REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE IBN KHALDOUN - TIARET

MEMOIRE

Présenté à :

FACULTÉ MATHEMATIQUES ET INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité : Réseaux et télécommunications

Par :

MAHREZ Djilali

ZERROUKI Abdel Nacer

Sur le thème

Pratique de solution tunnel VPN IPsec dans un environnement Virtuel et open source

---

Soutenu publiquement le 28 / 09 / 2020 à Tiaret devant le jury composé de :

Mr BENOUDA Habib	Grade	Université	MAA	Président
Mr DAHMANI Youcef	Grade	Université	PR	Encadreur
Mr LAARADJ Zohra	Grade	Université	MAA	Examinateur

Année Universitaire : 2019 /2020

Remerciement

Avant tout nous remercions Dieu le tout puissant de nous avoir donné le courage et nous avoir guidé pour pouvoir mener à bien ce modeste travail.

A notre promoteur Mr DAHMANI Youcef

Malgré vos multiples préoccupations, vous avez bien voulu nous confier ce travail et le diriger. Nous avons eu le privilège de travailler parmi votre équipe et d'apprécier vos qualités et vos valeurs. Votre sérieux, votre compétence et votre sens du devoir nous ont énormément marqués. Veuillez trouver ici l'expression de notre respectueuse considération et notre profonde admiration pour toutes vos qualités humaines et professionnelles.

A Mr. BENAOUDA Habib

C'est pour nous un grand plaisir de vous compter parmi le jury de ce travail, nous tenons à vous témoigner notre profonde reconnaissance d'avoir aimablement accepter de présider le jury de ce mémoire. Veuillez croire à notre gratitude et à notre respectueuse considération.

A Mme : LAARADJ.Z

Nous sommes profondément reconnaissantes de l'honneur que vous nous faites en acceptant d'examiner notre modeste travail, Veuillez trouver dans ce travail l'expression de notre attention et le témoignage de notre profonde et sincères considération.

Un grand Merci aux enseignants en particulier ***Mr. OUARED AEK*** *d'avoir aimablement accepté de répondre à nos questions. Ainsi que l'administration de la faculté informatique qui ont veillé sur notre formation et notre suivi durant tout le cursus d'étude.*

En fin nous adressons nos remerciements à tous ceux qui ont contribué par leurs conseils ou leurs encouragements à l'aboutissement de ce travail.

Dédicace

Je dédie ce mémoire à …

A mes parents

Aux plus belles créatures que dieu a créées sur terre, à cette source de tendresse, de Patience et de générosité. Aucune dédicace ne pourrait Exprimer mon respect, ma considération et mes chaleureux sentiments envers mes Chers Parents, Grâce à leurs tendres encouragements et leurs grands sacrifices, ils ont pu créer le climat affectueux et propice à la poursuite de mes études. Je prie le bon lieu de les bénir, de veiller sur eux, en espérant qu'ils soient toujours fiers de moi.

-A mes chers frères pour leurs conseils et leur soutien.

A tous les membres de ma famille

-A mes amis ***Anouar, Youcef, HOCIN****, merci à tous mes amis avec qui ont partagé des moments de ma vie au fil du temps*

A mon binôme ***Nacer***

En témoignage de l'amitié qui nous uni et des souvenirs de tous les moments que nous avons passés ensemble, je te dédie ce travail et je te souhaite une vie pleine de santé et de bonheur.

A ma promotion de Master 2 Informatique 2019/2020

Et tous les amis dans les autres promotions

Et Tous ceux que je connais de près ou de loin, merci à tous, sans exception.

Djilali

Dédicace

Je dédie ce mémoire à …

Dans cet espace je souhaiterai dédier ce travail `à mes très chers parents

En premier lieu mes dédicaces vont droit à ma chère mère. Tes encouragements et tes prières

ont ´été d'un grands soutien pour moi je te remercie infiniment.

Je remercie également mon cher père pour sa présence dans ma vie, de son soutien et tous

ses sacrifices et ses précieux conseils, j'espère avoir réussi `a te rendre fière chose que je tâcherai

de continuer à faire.

-A mes chers frères pour leurs conseils et leur soutien.

A mes chers mes neveux

-A mes amis, merci à tous mes amis avec qui ont partagé des moments de ma vie au fil du temps

A mon binôme ***Djilali***

Merci pour tous les moments que nous avons passés ensemble dans ce travail

A ma promotion de Master 2 Informatique 2019/2020

Et Tous ceux que je connais de près ou de loin, merci à tous, sans exception.

Abdel Nacer

Résumé :

La mise en œuvre d'un VPN (Virtual Private Network) avec le jeu de protocoles IPsec est un exercice difficile vu le nombre des combinaisons possibles entre les différents algorithmes, configurations et autres paramètres à prendre en compte. Le présent travail consiste à créer une liaison d'interconnexion site à site, à travers un réseau non sécurisé, tel qu'internet. Cette liaison est un réseau privé virtuel VPN avec une implémentation open source d'IPsec ayant pour objectif de sécuriser cette connexion, en adoptant l'environnement Linux comme plate-forme de base pour l'aboutissement de ce tunnel. StrongSwan un outil d'implémentation multi-plateforme d'IPsec nous a été d'une grande utilité pour mener à terme ce projet.

Mots clés : Tunnels VPN, IPsec, Virtualisation, plate-forme Linux, implémentation StrongSwan, open source, Echange de clés cryptographiques.

Abstract :

The implementation of a VPN (Virtual Private Network) with the set of IPsec protocols is a difficult exercise due to the number of possible combinations between the different algorithms, settings and other parameters to be taken into consideration. Our work consists of creating a site-to-site interconnection link, through an unsecured network, such as the Internet. This link is a VPN virtual private network with an open source implementation of IPsec, for the purpose of securing this connection, adopting the Linux environment as the base platform for the completion of this tunnel. StrongSwan, a multiplatform implementation tool of IPSec, was of great use to us in completing this project.

Keywords : VPN tunnels, IPsec, Virtualization, Linux platform, StrongSwan implementation, open source, Cryptographic key exchange.

الملخص:

يعد تنفيذ الشبكة الافتراضية مع مجموعة بروتوكولات الانترنت الامن تمرينا محفوفا بالمخاطر يمكن ان يتحول بسرعة
الى كابوس نظرا لعدد التوليفات الممكنة بين الخوارزميات المختلفة، يتمثل عملنا في انشاء ارتباط اتصال بيني من موقع الى موقع من خلال الشبكة غير الامنة (الانترنت)، هذا الرابط عبارة عن شبكة افتراضية خاصة مع تطبيق مفتوح المصدر لبروتوكول الانترنت الامن واعتماد بيئة لينكس كنظام أساسي لإكمال المشروع وانشاء النفق

كانت StrongSwan ، أداة تنفيذ IPSec عبر الأنظمة الأساسية ، مفيدة جدًا لنا في إكمال هذا المشروع.

الكلمات المفتاحية شبكة خاصة افتراضية، بروتوكول الانترنت الامن، المحاكاة الافتراضية، تطبيق لينكس، المصدر المفتوح، تبادل مفاتيح التشفير.

Sommaire

Liste des figures

Liste des abréviations

ADSL : Asymmetric Digital Subscriber Line

AH : Authentification Header

AES : Advanced Encryption Standard

ESP : Encapsulating Security Payload

FTP : File Transfer Protocol

IETF : Internet Engineering Task Force

IKE : Internet Key Exchange

IP : Internet Protocol

IPsec : Internet Protocol Security

L2F : Layer Two Forwarding

L2TP : Layer Two Tunneling Protocol

LAC : L2TP Access Concentrator

LAN : Local Area Network

LNS : L2TP Network Server

MPLS : MultiProtocol Label Switching

PPTP : Point-to-Point Tunneling Protocol

PSK : Pre Shared Key

SA : Security Association

SAD : Security Association Data base

SPD : Security Policy Data base

SSH : Secure Shell

SSL : Secure Sockets Layer

VPN : Virtual Private Network

Introduction générale :

La plupart d'entre nous sommes d'accord pour dire que nous utilisons internet de façon quotidienne, que ce soit pour la vie privée ou professionnelle, Sur l'internet on ne sait pas où passent les données car l'information traverse différents routeurs et les chemins changent nécessairement selon des conditions qui sont indépendantes de l'utilisateur.

Ces données peuvent donc être écoutées ou interceptées par un pirate (man in the middle), il n'est donc pas envisageable de faire connecter deux LAN (Local Area Network) entre eux par internet sans moyen de sécuriser le cheminement des données échangées.

Le problème qui se pose est : comment protéger les informations qu'ils circulent dans le réseau internet ?

Plusieurs mécanismes ont été adoptés pour mettre en œuvre et offrir les services de sécurité, parmi ces mécanismes :

1. Chiffrement 2. Authentification 3. Signature numérique 4. Tunnels …

Dans notre mémoire, nous nous sommes focalisés seulement sur la technique de tunnel.

Dans la littérature, on recense deux solutions :

- Relier les deux sites par une ligne spécialisée mais hors de prix.
- Créer un réseau privé virtuel sécurisé gratuit autrement dit un VPN.

Dans ce sens, l'objectif de notre travail est de créer un tunnel VPN utilisant l'implémentation d'IPsec dans un environnement virtuel sur la plateforme Linux (Debian) toutes cette architecture est une solution Open source, les VPN offrent quelques fonctionnalités telles que : l'authentification, la confidentialité et l'intégrité …

Pour se faire nous avons structuré le présent manuscrit comme suit : Dans le premier chapitre intitulé ***« Généralités sur le VPN »*** nous décrirons d'abord ce qu'est un VPN pour nous, puis nous déterminerons son fonctionnement et ses fonctionnalités, puis les typologies de ces VPN, puis nous présenterons rapidement les principaux protocoles aux niveaux 2 et 3.

Dans le deuxième chapitre intitulé ***« Internet Protocol Security »,*** nous décrirons ce qu'est IPsec, sa normalisation, ensuite la théorie ce jacente de ce protocole. Nous décrirons en générale IPsec, les méthodes utilisées, les types et les configuration possibles.

Dans le troisième chapitre intitulé « ***Implémentation et test*** », nous expliquons les outils de réalisation de cette travail puis on va commencer les étapes de réalisation l'une après l'autre avec des tests qui démontreront son bon fonctionnement.

Chapitre I

Généralités sur le VPN

Sommaire

Chapitre I : Généralités sur le VPN

1 Introduction :

Les réseaux sont nés de la nécessité d'échanger des informations de manière simple et rapide entre ordinateurs, mais le défi à l'heure actuelle est de connaître ces informations, parmi les solutions utilisées se trouvent les réseaux privés virtuels, car ils permettent d'échanger des données entre les membres d'une communauté via un réseau d'interconnexion partagé ou public d'une manière sûre et rentable.

Dans ce premier chapitre, nous définissons d'abord qu'est un VPN pour nous, puis nous déterminerons leur fonctionnement et leurs fonctionnalités, ensuite les typologies de ces VPN, et finalement nous présenterons rapidement les principaux protocoles.

2 Définition :

VPN pour (Virtual Private Network) ou RPV pour (Réseau Privé Virtuel), est un ligne spécialisé virtuel et privé installé sur un réseau, permet de relier deux sites distants (communication sécurisée et échange d'informations), le VPN garantit la protection et la confidentialité des données qui circulent, afin que personne de malintentionné ne puisse capturer et intercepter les informations.

Un VPN est essentiellement basé sur des lignes partagées et non dédiées, qui a une incidence directe sur les performances, car la connectivité Internet est plus lente qu'une connexion dédiée.

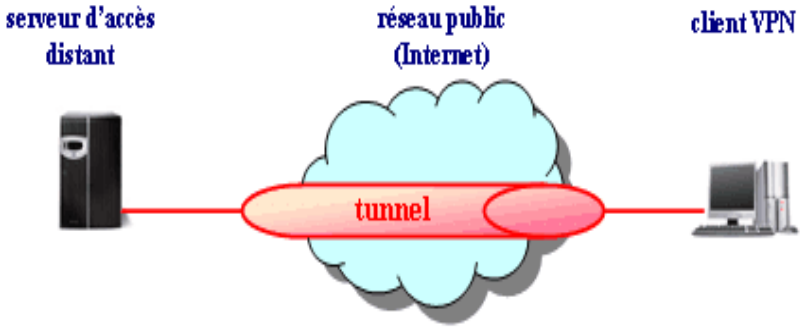

Figure I.1 - *composition d'un VPN* **[1]**

1. http://nicolas.roux.pagesperso-orange.fr/install/2003server/accesdistant.htm

3 Fonctionnement et fonctionnalités :

3.1 Fonctionnement :

Le VPN est basé sur un protocole de tunneling (tunnel) qui est un protocole de cryptage de données par un algorithme cryptographique entre les deux bouts du réseau en question.

Le principe de tunneling consiste à créer un chemin virtuel après la localisation de l'émetteur et du destinataire. Par la suite, la source crypte les données et les achemine le long de cette route virtuelle.

3.2 Fonctionnalités :

Le VPN se caractérise par les obligations suivantes :

- Authentification mutuelles entre les entités communicantes (authentification entre les serveurs VPN et les clients).
- Gestion des adresses très simple pour les clients (tous les clients peuvent obtenir une adresse facilement).
- Les données échangées sur internet sont obligatoirement cryptées et les clés doivent être régénérées de manière automatique.
- Un vrai tunnel VPN supporte tous les protocoles comme s'il y avait réellement un câble entre les deux réseaux.

4 Typologie de VPN

On peut distinguer deux grandes catégories de VPN : le VPN d'entreprise et le VPN d'opérateur.

4.1 VPN d'entreprise :

L'entreprise conserve la propriété des établissements des VPN entre ses différents points de présence ainsi que ceux situés à l'extérieur de l'entreprise et les sites principaux.

4.1.1 Site à site (LAN to LAN) :

Un VPN de site à site est également appelé routeur à routeur (router to router) est principalement utilisé pour les opérations commerciales. Étant donné que de nombreuses entreprises ont des bureaux nationaux et internationaux, un VPN de site à site est utilisé pour connecter le réseau des bureaux principaux au reste des bureaux. Ce type de VPN est basé sur l'intranet.**[2]**

Généralement ce type de VPN est mise en place par l'interconnexion de deux éléments matériels (routeur ou pare-feu) installées à la frontière entre le réseau interne et le réseau publique de chaque site. Ce sont les matériaux qui aident au cryptage, authentification et routage des paquets.

2. https://fr.vpnmentor.com/blog/les-differents-types-de-vpn-et-quand-les-utiliser

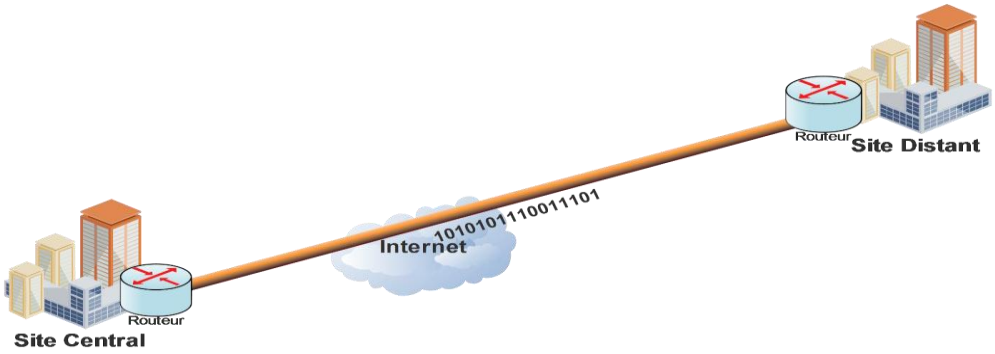

Figure I.2 - *Exemple d'un VPN site à site* **[3]**

Parmi les avantages de cette architecture, nous pouvons citer à titre non exhaustif :

- Le cryptage est assuré par des processeurs spécialisés, ce qui améliore considérablement les performances.
- Une merveilleuse installation pour le contrôle de la circulation réglementée.
- La possibilité de basculer les VPN de chaque côté.

Mais cette solution présente aussi quelques inconvénients :

- Aucune protection des données entre les stations et les pare-feu car le tunnel n'est installé qu'entre les deux pare-feu

4.1.2 VPN poste à site :

C'est aussi une utilisation très fréquente des VPN, qui consiste à permettre à des utilisateurs distants (travailleurs à domicile ...) d'accéder aux ressources de l'entreprise via un VPN.

Pour réaliser cette solution, un matériel (pare-feu, routeur ...) sera installé sur l'emplacement central, qui est le point de terminaison de tous les VPN de ce dernier, et un logiciel qui gère le type de protocole sélectionné et est compatible avec le matériel du site central est monté du côté des postes de travail distants. Dans certains cas, ce programme est déjà présent dans le système d'exploitation de ces ordinateurs, dans d'autres cas, il est important d'installer cette fonctionnalité logicielle. **[3]**

3. J.P ARCHIER, « Les VPN, fonctionnement et mise en œuvre et maintenance des privés virtuels » », 2 EME EDITIONS 11/12/2013

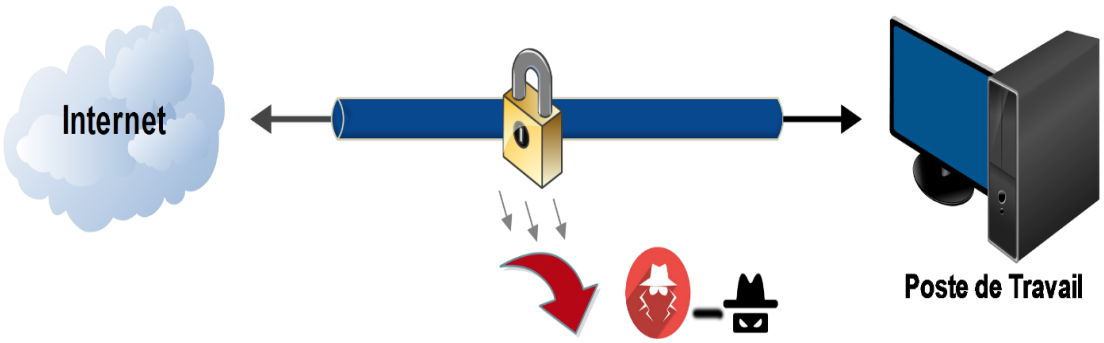

Figure I.3- *Exemple d'un VPN poste à site* **[3]**

Parmi les avantages de cette solution, on cite :

- L'accès au poste nomade (mobile) peut se faire depuis n'importe quelle partie du monde grâce à la connectivité Internet.
- Transfert de données entre les sites distants et centraux en toute sécurité via un mécanisme d'authentification.

Cependant, nous pouvons également citer quelques inconvénients :

- L'installation du logiciel est généralement nécessaire sur le poste distant.
- Le cryptage n'est pas assuré au-delà du firewall du site central.

4.1.3 VPN poste à postes :

Dans ce cas, il s'agit de créer un canal de bout en bout stable entre deux stations, ou plus généralement, entre une station et un serveur. Le poste et le serveur peuvent être placés sur le même réseau ou sur deux réseaux différents reliés par un VPN de site à site.

Seuls des composants logiciels sont utilisés pour cette configuration : un logiciel client sur le Poste "demandeur " et un logiciel serveur sur le poste " destinataire ".

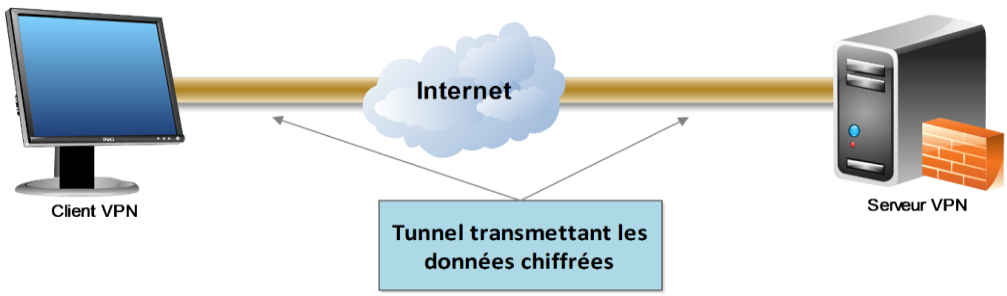

Figure I.4 - *Exemple d'un VPN poste à poste.* **[3]**

Le principal avantage de cette approche est que l'interaction entre les deux positions est complètement sécurisée de bout en bout. C'est donc un choix très sûr pour les communications les plus sensibles.

Par ailleurs, elle présente de nombreux inconvénients

- Le cryptage est uniquement logiciel, d'où un impact possible sur l'efficacité du haut débit, en particulier lorsque les deux extrémités se trouvent sur le même réseau local.
- Les messages étant placés sur des sites Internet différents, il est important que les deux extrémités puissent échanger leurs messages sur des protocoles et des ports qui doivent être approuvés par les pare-feu placés sur chaque site. Cela comprend également le traductions d'adresses car les machines concernées sont rarement équipées d'adresses IP publiques et ce n'est pas sans doute un problème anodin.

Avantages et inconvénients du VPN d'entreprise :

Les principaux **avantages** de cette solution sont :

- Aucun contrat à signer, déploiement, mise en place et la suppression de ces VPN.
- Aucun paiement récurrent autre que l'accès Internet n'alimente ces VPN.
- Grande polyvalence pour déplacer des tunnels, changer de périmètre ou réguler le trafic qui les traverse.
- Maîtrise des protocoles de sécurité (authentification, cryptage, filtrage ...).

Par ailleurs, il y'a quelques **inconvénients** :

- Aucune garantie de temps de récupération en cas de panne.
- Aucune garantie de performance car ces VPN prennent en charge une liaison Internet

4.2 VPN opérateur :

Lorsqu'il s'agit d'interconnecter plusieurs sites d'une même entreprise avec des engagements de performance et de disponibilité, il est plus judicieux, mais évidemment plus coûteux, de faire appel à un opérateur qui mettra donc en place un réseau privé entre tous les sites. Ce réseau possède plus d'un réseau de tunnels qu'un véritable réseau VPN, mais il est très populaire de parler d'opérateur VPN car il est difficile de décrypter les communications échangées entre sites sans l'implication des clients de l'opérateur.

4.2.1 Caractéristiques du VPN opérateur site à site :

Chaque site est connecté au POP (Point Of Presence) le plus proche avec le support souhaité (ADSL, SDSL, fibre optique ...) et un routeur contrôlé par l'opérateur.

Ensuite, établissez des tunnels ou des circuits privés entre les différents sites en utilisant les différents liens entre leurs POP.

La technologie pour cela diffère en fonction des évolutions techniques et nous sommes donc passés des réseaux Frame-Relay (Frame Relay) aux réseaux MPLS (MultiProtocol Label Switching) qui sont désormais les plus courants dans ce contexte. Selon le souhait du client et les possibilités technologiques ou budgétaires, ce réseau privé peut être conçu avec différentes topologies.

- Tous les sites secondaires convergent vers le site central et c'est celui-ci qui fait le relais : technologie hub (ou en Etoile).
- Tous les sites peuvent communiquer directement entre eux : full mesh ou maillage complet.
- Les sites les plus importants peuvent communiquer entre eux et les secondaires passent obligatoirement par un des sites principaux.
- L'opérateur supervise la totalité du réseau et peut affecter des classes de service selon le type de trafic, ce qui permet de rendre prioritairement certains flux **[3]**.

Principaux ***avantages*** de ce type de réseaux sont :

- Clarté totale en ce qui concerne les emplacements du réseau.
- Une possibilité de mettre en place QoS (Quality of Service) pour prioriser le trafic de haute priorité et assurer une bande passante optimale pour le trafic.
- Confirmation de l'efficacité du réseau tant en termes de débit que de temps de transit des messages.

Il y'a néanmoins certains ***inconvénients*** à considérer comme :

- Les frais d'abonnement à ce fournisseur de réseau à partir de chaque emplacement.
- La nécessité de fournir un seul opérateur VPN pour l'ensemble du réseau.

5 Les principaux protocoles de VPN :

Les principaux protocoles de tunneling VPN sont les suivants :

- PPTP (Point-to-Point Tunneling Protocol), L2F (Layer Two Forwarding) et L2TP (Layer Two Tunneling Protocol) sont des protocoles de niveau 2.
- MPLS (Multi Protocol Label Switching) est un protocole de niveau 2.5 (niveau 2 et 3).
- IPsec (Internet Protocol Security) est le protocole de niveau 3.
- SSH (Secure Shell) et le protocole SSL/TLS (Secure Sockets Layer / Transport Layer Security) sont les protocoles des niveaux 4 et 5 respectivement.

5.1 Niveau 2 :

Au niveau 2 du modèle OSI, la plupart des protocoles trouvés ici sont de plus en plus écartés au profit de protocoles plus polyvalents, comme peuvent l'être les protocoles des niveaux 3 à 7.

Le protocole PPTP :

L'idée du protocole PPTP (RFC2637) (Point To Point Tunneling Protocol) est de construire des trames avec le protocole PPP puis de les encapsuler dans un paquet IP. Cela permet à une connexion virtuelle point à point de connecter les deux réseaux via une liaison IP Internet. Cela fait supposer aux deux réseaux qu'ils sont liés par une ligne droite.

Il y a conservation des adresses des réseaux physiques dans la trame PPP cryptée, et cette trame est généralement transmise via Internet à l'autre réseau.**[4]**

B- L2F (Layer Two Forwarding)

Cisco a développé ce protocole vers 1996. L'IETF avait déjà une norme en 1998 avec la RFC 2341. Son fonctionnement est très similaire à PPTP. **[3]**

C- Le protocole L2TP (Layer Two Tunnelling protocol) :

C'est un protocole très similaire aux protocoles PPTP et L2F, et il est normalisé en RFC. Cette fois, les trames PPP sont encapsulées dans le protocole L2TP lui-même et les trames PPP encapsulent IP, IPX, NetBIOS ou d'autres paquets. Il est également principalement

Basé sur IPSec. Deux types de serveurs sont requis pour utiliser L2TP :

- LAC (L2TP Access Concentrator) : concentrateur d'accès L2TP. Il sert à fournir un moyen physique pour se connecter à un ou plusieurs LNS par le protocole L2TP. Il est responsable de l'identification et construit le tunnel vers les LNS. Il se trouve obligatoirement dans l'infrastructure du FAI (Fournisseur d'accès à Internet) de chaque utilisateur du VPN. Cela est donc très lourd (et cher) à mettre en place dans la mesure où il faut louer une place dans un serveur de connexion du FAI.
- LNS (L2TP Network Server) : serveur réseau L2TP, il assure la communication entre le réseau auquel il est connecté et les LAC vers lesquels il a un tunnel. Il se trouve généralement dans l'entreprise ou le service auquel appartient l'utilisateur distant.

L2TP est encapsulé dans des paquets UDP entre le LAC et le LNS et utilise le port 1701.

4. https://doc.lagout.org/network/VPN

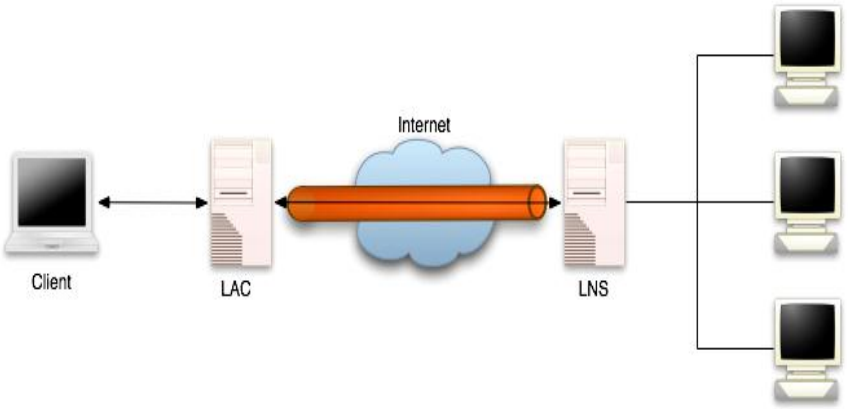

Figure I.5 - *architecture du Protocole L2TP***[5]**

5.2 Niveau 2 et 3 (MPLS) :

Le protocole MPLS *(*Multi Protocol Label Switching*)* est souvent considéré comme situé dans un niveau intermédiaire entre le niveau 2 et le niveau 3. C'est pourquoi on lui affecte souvent un niveau hybride 2.5 qui n'existe pas dans les couches OSI traditionnelles. Son placement en tant Que protocole de VPN peut être contesté lorsqu'il est utilisé dans ses fonctions de base. En effet il ne met pas en œuvre certaines fonctions de sécurité telles que le cryptage, ce qui est en principe un prérequis du VPN. **[6]**

5.3 Niveau 3 :

On retrouve ici le protocole de niveau 3, donc au niveau des paquets.

- **IPsec (Internet Protocol Security) :**

Est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP **[7].**

5.4 Niveau 4 + :

- **SSH (Secure Shell) :**

Est un protocole de niveau 4 et était souvent utilisé pour protéger des communications de type console (équivalent de Telnet) ou transferts de fichiers (de type FTP notamment). Son essor est

5. http://igm.univ-mlv.fr/~dr/XPOSE2007/cchamp01_VPN/L2TP.html

6. HTTP://WALLU.PAGESPERSO-ORANGE.FR/PAG-MPLS.HTM

7. SECRETARIAT GENERAL PARIS, LE 3 AOUT 2015,DE LA DEFENSE ET DE LA SECURITE NATIONALE, N° DAT-NT-003/ANSSI/SDE/NP, AGENCE NATIONALE DE LA SECURITE DES SYSTEMES

limité à la fois par le succès grandissant de SSL/TLS et par son champ d'application plus restreint. Néanmoins il reste encore un protocole à considérer pour certains usages. **[3]**

- **SSL/TLS (Secure Sockets Layer / Transport Layer Security) :**

Sont des protocoles de niveau 5, ces protocoles travaillent ensemble comme un protocole unique. Les deux sont utilisés pour construire une connexion VPN. Le navigateur Internet sert de client dans cette connexion VPN et l'accès des utilisateurs est limité à certaines applications uniquement plutôt qu'à un réseau entier, Les protocoles SSL et TLS sont principalement utilisés par les sites de vente en ligne et les prestataires de services, Un VPN SSL et TLS vous offre une session de navigateur sécurisée entre votre PC et le serveur d'applications. **[8]**

Network layer	IPsec **MPLS**
Data Link layer	PPTP, L2F ,L2TP
Physical layer	Scrambling, Hopping, Quantum Communications

Figure I.6 *: Les principaux protocoles de tunneling VPN*

6 Conclusion :

Dans ce chapitre nous avons présenté quelques notions de base nécessaires à la compréhension et au fonctionnement d'une solution VPN et leurs typologies, ainsi que les différents protocoles utilisés notamment IPsec, sur qui est porté notre choix dans notre travail.

Dans le chapitre suivant nous expliquons en détail ce protocole et son fonctionnement.

.

8. https://fr.vpnmentor.com

Sommaire

Chapitre II : Internet Protocol Security (IPsec)

1 Introduction :

Le protocole IPsec (Internet Protocol Security) est l'une des méthodes de création de VPN c'est-à-dire en s'appuyant sur une connexion sécurisée entre les systèmes informatiques réseau actuel.

IPsec a été conçu pour sécuriser le réseau de communications à partir de la couche 3 du modèle OSI, Il a été conçu de manière à être supporté par Ipv4 et a été intégré dans le protocole Ipv6.

Dans ce deuxième chapitre, nous définissons qu'est IPsec et sa normalisation, ensuite la théorie de travail du protocole et les méthodes utilisées seront expliquées.

2 Définition :

IPsec (Internet Protocol Security) est le mécanisme de sécurité Internet qui protège les échanges 'Données' sur un réseau IP à partir de la couche 3 du modèle OSI, il est souvent mentionné comme l'une des méthodes actuelles de développement, un VPN (réseau privé virtuel). Il établit la connexion entre deux systèmes informatiques, en toute sécurité, En exploitant un réseau établi. Il est spécifié par l'IETF (Internet Engineering Task Force) comme un système de normes ouvertes pour assurer des communications privées et sécurisées sur les réseaux IP grâce à l'utilisation des services de la sécurité cryptographique.

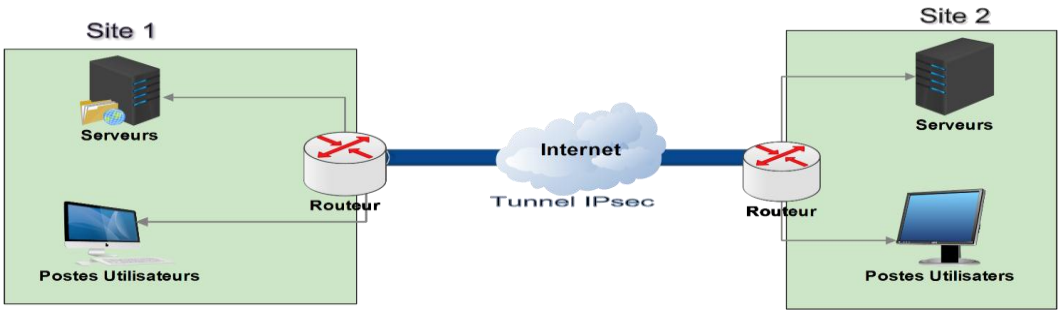

Figure II.1 - *Exemple d'emploi d'IPsec entre sites distants.* **[8]**

3 Normalisation d'IPsec :

- En 1994, l'IETF (Internet Engineering Task Force) a commencé à standardiser IPv6.
- L'IETF (Internet Engineering Task Force) débute la normalisation de IPv6 en 1994 IPsec natif sur IPv6 et optionnel sur IPv4.
- 1998 IPsec intègre son protocole d'échange de clés (IKE – Internet Key Exchange).
- Publication des RFC du protocole IPsec en 1995 puis 1998
- A la fin de l'année 1999 IPsec s'impose sur le marché

4 Le mode de fonctionnement du protocole IPSec :

Les implémentations IPsec sont basées sur les composants suivants :

4.1 SA (Security Association) :

Association de sécurité IPsec est une connexion qui fournit des services de sécurité au trafic qu'elle transporte. Il s'agit d'une structure de données utilisée pour stocker tous les paramètres associés à une communication donnée. Une SA est unidirectionnelle, Par conséquent, la protection des deux sens d'une communication classique nécessite deux associations, une dans chaque sens, La fonction d'une SA est d'enregistrer les informations suivantes pour chaque adresse IP avec laquelle l'implémentation IPsec peut communiquer.**[9]**

4.2 SPD (Security Policy Data base) :

Les protections fournies par IPsec sont basées sur des choix identifiés dans une base de données de politique de sécurité. Cette base de données est développée et gérée par un administrateur. Il permet de déterminer, pour chaque kit, quels services de sécurité seront fournis, s'il sera autorisé à passer outre ou à rejeter.

9 http://marc.boget.free.fr

4.3 SAD (Security Association Data base) :

Une base de données des associations de protection est utilisée pour surveiller les associations de sécurité actives. Il comprend tous les paramètres pertinents pour chaque SA et sera consulté sur la manière de traiter chaque paquet reçu ou émis.

5 Le principe de fonctionnement :

Le diagramme ci-dessous décrit tous les éléments ci-dessus (en bleu), leurs emplacements et leurs interactions.

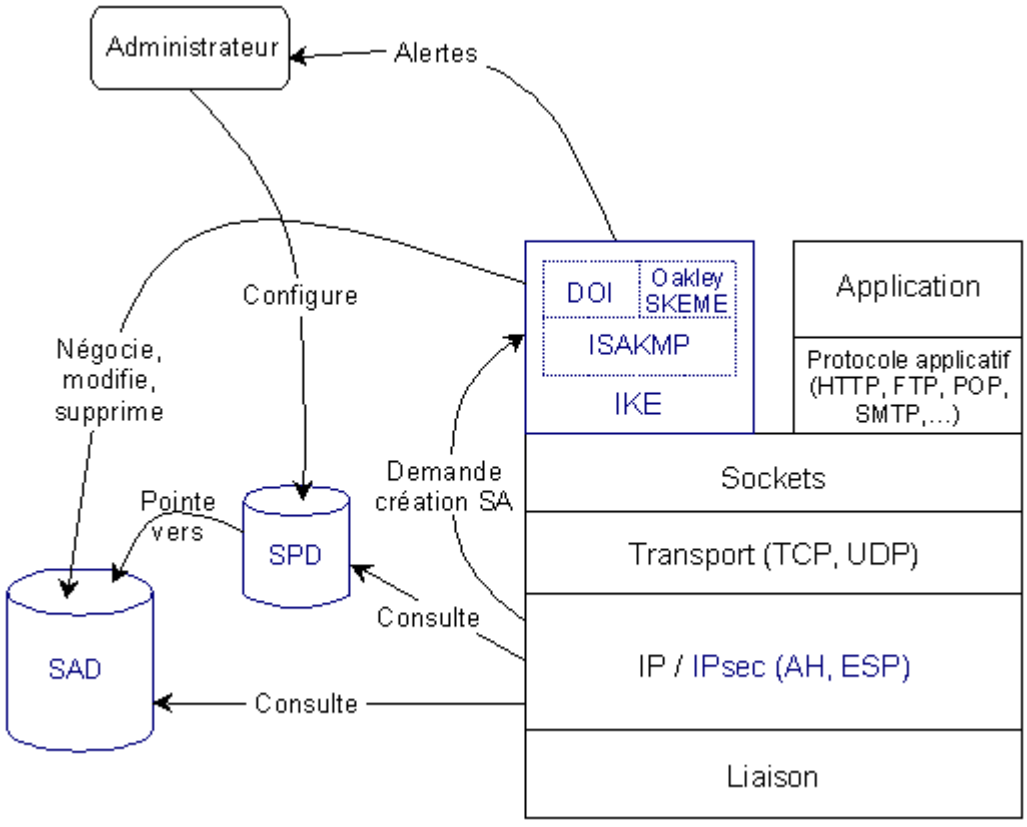

Figure II.2 : *principe de fonctionnement d'IPsec***[10]**

On distingue deux situations :

10. https://www.frameip.com/vpn/

5.1 Situation 1 : trafic sortant :

Lorsque la couche IPsec reçoit des données à envoyer, elle commence par vérifier la base de données de politique de sécurité (SPD) pour savoir comment gérer ces données. Si cette base indique que des mesures de sécurité doivent être appliquées au trafic, elle récupérera les caractéristiques nécessaires à l'AS correspondante et consultera la fondation SA (SAD), Si la SA nécessaire existe déjà, elle est utilisée pour gérer le trafic en question. Sinon, IPsec appellera IKE pour établir une nouvelle SA avec les fonctionnalités requises.

5.2 Situation 2 : trafic entrant :

Lorsque la couche IPsec reçoit un paquet en provenance du réseau, elle examine l'entête pour savoir si Ce paquet s'est vu appliquer un ou plusieurs services IPsec et si oui, quelles sont les références de la SA. Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet. Une fois le paquet vérifié et/ou déchiffré, la Spd est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par les politiques de sécurité.

6 Principe d'échange de clés internet (Internet Key Exchange) :

La gestion principale et la négociation des critères de sécurité sont effectuées par IKE (Internet Key Exchange). Au sens de réseaux privés virtuels. Ainsi, IPsec garantit la confidentialité, l'authenticité et l'intégrité des données transmises via un tunnel.

Le protocole IKE gère la sécurité en établissant un premier tunnel entre les deux machines. On s'appelle (le tunnel IKE). La deuxième étape consiste à créer des tunnels secondaires supplémentaires pour la Transmission des données utilisateur entre les deux machines.

L'authentification utilise des certificats électroniques pour vérifier que les machines sont utilisées Les sources et la destination conviennent mutuellement.

L2TP (Layer two Tunneling Protocol) négocie le tunnel si la protection de transport IPsec est définie correctement, ainsi la compression et les options d'authentification de l'utilisateur, puis procède à un contrôle d'accès basé sur l'identité de l'utilisateur.

- **ISAKMP/IKE**

ISAKMP, défini dans la [RFC 2408], est le protocole permettant la mise en place des associations de sécurité (SA) utilisables pour la mise en œuvre du tunnel chiffré. Ce protocole ne définit pas précisément les techniques d'authentification et d'échange de clefs utilisables mais fournit le contexte permettant de définir ces techniques.

Le protocole technique le plus utilisé du point de vue opérationnel semble être IKE, défini dans la [RFC 2409] à l'intérieur de l'ensemble normatif d'IPsec. D'autres protocoles sont possibles mais moins répandus, par exemple OAKLEY (défini dans la [RFC 2412] et utilisant une technique de type Diffie-Helmman) dont IKE est une variante simplifiée. **[11]**

7 Les deux modes d'échange IPsec :

La communication entre deux hôtes, protégée par IPsec, est susceptible de fonctionner suivant deux modes différents

7.1 Mode transport :

Ce mode est utilisé pour établir une communication entre deux hôtes prenant en charge IPsec. Une SA est établie entre les deux hôtes. Les en-têtes IP ne sont pas modifiés et les protocoles AH et ESP sont combinés entre cet en-tête et l'en-tête du protocole transporté.

Ce mode est également utilisé pour sécuriser une connexion point à point.

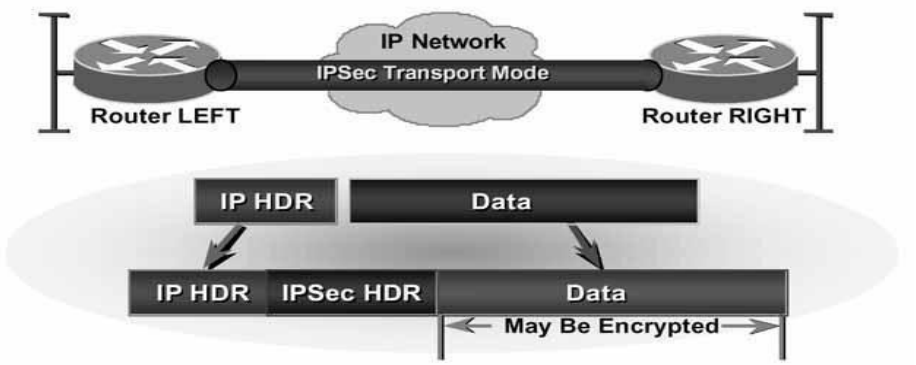

Figure II.3*:* IPsec mode transport**[11]**

7.2 Mode tunnel :

Ce mode est utilisé pour encapsuler les datagrammes IP dans IPsec. Le SA est connecté à un tunnel IP.

Ainsi, les en-têtes IP d'origine ne sont pas modifiés et un en-tête spécifique à IPsec est créé. Ce mode est souvent utilisé pour créer des tunnels entre des réseaux LAN distants. Il relie efficacement deux passerelles pouvant utiliser IPsec sans perturber le trafic IP des machines du réseau qui ne sont donc pas forcément prêtes à utiliser le protocole IPsec.

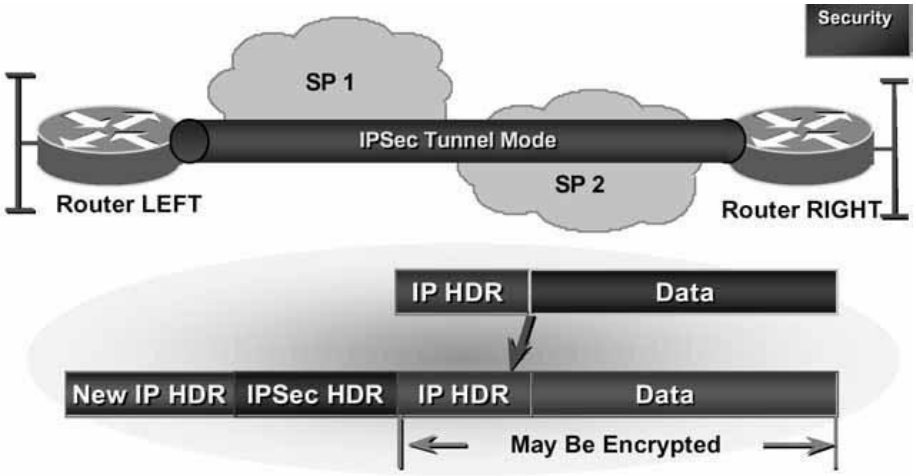

Figure II.4 - *IPsec mode tunnel*

11. https://webmail.mi.parisdescartes.fr

8 Les mécanismes AH et ESP :

IPsec utilise deux mécanismes de protection du trafic IP, les ‘protocoles’ AH et ESP, qui viennent au traitement IP classique :

8.1 AH (Authentification Header) :

AH est le premier et le plus simple protocole de sécurité des données (faisant partie de la spécification IPsec. Son objectif est de garantir :

- L’authentification : Les datagrammes IP reçus ont en fait été émis par l'hôte dont l'adresse IP est indiquée comme adresse source dans les en-têtes.
- L’unicité (optionnelle) : Un datagramme qui a été légitimement fourni et enregistré par un attaquant ne peut pas être réutilisé par l'attaquant, empêchant ainsi les attaques de rejet.
- L’intégrité : Les champs suivants du datagramme IP n'ont pas été modifiés depuis leur émission : données (en mode tunnel, cela inclut tous les champs, y compris les en-têtes, du datagramme IP encapsulé dans le datagramme sécurisé AH), version (4 en IPv4, 6 en IPv6), longueur de l'en-tête (en IPv4), longueur totale du datagramme (en IPv4), longueur des données (en IPv6)

AH ***assure*** :

- L’intégrité des données en mode non connecté
- L’authentification de l’origine des données
- De façon optionnelle assure la protection contre le rejet

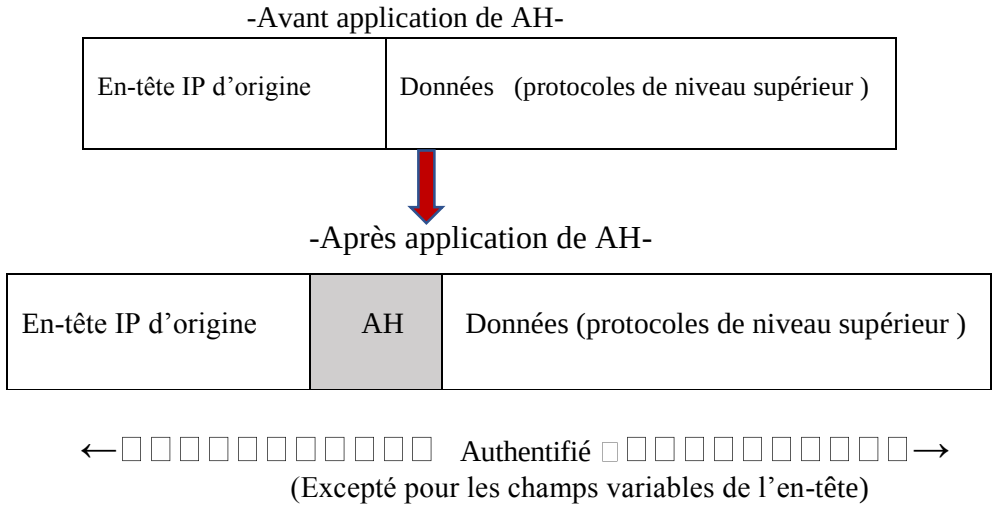

Figure II.5 - *Position de AH en mode transport (IPv4)*

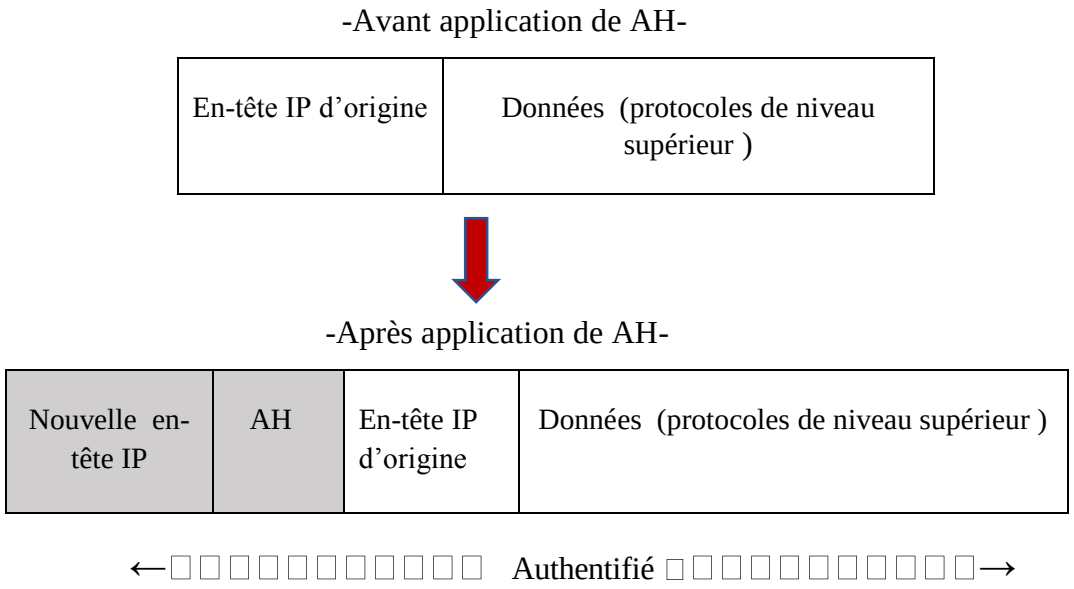

Figure II.6 - *Position de AH en mode tunnel (IPv4)***[12]**

12. IPsec : présentation technique – G. LABOURET

8.2 ESP (Encapsulating Security Payload) :

ESP est le deuxième protocole de sécurité des données qui fait partie de la spécification IPsec. Contrairement à AH, ESP ne couvre pas les en-têtes des datagrammes IP utilisés pour transmettre des informations. Les données sont sécurisées uniquement. En mode transport, il garantit :

- Le rôle principal est pour assurer la confidentialité, mais peut aussi assurer l'authenticité des données.
- Intégrité des données en mode non connecté et authentification de l'origine des données,

  • La confidentialité peut être choisie indépendamment des autres services, mais son utilisation sans intégrité / authentification (directement dans ESP ou avec AH) rend le trafic sensible à certaines formes d'attaques actives qui pourraient compromettre le service de confidentialité et Protection contre le rejet.

ESP ne définit pas d'algorithme de signature ou de cryptage spécifique, ceux-ci sont définis séparément, cependant, une implémentation conforme à la RFC 2406 est requise pour prendre en charge l'algorithme de cryptage DES en mode CBC et les signatures utilisant les fonctions de piratage MD5 et SHA-1.

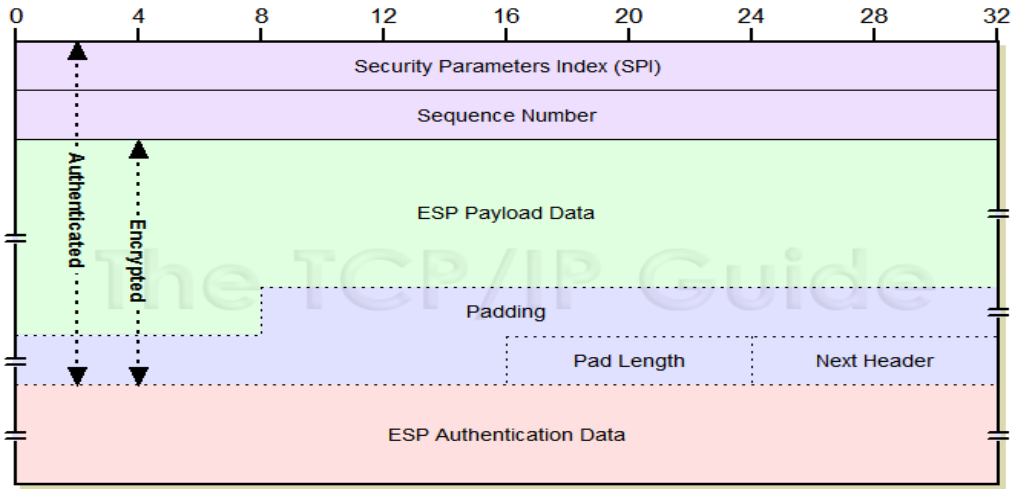

Figure II.7 - *Format de ESP* **[13]**

13. http://www.tcpipguide.com/free/t_IPSecEncapsulatingSecurityPayloadESP-4.htm

Le champ de remplissage (Padding) peut être nécessaire pour les algorithmes de chiffrement bloc par bloc ou pour faire correspondre le texte chiffré à un maximum de 4 octets.

Les données d'authentification ne sont disponibles que si ce service a été sélectionné.

Les figures ci-dessous indiquent la position de ESP et les services apportés en fonction du mode choisi (transport ou tunnel) :

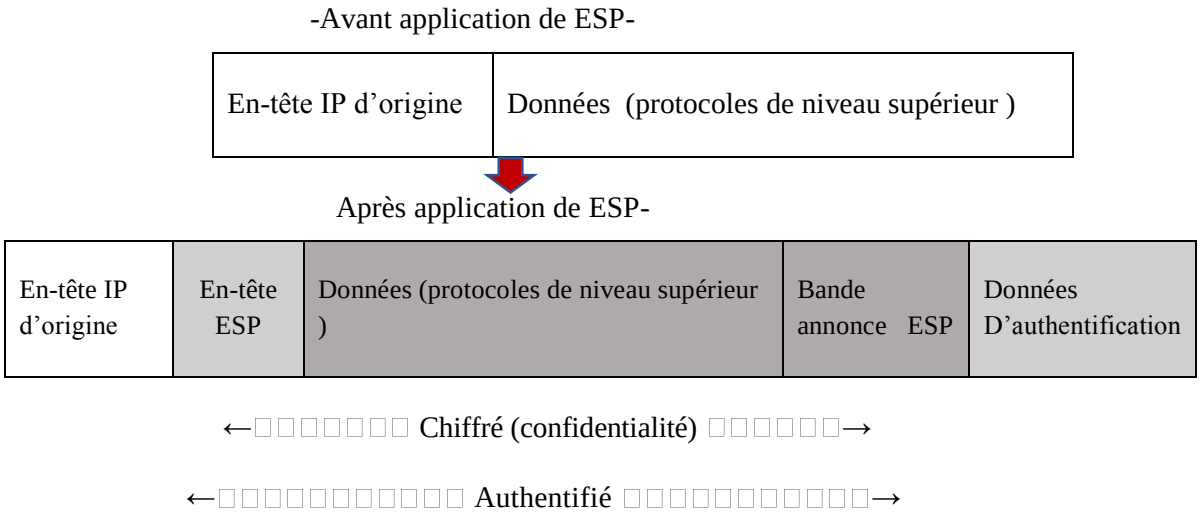

Figure II.8 -*Position de ESP en mode transport (IPv4)*

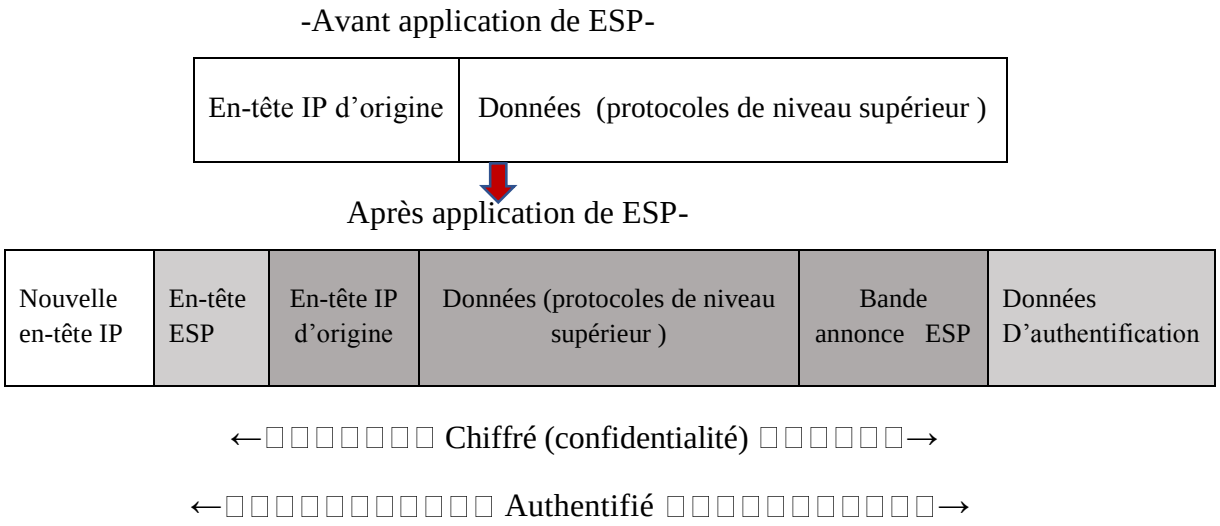

Figure II.9 - *Position de ESP en mode tunnel (IPv4)*

9 Conclusion :

Dans ce chapitre nous avons présenté les principales notions et concepts de base d'un tunnel VPN IPsec et son rôle de sécuriser la communication entre les entités différentes, et comment il fonctionne, Dans ce qui suit nous allons décrire les étapes que nous avons suivies pour implémenter cette solution dans un environnement virtuel.

Chapitre III

Implémentation et Test

Sommaire

Chapitre III : Implémentation et Test

1 Introduction :

Comme nous avons vu dans le premier chapitre il existe plusieurs types de tunnels VPN, parmi ces types nous avons choisi le tunnel VPN site à site pour l'implémenter dans un environnement virtuel sur une plate-forme Linux distribution Debian.

Dans ce chapitre nous expliquons les outils de réalisation de ce travail puis on va décrire les étapes de réalisation l'une après l'autre avec des tests qui démontreront son bon fonctionnement.

2 Les outils de réalisation

2.1 VirtualBox :

VirtualBox est un logiciel de virtualisation de systèmes d'exploitation. permettant l'utilisation des ressources matérielles de votre ordinateur (système hôte).

VirtualBox permet la création d'un ou de plusieurs ordinateurs virtuels (machines virtuelles) dans lesquels s'installent d'autres systèmes d'exploitation (systèmes invités).

Les systèmes invités fonctionnent en même temps que le système hôte, mais seul ce dernier a accès directement au véritable matériel de l'ordinateur.

Les systèmes invités exploitent du matériel générique, simulé par un « faux ordinateur » (machine virtuelle) créé par VirtualBox.

VirtualBox permet de faire fonctionner un ou plusieurs système(s) d'exploitation en même temps en toute sécurité.**[14]**

2.2 Debian :

Debian GNU/Linux est une distribution spécifique du système d'exploitation Linux disposant de nombreux paquets.

Debian GNU/Linux est :

- **Complète** : actuellement, Debian inclut plus de 58000 logiciels. Les utilisateurs peuvent choisir quels paquets installer ; Debian fournit un outil à cette fin. Vous pouvez trouver une liste et la description des paquets actuellement disponibles dans Debian sur n'importe quel miroir Debian.

14. https://doc.ubuntu-fr.org/virtualbox

- **Libre d'utilisation et de distribution** : il n'y a aucune exigence d'adhésion ou de paiement à un établissement pour participer à sa distribution et à son développement. Tous les paquets qui font formellement partie de Debian GNU/Linux sont libres d'être redistribués, généralement sous les termes de la licence GNU GPL.

Les archives FTP de Debian fournissent également environ 930 logiciels (dans les sections non-free et contribué), qui sont distribuables selon les conditions spécifiques incluses avec chaque paquet.

- **Dynamique** : avec environ 1343 volontaires qui contribuent constamment à la création et à l'amélioration du code, Debian évolue rapidement. Les archives FTP sont mises à jour deux fois par jour.

Parmi Ces fonctions principales qui distinguent Debian des autres distributions Linux, on peut citer :

- Liberté : Comme indiqué dans le Contrat social de Debian, Debian restera 100 % libre. Le projet Debian est très strict quant à la fourniture des logiciels vraiment libres.
- Le système de gestion de paquets de Debian : Le système entier ou n'importe quel composant individuel peut être mis à jour sans reformater, sans perdre les fichiers de configuration personnalisés et (dans la plupart des cas) sans redémarrer le système.
- Développement ouvert : alors que d'autres distributions Linux sont développées par des individus, des petits groupes fermés, ou des fournisseurs commerciaux. Debian est la seule distribution Linux majeure qui est développée comparativement par beaucoup d'individus qui ont pris pour cause commune de créer un système d'exploitation libre, dans le même esprit que Linux et d'autres logiciels libres.
- Le système d'exploitation universel : Debian fournit plus de 58000 paquets et fonctionne sur 10 architectures.**[15]**

2.3 StrongSwan :

StrongSwan est une implémentation IPsec Open Source. Il était à l'origine basé sur le projet Free S/WAN abandonné. Afin de disposer d'une plateforme IPsec stable sur laquelle se base les extensions de la norme X.509, les développeurs de ce dernier décidés de lancer le projet StrongSwan en 2005.

15. https://www.debian.org

Depuis lors, un nouveau démon IKE a été écrit dans un style de codage orienté objet moderne afin que la base de code actuelle ne partage plus le code avec son ancêtre. Initialement, ce démon ne supportait que IKEv2, tandis que IKEv1 était géré par une version étendue du démon Pluto de Free S / WAN. Mais comme l'adoption d'IKEv2 par d'autres fournisseurs a pris plus de temps que prévu, la prise en charge d'IKE v1 a été ajoutée au nouveau démon avec StrongSwan 5.0.0.

StrongSwan a été conçu à l'origine pour Linux, mais a depuis été porté sur Android, FreeBSD, Mac OS X, Windows et d'autres plates-formes.

- Pourquoi StrongSwan ?

Il existe plusieurs outils d'implémentation d'IPsec :

1. StrongSwan 2. Openswan 3. Libreswan…

Parmi ces outils nous avons choisi StrongSwan, puisqu'il concentre sur :

- Simplicité de configuration
- Méthodes de cryptage et d'authentification fortes
- Politiques IPsec puissantes prenant en charge les réseaux VPN vastes et complexes
- Conception modulaire avec une grande évolutivité **[16]**

3 Implémentation :

3.1 Préparation de l'environnement virtuel :

Avant de commencer notre travail, nous devons préparer l'environnement virtuel, et passons par les étapes suivantes :

- Installer l'outil de virtualisation (VirtualBox version **5.1**) : VirtualBox est un outil gratuit qui permet de virtualiser un système d'exploitation de votre choix.
- Dans cet outil nous avons installé quatre images ISO de systèmes d'exploitation Linux, (nous avons choisi la distribution Debian version **10.4**, deux machines configurer comme clients et les deux autres comme des routeurs).
- Maintenant nous pouvons configurer notre tunnel VPN basé sur IPsec à l'aide de l'implémentation StrongSwan (nous avons choisi la version **5.7.2**), entre les deux sites.

Nous avons appliqué notre travail sur l'architecture suivantes :

16. https://strongswan.net

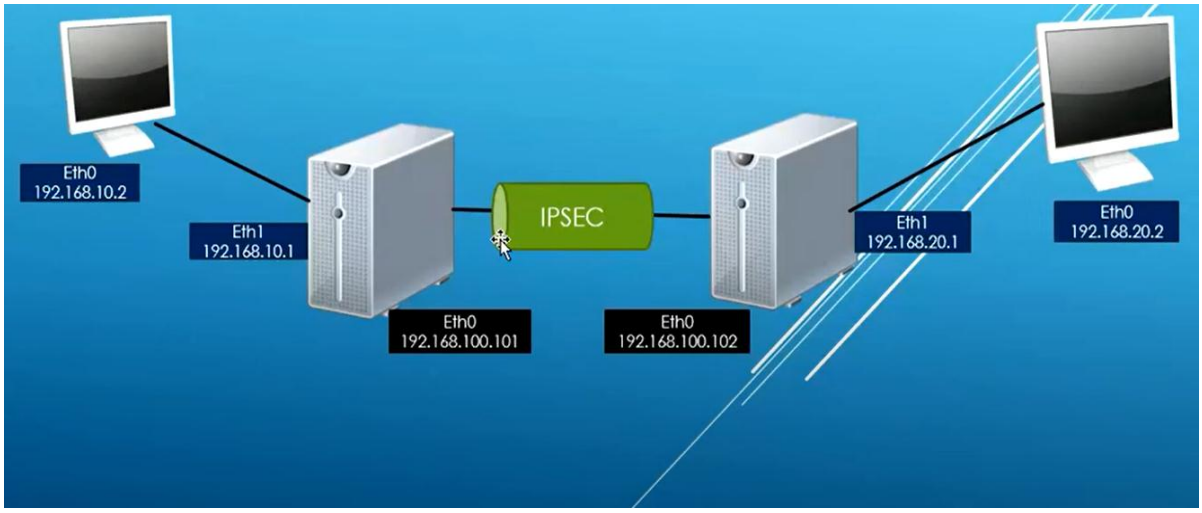

Figure III.1 – *L'architecture du tunnel IPsec site à site*

3.2 Adopter les interfaces des machines :

Dans VirtualBox cliquer sur settings puis Network après ajouter des interfaces aux quatre machines dans la partie adapter.

3.3 Activation et Installation du StrongSwan :

Nous décrivons en détail comment configurer des passerelles VPN IPsec de site à site à l'aide de StrongSwan sur les serveurs Debian, nous entendons que chaque passerelle de sécurité a un sous-réseau derrière elle. De plus, les pairs s'authentifient mutuellement à l'aide d'une clé pré-partagée (PSK).

3.3.1 Activation du transfert de paquets du noyau :

- Tout d'abord, vous devez configurer le noyau pour activer le transfert de paquets en ajoutant les variables système appropriées dans le fichier de configuration /etc/sysctl.conf sur les deux passerelles de sécurité, à travers la commande : `$ sudo vim /etc/sysctl.conf`
- Ensuite, chargez les nouveaux paramètres en exécutant la commande suivante :

`$ sudo sysctl -p`

```
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv6.conf.all.forwarding = 1
```

Figure III.2 - *Charger les paramètres du noyau Sysctl*

3.3.2 Affecter les adresses aux quatre machines :

Dans chaque machine Debian on va entrer dans le fichier : /etc/network/interfaces et affeceter les informations suivantes :

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback


auto enp0s8
iface enp0s8 inet static
        address 192.168.1.1
        netmask 255.255.255.0
        network 192.168.1.0

auto enp0s9
iface enp0s9 inet static
        address 192.168.3.1
        netmask 255.255.255.0
        network 192.168.3.0
```

Figure III.3 – *Affectation des adresses*

Après l'affectation des adresses aux sites et aux routeurs on va faire le routage statique entre les deux routeurs à travers la commande suivante :

```
~# ip r a 192.168.2.0/24 via 192.168.3.2
~#
```

3.3.3 Installer StrongSwan dans Debian :

- Mettre à jour le cache de votre package sur les deux passerelles de sécurité et installer le package StrongSwan à l'aide du gestionnaire de packages APT à travers la commande suivante :

```
$ sudo apt install strongswan
```

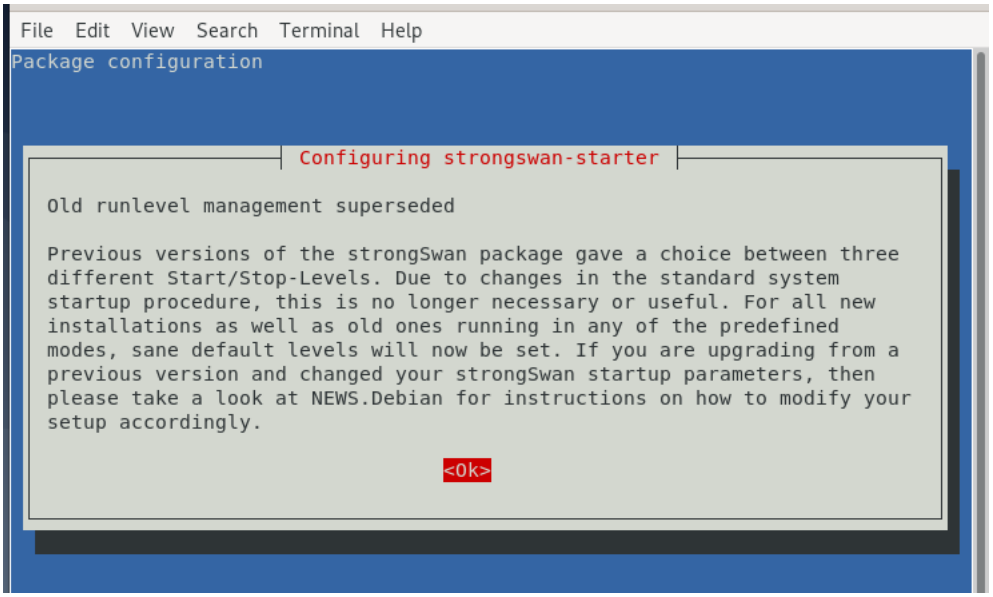

Figure III.4 - *Package de configuration*

3.3.4 Configuration des passerelles de sécurité :

- Ensuite, vous devez configurer les passerelles de sécurité sur les deux sites à l'aide du fichier de configuration /etc/ipsec.conf , à travers la commande `$ sudo nano /etc/ipsec.conf`

Et apportez les modifications suivantes sur les deux fichiers dans les deux machines (routeurs) :

```
config setup
        charondebug="all"
        uniqueids=yes
conn devgateway-to-prodgateway
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left=192.168.3.1
        leftsubnet=192.168.1.0/24
        right=192.168.3.2
        rightsubnet=192.168.2.0/24
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        aggressive=no
        keyingtries=%forever
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=30s
        dpdtimeout=120s
        dpdaction=restart
```

Figure III.5 - *Le fichier ipsec.conf dans le premier site .*

```
config setup
        charondebug="all"
        uniqueids=yes
conn devgateway-to-prodgateway
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left=192.168.3.2
        leftsubnet=192.168.2.0/24
        right=192.168.3.1
        rightsubnet=192.168.1.0/24
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        aggressive=no
        keyingtries=%forever
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=30s
        dpdtimeout=120s
        dpdaction=restart
```

Figure III.6 - *Le fichier ipsec.conf dans le deuxième site .*

Voici la signification de chaque paramètre de configuration :

- **config setup** : spécifie des informations de configuration générales pour IPsec qui s'appliquent à toutes les connexions.
- **charondebug** : définit la quantité de sortie de débogage de Charon qui doit être enregistrée.
- **uniqueids** :spécifie si un ID de participant particulier doit rester unique.
- **Conn devgateway-to-prodgateway :** définit le nom de la connexion.
- **type** : définit le type de connexion.
- **auto** : comment gérer la connexion lorsque IPsec est démarré ou redémarré.
- **keyexchange** : définit la version du protocole IKE à utiliser.
- **authby** :définit comment les pairs doivent s'authentifier.
- **left** : définit l'adresse IP de l'interface réseau public du participant gauche.
- **leftsubnet** : indique le sous-réseau privé derrière le participant gauche.
- **right** : spécifie l'adresse IP de l'interface de réseau public du bon participant.
- **rightsubnet** : indique le sous-réseau privé derrière le participant gauche.
- **ike** : définit une liste d'algorithmes de chiffrement / authentification IKE / ISAKMP SA à utiliser. Vous pouvez ajouter une liste séparée par des virgules.
- **esp** : définit une liste d'algorithmes de cryptage / authentification ESP à utiliser pour la connexion. Vous pouvez ajouter une liste séparée par des virgules.
- **aggressive** : indique s'il faut utiliser le mode agressif ou principal.
- **keyingtries** : indique le nombre de tentatives à effectuer pour négocier une connexion.
- **ikelifetime** : indique combien de temps le canal de saisie d'une connexion doit durer avant d'être renégocié.
- **lifetime** : définit la durée d'une instance particulière d'une connexion, de la négociation réussie à l'expiration.
- **dpddelay** : spécifie l'intervalle de temps avec lequel les messages R_U_THERE / échanges INFORMATIONAL sont envoyés au pair.
- **dpdtimeout** : spécifie l'intervalle de temporisation, après lequel toutes les connexions à un pair sont supprimées en cas d'inactivité.
- **dpdaction** : définit comment utiliser le protocole DPD (Dead Peer Detection) pour gérer la connexion

3.3.5 Configuration de PSK pour l'authentification Peer-to-Peer

Après avoir configuré les deux passerelles de sécurité, générez un PSK (Pre-shared-key) sécurisé à utiliser par les pairs à l'aide de la commande suivante : `$ sudo nano /etc/ipsec.secrets`

```
192.168.3.1 192.168.3.2 : PSK "covid19"
```

Figure III.7 - *Le PSK du premier site*

```
192.168.3.2 192.168.3.1 : PSK "covid19"
```

Figure III.8- *Le PSK du deuxième site*

Remarque : Le PSK utilisé dans les deux sites est le même.

- Redémarrez le programme IPSec et vérifiez son état pour afficher les connexions

avec la commande suivantes sur les deux machines :

```
root@vm1:~# ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.7.2 IPsec [starter]...
root@vm1:~#
```

Figure III.9 - *La commande restart*

Et lancer la commande $ ipsec statusall pour voir l'état de connexion entre les deux sites

```
Listening IP addresses:
  10.0.2.15
  192.168.3.2
  192.168.2.1
Connections:
devgateway-to-prodgateway:  192.168.3.2...192.168.3.1  IKEv2, dpddelay=30s
devgateway-to-prodgateway:   local:  [192.168.3.2] uses pre-shared key authentication
devgateway-to-prodgateway:   remote: [192.168.3.1] uses pre-shared key authentication
devgateway-to-prodgateway:   child:  192.168.2.0/24 === 192.168.1.0/24 TUNNEL, dpdactio
n=restart
Security Associations (1 up, 0 connecting):
devgateway-to-prodgateway[2]: ESTABLISHED 7 minutes ago, 192.168.3.2[192.168.3.2]...192
.168.3.1[192.168.3.1]
devgateway-to-prodgateway[2]: IKEv2 SPIs: 3155525da1095cf3_i 63e973f953752b92_r*, pre-s
hared key reauthentication in 7 hours
devgateway-to-prodgateway[2]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP
_1024
devgateway-to-prodgateway{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c0824f22_i cf0e3c2
c_o
devgateway-to-prodgateway{2}:  AES_CBC_256/HMAC_SHA1_96, 20076 bytes_i (239 pkts, 1s ag
o), 20076 bytes_o (239 pkts, 1s ago), rekeying in 38 minutes
devgateway-to-prodgateway{2}:   192.168.2.0/24 === 192.168.1.0/24
root@nacer:~#
```

Figure III.10- *La commande ipsec statusall*

Nous avons vu dans cette figure :

- Le tunnel est établi entre les deux sites 192.168.2.0/24 === 192.168.1.0/24.
- Les tunnels utilisent un PSK pour l'authentification, le PSK échangé entre les deux sites avec un IKE version 2.
- Le tunnel est établi avec une connexion nommée : **devgateway-to-prodgateway.**
- L'association de sécurité est activée.
- Les informations échangées sont cryptées par l'algorithme de chiffrement AES-CBC-256.

3.4 Tester la connexion entre les deux sites :

Lancer la commande ping entre les deux machines : Ping 192.168.1.2

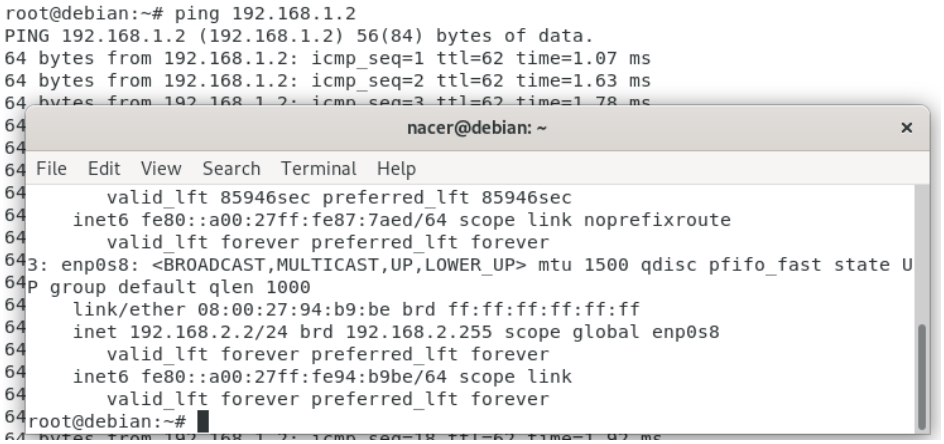

Figure III.11 – *Test de connexion entre les sites*

4 Conclusion :

Tout au long de ce chapitre, nous avons présenté tous les outils nécessaires pour la réalisation d'implémentation de notre tunnel VPN IPsec, et nous avons donné en détail toutes les étapes de la réalisation de ce tunnel, et nous avons terminé ce travail par un test afin de vérifier le bon fonctionnement du tunnel. Il est sans nul doute de mentionner la panoplie de combinaisons des paramètres à prendre en considération pour configurer le tunnel, ce qui dans certains cas peut fastidieux et difficile à comprendre tous les jeux possibles de ce tunnel.

Conclusion et perspectives

Dans le présent travail, nous avons essayé de donner une idée générale sur les tunnels VPN qui sont parmi les techniques majeurs utilisées dans la sécurité informatique en grande partie à cause de leur capacité de protéger l'information envoyée entre les sites ou les entreprises. Nous avons tenté, et sans prétendre l'exhaustivité, d'explique leurs fonctionnements et fonctionnalités ainsi que leurs typologies. Nous avons présenté les principaux protocoles des VPN aux niveaux 2 et 3et 7. Il faut cependant noter que pour, ce dernier point, il y a nuance entre le modèle OSI ou le niveau correspond à la couche session (5) alors du point de vue TCP/IP c'est la couche application et on fait allusion ici au protocole TLS/SSL. Nous avons touché la couche 3 qui contient IPsec sur qui est porté notre choix pour être étudié dans notre mémoire, nous avons défini cette technique et expliqué entre autre les composants.et les principes de ce protocole ainsi que son fonctionnement, puis nous avons implémenter cette technique dans une architecture site a site sur un environnement virtuel basé sur la plate-forme Linux (la distribution Debian), l'implémentation est gratuite grâce à l'outil StrongSwan.

Comme perspective à notre travail, nous voulons développer notre architecture site à site basée sur la plate-forme Linux seulement à une autre multi-plateforme comprenant les autres systèmes d'exploitation (Android, FreeBSD, Mac OS X, Windows et autres), et verrons les spécificités de chacune ainsi que leurs implémentations. De même, nous avons comme perspective de voir l'implémentation d'IPsec et son intégration dans le IPv6.

Bibliographie

[1] Réseau Privé Virtuel,

http://nicolas.roux.pagesperso-orange.fr/install/2003server/accesdistant.htm, Consulté (Mars 2020).

[2] Réseau Privé Virtuel, HTTPS://FR.VPNMENTOR.COM/BLOG/LES-DIFFERENTS-TYPES-DE-VPN-ET-QUAND-LES-UTILISER, Consulté (Mars 2020).

[3] J.P ARCHIER, « Les VPN, fonctionnement et mise en œuvre et maintenance des privés virtuels », 2 EME EDITIONS 11/12/2013

[4] Réseau Privé Virtuel, https://doc.lagout.org/network/VPN, Consulté (Avril 2020).

[5] VPN L2TP, http://igm.univ-mlv.fr/~dr/XPOSE2007/cchamp01_VPN/L2TP.html, Consulté (Avril 2020).

[6] MPLS, http://wallu.pagesperso-orange.fr/pag-mpls.htm, Consulté (Avril 2020).

[7] Secrétariat général Paris, le 3 août 2015,de la défense et de la sécurité nationale, N° DAT-NT-003/ANSSI/SDE/NP, Agence nationale de la sécurité des systèmes d'information.

[**8]** VPN, https://fr.vpnmentor.com, Consulté (Avril 2020).

[9] IPsec, http://marc.boget.free.fr, Consulté (Juin 2020).

[10] IPsec, https://www.frameip.com/vpn/, Consulté (Juin 2020).

[11] IPsec, https://webmail.mi.parisdescartes.fr, Consulté (Juin 2020).

[12] IPsec : présentation technique – G. LABOURET

[13] IPsec, http://www.tcpipguide.com/free/t_IPSecEncapsulatingSecurityPayloadESP-4.htm, Consulté (Juillet 2020).

[14] VirtualBox, https://doc.ubuntu-fr.org/virtualbox, Consulté (03 septembre 2020).

[15] Debian, https://www.debian.org, Consulté (07 septembre 2020).

[16] StrongSwan, https://strongswan.net, Consulté (08 septembre 2020).