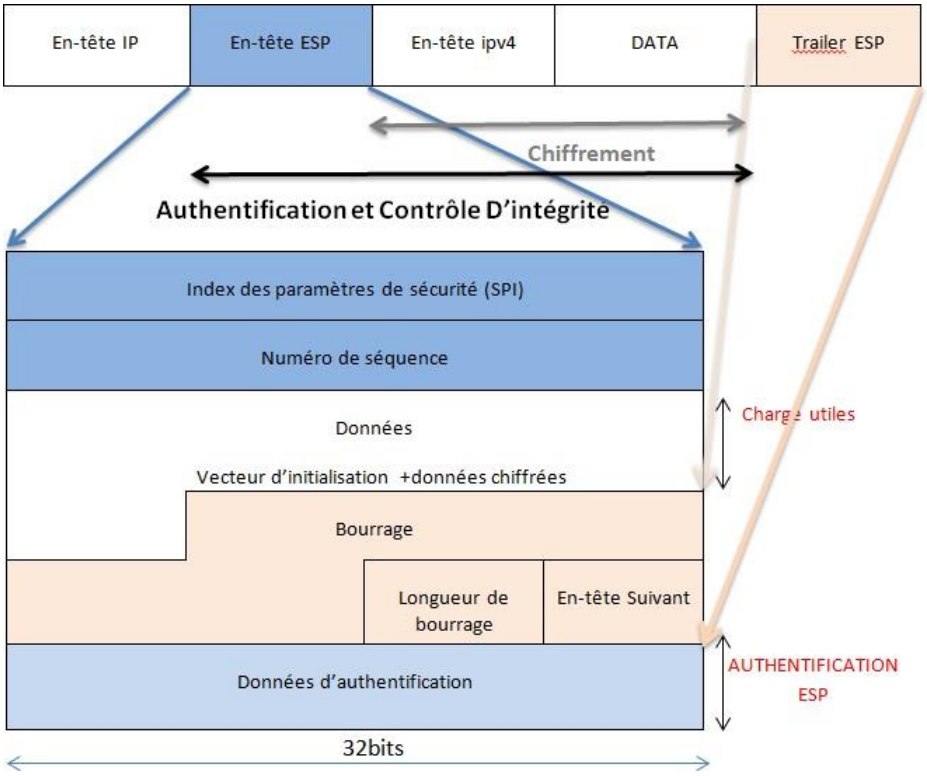

FIGURE 3.5 – En-tête ESP.

- **Mécanismes de sécurité :** Représente les algorithmes de chiffrement et d'authentification qui protègent les données des datagrammes IP Nous allons présenter ci-dessous les mécanismes les plus utilisés :
  - **Algorithme de chiffrement** [19] : C'est l'algorithme qui permet de chiffré les données à l'aide d'une clé, il existe trois algorithme de chiffrement : norme de chiffrement de données (DES) utilise une clé de 56 bits il s'agit du plus faible des trois algorithmes,triple norme de chiffrement de données (3DES) est à base de la norme DES, elle permet de chiffrer trois fois les données on employant la norme DES. norme de chiffrement avancée (AES) c'est l'algorithme le plus puissant, utilise les clés 128, 192 ou 256 bits.

  - **Algorithme d'authentification** [20]: Algorithme de hachage utilisé en cryptographie pour l'authentification es signatures numériques trouve : MD5(Message Digest Algorithm 5) il génère des valeur 128 bits, SHA1(Secure Hash Algorithm 1) il a les même fonctionnalité que MD5, mais SHA-1 génère des valeurs 160 bitset SHA2(Secure Hash Algorithm 2) le plus utilisé aujourd'hui, le successeur de sha1 en trouve SHA-512 une variante de SHA-512 qui génère 512 bits (utilise des mots de 64 octet).

- **Gestion des clés :** Les protocoles de sécurité utilisent des algorithmes de cryptages qui nécessitent des clés de sécurité. La gestion de ces clés se fait avec le protocole IKE.

  - **Internet Key Exchange Protocole IKE :**
    Est utilisé pour la négociation des associations de sécurité IPsec. Un canal de communication sécurisé est créé pour l'authentification et l'échange des clés. L'IKE est également utilisé pour authentifier les deux pairs IPsec. Pare-feu prend en charge IKEv1 et IKEv2 dans la configuration de la passerelle ou d'une interface virtuelle vpn [19]. Il procède avec deux phases :

    La phase une : Appeler également la Phase Internet Sécurité Association and Key Management protocole Sécurité Association (SA ISAKMP) est un moyen sécurisé sur lequel IKE se procure les numéros de clés des datagrammes IP. À l'inverse des SA IPsec, les SA ISAKMP sont bidirectionnelles. Une seule association de sécurité est donc nécessaire [21].

    La phase deux : Ou IPSec Security Associations (SA IPsec) elle se produit après la phase 1 et est également connu sous le nom de Quick mode, Les échanges de cette phase sont sécurisés grâce à la SA ISAKMP, cette phase permet la négociation des associations de sécurité qu'on désire établir dans mécanisme de sécurité que ce soit le AH ou ESP.

- **Les bases de données SPD et SAD**

  - **Security Policy Database, base de données de stratégie de sécurité (SPD) :** base de données indiquant le niveau de protection à appliquer à un paquet. La base de données SPD filtre le trafic IP et identifie le mode de traitement des paquets. Un paquet peut être rejeté, passer ou sécuriser à l'aide d'IPsec. En ce qui concerne les paquets sortants, les bases de données SPD et SADB déterminent le niveau de protection à appliquer. Pour les paquets entrants, la base de données SPD permet de déterminer l'acceptabilité du niveau de protection. Si le paquet est protégé par IPsec, une consultation de la base de données SPD est effectuée après déchiffrement et vérification du paquet [22].
    Les services de sécurité sont basés sur des mécanismes cryptographiques. IPSec met en jeu deux protocoles en

complément du protocole IP classique : AH et ESP [23].

- **Security Associations Database, base de données des associations de sécurité (SADB) :** Les associations de sécurité sont stockées dans une base de données (Security Association Database, SAD). Cette base de donnée est consultée par l'hôte afin d'identifier la manière dont doit être traité chaque paquet reçu ou à émettre[24].

- **Gestion des flux :**
  - **Security Associations (SA) :** Une association de sécurité (SA, Security Association) IPsec spécifie les propriétés de sécurité que reconnaissent les hôtes lors de la communication. Une seule SA protège les données dans une direction. La protection s'applique à un seul hôte ou à une adresse de groupe (multidiffusion). La communication s'effectuant généralement entre deux organes qui ontla même structure fondamentale ou entre client et serveur, d'oùla sécurité du trafic nécessite la présence de deux SA ainsi lors d'utilisation de AH et ESP [25].On trouve que SA est identifié par plusieurs paramètre de sécurité à savoir : spi sécurité paramètre index, adresses IP destination, paramètre d'authentification, paramètre de chiffrement, durée de vie des clés, Duré de vie de SA, mode de protocole.
  - **Security Policy (SP) :**
    Une politique de sécurité définit les objectifs et les contraintes du programme de sécurité. Elle spécifie les règles utilisées pour protéger les réseaux. Il est configuré par l'administrateur réseau afin de déterminer quel trafic peut passer à travers le pare-feu et quel trafic doit être bloqué. Les stratégies de sécurité sont un concept de base et une fonction essentielle des pare-feu [26].
- **Service de sécurités offert par IPsec :**
  - Authentification des extrémités.
  - Confidentialité des données échangées.
  - Authenticité des données.
  - Intégrité des données échangées.

3.6.3 Niveau 4

Dans ce niveau on trouve un seul protocole à ce niveau :

Secure Sockets Layer (SSL) et Transport Layer Security (TLS) : Ils fonctionnent ensemble comme un seul protocole. Les deux sont utilisés pour construire une connexion VPN. Dans cette connexion VPN, le navigateur internet sert de client et l'accès utilisateur est restreint à certaines applications seulement plutôt qu'un réseau entier. Les protocoles SSL et TLS sont principalement utilisés par des sites de vente en ligne et des fournisseurs de service.
Un VPN SSL et TSL vous offre une session sécurisée du navigateur de votre PC au serveur de l'application. C'est parce que les navigateurs internet passent facilement au SSL sans que l'utilisateur ait besoin de faire grand-chose. Les navigateurs web possèdent déjà SSL et TSL de façon intégrée. Les connexions SSL commencent SSL commencent par https au début de l'URL au lieu de http [16].

3.7 Conclusion

Ce chapitre, nous a permis d'avoir une connaissance générale et les différents concepts sur les réseaux VPN, et de comprendre leur principe de fonctionnement ainsi que les différents protocoles utilisé pour les réaliser. Dans le chapitre qui suivra nous intéresserons à l'interconnexion de deux sites VPN de l'entreprise Spa TMF grâce au pare-feu Fortigate, en illustrant les différentes étapes suivies pour aboutir à la réalisation de ce projet.

CHAPITRE 4

IMPLÉMENTATION ET RÉALISATION

4.1 Introduction

Après avoir établi l'étude nécessaire sur la sécurité des données qui circulent entre deux réseaux locaux nous allons dans cette partie présenter les différent étapes afin d'interconnecter les deux sites distants de l'entreprise TMF-AKBOU et celui de TMF-ALGER en spécifiant les outils utilisés ainsi que la configuration réalisée et quelques tests qui montrent le bon fonctionnement et efficacitéde cette solution.

4.2 Les logiciels et équipements utilisés

Nous avons employé déférents logiciels et outils de test a fin de simuler, virtualiser et de tester notre topologie réseau.

4.2.1 Logiciels

Nous avons utilisé trois logiciels :

- **Gns3 :** Graphique Network Simulator il est utilisé pour émuler, configurer, tester et dépanner des réseaux virtuels et réels on dit que Gns3 est un émulateur vu sa capacité d'exécuter des images réelles sur l'appareil virtuel, et un simulateur parce que simule les caractéristiques et les fonctionnalités d'un appareil, il se compose de deux composants logiciels :

  Le logiciel tout-en-un : c'est l'interface utilisateur graphique c'est làoù on peut créer notre topologie.

La machine virtuel (VM) :c'est un serveur étant sous ubuntu, il permet à Gns3 d'exécuter ces fonction sans problème [27].
Illustration de l'interface Gns3 est représenté dans la figure 4.1.

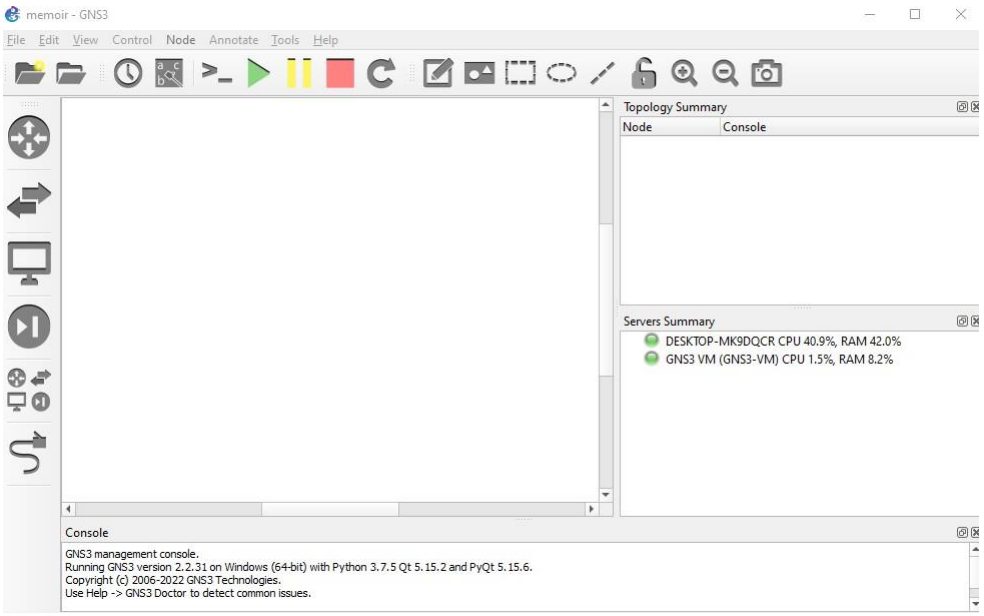

FIGURE 4.1 – L'interface Gns3.

- **Vmware worksation 16 pro :** Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 16 pro qui permet la création d'une ou plusieurs machines virtuelles, au sein d'un même système l'exploitation (généralement Windows ou Linux), celle-ci peuvent être reliées au réseau local avec des adresses IP différentes, tout en étant sur la même machine physique (machine existante réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps [28].
  La figure suivante représente l'interface de la VMware Workstation 16 Pro.

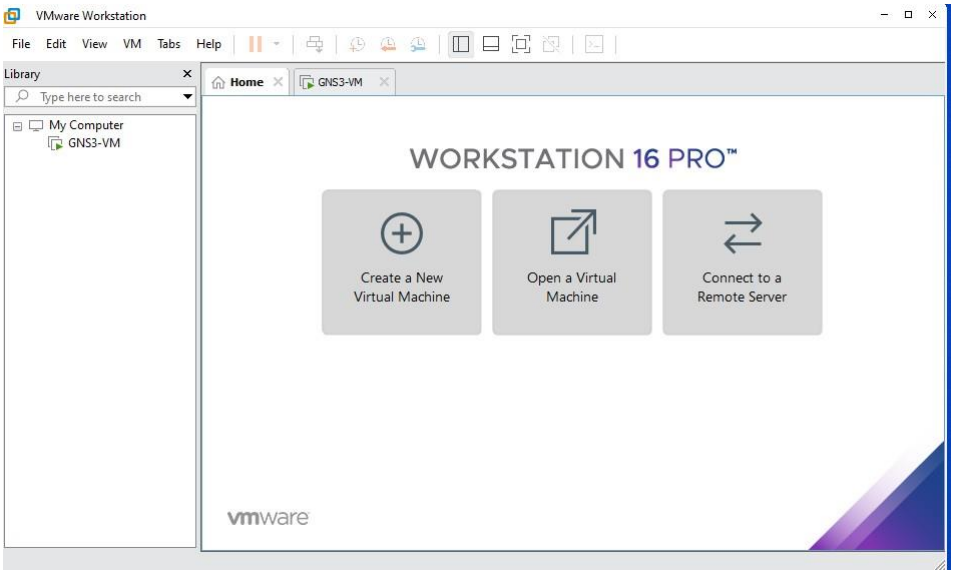

FIGURE 4.2 – L'interface Vmware workstation.

- **Wireshark :** C'est un outil de capture et d'analyse de paquets réseau Open Source destiné aux administrateurs réseau et aux développeurs, Wireshark est une référence en matière d'analyse des transactions réseau. Cet outil puissant supporte plusieurs centaines de protocoles et dispose de fonctions de filtrage avancé pour la capture et l'interprétation des données, la figue ci-dessous illustre l'interface wireshark [29].

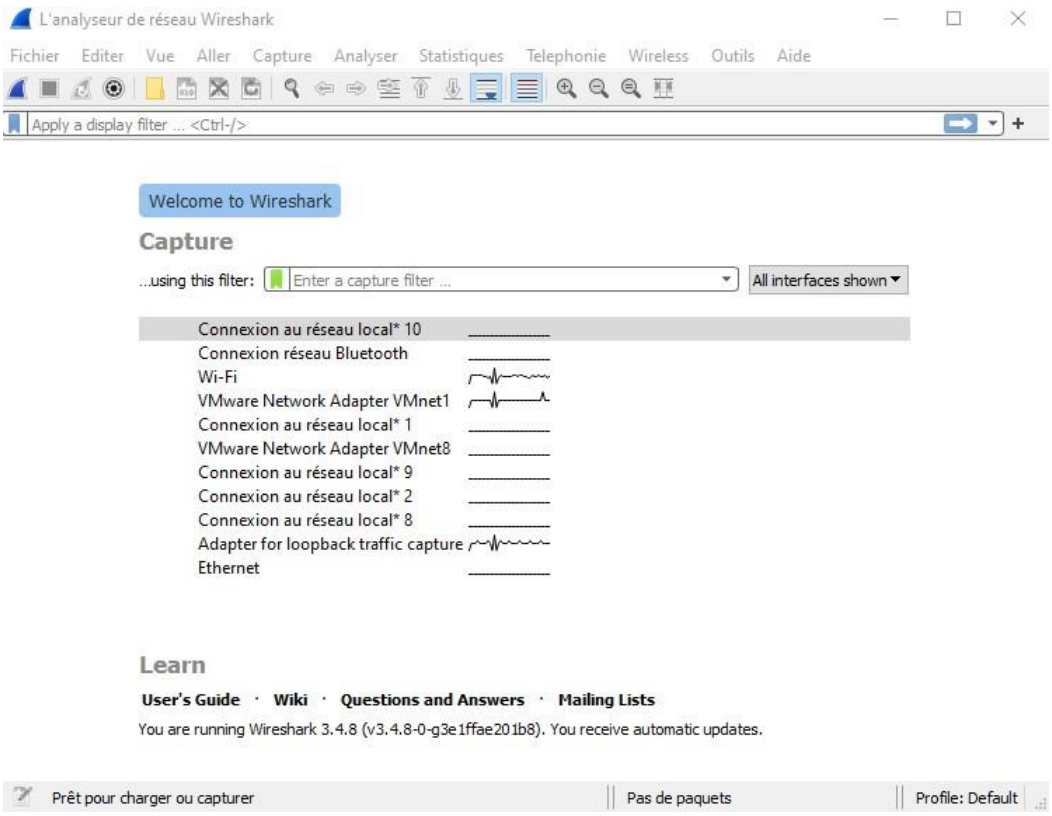

FIGURE 4.3 – L'interface Wireshark.

4.2.2 Équipement requis

Pour faire le test du protocole IPsec, nous avons créé deux réseaux LANs et afin d'assurer le bon fonctionnement de notre configuration nous avons utilisé plusieurs équipements parmi lesquels nous citons : Firewall (fortigate) version 6.4.9, Microsoft Windows serveur 2016, Microsoft Windows 7, Switch, VPC, cloud (Permet d'avoir adresse IP WAN).

4.3 La réalisation des deux architectures

Nous allons suivre plusieurs étapes pour la réalisation de notre topologie :

4.3.1 L'architecture réseau

L'architecture proposée dispose de deux sites distants site Spa TMF Logistics-AKBOU et site Spa TMF Logistics -ALGER, notre topologie illustre leurs interconnexions via un tunnel VPN.

Le site de Spa TMF-AKBOU (site central) est représenté par un Fortigate pourlequel nous avons attribué les interfaces suivantes :

-Relié au réseau public par le port 1 : 192.168.92.5/24.

-Relié au réseau local par le port 2 : 192.168.75.1/24.

Le site de Spa TMF-ALGER est représenté par un Fortigate pour lequel nousavons attribué les interfaces suivantes :

-Relié au réseau public par le port 1 : 192.168.92.65/24.

-Relié au réseau local par le port 2 : 192.168.35.1/24.

La figure ci-dessous nous montre l'architecture réseau réalisé. Logistics :

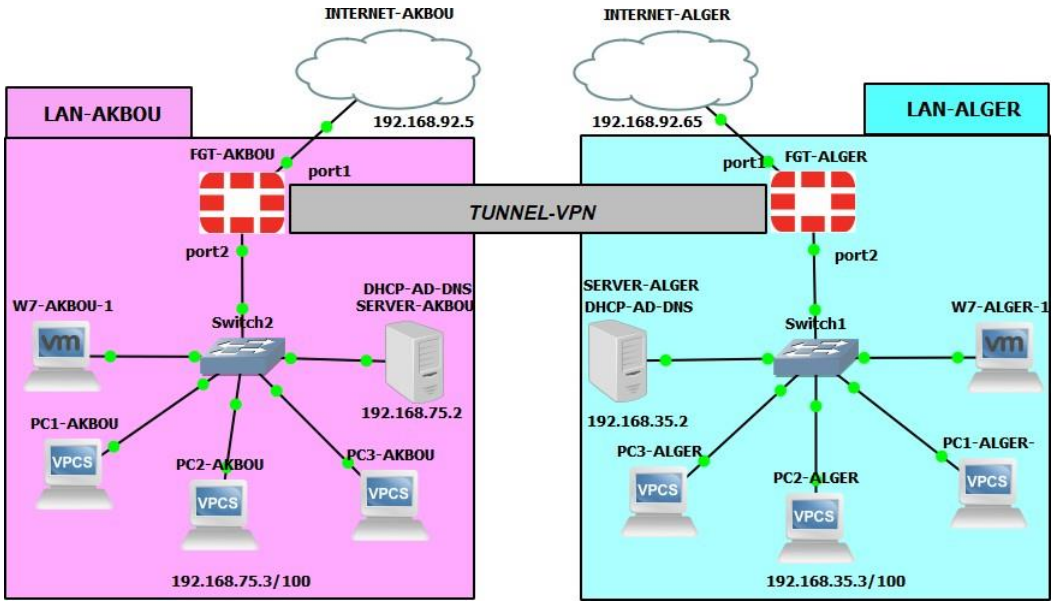

FIGURE 4.4 – Architecture réseaux réalisé.

4.3.2 La plage d'adresse

Les adresses utilisées dans l'architecture sont présenté dans ce tableau (voir la figure 4.5).

Equipement	Interface	Adresse ip d'interface	Masque
FGT-AKBOU	port1	192.168.92.5	255.255.255.0
	port2	192.168.75.1	255.255.255.0
FGT-ALGER	port1	192.168.92.65	255.255.255.0
	port2	192.168.75.1	255.255.255.0

FIGURE 4.5 – Tableau de la plage d'adressage.

4.3.3 Configuration de serveur et de DHCP :

- **Configuration de serveur Windows 2016 :** La configuration des deux serveurs qui se trouvent dans les deux LANs se fait statiquement. La figurequi suit nous montre comment attribuer une adresse IP manuellement pour les serveurs on prend exemple sur le serveur site Spa TMF-AKBOU.

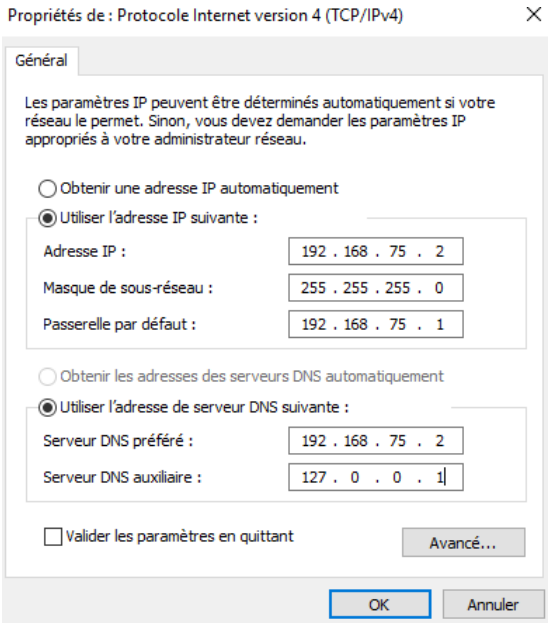

FIGURE 4.6 – Configuration statique de serveur d'AKBOU.

Après l'affectation de l'adresse IP pour le serveur Spa TMF-AKBOU et le serveur Spa TMF-ALGER, on a configuré l'active directory, le DNS et le DHCP. Nous allons nous intéresser seulement à l'illustration de la configuration du DHCP et nous allons présenter les étapes essentielles de la configuration du DHCP.

- **Configuration de DHCP :** Dans cette étape de configuration nous allons configurer le DHCP dans les deux serveurs pour que les ordinateurs aient une attribution automatique d'adresses IP.
  Pour activer le serveur DHCP nous passons par plusieurs étapes :

  - Nous autorisons DHCP dans le domaine du compte administrateur, aprèsavoir choisi le compte administrateur nous validons, l'assistant configuration post-installation crée des groupes de sécurité et l'autorisation du serveur.

  - Après le lancement de la console DHCP via le gestionnaire du serveur, nous créons une nouvelle étendue IPV4 afin que les

ordinateurs puissent obtenir une adresses ip, nous allons attribuer un nom à notre étendu que nous voulons créer, La figure ci-dessous nous montre le nom.

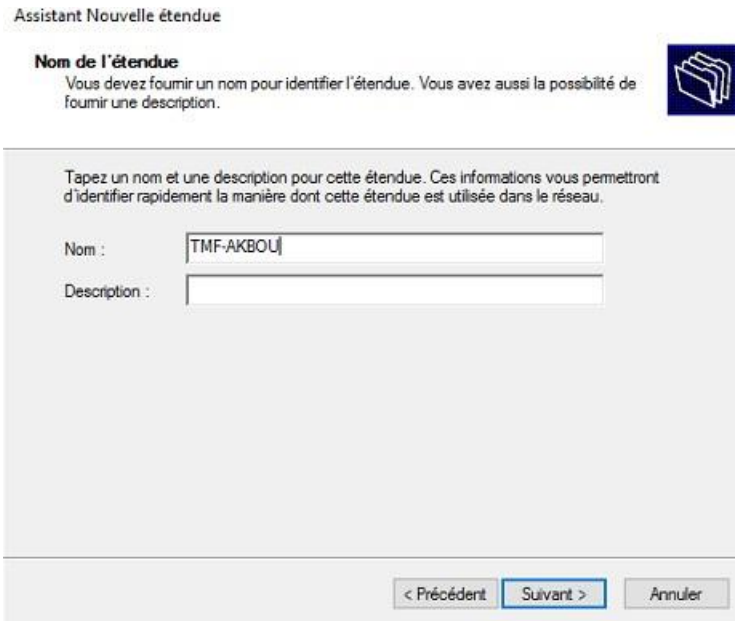

FIGURE 4.7 – Spécification du nom pour l'étendu.

- Dans cette étape nous introduisons la plage d'adresse à cet étendu c'est elle qui définis le nombre maximal d'adresses que nous pouvons distribuer aux ordinateurs par le serveur TMF-AKBOU. La figure ci-dessous nous montre l'ajout de la plage d'adresses de distribution.

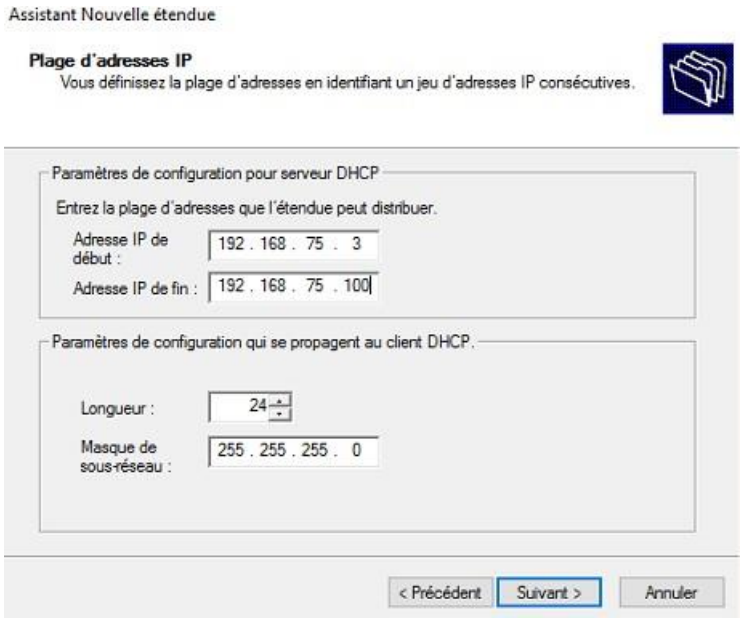

FIGURE 4.8 – La plage d'adresse IP de distribution du Serveur.

- En suit nous définissons une plage d'adresses qui ne seront pas distribuer par le serveur TMF-AKBOU. La figure ci-dessous nous montre l'ajout de la plage d'adresses exclusion.

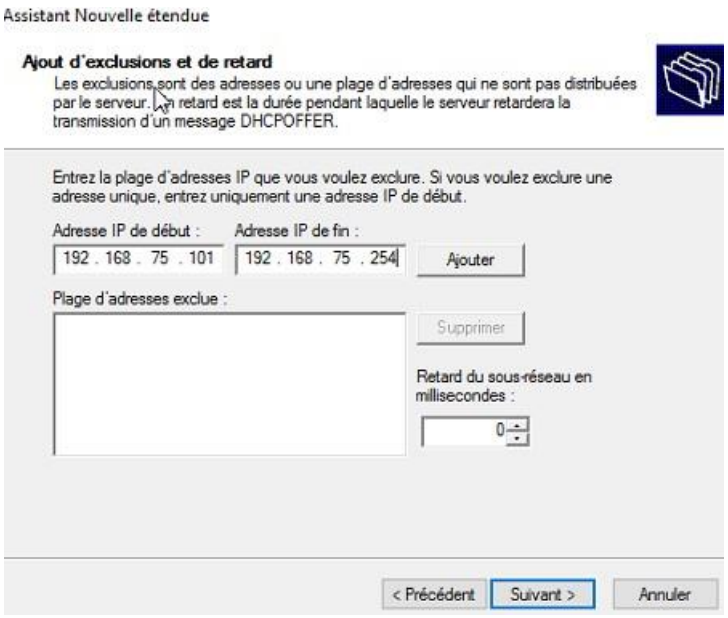

FIGURE 4.9 – La plage d'adresse IP d'exclusion de Serveur.

- La durée du bail : est la durée pendant laquelle un ordinateur peut utiliser une adresse ip de l'étendu que nous sommes en train de crée.La figure ci-dessous nous montre la durée du bail.

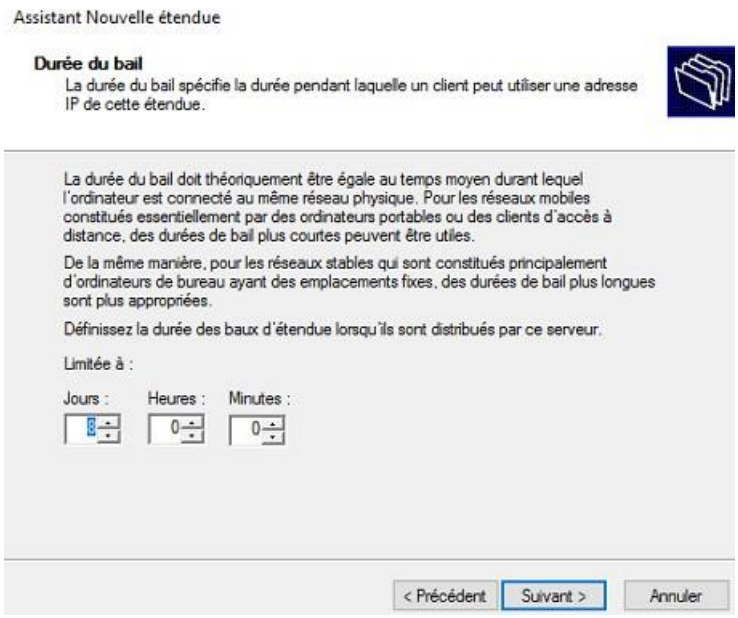

FIGURE 4.10 – La durée du bail.

- Confirmation de la configuration des paramètres de DHCP.
- ajouter la passerelle par défaut, c'elle ci sera ajouté pour tous les ordinateurs qui se trouvent dans Spa TMF-AKBOU. La figure ci-dessous nous montre ajout de la passerelle.

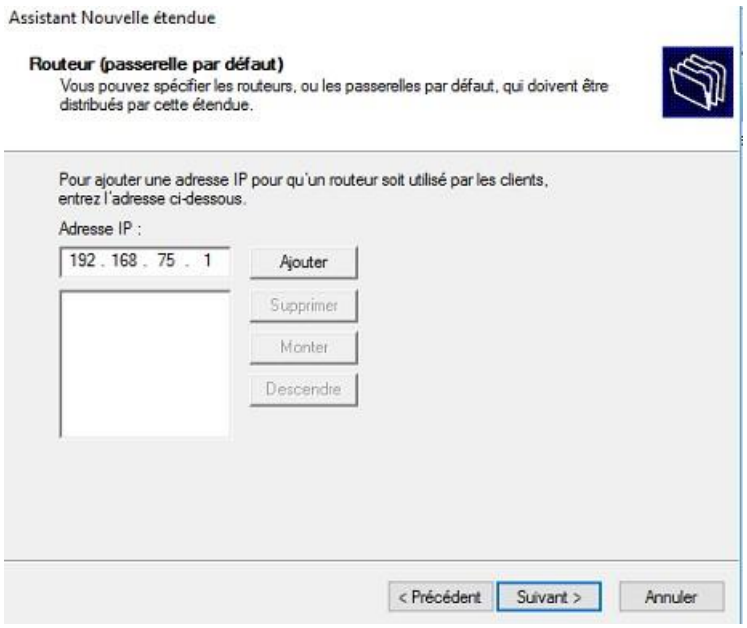

FIGURE 4.11 – Ajout de l'adresse de la passerelle.

- Nous rajoutons l'adresse de serveur DNS et nous spécifions le nom de domaine. La figure ci-dessous nous montre l'ajout d'adresse de serveur DNS et le nom de domaine.

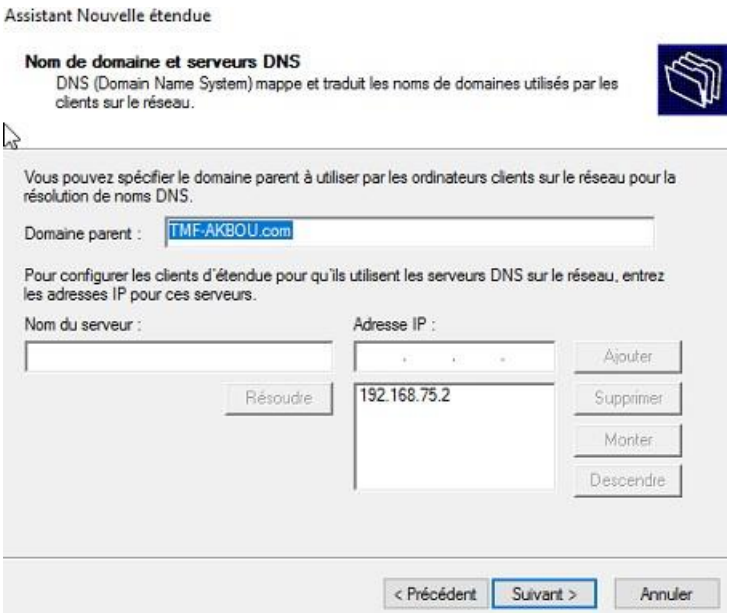

FIGURE 4.12 – L'ajout de l'adresse de Serveur DNS et le nom de domaine.

- Nous choisissons d'activer l'étendu maintenant.

4.3.4 Configuration de base du Fortigate Spa TMF

Pour la configuration des ports du Fortigate nous allons le faire dans le terminal en entrant dans l'interface système de configuration nous modifions le port1 (celui-ci qui représente le WAN) et le port 2 (celui qui représente le LAN) nous leur donnons des adresses ip et des masques après nous spécifions le rôle de chaque port du site Spa TMF-AKBOU ainsi que le port de site Spa TMF-ALGER. LA figure 4.13 représente les différentes commandes utilisées pour la configuration de base des ports pour les deux sites

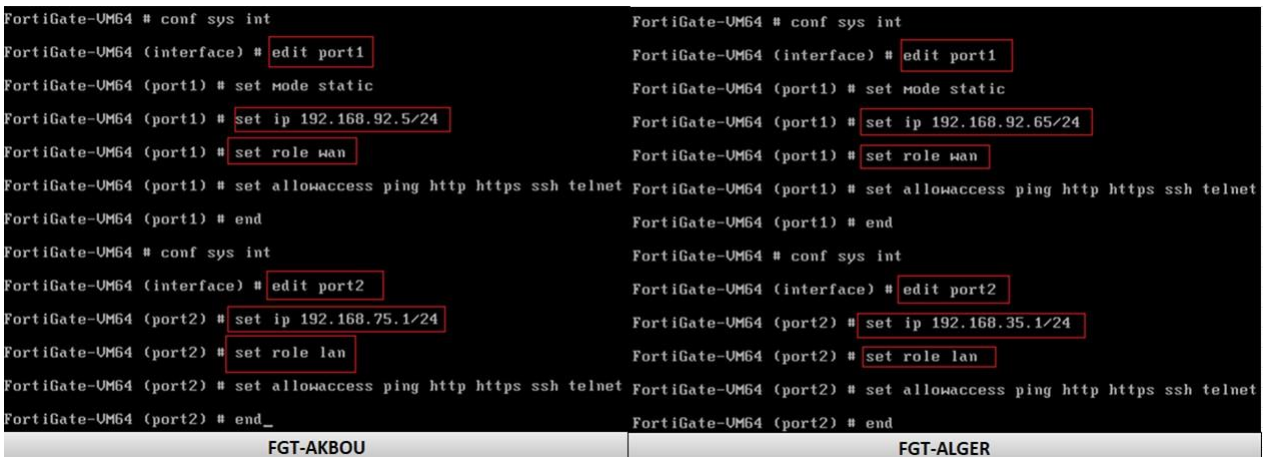

FIGURE 4.13 – La configuration basique des deux sites.

- config sys interface : configuration système interface elle permet d'accéder à interface du système de configuration.
- edit port : modifier le port.
- set role wan : spécifier que ce port est le port WAN.
- set role lan : spécifier que ce port est le port LAN.
- set mode static : on définit le mode de configuration statique.
- set allowaccess : configurer le protocole que les administrateurs peuventutiliser et parmi ces protocole on a choisi en trouve :

  - ping : commande qui permet de valider l'accessibilité entre les machines.
  - http : autoriser les connexions http a l'interface utilisateur web du Fortigate.
  - https : autoriser les connexions http sécurisées pour interface utilisateur web du Fortigate.
  - ssh : active la connexion ssh à interface de ligne de commande.
  - telnet : active la connexion telnet elle est recommandée pour les interfaces réseau connectées à un réseau privé.

Nous allons accéder dans le navigateur qui se trouve dans Windows 7, nous saisissons l'adresse ip de la passerelle qui se trouve dans le réseau lan, un nom d'utilisateur (username) et un mot de passe (password) vont apparaitre et ils sont obligatoires afin de pouvoir accéder à l'interface du Fortigate.

4.3.5 Création et configuration du VPN IPsec

Dans cette partie nous allons expliquer les étapes à suivre pour la création et la configuration de tunnel VPN entre deux sites distants le site Spa TMF-AKBOU et celui de Spa TMF-ALGER :

- **Création du tunnel VPN Site Spa TMF-AKBOU :**

  Pour créer un nouveau tunnel VPN IPsec, nous allons nous connecter à FGT-AKBOU, accéder au VPN puis dans IPsec Wizard on crée un nouveau tunnel. On procède par plusieurs étapes.

- **L'étape VPN setup :** Elle consiste à définir un nom pour notre tunnel qui est TMF-AKBOU, le type de modèle VPN dans notre cas est un VPNsite à site, le type de périphérique distant utilisé est Fortigate dans les deux sites et il faut choisir NOT NAT between site pour la configurationde NAT.

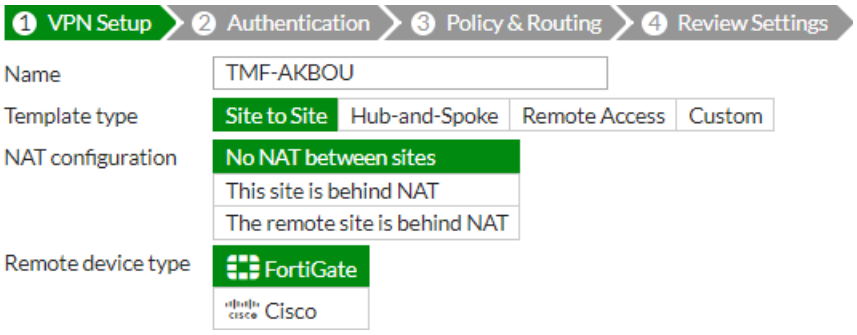

FIGURE 4.14 – L'étape VPN setup.

- **L'étape Authentification :** comme nous somme dans la configuration de site Spa TMF-AKBOU nous mettons dans adresse IP l'adresse IP publique du Fortigate d'Alger, après cela l'assistant attribue automatiquement le port de l'interface sortante, et nous sélectionnons la méthode d'authentification clé pré partagé et nous saisissons le mot de passe qui sera échangé entre les deux sites afin d'établir le tunnel VPN.

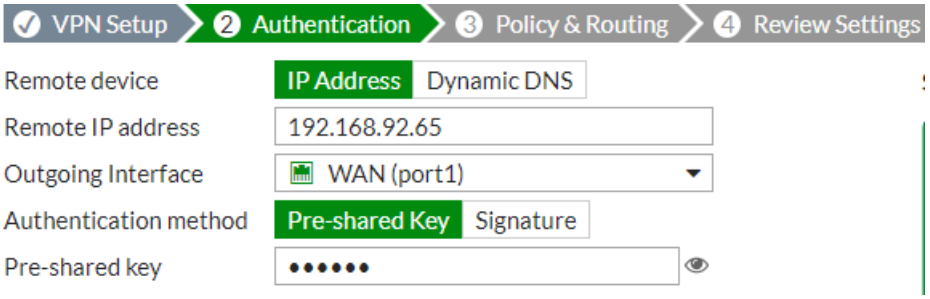

FIGURE 4.15 – L'étape d'authentification.

- **L'étape Policy et Routing :** nous définissons l'interface locale sur le port du LAN, l'assistant ajoute automatiquement le sous-réseau local, et dans remote subnet nous introduisons l'adresse du réseau LAN du site Spa TMF-ALGER, et nous choisissons l'accès internet sur none.

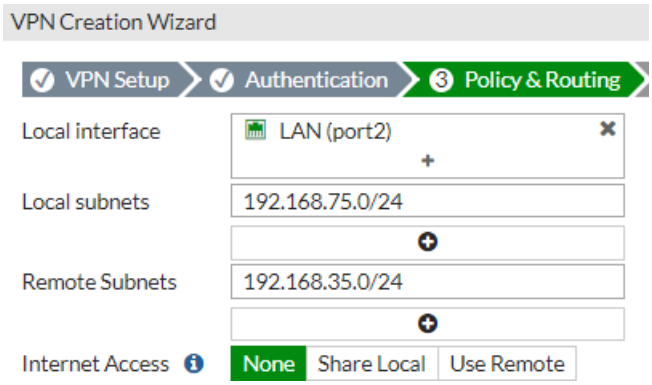

FIGURE 4.16 – L'étape de plicy et routing.

- **L'étape Review Settings :** L'assistant nous affiche un résumé de la configuration que nous avons créé, y compris les interfaces, les adresses de Fortigate ainsi que les routes et politiques. afin de finaliser la création de tunnel nous cliquons sur crée.

- **Négociation du tunnel VPN IPsec :** La négociation VPN est un processus qui consiste à la création d'un tunnel VPN, pour cela les deux périphériques d'extrémités qui sont des pairs IPsec échangent une série de messages relatifs au chiffrement et à l'authentification puis tentent de s'accorder sur de nombreux paramètres.

Pour gérer les négociations entre deux Fortigate, IPsec utilise le protocole IKE (Internet Key Exchange), ce dernier gère la connexion entre les deux Fortigate en deux phases : Phase une et phase deux.

Phase une :

La configuration doit être identique dans les deux extrémités pour définir les termes des négociations ISAKMP, On crée une politique ISAKMP, qui comprend :

-Une méthode d'authentification, dans notre cas on va utiliser la méthode des clés pré-partagées pour assurer l'identité des pairs.

-On choisit le mode principale comme mode de transfère avec la version IKE v1.

-Une méthode de cryptage, en utilisant deux l'algorithme de chiffrement DES afin de protéger les données et assurer la confidentialité.

-On definis comme méthode d'authentification de message haché le SHA-512 (le plus sécurisé utilise des mots de 64 octet) et pour garantir l'identité de l'expéditeur et pour assurer que le message n'a pas été

Modifié en transit.

-Un groupe Diffie-Hellman 14 et 5 pour déterminer la force de l'algorithme de détermination de la clé de chiffrement, utilisation de cet algorithme est indispensable.

-Limite de temps : le délai de vie d'association de sécurité pendant laquelle il peut utiliser une clé de chiffrement.

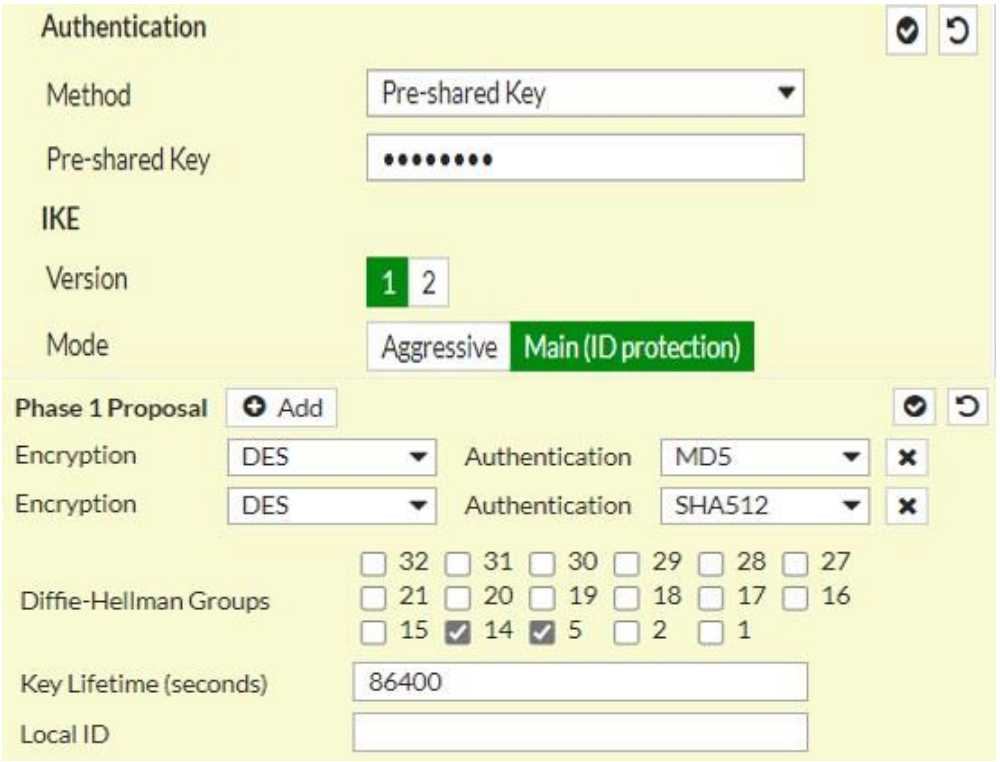

FIGURE 4.17 – Configuration de la phase une de site Spa TMF-AKBOU.

Phase deux :

Elle a pour but de définir les algorithmes de chiffrement et de transfert des données pour le reste de la session et d'associer les paramètres IPsec de la phase 2 avec la configuration de la phase 1 et spécifient le point finale à distance du tunnel VPN.

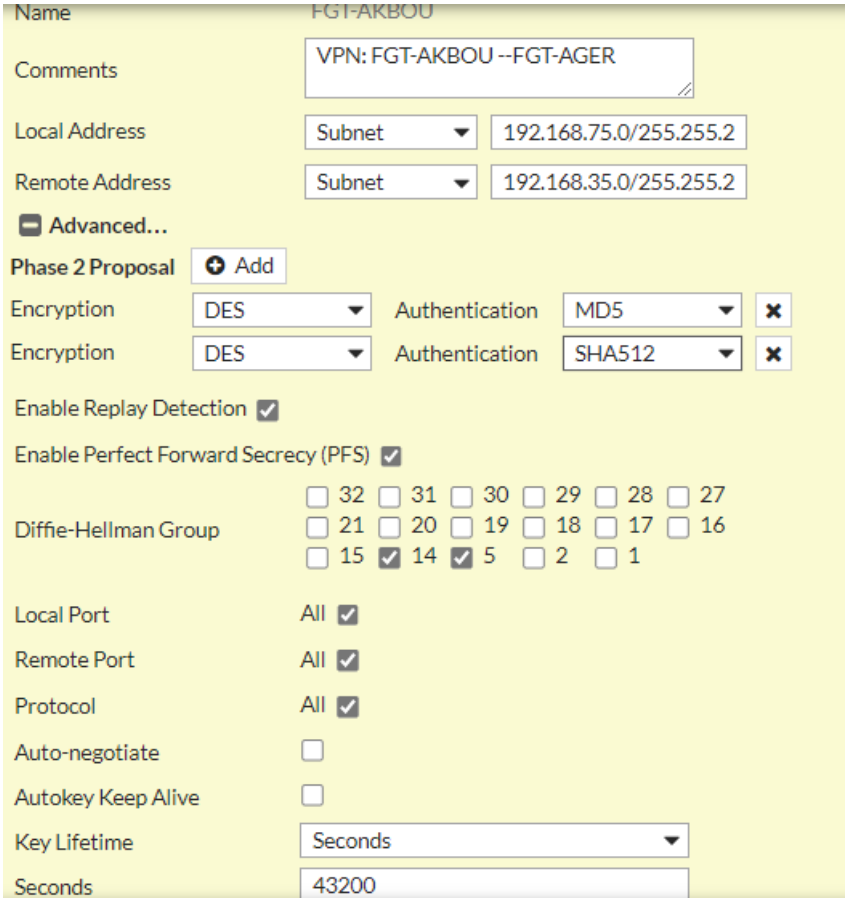

FIGURE 4.18 – Configuration de la phase deux de site Spa TMF-AKBOU.

- **Création du tunnel VPN Site Spa TMF-ALGER**

  On passera par les mêmes étapes lors de la création du tunnel dans Fortigate de TMF-AKBOU, on doit se connecter à GT-ALGER, accéder au VPN puis dans IPsec Wizard on crée un nouveau tunnel. En suis les même étapes lors de la création de tunnel coté TMF-AKBOU.
  Les étapes à suivre pour la création d'un tunnel VPN sont :

  - **L'étape VPN setup :** On définit le nom TMF-ALGER, et le type de modèle sur site à site, et type de périphérique distant sur Fortigate, on met NOT NAT between sit dans le NAT configuration.

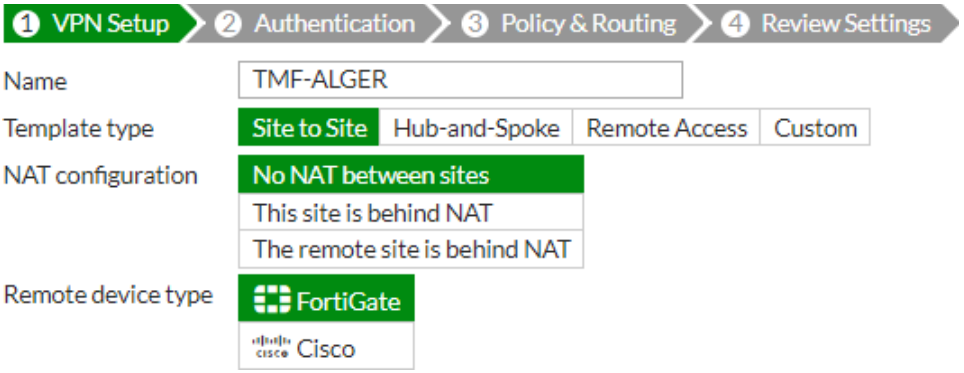

FIGURE 4.19 – L'étape vpn setup.

- **L'étape d'authentification :** comme nous somme dans la configuration de site Spa TMF-AKBOU nous mettons dans adresse IP l'adresse IP publique du Fortigate D'AKBOU, l'assistant attribue automatiquement le port de l'interface de sortie, et nous sélectionnons la méthode d'authentification clé pré-partagé et nous saisissons le même mot de passe que on a déjà saisi dans extrémité qui se trouve dans TMF-AKBOU.

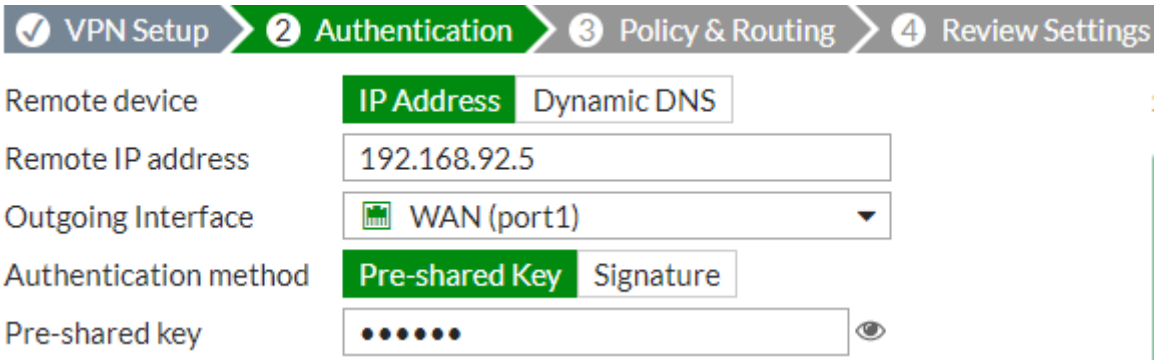

FIGURE 4.20 – L'étape d'authentification.

- **L'étape Policy et Routing :** nous définissons interface locale sur le port du LAN, l'assistant ajoute automatiquement le sous-réseau LAN du TMF-ALGER, et nous introduisons l'adresse du réseau LAN dusite Spa TMF-AKBOU dans Remote subnet, et enfin nous choisissons l'accès internet sur none.

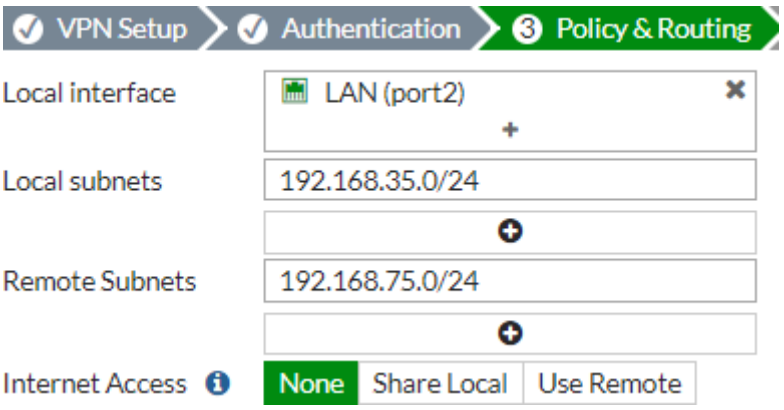

FIGURE 4.21 – L'étape Policy et Routing.

- **L'étape Review Settings :** L'assistant nous affiche un résumé de la configuration que nous avons créé, y compris les interfaces, les adresses de Fortigate ainsi que les routes et politiques. afin de finaliser la création de tunnel nous cliquons sur crée.

- **Négociation du tunnel VPN Ipsec de site Spa TMF-ALGER :** elle consisteà définir l'adresse de la passerelle de l'interface WAN ainsi que le mot de passe utilisé et les protocoles de cryptage de la clé partagée nécessaires pour le tunnel VPN :
  La négociation VPN ce fait en deux phase

  Phase une :
  La configuration doit être identique dans les deux extrémités pour définir les termes des négociations ISAKMP, On crée une politique ISAKMP, qui comprend :
  -Une méthode d'authentification, dans notre cas on va utiliser la méthode des clés pré-partagées pour assurer l'identité des pairs.
  -On choisit le mode principale comme mode de transfère avec la version IKE v1.
  -Une méthode de cryptage, en utilisant deux l'algorithme de chiffrement DES afin de protéger les données et assurer la confidentialité.
  -On definis comme méthode d'authentification de message haché le SHA-512 (le plus sécurisé utilise des mots de 64 octet) pour garantir l'identité de l'expéditeur et pour assurer que le message n'a pas été modifié en transit.
  -Un groupe Diffie-Hellman 14 et 5 pour déterminer la force de l'algorithme de détermination de la clé de chiffrement, utilisation de cet algorithme est indispensable.

-Limite de temps : le délai de vie d'association de sécurité pendant laquelle il peut utiliser une clé de chiffrement.

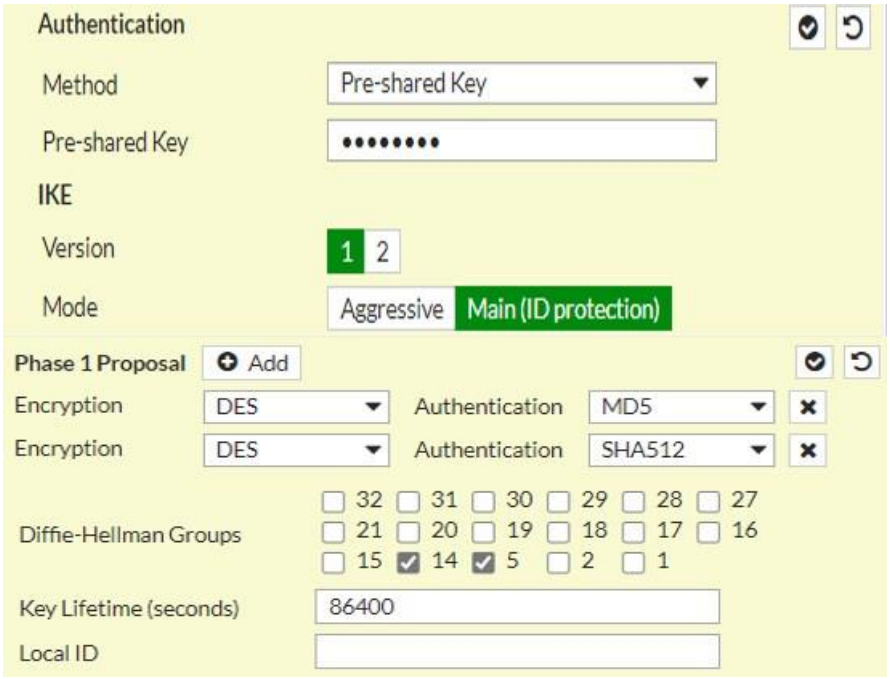

FIGURE 4.22 – Configuration de la phase une de site Spa TMF-ALGER.

Phase deux :

Elle permet de définir les algorithmes de chiffrement et de transfère de donnée que l'unité FortiGate peut utiliser pour le reste de la session et l'association des paramètres IPSec de la phase 2 avec la configuration de la phase 1 et spécifient le point final à distance du tunnel VPN.

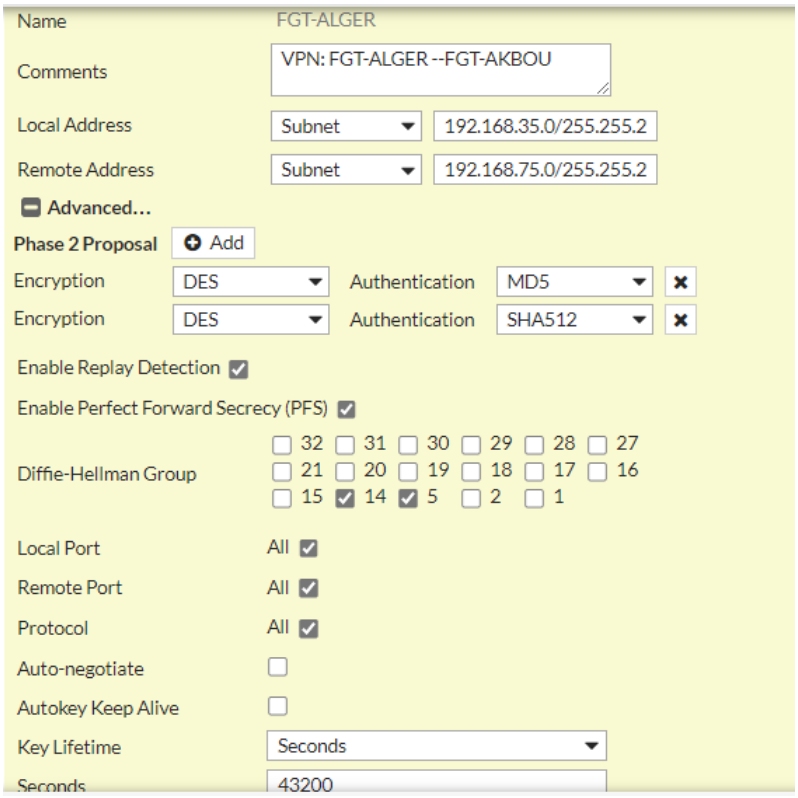

FIGURE 4.23 – Configuration de la phase deux de site Spa TMF-ALGER.

4.3.6 Création et configuration des routes statiques

Nous allons établir une route statique dans chaque site :

- **Site Spa TMF-AKBOU :** Pour créer la route statique de ce site vers le site d'ALGER nous allons accéder au Fortigate du site Spa TMF-AKBOU, nous sélectionnons l'icône network et parmi les options affichées nous choisissons statique route statique route et nous effectuons la configuration montrée sur la figure (4.25) pour la destination nous spécifions l'adresse LAN d'ALGER et pour l'interface il faut préciser le tunnel TMF-AKBOU.

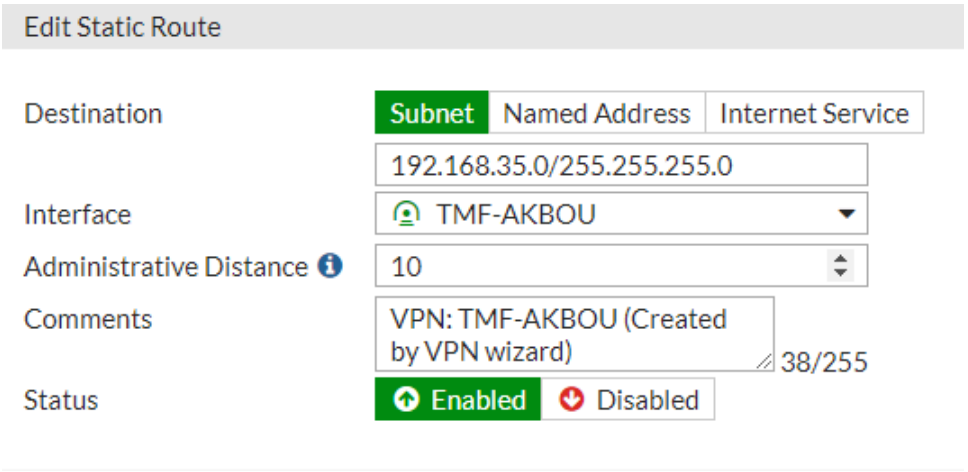

FIGURE 4.24 – La création de la route statique site Spa TMF-AKBOU.

- **Site Spa TMF-ALGER :** Pour créer la route statique de ce site vers le site d'AKBOU nous allons accéder au Fortigate du site Spa TMF-ALGER, nous sélectionnons l'icône network et parmi les options affichées nous choisissons statique route statique route et nous effectuons la configuration montrée sur la figure (4.26) pour la destination nous spécifions l'adresse LAN d'AKBOU et pour l'interface il faut préciser le tunnel TMF-ALGER.

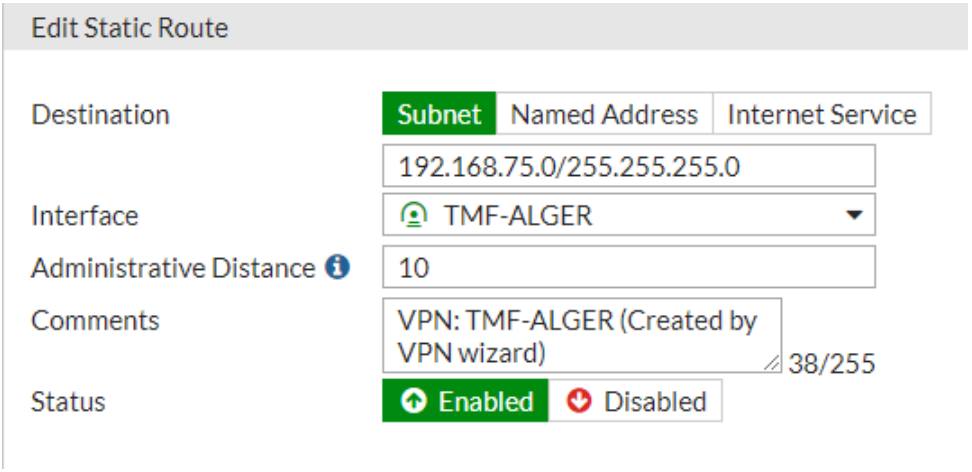

FIGURE 4.25 – La création de la route statique site Spa TMF-ALGER.

4.3.7 Définition des régles

La définition des règles se fait des deux côtés AKBOU et ALGER comme suit :

- **Coté Spa TMF-AKBOU :**

- **La première règle** : Dans la première règle on accorde l'accès à tous les ordinateurs qui se trouve dans le site Spa TMF-AKBOU d'accéder seulement au ordinateurs 1, 2 ,3 et 4 qui se trouve dans le site Spa TMF-ALGER.
- **La deuxième règle** : Dans la deuxième règle on accorde l'accès à tous les ordinateurs qui se trouve dans le site Spa TMF-ALGER d'accéder seulement au ordinateurs 1,3 et 4 qui se trouve dans le site Spa TMF-AKBOU.

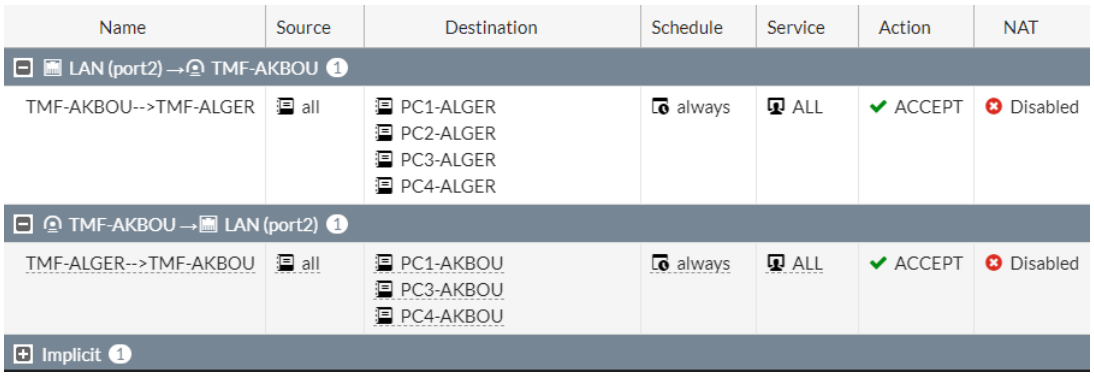

FIGURE 4.26 – Les règles coté Spa TMF-AKBOU.

2- Coté Spa TMF-ALGER :

- **La première règle** : Dans la première règle on accorde l'accès à tous les ordinateurs qui se trouve dans le site Spa TMF-ALGER d'accéder seulement au ordinateurs 1,3 et 4 qui se trouve dans le site Spa TMF-AKBOU.
- **La deuxième règle** : Dans la deuxième règle on accorde l'accès à tous les ordinateurs qui se trouve dans le site Spa TMF-AKBOU d'accéder seulement au ordinateurs 1, 2 ,3 et 4 qui se trouve dans le site Spa TMF-ALGER.

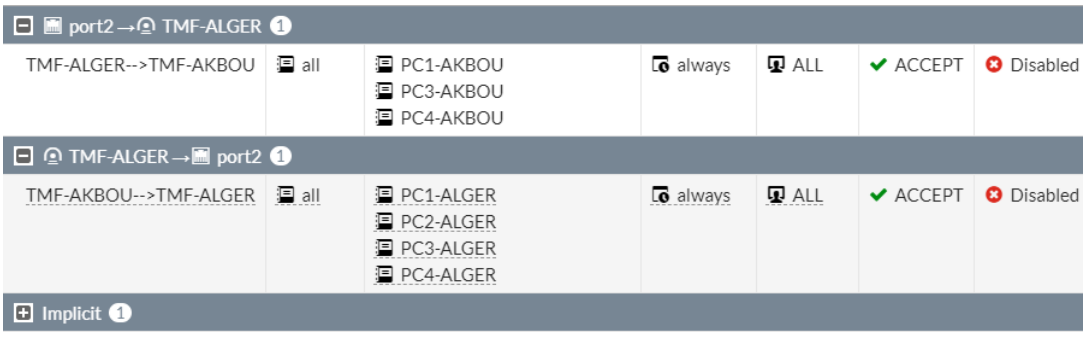

FIGURE 4.27 – Les règles coté Spa TMF-ALGER.

4.3.8 Tests de ping pour la vérification des règles

- **Test de Vérification des règles**

  - **Test de ping vers site Spa TMF-AKBOU :** Après la définition des règles ou on a fait un teste et en constat que le Ping ne passe dans pc1-ALGER vers serveur ayant adresse ip 192.168.75.2 et le pc ayant adresse ip 192.168.75.4 par contre il Ping vers les pc qui possède adresse ip 192.168.75.3, adresse ip 192.168.75.4 et adresse ip 192.168.75.5.

```
PC1-ALGER-> ping 192.168.75.2

192.168.75.2 icmp_seq=1 timeout
192.168.75.2 icmp_seq=2 timeout
192.168.75.2 icmp_seq=3 timeout
192.168.75.2 icmp_seq=4 timeout
192.168.75.2 icmp_seq=5 timeout

PC1-ALGER-> ping 192.168.75.3

84 bytes from 192.168.75.3 icmp_seq=1 ttl=62 time=5.940 ms
84 bytes from 192.168.75.3 icmp_seq=2 ttl=62 time=4.784 ms
84 bytes from 192.168.75.3 icmp_seq=3 ttl=62 time=3.222 ms
84 bytes from 192.168.75.3 icmp_seq=4 ttl=62 time=2.411 ms
84 bytes from 192.168.75.3 icmp_seq=5 ttl=62 time=4.470 ms

PC1-ALGER-> ping 192.168.75.4

192.168.75.4 icmp_seq=1 timeout
192.168.75.4 icmp_seq=2 timeout
192.168.75.4 icmp_seq=3 timeout
192.168.75.4 icmp_seq=4 timeout
192.168.75.4 icmp_seq=5 timeout

PC1-ALGER-> ping 192.168.75.5

84 bytes from 192.168.75.5 icmp_seq=1 ttl=62 time=9.019 ms
84 bytes from 192.168.75.5 icmp_seq=2 ttl=62 time=4.255 ms
84 bytes from 192.168.75.5 icmp_seq=3 ttl=62 time=3.938 ms
84 bytes from 192.168.75.5 icmp_seq=4 ttl=62 time=5.272 ms
84 bytes from 192.168.75.5 icmp_seq=5 ttl=62 time=6.783 ms

PC1-ALGER-> ping 192.168.75.6

84 bytes from 192.168.75.6 icmp_seq=1 ttl=62 time=8.548 ms
84 bytes from 192.168.75.6 icmp_seq=2 ttl=62 time=2.152 ms
84 bytes from 192.168.75.6 icmp_seq=3 ttl=62 time=2.738 ms
84 bytes from 192.168.75.6 icmp_seq=4 ttl=62 time=2.821 ms
84 bytes from 192.168.75.6 icmp_seq=5 ttl=62 time=2.715 ms
```

FIGURE 4.28 – Test de ping vers le site Spa TMF-AKBOU.

- **Test de ping vers site Spa TMF-ALGER :** Après la définition des règles ou on a fait un teste et en constat que on peut pinger du pc1-AKBOU vers les pc ayant adresse ip 192.168.35.3, adresse ip 192.168.35.4et adresse ip 192.168.35.5 et adresse ip 192.168.35.6 par contre il ne passe pas vers le serveur Alger qui possède adresse ip 192.168.35.2.

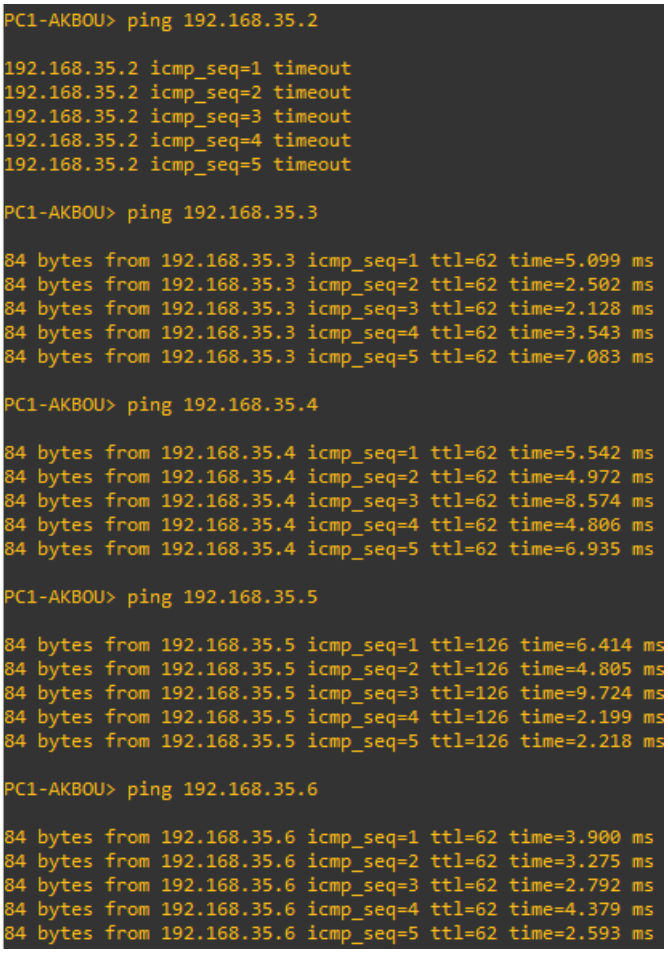

FIGURE 4.29 – Test de ping vers le site Spa TMF-ALGER.

4.4 Vérification du cryptage des données au niveau du tunnel avec Wireshark

On lance la capture wireshark dans l'interface de sortie du Fortigate, on voit que interface wireshark est décomposé en trois cercle (voire la figure 4.30) :

Cercle (1) (Filtrage) :
Permet d'afficher le filtrage de l'ensemble des paquets capture, il est possible de créer une combinaison de filtrage de plusieurs protocoles en même temps. Et cela permettra l'analyse d'un protocole spécifique. Sans spécifiés l'émetteur de la trame, le destinataire de la trame et le protocole réseau mis en œuvre.

Cercle (2) (Encapsulation) :
Permet d'afficher le détail d'un paquet sélectionné dans le premier Cercle et de visualiser la pile des protocoles employés.

Cercle (3) (Détail en hexadécimal) : présente l'ensemble du paquet sous forme octale et la traduction ASCII correspondante.

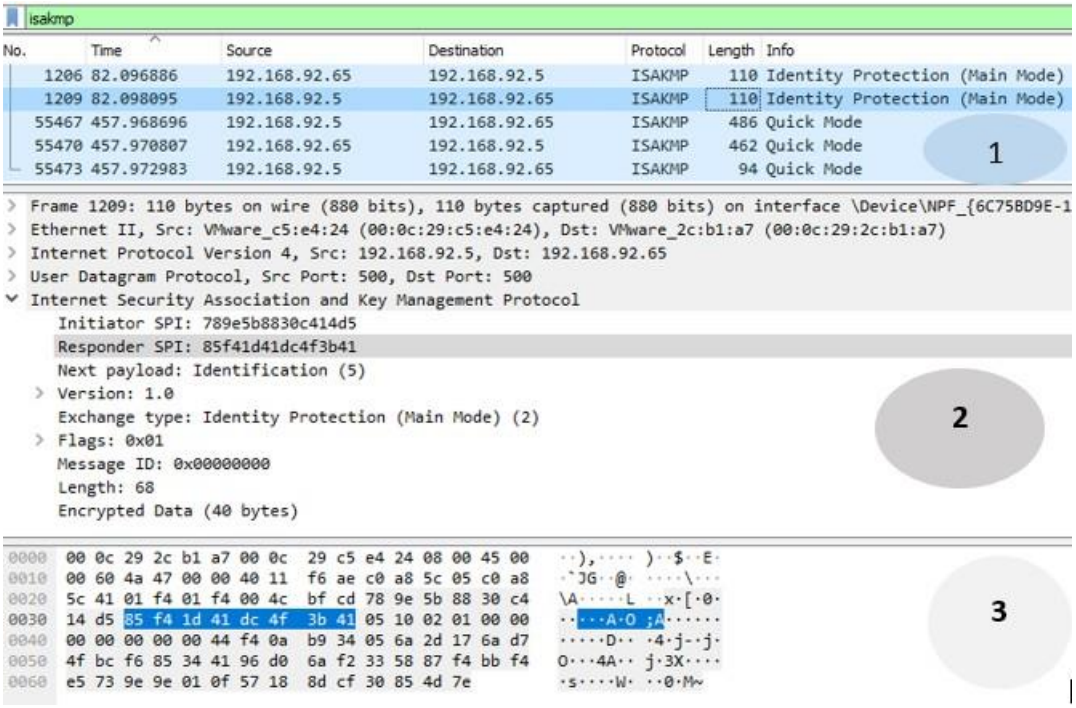

FIGURE 4.30 – Les données cryptés au niveau tunnel.

La figure ci-dessous nous montre que le protocole utilisé pour encapsuler et chiffrer ces paquets est ESP.

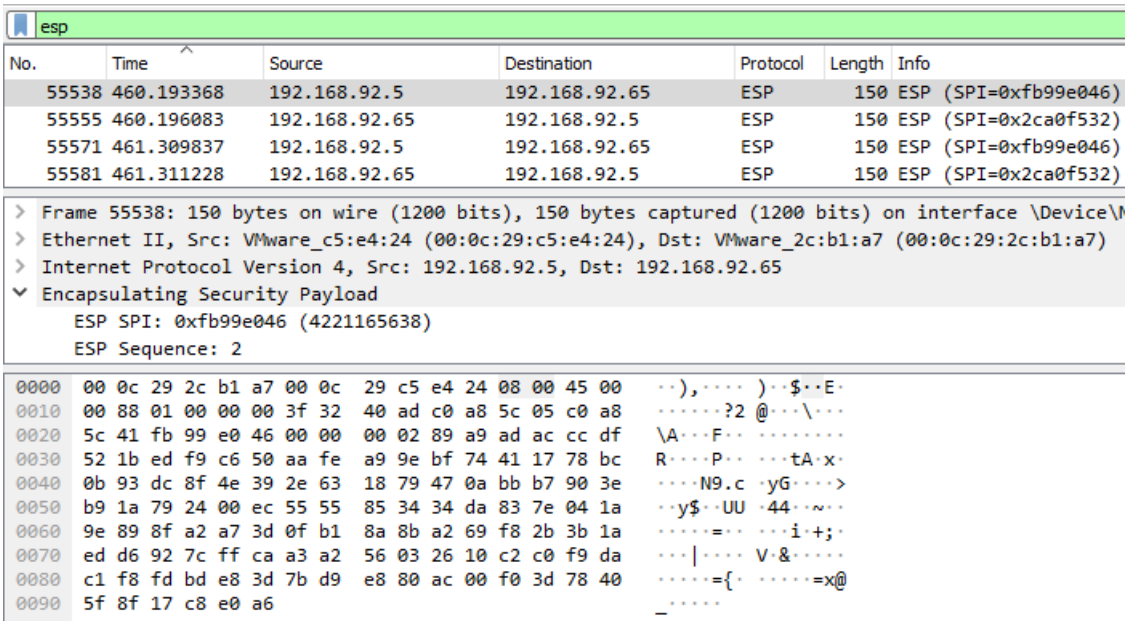

FIGURE 4.31 – L'affichage du protocole ESP.

- **La phase une du Protocole ISAKMP (ISAKMP SA) :** Les deux pairs ISAKMP établissent un tunnel sécurisé et authentifié, qui protège les messages de négociation ISAKMP en utilisant le mode main (voir la figure 4.32).

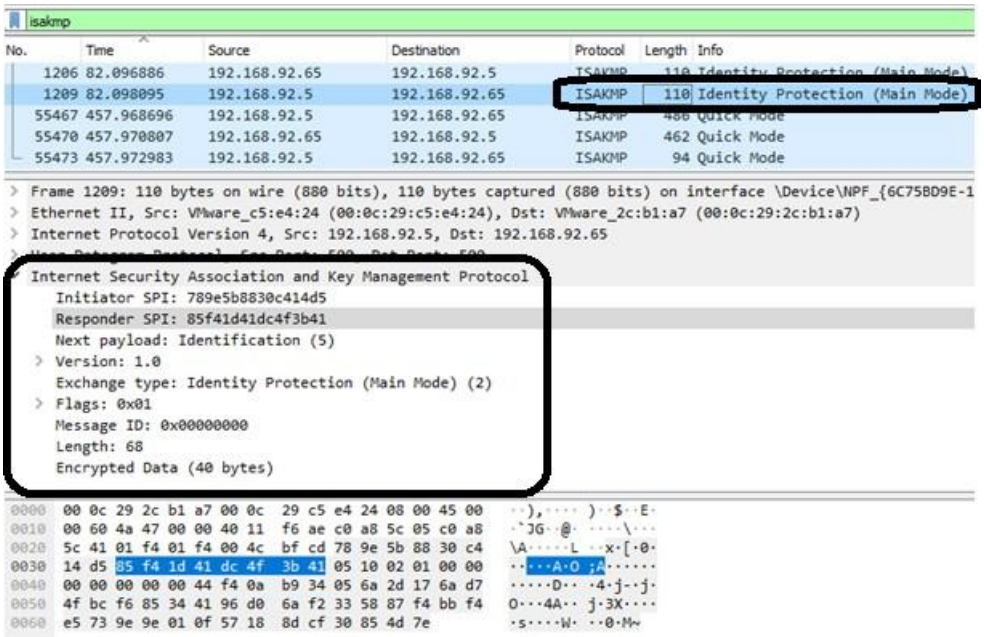

FIGURE 4.32 – La phase une du Protocole ISAKMP.

- **La phase deux du Protocole ISAKMP (Quick mode) :** Le Quick mode se produit après que IKE a établi un tunnel sécurisé durant la phase 1 main mode (voir la figure4.33). Le Quick mode échange des nonces qui offrent

une protection contre la relecture. L'authenticité et la confidentialité des données est assurée par établissement des associations de sécurité IPSec.

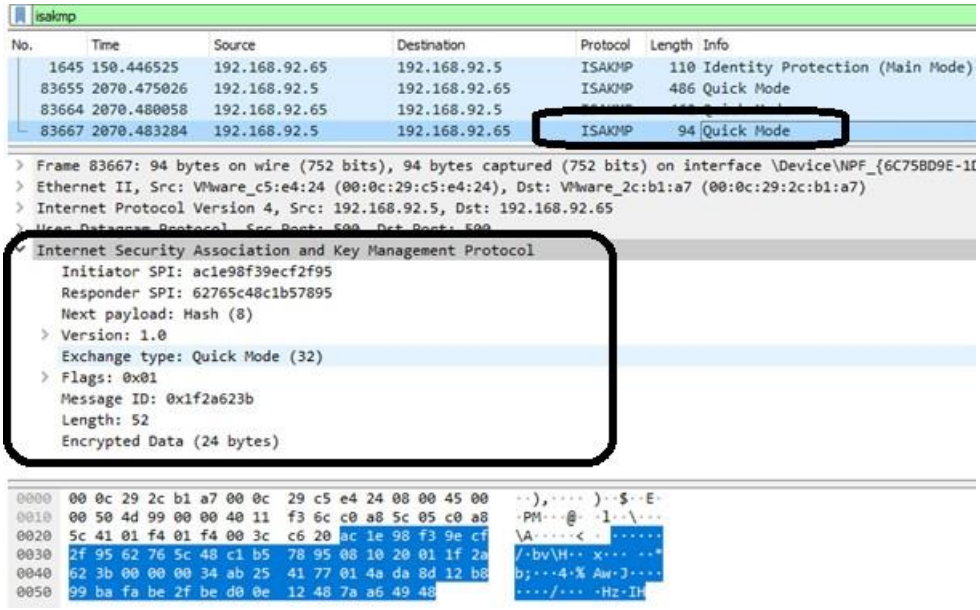

FIGURE 4.33 – La phase deux du Protocole ISAKMP.

4.5 Conclusion

Notre objectif dans ce chapitre était de mettre en place un tunnel VPN IPsec reliant deux sites distants celui de Spa TMF-AKBOU et celui de Spa TMF-ALGER, notre solution et de permettre une connexion sécurisée entre ces deux sites. Nous avons atteint cette objectif car nous constatons bien selon les tests précédents, que les VPNs sont bien créés et que les données son bien chiffrées, et les tests de connexion effectués montrent le bon fonctionnement du VPN.

CONCLUSION GÉNÉRAL

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats obtenus lors de l'interconnexion de deux sites d'un réseau VPN site à site dans l'entreprise Spa TMF .Grâce à cette nouvelle technologie nous avons permis aux employés de partager de façon sécurisée leurs données via le protocole IPSec qui est le principal outil permettant d'implémenter les VPN, ce partage était possible en interne ou en externe. Interne pour les utilisateurs du réseau local de l'entreprise, et externe situés en dehors du réseau local.

En conséquence, nous avons exposé un travail divisé en quatre chapitre, le premier chapitre a maintenu la description de l'organisme d'accueil ou nous avons présenté l'entreprise et exposé la problématique qui consiste dont la manière d'interconnecter deux sites distants d'une manière sécurisée, laquelle nous avons solutionné par un VPN site à site et une solution par la mise en place de deux architecture LANs. Le deuxième chapitre a porté sur les généralités surles réseaux informatiques et la sécurité informatique. Le troisième chapitre est dédié aux VPN où nous avons exposé le fonctionnement ainsi que les différents protocoles utilisés pour la mise en œuvre de réseau VPN. Et le dernier chapitre, a porté sur la présentation de l'environnement de travail et la réalisation de notre travail, à savoir GNS3 ou nous avons réalisé et expliqué différentes configurations, nous avons par la suite implémenté la solution VPN grâce au protocole IPSec.

En effet, la mise en place de VPN site à site permet aux réseaux privés de «Spa TMF de s'étendre, de se relier et d'interconnecter entre eux via internet en tout sécurité ainsi que la réduction du coût des infrastructures réseaux. La technologie VPN basée sur le protocole IPSec est considérée comme l'un des

facteurs clés de réussite qui est en constante évolution.

Le travail que nous avons accompli a pour principal objectifs l'interconnexionde deux sites d'un réseau VPN de l'entreprise Spa TMF Logistics, on reliantces deux sites distants site à site via un tunnel VPN.

La réalisation de ce projet a fait l'objet d'une expérience intéressante, personnelle et professionnelle très bénéfique, de plus nous avons enrichi, amélioré et approfondi nos connaissances sur l'administration et sécurité des réseaux informatiques, ainsi que de nous familiariser avec l'environnement du travail et le mode professionnel.

BIBLIOGRAPHIE

[1] J.DORDIOGNE. Réseaux informatiques, notions fondamentales, édition ENI.

[2] J.Dordoigne. Les réseaux Notions fondamentales. 2006.

[3] D.Slimanou. Mise en place d'une solution VPN sur pare-feu Cas d'étude : Entreprise Tchin-Lait(Candia). Mémoire de master, Université de Bejaïa, 2016-2017.

[4] D.Dominique. Architecture des réseaux. Pearson Education France. 2009.

[5] R.LEGRAND et amp. André VAUCAMPS, CISCO : Notions de base sur les réseaux, Editions ENI, Décembre 2014.

[6] G.Pujolle. Les réseaux, EYROLLES. Paris. 8 éme édition. 2014.

[7] A.Boukerram. Cours réseau et communication, cours 2ème année Licence informatique. Université de Bejaïa. 2014-2015.

[8] Z. Farah. Cours sécurité informatique, Cours Master 1 professionnel informatique. Université de Bejaïa. 2020-2021.

[9] N.Djebari. Cours sécurité, cours 3ème année Licence informatique. Université de Bejaïa. 2019-2020.

[10] www.iro.umontreal.ca/salvail/securite/notes2014securite10-2014long.pdf. Mars 2022.

[11] www.v6protect.fr/ressources-logiciel-securite-site/wiki/cyberattaques-courantes/cassage-mot-de-passe/. Mars 2022.

[12] N.Battat. Cours système sécurité, Cours Master 2 Administration et sécurité des réseaux. Université de Bejaïa. 2021-2022.

[13] glossary zone démilitarisée, https : // www. f5.com /frfr/services / resources /glossary/d zone – dmz .Mars 2022.

[14] "les VPN", http : //perso.modulonet.fr/placurie/ressources/bts2-amsi/chap-8-lesvpn.pdf. Avril 2022.

[15] "les VPN", http : //perso.modulonet.fr/placurie/ressources/bts2-amsi/chap-8-lesvpn.pdf. Avril 2022.

[16] VPN, https : //www.frameip.com/vpn.Avril 2022.

[17] les différents types de VPN, https : //fr.vpnmentor.com/blog/les-différents-types de-vpn-etquand-les-utiliser.pdf. Avril 2022.

[18] wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio 2000ttv01/Bac on Chappuis/Tunneling%20L2F.htm. Avril 2022.

[19] sylvestre.ledru.info/howto/securite/tunnels_et_vpn/node27.html}}.Avril 2022.

[20] https://www.watchguard.com/help/docs/fireware/12/fr FR/ Content/ frFR/ mvpn/general/ipsec_algorithms_protocols_c.html. Avril 2022.

[21] https://www.techtarget.com/searchsecurity/definition/MD5.Avril 2022.

[22] https://www.journaldunet.fr/web-tech/dictionnaire-duwebmastering /1445282-ikeprotocole-informatique-definition-et-presentation-detaillee.Avril 2022.

[23] https://docs.oracle.com/cd/E24843_01/html/820-2982/ipsec-ov-2.Html #scrolltoc.Avril 2022.

[24] https://sylvestre.ledru.info/howto/securite/tunnels_et_vpn/node20.html. Avril 2022.

[25] https://docs.oracle.com/cd/E24843_01/html/820-2982/ipsec-ov-5.html #scrolltoc. Avril 2022.

[26] https://support.huawei.com/enterprise/en/doc/EDOC1100172309#ENUS_ TOPIC_0269170981.Avril 2022.

[27] https://openclassrooms.com/fr/courses/2581701-simulez-des-architectures - reseaux-avecgns3.Juin 2022.

[28] http : //www.tuto-it.fr/vmware.php, 2010. juin 2022.

[29] J. Sebban. Analyseur de paquets réseau pour les pros. Édition 1997.

Résumé

L’objectif de notre projet consiste à l’interconnexion de deux sites distants de l’entreprise Spa TMF d’une manière sécurisée. Pour cela nous avons implémenté une solution réseau privé virtuel (VPN) site à site, qui permet d’interconnecter les sites via un tunnel sécurisé en utilisant le protocole Internet Protocole Sécurité (IPSec) pour la protection des communications réseaux.

Pour la mise œuvre de notre projet, nous avons configuré les machines virtuelles Fortigate et Windows 7 via VMware et les serveurs avec le simulateur GNS3.

Mots-clés : **VPN, Tunnel, IPSec, Site à site, FortiGate, GNS3.**

Abstract

The objective of our project is to interconnect two remote sites of the company Spa TMF in a secure way. To do this, we have implemented a site-to-site virtual private network (VPN) solution, which allows sites to be interconnected via a secure tunnel using the Internet Protocol Security (IPSec) for the protection of network communications.

For the implementation of our project, we configured Fortigate and Windows 7 virtual machines via VMware and servers with the GNS3 simulator.

Keywords : **VPN, Tunnel, IPSec, Site à site, FortiGate, GNS3.**