République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaïa

Faculté des Sciences Exactes
Département Informatique

Mémoire De Fin de Cycle

En vue de l'obtention d'un diplôme de Master en Informatique
Option : Administration et Sécurité des Réseaux

Thème

Mise en place d'une architecture réseau VPN sécurisée pour l'interconnexion des sites distants Cas d'étude : Entreprise CEVITAL de Béjaia

Réalisé par :

M^r. AMIMEUR Ghani
M^r. HABBACHE Nourdine

Devant le jury composé de :

Président : M^r. ALOUI S.
Examinateur 1 : M^r. ATMANI Mouloud
Examinateur 2 : M^r. CHERFA Hamida
Encadreur : M^{me}. LARBI Wahiba
Co-encadreur 1 : M^r. LARBI Ali
Co-encadreur 2 : M^r. SLIMANI Mennad

Promotion 2016-2017

Remerciements

Nous remercions tout d'abords, dieu le tout puissant de nous avoir accordé la force, la volonté et la connaissance pour accomplir ce travail ;

Nous tenons à remercier notre promotrice et co-promoteur Mme et Mr : Larbi Wahiba et Larbi Ali respectivement,pour leurs précieux conseils et orientations ;

Nous tenons à remercier l'ensemble du personnel de la direction des systèmes d'informations de l'entreprise Cevital de Bejaia en particulier notre Encadreur Mr Selimani Mennad et Mr Aloui Nadim qui nous a apporté son aide tout au long de notre stage ;

Nos remerciements vont également à tous les enseignants qui nous ont aidé tout au long de notre travail pour l'esprit de coopération et la courtoisie dont ils ont fait preuve à notre égard ;

Comme on remercie toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce modeste travail.

Dédicace

Je dédie ce modeste travail :

A mes très chers parents pour m'avoir apporté support et soutien, tant psychologique que financier, pendant toute la durée de mes études ;

A mes chers grands parents ;

A mes frères et sœurs ;

A mes chers oncles et tantes ;

A mes cousins et cousines ;

A mon binôme ;

A tous les étudiants de la promotion ASR de l'université de Bejaia ;

Je ne peux oublier l'ensemble de mes ami(e)s qui m'ont apporté leur soutien ;

AMIMEUR Ghani

Dédicace

Je dédie ce modeste travail :

A mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études ;

A toute ma famille pour leur soutien tout au long de mon parcours universitaire ;

A tous mes professeurs :
Leur générosité et leur soutien m'oblige de leurs témoigner mon profond respect et ma loyale considération ;

A tous mes amis et mes collègues :
Ils vont trouver ici le témoignage d'une fidélité et d'une amitié infinie ;

HABBACHE Nourdine

Table des matières

Table des figures v

Liste des abréviations vi

Introduction Générale 1

1 Généralités sur les réseaux et la sécurité informatique 3
- 1.1 Introduction . . . 3
- 1.2 Généralités sur les réseaux . . . 3
  - 1.2.1 Définition d'un réseau . . . 3
  - 1.2.2 Classification des réseaux . . . 3
  - 1.2.3 Typologie des réseaux informatiques . . . 5
  - 1.2.4 Principaux composants d'interconnexion . . . 5
  - 1.2.5 Modèle TCP/IP . . . 7
- 1.3 Sécurité Informatique . . . 9
  - 1.3.1 Objectifs de la sécurité informatique . . . 9
  - 1.3.2 Terminologies de la sécurité informatique . . . 9
  - 1.3.3 Attaques informatique . . . 10
  - 1.3.4 Éléments à sécuriser dans un réseau . . . 12
  - 1.3.5 Mécanismes de la sécurité des réseaux . . . 12
  - 1.3.6 Cryptographie . . . 14
- 1.4 Conclusion . . . 15

2 Réseaux privés virtuels 16
- 2.1 Introduction . . . 16
- 2.2 Présentation d'un réseau privé virtuel . . . 16
  - 2.2.1 Définition . . . 16
  - 2.2.2 Principe de fonctionnement . . . 16
  - 2.2.3 Fonctionnalités d'un réseau privé virtuel . . . 17
  - 2.2.4 Typologie des VPN . . . 17
- 2.3 Protocoles utilisés pour réaliser une connexion VPN . . . 21
  - 2.3.1 Le protocole PPP (Point-To-Point Protocol) . . . 21
  - 2.3.2 Le Protocol PPTP (Point-to-Point Tunneling Protocol) . . . 21

2.3.3 L2TP (Layer Two Tunneling Protocol) . . . 21
2.3.4 IPSEC (Internet Protocol Security) . . . 22
2.4 Conclusion . . . 28

3 Présentation de l'organisme d'accueil 29
3.1 Introduction . . . 29
3.2 Présentation de l'entreprise CEVITAL . . . 29
3.2.1 Organigramme de l'entreprise . . . 30
3.3 Directions de l'entreprise . . . 30
3.3.1 La direction des Finances . . . 30
3.3.2 La direction commerciale . . . 31
3.3.3 La direction Industrielle . . . 31
3.3.4 La direction des ressources humaines . . . 31
3.3.5 La direction Approvisionnements . . . 31
3.3.6 La direction Logistique . . . 31
3.3.7 La direction des Silos . . . 31
3.3.8 La direction des boissons . . . 32
3.3.9 La direction Corps Gras . . . 32
3.3.10 La direction pôle Sucre . . . 32
3.3.11 La direction QHSE (Qualité Hygiene et Securité) . . . 33
3.3.12 La direction Système d'informations . . . 33
3.4 Architecture du réseau informatique de Cevital . . . 34
3.5 Présentation du contexte du projet . . . 34
3.5.1 Problématique . . . 35
3.5.2 Solution proposée . . . 35
3.6 Conclusion . . . 35

4 Mise en œuvre des VPNs 36
4.1 Introduction . . . 36
4.2 Description de l'environnement de travail . . . 36
4.2.1 GNS3 . . . 36
4.2.2 Wireshark . . . 37
4.2.3 VMWARE . . . 38
4.3 Mise en place d'un VPN site à site . . . 40
4.4 Configuration des cartes réseaux virtuels sous vmware . . . 40
4.5 Affectation des adresses IP et protocole de routage . . . 42
4.5.1 Site de Bejaia . . . 42
4.5.2 Site LLK (Lala Khedidja) . . . 43
4.5.3 Site COJECK . . . 44
4.5.4 Site Elkheroub . . . 45
4.5.5 Vérification de routage . . . 46
4.6 Création des VPN . . . 48
4.6.1 Première étape « Creation de la strategie ISAKMP » . . . 48

4.6.2 Deuxième étape « Création de la clé pré-partagée "VPNPROJET" » 49
4.6.3 Troisième étape « Configuration IPSec » 49
4.7 Vérification 51
4.7.1 Vérification du transform-set 51
4.7.2 Vérification de la Crypto-Map 52
4.7.3 Vérification des paramètres IPsec 53
4.7.4 Vérification des opérations ISAKMP 54
4.8 Conclusion 56

Table des figures

1.1 l'architecture en couche de modèle TCP/IP. 8

2.1 VPN poste à site. 18
2.2 VPN poste à poste. 18
2.3 VPN site à site. 19
2.4 Exemple d'emploi d'IPsec entre sites distants. 23
2.5 AH en mode transport. 25
2.6 ESP en mode transport. 25
2.7 AH en mode tunnel. 26
2.8 ESP en mode tunnel. 26

3.1 Organigramme général de CEVITAL. 30
3.2 Organigramme du service Système d'informations. 33
3.3 Schéma d'interconnexion Réseaux WAN-VSAT au sein de CEVITAL. . . . 34

4.1 L'interface graphique de GNS3. 37
4.2 L'interface graphique de Wireshark. 38
4.3 L'interface graphique VMWare workstation 11. 39
4.4 La topologie réseau étendu de l'entreprise CEVITAL. 40
4.5 Configuration des cartes réseaux virtuels 41
4.6 Configuration Frame Relay (Site Bejaia et site LLK). 42
4.7 Configuration réseau local (site de Bejaia). 43
4.8 Protocole de routage OSPF (Site de Bejaia). 43
4.9 Configuration site Lala Khedidja. 44
4.10 Configuration de routeur de Cojeck. 45
4.11 Configuration de routeur de site Kheroub. 46
4.12 Résultat d'une requête ICMP de site centrale vers les autres sites. 47
4.13 La capture après le ping sous Wireshark. 47
4.14 Activation de protocole ISAKMP. 48
4.15 Configurer la politique de sécurité ISAKMP. 49
4.16 Création de la clé pré-partagée. 49
4.17 Configuration de la Transform-Set. 50
4.18 Configuration la durée de vie de la clé partagée. 50

4.19 Création des ACL. 50
4.20 Configuration de la Crypto-Map. 51
4.21 Configuration crypto-map sur l'interface de sortie de routeur. 51
4.22 Vérification du mode. 51
4.23 Vérification de la MAP. 52
4.24 Vérification des opérations d'IPsec. 53
4.25 Vérification des opérations ISAKMP. 54
4.26 Le protocole ISAKMP en mode main. 54
4.27 Le protocole ISAKMP en mode quick. 55
4.28 Le protocole ESP. 56

Liste des abréviations

AAA : Authentication Authorization and Accounting.
ACL : Access Control List.

AES : Advanced Encryption Standard

AH : Authentication Header.

ASCII : American Standard Code for Information Interchange.

DES : Data Encryption Standard.

DH : Diffie Hellman.

DHCP : Dynamic Host Configuration Protocol.

DNS : Domain Name System.

DoS : Denial Of Service.

DSA : Digital Signature Algorithm.

ESP : Encapsulating Security Payload.

FTP : File Transfer Protocol.

GNS3 : Graphical Network Simulator.

HMAC : Hash base Message Aetwork Cuthentication.

HTTP : Hypertext Transfer Protocol.

ICMP : Internet Control Message Protocol.

IDS : Instruction Detection System.

IETF : Internet Engineering Task Force.

IKE : Internet Key Exchange.

IOS : Internetwork Operating Systems.

IP : Internet Protocol.

IPsec : Internet Protocol Security.

IPv4 : Internet Protocol version 4.

Liste des abréviation

IPv6 : Internet Protocol version 6.

IPX : Internetwork Packet Exchange.

ISAKMP : Internet Security Key Management Protocol.

L2TP : Layer Two Tunneling Protocol.

LAN : local Area Network.

LLK : Lala Khedidja.

MAN : Metropolitan Area Network.

MD5 : Message Digest 5.

MPLS : Multiprotocol Label Switching.

NAS : Network Access Server.

OSI : Open System Interconnect.

OSPF : Open Shortest Path First.

PAN : Personal Area Network.

PIX : Private Internet eXchange.

POP : Point Of Presence.

PPP : Point to Point Protocol.

PSTN : Public Switched Telephone Network.

PPTP : Point to Point Tunneling Protocol.

PVC : Permanent Virtuel Circuit.

QOS : Quality Of Service.

RFC : Request for Comments.

RSA : Rivest Shamir Adleman.

SA : Security Association.

SHA : Secure Hash Algorithm.

SLC : Smart Link Communication.

SVC : Switched Virtual Circuit.

TCP : Transmission Control Protocol.

VPN : Virtual Private Network.

VSAT : Very-small-aperture terminal.

WAN : Wide Area Network.

Introduction générale

L'humanité a longtemps imaginé un monde où nous contrôlons tout, un univers sans frontières ni limites où tout est possible, c'est de ces besoins qu'est née l'informatique, cette science qui met en œuvre des ensembles complexes de machines appelées Automates, Calculateurs, Ordinateurs, et Systèmes informatiques. L'évolution de la technologie ne s'est pas arrêtée là, en effet un moyen de relier ces équipements informatiques fut élaboré, c'est ce que nous appellons les réseaux informatiques, leur première apparition date de 1960, ces derniers permettent le partage d'informations et de données, entre les équipements reliés entre eux.

Au départ les réseaux informatiques ont été conçus pour l'armée américaine, afin que cette dernière puisse protéger ses infrastructures informatiques contre d'éventuelles attaques, mais ces réseaux présentaient l'inconvénient de ne pouvoir couvrir que des distances géographiquement limitée.

Mais c'est surtout avec l'apparition d'internet que l'informatique a fait un bond en avant, les réseaux n'étaient plus limités, ils pouvaient enfin communiquer entre eux et ce indépendamment des distances, internet offre donc un grand éventail de possibilités, qui sont de plus en plus importantes de jour en jour, avec entre autre des connections haut débit comme le Câble ou l'ADSL.

Cette croissance s'accompagne naturellement avec l'augmentation du nombre d'utilisateurs, connus ou non, ces utilisateurs ne sont pas forcément pleins de bonnes intentions vis-à-vis de ces réseaux. Ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour essayer d'accéder à des informations sensibles dans le but éventuellement de les modifier ou les détruire, pour porter atteinte au bon fonctionnement du système ou encore tout simplement par curiosité.

Dès lors que ces réseaux sont apparus comme des cibles d'attaques potentielles, leur sécurisation est devenue un enjeu incontournable pour les différentes institutions, ainsi l'entreprise CEVITAL ne fait pas exception à cette règle surtout avec sa communauté (fonctionnaires, responsables, . . .) et ses différents sites qui ne cessent d'augmenter. Cette sécurisation va garantir la confidentialité, l'intégrité, la disponibilité et la non-répudiation. Et pour cela de nombreux outils et moyens sont disponibles, tels que les solutions matériels, logiciels d'audits, les systèmes de détection d'intrusions (IDS), firewalls (pare-feu), les antivirus, les réseaux privés virtuels (VPN).

Le stage que nous avons effectué au sein de l'entreprise CEVITAL de Bejaia, nous a permis de découvrir son réseau et de comprendre son fonctionnement. Le but de

notre travail est de leur proposer une architecture sécurisée du réseau et de mettre des mécanismes de sécurisation des échanges de données. Afin de réaliser les objectifs visés, nous avons organisé ce travail en quatre chapitres :

Le premier chapitre est consacré aux généralités sur les réseaux, la sécurité informatique et les dispositifs de sécurité.

Le deuxième chapitre est focalisé sur les réseaux Privés Virtuels : leurs principes et fonctionnement, ses différents types et les différents protocoles utilisés pour sa réalisation.

Le troisième chapitre qui portera sur la présentation de l'organisme d'accueil et sa structure hiérarchique, ensuite nous passerons à l'étude de l'architecture existante, les critiques, donc évoquer la problématique et enfin la proposition d'une solution adéquate.

Le quatrième chapitre est consacré pour la mise en œuvre des VPNs, cette phase est décomposée en deux parties, dans la première nous introduirons les outils et logiciels ayant servi à l'élaboration du projet, ensuite présentation de l'architecture proposé, tout en expliquant les configurations des différents sites, nous nous passerons enfin à la deuxième partie qui sera principalement consacrée à la création de VPN site à site.

Enfin, nous terminerons par une conclusion générale résumant les éléments essentiels qui ont été abordés dans ce mémoire ainsi que l'expérience acquise durant ce projet.

Chapitre 1

Généralités sur les réseaux et la sécurité informatique

1.1 Introduction

La sécurité des réseaux informatiques est un sujet essentiel qui favorise le développement des échanges d'information dans tous les domaines. L'expansion et l'importance grandissante des réseaux informatiques ont engendré le problème de sécurité des systèmes de communication. Dans la plupart des organisations informatisées, partager les données directement entre machines est un souci majeur. Il s'avère indispensable de renforcer les mesures de sécurités, dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques.

1.2 Généralités sur les réseaux

1.2.1 Définition d'un réseau

Un réseau informatique est l'interconnexion d'au moins deux ou plusieurs ordinateurs en vue d'échanger, de partager des données, des ressources ou des informations. En d'autre terme c'est une infrastructure de communication reliant des équipements informatiques (ordinateurs, concentrateur, commutateur, routeur, imprimante...) permettant de partagé des ressources communes. Il est caractérisé par un aspect physique (câble véhiculant des signaux électriques) et un aspect logique (les logiciels qui réalisent les protocoles)[1].

1.2.2 Classification des réseaux

Les réseaux peuvent être classifiés selon plusieurs critères, dans ce qui suit, nous allons voir leur classification selon la taille [1].

A. Les réseaux personnels PAN (Personal Area Network)

Egalement appelé réseau domestique, un réseau personnel désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour d'un utilisateur. Ce type de réseau sert généralement à relier des périphériques tels qu'imprimante, téléphone portable, appareils domestiques à un ordinateur personnel. La liaison avec ces périphériques peuvent être câblées ou sans fil.

B. Les réseaux locaux LAN (Local Area Network)

De taille supérieure, s'étendant sur quelques dizaines à centaines de mètres, un réseau local relie plusieurs ordinateurs appartenant à une même organisation et situés dans une même salle, un même bâtiment ou un même terrain. Un tel réseau peut reposer sur différentes technologies (câblés ou wifi), la plus répandue étant Ethernet. Du fait de la faible dimension de ce type de réseau, les délais de transmission sont courts avec peu d'erreurs, ce qui a l'avantage d'en simplifier l'administration. Couramment utilisé pour le partage de ressources communes, comme des périphériques, des données ou des applications, un réseau local bénéficie d'une vitesse de transfert de données s'échelonnant entre 10 Mbps et 1 Gbps. La taille d'un tel réseau peut atteindre jusqu'à 100 voire 1000 utilisateurs.

C. Les réseaux métropolitains MAN (Metropolitan Area Network)

Un réseau métropolitain, également nommé réseau fédérateur, assure des communications sur de plus longues distances, inter-connectant souvent plusieurs réseaux LAN avec des débits plus importants. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments, distants de quelques dizaines de kilomètres. Ainsi, un MAN permet à deux nœuds distants de communiquer comme s'il faisait partie d'un même réseau local. Un MAN est formé de commutateurs et de routeurs inter-connectés par des liens à haut débit généralement en fibre optique.

D. Les réseaux étendus WAN (Wide Area Network)

Constitués d'interconnexions de LAN, voire de MAN, les réseaux étendues sont capables de transmettre des informations sur des milliers de kilomètres à travers le monde entier par le biais de routeurs et de liaisons nationales ou internationales à très haut débit, appelées épines dorsales (backbone en anglais). Puisque la majeure partie du trafic d'un WAN se situe dans les LAN qui le constituent, les routeurs sont investis d'une mission importante : contrôler le trafic. Ils doivent être paramétrés avec des informations appelées routes qui leur indiquent comment acheminer des données entre réseaux. En outre, l'épine dorsale est un ensemble de lignes téléphoniques très rapides utilisées par les opérateurs de télécommunications pour transmettre de gros volumes de trafic.

1.2.3 Typologie des réseaux informatiques

A. Internet

Internet est un réseau qui permet de connecter les ordinateurs entre-eux. A l'image du réseau routier, Internet est composé de réseaux internationaux, nationaux, régionaux etc... Mais à la différence des routes ou les règles de circulations peuvent changer d'un pays à l'autre, la technologie Internet est universelle et tous les ordinateurs parlent le même langage (protocole).

B. Intranet

Un intranet est un ensemble de services internet (par exemple un serveur web) internes à un réseau local, c'est-à-dire accessibles uniquement à partir des postes d'un réseau local, ou bien d'un ensemble de réseaux bien définis, et invisibles (ou inaccessibles) de l'extérieur. Il consiste à utiliser les standards client-serveur de l'internet (en utilisant les protocoles TCP/IP), comme par exemple l'utilisation de navigateurs internet (client basé sur le protocole HTTP) et des serveurs web (protocole HTTP), pour réaliser un système d'information interne à une organisation ou une entreprise.

C. Extranet

Un extranet est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau. L'accès à l'extranet doit être sécurisé dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise. Il peut s'agir soit d'une authentification simple (authentification par nom d'utilisateur et mot de passe) ou d'une authentification forte (authentification à l'aide d'un certificat). Il est conseillé d'utiliser HTTPS pour toutes les pages web consultées depuis l'extérieur afin de sécuriser le transport des requêtes et des réponses HTTP et d'éviter notamment la circulation du mot de passe en clair sur le réseau .Un extranet n'est donc ni un intranet, ni un site internet. Il s'agit d'un système supplémentaire offrant par exemple aux clients d'une entreprise, à ses partenaires ou à des filiales, un accès privilégié à certaines ressources informatiques de l'entreprise par l'intermédiaire d'une interface Web.

1.2.4 Principaux composants d'interconnexion

Pour mettre en place un réseau informatique, plusieurs équipements informatiques sont mis en jeux. La plupart de ces équipements sont des équipements d'interconnexion. Chacun de ces équipement joue un rôle spécifique, par exemple prendre un message qui ne lui est pas destiné pour l'acheminer correctement, prendre un message pour l'amplifier et la remettre[2].

- **La carte réseau**

La carte réseau constitue l'interface physique entre l'ordinateur et le support de communication. Pour qu'un ordinateur soit mis en réseau, il doit être muni d'une carte réseau.

- **Le concentrateur (Hub)**

Le concentrateur appelé hub en anglais est un équipement physique à plusieurs ports. Il sert à relier plusieurs ordinateurs entre eux. Son rôle c'est de prendre les données reçues sur un port et les diffuser bêtement sur l'ensemble des ports.

- **Le répéteur (Repeater)**

Le répéteur appelé repeater en anglais, est un équipement qui sert à régénérer le signal entre deux nœuds pour le but d'étendre la distance du réseau. Il est à noter qu'on peut utiliser un répéteur pour relier deux supports de transmission de type différents.

- **Le pont (Bridge)**

Le pont appelé bridge en anglais est un équipement qui sert à relier deux réseaux utilisant le même protocole. Quand il reçoit la trame, il est en mesure d'identifier l'émetteur et le récepteur, comme ça il dirige la trame directement vers la machine destinataire.

- **Le commutateur (Switch)**

Le commutateur appelé switch en anglais, est un équipement multiport comme le concentrateur. Il sert à relier plusieurs équipements informatiques entre eux. Sa seule différence avec le hub, c'est sa capacité de connaître l'adresse physique des machines qui lui sont connectés et d'analyser les trames reçues pour les diriger vers la machine de destination.

- **La passerelle**

La passerelle est un système matériel et logiciel qui sert à relier deux réseaux utilisant deux protocoles et/ou architectures différents ; comme par exemple un réseau local et internet. Lorsque un utilisateur distant contact un tel dispositif, celui-ci examine sa requête, et si celle-ci correspond aux règles que l'administrateur réseaux a défini, la passerelle crée un pont entre les deux réseaux. Les informations ne sont pas directement transmises, elles sont plutôt traduites pour assurer la transmission tout en respectant les deux protocoles.

- **Le routeur**

Le routeur est un matériel de communication de réseau informatique qui a pour rôle d'assurer l'acheminement des paquets, le filtrage et le contrôle du trafic. Le terme router signifie emprunter une route. Le routage est la fonction qui consiste à trouver le chemin optimal que va emprunter le message depuis l'émetteur vers le récepteur.

- **Pont routeur ou B-routeur**

Le B-routeur se comporte à la fois comme un pont et un routeur. Si le protocole n'est pas routable, le B-routeur est capable de se replier vers un niveau inférieur et se comporter comme un pont. Dans le cas contraire, le B-routeur joue le rôle d'un routeur.

- **Frame Relay (Service)**

Le Frame Relay (ou relais de trames) est un service de télécommunication à commutation de paquets conçu pour assurer à faible coût la transmission de données pour un trafic intermittent entre réseaux locaux (LAN), et entre points de terminaison sur les réseaux étendus (WAN).

Le relais de trames encapsule les données dans une unité de taille variable appelée trame et laisse les points de terminaison se charger des corrections d'erreurs (la retransmission de données), ce qui accélère globalement la transmission des données. Pour la plupart des services, le réseau fournit un circuit virtuel permanent (PVC) : le client voit une connexion dédiée continue sans payer une ligne louée à plein temps, tandis que le fournisseur de services identifie le chemin de chaque trame jusqu'à sa destination et peut facturer à l'utilisation. Les circuits virtuels commutés (SVC), en revanche, sont des connexions temporaires détruites après le transfert complet des données.

- **Le modem**

Le modem (modulateur-démodulateur) est un équipement qui sert à lier le réseau téléphonique au réseau informatique. Souvent pour transmettre des données informatiques à distance, on utilise la ligne téléphonique comme support de transmission. Et comme nous savons que la ligne téléphonique ne transporte que des signaux analogiques et que les réseaux informatiques n'utilisent que des signaux numériques, le modem a pour rôle de convertir le signal numérique en signal analogique et vis versa. Le modem utilise donc les techniques de modulation et de démodulation.

- **Le MAU**

C'est l'équivalent de Hub utilisé en token ring. Sa seule différence avec le Hub, c'est sa capacité d'isoler le circuit non utilisé. Il travaille au niveau physique du modèle OSI.

1.2.5 Modèle TCP/IP

TCP diffère fortement du modèle OSI, non seulement par le nombre de couches, mais aussi par l'approche. Le modèle OSI spécifie des services (approche formaliste), TCP/IP des protocoles (approche pragmatique).Développé au-dessus d'un environnement existant, TCP/IP ne décrit, à l'origine, ni de couche physique ni de couche liaison de données. Les applications s'appuient directement sur le service de transport. L'architecture TCP/IP ne comprend que deux couches : la couche transport (TCP) et la couche inter réseau (IP)[3][4].

- **IP (Internet Protocol)**

IP est un protocole qui se charge de l'acheminement des paquets. Il fournit un système de remise de données optimisées sans connexion. Le terme « optimisé » souligne le fait qu'il ne garantit pas que les paquets transportés parviennent à leur destination, ni qu'ils soient reçus dans leur ordre d'envoi. Ainsi, seuls les protocoles de niveau supérieur sont responsables des données contenues dans les paquets IP et de leur ordre de réception.

Le protocole IP travaille en mode non connecté, c'est-à-dire que les paquets émis sont acheminés de manière autonome (datagrammes), sans garantie de livraison.

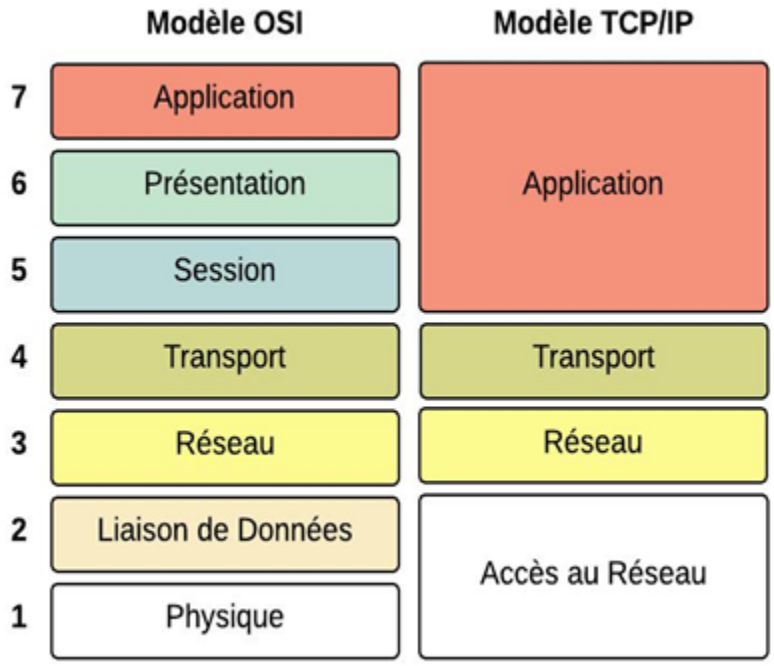

FIGURE 1.1 – l'architecture en couche de modèle TCP/IP.

- **TCP (Transmission Control Protocol)**

TCP est le protocole IP de niveau supérieur. Il fournit un service sécurisé de remise des paquets. TCP fournit un protocole fiable, orienté connexion, au-dessus d'IP (ou encapsulé à l'intérieur d'IP). TCP garantit l'ordre et la remise des paquets, il vérifie l'intégrité de l'en-tête des paquets et des données qu'ils contiennent. TCP est responsable de la retransmission des paquets altérés ou perdus par le réseau lors de leur transmission. Cette fiabilité fait de TCP/IP un protocole bien adapté pour la transmission de données basées sur la session, les applications client-serveur et les services critiques tels que le courrier électronique.

La fiabilité de TCP a son prix. Les en-têtes TCP requièrent l'utilisation de bits supplémentaires pour effectuer correctement la mise en séquence des informations, ainsi qu'un total de contrôle obligatoire pour assurer la fiabilité non seulement de l'en-tête TCP, mais aussi des données contenues dans le paquet. Pour garantir la réussite de la livraison des données, ce protocole exige également que le destinataire accuse la réception des données.

Ces accusés de réception (ACK) génèrent une activité réseau supplémentaire qui diminue le débit de la transmission des données au profit de la fiabilité. Pour limiter l'impact de cette contrainte sur la performance, la plupart des hôtes n'envoient un accusé de réception que pour un segment sur deux ou lorsque le délai imparti pour un ACK expire.

Sur une connexion TCP entre deux machines du réseau, les messages (ou paquets TCP) sont acquittés et délivrés en séquence.

1.3 Sécurité Informatique

La sécurité est un ensemble de stratégies, conçues et mises en place pour détecter, prévenir et lutter contre une attaque. Actuellement, il existe beaucoup de mécanismes de sécurité.

1.3.1 Objectifs de la sécurité informatique

La sécurité informatique est l'ensemble des moyens (méthode, technique et outils) mise en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles[5]. Dans l'objectif d'assurer :

A. La confidentialité

La confidentialité est le fait de s'assurer qu'une information est accessible uniquement par les entités qui ont le droit d'accéder à celle-ci. C'est-à-dire Une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

B. L'authentification

Permet de s'assurer que seules les entités autorisées ont accès au système.

C. Intégrité

C'est garantir que la donnée est restée intègre (non altérée) depuis sa création.

D. La Disponibilité

La disponibilité est le fait de s'assurer que l'information soit toujours disponible peu importe le moment choisit. (Permettant de maintenir le bon fonctionnement du système d'information).

E. Non répudiation

L'élément de la preuve de non-répudiation doit permettre l'identification de celui qu'il représente c'est-à-dire une entité ne peut nier son implication dans une action à laquelle elle a participé.

1.3.2 Terminologies de la sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini, que nous énumérons dans ce qui suit [5][6] :

A. Vulnérabilité (faiblesse/ faille)

Ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.

B. Menaces

Ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité et qui posent un danger sur l'intégrité, la confidentialité et la disponibilité d'un patrimoine. Il existe deux types de menaces, les menaces accidentelles (exposition) et les menaces intentionnelle (attaques).

C. Risque

Le risque désigne la probabilité d'un évènement préjudiciable, ainsi que les couts qui s'ensuivent. Le risque dépend également du montant des valeurs à protéger.

D. Intrusion (Hacking)

Accès par effraction à un système informatique, en vue d'en modifier ou d'en subtiliser des informations. Le hacking décrit l'intrusion non autorisée dans le système informatique d'une entreprise. Il consiste souvent a utiliser des programmes ciblé (cheval de trois, espiogiciels).

1.3.3 Attaques informatique

Dans ce qui suit, nous présenterons les types d'attaques et différentes attaques courante.

A. Les types d'attaques

Il existe trois types d'attaques [5] :

- **Attaque direct**

Le hacker attaque directement la victime à partir de son propre ordinateur.

- **Attaque indirecte par rebond**

Les Hacker privilégient habituellement les attaques par rebond, qui consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.

- **Attaque indirecte par réponse**

Cette attaque est un dérivé de l'attaque par rebond. Son principe consiste a envoyé une requête à la machine intermédiaire Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.

B. Les différentes attaques [7]

- **IP spoofing**

IP spoofing est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine de manière à accéder à un serveur ayant une relation de confiance avec la machine «spoofèe».

- **Le sniffing**

Le reniflage (en anglais Sniffing) est une technique qui consiste à analyser le trafic réseau. Lorsque un entité se connecte par Telnet par exemple, son mot de passe transitant en clair sur le net, il sera facile a lire. De même, il est facile de savoir à tout moment les sessions FTP en cours, les mails en envois ou réception. Une restriction de cette technique est de se situer sur le même réseau que la machine ciblé.

- **Le Dos (Denial of service)**

Le dos est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données. En générale, il exploite les faiblesses d'implémentation, d'architecture d'un réseau ou d'un protocole.

- **Virus**

Un virus se présente sous la forme de quelques lignes de code en langage machine binaire qui se greffent sur un programme utilisé sur le système cible, qui lorsque nous l'exécuterons, se charge d'infecter le système.

- **Le scanning**

Le scanning consiste à balayer tous les ports sur une machine en utilisant un outil appelé scanner. Le scanner envoie des paquets sur plusieurs ports de la machine. En fonction de leurs réactions, le scanner va en déduire si les ports sont ouverts. C'est un outil très utile pour les hackers. Cela leur permet de connaitre et d'obtenir l'adresse IP utilisé, les services accessibles. D'autant plus que les scanners ont évolué. Aujourd'hui, ils peuvent déterminer un grand nombre d'information de topologie détaillée (OS, règle de firewall, subnet ...).

- **Le craquage de mots de passe**

Consiste à faire de nombreux essais pour trouver le bon mot de passe en testant un mot pris dans une liste prédéfinie contenant les mots de passe les plus courants, ou par la méthode de force brute en essayant toutes les possibilités qui sont faites dans l'ordre pour trouver la bonne solution.

- **Le flood**

Le flood est une action généralement malveillante qui consiste à envoyer rapidement une grande quantité de données inutiles dans un réseau afin de le rendre inutilisable.

1.3.4 Éléments à sécuriser dans un réseau

Les réseaux sont constitués de divers équipement interconnectés par un lien filaire ou non filaires. Ces équipement peuvent être gères par des programmes adaptés et plusieurs sortes de données y sont stockées. Certaines d'entre elles peuvent être l'objet de transferts selon des protocoles appelés protocole de réseau Dans ce cadre, la sécurité concerne celle du matériel, celle des programmes, celle des données et celle des protocoles[5].

Avant de réaliser un système de sécurité, il faut spécifier d'abord les éléments à protéger. Nous dénombrons trois types essentiels qui sont :

- **Matériel**

C'est tous les équipements que le réseau relie. La limitation d'accès à chaque matériel participe à la sécurité de l'ensemble.

- **Programme**

Programme est un ensemble de séquences d'instructions interprétables par une machine nécessaires à ces opérations ainsi que les logiciels programmes gérant les différents mécanisme de réseau. Les services permettant une meilleure gestion à distance et plus d'autonomie, on parle dans ce cas-là des services réseaux (DHCP, DNS, FTP, etc).

- **Donnée**

Nous distinguons deux sortes de données, celles qui ne sont pas en rapport avec le fonctionnement du réseau (les documents, les archives), et on trouve les données qui servent au fonctionnement du réseau comme les tables de routage, les bases de données des clients, les fichiers relatifs aux droits d'accès.

1.3.5 Mécanismes de la sécurité des réseaux

A. Pare feu

Pare feu est un outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise). Il permet d'assurer la sécurité des informations d'un réseau en filtrant les paquets de données entrants et sortants selon des règles définies par son administrateur[8].

B. Proxy

Un serveur proxy, appelé également serveur mandataire en français, est une machine faisant l'intermédiaire entre un réseau local (LAN) et internet. Généralement utilisé pour relayer les requêtes HTTP, il peut aussi servir à d'autres protocoles tels que FTP, SOCKS, Gopher, streaming, etc [9].

C. Liste de contrôle d'accès

Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers. Une ACL est un ensemble de conditions qui sont appliqué au trafic circulant via une interface de routeur. Elle indique au routeur les types des paquets à accepter ou à rejeter. Les ACL permettent de sécuriser l'accès d'un réseau en entrée comme en sortie.

D. Technologies AAA (Authentication, Authorization, and Accounting)

Nous vivons dans un monde où presque tout doit être protégé contre une utilisation abusive ou impropre. Que nous soyons administrateur système, responsable, ingénieur réseau ou étudiant. Lorsque nous accédons à un réseau, nous sommes toujours confrontés aux trois aspects [10] :

- **Authentification**

Il s'agit de la vérification de l'identité d'un utilisateur, elle est généralement assuré au moyen d'un secret partagé ou d'un logiciel approuvé (protocole RADIUS).

- **Autorisation**

Elle intervient à l'issue de l'authentification. Une fois l'utilisateur authentifié, il faut s'assurer qu'il est autorisé à accomplir les actions qu'il demande, tels que l'accès à des fichiers, le droit d'écrire, etc. L'autorisation est gérée au moyen de liste ACL ou de stratégie.

- **Accounting (Traçabilité)**

Elle permet de collecter des informations sur les utilisateurs et les actions qu'ils accomplissent lorsqu'ils sont connectés aux équipements du réseau.

E. Les réseaux Privé virtuel

Il correspond à une liaison permanente, distante et sécurisée entre deux sites d'une organisation. Cette liaison autorise la transmission de données cryptées par le biais d'un réseau non sécurisé, comme Internet. En d'autres termes, un réseau privé virtuel est l'extension d'un réseau privé qui englobe les liaisons sur des réseaux partagés ou publics, tels qu'Internet. Il permet d'échanger des données entre deux ordinateurs sur un réseau partagé ou public, selon un mode qui émule une liaison privée point à point.

F. Système de détection d'intrusion (IDS)

Un IDS est le système d'alarme du réseau, il permet de savoir ou de repérer les intrus dans le flot du trafic courant transitant par les ports de communication laissés ouverts par le pare-feu. Les systèmes de détection sont conçus pour informer des accès non autorisés ou des intrusions dans les réseaux. Ces derniers peuvent être déployé en plusieurs endroit du réseau afin d'augmenter le sécurité, ils sont généralement de deux types :

- Le N-IDS (Network Based Intusion Detection System), est implémenté en tant qu'analyseur intelligent de protocole, il assure la sécurité au niveau du réseau.
- Le H-IDS (Host Based Intrusion Detection System), doit être installé sur chaque machine à protéger. Il est, en général, intégré au système d'exploitation qu'il protège, il assure la sécurité au niveau des hôtes.

1.3.6 Cryptographie

La cryptographie est l'étude des méthodes permettant de transmettre des données de manière confidentielle, il existe deux catégories de cryptage : le cryptage symétrique et cryptage asymétrique.

A. La cryptographie Symétrique

La cryptographie à clé secrète, dite aussi chiffrement symétrique, fonctionne selon le principe suivant :

Les deux parties communicante partage la même clé entre eux, cette clé sert à chiffrer et à déchiffrer les messages échangés. L'avantage de ce système est sa rapidité d'exécution car il utilise des opérations simples. Les algorithmes développés pour réaliser les opérations de chiffrement Symétrique sont DES, 3DES et AES.

B. La cryptographie Asymétrique

La cryptographie asymétrique, dite aussi à clé publique, ce système de cryptage utilise un couple de clés, une est privé qui est gardée confidentielle par l'utilisateur et la deuxième publique accessible par tout le monde. Chaque clé a une relation logique avec la clé duale de telle manière qu'un message chiffré avec une clé publique ne puisse être déchiffre qu'avec la clé privée correspondante. Ce système présente l'avantage de permettre la signature numérique des messages et ainsi permette l'authentification de l'émetteur. Les algorithmes les plus fréquemment employée dans ce système sont DSA, RSA et DH.

C. Fonction de hachage

Il s'agit de la troisième grande famille d'algorithmes utilisés en cryptographie. Le principe est qu'un message clair de longueur quelconque doit être transformé en un message de longueur fixe inférieure à celle de départ. Le message réduit portera le nom de "Haché" ou de "Condensé". L'intérêt est d'utiliser ce condensé comme empreinte digitale du message original afin que ce dernier soit identifié de manière univoque. Deux caractéristiques importantes sont les suivantes les fonctions unidirectionnelles et les fonctions sans collisions.

D. Signature numériquement

Une signature numérique est une empreinte chiffrée par la clé privée de l'auteur, la signature est un procédé permettant de garantir l'authenticité de l'expéditeur ainsi que la

vérification du message reçu (l'intégrité) et assure aussi la fonction de non-répudiation.

1.4 Conclusion

Dans ce chapitre, nous avons défini les notions fondamentaux dans les réseaux informatiques et les stratégies de sécurité à prendre pour remédier aux attaques. Le prochain chapitre sera consacré aux VPNs (Virtuel Privat Network).

Chapitre 2

Réseaux privés virtuels

2.1 Introduction

Le VPN est avant tout une réponse à un besoin actuellement de plus en plus présent. En effet, toutes entreprises composées d'au moins deux bâtiments distants ont besoins de pouvoir communiquer entre eux pour les besoins d'un système d'information. De plus, les VPN permettent de connecter ponctuellement un utilisateur distant ayant une connexion internet aux services de son entreprise (mails, transfert de fichiers, ...).

Dans ce chapitre nous présenterons les principales caractéristiques des VPN, quelques définitions et principes de fonctionnement, les différentes typologies ainsi que les détails sur le protocole IPsec.

2.2 Présentation d'un réseau privé virtuel

2.2.1 Définition

Les VPNs est une technique permettant à un ou plusieurs poste distant de communiquer de manière sur, tout en empruntant les infrastructures publiques, ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites et ce de façon simple et économique.

En d'autre terme, c'est un tunnel sécurisé permettent la communication entre deux entités y compris au travers des réseaux peu surs comme peut l'être le réseau Internet. Les VPNs ont pour objectif de contribuer à la sécurisation des échanges de données privées, sensible sur les réseaux publics [11].

2.2.2 Principe de fonctionnement

Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre

du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

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 coûteux 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 partagée comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un entête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation[12].

2.2.3 Fonctionnalités d'un réseau privé virtuel

Le VPN n'est qu'un concept, ce n'est pas une implémentation. Il se caractérise par les obligations suivantes :

- Authentification des entités communicantes : le serveur VPN doit pouvoir être sûr de parler au vrai client VPN et vice-versa.
- Authentification des utilisateurs : seuls les bonnes personnes doivent pouvoir se connecter au réseau virtuel. Les logos de connexions doivent aussi être conservés.
- Gestion des adresses : tous les utilisateurs doivent avoir une adresse privée et les nouveau client en obtenir une facilement.
- Cryptage du tunnel : les données échangées sur Internet doivent être dûment cryptées entre le client VPN et le serveur VPN et vice-versa.
- Les clés de cryptage doivent être régénérées souvent (automatiquement)
- Le VPN dit supporter tous les protocoles afin de réaliser un vrai tunnel comme s'il y avait réellement un câble entre les deux réseaux.

2.2.4 Typologie des VPN

Il existe deux grandes catégories des VPNs : le VPN d'entreprise et le VPN d'opérateur.

A. VPN d'entreprise

Suivant le besoin, dans cette catégorie nous pouvons distinguer trois types standards d'utilisation des VPNs [13].

A.1 VPN d'accès (poste à site)

Un VPN d'accès est utilisé pour permettre à des utilisateurs distants (travailleurs à domicile, commerciaux) d'accéder aux ressources de l'entreprise via un VPN. Afin de réaliser cette solution il existe deux cas :

- 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.
- 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 connexion cryptée.

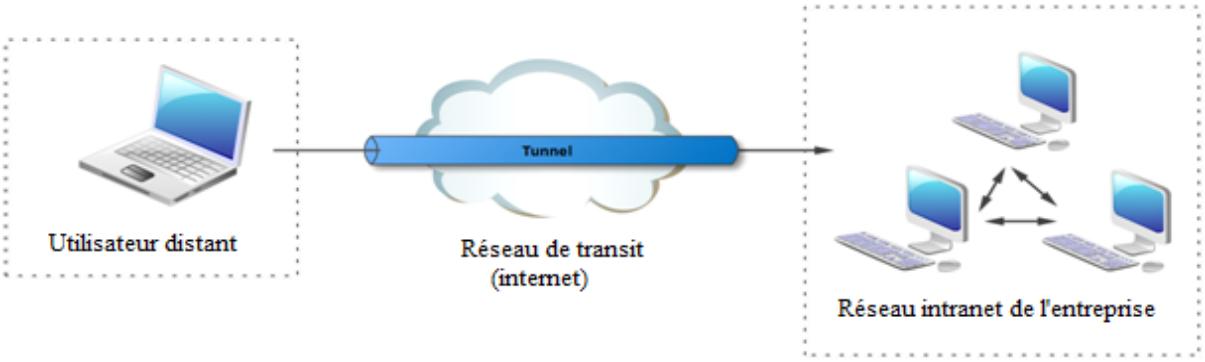

FIGURE 2.1 – VPN poste à site.

A.2 L'extranet VPN (poste à poste)

L'extranet VPN est utilisé pour connecter deux postes distants entre eux pour des raisons de confidentialité. Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

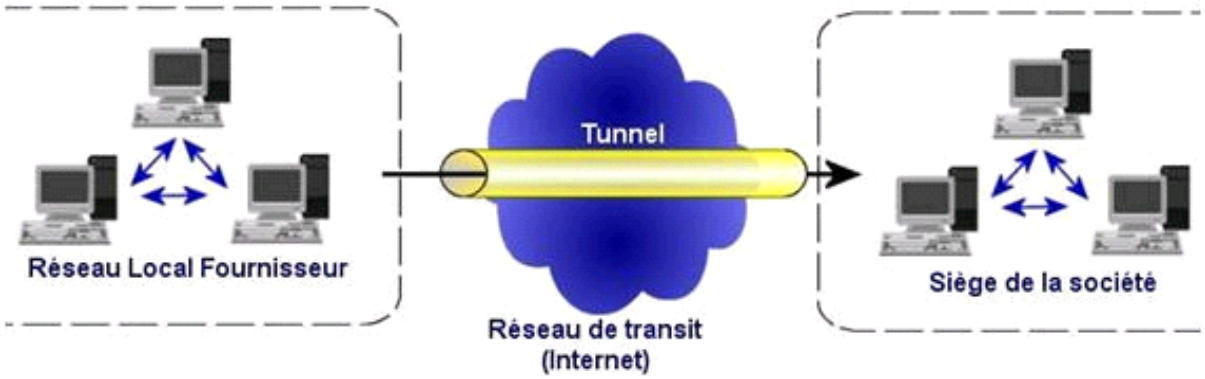

FIGURE 2.2 – VPN poste à poste.

A.3 L'intranet VPN (site à site)

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage " infaillible ". Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable.

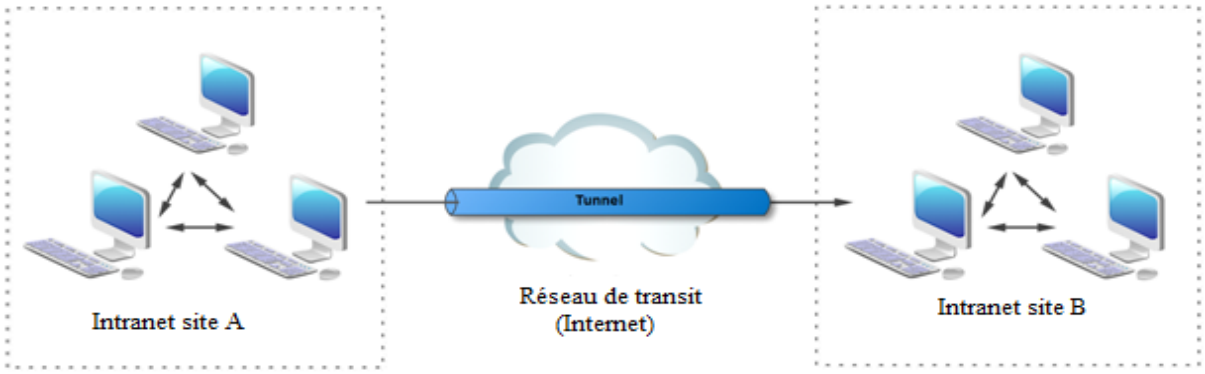

FIGURE 2.3 – VPN site à site.

B. VPN Operateur

VPN operateur, c'est à dire un opérateur spécialisé dans les offres VPN. Il assure la sécurité du réseau et sa performance. Il peut aussi ajouter des services comme l'hébergement de serveurs, la téléphonie ou encore le cloud computing. Cette technologie facilite la transmission des données sans entraîner d'encombrements, Les offres d'un opérateur VPN sont donc ciblées et permettent de mettre en place un réseau privatif, de connecter des entreprises entre elles et même de créer un réseau entre ses filiales et ses collaborateurs.

Ce réseau tient plus d'un réseau de tunnels que d'un véritable réseau VPN mais il est assez courant de parler quand même d'un VPN operateur, car il est difficile, sans la

complicité du personnel de l'opérateur, d'intercepter les communications échangés entre les sites[14].

B.1 Caractéristiques du VPN operateur site à site

Chaque site est relié au POP (Point Of Presence) le plus proche avec le medium souhaité (ADSL, SDSL, fibre optique ...) et un routeur complètement contrôlé par l'opérateur. Ensuite établit des tunnels ou des circuits privatifs entre les différents sites au moyen des différents liens interconnectant ses POP. La technologie pour ce faire varie en fonction des avancées technologiques et c'est ainsi que nous sommes passés des réseaux en Frame-Relay (Relai de trame) aux réseaux MPLS (MultiProtocol Label Switching) qui sont maintenant les plus courants dans ce cadre-là.

Selon le désir du client et les possibilités techniques ou budgétaires, ce réseau privatif peut être bâti avec différentes topologies :

- Tous les sites secondaires convergent vers le site central et c'est celui-ci qui fait le relais : technologie en hub (ou en étoile).
- Tous les sites peuvent communiquer directement entre eux : full mesh ou maillage complet.
- Les sites les plus importants peuvent communiquer entre eux et les secondaires passent obligatoirement par un des sites principaux.
- L'opérateur supervise la totalité du réseau et peut affecter des classes de service selon le type de trafic, ce qui permet de rendre prioritairement certains flux[14].

B.2 Avantages et inconvénients du VPN operateur

Les principaux avantages de ce type de réseaux sont :

- Une transparence totale vis-à-vis des postes du réseau.
- Une possibilité de mettre en place de la QOS (Quality Of Service) pour privilégier les trafics les plus prioritaires et garantir à ceux-ci un maximum de bande passante.
- Une assurance sur les performances proposées par le réseau aussi bien en termes de débit que de temps de transit des messages.

Il y'a néanmoins de points à considérer comme des inconvénients :

- Le coût engendré par l'abonnement de chaque site à ce réseau operateur.
- La nécessité d'avoir un opérateur unique pour l'ensemble du réseau mis en VPN.
- Afin que les messages échangés dans ce réseau privatif ne puissent être capturés, il faut ajouter un protocole de cryptage entre les stations ou entre les sites.

2.3 Protocoles utilisés pour réaliser une connexion VPN

Comme la plupart des technologie réseaux les VPN utilisent des protocoles. Plusieurs protocoles sont utilisés dans les technologies de VPN, certaines d'entre eux visent uniquement à établir un tunnel, d'autres y ajoutent la composante sécurité. Les différents protocoles utilisés sont :

2.3.1 Le protocole PPP (Point-To-Point Protocol)

C'est un ensemble de protocoles standard, définit par la RFC 1661 appuyé de la RFC 2153.il permet de transférer des données, généralement entre un client d'accès à distance et un serveur d'accès réseau sur un lien synchrone ou asynchrone, il est full duplex, garantie l'ordre d'arrivée des paquets et encapsule les paquets IP, IPX dans des trames PPP, puis transmet ces paquets encapsulés au travers de liaison point à point [15].

Ce protocole n'est pas un protocole sécurisé mais sert de support aux protocoles PPTP ou L2TP.

2.3.2 Le Protocol PPTP (Point-to-Point Tunneling Protocol)

Le PPTP est un protocole d'encapsulation de bout en bout sur IP qui permet la mise en place de VPN au-dessus d'un réseau public. Ce protocole fortement soutenu par Microsoft ou cette dernière a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de Windows.

Les différents rôles que le protocole PPTP peut assurer sont [14] :

- Permet la création des VPN sur demande sur des réseaux basés sur TCP/IP.
- Peut être utilisé sur un même réseau local entre deux machines.
- Peut être utilisé comme support pour la création de VPN aussi bien Internet que le réseau téléphonique public (PSTN).
- Offre une communication encryptée sûr à travers ces deux réseaux publics.
- Simplifie les accès longues distances pour les utilisateurs distants.

2.3.3 L2TP (Layer Two Tunneling Protocol)

L2TP est un protocole crée par Microsoft et Cisco inspiré des deux protocoles L2F et PPTP et qui réunit leurs avantages. Le protocole L2TP est un protocole standard de tunnelisation très proche de PPTP. Ainsi le protocole L2TP encapsule des trames protocole PPP, encapsulant elles-mêmes d'autres protocoles (tels que IP, IPX ou encore NetBIOS), Il faut deux types de serveur pour utiliser L2TP :

- **LAC (L2TP Access Concentrator) :** Il sert à fournir un moyen physique pour se connecter à un ou plusieurs LNS par le protocole L2TP. Il est responsable de l'identification et construit le tunnel vers les LNS.
- **LNS (L2TP Network Server) :** Il assure la communication entre le réseau auquel il est connecté et les LAC vers lesquels il a un tunnel[15].

2.3.4 IPSEC (Internet Protocol Security)

A Présentation et fonctionnement d'IPsec

IPSec (Internet Protocol Security) est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau du modèle OSI. Il assure la confidentialité (grâce au cryptage), l'authentification (qui permet d'être certain de l'identité de l'émetteur) et l'intégrité des données permettant de s'assurer que personne n'a pu avoir accès aux informations. IPSec permet de protéger les données et également l'en-tête d'une trame, en masquant le plan d'adressage grâce à l'ajout d'un en-tête IPSec à chaque datagramme IP. IPSec de par sa position, il agit sur chaque datagramme IP et permet ainsi d'offrir une protection unique pour toutes les applications.

Ce protocole est indissociable d'IPv6 est utilisable aussi sur IPv4 si le fournisseur a choisi de l'implanter dans son produit. Les concepteurs, S. Kent et R. Atkinson de chez IETF (Internet Engineering Task Force) ont proposé une solution en novembre 1998 afin de répondre aux besoins directs du développement des réseaux en matière de sécurité. En effet, en sécurisant le transport des données lors d'échanges internes et externes, la stratégie IPSec permet à l'administrateur réseau d'assurer une sécurité efficace pour son entreprise contre toute attaque venant de l'extérieur.

A.1 Concept de base d'IPSec

Le protocole IPSec est destiné à fournir différents services de sécurité. Il permet grâce à plusieurs choix et options de définir différents niveaux de sécurité afin de répondre de façon adaptée aux besoins de chaque entreprise. La stratégie IPSec permettant d'assurer la confidentialité, l'intégrité et l'authentification des données entre deux hôtes est gérée par un ensemble de normes et de protocoles :

- **Authentification des extrémités**
  Elle permet à chacun de s'assurer de l'identité de chacun des interlocuteurs. Précisons que l'authentification se fait entre les machines et non entre les utilisateurs, dans la mesure où IPSec est un protocole de couche 3.
- **Confidentialité des données échangées**
  Le contenu de chaque paquet IP peut être chiffré afin qu'aucune personne non autorisée ne puisse le lire.
- **Authenticité des données**

IPSec permet de s'assurer que chaque paquet a bien été envoyé par l'hôte et qu'il a bien été reçu par le destinataire souhaité.

- **Intégrité des données échangées**
  IPSec permet de vérifier qu'aucune donnée n'a été altérée lors du trajet.
- **Protection contre les écoutes et analyses de trafic**
  Le mode tunneling permet de chiffrer les adresses IP réelles et les en-têtes des paquets IP de l'émetteur et du destinataire. Ce mode permet ainsi de contrecarrer toutes les attaques de ceux qui voudraient intercepter des trames afin d'en récupérer leur contenu.
- **Protection contre le rejet**
  IPSec intègre la possibilité d'empêcher un pirate d'intercepter un paquet afin de le renvoyer à nouveau dans le but d'acquérir les mêmes droits que l'envoyeur d'origine.

A.2 Application de l'IPSec au modèle OSI

Le mode tunneling d'IPSec est un protocole de couche 3 fournissant ses services pour sécuriser l'IP qui est de même couche. Il a pour avantage d'offrir la protection des protocoles de couches supérieurs TCP/IP. Il s'étend également aux protocoles de couches 2 comme L2TP et PPTP. Il est utilisé :

- Entre deux routeurs, il permet de créer des VPN sécurisés, au-dessus d'un réseau public pas forcément réputé pour sa fiabilité (comme l'internet) ; par exemple pour protéger les échanges entre les différents sites.
- Entre un serveur et un poste individuel relié par Internet, il permet à un utilisateur d'accéder à des données internes sans réduire le niveau de sécurité ; par exemple pour un administrateur désirant administrer ses machines lorsqu'il est en congé.
- En interne pour protéger une machine particulièrement sensible et pour réaliser un contrôle d'accès fort ; par exemple pour limiter l'accès à une autorité de certification à quelques postes de travail bien identifiés et en protéger les communications[16].

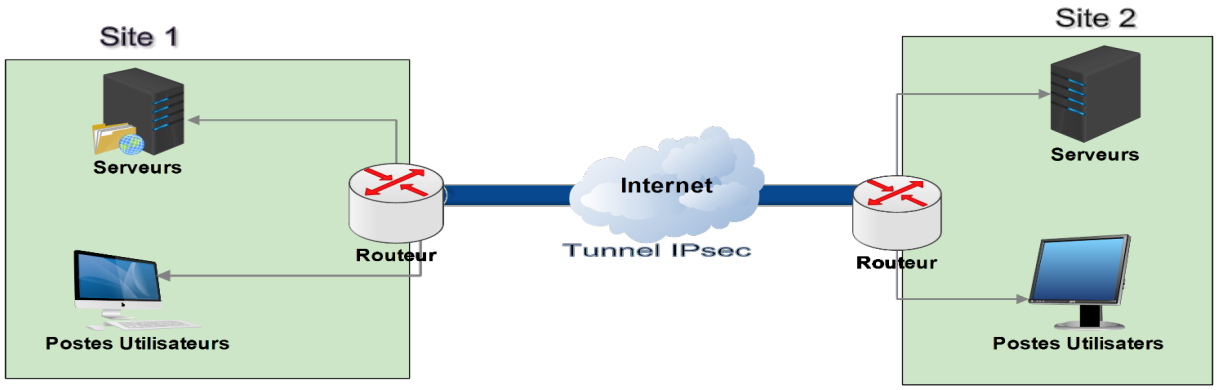

FIGURE 2.4 – Exemple d'emploi d'IPsec entre sites distants.

B. Protocoles de sécurisation IPsec

Il existe deux protocoles AH et ESP

B.1 Protocole AH (Authentification Header)

Le protocole AH authentifie l'émetteur des données, contrôle l'intégrité du paquet IP (en-tête et charge utile) et assure le service anti rejeu. Les traitements associés utilisent des algorithmes de "hachage" tels que Message Digeste (MD5) ou Secure Hash Algorithme (SHA-1, SHA-256, etc.).Un algorithme de hachage est associé à une clé issue de la méthode d'authentification choisie pour constituer un Hash de base Message authentification Code (HMAC). L'entête AH est inséré à la suite de l'entête IP pour garantir l'intégrité et l'authentification des données. Se protège ainsi contre toute altération du paquet lors de son transit[12].

B.2 Protocole ESP (Encapsulating Security Payload)

Le protocole ESP assure la confidentialité et l'authentification grâce au chiffrement de paquet IP tel que sa fonction masque les données et l'identité de leurs sources et leurs destinations. Ce protocole authentifie le paquet IP interne et l'en-tête ESP. L'authentification permet d'identifier la source des données et garantir leur intégrité[12].

C. Les modes d'IPSec

La technologie IPSEC présente deux modes de fonctionnement qui sont :

C.1 Mode transport

Le mode transport (figure 2.5 et figure 2.6), seules les données contenues dans la couche transport sont protégées par IPsec, l'en-tête IP reste inchangé.

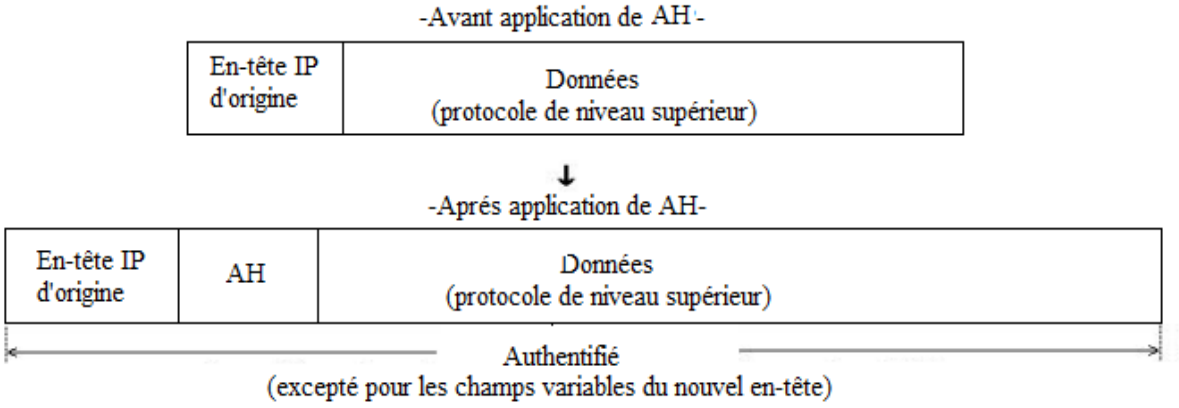

FIGURE 2.5 – AH en mode transport.

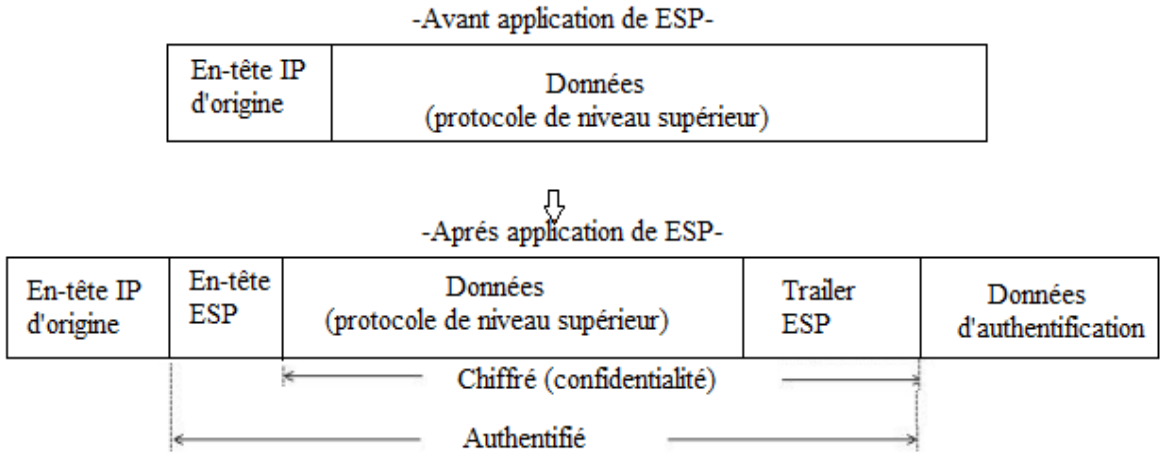

FIGURE 2.6 – ESP en mode transport.

C.2 Mode tunnel

Dans le mode tunnel, tout le paquet IP est protégé (figure 2.7 et figure 2.8). Pour cela il est considéré comme un simple message et un nouvel en-tête IP est créé.

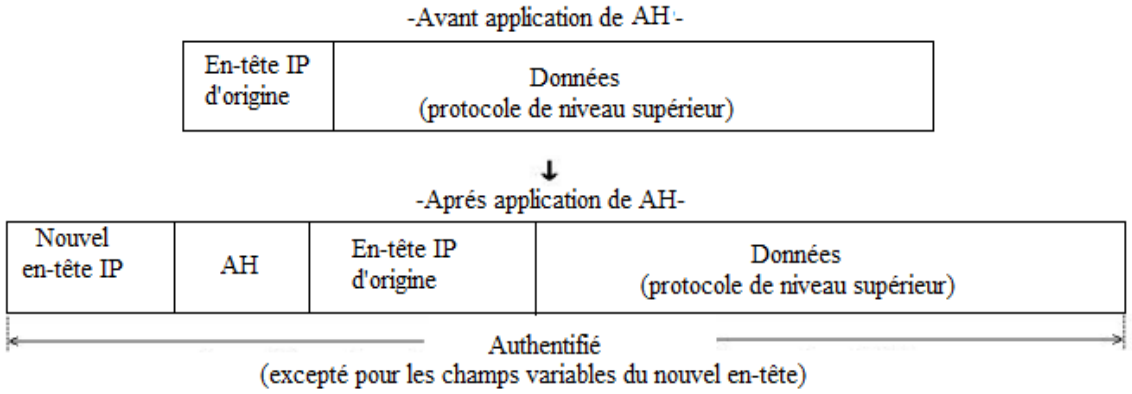

FIGURE 2.7 – AH en mode tunnel.

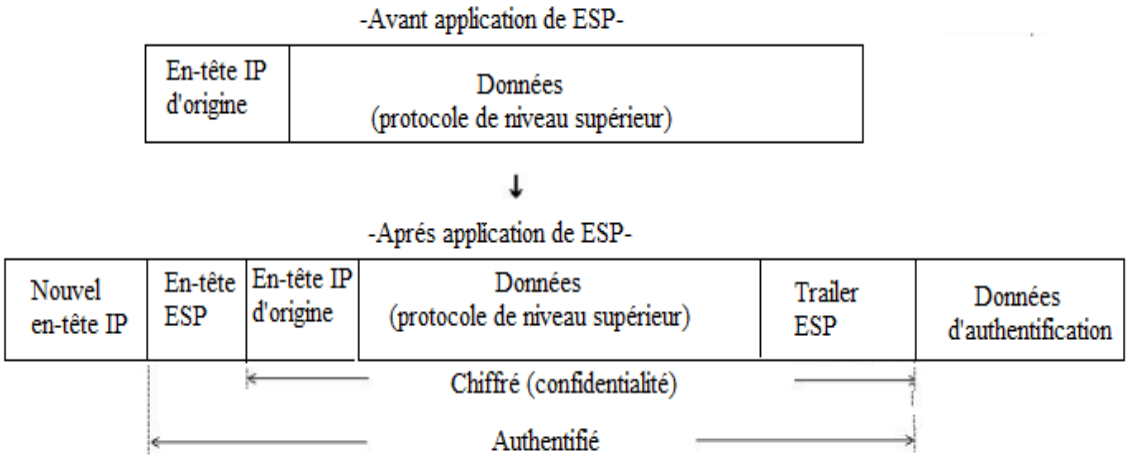

FIGURE 2.8 – ESP en mode tunnel.

Le mode tunnel possède comme grand intérêt de pouvoir créer des tunnels sécurisés. Deux machines ou passerelles de deux réseaux voulant sécuriser leurs communications qui passent par une zone non protégée, vont créer un tunnel IPsec entre ces deux passerelles. Toute communication d'une machine d'un réseau vers l'autre sera encapsulée dans un nouvel en-tête IP.

Une personne écoutant la communication ne verrait que des paquets allant d'une passerelle à l'autre sans pouvoir déchiffrer le contenu de ces paquets. Ce mode correspond à l'utilisation d'un réseau privé virtuel ou VPN (Virtual Private Network)[17].

D. Gestion des clés

Les protocoles sécurisés ont recours à des algorithmes de cryptage, et ont donc besoin de clefs. Un des problèmes principaux dans ce cas est la gestion de ces clefs. Par gestion, nous entendons la génération, le stockage et la suppression de ces clefs. Ces différentes tâches sont évoluées à des protocoles spécifiques de gestion de ces clefs à savoir [18][19] :

D.1 Protocole ISAKMP (Internet Security Association and Key Management Protocol)

Le protocole ISAKMP, utilisé par IPSec pour la création de tunnel, à pour rôle d'établir, de négocier, de modifier ou de supprimer des Associations de Sécurité et leurs attributs.

Les SA contiennent les paramètres de sécurité suivants :

- Algorithme de chiffrement et taille des clés
- Clé de session
- Choix du protocole AH ou ESP
- Mode tunnel ou transport

ISAKMP se déroule en deux phases : Création de la SA ISAKMP, qui servira à la sécurisation de l'ensemble des échanges futurs : on a donc négociation d'attributs relatifs à la sécurité, vérification des identités des tiers, génération des clés... Négociation de paramètres de sécurité relatifs à une SA à établir pour un mécanisme donné (par exemple AH ou ESP), via la SA ISAKMP établie en phase 1.

D.2 Protocole IKE (Internet Key Exchange)

IKE est le protocole de gestion des clés implémenté par IPSec. Il comprend 3 modes, qui gèrent les échanges de paramètres entre les entités souhaitant communiquer, le but est de créer la SA dans les deux pairs à l'aide des deux phases d'ISAKMP. La première phase est utilisée pour créer une SA IKE via les échanges identity protect exchange et aggressive exchange d'ISAKMP , la deuxième pour négocier les paramètres nécessaires à la création de la SA IPSec.

Le protocole IKE utilise, quant à lui, trois modes différents pour ses échanges :

- **Main Mode Exchange**

  Pour l'établissement de la SA IKE, six messages sont utilisés : trois requêtes et trois réponses. Cet échange se déroule en trois étapes :

  - **Echange des paramètres Diffie-Hellman.**
  - **Echange d'aléas.**
  - **Authentification des parties**

  Le premier échange sert à la négociation des paramètres nécessaires à la mise en place de la SA IKE. Le deuxième échange sert à la négociation des valeurs publiques

de l'algorithme Diffie-Hellman et des valeurs pseudo-aléatoires contenues dans le bloc d'aléas (NoncePayload). Lors du dernier échange les deux pairs s'envoient leurs identités respectives et le bloc Hash nécessaire à l'authentification.

- **Aggressive Mode Exchange**

  Ce mode utilise directement l'Aggressive Exchange de ISAKMP ; l'échange se déroule donc en seulement trois messages.

- **Quick Mode Exchange**

  Une fois la SA IKE établie avec le Main Mode ou l'Aggressive Mode, le Quick Mode est utilisé pour établir une SA pour un autre protocole de sécurité, comme AH ou ESP, sous la protection de la SA IKE précédemment établie. Dans un échange en Quick Mode, les deux pairs négocient les caractéristiques de la SA IPSec à établir, et génèrent les clés correspondantes. La SA IKE protège ces échanges en chiffrant et en authentifiant les messages transmis. En plus de l'en-tête ISAKMP, du Hash, de la SA, du Nonce et des paramètres optionnels de Diffie-Hellman, les deux pairs peuvent s'échanger des informations concernant leur identité, comme leur adresse IP. La connexion sécurisée ayant été établie par les protocoles ci-dessus, il est alors nécessaire de protéger les données utiles : c'est le rôle des protocoles AH et ESP.

2.4 Conclusion

A travers ce chapitre, nous avons effectué une présentation des réseaux privés virtuels (VPNs) ainsi que les protocoles utilisés pour les réaliser, et particulièrement la solution que présente IPSec qui est un standard sur le marché . Mais également que le terme VPN ne se référençait pas qu'à la solution IPSec mais il est avant tout un concept et ne précise rien concernant ses moyens.

Chapitre 3

Présentation de l'organisme d'accueil

3.1 Introduction

Dans ce chapitre nous allons présenter l'entreprise dans laquelle nous avons effectué notre stage pour la réalisation de notre projet de fin de cycle, ensuite nous ferons le point sur les problèmes rencontres et la solution proposé.

3.2 Présentation de l'entreprise CEVITAL

Cevital est une Société par Actions au capital privé de 68 ,760 milliards de DA, elle est implantée à l'extrême du port de Bejaia, elle est l'un des fleurons de l'industrie agroalimentaire en Algérie qui est constituée de plusieurs unités de production équipées de la dernière technologie et poursuit son développement par divers projets en cours de réalisation. Son expansion et son développement durant les 5 dernières années, font d'elle un important pourvoyeur d'emplois et de richesses,CEVITAL Food est passé de 500 salariés en 1999 à 3996 salariés en 2008.

Cevital Agro-industrie est une filiale du Groupe Cevital, créée en 1998, implantée au sein du port de Bejaia, Cevital Agro-industrie dispose de plusieurs unités de production :

- Deux raffineries de sucre.
- Une unité de sucre liquide.
- Une raffinerie d'huile.
- Une margarinerie.
- Une unité de conditionnement d'eau minérale.
- Une unité de fabrication et de conditionnement de boisson rafraichissante et une conserverie.

Elle possède également plusieurs silos portuaires ainsi qu'un terminal de déchargement portuaire d'une capacité de 2000 tonnes/heure, de plus elle exporte ses produits dans plusieurs pays, notamment en : Europe, au Maghreb, au Moyen Orient et en Afrique de

l'Ouest. Elle compte parmi ses clients de grandes marques mondiales d'agro-business, tel que : Coca Cola, Kraft Food, Danone...

Cevital est le plus grand complexe privé en Algérie et le leader en Afrique et dans le bassin méditerranéen dans l'industrie du sucre et l'huile végétale, Sa Situation géographique à l'arrière port de Béjaia à 200 ML du quai :Ce terrain à l'origine marécageux et inconstructible a été récupéré en partie d'une décharge publique[20].

3.2.1 Organigramme de l'entreprise

Voici un organigramme représentant la composition des directions de l'entreprise

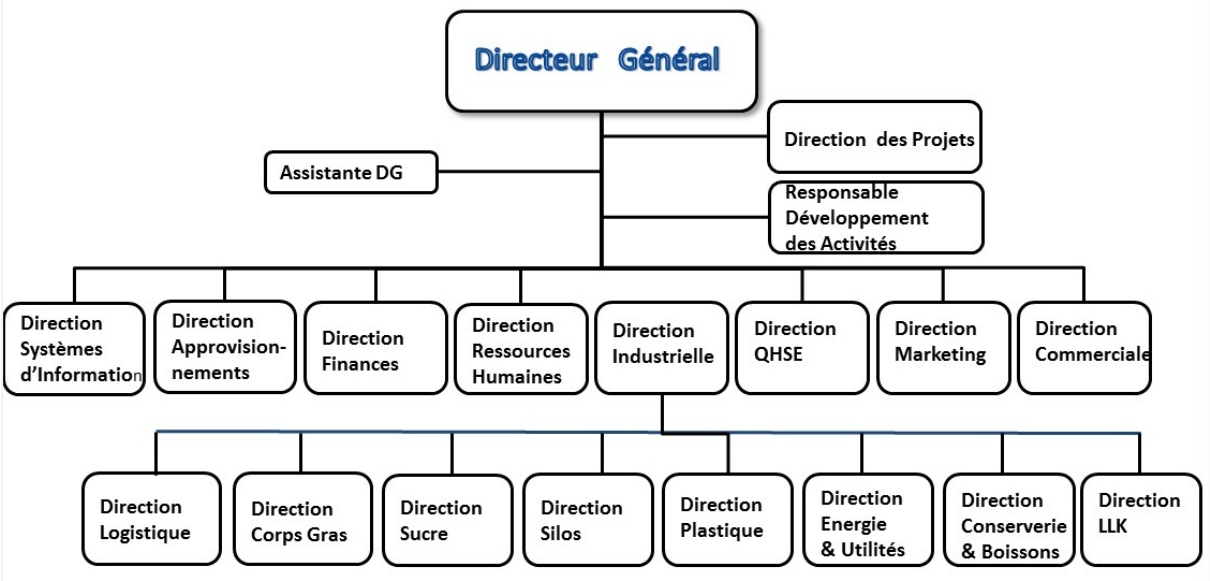

FIGURE 3.1 – Organigramme général de CEVITAL.

3.3 Directions de l'entreprise

Les directions de l'entreprise sont les suivants [20] :

3.3.1 La direction des Finances

Le rôle de cette direction est :

- Préparer et mettre à jour les budgets.
- Tenir la comptabilité et préparer les états comptables et financiers.
- Pratiquer le contrôle de gestion.

3.3.2 La direction commerciale

Elle a en charge de commercialiser toutes les gammes des produits, le développement du Fichier clients de l'entreprise, de la gestion de la relation client.

3.3.3 La direction Industrielle

Elle est chargée de l'évolution industrielle des sites de production et définit, avec la direction générale, les objectifs et le budget de chaque site. Elle analyse les dysfonctionnements sur chaque site (équipement, organisation...) et recherche les solutions techniques ou humaines pour améliorer en permanence la productivité, la qualité des produits et des conditions de travail. Elle anticipe aussi les besoins en matériel et supervise leur achat (étude technique, tarif, installation...).

3.3.4 La direction des ressources humaines

Cette direction a pour mission :

- D'assurer un support administratif à l'ensemble du personnel de CEVITAL.
- Piloter les activités du social.
- Assiste à la direction générale ainsi que tous les managers sur tous les aspects de gestion ressources humaines.
- Elle garantit également le recrutement.
- Chargé de la gestion des carrières et identifie les besoins de mobilité.

3.3.5 La direction Approvisionnements

Dans le cadre de la stratégie globale d'approvisionnement et des budgets alloués (investissement et fonctionnement), cette direction met en place les mécanismes permettant de satisfaire les besoins en matières et en service afin de permettre la réalisation des objectifs de production et de vente.

3.3.6 La direction Logistique

Cette direction expédie les produits finis, prenant la responsabilité de charger les camions, à livrer aux clients sur site et des dépôts. Elle assure, et gère le transport de tous les produits finis, que ce soit au moyen propre (camion de CEVITAL), ou en moyens de transport des clients.

3.3.7 La direction des Silos

Cette direction décharge les matières premières en vrac arrivées par navire ou camions vers les points de stockage et stocke dans les conditions requises les matières premières.

Elle est chargée aussi de :

- D'expédier et transférer vers les différents utilisateurs de ces produit dont l'alimentation de raffinerie de sucre et les futures unités de trituration.
- De faire également l'entretien et maintien en état de services les installations des unités silos.

3.3.8 La direction des boissons

Le pôle boissons et plastique comprend trois unités industrielles situées en dehors du site de Bejaia :

- Unité Lala Khedija domiciliée à agouni-gheghrane (wilaya de Tizi Ouzou) a pour vocation principale la production d'eau minérale et de boissons carbonatées à partir de la célèbre source de Lala Khedidja.
- Unité plastique, installée dans la même localité, assure la production des besoins en emballages pour les produits de Margarine, Les Huiles et à terme des palettes, des étiquettes...etc.
- Unité Cojeck, implantée dans la zone industrielle d'El Kseur, elle transforme des fruits et légumes frais en jus, Nectars et conserves.

3.3.9 La direction Corps Gras

Le pôle corps gras est constitué des unités de production suivantes :

- Une raffinerie d'huile de 1800 T/J.
- Un conditionnement d'huile de 2200T/J.
- Une margarinerie de 600T/J.
- Une unité chimique.
- Hydrogénation.
- Pate chocolaterie.

La mission principale de cette direction est de raffiner et de conditionner différentes huiles végétales ainsi que la production de différentes types de margarines et beurre.

3.3.10 La direction pôle Sucre

Le pôle sucre est constitué de Trois unité de production :

- Une raffinerie de sucre solide 300T/J.
- Une unité de sucre liquide 600T/J.
- Une unité de conditionnement de sucre 200T/J (mise en service mars 2010).

Sa vocation est de produire du sucre solide et liquide dans le respect des normes de qualité, ses produits sont destinés aux industriels et aux particuliers et ce pour le marché local et à l'export.

3.3.11 La direction QHSE (Qualité Hygiene et Securité)

Cette direction met en place, maintient et améliore les différents systèmes de management et référentiels pour se conformer aux standards internationaux, elle veille aussi au respect des exigences réglementaires produits, environnement et sécurité.

3.3.12 La direction Système d'informations

Elle assure la mise en place des moyens des technologies de l'information nécessaires pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise. Elle doit ainsi veiller à la cohérence des moyens informatiques et de communication mis à la disposition des utilisateurs, à leur mise à niveau, à leur maîtrise technique et à leur disponibilité et opérationnalité permanente et en toute sécurité. Elle définit, également, dans le cadre des plans pluriannuels, les évolutions nécessaires en fonction des objectifs de l'entreprise et des nouvelles technologies.

Dans la figue(3.2) nous présentons l'organigramme de la direction système d'information qu'est organisé comme suit :

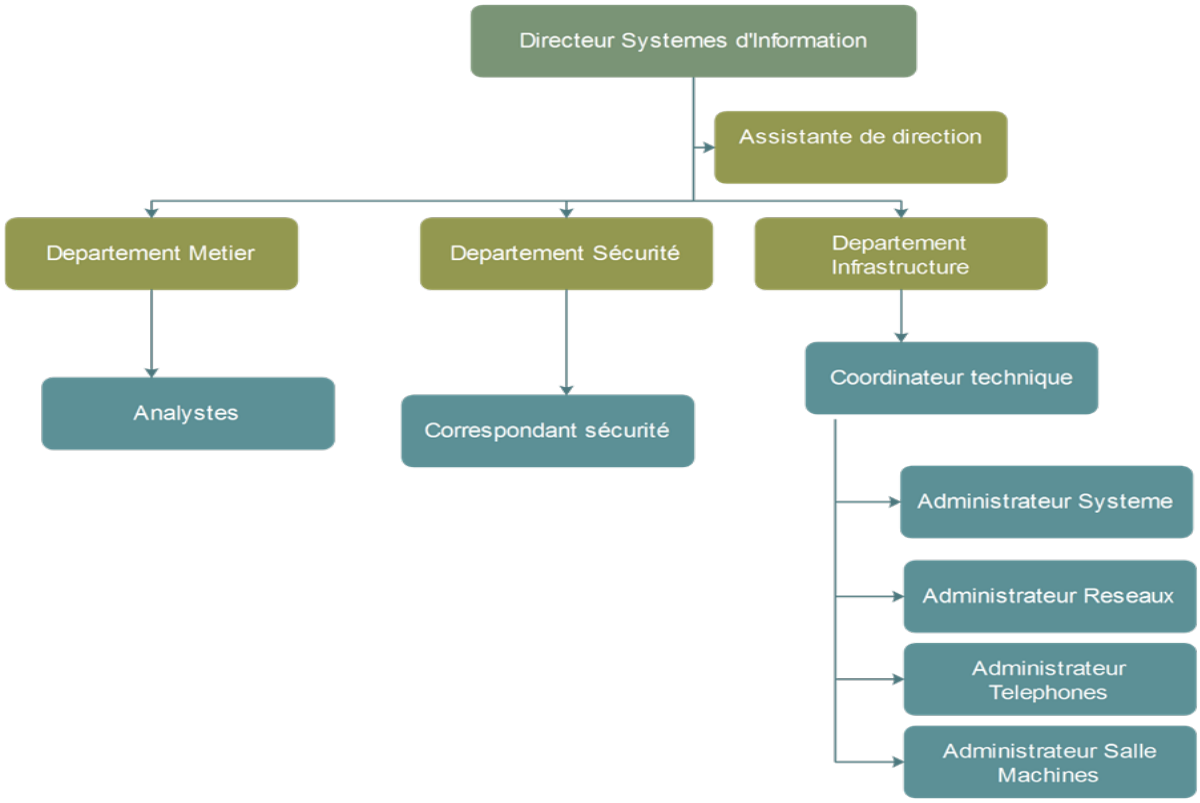

FIGURE 3.2 – Organigramme du service Système d'informations.

3.4 Architecture du réseau informatique de Cevital

Cevital dispose d'un réseau commuté (téléphonique) de taille importante composé d'une plateforme de services reliant les sites locaux dans chacune des entités physiques. Il est constitué de plusieurs équipements dont :

- Un seul Switch (EtherSwitch router), qui a une architecture réseau en étoile.
- Des routeurs et des firewalls, pour la plupart, de marque Cisco.
- Équipements satellitaires VSAT (Very Small Aperture Terminal) pour établir la communication entre différents sites interconnectés.

Cette architecture est également composée des opérateurs SLC (Smart Link Communication) qui sont utilisés comme étant des liaisons d'accès à Internet avec des adresses IP publics.

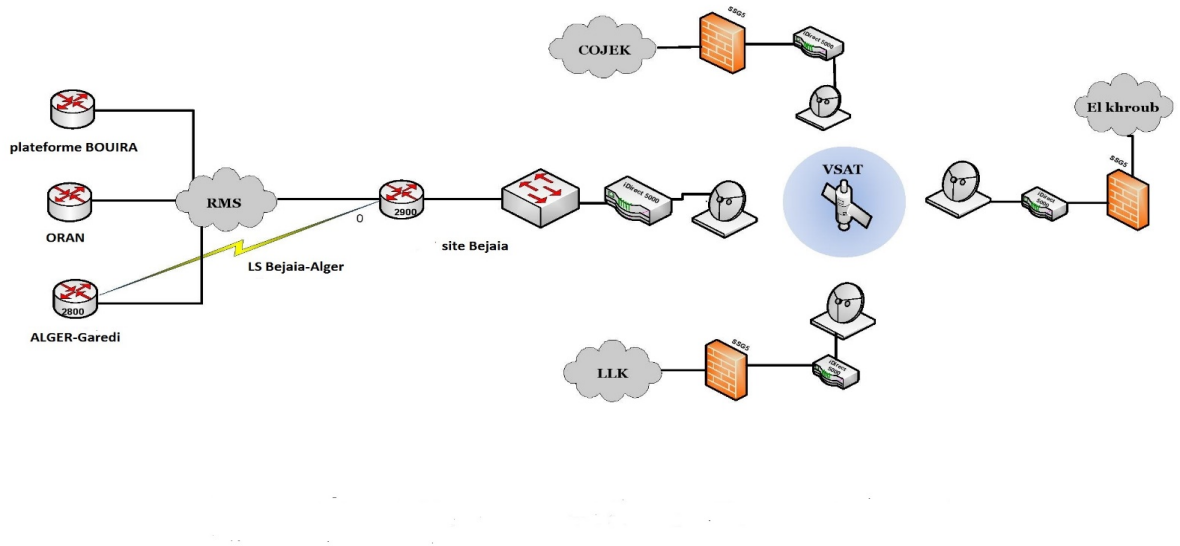

FIGURE 3.3 – Schéma d'interconnexion Réseaux WAN-VSAT au sein de CEVITAL.

3.5 Présentation du contexte du projet

Notre projet consiste à mettre en place une connexion sécurisée entre les différents sites distants de l'entreprise CEVITAL, dont les communications sont faites à travers un réseau backbone d'un opérateur privé (ooredoo) utilisant le protocole de liaison Frame

relay. L'intérêt majeur de ce travail est de découvrir les différents aspects de la sécurité sur la transmission des données dans un réseau, à savoir, les réseaux privé virtuel (VPN).

3.5.1 Problématique

De nombreuses difficultés de communication et de diffusion de l'information sont rencontrées lors de l'utilisation des liaisons satellitaires VSAT parmi lesquelles :

- Problème de coût : quatre-vingt millions par mois, 960 millions par ans.
- Problème de lenteur : les utilisateurs des autres sites accèdent aux serveurs de site central (serveur de messagerie, serveurs de stockage et serveur sage pour la facturation).
- Si l'élément central hub tombe en panne empêche la communication entre les différant sites.

D'où la nécessité d'une intervention faisant appel aux moyens de sécurité informatique, car lors d'échange des données entre ses différents sites, ces données transitent par le réseau privé (opérateur), ce qui les rendent possible d'être interceptées et rend la communication vulnérable.

3.5.2 Solution proposée

Afin de résoudre au mieux les différentes préoccupations manifestées par les responsables informatiques de CEVITAL.

Nous avons opté pour une solution VPN site à site, qui consiste à mettre en place une architecture réseau VPN sécurisée, pour l'interconnexion des sites distant de l'entreprise, cette solution permet de garantir la sécurité, la confidentialité, et l'intégrité des données sur des canaux privés, et sur l'aspect financier. Cette solution permet d'obtenir une liaison sécurisée à moindre coût.

3.6 Conclusion

Au terme de ce troisième chapitre consacré à la présentation de l'organisme d'accueil et ses différents sites, l'analyse de l'existant, critique de l'existant et proposition d'une solution VPN site-à-site qui consiste à mettre en place une liaison permanente, distante et sécurisée. Le chapitre suivant, quant à lui, sera consacré à la mise en œuvre de la solution proposée.

Chapitre 4

Mise en œuvre des VPNs

4.1 Introduction

La mise en œuvre des VPNs est l'une des solutions à laquelle nous avons abouti suite à notre étude faite dans le chapitre précèdent.

Dans ce chapitre, nous décrirons les outils utilisés, présenterions l'architecture permettant de relier les différents sites de l'entreprise ainsi que les principales étapes de configuration pour mettre en œuvre un VPN site à site.

4.2 Description de l'environnement de travail

4.2.1 GNS3

GNS3 signifie Graphical Network Simulator, est un simulateur graphique de réseau qui permet l'émulation de réseaux informatique (voir figure 4.1). Contrairement à « Cisco Packet Tracer », qui est un simulateur de matériel réseau Cisco, GNS3 est une solution libre disponible sous Windows, GNU/Linux et MacOs permettant l'émulation ou la simulation de véritable IOS Cisco (Internetworking Operating System) via une interface graphique[21], il permet de reproduire une architecture physique ou logique grâce à :

- **Dynamips**
  Un émulateur d'image IOS qui permet de lancer des images binaires IOS provenant de Cisco Systèmes.
- **Dynagen**
  Qui est une interface en mode texte pour Dynamips. Cet outil va permettre l'interconnexion de plusieurs machines émulées.
- **Qemu**
  Qui est un émulateur de système. Cet outil va permettre à GNS3 d'exécuter Cisco ASA, PIX et IDS.

- **Virtualbox**
  Qui va nous permettre de créer et lancer ces machines virtuelles
- **Wireschark**
  Wireschark est un logiciel pour analyser les trames.

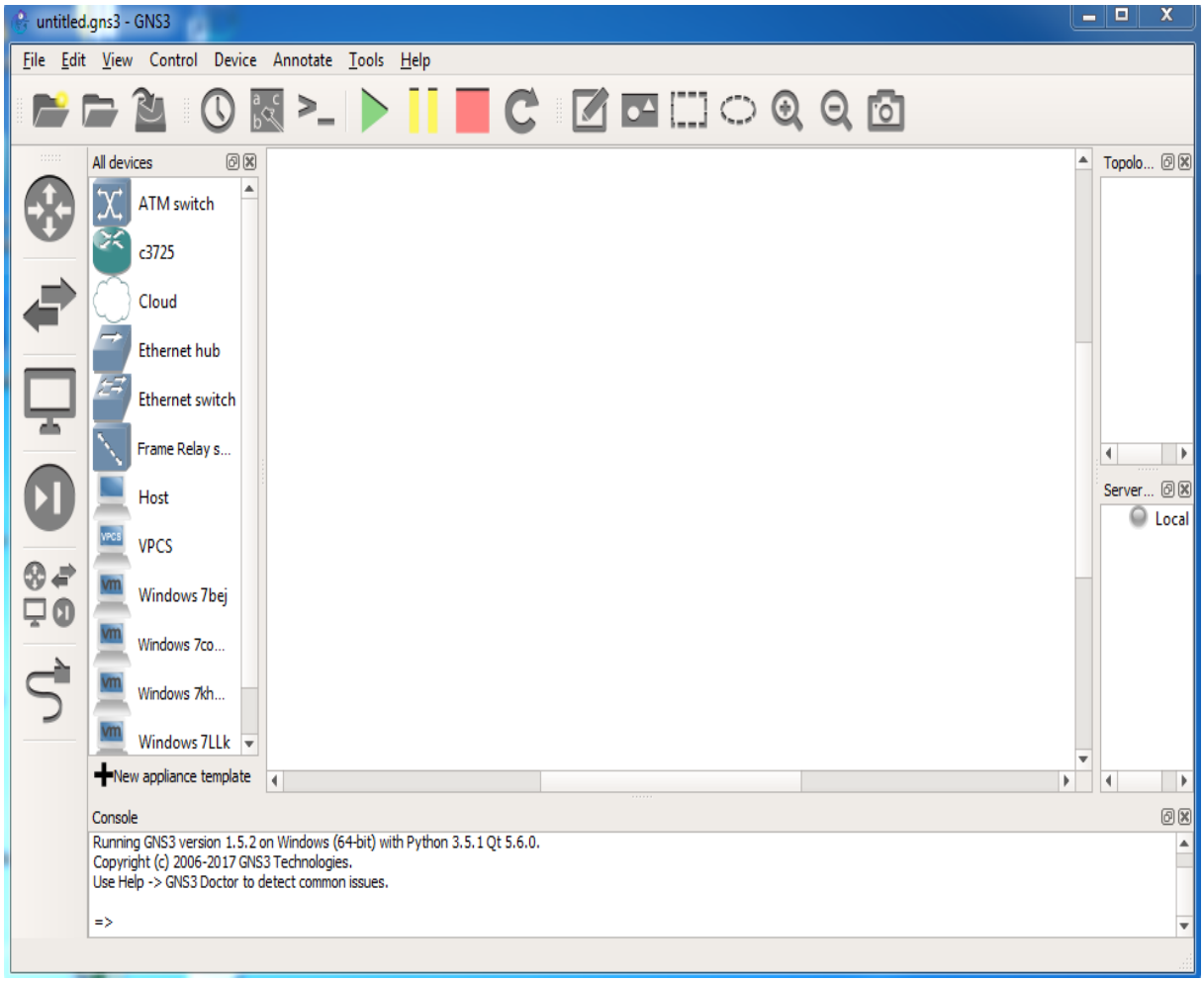

FIGURE 4.1 – L'interface graphique de GNS3.

4.2.2 Wireshark

Wireshark est l'analyseur réseau le plus populaire du monde. Cet outil extrêmement puissant fournit des informations sur des protocoles réseaux et applicatifs à partir de données capturées sur un réseau. Il permet à l'utilisateur de visualiser une liste de paquets capturés, analyser des données sur chaque paquet. Les données contenues dans ce paquet au format hexadécimal. Il a intégré des fonctionnalités de codage couleur qui aident

l'utilisateur à identifier notamment les types de trafic réseau, tels que DNS en bleu et en vert HTTP. Son interface graphique est représentée dans la figure 4.2 .

Comme un grand nombre de programmes, Wireshark utilise la librairie réseau pcap pour capturer les paquets.

La force de Wireshark vient de :

- Sa facilité d'installation.
- sa simplicité d'utilisation de son interface graphique.
- son très grand nombre de fonctionnalités.

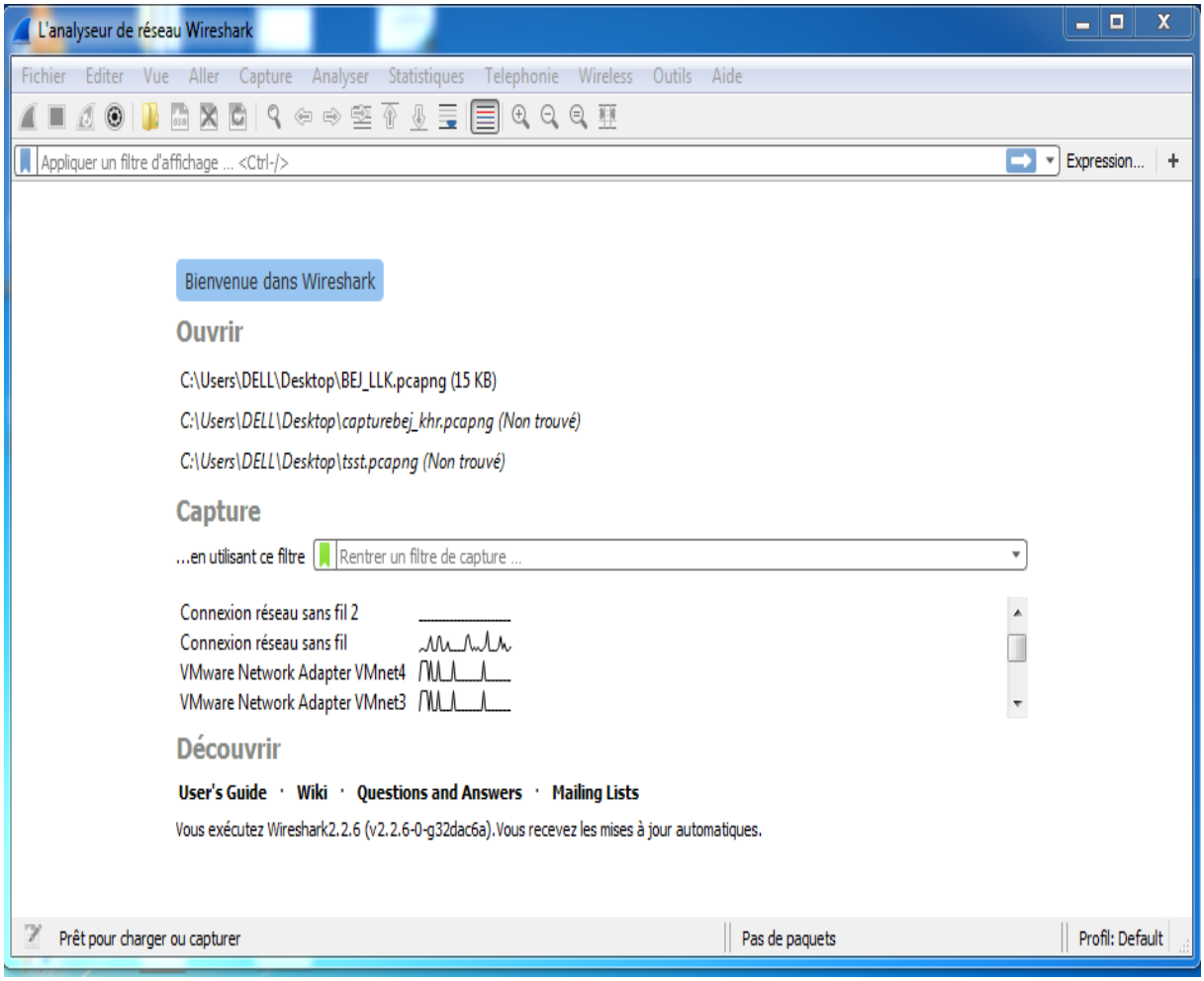

FIGURE 4.2 – L'interface graphique de Wireshark.

4.2.3 VMWARE

Permet la création d'une ou plusieurs machines virtuelles, au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau

local avec une adresse IP différente, tout en étant sur la même machine physique (machine existante réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps[22]. La figure suivante représente l'interface de la VMWare workstation 11.

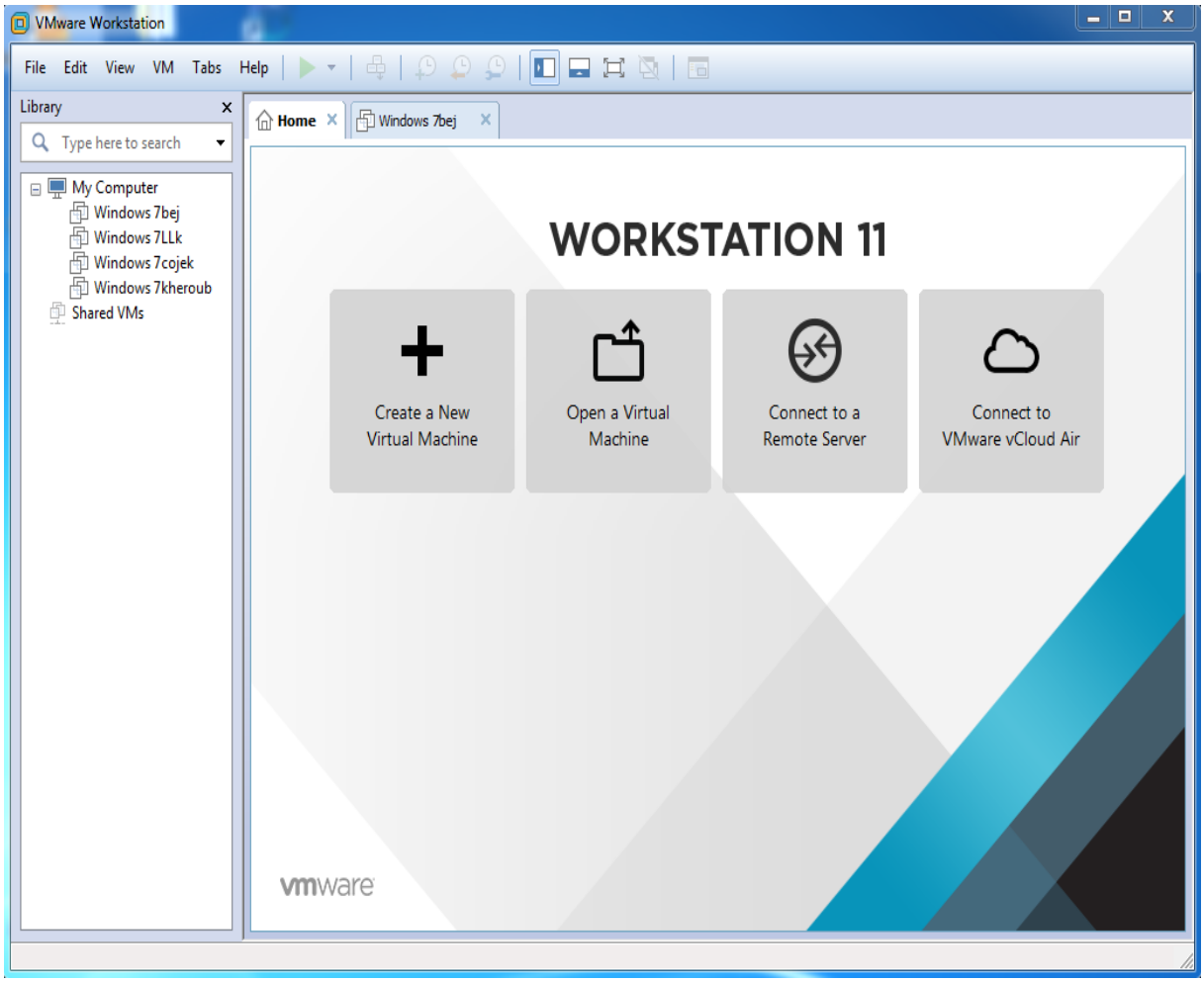

FIGURE 4.3 – L'interface graphique VMWare workstation 11.

4.3 Mise en place d'un VPN site à site

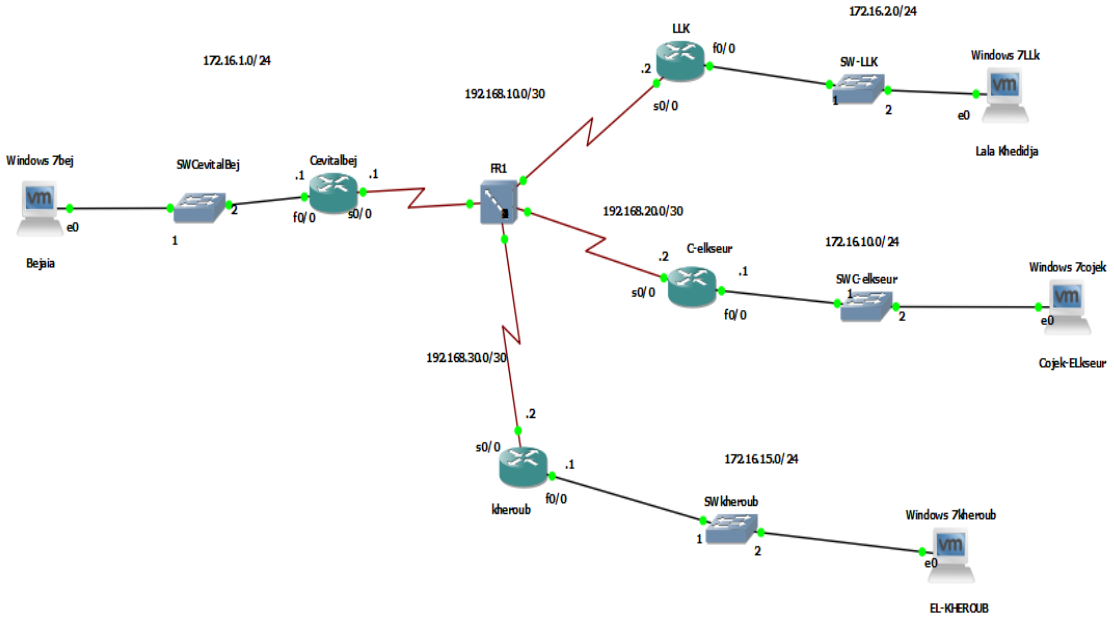

FIGURE 4.4 – La topologie réseau étendu de l'entreprise CEVITAL.

La nouvelle architecture proposée dispose de quatre sites (voir figure 4.4), notre topologie illustre leurs interconnexions via un tunnel VPN. Pour cela, il faudrait définir une clef partagée, une association de sécurité, une fonction de hachage.

Ainsi, cette solution permettra au site central CEVITAL Bejaia d'échanger des données avec les autres sites de CEVITAL (Lala Khedidja, Cojeck Elkseur, Elkhroub) en passant par un protocole de liaison Frame Relay d'une façon sécurisée, en utilisant le tunnel VPN.

Le site central se connecte a chaque site avec la même clé partagé, le type de hachage, la taille de police, la longueur des clés, la durée de vie de clé avant renégociation, la méthode de cryptage des données, la durée de vie de la clé de cryptage, une ACL permettant d'identifier le trafic à traiter par le tunnel et enfin la création d'une cryptomap.

4.4 Configuration des cartes réseaux virtuels sous vmware

Après installation des machines virtuelles sous Vmware, nous devons leurs affectés des adresses IP en les connectant vers une carte réseaux virtuel, afin de configurer cette dernière nous allons ouvrir Vmware en tant qu'administrateurs cliquer sur édite puis virtuel network

editor ensuite une fenêtre s'ouvrira comme le montre la figure 4.5 cliqué sur add network puis saisir l'adresse IP ensuite coucher host-only et connect a host virtuel adapter To this network.

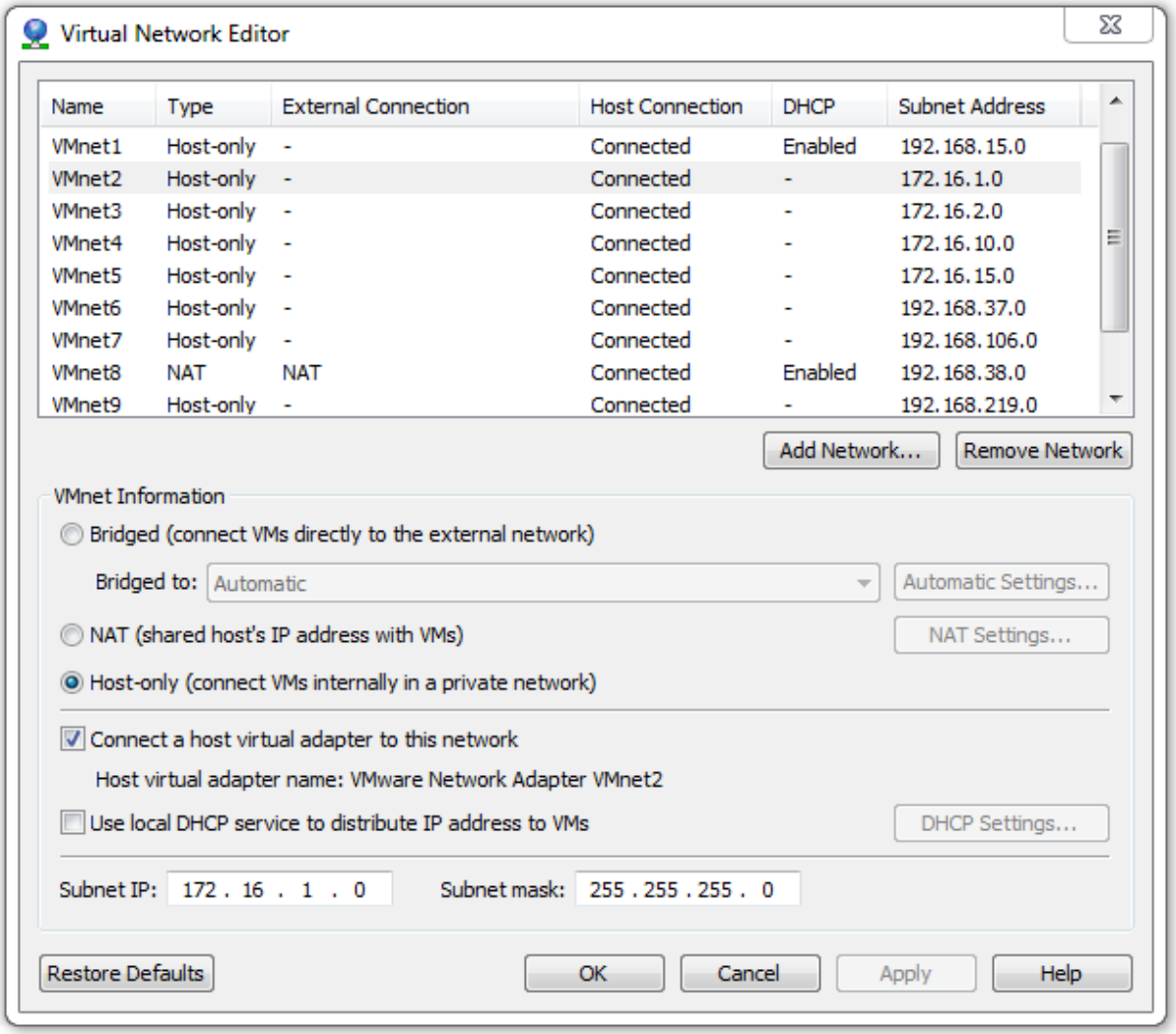

FIGURE 4.5 – Configuration des cartes réseaux virtuels

Après la configuration des cartes réseaux virtuel, nous allons connecter chaque machine vers une carte réseau qui lui correspond.

4.5 Affectation des adresses IP et protocole de routage

Nous allons configurer chaque routeur des différents sites en les attribuons les adresses IP, affectant le protocole de routage.

4.5.1 Site de Bejaia

Le site de Bejaia (site central) est représenté par un routeur Cisco de gamme 3725 pour lequel nous avons attribué les interfaces suivantes :

Reliée au réseau local par f0/0 : 172.16.1.1/24.

Reliée au Frame Relay par :

S0/0.102 : 192.168.10.1/30 avec le site LLK (Lala Khedidja).

S0/0.103 : 192.168.20.1/30 avec le site Cojek Elkseur.

S0/0.104 : 192.168.30.1/30 avec le site ElKheroube.

/30 car chaque routeur possède au maximum 3 interface.

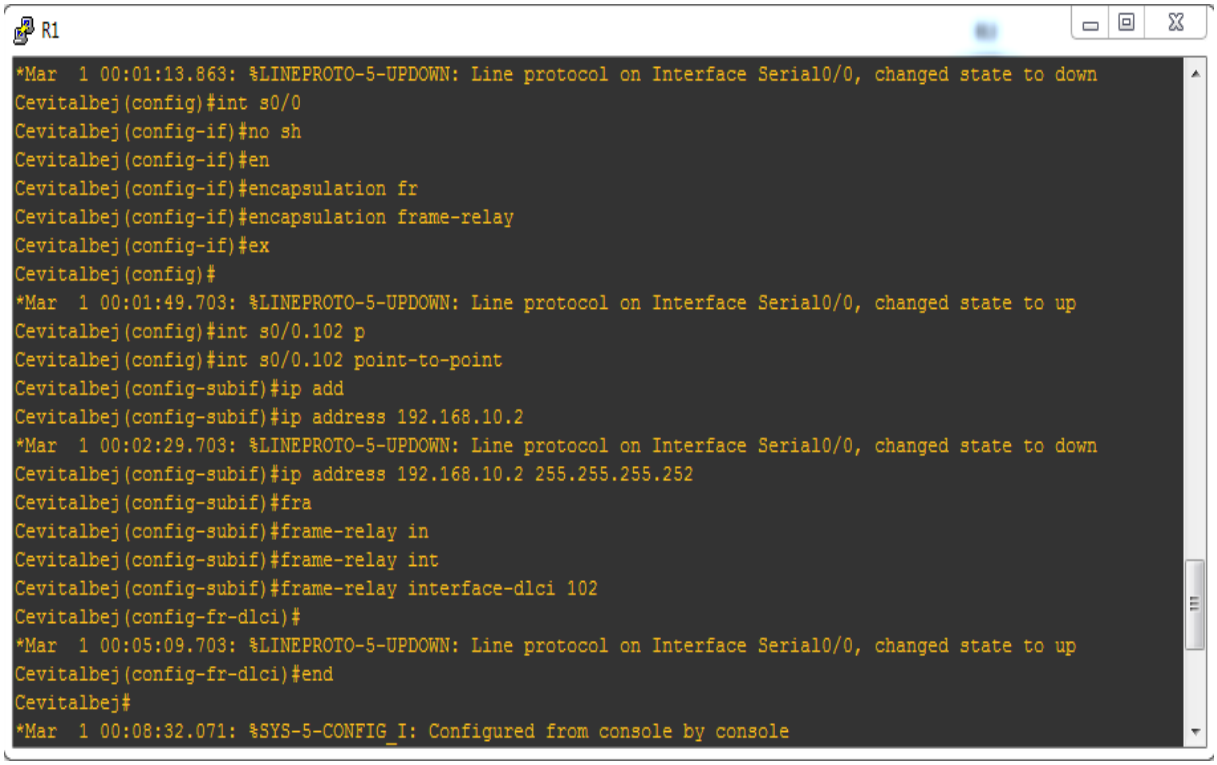

FIGURE 4.6 – Configuration Frame Relay (Site Bejaia et site LLK).

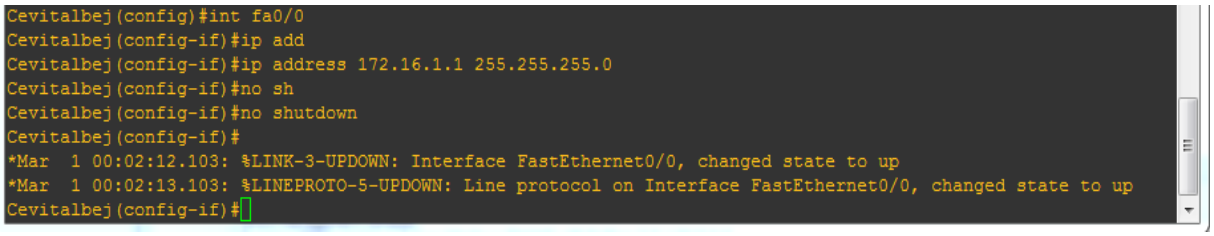

FIGURE 4.7 – Configuration réseau local (site de Bejaia).

Nous avons utilisé OSPF (Open Shortest Path First) comme protocole de routage pour plusieurs raisons :

- OSPF est un protocole de routage dynamique conçu à choisir la voie la plus efficace pour livrer des paquets IP au sein d'un seul réseau, il est utilisé dans l'architecture du réseau réel.
- OSPF est un protocole conçu pour fonctionner avec les grands réseaux (comme dans notre cas). Ainsi, il permet de diviser le domaine de routage afin de faciliter sa gestion.

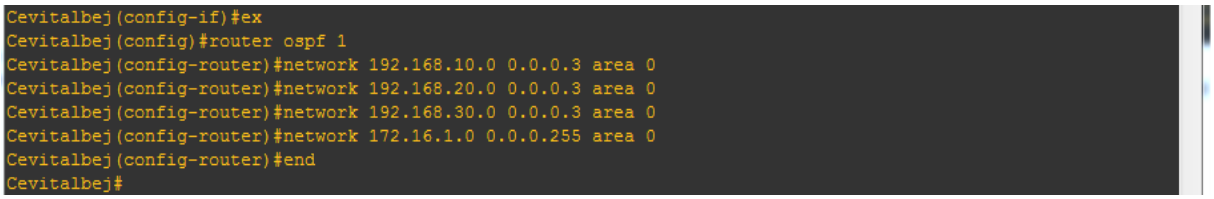

FIGURE 4.8 – Protocole de routage OSPF (Site de Bejaia).

4.5.2 Site LLK (Lala Khedidja)

Il est représenté par un routeur Cisco de gamme 3725 pour lequel nous avons attribué les interfaces suivantes :

Reliée au réseau local f0/0 : 172.16.2.1/24.

Reliée au Frame Relay S0/0.201 : 192.168.10.2/30.

Le protocole de routage utilisé OSPF.

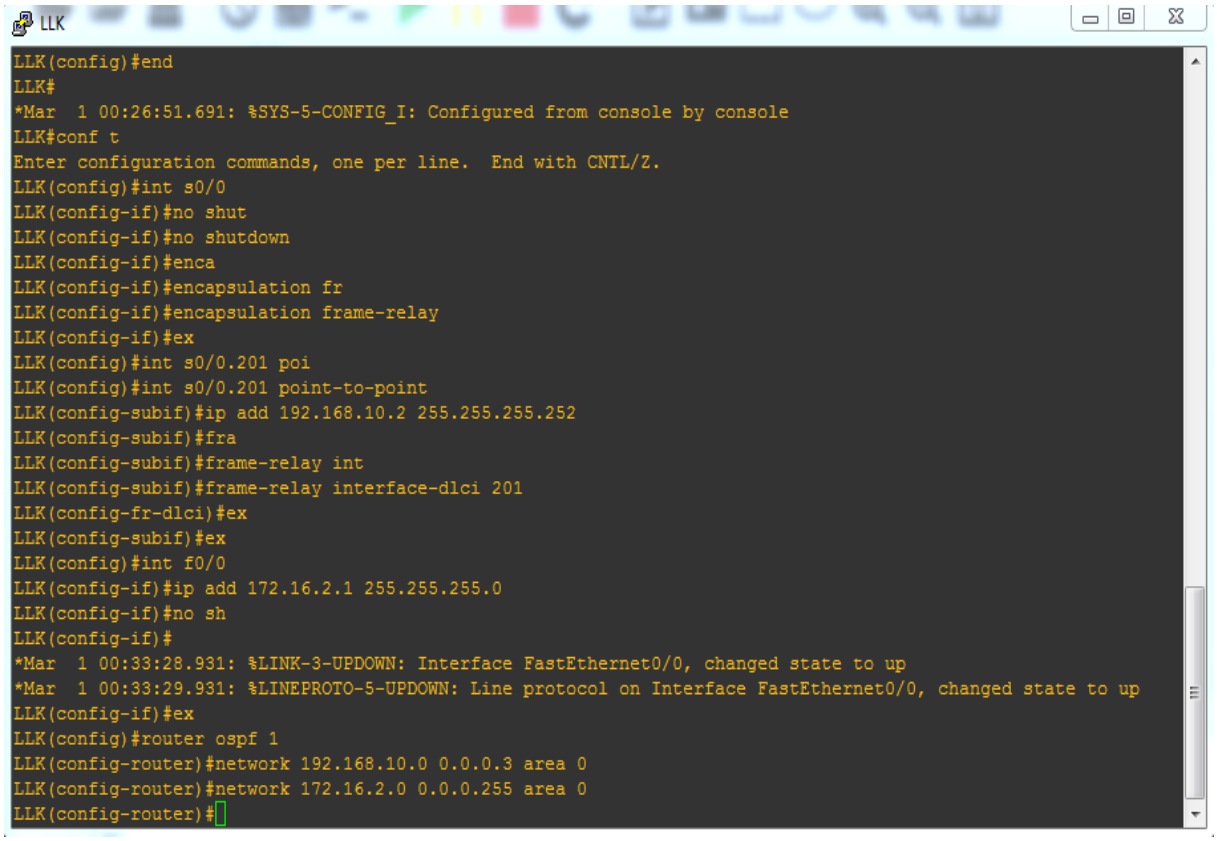

FIGURE 4.9 – Configuration site Lala Khedidja.

4.5.3 Site COJECK

Il est représenté par un routeur Cisco de gamme 3725 pour lequel nous avons attribué les interfaces suivantes :

Reliée au réseau local f0/0 : 172.16.10.1/24.

Reliée au Frame Relay S0/0.301 : 192.168.20.2/30.

Le protocole de routage utilisé OSPF.

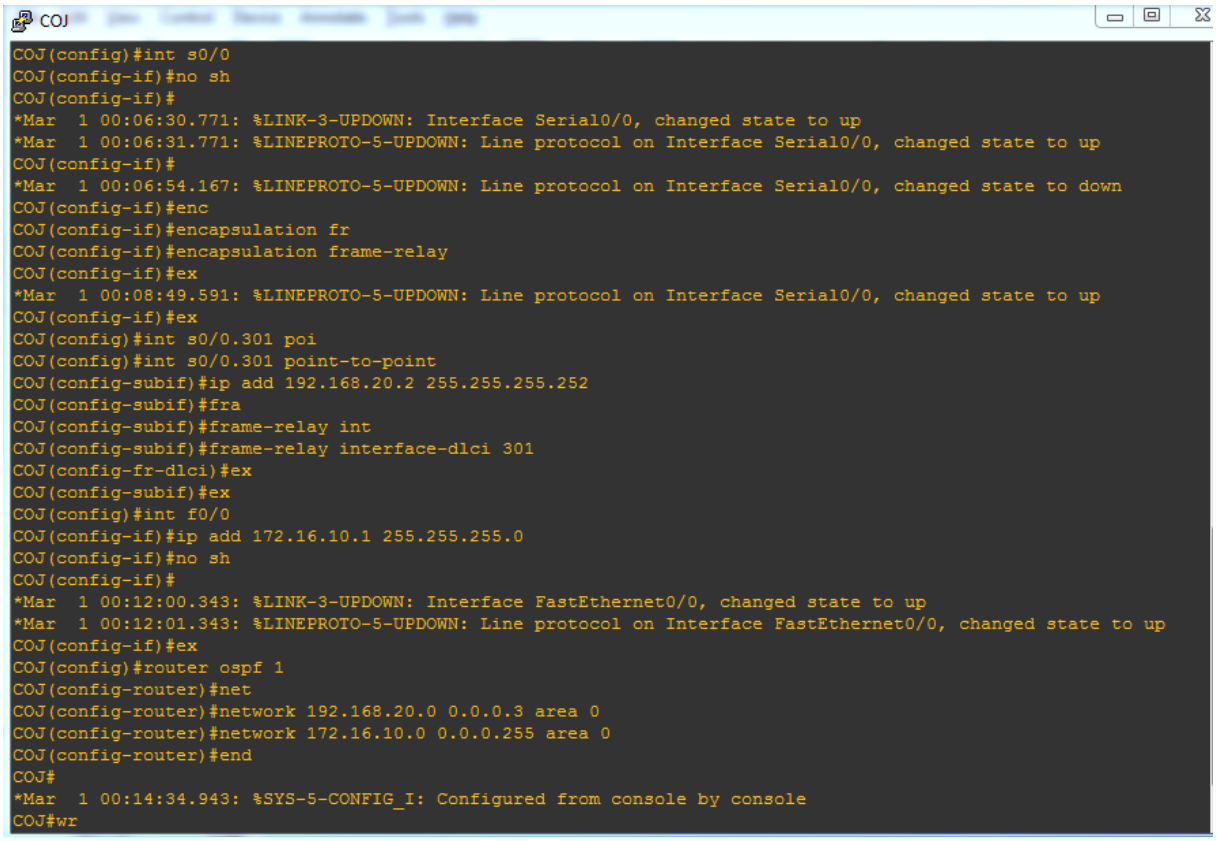

FIGURE 4.10 – Configuration de routeur de Cojeck.

4.5.4 Site Elkheroub

Il est représenté par un routeur Cisco de gamme 3725 pour lequel nous avons attribué les interfaces suivantes :

Reliée au réseau local f0/0 : 172.16.15.1/24.

Reliée au Frame Relay S0/0.401 : 192.168.30.2/30.

Le protocole de routage utilisé OSPF.

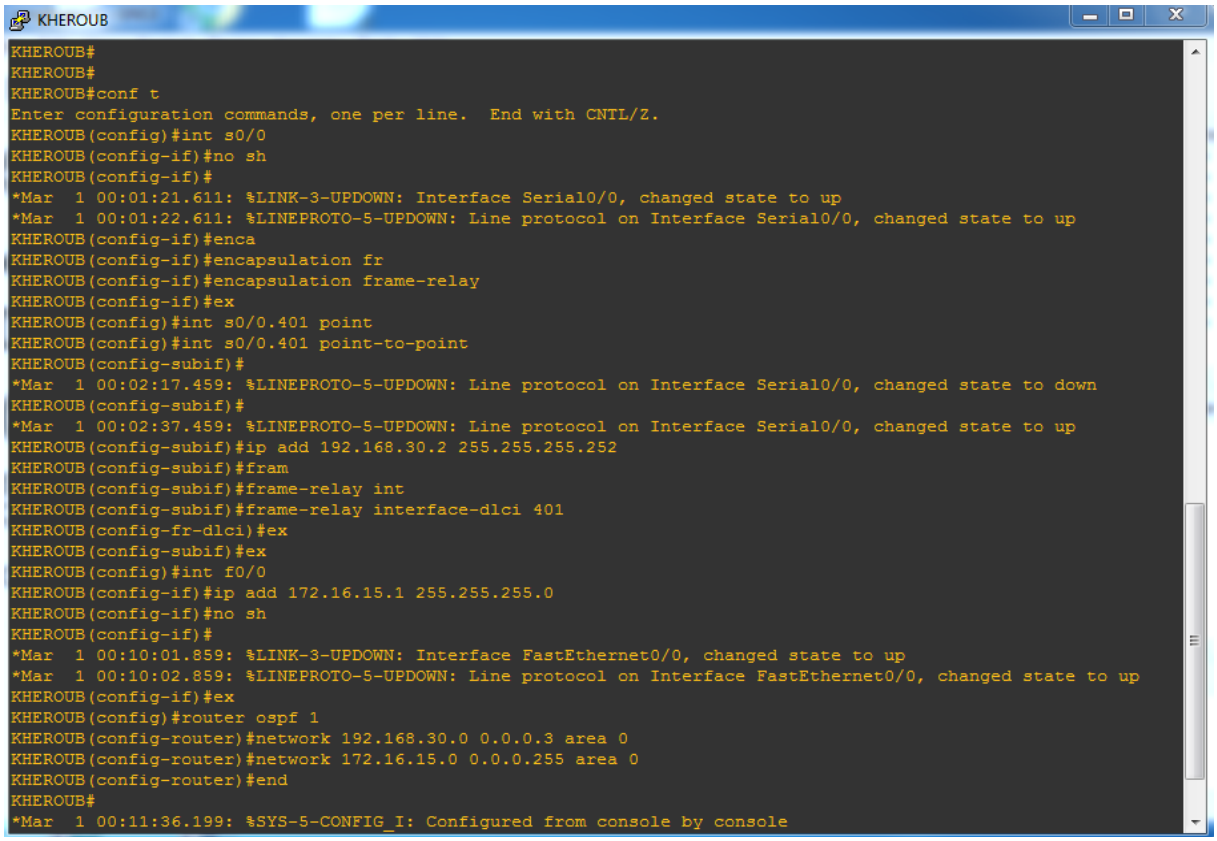

FIGURE 4.11 – Configuration de routeur de site Kheroub.

4.5.5 Vérification de routage

Pour vérifier la connectivité à partir de routeur de site central de Bejaia vers les autres sites (LLK, Cojeck, Elkhroub) , à l'aide de la commande ping, les routeurs Cisco envoient cinq requêtes ping consécutives et mesurent les durées de transmission minimale, moyenne et maximale. Les points d'exclamation permettent de vérifier la connectivité. Dans notre cas, nous lançons un ping de site central vers tous les sites comme le montre la figure 4.12.

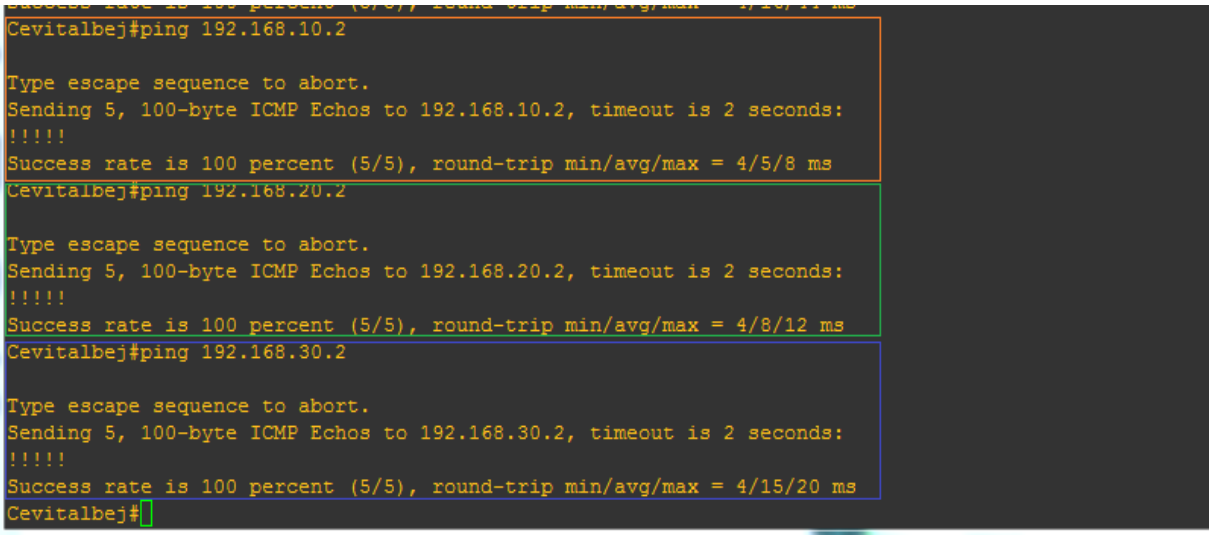

FIGURE 4.12 – Résultat d'une requête ICMP de site centrale vers les autres sites.

Pour voir ce qui se passe sur notre architecture pendant la commande ping, nous utilisons le logiciel wireshark dans GNS3.

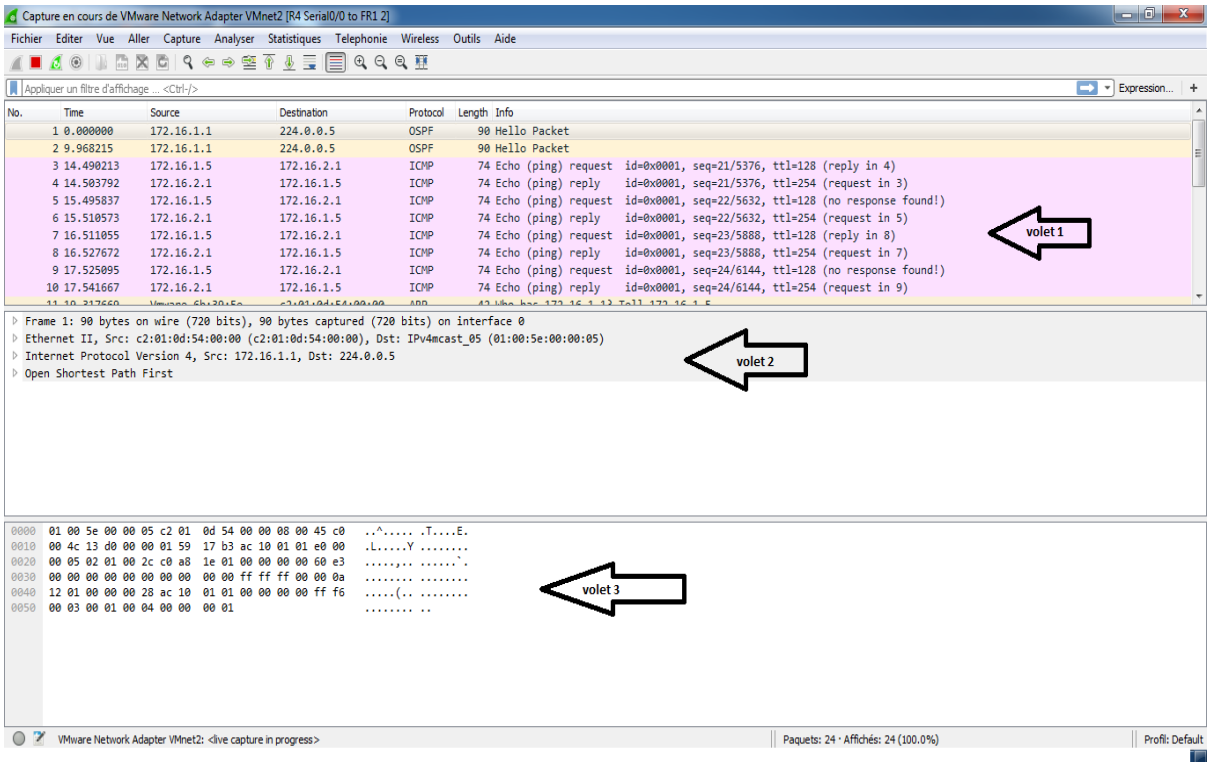

FIGURE 4.13 – La capture après le ping sous Wireshark.

Nous remarquons dans la figure 4.13, que l'affichage des résultats se décompose en trois parties :

- **Le volet 1** Qui permet de recenser l'ensemble des paquets capturés, après un ping, des échanges de messages entre deux sites grâce au protocole ICMP (Internet Control Message Protocol).
- **Le volet 2**
  La décomposition exacte de paquet. Cette décomposition permet de visualiser les champs des entêtes des protocoles ainsi que l'imbrication des différentes couches de protocoles connus.
- **Le volet 3**
  contient la capture affichée en hexadécimal et en ASCII.

4.6 Création des VPN

Il y a deux tâches principales pour l'implémentation d'un VPN IPSec :

- La configuration des paramètres ISAKMP.
- La configuration des paramètres IPSec.

Avant d'entamer la création des VPNs, nous devons activer le protocole qui gère l'échange des clés qui seront utilisées entre les deux extrémités du tunnel.

```
Cevitalbej#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cevitalbej(config)#crypto isakmp enable
```

FIGURE 4.14 – Activation de protocole ISAKMP.

4.6.1 Première étape « Creation de la strategie ISAKMP »

Il faut créer une stratégie ISAKMP et configurer une association d'extrémité incluant la stratégie ISAKMP. Une stratégie ISAKMP définit les algorithmes d'authentification, de cryptage et de hachage utilisés pour transmettre le trafic entre les deux extrémités VPN.

```
Cevitalbej(config)#crypto isakmp policy 2
Cevitalbej(config-isakmp)#encr
Cevitalbej(config-isakmp)#encryption aes 256
Cevitalbej(config-isakmp)#aut
Cevitalbej(config-isakmp)#authentication pre
Cevitalbej(config-isakmp)#authentication pre-share
Cevitalbej(config-isakmp)#hash sha
Cevitalbej(config-isakmp)#group
Cevitalbej(config-isakmp)#group 2
Cevitalbej(config-isakmp)#life
Cevitalbej(config-isakmp)#lifetime 86400
Cevitalbej(config-isakmp)#
```

FIGURE 4.15 – Configurer la politique de sécurité ISAKMP.

La description des commandes utilisées dans la figure 4.15 est présentée ci-dessous :

- **Policy :** Policy qui définit la politique de connexion pour les SA (Security Association) de ISAKMP. Un numéro indiquant la priorité de l'utilisation lui est attribué à la fin de la commande.
- **Encryption :** Nous avons utilisé AES comme algorithme de chiffrement.
- **Pre-share :** Utilisation d'une clé pré-partagée comme méthode d'authentification.
- **Sha :** L'algorithme de hachage.
- **Group 2 :** Spécifie l'identifiant Diffie-Hellman pour l'échange de clef.
- **Lifetime :** Spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs.

4.6.2 Deuxième étape « Création de la clé pré-partagée "VPN-PROJET" »

Configurez une clé sur chaque routeur qui pointe vers l'autre extrémité du VPN. Ces clés doivent correspondre pour que l'authentification soit réussie.

```
Cevitalbej(config)#crypto isakmp key 0 VPNPROJET add
Cevitalbej(config)#crypto isakmp key 0 VPNPROJET address 192.168.30.2
Cevitalbej(config)#
```

FIGURE 4.16 – Création de la clé pré-partagée.

4.6.3 Troisième étape « Configuration IPSec »

Pour configurer le protocole IPSec nous avons besoin de configurer les éléments suivants :

- Créer l'IPSec Transform.
- Créer un ACL étendue.
- Créer le crypto map.
- Appliquer crypto map à l'interface publique.
- **Phase 1 :** Cette étape consiste à créer la transformation définie utilisée pour protéger les données (IPSec) nommé « PRJVPNSET ».

```
Cevitalbej(config)#crypto ipsec transform-set PRJVPNSET esp-aes esp
Cevitalbej(config)#crypto ipsec transform-set PRJVPNSET esp-aes esp-sh
Cevitalbej(config)#crypto ipsec transform-set PRJVPNSET esp-aes esp-sha-hmac
Cevitalbej(cfg-crypto-trans)#
```

FIGURE 4.17 – Configuration de la Transform-Set.

Ensuite, nous fixons une valeur de la durée de vie de la clé partagée en Seconde.

```
Cevitalbej(config)#crypto ipsec security-association lif
Cevitalbej(config)#crypto ipsec security-association lifetime sec
Cevitalbej(config)#crypto ipsec security-association lifetime seconds 1800
Cevitalbej(config)#
```

FIGURE 4.18 – Configuration la durée de vie de la clé partagée.

- **Phase 2 :** Cette étape consiste à créer une ACL (Access List) qui va déterminer le trafic autorisé de passer à travers le tunnel VPN. Dans notre projet, le trafic s'achemine du réseau 172.16.1.0/24 à 172.16.15.0/24.

```
Cevitalbej(config)#ip access-list extended VPN
Cevitalbej(config-ext-nacl)#$72.16.1.0 0.0.0.255 172.16.15.0 0.0.0.255
```

FIGURE 4.19 – Création des ACL.

- **Phase 3 :** Dans cette dernière étape, nous configurons la crypto-map pour l'installation et l'établissement du lien entre ISAKMP définie précédemment et la configuration IPSEC.

```
Cevitalbej(config)#crypto map BEJ_KHR 13 ipsec-is
Cevitalbej(config)#crypto map BEJ_KHR 13 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Cevitalbej(config-crypto-map)#match add VPN
Cevitalbej(config-crypto-map)#set peer 192.168.30.2
Cevitalbej(config-crypto-map)#set tran
Cevitalbej(config-crypto-map)#set transform-set PRJVPNSET
```

FIGURE 4.20 – Configuration de la Crypto-Map.

- **Phase 4 :** La configuration de Site de Bejaia est presque terminée, nous devons appliquer la crypto-map sur l'interface de sortie de routeur, dans notre cas Serial 0/0.104.

```
Cevitalbej(config)#int s0/0.104
Cevitalbej(config-subif)#crypto map CEVBEJ_KHR
Cevitalbej(config-subif)#
*Mar  1 02:43:04.991: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Cevitalbej(config-subif)#end
```

FIGURE 4.21 – Configuration crypto-map sur l'interface de sortie de routeur.

Les paramètres pour Kheroub sont identiques, la seule différence étant les adresses IP attribuées et les listes d'accès.
Les mêmes paramètres de VPN pour :

- Le VPN entre le site de Bejaia et le site LLK.
- Le VPN entre le site de Bejaia et le site Cojeck.

4.7 Vérification

Pour pouvoir vérifier la validité de notre configuration, nous allons vérifier les informations retournées par le VPN sur le routeur CevitalBej (Central)

4.7.1 Vérification du transform-set

```
Cevitalbej#show cry
Cevitalbej#show crypto ipsec tr
Cevitalbej#show crypto ipsec transform-set
Transform set PRJVPNSET: { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Cevitalbej#
```

FIGURE 4.22 – Vérification du mode.

La commande show crypto IPSec transform-set nous a permit de savoir quel mode utilisé, dans notre cas c'est le mode tunnel.

4.7.2 Vérification de la Crypto-Map

```
Cevitalbej#show crypto map
Crypto Map "CEVBEJ_KHR" 13 ipsec-isakmp
        Peer = 192.168.30.2
        Extended IP access list VPN
            access-list VPN permit ip 172.16.1.0 0.0.0.255 172.16.15.0 0.0.0.255
        Current peer: 192.168.30.2
        Security association lifetime: 4608000 kilobytes/1800 seconds
        PFS (Y/N): N
        Transform sets={
                PRJVPNSET,
        }
        Interfaces using crypto map CEVBEJ_KHR:
                Serial0/0.104
```

FIGURE 4.23 – Vérification de la MAP.

L'exécution de la commande show crypto map permet d'afficher l'adresse IP de destination et l'interface de sortie activée.

4.7.3 Vérification des paramètres IPsec

```
Cevitalbej#show crypto ipsec sa

interface: Serial0/0.104
    Crypto map tag: CEVBEJ_KHR, local addr 192.168.30.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0)
   current_peer 192.168.30.2 port 500
     PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
    #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xBC981099(3164082329)

     inbound esp sas:
      spi: 0x56EB86C2(1458276034)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: 1, crypto map: CEVBEJ_KHR
        sa timing: remaining key lifetime (k/sec): (4491836/1780)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xBC981099(3164082329)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: 2, crypto map: CEVBEJ_KHR
        sa timing: remaining key lifetime (k/sec): (4491836/1768)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
```

FIGURE 4.24 – Vérification des opérations d'IPsec.

La commande show Crypto IPSec permet d'afficher l'interface de sortie (192.168.30.1) et l'interface d'entrée (192.168.30.2), les ACLs qui autorisent l'accès entre le site central et le site Kheroub avec le masque et le numéro de port, le nombre de paquets envoyés et reçus sont égaux et le protocole utilisé est ESP.

4.7.4 Vérification des opérations ISAKMP

```
Cevitalbej#show crypto isakmp sa
dst             src             state          conn-id slot status
192.168.30.2    192.168.30.1    QM_IDLE              1    0 ACTIVE

Cevitalbej#
```

FIGURE 4.25 – Vérification des opérations ISAKMP.

Nous terminons avec les captures faites avec Wireshark.

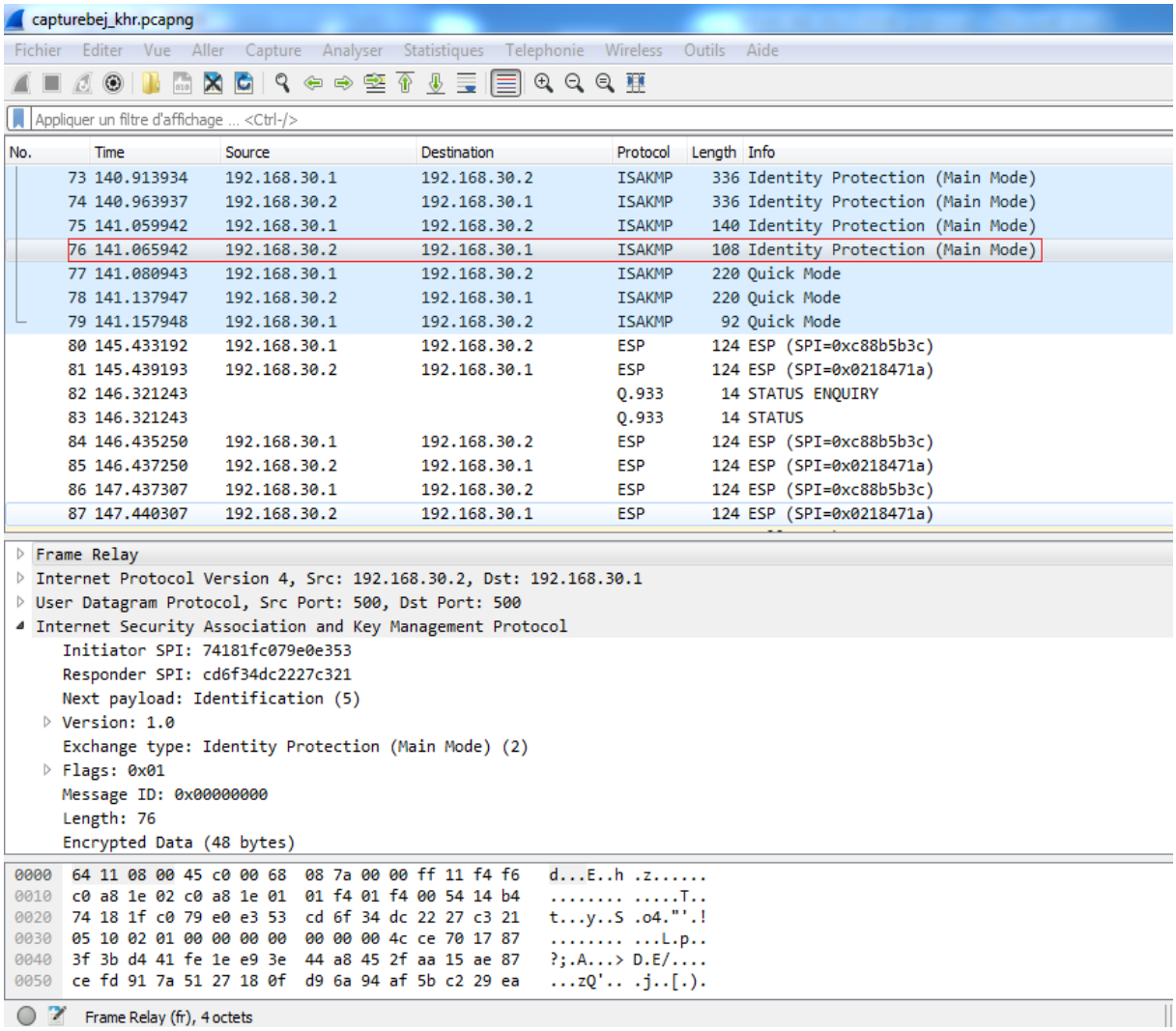

FIGURE 4.26 – Le protocole ISAKMP en mode main.

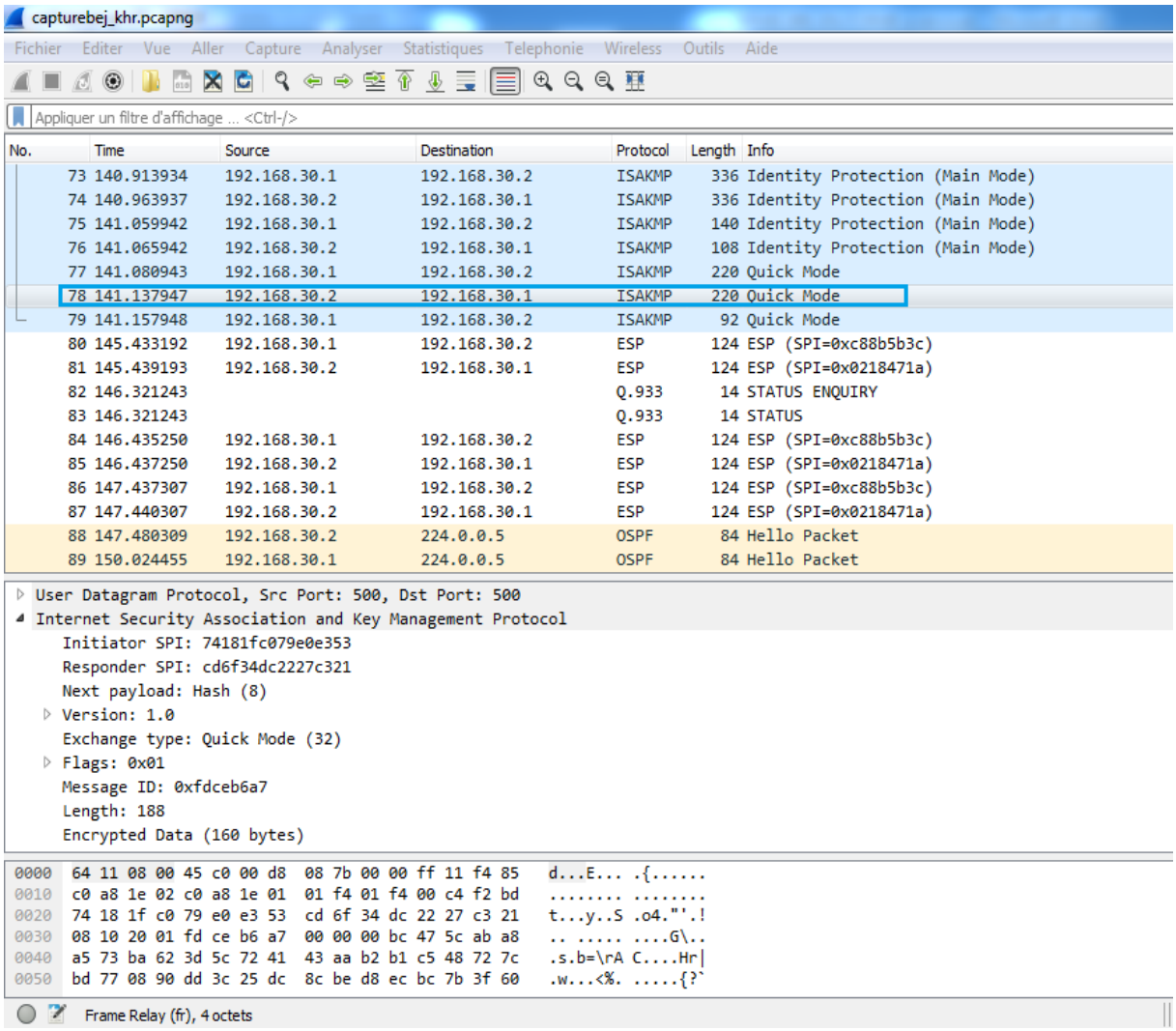

FIGURE 4.27 – Le protocole ISAKMP en mode quick.

Les messages échangés durant le mode quick (Quick mode) sont protégés en authenticité et en confidentialité grâce aux éléments négociés durant le mode main (main mode). L'authenticité des messages et assurée par l'ajout d'un bloc HASH après l'en-tête ISAKMP, et la confidentialité est assurée par le chiffrement de l'ensemble des blocs du message. Enfin, la capture dans la figure 4.28, nous montre clairement que le trafic est crypté avec le protocole ESP.

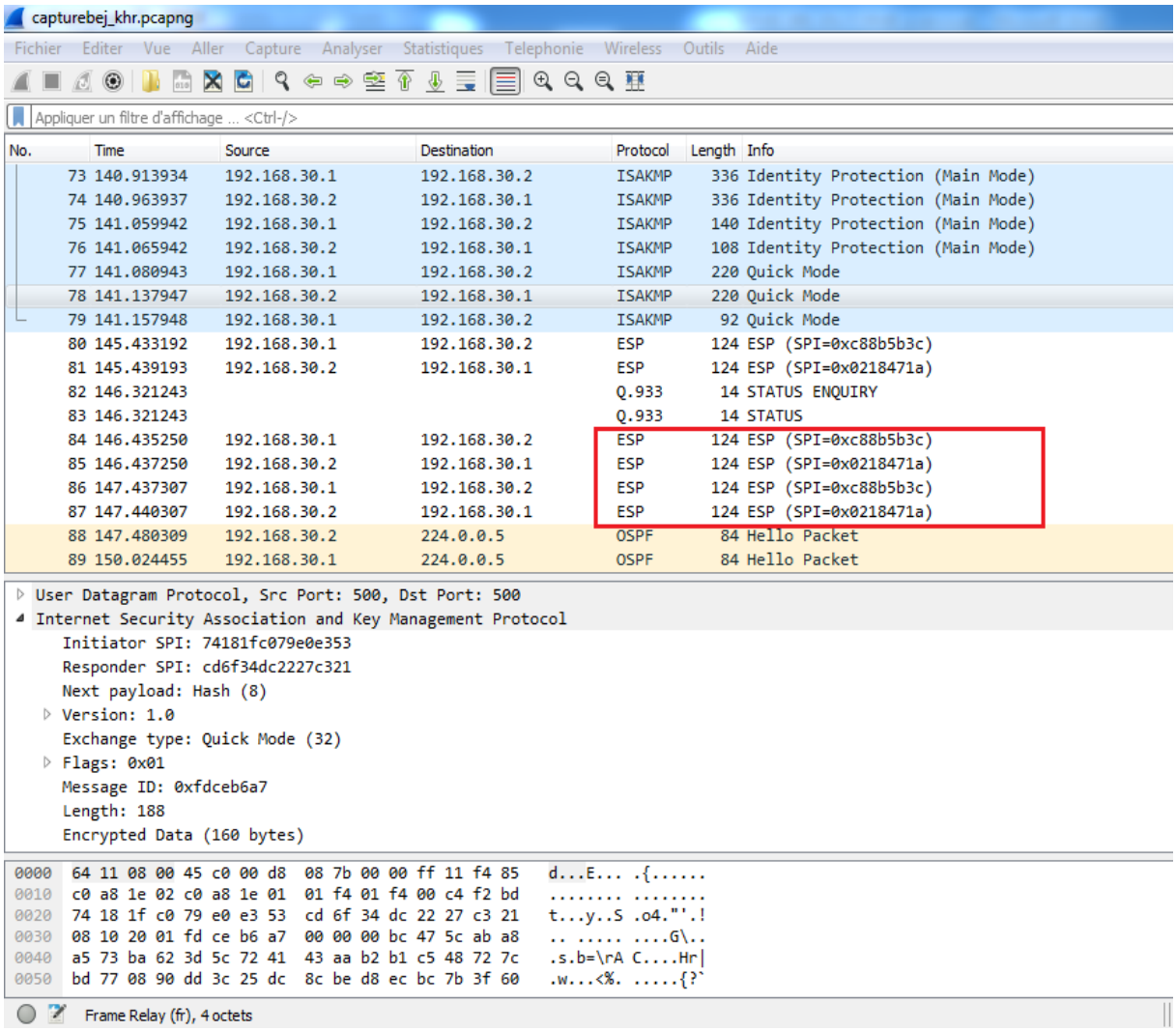

FIGURE 4.28 – Le protocole ESP.

4.8 Conclusion

Dans ce chapitre, nous avons présenté les outils que nous avons utilisé, ensuit, nous avons présenté les différents étapes de la configuration de notre solution qui est la mise en place d'un tunnel VPN reliant les quatre sites distants site à site de l'entreprise Cevital, ainsi que les résultats des différents tests effectués afin de vérifier le bon fonctionnement de notre solution.

Conclusion générale

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats obtenus lors de la mise en place d'un réseau VPN site-à-site pour l'entreprise Cevital. Nous avons en effet grâce à cette nouvelle technologie permis aux employés de partager de façon sécurisée leurs données via le protocole IPSec qui est le principal outils permettant d'implémenter les VPN, ce partage était possible en interne pour les utilisateurs du réseau local de l'entreprise.

En effet, nous avons présenté un travail divisé en deux parties, à savoir l'approche théorique qui est subdivisé en deux chapitres dont le premier a porté sur les généralités sur les réseaux informatiques et la sécurité informatique ; le second a porté sur le VPN (Virtual Private Network) où nous avons brossé de façon claire les notions, le fonctionnement ainsi que les différents protocoles utilisés pour la mise en œuvre de réseau VPN et la deuxième partie beaucoup plus pratique qui était aussi subdivisé en trois parties dont la première a porté sur l'étude préalable dans laquelle nous avons présenté l'entreprise et nous avons fait l'analyse de l'existant, critique de l'existant et proposé une solution VPN site-à-site qui consiste à mettre en place une liaison permanente, distante et sécurisée entre deux ou plusieurs sites de l'entreprise Cevital ; la seconde a porté sur la présentation de l environnement du travail et enfin , la réalisation du projet.

En effet, la mise en place de VPN site-à-site permet aux réseaux privés de s'étendre et de se relier entre eux au travers d'internet. Cette solution mise en place est une politique de réduction des couts liés à l'infrastructure réseau des entreprises. Il en ressort que la technologie VPN basée sur le protocole IPSec est l'un des facteurs clés de succès qui évolue et ne doit pas aller en marge des infrastructures réseaux sécurisés et du système d'information qui progressent de façon exponentielle.

Nous avons donc pu atteindre notre objectifs qui était la mise en place d'un tunnel VPN reliant les quatre sites distant site à site de l'entreprise Cevital et d'avoir enfin un réseau répondant toujours à nos attentes, ce qui est obligatoire surtout sur un domaine comme l'informatique. La réalisation de ce projet a été bénéfique et fructueux pour nous dans le sens ou il nous a permis d'approfondir et d'acquérir de nouvelles connaissances qui seront utiles et déterministes pour nous à l'avenir.

En définitive, comme tout travail scientifique, nous n'avons pas la moindre prétention d'avoir réalisé un travail inaccessible à la critique, ni fermé à la suggestion. Nous attendons de la part de tout lecteur une retouche qui puisse la rendre meilleur.

Bibliographie

[1] P. Guy, *Initiation-aux-réseaux,* Eyrolles 7éme édition, 2011.

[2] F. Jacquenod, Cours Réseaux No5, les matériels d'interconnections, http : //www.netalya.com/fr/reseaux5.asp.

[3] Pierre Erny, *Les réseaux informatiques d'entreprise*, 1998.

[4] J. Pillou, *Tout sur les réseaux et Internet*, DUNOD 2006.

[5] L. Bloch et C. Wolfhugel, Eyrolles, 2éme édition, 2005.

[6] Manuel S. lic et I. Phil, collaborateur scientifique ,Center for security Studies(CSS), ETH Zurich, aout 2006

[7] N. Baudoin et M. Karle, NT Réseaux : IDS et IPS, Rapport Ingéniorat, Institut d'électronique et d'informatique Gaspard-Monge, 2000.

[8] M. Riguidel, *Pour l'émergence d'une nouvelle sécurité dans les réseaux de communication et les systemes d'information futurs,* OFTA, Arago Vol23, Paris, 2000.

[9] S. Ikhalef, Sécurité informatique proxy, mémoire de fin d'étude ingéniorat, Université de Bejaia, 2003.

[10] TOM Thomas, *La sécurité des réseaux,* 2005.

[11] José DORDOIGNE, *Réseau informatiques,* eni, février 2011.

[12] Tomas Klein, http ://www.frameip.com/vpn/ : Document sur les Réseaux privés Virtuels-VPN, suivi Xavier Lasserre, 2014.

[13] fr.scribd.com/doc/Chap-8-Les-VPN.

[14] J.P. ARCHIER, *Les VPN, fonctionnement et mise en œuvre,* édition eni,2011.

[15] http ://www.frameip.com/vpn, 28/04/2017.

[16] Eric BAHATI, Mise en place d'un réseau VPN au sein d'une entreprise Cas de la BRALIMA, mémoire de fin d'étude, Institut supérieur de commerce Kinnshasa, 2011.

[17] www.securiteinfo.com/cryptographie/IPSec.shtml, 02/05/2017.

[18] Pierre Leonard, Mobilité et sécurité sur le réseau réaumur, mise en place de solutions DHCP et VPN, Rapport, juin 2006.

[19] S.tan, de Reynal, de Rorthais, Representation sur les VPN , rappot informatique et Réseaux, fervrier 2004.

[20] Brochure d'accueil CEVITAL.

[21] Stéphane Maas. Partie i. installer gns3 sur windows et debian.
http ://www.smnet.fr/gns3/gns3-install-intro.html, 2013-2016.

[22] Vmware workstation, http ://www.tuto-it.fr/vmware.php, 2010.

Résumé

CEVITAL est une entreprise agroalimentaire composée de sites distants répartis sur le territoire national. Pour des besoins de communication entre ces sites, CEVITAL met à leur disposition son réseau qui est alors à la merci de tous genres d'utilisateurs. Pour protéger ce réseau, une idée serait d'acquérir un mécanisme de gestion qu'il soit à la fois robuste et sécurisé pour le réseau.

En effet, l'objectif de notre travail consiste à proposer un architecteur réseau sécurisé pour CEVITAL, pour cela nous avons procédé à une étude de l'architecture actuelle, ainsi que les dispositifs de sécurité mis en place. Ce qui nous a permis de la critiquer et de suggérer des solutions afin de proposer une nouvelle architecture réseau qui donne une meilleure fluidité pour le trafic ainsi que sa sécurité.

Sur le plan applicatif, nous avons relié les quatre sites de l'entreprise CEVITAL à l'aide de protocole Frame-Relay point à point, nous avons configuré les machines virtuelles via VMWare. En fin, nous avons configuré le tunnel sécurisé au niveau du routeur des sites en utilisant le simulateur GNS3 afin de sécuriser le trafic passant par les routeurs des sites distants.

Mots-clés : VPN, IPSec, ISAKMP, GNS3, VMWare, Securité, Réseau.

Abstract:

CEVITAL is an agri-food company consisting of distant sites spread over the national territory. In order to communicate data between these sites, CEVITAL puts at their disposal its network which is subject to all kinds of users. To protect this network, one idea would be to provide a managing mechanism that is both robust and secure for the network.

Indeed, our work aims to propose a secure network architect for CEVITAL. That is why we have carried out a study of the current architecture, as well as the implemented security features. This allowed us to analyze and suggest solutions leading to a new network architecture that gives better fluidity for the traffic as well as for its security.

On the application level, we connected the four CEVITAL sites using point-to-point Frame-Relay protocol, we configured the virtual machines via VMWare. Finally, we configured the secure tunnel at the site router using the GNS3 simulator to secure the traffic passing through the routers of distant sites.

Keywords: VPN, IPSec, ISAKMP, GNS3, VMWare, Security, Network