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

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER PROFESSIONEL

En
Informatique

Option
Administration et Sécurité des Réseaux

Thème

Solution de sécurité pour le LAN étendu de la BNA

Présenté par : Mlle BELANTEUR HANIA HASSIBA
Mme BOUNECER FATEN

Soutenu le 21 Juin 2016 devant le jury composé de :

Président	**Mr AISSANI SOFIANE**	**U. A/Mira Béjaia.**
Examinateur	**Mr DEMOUCHE MOULOUDE**	**U. A/Mira Béjaia.**
Examinatrice	**Mlle ALBANE SAADIA**	**U. A/Mira Béjaia.**
Encadreur	**Dr BAADACHE ABDERRAHMENE**	**U. A/Mira Béjaia.**
Co-Encadreur	**Mr BENMANSOUR DJAMEL**	**BNA DRE de Bejaia.**

Béjaia, Juin 2016.

⁕ *Remerciements* ⁕

En préambule à ce mémoire, nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce modeste travail, ainsi qu'à la réussite de master nous tenons à remercier sincèrement le corps enseignant, académique et administratif de l'université A/Mira de Bejaia , plus particulièrement Monsieur A.Baadache, qui en tant qu'encadreur, s'est toujours montré à l'écoute tout au long de la réalisation de ce mémoire. Nos remerciements s'adressent également à Monsieur D. Benmenssoure responsable du département d'informatique de la BNA, dont l'expertise dans le domaine étudié a été essentielle dans la réalisation de ce travail. Nous souhaitons également exprimer notre gratitude à tous le personnel du département informatique de l'entreprise ,ainsi qu'à Monsieur Z.Boudraheme qui ont accepté de répondre à nos questions avec une grande compréhension et générosité. Nous n'oublions pas nos familles, proches et amis pour leur contribution, soutien et patience au cours de la réalisation de ce mémoire.

⁕ *Dédicaces* ⁕

Je dédie ce travail à mes chers parents qui m'ont soutenu durant mon existence et ma scolarité. A mes frères, sœur et toute ma famille. J'exprime mes sentiments les plus profonds à mes amis et je leurs dédie ce modeste travail.

HANIA

Je dédie ce travail à mon chère mari, ma fille et à Tout ma famille et ma belle famille.

FATEN

Table des matières

Notations et symboles

CLI : Command-Line Interpreter,
DHCP : Dynamic Host Configuration Protocol,
DMZ : DeMilitarized Zone,
ESP : Encapsulating Security Payload,
FAI : Fournisseurs d'Accès à Internet,
GRE : Generic Routing Encapsulation,
HIDS : Host Intrusion Detection System,
HTTP : Hypertext Transfer Protocol,
ICMP : Internet Control Message Protocol,
IETF : Internet Egineering Task Force,
IKE : Internet Key Exchange,
IOS : Internetwork Operating Systems,
IP : Intenet Protocol,
IPSec : Internet Protocol Security,
ISAKMP : Internet Security Association and Key Management Protocol,
L2F : Layer Two Forwarding,
L2TP : Layer Two Tunneling Protocol,
LAN : Local Area Network,
MPPE : Microsoft Point-to-Point Encryption,
Ms-Chap2 : Microsoft Challenge Handshake Authentification Protocol v.2,
NIDS : Network Intrusion Detection System,
NVRAM : No Volatil Random Access Memory,
OS : Operating Systems,
OSI : Open System Interconnection,
PING : Packet InterNet Groper,
PPP : Point to Point Protocol,
PPTP : Point to Point Tunneling Protocol,
RAM : Random Access Memory,

RFC : Request for Comments,
SA : Security Association,
SAD : Security Association Database,
SMTP : Simple Network Management Protocol,
SPD : Security Policy Database,
SPI : Security Parameter Index,
SSL : Secure Socket Layers,
SYN : SYNcronize,
TCP : Transmission Control Protocol,
UDP : Transmission Control Protocol,
VLAN : Virtual Local Area Network ou Réseau Local Virtuel,
VPN : Virtual Private Network,
WAN : Wide Area Network,
WIFI : WIreless Fidelity Internet.

Introduction générale

Les réseaux informatiques sont devenus essentiels à la bonne marche des entreprises. La croissance accélérée de ces réseaux qui sont de plus en plus ouverts sur internet, est à priori bénéfique, mais pose néanmoins un problème important de sécurité.En effet il en résulte un nombre croissant d'attaques qui peuvent aboutir à de graves conséquences professionnelles et financières en menaçant l'intégrité, la confidentialité et la disponibilité de l'information.
De nombreuses entreprises ont d'ores et déjà compris l'importance de ces enjeux, ce qui les a poussées à émerger dans le domaine de la sécurité informatique.
La sécurité se place actuellement au premier plan de la mise en œuvre et de l'administration réseau. La difficulté que représente la sécurité dans son ensemble, est de pouvoir trouver un compromis entre deux besoins essentiels :
le besoin d'ouverture de réseaux afin de profiter des différentes fonctionnalités offertes et le besoin de protection des informations. L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau .Les outils classiques offrant des solutions de sécurité minimum (authentification par login et mot de passe, installation d'un anti-virus, etc.) se révèlent utiles mais dans la plupart des cas, insuffisantes.

Problématique

Aucune personne n'ignore l'importance de l'information dans une institution qui nécessite l'organisation, la fiabilité et le bon fonctionnement du système d'information.

La nouvelle technologie de l'information et de la communication (NTIC) nous introduit dans un siècle de vitesse en nous offrant de nouvelles perspectives en ce qui concerne la communication de l'information au sein de nos organisations.

Voilà la question que nous avons retenu et qui traduisent et reflètent nos préoccupations : Comment garantir la confidentialité , la sécurité et l'intégrité des données ?

Hypothèse du sujet

Nous essayons dans la mesure du possible d'envisager une politique optimale de partage des informations afin que l'échange des ressources ne pose plus de problème au sein de l'entreprise.

Dans le cadre de notre travail, nous avons jugé bon de joindre au système d'information existant au sein de l'entreprise des dispositifs VPNs.

En vue de remédier toujours aux inquiétudes soulevées au travers de la question Posée dessus, nous pensons :

- Qu'il existe un moyen de permettre la connexion sécurisée des ordinateurs distants au travers d'une liaison non fiable (internet) : Le VPN.
- Qu'une configuration appropriée existe et le logiciel GNS3 serait le mieux adapté pour cela. Vu l'objectif de l'entreprise, nous avons jugé bon de porter notre choix sur ce sujet qui s'intitule : " Solution de sécurité pour le LAN étendu de la BNA" dans une entreprise afin de lui faire profiter de nos connaissances acquises durant notre parcours d'études.

Et Vu la grandeur du sujet que nous allons aborder, notre travail sera subdivisé en deux grandes parties et chaque partie sera suivie de chapitres que nous développerons dans les lignes ci-dessous. La première partie, est la présentation des aspects théoriques qui comporte deux chapitres : Le premier est consacré aux généralités sur les réseaux informatiques et le deuxième à la généralité et sécurité des VPNs. La deuxième partie, comporte la présentation de l'organisme d'accueil (BNA), ainsi qu'un chapitre consacré à la mise en œuvre des VPNs.

Chapitre 1

Généralités sur les réseaux informatiques

1.1 Introduction

Les réseaux sont nés du besoin d'échanger des informations de manière simple et rapide entre des machines. En d'autres termes, les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux, et enfin des machines terminales, telles que les stations à leur serveur.
Dans un premier temps, ces communications étaient uniquement destinées au transfert des données informatiques, mais aujourd'hui avec l'intégration de la voix et de la vidéo, elle ne se limitent plus aux données mêmes si cela ne va pas sans difficulté.
Avant de nous attaquer aux infrastructures réseaux, reprenons quelques notions théoriques de base sur les réseaux informatiques en général, au cours de ce chapitre.
Un réseau permet de partager des ressources entre des ordinateurs : données ou périphériques (Imprimantes, connexion internet, sauvegarde sur bandes, scanner, etc.).

1.2 Le réseau informatique et son intérêt

1.2.1 Le réseau informatique

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies. Dans le cas où les objets sont des ordinateurs on parle d'un réseau informatique. [18] Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types, d'ordinateurs que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (banques, gestion, commerce, bases de données, recherche,...) et des particuliers (messagerie, loisirs, services d'informations par minitel et Internet ...

1.2.2 intérêts d'un réseau

Un ordinateur est une machine permettant de manipuler des données. L'homme, un être de communication a vite compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations. Voici un certain nombre de raisons pour lesquelles un réseau est utile, un réseau permet :

- Le partage de fichiers, d'applications et de ressources.
- La communication entre personnes (grâce au courrier électronique, la discussion en direct, ...).
- La communication entre processus (entre des machines industrielles).
- La garantie de l'unicité de l'information (bases de données).
- Le jeu à plusieurs, etc.
- Le transfert de la parole, de la vidéo et des données (réseaux à intégration de services ou multimédia).[11]

1.3 Type des réseaux

On peut distinguer différent types de réseaux selon plusieurs critère tel que (la taille de réseau, sa vitesse de transfert des données ainsi que leurs étendues) :

a) **LAN (Local Area Network en français Réseau Local)** : Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre

eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).[11]

b) **Les MAN (Métropolitain Area Network)** : Interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local. Un MAN est formée de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).[11]

c) **Les WAN (Wide Area Network ou réseau étendu)** : Interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.[11]

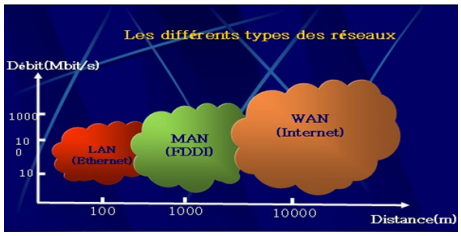

FIGURE 1.1 – les différents types des réseaux

1.4 LAN

1.4.1 Les catégorie des réseaux

On distingue également deux catégories de réseaux :

$\frac{3}{4}$ Réseaux poste à poste (peer to peer= P2P).

$\frac{3}{4}$ Réseaux avec serveur dédié (Server/client).

a) **Le réseau (peer to peer ou pair à pair)** Chaque poste ou station fait office de serveur et les données ne sont pas centralisées, l'avantage majeur d'une telle installation est son faible coût en matériel (les postes de travail et une carte réseau par poste). En revanche, si le réseau commence à comporter plusieurs machines (>10 postes) il devient impossible à gérer. [21]

Par exemple : Si on a 4 postes et 10 utilisateurs, chaque poste doit contenir les 10 mots de passe afin que les utilisateurs puissent travailler sur n'importe lequel des postes. Mais si maintenant il y a 60 postes et 300 utilisateurs, la gestion des mots de passe devient périlleuse.

1.4.2 Le réseau Server/Client

Il ressemble un peu au réseau poste à poste mais cette fois-ci, on y rajoute un poste plus puissant, dédié à des tâches bien précises. Cette nouvelle station s'appelle serveur. Le serveur Centralise les données relatives au bon fonctionnement du réseau. Dans l'exemple précédant, C'est lui qui contient tous les mots de passe. Ainsi ils ne se trouvent plus qu'à un seul endroit. Il est donc plus facile pour l'administrateur du réseau de les modifier ou d'en créer d'autres.
L'avantage de ce type de réseau est sa facilité de gestion des réseaux comportant beaucoup de postes. Son inconvénient majeur est son coût souvent très élevé en matériel.
En effet, en plus des postes de travail il faut se procurer un serveur qui coûte cher car c'est une machine très puissante et perfectionnée. De plus la carte réseau que l'on y met est de meilleure qualité que Celle des postes de travail. [21]

1.5 Les Topologie des réseaux

1.5.1 Les topologies physiques simples

Une topologie physique correspond à la disposition physique d'un réseau, mais ne spécifie pas le type de périphérique, les méthodes de connectivité ou les adresses d'un réseau. Les topologies physique sont disposées selon trois principaux groupe de formes géométrique :le bus,l'anneau et l'étoile.

- **La topologie en Bus**
  Dans cette topologie un même câble relie tous les nœuds d'un réseau sans périphérique de connectivité intermédiaire .les deux extrémités des réseaux en bus sont équipées de résistances de 50 ohms (terminateurs) qui arrêtent les signaux une fois arrivés a la destination .les signaux d'un réseau en bus continueraient à circuler sans fin ; ce qu'on appelle le rebond de signal.
- **La topologie en étoile**
  Dans cette topologie, chaque nœud du réseau est relié à un périphérique cen-

FIGURE 1.2 – Topologie en bus.

tral, tel qu'un concentrateur (hub). Un même câble de réseau en étoile ne peut relier que deux périphérique, donc un problème de câblage ne touchera jamais plus de deux nœuds .les nœuds transmettent des données au concentrateur, qui a son tour retransmet les informations au segment de réseau ou le nœud de destination pourra les ramasser.

FIGURE 1.3 – Topologie en étoile.

- **La topologie en anneau**
  Dans une topologie en anneau, chaque nœud est relié aux deux nœud les proches, et l'ensemble du réseau forme un cercle les données sont transmises autour de l'anneau dans une seul direction chaque station de travail accepte et répond aux paquets qui lui sont adressés, puis les fait suivre à la prochaine station de l'anneau.[11]

FIGURE 1.4 – Topologie en anneau.

1.5.2 Les topologies logiques

Le terme topologie logique désigne la façon par laquelle les données transmises entre les nœuds, plutôt que la disposition des voies ou chemins qu'empruntent les données. Une topologie logique s'appelle aussi un système de transport réseau .la topologie logique d'un réseau décrit la manière par laquelle les données sont mises en trames et comment les impulsions électrique sont envoyées sur le support physique du réseau les éléments d'une topologie logique appartiennent à la fois aux couche liaison du modèle OSI. Chaque topologie logique possède son propre ensemble de principe de signalisation de données, mais impose aussi des exigences particulières au niveau du média de transmission et de la topologie physique Ethernet et Token Ring sont les deux systèmes de transport réseau (topologie logique) les plus courants .mais il y a également d'autre topologie logique tel que FDDI et LocalTk. . .etc. [8]

1.6 Les architecture des réseaux

1.6.1 Le modèle de référence OSI

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocole privés et il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux si une norme internationale n'était pas établie. Cette norme établie par l'internationale standard organisation (ISO) est la norme open system interconnexion (OSI, interconnexion de systèmes ouverts).
Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des informations avec d'autres équipement hétérogènes et issus de constructeurs différents.
Le premier objectif de la norme OSI a été de définir un modèle de toute architecture de réseau base sur découpage en sept couches chacun de ces couches correspondant à une fonctionnalité particulière d'un réseau.
Les couches 1, 2, 3,et 4 sont dites basses et les couches 5,6 et 7 sont dites hautes.[21]

- **La couche physique**
  Cette couche définit les caractéristiques techniques, électriques, fonctionnelles et procédure les nécessaires à l'activation et à la désactivation des connexions physiques destinées à la transmission de bits entres deux entités de la couche liaisons de données.
- **La couche liaison**
  Cette couche définit les moyens fonctionnels et procéduraux nécessaires à

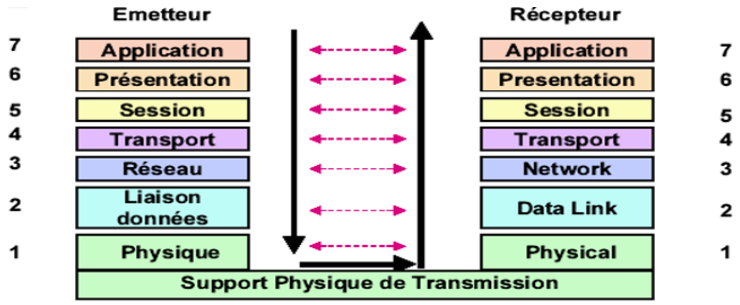

FIGURE 1.5 – Le model OSI.

l'activation et à l'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de donnes entre les entités du réseau. Cette couche détecte et corrige, quand cela est possible,les erreurs de la couche physique et signalé à la couche réseau les erreurs irrécupérables.

- **La couche réseau**
  Cette couche assure toutes les fonctionnalités de services entre les entités du réseau, c'est à dire : l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche liaison pour préparer le travail de la couche transport.
- **La couche transport**
  Cette couche définit un transfert de données entre les entités en les déchargeant des détails d'exécution (contrôle entre l'OSI et le support de transmission). Son rôle est d'optimiser l'utilisation des services de réseau disponibles afin d'assurer à moindre coût les performances requise par la couche session.
- **La couche session**
  Cette couche fournit aux entités de la couche présentation les moyens d'organiser et de synchroniser les dialogues et les échanges de données.
  Il s'agit de la gestion d'accès, de sécurité et d'identification des services.
- **La couche présentation**
  Cette couche assure la transparence du format des données à la couche application.
- **La couche application**
  Cette couche assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tous les services directement utilisables par l'application (transfert de données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications). [21]

1.6.2 Le modèle TCP/IP

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches :

Le modèle OSI a été mis à côté pour faciliter la comparaison entre les deux modèles. Il y a 4 couches principales dans l'environnement TCP/IP :

- **La couche application** : Les applications interagissent avec les protocoles de la couche transport pour envoyer ou recevoir des données.
- **La couche transport** : Cette couche est chargé de fournir un moyen de communication de bout en bout entre 2 programmes d'application. Agi en mode connecté et en mode non connecté. Elle divise le flux de données venant des applications en paquets, transmis avec l'adresse destination IP au niveau IP.

FIGURE 1.6 – La couche transport.

- **La couche internet** : Encapsule les paquets reçus de la couche Transport dans des datagrammes IP. Mode non connecté et non fiable.
- **La couche hôte réseau** : Assure la transmission d'un datagramme venant de la couche IP en l'encapsulant dans une trame physique et en transmettant cette dernière sur un réseau physique. [8]

1.7 Les équipements réseaux

L'interconnexion de réseaux peut être locale : les réseaux sont sur le même site géographique. Dans ce cas, un équipement standard (Répéteur, routeur, etc.) fait à réaliser physiquement la liaison.
L'interconnexion peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces réseaux par une liaison téléphonique (modems, etc.).

a) **Le multiplexeur** : Les formes de transmission qui permet à plusieurs signaux de voyager simultanément sur un même media s'appelle transmission multiplex ou multiplexage. Pour accommoder plusieurs signaux sur le même support est logiquement séparé en plusieurs canaux donc un multiplexeur sert à transiter sur une seule et même ligne de liaison, dite voie haute vitesse,

des communications appartenant à plusieurs paires d'équipements émetteurs et récepteurs. Chaque émetteur (respectivement récepteur) est raccordé à un multiplexeur (respectivement démultiplexeur) par une liaison dite voie basse vitesse. Plusieurs techniques de multiplexage sont possibles. [18],[6]

FIGURE 1.7 – Multiplexeur.

b) **Multiplexage temporel** : ensemble de voies "basses vitesses" (VBi).Débit utile inférieur au débit théorique de la ligne de transmission (divisé par le nombre de transmission en parallèle), cas des voies muettes.

c) **Multiplexage statistique** : optimisation multiplexage temporel utilise un codage spécial type Huffman en vue d'améliorer la transmission, notamment prise en charge des voies muettes.

d) **Multiplexage fréquentiel** : partage de la bande passante disponible sur un système de transmission en canaux.

e) **Le concentrateur (hub)** : servent à relier entre elles toutes les parties d'un même réseau physique, généralement tous les ordinateurs sont reliés à un Hub, sauf dans le cas d'un câblage coaxial où le Hub est inutile. Lorsqu'une information arrive sur un Hub,elle est rediffusée vers toutes les destinations possibles à partir de celui-ci, c'est à dire vers toutes ses prises [11],[6].

f) **Le commutateur (Switches)** : le commutateur (ou Switch) est un système assurant l'interconnexion de stations ou de segments d'un LAN en leur attribuant l'intégralité de la bande passante, à l'inverse du concentrateur qui la partage.
Les commutateurs ont donc été introduits pour augmenter la bande passante globale d'un réseau d'entreprise et sont une évolution des concentrateurs Ethernet (ou HUB) [8].

g) **Le pont (Bridges)** : Ils servent à relier entre eux deux réseaux différents d'un point de vue physique. De plus ils filtrent les informations et ne laissent passer que celles qui doivent effectivement aller d'un réseau vers l'autre. Ils peuvent être utilisés pour augmenter les distances de câblage en cas d'affaiblissement prématuré du signal [11],[6].

h) **Le routeur (routers)** : ils relient des réseaux physiques et/ou logiques différents, généralement distants. Comme les ponts filtrent les informations mais à un niveau beaucoup plus fin (le niveau logique), et l'on peut même s'en servir pour protéger un réseau de l'extérieur tout en laissant des réseaux "amis" accéder au réseau local [11],[6].

FIGURE 1.8 – Routeur.

i) **Le répéteur (repeater)** : sont des dispositifs permettant d'étendre la distance de câblage d'un réseau local. Leurs rôle consiste à amplifier et à répéter les signaux qui leurs parviennent. Il existe également des répéteurs qui en plus régénèrent les signaux. Ceci réduit le bruit et la distorsion. Le répéteur intervient au niveau 1 du modèle OSI. [11]

j) **Les passerelles (gateway)** : sont des dispositifs permettant d'interconnecter des architectures de réseaux différentes. elles offrent donc la conversion de tous les protocoles, au travers des 7 couches du modèle OSI.
L'objectif étant de disposer d'une architecture de réseau évolutive, la tendance actuelle est d'interconnecter les réseaux par des routeurs, d'autant plus que le prix de ceux-ci est en baisse [21],[6].

FIGURE 1.9 – Passerelle.

k) **Modem (modulateur démodulateur)** : le modem est un périphérique qui permet de transmettre et de recevoir les données numériques en signaux ana-

logiques et inversement pouvons être acheminés par une ligne téléphonique.Il existe trois types de modems :

1. **Modem intégré** : est un périphérique soudé à la carte mère.
2. **Modem interne** : il s'installe dans un connecteur d'extension de la carte mère (dans l'unité centrale).
3. **Modem externe** : se présente sous la forme d'un petit boitier, il suffit de le relier à l'ordinateur par l'intermédiaire du port série ou port USB [21],[6].

FIGURE 1.10 – Modem.

1.8 Supports de transmission

On distingue trois types de câbles :

- **Le câble coaxial (10 base 2)** : est le câble le plus ancien, il est illustré dans la figure suivante :

FIGURE 1.11 – Cable coaxial.

- **Connecteur du câble coaxial** :
  1. Connecteur BNC en T : relie la carte réseau et le câble
  2. Prolongateur BNC : relie deux segments de câble coaxial afin d'obtenir un câble plus long ;

3. Bouchon de terminaison BNC : il est placé à chaque extrémité du câble d'un réseau en bus pour absorber les signaux parasites, il est relié a la masse (le bouchon est absolument nécessaire pour le fonctionnement d'une installation de type bus).

- **Câblage à paire torsadée** : dans sa forme la plus simple, le câble à paire torsadée (en anglais Twisted-pair cable) est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolants. On distingue généralement deux types de paires torsadées :
  a. Les paires blindées (STP : Shielded Twisted-Pair) ;
  b. Les paires non blindées (UTP : Unshielded Twisted-Pair).

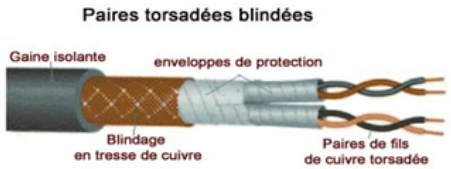

FIGURE 1.12 – Cable a paire torsadée.

Un câble est souvent fabriqué à partir de plusieurs paires torsadées regroupées et placées à l'intérieur de la gaine protectrice. L'entrelacement permet de supprimer les bruits (interférences électriques) dus aux paires adjacentes ou autres sources (moteurs, relais, transformateur).
La paire torsadée est donc adaptée à la mise en réseau local d'un faible parc avec un budget limité, et une connectique simple. Toutefois, sur de longues distances avec des débits élevés elle ne permet pas de garantir l'intégrité des données (c'est-à-dire la transmission sans perte de données).

- **La paire torsadée non blindée (UTP)** : le câble UTP obéit à la spécification (10 Base T). C'est le type de pair torsadée le plus utilisé et le plus répandu pour les réseaux locaux, il peut transmettre un signal d'information sur un segment de 100 mètres au maximum.

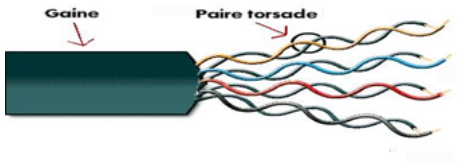

FIGURE 1.13 – La paire torsadée non blindée.

- **Normes UTP** : conditionnent le nombre de torsions par pied (33 cm) de câble en fonction de l'utilisation prévue.
  UTP : répertorié dans la norme Commercial Building Wiring Standard 568 de l'EIA/TIA (Electronic Industries Association / Telecommunication Industries Association). La norme EIA/TIA 568 a utilisé UTP pour créer des normes applicables à toutes sortes de locaux et de contextes de câblage qui garantissent au public l'homogénéité des produits. Ces normes incluent cinq catégories de câbles UTP :

  ✓ **Catégorie 1** : câble téléphonique traditionnel (transfert de voix mais pas de données).
  ✓ **Catégorie 2** : transmission des données à 4 Mbit/s maximum (RNIS). Ce type de câble est composé de 4 paires torsadées.
  ✓ **Catégorie 3** : 10 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées et de 3 torsions par pied.
  ✓ **Catégorie 4** : 16 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées en cuivre.
  ✓ **Catégorie 5** : 100 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées en cuivre.
  ✓ **Catégorie 5e** : 1000 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées en cuivre.
- **La paire torsadée blindée (STP)** : le câble STP (Shielded Twisted Pair) utilise une gaine de cuivre de meilleure qualité et plus protectrice que la gaine utilisée par le câble UTP. Il contient une enveloppe de protection entre les paires et autour des paires. Dans le câble STP, les fils de cuivre d'une paire sont eux-mêmes torsadés, ce qui fournit au câble STP un excellent blindage, c'est-à-dire une meilleure protection contre les interférences). D'autre part il permet une transmission plus rapide et sur une plus longue distance.

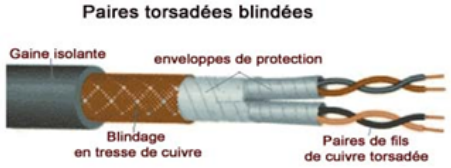

FIGURE 1.14 – La paire torsadée blindée.

- **Connecteurs pour paire torsadée** : la paire torsadée se branche à l'aide d'un connecteur RJ45. Ce connecteur est similaire au RJ-11 utilisé dans la

téléphonie mais différent sur certains points : le RJ-45 est légèrement plus grand et ne peut être inséré dans une prise de téléphone RJ-11. De plus, le RJ-45 se compose de huit broches alors que le RJ-11 n'en possède que six, voire quatre généralement.

- **Fibre optique** : est un câble possédant de nombreux avantages :
  - Légèreté.
  - Immunité au bruit.
  - Faible atténuation.
  - Tolère des débits de l'ordre de 100 Mbps.
  - Largeur de bande de quelques dizaines de mégahertz à plusieurs gigahertz (fibre monomode)

Le câblage optique est particulièrement adapté à la liaison entre répartiteurs (liaison centrale entre plusieurs bâtiments, appelé backbone, ou en français épine dorsale) car elle permet des connexions sur des longues distances (de quelques kilomètres à 60 km dans le cas de fibre monomode) sans nécessiter de mise à la masse. De plus ce type de câble est très sûr car il est extrêmement difficile de mettre un tel câble sur écoute.
Toutefois, malgré sa flexibilité mécanique, ce type de câble ne convient pas pour des connexions dans un réseau local car son installation est problématique et son coût élevé. C'est la raison pour laquelle on lui préférera la paire torsadée ou le câble coaxial pour de petites liaisons [21],[6].

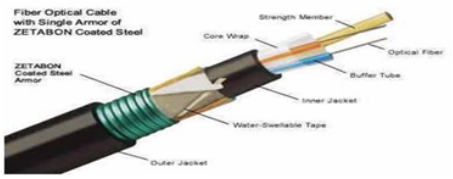

FIGURE 1.15 – Fibre optique.

1.9 Conclusion

Au cours de ce chapitre, nous avons parcouru les différentes architectures protocolaires, les types des réseaux, ainsi les topologies logiques et les topologies physiques les plus répandus.

Suite à cela, on a pu avoir une vision plus élargie sur ces différents domaines ce qui nous permettra de mieux élaborer le reste de notre projet.

Chapitre 2

sécurité et géneralités sur les VPNs

Partie I :La sécurité des VPNs

2.1 Introduction

La sécurité informatique est le domaine de l'informatique qui analyse les propriétés de sécurité des systèmes informatiques. Elle a pour but la protection des ressources matérielles et logicielles (incluant les données et les programmes) d'un système informatique contre la révélation, la modification, ou la déstruction accidentelle ou malintentionnée.
Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles portant sur celui-ci, et donc de connaître et de prévoir la façon de procéder de ces menaces et ensuite la mise en oeuvre des mécanismes de sécurité qui permettent de minimiser la vulnérabilité d'un système informatique contre ces menaces [22].

2.2 Quelques définitions

2.2.1 Les enjeux de la sécurité des réseaux informatiques :

La sécurité d'un réseau informatique, d'une manière générale, vise les objectifs suivants :
– La confidentialité : La protection de données émises sur le réseau,

de façon à ce qu'elles ne soient compréhensibles que par des entités autorisées.
- **L'authentification : La garantie que les données reçues proviennent bien de l'entité émettrice.**
- **L'intégrité : La garantie que les données reçues n'ont subi aucune modification lors du transport dans le réseau.**
- **La non-répudiation : Constitue un moyen efficace pour identifier l'auteur d'une transaction et d'assurer la preuve de l'authenticité de cette dernière.**

2.2.2 Les attaques intentionnelles

C'est l'ensemble des actions malveillantes qui constituent la plus grosse partie du risque.
Elles font principalement l'objet de mesures de protection. Parmi elles, on compte les menaces passives et les menaces actives.

2.2.3 Les attaques passives

Méthode se basant sur l'écoute du réseau à l'aide de sniffeurs : (analyseurs du trafic réseau), elle consiste au détournement des données et des logiciels sans modifier le fonctionnement du réseau.
On cite : Espionnage industriel et commercial, copies illicites de logiciels.

2.2.4 Les attaques actives

elles consistent à modifier des données, à se glisser dans des équipements réseaux ou à perturber le bon fonctionnement de ce réseau.
On cite : Modification et sabotage des informations (ex : fraude financière informatique), modifications des logiciels (ex : virus).

2.2.5 La cryptographie

La cryptographie est l'étude de méthodes de chiffrement et de déchiffrement. Elle permet d'assurer l'authenticité, l'intégrité et la confidentialité des données.

- **La cryptographie symétrique** Elle est basée sur une clé unique partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages.
- **La cryptographie asymétrique (à clé publique)** Contrairement à la cryptographie symétrique, la cryptographie asymétrique utilise deux clés : une est privée et n'est connue que par l'utilisateur, l'autre est publique et donc accessible par tout le monde.

2.2.6 Menace

La menace (en anglais « threat ») représente le type d'action susceptible de nuire dans l'absolu. Les menaces sont caractérisées par les possibilités et les probabilités d'attaque contre la sécurité. Elles engendrent des risques et des coûts humains et financier :

perte de confidentialité de données sensibles, indisponibilité des infrastructures et des données, etc. Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités.[26],[27].

2.2.7 Vulnérabilité

La vulnérabilité (en anglais « vulnerability », appelée parfois faille ou brèche) est une faute de conception ou de configuration du système informatique, intentionnelle ou accidentelle, qui favorise la réalisation d'une menace ou la réussite d'une attaque [17].

2.2.8 Attaque

Une attaque est une action visant à violer une ou plusieurs propriétés de sécurité des systèmes informatiques. C'est l'exploitation d'une faille d'un système informatique (système d'exploitation, réseau, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables [17].

2.2.9 Intrusion

Une intrusion est définie comme une faute malveillante interne d'origine externe, résultant d'une attaque qui a réussi à exploiter une vulnérabilité. Elle est susceptible de produire des erreurs pouvant provoquer une défaillance vis-à-vis de la sécurité, c'est-à-dire une violation de la politique de sécurité du système.
Le terme d'intrusion sera employé dans le cas où l'attaque est menée avec succès et où l'attaquant a réussi à introduire et/ou compromettre le système [16].

2.2.10 Contre-mesure

La contre-mesure est l'ensemble des actions mises en oeuvre en prévention de la menace [16].

2.2.11 Risque

Les risques sont le résultat de la combinaison des menaces et des vulnérabilités. Ils doivent être évalués, soit pour obtenir le meilleur compromis possible entre sécurité et coût pour un système donné, soit simplement pour calculer le montant des primes d'assurance pour couvrir ces risques.
Le risque en termes de sécurité est généralement caractérisé par l'équation suivante.[26],[6]

2.2.12 Les mécanismes de défense et de sécurité

Un mécanisme est un moyen pour la mise en oeuvre de la politique. La sécurité ne doit jamais reposer sur un seul mécanisme de sécurité. Une imbrication de mécanismes offre une garantie de sécurité bien supérieure.

- **Les défenses logicielles**
- **Les défenses Matérielles**

2.3 Techniques de sécurité dans un réseau local

2.3.1 Pare-feu et DMZ

2.3.1.1 Pare-feu

Définition :un firewall (ou par-feu) est un outil informatique (materiel et /ou logiciel) concu pour protéger les données d'un réseau (protection d'un ordinateur personnel relie a Intenet par exemple, ou protection d'un réseau d'entreprise). Il permet d'assurer la sécurité dans des informtions d'un réseau en filtrant les entrées et en controlant les sorties selon des regles définies par son administrateur [1].

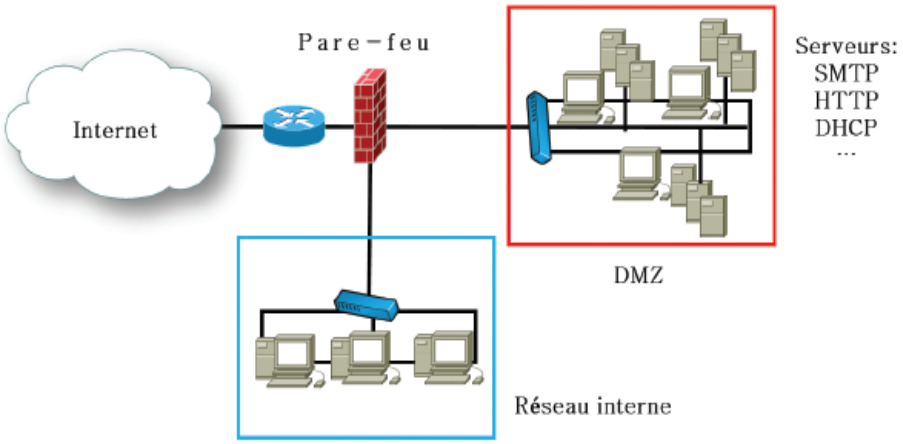

FIGURE 2.1 – Emplacement d'un pare-feu.

2.3.1.2 Obgectif du firewall

Les firewalls ont obtenu une grande renommee en matiére de sécurité internet.ils ont deux principaux objectifs.[2] [23].

- **Protéger le réseau interne contre les tentatives d'intrusion provenant de l'exterieur.**
- **Limiter et vérifier les connexions provenant du réseau interne vers l'extrerieur .[14]**

2.3.1.3 Fonctionnement du firewall

Le fonctionnement d'un parfeu repose sur un ensemble de regles prédéfinies permettant

- **D'autoriser la connexion (allow).**
- **De bloquer la connexion(deny).**

2.3.1.4 Principale difference entre un FW et un routeur IP

Le routeur prend en charge les paquets jusqu'à la couche IP.le routeur transmet chaque paquet en fonction de l'adresse de destination du paquet et la route vers la destination precisee dans la table de routage.par contre le firewall ne transmet pas les paquets.le pare-feu accepte les paquets et les prend en charge jusqu'à la couche application.

2.3.1.5 Types de firewall

- **Pare-feu : Il existe 3 types de filtrages.**
  - **le filtrage simple de paquet qui travaille au niveau de la couche 3 du model OSI.le pare-feu Analyse les en-têtes de chaque parquet de données échangé entre une machine interne et externe Afin d'étudier les adresses IP éméttrice et réceptrice ,les types de paquets et les numéros de prot.**

  - **le filtrage dynamique travaille au niveau des couches 3 et 4 du modele OSI.**
    Le par-feu peut ainsi prévoir les ports a autoriser ou a interdire.

  - **le filtrage applicatif permet de filtrer les communications application par application au niveau de la couche 7 du modèle OSI.ce type de filtrage impose la connaissance des protocoles utilises par. chaque application[12].**
- **Proxy**
  - **Un proxy est un serveur qui fait la fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet.le proxy est un serveur mandate par une application pour éffectuer une requête sur internet a sa place .**

- **Le proxy assure une fonction de caches,les pages les plus souvent visitées sont stockées sur le serveur.**
- **Il peut également assurer un suivi des connexions (logs utilisateurs) et filtrer les connexions a internet en analysant les requêtes des clients et les réponses des serveurs pour les comparer A la lsite blanche (liste de requête autorisées) ou a la liste noire (liste de requêtes interdites).**
- **Il peut aussi assurer l'authentification des utilisateurs gérer l'acces aux ressources extrenes.**

2.3.1.6 DMZ (Delimitarised Zone)

Definition de DMZ **Une DMZ(en anglais :De-Militarized zone),est une partie du reseau local dont l'objectif est d'être accessible depuis l'exterieur du réseau local,avec ou sans authentification préalable. En effet,pour des raisons a la fois techniques et strategique,les réseaux IP locaux(LANs) Sont (paradoxalement) devenus des zones inaccessibles depuis internet.[7],[6]**

2.3.1.7 Serveur installes sur la DMZ

Le DMZ permet de fournir des services au réseau externe,tout en protegeant le réseau interne contre des intrusions possibles sur ces serveurs :

- **les serveurs Web (http),**
- **les serveurs de fichiers (ftp),**
- **Les serveurs d'e-mails (SMTP),**
- **Les serveurs de noms (DNS).**

2.3.2 VLAN (Virtual Local Area Network)

Les réseaux virtuels (Virtual LAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs. Le VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusion restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les

stations de ce même VLAN. Un VLAN est donc, un regroupement logique et non physique de plusieurs stations.

Partie II : géneralités sur les VPNs

2.4 Introduction

c'est une technique permettant d'interconnecter des entités distantes, qui relient un réseau ou un poste de travail avec un autre réseau.
Les VPN sont privés d'accès, seul un groupe limité d'entités peuvent y accéder. Ils sont virtuels dans le sens où ils s'appuient sur des architectures de réseaux partagées et partitionnement logique de ses ressources sans s'appuyer sur des connexions physiques dédiées.
Les VPN reposent sur un protocole appelé " tunneling ". Ce principe consiste à fournir un chemin (tunnel) sécurisé de bout en bout, entre un client et un serveur. Les VPNs permettent, entre autre, d'identifier et d'autoriser l'accès ainsi que de chiffrer tout trafic circulant dans le réseau.
L'utilisation d'un VPN, est la manière la plus fiable de sécuriser un réseau. C'est aussi la méthode la plus utilisée.
Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet.

2.4.1 Principe de fonctionnement d'un VPN

Un réseau VPN repose sur un protocole appelé " protocole de tunneling ", ce protocole permet de faire circuler les informations échangées de bout a un autre bout du tunnel d'une façon crypté (chiffrement des données et encapsulation des entêtes), ainsi les utilisateurs ont l'impression de se connecter directement sur le réseau de leurs entreprise. Les données transmises avec un tunnel VPN seront sécurisées .

2.4.2 Les avantages et inconvénients des VPNs d'entreprise

- **Avantages[15] [9].**

  les principaux avantages des VPNs d'entreprise sont :
  - **Pas de contrat de négociation,Pas de frais mensuels autre que ceux de l'abonnement internet servant de support a ces VPNs,**
  - **Une Independence quasi-totale vis-à-vis des opérateurs, ce qui fait que la solution peut être bâtie avec operateurs différents selon des sites et leurs éligibilités,**
  - **Le déplacement des tunnels, le chargement des périmètres et le contrôle du trafic circulant s'effectuent avec une grande souplesse,**
  - **Maitrise des protocoles de sécurité,**
  - **Possibilité notamment pour de nomades d'associer de l'authentification forte facilement, avec une conversation de toute latitude dans le choix de la solution,**
  - **Capacité de mis en place d'un VPN par un faible usage (par exemple : connexion occasionnelle d'un prestataire) sans que cela n'augmente le montant de mensuel du budget télécom.**
- **Inconvénients et limites il est évident que les VPN d'entreprise représente quelque inconvénients et limites que l'on cite dans ce qui suit [15],[9].**
  - **Adresses IP fixes recommandées au moins pour les sites principaux.**
  - **Nécessité d'avoir une personne compétente dans le réseau interne,**
  - **Pas de garantie de temps de rétablissement en cas de défaillance,**
  - **Pas de garantie de performance,car les VPNs ont comme support un lien internet.**

2.4.3 Types des VPNs

Selon le mode d'utilisation, on distingue trois types d'architecture VPN :[25]

- **Le VPN d'accès.**
- **L'intranet VPN.**
- **L'extranet VPN.**

2.4.3.1 VPN d'accès (host to LAN)

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur distant se sert d'une connexion Internet pour établir la connexion VPN, il sera connecté logiquement au réseau LAN de l'entreprise comme s'il l'était physiquement.

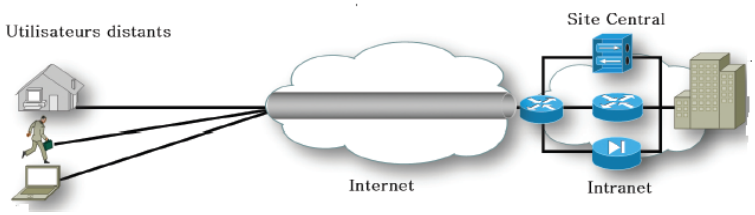

FIGURE 2.2 – VPN poste à site.

2.4.3.2 Intranet VPN (LAN to LAN)

L'intranet VPN est utilisé pour relier deux ou plusieurs intranets d'une même Entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants...).

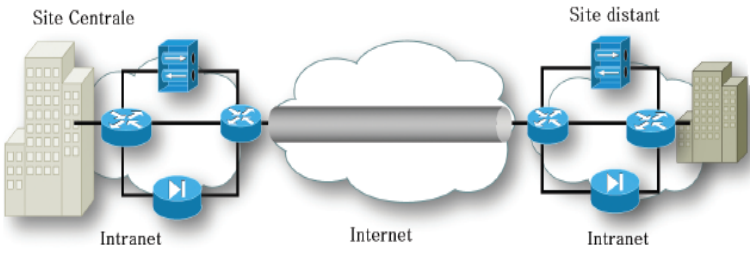

FIGURE 2.3 – VPN site à site.

2.4.3.3 Extranet VPN (host to host)

C'est le cas d'utilisation le plus simple. Il s'agit de mettre en relation deux serveurs. Le cas d'utilisation peut être le besoin de synchronisation de bases de données entre deux serveurs d'une entreprise disposant de chaque coté d'un accès Internet. L'accès réseau complet n'est pas indispensable dans ce genre de situation. Une entreprise peut utiliser le VPN

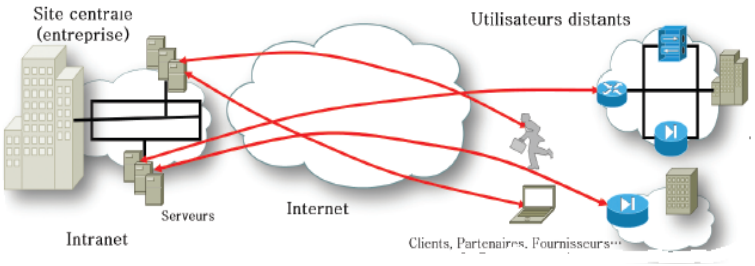

FIGURE 2.4 – VPN poste à poste.

pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.

2.5 protocoles utilisés pour réaliser une connexion VPN

Les protocoles permettant un tunneling sécurisé se classent en deux catégories[24].

- **Les protocoles de niveau 2 comme PPTP (soutenu par Microsoft), L2F (développé par Cisco) et L2TP (évolution reprenant les avantages des 2 précédents), tous étant dépendants de PPP.**
- **Les protocoles de niveau 3 comme IPSec.**
- **À ces deux catégories peut s'ajouter le protocole SSL, de niveau 4, dans le cadre de VPN-SSL.**

2.5.1 Le protocole PPP

PPP (Point to Point Protocol) est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule les paquets IP dans des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau. Le protocole PPP est défini dans la RFC 2153.
PPP n'est pas un protocole permettant l'établissement d'un VPN mais il est principalement utilisé pour transférer les informations au travers d'un VPN, et sert comme support aux protocoles PPTP ou L2TP.[24]

2.5.2 Le protocole PPTP

Point to Point Tunneling Protocol est défini par la RFC 2637. Microsoft a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de Windows. PPTP est ainsi une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet l'encapsulation des données ainsi que leur compression. L'authentification se fait grâce au protocole Ms-Chap2 (Challenge Handshake Authentification Protocol v.2, RFC 2759) de Microsoft. Le cryptage s'effectue grâce au protocole MPPE (Microsoft Point-to-Point Encryption). Le protocole PPTP encapsule les trames PPP dans des datagrammes IP pour leur transmission sur le réseau. Il utilise une connexion TCP pour la gestion de tunnel et une version modifiée de GRE (Generic Routing Encapsulation, RFC 2784) pour encapsuler les trames PPP pour les données tunnelées. Les charges utilese des trames PPP encapsulées peuvent être chiffrées, compressées ou les deux en même temps.
La figure suivante illustre la structure d'un paquet PPTP contenant un datagramme IP.[24]

2.5.3 Le protocole L2F

Layer Two Forwarding est un protocole de niveau 2 qui permet à un serveur d'accès distant de véhiculer le trafic sur PPP et transférer ces

données jusqu'à un serveur L2F (routeur). Ce serveur L2F désencapsule les paquets et les envoie sur le réseau. Il faut noter que contrairement à PPTP et L2PT, L2F n'a pas besoin de client. Ce protocole est progressivement remplacé par L2TP qui est plus souple [24].

2.5.4 Le protocole L2TP

L2TP (Layer Two Tunneling Protocol) est un protocole combinant les avantages du PPTP de Microsoft et du L2F de Cisco, ce protocole est décrit dans la RFC 2661 et a été créé par l'IETF (Internet Egineering Task Force). L2TP est aujourd'hui principalement utilisé par les FAI (Fournisseurs d'Accès à Internet).
Sur la base des spécifications des protocoles L2F et PPTP, Nous pouvons utiliser le protocole L2TP pour configurer des tunnels entre les réseaux concernés. À l'instar de PPTP, L2TP encapsule les trames PPP qui encapsulent ensuite les protocoles IP et permettent aux utilisateurs d'exécuter à distance des programmes qui sont tributaires de protocoles réseau déterminés [20].

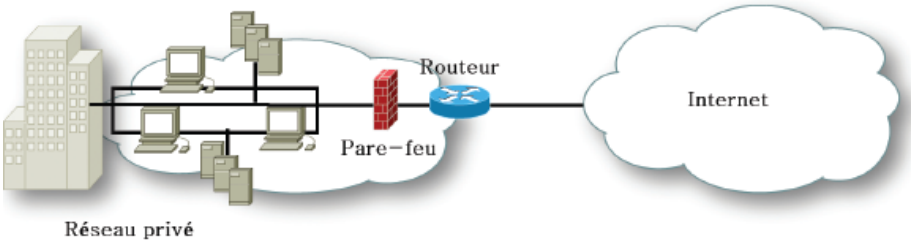

FIGURE 2.5 – Principe de fonctionnement d'IPSec.

2.5.5 Le protocole IPSec

IPSec (Internet Protocol Security), définit par la RFC 2411, est un ensemble de protocoles pour sécuriser les communications IP et garantir le chiffrement, l'intégrité et l'authentification. Ce protocole spécifie les messages nécessaires pour sécuriser les communications du réseau privé tout en se basant sur les algorithmes existants[25].
Aujourd'hui, le protocole le plus utilisé pour la mise en place des VPNs

est IPSec. Il est l'un des standards les plus diffusé et le plus ouvert. Effectivement IPSec vise à sécuriser les échanges au niveau de la couche réseau.
Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitent encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6. Ces mécanismes sont couramment désignés par le terme IPSec. Le protocole IPSec fournit ainsi[24].

- **Des mécanismes de confidentialité et de protection contre l'analyse du trafic.**
- **Des mécanismes d'authentification des données.**
- **Des mécanismes garantissants l'intégrité des données.**
- **Des mécanismes de protection contre le rejeu .**
- **Des mécanismes de contrôle d'accès.**

2.5.6 Architecture du protocole IPSec

IPSec repose en fait sur plusieurs protocoles différents dont certains existent à part entière hors d'IPSec qui lui offrent en retour une grande souplesse d'utilisation[19],[20] :
Le protocole initial et principal est le protocole IKE (Internet Key Exchange, RFC 2409). Appliqué à IPSec, ce protocole a pour objectif dans un premier temps d'établir un premier tunnel entre les deux machines (le tunnel IKE), que l'on pourra qualifier de tunnel administratif. C'est la phase 1 du protocole IKE. Ce protocole est dit administratif car il ne sert pas à la transmission des données utilisateur ; il est utilisé pour gérer les tunnels secondaires, leur création, le rafraîchissement des clés, etc... La phase 2 du protocole IKE consiste en effet à établir autant de tunnels secondaires que nécessaire pour la transmission des données utilisateur entre les deux machines. IKE est un protocole hybride qui implémente les échanges de clés dans le cadre ISAKMP (Internet Security Association and Key Management Protocol, RFC 2408).
Les tunnels destinés aux échanges de données vont s'appuyer sur deux protocoles différents suivant les besoins en sécurité des utilisateurs.

- **Le premier est le protocole AH (Authentication Header, RFC 2402) qui vise à établir l'identité des extrémités de façon certaine. Il inclut un hachage du paquet IP et garantit l'intégrité. Bien que le contenu du datagramme ne soit pas chiffré, le destinataire est sûr que le**

contenu du paquet n'a subi aucune modification et que l'expéditeur a envoyé les paquets.
- **Le deuxième protocole est le protocole ESP (Encapsulating Security Payload, RFC 2406) qui chiffre les données IP et obscurcit, par conséquent, le contenu des paquets lors de leur transmission (confidentialité). ESP garantit également l'intégrité des données par le biais d'une option d'algorithme d'authentification.**

2.5.6.1 Les deux modes de fonctionnement d'IPSec

Pour chacun des mécanismes de sécurité d'IPSec, il existe deux modes de fonctionnement : Le mode transport prend un flux de niveau transport (couche de niveau 4 du modèle OSI) et réalise les mécanismes de signature et de chiffrement puis transmet les données à la couche IP. Dans Ce mode, l'insertion de la couche IPSec est transparente entre TCP et IP. TCP envoie ses données vers IPSec comme il les enverrait vers IP. L'inconvénient de ce mode réside dans le fait que l'en-tête extérieur est produit par la couche IP c'est-à-dire sans masquage d'adresse. De plus, le fait de terminer les traitements par la couche IP ne permet pas de garantir la non-utilisation des options IP. L'intérêt de ce mode réside dans une relative facilité de mise en oeuvre.
Dans le mode tunnel, les données envoyées par l'application traversent la pile de protocole jusqu'à la couche IP incluse, puis sont envoyées vers le module IPSec. L'encapsulation IPSec en mode tunnel permet le masquage d'adresses. Le mode tunnel est utilisé entre deux passerelles de sécurité (routeur, firewall, ...) alors que le mode transport se situe entre deux hôtes.

2.5.7 Le protocole SSL

SSL (Secure Socket Layers, RFC 2246) est un procédé de sécurisation des transactions effectuées via Internet. Il repose sur un procédé de cryptographie à clés publique afin de garantir la sécurité de la transmission des données sur Internet. Son principe consiste à établir un canal de transmission sécurisé (chiffré) entre un client et un serveur après une étape d'authentification.
SSL a deux grandes fonctionnalités : l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données du-

rant la connexion. SSL est un protocole de niveau transport, utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

2.5.7.1 Fonctionnement du protocole SSL

Le protocole SSL Handshake débute une communication SSL. Suite à la requête du client, le serveur envoi son certificat ainsi que la liste des algorithmes qu'il souhaite utiliser. Le client commence par vérifier la validité du certificat. Cela se fait à l'aide de la clé publique de l'autorité de certification contenue dans le navigateur du client. Le client vérifie aussi la date de validité du certificat. Si toutes vérifications sont passées, le client génère une clé symétrique et l'envoi au serveur. Ce dernier peut alors envoyer un teste au client, que le client doit signer avec sa clé privée correspondant à son propre certificat.
Ceci est fait de façon à ce que le serveur puisse authentifier le client.
De nombreux paramètres sont échangés durant cette phase : type de clés, valeur de la clé, algorithmes de chiffrement.
La phase suivante consiste en l'échange de données cryptées avec le protocole SSL Record.
Les clés générées avec le protocole Handshake sont utilisées pour garantir l'intégrité et la confidentialité des données échangées. Les différentes phases de protocole sont :

- **Segmentation des paquets en paquets de taille fixe.**
- **Compression (mais peu implémenté dans la réalité).**
- **Ajout du résultat de la fonction de hachage composé de la clé de cryptage, du numéro de message, de la longueur du message et des données.**
- **Chiffrement des paquets et du résultat du hachage à l'aide de la clé symétrique générée lors du Handshak.**
- **Ajout d'un en-tête SSL au paquet.**

2.6 Conclusion

Les réseaux privés virtuels permettent à un utilisateur de relier une source et une destination en utilisant un réseau public (Internet) c'est cette voie par laquelle transitent les informations, que certains tenteront

de violet les secrets de votre entreprise, et facilite le travail d'espionnage puis d'attaques des machines d'un réseau, c'est pour cela un VPN utilise un ensemble de moyens pour protéger les informations, c'est ce que l'on va étudier dans le chapitre suivant.

Chapitre 3

Organisme daccueil

3.1 Introduction

Afin de nous familiariser avec l'environnement de la Banque Nationale d'Algerie nous avons en premier lieu pris connaissance de celle-ci, des différents services qui la constituent, ainsi que les taches associées à chaque service. En second lieu, nous nous sommes intéressées au département informatique afin de comprendre l'architecture réseau requise par l'entreprise et illustrer par la suite les différents équipements qui la constituent sous trois aspects : réseau, système et sécurité.
Ce chapitre est donc, une introduction au réseau et à l'environnement de l'entreprise BNA DRE

3.2 Historique de la BNA

La Banque Nationale d'Algérie (BNA), crée le 13 juin 1966, par l'ordonnance N66-178, Elle était directement placée sous tutelle de l'état a travers le ministre des finances jusqu'au 12 janvier 1988, date a la quelle la BNA devient une entité juridique chargée du statut d'entreprise publique et économique (EPE). Pour avoir l'exclusivité et le monopole du financement du secteur agricole socialiste et traditionnel.
En 1995 elle devient la première Banque qui a bénéficié du statut de la monnaie et du crédit ; aujourd'hui la BNA exerce toutes les activités d'une banque de dépôts, elle assure notamment le service financier des groupements professionnels, des entreprises industrielles. Elle traite toutes les

opérations de banque, de change et de crédit dans le cadre de la législation et de la réglementation des banques.
Notre cas d'étude ce situe à la Direction du Réseau d'Exploitation de Bejaia dans le Service Informatique.

3.3 Presentation de la DRE

La Direction du réseau d'exploitation de Bejaia est située au Boulevard Krim Belkacem Ihaddaden Bejaia.
La DRE Bejaia 191 est l'une des 17 Directions au niveau national, elle a pour mission de mettre en place les instructions et orientations de la Direction Générale et de coordonner, contrôler et d'assister ces agences rattachées.

3.3.1 Organigrame de la DRE

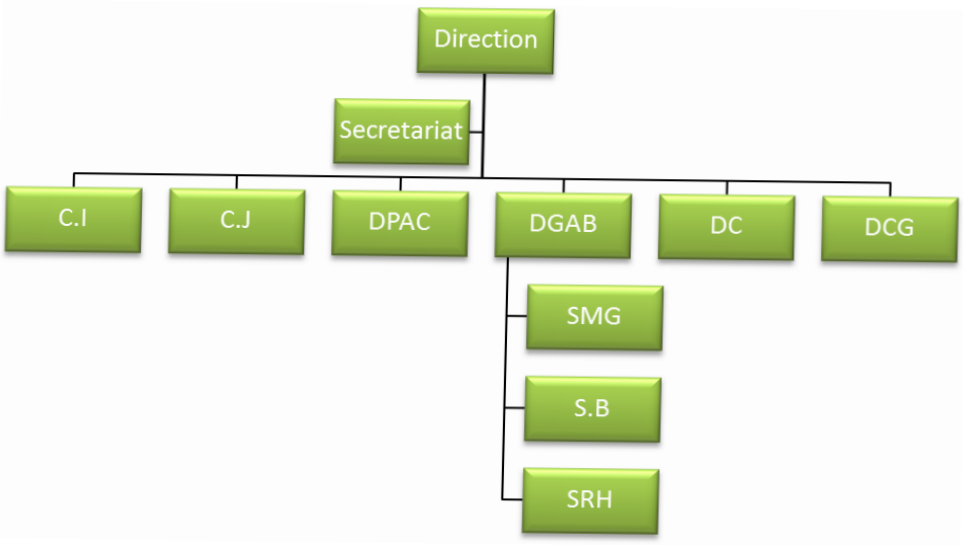

FIGURE 3.1 – Organigramme de la DRE

DRE : Direction
Secrétariat de Direction :

C.I : Cellule Informatique.
C.J : Cellule Juridique.
DPAC : Département Promotion et Administration Commerciale.
DGAB : Département de Gestion et Administration et Budget avec ses services
DC : Département Crédit.
DCG : Département Contrôle Gestion.

3.3.2 Présentation de la cellule informatique

La cellule informatique à sa dimension a un impact lié au destin de la société, car son apport est tellement présent et visible dans l'interchangeabilité des données et de l'information au sein de la DRE de la BNA, dans l'administration et la maintenance du réseau informatique, etc.

3.3.3 Rôle de la cellule informatique de la DRE

de la cellule informatique rassemble 04 personnes qui exercent différentes taches, dans le but d'assurer le bon fonctionnement du réseau de l'entreprise.

3.4 La Situation Informatique de la Banque

3.4.1 Materiel

A **Les terminaux ou les stations de travail Leurs fonctions est de permettre a l'utilisateur d'acceder aux ressources du reseau. On peut distinguer deux types de terminaux :**

- ✓ **Les terminaux a usage specifique, par exemple les terminaux bancaires (Des unites type FUTRO siemens).**
- ✓ **Les micro-ordinateurs. La plupart des stations de travail sont maintenant des micro-ordinateurs. Elles effectuent le traitement des donnees au moyen de leur propre unite centrale. Ces stations sont connectees au reseau par l'intermediaire de cartes d'extensions.**

✓ **Equipements Reseaux.**

- **Le routeur de type Cisco 2900**
- **LE PARE-FEU (FIREWALL) type FW-310.**
- **Un commutateur reseau (switch) : type CISCO 2960.**
- **Le Equipement reseau pour la VSAT : La VSAT, pour Very Small Aperture Terminal (terminal a tres petite ouverture) designe une technique de communication par satellite bidirectionnelle.**
  Elle utilise des equipements tels que :
  1. **UDgatway c est un ordinateur qui integre des fonctions de reseaux et de routages connecte au Switch du LAN et a l EMS pour assurer la communication entre le site emetteur et le site recepteur.**
  2. **EMS le modem liant la parabole en entree (in) et sortie (out) avec les cables speciaux.**
  3. **La parabole Fixee au toit d un immeuble avec certaines normes fixees par Algerie Telecom et assure l emission et la reception des ondes magnetiques selon des politiques d emission et de reception.**
- **des imprimante Les imprimantes ont été conçues dès l'apparition des premiers ordinateurs, pour permettre la consultation et la conversation sur support papier des résultats produits par les programmes informatiques. En effet, à l'époque des premiers calculateurs, les écrans n'existaient pas encore et les méthodes de stockage de l'information étaient très rudimentaires très couteuses. Avec le temps, les imprimantes on énormément évolue dans leur méthode d'impression et de traction du papier, mais également dans leur qualité d'impression, leur encombrement et leur cout.**
- **Des appareilles téléphoniques**
- **Des prises RJ45 et RJ11**

C **Les Serveurs :Les serveurs utilisés a la DRE sont de type IBM (RS 6000, Power 4, Power 520, P6,...) implementés au niveau des LAN des agences et la DRE de la Banque.**

- **Connectique de réseau avec serveur IBM**
  - **RMS :Réseau Multi-Services, accés spécialisé d'AT.**
  - **LAN :Local Area Network (réseau local)**

3.4.2 Logiciels

- **Logiciel de Transfert Filezilla :**
- **Outlook Web Access :**
- **IBM Informix :**

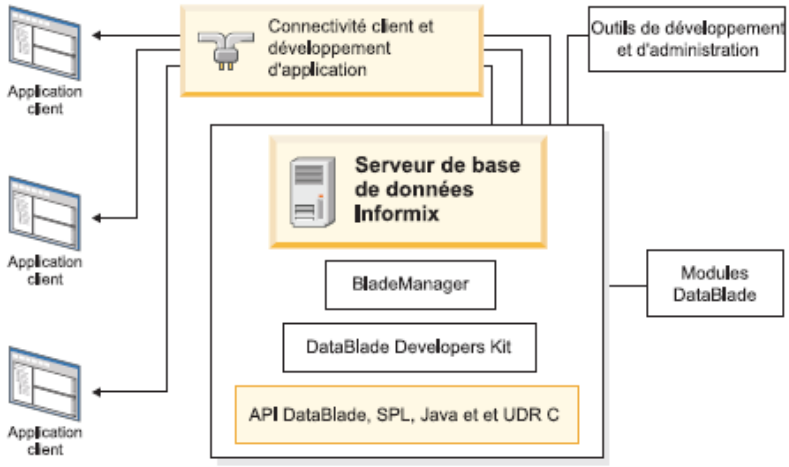

FIGURE 3.2 – architecture de base d'Informix.

3.5 types de réseaux informatiques de la banque

On distingue différents types de réseaux (privés) selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. Les réseaux privés sont des réseaux appartenant à une même organisation. Il existe deux types de réseaux : les réseaux publics (WAN et MAN), et les réseaux locaux (LAN).

3.5.1 Architecture du réseau informatique d'un site BNA

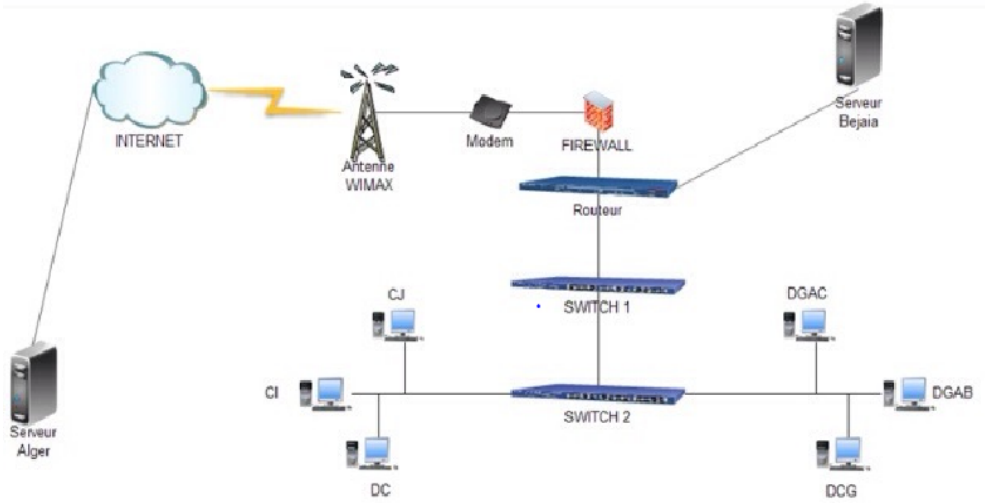

FIGURE 3.3 – architecture de base d'Informix.

3.5.2 Autre équipement

Armoire de brassage : une armoire de brassage appelée aussi «baie de brassage» est conçu pour héberger et protéger les différents équipements et composants du système de câblage du réseau informatique. Le choix d'une baie de brassage informatique s'effectue après avoir déterminé les équipements à intégrer (nombre de panneaux de brassage, commutateur Ethernet,. . . , etc.).Voici quelques photos prises au sein du district BNA de Bejaïa :

3.6 Critique

Durant la première période de notre stage au sein de l'agence BNA, nous avons étudié et analysé le fonctionnement du système informatique ainsi nous avons pu constater que l'agence avait une grande activité informatique ce qui pourrait rendre le réseau de l'agence vulnérable et sujet aux intrusions malveillantes.

FIGURE 3.4 – (a) Armoire.

Compte tenu des carences constatées lors de l'analyse du fonctionnement du système informatique de la banque nous proposons le développement d'un réseau privé virtuel.

3.7 Besoin de la banque :

L'information est à la base de toutes prises de décisions que ce soit pour mesurer le taux de satisfaction de la clientèle et surtout d'accroitre la vente afin d'atteindre l'objectif. C'est la raison pour laquelle la BNA ne peut que tirer d'avantages de se doter d'un réseau VPN site-à-site, moyen efficace et fiable dans le traitement de l'information.

3.8 Solution retenue

La solution retenue pour répondre à ce besoin de communication sécurisée consiste à relier les réseaux distants à l'aide d'une liaison

spécialisée. Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission. Un bon compromis consiste à utiliser Internet comme support de transmission à l'aide d'un protocole.
Nous avons opté pour la solution VPN IPSec site-à-site, qui consiste à mettre en place une liaison permanente, distante et sécurisée entre les deux sites le SITE CENTRAL, afin de résoudre au mieux aux différentes préoccupations manifestées par les responsables informatiques du district DRE de Bejaïa et aussi pour pallier aux différents problèmes relevés au niveau de la critique.
Il est néanmoins important de préciser que la solution retenue garantie la confidentialité, la sécurité et l'intégrité des données. Elle permet d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en oeuvre des équipements terminaux.
La mise en place d'un VPN permettra de distribuer un accès à Internet et des applications Web depuis leurs emplacements. Les VPN site-à-site étendent le WAN à moindre coût et en toute sécurité vers des entités non desservies, telles que des administrateurs et des partenaires commerciaux (extranet).

3.9 présentation du projet

- **Intitulé du projet : Solution de sécurité pour le LAN étendu de la DRE .**
- **Définition : Il est question ici de proposer un moyen sécurisé et sûr pour les échanges de données entre deux LANs (sites) d'une entreprise.**
- **Caractéristiques : Un routeur « CISCO » sur lequel nous implémenterons le protocole IPSec.**
- **Motif : L'architecture VPN se fait de plus en plus présente dans les entreprises, surtout chez celles qui ont ce besoin naturel d'interconnecter des LANs étendus en garantie d'un service toujours disponible et de meilleure qualité. Il est nécessaire de noter ici que la solution VPN ou plus précisément le protocole IP-Sec sera implémenter aux extrémités de chaque réseau sur le routeur servant de passerelle entre l'intranet et internet.**

3.10 Conclusion

Dans ce chapitre, nous avons présenté le cadre de travail dans lequel nous avons effectué le stage, ce qui nous a permis de mieux comprendre et apprécier le travail abattu par l'ensemble du personnel de la DRE de BNA, de comprendre la place qu'occupe cette structure dans le domaine, ainsi, l'étude de son réseau nous a permis de bien comprendre son architecture et ses faiblesses, et a conduit à proposer la solution pour palier à ces dernières.

Chapitre 4

Mise en oeuvre de la solution

4.1 Introduction

Chaque projet ou travail, commence généralement par une étude théorique, et se termine par une étude pratique qui est la mise en oeuvre de la solution ou bien la réalisation du projet.
Ce présent chapitre, consistera à mettre en oeuvre la solution proposée pour la réalisation de notre projet, avec l'ensemble des configurations nécessaires à implémenter sur les LANs de la BNA. Ces configurations entourent entre la configuration de routage et des différents protocoles de sécurité pour le VPN.
Pour visualiser l'efficacité de notre travail et mettre en évidence l'efficacité de notre solution, nous avons utilisé le simulateur GNS3 version 0.8.6 qui est un logiciel très pratique open source pour maquetter un réseau. Il pourra nous servir à reproduire une architecture physique ou logique complète avant la mise en production.

4.2 Présentation du simulateur Cisco GNS3

4.2.1 Définition

GNS3 (Graphical Network Simulator) est un simulateur graphique de réseaux qui permet de créer des topologies du réseau complexes et d'en établir des simulations. Ce logiciel est un excellent outil pour l'administration des réseaux Cisco. Il est possible de s'en servir pour tester les

fonctionnalités des IOS Cisco ou pour tester les configurations devant être déployées dans le futur sur des routeurs réels. Ce projet est évidemment Open Source et multi-plates-formes.[10]

4.2.2 Les composants du logiciel

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à :

- **DynamipsDynamips est un émulateur de routeurs Cisco capable de faire fonctionner des images Cisco IOS non modifiées comme si elles s'exécutaient sur de véritables équipements. Le rôle de Dynamips n'est pas de remplacer de véritables routeurs, mais de permettre la réalisation de maquettes complexes avec de vraies versions d'IOS.[13] Écrit en langage C par Christophe Fillot. Il émule 1700, 2600, 3600, 3700, et 7200 plates-formes de matériel .[10] Pour permettre l'exécution d'une image IOS, Dynamips doit émuler le processeur ainsi que tous les périphériques de la plateforme cible : mémoire RAM (Random Access Memory), NVRAM (No Volatil RAM), mémoire Flash, interfaces réseaux . . . .[13]**
- **DynagenDynagen est un produit complémentaire écrit en Python s'interfaçant avec Dynamips grâce au mode hyperviseur. Dynagen facilite la création et la gestion de maquettes grâce à un fichier de configuration simple décrivant la topologie du réseau à simuler et une interface texte interactive. GNS3 reprend ces mêmes fonctionnalités sous forme d'interface graphique. Il s'appuie sur des modules de Dynagen. Dynagen fournit aussi une CLI (Command-line Interpreter) de gestion pour les périphériques d'inscription, démarrage, arrêt, recharge, la suspension, la reprise et la connexion aux consoles de routeurs virtuels.[13]**
- **QemuQemu est un émulateur et une machine de virtualisation qui permet de courir à un système d'exploitation complet juste en tant que autre tâche sur l'ordinateur de bureau. Il peut être très utile pour essayer différents logiciels d'exploitation, logiciels d'essai, et le fonctionnement des applications qui ne fonctionneront pas sur la plate-forme indigène de notre ordinateur de bureau. Qemu fonctionne sur plusieurs plates-formes, et peut accueillir des systèmes de cible d'une gamme de différents microprocesseurs.[3]**
- **VirtualBoxVirtualBox est un logiciel de virtualisation de systèmes**

d'exploitation. En utilisant les ressources matérielles de l'ordinateur (système hôte), VirtualBox permet la création d'un ou de plusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation (systèmes invités). Les systèmes invités fonctionnent en même temps que le système hôte, mais seul ce dernier a accès directement au véritable matériel de l'ordinateur. Les systèmes invités exploitent du matériel générique, simulé par un faux ordinateur (machine virtuelle) créé par VirtualBox. VirtualBox permet de faire fonctionner plus d'un système d'exploitation en même temps en toute sécurité. En effet, les systèmes invités n'interagissent pas directement avec le système hôte, et n'interagissent pas entre eux. Le champ d'action des systèmes invités est confiné, limité à leur propre machine virtuelle .[5]

- **WiresharkWireshark, anciennement Ethereal, est un logiciel libre d'analyse de protocole, ou packet sniffer, utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage. Wireshark est multiplateformes, il fonctionne sous Windows, Mac OS, Linux, Solaris, ainsi que sous FreeBSD. Wireshark reconnait 759 protocoles.[4] Grâce à ces composants, GNS3 nous permet :[10]**
  - **Le design de topologies réseaux complexes en haute qualité.**
  - **Émulation de plusieurs plates-formes de routeurs Cisco IOS, ou encore IPS, PIX et Firewalls ASA...**
  - **Simulation de switches Ethernet, ATM et Frame Relay.**
  - **Connexion de réseaux simulés au monde réel.**
  - **Capture de paquets grâce à Wireshark.**

4.2.3 L'objectif de GNS3

L'objectif de GNS3 est d'apporter aux étudiants et aux professionnels travaillant dans le domaine d'administration des systèmes et réseaux des nouvelles technologies de communication. C'est un outil pour virtualiser et modéliser fidèlement des réseaux informatiques. Grâce à GNS3, les utilisateurs peuvent tester et estimer, dans des conditions quasi réelles et sans avoir à financer le matériel, leurs configurations avant de les mettre en place physiquement.[10]

4.2.4 Configuration de GNS3

1. **Lors du lancement du logiciel une fenêtre similaire à celle-ci apparait, c'est l'espace de travail de GNS3**

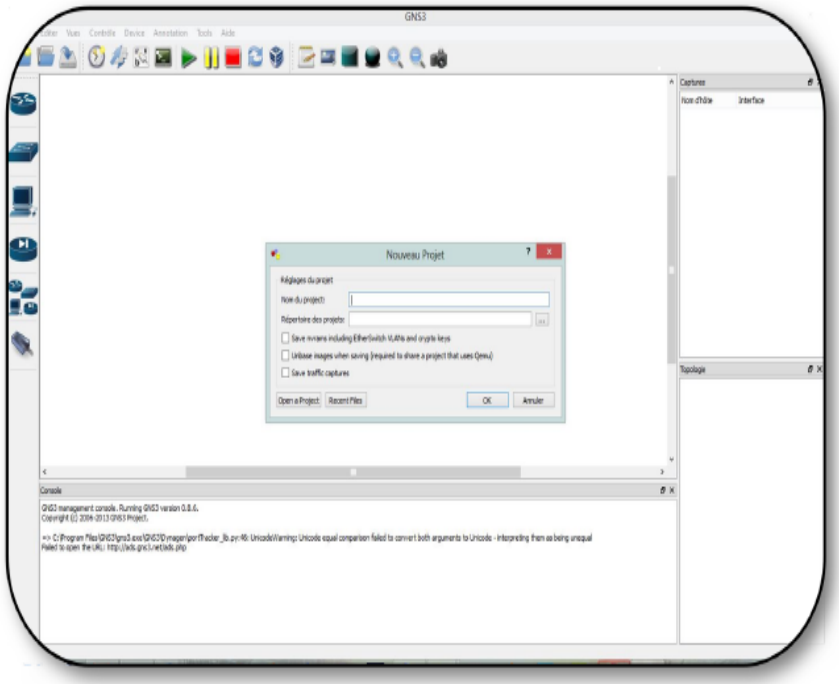

FIGURE 4.1 – L'espace de travail GNS3.

L'interface de GNS3 est divisée en trois parties, la partie gauche affiche la liste des équipements matériels disponibles que nous pouvons ajouter dans notre topologie, la partie droite affiche la liste des éléments actifs et au milieu c'est l'espace de travail. La petite fenêtre qui apparait au milieu, au lancement de GNS3, à pour objectif la création d'un nouveau projet. Pour cela il faut spécifier dans nom du projet et le chemin où sauvegarder le projet, ensuit cocher les trois cases dessous.

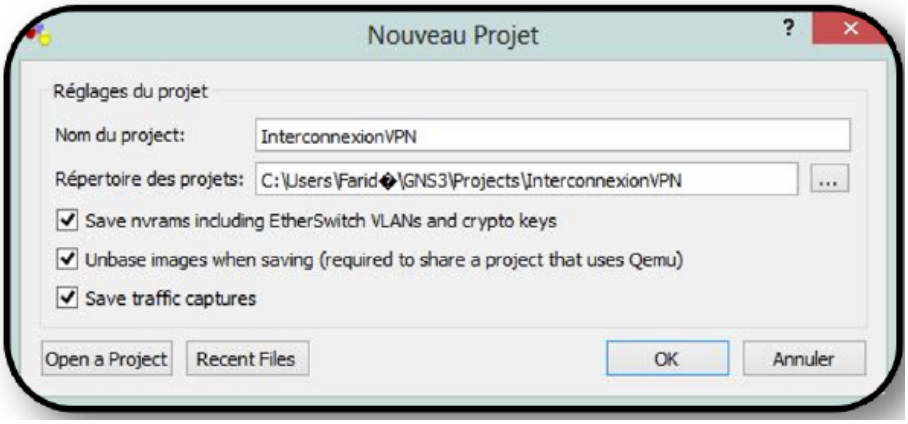

FIGURE 4.2 – Création d'un nouveau projet sous GNS3.

La manipulation d'interface de GNS3 est très simple, généralement son fonctionnement se base sur le principe du glisser-déposer. Il suffit de prendre un élément à placer sur l'espace du travail dans la liste des équipements à gauche.

2. **Pour commencer à travailler avec GNS3, nous devons avoir les différentes images (IOS) des équipements Cisco. Une fois téléchargées, Nous devons donner pour chaque modèle d'équipement que nous voulons utiliser, le chemin vers l'image IOS .**
3. **Pour ajouter l'IOS à la plate-forme adéquate aller sur le "Menu Éditer -¿ Images IOS et hyperviseurs". Cliquer sur "Image binaire", et sélectionner l'une des IOS précédemment téléchargée, puis choisir la plateforme et le modèle d'équipement adéquat puis cliquer sur "Sauvegarder". La figure ci-dessous montre deux modèles d'IOS que nous avons ajoutés.**

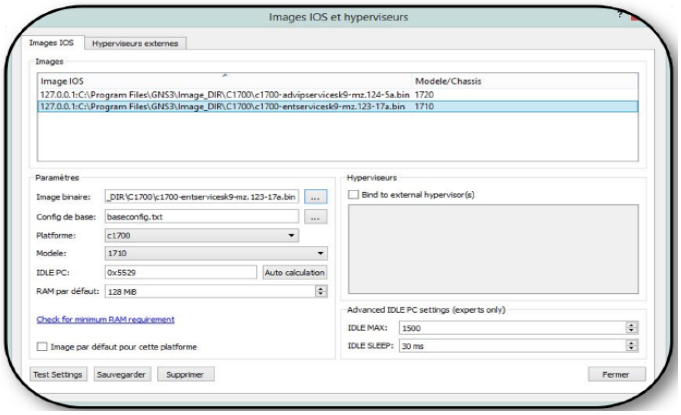

FIGURE 4.3 – L'ajout des IOS.

4. **Maintenant pour ajouter un équipement il suffit de faire un glisser-déposer à partir de la liste gauche et de le déposer dans la partie centrale de GNS3. Un clic droit sur l'équipement pour le démarrer.**
5. **Pour ajouter une machine virtuelle dans notre architecture GNS3, il nous faut d'abords préalablement installer VirtualBox et avoir déjà configuré au moins une machine virtuelle**
6. **Pour intégrer la machine virtuelle dans GNS3 Il faut d'abord l'importer comme suit : aller dans "Éditer − >Préférences − > VirtualBox − > VirtualBoxGuest − > RefreshVM List", puis donner un nom à la machine et dans le menu "VM list", sélectionner la machine à importer en suit sélectionner le numéro de la carte réseau laquelle elle va utiliser dans "Number of NICs" pour se connecter, en fin "Sauvegarder − >Appliquer− >OK".**

FIGURE 4.4 – L'ajout d'une machine virtuelle à la topologie GNS3.

Maintenant un glisser-déposer de la machine sur l'interface de travail nous permet de l'utiliser, et pour la configurer un clic droit sur la machine permet d'afficher le menu contextuel de configuration.

4.3 Présentation générale et principe de la solution proposée

4.3.1 Description de la maquette à configurer

Avant d'entamer la mise en oeuvre de la solution proposée, il est essentiel de définir l'architecture réseaux utilisée.
Pour cela, nous utiliserons la maquette du réseau WAN ci-dessous,

constitué de 2 sites distants (LAN de laBNA DRE de Béjaïa et le LAN de la direction générale située à Alger), possédant chacun :

- **Un routeur Cisco, avec un IOS supportant les fonctions de cryptage (modules d'accélération de cryptage matériel).**
- **Une connexion Internet avec des adresses IP fixes.**

-	Interface/IP locale	Interface/IP Internet
Site 1	FastEthernet 0/1 192.168.1.1	Serial 0/1 192.168.10.1
Site 2	FastEthernet 0/1 192.168.2.1	Serial 0/1 192.168.20.1

FIGURE 4.5 – Caractéristiques des deux routeurs.

4.3.2 Schéma idéalisé

Le but du VPN est de faire en sorte que les 2 sites communiquent exactement comme s'ils étaient directement reliés entre eux, de manière à ce que les 2 réseaux puissent êtres directement routés.

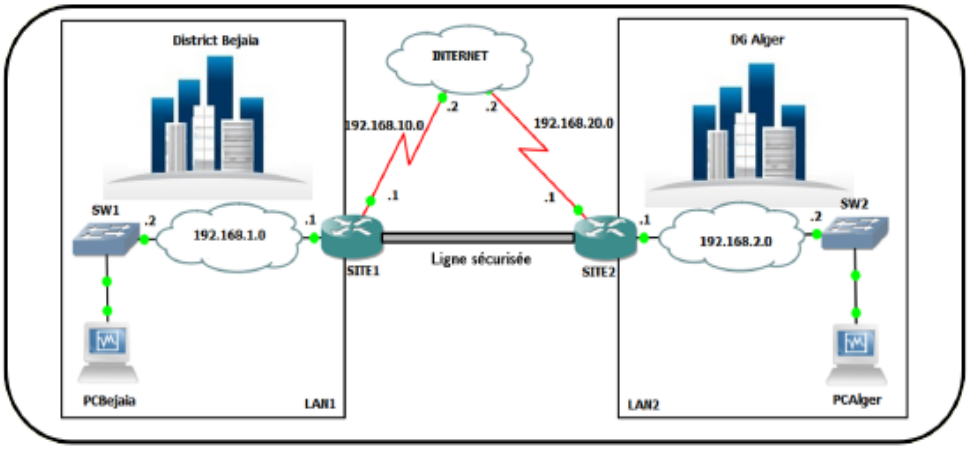

FIGURE 4.6 – Schéma idéalisé.

La liaison directe entre les 2 routeurs que nous avons ajouté symbolise dans le cas idéalisé une ligne sécurisée et fiable.

4.3.3 Schéma réel – Principe de mise en place

Dans la réalité il est évidement hors de question de connecter directement les 2 routeurs, puisque le but premier du VPN est justement de se passer d'une ligne spécialisée.
Ce lien sera donc créé grâce à un tunnel crypté, qui permettra aux 2 sites de communiquer entre eux de manière sécurisée. Pour cela, nous allons réaliser la configuration d'IPSec sur les deux routeurs : en mode automatique avec un secret pré-partagé via le protocole ISAKMP.

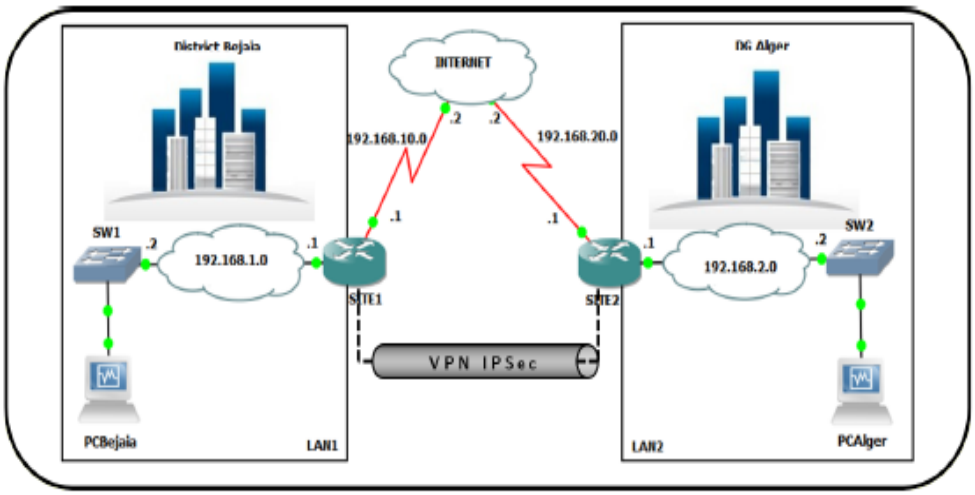

FIGURE 4.7 – Schéma réel.

Les critères de configuration d'IPSec à mettre en place seront :
- **Chiffrement et authentification avec le protocole ESP.**
- **Mode tunnel.**
- **Les algorithmes de chiffrement et d'authentification sont AES et SHA. Une fois le tunnel IPSec mis en place, nous lancerons un Ping entre les deux machines (PCBejaia et PCAlger), et visualiser les SA établies ainsi que certaines informations sur le trafic échangé.**

4.4 Configuration (En ligne de commandes)

4.4.1 Configuration des routeurs

Pour commencer, nous allons configurer les deux routeurs (SITE1 de Béjaïa et SITE2 d'Alger), en indiquant les adresses IP des interfaces associés à chacun d'entre eux, ainsi que le protocole de routage utilisé par chaque routeur.

```
Router1>enable
Router1#configure terminal
Router1(config)#hostname SITE2
SITE1(config)#interface fa0/0
SITE1(config-if)#ip address 192.168.1.1 255.255.255.0
SITE1(config-if)#no shutdown
SITE1(config-if)#exit
SITE1(config)#interface s0/1
SITE1(config-if)#ip address 192.168.10.1 255.255.255.0
SITE1(config-if)#no shutdown
SITE1(config-if)#exit
SITE1(config)#router rip
SITE1(config-if)#version 2
SITE1(config-if)#network 192.168.1.0
SITE1(config-if)#network 192.168.10.0
SITE1(config-if)#no auto-summary
SITE1(config-if)#exit
SITE1(config)#exit
SITE1#writ
```

De même, nous avons effectué la même configuration pour le routeur2 : Pour vérifier le bon fonctionnement du réseau créé, nous allons envoyer un Ping depuis la machine PCBejaia vers la machine PCAlger. Une analyse du trafic à l'aide de Wireshark au niveau de l'interface Internet de routeur SITE2 nous a donnée le résultat suivant :

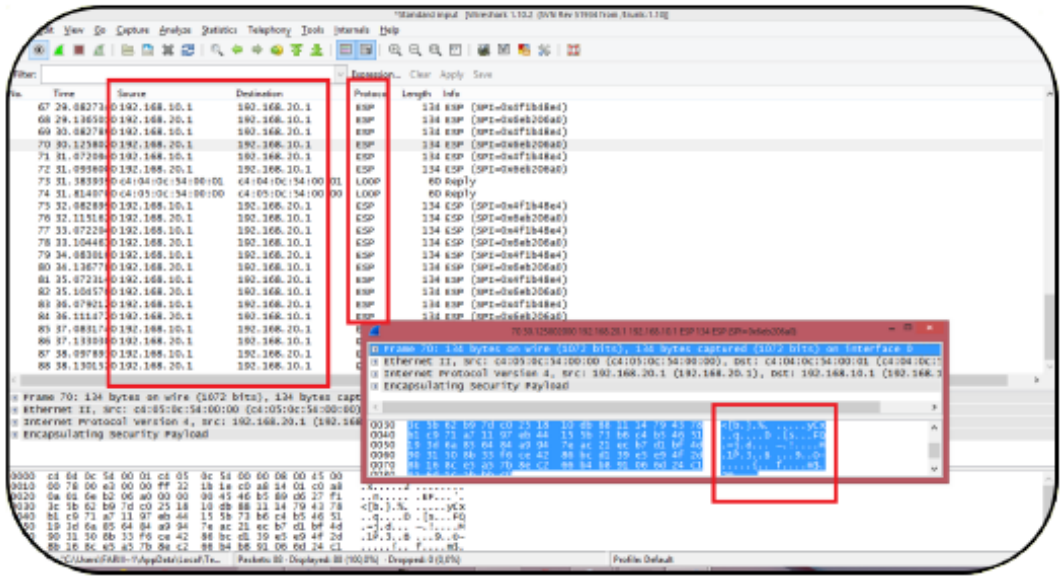

FIGURE 4.8 – Capture d'un échange de données non sécurisé entre SITE1 et SITE2.

Nous remarquons que des informations importantes et détaillées ainsi que des adresses du réseau locale, sont transportées en claire, cela présente une vulnérabilités, car un utilisateur malveillant, en possession de ces informations peut anticiper plusieurs types d'attaques.

4.4.2 Configuration du protocole IPSec

La configuration d'IPSec s'effectue généralement en suivant les étapes ci-dessous :

1. **Configuration de la politique d'ISAKMP de la phase 1 du protocole IKE : algorithmes, clés, durée de vie du tunnel ISAKMP qui se trouveront à la suite de la ligne de configuration commençant par crypto isakmp.**
2. **Configuration de la SA IPSec de la phase 2 du protocole IKE (protocoles AH/ESP, algorithmes, durée de vie du tunnel IPSec) se trouveront à la suite de la ligne de configuration commençant par crypto ipsec.**

3. **Description d'une carte de cryptage (crypto map) rassemblant les paramètres des deux phases, l'extrémité du tunnel et la définition du trafic à sécuriser se trouvera à la suite de la ligne de configuration commençant par crypto map. Il est très important de faire attention à ce que les configurations des deux routeurs soient cohérentes et symétriques, l'une par rapport à l'autre.**

4.4.3 Configuration d'IKE

Pour configurer le protocole IKE, nous allons réaliser les taches suivantes :

- **Activation du protocole IKE.**
- **Configuration de la politique d'IKE (phase 1).**
- **Configuration de l'authentification mutuelle par clé pré-partagée.**

4.4.3.1 Activation du protocole IKE

Le mécanisme IKE est activé par défaut sur la plupart des IOS Cisco. Il est validé globalement pour toutes les interfaces sur un routeur Cisco. Pour s'assurer, nous allons exécuter les commandes suivantes sur les deux routeurs :

```
SITE1(config)#no crypto isakmp enable
SITE1(config)#crypto isakmp enable
```

De même pour le routeur SITE2 :

```
SITE2(config)#no crypto isakmp enable
SITE2(config)#crypto isakmp enable
```

4.4.3.2 Configuration des paramètres de la SA ISAKMP (IKE phase 1)

Dans cette étape nous allons créer une politique pour le mécanisme IKE sur chaque routeur, cette politique se définit par une combinaison

des paramètres de sécurité à employer, le tableau ci-dessous indique la liste de ces paramètres.

Paramètre	Valeurs acceptées	Mot-clé	Par défaut
algorithme d'encryption	DES 56-bit	Des	DES 56-bit
	DES 168-bit	3des	DES 168-bit
	AES 128-bit	aes-128	AES 128-bit
	AES 256-bit	aes-256	
algorithme de hachage	SHA1 (HMAC variant)	Sha	SHA1
	MD5 (HMAC variant)	md5	
méthode d'authentification	Signatures RSA	rsa-sig	RSA signatures
	Chiffrement RSA	rsa-encr	
	Clés pré-partagées	pre-share	
groupe Diffie-Hellman	D-H 768-bit	1	D-H 768-bit
	D-H 1024-bit	2	
durée de vie de la SA	Spécifier une valeur	-	86400 seconds

FIGURE 4.9 – Liste des paramètres de sécurité pour IKE.

Une politique définie indique quels paramètres de sécurité seront employés pour protéger les négociations suivantes et précise également comment les deux routeurs seront mutuellement authentifiés. Pour la configuration des paramètres relatifs à la SA ISAKMP, nous allons procéder comme suit :

étape 1	SITE1(config)#crypto isakmp policy 7
étape 2	SITE1(config-isakmp)#encryption aes
étape 3	SITE1(config-isakmp)#hash sha
étape 4	SITE1(config-isakmp)#authentication pre-share
étape 5	SITE1(config-isakmp)#group 2
étape 6	SITE1(config-isakmp)#lifetime 86400
étape 7	SITE1(config-isakmp)#exit
étape 8	SITE1(config)#exit

FIGURE 4.10 – Description des étapes de configuration de la SA ISKAMP.

La même SA, avec les mêmes commandes seront implémentées sur le routeur SITE2.

étape 1	`SITE2(config)#crypto isakmp policy 7`
étape 2	`SITE2(config-isakmp)#encryption aes`
étape 3	`SITE2(config-isakmp)#hash sha`
étape 4	`SITE2(config-isakmp)#authentication pre-share`
étape 5	`SITE2(config-isakmp)#group 2`
étape 6	`SITE2(config-isakmp)#lifetime 86400`
étape 7	`SITE2(config-isakmp)#exit`
étape 8	`SITE2(config)#exit`

Le tableau ci-dessous décrit les différentes commandes utilisées :

Paramètre	Description
étape 1	Création d'une politique ISAKMP avec priorité 7/65535.
étape 2	Spécification d'un algorithme de cryptage.
étape 3	Spécification d'algorithme de hachage.
étape 4	Spécification d'une méthode d'authentification.
étape 5	Spécification de groupe Diffie Hellman.
étape 6	Spécification de la durée de vie de la SA.
étape 7	Quitter le mode de configuration isakmp.
étape 8	Quitter le mode de configuration terminal.

FIGURE 4.11 – VPN site à site.

À l'issue de cette négociation, un tunnel sécurisé (phase 1 du protocole IKE) est établi entre les deux routeurs SITE1 et SITE2. Désormais, la politique de sécurité de phase 2 (SA IPSec) sera négocié à travers ce tunnel ISAKMP pour ces deux derniers.

4.4.3.3 Configuration de l'authentification par clé pré-partagée

Dans cette étape nous allons configurer les clés pré-partagées que doit utiliser chaque hôte IPSec dans sa politique d'IKE en mode de configuration globale. Pour le routeur SITE1 nous indiquons "kdfrd" comme clé pré-partagée :

```
SITE1(config)#crypto isakmp key 0 kdfrd address 192.168.20.1
SITE1(config)#exit
```

La même commande doit être saisie pour le routeur SITE2 :

```
SITE2(config)#crypto isakmp key 0 kdfrd address 192.168.10.1
SITE2(config)#exit
```

4.4.4 Configuration des paramètres IPSec (transform-set)

Une fois la négociation de la phase 1 faite, nous devons configurer les paramètres de négociation pour la phase 2. Il s'agit de définir une transformation qui explicite les algorithmes IPSec (AH et/ou ESP) nécessaires pour la mise en oeuvre du tunnel IPSec. Le tableau ci-dessous définit la liste des transformations disponibles. Le nom de la transformation est suivi de la commande crypto ipsec transform-set. Les transform-sets doivent être identiques aux deux paires.

Paramètre	Transform	Description
AH Transform	ah-md5-hmac	AH avec authentification MD5
	ah-sha-hmac	AH avec authentification SHA
ESP Encryption-Transform	esp-des	ESP avec cryptage DES
	esp-3des	ESP avec cryptage 3DES
	esp-aes	ESP avec cryptage AES
	esp-null	ESP sans cryptage
ESP Authentification -Transform	esp-md5-hmac	ESP avec authentification MD5
	esp-sha-hmac	ESP avec authentification SHA

Pour la mise en place de notre transformation, nous allons taper la commande suivante sur le routeur SITE1 :

```
SITE1(config)#crypto ipsec transform-set TRANS esp-sha-hmac esp-aes
SITE1(config)#exit
```

La même commande sur le routeur SITE2 :

```
SITE2(config)#crypto ipsec transform-set TRANS esp-sha-hmac esp-aes
SITE2(config)#exit
```

FIGURE 4.12 – Liste des transformations disponibles.

4.4.5 Configuration des listes d'accès

Il faut configurer une liste d'accès qui définit le trafic à sécuriser. Ces listes d'accès sont différentes des ACLs qui déterminent quel trafic à expédier ou bloquer sur une interface. C'est l'entrée de la crypto map référençant la liste d'accès qui décide si le traitement d'IPSec est appliqué au trafic en fonction de l'action (permit et/ou deny) définie dans la liste d'accès. Pour le routeur SITE1 nous allons procéder comme suit :

```
SITE1(config)#ip access-list extended VPN-ACL
SITE1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255
SITE1(config-ext-nacl)#exit
```

De même, nous allons définir l'ACL associée au SITE2 :

```
SITE2(config)#ip access-list extended VPNACL
SITE2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255
SITE2(config-ext-nacl)#exit
```

4.4.6 Configuration de la carte de cryptage (crypto map)

La carte de cryptage (ou crypto map) permet de lier les SA négociées et la politique de sécurité (SP : Security Policy). En d'autres termes, elle permet de renseigner :

1. **Quel trafic devrait être protégé par IPSec.**
2. **L'autre extrémité du tunnel vers lequel le trafic IPSec devrait être envoyé.**
3. **L'adresse locale à employer pour le trafic d'IPSec.**
4. **Quelle sécurité d'IPSec devrait être appliquée à ce trafic (transform-set). Pour créer les différentes entrées de la carte de cryptage, qui emploieront IKE pour établir les associations de sécurité, nous allons procéder comme suit en suivant les étapes ci-dessous.**

```
étape 1    SITE1(config)#crypto map VPN-MAP 10 ipsec-isakmp
étape 2    SITE1(config-crypto-map)#set peer 192.168.20.1
étape 3    SITE1(config-crypto-map)#match address VPN-ACL
étape 4    SITE1(config-crypto-map)#set transform-set TRANS
étape 5    SITE1(config-crypto-map)#exit
étape 8    SITE1(config)#exit
```

Les mêmes commandes seront implémentées sur le routeur SITE2 :

```
étape 1    SITE2(config)#crypto map VPNMAP 10 ipsec-isakmp
étape 2    SITE2(config-crypto-map)#match address VPNACL
étape 3    SITE2(config-crypto-map)#set peer 192.168.10.1
étape 4    SITE2(config-crypto-map)#set transform-set TRANS
étape 5    SITE2(config-crypto-map)#exit
étape 6    SITE2(config)#exit
```

Le tableau ci-dessous décrit les différentes commandes utilisées :

Paramètre	Description
étape 1	Création d'une carte de cryptage avec priorité 1/65535.
étape 2	Spécification du trafic à sécuriser..
étape 3	Spécification de l'autre extrémité du tunnel IPSec.
étape 4	Application du modèle de transformation à la carte de cryptage.
étape 5	Quitter le mode de configuration de la carte de cryptage.
étape 6	Quitter le mode de configuration terminal.

FIGURE 4.13 – Description des étapes de configuration de la crypto map.

4.4.7 Application des crypto map aux interfaces

Il faut lier la crypto map ainsi définie à une interface du routeur par laquelle le trafic d'IPSec passera. Tout trafic arrivant ou sortant de cette interface est comparé avec le trafic à sécuriser défini dans une liste d'accès : s'il y a correspondance ce dernier est chiffré. Pour appliquer

la crypto map VPN-MAP à l'interface Internet sur SITE1, nous allons procéder comme suit :

```
SITE1(config)#int s1/0
SITE1(config-if)#crypto map VPN-MAP
SITE1(config-if)#exit
```

La même chose pour le routeur SITE2 :

```
SITE2(config)#int s1/0
SITE2(config-if)#crypto map VPNMAP
SITE2(config-if)#exit
```

4.5 tests de fonctionnement

Afin de vérifier le bon fonctionnement du VPN, plusieurs commandes sont à notre disposition en mode privilégié.

▷ La commande "show crypto engine connections active" nous permet de voir les connexions cryptées actives :

```
SITE1#show crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   1 FastEthernet0/1      192.168.10.1    set    HMAC_SHA+AES_CBC          0        0
2001 FastEthernet0/1      192.168.10.1    set    AES+SHA                   0       73
2002 FastEthernet0/1      192.168.10.1    set    AES+SHA                  74        0

SITE1#
```

FIGURE 4.14 – Affichage des connexions cryptées actives.

▷ La commande "show crypto ipsec transform-set" nous permet de voir les différents types d'encodage actifs.

```
SITE1#show crypto ipsec transform-set
Transform set TRANS: { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },


SITE1#
```

FIGURE 4.15 – Affichage des types d'encodage actifs.

▷ **La commande "show crypto ipsec sa" fourni une version plus détaillé que les deux commandes citées plus haut.**

```
#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: VPN-MAP, local addr 192.168.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   current_peer 192.168.20.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 13, #pkts encrypt: 13, #pkts digest: 13
    #pkts decaps: 13, #pkts decrypt: 13, #pkts verify: 13
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.10.1, remote crypto endpt.: 192.168.20.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x7729B3FA(1999221754)

     inbound esp sas:
      spi: 0xD910E476(3641762934)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4483604/3233)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x7729B3FA(1999221754)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
```

FIGURE 4.16 – Affichage en détails de la SA IPSec.

▷ **La commande "show ip route" nous permet de vérifier les routes crées.**

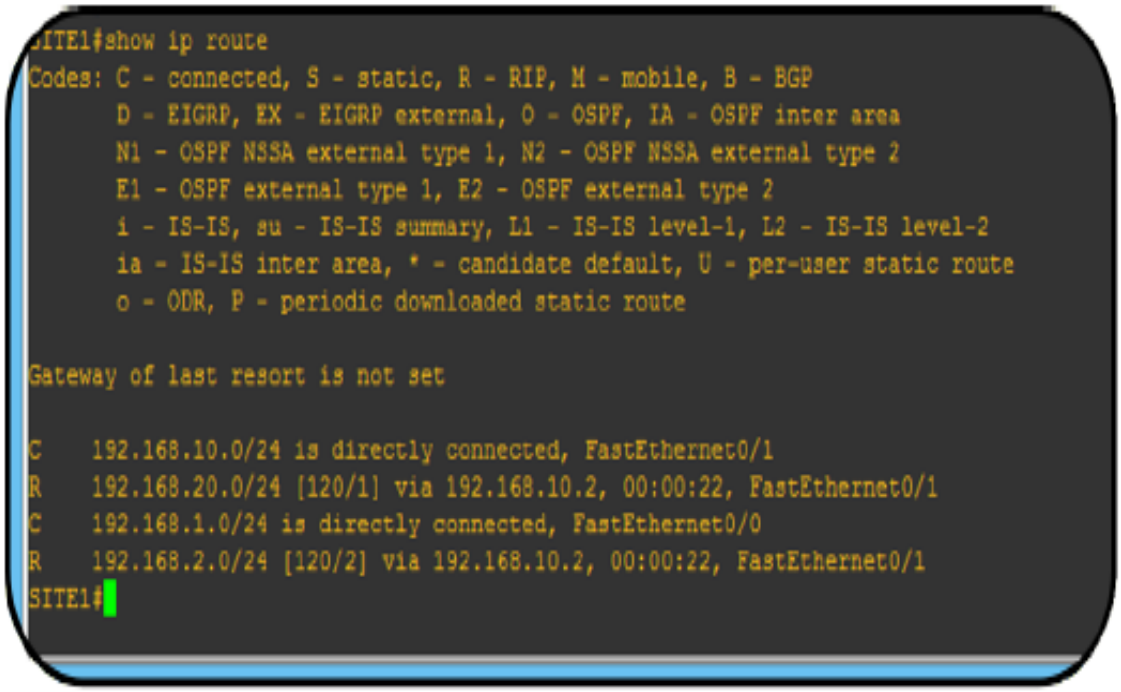

FIGURE 4.17 – Affichage des routes crées.

▷ **La commande "show crypto isakmp sa" fourni des informations sur l'association de sécurité d'ISAKMP**

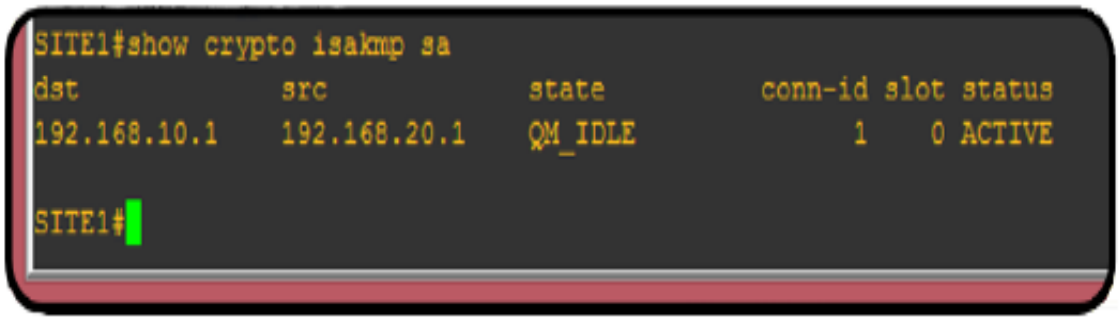

FIGURE 4.18 – Affichage de la SA ISAKMP.

▷ **La commande"show crypto map sa" nous permet de visionner des informations relatives aux cartes cryptage crées.**

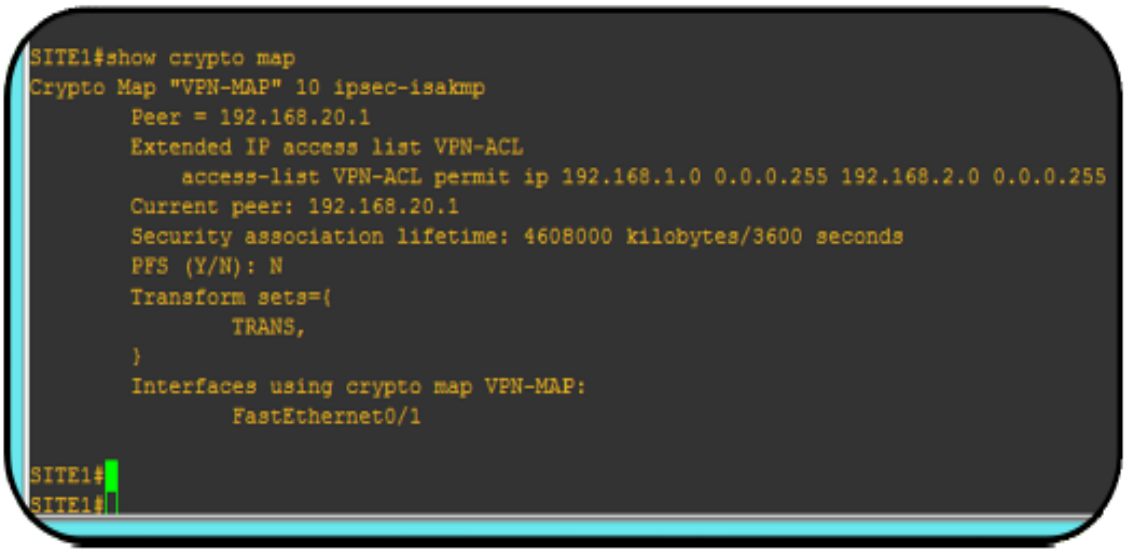

FIGURE 4.19 – Affichage des crypto map.

▷ **En fin, nous allons effectuer un sniffing à l'aide de Wireshark pour visionner le trafic échangés entre les deux sites. Un "Ping 192.168.2.2 -t" de PCBejaia vers PCAlger nous donne le résultat suivant :**

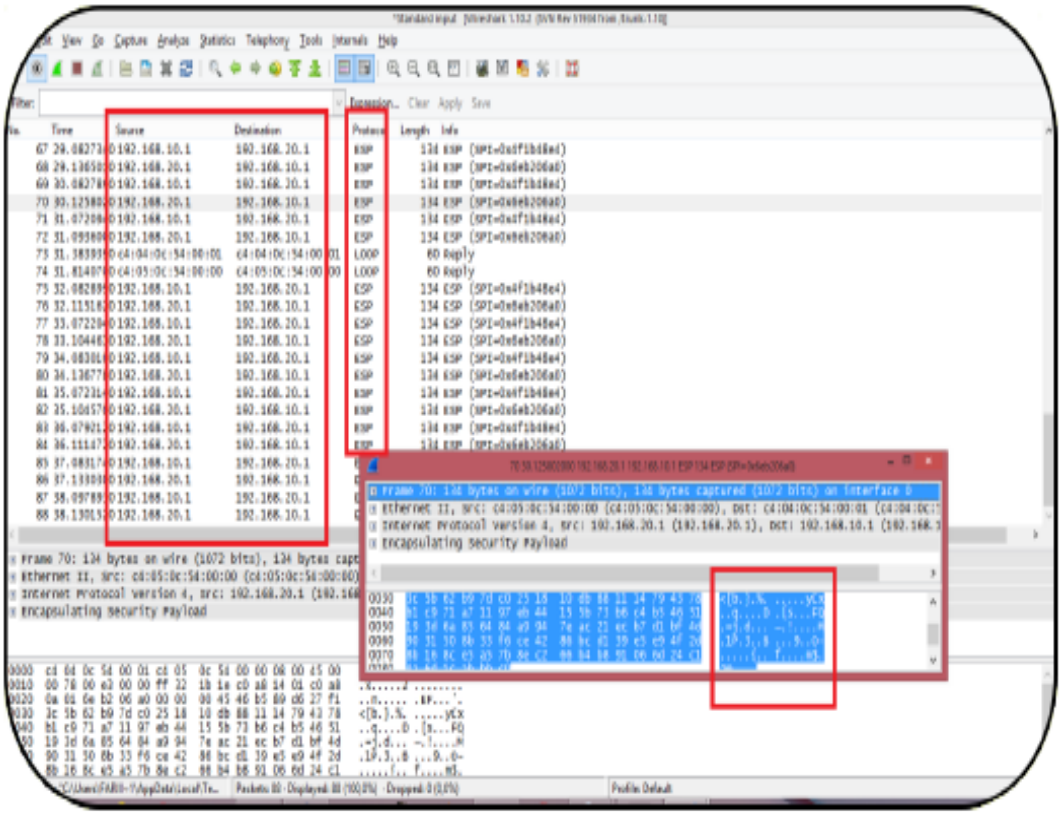

FIGURE 4.20 – Capture d'un échange de données sécurisé entre SITE1 et SITE2.

4.6 Conclusion

Au cours de ce chapitre, nous avons implémenté une solution de sécurité pour le réseau de la BNA qui permet de remédier aux différents problèmes et failles de sécurité constatées lors de stage effectué au sein du district DRE de Béjaïa. Le simulateur GNS3 nous a permis à partir de son interface graphique de concevoir et tester notre topologie comprenant des commutateurs, des routeurs et des stations de travail ainsi que leurs configurations qui nous a permis de bien concrétiser notre travail. Après la configuration nous avons exposé quelques tests afin de vérifier le bon fonctionnement et la fiabilité de VPN créé.

Conclusion et perspectives

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats de la mise en place d'un réseau VPN site-à- site à la BNA. Grâce à cette technologie nous permettrons aux employés de partager de façon sécurisée leurs données via le protocole IPSec qui est le principal outil permettant d'implémenter les VPNs, ce partage est possible en interne pour les utilisateurs du réseau local de l'entreprise, mais aussi en externe pour les utilisateurs dit « distants »situés en dehors du réseau local.
Nous avons présenté un travail divisé en deux parties, à savoir l'approche théorique qui était subdivisé en deux chapitres dont le premier a porté sur les généralités sur les réseaux informatiques ; le second 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 ainsi quelques définitions essentiels concernant la sécurité des réseaux informatiques .La deuxième partie offre une présentation de l'organisme d'accueil et traite l'aspect pratique , qui était aussi subdivisé en deux chapitres, le premier 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 la BNA. Et enfin le second, la réalisation du projet. Ce travail d'une part n'a pas été facile du point de vue conception car afin de simuler notre réseau, il fallait comprendre le fonctionnement des équipements Cisco et leurs fonctionnalités, comprendre les notions de VPN compliquées et apprendre à simuler avec le logiciel GNS3.
En effet, la mise en place de VPN 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 basé 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.En conclusion, les résultats obtenus lors des simulations effectuées sur le GNS3 ont montré le bon fonctionnement du VPN au sein de l'entreprise pour l'amélioration de la QoS, dans les réseaux informatiques.
Notons que ces résultats se concordent avec les objectifs tracés au début de l'étude, à savoir, sécuriser le partage entre les sites distants. Ce travail a fait l'objet d'une expérience intéressante, qui nous permis d'améliorer nos connaissances et nos compétences dans le domaine de sécurité des réseaux informatiques.

Bibliographie

[1] http://www.futura-sciences.com/magazines/high-tech/infos/dico/d/internet-firewall474, (2016).

[2] http://www.altcrn.org/tromtromh@yahoo.com, (2016).

[3] http://wiki.qemu.org/Main/Page., 2014.

[4] http://www.wireshark.org/docs/, 2014.

[5] Créer un serveur virtuel avec virtualbox. http://colibri-libre.org, 2014.

[6] http://www.google.dz/Equipements-de-transmissionresaux/Images, (Consulté avril 2016).

[7] *Guide SSI Etablir une barriere de securite entre les donnees externe et internes*. edition eni,552P, mai 2005.

[8] G. Andrew. *TCP/IP*. JumpStart-Internet Protocol Basics. Edition, 2002.

[9] J. Archier. *Les vpn*. edition eni,552P, 2o10.

[10] Présentation de gns3. http://www.gns3.net, 2014.

[11] T. Dean. *Réseaux Informatique*. Edition RYNALD GOULET, 2001.

[12] Cyrille Dufrenes. pare-feu-proxy-dmz. http://notionsinformatique.free.fr, (08/06/2008).

[13] Christophe FILLIOT and BERENGUIER Jean-Marc. *Dynamips : Un émulateur de routeur cisco sur pc*. Rapport technique, Université de Technologie de Compiègne, Service Informatique.

[14] G. Florin. *Cours securite pare-feu(Firewalls)*. CNAM-Laboratoire Cedric, 2000.

[15] **S. Kbaili, S. Mejbri, F. Mkacher, M. Ben Ammar, and I. Kabouri. *Securiday.* cyber War, 2o13.**

[16] **Malicious and accidental fault tolerance in internet applications. *Towards taxonomy of intrusion detection systems and attacks.* Rapport technique, Laboratoire MAFTIA Project Delivrable, 2001.**

[17] **ELUARD Marc. *Analyse de sécurité pour la certification d'applications Java Card. Thèse de doctorat.* Ecole doctorale MATISSE de l'université de Rennes 1, 2001.**

[18] **F. Modou and M. Malik. *Téléphonie sur IP. Mémoire de fin d'étude pour l'optimisation de diplôme d'ingénieur d'état spécialité télécommunication.* institut de la télécommunication Abdelhafid boussouf –ORAN, 2004.**

[19] **ORACLE. Sécurisation du réseau dans oracle solaris 11.1.** `http://docs.oracle.com/cd/E38898_01/html/E38852/ipsectm-1.html#scrolltoc`**, (2013).**

[20] **ROUDEL Philippe and MAROC Alain. Les vpns et les protocoles slip, ppp, pptp, l2f, l2tp, lcp, ipsec, mpls, nat.** `shttp://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2001ttv02/Roudel_Maroc/main.PDF.`**, (2002).**

[21] **G. Pujolle. *Les reseaux.* Paris,Edition, 2014.**

[22] **A. Richard. *An introduction to computer security. Rapport technique, Computer Science Department.* University of California, Santa Barbara, California, USA, 2010.**

[23] **Cisco System. *Cisco PIX Firewall and VPN configuration Guide Version 6.3.* Inc.170 Weat Tasman Drive san jose,CA 95134-1706, 2001-2003.**

[24] **LANDRY William. *Mise en place d'une architecture vpn mpls avec gestion du temps de connexion et de la bande passante utilisateur.* Institut d'ingenierie d'informatique de Limoge, ISTDI - Master Europeen en Informatique OPTION : Administration systèmes résaux, 2009.**

[25] **LASSERRE Xavier and KLEIN Thomas. Réseaux privés virtuels - vpn.** `http://www.frameip.com/vpn/`**, 2014.**

[26] DESWARTE Yves. ***Comment mesurer la sécurité informatique. Rapport technique.*** **Laboratoire d'Analyse et d'Architecture des Systèmes, CNRS, 2000.**

[27] DESWARTE Yves. ***BLOCH Laurent et WOLFHUGEL Christophe : Sécurité Informatique : Principes et méthodes.*** **Editions Eyrolles, 2009.**

RÉSUMÉ

Le travail réalisé dans ce mémoire de fin d'étude fait état des résultats obtenus lors de la proposition d'une solution de sécurité pour le LAN étendu de la BNA. Il s'agit d'une architecture VPN IPSec site-to-site, reliant le district DRE de Béjaia avec la direction générale de BNA à Alger. 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 passer en marge des infrastructures réseaux et des systèmes d'information qui progressent de façon exponentielle. En effet, grâce à cette nouvelle technologie, nous avons offert aux employés une solution pour partager de façon sécurisée leurs données via le protocole IPSec qui est le principal outil permettant d'implémenter les VPNs.

Mots clés : VPN,RPV, IPSec, Tunneling, Site-to-site.

ABSTRACT

The work done in this memory of end of study reported the results achieved at the proposal of asecurity solution for the extended LAN of BNA. It is an architecture site-to-site of IPSec VPN, linking the DRE district of Bejaia with BNA branch in Algiers. It appears that based on IPSec VPN technology is one of the key factors of success that evolves and should not go outside the network infrastructure and information system progressing exponentially. Indeed, with this new technology, we have offered employees a solution tosecurely share their data via the IPSec protocol, which is the primary tool to implement VPN.

Key words : VPN, RPV, IPSec, Tunneling, Site-to-site.