الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

UNIVERSITÉ BADJI MOKHTAR - ANNABA
BADJI MOKHTAR – ANNABA UNIVERSITY

جامعة باجي مختار – عنابـــة

Faculté : Sciences de l'ingéniorat

Département : Electronique

Domaine : Sciences et technologie

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Mémoire

Présenté en vue de l'obtention du Diplôme de Master

Thème:

Configuration et mise en place de réseaux VPN

Présenté par : DOUMBIA FATOUMATA

Encadrant : *SAHRAOUI LEILA* *MCB* *UMBA*

Jury de Soutenance :

TAIBI MAHMOUD	Pr	UMBA	Président
SAHRAOUI LEILA	MCB	UMBA	Encadrant
TOUFIK HAFS	MCA	UMBA	Examinateur

Année Universitaire : 2020/2021

Résumé

Notre projet concerne la mise en place d'un réseau VPN à base de la technologie MPLS. L'objectif de notre travail est de proposer une architecture réseau sécurisée d'une Entreprise basé sur un site central et quatre sites distants. À l'aide du simulateur réseau GNS3, nous avons mis en place et configuré le réseau tunnel VPN avec la technologie MPLS. Des tests ont été réalisés afin de procédé au contrôle et pour assurer et garantir l'intégrité et confidentialité des données avec le protocole IPsec.

Mots clés : VPN, MPLS, GNS3, Wireshark, IPsec

Abstract

Our project concerns the establishment of a VPN network based on MPLS technology. The objective of our work is to provide a secure network architecture for a company based on a central site and four remote sites. Using the GNS3 network simulator, we set up and configured the VPN tunnel network with MPLS technology. Tests were carried out in order to carry out the control and to ensure and guarantee the integrity and confidentiality of data with the IPsec protocol.

Keys words: VPN, MPLS, GNS3, Wireshark, IPsec

ملخص

الهدف من عملنا هو توفير بنية شبكة آمنة لشركة تعتمد على .MPLS تعتمد على تقنية VPN يتعلق مشروعنا بتنفيذ شبكة باستخدام تقنية VPN ، قمنا بإعداد وتكوين شبكة أنفاقGNS3 موقع مركزي وأربعة مواقع بعيدة. باستخدام محاكي شبكة MPLS.

تم إجراء الاختبارات من أجل إجراء المراقبة ولضمان وضمان سلامة وسرية البيانات مع بروتوكول IPsec.

الكلمات المفتاحية

IPsec, VPN, MPLS ،GNS3 ، Wireshark

Après avoir rendu grâce à ***Allah le Tout Puissant et Le Tout-Miséricordieux*** *de m'avoir donné la force et le courage pour accomplir ce mémoire de fin d'étude ainsi que tout au long de mes années études, je tiens à remercier tous le staff du département Electronique de m'avoir accueilli au département et tout le groupe d'enseignants de la Filière Télécommunication de m'avoir permis de suivre ce cursus de « Master Réseaux et Télécommunications ». Je remercie aussi les personnes qui m'ont aidé pour mener à bien ce projet de stage et pour l'élaboration de ce mémoire, à commencer par mon encadreur* ***Mme SAHRAOUI Leila*** *pour sa disponibilité, son aide, ses conseils et encouragements.*

Je remercie également les membres de jury de m'avoir fait l'honneur en acceptant d'examiner et de juger mon travail Messieurs : ***Pr. TAIBI*** *et* ***Dr HAFS****.*

Je remercie très vivement tous mes professeurs, mes promotionnaires, ami(e)s et tous le cadre scientifique de l'université Badji Mokhtar-Annaba qui mont aider à mener à bien ce projet de fin d'étude.

Je dédie ce travail aux personnes qui sont chères à mon Cœur :

A commencer par ma mère DIALLO Fatoumata et à mon père DOUMBIA ADAMA pour leur amour inconditionnel et leur soutien sans faille.

***A tous mes parents** sans qui, je ne serais pas là où j'en suis maintenant.*

Pour tous leurs sacrifices, leurs prières, leurs amours et leurs soutiens.

***Mes Frères** pour leurs appuis et leurs encouragements permanents.*

*A toute **ma Famille et surtout à ma FAMILLE D'ALGERIE** pour leur soutien tout au long de mon parcours et tous les bons moments passé ensemble.*

*A Mes **Ami(e)s** ainsi que toutes **les personnes** qui m'ont soutenu et aidé tout au long de mes études.*

Liste des figures

Liste des figures

GNS3 : Graphical Network Simulator 3

AH : Authentification Heade

ESP : Encapsulation Security Payload

QOS : Quality Of Service

VPN : Virtual Private Network

L2F : Layer 2 Forwarding

L2TP : Layer Two Tunneling Protocol

PPTP : Point To Point Tunneling Protocol

ATM : Asynchronous Transfert Mode

FR : Frame Relay

IP : Internet Protocol

PPP : Point To Point Protocol

SDH : Synchronous Digital hierarchy

LSR : Label Switch Router

LER : Label Edge Router

FEC : Forwarding Equivalence classes

VPI : Virtual Path Identifier

VCI : Virtual Channel Identifier

SSL : Secure Socket Layer

TLS : Transport Layer Security

WAN : Wide Area Network

OSI : Open Sysyems Interconnection

VLAN : Virtual local Agrea Network

NAT : Network Address Translation

ACL : Access Control List

SSH : Secure Shell

ISP : Internet Service Providers

RTC : Réseau Téléphonique Commuté

GAN : Global Area Network

DSL : Digital Subscriber Line

FAI : Fournisseur d'Accès à Internet

AS : Système Autonome

RIR : Registre Internet Régional

GIX : Global Internet Echange

IXP : Internet echange Point

DNS : Domain Name System

NTP : Network Time Protocol

BGP : Border Gateway Protocol

MPLS : Multi-Protocol Label Switching

OSPF : Open Shortest Path First

RIP : Routing Information Protocol

SDN : Software Defined Network

NAS : Network Attached Storage

CPE : Custumer Premises Equipement (Equipement dans les locaux clients)

ADSL : Asymetric Digital Suubscriber Line

SDSL : Symetric Digital Suubscriber Line

BLR : Boucle Local Radio

IPX : Internetwork Packet Exchange

UDP : User Datagram Protocol

IPSec : Internet Protocol Security

HTTP : Hypertext Transfert Protocol

RFC : Requests For Comments

LER : Label Edge Router

LSR : Label Switching Router

LSP : Label Switched Path

IETF : Internet Engineering Task Force

ICV : Integration du Cycle de la Vie

BSD : Berkeley Software Distribution

Pcap : Packet capture

Liste des abréviations

TTY : TéléTYpe

IDS : Système de détection d'intrusion

SNMP : Simple Network Managemet Protocol

WEP : Wired Equivalent Privacy

WPA : WI-Fi Protected Access

ISAKMP : Internet Security Association and Key Managemet Protocol

HDLC : High-Level Data Link Control

FDDI : Fiber Distributed Data Interface

XML : Extensible Markup Language

ISDN : Integrated Service Digital Network

PSTN : Public Switched Telephone Network

RAS : Remote Access Server

RAC: Remote Access Concentrator

Sommaire

Introduction générale

Un réseau de communication a pour objectif d'échanger des informations et de partager des ressources matérielles et logicielles (imprimante, scanner, données, etc.). Suivant leur organisation, architecture, les distances, les vitesses de transmission et la nature des informations transmises, les réseaux font l'objet d'un certain nombre de spécifications et de normes. Plusieurs architectures de réseaux existent en pratique les réseaux étendus et réseaux d'opérateurs.

Les réseaux de communication assurent la connexion entre des sites distants des entreprises, leurs partenaires et leurs clients de façon transparente. Ils permettent la possibilité de communication et de partage de données avec une certaine sécurité et confidentialité.

L'accès à distance est une technologie complexe qui permet aux utilisateurs de maximiser leur plein potentiel sans être confinés à un seul endroit. La communication entre les sites distants, se fait généralement via Internet. Malheureusement, les sites web ne sont pas très bien protégées et vulnérable aux attaques des cybercriminels.

Plusieurs méthodes de sécurité ont été conçues pour remédier aux attaques malveillantes et aux cybercriminalités. Parmi ces méthodes, nous pouvons citer l'antivirus, la cryptographie symétrique et asymétrique, les pare-feu, les VLAN, le NAT, les ACL, VPN, …etc.

De nombreux internautes et sociétés choisissent d'utiliser les services VPN, En effet, une gamme de solutions de sécurité basée sur le réseau privé virtuel (VPN) existe, il peut garantir la sécurité et la confidentialité des données, qui circulent de manière cryptée par Internet afin d'éviter qu'une personne malveillante ne puisse intercepter les informations.

Un VPN a pour objectif de faciliter les communications entre entreprises partenaires ou les communications internes d'une entreprise dans le cas d'un réseau d'entreprise réparti géographiquement sur un, deux ou plusieurs sites distants, ainsi que les télétravailleurs qui ont besoin de se connecter aux ressources de leur entreprise. Un VPN permet de s'étendre virtuellement, grâce à la technologie de tunnel, un réseau privé ou le terminal du télétravailleur, un autre réseau privé, et ce au travers d'un réseau public.

Plusieurs types de VPN existent selon que l'opérateur du réseau public intervient ou pas dans la mise en œuvre du VPN. Il existe deux types, le mode transport et le mode tunnel. En utilisant la technologie MPLS (Multi Protocol Label Switching) par exemple, l'opérateur doit configurer les commutateurs MPLS de son infrastructure, de manière à garantir une certaine qualité de service à l'entreprise cliente.

Les données échangées dans le tunnel peuvent être sensibles et être la cible de cyber-attaques. Pour protéger les flux, on utilise diffèrent protocole de cryptage tels SSL/TLS, SSH, IPsec,

Dans ce concept ce travail est fondé sur la conception et la mise en place d'un réseau basé sur la technologie VPN. Nous avons créé une conception du réseau qui représente une entreprise avec un site central autour de 4 sites (villes) distant.

Pour implémenter les services de sécurité et protéger notre système VPN, le protocole IPsec pour IP Security peut être utilisé pour sécuriser les tunnels dans une interconnexion site-à-site ou bien pour sécuriser la connexion du poste nomade au réseau privé.

Ce mémoire est scindé en trois

-Le premier est consacré aux réseaux opérateurs leurs conception et les relations entre opérateurs et clients

-Le deuxième chapitre représente le réseau privé virtuel (VPN), les différentes topologies et architecture du réseau ainsi que protocoles utilisés afin de garantir la sécurité et confidentialité du réseau.

- Le troisième chapitre intitulé simulation et test basé sur configuration d'un réseau VPN avec une réalisation sous le logiciels GNS3 suivi d'essayes et de tests pour assurer l'intégrité et confidentialité des données. Des captures de trafic de données ont été réalisées avec le logiciel Wireshark pour confirmer le transfert de données.

Enfin, une conclusion générale vient clôturer ce mémoire, résumant les éléments essentiels qui ont été abordés.

Chapitre 1 : Les réseaux Opérateurs

Introduction

Ce chapitre est consacré aux réseaux opérateurs la topologie, l'architecture de base des réseaux et les connexions et les relations à l'intérieur du réseau ainsi que l'acheminement de l'information à travers les Réseaux opérateurs.

Un réseau de communication est l'ensemble des ressources matérielles et logicielles liées à la transmission et l'échange d'information entre différentes entités. Les réseaux font l'objet d'un certain nombre de spécifications et normes suivant leur organisation, architecture, les distances, les vitesses de transmission et la nature des informations transmises.

Les réseaux étendus et les réseaux d'opérateurs sont basés sur le concept d'un réseau étendu ou WAN (Wide Area Network), c'est un réseau couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière. Généralement, c'est un opérateur qui fait le lien avec des réseaux de communication distant en offrant des services de communications [1].

1. Types de réseaux

Les réseaux de communications peuvent être classes en fonction du type d'informations transportées et de la nature des entités impliquées ainsi que le domaine d'application. On distingue ainsi trois principales catégories de réseaux :

-Les réseaux informatiques (les données).

-Les réseaux de télécommunications (la voix, la parole).

-Les réseaux de télévision (l'image, la vidéo).

Actuellement, la technologie fournis la réunion de ces trois types de réseaux pour obtenir ce qui est appelé : réseaux multimédia.

1.1 Les réseaux d'opérateurs

L'objectif des réseaux d'opérateurs est de fournir des services de mise en réseau à ses clients. Un opérateur doit fournir ces services en fonction des besoins de ses clients et doit en assurer la bonne performance. Ainsi, il doit gérer le dimensionnement du réseau, le choix des technologies et la tarification appropriée.

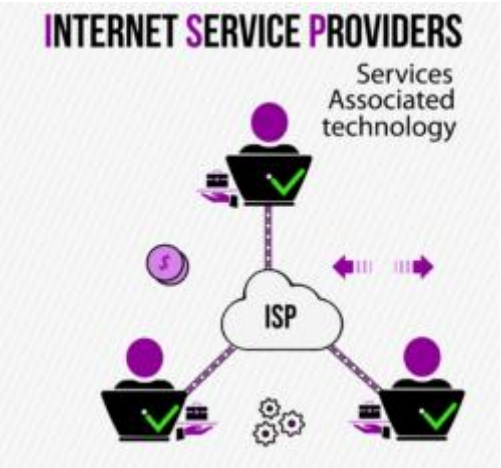

Figure 1.1 : réseaux d'opérateurs ISP [2]

- Les clients d'un opérateur peuvent être :

- Des particuliers qui souhaitent avant tout des services comme la téléphonie, la télévision et Internet

- Des entreprises qui ont des besoins divers comme la connexion réseau haut débit fiable ou encore la connexion de tous leurs sites distants.

Certains opérateurs peuvent même avoir d'autres opérateurs comme clients qui paient pour la location de la ligne. Le résultat est une hiérarchisation de différents réseaux d'opérateurs.

- L'une des offres les plus prisée des particuliers est le triple play. Ce service regroupe Internet, la télévision et la téléphonie [2].

D'autres nouveaux services comme la vidéoconférence et l'Internet des objets se développent de plus en plus.

1.2. La topologie des réseaux d'opérateurs

La topologie typique des réseaux d'opérateurs est divisée en 3 parties : réseau cœur, réseau de collecte et réseau d'accès.

Le réseau cœur est le « backbone » (ou colonne vertébrale en français) du réseau. Il transporte beaucoup de trafic sur de longues distances. Il utilise des lignes et des technologies à haute bande passante pour transférer le trafic rapidement.

Le réseau de collecte ou réseau métropolitain constitue des liens de très haut débit raccordés aux backbone nationaux pour collecter et acheminer le trafic des agglomérations.

Le réseau d'accès se réfère à la partie du réseau reliant l'abonné aux services de télécommunication. Il fournit le dernier lien vers l'utilisateur. On l'appelle aussi boucle locale, réseau de distribution ou dernier kilomètre du réseau.

Sur le schéma nous voyons la représentation de la topologie de réseau. Le backbone relie les réseaux métropolitains, qui à leur tour connectent les réseaux d'accès. Ceux-ci raccordent ensuite les abonnés [2].

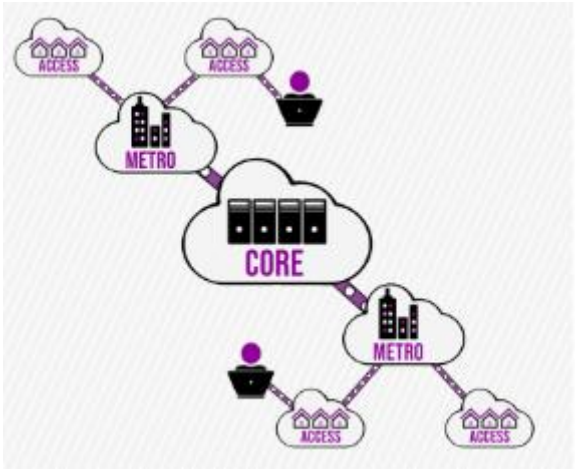

Figure 1.2 : la topologie des réseaux d'opérateurs [2]

2. L'architecture d'Internet

Internet est un ensemble de réseaux hétérogènes contrôlés par des acteurs divers. Cela provient de nombreux facteurs, mais l'un des plus marquants est sans aucun doute la construction d'Internet. A l'image de la connexion téléphonique RTC figure 2.3

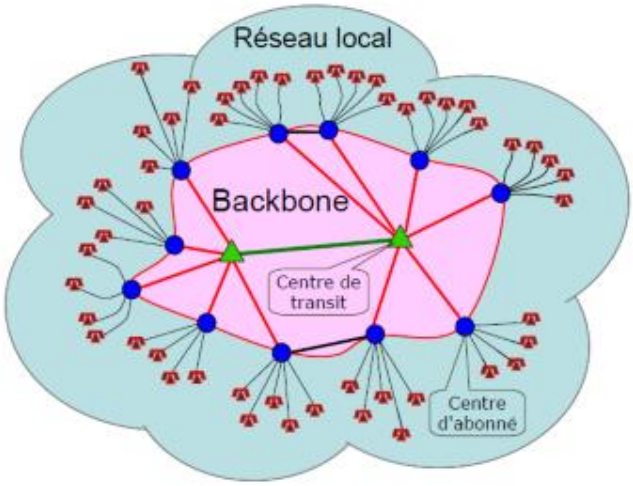

Figure 1.3 : Structure du RTC [1]

2.1. Classification

Selon la distance maximale reliant deux points, ces réseaux peuvent être classes en cinq catégories. [1]

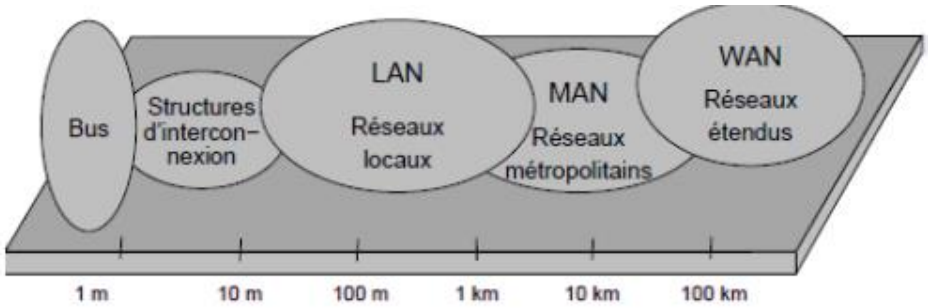

Figure 1.4 : Catégories des réseaux informatiques [1]

2.1.1. Bus

Ils interconnectent les processeurs, les mémoires, les entrées-sorties, connexion des équipements, un PC ou plus probable encore un périphérique comme une imprimante. Pour une distance séparant les composants est inferieurs à 1 mètre.

2.1.2. Structures d'interconnexion

Ils permettent d'interconnecter plusieurs calculateurs dans une même pièce pour former des réseaux fermes a très haut débit allant jusqu'à plusieurs centaines de Mbit/s pour une distance

ne dépassant pas les quelques mètres. On parle ici du PAN (Personal Area Network), utilisés pour des distances de quelques mètres Pour interconnecter les équipements personnels : téléphone mobile, portables, tablettes, etc.

2.1.3. LAN (Local Area Network)

Ou réseaux locaux, utilises pour des distances de plusieurs centaines de mètres. Ils interconnectent les équipements informatiques d'une même entreprise, d'une même université, et ils assurent un débit de quelques Mbit/s à quelques Gbit/s.

2.1.4. MAN (Métropolitain Area Network) :

C'est les réseaux métropolitains, utilisés pour l'interconnexion de plusieurs sites dans une même ville ou l'interconnexion des réseaux locaux situés dans des bâtiments différents.

2.1.5. WAN (Wide Area Network) :

Ou réseaux étendus, ils interconnectent des sites et des réseaux à l'échelle d'un pays et ils peuvent être terrestres ou satellitaires. Enfin au-delà de ça, Internet est considéré comme un Global Area Network (GAN).

3. Les connexions réseaux

Une autre manière d'envisager les réseaux, c'est via le rôle du réseau. Certes, il y a les réseaux locaux et les réseaux domestiques des utilisateurs privés… mais il faut les connecter à Internet. [3]. Tout d'abord vous avez les réseaux qui offrent l'accès aux utilisateurs finaux :

3.1. Les réseaux d'accès

Parmi ceux-ci on a les réseaux xDSL, la 4G ou encore la "fibre". Dans les réseaux téléphoniques, on utilisait avant le terme boucle locale. Il y a les réseaux qui permettent d'alimenter les réseaux d'accès que l'on nomme aujourd'hui le backhaul, équivalent du réseau de collecte dans le réseau (un lien satellite qui alimente des relais 4G)

3.2. Les réseaux de cœurs

Aussi appelés core, qui sont là où l'opérateur rend son service, comme le réseau de cœur d'un opérateur 4G ou d'un fournisseur d'accès Internet.

L'interconnexion des cœurs de réseau ou les grands liens dans les cœurs se dit souvent **backbone**, dorsale en français (très peu utilisée) comme le câble sous-marin transatlantique.

3.3. Relations entre les opérateurs

Internet est un réseau de réseaux. Le client ayant besoin d'Internet se connecte à un opérateur qui lui-même est connecté à un autre FAI (ou ISP en anglais) et ainsi de suite. En plus de fournir différents services à son client, un opérateur doit également gérer les interconnexions avec les autres opérateurs. [2]

Différents types de relations existent entre les opérateurs :

3.3.1 Le Transit

Est une option payée lorsque le Fournisseur d'Accès à Internet de niveau supérieur facture le FAI qui l'achète

3.3.2. Le Peering

Ou appairage en français est une interconnexion entre deux FAI de même niveau. Lorsque deux opérateurs échangent beaucoup de trafic pour lequel ils paient un fournisseur de niveau supérieur, ils établissent alors un « peering » direct pour faire des économies et ne plus passer par leur FAI supérieur.

3.4. Système Autonome (AS)

Il n'y a pas une entité unique qui aurait tous les réseaux d'Internet mais une multitude. Une entité administrative (Free, Orange, Google, ou Apple) qui gèrent un nombre important de réseaux forme un (parfois plusieurs) Système Autonome dit AS.

Dans un AS, les équipements et les réseaux sont gérés par la même entité et utilisent un protocole de routage commun. Souvent les AS offrent un service : cela peut être des services webs mais aussi l'accès à Internet. Dans le premier cas on parle de Fournisseur de Services (Google) et dans l'autre cas de Fournisseurs d'Accès Internet. Les AS ont des numéros codés sur 32 bits depuis 2006 et affectés par les RIRs comme pour les plages d'adresses IP.

Un AS a aussi un rôle très fort dans Internet : les interconnexions entre AS font le liant d'Internet. En fonction de son rôle dans l'interconnexion, on décompte différents types d'AS :

3.4.1 Stub AS

C'est un AS qui dépend d'un seul autre AS pour se connecter aux autres, un cul de sac dans Internet.

3.4.2. Un AS Multi-domicilié

C'est un AS qui utilise plusieurs AS pour se connecter aux autres, toutefois il ne permet pas aux autres de l'utiliser pour s'interconnecter.

3.4.3. Un AS de transit

C'est un AS dont le rôle est d'interconnecter d'autres AS.

Il existe enfin des ASs très particuliers : AS Internet Exchange Point qui sont des AS dédiés à être le point de rencontre des autres AS.

Comme vous l'aurez compris, l'enjeu est d'interconnecter les ASs. Deux méthodes, très différentes sont utilisées :

- La relation commerciale qui consiste à payer un AS de transit pour acheminer le trafic provenant ou à destination de son AS
- Le peering ou relation d'égal à égal qui consiste à échanger directement entre deux AS ses trafics provenant d'un AS vers l'autre.

Il faut être en mesure d'interconnecter physiquement les deux AS. Cela se fait dans des points de rencontre des AS nommés (Global) Internet échange Point (IX ou IXP ou GIX) qui peut être

géré par un AS transparent, AS Internet Exchange Point qui regroupe les différents acteurs majeurs du GIX.

L'IX est avant tout un point de peering mais rien n'y empêche la mise en place des relations commerciales. Chaque accord est traité directement entre les AS. L'IX peut aussi être le lieu

- De DNS

- De services différents (NTP, web, sécurité, VLAN, VPN, multicast…) Peut être localisé en différents endroits, bâtiments …

-Un protocole BGP (Border Gateway Protocol) utilise des équipements et commutateurs des accords qui peuvent être très précis sur : Les débits échangés, les pics autorisés, les taux d'utilisation.

5. Réseaux opérateurs et acheminement des l'information

Les réseaux d'opérateurs permettent de véhiculer différents types d'informations : voix, vidéo, image, graphique, etc.

Aujourd'hui on tend vers un réseau unifié où les technologies IP (Internet Protocol), MPLS (Multiprotocol Label Switching) et d'autres, permettent de combiner réseau de télécommunication et réseau informatique, initialement séparés. L'idée de la convergence est de fournir différents services à partir du même support. On parle de convergence vers un réseau unifié.

Dans les années 90, motivé par la convergence, le choix des opérateurs télécoms s'est porté vers une solution appelée ATM pour Asynchronous transfer mode (ou mode de transfert asynchrone). C'est une technologie de commutation de cellules qui prend en charge la qualité de service (ou QoS en anglais). La migration était bien avancée mais c'était sans compter sur le succès du réseau IP (Internet Protocol) qui est venu tout bouleverser. ATM était en comparaison trop complexe et les opérateurs ont de plus en plus adopté les solutions IP.

Dans le réseau cœur, les nœuds de transfert de données reçoivent des informations à transmettre, découpées en paquets. Ces nœuds doivent déterminer le chemin de chaque paquet reçu et le transmettre à la bonne sortie. Lorsqu'un paquet arrive, il est placé dans une file d'attente d'entrée où son en-tête est examiné, puis un processus identifie l'interface de sortie appropriée. Enfin, chaque paquet est ensuite placé dans la file d'attente de sortie.

Deux techniques de transfert de données utilisées dans le réseau cœur : **le routage de paquets** et **la commutation de paquets**.

5.1. Le routage de paquets

Regardons tout d'abord le routage de paquets. Le routage vient d'Internet pour lequel il existe de nombreux protocoles : OSPF (Open Shortest Path First), RIP (Routing Information Protocol), BGP, etc.

Le routeur analyse l'adresse de la destination dans l'en-tête du paquet. Pour trouver une route, il se réfère à sa table de routage dynamique. Celle-ci est gérée par des algorithmes de routage spécifiques. Le routeur cherche la correspondance entre l'adresse de destination et les entrées dans sa table de routage [4].

Les routes empruntées par les paquets peuvent donc changer de manière dynamique et les paquets d'un client peuvent suivre différentes routes.

5.2. La commutation de paquets

Avant la révolution du numérique, les réseaux télécoms utilisaient une technique appelée commutation de circuits. La commutation de circuits établissait exclusivement un circuit entre un émetteur et un récepteur. Ce circuit ne servait que cet équipement, ces lignes ne pouvaient pas être utilisées pour d'autres communications. C'était donc un gaspillage de ressources !

Ainsi, de nouvelles techniques sont apparues : le transfert de messages, la commutation de paquets, la commutation de cellules, etc.

La commutation de paquets venant du monde des Télécoms. Avec la commutation de paquets, le chemin vers une destination est prédéterminé avant même que la communication passe, grâce à une procédure appelée signalisation. Ce chemin est également appelé circuit virtuel (VC). Une fois ce chemin établi, tous les paquets de cette destination suivent ce chemin.

À leur arrivée, les paquets sont tagués sous différents labels. La correspondance entre les étiquettes (labels, tag) et les interfaces de sortie se situent sur la table d'acheminement du commutateur. Cette correspondance est prédéterminée et reste fixe.

Notez que dans le cas où un lien échoue, le processus de signalisation pour l'établissement d'un chemin recommence et un nouveau chemin est établi. En résumé, lorsque le paquet arrive, il est transmis à l'interface de sortie appropriée en fonction de son « label ».

5.3. Comparaison des deux approches

Si on prend le modèle OSI comme référence (de l'anglais Open Systems Interconnexion) figure 1.5, le routage est réalisé dans la couche 3 et la commutation de paquets est réalisée dans la couche inférieure (2).

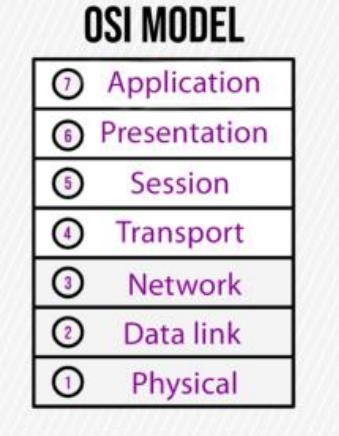

Figure 1.5 : Le Modèle ISO [2]

Avec le routage, les paquets d'un flux donné peuvent suivre des chemins différents, mais avec la commutation de paquets, les paquets d'un même flux suivent un chemin prédéterminé et fixe [2].

Le routage est généralement plus lent parce qu'il nécessite le traitement du paquet dans des couches supplémentaires, si on se réfère au modèle OSI. De plus, la gestion dynamique des tables de routage est complexe et lente. Avec la commutation de paquets, une fois qu'un chemin est déterminé et ouvert, les commutateurs ont une vitesse supérieure de 10 à 50 fois par rapport aux routeurs. Cependant, aujourd'hui, l'avantage de la vitesse n'est plus valable en raison de l'arrivée des giga- routeurs [4].

Il est plus facile d'assurer la qualité de service avec la commutation de paquets car les chemins empruntés restent identiques. Il est également plus aisé d'attribuer des ressources exigées par des flux et assurer les garanties QoS avec les chemins fixes.

Toutefois, avec la commutation par paquets, l'établissement et la signalisation du chemin sont complexes et coûteux par rapport au routage.

Aujourd'hui, le routage et la commutation sont présents/employés tous les deux, mais leur mise en œuvre a évolué avec l'apparition du protocole IP (Internet Protocol) dans les deux technologies.

Dans les dernières années, les techniques de routage ont peu changé. Cependant, il y a eu beaucoup d'évolution des techniques de commutation : du protocole X.25 au protocole MPLS. Et cela pourrait continuer avec/vers le Software Defined Networking (SDN).

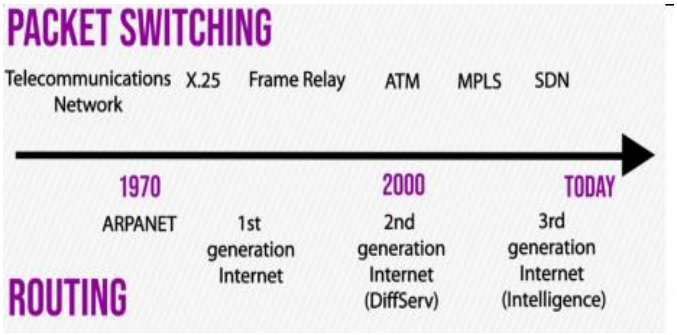

Figure 1.6 : Evolution des techniques de commutation et de routage [2]

5.4. La technologie MPLS

La technologie MPLS très répandue pour la commutation de paquets.

MPLS est une technologie d'acheminement de paquets très répandue pour la commutation de paquets. Le protocole MPLS fonctionne généralement entre la couche 2 (couche de liaison de données) et la couche 3 (couche réseau) du modèle OSI. Ainsi, elle est parfois appelée protocole de couche 2.5 [2].

La commutation des paquets est basée sur la labellisation (tag ou étiquette). Une étiquette est ajoutée au paquet, puis le routeur suivant transmet ce paquet uniquement en fonction de son étiquette. Le transfert de paquets MPLS à l'aide de labels/étiquettes aboutit à de nombreuses fonctionnalités intéressantes. Le MPLS peut transporter n'importe quel protocole. Aussi, il permet de gérer l'ingénierie de trafic, d'assurer la qualité de service, ou encore de fournir des services comme le VPN.

6. Conclusion

Les réseaux opérateurs on fait l'objet de ce chapitre ou nous avons mis l'accent sur leur topologie, l'architecture de base des réseaux et les connexions ainsi que les interconnexions à l'intérieur du réseau. Les Réseaux opérateurs assure la communication des informations à travers avec de multiple système et technologie tels que l'MPLS et le VPN.

Effectivement, Les services que proposent les entreprises sont essentiellement des réseaux privés virtuels ou VPN. Un VPN est une connexion avec un site distant donnant l'impression que nous sommes dans le même réseau local même si nous sommes connectés à distance. Il existe plusieurs types de VPN, ceux-ci peuvent offrir par exemple la connectivité Ethernet internationale. Les réseaux VPN et la technologie MPLS feront l'objet du chapitre 2.

Chapitre2 : Réseau Privé Virtuel (VPN)

Introduction

Ce chapitre est consacré au réseau privé virtuel (VPN), les type de réseaux VPN, les différentes topologies et architecture du réseau ainsi qu'aux protocoles associés et utiliser par les opérateurs dans les applications et les réseaux publics

Les grandes sociétés et les groupements d'entreprises cherchent à pouvoir se connecter à des sites distants et à communiquer avec leurs clients et partenaires de façon transparente. Le réseau privé virtuel (VPN) a pour tâche de permettre de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local. C'est dans cette vision que de nombreuses entreprises l'utilisent afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise à distance et hors lieu de travail.

1. Le réseau privé virtuel

1.1 Définition d'un VPN

Le réseau privé virtuel représente un réseau privé virtuel qui est un réseau crypté dans le réseau internet permettant à une société dont ses locaux sont géographiquement dispersés de communiquer et partager des documents d'une façon complètement sécurisée, comme s'il n'y avait qu'un local avec un réseau interne [13].

Le VPN est basé sur un protocole appelé protocole de tunnélisation (tunneling). Ce protocole permet aux données de circuler d'un site à l'autre en étant sécurisées par des algorithmes de cryptographie. Le terme «tunnel» est utilisé dans le sens où entre l'entrée et la sortie du VPN, les données sont cryptées [10]

1.2 Topologie des VPN

Les VPN s'appuient principalement sur Internet comme support de transmission, avec un protocole d'encapsulation et un protocole d'authentification, au niveau des topologies, on retrouve des réseaux privés virtuels en étoile, maillé ou partiellement maillé [11].

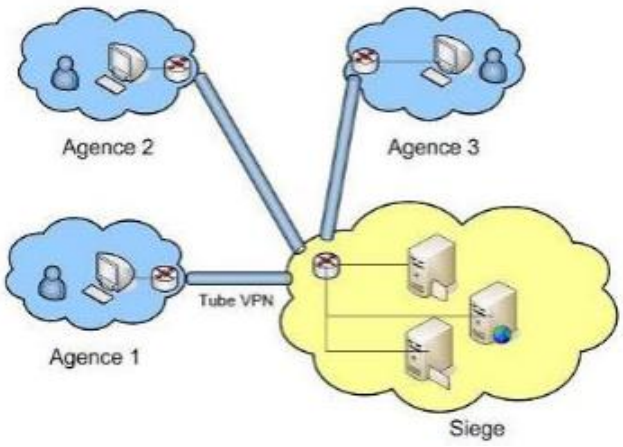

Figure 2.1 : VPN en étoile

Dans cette topologie toutes les ressources sont centralisées au même endroit et c'est à ce niveau qu'on retrouve le serveur d`accès distant ou serveur VPN, dans ce cas de figure tous les employés du réseau s'identifient ou s'authentifient au niveau du serveur et pourront ainsi accéder aux ressources qui se situent sur l'intranet.

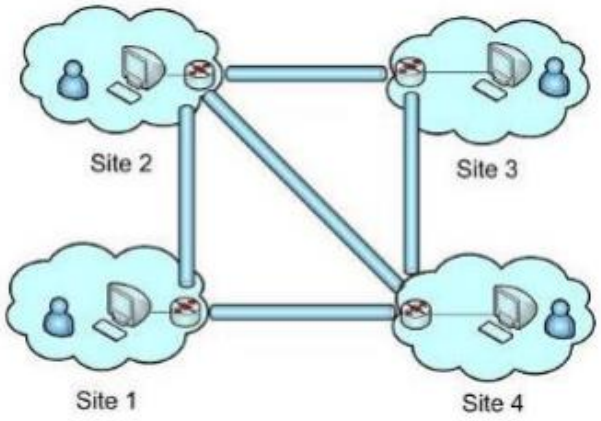

Figure 2.2 : VPN maillé

Dans cette autre topologie les routeurs ou passerelles présents aux extrémités de chaque site seront considérés comme des serveurs d'accès distant, les ressources ici sont décentralisées sur chacun des sites autrement dit les employés pourront accéder aux informations présents sur tous les réseaux [11].

1.3. Les différents types de VPN

Parmi ces différents types on peut citer les :

- Le VPN d'accès
- Intranet VPN
- Extranet VPN

1.3.1 Le VPN d'accès

Le 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 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.

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

- La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée Ce qui peut poser des problèmes de sécurité.
- Sur la deuxième méthode Ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs [12].

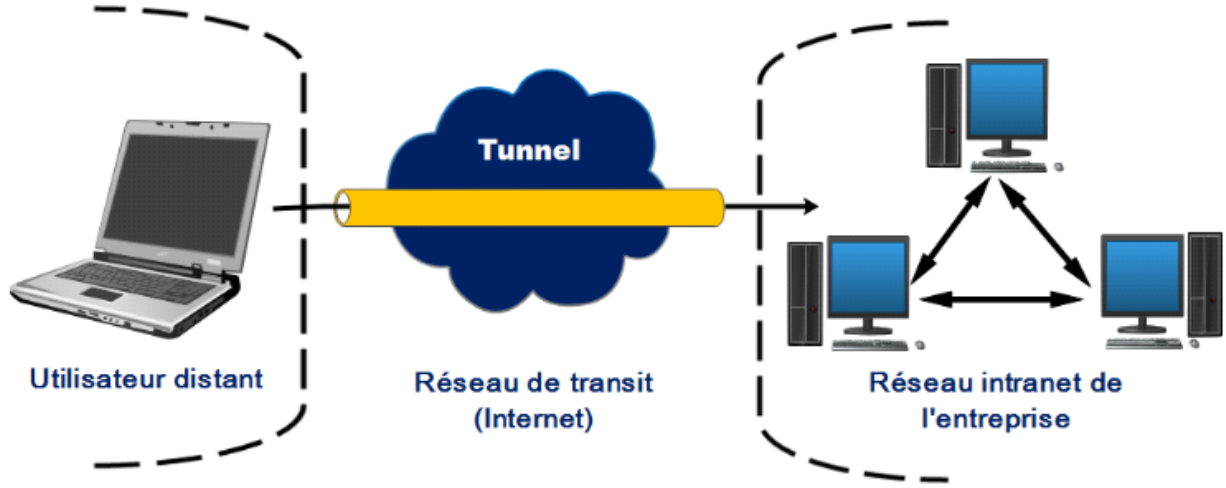

Figure 2.3 : Architecture d'un VPN d'accès [9]

1.3.2 L'intranet VPN

Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants, l'intranet VPN est utilisé pour relier au moins deux intranets entre eux toutes en garantissant la sécurité, la confidentialité et l'intégrité des données.

Un VPN permet aux utilisateurs éloignés de se connecter à un réseau. Dans ce cas, on parle de l'intranet VPN car il s'agit aussi de connecter plusieurs clients distants à un site de l'entreprise. [12]

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.

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 [9].

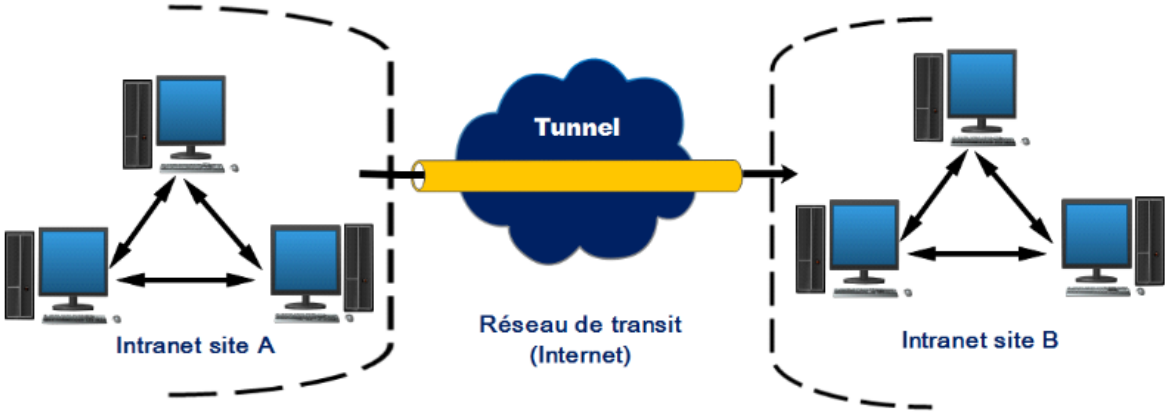

Figure 2.4 : Architecture d'un VPN intranet [9]

1.3.3 L'extranet VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

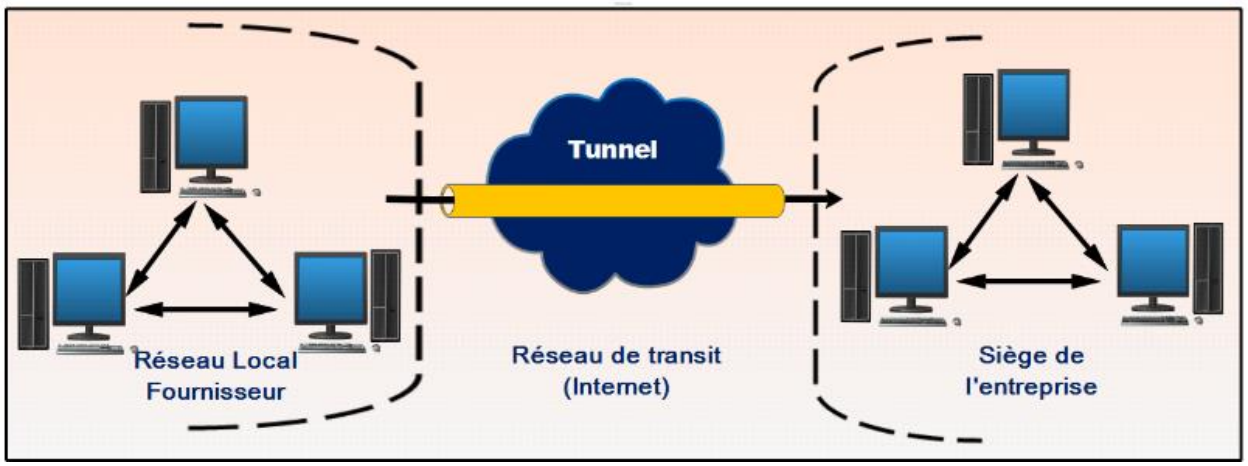

Figure 2.5 : Architecture d'un VPN extranet [9]

Les utilisateurs externes n'ont pas accès à l'ensemble de l'Intranet, mais seulement à certaines zones donc l'accès à l'Extranet est possible à partir de plusieurs endroits. L'accès dans un extranet est limité à certaines informations qui sont différents par rapport aux groupes et les rôles d'utilisateurs. Par exemple, les fournisseurs et les clients ont des droits d'accès différents.

1.4. Les différentes architectures des VPN

1.4.1 VPN d'entreprise

Dans ce cas, l'entreprise garde le contrôle de l'établissement des VPN entre ses différents points de présence ainsi qu'entre ses postes situés à l'extérieur de l'entreprise et les sites principaux.

1.4.1.1 De poste à poste

Le VPN poste à poste présente comme intérêt majeur de protéger la conversation de bout en bout. Il est donc particulièrement indiqué dans des contextes où le besoin de confidentialité, y compris pour des conversations se déroulant sur un réseau local, est primordial.

Il s'agit de mettre en relation deux serveurs. Le cas d'utilisation peut être le besoin de synchronisation de base de données entre deux serveurs d'une entreprise disposant de chaque côté d'un accès Internet. L'accès réseau complet n'est pas indispensable dans ce genre de situation (figure 2.6) [11].

Le poste à poste désigne également une conversation entre deux postes d'utilisateurs que la connexion entre un poste de travail et un serveur. Généralement ce dernier cas est le plus souvent utilisé.

En effet, il serait quand même difficile d'imaginer qu'un nombre important de postes individuels puissent être concernés par des VPN poste à poste établis, la mise en place serait compliquée à déployer d'un point de vue pratique. Nous pouvons également craindre que l'utilisation de protocoles de VPN en maillage d'un nombre important de postes puisse avoir un impact négatif sur les performances de ceux-ci ainsi que sur les besoins en matière d'assistance aux utilisateurs finaux [10].

Une autre contrainte des VPN poste à poste est que les postes constituant les extrémités doivent pouvoir se contacter plus ou moins directement [10].

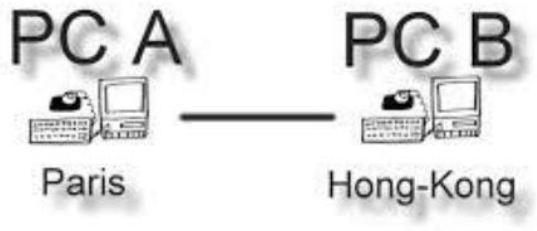

Figure 2.6 : VPN de poste à poste

- **Avantages et inconvénients :**

Le principal intérêt dans cette solution est que la conversation entre les deux postes est parfaitement protégée de bout en bout.

Par contre, elle présente de nombreux inconvénients

- Un impact très important sur les performances en cas de fort débit puisque le cryptage est uniquement logiciel.
- Quand les postes se situent sur des locaux sépares par internet il est nécessaire que les deux extrémités puissent échanger leurs messages sur des protocoles et des ports qui doivent autorisés par les firewalls situés sur chaque site, cela nécessite également des translations d'adresses puisque les machines concernées sont rarement dotées d'adresses IP publiques et cela n'est pas sans poser quelques problèmes.
- Ne peut être utilisé pour atteindre des matériels peu intelligents. [11]

1.4.1.2 De poste à site

Le VPN poste à site présente plusieurs atouts. Le premier est qu'il permet potentiellement à n'importe quelle machine distante, qu'elle soit isolée ou sur un réseau, de joindre une ou plusieurs machines d'un autre réseau en utilisant seulement les adresses privées.

Il est donc utilisable pour joindre depuis un poste distant des ordinateurs mais aussi pour atteindre des imprimantes, des fax, des webcams. Avec l'essor des cartes 3G et des fonctions modem des téléphones portables, la demande est de plus en plus forte pour ce type de service. Le nomadisme des individus qui peuvent être amenés à travailler à distance depuis le train, l'hôtel, les locaux d'un client consolide également cette demande. [10]

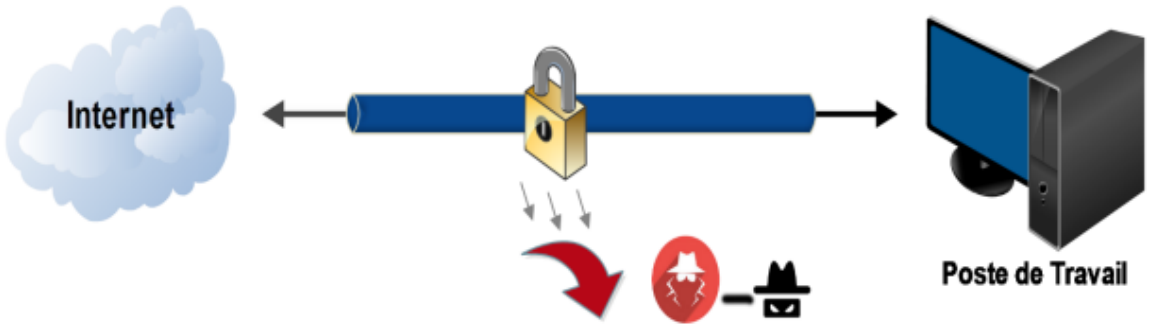

Figure 2.7 : VPN de poste à site

- **Avantages et inconvénients :**

Parmi les avantages de cette solution, on trouve :

- L'accès du poste mobile peut se faire de n'importe quel point du monde avec un à accès Internet.
- Assurer la transition des données entre le poste distant et le site central d'une façon sécurisée grâce à l'authentification.

- L'avantage est que le côté de la connexion entre le poste et le pare-feu de l'entreprise est chiffré. Par contre, celui entre le pare-feu et les postes du réseau local ne l'est pas puisque le cryptage, côté site central, est assuré par le pare-feu.

Les inconvénients de cette configuration :

- Nécessite une installation logicielle sur le poste distant
- Le cryptage exige une charge au poste distant, cela peut dégrader les performances
- Le cryptage n'est pas assuré au-delà du firewall du site central. [11]

1.4.1.3. De site à site

En utilisant seulement les adresses privées, le VPN site à site assure potentiellement à n'importe quelle machine d'un réseau de joindre celle d'un autre réseau. Il est donc utilisable pour des imprimantes, des fax, des webcams. Le deuxième intérêt est que le travail de mise en tunnel est effectué par les équipements d'extrémité les routeurs et/ou les firewalls, cela permet de ne pas charger les postes de travail et d'utiliser éventuellement des composants électroniques appliqués au cryptage par exemple, pour de meilleures performances.

Enfin ce type de VPN ne garantit pas la conversation de bout en bout puisque le flux est seulement crypté entre les deux extrémités du tunnel (c'est-à-dire les routeurs ou les pare-feu), ce qui peut nécessiter d'autres mesures si les échanges doivent être en continu ... [10]

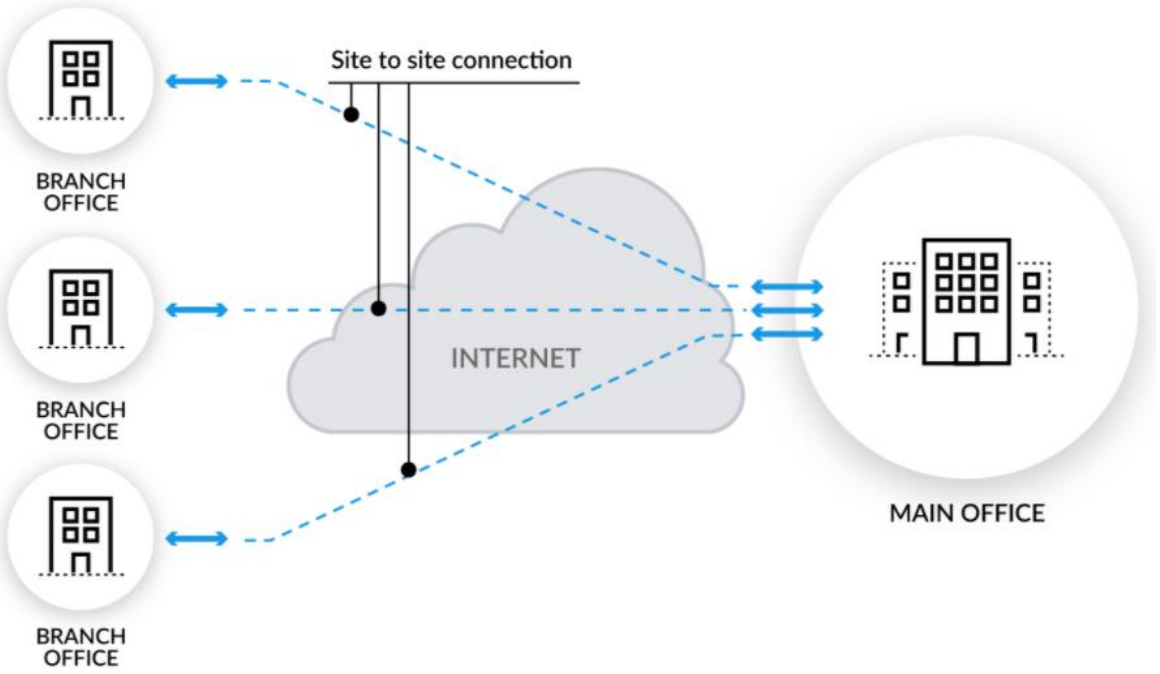

Figure 2.8 : Exemple d'un VPN de site à site

- **Avantages et inconvénients :**

Parmi les avantages fournis par cette configuration nous pouvons citer :

- Le cryptage est pris en charge par des processeurs spécialisés, pour de meilleures performances.
- Une facilité notable pour le contrôle de trafic autorisé.
- Aucun impact sur les performances des postes puisqu'il n'assure pas le cryptage.
- La possibilité d'initier les VPN d'un côté ou de l'autre.

Ils existent quelques inconvénients :

- Aucune protection de données entre les postes et les firewalls puisque le tunnel n'est établi qu'entre les deux firewalls.
- La connexion des VPN nécessite que les deux extrémités soient bien identifiées soit par une adresse IP publique fixe, soit par un nom référencé dans des DNS officiels [11].

1.4.2 VPN Opérateur

Un réseau privé VPN (Virtual Private Network) est considéré comme virtuel si partageant le réseau public d'ADD - ON **TELECOM**, il dispose de mécanismes garantissant la communication uniquement entre les clients du VPN. Ces mécanismes utilisent un identifiant unique permettant aux clients réseau disposant du même identifiant de dialoguer entre eux.

Ce réseau privé est complètement sécurisé puisque les adresses IP publiques, support des échanges de données, ne sont pas connues de l'Internet de manière générale.

VPN opérateur permet entre autre une diminution du temps de transit des informations sur le réseau, le maintien d'un réseau haute disponibilité, la mise en œuvre de QOS (Qualité Of Services) et la gestion souple des VPN, par simple adjonction d'un équipement de routage supplémentaire (CPE).

Les différents supports de connectivité accessibles pour cette offre peuvent être :

- ADSL
- SDSL à débit garanti
- BLR (Boucle Local Radio) – si pearing ADD-ON TELECOM sur la zone géographique concernée
- Fibre Optique – si pearing ADD-ON TELECOM sur la zone géographique concernée.

L'offre se compose des éléments suivants :

- un lien IP d'accès disposant des caractéristiques décrites précédemment,
- un port d'accès et le transit VPN regroupant les ressources utilisées au sein de la dorsale IP
  par la connexion VPN du site. Plus précisément, le port d'accès matérialise le port physique

sur lequel est raccordé le lien IP. Ces deux éléments, le port d'accès et le transit, sont packagés en un seul et même élément : le port VPN.

- un équipement d'accès spécifique suivant le lien IP choisi.

Les tarifs de l'offre VPN Opérateur sont en fonction de la zone d'éligibilité du site à équiper.

2. Principaux protocoles

La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP. Les Protocoles de tunneling niveau 2 supportent plusieurs protocoles de liaisons de données (Ethernet, PPP, FR, MPLS, etc.). Les Protocoles de tunneling niveau 3, tels que IPSEC, supportent uniquement les couches cibles utilisant le protocole IP. [12]

2.1 Les tunnels de niveau 2 (liaison de données)

• Protocoles : PPTP et L2TP

• PPTP (Point-to-Point Tunneling Protocol) a été développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.

• L2TP (Layer Two Tunneling Protocol) est une évolution de PPTP et de L2F, reprenant les avantages des deux protocoles.

• L2F (Layer Two Forwarding) développé par Cisco est remplacé par L2TP.

• PPTP et L2TP dépendent des fonctionnalités du protocole PPP (Point to Point Protocole). [12]

2.1.1 Point-to-Point Tunneling Protocol (PPTP)

Le protocole PPTP (Point to Point Tunneling Protocol), est un protocole qui utilise une connexion Point to Point Protocol à travers un réseau IP en créant un réseau privé virtuel(VPN). Il est en même temps une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation tels que Windows. Tout en étant un protocole de niveau 2, Le PPTP permet aussi l'encryptage des données ainsi que leur compression.

- Microsoft chiffrement MPPE (RC4 40 ou 128 bits) – Protocole réseau qui encapsule des trames PPP dans des datagrammes IP.
- Compresse éventuellement les communications
- PPTP crée ainsi un tunnel de niveau 3 défini par le protocole GRE (Generic Routing Encapsulation)
- Utilise les canaux de communication :

• Port TCP 1723

• Protocole IP 47 (GRE) [12]

• Inconvénients :

- Faiblesse de l'authentification (attaques facile par force brute)
- Mauvaise gestion des mots de passe dans les environnements mixtes Windows 95/NT,
- Identification des paquets non implémentée (vulnérabilité à la mascarade d'adresse),
- Protocole IP 47 (GRE) pas toujours traité par certains routeurs ce qui nécessite d'ouvrir tout IP vers le serveur VPN. [12]

• Avantages :

- Facile à installer sur Windows
- Utilise l'authentification Radius des Windows

• application :

- VPN d'accès (nomades à site)

2.1.2 Le protocole PPP :

• Le protocole PPP (Point -to-Point Protocol) est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone. Utilisé dans les liaisons d'accès au réseau Internet ou sur une liaison entre deux routeurs. Son rôle est d'encapsuler un paquet IP pour le transporter vers le nœud suivant et sa fonction consiste à indiquer le type des informations transportées dans le champ de données de la trame.

- Il est full duplex et garantit l'ordre d'arrivée des paquets.
- Il encapsule les paquets IP, IPX et Netbeui dans des trames PPP, puis transmet ces paquets encapsulés sur la liaison point à point. [12]

2.1.3 L2TP :

• L2TP (Layer Two Tunneling Protocol)

– Protocole réseau qui encapsule des trames PPP pour les envoyer sur des réseaux IP, X25, relais de trames ou ATM. [12]

- Utilise le port UDP 1701

- Par défaut, utilise le protocole IPsec

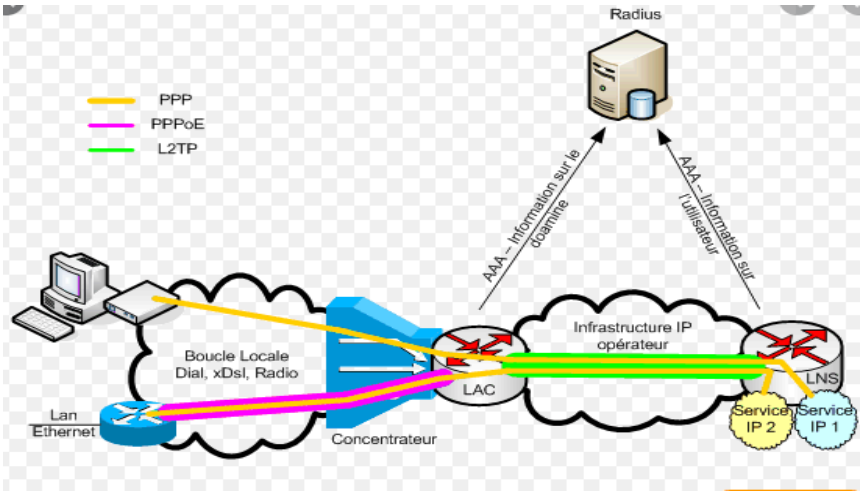

Figure 2.9 : Schémas réseau utilisé pour les protocoles

• Inconvénients :

- L2TP repose sur UDP lui-même repose sur IP. Au total, l'empilement total des couches protocolaires est assez lourd : IP/PPP/L2TP/UDP/IP/Couche2,
- Si utilisé avec IPsec, authentification à la machine, pas d'authentification de l'utilisateur => mettre en place Radius.
- Empilement des couches lorsque qu'un client surf sur le web [12].

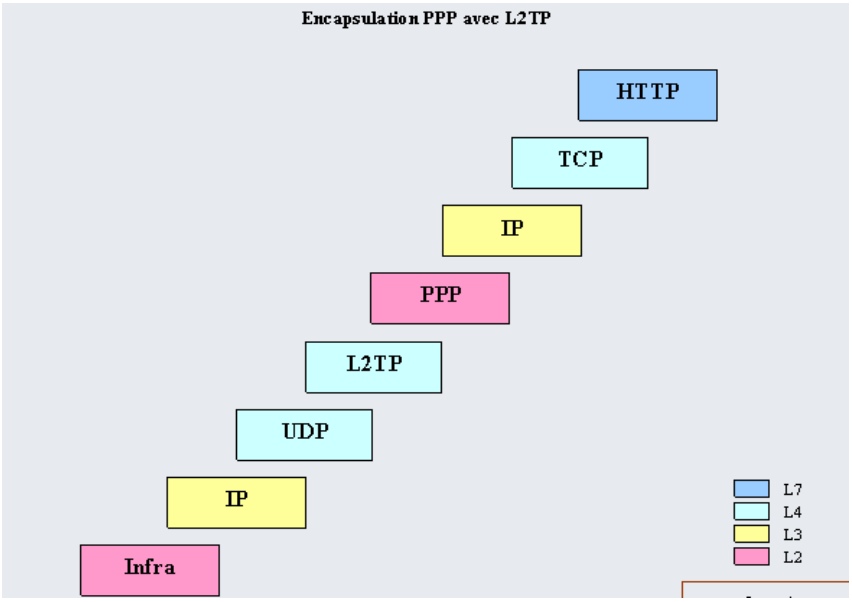

Figure 2.10 : Encapsulation PPP avec L2TP.

• Avantages :

- Facile à installer sur les Windows

• Prérequis :

- Authentification Radius à mettre en place

• Application :

- VPN d'accès (nomades à site)

2.1.4 L2F :

• Protocole développé Cisco Systems (RFC 2341)

• L2F fournit un tunnel sécurisé entre utilisateurs distants et la passerelle VPN

- Authentification basée sur PPP / Chiffrement basé sur PPP

• Composants :

- Tunnel L2F entre l'ISP et le serveur d'accès distant,
- Connexion PPP entre le client et l'ISP, que l'ISP fait suivre au serveur d'accès distant via le tunnel L2F [12]

2.2 Niveau 2 et 3 :

2.2.1 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. [13]

2.2.1.1 Fonctionnalité :

La première fonctionnalité de MPLS consiste à accélérer la transmission des informations au sein d'un backbone IP, car l'acheminement est basé sur la reconnaissance d'un Label qui permet dans le réseau de transit de ne plus se préoccuper de l'adresse mais de traiter le message en fonction de ce Label. La seconde est de permettre la création de VPN (Virtual Private Network) ou groupe fermé d'utilisateurs. [13]

MPLS est une technologie toujours en cours de standardisation à l'IETF. L'un des objectifs initiaux était d'accroître la vitesse du traitement des datagrammes dans l'ensemble des équipements intermédiaires. Cette volonté, avec l'introduction des gigarouteurs, est désormais passée au second plan. Depuis, l'aspect "fonctionnalité" a largement pris le dessus sur l'aspect "performance", avec notamment les motivations suivantes :

- Intégration IP/ATM
- Création de VPN
- Flexibilité : possibilité d'utiliser plusieurs types de media (ATM, FR, Ethernet, PPP, SDH).
- Differential Services (DiffServ),
- Routage multicast,

- Traffic Enginnering permettant de définir des chemins de routage explicites dans le réseau IP [13].

2.2.1.2 Principes MPLS :

Basée sur la permutation d'étiquettes, un mécanisme de transfert simple offre des possibilités de nouveaux paradigmes de contrôle et de nouvelles applications. Au niveau d'un LSR (Label Switch Router) du nuage MPLS, la permutation d'étiquette est réalisée en analysant une étiquette entrante, qui est ensuite permutée avec l'étiquette sortante et finalement envoyée au saut suivant.

A l'entrée du réseau MPLS, les paquets IP se voient insérés un label par le "Ingress Label Edge Routeur" ou "Ingress LER" (interface d'entrée ou point de départ d'une donnée). Les LER sont les routeurs MPLS se situant à la périphérie du réseau de l'opérateur. Les paquets labélisés sont ensuite commutés vers le cœur du réseau selon son numéro de label. Les routeurs MPLS du cœur de réseau, les Label Switching Router, commute ensuite les labels jusqu'au LER de sortie (Egress LER). Le chemin qui a été pris par le paquet, et préalablement établi, au travers du réseau s'appelle un Label Switched Path (LSP). [13]

La première fois que le datagramme d'un flux arrive à un Ingress E-LSR. Ce label est supprimé à l'autre extrémité par le Egress E-LER. Donc le mécanisme est le suivant :

1. Le Ingress LSR (E-LSR) reçoit les paquets IP.
2. Réalise une classification des paquets.
3. Y assigne un label et transmet les paquets labellisés au nuage MPLS.

En se basant uniquement sur les labels, les LSR du nuage MPLS commutent les paquets labellisés jusqu'à l'Egress LSR qui supprime les labels et remet Les paquets à leur destination finale. L'affectation des étiquettes aux paquets dépend des groupes ou des classes de flux FEC (forwarding équivalence classes). Les paquets appartenant à une même classe FEC sont traités de la même manière. Le chemin établi par MPLS appelé LSP (Label Switched Path) est emprunté par tous les datagrammes de ce flux.

L'étiquette est ajoutée entre la couche 2 et l'en-tête de la couche 3 (dans un environnement de paquets) ou dans le champ VPI/VCI (identificateur de chemin virtuel/identificateur de canal virtuel dans les réseaux ATM (Asynchronous Transfert Mode)).

Le switch LSR du nuage MPLS lit simplement les étiquettes, applique les services appropriés et redirige les paquets en fonction des étiquettes. Ce schéma de consultation et de transfert MPLS, offre la possibilité de contrôler explicitement le routage en fonction des adresses source et destination, facilitant ainsi l'introduction de nouveaux services IP [13].

2.3 Niveau 3 :

Ces protocoles agissent au moins au niveau 3 (au niveau paquet).

2.3.1. SSL/TLS

Ces protocoles sont en plein envol, très simples à mise en œuvre en utilisant le port (443), facilitant ainsi le passage des firewalls. Dans certain cas, ils ne nécessitent qu'un simple navigateur pour être utilisables. Ils sont implémentés de façon native dans d'autres logiciels (client de messagerie, client FTP) [14].

2.3.2 SSH

Utilisé souvent pour protéger des communications de type console (équivalent de Telnet) ou transferts de fichiers (de type FTP notamment). Son démarrage est limité car moins utilisé que de SSL/TLS et avec un son champ d'application plus restreint. Cependant il reste encore un protocole à considérer pour certains usages [14].

2.3.3. IPSec :

IPSEC (Internet Protocol Security) est une suite de protocoles normalisés par l'IETF qui fournit des services de sécurisation des données au niveau de la couche réseau. Il présente l'avantage d'être à la fois commun aux normes Ipv4 et Ipv6 [15].

Il assure les services ci-dessous [15] :

- **Confidentialité** : service qui consiste à rendre impossible l'interprétation de données si on n'en est pas le destinataire. C'est la fonction de chiffrement qui assure ce service en transformant des données intelligibles (en clair) en données inintelligibles (chiffrées).

- **Authentification** : service qui permet de s'assurer qu'une donnée provient bien de l'origine de laquelle elle est censée provenir.

-**intégrité** : service qui consiste à s'assurer qu'une donnée n'a pas été altérée accidentellement ou frauduleusement.

-**Protection contre le rejeu** : service qui permet d'empêcher les attaques consistant à envoyer de nouveau un paquet valide intercepté précédemment sur le réseau pour obtenir la même autorisation que ce paquet à entrer dans le réseau. Ce service est assuré par la présence d'un numéro de séquence.

-**Gestion des clés** : mécanisme de négociation de la longueur des clés de chiffrement entre deux éléments IPSEC et d'échange de ces clés.

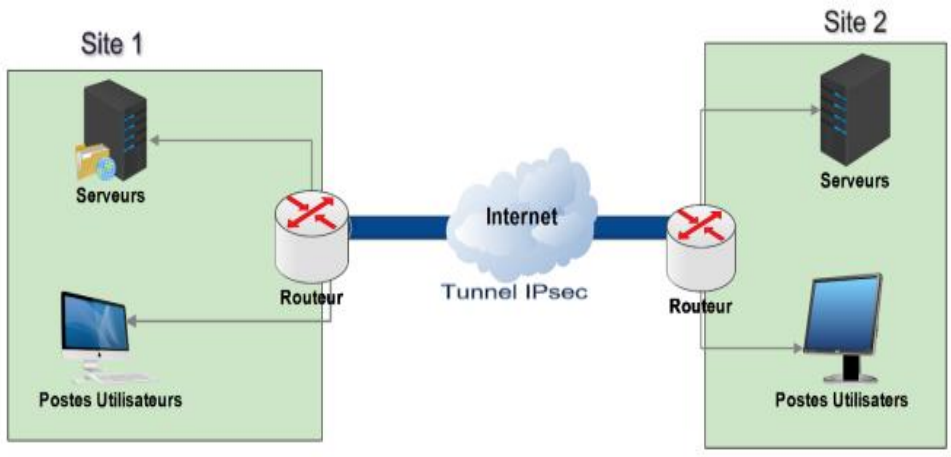

Figure 2.11 : Exemple d'emploi d'IPsec entre sites distants.

2.3.3.1. Mécanismes de sécurité :

IPSEC fait appel à deux mécanismes de sécurité pour le trafic IP :

- AH (Authentification Header).
- ESP (Encapsulation Security Payload)

Le but du protocole AH est de remettre au destinataire final un message possédant une identification sécurisée.

- **AH :** Le protocole AH assure l'intégrité des données en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données. Son principe est d'ajouter un bloc au datagramme IP. Une partie de ce bloc servira à l'authentification, tandis qu'une autre partie, contenant un numéro de séquence, assurera la protection contre le rejet [16].
  AH est approprié lorsque la confidentialité n'est pas requise ou n'est pas permise.
- **ESP :** Le protocole ESP assure, en plus des fonctions réalisées par AH, la confidentialité des données et la protection partielle contre l'analyse du trafic, dans le cas du mode tunnel. C'est pour ces raisons que ce protocole est le plus largement employé [16].

Le mécanisme est différent de celui d'AH. En effet, ce protocole utilise les mécanismes d'encapsulation et de chiffrement des données.

La technologie IPSEC présente deux modes de fonctionnement qui sont :

- Le mode « transport »
- Le mode « tunnel ».

Dans le cas du mode transport, les données sont prises au niveau de la couche 4 du modèle OSI (couche transport). Elles sont cryptées et signées avant d'être transmise à la couche IP. Ce mode est relativement facile à mettre en œuvre.

Le défaut présenté par le mode transport, et que, étant donné que le mécanisme s'applique au niveau de la couche transport, il n'y a pas de masquage d'adresse. C'est pourquoi un deuxième mode peut être mis en œuvre, le mode tunnel, dans lequel l'encapsulation Ipsec a lieu après que les données envoyées par l'application ont traversé la pile de protocole jusqu'à la couche IP incluses. Dans ce cas, il y a bien masquage des adresses.

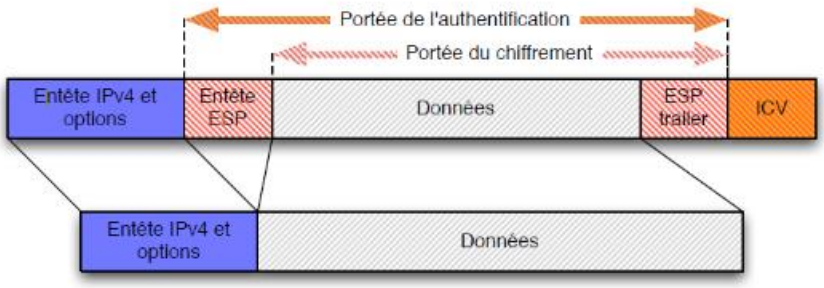

Figure 2.12 : Utilisation d'ESP en mode transport [16].

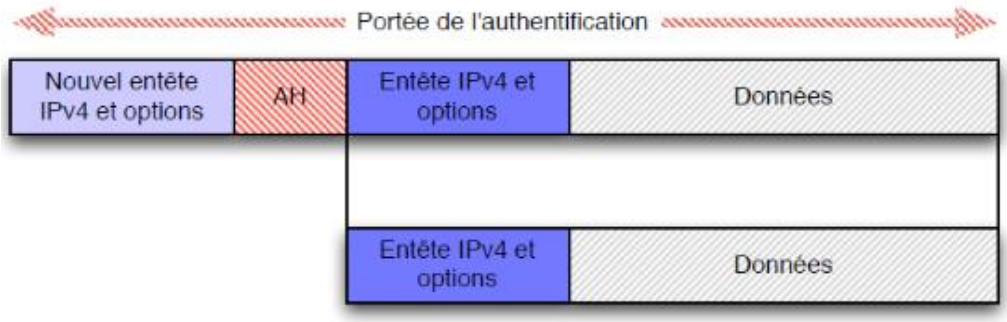

Figure 2.13 : Utilisation d'AH en mode transport [16].

• Prérequis :

- Une passerelle IPsec et IPsec sur les clients.

• Inconvénients :

- IPsec ne permet d'identifier que des machines et non pas des utilisateurs => Mettre en place un système d'authentification.
- IPsec à cause de la lourdeur des opérations de cryptage/décryptage réduit les performances globales des réseaux. => L'achat de périphériques dédiés, coûteux est souvent indispensable. Nécessite un bon débit réseau.

• Utilisation :

- Intranet, extranet (Sites à sites).

3. Conclusion :

Les VPNs sont très utilisés par les multinationales et les grandes sociétés. Le VPN peut garantir la sécurité et la confidentialité des données, qui circulent de manière cryptée par Internet afin que personne de malintentionné ne puisse intercepter les informations. Dans ce chapitre nous avons présenté les notions de base nécessaires au fonctionnement et à la réalisation d'un réseau VPN ainsi que les différents protocoles utilisés.

Chapitre 3 : Simulation et Tests

Introduction :

Ce chapitre représente la configuration du réseau VPN est la mise en place des différents acteurs du réseau qui peuvent constituer les éléments d'une entreprise. Nous allons également définir l'architecture permettant de relier les différents sites de l'entreprise. Une présentation des différents logiciels utilisés afin d'élaborer la simulation et les tests démontreront le bon fonctionnement du réseau VPN est effectuée à la fin de ce chapitre.

1. Les outils de réalisation :

1.1. GNS3 :

GNS3 est un logiciel libre qui fonctionne sur de multiples plateformes, incluant Windows et Linux. GNS3 est un simulateur de réseau graphique qui permet de concevoir facilement les topologies de réseau, puis exécuter des simulations. Nous pouvons même prolonger le réseau en le connectant à une topologie virtuelle.

Pour ce faire, GNS3 est basé sur Dynamips, Qemu (y compris son emballage) et en partie sur Dynagen, il a été développé en python et par PyQt. GNS3 utilise également le la technologie SVG (Scalable Vector Graphics) pour fournir des symboles de haute qualité pour la conception de la topologie du réseau [17] [18]

Dynamips : un émulateur d'image IOS qui permet de lancer des images binaires IOS Provenant de Cisco Systèmes.

Dynagen : une interface en mode texte pour Dynamips.

IOS : À l'instar d'un ordinateur personnel, un routeur ou un commutateur ne peut pas fonctionner sans système d'exploitation. Sans système d'exploitation, le matériel est inopérant. Cisco IOS est le logiciel système des périphériques Cisco. (IOS signifie Internetworking Operating System) [18] [19]

Qemu, est un logiciel libre de machine virtuelle, pouvant émuler un processeur et, plus généralement, une architecture différente si besoin. Il permet d'exécuter un ou plusieurs systèmes d'exploitation [18] [19]

Figure 3.1 : Logo du logiciel GNS3 [18]

1.2. WIRESHARK :

Wireshark est l'analyseur de protocole de réseau le plus utilisé au monde. Il vous permet de voir ce qui se passe sur votre réseau à un niveau microscopique. Ce programme est capable

d'intercepter les paquets transmis sur le réseau et de compiler des statistiques sur l'utilisation du réseau.

Il permet de visualiser une liste de paquets capturés, analyser des données sur chaque paquet, au format hexadécimal. Il intègre également des fonctionnalités de codage couleur qui permet d'identifier le type de trafic réseau, tels que DNS en bleu et en vert http.

Le développement de Wireshark prospère grâce aux contributions bénévoles d'experts en réseautage du monde entier et s'inscrit dans la continuité d'un projet lancé par Gerald Combs en 1998.

Wireshark dispose d'un riche ensemble de fonctionnalités qui comprend les éléments suivants [19] :

- Inspection approfondie de centaines de protocoles, et d'autres sont ajoutés en permanence
- Capture en direct et analyse hors ligne
- Navigateur de paquets standard à trois volets
- Multiplateforme : fonctionne sous Windows, Linux, macOS, Solaris, FreeBSD, NetBSD et bien d'autres
- Les données réseau capturées peuvent être parcourues via une interface graphique ou via l'utilitaire TShark en mode TTY
- Les filtres d'affichage les plus puissants de l'industrie
- Analyse VoIP riche
- Lecture / écriture de nombreux formats de fichiers de capture différents : tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressé et non compressé), Sniffer® Pro et NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN / LAN Analyzer, Shomiti / Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek / TokenPeek / AiroPeek, et bien d'autres
- Les fichiers de capture compressés avec gzip peuvent être décompressés à la volée
- Les données en direct peuvent être lues à partir d'Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI et autres (selon votre plate-forme)
- Prise en charge du décryptage pour de nombreux protocoles, notamment IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP et WPA / WPA2
- Des règles de coloration peuvent être appliquées à la liste de paquets pour une analyse rapide et intuitive
- La sortie peut être exportée au format XML, PostScript®, CSV ou texte brut.

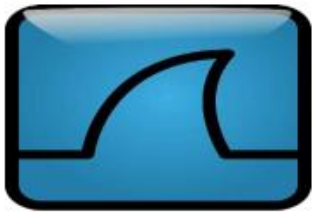

Figure 3.2 : Logo du logiciel wireshark

1. Architecture du réseau :

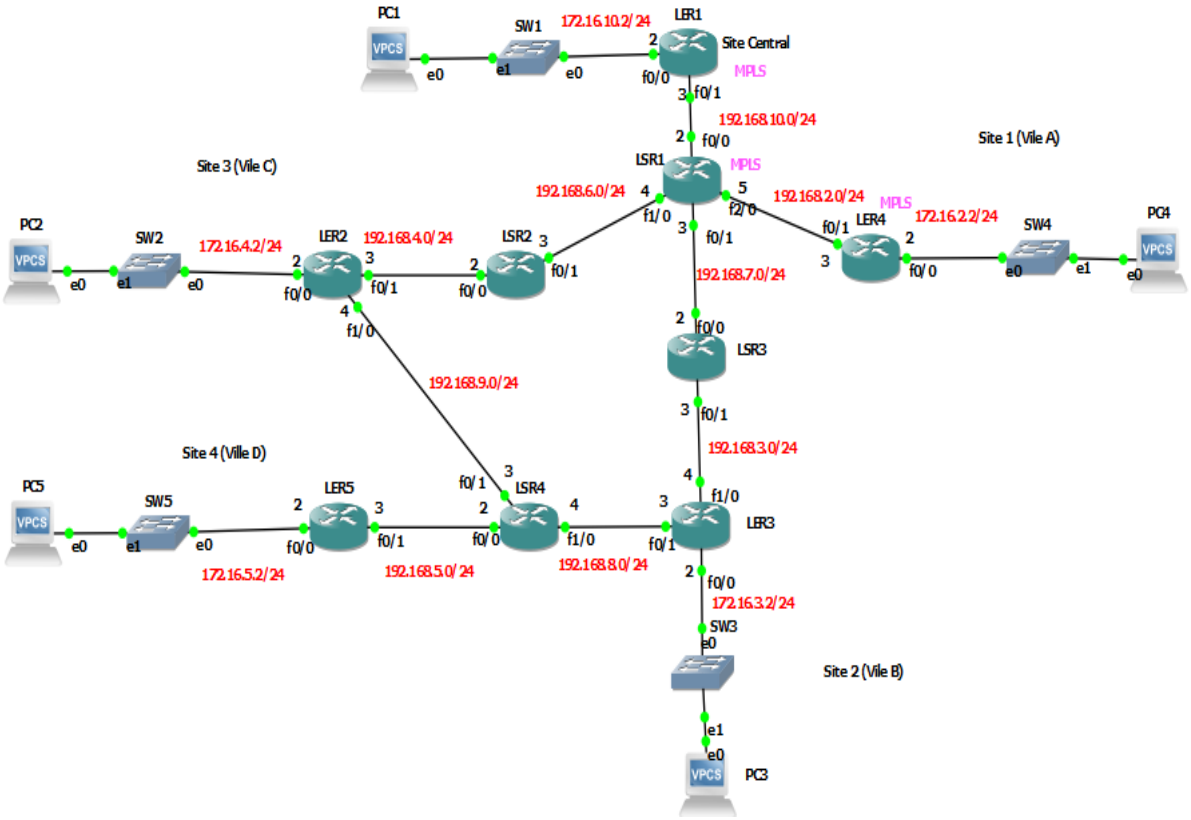

Figure 3.3 : Architecture du Réseau sous GNS3

2.1. Configuration :

Dans cette partie nous allons mettre la configuration des routeurs. L'architecture ci-dessus relie quatre sites situés dans quatre villes différentes disposant chacun d'un réseau local que nous avons défini avec une adresse de classe B.

2.1.1. Site central

Considérons le site central (LER1) qui est représenté par un routeur 3725 avec les interfaces :

- F0/0 : 172.16.10.2/24, qui relie au réseau local
- F0/1 : 192.168.10.3/30, qui relie au backbone opérateur.
- Loopback 0 : 1.1.1.1/32.

-172.16.0.0 : On a choisi de la classe B pour segmenter le réseau en nombre suffisant de sous-réseaux afin de pouvoir représenter les différents services et dans chaque sous-réseau on peut avoir jusqu'à 2^8 hôtes.

-192.168.0.0 : pour relier les différents réseaux entre eux, et on prit un masque /30 car chaque routeur possède au maximum quatre interfaces (adresses), d'où on a besoin de deux bits dans la partie hôte (2 bits ---> 4 hôtes).

-Loopback 0 : c'est une interface virtuelle qui permet le bon fonctionnement du routeur.

```
LER1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER1(config)#int f0/0
LER1(config-if)#ip address 172.16.10.2 255.255.255.0
LER1(config-if)#no sh
LER1(config-if)#
*Mar  1 00:20:34.995: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 00:20:35.995: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
LER1(config-if)#int f0/1
LER1(config-if)#ip address 192.168.10.3 255.255.255.0
LER1(config-if)#no sh
LER1(config-if)#
*Mar  1 00:21:49.007: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:21:50.007: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
LER1(config-if)#end
LER1#
*Mar  1 00:21:55.771: %SYS-5-CONFIG_I: Configured from console by console
LER1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
LER1#
```

Figure 3.4 : Attribution des adresses aux interfaces du routeur central (LER1).

On voit dans la figure, que les deux interfaces f0/0 et f0/1 sont activées avec succès.

Les interfaces configurées, il ne reste plus qu'à configurer le routage

```
LER1(config)#router rip
LER1(config-router)#version 2
LER1(config-router)#no auto-summary
LER1(config-router)#network 172.16.10.0
LER1(config-router)#network 192.168.10.0
LER1(config-router)#exit
LER1(config)#
```

Figure 3.5 : Configuration du routage de LER1

Nous avons utilisé OSPF comme protocole de routage car :

D'abord, il est utilisé dans l'architecture du réseau réel, ensuite c'est un protocole conçu pour gérer de large réseau (comme dans notre cas). Ainsi, il permet de diviser le domaine de routage afin de faciliter sa gestion. Enfin OSPF gère plus astucieusement l'allocation des adresses.

```
LER1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER1(config)#router ospf 1
LER1(config-router)#network 172.16.10.0 0.0.0.255 area 0
LER1(config-router)#network 192.168.10.0 0.0.0.255 area 0
LER1(config-router)#end
LER1#
*Mar  1 00:35:31.451: %SYS-5-CONFIG_I: Configured from console by console
LER1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
LER1#
```

Figure 3.6 : routage OSPF sur le routeur du site central (LER1).

2.1.2. Site 1 (Ville A) :

Il est représenté par un routeur Cisco de gamme 3725 (LER4) pour lequel nous avons attribué les interfaces suivantes :

- F0/0 : 172.16.2.2/24, qui relie au réseau local
- F0/1 : 192.168.2.3/30, qui relie au backbone opérateur.
- Loopback 0 : 2.2.2.2/32.

```
LER4#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER4(config)#int f0/0
LER4(config-if)#ip address 172.16.2.2 255.255.255.0
LER4(config-if)#no sh
LER4(config-if)#
*Mar  1 00:14:14.403: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 00:14:15.403: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
LER4(config-if)#int f0/1
LER4(config-if)#ip address 192.168.2.3 255.255.255.0
LER4(config-if)#no sh
LER4(config-if)#
*Mar  1 00:16:15.263: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:16:16.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
LER4(config-if)#end
LER4#c
*Mar  1 00:16:34.391: %SYS-5-CONFIG_I: Configured from console by console
```

Figure 3.7 : Attribution des adresses aux interfaces du routeur de la ville A.

Configuration du routage :

```
LER4(config)#router rip
LER4(config-router)#version 2
LER4(config-router)#no auto-summary
LER4(config-router)#network 172.16.2.0
LER4(config-router)#network 192.168.2.0
LER4(config-router)#exit
LER4(config)#
```

Figure 3.8 : Configuration du routage de LER4

```
LER4#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER4(config)#router ospf 1
LER4(config-router)#network 172.16.2.0 0.0.0.255 area 0
LER4(config-router)#network 192.168.2.0 0.0.0.255 area 0
LER4(config-router)#end
LER4#
*Mar  1 02:15:48.075: %SYS-5-CONFIG_I: Configured from console by console
LER4#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
LER4#
```

Figure 3.9 : routage OSPF sur le routeur de la ville A.

2.1.3. Site 2 (Ville B) :

Un routeur Cisco de gamme 3725 est utilisé dont les interfaces suivantes :

- F0/0 :172.16.3.2/24, qui relie au réseau local
- F0/1 : 192.168.8.3/30, qui relie au backbone opérateur.
- F1/0 : 192.168.3.4/30, qui relie au backbone opérateur.
- Loopback 0 : 3.3.3.3/32.

```
LER3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER3(config)#int f0/1
LER3(config-if)#ip address 192.168.8.3 255.255.255.0
LER3(config-if)#no sh
LER3(config-if)#
*Mar  1 01:12:50.371: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 01:12:51.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
LER3(config-if)#int f0/0
LER3(config-if)#ip address 172.16.3.2 255.255.255.0
LER3(config-if)#no sh
LER3(config-if)#
*Mar  1 01:13:34.551: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 01:13:35.551: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
LER3(config-if)#int f1/0
LER3(config-if)#ip address 192.168.3.4 255.255.255.0
LER3(config-if)#no sh
LER3(config-if)#
*Mar  1 01:14:19.911: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state t
o up
*Mar  1 01:14:20.911: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to up
LER3(config-if)#end
LER3#
*Mar  1 01:14:26.111: %SYS-5-CONFIG_I: Configured from console by console
LER3#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
LER3#
```

Figure 3.10 : Attribution des adresses aux interfaces du routeur de la ville B (LER3).

Configuration du routage :

```
LER3(config)#router rip
LER3(config-router)#version 2
LER3(config-router)#no auto-summary
LER3(config-router)#network 172.16.3.0
LER3(config-router)#network 192.168.3.0
LER3(config-router)#network 192.168.8.0
LER3(config-router)#exit
```

Figure 3.11 : Configuration du routage LER3

```
LER3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER3(config)#router ospf 1
LER3(config-router)#network 172.16.3.0 0.0.0.255 area 0
LER3(config-router)#network 192.168.3.0 0.0.0.255 area 0
LER3(config-router)#network 192.168.8.0 0.0.0.255 area 0
LER3(config-router)#end
LER3#
*Mar  1 01:20:11.995: %SYS-5-CONFIG_I: Configured from console by console
LER3#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
LER3#
```

Figure 3.12 : routage OSPF sur le routeur de la ville B

2.1.4 Site 3 (Ville C) :

Comme pour les sites précédents, le routeur avec gamme 3725 est utilisé, où les liaisons FastEthernet avec les interfaces suivantes ont été activées :

- F0/0 : 172.16.4.2/24, qui relie au réseau local
- F0/1 : 192.168.4.3/30, qui relie au backbone opérateur.
- F1/0 : 192.168.9.4/30, qui relie au backbone opérateur.
- Loopback 0 : 4.4.4.4/32.

```
LER2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER2(config)#int f0/0
LER2(config-if)#ip address 172.16.4.2 255.255.255.0
LER2(config-if)#no sh
LER2(config-if)#
*Mar  1 00:24:38.107: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 00:24:39.107: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
LER2(config-if)#int f0/1
LER2(config-if)#ip address 192.168.4.3 255.255.255.0
LER2(config-if)#no sh
LER2(config-if)#
*Mar  1 00:25:29.747: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:25:30.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
LER2(config-if)#int f1/0
LER2(config-if)#ip address 192.168.9.4 255.255.255.0
LER2(config-if)#no sh
LER2(config-if)#
*Mar  1 00:26:11.787: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state t
o up
*Mar  1 00:26:12.787: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to up
LER2(config-if)#end
LER2#
*Mar  1 00:26:19.723: %SYS-5-CONFIG_I: Configured from console by console
LER2#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
LER2#
```

Figure 3.13 : Attribution des adresses aux interfaces du routeur de la ville C (LER 2)

Configuration du routage

```
LER2(config)#router rip
LER2(config-router)#version 2
LER2(config-router)#no auto-summary
LER2(config-router)#network 172.16.4.0
LER2(config-router)#network 192.168.9.0
LER2(config-router)#network 192.168.4.0
LER2(config-router)#exit
```

Figure 3.14 : Configuration du routage LER2

```
LER2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER2(config)#router ospf 1
LER2(config-router)#network 172.16.4.0 0.0.0.255 area 0
LER2(config-router)#network 192.168.4.0 0.0.0.255 area 0
LER2(config-router)#network 192.168.9.0 0.0.0.255 area 0
LER2(config-router)#end
LER2#
*Mar  1 01:09:09.995: %SYS-5-CONFIG_I: Configured from console by console
LER2#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
LER2#
```

Figure 3.15 : routage OSPF sur le routeur de la ville C (LER 2).

2.1.5 Site 4 (Ville D) :

Comme pour les sites précédents, le routeur avec gamme 3725 est utilisé, où les liaisons FastEthernet avec les interfaces suivantes ont été activées :

- F0/0 : 172.16.5.2/30, qui relie au réseau local
- F0/1 : 192.168.5.3/30, qui relie au backbone opérateur.
- Loopback 0 : 5.5.5.5/32.

```
LER5#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER5(config)#int f0/0
LER5(config-if)#ip address 172.16.5.2 255.255.255.0
LER5(config-if)#no sh
LER5(config-if)#int
*Mar  1 01:38:59.191: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 01:39:00.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
LER5(config-if)#int f0/1
LER5(config-if)#ip address 192.168.5.3 255.255.255.0
LER5(config-if)#no sh
LER5(config-if)#en
*Mar  1 01:39:35.975: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 01:39:36.975: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
LER5(config-if)#end
LER5#
*Mar  1 01:39:42.963: %SYS-5-CONFIG_I: Configured from console by console
LER5#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
LER5#
```

Figure 3.16 : Attribution des adresses aux interfaces du routeur de la ville D (LER 5)

```
LER5(config)#router rip
LER5(config-router)#version 2
LER5(config-router)#no auto-summary
LER5(config-router)#network 172.16.5.0
LER5(config-router)#network 192.168.5.0
LER5(config-router)#exit
```

Figure 3.17 : Configuration du routage LER2

```
LER5#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER5(config)#router ospf 1
LER5(config-router)#network 172.16.5.0 0.0.0.255 area 0
LER5(config-router)#network 192.168.5.0 0.0.0.255 area 0
LER5(config-router)#end
LER5#
*Mar  1 01:55:57.287: %SYS-5-CONFIG_I: Configured from console by console
LER5#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
LER5#
```

Figure 3.18 : routage OSPF sur le routeur de la ville D (LER 5).

2.2. Routage et activation de MPLS :

Après avoir réalisé la configuration sur les cinqs sites en utilisant le routage dynamique avec le protocole OSPF (Open Shortest Path First) nous allons passer à l'activation de MPLS (Multi Protocol Layer Switching) sur le réseau backbone de l'opérateur afin d'avoir une architecture similaire aux cas réels utilisés dans plusieurs sociétés.

2.2.1. Vérification du routage :

- Afin de pouvoir effectuer un test du routage, on lance un Ping à destination de la passerelle du réseau local connecté à l'interface du routeur de chaque ville (A, B, C et D) le résultat est montré dans les figures suivante pour la ville D et la ville A (comme exemple) **:**

```
LER1#ping 192.168.5.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1308/1434/1700 ms
LER1#
```

Figure 3.19 : résultat d'une requête ICMP du site central vers la ville D

Un autre ping destiné à l'interface d'entrée du routeur de la ville A. Le résultat est montré à la figure suivante :

```
LER1#ping 192.168.2.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 396/591/796 ms
LER1#
```

Figure 3.20 : résultat d'une requête ICMP du site central vers la ville A

Avec une capture Wireshark (**figure 3.21 et 3.22**) :

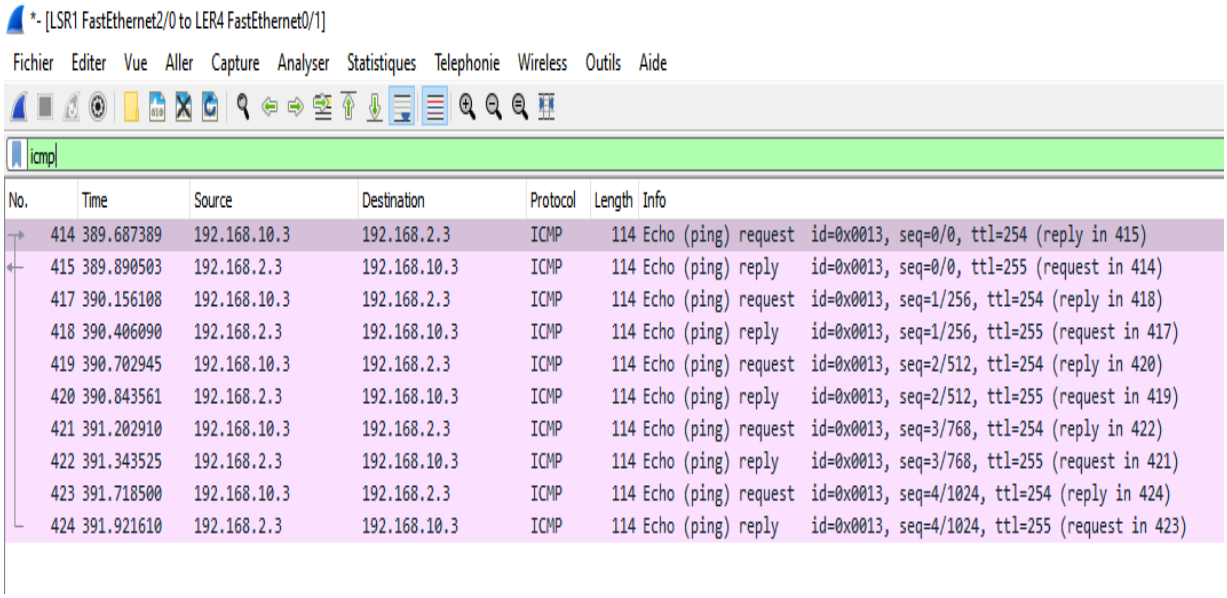

Figure 3.21 : résultat d'une requête ICMP de LER1 vers LER4 sous Wireshark.

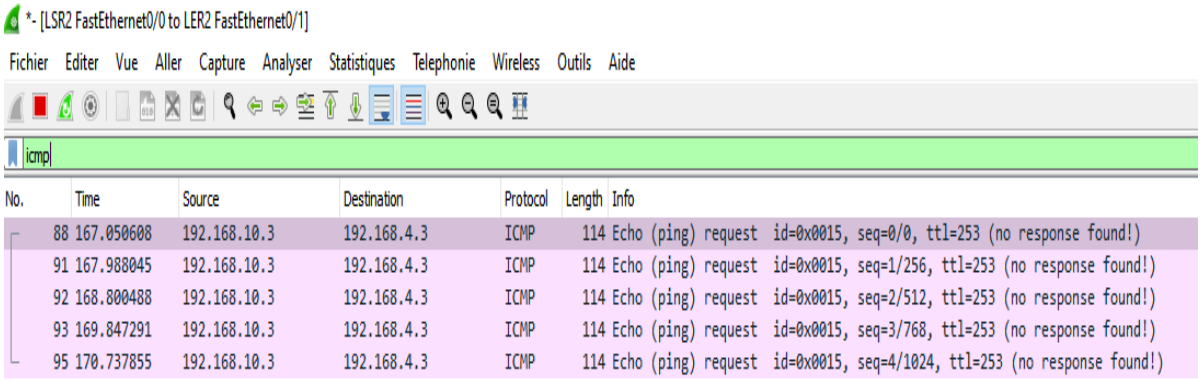

Figure 3.22 : résultat d'une requête ICMP de LER1 vers LER2 sous Wireshark.

2.2.2. Activation de MPLS :

Nous allons d'abord activer le protocole MPLS (le routage est déjà fait avec OSPF) sur les 3 routeurs, nommés LER1, LSR1, LER4. Exemple d'activation sur l'un des routeurs(LER1) :

```
LER1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER1(config)#ip cef
LER1(config)#tag-switching advertise-tags
LER1(config)#mpls label protocol ldp
LER1(config)#int f0/0
LER1(config-if)#mpls ip
LER1(config-if)#exit
LER1(config)#int f0/1
LER1(config-if)#mpls ip
LER1(config-if)#end
LER1#
*Mar  1 00:29:20.875: %SYS-5-CONFIG_I: Configured from console by console
LER1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
LER1#
```

Figure 3.23 : Activation du MPLS sur le routeur LER1.

Ip cef: permet d'activer Cisco Express Forwarding.

tag-switching advertise-tags : active MPLS et démarre la distribution des labels.

MPLS label protocol ldp : permet d'utiliser le protocole LDP pour la distribution des labels.

MPLS IP : permet d'encapsuler les paquets avant de les envoyer (doit être activer sur toutes les interfaces de sorties sauf celles connectées directement aux réseaux locaux).

2.2.3 Vérification du fonctionnement de MPLS :

On aperçoit sur la figure (3 .24**)** que MPLS fonctionne sur les interfaces de sorties avec la commande « show mpls forwarding-table ».

```
LER1#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     16          192.168.8.0/24   0          Fa0/1       192.168.10.2
17     17          192.168.9.0/24   0          Fa0/1       192.168.10.2
18     19          172.16.4.0/24    0          Fa0/1       192.168.10.2
19     20          172.16.5.0/24    0          Fa0/1       192.168.10.2
20     21          172.16.2.0/24    0          Fa0/1       192.168.10.2
21     22          172.16.3.0/24    0          Fa0/1       192.168.10.2
22     23          192.168.4.0/24   0          Fa0/1       192.168.10.2
23     24          192.168.5.0/24   0          Fa0/1       192.168.10.2
24     Pop tag     192.168.6.0/24   0          Fa0/1       192.168.10.2
25     Pop tag     192.168.7.0/24   0          Fa0/1       192.168.10.2
26     Pop tag     192.168.2.0/24   0          Fa0/1       192.168.10.2
27     25          192.168.3.0/24   0          Fa0/1       192.168.10.2
LER1#
```

Figure 3 .24 : Vérification de l'activation de MPLS sur le routeur LER1.

3. Création des VPNs site-à-site

Dans cette partie, nous allons configurer un tunnel VPN IPsec entre LER1 et LER4. Ensuite testez les résultats de notre configuration, en validant les stratégies IKE sur LER1 et LER4

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

- La configuration des paramètres IKE (Internet Key Exchange).
- La configuration des paramètres IPSec

3.1. La configuration des paramètres IKE (Internet Key Exchange)

a. Vérifions qu'IKE est supporté et validé.

IKE Phase 1 définit la méthode d'échange de clés utilisée pour passer et valider les stratégies IKE entre les extrémités. Dans IKE Phase 2, les extrémités échanges et négocient les stratégies IPSec pour l'authentification et le cryptage du trafic de données.

IKE doit être validé pour qu'IPsec fonctionne. IKE est validé par défaut sur les images de l'IOS avec les ensembles fonctionnels de cryptographie. S'il n'est pas validé pour une raison quelconque, vous pouvez le revalider avec la commande **crypto isakmp enable.** Il faut donc utilisez cette commande pour vérifier que l'IOS du routeur supporte IKE et que celui-ci est validé.

```
LER1#
LER1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER1(config)#crypto isakmp enable
LER1(config)#
```

Figure 3.25 : Validation des stratégies IKE sur LER1

```
LER4#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER4(config)#crypto isakmp enable
LER4(config)#
```

Figure 3.26 : Validation des stratégies IKE sur LER4

Si on n'arrive pas à exécuter cette commande sur le routeur, on doit mettre à niveau l'image de l'IOS avec une image incluant l'ensemble des services de cryptographie Cisco.

b. Etablissons une stratégie ISAKMP (Internet Security Association and Key Management Protocol) et on affiche les options disponibles.

Pour permettre la négociation IKE Phase 1, vous devez créer une stratégie ISAKMP et configurer une association d'extrémité incluant la stratégie ISAKMP. Une stratégie ISAKMP définit les algorithmes d'authentification, de cryptage et de hachage utilisés pour transmettre le trafic de contrôle entre les deux extrémités VPN. Quand une association ISAKMP a été acceptée par les extrémités IKE, IKE Phase 1 est terminé. Les paramètres IKE Phase 2 sont configurés plus tard.

Entrons la commande de configuration **crypto isakmp policy 10** sur LER1 pour la stratégie 10.

```
LER1(config)#crypto isakmp policy 10
LER1(config-isakmp)#
```

Figure 3.27 : Stratégie ISAKMP sur LER1

Les différents paramètres IKE sont disponibles et illustrer dans la figure suivante figure (3.28).

```
LER1(config-isakmp)#
LER1(config-isakmp)# ?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults

LER1(config-isakmp)#
```

Figure 3.28 : Paramètre isakmp sur LER1

3.1.2. Validation des stratégies IKE sur LER1 et LER4

-Configuration des paramètres de stratégie ISAKMP sur LER1 et LER 4 :

Le choix d'un algorithme de cryptage détermine le degré de confidentialité du canal de contrôle entre les extrémités. L'algorithme de hachage contrôle l'intégrité des données, assurant que les données reçues d'une extrémité n'ont pas été modifiées pendant leur transit. Le type d'authentification assure que le paquet a bien été transmis et signé par cette extrémité distante. Le groupe Diffie-Hellman utilisé pour créer une clé secrète partagée par les extrémités qui ne sont pas transmise à travers le réseau.

-Il faut configurer un type d'authentification avec clés pré-partagées. Utilisons AES-256 pour le cryptage, SHA pour l'algorithme de hachage et Diffie-Hellman group 5 pour l'échange de clés pour cette stratégie IKE.

Note : A ce point il faut être au niveau du LER1 (config-isakmp)#. La commande crypto isakmp policy 10 est répétée ci-dessous pour restituer le contexte.

```
LER1(config)#crypto isakmp policy 10
LER1(config-isakmp)#
LER1(config-isakmp)#authentication pre-share
LER1(config-isakmp)#encryption aes 256
LER1(config-isakmp)#hash sha
LER1(config-isakmp)#group 5
LER1(config-isakmp)#lifetime 3600
LER1(config-isakmp)#end
LER1#
*Mar  1 01:15:25.939: %SYS-5-CONFIG_I: Configured from console by console
LER1#
```

Figure 3.29 : Création d'une stratégie de négociation de clés sur LER1

La commande group 5 : Spécifie l'identifiant Diffie-Hellman

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

```
LER4(config)#
LER4(config)#crypto isakmp policy 10
LER4(config-isakmp)#authentication pre-share
LER4(config-isakmp)#encryption aes 256
LER4(config-isakmp)#hash sha
LER4(config-isakmp)#group 5
LER4(config-isakmp)#lifetime 3600
LER4(config-isakmp)#end
LER4#
*Mar  1 01:17:59.011: %SYS-5-CONFIG_I: Configured from console by console
LER4#
```

Figure 3.30 : Création d'une stratégie de négociation de clés sur LER4

```
LER1#
LER1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
LER1#
```

Figure 3.31 : Vérification de la stratégie IKE sur LER1 avec la commande Show crypto isakmp policy

3.1.3. Configuration des clés pré-partagées :

a. Comme les clés pré-partagées sont utilisées comme méthode d'authentification dans la stratégie IKE, on doit configurer une clé sur chaque routeur qui pointe vers l'autre extrémité du VPN. La commande configuration **globale crypto isakmp key key-string address** est utilisée pour entrer une clé pré-partagée (il faut utiliser l'adresse IP de l'extrémité distante, interface distante pour router le trafic vers le routeur local).

b. Chaque adresse IP qui est utilisée pour configurer les extrémités IKE est également référencée comme l'adresse IP de l'extrémité VPN distante. Configurons la clé pré-partagée cisco123 sur le routeur LER1 en utilisant la commande suivante.
Les réseaux de production doivent utiliser une clé plus complexe. Cette commande pointe vers l'adresse IP l'extrémité distante LER4 f0/1

```
LER1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
LER1(config)#crypto isakmp key cisco123 address 192.168.2.3
LER1(config)#
```

Figure 3.32 : Configuration des clés pré-partagées sur LER1

```
LER4(config)#
LER4(config)#crypto isakmp key cisco123 address 192.168.10.3
LER4(config)#
```

Figure 3.33 : Configuration des clés pré-partagées sur LER4

3.2. Configuration du transform set IPSec et des durées de vie :

Le transform set IPSec est un autre paramètre de configuration IPSec que les routeurs négocient pour former une association de sécurité. Pour créer un transform set IPSec, utilisez la commande **crypto ipsec transform-set** tag **parameters**. Utilisez-le signe"**?**" pour voir quels sont les paramètres disponibles.

```
LER1(config)#crypto ipsec transform-set 50 ?
  ah-md5-hmac    AH-HMAC-MD5 transform
  ah-sha-hmac    AH-HMAC-SHA transform
  comp-lzs       IP Compression using the LZS compression algorithm
  esp-3des       ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes        ESP transform using AES cipher
  esp-des        ESP transform using DES cipher (56 bits)
  esp-md5-hmac   ESP transform using HMAC-MD5 auth
  esp-null       ESP transform w/o cipher
  esp-seal       ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac   ESP transform using HMAC-SHA auth

LER1(config)#crypto ipsec transform-set 50
```

Figure 3.34 : Configuration du transform-set IPsec sur LER1

Sur LER1 et LER4 on va créer un transform set avec ESP (Encapsulating Security Protocol) avec cryptage AES transform set identiques.

```
LER1(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
LER1(cfg-crypto-trans)#
LER1(cfg-crypto-trans)#
```

Figure 3.35 : Création du transform-set sur LER1

```
LER4(config)#
LER4(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
LER4(cfg-crypto-trans)#exit
LER4(config)#
```

Figure 3.36 : Création du transform-set sur LER4

Nous pouvons également changer les durées de vie des associations de sécurité IPSec qui sont par défaut 3600 secondes ou 4608000 kilobytes. Sur LER1 et LER4 et fixer la durée de vie de l'association de sécurité IPSec à 30 minutes ou 1800 secondes.

```
LER1(config)#
LER1(config)#crypto ipsec security-association lifetime seconds 1800
LER1(config)#
LER1(config)#
```

Figure 3.37 : fixation de la durée de vie de l'association de sécurité IPSEC sur LER1

```
LER4(config)#
LER4(config)#crypto ipsec security-association lifetime seconds 1800
LER4(config)#
LER4(config)#
```

Figure 3.38 : fixation de la durée de vie de l'association de sécurité IPSEC sur LER4

3.2.1. Définition du trafic intéressant :

a. Pour utiliser le cryptage avec le VPN IPSec, il est nécessaire de définir une liste d'accès étendue pour indiquer au routeur quel trafic il doit crypter. Un paquet qui est permis par une liste d'accès utilisée pour définir le trafic IPSec est crypté si la session IPSec est configurée correctement. Un paquet qui est rejeté par une de ces listes d'accès (n'est pas rejeté mais transmis sans être crypté). Tout comme les autres listes d'accès, il y a une instruction implicite de rejet à la fin de la liste d'accès qui dans ce cas veut dire que l'action par défaut est de ne pas crypter le trafic.

b. Dans ce scénario, le trafic que nous voulons crypter est le trafic allant du LAN Ethernet de LER1 vers le LAN Ethernet de LER4 ou vice versa. Ces listes d'accès sont utilisées en sortie sur les interfaces des extrémités VPN et doivent être un miroir l'une de l'autre.

access-list 101 permit IP 192.168.11.0 0.0.0.255 192.168.12.0 0.0.0.255

```
LER1(config)#
LER1(config)#$ 101 permit ip 172.16.10.0 0.0.0.255 172.16.2.0 0.0.0.255
LER1(config)#
LER1(config)#
```

Figure 3.39 : Configuration de l'ACL du trafic intéressant VPN IPsec sur LER1

```
LER4(config)#
LER4(config)#$ 101 permit ip 172.16.2.0 0.0.0.255 172.16.10.0 0.0.0.255
LER4(config)#
LER4(config)#
```

Figure 3.40 : Configuration de l'ACL du trafic intéressant VPN IPsec sur LER4

3.2.3. Créer et appliquer une crypto map :

Une crypto map associe le trafic intéressant qui correspond à la liste d'accès avec une extrémité et différents paramètres IKE et IPSec. Après la création de la crypto map, celle-ci peut être appliquée à une ou plusieurs interfaces. Les interfaces auxquelles elle est appliquée doit être une de celle faisant face à l'autre extrémité IPSec.

Créez la crypto map nommée CMAP sur LER1 avec 10 comme numéro de séquence. Un message est affiché à l'exécution de la commande.

```
LER1(config)#
LER1(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
LER1(config-crypto-map)#
LER1(config-crypto-map)#
```

Figure 3.41 : Création de la crypto map nommée CMAP sur LER1

Utilisation de la commande match address pour l'accès de la liste sur LER1 et définir le trafic à crypter. Afficher l'ensemble des commandes qui inclus la crypto map utiliser avec le signe "?".

```
LER1(config-crypto-map)#
LER1(config-crypto-map)#set ?
  identity              Identity restriction.
  ip                    Interface Internet Protocol config commands
  isakmp-profile        Specify isakmp Profile
  nat                   Set NAT translation
  peer                  Allowed Encryption/Decryption peer.
  pfs                   Specify pfs settings
  reverse-route         Reverse Route Injection.
  security-association  Security association parameters
  transform-set         Specify list of transform sets in priority order

LER1(config-crypto-map)#set
```

Figure 3.42 : Affichage de l'ensemble des commandes sur LER1

Configurons maintenant un nom de host ou une adresse IP d'extrémité. L'adresse IP de l'interface de l'extrémité VPN distante de LER4 est configurée avec la commande suivante :

```
LER1(config-crypto-map)#set peer 192.168.2.3
LER1(config-crypto-map)#
LER1(config-crypto-map)#
```

Figure 3.43 : configuration d'un nom de host sur LER1

Nous allons maintenant indiquer le transform set à utiliser avec cette extrémité en utilisant la commande set transform-set tag. Fixer le type de pfs (Perfect forwarding secrecy) avec la commande set pfs type et modifier également la durée de vie par défaut de l'association de sécurité Ipsec avec la commande set security.

```
LER1(config-crypto-map)#set pfs group5
LER1(config-crypto-map)#set transform-set 50
LER1(config-crypto-map)#set security-association lifetime seconds 900
LER1(config-crypto-map)#match address 101
LER1(config-crypto-map)#exit
LER1(config)#
```

Figure 3.44 : Utilisation du transform set et fixation du PFS sur LER1 (modification la durée de vie

Faire la même chose avec le routeur LER4 :

-Créez une crypto map miroir sur LER4 :

```
LER4(config-crypto-map)#set peer 192.168.10.3
LER4(config-crypto-map)#set pfs group5
LER4(config-crypto-map)#set transform-set 50
LER4(config-crypto-map)#set security-association lifetime seconds 900
LER4(config-crypto-map)#match address 101
LER4(config-crypto-map)#exit
LER4(config)#
```

Figure 3.45 : Utilisation du transform set et fixation du pfs sur LER4

La dernière étape est l'application des crypto map aux interfaces. Notez que les associations de sécurité (SAs) ne seront pas établies tant que la crypto map n'aura pas été activée par le trafic intéressant. Le routeur va générer un message pour indiquer que la crypto map est opérationnelle.

-Appliquez les crypto map aux interfaces appropriées sur LER1 et LER4:

```
LER1(config)#int f0/1
LER1(config-if)#crypto map CMAP
LER1(config-if)#
*Mar  1 01:06:03.539: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
LER1(config-if)#end
LER1#
```

Figure 3.46 : Application des crypto map aux interfaces sur LER1

```
LER4(config)#interface f0/1
LER4(config-if)#crypto map CMAP
LER4(config-if)#
*Mar  1 03:29:53.819: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
LER4(config-if)#end
```

Figure 3.47 : Application des crypto map aux interfaces sur LER4

3.2.4. Vérifier la configuration VPN IPSec site à site

-Vérification de la configuration IPSec sur LER1 et LER4 :

Nous avons déjà utilisé la commande **show crypto isakmp policy** pour afficher les stratégies ISAKMP configurées sur le routeur. De manière similaire la commande **show crypto ipsec transform-set** affiche la configuration des stratégies IPSec configurées sous la forme d'un transform set.

```
LER1#show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },


LER1#
```

Figure 3.48 : Vérification de la configuration Ipsec sur LER1

```
LER4#show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

Figure 3.49 : Vérification de la configuration Ipsec sur LER4

```
LER1#show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
        Peer = 192.168.2.3
        Extended IP access list 101
            access-list 101 permit ip 172.16.10.0 0.0.0.255 172.16.2.0 0.0.0.255
        Current peer: 192.168.2.3
        Security association lifetime: 4096 kilobytes/900 seconds
        PFS (Y/N): Y
        DH group:  group5
        Transform sets={
                50,
        }
        Interfaces using crypto map CMAP:
                FastEthernet0/1
```

Figure 3.50 : Affichage du crypto map sur LER1

```
LER4#show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
        Peer = 192.168.10.3
        Extended IP access list 101
            access-list 101 permit ip 172.16.2.0 0.0.0.255 172.16.10.0 0.0.0.255
        Current peer: 192.168.10.3
        Security association lifetime: 4608000 kilobytes/900 seconds
        PFS (Y/N): Y
        DH group:  group5
        Transform sets={
                50,
        }
        Interfaces using crypto map CMAP:
                FastEthernet0/1


LER4#
```

Figure 3.51 : Affichage du crypto map sur LER4

La sortie de ces commandes ne change pas si le trafic intéressant passe par la connexion VPN.

3.2.5. Vérification du fonctionnement du VPN IPSec

-Affichage des associations de sécurité ISAKMP :

La commande **show crypto isakmp** révèle qu'il n'y a pas encore de SA IKE. Quand du trafic intéressant est transmis, la sortie de cette commande change.

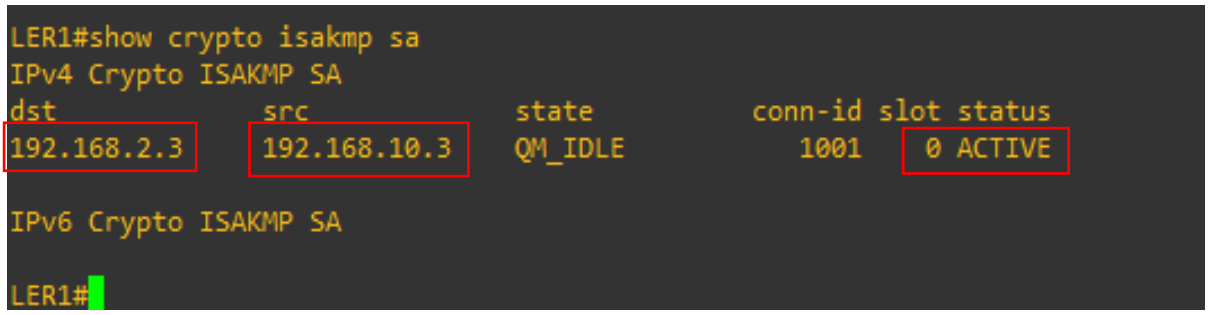

Figure 3.52 : Affichage des associations de sécurité ISAKMP sur LER1

On aperçoit sur la figure ci-dessus figure (3.52), que les opérations de ISAKMP sont activées entre les deux extrémités du tunnel LER1 (192.168.10.3) et LER4 (192.168.2.3).

-Affichage des associations de sécurité IPSec **:** La commande **show crypto ipsec sa** affiche les SA entre LER1 (192.168.10.3) et LER4 LER4 (192.168.2.3). Notez le nombre de paquets transmis sont 46 et qu'il existe une d'association de sécurité et de cryptage qui a été établie.

```
LER1#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: CMAP, local addr 192.168.10.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.16.2.0/255.255.255.0/0/0)
   current_peer 192.168.2.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
    #pkts decaps: 46, #pkts decrypt: 46, #pkts verify: 46
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 4, #recv errors 0

     local crypto endpt.: 192.168.10.3, remote crypto endpt.: 192.168.2.3
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0xB4A9D299(3031028377)

     inbound esp sas:
      spi: 0x51B2D220(1370673696)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 7, flow_id: SW:7, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4483646/853)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB4A9D299(3031028377)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 8, flow_id: SW:8, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4483646/833)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:
```

Figure 3.53 : Vérification des paramètres IPsec sur LER1

On distingue sur la figure ci-dessous figure (3.54) avec Wireshark, que les opérations de protection avec le protocole de ISAKMP sont activées entre les deux extrémités du tunnel LER1 (192.168.10.3) et LER4 (192.168.2.3).

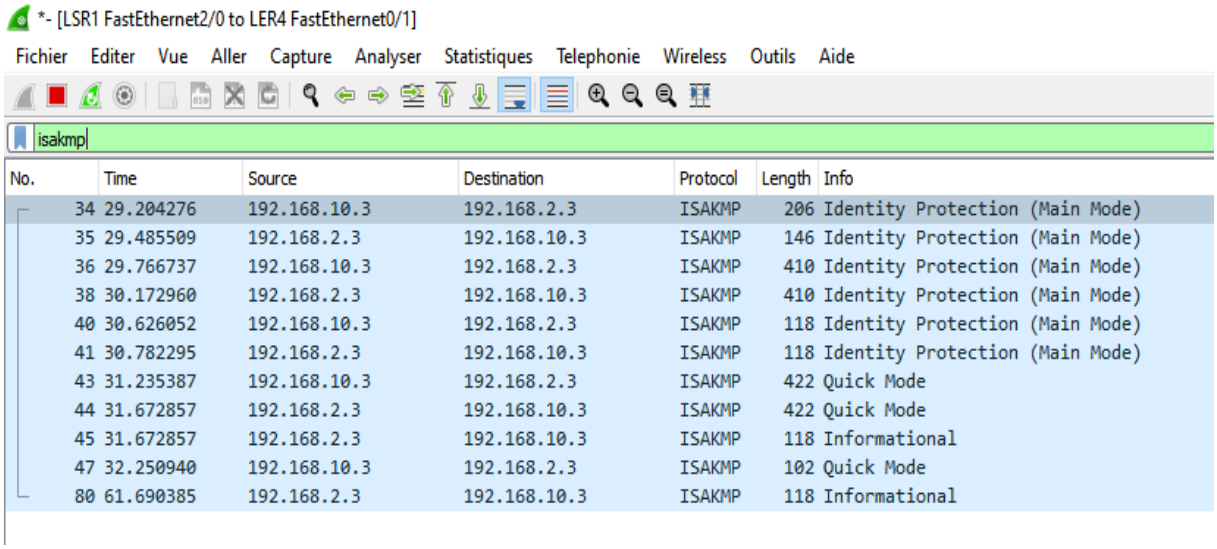

Figure 3.54 : résultat avec Wireshark du protocole ISAKMP

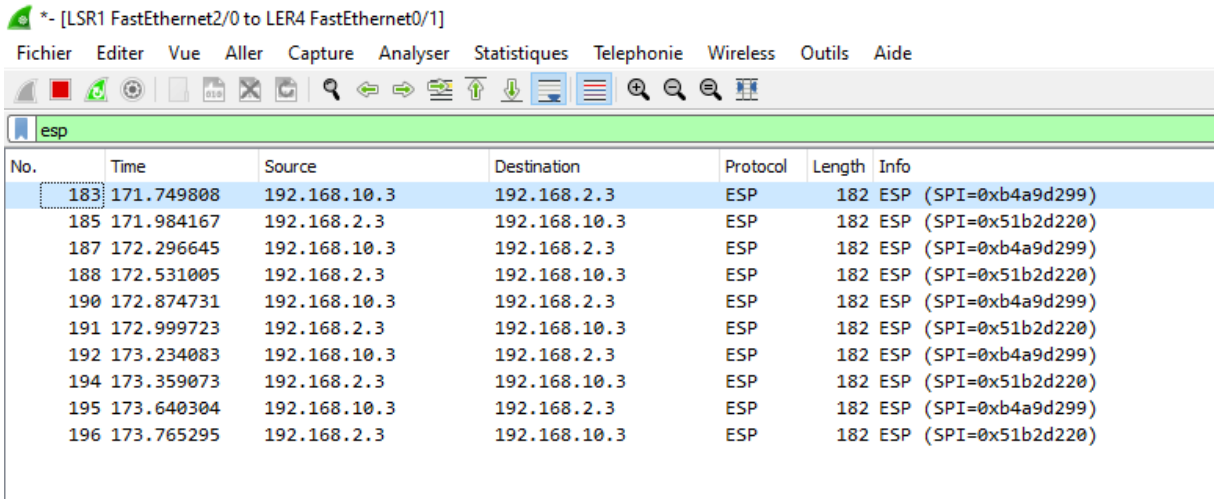

Figure 3.55 : résultat avec Wireshark du protocole ESP

- la dernière étape de vérification avec un test de Wireshark est effectuée, la figure (3.55) nous montre l'établissement le trafic du cryptage avec le protocole ESP.

4. Conclusion :

Ce chapitre a fait l'objet d'une configuration de réseau VPN site-à-site pour faire la simulation d'un réseau d'entreprise créé autour d'un site central et quatre sites distants, après avoir bien défini le routage et la topologie du réseau avec routage basé sur l'OSPF. La sécurité du réseau a été assurée par le protocole IPsec

La simulation a été réalisée sous le logiciel GNS3. Des captures de trafic de données ont été réalisées avec le logiciel Wireshark pour confirmer le transfert de donnée.

Conclusion générale

Le secteur des technologies de l'information étant en constante évolution, en effet dans le cadre du projet de fin d'étude nous avons testé de la mise place d'un réseau VPN site-à-site. Grâce à cette nouvelle technologie qui va permettre de partager de façon sécurisée la connexion et les données, ce partage étant possible en interne pour les utilisateurs du réseau local de l'entreprise, mais aussi en externe pour les utilisateurs dit « distants » situés en dehors du réseau local.

Nous avons abordé dans notre travail, conçus autour de trois chapitres, le premier chapitre, ou nous avons présenté les réseaux opérateurs, le deuxième chapitre consacré aux généralités sur les réseaux VPNs et ces fonctionnalités, ainsi que les protocoles de sécurité le plus utilisés, également l'IPsec implémenté avec notre configuration du réseau.

La réalisation de ce travail conçu comme suite :

Configuration de l'architecture réseau des sites de l'entreprise basé sur le routage dynamique avec le protocole OSPF

Activation du protocole MPLS sur le réseau avec la création des VPNs entre le site central et les quatre autres sites distants.

Ce travail nous a apporté énormément de connaissances et de compétences en termes de configuration et de simulation avec le logiciel GNS3. Ces connaissances ont été renforcé dans le domaine de la sécurité informatique notamment la sécurité d'un réseau d'entreprise grâce à l'implémentation d'un réseau privé virtuel (VPN).

Nous avons implémenté le protocole IPsec (site à site), afin de contrôler et expérimenter la sécurité du réseau.

La technologie IPsec permet d'offrir des services de sécurité classiques (authentification, confidentialité, intégrité, etc.) pour chaque datagramme transitant par un réseau de transport (par exemple, Internet). Cette technologie peut être mise en œuvre par l'entreprise utilisatrice ou par un fournisseur de service dans le cadre d'infogérance. Deux limitations essentielles sont à retenir pour cette technologie :

- elle ne permet pas de gérer la qualité de service au cœur du réseau ;

- elle ne transporte que les datagrammes IP.

Comme perspectives, on peut suggérer d'implémenter d'autre protocole de sécurité (site à site) et (poste à site) par exemple, le protocole L2TP/IPSEC et le TLS/IPSEC, dans le but de mieux sécuriser les connexions (poste à site) et les connexions nomades.

Bibliographie

Références bibliographiques :

[1] Abderrahmane BAADACHE " Réseaux étendus et réseaux d'opérateurs" de cours Master II Professionnel en Informatique, Université Abderrahmane Mira de Bejaia 2013-2014

[2] Kamal Singh "Comprendre le cœur d'Internet : les réseaux d'opérateurs", cours en ligne Kamal Singh – Télécom Saint-Étienne 2020.

[3] C. Pham "Les réseaux grande distance Routage et réseaux de Routage et réseaux d'accès", Université de Pau et des Pays de l'Adour Département Informatique 2005

[4] Etienne Duris Réseaux – Licence 3 Informatique"Université Paris-Est Marne, la Vallée, Janvier 2010

[5] http://igm.univ-mlv.fr/~dr/XPOSE2007/cchamp01_VPN/introduction.html

[6] https://www.tplpc.com/tutoriels/dossier-48-01083.html

[7] Tebani.T " Simulation d'un tunnel VPN-SSL pour la sécurisation d'une interconnexion de deux réseaux LANs", Mémoire de fin d'études de master Génie électrique, Université Mouloud Mammeri De Tizi-Ouzou, 2015.

[8] Razafiarinomenjanahary Antsanirina Miora "APPLICATION DE LA TECHNOLOGIE VPN SSL SOUS CONTRAINTE DE SECURISATION DES DONNEES", Mémoire de fin d'études en vue de l'obtention du diplôme de Licence ES Sciences Techniques en Télécommunication, Université D'Antananarivo. 2013

[9] Jacob NDWO MAYELE," Déploiement d'un cœur de réseau IP/MPLS", Licence en génie informatique, Université de Kinshasa,2016

[10] Jean paul Archier, Les VPN Fonctionnement, mise en œuvre et maintenance (2ième édition) Informatique Technique. 2011

[11] Baa Adel Saker Karim " Mise en place d'une architecture VPN-IPsec pour le compte de CEVITAL", Mémoire de fin d'études en vue de l'obtention du diplôme Master en en informatique, Option : Administration et Sécurité des Réseaux, Université Abderrahmane Mira BEJAIA,2016

[12] http://docshare02.docshare.tips/files/12479/124793198.pdf

[13] https://wallu.pagesperso-orange.fr/pag-mpls.htm

[14] https://loudni.users.greyc.fr/Enseignement/Cours/TRc8/CM/CM3_VPN.pdf

[15] https://wallu.pagesperso-orange.fr/pag-ipsec.htm

[16] Gauchard. D " Simulation Hybride des Réseaux IP-DiffServ-MPLS Multi-services sur Environnement d'Exécution Distribuée", Thèse de doctorat en Systèmes Informatiques, Université Toulouse III Paul Sabatier,2003.

[17]http://icourse.cuc.edu.cn/computernetworks/cisco/Simulator/Dynamips/GNS3-0.4_documentation.pdf

Références bibliographiques :

[18] https://www.gns3.com/software/download

[19] A. ROUX , D. SEBA, «Cisco, Maitrisez la configuration des routeurs et des commutateurs », editions eni, date de parrution 19/12/2005 EAN : 9782746030503

[20] https://www.wireshark.org/