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 Informatique

Mémoire de Fin d'études

En vue de l'obtention du diplôme Master professionnel en Informatique

Spécialité : Administration et Sécurité des Réseaux

THÈME

Proposition d'une architecture réseaux sécurisée pour l'université A.Mira de Bejaïa

---

Réalisé par :

Mr Abid Yacine.
Mr Belhocine Meziane.

Devant le jury composé de :

Président :	Dr	BAADACHE Abderrahmane
Examinatrice :	Mme	HALFOUNE Nadia
Promoteur :	Dr	BOUDRIES AbdelMalek

Promotion 2014/2015

Remerciements

NOUS tenons dans un premier temps à remercier le bon dieu le tout puissant qui nous a donné le courage et la volonté pour mener à bien ce modeste travail.

Nous exprimons notre reconnaissance à Monsieur **BOUDRIES A.Malek** d'avoir joué pleinement son rôle de promoteur en étant à nos côtés tout au long de l'étude de notre projet, ses conseils et orientations nous ont guidés jusqu'à l'aboutissement de ce travail.
Nous remercions également **Mme N. Baiche** administrateur réseau au niveau du centre de calcule, pour son aide et ses remarques pertinentes qui ont apporté une amélioration certaine à notre travail.
Nous remercions aussi **Dr BAADACHE Abderrahmane** d'avoir accepté de présider le jury de notre soutenance.
Nos remerciements s'adressent aussi à **Mme HALFOUNE Nadia** d'avoir accepté de juger ce modeste travail.
Nos sincères remerciements s'adressent à nos parents, nos frères, nos sœurs ainsi qu'à toute la famille pour leur soutien moral, leur encouragement inconditionnel, et surtout pour la confiance qu'ils nous accordent.

Enfin, Nous remercions tous ceux qui ont contribué de près ou de loin à l'élaboration de ce travail, en particulier tous nos ami(e)s pour leur soutien moral et leur présence à nos cotés.

Meziane & Yacine

Dédicaces

Avec un énorme plaisir, un coeur ouvert et une immense joie,
que je dédie mon travail à mes très chers et respectueux parents
qui m'ont soutenus tout en long de ma vie ainsi qu'à mes soeurs et mes frères et en particulier
À mon binôme Meziane ainsi que sa famille
À mes ami(e)s et collègues de la promo
À toute personne qui ma aider et encourager de prêt ou de
loin toute au long de mes études

Yacine

À mes très chers parents,
À mes frère et sœurs, mes grandes mères,
À ma précieuse famille, mes cousins et cousines, Oncles et tantes,
À mon binôme yacine ainsi que sa famille
À mes amis et collègues,
Et à toutes les personnes que j'ai connues et qui m'ont aidées, un grand MERCI à tous.

Meziane

Résumé

L'université A. Mira de Bejaïa accueille chaque année des milliers de nouveaux bacheliers (d'Algérie et des quatre coins du monde). Elle met à leur disposition son réseau qui est alors à la merci de tout genre d'utilisateurs ! Pour protéger ce réseau, une idée serait d'acquérir un mécanisme de gestion qui soit à la fois robuste et sécurisés pour le réseau. L'objectif de notre travail consiste à proposer une architecteur réseau sécurisée de l'université A. Mira de Bejaïa, pour cela nous avons procédé à une étude de l'architecture actuelle, ainsi que les dispositifs de sécurité mis en place. Ce qui nous a permis de la critiquer et de suggérer des solutions afin de proposer une nouvelle architecture réseau qui donne une meilleure fluidité pour le trafic ainsi que sa sécurité. Sur le plan applicatif, nous avons séparé le réseau des deux campus en ajoutant une nouvelle ligne spécialisée vers le campus ABOUDAOU, nous avons configuré un tunnel sécurisé entre les deux réseaux reliant TARGA OUZEMOUR et ABOUDAOU en utilisant le simulateur GNS3, Finalement, nous avons mis en place un VPN d'accès en utilisant le firewall (open-source) Pfsense.

Mots clés **: VPN, IPSec, ISAKMP, GNS3, Pfsense.**

Abstract

The university A. Mira of Bejaia welcome every year thousands of new graduates (Algeria and around the world) and makes available its network for them. To protect the network, one idea would be to acquire a management mechanism that is both sturdy and safe for the network. The goal of our work is to propose a secure network architector for A. Mira university, in order to achieve that, we conducted a study of the current architector and safety devices put in place. This allowed us to criticism it and to suggest solutions in order to propose a new network architector that gives a better flow for traffic and safety. On the application side, we have separated the two campus network by adding a new line dedicated to the ABOUDAOUD campus, we configured a secure tunnel between the two networks and connecting TARGA OUZEMOUR and ABOUDOU using GNS3 simulator, finally, we have establish a VPN access using the firewall (open-source) Pfsense.

Keywords **: VPN, IPSec, ISAKMP, GNS3, Pfsense.**

Table des matières

Liste des figures

Liste des Acronymes

AES	**A**dvanced **E**ncryption **S**tandard
AH	**A**uthentication **H**eader
CA	**C**ertificate **A**utority
DES	**D**ata **E**ncryption **S**tandard
DH	**D**iffie **H**ellman
DoS	**D**enial **O**f **S**ervice
DSA	**D**igital **S**ignature **A**lgorithm
ESP	**E**ncapsulating **S**ecurity **P**ayload
FAI	**F**ournisseur d'**A**ccès **I**nternet
GARP	**G**eneric Attribute Registration Protocol
GNS3	**G**raphical **N**etwork **S**imulator
GVRP	**G**eneric **V**lan **R**egistration **P**rotocol
HMAC	**H**ash base **M**essage **A**etwork **C**uthentication
IDS	**I**nstruction **D**etection **S**ystem
IPS	**I**ntrusion **P**revention **S**ystem
IKE	**I**nternet **K**ey **E**xchange
IOS	**I**nternetwork **O**perating **S**ystems
IP	**I**nternet **P**rotocol
IPsec	**I**nternet **P**rotocol **S**ecurity
ISAKMP	**I**nternet **S**ecurity **K**ey **M**anagement **P**rotocol
L2F	**L**ayer **T**wo **F**orwarding
L2TP	**L**ayer **T**wo **T**unneling **P**rotocol
LAN	**L**ocal **A**rea **N**etwork
MD5	**M**essage **D**igest5
NAS	**N**etwork **A**ccess **S**erver
OSI	**O**pen **S**ystem **I**nterconnect
PA	**P**oint **A**ccès
PFS	**P**erfect **F**orward **S**ecrecy
PPP	**P**oint to **P**oint **P**rotocol
PPTP	**P**oint to **P**oint **T**unneling **P**rotocol
QoS	**Q**ualité **O**f **S**ervice
RSA	**R**ivest **S**hamir **A**dleman
SA	**S**ecurity **A**ssociation
SAD	**S**ecurity **A**ssociation **D**atabase

SHA	**S**ecure **H**ash **A**lgorithm
SP	**S**ecurity **P**olicy
SPD	**S**ecurity **P**olicy **D**atabase
SPI	**S**ecurity **P**arameter **I**ndex
TCP	**T**ransmission **C**ontrol **P**rotocol
UDP	**U**ser **D**atagram **P**rotocol
VLAN	**V**irtual **L**ocal **A**rea **N**etwork
VPN	**V**irtual **P**rivate **N**etwork

Introduction générale

Les réseaux et les systèmes d'information sont des outils indispensables au fonctionnement des entreprises. Ils sont aujourd'hui déployés dans des domaines aussi critique que la sécurité, la santé ou encore les finances. Ces derniers ont beaucoup d'ampleur et leur nombre de points d'accès ne cesse de croître.

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

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

Le stage que nous avons effectué au centre de calcul de l'université A .MIRA de Bejaia, nous a permis de découvrir son réseau et de comprendre son fonctionnement. Le but de notre travail est de proposer une architecture sécurisée du réseau de l'université A.MIRA de Bejaïa et de mettre des mécanismes de sécurisation des échanges de données. Afin de réaliser les objectifs visés, nous avons organisé ce travail en quatre chapitres :

- Le premier chapitre est consacré aux généralités sur les réseaux, la sécurité informatique et les dispositifs de sécurité.
- Le deuxième chapitre est focalisé sur les réseaux Privés Virtuels : leurs principes et fonctionnement, ses différents types et les différents protocoles utilisés pour sa réalisation.

- Le troisième chapitre concerne l'étude de l'architecture existante, les critiques, suggestion de solutions et enfin la proposition d'une nouvelle architecture pour le réseau.
- Le quatrième chapitre est consacré pour la mise en œuvre des VPNs, pour cela nous avons utilisé le router-firewall (Pfsense) pour la mise en place d'un VPN d'accès et Le simulateur GNS3 pour simuler la mise en place d'un VPN site à site.

Enfin, nous terminerons par une conclusion générale résumant les éléments essentiels qui ont été abordés dans ce mémoire.

Chapitre 1

Généralités sur les Réseaux et la Sécurité Informatique

1.1 Introduction

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

Au cours de ce chapitre nous établissons quelques généralités sur les réseaux et la sécurité informatique. Nous commencerons par les généralités sur les réseaux qui porteront sur la classification des réseaux, puis leurs types suivie de leurs topologies, et en fin les équipements utilisés, la deuxième partie qui sera la sécurité informatique portera sur les objectifs de la sécurité en premier lieu, puis sa terminologie, ensuite nous parlerons des attaques, suivie des éléments à sécuriser dans le réseau et la stratégie de sécurité, et nous terminerons ce chapitre par une conclusion.

1.2 Généralités sur les réseaux

1.2.1 Définition d'un réseau

Un réseau est un ensemble d'équipements interconnectés pouvant communiquer (ou échanger des informations). Il a pour but de transmettre des informations d'un équipement ordinateur à un autre [1].

1.2.2 Classification des réseaux

On distingue différentes catégories de réseaux selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue [1].

- **Les réseaux personnels, ou PAN (Personnel Area Network :)** interconnectent sur quelques mètres des équipements personnels tels que les terminaux GSM, portables, etc. d'un même utilisateur.
- **Les réseaux locaux, ou LAN (Local Area Network :)** un réseau LAN permet de connecter deux ou plusieurs centaines de machines à l'intérieur d'une même enceinte (Entreprise, administration, etc.), sur de courte distance (quelques kilomètres au maximum). On fait généralement appel à la technologie Ethernet pour relier les postes de travail.
- **Les réseaux métropolitains, ou 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 équipements distants de communiquer comme s'ils faisaient partie d'un même réseau local, Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).
- **Les réseaux étendus, ou WAN (Wide Area Network :)** sont des réseaux destinés à transporter des données à l'échelle d'un pays voir même d'un continent ou de plusieurs continents. Le réseau est soit terrestre, il utilise dans ce cas une infrastructure au niveau de sol essentiellement de grands réseaux de fibre optiques, soit hertzien, comme le réseau satellitaire.

Les différentes catégories des réseaux informatiques cités auparavant sont illustrées dans la figure 1.1

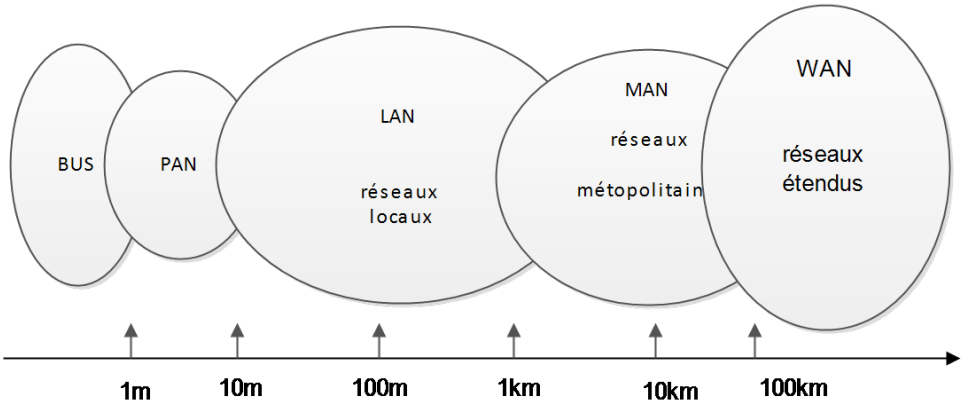

FIGURE 1.1 – Catégories des réseaux informatiques

1.2.3 Les types des réseaux

Internet

L'internet est par définition un ensemble de réseaux d'ordinateurs interconnectés, utilisant le protocole TCP/IP. C'est un service donnant l'accès à un réseau mondial mettant en contact divers mediums de communication et des serveurs, procurant aux utilisateurs une possibilité de partage d'informations, de recherche sur des sujets, d'échange de messages et dossiers à l'aide des courriers électroniques[1].

Intranet

L'intranet est la partie sécurisée d'un réseau informatique (d'une entreprise ou d'une organisation) basé sur les mêmes technologies que l'Internet (protocoles de communication TCP/IP, serveur, browser, e-mail, etc.). Il est destiné à l'échange et au partage d'informations entre des programmes et/ou des utilisateurs connus et autorisés. L'intranet est généralement connecté au réseau Internet pour permettre la communication avec le monde extérieur[1].

Extranet

Un extranet est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau. L'accès à l'extranet doit être sécurisé dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise. Il peut s'agir soit d'une authentification simple (authentification par nom d'utilisateur et mot de passe) ou d'une authentification forte (authentification à l'aide d'un certificat). Il est conseillé d'utiliser HTTPS pour toutes les pages web consultées depuis l'extérieur afin de sécuriser le transport des requêtes et des réponses http et

d'éviter notamment la circulation du mot de passe en clair sur le réseau[1].

1.2.4 Topologies des réseaux

La topologie d'un réseau recouvre tout simplement la manière dont sont reliés entre eux ses différents composants et la manière dont ils interagissent. Il convient de distinguer [2] :

- **La topologie logique :** qui représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token ring et FDDI2
- **La topologie physique :** C'est le chemin de câblage apparent, donc ce que voit l'utilisateur. On distingue principalement quatre types : en bus, en étoile, en anneau, et point-à-point :

  a) La topologie en bus : Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot " bus" désigne la ligne physique qui relie les machines du réseau.

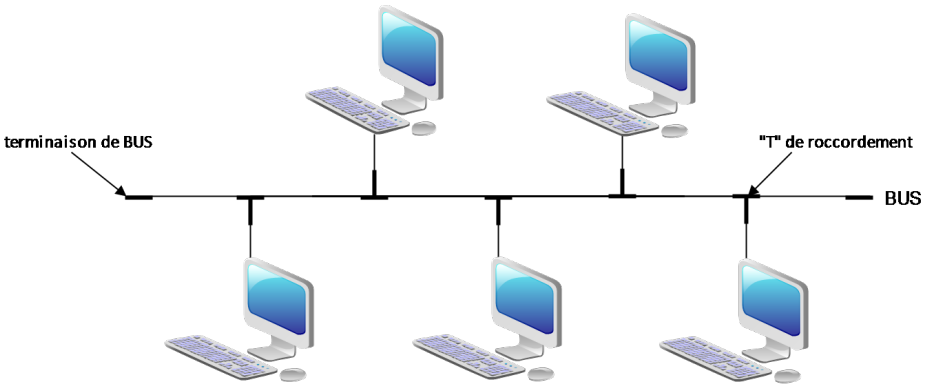

FIGURE 1.2 – La topologie en bus

  Elle a pour avantages d'être facile à mettre en œuvre, par contre elle est extrêmement vulnérable étant donné que si un des coupleurs est défectueux, c'est l'ensemble du réseau qui est affecté.

  b) Topologie en anneau : Une topologie en anneau ressemble assez à une topologie en bus, sauf qu'elle n'a pas de fin ni de début, elle forme une boucle. Quand un paquet est envoyé, il parcourt la boucle jusqu'à ce qu'il trouve le destinataire. Il existe soit la topologie en anneau simple soit la topologie en

double boucle FDDI (Fiber Distributed Data Interface), qui permet une redondance et qui comme son nom l'indique est formé de deux anneaux. La topologie en anneau est représentée dans la figure1.3.

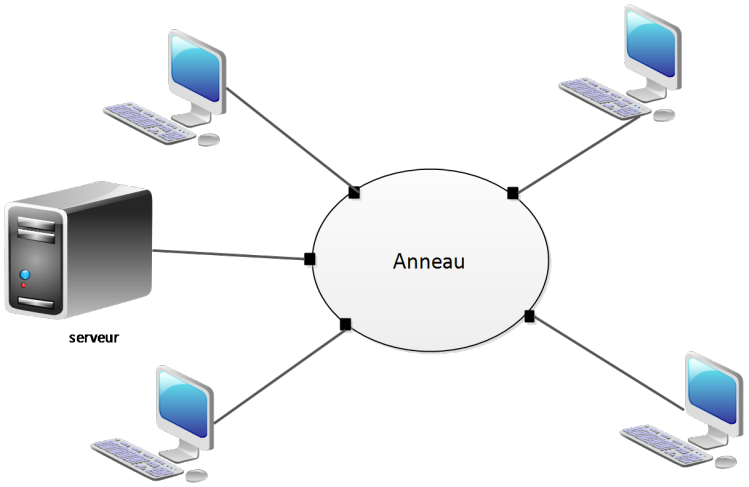

FIGURE 1.3 – La topologie en anneau

c) Topologie en étoile : Dans cette topologie chaque périphérique (ordinateur ou imprimante) est relié au nœud central. Les performances d'un réseau Ethernet dépendent principalement du nœud central. C'est un type de réseau relativement efficace et économique. La plupart des petits réseaux locaux fonctionnent sur ce principe, en utilisant un Switch central reliant tous les périphériques sur un même nœud.

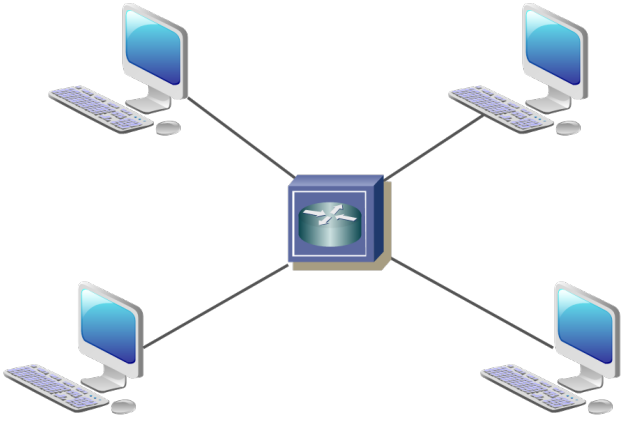

FIGURE 1.4 – Topologie en étoile

d) La topologie point-à-point : Dans un réseau point-à-point, chaque interface possède une liaison spécifique avec chacun des autres points. Ceci n'est utilisé

que sur de tous petits réseaux ou pour des raisons de robustesse des liaisons, la redondance diminue la sensibilité aux pannes. La Figure 1.5 montre un exemple d'une topologie point à point.

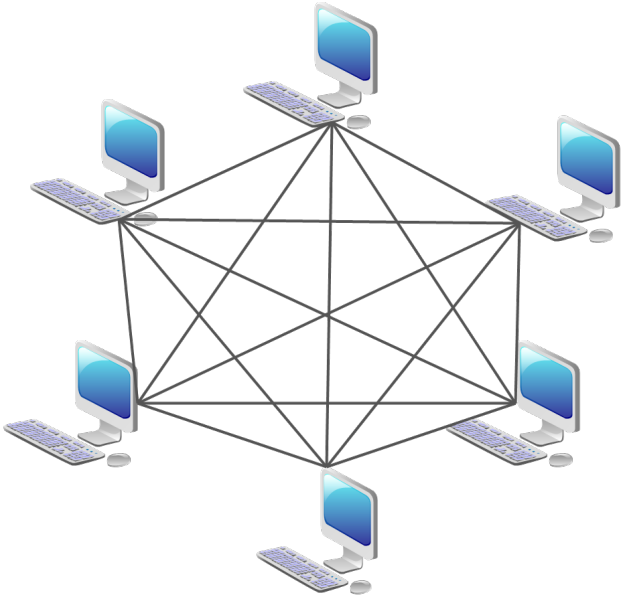

FIGURE 1.5 – topologie point à point

1.2.5 Equipement d'interconnexion

La mise en place d'un réseau soulève de nombreuses questions sur les contraintes d'utilisation. Comment faire si le réseau à créer dépasse les distances maximales imposées par le type de câble utilisé ? Comment faire parvenir les informations a d'autres réseaux que le sien ? Comment relier des réseaux utilisant des protocoles de communication différents ? Toutes ces questions peuvent être résolues grâce à différents types de matériels qui sont [3] :

- **Répéteur :** dispositif permettant d'étendre la distance de câblage d'un réseau local. Il amplifier et répète les signaux qui lui parviennent. .
- **Pont :** Un pont (bridge) est un dispositif permettant de relier des réseaux de même nature.
- **Routeur :** Un routeur (router) est un dispositif permettant de relier des réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de façon optimale
- **Passerelle :** Une passerelle (Gateway) est un dispositif permettant d'interconnecter des architectures de réseaux différents. Elle assure la traduction d'un protocole d'un haut niveau vers un autre.

— **Concentrateur :** Un concentrateur (hub) est un dispositif permettant de connecter divers éléments de réseau.
— **Commutateur** :Un commutateur (Switch) est un dispositif permettant de relier divers éléments tout en segmentant le réseau.
— **Adaptateur :** Un Adaptateur (adapter) est un Dispositif permettant de connecter deux systèmes qui n'avaient pas été conçus pour cela à l'origine .

1.2.6 Le modèle de référence OSI

Sur un réseau, la communication entre les différents éléments implique une logique dans leur façon d'interagir, et le respect d'un certain nombre de conventions et de règles afin d'assurer le bon déroulement du processus de transfert et de vérification des données reçues. L'ensemble de ces règles et conventions s'appelle un protocole. Il en existe un grand nombre et afin que tous ces protocoles puissent cohabiter, afin également de faciliter la conception de nouveaux matériels compatibles avec les appareils existants, il est souhaitable que tous ces protocoles utilisent un langage commun [4].

Le modèle de référence OSI (Open System Interconnexion) définit une sorte de langage commun. Ce modèle a été mis au point par l'ISO (Organisation Internationale des Standards) et il est devenu le socle de référence pour tout système de traitement de communications. Il repartit les questions relatives au domaine des communications informatiques selon sept couches classées par ordre d'abstraction croissant. Son objectif est d'assurer que les protocoles spécifiques utilisés dans chacune des couches coopèrent pour assurer une communication efficace. Décrivons succinctement le rôle de chaque couche [4] :

- **Physique** : Elle convertit les signaux électriques en bits de données et inversement, selon qu'elle transmet ou reçoit les informations à la couche liaison.
- **Liaison** :Elle est divisée en deux sous-couches :

  -La couche MAC qui structure les bits de données en trames et gère l'adressage des cartes réseaux.

  -La couche LLC qui assure le transport des trames et gère l'adressage des utilisateurs, c'est à dire des logiciels des couches supérieures.
- **Réseau** : Elle traite la partie donnée utile contenue dans la trame. Elle connait l'adresse de tous les destinataires et choisit le meilleur itinéraire pour l'acheminement. Elle gère donc l'adressage logique et le routage.
- **Transport** : Elle segmente les données de la couche session, prépare et contrôle les tâches de la couche réseau. Elle peut multiplier les voies d'accès et corriger les erreurs de transport.

- **Session** : Son unité d'information est la transaction. Elle s'occupe de la gestion et la sécurisation du dialogue entre les machines connectées, les applications et les utilisateurs (noms d'utilisateurs, mots de passe, etc.)
- **Présentation** : Elle convertit les données en information compréhensible par les applications et les utilisateurs : syntaxe, sémantique, conversion des caractères graphiques, format des fichiers, cryptage, compression.
- **Application** : C'est l'interface entre l'utilisateur ou les applications et le réseau. Elle concerne la messagerie, les transferts et partages de fichiers, l'émulation de terminaux.

La figure 1.6 illustre les couches du modèle OSI et leurs protocoles.

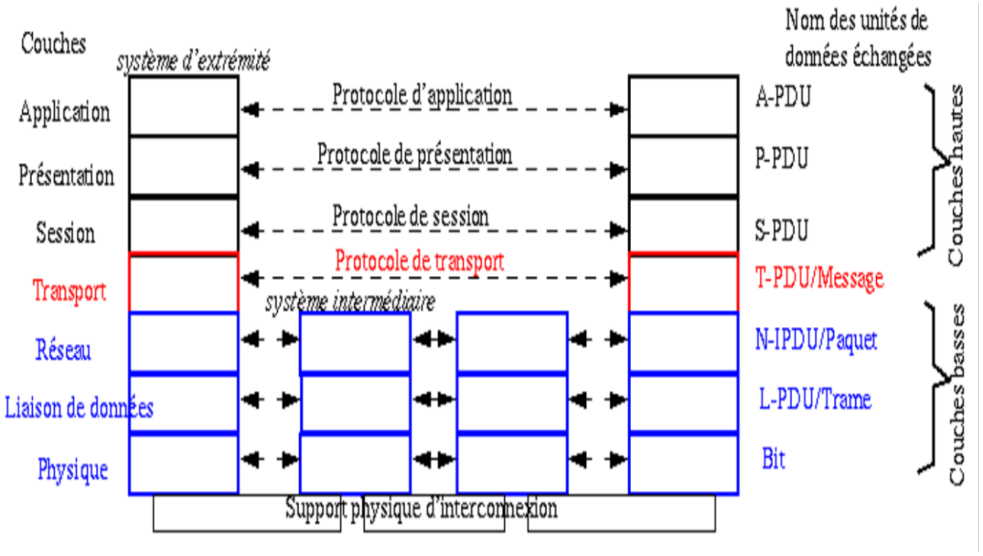

FIGURE 1.6 – Les couches du modèle OSI et leurs protocoles.

1.2.7 Le modèle TCP/IP

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation mais il est inspiré du modèle OSI. Il reprend l'approche modulaire (utilisation de modules ou couches) mais il contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application [4] [5]. Le schéma de la figure 1.7 nous montre la différence entre le modèle TCP/IP et le modèle OSI.

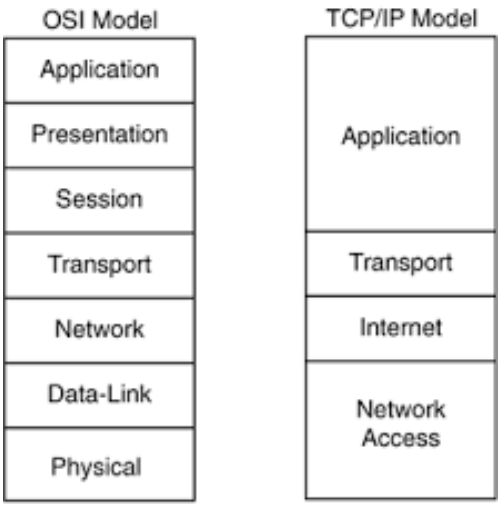

FIGURE 1.7 – Comparaison entre le modèle TCP/IP et le modèle OSI

1.3 Sécurité informatique

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

1.3.1 Objectifs de sécurité informatique

La sécurité informatique (SI) est l'ensemble des moyens (méthodes, techniques et outils) mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles. Et qui a pour objectif d'assurer les propriétés suivantes [6] :

- **La Confidentialité** : Assurer que l'information ne soit divulguée ou révélée qu'aux personnes autorisées.
- **L'Authentification** : C'est la propriété qui assure que seules les entités autorisées ont accès au système.
- **L'Intégrité** : Assurer que l'information contenue dans les objets ne soit ni altérée, ni détruite de manière non autorisée.
- **La Disponibilité** : L'accès par un sujet autorisé aux ressources et informations du système doit être toujours possible.
- **Non répudiation** : C'est la propriété qui assure la preuve de l'authenticité d'un acte c'est-à-dire que l'auteur d'un acte ne peut denier l'avoir effectué.

1.3.2 Terminologie de la sécurité informatique

La sécurité informatique utilise un ensemble de terme bien spécifique, que nous énumérons dans ce qui suit [6] :

— **Vulnérabilité (faiblesse/faille)** : C'est une faille ou un point où le système est susceptible d'être attaque.

— **Menaces** : Ce sont les violations potentielles de la sécurité. C'est l'ensemble des personnes, choses, évènements qui posent danger pour un patrimoine en termes de confidentialité, d'intégrité, et de disponibilité. Il existe deux types de menaces, les menaces accidentelles (expositions) et les menaces intentionnelles (attaques).

— **attaques** : Une attaque désigne un accès ou une tentative d'accès non autorisés à un système.

— **Les contre-mesures** : Ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.

— **Une politique de sécurité** : La politique de sécurité d'un réseau se fonde avant tout sur une analyse des risques décrivant les ressources critiques du réseau, ses vulnérabilités, les probabilités d'occurrence des menaces sur ces ressources vitales, ainsi que leurs conséquences. A partir de cette politique de sécurité, une architecture, des outils et des procédures sont définis et déployés afin de protéger les ressources critiques et de répondre aux objectifs de sécurité.
L'établissement d'une politique de sécurité se fait selon les étapes suivantes :
- Identification des vulnérabilités ;
- Evaluation des probabilités associées à chacune des menaces ;
- Evaluation du coût d'une intrusion réussie ;
- Choix des contre-mesures ;
- Evaluation des coûts des contre-mesures ;
- Décision.

1.3.3 Les attaques

Dans ce qui suit, nous présenterons les différentes étapes ,les types et quelques attaques courantes.

1.3.3.1 Les différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma [7] :

- Identification de la cible : Cette étape est indispensable à toute attaque organisée, elle permet de récolter un maximum de renseignements sur la cible en utilisant

des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'utilisation des bases Whois, l'interrogation des serveurs DNS1,... ;

- **Le scanning** : L'objectif est de compléter les informations réunies sur une cible visées, il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall. . .). Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entrainer la défaillance de certains systèmes ;
- **L'exploitation** : Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau ;
- **La progression** : Il est temps pour l'attaquant de réaliser ce pourquoi il a franchi les précédentes étapes. Le but ultime étant d'élever ses droits vers root (administrateur) sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, nettoyage des traces,. . .).

1.3.3.2 Les différents types d'attaques

Il existe trois types d'attaques [6] :

1. **Attaque directe :** C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son propre ordinateur. La figure 2.1 illustre l'attaque directe.

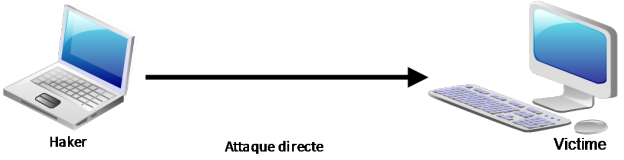

FIGURE 1.8 – Attaque directe

2. **Attaque indirecte par rebond :** Cette attaque est très prise des hackers, car le principe est simple, les paquets d'attaques sont envoyés à l'ordinateur intermédiaire, qui récupère l'attaque vers la victime. D'où le terme de rebond qui permet de :

   - Masquer l'identité (l'adresse IP) du hacker ;

   - Utiliser éventuellement les ressources de l'ordinateur intermédiaire, car il est plus puissant pour l'attaque.

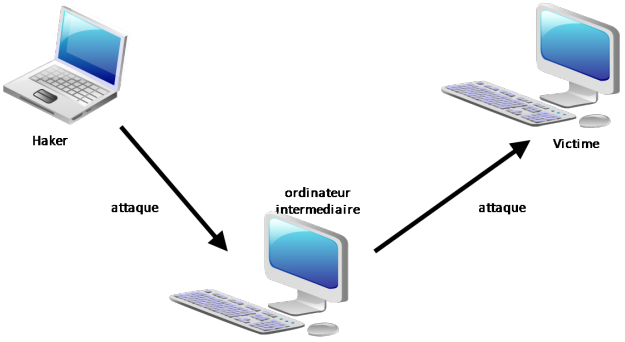

FIGURE 1.9 – Attaque par rebond

3. **Attaque indirecte par réponse :** Cette attaque est dérivée de l'attaque par rebond. Cependant au lieu d'envoyer une attaque à la machine intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête, cette dernière va être envoyée à la machine.

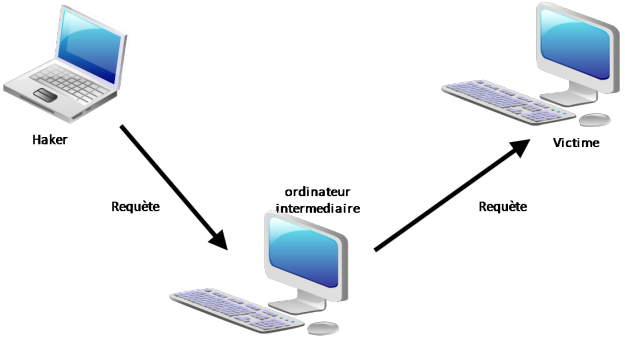

FIGURE 1.10 – Attaque indirecte par réponse

1.3.3.3 Quelques attaques courantes

Il existe un grand nombre d'attaques permettant à une personne mal intentionnée désapproprier des ressources, de les bloquer ou de les modifier. Certaines requièrent plus de compétences que d'autres, en voici quelques-unes :

- **IP spoofing** : Cette attaque est difficile à mettre en œuvre et nécessite une bonne connaissance du protocole TCP, elle consiste, le plus souvent, à se faire passer pour une autre machine en falsifiant son adresse IP de manière à accéder à un serveur ayant une "relation de confiance" avec la machine "spoofee". Cette attaque n'est intéressante que dans la mesure où la machine de confiance dont l'attaquant a pris l'identité peut accéder au serveur cible en tant que root ;
- **Le sniffing** : Grace à un logiciel appelé "sniffer", il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées. Si quelqu'un

se connecte par Telnet par exemple à ce moment-là, son mot de passe transitant en clair sur le net, il sera aisé de le lire. De même, il est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Une restriction de cette technique est de se situer sur le même réseau que la machine ciblée ;

- **Le Dos (Denial of Service)** : Le Dos est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d'un système. Cette attaque ne permet pas en elle-même d'avoir accès à des données. En général, le déni de service va exploiter les faiblesses de l'architecture d'un réseau ou d'un protocole. Il en existe plusieurs types comme le flooding, le smurf ou le débordement de tampon (buffer-overflow) ;
- **Les programmes cachés ou virus** : Il existe une grande variété de virus. On ne classe cependant pas les virus d'après leurs dégâts mais selon leur mode de propagation et de multiplication. On recense donc les vers (capables de se propager dans le réseau), les troyens (créant des failles dans un système), Les bombes logiques (se lançant suite à un évènement du système (appel d'une primitive, date spéciale)) ;
- **Le scanning (appelé analyseur de réseaux)** : L'objectif est de compléter les informations réunies sur une cible visée, il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles, de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall. . .).
  Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entrainer la défaillance de certains systèmes ;
- **L'ingénierie sociale (social engineering)** : Ce n'est pas vraiment une attaque informatique en soit, mais plutôt une méthode qui est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs
- **Le craquage de mots de passe (Brute force)** : Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines ;
- **Le flood** : un flood consiste à envoyer très rapidement de gros paquets d'informations à une personne. Cette dernière visée ne pourra plus répondre aux requêtes et le modem va donc se déconnecter, c'est cette méthode qui a été employée à grande échelle dans l'attaque des grands sites commerciaux [6].

1.3.4 Les éléments à sécuriser dans un réseau

Les réseaux sont constitués de divers équipements d'une part et de liens filaires ou non filaires, qui, les relient d'autre part. Toute ou partie de ces équipements peuvent être gères par des programmes adaptés et plusieurs sorts de données y sont stockées. Certains d'entre elles peuvent être l'objet de transferts selon des protocoles appelés protocole de réseaux. Dans ce cadre, la sécurité concerne celle du matériel, celle des programmes, celle des données et celle des protocoles [6].

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

- **Matériel** : Mis à part les ordinateurs que les réseaux relient, le matériel inclut aussi, les équipements intermédiaire comme les répéteurs, commutateurs (switch), routeurs, serveur, modems, firewalls, etc. La limitation d'accès à chaque matériel participe à la sécurité de l'ensemble
- **Programme** : les programmes incluent les systèmes d'exploitation y compris les pilotes de périphériques ainsi que les logiciels programmes gérant les différents mécanismes de réseaux. Les services permettant une meilleure gestion à distance et plus d'autonomie, on parle dans ce cas-là de services réseau tels que : DHCP, DNS, FTP, etc.
- **Données** : On distingue deux sortes de données , celles qui servent au fonctionnement du réseau comme les tables de routage, les bases de données de clients, les fichiers relatifs aux droits d'accès, etc. On trouve aussi des données qui ne sont pas en rapport avec le fonctionnement du réseau tels que : les documents et les archives

1.3.5 Stratégies de sécurité

Elles consistent à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles dénient dans une politique de sécurité. En voici Les principaux dispositifs permettant de sécuriser un réseau contre les attaques.

1.3.5.1 Un pare-feu

est un élément du réseau informatique, logiciel et/ou matériel, qui est aujourd'hui incontournable dans la sécurité de tout système informatique car il permet d'appliquer une politique d'accès aux ressources informatiques. Il a pour principale tâche de contrôler le trafic entre les différentes zones de confiance, en filtrant les flux de données qui y

transitent [8]. Le pare-feu est également intéressant dans le sens où il constitue un point unique (goulot d'étranglement) où l'audit et la sécurité peuvent être imposés. Tous les échanges passeront par lui. Il pourra donner des résumés de trafic, des statistiques sur ce trafic, ou encore toutes les connexions entre les réseaux.

a) Principes de fonctionnement d'un pare-feu

Dans ce qui suit nous expliquerons les principes de fonctionnement d'un pare-feu [9] :

• **Le filtrage de paquets (Packet Filtering)** : Les paquets sont analysés en les comparants à un ensemble de filtres (c'est-à-dire à un ensemble de règles). Les paquets seront alors soit rejetés, soit acceptés et transmis au réseau interne. Ce filtrage a lieu sur les couches Réseau (IP) et Transport (TCP/UDP). Au niveau de la couche réseau, le firewall vérifiera 3 informations :

- L'adresse IP de destination ;

- L'adresse IP de la source ;

- Quelques options présentes à ce niveau.

Au niveau de la couche Transport, le firewall analysera d'autres informations telles que :

- Le port de destination ;

- Le port de la source ;

- Le type de protocole utilisé (TCP ou UDP) ;

- Les filtrages TCP.

Lorsque le paquet arrive au firewall, celui-ci analyse les champs IP et TCP/UDP. Ils sont confrontés à chacune des règles spécifiées dans la table des autorisations présentes dans le firewall, et configurées par l'administrateur du système. Selon les règles qui autorisent ou refusent la transmission des paquets, le firewall obéira aux ordres. Si un paquet ne satisfait à aucune des règles, il est soit rejeté, soit accepté, suivant la philosophie choisie par l'administrateur réseau :

- Ce qui n'est pas expressément permis est interdit.

- Ce qui n'est pas expressément interdit est permis.

La première de ces deux approches est beaucoup plus sûre. La seconde est plus risquée car elle suppose que l'administrateur est certain d'avoir envisagé tous les cas pouvant engendrer des problèmes. L'avantage du filtrage par paquet est sa rapidité. Il est de plus relativement simple à implanter dans un réseau.

• **La passerelle applicative (Application Gateway)** : A la différence du filtrage de paquets, qui analyse les paquets individuellement, l'application Gateway permet de limiter les commandes à un service plutôt que de l'interdire. Ce principe

de fonctionnement empêche le trafic direct entre le réseau protégés et l'Internet, et ce dans les deux sens. Le trafic interne n'atteindra jamais Internet, et inversement, aucun trafic Internet ne voyagera sur le réseau interne. En effet, chaque client interne se connectera sur un serveur proxy (qui est la base de ce principe). Toutes les communications se feront par l'intermédiaire de celui-ci. Il déterminera si le service demandé par l'utilisateur est permis et se connectera avec le destinataire en cas d'autorisation, le destinataire ne connaitra pas l'adresse de son correspondant. Il ne communiquera qu'avec le serveur proxy, qui jouera en réalité le rôle d'un translateur d'adresse réseau (NAT). La sécurité est ici très élevée. Agissant au niveau applicatif, on peut notamment la retrouver dans l'authentification par mot de passe des utilisateurs.

• **Le filtrage du flux** : Le filtrage de flux ne prête pas attention au contenu des paquets transitant sur la connexion. De ce fait, ce type de filtrage ne peut être utilisé pour assurer l'authentification des parties, ou la sécurité du protocole par l'intermédiaire duquel a lieu la connexion. A la différence du filtrage de paquets, qui est considéré comme permissif, le filtrage de flux est restrictif. En effet, il n'autorisera le flux entre deux entités que si la connexion entre ces deux entités existe. On peut voir ce principe comme la création d'un tunnel entre deux machines. De ce fait, le filtrage du flux ne sera souvent utilisé qu'en complément de l'application Gateway.

b) Limitations d'un pare-feu

Un pare-feu est un composant dédie à la sécurisation du réseau. Il représente une solution aux problèmes de protection de la confidentialité et d'intégrité des ressources sur le réseau et l'authentification du trafic. L'avantage de l'inclure dans une stratégie de sécurité est évident, toute fois un pare-feu s'accompagne des limitations suivantes [10] :

- Un pare-feu ne peut empêcher des utilisateurs ou des attaquants utilisant des modems d'accéder par numérotation à l'extérieur ou à l'intérieur du réseau dans le but de contourner sa protection.

- Un pare-feu ne peut faire respecter une stratégie de mots de passe, ni empêcher une mauvaise utilisation de ces derniers. Il est donc important qu'une stratégie expose clairement les comportements acceptables ainsi que les conséquences en cas de non-respect des règles.

- Un pare-feu n'est pas efficace contre les risques non techniques, tel que l'ingénierie sociale.

- Dans son rôle de porte d'entrée/sortie du réseau, le pare-feu concentre le trafic et la sécurité en un seul point, constituant ainsi un goulet d'étranglement et une

source de panne fatale.

1.3.5.2 Zone Démilitarisée

Si une entreprise doit héberger elle-même un site web public complet avec des serveurs tel qu'un serveur de messagerie, elle pourra envisager l'emploi d'un pare-feu avec deux interfaces (interne et externe) et lui laisser la tâche de créer les règles de traduction qui dirigent le trafic en entrée vers les serveurs appropriés au réseau d'entreprise. Cela peut s'avérer désastreux si un pirate a des vues sur ce réseau. D'où l'idée de recourir à une DMZ (DeMilitarized Zone). Une DMZ est une interface située entre un réseau connu (réseau interne) et un réseau externe (internet). Une série de règles de connexion configurées sur le pare-feu font de cette interface une zone physiquement isolée entre les deux réseaux. Cette séparation physique permet d'autoriser les accès internet à destination des serveurs placés dans la DMZ et non à ceux destinés au réseau privé (interne) La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante [11] :

- Trafic du réseau externe vers la DMZ autorisé ;
- Trafic du réseau externe vers le réseau interne interdit ;
- Trafic du réseau interne vers la DMZ autorisé ;
- Trafic du réseau interne vers le réseau externe autorisé ;
- Trafic de la DMZ vers le réseau interne interdit ;
- Trafic de la DMZ vers le réseau externe refusé.

La DMZ possède donc un niveau de sécurité intermédiaire, mais il n'est pas suffisant pour y stocker des données critiques pour l'entreprise. Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

1.3.5.3 La technologie AAA

Nous vivons dans un monde où presque tout doit être protégé contre une utilisation abusive ou impropre et où rien n'est gratuit. Que vous soyez administrateur système, responsable, ingénieur réseau ou étudiant. Lorsque vous accédez à un réseau, vous êtes toujours confronté aux trois aspects suivants [10] :

- **Authentification(Authentication)** : il s'agit de la vérification de l'identité d'un utilisateur, elle est généralement assurée au moyen d'un secret partage ou d'un logiciel approuvé (protocole RADIUS).
- **Autorisation (Authorisation)** : Elle intervient à l'issue de l'authentification. Une fois l'utilisateur authentifié, il faut s'assurer qu'il est autorisé à accomplir les

actions qu'ildemande, tels que l'accès à des fichiers, le droit d'écrire, etc. L'autorisation est gérée au moyen de liste ACLou des stratégies.

- **Comptabilité (Accounting)** : Elle permet de collecter des informations sur les utilisateurs et les actions qu'ils accomplissent lorsqu'ils sont connectés aux équipements du réseau.

1.3.5.4 Liste de contrôle d'accès(ACL)

Les administrateurs réseaux doivent trouver le moyen d'interdire l'accès au réseau à certains utilisateurs tout en permettant aux utilisateurs internes d'accéder aux services nécessaires, les routeurs assurent cette fonction à l'aide des listes de contrôle d'accès. Une ACL est un ensemble de conditions qui est appliqué au trafic circulant via une interface du routeur. Elle indique au routeur les types des paquets à accepter ou à rejeter. Les ACLs permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.

1.3.5.5 Proxys

Un proxy, parfois appelé mandataire, c'est un composant logiciel qui se place entre deux autres pour faciliter ou surveiller leurs échanges. Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement internet. Par extension, on appelle aussi proxy un matériel (un serveur par exemple) mis en place pour assurer le fonctionnement de tels services [12].

1.3.5.6 Les réseaux privés virtuel

Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Grace à un principe de tunnel (tunneling) dont chaque extrémité est identifiée, les données transitent après avoir été éventuellement chiffrées. 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. Il faut par contre tenir compte de la toile, dans le sens où aucune qualité de service n'est garantie.

1.3.5.7 Systèmes de détection d'intrusion

Divers raison peuvent conduire un attaquant (pirate) à vouloir s'introduire sur un réseau : défi personnel, espionnage, motivation politique, gain financier ou simplement nuisance. Surveiller le réseau pour détecter les attaques éventuelles relève non

seulement du bon sens mais constitue également un impératif pour n'importe quelle entreprise, D'où l'utilisation des systèmes de détection d'intrusion, ou IDS (Instruction Détection System). Par définition un IDS est le système d'alarme du réseau. Ce dernier à beau être protégé par des moyens divers, seul l'IDS permet de savoir qu'un intrus tente d'y accéder. Les sondes de détection d'intrusion constituent le complément d'un pare-feu. Elles permettent d'analyser les actions ou les flux pour y détecter une tentative d'intrusion. Les IDS peuvent être déployés en plusieurs endroits du réseau afin d'augmenter la sécurité, ils sont généralement de deux types :

- Les N-IDS (Network Based Intrusion Detection System), ils assurent la sécurité au niveau du réseau.
- Les H-IDS (Host Based Intrusion Detection System), ils assurent la sécurité au niveau des hôtes.

1.3.6 La cryptographie

Il existe à l'heure actuelle deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui, repose sur un codage à deux clés, une privée et l'autre publique.

1.3.6.1 La cryptographie symétrique

Le cryptage à clé privée ou symétrique est basé sur une clé partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. L'avantage de la cryptographie symétrique est sa rapidité d'exécution car elle met en œuvre des opérations simples. Les algorithmes développés pour réaliser les opérations de cryptographie sont : DES, 3DES, AES.

1.3.6.2 La cryptographie asymétrique

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par l'utilisateur ; l'autre est publique et donc accessible par tout le monde. Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypte avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Ce cryptage présente l'avantage de permettre la signature numérique des messages et ainsi permettre l'authentification de l'émetteur. Les trois algorithmes à clé publique suivants sont les plus fréquemment employés : RSA, DSA, DH.

1.3.6.3 Les fonctions de hachage

Il s'agit de la troisième grande famille d'algorithmes utilisés en cryptographie. Le principe est qu'un message clair de longueur quelconque doit être transformé en un message de longueur fixe inferieure à celle de départ. Le message réduit portera le nom de Haché ou de Condensé. L'intérêt de ce condensé est de l'utiliser comme empreinte digitale du message original afin que ce dernier soit identifié de manière univoque. Pour cela, on utilise des algorithmes de hachage tels que le MD5 ou encore le SHA.

1.3.6.4 La signature numérique

Le paradigme de signature électronique est un procédé permettant de garantir l'authenticité de l'expéditeur (fonction d'authentification), ainsi que de vérifier l'intégrité du message reçu. La signature électronique assure également une fonction de non-répudiation, c'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message(autrement dit elle empêche l'expéditeur de nier avoir expédié le message).

1.4 Conclusion

Dans ce chapitre, nous avons définit les notions fondamentales dans les réseaux informatiques et les stratégies de sécurité à prendre pour remédier aux attaques. Le prochain chapitre sera consacré aux VPNs.

Chapitre 2

Les réseaux privés virtuels

2.1 Introduction

La confidentialité et la vie privée sur Internet sont régulièrement remises en question, car les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation et cela est dû au chemin emprunté, qui n'est pas défini à l'avance. Ainsi, il est probable que sur le chemin parcouru, le réseau soit écouté par un utilisateur malveillant.

Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation de l'entreprise. La solution d'interconnexion que fournit Internet pour répondre à ce besoin de communication sécurisé, consiste à utiliser les réseaux privés virtuels (VPN), qui sont idéals pour pouvoir exploiter au mieux les capacités du réseau Internet et de relier des sites à l'échelle de la planète en toute sécurité.

Au cours de ce chapitre nous présenterons les principales caractéristiques des VPN, à travers certaines définitions et principes de fonctionnement, les différentes typologies ainsi que les détails sur le protocole IPsec.

2.2 Présentation d'un réseau privé virtuel

2.2.1 Définition

VPN (Virtuel Private Network) est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure. C'est un environnement de communication, dans lequel l'accès est contrôlé, afin de permettre des connexions entre une communauté d'intérêt seulement. Il est construit avec un partitionnement d'un media

de communication commun, qui offre les services de façon non exclusive [18].

2.2.2 Principe de fonctionnement

Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise. Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée comme Internet. Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation [19].

2.2.3 Les fonctionnalités d'un réseau privé virtuel

Un réseau privé, repose sur les principes fondamentaux de la sécurité, en assurant la mise en œuvre de diverses fonctionnalités [20] :

2.2.3.1 Authentification d'utilisateur

Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.

2.2.3.2 Gestion d'adresses

Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.

2.2.3.3 Cryptage des données

Lors de leurs transports sur le réseau public, les données doivent être protégées par un cryptage efficace.

2.2.3.4 Gestion de clés

Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et regénérées.

2.2.3.5 Prise en charge multi-protocole

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

2.2.3.6 Intégrité des données

L'intégrité des données garantit qu'aucune altération ou modification n'a été apportée aux données lors de leurs parcours entre la source et la destination. En général, les réseaux privés virtuels utilisent des fonctions de hachages, qui ressemblent à une somme de contrôle, et garantissent que personne n'a lu le contenu, tout en étant plus robuste.

2.2.4 Type de VPN

ll existe 3 types standards d'utilisation des VPNs selon leur mode d'utilisation [21] :

2.2.4.1 VPN d'accès (Host to Lan)

Un VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas :

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise. La figure 2.1 illustre le VPN poste à site.

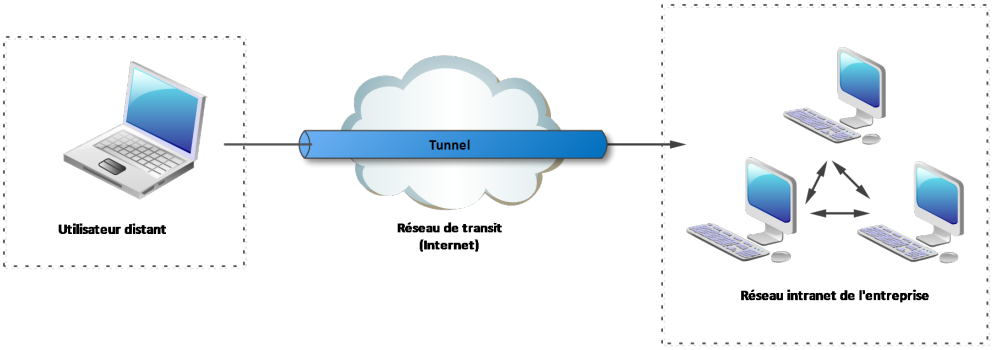

FIGURE 2.1 – VPN poste à site

2.2.5 L'intranet VPN (LAN to LAN)

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux, comme l'illustre la figure 2.1. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et de décryptage ainsi que les limites légales interdisent l'utilisation d'un codage "infaillible". Généralement pour la confidentialité, le codage en lui même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable.

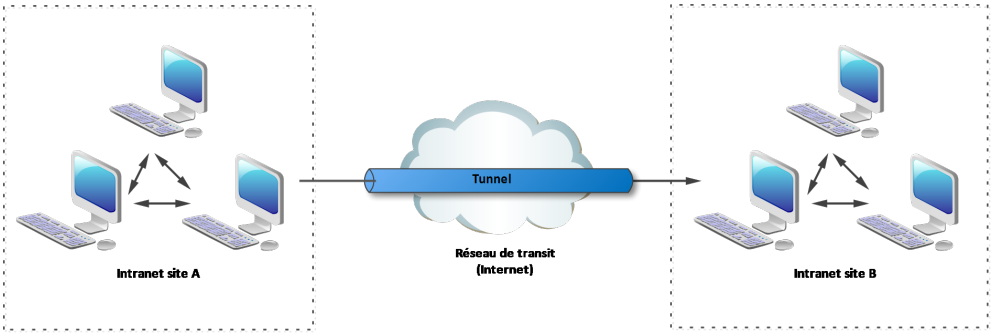

FIGURE 2.2 – VPN site à site

2.2.6 L'extranet VPN (Host to Host)

L'extranet VPN est utilisé pour connecter deux ordinateurs distants entre eux pour des raisons de confidentialité. On crée donc un VPN entre eux, et toutes les données y transmises sont encryptées et compréhensibles que par les deux paires correspondantes. La Figure 2.3 montre un exemple d'un VPN poste à poste.

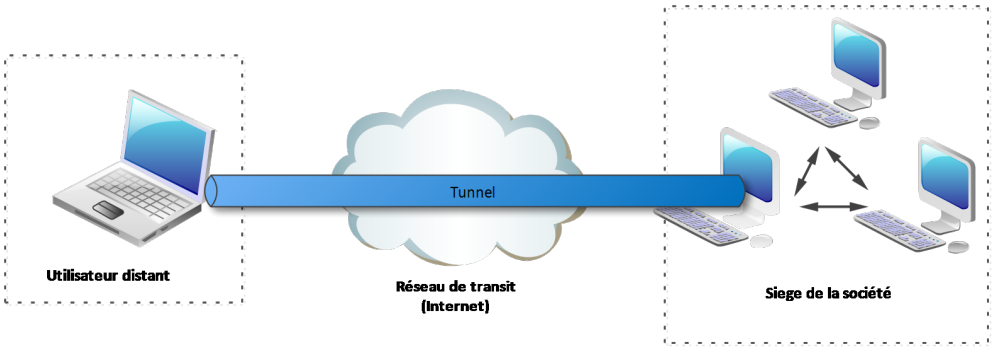

FIGURE 2.3 – VPN poste à poste

2.3 Protocoles utilisée pour réaliser une connexion VPN

Il existe plusieurs protocoles dit de tunnellisation qui permettent la création des réseaux VPN. Les technologies les plus utilisés pour la création de tunnels sécurisés pour tout type de flux sont PPP, PPTP, L2F, L2TP et IPSec [19].

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

C'est un ensemble de protocoles standard garantissant l'interopérabilité des logiciels d'accès distant de divers éditeurs, il permet de transférer des données sur un lien synchrone ou asynchrone, il est full duplex, garantie l'ordre d'arrivée des paquets et encapsule les paquets IP, IPX dans des trames PPP, puis transmet ces paquets encapsulés au travers de liaison point à point [19].

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

PPTP est un protocole réseau permettant un transfert sécurisé entre un client distant et un serveur privé. Ceci est réalisé à l'aide d'un VPN basé sur TCP/IP. La technologie utilisée est une extension du protocole PPP permettant l'accès à distance.

Les différents rôles que le protocole PPTP peut assurer sont listées ci-dessous :

a) permet la création des VPN sur demande sur des réseaux basés sur TCP/IP.

b) peut être utilisé sur un même réseau local entre deux machines.

c) peut être utilisé comme support pour la création de VPN aussi bien Internet que le réseau téléphonique public (PSTN).

d) offre une communication encryptée sûr à travers ces deux réseaux publics.

e) simplifie les accès longues distances pour les utilisateurs distants [19].

2.3.3 L2F (Layer Two Forwarding)

L2F est un protocole de niveau 2, qui permet à un serveur distant de véhiculer le trafic sur PPP et de transférer ces données jusqu'au serveur L2F (routeur). Ce serveur L2F dés-encapsule les paquets et les envoie sur le réseau. Il faut noter que contrairement à PPTP et L2TP, L2F n'a pas besoin de client [22].

2.3.4 L2TP (Layer Two Tunneling Protocol)

Microsoft et Cisco, reconnaissent les mérites des deux protocoles L2F et PPTP, ils se sont associés pour créer le protocole L2TP, qui réunit les avantages de ces deux premiers. L2TP est un protocole réseau qui encapsule des trames PPP pour les envoyer sur des réseaux IP. On utilise souvent ce protocole pour créer des VPN sur Internet. Dans ce cas, il transporte des trames PPP dans des paquets IP. Il sert d'une série de messages L2TP afin d'assurer la maintenance du tunnel et UDP pour envoyer les trames PPP [22].

2.3.5 IPSEC (Internet Protocol Security)

IPSec (Internet Protocol Security) définit par la RFC 2401, est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau du modèle OSI. Il assure la confidentialité (grâce au cryptage), l'authentification (qui permet d'être certain de l'identité de l'émetteur) et l'intégrité des données permettant de s'assurer que personne n'a pu avoir accès aux informations. IPSec permet de protéger les données et également l'en-tête d'une trame, en masquant le plan d'adressage grâce à l'ajout d'un en-tête IPSec à chaque datagramme IP [23].

2.3.5.1 Les protocoles de sécurisation IPsec : AH et ESP

• **Protocole AH (Authentification Header) :** Le protocole AH authentifie l'émetteur des données, contrôle l'intégrité du paquet IP (en-tête et charge utile) et assure le service

anti rejeu. Les traitements associés utilisent des algorithmes de ''hachage'' tels que Message Digeste(MD5) ou Secure Hash Algorithm (SHA-1, SHA-256, etc.).Un algorithme de hachage est associé à une clé issue de la méthode d'authentification choisie pour constituer un Hash de base Message authentification Code (HMAC). L'entête AH est inséré à la suite de l'entête IP pour garantir l'intégrité et l'authentification des données. Se protège ainsi contre toute altération du paquet lors de son transit [19]. La Figure 2.4 illustre l'en-tête AH.

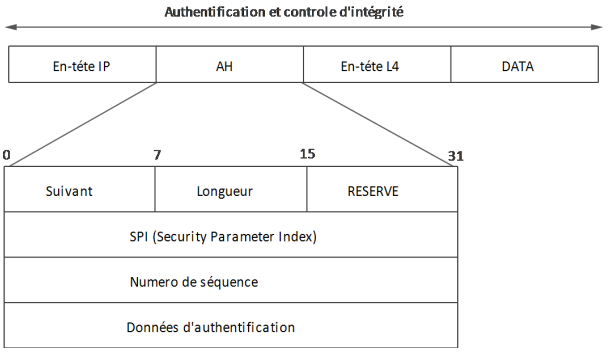

FIGURE 2.4 – En-tête AH

• **Protocol ESP (Encapsulating Security Payload) :** Le protocole ESP assure la confidentialité et l'authentification grâce au chiffrement de paquet IP tel que sa fonction masque les données et l'identité de leurs sources et leurs destinations. Ce protocole authentifie le paquet IP interne et l'en-tête ESP. L'authentification permet d'identifier la source des données et garantir leur intégrité [19]. La Figure 2.5 illustre l'en-tête ESP.

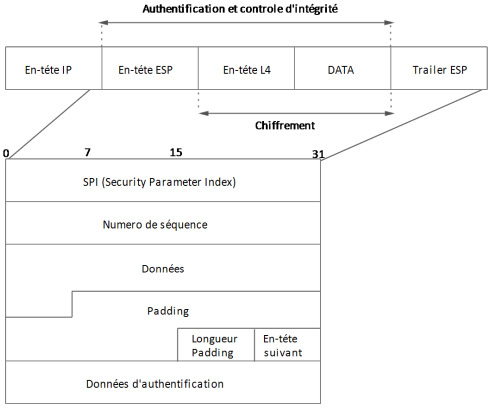

FIGURE 2.5 – En-tête ESP

2.3.5.2 Modes d'IPSec

Il existe deux modes d'utilisation d'IPSec : le mode transport et le mode tunnel. La génération des datagrammes sera différente selon le mode utilise [24] :

• **Mode transport** : Ce mode est utilisé pour créer une communication entre deux hôtes qui supportent IPSec. Une SA(Security Association) est établie entre les deux hôtes. Les entêtes IP ne sont pas modifiées et les protocoles AH et ESP sont intégrés entre cette entête et l'entête du protocole transporté. Ce mode est souvent utiliser pour sécuriser une connexion Point-To-Point. La Figure 2.6 montre l'en-tête IPSec en mode transport.

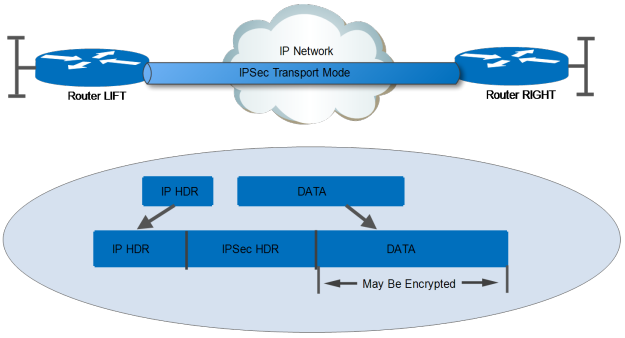

FIGURE 2.6 – En-tête IPSec en Mode Transport.

• **Mode Tunnel** : Ce mode est utilisé pour encapsuler les datagrammes IP dans IPSec. La SA est appliquée sur un tunnel IP. Ainsi, les entêtes IP originales ne sont pas modifiés et un entête propre à IPSec est créé. Ce mode est souvent utilisé pour créer des tunnels entre les réseaux LAN distant. Effectivement, il permet de relier deux passerelles étant capables d'utiliser IPSec sans perturber le trafic IP des machines du réseau qui ne sont donc pas forcément prêtes à utiliser le protocole IPSec. La Figure 2.7 montre l'en-tête IPSec en mode tunnel.

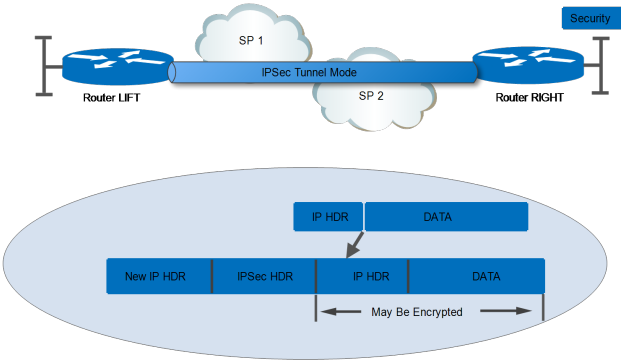

FIGURE 2.7 – En-tête IPSec en Mode Tunnel

2.3.5.3 Détails du protocole

Le mécanisme interne d'IPSec est complexe. Le fait que ce protocole soit hautement configurable introduit des notions de gestion et configuration inconnues du monde IP.

2.3.5.4 Gestion des flux IPSec

Les flux IPSec sont gérés unidirectionnellement. Ainsi, une communication bidirectionnelle entre deux machines utilisant IPSec sera définie par divers processus pour chacun des sens de communication. Les procédés détaillés ci-dessous respectent les lois suivantes [25] :

a) Security Policy : Une SP défini ce qui doit être traité sur un flux, et comment nous voulons transformer un paquet. Il y sera indiqué pour un flux donné :

- Les adresses IP de l'émetteur et du récepteur (unicast, multicast ou broadcast) ;
- Par quel protocole il devra être traité (AH ou ESP) ;
- Le mode IPSec à utiliser (tunnel ou transport) ;
- Le sens de la liaison (entrante ou sortante) ;

Notons qu'une SP ne définit qu'un protocole de traitement à la fois. Pour utiliser AH et ESP sur une communication, deux SP devront être créée.

b) Security Association : Une SA défini comment sera traité le paquet en fonction de sa SP associée. Elles ne sont que la "réalisation" des SP. Elle possède l'ensemble des propriétés de la liaison. Ainsi, elle sera représentée par une structure de donnée contenant les informations suivantes :

- Un compteur permettant de générer les numéros de séquence des entêtes AH et ESP.
- Un flag (drapeau) permettant d'avertir qu'en cas de dépassement du compteur précédemment décrit, on doit interrompre la communication.
- Une fenêtre d'anti répétition dans laquelle doit tomber le prochain numéro de séquence.
- Information sur l'AH : algorithme d'authentification, clefs, durée de vie, etc.
- Information sur l'ESP : algorithme d'authentification et de chiffrement, clefs, etc.
- Mode IPSec : tunnel ou transport.
- Durée de vie de la SA.

Une SA est identifiée à un seul et unique flux unidirectionnel grâce à trois champs :

- L'adresse IP de destination (unicast, multicast ou broadcast).
- Le protocole utilisé, AH ou ESP.
- Le SPI (Security Parameter Index).

* **LE SPI** : est un indice (ou ID) sur 32 bits attribué au SA lors de sa création. Nous verrons plus loin que sa génération dépendra du mode de gestion des clés de sessions. Il sert à distinguer les différentes SA qui aboutissent à une même destination et utilisant le même protocole.

c) Bases de données SPD et SAD : Tout système implémentant IPSec possède donc 2 bases de données distinctes dans lesquelles il stocke son SP (ici, SPDatabase) et son SA (ici, SADatabase).

*** La SPD (Security Policy Database)** : est la base de configuration de IPSec. Elle permet de dire au noyau quel paquet IP doit traiter. C'est à sa charge de savoir avec quel SA fait-il le traitement.

*** La SAD (Security Association Database)** : stocke les SA afin de savoir comment traiter les paquets arrivant ou partant. Elles sont identifiées par les triplets :

- Adresse de destination des paquets ;
- Identifiant du protocole AH ou ESP utilisé ;
- Un index des paramètres de sécurité (Security parameter index) qui est un champ de 32 bits envoyé en clair dans les paquets.

2.3.5.5 principes et fonctionnement d'IPsec

Etant donné un trafic qui doit être chiffré avec un protocole, un autre avec un autre protocole et un dernier ne devant pas être chiffré, comment ce trafic est-il effectivement traité ? Lorsque les paquets arrivent (figure 2.8) entre la couche de transport et la couche réseau, le noyau vérifie tout d'abord si ce trafic doit subir un traitement IPSec ou non en fonction de différents champs contenus, entre autre, dans l'en-tête IP. Pour cela, le noyau cherche une politique de sécurité correspondant au paquet, dans une base de politique (SPD) préalablement configurée par l'administrateur. La SPD permet de savoir si un type de trafic doit subir un traitement IPSec ou pas. Si ce n'est pas le cas, le paquet sera envoyé en clair.

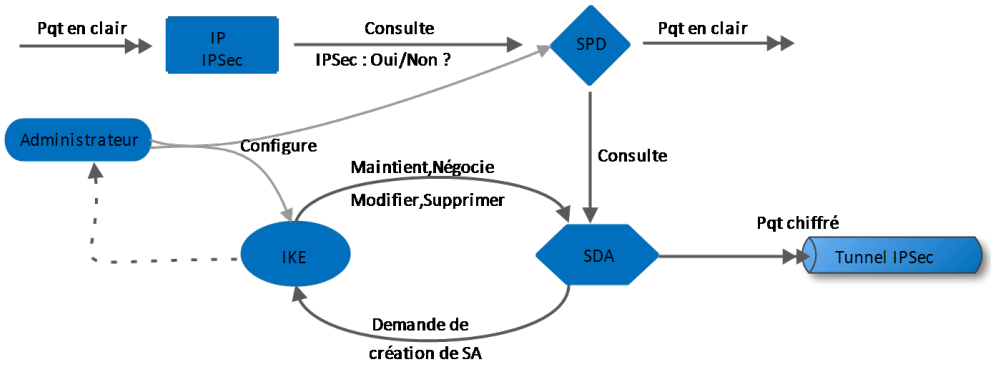

FIGURE 2.8 – Fonctionnement IPSec.

Si c'est le cas, il faut à présent savoir à quel type de tunnel il correspond. Le type (tunnel, Transport, ESP, AH) est également stocké dans la SPD. Une base de données de SA(SAD) est maintenue en temps réel et contient l'ensemble des SAs des politiques IPSec actives. Dans le cas où le noyau trouve une SA correspondante, il va lire les paramètres nécessaires (protocole à utiliser, taille des clés, etc.) et traiter le paquet en conséquence (ESP ou AH, Tunnel ou transport) avant de l'envoyer. Dans le cas contraire IPSec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises. Durant cette négociation, l'ensemble des paquets devant subir un traitement IPSec à destination de cet hôte sont ignorés. Ceci explique le temps de latence lors de la première communication à travers un tunnel IPSec [26].

2.3.5.6 Gestion des clés

Les protocoles sécurisés ont recours à des algorithmes de cryptage, et ont donc besoin de clefs. Un des problèmes principal dans ce cas est la gestion de ces clefs. Par gestion, on entend la génération, le stockage et la suppression de ces clefs. Ces différentes tâches sont évolués à des protocoles spécifiques de gestion de ces clefs à savoir [19,21] :

a) ISAKMP (Internet Security Association and Key Management Protocol) : ISAKMP présente un mécanisme d'authentification et d'échange de clés et des algorithmes de chiffrement, il est possible de l'utiliser pour des protocoles différents. Il comporte trois aspects principaux :

- Il définit une façon de procéder, en deux étapes appelées phase 1 et phase 2 : dans la première, un certain nombre de paramètres de sécurité propres à ISAKMP sont mis en place, afin d'établir entre les deux tiers un canal protéger ; dans un second temps, ce canal est utilisé pour négocier les associations de sécurité pour les mécanismes de sécurité que l'on souhaite utiliser (AH et ESP par exemple).

- Il définit des formats de messages, par l'intermédiaire de blocs ayant chacun un rôle précis et permettant de former des messages clairs.

- Il présente un certain nombre d'échanges types, composes de tels messages, qui permettent des négociations présentant des propriétés différentes : protection ou non de l'identité, perfect forward secrecy.

b) IKE (Internet Key Exchange) : IKE utilise ISAKMP, pour construire un protocole pratique. Il comprend les modes suivants [21] :

- **Phase 1 : Main Mode et Aggressive Mode** : Les attributs suivants sont utilisés par IKE et négociés durant la phase 1 : un algorithme de chiffrement, une fonction de hachage, une méthode d'authentification et un groupe pour Diffie-Hellman.

  Trois clefs sont générées à l'issue de la phase 1 : une pour le chiffrement, une pour l'authentification et une pour la dérivation d'autres clefs. Ces clefs dépendent des cookies, des aléas échangés et des valeurs publiques Diffie-Hellman ou du secret partagé préalable. Leur calcul fait intervenir la fonction de hachage choisie pour la SA ISAKMP et dépend du mode d'authentification choisi.

- **Phase 2 : Quick Mode** : Les messages échangés durant la phase 2 sont protégés en authenticité et en confidentialité grâce aux éléments négociés durant la phase 1. L'authenticité des messages est assurée par l'ajout d'un bloc HASH après l'en-tête ISAKMP, et la confidentialité est assurée par le chiffrement de l'ensemble des blocs du message.

  Quick Mode est utilisé pour la négociation de SA pour des protocoles de sécurité donnés comme IPsec. Chaque négociation aboutit en fait à deux SA, une dans chaque sens de la communication. Durant cette phase, il s'agit de :

  - Négocier les paramètres IPSec.

  - Générer une nouvelle clef dérivée de celle négociée en phase 1 grâce au protocole Diffie-Hellman. (Si on prend on compte les mécanismes de sécurisation des échanges tels que PFS Perfect Forward Secrecy, ou le Back trafic Protection, il peut y avoir d'autres échanges tels qu'une nouvelle négociation Diffie-Hellman..).

  - Identifier le trafic que les SA négociées protégeront.

le schéma de la Figure 2.9 résume la procédure précédente

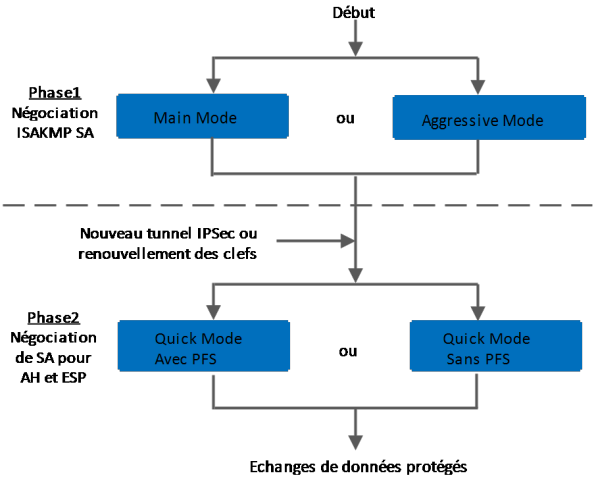

FIGURE 2.9 – Echanges de données protégées

Puisque IPSEC est embarqué par défaut dans IPv6, c'est forcément un protocole d'avenir et déjà du présent. On voit poindre la complexité supérieure que cela engendre pour les échanges entre deux postes. C'est également cette complexité qui assure une meilleure gestion du trafic et de sa sécurité.

Du point de vue des VPN, on voit tout de suite l'impact que peut avoir IPSec. En effet, on n'inclut plus la couche de chiffrement à un niveau supérieure, mais directement dans IP. Il en va de même pour la liaison entre deux hôtes, c'est donc une avancée non négligeable et cela explique pourquoi, aujourd'hui, IPSec est très employé dans la gestion des VPNs.

2.4 Conclusion

Tout au long de ce chapitre, nous avons effectué une présentation des réseaux privés virtuels (VPNs) ainsi que les protocoles utilisés pour les réaliser. Le chapitre suivant, quant à lui, sera consacré à l'étude de l'architecture réseau de l'université de Bejaïa.

Chapitre 3

Etude de l'architecture existante et proposition de solutions

3.1 Introduction

Dans ce chapitre, nous commencerons par une présentation globale du réseau Intranet de l'université, nous expliquerons comment se fait le routage inter-LAN et la commutation entre les zones et les différents blocs de chaque zone, ensuite nous essayerons de voir les points faibles du réseau et donné des suggestions afin d'amélioré sa sécurité et de rendre le trafic plus efficace, enfin nous présenterons l'architecture améliorée du réseau de l'université.

3.2 Présentation globale du réseau Intranet

Le réseau informatique de l'université de Bejaia est constitué de quatre zones, sa topologie physique est en étoile étendue (voir figure 3.1), chaque zone à l'architecture d'un arbre, et qui est connectée au backbone (zone 1).

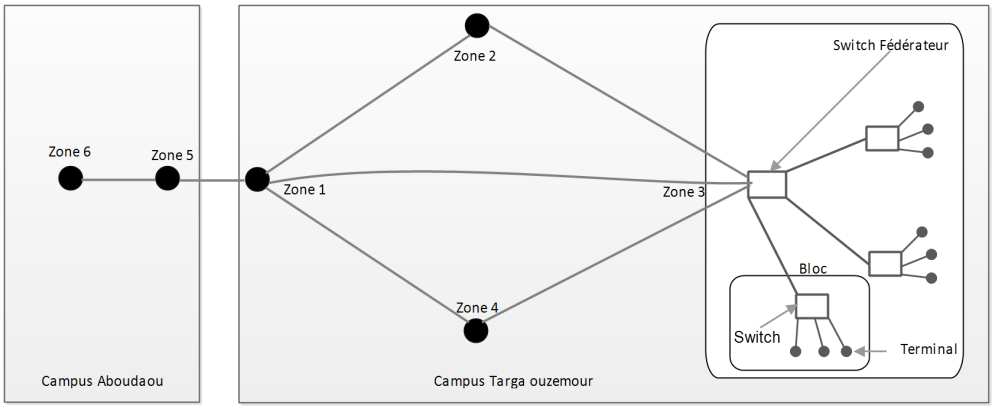

FIGURE 3.1 – La topologie physique du réseau local.

Le choix de la zone 1 comme étant le backbone (épine dorsale en anglais) est justifié par le fait de la présence du centre de calcul qui héberge la salle des administrateurs ainsi que tous les serveurs du réseau local. Tandis que, le campus ABOUDAOU est connecté directement au backbone via une fibre optique.

Chaque zone regroupe des blocs proches les uns des autres en termes physique, en d'autres termes, constitués de blocs avoisinants et ce de la manière suivante :

Zone 1 :

1. Centre de calcul.
2. Bloc 01.
3. Bloc 11 chimie industrielle.
4. Vice rectorat.
5. Faculté de technologie.

Zone 2 :

6. Génie des procédés.
7. Nouvelle bibliothèque (informatique).
8. Nouvelle bibliothèque 250 place.
9. Bloc enseignant.
10. Auditorium.

Zone 3 :

11. Bloc 05.
12. Faculté des sciences exactes.
13. Hall de technologie.
14. Centre culturel et CNAS.
15. Labo de recherche.
16. Moyen généraux.
17. Rectorat.

18. Bibliothèque centrale.

Zone 4 :

19. Bloc 10 Labo électronique.
20. Bloc 12.
21. Bloc 9.
22. Département de biologie.
23. Faculté des sciences naturelle et vie.
24. Haut tension.

Zone 5 :

25. Bloc 02.
26. Bloc 03.
27. Bloc 07.
28. Bibliothèque central.

Zone 06 :

29. Bibliothèque 750.
30. Bibliothèque 250.
31. Bloc enseignement 01.
32. Bloc enseignement 02.

Tout cela est illustré par le schéma de la figure 3.2 :

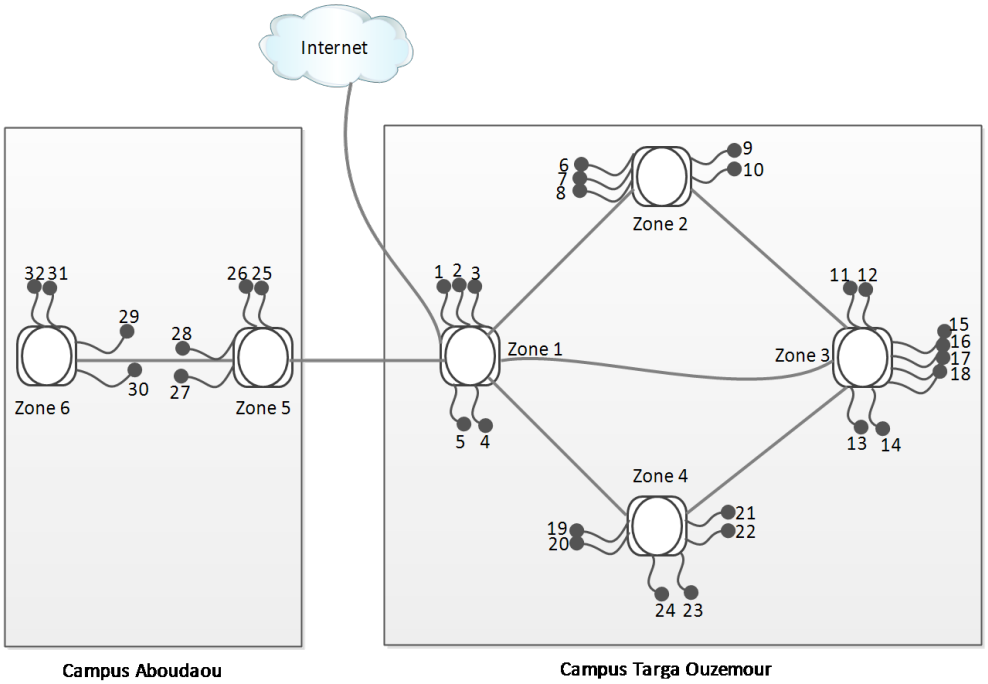

FIGURE 3.2 – Description des zones constituant le réseau Intranet de l'université.

3.3 Description détaillée des Zones

Dans cette partie nous allons décrire les zones :

3.3.1 Description du backbone (Zone 1)

La zone 1 est le backbone du réseau, elle permet la connexion en amont vers l'extérieur car c'est à ce niveau que se trouve le routeur, on trouve aussi le pare-feu qui se charge de filtrer les paquets entrants. Ce système de pare-feu permet aussi le routage inter-LAN car l'une de ces interfaces est reliée directement à un switch fédérateur et que ce dernier offre une liaison vers la zone 3, un autre vers la zone 2, un autre vers la zone 4 et ces deux dernières zones sont reliées à leur tour à la zone 3, comme l'illustre la figure 3.3.

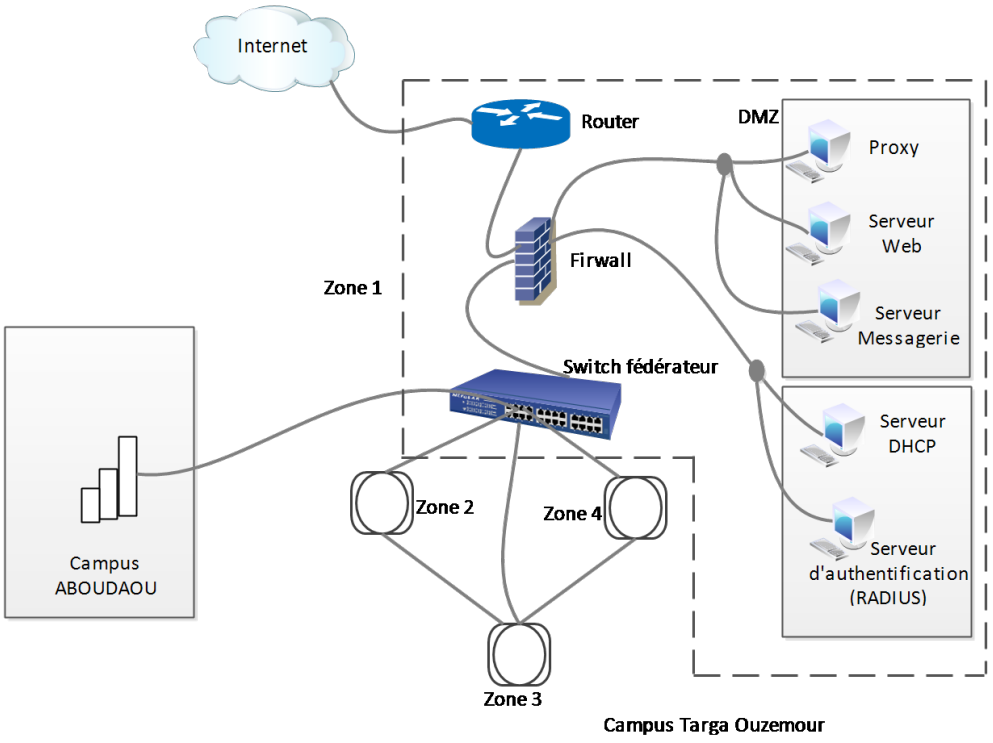

FIGURE 3.3 – Description de la Zone 1 (backbone).

L'autre interface du pare-feu donne sur une zone qui héberge les serveurs du réseau Intranet tel que : le serveur Web, le serveur DHCP, le serveur Mail, le serveur proxy ou encore le serveur d'authentification (RADIUS).

3.3.2 Description D'une zone

Chaque zone s'appuie sur un modèle en couches car ce dernier a beaucoup d'avantages tels que :

- La hiérarchisation, c'est-à-dire que le rôle de chaque couche est précis et spécifique.

- L'évolution, les zones sont constituées de blocs, l'évolution est alors plus facile à planifier et à gérer.

- La gestion, car c'est facile de gérer une zone à cause de sa structure en couches.

Le schéma ci-après (figure 3.4) décrit la structure en couches, on y distingue :

• Les Terminaux, qui sont des postes, des stations ou des imprimantes réseau par exemple.

• La couche d'accès, c'est le point d'entrée des postes clients ou des serveurs sur le réseau. C'est dans ce rang qui sont définit tous les services de niveau 2, tel que l'appartenance à un Vlan.

• La couche de distribution (Switch fédérateur), c'est à ce niveau que le routage et le filtrage sont accomplis.

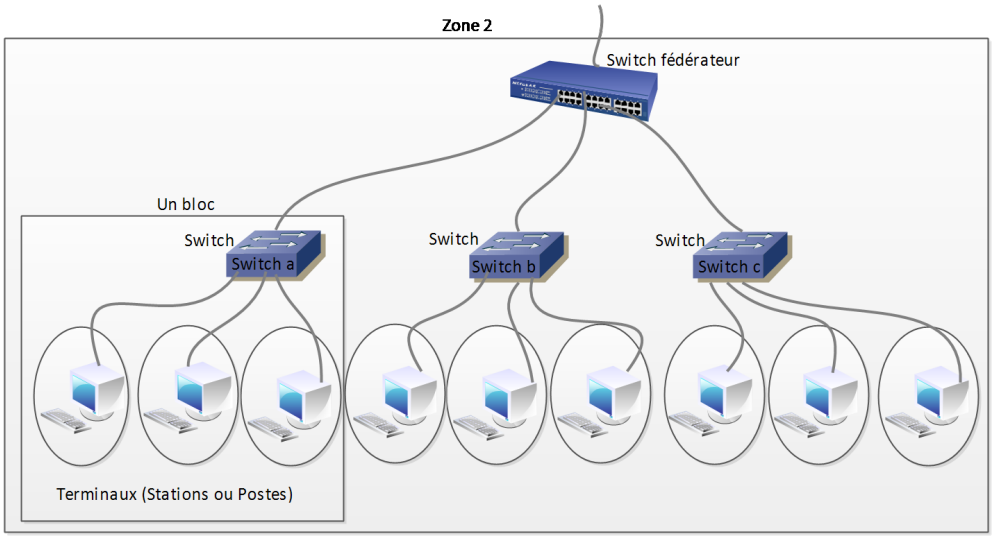

FIGURE 3.4 – Description d'une zone.

3.4 Critique et suggestion sur le réseau

3.4.1 IDS/IPS

La présence d'un système de Détection et Prévention d' Intrusions (N-IDS/IPS) se fait désirer afin de détecter et de prévenir des actes malveillants ou anormales sur les principaux liens du réseau à savoir du LAN vers la DMZ ou l'extérieur ainsi que de l'extérieur vers la DMZ. La mise en place de l'N-IDS/IPS comme un module dans le firewall le surcharge encore plus, donc il est nécessaire de le mettre comme un module à part pour alléger la charge sur le firewall.

3.4.2 Serveur d'Antivirus

Il faut noter que le firewall ne protège pas très bien des virus. Beaucoup de manières permettent de coder des fichiers pour les transférer. En d'autres termes, un firewall ne peut pas remplacer l'attention et la conscience des utilisateurs qui doivent respecter un certain nombre de règles pour éviter les problèmes. La toute première étant bien évidemment de ne jamais ouvrir un fichier attaché à un mail (ou autre) sans être très sûr de sa provenance. Mais dans un réseau comme le nôtre (de l'université), avec un effectif de plus en plus croissant et donc varié, il est très difficile de faire respecter ce genre de règles. Les virus quant à eux passent aussi très facilement par des supports de stockage, et ces derniers (virus sur support de stockage) sont beaucoup plus importants que ceux sur Internet.

Il faut alors prendre des mesures globales et importantes contre les virus. Avant de les traquer à l'entrée du réseau, il faut s'assurer que chaque poste de travail dispose d'un antivirus à jour. Et surtout mettre en place un serveur d'antivirus qui est un pas en avant dans la lutte antivirus et anti-spams. En effet, avec l'installation du logiciel serveur antivirus , on peut bloquer les messages infectés de virus ou indésirables sur le serveur avant qu'ils ne parviennent sur la machine des utilisateurs finals. Une notification est envoyée à l'administrateur du réseau et au destinataire chaque fois qu'un message a été bloqué.

3.4.3 les liaisons

Si on apparente un réseau à un graphe, une meilleure tolérance aux fautes est obtenue avec un graphe complet, ce qui correspond à une topologie en "maille" du réseau.

Dans ce type de réseau, chaque point ou nœud (sommet) est relié à tous les autres nœuds du réseau. Si une liaison est défaillante, il est toujours possible d'accéder à un nœud à partir d'un autre, et par un autre chemin qui est le cas dans notre réseau actuel

(Figure 3.5), mais il est tout de même possible d'ajouter une nouvelle liaison entre la zone 2 et la zone 4 pour une meilleure tolérance aux fautes (Figure 3.6).

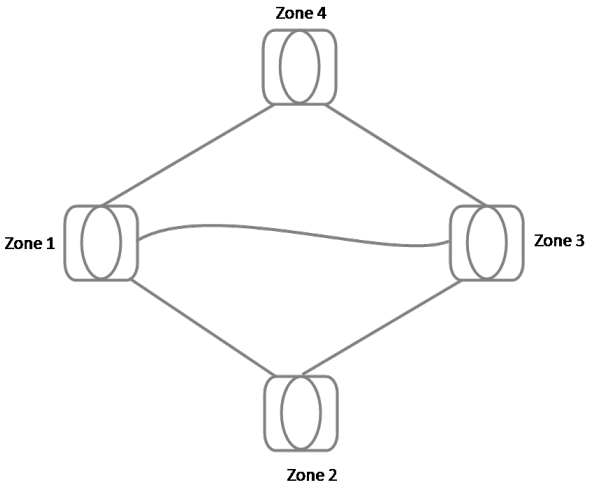

FIGURE 3.5 – Graphe Représentant le Réseau Actuel.

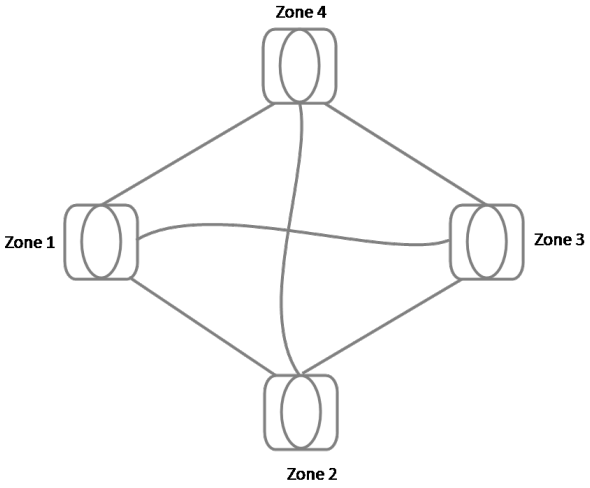

FIGURE 3.6 – Réseau ou Graphe Complet.

3.4.4 VPN site à site

La séparation du réseau des deux campus devient une nécessité primordiale et cela, vu le nombre de poste qui est de plus en plus croissant, il est donc nécessaire d'ajouter une nouvelle ligne spécialisée vers le campus ABOUDAOU pour permettre au réseau d'être moins surchargé, et relier les deux réseaux, qui évolueront désormais indépendamment, par un tunnel sécurisé (VPN), la mise en place d'un VPN site à site assure les propriétés de sécurité ainsi que la confidentialité et l'authentification.

3.4.5 VPN pour les accès distants

Ce type de VPN peut être utilisé pour accéder à certaines ressources prédéfinies de l'université sans y être physiquement présent. Cette opportunité peut ainsi être très utile aux enseignants ou aux cadres qui souhaitent se connecter au réseau de l'université pour divers raisons. En général, l'utilisateur de ce type de VPN possède un accès Internet chez un fournisseur d'accès standard (ISP).

Dans le cas de l'université de Bejaïa la solution VPN n'existe pas alors il faut mettre en œuvre un VPN pour les accès distants.

3.5 Architecture proposée

Après ces quelques critiques et suggestions sur le réseau actuel, nous proposons la nouvelle architecture qui est représentée dans la figure 3.7.

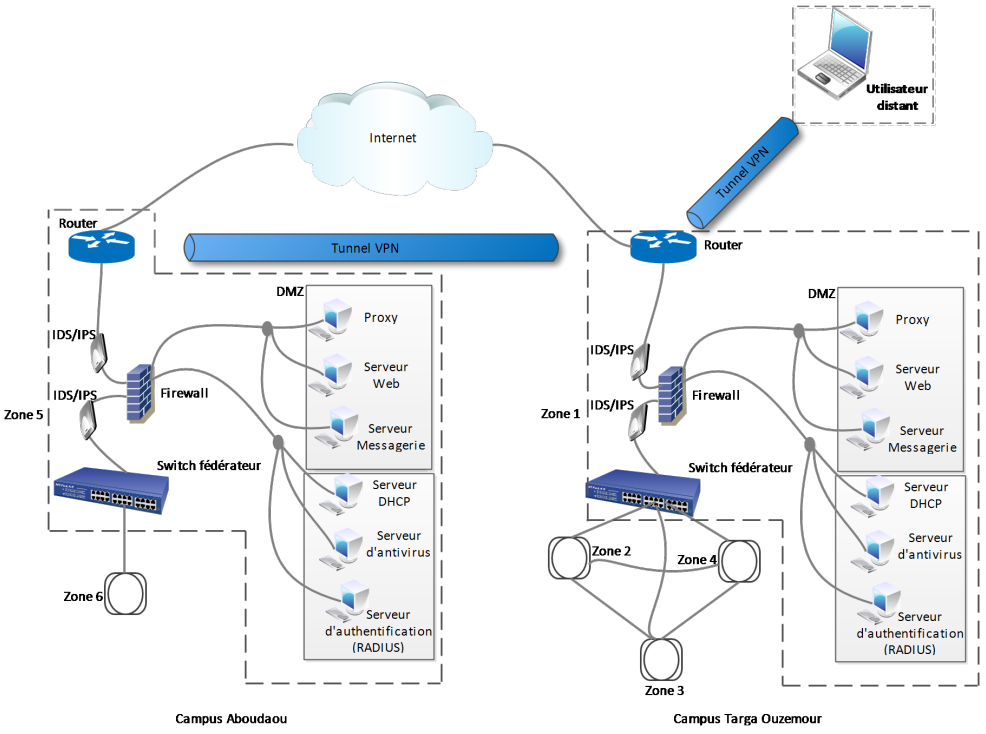

FIGURE 3.7 – Schéma de la Nouvelle Architecture Possible.

3.6 Conclusion

Cette étude du réseau de l'université nous a permis de comprendre l'architecture de notre réseau et de matérialiser tout ce qu'on a eu à étudier jusque-là, en effet grâce à cette étude nous avons pu critiquer cette architecture, suggérer quelques solutions et proposer une nouvelle architecture pour le réseau. Cette nouvelle architecture demande certes plus d'investissement financier mais offre sans doute une meilleure sécurité et une meilleure souplesse pour le réseau.

CHAPITRE 4

Mise en oeuvre des VPNs

4.1 Introduction

La mise en œuvre des VPNs est l'une des solutions à laquelle nous avons abouti après la concrétisation de notre étude dans le chapitre précèdent.

Dans ce chapitre nous décrirons les outils utilisés et les principales étapes de configuration pour mettre en œuvre un VPN site à site et un VPN d'accès.

4.2 Description de l'environnement de travail

4.2.1 GNS3(2.1.0)

a) Définition

GNS3 signifie Graphical Network Simulator, est un simulateur graphique de réseau qui permet l'émulation de réseaux complexe. Il est utilisé pour reproduire différentes systèmes d'exploitation dans un environnement virtuel. Il permet l'émulation en exécutant un IOS Cisco (Internetwork Operating Systems).

b) Les composants du logiciel

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à [27] :

- Dynamips : Emulateur d'IOS Cisco.

- Dynagen : Interface écrite en python et permettant l'interconnexion de plusieurs machines émulées.

- Qemu : Emulateur de système.

- Virtualbox : Logiciel permettant la création de machines virtuelles.

- Wireschark : est un logiciel pour analyser les trames.

Grâce à ces composants, GNS3 nous permet :

- Le design de topologies réseaux de haute qualité et complexes.

- Emulation de plusieurs plate-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 Wireschark.

4.2.2 PFSENSE

a) Définition

Pfsense est un logiciel open source tournant sous FreeBSD. Il possède les fonctionnalités d'un pare-feu mais également d'un routeur. Il permet d'intégrer également de nouveaux services tels que l'intégration d'un portail captif, la mise en place d'un VPN, et bien d'autres.

b) Fonctionalité

Pfsense est :

- Un fournisseur de services tel que :

• Serveur de temps : NTPD ;

• Relais DNS ;

• Serveur DHCP ;

• Portail captif de connexion.

- Un routeur entre un WAN et un LAN, différents segments, VLANs, DMZs :

• il implémente les protocoles RIP, OLSR, BGP ;

• il permet de mettre en place des VPNS : OpenVPN,IPsec, PPTP.

- Un firewall capable de :

• faire de la traduction d'adresses : NAT, SNAT, DNAT ;

• faire du filtrage de paquets entre WAN et LAN et entre deux réseaux reliés par VPN ;

• faire de la QoS : « traffic shaper » ;

• faire du « load balanching » avec plusieurs connexions Internet.

4.3 Mise en place d'un VPN site à site

4.3.1 Architecture

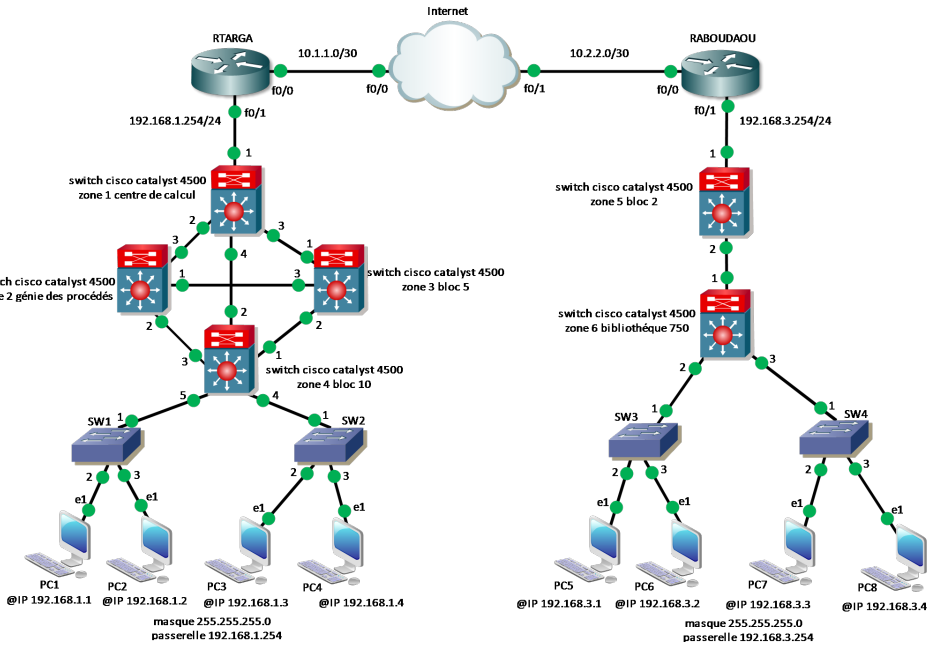

FIGURE 4.1 – La topologie réseau étendu université de Bejaia

La nouvelle architecture proposé dispose de deux sites, notre topologie illustre leurs interconnexion via un tunnel VPN. Pour cela, il faudrait définir une clef partagée, une association de sécurité, une fonction de hachage ... Ainsi, cette solution permettra aux sites RTARGA et RABOUDAOU d'échanger des données en passant par Internet d'une façon sécurisée en utilisant le tunnel VPN.

Nous choisirons pour les deux sites les même clefs de chiffrement, le type de hachage, la taille de police, la longueur des clés, la durée de vie de clé avant renégociation, la méthode de cryptage des données, la durée de vie de la clé de cryptage, une ACL permettant d'identifier le trafic à traiter par le tunnel et enfin la création d'une crypto-map.

4.3.2 Exigences IPSec VPN

Pour accomplir ce projet, il faut diviser le travail en deux étapes qui sont nécessaires pour obtenir le tunnel VPN IPSec. Ces étapes sont les suivantes :

- Configuration ISAKMP (phase 1 ISAKMP).
- Configuration IPSec (phase 2 ISAKMP, ACL, crypto map).

4.3.2.1 Configuration ISAKMP

IKE n'existe que pour établir une SA pour IPSec. Il doit d'abord négocier cette SA (une SA ISAKMP) : les relations avec les routeurs des sites distants.

Maintenant, nous allons commencer à travailler sur le site de Targa Ouzemour (RTARGA).

- La première étape consiste à configurer la politique de sécurité ISAKMP :

```
RTARGA(config)#crypto isakmp policy 7
RTARGA(config-isakmp)#authentication pre-share
RTARGA(config-isakmp)#encryption aes 128
RTARGA(config-isakmp)#group 2
RTARGA(config-isakmp)#hash sha
RTARGA(config-isakmp)#lifetime 100
RTARGA(config-isakmp)#exit
RTARGA(config)#
```

Description des commandes ci-dessus :

- AES : est un procédé de cryptage utilisé pour la phase 1.

- Sha : l'algorithme de hachage.

- Pre-share : utilisation d'une clé pré-partagée comme méthode d'authentification.

- Group : l'algorithme d'échange de clef Diffie-Hellman est utilisé.

- lifetime : Spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs.

la deuxième étape consiste à configurer la clef à l'aide de la commande suivante :

```
RTARGA(config)#crypto isakmp key 0 vpnkey address 10.2.2.1 no-xauth
RTARGA(config)#
```

A chaque fois que RTARGA tentera d'établir un tunnel VPN avec RABOUDAOU, cette clé partagée (vpnkey) sera utilisée.

4.3.2.2 Configuration IPSec

Pour configurer le protocole IPSec on a besoin de configurer les éléments suivants :

- Créer l'IPSec Transform.
- Créer un ACL étendue.
- Créer le crypto map.
- Appliquer crypto map à l'interface publique.

Cette étape consiste à créer la transformation définie utilisée pour protéger les données (IPSec) nommé ''vpntrans".

```
RTARGA(config)#crypto ipsec transform-set vpntrans esp-aes 128 esp-sha-hmac
RTARGA(cfg-crypto-trans)#
```

L'ACL étendu que l'on crée permettra de définir le trafic qui passera à travers le tunnel VPN. Dans notre projet, le trafic s'achemine du réseau 192.168.1.0/24 à 192.168.3.0/24.

```
RTARGA(config)#ip access-list extended vpn-acl
RTARGA(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
RTARGA(config-ext-nacl)#
```

La crypto map est la dernière étape d'installation et d'établissement du lien entre ISAKMP définie précédemment et la configuration IPSEC :

```
RTARGA(config)#crypto map vpn-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
RTARGA(config-crypto-map)#set peer 10.2.2.1
RTARGA(config-crypto-map)#match address vpn-acl
RTARGA(config-crypto-map)#set transform-set vpntrans
RTARGA(config-crypto-map)#
```

Maintenant il suffit d'appliquer la crypto map sur l'interface de sortie de routeur :

```
RTARGA(config)#interface f0/0
RTARGA(config-if)#crypto map vpn-map
RTARGA(config-if)#
```

Dès que nous appliquons crypto map sur l'interface, nous recevons un message de router qui confirme ISAKMP : ISAKMP is ON.

```
*Mar  1 00:24:25.535: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Les paramètres pour RABOUDAOU sont identiques, la seule différence étant les adresses IP attribuées et les listes d'accès.

4.3.3 Démonstration

Ping de RTARGA vers RABOUDAOU

```
RTARGA#ping 192.168.3.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/164/180 ms
RTARGA#
```

Vérifions les informations retournées par le VPN sur RTARGA

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


RTARGA#
```

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

La vérification de la MAP VPN

```
RTARGA#show crypto map
Crypto Map "vpn-map" 10 ipsec-isakmp
        Peer = 10.2.2.1
        Extended IP access list vpn-acl
            access-list vpn-acl permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
        Current peer: 10.2.2.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                vpntrans,
        }
        Interfaces using crypto map vpn-map:
                FastEthernet0/0
```

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

On vérifie les opérations d'IPsec

```
RTARGA#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: vpn-map, local addr 10.1.1.1

   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): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x6927D7AB(1764218795)

     inbound esp sas:
      spi: 0xF99DF33A(4187878202)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, crypto map: vpn-map
        sa timing: remaining key lifetime (k/sec): (4607218/3569)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6927D7AB(1764218795)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: SW:2, crypto map: vpn-map
        sa timing: remaining key lifetime (k/sec): (4607218/3555)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
```

Crypto IPSec permet d'afficher l'interface de sortie (10.1.1.1) et l'interface d'entré (10.2.2.1), les ACLs qui autorise l'accès entre TARGA et ABOUDAOU avec le masque et le numéro de port, le nombre de paquets envoyés et reçus sont égaux et le mécanisme utilisé est ESP.

Pour finir, on vérifie les opérations d'isakmp

```
RTARGA#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.2.2.1        10.1.1.1        QM_IDLE           1001    0 ACTIVE

IPv6 Crypto ISAKMP SA

RTARGA#
```

Pour voir ce qui se passe sur notre architecture on utilise le logiciel wireshark dans GNS3, pour cela on fait un clic-droit sur le lien que nous voulons analyser et cliquer sur ''Start capturing ''(voir Figure 4.2) :

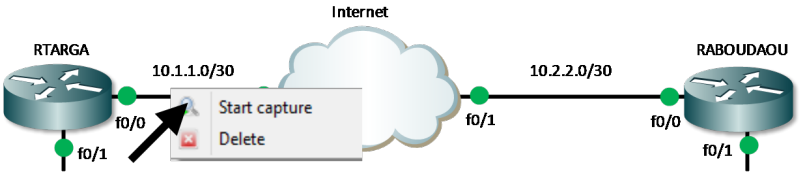

FIGURE 4.2 – Debut de capture.

Nous devons ensuite choisir dans la liste proposée (voir Figure 4.3) l'interface que nous souhaitons analyser. Une fois choisie, dans la partie ''Capture" de GNS3 apparaît notre première capture, on fait un clic-droit dessus pour lancer wireshark, on peut ainsi analyser le trafic sur cette interface :

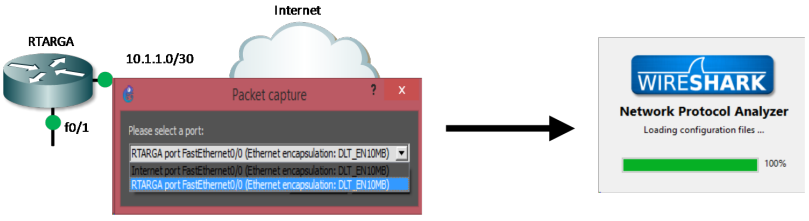

FIGURE 4.3 – Choix d'interface a annalysé.

Les données passent à travers le tunnel VPN IPSec précédemment crée et elles sont cryptées :

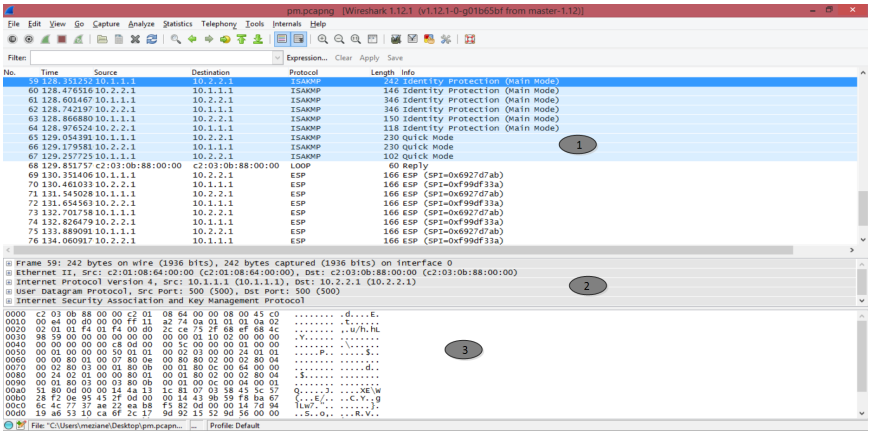

FIGURE 4.4 – Les données cryptés au niveau du tunnel.

- Le volet 1 : permet de recenser l'ensemble des paquets capturés. Sans spécifiés l'émetteur de la trame, le destinataire de la trame et le protocole réseau mis en œuvre.

- Le volet 2 : permet de visualiser la pile des protocoles employés dans le paquet sélectionné dans le premier volet.

- Le volet 3 : permet de visualiser l'ensemble du paquet capturé au format hexadécimal et la traduction ASCHII correspondante.

Protocole ISAKMP en phase 1

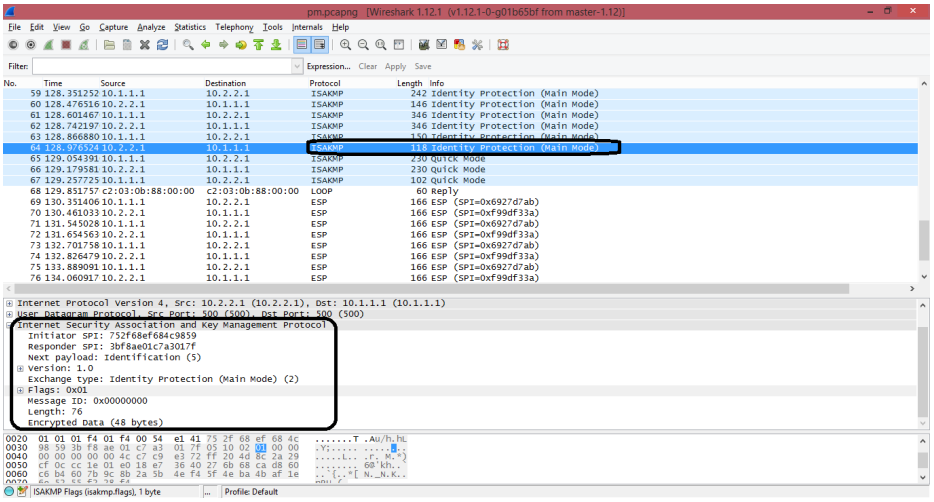

FIGURE 4.5 – L protocole ISAKMP en phase 1.

Protocole ISAKMP en phase 2

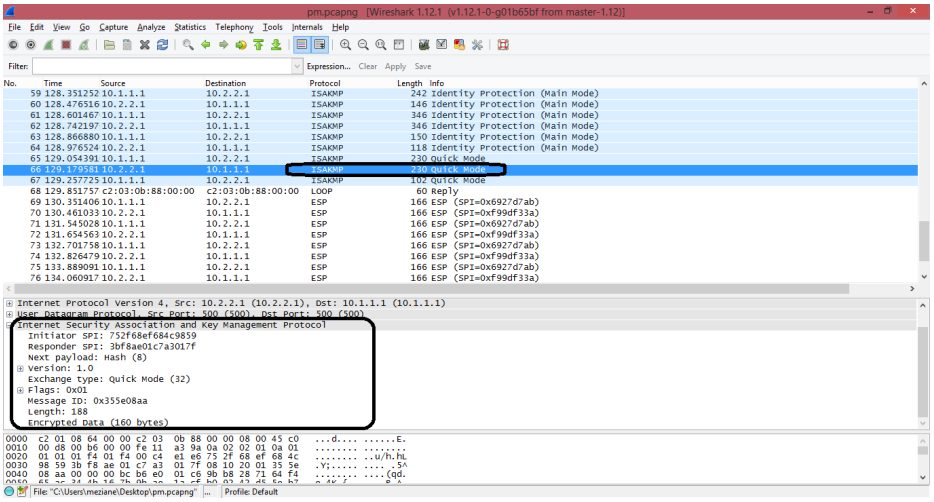

FIGURE 4.6 – Le protocole ISAKMP en phase 2.

Les messages échangés durant la phase2 (Quick mode) sont protégés en authenticité et en confidentialité grâce aux éléments négociés durant la phase1 (main mode). L'authenticité des messages et assurée par l'ajout d'un bloc HASH après l'en-tête ISAKMP, et la confidentialité est assurée par le chiffrement de l'ensemble des blocs du message.

4.4 Mise en place d'un VPN d'accès

La mise en place d'une solution qui va permettre un accès externe à notre réseau d'entreprise via une connexion VPN de type OpenVPN qui s'appuiera sur un équipe-

ment de type Firewall Pfsense et se fera via le biais d'une authentification local, comme l'illustre la figure 4.7.

Cette authentification permettra la connexion VPN à un groupe d'utilisateur et installation/configuration pour le client final afin qu'il soit autonome sur sa mise en place grâce à un package générer et à télécharger directement depuis l'interface web du firewall.

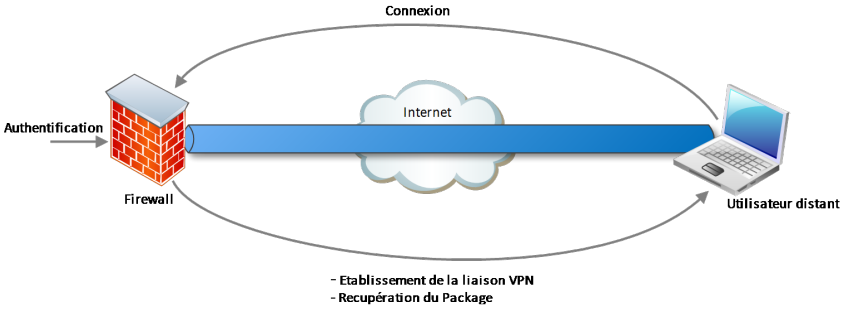

FIGURE 4.7 – Etablissement de liaison VPN.

4.4.1 Configuration et mise en place

Nous décrirons dans ce qui suit les principales configuration à mettre en place au niveau du firewall, le serveur Open VPN et le client.

4.4.1.1 Configuration au niveau de Pfsense

Après authentification pour l'accès à l'interface de Pfsense nous suivrons les étapes suivante afin de mettre en place un tunnel VPN.

• **Etap1 : Création des Certificats**

Le client et le serveur OpenVPN sont authentifié à l'aide de certificats. Pour cela, ces certificats doivent être émis par une autorité de certification reconnue comme sur aussi bien par le serveur que par le client.

Dans notre cas nous créerons une autorité de certification « certificat_2 » sur le Pfsense faisant office de serveur. Puis nous créerons deux certificats : un certificat client qui sera utilisé coté client et un certificat serveur qui sera utilisé coté Serveur. Ces deux certificats seront signé par l'autorité de certification (certificat_2).

1) Création de la CA (Certificate Authority)

Pour la création de l'autorité de certification (Figure 4.8) nous allons spécifié :

le nom qu'on donne à la CA, la méthode (créate an internal Certificate Authority) qui va nous permettre de créer une nouvelle CA ,la longueur de la clé de chiffrement du certificat, la fonction de hashage qui sera utilisé et la durée de vie de la CA.

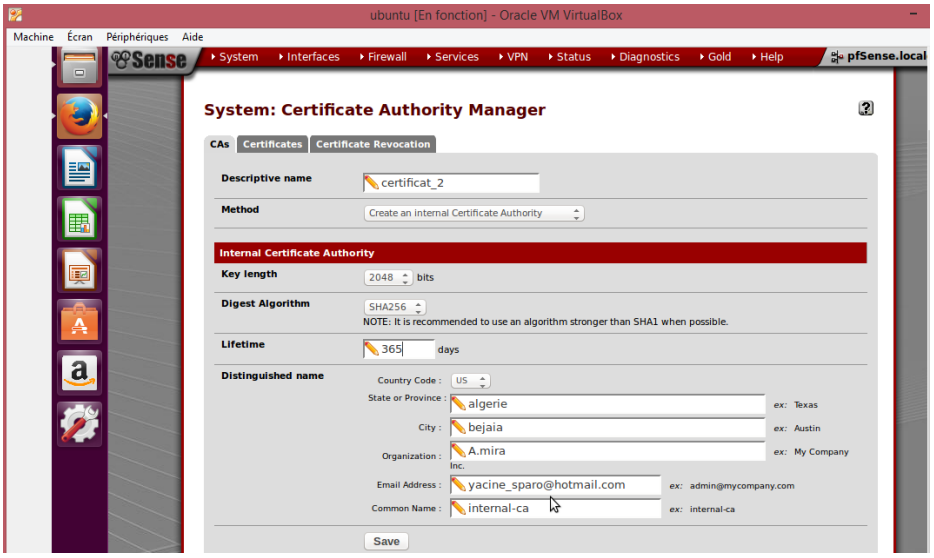

FIGURE 4.8 – Création de la CA.

2) Création du certificat serveur

Pour la création du certificat serveur(Figure 4.9) nous allons spécifier :le nom, la méthode,l'autorité de certification qui signera le certificat, le type de certificat(Server Certificate), la longueur de la clé et la fonction de hashage.

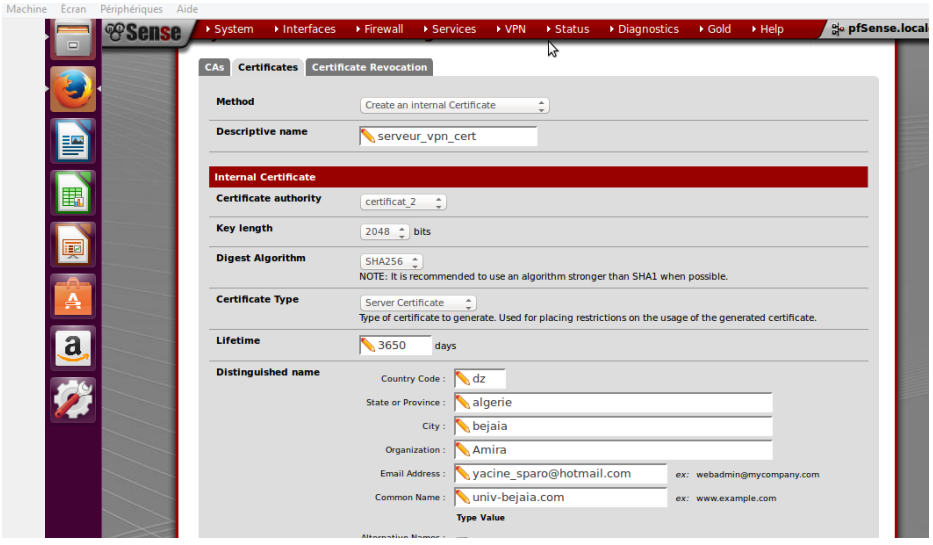

FIGURE 4.9 – Création du Certificat Serveur.

- **Etape 2 : Création d'utilisateurs et les groupes**

1) Création d'utilisateur OpenVPN

Chaque utilisateur doit avoir : un nom d'utilisateur, un mot de passe, une date d'expiration et un certificat qui sera signé par l'autorité de certification(Figure 4.10).

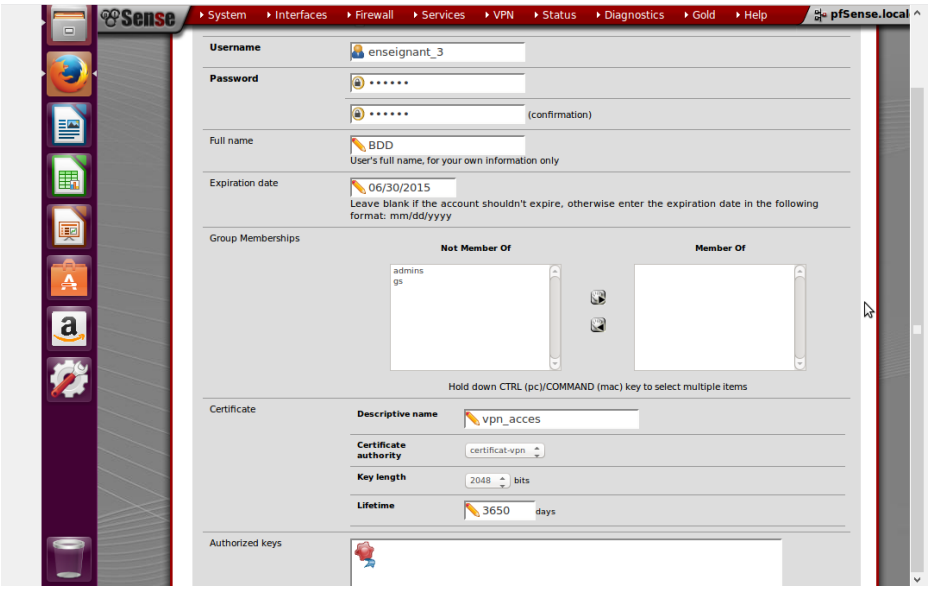

FIGURE 4.10 – Création d'utilisateur OpenVPN.

2) Création du groupe

plusieurs utilisateurs auront accès au VPN, d'où l'importance de créer un groupe d'utilisateurs(figure 4.6) locaux afin de les regrouper et leurs assigné des privilèges (Figure 4.11) qui leurs permettront l'accès à la page client Open VPN.

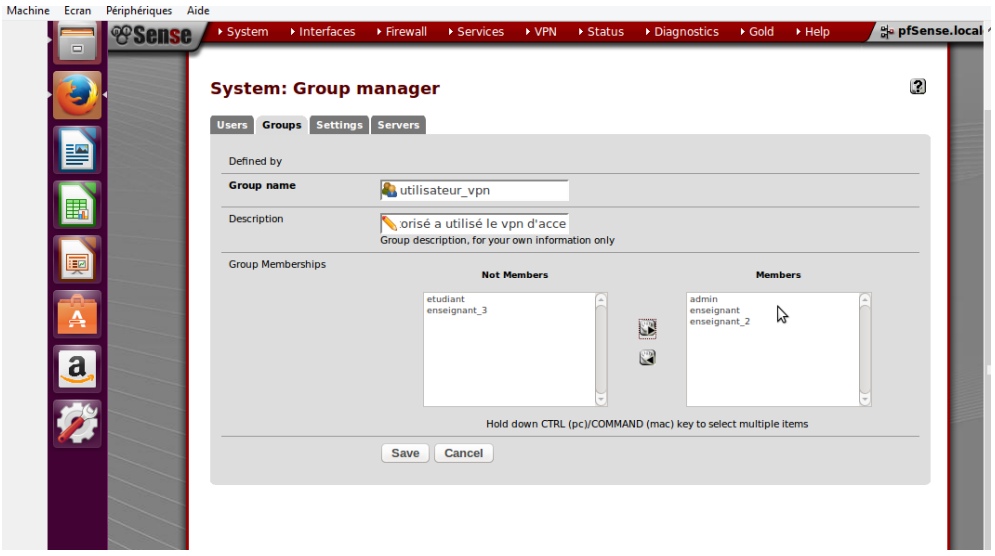

FIGURE 4.11 – Création du groupe.

Assignation de privilège

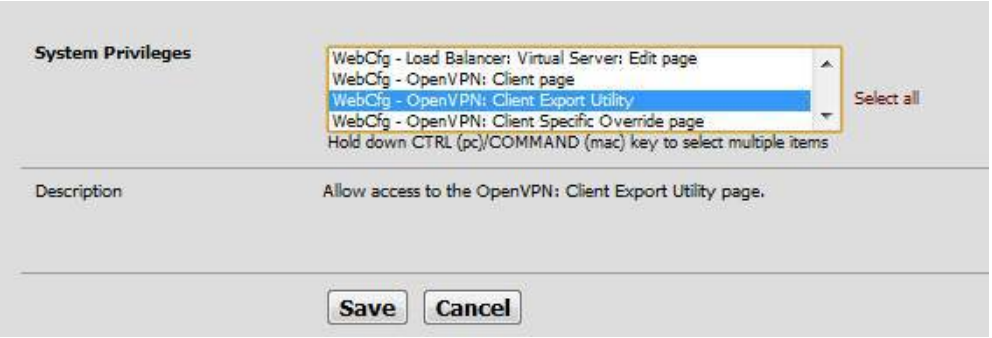

FIGURE 4.12 – Assignation de privilège.

• **Etape 3 : Installation du package OpenVPN Export Utility**

Depuis l'interface de gestion du firewall, nous allons installer le package OpenVPN Export Utility (Figure 4.13) qui va nous permettre par la suite l'installation du client OpenVpn ainsi que l'export de la configuration vers les utilisateurs distans.

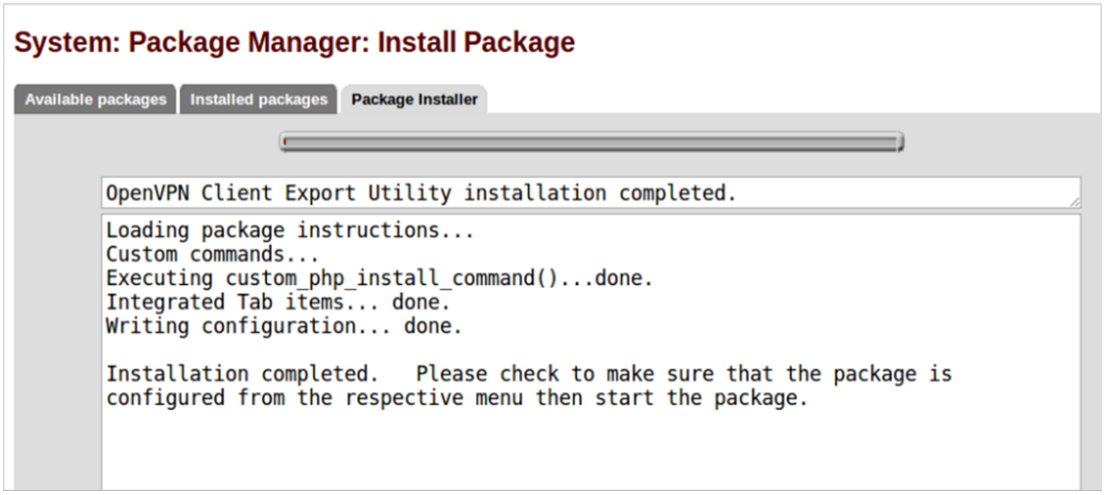

FIGURE 4.13 – Installation du package OpenVPN Export Utility.

• **Etape 4 : configuration au niveau du serveur**

Au niveau du serveur OpenVPn nous allons :

1) Définir le type d'authentification : Dans notre cas, les utilisateurs sont enregistrés localement donc nous choisissons "Local User Access".

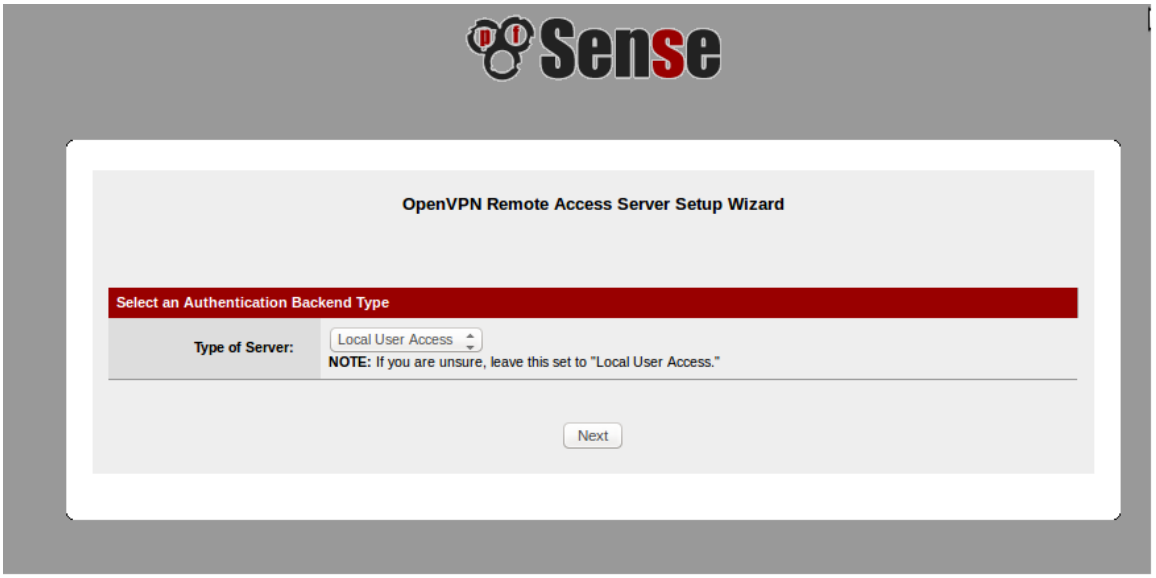

FIGURE 4.14 – Choix du serveur d'authentification

2) Choisir le certificat d'autorité « certificat_2 » qu'on a créé dans la première étape et qui va valider le certificat donné à l'utilisateur distant.

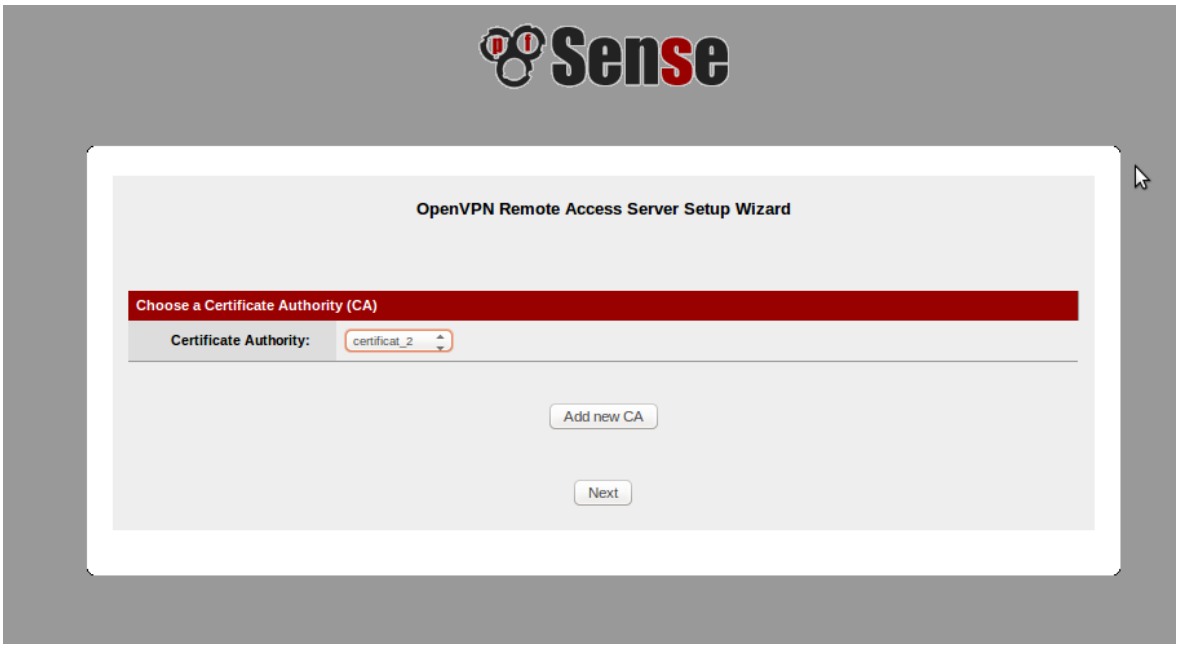

FIGURE 4.15 – Choix du certificat d'autorité

3) sélectionner le certificat du serveur qu'on a créé à la première étape .

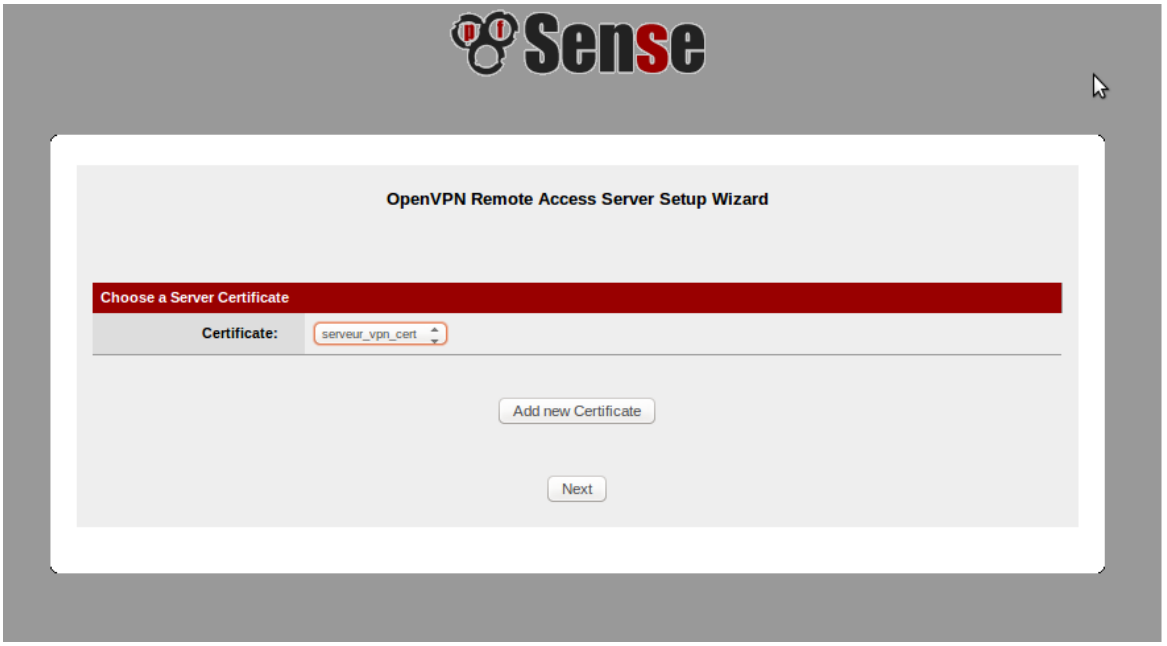

FIGURE 4.16 – Choix du certificat du serveur.

4) Choisir l'interface sur laquelle le serveur va recevoir les connexions entrantes , le protocole et le port d'écoute du serveur OpenVPN.

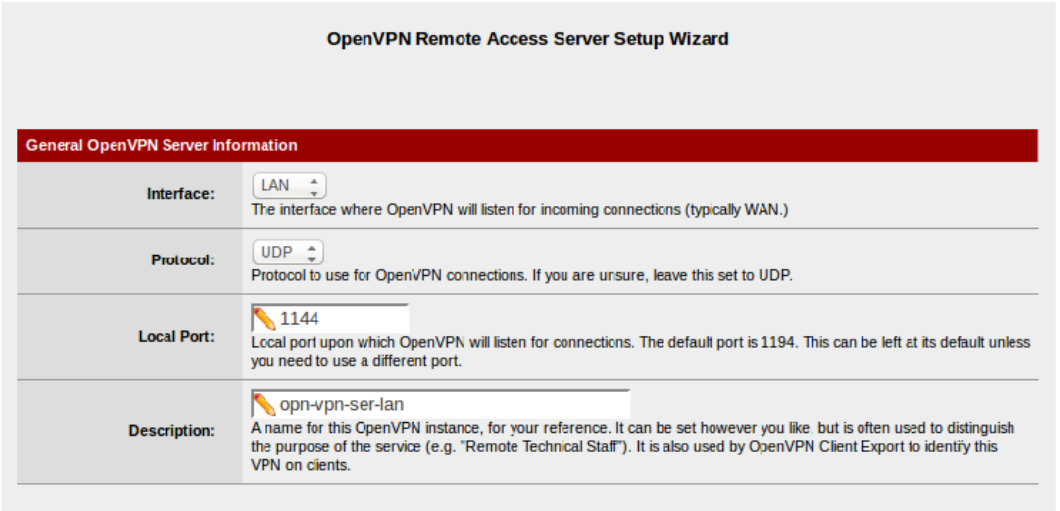

FIGURE 4.17 – Configuration serveur

5) Configurer le tunnel : Pour cela il faut précisé :

- l'adresse réseau qu'on va lui atrribué tout en 'assurant que cette addresse ne soit pas utilisé chez le client.

- l'adresse du réseau LAN qu'on souhaite atteindre depuis le VPN .

- le nombre de connexion client possible.

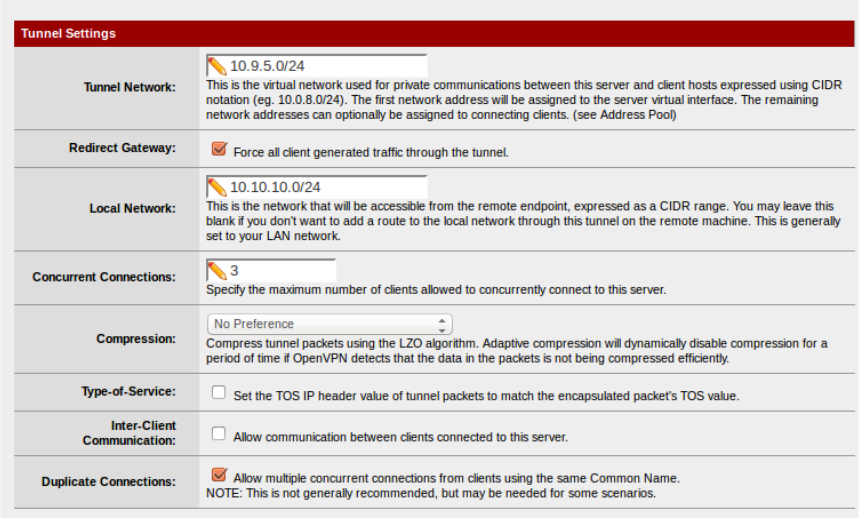

FIGURE 4.18 – Configuration du tunnel.

6) Sélectionner l'authentification par certificat, la génération automatique d'une clé d'authentification partagée TLS ,la longueur des paramètre de clé de Diffie-Helman(DH), l'algorithme utilisé pour crypté le trafic (serveur-client) et le type de hashage qui sera utilisé.

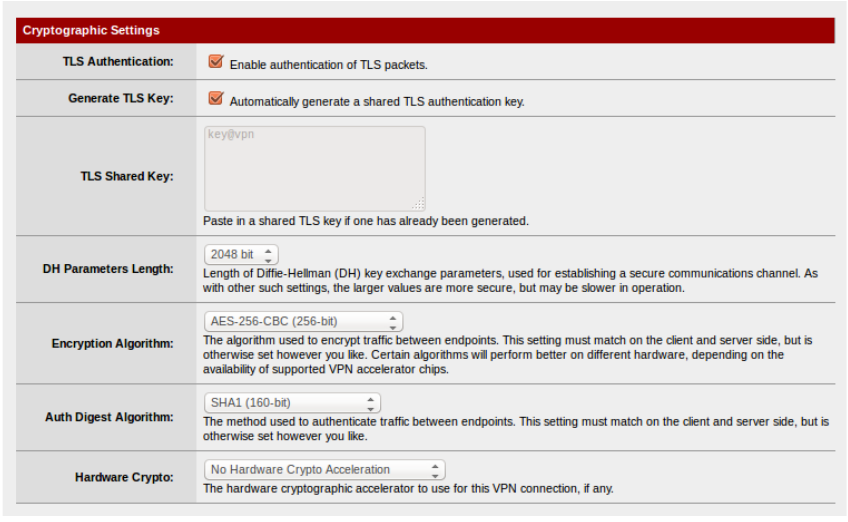

FIGURE 4.19 – Paramètre de chiffrement

7) Cocher l'attribution d'adresse IP dynamiquement pour le client vpn .

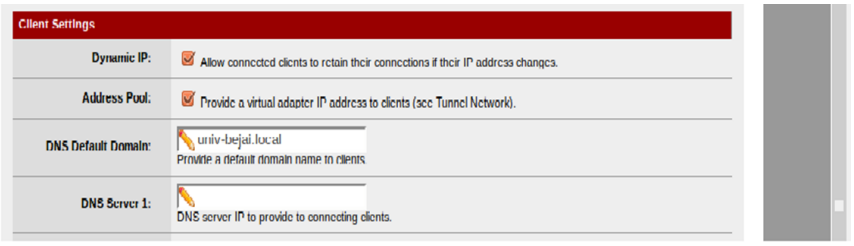

FIGURE 4.20 – Attribution d'adresse IP

8) créer une règles sur le Firewall afin d'autoriser la connexion à s'établir depuis l'extérieur ainsi qu'une règle autorisant tout le trafic client à voir l'ensemble du réseau derrière le VPN.

FIGURE 4.21 – Création des règles sur le Firewall.

9) Vérifier que le tunnel VPN a bien été créé .

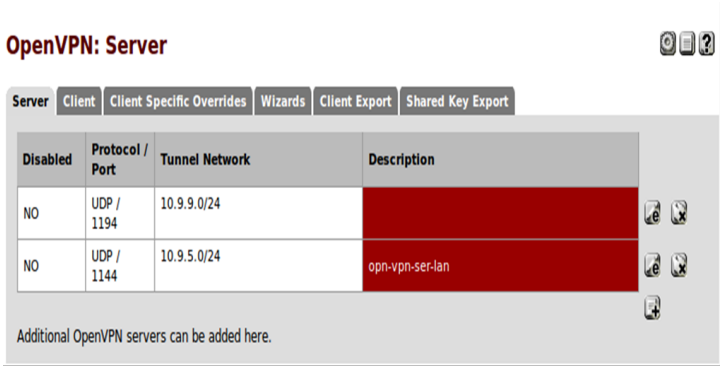

FIGURE 4.22 – Vérification de la création tunnel VPN

4.4.1.2 Configuration au niveau du client

Après authentification, le client aura accès à la page client Open VPN pour qu'il puisse télécharger le package qui contient le client Open VPN et la configuration intégrée.

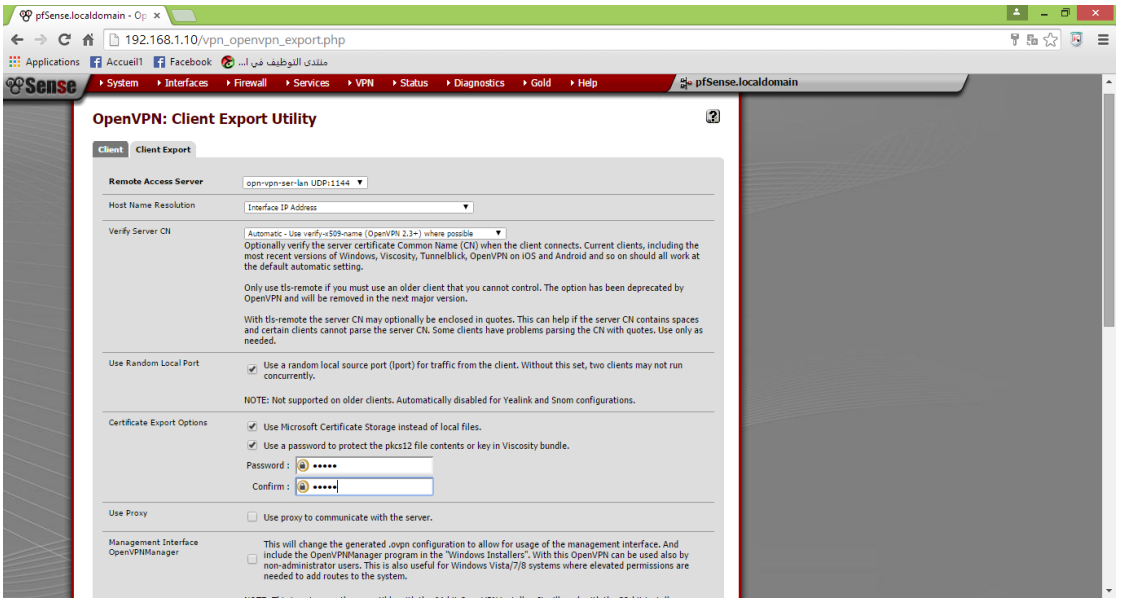

FIGURE 4.23 – page client OpenVPN.

Dans ce qui suit nous allons décrire les principales étapes de configuration au niveau du client OpenVPN

- **Etape 1 : Téléchargement du package**

Le client télécharge le package qui correspond à son système.

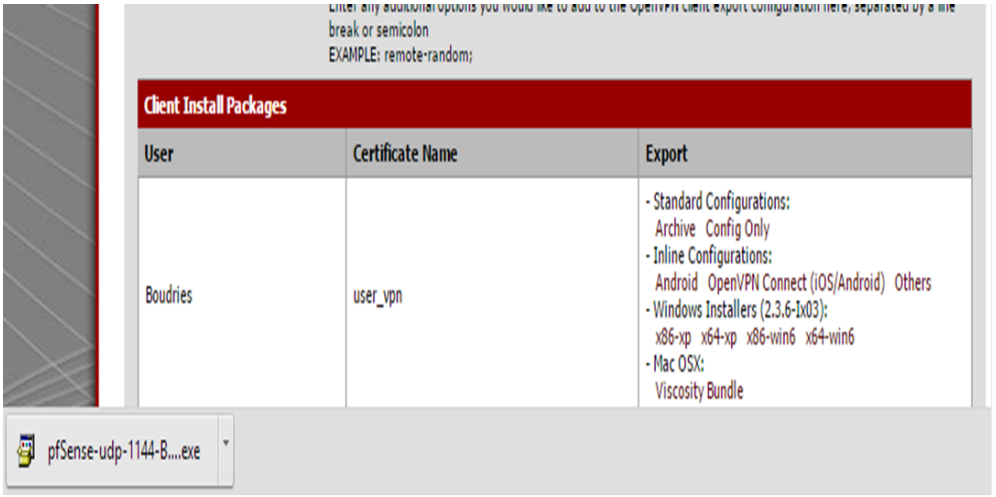

FIGURE 4.24 – Téléchargement du package.

- **Etape 2 : Instalation**

Le client installe le package téléchargé depuis le site qui contient le client OpenVPN avec la configuration intégrée.

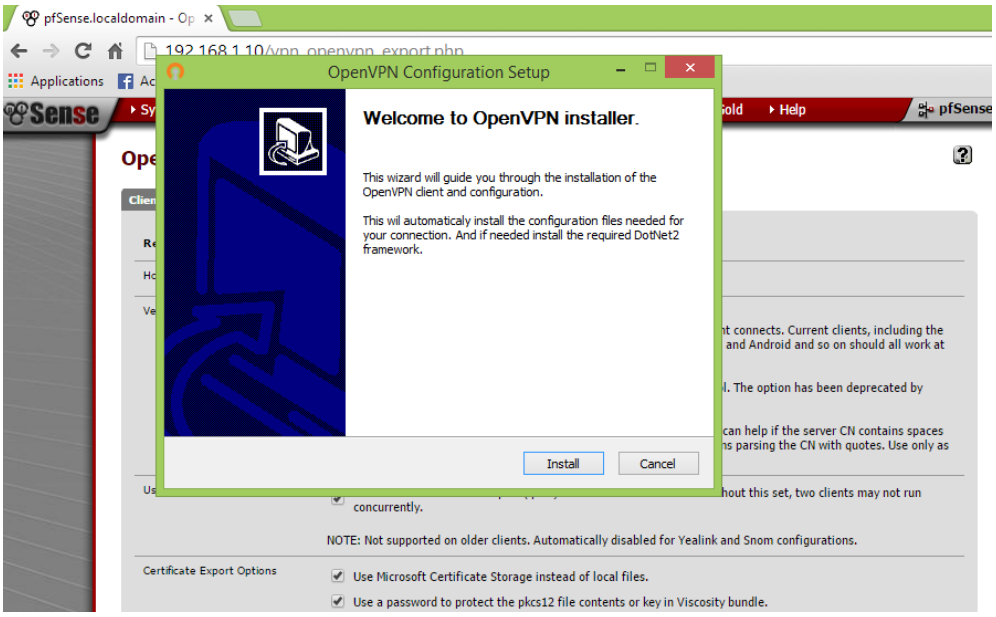

FIGURE 4.25 – Instalation du package.

- **Etape 3 : Importation de certificat**

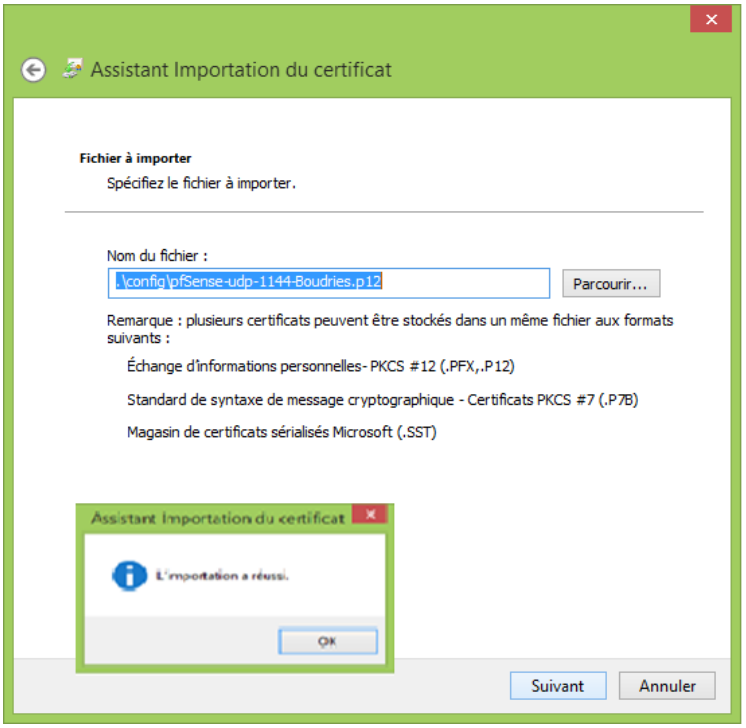

FIGURE 4.26 – Importation de certificat.

- **Etape 4 : Connexion**

Après l'installation du package et l'importation du certificat le client pourra se connecter au VPN et une adresse ip du tunnel lui sera attribuée.

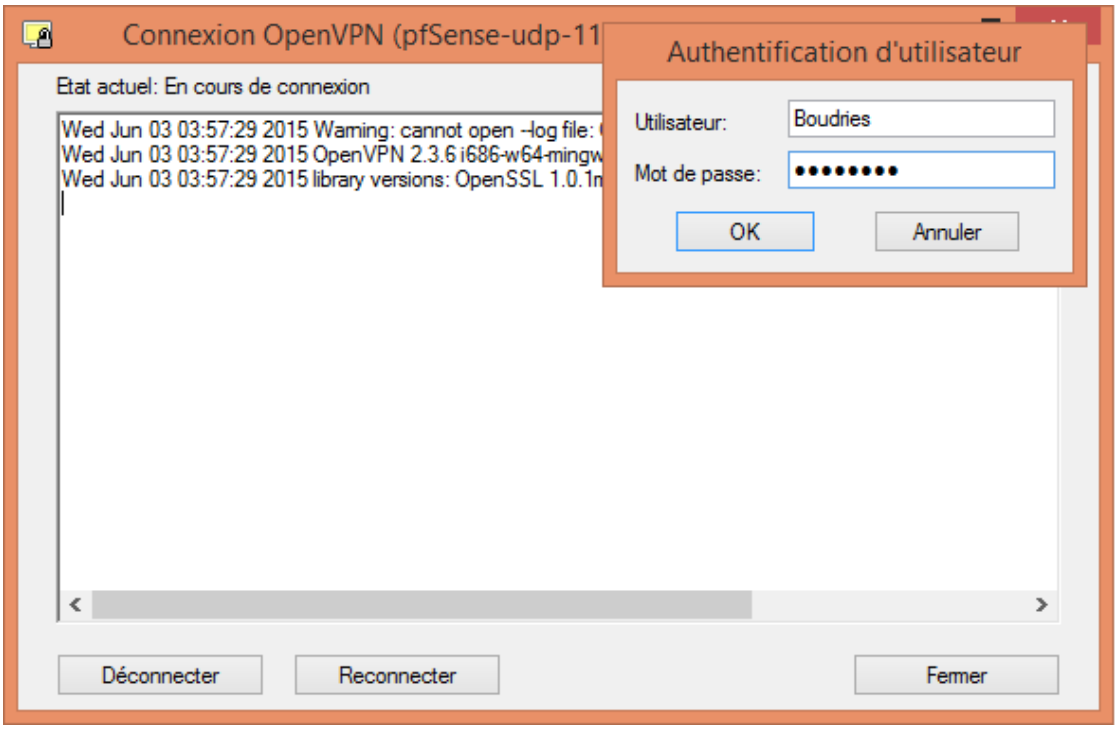

FIGURE 4.27 – Connexion au VPN.

4.5 Conclusion

Notre objectif dans ce chapitre était la mise en place d'un tunnel VPN reliant les deux sites de notre solution et permettre aux utilisateurs distants (client VPN) d'accéder au réseau interne via Internet. Nous avons atteint cette objectif car nous constatons bien selon les captures précédente, que les VPNs sont bien créés.

Conclusion générale

Le travail que nous avons accompli a pour principal objectif la proposition d'une architecture réseau sécurisée pour l'université A.mira de Bejaïa. ce projet nous a permis de mettre en pratique les connaissances acquises durant le cycle de notre formation, de se familiariser avec un environnement dynamique et d'avoir une idée plus profonde sur la sécurité des réseaux. Dans ce mémoire, nous avons présenté quelques généralités sur les réseaux, la sécurité informatique ainsi que les principales caractéristiques des réseaux privés virtuels et leur principe de fonctionnement.

Nous avons ensuite étudié l'architecture existante du réseau et ces différentes zones où nous avons expliqué comment se fait le routage inter-LAN, ce qui nous a permis de critiqué cette architecture et de suggérer quelques solutions afin de proposé une nouvelle avec une meilleur fluidité et sécurité du réseau.

Dans cette nouvelle architecture, nous avons proposé de diviser le réseau en deux réseaux indépendants à savoir TARGA, ABOUDAOU pour une meilleure fluidité du trafic, qui devient de plus en plus important et de moins surcharger le firewall, ces deux réseaux seront ensuite reliés par un tunnel sécurisé.

Dans chaque site nous avons proposé la mise en place :

— d'un système de détection et de prévention d'intrusion afin de détecter et d'interrompre les actions malveillantes sur les principaux liens du réseau à savoir du LAN vers la DMZ ou l'extérieur, ainsi que de l'extérieur vers la DMZ. Quant à cette dernière, il est important de n'y laisser que ces serveurs qui sont accessibles de l'extérieur.

— d'un serveur d'antivirus afin de bloquer les messages infectés de virus ou indésirables sur le serveur avant qu'ils ne parviennent sur la machine des utilisateurs finaux.

— d'une liaison entre la zone 4 et la zone 2 pour une meilleure tolérance aux fautes.

— d'un VPN site à site pour relié les deux sites tout en assurant les propriétés de sécurité, de confidentialité et d'authentification.

— d'un VPN d'accès pour permettre aux utilisateurs distants (enseignants, personnels ...) d'accéder à certaines ressources prédéfinies de l'université sans y être

physiquement présent.

La réalisation de ce projet a été bénéfique et fructueux pour nous dans le sens où il nous a permis d'apporter une contribution à l'université A.MIRA de Bejaïa. mais aussi d'approfondir et d'acquérir de nouvelles connaissances qui seront utiles et déterministes pour nous à l'avenir.

bibliographie

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

[2] A.ZBAKH. Module Informatique, Prince Molay Rchid,2007 ,http ://lycee.voila.net/mod4_chap1.pdf.

[3] Frédéric Jacquenod. Cours Réseaux N°5, les matériels d'interconnections, http ://www.netalya.com/fr/reseaux5.asp.

[4] Pierre Erny. LES RESEAUX INFORMATIQUES D'ENTREPRISE, 1998

[5] Jean-François Pillou. Tout sur les réseaux et Internet, DUNOD 2006.

[6] Lourent Bloch-Christophe Wolfhugel. EYROLLES, 2éme édition. 2005.

[7] Nicolas Baudoin et Marion Karle. NT Réseaux : IDS et IPS, Rapport Ingéniorat. 2000

[8] M.Righidel. Pour l'émergence d'une nouvelle sécurité dans les réseaux de communications et les systèmes d'information futurs, OFTA, Arago Vol.23, paris, 2000.

[9] http : //www.tele.ucl.ac.be/EDU/ELEC/1997/firewall/Firewalls.html.

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

[11] Encyclopédie informatique comment ça marche : introduction à la cryptographie introduction à la sécurité, http : //www.commentcamarche.com.

[12] S.Ikhalef. sécurité informatique Proxy, mémoire de fin d'études Ingéniorat, université de Bejaia 2003.

[13] Guillaume Desgeorge. la sécurité des réseaux, 2000, http : www.guill.net/réseaux/La sécurité des reseaux.htm.

[14] Marc BOGET. étude des vulnérabilités d'un grand réseau d'entreprise et solutions de sécurité, 2003.

[15] H.Lauadah.Communication de groupe sécurisée dans le réseau virtuel de l'université de Bejaia : Implémentation d'un protocole d'accord de clé de groupe, mémoire, Université de Bejaia, 2008.

[16] S.Manuel,lic.phil.I, collaborateur scientifique, Center for Security Studies(CSS), ETH Zurich, août 2006.

[17] Sara del Socorro MOTA GONZALEZ. Modélisation et vérification de protocoles pour des communications sécurisées de groupes, thèse doctorat, Université de TOULOUSE, 2008.

[18] M.Guermah. les réseaux privés virtuels : un accès sécurisé au réseau d'entreprise, conférence. Blida, 2010.

[19] Tomas Klein et Sebf2004.2007.http ://www.frameip.com/vpn/ : Document web site consacré à les Réseaux privés Virtuels-VPN, suivi Xavier Lasserre, 2014.

[20] Cisco networking Academy, 2007/2008.

[21] http ://fr.scribd.com/doc/Chap-8-Les-VPN.

[22] http :// saquet.users.greyc.fr/docradis/VPN Tunneling.pdfLes Réseaux Privés Virtuels (VPN).2014.

[23] Denis de REYNAL, Jehan-Guillaume de RORTHAIS et Sun Seng TAN.Présentation sur les VPN, UFR Ingénieurs, France, 2004.

[24] H.Benameurlaine. réseaux prives virtuel, rapport de TER de Tsedeye TIBEBU, Université Tlemcen, 2011.

[25] C.Rafael et C Ernesto et Yoann Le CORVIC. Les VPN : principes, conception et déploiement des RPV, édition Dunod, Paris, p 287, 2003.

[26] Y.Vanhullebus. étude IPsec et intégration de l'extension-mode config- Dans le module IPsec des utms Netasq, rapport de stage, Université : Emmanuel Fleury NETASQ : Yvan, 2008.

[27] A.Ksiks. Etude et simulation sur GNS3 du service MP-BGP/VPN-IP , 2011.

[28] http :// www.noplay.net/GNS3.html.