وزارة البحث العلمي والتعليم العالي
MINISTERE DE L'ENSEIGNEMENT SUPEREUR ET DE LA RECHERCHE SCIENTIFIQUE
جامعـة عبد الحميد بن باديس مستغانم
Université Abdelhamid Ibn Badis Mostaganem
كـلـيـة الـعـلـوم و الـتـكـنـولـوجـيـا
Faculté des Sciences et de la Technologie
DEPARTEMENT DE GENIE ELECTRIQUE

N° d'ordre : M...../GE/2021

MEMOIRE

Présenté pour obtenir le diplôme de

MASTER EN GENIE ELECTRIQUE

Filière : Télécommunications

Spécialité : Systèmes des télécommunications

Par

GUEZGOUZ SIHAM

FELLOUH HOURIA

Etude et simulation d'une architecture réseau basée sur le cloud dans un environnement VPN IP SEC multi site.

Soutenu le 15 / 07 / 2021 devantle jury composé de :

Président : Mr. BENSTAALI Wissam	Grade MCA	Université de Mostaganem
Examinateur : Mme. BENCHELLAL Amel	Grade MCB	Université de Mostaganem
Rapporteur : Mr. RESFA Abbes	Grade MCB	Université de Mostaganem

Année Universitaire 2020/2021

Remerciements

Nous remercions, Tout d'abord, ALLAH pour la volonté, la force, la santé et la patience qu'il nous a donné afin de réaliser ce travail.

Un grand merci à nos parents, pour leur amour, leurs conseils ainsi que leur soutien inconditionnel, à la fois moral et économique, qui nos a permis de réaliser les études que nous voulons et par conséquent ce mémoire.

Nous tenons à remercier et a exprimer nos gratitudes à notre encadreur Mr RESFA ABBES qui nous a orienté et nous a soutenu durant notre projet de fin d'études.

Nous adressons également nos vifs remerciements à Mr. BENSTAALI WISSAM, Enseignant à l'Université de Mostaganem, d'avoir bien voulu présider le jury.

Nous sommes également très reconnaissants à Mme. BENCHELLAL AMEL, Enseignante à l'Université de Mostaganem, d'avoir acceptée d'examiner ce modeste travail.

Nous témoignons reconnaissance et gratitudes aux aimables personnes, quelque soit de prés ou de loin, qui nous ont soutenu, acceptent et orientant durant notre projet de fin d'étude.

Dédicaces

Je dédie ce mémoire :

***A** mes très chères **parents** ; qui ont tout fait pour m'encourager durant toutes mes études, et grâce a eux que je suis arrivé à réaliser ce résultat ;*

***A** mes chères **sœurs** et mon cher **frère**. Aux êtres chers auxquels je ne saurais exprimer ma gratitude et ma reconnaissance ;*

A *mon encadreur directeur de mémoire Docteur **RESFA ABBES** pour toutes ses conseils et son aide jusqu'à la dernière minute, que Dieu la garde en bonne Santé ;*

***A** mes proches amis qui n'ont cessé de m'encourager ;*

***A** mon binôme et chère amie Melle **FELLOUH HOURIA** ainsi que sa famille ;*

***A** tous ceux qui m'ont aidé dans l'élaboration de ce travail.*

SIHAM GUEZGOUZ

Dédicaces

Je dédie ce mémoire :

***A** mes très chères **parents** ; qui ont tout fait pour m'encourager durant toutes mes études, et grâce a eux que je suis arrivé à réaliser ce résultat ;*

***A** mes chères **sœurs** et mes chers **frères**. Aux êtres chers auxquels je ne saurais exprimer ma gratitude et ma reconnaissance ;*

A *mon encadreur directeur de mémoire Docteur **RESFA ABBES** pour toutes ses conseils et son aide jusqu'à la dernière minute, que Dieu la garde en bonne Santé ;*

***A** mes proches amis qui n'ont cessé de m'encourager ;*

***A** mon binôme et chère amie Melle **SIHAM GUEZGOUZ** ainsi que sa famille ;*

***A** tous ceux qui m'ont aidé dans l'élaboration de ce travail.*

HOURIA FELLOUH

Table des matières

Listes des abréviations et acronymes :

AES : Advanced Encryption Standard

ARP : Adress Resolution Protocol

ANSI : American National Standard Institute

ADSL : Asymmetrical bit rate Digital Subscriber Line

AES : Application Environment Service

ASCII : American Standard Code for Information Interchange

BNC : Bayonet Neill–Concelman Connector

CDMA : Code Division Multiple Access

CSMA/CD : Carrier Sense Multiple Access / Collision Detection.

DHCP : Dynamic Host Configuration Protocol

DNS : Domain Name System/Service

DMZ : De Militarized Zone

DES : Data Encryption Standard

EAP : Extensible Authentication Protocol

ERP : Enterprise Resource Planning

FAI : Fournisseur d'Accès à Internet

FDDI : Fiber Distributed Data Interface

FTP : File Transfer Protocol

FTTH : Fiber To The Home

HTML: Hyper Text Markup Language

HTTP: Hyper Text Transfer Protocol

IKE : Internet Key Exchange

ISO : International Standards Organisation

IPsec : Internet Protocol Security

IS : Interim Standard

IEEE : Institute of Electrical and Electronics Engineers

ICMP : Internet Control Message Protocol

ISP : Internet Service Provider

ISAKMP: Internet Security Association and Key Management Protocol

L2F : Layer Tow Forwarding

L2TP : Layer Tow Tunneling Protocol

MAU : Multisession Access Unit

MAC : Message Authentification Code

NAT : Network Adress Traduction

NAS : Network Attached Storage

NTIC : Nouvelles Technologies de l'Information et de la Communication

OSI : Open System Interconnection

PPP : Point to Point Protocol

PoE : Power over Ethernet

PKI : Public Key Infrastructure

PING: Packet Internet Groper

PPTP : Point-to-Point Tunneling Protocol

QoS : Quality Of Service

RA : Registration Authority

RIP : Routing Information Protocol

RNIS : Réseau Numérique à Intégration de Services

SHA : Secure Hash Algorithm

SSL : Secure Socket Layer

STP : Shielded Twisted Pair

SA : Security Association

SNMP: Simple Network Management Protocol

TCP/IP: Transmission Control Protocol/Internet Protocol

UDP : User Datagram Protocol

UTP : Unshielded Twisted Pair

VSAT : Very Small Aperture Terminal

WAN : Wide Area Network ou réseau étendu

WIFI : Wireless Fidelit

Liste des figures :

Liste des tableaux :

Abstract

Since the appearance of computer science in the 1950s, it has gradually established itself as a primordial instrument in the professional world, becoming the essential tool for the management of information up to decision-making. Of importance capital for companies.

And as all progress generates new challenges, over time another need arose which was to
have access at any time and from anywhere to the resources offered by computerized entities (business, home, administrations, etc.) in a secure manner, hence the need for VPN (Virtual Private Network or Virtual Private Network).

The development of technology in general and computer science in particular has sparked a craze for modernizing the processing of information systems.

These technologies have been able to develop thanks to the increasingly important performances of local networks. But the success of these information systems has also revealed one of their pitfalls.

This study allowed us to better understand the problems associated with local networks, including those relating to the deployment of a VPN network comprising several remote sites while guaranteeing quality of service.

In addition, it allowed us to become more familiar with CISCO equipment.
It emerges, among other things, from this present study that there is agreement between the theoretical reflection carried out and the practical implementation of VPNs, a finding which in
our view validates our project.

However, we admit that our theories and our reflections, although empirical, are not
indubitable and definitive truths.

They are likely to be refuted by more robust models or by later diverging observations which would be linked to the evolution of technologies, themselves constantly changing. It is characteristic of any intellectual proposition to expect to be out of date one day or another.

But it can just as well be reinforced later by other approaches and implemented.

Keys words: network, Virtual, private, security.

Résumé

Depuis l'apparition de l'informatique dans les années 1950, celui-ci s'est imposé graduellement comme un instrument primordial dans le monde professionnel, devenant l'outil incontournable pour la gestion de l'information allant jusqu' à la prise de décision d'une importance capitale pour les entreprises.

Et comme tout progrès engendre de nouveaux défis, au fil du temps naquit un autre besoin qui était celui d'avoir accès à tout moment et de n'importe où aux ressources offertes par les entités informatisées (entreprise, foyer, administrations, etc..) de manière sécurisée d'où la naissance du besoin en VPN (Virtual Private Network ou Réseau Privé Virtuel).

Le développement de la technologie en général et de l'informatique en particulier a suscité un engouement pour la modernisation du traitement des systèmes d'information.

Ces technologies ont pu se développer grâce aux performances toujours plus importantes des réseaux locaux. Mais le succès de ces systèmes d'information a fait aussi apparaître un de leur écueil.

Cette étude nous a permis de mieux appréhender les problèmes liés aux réseaux locaux dont ceux relatifs au déploiement d'un réseau VPN comprenant plusieurs sites distants tout en garantissant une qualité de service.

En outre il nous a permis de nous familiariser davantage aux équipements CISCO.

Il ressort entre autres de cette présente étude qu'il y a accord entre la réflexion théorique menée et la mise en place pratique des VPN, constat qui à notre sens valide notre projet.

Toutes fois nous admettons que nos théories et nos réflexions bien qu'empiriques ne soient pas des vérités indubitables et définitives.

Elles sont susceptibles d'être réfutées par des modèles plus robustes ou par des observations postérieures divergentes qui seraient liées à l'évolution des technologies, elles-mêmes en constante mutation. C'est le propre de toute proposition intellectuelle de s'attendre à être un jour ou l'autre dépassée.

Mais elle peut tout aussi bien être plus tard renforcée par d'autres approches et mises en place.

Mot clés : réseau informatique, Virtual, privé, sécurité.

ملخص

منذ ظهور الحوسبة في الخمسينيات من القرن الماضي , رسخت نفسها تدريجيا لتصبح جزءا أساسيا في العالم المهني , حيث أصبحت أداة مهمة لترتيب و تنسيق المعلومات , التي بدورها ساهمت في تنظيم و تسيير المؤسسات و المصانع.

وبما أن كل التقدم يولد تحديات جديدة ، فقد نشأت مع مرور الوقت حاجة أخرى تتمثل في الوصول في أي وقت ومن أي مكان إلى الموارد التي تقدمها الكيانات المحوسبة (الأعمال ، والمنزل ، والإدارات ، وما إلى ذلك) بطريقة آمنة.

ومن هنا جاءت الحاجة إلى الشبكة الافتراضية الخاصة VPN .

أثار تطور التكنولوجي بشكل عام و الإعلام الآلي بشكل خاص جنونًا لتحديث معالجة أنظمة المعلومات .

تمكنت هذه التقنيات من التطور بفضل الأداء المتزايد باستمرار لشبكات المحلية الهامة . لكن نجاح أنظمة المعلومات هذه كشف أيضًا عن أحدى ثغراتها .

مكنتنا هذه الدراسة من فهم المشكلات المرتبطة بالشبكات المحلية بشكل أفضل، بما في ذلك تلك المتعلقة بنشر شبكة

VPN تضم العديد من المواقع البعيدة مع ضمان جودة الخدمة .

بالإضافة إلى ذلك, فقد سمح لنا بالتعرف والبحث أكثر في معدات CISCO.

يتضح، من بين أمور أخرى، من هذه الدراسة الحالية أن هناك اتفاقًا بين التفكير النظري الذي تم تنفيذه و التنفيذ العملي لشبكات VPN ، وهي نتيجة في رأينا تؤكد صحة مشروعنا.

ومع ذلك فإننا نعترف بأن نظرياتنا وانعكاساتنا ، على الرغم من كونها تجريبية ، ليست لا لبس فيها ونهائية . حقائق.

ومن المحتمل أن يتم دحضها من خلال نماذج أكثر قوة أو من خلال ملاحظات متباينة لاحقة والتي من شأنها أن ترتبط بتطور التقنيات، والتي تتغير باستمرار. من سمات أي اقتراح فكري أن نتوقع أن يكون قديمًا في يوم أو آخر.

ولكن يمكن أيضًا تعزيزها لاحقًا من خلال مناهج أخرى وتطبيقها.

الكلمات المفتاحية : شبكة كمبيوتر ، افتراضية ، خاصة ، أمنة

INTRODUCTION GENERALE :

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

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

Pour y remédier des politiques de la sécurité informatique ont été misent en place afin d'assurer la confidentialité et garder ses données secrètes.

Parmi elles, les VPNs qui offrent un moyen d'échange sécurisé. Le principe du VPN est relativement simple, il a pour but de créer au travers d'un réseau public un tunnel crypté permettant de faire transiter des données jusqu'à un réseau privée disposant d'une connexion internet.

L'objectif principal de ce projet est basé sur le réseau CLOUD dans un environnement VPN IP SEC multi site en utilisant le simulateur CISCO PACKET TRACER.

A fin de présenter notre travail, nous avons structuré notre mémoire comme suit :

- **le premier chapitre** est dédié aux généralités des réseaux informatiques. Nous présenterons les notions de base sur le réseau informatique, sa définition, ses différentes classes ou typologies et les différents équipements d'interconnexion.
- **Le deuxième chapitre** est focalisé sur les réseaux Privés Virtuels : leurs principes et fonctionnement, ses différents types et les différents protocoles utilisés pour sa réalisation.
- **Le troisième chapitre** donne une indication sur l'administration et la sécurité adéquate à mettre en place afin de sécuriser le réseau. Cette réflexion constitue en quelque sorte une transition pour entamer la partie implémentation du programme de configuration des réseaux choisis pour la simulation qui instruit réellement sur la mise en œuvre de l'interconnexion et des services VPN.
- **Le quatrième chapitre** C'est la partie conception et de simulation des déférentes architec-

tures réseaux et nous interprétons les résultats de simulation de chaque réseau, ou on entame à la configuration et les tests qui sont notre partie pratique ou nous concevant notre architecture réseau et faire les configurations nécessaires au niveau des routeurs afin de créer les tunnels VPNs entre les sites.

Enfin, notre mémoire s'achève avec une conclusion générale résumant les connaissances acquises durant la réalisation du projet ainsi que les perspectives.

Chapitre I :

Généralité sur les différents réseaux

1.1 Introduction :

En connectant tous les postes de travail, périphériques, terminaux et autres contrôleurs de trafic, les réseaux informatiques ont permis aux entreprises de partager efficacement divers éléments (fichiers, imprimantes, etc.) et de communiquer entre elles, notamment par courrier électronique et messagerie instantanée. Il a également permis de se connecter à des serveurs de données, de communications et de fichiers.

1.2 Définition d'un réseau :

Un réseau est un groupe de deux ou plusieurs ordinateurs ou autres appareils électroniques qui permettent d'échanger des données et de partager des ressources.

1.3 Intérêts d'un réseau :

Un ordinateur est une machine de traitement de données. Les humains, en tant qu'être connecté, ont rapidement compris l'intérêt qu'il y avait à connecter ces ordinateurs entre eux pour qu'ils puissent échanger des informations.
Un réseau permet :

- Le partage de ressources (fichiers, applications ou matériels).
- La communication entre personnes (courrier électronique, discussion en direct…)
- La communication entre processus (entre des machines industrielles par exemple).
- La garantie de l'unicité de l'information (bases de données).
- Le jeu vidéo multi-joueurs.

Les réseaux permettent également la standardisation des applications, et on parle généralement de groupware. Par exemple, des e-mails et des calendriers de groupe qui vous permettent de communiquer plus efficacement et plus rapidement. Voici les avantages de ces systèmes:

- Diminution des couts grâce aux partages de données et de périphériques.
- Standardisation des applications.
- Accès aux données en temps utile.
- Communication et organisation plus efficace. [1]

1.4 Topologie d'un réseau :

La topologie d'un réseau correspond à son architecture (physique ou logique), définissant les connexions entre les équipements du réseau et la hiérarchie possible entre eux.

1.4.1 Topologie physique :

La disposition physique, c'est-à-dire la configuration spatiale d'un réseau, est appelée topologie physique. Une distinction est généralement faite entre les topologies suivantes:

- La topologie en bus
- La topologie en étoile
- La topologie en anneau
- La topologie en arbre
- la topologie maillée. [2]

1.4.1.1 Topologie en bus :

Dans une architecture de bus, les ordinateurs sont connectés à la même ligne de transmission, chaque ordinateur étant connecté via un connecteur BNC. [2]

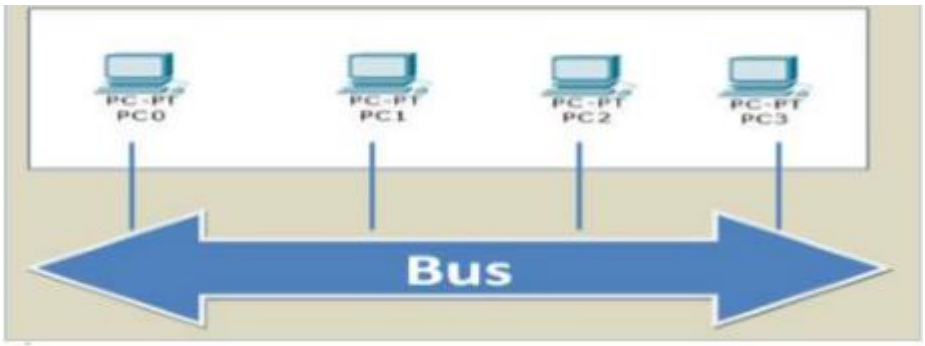

Figure I.1 : Topologie en bus

1.4.1.2 Topologie en étoile :

Cette topologie de réseau informatique présente de meilleures caractéristiques que la topologie en bus. Les terminaux sont reliés entre eux par le biais d'un dispositif appelé « nœud central ». Un nœud peut être un concentrateur, un commutateur ou un routeur. Les données y sont transmises avant d'être redirigées à l'adresse de destination. Le nombre des postes de travail pouvant être relié à un réseau en étoile dépend du nombre de ports disponibles sur le nœud central. [2]

Figure I.2 : Topologie en étoile

1.4.1.3 Topologie en anneau :

C'est une topologie de réseau fermé. Les données circulent dans une seule direction. Il est envoyé d'une station à une autre jusqu'à ce qu'il atteigne l'adresse de destination. [2]

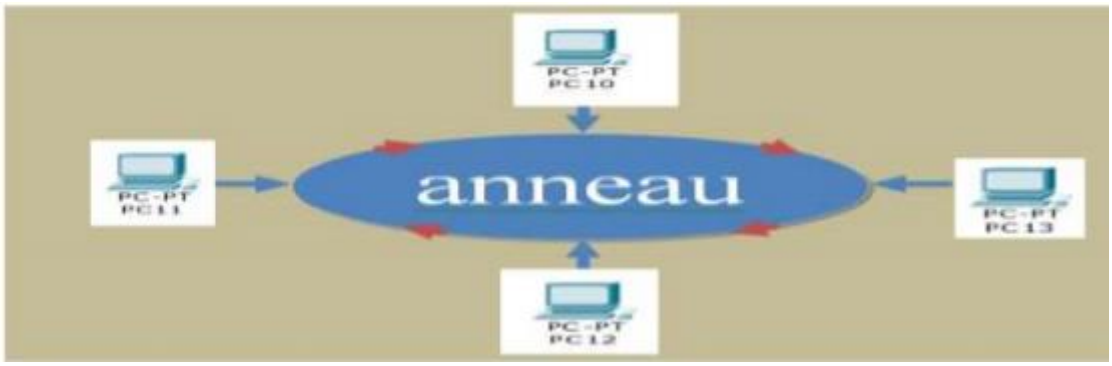

Figure I.3 : Topologie en anneau

1.4.1.4 Topologie en arbre :

Également appelé topologie hiérarchique. Le réseau est divisé en différents niveaux hiérarchiques et un élément du réseau est lié à d'autres sites de niveau inférieur. [2]

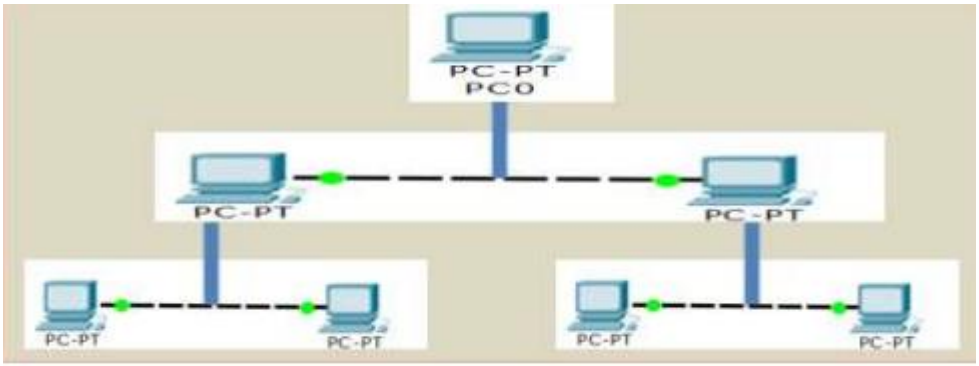

Figure I.4 : Topologie en arbre

1.4.1.5 Topologie maillée :

La topologie maillée est un réseau en étoile amélioré. Chaque poste de travail connecté à tous les autres appareils. Le nombre de connexions est plus élevé en l'absence de poste de travail. [2]

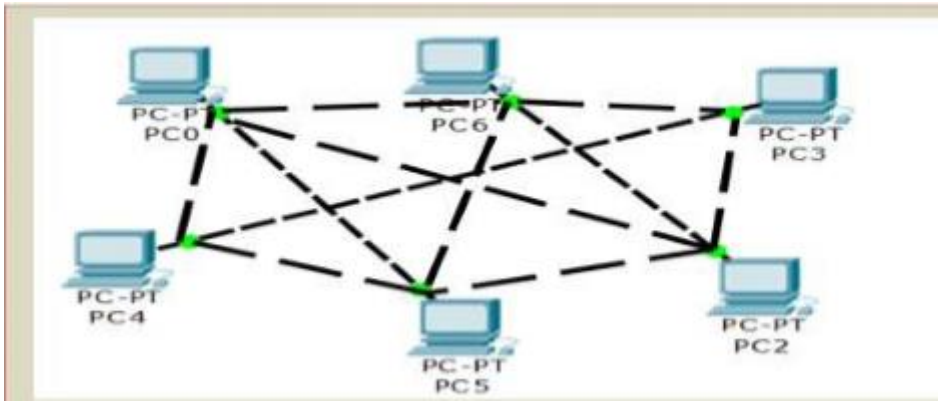

Figure I.5 : Topologie maillée

- **Les avantages et les inconvénients de chaque topologie :**

	Les avantages	Les inconvénients
Topologie en bus	*Diffusion facile. *Suppression facile. * Mise en place facile. * Coût faible	* Pas de transfert privé. * Bus principal trop sensible.
Topologie en étoile	* la précision d'envoi. * L'ajout facile de postes. * Diffusion facile. * La suppression du (des) site (s) n'affecte pas le fonctionnement du réseau	* Dépend du nœud central (Switch ou hub). * Cher (nécessite plusieurs câbles). * collision.
Topologie en anneau	*Pas de collision puisqu'on parle que lorsque l'on n'est en possession du jeton diffuseur. * Plusieurs transferts sont possibles.	* Le dysfonctionnement de la station est un dysfonctionnement du réseau. * Diffusion longue. * Le nombre de machines susceptibles d'être affectées au moment de la transmission des informations.
Topologie en arbre	*la plus adaptée pour les réseaux de grande taille. * plus facile de gérer le réseau en définissant des droits d'accès pour chaque branche du réseau.	* la dépendance des unités inférieures. * Une panne se situant en haut de la hiérarchie est critique et bloque tous les postes en dessous.
Topologie maillée	* Une fois mise en œuvre, la grille en filet offre la sécurité la plus fiable et des performances inégalées. *Chaque poste de travail est indépendant de l'autre. Un échec à une station particulière n'empêche pas les autres stations de communiquer entre elles.	* la mise en place devient de plus en plus difficile en fonction du nombre des stations à installer. *Les ressources nécessaires sont énormes que ce soit en matière d'équipement de connexion ou de câblage.

Tableau I.1 : Les avantages et les inconvénients de chaque topologie.

1.4.2 Topologies logiques :

Une topologie logique, contrairement à une topologie physique, représente la façon dont les données se déplacent le long des lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI. [3]

1.4.2.1 Topologie Ethernet :

Un réseau Ethernet est de type topologie logique en bus. Cela signifie que toutes les stations reliées à un segment Ethernet accèdent à un même support partagé (shared medium). Ethernet utilise des technologies de base de bande et de multiplexage. L'algorithme de détection de porteuse (accès multiple / détection de collision) (CSMA / CD) est utilisé pour communiquer entre eux. [4]

1.4.2.2 Topologie du Token Ring (réseau en anneau à jeton):

La topologie d'un réseau token ring est un anneau logique qui se concrétise physiquement par une étoile. Cela signifie qu'un concentrateur (Medium Attachment Unit – MAU ou hub) relie la ligne d'émission d'une station à la ligne de réception de la station suivante, ce qui, logiquement, crée un anneau. [4]

1.4.2.3 Topologie FDDI (Fiber Distributed Data Interface) :

LAN FDDI (Fiber Distributed Data Interface) est une technologie d'accès au réseau utilisant des câbles à fibre optique. FDDI se compose de deux anneaux: une boucle primaire et une boucle secondaire. La boucle secondaire est utilisée pour compenser les erreurs de la boucle primaire. FDDI utilise une boucle symbolique utilisée pour découvrir et corriger les erreurs. Donc, si la MAU est en panne, le réseau continuera à fonctionner. [3]

1.5 Architectures réseaux :

En étendant le contexte de la définition du réseau aux services qu'il fournit, il est possible de distinguer les deux types d'exploitation.

- **Architecture d'égal à égal** (peer to peer parfois appelée poste à poste), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur joue un rôle similaire.
- **Architecture de type client serveur**, ou un ordinateur (serveur) fournit des services réseau aux ordinateurs clients. **[5]**

1.6 Types de réseaux :

Il existe différents types de réseaux en fonction de leur taille (en termes de nombre d'appareils), de leur vitesse de transfert de données et de leur portée. Les catégories de réseaux suivantes sont généralement identifiées:

- Réseaux personnels ou PAN (Personal Area Network).
- Réseaux locaux ou LAN (Local Area Network).
- Réseaux métropolitains ou MAN (Metropolitain Area Network).
- Réseaux étendus ou WAN (Wide Area Network).

1.6.1 Les Réseaux personnels (PAN) :

Les réseaux personnels (Personal Area Networks), sont des réseaux à très faible portée, de l'ordre d'une dizaine de mètres. Ils sont utilisés pour relier des équipements informatiques entre eux sans liaison filaire tel que le Bluetooth, le ZigBee, les liaisons infrarouges. Chaque personne a un réseau local qui comprend son box internet et tout ce qui est connecté dessus, c'est le Personal Area Network. [6]

1.6.2 Réseaux locaux (LAN) :

Ce sont des réseaux de taille plus ou moins modeste, complexes, qui permettent l'échange de données informatiques et le partage de ressources (données, disques durs, périphériques divers, etc.). L'étendue géographique des réseaux locaux ne dépasse pas 10 km. Le débit, ou la vitesse de communication, varie de quelques Mbps à 100 Mbps. Le nombre de stations ne dépasse généralement pas 1 000. Une variante du LAN est le LAN fédérateur ou réseau de base (backbone) qui est la voie principale empruntée par le trafic. [4]

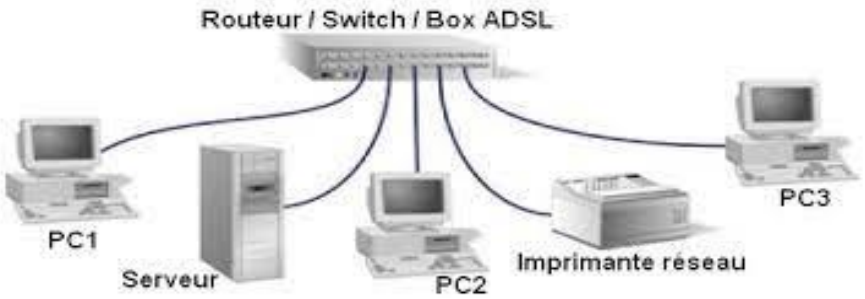

Figure I.6 : LAN

1.6.3 Réseau métropolitain (MAN) :

Les réseaux métropolitains permettent l'interconnexion de plusieurs réseaux locaux répartis sur différents sites dans une zone urbaine dont l'étendue géographique n'excède

pas 200 km. Ces réseaux peuvent être privés ou publics. Ils se distinguent aussi par leurs taux d'erreurs de communication. Le taux d'erreurs pour les réseaux MAN reste faible bien que plus élevé que pour les réseaux locaux : de 1 bit erroné sur 108 à 1 bit sur 1015. Le débit est élevé car supérieur à 100 Mbps (sur liens de fibre optique). [4]

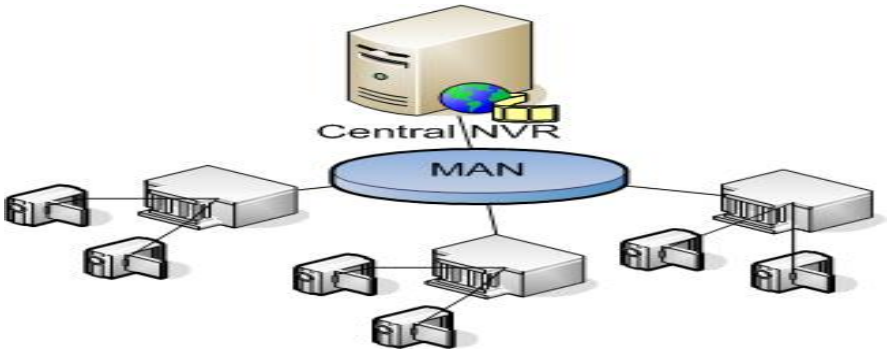

Figure I.7 : Réseau MAN

1.6.4 Réseaux étendus (WAN) :

Les WAN (Wide Area Network) appelés aussi réseaux longue distance se situent à l'échelle nationale et internationale. Ce sont généralement des réseaux de télécommunications gérés par des opérateurs, qui assurent la transmission des données entre les villes et les pays à l'échelle de la planète. Leurs supports de transmission sont variés (ligne téléphonique, ondes hertziennes, fibre optique, satellite, etc.). La plupart de ces types de réseaux sont publics. Le taux d'erreurs de communication est plus élevé que celui des MAN : de 1 bit erroné sur 106 à un bit erroné sur 1012. Les débits généralement plus faibles que dans les réseaux locaux dépendent du support de transmission : ils varient de 56 kbps à plus de 625 Mbps pour les réseaux ATM (Asynchronous Transfer Mode) que nous verrons plus loin. [4]

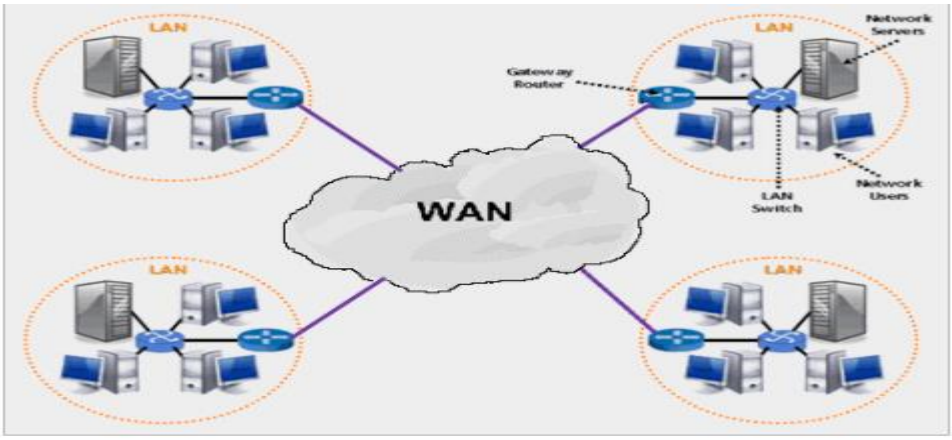

Figure I.8 : Réseau WAN

Classification des réseaux :

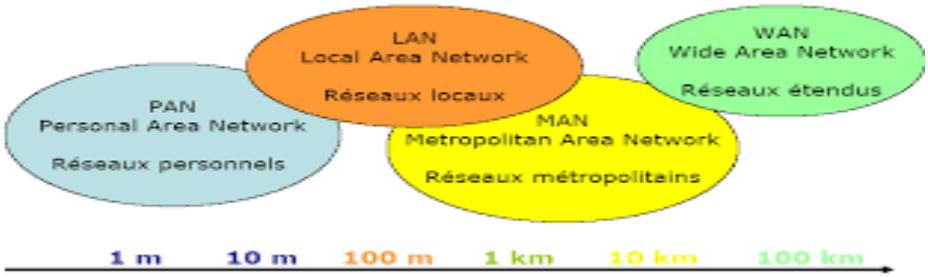

Figure I.9 : Classification des réseaux.

1.7 Supports de transmission :

Pour connecter les différentes entités d'un réseau, plusieurs supports physiques de transmission de données peuvent être utilisés. L'une de ses possibilités est l'utilisation de câbles.

Il existe de nombreux types de câbles, mais on distingue généralement :

- Le câble de type coaxial.
- Le câble de type pair torsadé
- La fibre optique.

En plus des liaisons physiques, actuellement il y'a des réseaux qui utilisent la liaison sans fil comme support de transmission. [5].

1.7.1 Le Câble coaxial :

Le câble coaxial est une ligne de transmission ou de liaison asymétrique, utilisée à des fréquences élevées, et se compose d'un câble à deux conducteurs. Ce type de câble est fait de cuivre spécialement conçu avec une gaine métallique et d'autres composants conçus pour éviter les interférences du signal. C'est une technologie utilisée à l'origine pour les antennes de télévision. Il connecte le téléviseur à l'antenne.

Figure I.10 : Câble coaxial et le connecteur BNC

La capacité de transmission d'un câble coaxial dépend de sa longueur, des propriétés physiques des conducteurs et de l'isolation.

Il existe deux grands types de câbles coaxiaux :

- **Le câble coaxial épais (Thicknet ou 10base5):** Epais et raide à cause de son blindage, il est recommandé pour l'installation de câble fédérateur. Sa gaine est jaune.
- **Le câble coaxial fin (Thinnet ou 10base 2)** : D'un diamètre plus réduit, il est plus pratique dans des installations comprenant des courbes. De plus il est plus économique mais dispose d'un blindage moins conséquent.

Le thinnet et le thicknet utilisent les deux des connecteurs BNC (bayonet Neill concelman) servant à relier les câbles aux ordinateurs. [5]

Figure I.11 : Câble coaxial (le thinnet et le thicknet)

1.7.2 La paire torsadée :

Dans sa forme la plus simple, le câble à paire torsadée se compose de brins de cuivre torsadés ensemble et recouverts d'isolant.

Le câble est souvent fabriqué à partir de plusieurs paire torsadées regroupées et placer à l'intérieur de la gaine productrice.

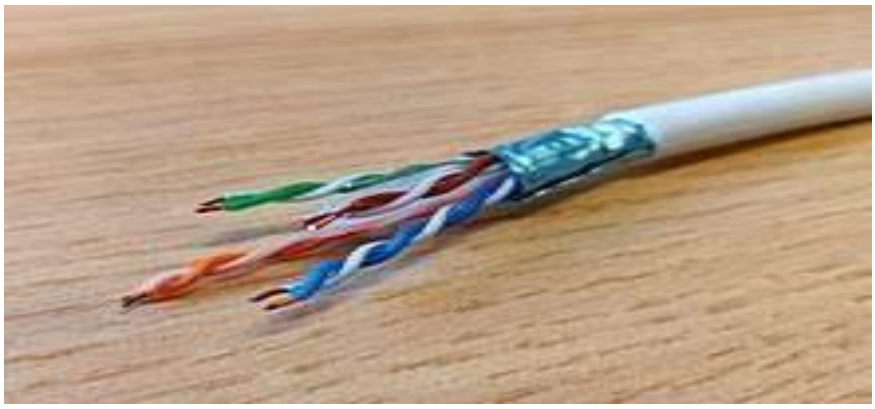

Figure I.12 : Câble à paire torsadées

L'entrelacement permet de supprimer les bruits (interférences électriques) dus aux paires adjacentes ou aux autres sources (moteur, relais, transformateur…) en réseau informatique.

On distingue plusieurs types de câbles à paires torsadées, UTP et STP sont les plus utilisées et les plus répondu pour les réseaux locaux.

- **La paire torsadée non blindées (UTP) :**

Les caractéristiques de UTP :

- l'UTP est composé de deux fils de cuivre recouverts d'isolant
- la longueur maximale d'un segment est de 100 mètres.

- **La paire torsadée blindée (STP) :**

Le câble STP utilise une gaine en cuivre meilleure et plus protectrice que le câble UTP.

Les caractéristiques de ce câble :

- Les fils de cuivre de la paire sont torsadés par eux-mêmes, offrant une excellente protection STP.
- Il permet un transport plus rapide sur de longues distances.

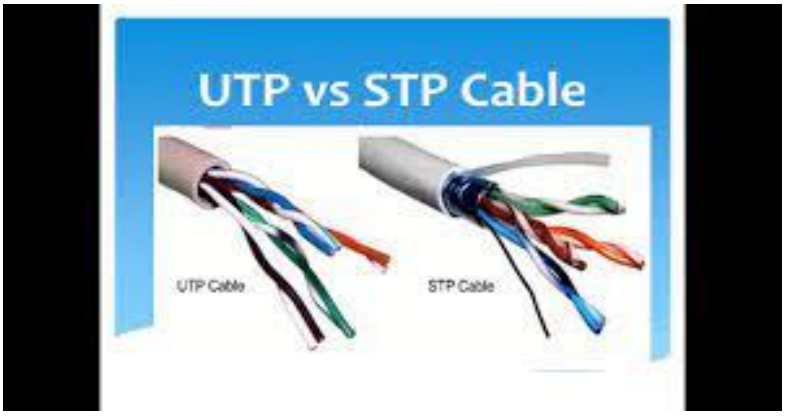

Figure I.13 Câble UTP et STP

Connecteurs à paire torsadée: la paire torsadée se connecte à l'aide d'un connecteur RJ-45. Ce connecteur est similaire au RJ-11 avec la seule différence dans le nombre de branches, puisque le RJ-45 a huit broches tandis que le RJ-11 n'a que six broches, ou généralement quatre. [5]

1.7.3 La fibre optique :

Une fibre optique est un fil dont l'âme, très fine, en verre ou en plastique, a la propriété de la transmission de données sous forme d'impulsions lumineuses à un débit plus élevé que les autres supports filaires. La fibre optique se compose d'un cœur, d'une gaine op-

tique et d'une enveloppe de protection, comme illustré dans la figure suivante:

Figure I.14 Fibre optique

Caractéristiques de la fibre optique :

- Légèreté
- Immunité au bruit
- Faible atténuation
- Tolère des débits de l'ordre de 100Mbits/s
- Largeur de bande de quelques dizaines de MH à plusieurs GH.

On distingue deux types de fibre optique :

- **Les fibres multi modes :** ou le cœur de la fibre est très volumineux ce qui permet la propagation de plusieurs modes (trajets) simultanément. Il existe deus sortes de MMF ; une à saut d'indice et l'autre à gradient d'indice.
- **Les fibres monomodes** : SMF (single mode fiber) avec un cœur fin et ne peut transporter le signal que sur un seul trajet, elle permet de transporter le signal à une distance plus longue (50 fois) que celle de la multi mode. [5]

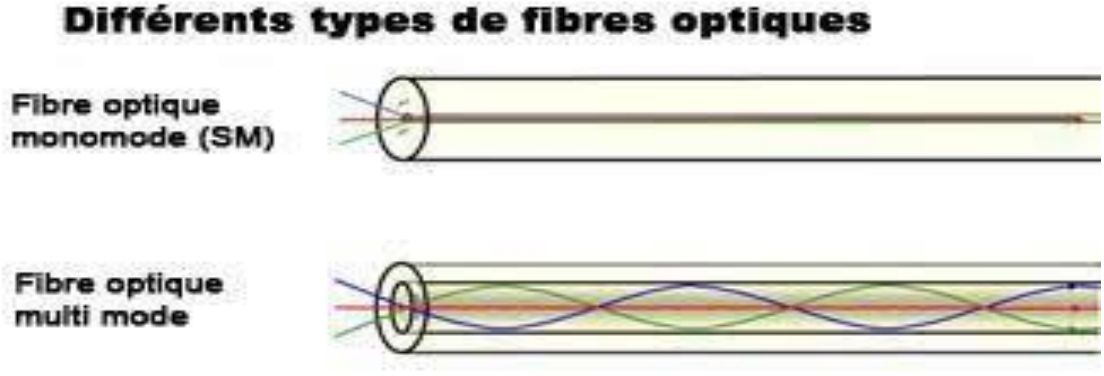

Figure I.15 : Fibre optique monomode et multi mode

- **Les avantages et les inconvénients de chaque câble :**

	Les avantages	les inconvénients
Le câble coaxial	-Bande passante relativement importante (multiplexage de signaux). -Résistance assez importante face aux perturbations électriques et électromagnétiques.	-Installation difficile. Gros diamètre (1 – 1.9 cm). -Assez rigide difficultés de câblage et souffre aussi d'un manque d'adaptation face à de futures modifications. -Le coût plus élevé.
La paire torsadée	-Simple à installer. -Possibilité de travailler en Full Duplex. -Petit diamètre (pour installation dans des conduits existants). -Permet d'avoir un câblage dit universel: Téléphone, Fax, Info, etc. ...	-Sensible aux interférences. -Câblage plus cher et prend plus de place dans les gaines techniques et par conséquence Plus d'appareils actifs (Hubs, Switch).
La fibre optique	-La sensibilité nulle aux interférences. -faible atténuation du signal Pas d'échauffement. -grande bande passante.	-Le coût important. - Des composants fragiles, elle exige plus de protection autour du câble par rapport au autre câble.

Tableau I.2 : les avantages et les inconvénients de chaque câble.

1.8 Les différents dispositifs de la connectivite :

1.8.1 Modem :

Le modem est appareil qui permet d'adapter les signaux électriques entre le routeur et le support physique extérieur pour la connexion à un réseau externe (ligne téléphonique). [7]

Figure I.16 : Modem.

1.8.2 Le firewall :

Un firewall (pare-feu), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-

feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante. [7]

Figure I.17 : Firewall

1.8.3 Le commutateur/ Le concentrateur :

Le commutateur réseau ou switch est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs ports Ethernet. Il a donc la même apparence qu'un concentrateur (hub). Contrairement à un concentrateur, un commutateur ne se contente pas de reproduire sur tous les ports chaque trame (informatique) qu'il reçoit. Il sait déterminer sur quel port il doit envoyer une information, en fonction de l'ordinateur auquel elle est destinée. Les commutateurs sont souvent utilisés pour remplacer des concentrateurs. [7]

Commutateur Concentrateur

Figure I.18 : Commutateur / Concentrateur

1.8.4 Carte réseaux : (Network Interface Card) :

Une carte réseau est un périphérique informatique qui fait le lien entre l'ordinateur dans lequel elle est installée et le réseau auquel elle le connecte. Elle est constituée d'un ensemble de composants électroniques soudés entre eux sur un même circuit imprimé. [7]

Figure I.19 : Carte réseaux.

1.8.5 La passerelle (routeur):

Une passerelle est un dispositif qui permet de relier deux réseaux informatiques comme par exemple un réseau local et Internet. Ainsi, plusieurs ordinateurs ou l'ensemble du

réseau local peuvent accéder à Internet par l'intermédiaire de la passerelle. Le plus souvent, elle sert également de firewall. [7]

Figure I.20 : Routeur

1.8.6 Le répéteur :

Un répéteur est un simple équipement utilisé pour régénérer un signal entre deux nœuds d'un réseau, afin d'étendre la distance du câble au réseau. Le répéteur ne fonctionne qu'au niveau physique (couche 1 du modèle OSI), c'est-à-dire qu'il ne fonctionne qu'au niveau des informations binaires circulant sur la ligne de transmission et il n'est pas en mesure d'interpréter des paquets d'informations.

D'autre part, le répéteur peut permettre de former une interface entre deux supports physiques de types différents, c'est-à-dire qu'il peut permettre par exemple de permettre de connecter une pièce paire torsadée à une bande de fibres optiques. [5]

Figure I.21 : Répéteur

1.8.7 Le pont :

Un pont est un appareil qui connecte des réseaux exécutant le même protocole. Il fonctionne sur la couche liaison de données du modèle OSI, et est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à un périphérique situé en face du pont.

Ainsi, le pont permet de diviser le réseau en conservant les trames affectées au niveau local au niveau du réseau local et en envoyant les trames allouées aux autres réseaux.

Cela permet de réduire le trafic (notamment les collisions) sur chaque réseau et d'augmenter le niveau de confidentialité car les informations destinées à un réseau ne peuvent pas être entendues à l'autre extrémité. [5]

1.9 Le protocole informatique:

Le protocole informatique définit les règles et procédures permettant à deux processus informatiques d'échanger des données, notamment sur un réseau. Le rôle des protocoles est de préserver les données pour qu'elles ne se perdent pas. Certains protocoles, par exemple, seront spécialisés dans le partage de fichiers (ftp), d'autres pourront être utilisés simplement pour gérer l'état de transmission et les erreurs (c'est le cas de l'ICMP) ... Sur Internet, les protocoles utilisés font partie de la chaîne protocole, c'est-à-dire un groupe de protocoles avec The link. Ce groupe de protocoles est appelé TCP / IP. Il contient, entre autres, les protocoles suivants: http, FTP, ARP, ICMP, IP, TCP, UDP, SMTP, Telnet, NNTP. [8]

1.10 Le modèle OSI (Open Systems Interconnection) :

Le modèle OSI (de l'anglais Open Systems Interconnection) est une norme de communication, dans un réseau, pour tous les systèmes informatiques. Le modèle OSI sert de base à la théorie générale des réseaux, et est un modèle théorique qui affiche la circulation des données dans un réseau, et est décrit en 7 couches: la partie supérieure est abstraite et la partie inférieure est tangible.

Ce modèle décrit très précisément le lien entre deux nœuds de réseau consécutifs (deux ordinateurs, par exemple) de manière descendante et décomposée:

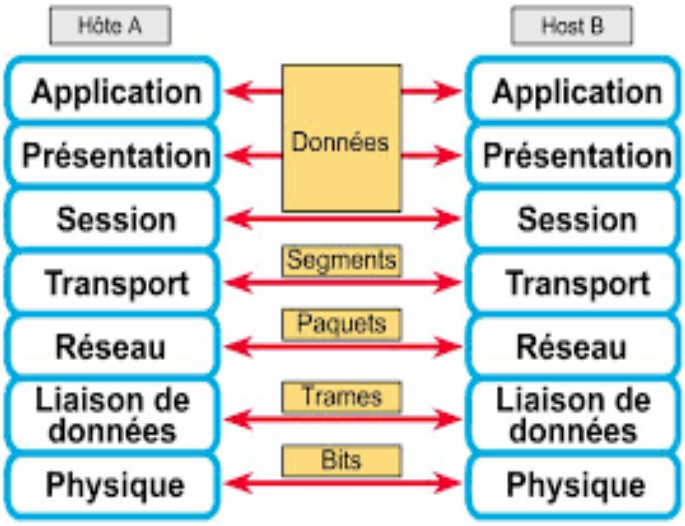

Figure I.22 : Les 7 couches du modèle OSI

Chaque couche rend un service décrit dans la documentation de l'ISO et géré par un protocole permettant de réaliser ce service lorsque la couche est abstraite. Lorsque la couche est matérielle la documentation décrit comment le service est rendu par le composant matériel.

Nous décrivons brièvement chacune des 7 couches du modèle OSI :

Couche 1 : Couche physique : La couche physique définit les spécifications du média (câblage, connecteur, voltage, bande passante…).

- **Couche 2 : Couche liaison de donnée** : La couche liaison de donnée s'occupe de l'envoi de la donnée sur le média. Cette couche est divisée en deux sous-couches :

- La sous-couche MAC (Média Access Control) est chargée du contrôle de l'accès au média. C'est au niveau de cette couche que l'on retrouve les adresses de liaison de donnée (MAC, DLCI).
- La sous-couche LLC (Layer Link Control) s'occupe de la gestion des communications entre les stations et interagit avec la couche réseau.

- **Couche 3 : Couche réseau** : Cette couche gère l'adressage de niveau trois, la sélection du chemin et l'acheminement des paquets au travers du réseau.
- **Couche 4 : Couche transport :** La couche transport assure la qualité de la transmission en permettant la retransmission des segments en cas d'erreurs éventuelles de transmission. Elle assure également le contrôle du flux d'envoi des données.
- **Couche 5 : Couche session :** La couche session établit, gère et ferme les sessions de communications entre les applications.
- **Couche 6 : Couche présentation :** La couche présentation spécifie les formats des données des applications (encodage MIME, compression, encryptions).
- **Couche 7 : Couche application :** Cette couche assure l'interface avec les applications, c'est la couche la plus proche de l'utilisateur.

Les Avantages du modèle OSI :

- Diviser les communications réseau en morceaux plus petits et plus simples pour: Une meilleure compréhension.
- L'uniformisation des éléments afin de permettre le développement multi constructeur.
- La possibilité de modifier un aspect de la communication réseau sans modifier le reste (Exemple : un nouveau média) Pour communiquer entre les couches et entre les hôtes d'un réseau, OSI a recourt au principe d'encapsulation.

- Encapsulation : processus de conditionnement des données consistant à ajouter une en-tête de protocole déterminé avant que les données ne soient transmises à la couche inférieure.

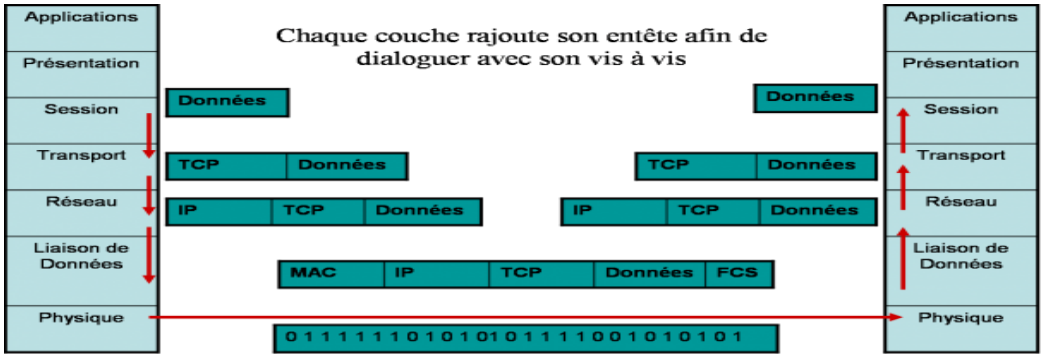

Figure I.23 : Principe de l'encapsulation

Lorsque deux hôtes communiquent, on parle de communication d'égale à égale, c'est-à-dire que la couche N de la source communique avec la couche N du destinataire. Lorsqu'une couche d'émetteur construit des données, elle encapsule ces données avec ses informations, puis les transmet à la couche inférieure. Le mécanisme inverse se produit au niveau du destinataire lorsqu'une couche reçoit les données de la couche inférieure, supprime les informations qui lui sont associées, puis transmet les informations restantes à la couche supérieure. Par conséquent, les données qui passent par la couche N de la source sont les mêmes données que celles qui passent par la couche N du destinataire.

- Pour identifier les données lors de leur passage au travers d'une couche, l'appellation PDU (Unité de données de protocole) est utilisée. [9]

1.11 Le modèle TCP/IP

Le modèle TCP / IP (également appelé modèle Internet), a été installé bien avant la publication du modèle OSI. Il propose également une approche standardisée (utilisation de couches) mais il n'en contient que quatre: [5]

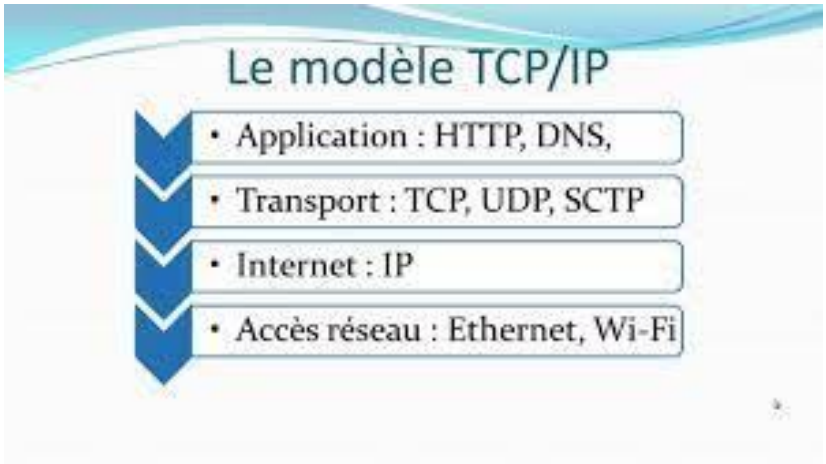

Figure I.24 : Les 4 couches TCP/IP

Aujourd'hui, le modèle TCP / IP plus flexible remporte le marché. Le modèle OSI plus strict est principalement utilisé pour certaines applications importantes, ou pour ses fonctions qui permettent de garantir une qualité de service.

- **Les rôles des différentes couches sont les suivants :**
  - **Couche Accès réseau :** elle spécifie la forme sous laquelle les données doivent être acheminées quelque soit le type de réseau utilisé.
  - **Couche Internet :** elle est chargée de fournir le paquet de données (datagramme).
  - **Couche Transport :** elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.
  - **Couche Application :** elle englobe les applications standard du réseau.

1.12 Comparaison entre le modèle TCP/IP et le modèle OSI :

Ces deux modèles sont très similaires en ce qu'ils sont tous deux des modèles de connexion de couche et utilisent l'encapsulation de données.

On remarque cependant deux différences majeures :

• TCP/IP regroupe certaines couches du modèle OSI dans des couches plus générales.

•TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau. [5]

- Les couches de chaque modèle :

<table>
<tr><th colspan="2">Modèle OSI</th><th colspan="2">Modèle TCP/IP</th></tr>
<tr><th>Couche</th><th>Désignation</th><th>Couche</th><th>Désignation</th></tr>
<tr><td>Application</td><td rowspan="3">Couche application</td><td rowspan="2">Application</td><td rowspan="3">Protocoles</td></tr>
<tr><td>Présentation</td></tr>
<tr><td>Session</td><td>Transport</td></tr>
<tr><td>Transport</td><td rowspan="4">Couche flux de données</td><td rowspan="2">Internet</td><td rowspan="4">Réseau</td></tr>
<tr><td>Réseau</td></tr>
<tr><td>Liaison de données</td><td rowspan="2">Accès réseau</td></tr>
<tr><td>Physique</td></tr>
</table>

Tableau I.3 : Les modèles OSI et TCP/IP

1.13 Le protocole UDP :

Le protocole de datagramme utilisateur UDP (User Datagram Protocol) est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la

couche transport du modèle OSI, quatrième couche de ce modèle, comme TCP.
Le rôle de ce protocole est de permettre la transmission de données (sous forme de datagrammes) de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. Aucune communication préalable n'est requise pour établir la connexion, au contraire de TCP (qui utilise le procédé de handshaking). UDP utilise un mode de transmission sans connexion. [10]

1.14 Conclusion :

Utilisation de serveurs partagés pour les réseaux informatiques (offre une grande flexibilité). Les réseaux permettent d'accéder à un grand nombre de ressources et c'est la raison de l'augmentation de la demande d'utilisation des réseaux. Par conséquent, les risques augmentent.

Chapitre II :

Les réseaux privés virtuels

2.1 Introduction :

Avant l'émergence des VPN, les entreprises devaient utiliser des liens appelés TRANSPAC, ou lignes louées. Ensuite, les VPN ont permis de démocratiser ce type de connexion. Le terme VPN sera utilisé spécifiquement pour accéder aux structures de types de Cloud computing.

Nous allons aborder dans ce chapitre, quelques notions sur les réseaux privés virtuels ainsi que les concepts sur leurs fonctionnements.

2.2 Transpac :

2.2.1 Définition de TRANSPAC :

Réseau de transmission de données par paquets exploité par France Télécom .Le réseau Transpac est le plus grand réseau X.25 (Le terme X25 désigne le niveau 3 du modèle OSI où les paquets sont transportés entre les champs d'information des trames LAPB) du monde. Il était destiné à écouler une forte proportion du trafic téléinformatique de l'époque avec les principales caractéristiques suivantes :

- un temps moyen de traversée du réseau de 0,2 seconde;

- une disponibilité élevée;

- des vitesses de raccordement s'échelonnant entre 50 bits/seconde (terminaux télex) à 64 kilobits/seconde (gros ordinateurs);

- déploiement sur l'ensemble du territoire avec une douzaine de Commutateurs, 30 points de raccordement pour 10.000 terminaux asynchrones; [1]

2.2.2 Historique de TRANSPAC :

Transpac était une filiale de l'opérateur public de télécommunications France Télécom, créée en 1979 et spécialisée dans la fourniture d'accès réseaux pour les entreprises. Elle détenait le monopole commercial pour la fourniture d'accès X.25 (protocole de communication normalisé par commutation de paquets) de 1979 jusqu'à 2006. Le réseau Télétel du Minitel distribué par France Télécom reposait sur le réseau X.25 de Transpac.

Depuis le printemps 1994, Transpac propose une gamme de produits de connectivité Internet principalement centrée sur X.25. Ce réseau commuté a été soumis à la concurrence de protocoles permettant des vitesses de transmission plus élevées, notamment

ceux de l'Internet et du protocole Internet (Internet Protocol) moins coûteux à mettre en œuvre, éludant l'idée de monopole et donc proposés par d'autres. Des entreprises du secteur privé comme Bouygues Telecom ou Cegetel. Vers la fin des années 90, l'activité de Transpac a ensuite évolué vers la fourniture de réseaux IP, mais aussi vers des offres d'hébergement et de fourniture de services.

Cette filiale a fusionné avec France Télécom le 1er janvier 2006. Après le 1er juin 2006, les offres commerciales de Transpac ont été opérées par Orange Business Services.

Orange Business Services a assuré la commercialisation et la maintenance du réseau X.25 jusqu'en juin 2012, date d'expiration de l'exploitation technique et commerciale. Cet arrêt a entraîné l'arrêt des services Minitel basés sur ce réseau. [2]

2.2.3 Architecture de TRANSPAC :

Seuls les trois premiers niveaux du modèle OSI de l'ISO sont implantés dans Transpac :

Le niveau 3 (couche réseau) offre à l'usager un service de transmission de données sur connexion, appelé X25. Les informations circulant à ce niveau s'appellent des paquets, N PDU.

Le niveau 2 (couche liaison) assure la transmission des données par blocs, L SDU sans erreurs. Les informations circulant à ce niveau s'appellent des trames, L PDU. Ce niveau gère le protocole de transmission entre les deux entités (gestion des ressources, traitement des erreurs) et s'occupe de l'enveloppe des trames pour leur délimitation dans le flot continu de données. Le protocole utilisé, appelé LAP B (Link Access Protocol version B), est un protocole de transfert de données sur connexion. Transpac utilise diverses versions de protocoles (LAP D...). Néanmoins le segment terminal d'accès usager utilise toujours le protocole LAP B.

Le niveau 1 (couche physique) permet le transport des informations élémentaires (bits) à un rythme fixe (vitesse de la liaison). Il utilise un format de trame, MA PDU, connu sous le nom de HDLC (High Level Data Link Control). La couche physique est mise en œuvre sur les liaisons spécialisées. [1]

2.2.4 Avantages et inconvénient de réseau TRANSPAC :

Les avantages	Les inconvénients
-Couverture du territoire. -Connexion de matériels hétérogènes. -La sécurité et la fiabilité sont garanties par la société Transpac -Services complémentaires (Groupe fermé d'abonnés, Doublement de lignes) qui augmente de la sécurité.	-Adaptation aux nouvelles technologies. - Dépenses supplémentaires. -Configuration plus longue.

Tableau II. 1 : Les avantages et inconvénient de réseau TRANSPAC. [1]

2.3 Réseau privé virtuel (VPN):

2.3.1 Définition d'un VPN :

VPN est l'abréviation de « virtual private network » (réseau privé virtuel) un service qui protège notre connexion Internet et notre confidentialité en ligne. Un VPN crée un tunnel chiffré pour nos données, protège notre identité en ligne, nous permet de cacher notre adresse IP et d'utiliser les points d'accès Wi-Fi publics en toute sécurité. [3]

2.3.2 Le rôle d'un VPN :

Un VPN est un outil qui permet de connecter un ordinateur à un serveur distant. Cela en isolant le trafic généré par l'utilisateur et son serveur distant.

2.3.3 Le fonctionnement du VPN :

Un VPN est basé sur le tunneling, qui est un protocole utilisé pour tricher données par un algorithme de cryptage entre les deux réseaux.

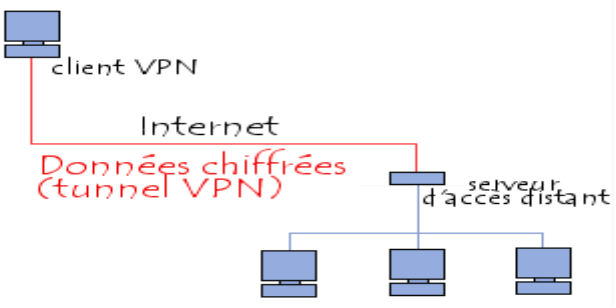

Figure II. 1 : exemple de fonctionnement du VPN

2.3.3.1 Le principe de tunneling :

Le tunnel permet de transférer des données du point A au point B, ce qui signifie que les données qui "pénètrent" dans le tunnel quand "sort" se trouvent nécessairement au point b.

Les données sont transférées par encapsulation, à la fin du tunnel, les données à transférer sont entrées dans un paquet de protocole "tunneling", puis dans un paquet de protocole de transfert de données. L'autre extrémité du tunnel. Données tirées du «creusement du tunnel» et leur voyage se poursuit dans sa forme originale. [4]

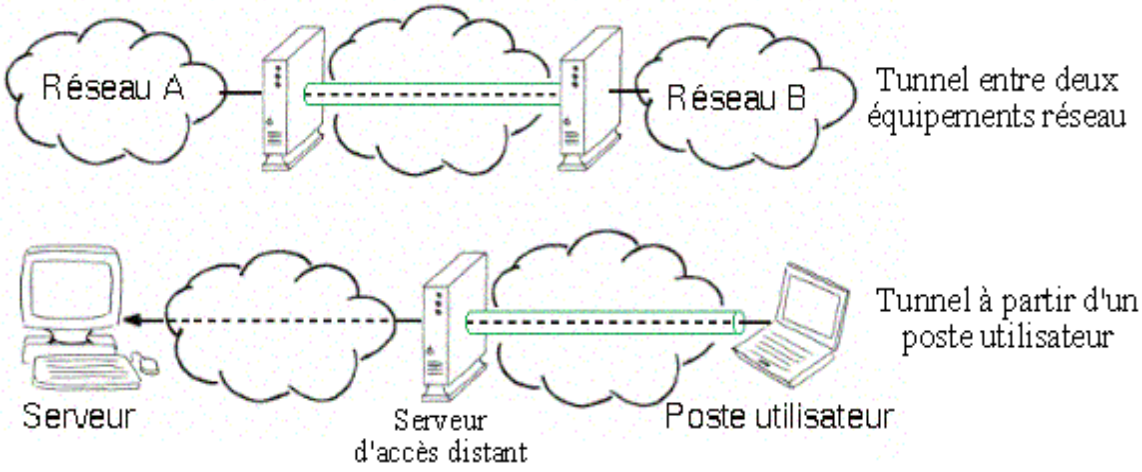

Figure II. 2: exemple de transmettre de donnée entre deux points.

2.3.4 Les exigences de base de VPN :

Pour garantir la confidentialité et l'intégrité des données lorsqu'elles transitent sur Internet, des procédures et des mécanismes de sécurité sont également utilisés pour garantir que ces données sont transférées en toute sécurité dans un environnement non sécurisé.

Les mécanismes de sécurité les plus importants pour les VPN sont:

• authentification,
• mode d'encapsulation,
• chiffrement des données,
• intégrité des paquets,
• gestion des clés,
• la non-répudiation,
• support de protocole et applications,
• gestion des adresses. [5]

2.3.4.1 Authentification :

L'authentification vérifie l'équipement d'un utilisateur ou l'identité de l'utilisateur lors de

l'établissement d'une connexion VPN dans le réseau. Il existe deux classes générales d'authentification:

- authentification de l'équipement,
- authentification de l'utilisateur. [5]

2.3.4.1.1 Authentification de l'équipement :

L'authentification de l'appareil vous permet de restreindre l'accès VPN au réseau afin de fournir des informations d'authentification à partir d'un appareil VPN distant. Une ou plusieurs clés sont configurées et utilisées pour authentifier l'identité de l'appareil. Les clés pré-partagées sont généralement utilisées dans un petit environnement VPN. 9- * Des signatures numériques ou des certificats sont utilisés pour authentifier l'appareil sur les grands déploiements VPN. [5]

2.3.4.1.2 Authentification de l'utilisateur :

De nombreuses applications VPN ajoutent une couche d'authentification supplémentaire, appelée authentification de l'utilisateur, afin de vérifier si la connexion VPN est autorisée par un utilisateur utilisant certains équipements, dans laquelle l'utilisateur doit fournir un nom d'utilisateur et un mot de passe. Ce mot de passe peut être un mot de passe statique ou un mot de passe instantané. [5]

2.3.4.2 Chiffrement des données :

Le cryptage est le processus de modification des données dans un format qui ne peut être lu que par le destinataire prévu. Pour lire le message, le destinataire des données doit disposer de la clé de déchiffrement correcte. Le cryptage des données est utilisé pour résoudre les problèmes d'écoute. Le cryptage des données se compose principalement de données utilisateur et de valeur de clé de décryptage et fonctionne via des algorithmes de chiffrement tels que DES, 3DES, AES, Blowfish, RSA, IDEA, SEAL et RC4. [5]

2.3.4.3 Intégrité d'un paquet :

En raison du potentiel de falsification de paquets ou d'usurpation de paquets, certaines applications VPN utilisent l'authentification de paquets. SHA et MD5 sont deux des fonctions de hachage les plus courantes utilisées pour vérifier l'intégrité des packages.

2.3.4.4 Gestion des clés :

Pour utiliser le cryptage, la solution VPN doit fournir une sorte de mécanisme de chif-

frement de clé pour créer la session tunnel. La solution doit générer et régénérer des clés de chiffrement pour les données chiffrées sur un accord mutuel de façon périodique afin que la sécurité et la confidentialité puissent être maintenues. [5]

2.3.4.5 La non-répudiation :

La non-répudiation ou la comptabilité est l'enregistrement de la session VPN. Cela pourrait inclure l'identité des deux dispositifs pour établir la connexion, la durée de la connexion qui a été utilisée, la quantité d'information qui a été transmise, le type d'informations traversé pendant la connexion, etc. Cela peut ensuite être utilisé pour détecter les attaques et pour l'accès à des fins de gestion, telles que la création des lignes de base et la recherche de problèmes de bande passante. [5]

2.3.4.6 L'autorisation :

L'autorisation est le processus d'octroi ou de refus de l'accès aux ressources situées dans un réseau après que l'utilisateur ait été identifié et authentifié. [5]

2.3.4.7 Gestion des adresses :

Un client VPN doit avoir une adresse sur l'intranet et s'assurer que les adresses utilisées dans l'intranet sont gardées confidentielles. Pour cela une solution commune consiste à utiliser un serveur DHCP externe ou un serveur AAA (authentification, autorisation et comptabilité) pour l'attribution d'une adresse à l'utilisateur. En outre, certaines informations pour permettre au client d'accéder aux ressources sur le réseau protégé doivent être fournies. Par exemple, les informations de routage, la résolution de nom de la source, et de la sécurité ainsi que des filtres de sécurité pour assurer la protection des données internes de toute utilisation non autorisée. [5]

2.3.5 Catégories des VPN :

On distingue deux grandes catégories de VPN:

- un VPN d'entreprise.
- un opérateur VPN.

Chacun a ses propres avantages et inconvénients et ils ne s'excluent pas mutuellement car il n'est pas rare de trouver les deux à la fois au sein d'une même entreprise. [6]

2.3.5.1 VPN d'entreprise :

Dans ce cas, l'entreprise garde le contrôle des entreprises VPN entre ses différents

points de présence ainsi qu'entre ses terminaux extérieurs à l'entreprise et les emplacements de premier choix. [6]

2.3.5.1.1 VPN site à site :

C'est l'un des cas les plus courants. Il s'agit de relier deux sites au même site d'entreprise ou d'entreprise et à un site fournisseur ou client. Mais il est également nécessaire que tout ou partie des équipements des deux réseaux puissent communiquer avec les équipements distants du réseau en utilisant les adresses privées de chaque réseau.

Généralement, ce type de VPN est mis en place en interconnectant deux éléments matériels (routeurs ou pare-feu) situés aux limites entre le réseau interne et le réseau public de chaque site. Ce sont ces appareils qui sont concernés par le cryptage, l'authentification et le routage des paquets.

Lorsqu'un matériel spécifique est utilisé, des processeurs spécialisés peuvent prendre en charge la partie du codage qui consomme le plus de ressources CPU. [6]

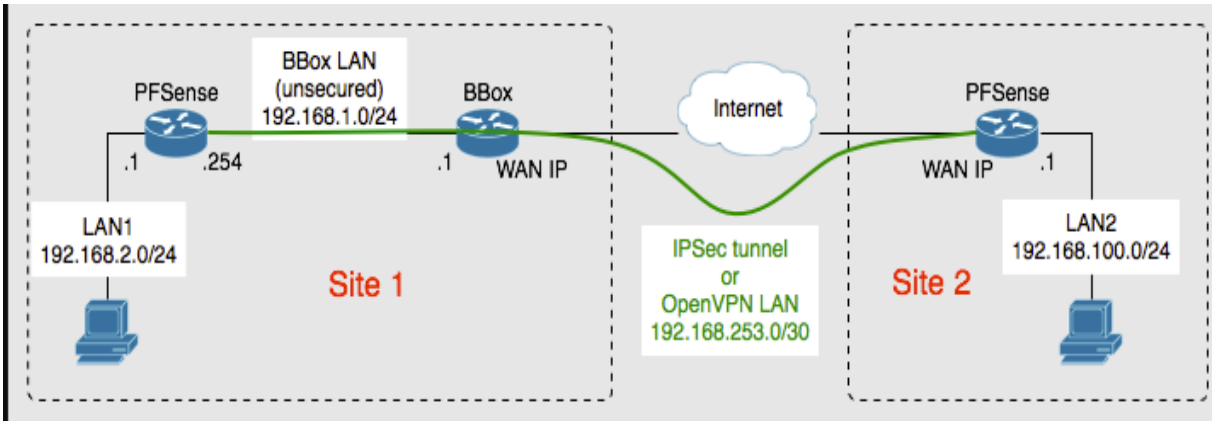

Figure II. 3 : Exemple d'un VPN site à site

Les avantages :

- Le cryptage est souvent pris en charge par des processeurs spécialisés, ce qui améliore notablement les performances.
- Une grande facilité pour le contrôle de trafic autorisé.
- Aucun impact sur les performances des poste puisque ceux-ci ne font pas de cryptage.
- La possibilité d'initier les VPN d'un côté ou de l'autre.

Les inconvénients :

- Aucune protection de données entre les postes et les firewalls puisque le tunnel n'est établi qu'entre les deux firewalls.

- L'établissement 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.

2.3.5.1.2 VPN poste à site :

C'est aussi une utilisation très populaire des VPN pour permettre aux utilisateurs distants (travailleurs à domicile ...) d'accéder aux ressources de l'entreprise via un VPN.
Afin de réaliser cette solution, un équipement (pare-feu, routeur, etc.) sera implanté sur le site central, constituant le point final de tous les VPN de ce dernier. Un logiciel qui gère le type de protocole choisi et est compatible avec les appareils du site central est installé du côté des postes de travail distants. Dans certains cas, ce programme est déjà présent dans le système d'exploitation de ces stations de travail, et dans d'autres cas, il est nécessaire d'installer ce composant logiciel. [6]

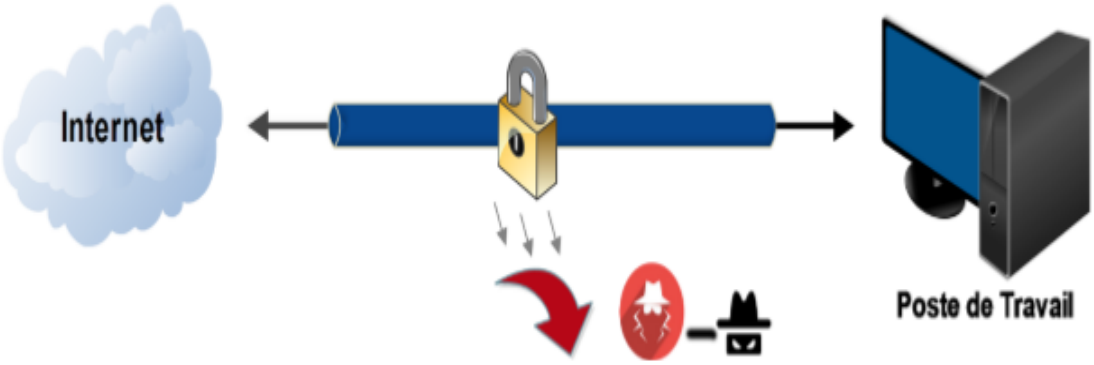

Figure II. 4 : Exemple d'un VPN poste à site

Les avantages :

- La station Nomad (mobile) est accessible depuis n'importe quel point de la planète avec un accès Internet.
- La transmission des données entre la station distante et le site central de manière sécurisée grâce à l'authentification.

Les inconvénients :

- L'installation du logiciel est généralement nécessaire sur la station distante.
- Le chiffrement impose une charge importante à la station distante, ce qui peut dégrader ses performances.
- Le chiffrement n'est pas fourni en dehors du pare-feu du site central.

2.3.5.1.3 VPN poste à poste :

L'objectif est de créer un canal sécurisé de bout en bout entre deux postes de travail, ou plus communément, entre un poste de travail et un serveur pour des raisons de confidentialité, et ainsi un VPN est créé entre eux, et toutes les données qui y sont transmises sont cryptées et compris uniquement par les paires correspondantes. Le poste de travail et le serveur peuvent être situés sur le même réseau ou sur deux réseaux différents reliés à un réseau VPN de site en site. Pour cette configuration, nous n'utilisons que des composants logiciels: le logiciel client sur le poste "demandeur" et le logiciel utilisé comme-serveur sur le poste "destinataire". [6]

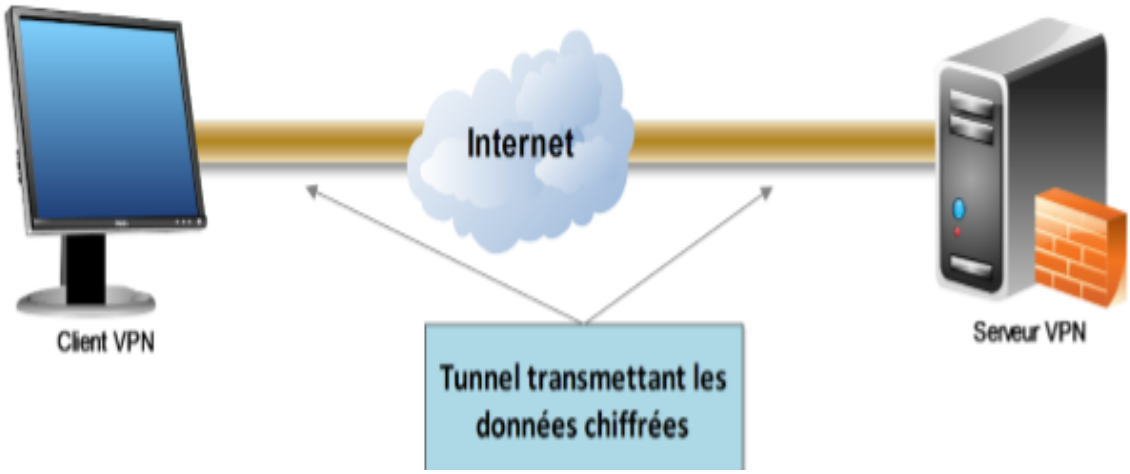

Figure II. 5: Exemple d'un VPN poste à poste.

Les avantages :

- La conversation entre les deux postes est parfaitement protégée de bout en bout. C'est donc une très bonne option pour les communications les plus sensibles.

Les inconvénients :

- Le cryptage est uniquement logiciel d'où un possible impact sur les performances en cas de fort débit, notamment quand les deux extrémités sont sur le même réseau local.
- Les matériaux mal intelligents ne sont pas accessibles.

2.3.5.2 VPN Operateur :

Lorsqu'il s'agit de relier plusieurs sites de la même entreprise avec des engagements de performance et de disponibilité, il est préférable, mais nettement plus coûteux, de contacter un opérateur qui crée ainsi un réseau privé entre tous les sites.

Ce réseau ressemble plus à un réseau de tunnel qu'à un vrai VPN, mais il est très courant de parler quand même d'un opérateur VPN car il est encore difficile, sans la com-

plicité du personnel de l'opérateur, d'intercepter les communications mutuelles entre sites. [6]

2.3.5.2.1 Caractéristiques du VPN operateur site à site :

Chaque site est connecté au POP (point de présence) le plus proche avec le support requis (ADSL, SDSL, fibre optique, etc.) et un routeur entièrement contrôlé par l'opérateur.

Créez ensuite des tunnels ou circuits spéciaux entre les différents sites au moyen des différents liens reliant leurs POP.

La technologie requise pour cela varie en fonction des progrès technologiques, et c'est ainsi que nous sommes passés des réseaux à relais de trames aux réseaux MPLS (Multiple Round Label Switching) qui deviennent de plus en plus populaires dans ce contexte. En fonction du souhait du client et des capacités techniques ou budgétaires, ce réseau particulier peut être construit avec différentes topologies.

- Tous les sites secondaires convergent vers le site central et c'est ce qui prend le relais: la technologie en hub (ou étoile).
- Tous les sites peuvent communiquer directement entre eux: un réseau entier ou un réseau entier.
- Les sites principaux peuvent communiquer entre eux et les sites secondaires doivent passer par l'un des sites principaux.
- L'opérateur supervise l'ensemble du réseau et peut personnaliser les classes de service en fonction du type de trafic, ce qui permet de prioriser des flux spécifiques.

2.3.6 Principaux protocoles :

Les principaux protocoles de tunneling sont nombreux, et il faut également noter que dans un VPN, les trames ne sont pas envoyées telles quelles, mais sont d'abord encapsulées par le protocole de tunneling, et elles sont décodées par le même protocole à l'arrivée.

Ainsi, le tunnel comprend un processus complet qui peut se résumer à l'emballage, au transport et au déroulement.

La création d'un tunnel pour transférer ces données est soumise à l'utilisation du même protocole pour les ordinateurs connectés (PPTP, SSL, IPsec, etc.).

Nous pouvons classer les protocoles que nous étudierons en trois catégories, qui sont:

- Les protocoles de niveau 2 tels que le PPTP, L2TP et L2F
- Les protocoles de niveau 3 tels que IPsec et MPLS
- Les protocoles de niveau 4 tels que SSL et SSH

Les principaux protocoles permettant de créer des VPN sont les suivants :

- **GRE (Generic Routing Encapsulation)** développé au départ par Cisco, à l'origine protocole transportant des paquets de couche 3, mais pouvant désormais aussi transporter la couche 2.
- **PPTP (Point-to-Point tunneling Protocol)** est un protocole transportant des trames de couche 2 (du PPP) développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- **L2F (Layer Two Forwarding)** est un protocole transportant des trames PPP (couche 2) développé par Cisco Systems, Nortel et Shiva. Il est désormais obsolète.
- **L2TP (Layer Two Tunneling Protocol)** est l'aboutissement des travaux de l'IETF (RFC 393110) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole transportant des sessions PPP (couche 2).
- **IPsec** est un protocole transportant des paquets (couche 3), issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. Il est associé au protocole IKE pour l'échange des clés.
- **L2TP/IPsec** est une association de ces deux protocoles (RFC 3193) pour faire passer du PPP sur L2TP sur IPsec, en vue de faciliter la configuration côté client sous Windows.
- **SSL/TLS**, déjà utilisé pour sécuriser la navigation sur le web via HTTPS, permet également l'utilisation d'un navigateur Web comme client VPN. Ce protocole est notamment utilisé par OpenVPN.
- **SSH** permet, entre autres, d'envoyer des paquets depuis un ordinateur auquel on est connecté.
- **MPLS** permet de créer des VPN distribués (VPRN) sur un nuage MPLS, de niveau 2 (L2VPN) point à point, point à multipoint (VPLS), ou de niveau 3 (L3VPN) notamment en IPv4 (VPNv4) et/ou IPv6 (VPNv6 / 6VPE), par extension et propagation de VRF (Virtual routing and forwarding – tables de routage virtuelles) sur l'ensemble du réseau MPLS.

Les protocoles de couche 2 dépendent des fonctionnalités spécifiées de PPP (Point to Point Protocol), c'est pourquoi nous allons tout d'abord rappeler le fonctionnement de ce protocole. [7]

2.3.6.1 Le protocole PPP :

PPP (Point-to-Point Protocol) est un ensemble de protocoles standard qui garantissent l'interopérabilité des programmes d'accès à distance de différents fournisseurs.

Les communications compatibles PPP peuvent se connecter à des réseaux distants via un serveur PPP standard. PPP permet également au serveur d'accès à distance de recevoir des appels entrants et d'assurer l'accès au réseau aux logiciels d'accès à distance d'autres fournisseurs, conformément aux normes PPP.

Il a l'avantage d'être supporté nativement par Windows et de nombreuses autres plates-formes, sans avoir besoin d'installer d'autres logiciels. Malheureusement, il faut l'oublier car il n'est pas considéré comme fiable. [7]

2.3.6.2 Le protocole PPTP :

Le principe PPTP est de créer des trames sous le protocole PPP et de les encapsuler dans un datagramme IP.

Un protocole développé en partie par Microsoft et qui est le protocole standard d'un VPN depuis sa création. Premier protocole VPN pris en charge par Windows, PPTP offre une bonne sécurité en tirant parti d'une variété de méthodes d'authentification, telles que MS_CHAP v2, la plus populaire du groupe.

Chaque appareil ou plate-forme prenant en charge VPN a un mode PPTP par défaut, et en raison de sa facilité de configuration, il reste le choix le plus populaire pour les fournisseurs de VPN, mais aussi pour les entreprises.

Son installation ne nécessite pas de performances techniques avancées, ce qui en fait l'un des protocoles VPN les plus rapides du marché.

Toutefois, même s'il utilise d'habitude un cryptage 128 bits, il existe quelques vulnérabilités en matière de sécurité, la plus sérieuse étant la possibilité de faille de l'authentification MS-CHAP v2.

Pour cette raison, PPTP peut être craqué en deux jours. Et bien que Microsoft ait corrigé ce bogue, il recommande toujours aux utilisateurs VPN d'utiliser SSTP ou L2TP à la place. [7]

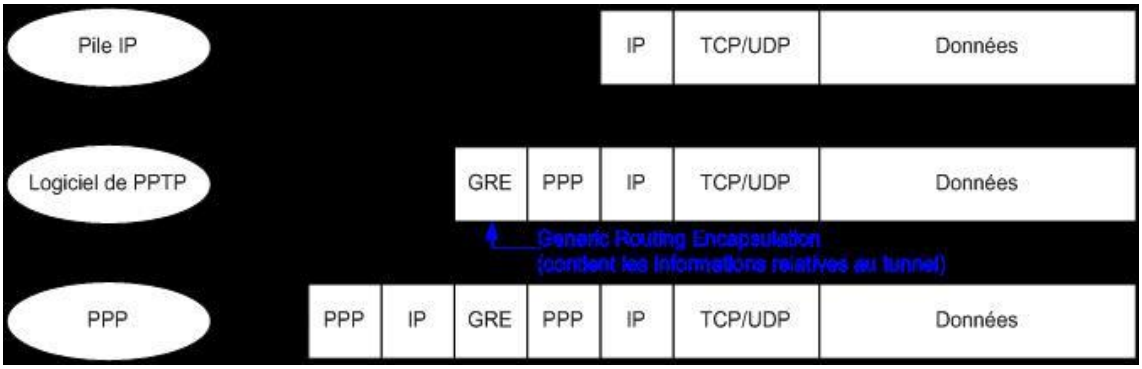

Figure II. 6: La transmission d'informations via PPTP

Avantage : formes sans avoir besoin d'installer d'autres logiciels.

Inconvénient : Il est réputé pour n'être pas fiable.

2.3.6.3 Le protocole L2F :

L2F : (Layer Two Forwarding) est un protocole de niveau 2 développe par Cisco, Northern Telecom et Shiva. IL est désormais quasi-obsolète. L2F a été spécialement conçu pour le tunnel de trafic PPP. [7]

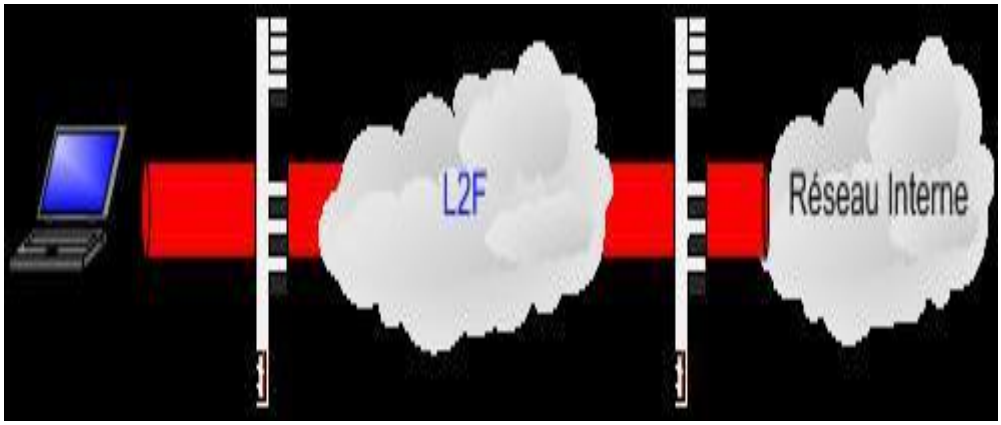

Figure II. 7: Mode de fonctionnement du protocole L2F

2.3.6.4 Le protocole L2TP :

L2TP : (Layer Two Tunneling Protocol) a été proposé pour la première fois en 1999 comme amélioration à la fois de L2F et de PPTP Sachant que L2TP ne permet pas un chiffrement ou un système d'identification robuste. Parfois bloqué par des pare-feu mais Plus sécurisé que PPTP. IL permet au trafic IP, IPX ou NetBEUI d'être encrypté et ensuite d'être envoyé à travers n'importe quel type de média qui supporte la livraison de datagramme point à point, comme IP, X.25, Frame Relay ou ATM. [7]

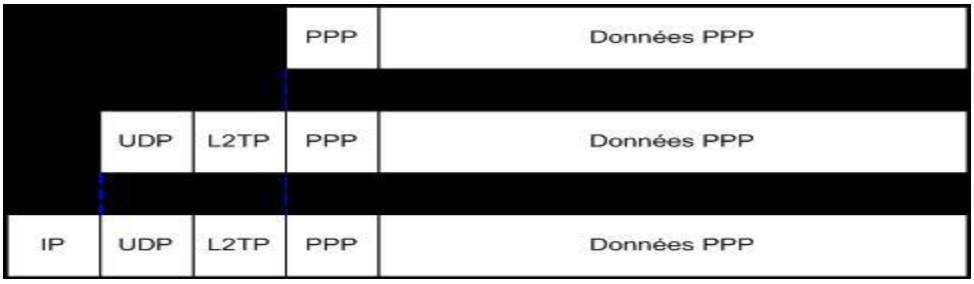

Figure II. 8: Mode de fonctionnement du protocole L2TP

2.3.6.5 Le protocole IPsec :

IPSec : est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. Il est très flexible pour une sécurité complète qui authentifie et chiffre chaque paquet individuel d'IP dans une communication donnée. Les applications d'IPsec sont multiples dans la couche Internet de la suite de protocoles Internet. [7]

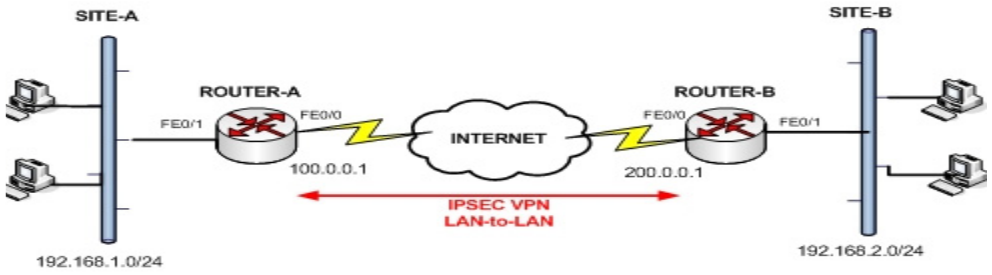

Figure II. 9: Le mode de fonctionnement du protocole IPSec

2.3.6.6 Le protocole SSL :

SSL : (Secure Socket Layer) est un protocole de niveau 4 utilise par une application pour établir un canal de communication sécurise avec une autre application. Il permet de l'authentification du serveur et du client et de chiffrement des données. [7]

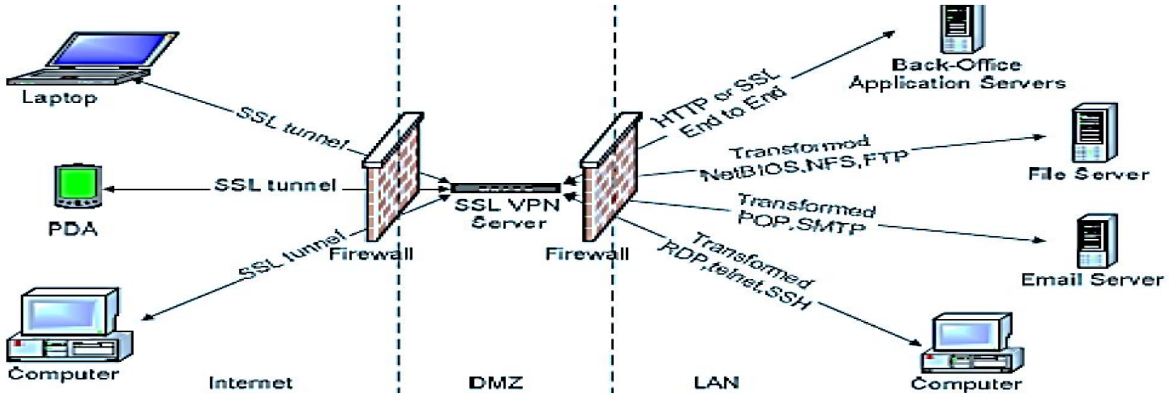

Figure II. 10 : VPN.SSL

2.3.6.7 Open VPN :

Comme son nom l'indique, OpenVPN est un protocole VPN open source qui utilisent Secure Socket Layer (SSL) pour créer une authentification pour une connexion Internet cryptée. Etablir une connexion OpenVPN peut être difficile pour les utilisateurs qui n'ont pas de compétences techniques, Le VPN le rend simple, avec notre logiciel. Dans l'ensemble, le protocole OpenVPN offre l'une des meilleures combinaisons de performance et de sécurité, et il peut être utilisé pour contourner facilement les pare-feu ainsi que les restrictions des FAI

Avantage : Hautement sécurisé et configurable. Il peut contourner facilement les pares-feux et étant open source, on peut facilement vérifier la présence de backdoors.

Inconvénients : Nécessite des logiciels tiers. [7]

2.3.7 Comparaison entre les protocoles VPNS :

Protocole	OpenVPN	PPTP	L2TP/IPsec
Chiffrement	Fort	Faible	Fort
Vitesse	Rapide	Très rapide	Lent
Ports	UDP, TCP (443)	TCP 1723, GRE	UDP 500, 50, UDP 1701, UDP 4500
Compatibilité	-Windows -macOS -Linux -Android (avec une application)	-Windows -macOS -Linux -iOS -Android -DD-WRT	-Windows -macOS -Linux -iOS -Android

Tableau II. 2: Comparaison entre les protocoles VPNS. [8]

2.3.8 Motivations pour le choix d'une solution VPN :

Il y a plusieurs raisons qui induisent à utiliser le VPN, mais le point commun à chaque raison est celui de vouloir virtualiser une partie des communications d'une organisation. Autrement dit, le besoin d'avoir une partie (ou toutes) des communications, essentiellement invisible de la part d'un observateur externe, tout en préservant les avantages d'une infrastructure commune.

La principale motivation pour choisir une solution VPN couvre les aspects économiques des communications. Les systèmes de communication d'aujourd'hui ont l'avantage d'avoir un prix Fixe et élevé avec de petits coûts variables qui changent en fonction de la capacité de transport ou de la bande passante du système.

Dans cet environnement, il est financièrement préférable de combiner un certain

nombre de communications secrètes sur une plateforme de communication de grande capacité, permettant aux prix des composants d'être éteints par un grand nombre de clients, plutôt que d'utiliser une ligne dédiée. Pour chaque appel. Par conséquent, un groupe de VPN mis en œuvre sur un support physique partagé est moins cher qu'un ensemble équivalent de petits supports séparés, chacun connecté à un client réseau.

Une autre motivation est liée au secret des communications. Les caractéristiques et l'intégrité des services de télécommunications isolés diffèrent des autres environnements qui partagent un support commun. Le niveau de confidentialité dépend de la politique de l'organisation. Si le besoin de confidentialité est faible, une simple abstraction de la discrétion peut suffire. Bien que le besoin de confidentialité soit grand, il existe un fort besoin de sécuriser l'accès et l'accès aux données via des supports partagés. [9]

2.3.9 Les avantages et les inconvénients de VPN :

Les avantages	**Les inconvénients**
*Faible coût. * Universalité, la possibilité d'accéder à partir de différentes technologies. *Augmentez la connectivité. *Échange sécurisé d'informations. *L'évolutivité est facile à améliorer. *La possibilité de former un réseau LAN qui n'est pas limité en place et en temps, car la connexion se fait via Internet. *Nous pouvons imprimer de votre domicile à bureau via Internet. * Nous pouvons transférer des données ou une vue à distance pour contrôler les ordinateurs à la maison / au bureau n'importe où. * Surfez en toute sécurité lorsque vous êtes sur un accès Internet public / hotspots.	*Une connexion internet plus lente. * Un blocage de l'accès par certains services (par exemple Netflix). * L'utilisation illégale des VPN. * Ne pas savoir si le cryptage fournit par votre VPN est fort. *La journalisation et potentiellement la revente de vos données à des tiers. *Pertes de connexion. * Un sentiment injustifié d'impunité en ligne. * VPN gratuits : parfois pire que rien du tout.

Tableau II. 3 : Les avantages et les inconvénients de VPN

2.4 Conclusion :

Les VPN ont joué un rôle important dans la protection des réseaux privés contre les cyber-attaques. Non seulement les organisations, mais aussi les particuliers et les utilisateurs à domicile accèdent souvent à internet à l'aide d'un VPN.

Chapitre III :

La mise en place des VPNs

3.1 Introduction:

Le réseau est devenu une ressource indispensable au bon fonctionnement d'une organisation, une entreprise, une université,.... ; donc les réseaux informatiques nécessitent un administrateur pour gérer tous les services et fonctions de transmission entre les réseaux. Ils ont également besoin d'un ensemble d'outils, de techniques, de méthodes et d'appareils pour protéger les informations contre le piratage et réduire l'exposition du système aux menaces accidentelles ou intentionnelles, en particulier lorsqu'ils sont connectés à Internet.

Nous allons aborder dans ce chapitre quelques concepts de base sur l'administration et la sécurité des réseaux informatiques.

3.2 Le but de l'administration d'un réseau informatique:

L'administration Réseau est le processus permettant le contrôle d'un réseau de données pour en assurer l'efficacité et la productivité. Le but Final de l'administration Réseau est d'aider à maîtriser la complexité des réseaux de données et d'assurer que les données transitent sur le réseau avec le maximum d'efficacité et de transparence aux utilisateurs.

L'administration des réseaux est couramment classée en trois activités :

- La supervision
- L'administration
- L'exploitation

3.2.1 La supervision:

La supervision consiste à surveiller les systèmes et à récupérer les informations sur leur état et leur comportement, ce qui peut être fait par interrogation périodique ou par remontée non sollicitée d'informations de la part des équipements de réseaux eux-mêmes. Le plus grand souci d'un administrateur est la panne. En effet, il doit pouvoir réagir le plus rapidement possible pour effectuer les réparations nécessaires. Il faut pouvoir surveiller de manière continu l'état des réseaux afin d'éviter un arrêt prolongé de celui-ci. La supervision doit permettre d'anticiper les problèmes et de faire remonter les informations sur l'état des équipements et des logiciels.

Plus le système est important et complexe, plus la supervision devient compliquée sans les outils adéquats. Une grande majorité des logiciels de supervision sont basés sur le protocole SNMP qui existe depuis de nombreuses années. La plupart de ces outils per-

mettent de nombreuses fonctions dont voici les principales :

- Surveiller le système d'information ;
- Visualiser l'architecture du système ;
- Analyser les problèmes ;
- Déclencher des alertes en cas de problèmes ;
- Effectuer des actions en fonction des alertes ;
- Réduire les attaques entrantes.

La tâche de l'administrateur est alors simplifiée. Il n'a plus qu'à faire une vérification ou réaliser une action en fonction d'une alerte déclenchée. [1]

3.2.2 L'administration:

L'administration désigne plus spécifiquement les opérations de contrôle du réseau avec la gestion des configurations et de sécurité. De façon générale, une administration de réseaux a pour objectif d'englober un ensemble de techniques de gestion mises en œuvre pour :

- Offrir aux utilisateurs une certaine qualité de service;
- Permettre l'évolution du système en incluant de nouvelles fonctionnalités;
- Rendre opérationnel un système ; [1]

3.2.3 L'exploitation:

De nos jours, les systèmes d'exploitation à savoir les systèmes UNIX, MacOs et Windows gèrent tous l'aspect de l'exploitation des réseaux, les procédures, et les fonctions associés. Un système d'administration réseau est une collection d'outils pour la supervision et le contrôle du réseau qui sont intégrés dans le sens qu'ils impliquent :

- Une interface opérateur unique avec un puissant, mais convivial ensemble de commandes pour exécuter toutes les tâches d'administration réseau ;
- Un nombre minimal d'équipements séparés qui sont le plus souvent des composants matériels et logiciels requis pour l'administration réseau, et incorporés dans les équipements utilisateurs existants.

Les objectifs (*les finalités*) de l'administration des réseaux pour un administrateur :

- Supervision du fonctionnement des réseaux ;
- Optimisation pour l'utilisation des ressources ;
- Détection et prévision des erreurs ;

- Signalisation des pannes ;
- Calculs de facturations à l'utilisation des ressources ;
- Le support technique pour utilisateurs.

L'administration d'un réseau suppose l'existence d'un système d'information décrivant le réseau de l'entreprise et recensant toutes les données et événements relatifs à chaque constituant du réseau administré.

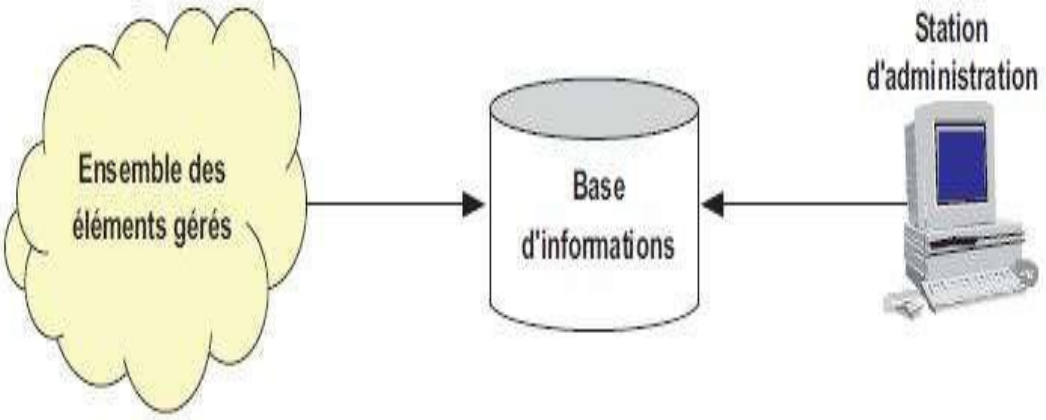

Figure III. 1: Principe générale d'un système d'administration des réseaux.

Un réseau comporte un grand nombre de composants (*objets*) que le système d'administration surveille. Dans chaque objet, un programme en tâche de fond (*Daemon*) transmet régulièrement, ou sur sollicitation, les informations relatives à son état.

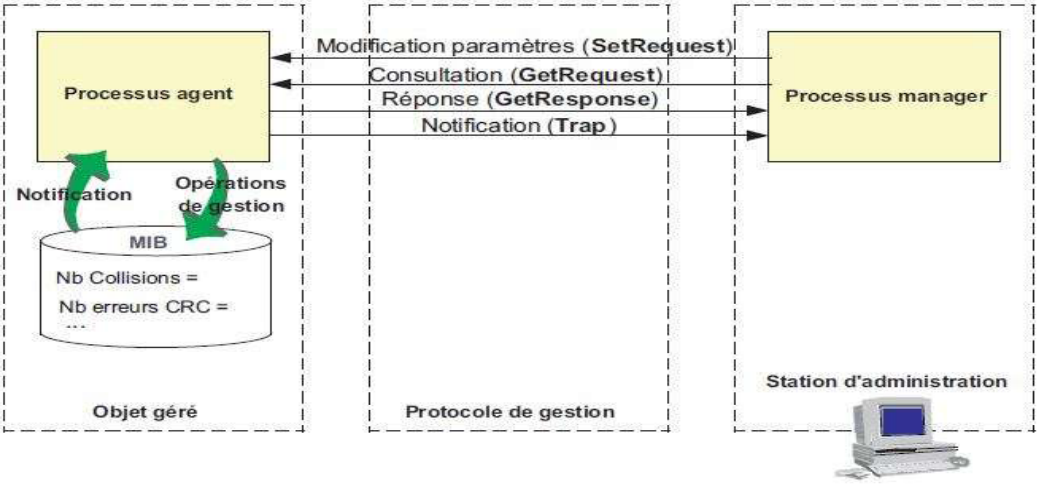

Figure III. 2: Structure fonctionnelle d'un système d'administration. [1]

3.3 Topologie de l'administration des réseaux informatiques: [1]

L'administration des réseaux informatiques peut se décomposer en trois types d'administration :

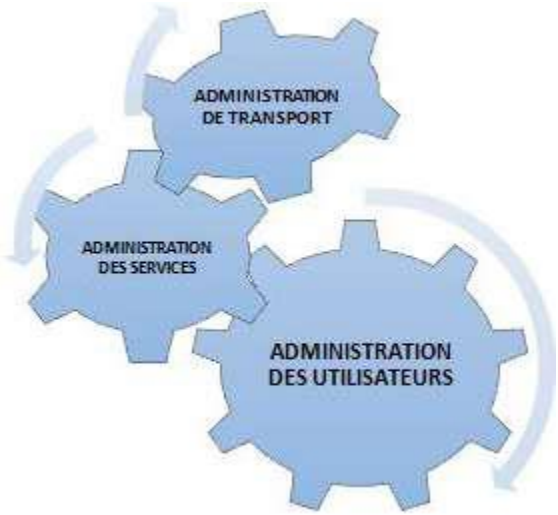

Figure III. 3: Topologie de l'administration de réseau.

3.3.1 L'administration des utilisateurs:

L'administration des utilisateurs fournit l'ensemble des mécanismes nécessaires pour une personne afin d'utiliser le réseau, à savoir :

- ***Accessibilité et Connectivité aux applications :*** l'utilisateur doit pouvoir se connecter aux différentes applications fournit par le réseau et doit disposé d'un ensemble d'outils lui assurant une certaine transparence au niveau des méthodes d'accès et connexions aux applications;
- ***L'accès aux serveurs de noms* :** afin de permettre la localisation des ressources et d'assurer à l'utilisateur l'existence et l'utilisation de ces ressources.
- ***La Confidentialité et la Sécurité :*** Le système doit fournir l'ensemble des mécanismes qui permettent de garantir la confidentialité des informations de l'utilisateur, de sécuriser son environnement et de prévenir toute perte ou altération des échanges effectués par l'utilisateur.
- ***La Qualité de service fournit à l'utilisateur* :** Il s'agit principalement de la disponilté et des performances du système et sa capacité à assurer le service attendu. [1]

3.3.2 L'administration des serveurs:

L'administration des serveurs fournit tous les mécanismes suivant : [1]

- ***La Connexion et la Distribution des applications sur tout le réseau* :** afin de permettre la relation entre les différents services;
- ***La Gestion et la Distribution des données* :** comme pour les utilisateurs, doivent garantir la fiabilité de transmission des informations et offrir des outils permet-

tant le transfert de ces informations. C'est le rôle des outils de transfert de fichiers, qui permettent le partage des capacités de stockage entre plusieurs systèmes;

- ***la Gestion des applications* :** est essentiellement lié au contrôle et à la protection des accès de ces applications par la distribution de droits, et de différents protocoles de contrôle d'utilisation de ressources concernant les applications utilisés.

3.3.3 L'administration de la machine de transport:

L'administration de la machine de transport consiste à fournir :

- ***les opérations de réseau,*** dont le rôle est de permettre l'intervention sur le fonctionnement et la modification du réseau;
- ***la liste des incidents réseaux par la mise en place de protocoles de détection et de correction*:** Lorsqu'une alerte est déclenchée, des actions vont être prises pour résoudre l'incident et de ce fait, réduire son influence et ses perturbations sur l'ensemble du réseau;
- ***les performances fournies par le réseau,*** le but est d'afficher et d'évaluer le système par un ensemble de paramètres comme le temps de réponse ou la charge du système;
- ***les coûts,*** afin de pouvoir les mesurer (dans un réseau, les coûts d'utilisation sont complexes à évaluer puisqu'ils concernent un ensemble de composants distribués);
- ***la configuration,*** le but est de déterminer la meilleure configuration du réseau afin d'améliorer les performances du système et la qualité du service;
- ***l'inventaire,*** qui a pour rôle de tenir à jour en temps réel la liste des éléments logiciels et matériels qui constituent un réseau;
- ***l'évolution et les changements,*** l'objectif est de fournir les informations permettant de déterminer les nouveaux besoins et les parties du système concernées par ces besoins de changement. [1]

3.4 Le rôle de l'administrateur réseau:

L'administrateur réseau est responsable de ce qui peut se passer dans un réseau administré ; ainsi les rôles d'un administrateur réseau consiste à :

- Mettre en place et maintenir l'infrastructure du réseau *(organisation, ...)* ;
- Installer et maintenir les services nécessaires au fonctionnement du réseau ;

- Assurer la sécurité des données internes au réseau (*particulièrement face aux attaques extérieures)* ;
- S'assurer que les utilisateurs n'outrepassent pas leurs droits ;
- Gérer les « *logins* » (*i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...)* ;
- Gérer les systèmes de fichiers partagés et les maintenir.

3.5 La sécurisation des réseaux:

Avec l'apparition des nouvelles technologies et la diversification des types de réseaux comme la multiplication des mobiles connectés et le développement des solutions de cloud computing, la gestion des solutions de sécurité réseau est devenue une tâche complexe. [2]

- **Menaces**

Voici une liste des menaces pouvant affecter la sécurité d'un réseau informatique.

- Virus
- Cheval de Troie
- Mouchards
- Attaque par déni de service
- Analyseur de paquets
- Ingénierie sociale

- **Outils**

Voici une liste des outils généralement utilisés pour gérer ces différentes menaces.

- Logiciel antivirus
- Réseau privé virtuel
- Service de vérification d'identité
- Chiffrement
- Gestion de la sécurité

3.5.1 Programme antivirus:

Logiciel permettant de détecter et de supprimer les virus informatique sur n'importe quels types de stockage (disque dur, disquette, CD-ROM…..). Pour être efficace ce type de logiciel demande une mise à jour très fréquente au cours desquelles il mémorise les nouvelles formes de virus de circulation. [3]

3.5.2 Pare-feu (firewall):

C'est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (internet).

Le pare feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- Une interface pour le réseau à protéger (réseau interne).
- Une interface pour le réseau externe.

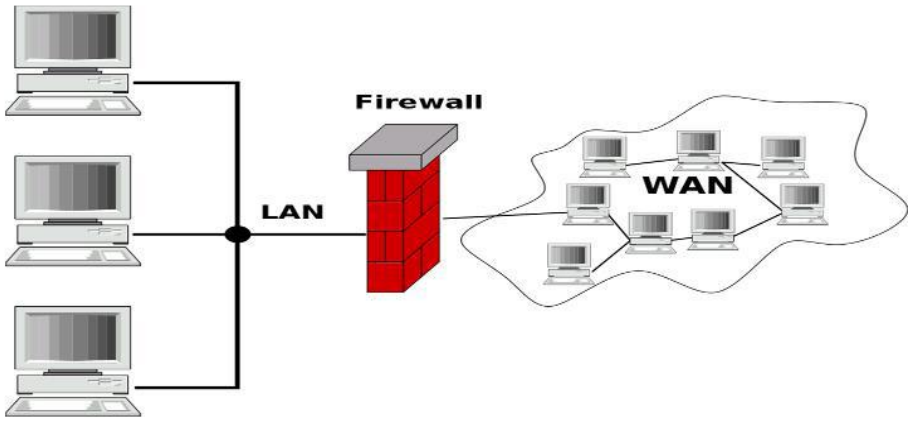

Figure III. 4: Pare-feu

Le système firewall est un système logiciel ou matériel, constituant un intermédiaire entre le réseau local (ou la machine local) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel systèmes pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic.
- Le système soit sécurisé.
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Un système pare-feu contient un ensemble de règles permettant :

- D'autoriser la connexion (allow).
- De bloquer la connexion (deny).
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en oeuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- Soit d'autoriser uniquement la communication ayant explicitement autorisées.
- Soit d'empêcher les échanges qui ont été explicitement interdites.

La première méthode est plus sure, mais elle impose toutes fois une définition précise et contraignante des besoins en communication. [3]

3.5.3 Proxy:

Un proxy est un outil de confidentialité qui peut masquer notre adresse IP et la faire apparaître comme si nous étions ailleurs. Contrairement aux VPN, nous n'avions pas besoin de télécharger de logiciel et nous nous connectons uniquement à une application spécifique, pas à l'ensemble de notre réseau.

L'objectif principal d'un proxy est de contourner des filtres, tels que les blocages de géo localisation ou ceux mis en place sur certains sites Web par les écoles, bibliothèques ou universités. Par exemple, si une bibliothèque a bloqué l'accès à un site de réseaux sociaux, nous pouvons utiliser un proxy pour y accéder. [4]

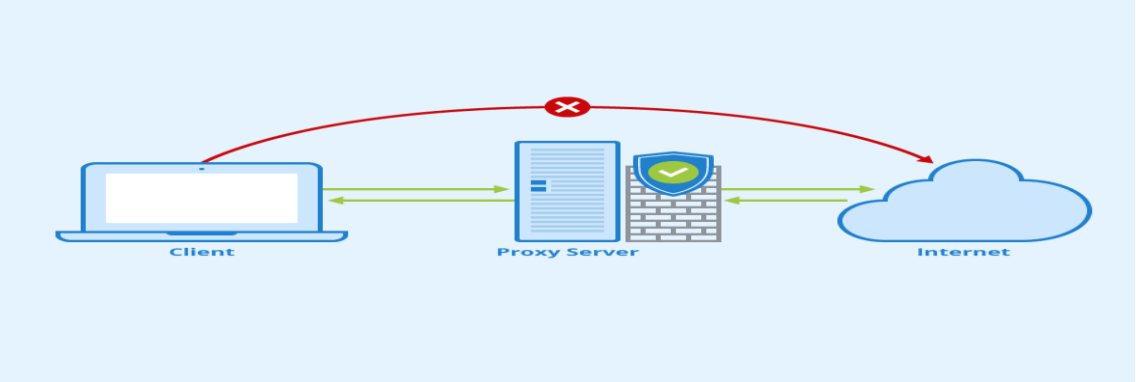

Figure III. 5: serveur Proxy

3.5.4 Routeur filtrant:

Les mécanismes de filtrage qui peuvent être associes a l'´equipement routeur autorisent des analyses de couche 3 du modèle OSI. L'examen des paquets portera ainsi sur l'entête IP, ce qui permet le blocage des adresses IP (source et destination) ainsi que l'interdiction de transmission de protocole de couche 3 ou 4 utilises (UDP , TCP . .). [5]

3.5.5 Zone démilitarisée:

Une DMZ (Demilitarized zone) est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet, derrière le pare-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (HTTP, DHCP, mails, DNS, etc.). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et, pour certains, depuis les réseaux externes. Le but est ainsi d'éviter toute connexion directe au réseau interne. [5]

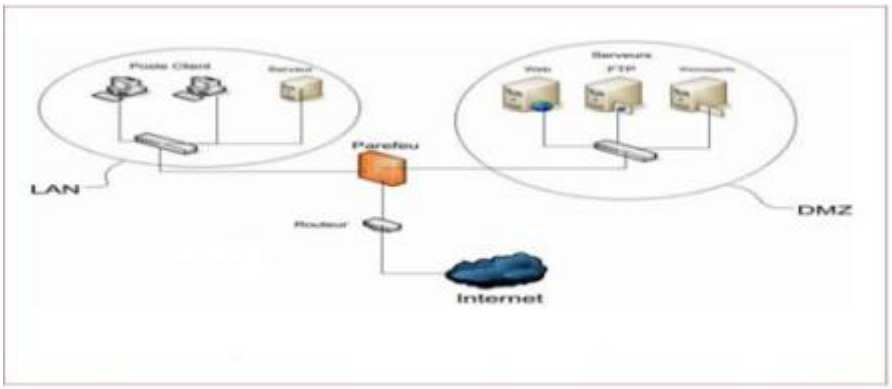

Figure III. 6: Zone Démilitarisée

3.6 Les classes d'adresses :

❖ ***L'adresse IP :*** [6]

L'Internet Protocol Address, abrégée en « adresse IP » ou tout simplement « IP », est basée sur le protocole Internet qui constitue également la base du réseau Internet. Il s'agit de l'adresse clairement identifiable d'un équipement (par ex. d'un ordinateur, d'un serveur Web, d'une imprimante) au sein d'un réseau interne ou externe. Une adresse IP peut également se référer à un ensemble d'appareils, notamment en cas de diffusion broadcast ou multicast. De même, plusieurs adresses peuvent être attribuées à un même ordinateur. Dans tous les cas, une chose est immuable : chaque adresse IP ne peut être attribuée qu'une seule fois au même moment au sein d'un réseau.

Il existe deux versions d'adresses IP de structures bien différentes. Elles ont en commun le fait d'être composées d'une partie réseau (pour l'acheminement en cas de routage IP) et d'une partie hôte (pour l'attribution à un ordinateur en particulier).

- Adresses IPv4 : les adresses du moment
- Adresses IPv6 : les adresses de l'avenir

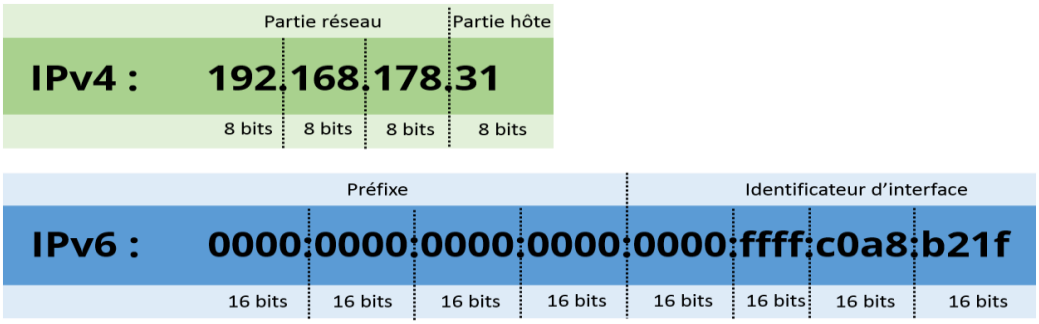

Figure III. 7 : Structure des adresses IPv4 et IPv6

❖ *Classes d'adresses IP :*

Chaque adresse IP appartient à une classe qui correspond à une plage d'adresses IP. Ces classes d'adresses sont au nombre de 5, c'est-à-dire les classes A, B, C, D et E. La présence de classes d'adresses permet d'adapter l'adresse en fonction de la taille du réseau, c'est-à-dire du besoin d'adresses IP.

Le format d'une adresse IP selon sa classe est le suivant :

Figure III. 8: Les classes d'adresse IP

❖ *Masques de sous réseaux :*

Une adresse IP est toujours associée à un "masque de sous-réseau", grâce auquel nous pouvons extraire l'adresse IP, le numéro de machine et l'adresse réseau / sous-réseau auquel elle appartient. Par défaut, en l'absence de sous-réseaux, les masques sont les suivants:

Classe	Bits de départ	Début	Fin	Notation CIDR par défaut	Masque de sous-réseau par défaut
Classe A	0	0.0.0.0	126.255.255.255[3] (127 est réservé)	/8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
Classe D (multicast)	1110	224.0.0.0	239.255.255.255		255.255.255.255
Classe E (réservée)	1111	240.0.0.0	255.255.255.255		non défini

Figure III. 9: Les classes d'adresse IP

❖ *Adresses Public / Adresses Privée :*

C'est celui qui peut être utilisé pour se connecter à Internet. Ils sont nommés par l'IANA (Internet Assigned Numbers Authority) auprès de laquelle vous devez vous inscrire. Tout ordinateur sur un réseau local qui souhaite se connecter à Internet doit avoir sa propre adresse IP.

- **Adresse publique**: L'adresse IP dite «publique» est une adresse mondiale unique attribuée à une seule entité. Par exemple, l'adresse IP: 198.133.219.25 est l'adresse du fabricant Cisco et seul Cisco a le droit de l'utiliser.
- **Adresse privée**: L'adresse IP dite "privée" est une adresse qui n'est pas universellement unique et qui peut donc être attribuée à plusieurs entités en même temps. La limitation de ceci est que l'adresse IP privée ne peut pas sortir ou simplement ne peut pas sortir sur Internet.

Classe d'adresses privées	Plage d'adresses privées
Réseau privé de classe A	De 10.0.01 à 10.255.255.254
Réseau privé de classe B	De 172.16.0.1 à 172.31.255.254
Réseau privé de classe C	De 192.168.0.1 à 192.168.255.254

Tableau III. 1: Classe et plage des adresses privée

3.6.1 Notions de base sur le routage:

Lorsque le réseau interne d'une entreprise prend de l'ampleur, il peut devenir nécessaire, pour des raisons de sécurité et d'organisation, de le diviser en plusieurs petits réseaux. Pour ce faire, on crée généralement des sous-réseaux. La création de sous-réseaux implique l'existence d'un routeur qui achemine le trafic d'un sous-réseau vers un autre.

Un routeur utilise une table de routage pour déterminer le lieu d'expédition des paquets. La table de routage contient un ensemble de routes. Chaque route décrit la passerelle ou l'interface utilisée par le routeur pour atteindre un réseau donné. Une route possède quatre composants principaux :

- le réseau de destination ;
- le masque de sous-réseau ;
- l'adresse de passerelle ou d'interface ;
- le coût de la route ou la mesure. [7]

3.6.2 Les protocoles de tunnelisation:

- Voici les principaux protocoles de tunnelisation :
- PPTP (Point-to-Point Tunneling Protocol) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.

- L2F (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète
- L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- IPSec est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

En règle générale, ces types de protocoles sont utilisés pour envoyer des données de réseau privé sur un réseau public, principalement lors de la création d'un réseau VPN, mais ils peuvent également être utilisés pour renforcer la sécurité de transmission des données chiffrées sur un réseau public. [8]

3.6.3 Les protocoles de routage:

Le but d'un protocole de routage est de fournir l'information nécessaire pour effectuer un routage, ils établissent des règles d'échange des messages d'état entre routeurs pour mettre à jours leurs tables selon des critères de coût comme, par exemple, la distance, l'état de la liaison, le débit, et ainsi améliorer l'efficacité du routage.

- ***Routing Information Protocol (RIP)*** a été conçu pour fonctionner en tant qu'IGP (Interior Gateway Protocol) dans des systèmes autonomes de taille modérée. Il utilise un algorithme d'une classe connue sous le nom d'« algorithmes à vecteurs de distance », qui recherche le plus court chemin au sens d'un critère de coût où seul le nombre de routeurs traversés intervient, un coût unitaire étant associé à la traversée de chaque réseau. Ce protocole est limité aux réseaux dont le plus long chemin implique 15 routeurs maximum. Il est mal adapté au traitement de boucles dans les chemins et utilise des métriques fixes pour comparer les routes alternatives. Cela n'est pas toujours approprié pour les situations où les routes doivent être choisies en fonction de paramètres temps réel comme un délai, une fiabilité ou une charge mesurés. [9]

- ***Open Shortest Path First (OSPF)*** est plus performant que RIP et commence donc à le remplacer petit à petit. Il s'agit d'un protocole de type protocole route-link que l'on pourrait traduire par « Protocole d'état de lien ». Contrairement à RIP, ce protocole n'envoie pas aux routeurs adjacents le nombre de sauts qui les sépare, mais l'état de la liaison qui les sépare. De cette façon, chaque routeur est

capable de dresser une carte de l'état du réseau et peut par conséquent choisir à tout moment la route la plus appropriée pour un message donné. [9]

- ***Enhanced Interior Gateway Routing Protocol (EIGRP)*** est un protocole de routage propriétaire développé par Cisco à partir de leur protocole original IGRP. De ce fait, EIGRP ne pouvait être utilisé que sur des équipements Cisco. EIGRP est un protocole de routage à vecteur de distance IP, avec une optimisation permettant de minimiser l'instabilité de routage due aussi bien au changement de topologie qu'à l'utilisation de la bande passante et la puissance du processeur du routeur. [10]

3.7 Les réseaux locaux virtuels (VLAN):

Avant d'arriver à la conception technique globale de la solution retenue, nous ferons une étude brève sur les fonctionnalités des VLANs. Celle-ci nous permettra de définir à travers ces fonctionnalités, une meilleure planification du déploiement future. [11]

3.7.1 Généralités:

Par définition, un VLAN (Virtual Local Area Network) Ethernet est un réseau local virtuel (logique) utilisant la technologie Ethernet pour regrouper les éléments du réseau (utilisateurs, périphériques, etc.) selon des critères logiques (fonction, partage de ressources, appartenance à un département, etc.), sans se heurter à des contraintes physiques (dispersion des ordinateurs, câblage informatique inapproprié, etc.). [11]

3.7.2 Avantages offerts par les Vlan:

Ce nouveau mode de segmentation des réseaux locaux modifie radicalement la manière dont les réseaux sont conçus, administrés et maintenus. La technologie de VLAN comporte ainsi de nombreux avantages et permet de nombreuses applications intéressantes. Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment :

• ***La flexibilité de segmentation du réseau*** : Les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés sans devoir prendre en considération leur localisation physique.

• ***La simplification de la gestion :*** L'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement.

• ***L'augmentation considérable des performances du réseau (réduction du domaine de collision) :*** Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du

VLAN qui lui est associé, de la bande passante est libérée, ce qui augmente les performances du réseau.

• ***Une meilleure utilisation des serveurs réseaux***.

• ***Le renforcement de la sécurité du réseau :*** Les frontières virtuelles créées par les VLANs ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcée. [11]

3.7.3 Technique et méthodes d'implantation des Vlan:

On distingue généralement trois techniques pour construire des VLAN, en fonction de leurs méthodes de travail, nous pouvons les associer à une couche particulière du modèle OSI :

- **VLAN de niveau 1 ou VLAN par port :**

On affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN.

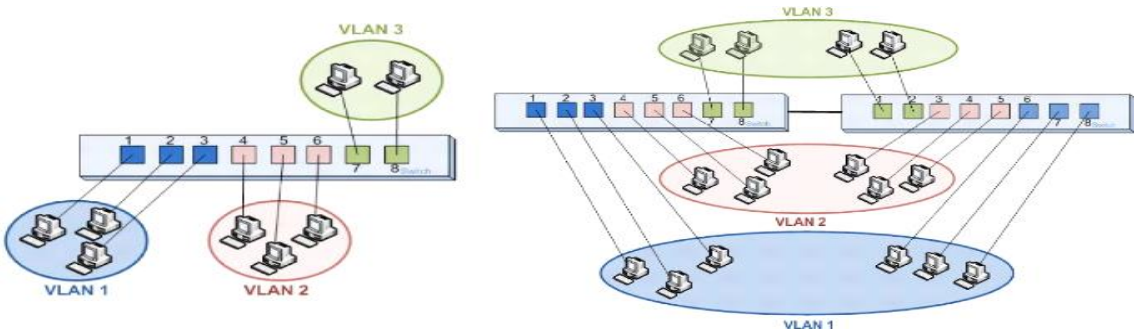

Figure III. 10: Vlan par port

- **VLAN de niveau 2 ou VLAN MAC :**

On affecte chaque adresse MAC à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminé par son adresse MAC. En faite il s'agit à partir de l'association Mac/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

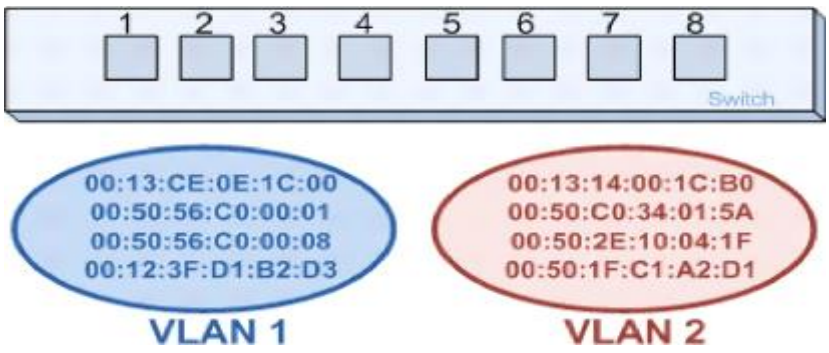

Figure III. 11: Vlan par adresse MAC

- **VLAN de niveau 3 ou VLAN d'adresses réseaux :**

On affecte un protocole de niveau 3 ou de niveau supérieur à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par le protocole de niveau 3 ou supérieur qu'elle utilise. En faite il s'agit à partir de l'association protocole/VLAN d'affecter dynamiquement les ports des commutateurs a chacun des VLAN. [12]

3.7.4 Principe du routage INTER-VLAN:

La méthode la plus basique, parfois appelée routage inter-VLAN sur plusieurs interfaces, consiste à utiliser une interface physique du routeur pour chaque VLAN. Tous les ports du commutateur sont alors placés en mode accès dans le VLAN approprié.

Chaque interface du routeur participant au routage inter-VLAN existant doit avoir une adresse IP définie dans un des sous-réseaux utilisés.

Cette approche est identique à celle adoptée pour router les informations entre deux réseaux physiques ... [13]

3.7.5 Gestion de l'adressage:

Plusieurs groupes d'adresses ont été définis dans le but d'optimiser l'acheminement (ou le routage) des paquets entre les différents réseaux. Ces groupes ont été baptisés classes d'adresses IP qui correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum.

En ce qui concerne notre projet, nous utiliserons des adresses de classe C pour la configuration des différents nœuds (poste, routeur) du réseau.

En théorie, une adresse de classe C offre la possibilité d'identifier 254 machines (sans adresses broadcast et réseau) et a un masque réseau qui est 255.255.255.0.

Pour prévoir une extensibilité future du réseau, il convient d'attribuer une adresse de cette classe à chacun des sites. Les adresses étant différentes, les différents sites ne pourront pas communiquer sans l'implémentation d'un mécanisme de routage soit par un routeur ou un commutateur multicouche (commutateur faisant le routage IP). Nous opterons pour le commutateur multicouche, étant donné qu'il est plus rapide dans le traitement en interne.

Des Switch seront utilisés à plusieurs niveaux du réseau pour permettre la segmentation et réduire le domaine de collision.

Dans la même veine, pour réduire les domaines de diffusion et pour ne permettre que les communications autorisées, des VLAN et un routage Inter-VLAN sera définis. [11]

Equipements	Login par défaut	IP dans le réseau
Routeur & Switch	192.168.1.0/24	Vlan 1
Serveur de Domaine & Hyperviseur	192.168.2.0/24	Vlan 2
Copieurs IP & Imprimantes	192.168.3.0/24	Vlan 3
Téléphone IP + Autocom VoIP	192.168.4.0/24	Vlan 4
Pointeuse Biométrique (IP)	192.168.5.0/24	Vlan 5
Camera et Serveur de Vidéosurveillance	192.168.6.0/24	Vlan 6

Tableau III. 2: donnant une répartition des Vlans et de l'adressage.

3.8 Sécurité des liaisons et de l'accès aux services: [11]

Dès lors que le réseau privé transite par internet, le problème de la sécurité se pose : les informations qu'il véhicule possèdent de la valeur et ne doivent pas être accessibles à tout le monde, l'infrastructure réseau n'y échappent pas aussi. Il convient donc de mettre en place toute une politique de sécurité pour garantir un maximum de sécurité.

3.8.1 Charte de sécurité:

Établir une charte de sécurité est une étape indispensable pour toute organisation lorsque que celle-ci souhaite faire respecter les bonnes pratiques dans le domaine de sécurité. Elle se présente sous forme d'un document court, d'une à plusieurs pages, sur lequel est décrit en grands traits la stratégie de l'organisation du point de vue sécurité de l'information et les règles de base à appliquer par tout membre.

Exemple de sections d'une charte de sécurité :

- La sécurité est l'affaire de tous.
- Chacun est responsable à son niveau de la sécurité de l'information de toute l'organisation.
- Chacun se doit d'avertir le responsable sécurité lors de la détection d'un problème de sécurité. [14]

3.8.2 Sécurité logicielle:

C'est l'ensemble des règles applicatives implémentées au niveau des nœuds pour protéger le réseau contre toutes sortes de compromissions, d'agressions venant de l'extérieur et même de l'intérieur.

- **Pare-feu et Antivirus :**

• Nous aurons à utiliser des **ACL sur le routeur en firewall** à l'entrée du réseau filtrant tout ce qui entre et tout ce qui sort du réseau (services Netbios, RPC, Telnet, NFS…).
• Mettre un pare-feu logiciel sur les serveurs de sorte à empêcher l'accès aux données confidentielles.
• Installer des programmes antivirus mis à jour régulièrement sur tous les postes.

- **Authentification :**

• Filtrage par adresse MAC des liens Radio avec Non-diffusion du SSID et Clé WPA2-PSK(AES).
• Authentification avec code d'accès pour les utilisateurs Wifi.
• Mise en place de mots de passe sur les nœuds les plus importants du réseau (serveur, routeur).

- **Autres :**

• Configurer des VLANs relatifs aux différents services à l'intérieur de chaque site dans le but de ne permettre que les communications autorisées entre ces services.
• Utiliser que des protocoles sécurisés, basés sur SSL (Secure Socket Layer) : HTTPS, SSH, IMAPS, DNSSEC, etc. [11]

3.8.3 La sécurité d'un réseau:

Comme des informations confidentielles circulent dans les réseaux, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises. Tous cherchent à se protéger contre une utilisation frauduleuse de leurs données ou contre des intrusions malveillantes dans les systèmes informatiques. Par ailleurs, une multitude de virus se propagent à l'insu des utilisateurs dans les fichiers téléchargés. Les virus sont susceptibles de détruire des documents ou même de provoquer la perte totale des informations stockées dans les machines. La tendance actuelle est de mettre en place des mécanismes de contrôle d'accès et des protocoles sécurisés qui apportent plusieurs services : l'authentification, la confidentialité, l'intégrité, la non-répudiation.

3.8.4 Définition de la sécurité informatique:

La sécurité informatique est une discipline qui se veut de protéger l'intégrité et la confidentialité des informations stockées dans un système informatique. Quoi qu'il en soit, il n'existe aucune technique capable d'assurer l'inviolabilité d'un système.

Les trois principaux objectifs la sécurité informatique:

- Confidentialité
- Intégrité
- disponibilité

3.9 Conclusion:

IPsec, semble aujourd'hui indispensable pour construire des VPN de site à site. Nous avons appris plusieurs points clés tels que:

- La technologie IP Sec 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 :

  1- elle ne permet pas de gérer la qualité de service en cœur du réseau.

  2- elle ne transporte que les datagrammes IP.

Chapitre IV :

Résultats de simulation et discussion

4.1 Introduction :

Pour faciliter le travail dans notre projet on va utiliser un logiciel qui s'appelle Cisco Packet Tracer, ce dernier fait la création, l'installation et la vérification du fonctionnement de VPN.

Nous allons voir dans ce chapitre la simulation de ces trois réseaux suivants :

1. Le premier réseau c'est pour l'installation de VPN entre trois sites (site FAC TECH/ site KHEROUBA/ site ITA);
2. Le deuxième réseau c'est pour l'installation de VPN via un réseau Cloud entre trois sites;
3. Le troisième réseau c'est pour l'installation de VPN via un réseau Cloud situé à l'extérieur de ces trois site.

4.2 Interface de logiciel cisco packet tracer :

4.2.1 Définition de Cisco Systems :

Cisco Systems est une entreprise informatique américaine spécialisée, à l'origine, dans le matériel réseau (routeurs et commutateurs Ethernet); et depuis 2009 dans les serveurs Fondé en 1984 par Leonard Bosack et Sandra Lerner, Cisco n'a pas été la première société à créer et vendre des routeurs mais Cisco créa le premier routeur multi-protocoles permettant d'interconnecter des réseaux utilisant des protocoles de communication différents. [1]

4.2.2 Packet Tracer :

4.2.2.1 Présentation et utilisation de Packet Tracer:

Packet Tracer est un logiciel développé par Cisco pour faire des plans d'infrastructure de réseau locaux en temps réel et voir toute les possibilités d'un réseau et sa future mise en œuvre. Il fournit la simulation, la visualisation, la création, l'évaluation et les capacités de collaboration et facilite l'enseignement et l'apprentissage des concepts technologiques complexes. Packet Tracer est un logiciel permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des con-

nexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles. Les machines sont configurables physiquement, via une interface GUI ou une interface CLI simulé. Les protocoles disponibles sont : HTTP, DNS, TFTP, Telnet, TCP, UDP, ainsi que le routage de base avec RIP, OSPF, EIGRP. [2]

4.2.2.2 Interface et outils :

A. **Présentation de l'écran principal** : [3]

- Une barre de menu classique.
- Une barre d'outils principale avec les fonctionnalités de base de gestion de
- fichier, d'impression, etc.….
- Pour créer votre schéma :
- On suppose qu'il n'y a pas de schéma au départ sinon cliquer sur File/New. Se placer dans l'onglet LOGICAL sous la barre d'outils principale.

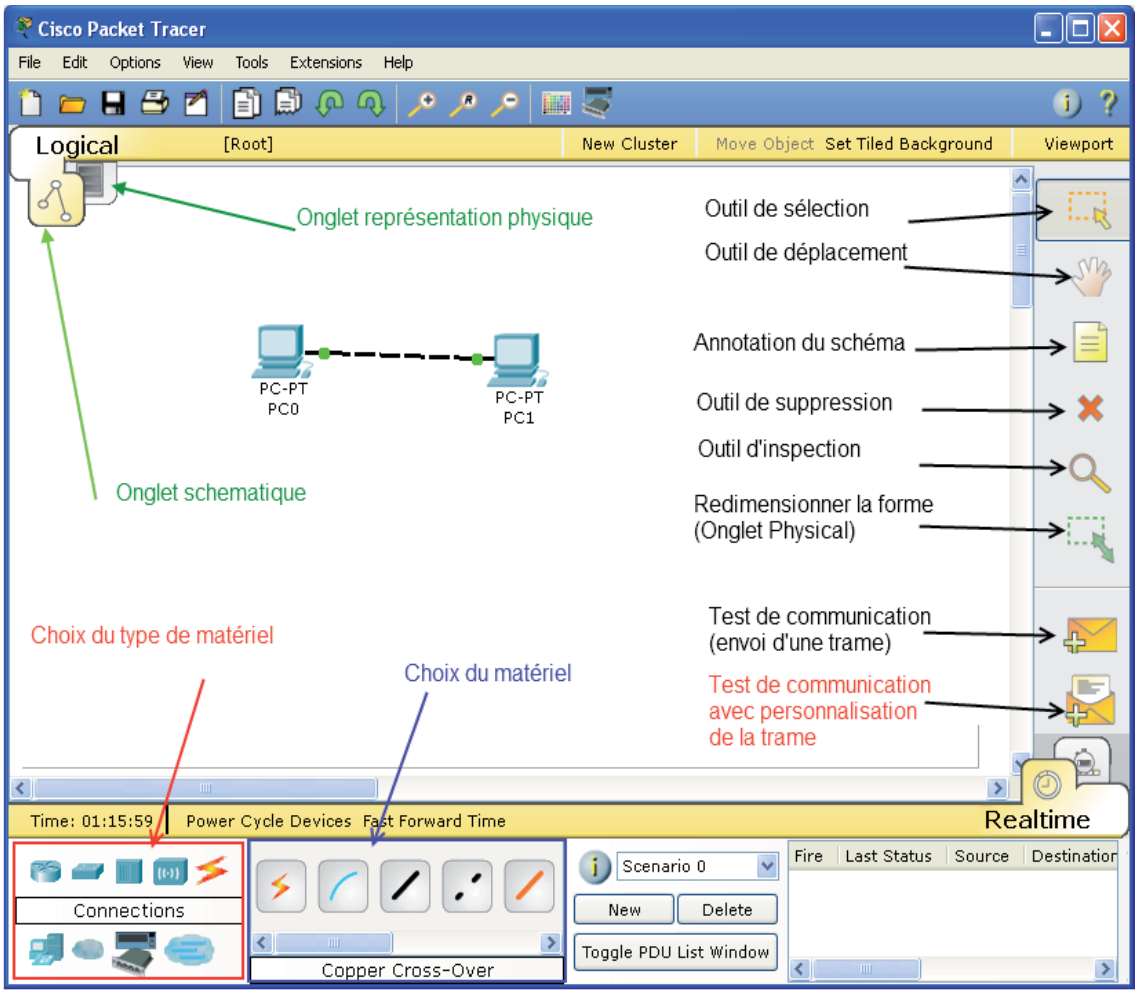

Figure IV. 1 : Présentation de l'écran principal.

B. Placement de matériels :

- Choisir le Type de matériel
- Selon le type, la liste du matériel change de manière dynamique
- Placer tout le matériel souhaité pour créer notre architecture.

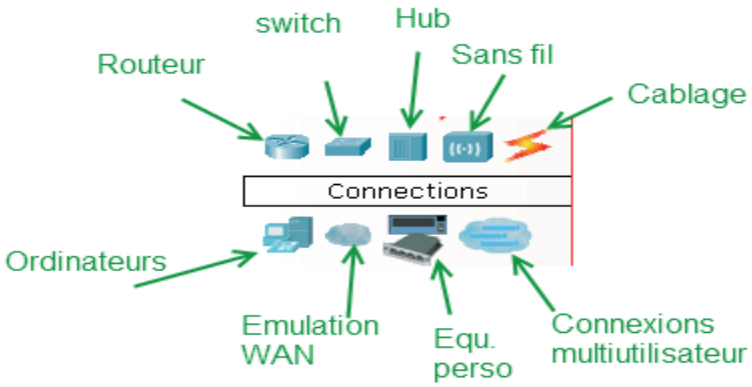

Figure IV. 2 : Types d'équipements.

C. Interconnecter les équipements :

- Choisir l'outil câblage.
- Choisir le type de connexion.
- Cliquer sur le premier équipement.
- Choisir le connecteur désiré.
- Cliquer ensuite sur le deuxième équipement et choisir le connecteur désiré.
- La connexion doit être visible sur le schéma.
- Les points de couler aux extrémités de la connexion informe de l'état de la liaison. Ils peuvent être rouges, orange ou vert.
- Il est possible de modifier le nom des éléments en double cliquant sur leur nom.
- Il est souhaitable également d'annoter le schéma (adresse IP, adresse du réseau, etc.…) avec l'outil Note

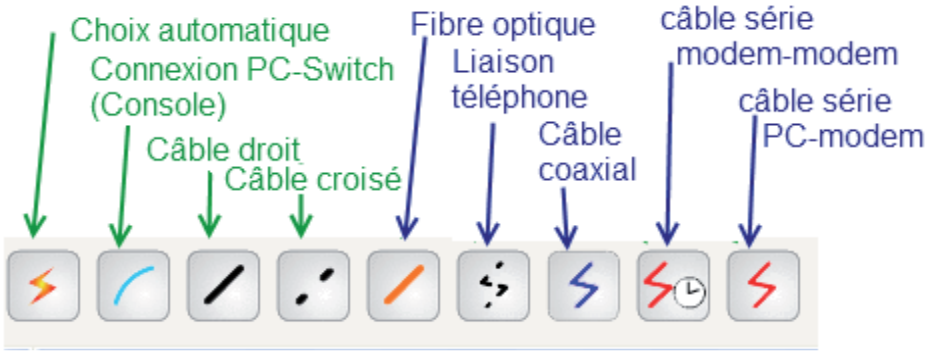

Figure IV. 3 : Les différentes connexions proposées.

4.3 La partie de simulation :

Notre thème est de créer un réseau basé sur le Cloud dans un environnement VPN IP SEC multi site .Nos sites ayant besoin d'une connexion WAN entre son siège et ses succursales basées à l'intérieur du réseau, nous allons créer une liaison avec un tunnel IPsec. [4]

4.3.1 Réseau 1 (L'installation du réseau VPN):

Le choix des matériels pour définir le graphique de notre réseau.

Notre réseau contient 3 sites :

- Le site jaune correspondant au site de KHAROUBA
- Le site vert correspondant à la faculté ITA
- Site bleu correspondant au site de la faculté FST

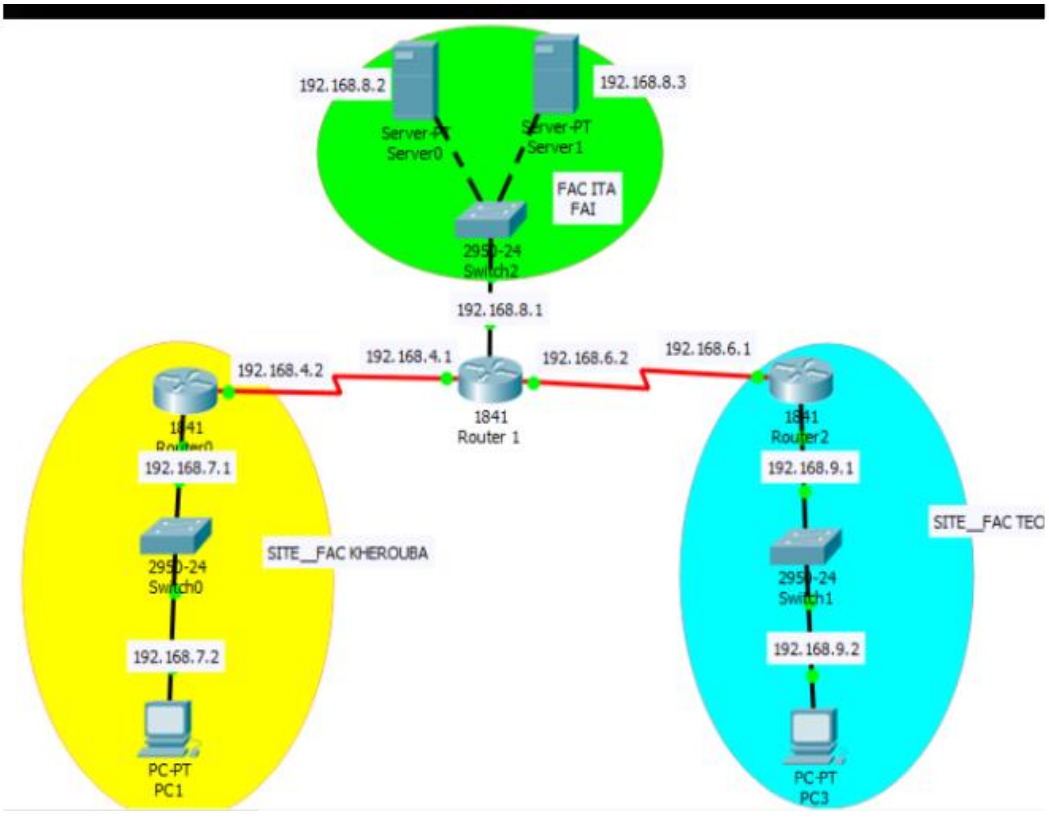

Figure IV. 4 : Schéma de réseau VPN.

- **Le tableau d'adressage :**

Sites	Device	Interface	IP Address	Subnet Mask	Default Gateway
Site1 FAC KHA-ROUBA	PC0	Fa0	192.168.7.2	255.255.255.0	192.168.7.1
	Routeur 0	Fa0/0	192.168.7.1	255.255.255.0	N/A
		S0/0/0	192.168.4.2	255.255.255.0	N/A
Site2 FAC ITA FAI	Server0	Fa0	192.168.8.2	255.255.255.0	192.168.8.1
	Server1	Fa0	192.168.8.3	255.255.255.0	192.168.8.1
	Routeur 1	Fa0/0	192.168.8.1	255.255.255.0	N/A
		Se0/0/0	192.168.4.1	255.255.255.0	N/A
		Se0/0/1	192.168.6.1	255.255.255.0	N/A
Site3 FAC TECH	PC1	Fa0	192.168.9.2	255.255.255.0	192.168.9.1
	Routeur 2	Fa0/0	192.168.9.1	255.255.255.0	N/A
		Se0/0/0	192.168.6.1	255.255.255.0	N/A

Tableau IV. 1 : tableau d'adressage du réseau 1

- **La configuration des sites :**

  a. ***La configuration des PC :***

On commence par les adresses IP de chaque ordinateur :

On tape Desktop puis l'adresse IP, le Gateway et le masque par défaut.

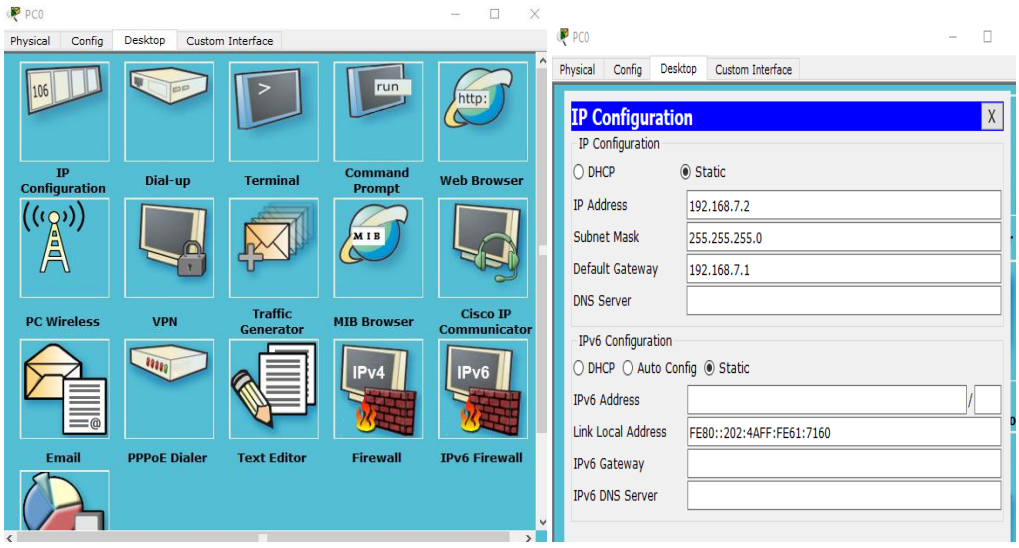

Figure IV. 5 : Configurations des PC par Desktop.

  b. ***La configuration des Switch :***

Pour nommer le Switch on utilise directement config ou par les commandes.

Figure IV. 6 : La configuration des Switch.

c. La configuration des routeurs :

Il existe deux méthodes de configuration :

- **Configuration statique :**

On active les interfaces puis on tape l'adresse correspondant à chaque interface.

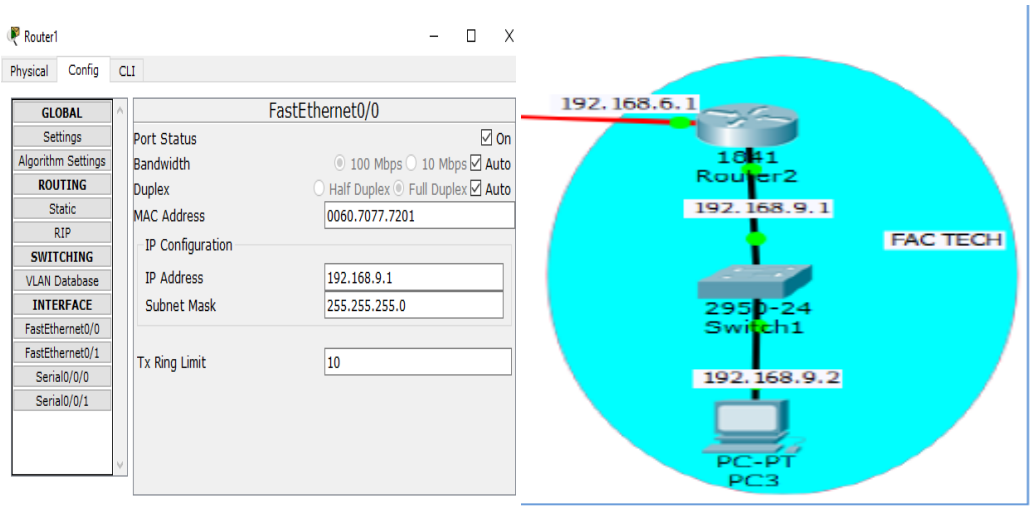

Figure IV. 7 : Configuration des router méthode statique.

- **Configuration par commande :**

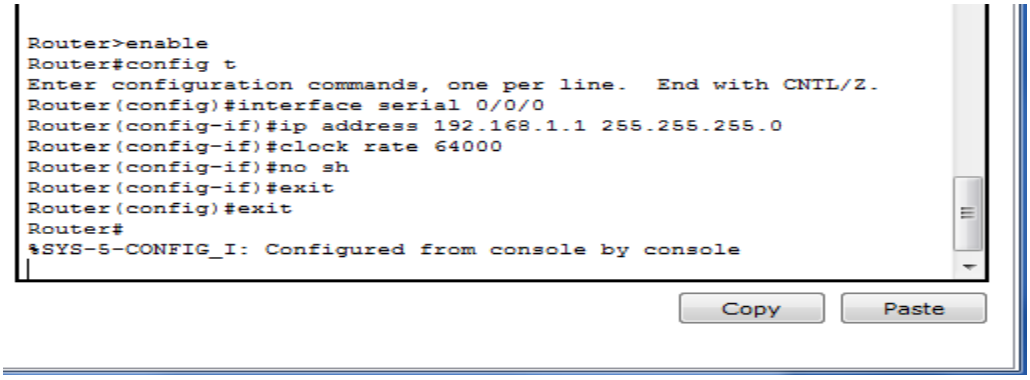

Figure IV. 8 : Configuration des router par des commandes.

d. Configuration des serveurs :

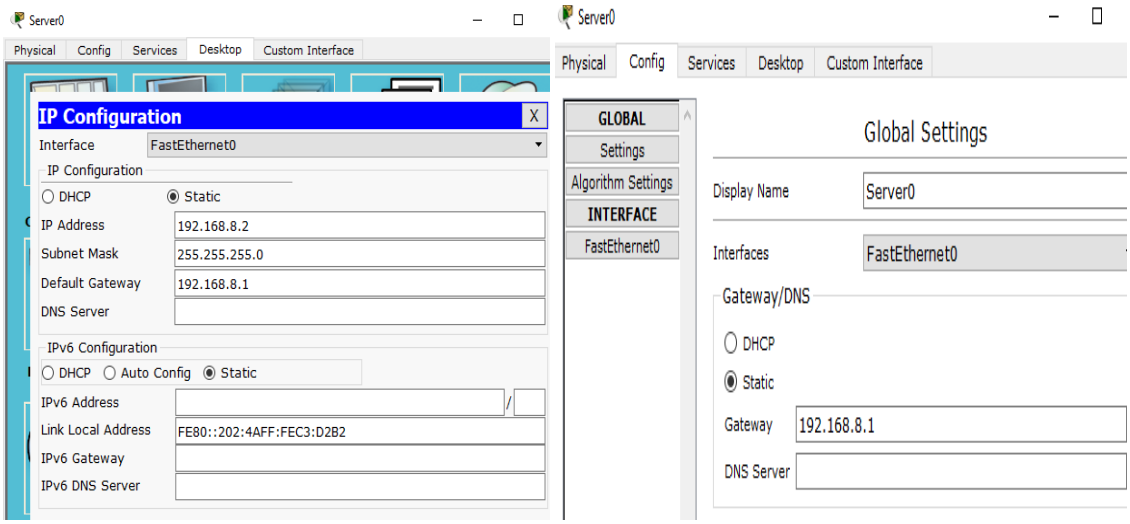

Figure IV. 9 : Configuration de server.

Après un **ping** de vérification, nous pouvons confirmer que les trois routeurs peuvent communiquer. Maintenant que le routage s'est bien passé nous allons sécuriser le réseau.

4.3.2 Mise en place d'un VPN IPSec :

La procédure de configuration comporte six étapes : [5]

• Définir la politique **ISAKMP (IKE Phase1:** Méthode de chiffrement, durée de vie, méthode d'intégrité, ce qui va permettre de définir *une IKE Security Association*).

• Créer la **clé partagée**

• Créer une **transform-set (IKE Phase2:** Nous allons configurer les politiques de sécurité IPSec «protocole esp, vérifier le type de liaison »afin d'avoir *un IPSec Security Association*).

• Mettre en place une **ACL (qui définira quel trafic peut/doit emprunter le VPN)**

• Créer un crypto **map**

• Appliquer le crypto map à l'**interface de sortie du routeur**

4.3.2.1 Configuration de base de routeur gauche :

1) Définition de la politique ISAKMP : [6]

```
Router0(config)#crypto isakmp enable          ⟹ active IKE
Router0(config)#crypto isakmp policy 1        ⟹ active une politique IKE
Router0(config-isakmp)#encryption aes         ⟹ fixe l'algorithme de cryptage
Router0(config-isakmp)#hash md5               ⟹ fixe l'algorithme de hachage
Router0(config-isakmp)#authentication pre-share ⟹ fixe la methode d'authentification
```

```
Router0(config-isakmp)#group 2          ⇒ definit le groupe Diffie Hellman
Router0(config-isakmp)#lifetime 86400   ⇒ fixe la duree de vie
Router0(config-isakmp)#exit
```

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

Crypto isakmp policy 1 : il s'agit d'une stratégie de la gestion de négociation des clés et l'établissement de la liaison VPN.

Pour ceci il faut prendre en considération les éléments suivants :

Policy : qui définit la politique de connexion pour les SA (Security Association) de ISAKMP. Un numéro indiquant la priorité de l'utilisation lui est attribué à la fin de la commande.

encryption aes - L'algorithme de cryptage AES **(Advanced Encryption Standard)** Sera utilisé **pour la confidentialité**.

hash md5 - L'algorithme de hachage md5 sera utilisé **pour l'intégrité**.

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

Groupe 2 : L'algorithme d'échange de clef Diffie-Hellman est utilisé, par defaut c'est le groupe 1 qui est utilisé (768 bits), dans notre cas nous avons utilisé le groupe 2 (1024 bits).

86400 : est la durée de vie de la clé de session (en secondes). [7]

2) **Création de la clé de partage :** [6]

```
Router0(config)#crypto isakmp key cisco@123 address 192.168.6.1 ⇒ indique la clé partagée et l'adresse du routeur pair qui doit être contacte
```

3) **Création d'une transform-set :**

```
Router0(config)#crypto ipsec transform-set vpnset esp-aes esp-md5-hmac
Router0(config)#crypto ipsec security-association lifetime seconds 3600
```

- **Crypto ipsec transform-set vpnset** Crée un ensemble de transformation appelé vpnset
- **esp-aes** – la méthode de cryptage AES et le protocole ESP IPSec seront utilisés.
- **esp-md5-hmac** - L'algorithme de hachage MD5 sera utilisé.

- **Crypto ipsec security-association lifetime seconds-** Il s'agit de la durée de vie de la clé de cryptage. [7]

4) **Configuration de la liste de contrôle d'accès étendu pour un trafic intéressant (ACL) :**

```
Router0(config)#ip access-list extended vpn-traffic
Router0(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 192.168.9.0 0.0.0.255
Router0(config-ext-nacl)#exit
```

Nous créons la crypto ACL qui est une ACL qui va identifier le trafic «intéressant» c'est-à-dire le trafic qui doit passer par le tunnel VPN (ici c'est le trafic depuis le LAN KHEROUBA vers le LAN FAC TECH, ça sera l'inverse sur l'autre routeur). Le trafic permit par cette ACL sera chiffré dans le tunnel IPSEC, le reste non…On crée donc une Access-List étendue:

Cette ACL définit le trafic qui doit passer par le tunnel VPN. Ici, le trafic en provenance du réseau 192.168.7.0 vers le réseau 192.168.9.0 sera acheminé via le tunnel VPN.

Cette ACL sera utilisé à l'étape 5 de Crypto Map. [7]

5) **Configuration de Crypto Map :**

Nous créons la crypto map qui définit le chemin qu'emprunte notre tunnel avec : La politique IPSec, l'adresse IP du routeur distant avec lequel on veut communiquer, la crypto ACL et le transform-set pour la politique IPSec. [6]

```
Router0(config)#crypto map IPSEC-VPN 10 ipsec-isakmp ⇨Crée une nouvelle carte de chiffrement avec le numéro de séquence 10.
Router0(config-crypto-map)#set peer 192.168.6.1⇨Associe l'IP destination, ici l'adresse IP publique de FAC TECH
Router0(config-crypto-map)#match address vpn-traffic⇨Associe l'ACL précédemment crée et nommé vpn-traffic.
Router0(config-crypto-map)#set transform-set vpnset⇨Ceci relie le transform-set à la configuration de la crypto map
Router0(config-crypto-map)#exit
```

6) **Application de la Crypto Map à l'interface sortante de KHEROUBA :**

La configuration de KHEROUBA est presque terminée nous devons appliquer la crypto map sur L'interface de sortie de ce routeur, dans notre cas s0/0/0. [7]

```
Router0(config)#int s0/0/0
Router0(config-if)#crypto map IPSEC-VPN
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON ⇨ Un message nous indique que la crypto map fonctionne.
```

7) Exclue le traffic VPN du NAT Overload : [6]

```
Router0(config-if)#ip access-list extended 101 ⇒le trafic intéressant sera exclu du NAT
Router0(config-ext-nacl)#deny ip 192.168.7.0 0.0.0.255 192.168.9.0 0.0.0.255
Router0(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 any
Router0(config-ext-nacl)#ip nat inside source list 101 interface S0/0/0 overload
Router0(config)#exit
```

4.3.2.2 Configuration de base de routeur droit :

La configuration est la même que pour le Routeur Siège à certaines exceptions :

- Dans l'ACL «vpn-traffic» on doit inverser l'adresse IP de l'hôte source et de l'hôte de destination
- Dans la définition du transform-set on doit changer l'adresse du peer en mettant l'adresse IP de KHEROUBA
- Dans l'ACL CRYPTOACL on doit inverser le réseau source et le réseau de destination
- Dans la crypto map on doit mettre comme adresse du peer l'adresse IP de KHEROUBA.
- Nous allons répéter les étapes de KHEROUBA à l'identique sur le routeur FAC TECH à l'exception de l'Access-List qui doit être inversé au vu de la source et de la destination. [7]

1) Définition de la politique ISAKMP :

```
Router2(config)#crypto isakmp enable
Router2(config)#crypto isakmp policy 1
Router2(config-isakmp)#encryption aes
Router2(config-isakmp)#hash md5
Router2(config-isakmp)#authentication pre-share
Router2(config-isakmp)#group 2
Router2(config-isakmp)#lifetime 86400
Router2(config-isakmp)#exit
```

2) Création de la clé de partage :

```
Router2(config)#crypto isakmp key cisco@123 address 192.168.4.2
```

3) Création d'une transform-set :

```
Router2(config)#crypto ipsec transform-set vpnset esp-aes esp-md5-hmac
Router2(config)#crypto ipsec security-association lifetime seconds 3600
```

4) **Configuration de la liste de contrôle d'accès étendu pour un trafic intéressant (ACL) :**

```
Router2(config)#ip access-list extended vpn-traffic
Router2(config-ext-nacl)#permit ip 192.168.9.0 0.0.0.255 192.168.7.0 0.0.0.255
```

5) **Configuration de Crypto Map :**

```
Router2(config-ext-nacl)#crypto map IPSEC-VPN 10 ipsec-isakmp
Router2(config-crypto-map)#set peer 192.168.4.2
Router2(config-crypto-map)#match address vpn-traffic
Router2(config-crypto-map)#set transform-set vpnset
Router2(config-crypto-map)#exit
```

6) **Application de la Crypto Map à l'interface sortante de FAC TECH :**

```
Router2(config)#int s0/0/0
Router2(config-if)#crypto map IPSEC-VPN
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

7) **Exclue le traffic VPN du NAT Overload :**

```
Router2(config-if)#ip access-list extended 101
Router2(config-ext-nacl)#deny ip 192.168.9.0 0.0.0.255 192.168.7.0 0.0.0.255
Router2(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 any
Router2(config-ext-nacl)#exit
Router2(config)#ip nat inside source list 101 interface S0/0/0 overload
```

4.3.3 Teste de l'installation de VPN :

1. Tout d'abord envoyer un message de la station PC 1 vers la station PC0
2. Sélectionner la rubrique **CLI (Command Line Interface)** de Router2
3. Nous mettons à l'emplacement ci-dessous pour écrire les lignes commandes suivantes :

Router>enable

Router # sh crypto isakmp sa

Cette commande affiche les associations de sécurité (SA) Internet Security Association Management Protocol (ISAKMP) créées entre les homologues. [8]

4. Nous aurons ce qui dessous (c'est à dire) que le VPN est installer

```
Router>enable
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.4.2     192.168.6.1     QM_IDLE           1020    0 ACTIVE
```

QM_IDLE : Signifie que le Tunnel est bien monté.

5. puis nous tapons la ligne commande suivante :

Router # sh crypto ipsec sa

Et nous aurons ce qui est dessous :

```
      inbound esp sas:
       spi: 0x0F4A022E(256508462)
         transform: esp-aes esp-md5-hmac ,
         in use settings ={Tunnel, }
         conn id: 2008, flow_id: FPGA:1, crypto map: IPSEC-VPN
         sa timing: remaining key lifetime (k/sec): (4525504/2152)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE
--More--
```

--**More—** (C'est-à-dire nous appuyions sur la touche entrer jusqu'à l'éditeur ligne command revient à sa nature).

```
      outbound esp sas:
       spi: 0x59C215CC(1505891788)
         transform: esp-aes esp-md5-hmac ,
         in use settings ={Tunnel, }
         conn id: 2009, flow_id: FPGA:1, crypto map: IPSEC-VPN
         sa timing: remaining key lifetime (k/sec): (4525504/2152)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

    Router#
```

Router#

Cela veut dire qu'on a installé le VPN dans notre réseau et il est ACTIVE.

Et on va faire la même chose pour le deuxième routeur (gauche) pour vérifier si le VPN est installé de l'autre coté.

```
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.6.1     192.168.4.2     QM_IDLE           1027    0 ACTIVE

IPv6 Crypto ISAKMP SA
```

```
      inbound esp sas:
       spi: 0x780B6254(2014011988)
         transform: esp-aes esp-md5-hmac ,
         in use settings ={Tunnel, }
         conn id: 2008, flow_id: FPGA:1, crypto map: IPSEC-VPN
         sa timing: remaining key lifetime (k/sec): (4525504/3582)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0x378963BC(931750844)
         transform: esp-aes esp-md5-hmac ,
         in use settings ={Tunnel, }
         conn id: 2009, flow_id: FPGA:1, crypto map: IPSEC-VPN
         sa timing: remaining key lifetime (k/sec): (4525504/3582)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

Router#
```

4.3.4 Réseau 2(l'installation de VPN via un réseau Cloud entre 3 sites) :

L'informatique en nuage (Cloud) :

La transformation numérique aide les entreprises à gagner rapidement en efficacité, en agilité et en connectivité, car elles utilisent la technologie pour transformer leurs processus d'affaires en quelque chose de plus facile, de plus rapide, de plus sûr, de plus flexible et de plus rentable. Pour mieux sécuriser nos réseaux, protéger les identités en nuage multiservice, la connectivité directe au nuage, les données et les applications, étendez et connectez en toute sécurité pour garantir une expérience cohérente des applications. Et aussi pour déployer, gérez et optimisez les applications dans les environnements en nuage multiservice.

La technologie de l'informatique en nuage est une pierre angulaire de la transformation numérique.

On suit ces étapes pour réaliser et configurer ce réseau :

a) Réaliser le scénario du réseau
b) configurer le réseau pour que les stations puissent se communique entre eux
c) configurer les deux Routeurs avec la configuration VPN (les lignes commandes comme nous avons fait avec le réseau précédent)
d) Vérifier si le VPN est installé dans ce type de réseau Cloud

i. Réalisation de scénario du réseau suivant :

On suit les étapes précédentes pour réaliser le scénario :

Dans ce réseau on ajoute le cloud et on placé le au milieu de la liaison tunnel VPN.

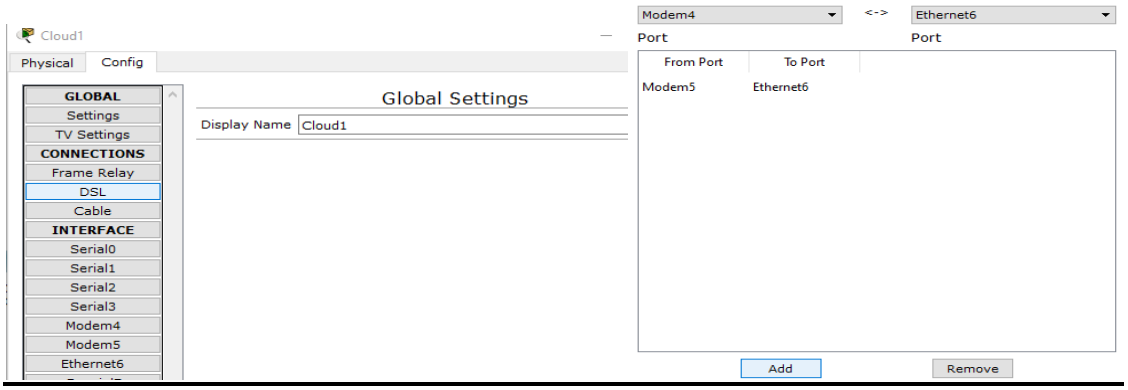

Figure IV. 10 : Configurations des CLOUD

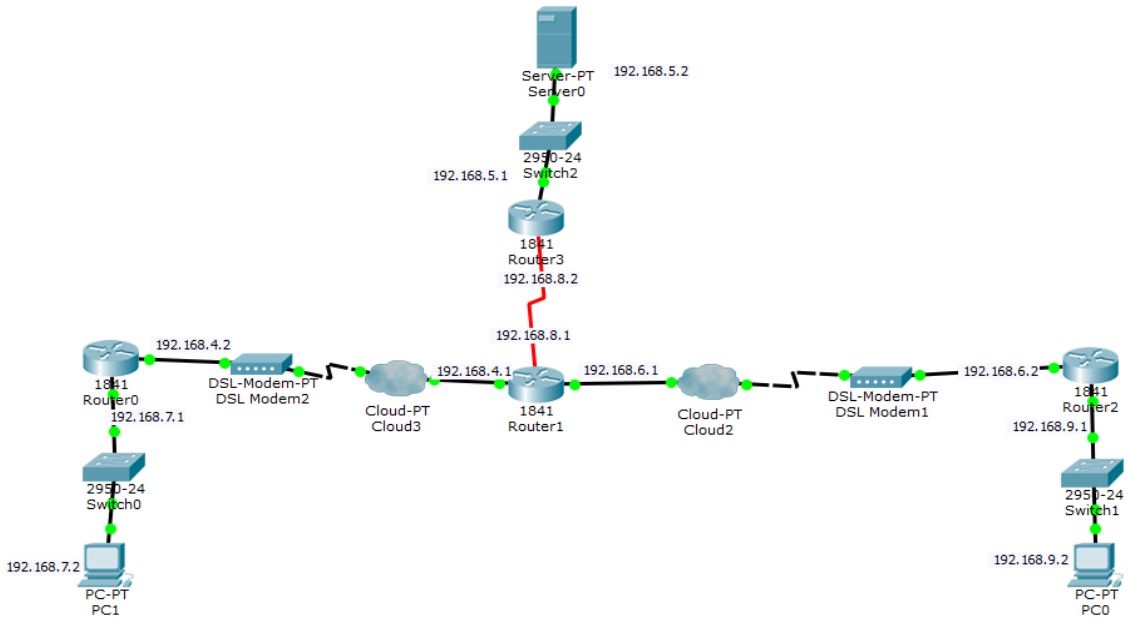

Figure IV. 11 : Installation de VPN via un réseau Cloud

- **Le tableau d'adressage :**

Sites	**Device**	**Interface**	**IP Address**	**Subnet Mask**	**Default Gateway**
Site01	PC0	Fa0	192.168.7.2	255.255.255.0	192.168.7.1
	Router0	Fa0/0	192.168.7.1	255.255.255.0	N/A
		Fa0/1	192.168.4.2	255.255.255.0	N/A
Site02	Serveur0	Fa0	192.168.5.2	255.255.255.0	192.168.5.1
	Router 3	Fa0/0	192.168.5.1	255.255.255.0	N/A
		Se0/0/0	192.168.8.2	255.255.255.0	N/A
	Router 1	Fa0/0	192.168.4.1	255.255.255.0	N/A
		Fa0/1	192.168.6.1	255.255.255.0	N/A
		Se0/0/0	192.168.8.1	255.255.255.0	N/A
Sites03	PC1	Fa0	192.168.9.2	255.255.255.0	192.168.9.1
	Router2	Fa0/0	192.168.9.1	255.255.255.0	N/A
		Fa0/1	192.168.6.2	255.255.255.0	N/A

Tableau IV. 2 : tableau d'adressage de réseau 2

Pour tester la connexion entre les sites, nous envoyons tout d'abord une **requête ping de PC0 à PC1 :**

```
PC>ping 192.168.9.2

Pinging 192.168.9.2 with 32 bytes of data:

Reply from 192.168.9.2: bytes=32 time=111ms TTL=125
Reply from 192.168.9.2: bytes=32 time=119ms TTL=125
Reply from 192.168.9.2: bytes=32 time=93ms TTL=125
Reply from 192.168.9.2: bytes=32 time=104ms TTL=125

Ping statistics for 192.168.9.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum = 119ms, Average = 106ms
```

Cela indique que les sites communiquent entre eux

ii. Configuration des deux Routeurs avec la configuration VPN (les lignes commandes) :

Configuration de routeur gauche:

On suit les étapes précédentes pour la configuration(les lignes commandes) :

```
Router(config)#crypto isakmp enable
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
```
→ Définition de la politique ISAKMP.

```
Router(config)#crypto isakmp key cisco@123 address 192.168.6.1
```
→ Création de la clé de partage

```
Router(config)#crypto ipsec transform-set vpnset esp-aes esp-md5-hmac
Router(config)#crypto ipsec security-association lifetime seconds 3600
```
→ Création d'une transform-set

```
Router(config)#ip access-list extended vpn-traffic
Router(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 192.168.9.0 0.0.0.255
Router(config-ext-nacl)#exit
```
→ Configuration de la liste de contrôle d'accès étendu pour un trafic intéressant (ACL).

```
Router(config)#crypto map IPSEC-VPN 10 ipsec-isakmp
Router(config-crypto-map)#set peer 192.168.6.1
Router(config-crypto-map)#match address vpn-traffic
Router(config-crypto-map)#set transform-set vpnset
Router(config-crypto-map)#exit
```
→ Configuration de Crypto Map.

```
Router(config)#int s0/0/0
Router(config-if)#crypto map IPSEC-VPN
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```
→ Application de la Crypto Map

```
Router(config-if)#ip access-list extended 101
Router(config-ext-nacl)#deny ip 192.168.7.0 0.0.0.255 192.168.9.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 any
Router(config-ext-nacl)#ip nat inside source list 101 interface S0/0/0 overload
```
→ Exclue le traffic VPN du NAT Overload

Le même travail pour le routeur droit :

Configuration de routeur droit :

```
Router(config)#crypto isakmp enable
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
Router(config)#crypto isakmp key cisco@123 address 192.168.4.2
Router(config)#crypto ipsec transform-set vpnset esp-aes esp-md5-hmac
Router(config)#crypto ipsec security-association lifetime seconds 3600
Router(config)#ip access-list extended vpn-traffic
Router(config-ext-nacl)#permit ip 192.168.9.0 0.0.0.255 192.168.7.0 0.0.0.255
Router(config-ext-nacl)#crypto map IPSEC-VPN 10 ipsec-isakmp
Router(config-crypto-map)#set peer 192.168.4.2
Router(config-crypto-map)#match address vpn-traffic
Router(config-crypto-map)#set transform-set vpnset
Router(config-crypto-map)#exit
Router(config)#int s0/0/0
Router(config-if)#crypto map IPSEC-VPN
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#ip access-list extended 101
Router(config-ext-nacl)#deny ip 192.168.9.0 0.0.0.255 192.168.7.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#ip nat inside source list 101 interface S0/0/0 overload
Router(config)#exit
```

iii. Vérification si le VPN est installé dans ce type de réseau Cloud :

Nous écririons les lignes commandes suivantes :

Router>enable

Router # sh crypto isakmp sa

```
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

Nous avons remarqué que le VPN n'est pas installé.

Puis on tape la commande suivante :

Router # sh crypto ipsec sa

```
Router#sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: IPSEC-VPN, local addr 0.0.0.0

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.7.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.9.0/255.255.255.0/0/0)
   current_peer 192.168.6.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 0.0.0.0, remote crypto endpt.:192.168.6.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

Router#
```

Lorsque on installe le VPN dans le réseau CLOUD qui est au milieu de la liaison tunnel VPN le VPN ne se colle pas ou bien ne reste pas activer ; mais le réseau garde sa connectivité entre les différentes stations qui se connectent entre eux.

Parce que c'est à cause de la sécurité du réseau en nuage, le réseau Cloud (réseau en nuage) lui absorbe l'installation de VPN et rendre l'installation de VPN inefficace, sache bien le réseau Cloud est complexe qui y est constitue d'un ensemble de matériels, de raccordements réseau et de logiciels fournissant des services qu'individus et collectivités peuvent exploiter depuis n'importe où dans le monde.

4.3.5 Réseau 03(l'installation de VPN via un réseau Cloud situé à l'extérieur de 3 sites) :

Maintenant on va simuler un réseau qui a de CLOUD mais de l'extérieur ou bien de son périmètre, on installant le VPN et on va voir si le VPN reste installé dans ce réseau ou bien non.

On va configurer le réseau avec les étapes suivantes :

a) Réaliser le scénario du réseau
b) Configurer le réseau pour que les stations puissent se communique entre eux
c) Installer ou bien configurer les deux Routeurs avec la configuration VPN (les lignes commandes comme nous avons fait avec les réseaux précédents)
d) Vérifier si le VPN est installé dans ce type de réseau Cloud

i. Réalisation de scénario du réseau suivant :

Nous allons maintenant mettre CLOUD en dehors du lien du tunnel VPN, comme indiqué sur la figure.

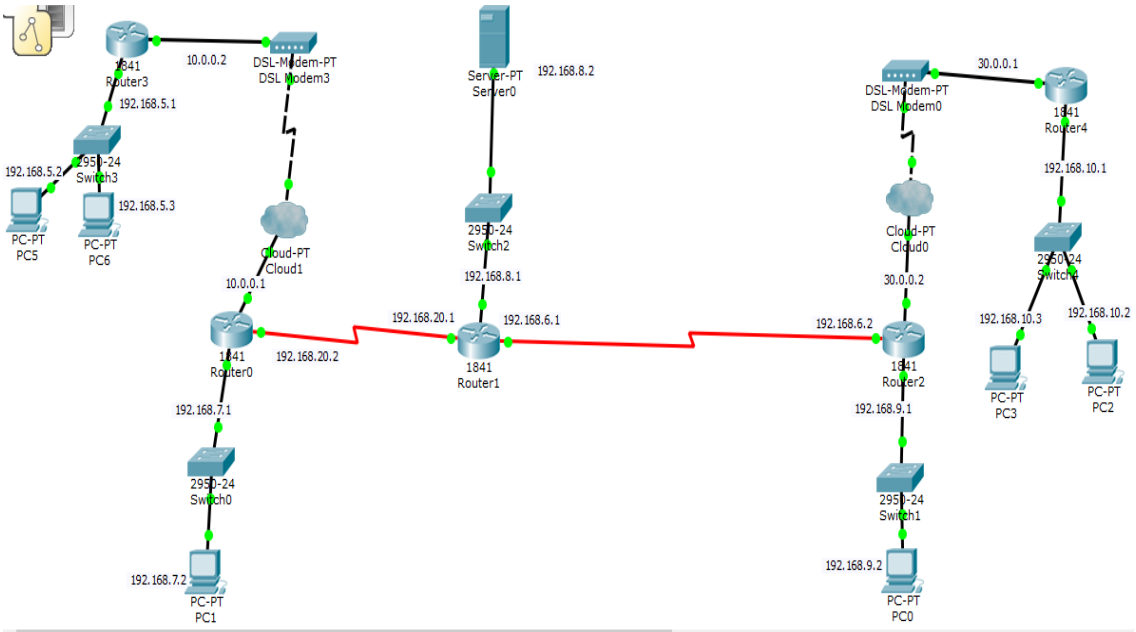

Figure IV. 12 : Installation de VPN via un réseau Cloud situé à l'extérieur de 3 sites

- **Le tableau d'adressage :**

Sites	Device	Interface	IP Address	Subnet Mask	Default Gateway
Site01	PC4	Fa0	192.168.5.2	255.255.255.0	192.168.5.1
	PC5	Fa0	192.168.5.3	255.255.255.0	192.168.5.1
	Router 3	Fa0/0	192.168.5.1	255.255.255.0	N/A
		Fa0/1	10.0.0.2	255.0.0.0	N/A
	PC0	Fa0	192.168.7.2	255.255.255.0	192.168.7.1
	Router 0	Fa0/0	192.168.5.1	255.255.255.0	N/A
		Fa0/1	10.0.0.1	255.0.0.0	N/A
		Se0/0/0	192.168.20.2	255.255.255.0	N/A
Site02	Serveur0	Fa0	192.168.8.2	255.255.255.0	192.168.8.1
	Router 1	Fa0/0	192.168.8.1	255.255.255.0	N/A
		Se0/0/0	192.168.6.1	255.255.255.0	N/A
		Se0/0/1	192.168.20.1	255.255.255.0	N/A
Site03	PC2	Fa0	192.168.10.2	255.255.255.0	192.168.10.1
	PC3	Fa0	192.168.10.3	255.255.255.0	192.168.10.1
	Router 4	Fa0/0	192.168.10.1	255.255.255.0	N/A
		Fa0/1	30.0.0.1	255.0.0.0	N/A
	PC1	Fa0	192.168.9.2	255.255.255.0	192.168.9.1
	Router 2	Fa0/0	192.168.9.1	255.255.255.0	N/A
		Fa0/1	30.0.0.2	255.0.0.0	N/A
		Se0/0/0	192.168.6.2	255.255.255.0	N/A

Tableau IV. 3 : tableau d'adressage réseau 3

Pour tester la connexion entre les sites, nous envoyons tout d'abord une **requête ping de PC0 à PC1 :**

```
PC>ping 192.168.9.2

Pinging 192.168.9.2 with 32 bytes of data:

Reply from 192.168.9.2: bytes=32 time=111ms TTL=125
Reply from 192.168.9.2: bytes=32 time=119ms TTL=125
Reply from 192.168.9.2: bytes=32 time=93ms TTL=125
Reply from 192.168.9.2: bytes=32 time=104ms TTL=125

Ping statistics for 192.168.9.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum = 119ms, Average = 106ms
```

Cela indique que les sites communiquent entre eux

ii. Configuration des deux Routeurs avec la configuration VPN (les lignes commandes) :

Configuration de routeur gauche :

```
Router(config)#crypto isakmp enable
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
Router(config)#crypto isakmp key cisco@123 address 192.168.6.2
Router(config)#crypto ipsec transform-set vpnset esp-aes esp-md5-hmac
Router(config)#crypto ipsec security-association lifetime seconds 3600
Router(config)#ip access-list extended vpn-traffic
Router(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 192.168.9.0 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#crypto map IPSEC-VPN 10 ipsec-isakmp
Router(config-crypto-map)#set peer 192.168.6.2
Router(config-crypto-map)#match address vpn-traffic
Router(config-crypto-map)#set transform-set vpnset
Router(config-crypto-map)#exit
Router(config)#int s0/0/0
Router(config-if)#crypto map IPSEC-VPN
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#ip access-list extended 101
Router(config-ext-nacl)#deny ip 192.168.7.0 0.0.0.255 192.168.9.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 any
Router(config-ext-nacl)#ip nat inside source list 101 interface S0/0/0 overload
Router(config)#exit
```

Configuration de routeur droit :

```
Router(config)#crypto isakmp enable
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
Router(config)#crypto isakmp key cisco@123 address 192.168.20.2
Router(config)#crypto ipsec transform-set vpnset esp-aes esp-md5-hmac
Router(config)#crypto ipsec security-association lifetime seconds 3600
Router(config)#ip access-list extended vpn-traffic
Router(config-ext-nacl)#permit ip 192.168.9.0 0.0.0.255 192.168.7.0 0.0.0.255
Router(config-ext-nacl)#crypto map IPSEC-VPN 10 ipsec-isakmp
Router(config-crypto-map)#set peer 192.168.20.2
Router(config-crypto-map)#match address vpn-traffic
Router(config-crypto-map)#set transform-set vpnset
Router(config-crypto-map)#exit
Router(config)#int s0/0/0
Router(config-if)#crypto map IPSEC-VPN
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#ip access-list extended 101
Router(config-ext-nacl)#deny ip 192.168.9.0 0.0.0.255 192.168.7.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#ip nat inside source list 101 interface S0/0/0 overload
Router(config)#exit
```

iii. Vérification si le VPN est installé dans ce type de réseau Cloud :

Nous écririons les lignes commandes suivantes :

Router>enable

Router # sh crypto isakmp sa

```
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.6.2     192.168.20.2    QM_IDLE           1063    0 ACTIVE

IPv6 Crypto ISAKMP SA
```

Le Tunnel est bien monté et l'installation de VPN dans notre réseau et il est ACTIVE

Puis on tape la ligne commande suivante :

Router # sh crypto ipsec sa

```
      inbound esp sas:
       spi: 0x03B87145(62419269)
         transform: esp-aes esp-md5-hmac ,
         in use settings ={Tunnel, }
         conn id: 2009, flow_id: FPGA:1, crypto map: IPSEC-VPN
         sa timing: remaining key lifetime (k/sec): (4525504/3538)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0x16B9368F(381236879)
         transform: esp-aes esp-md5-hmac ,
         in use settings ={Tunnel, }
         conn id: 2010, flow_id: FPGA:1, crypto map: IPSEC-VPN
         sa timing: remaining key lifetime (k/sec): (4525504/3538)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

Router#
```

Cela veut dire qu'on a installé le VPN dans notre réseau et il est ACTIVE

Discussion :

Le VPN maintenant est installé donc on peut dire que lorsqu'on installe le VPN via un réseau Cloud situé à l'extérieur de site le VPN reste installé dans ce réseau CLOUD

4.4 Conclusion :

La mise en place optimale d'une solution VPN, exige une connaissance suffisante en matière d'architecture informatique et de liaison d'interconnexion, tant au plan général des infrastructures réseaux qu'au niveau spécifique des télécommunications. La présente étude s'efforce d'apporter cette indispensable connaissance.

Les tunnels VPN IPsec de site à site sont utilisés pour permettre la transmission sécurisée de données, de voix et de vidéo entre deux ou plusieurs sites. Le tunnel VPN est créé sur le réseau public Internet et crypté à l'aide d'un certain nombre d'algorithmes de cryptage avancés pour assurer la confidentialité des données transmises entre les deux sites.

Dans ce chapitre, nous présentons l'interface et la performance de simulation du logiciel Cisco Packet Tracer sur lequel nous avons travaillé. Notre étude est basée sur la simulation et la discussion pour mieux appréhender la création et la configuration d'un tunnel VPN IPSec avec des commandes bien exécutées à l'aide d'un certain nombre d'algorithmes de cryptage avancés. Les résultats de la simulation obtenus confirment que le tunnel fonctionne correctement à l'absence de réseau CLOUD et est bien sécurisé car il assure la confidentialité des données transmises entre les deux sites.

Et bien sûr quand le réseau CLOUD se trouve entre la liaison tunnel VPN, ce dernier ne fonctionne pas malgré son installation c.-à-d il devient inefficace via un réseau CLOUD inclus le VPN, mais il garde la connectivité dans le réseau globale. Mais il reste à dire que la liaison tunnel VPN devient efficace et installé à condition que si le réseau CLOUD soit à l'extrémité de la liaison tunnel VPN. Par conséquence notre objectif d'étude est atteint et confirment la validité de l'étude.

Conclusion générale :

Ce projet nous a permis de mieux appréhender les problèmes liés aux réseaux locaux dont ceux relatifs au déploiement d'un réseau VPN comprenant plusieurs sites distants tout en garantissant une qualité de service.

Le développement de la technologie en général et de l'informatique en particulier a suscité un engouement pour la modernisation du traitement des systèmes d'information.

Car ces technologies ont pu se développer grâce aux performances toujours plus importantes des réseaux locaux. Mais le succès de ces systèmes d'information a fait aussi apparaître un de leur écueil.

En outre il nous a permis de nous familiariser davantage aux équipements CISCO.

Il ressort entre autres de cette présente étude qu'il y a accord entre la réflexion théorique menée et la mise en place pratique des VPN, constat qui à notre sens valide notre projet.

Toutes fois nous admettons que nos théories et nos réflexions bien qu'empiriques ne soient pas des vérités indubitables et définitives.

Elles sont susceptibles d'être réfutées par des modèles plus robustes ou par des observations postérieures divergentes qui seraient liées à l'évolution des technologies, elles-mêmes en constante mutation. C'est le propre de toute proposition intellectuelle de s'attendre à être un jour ou l'autre dépassée.

Mais elle peut tout aussi bien être plus tard renforcée par d'autres approches et mises en place.

Références bibliographiques

Chapitre I :

WEBOGRAPHIE :

[1] : https://www.commentcamarche.net/contents/508-le-concept-de-reseau#:~:text=Int%C3%A9r%C3%AAt%20d'un%20r%C3%A9seau,-Un%20ordinateur%20est&text=Un%20r%C3%A9seau%20informatique%20peut%20servir,discussion%20en%20direct%2C%20etc.)

[2]: https://cablage-informatique.com/topologie-en-bus-reseau-etoile-avantages-inconvenients/

[3] :https://web.maths.unsw.edu.au/~lafaye/CCM/initiation/topologi.htm#:~:text=La%20topologie%20logique%2C%20par%20opposition,Ethernet%2C%20Token%20Ring%20et%20FDDI.

[4] : https://spip.teluq.ca/inf1160/IMG/pdf/inf1160-notionsfondamentales.pdf

[5]: https://www.cours-gratuit.com/cours-reseau/formation-complet-sur-l-architecture-d-un-reseau-informatique

[6] : https://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre/

[7] : https://sti.ac-versailles.fr/IMG/pdf/reseau.pdf

[8] : https://fr.wikipedia.org/wiki/Protocole_informatique

[9] : https://rmdiscala.developpez.com/cours/LesChapitres.html/Cours1/Chap1.7.htm

[10] : https://fr.wikipedia.org/wiki/User_Datagram_Protocol

Chapitre II :

WEBOGRAPHIE :

[1] : TRANSPAC — WikiA3C7

[2] : http://www.letenneur.com/ho-transpac.htm

[3] : https://nordvpn.com/fr/what-is-a-vpn/

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

[5] : Microsoft Word - VPN sur les réseaux maillés sans fil_djedjiga_benzid.docx (etsmtl.ca)

[6] : http://www.univ-bejaia.dz/jspui/handle/123456789/436

[7] : https://www.coursehero.com/file/59749446/MISE-EN-PLACE-D-UN-VPN-SITE-TO-SITE-AU-Spdf/

[8] : https://lesmeilleursvpn.com/protocoles-vpn-pptp-l2tp-openvpn/

[9] : http://e-biblio.univ-mos-ta.dz/bitstream/handle/123456789/15648/M%C3%89MOIRE%20CORRIG%C3%89E%20FINALE.pdf?sequence=1&isAllowed=y

Chapitre III :
WEBOGRAPHIE :

[1]: https://hal.archives-ouvertes.fr/cel-01995184/document#:~:text=L'administration%20de%20r%C3%A9seaux%20informatique,la%20fourniture%20des%20r%C3%A9seaux%20informatiques.

[2]: http://dspace.univ-tlemcen.dz/bitstream/112/4836/1/LAHFA%2C%20NADIR.PDF.pdf

[3]:https://dl.ummto.dz/bitstream/handle/ummto/6669/RahmaniTinhinan_SadaouiFadhila.pdf?sequence=1

[4]: https://fr.wizcase.com/blog/proxy-contre-vpn-lequel-vous-convient-le-mieux-et-pourquoi/

[5]: http://www.univ-be-jaia.dz/dspace/bitstream/handle/123456789/5706/Mise%20en%20place%20d%E2%80%99une%20solution%20VPN%20sur%20pare-feu.pdf?sequence=1&isAllowed=y

[6]: https://www.it-connect.fr/les-adresses-ip-privees-et-publiques/#:~:text=-%20La%20classe%20A%20de%20l,(adresses%20priv%C3%A9es%20et%20publiques)

[7]: http://e-biblio.univ-mo-sta.dz/bitstream/handle/123456789/15648/M%C3%89MOIRE%20CORRIG%C3%89E%20FINALE.pdf?sequence=1&isAllowed=y

[8]: http://docshare01.docshare.tips/files/22567/225675317.pdf

[9]: http://biblio.univ-antananarivo.mg/pdfs/mahandrirantosoaMiharimanana_ESPA_Lic_13.pdf

[10]: https://fr.wikipedia.org/wiki/Enhanced_Interior_Gateway_Routing_Protocol

[11]: https://www.coursehero.com/file/59749446/MISE-EN-PLACE-D-UN-VPN-SITE-TO-SITE-AU-Spdf/

[12]: https://www.memoireonline.com/04/10/3431/Etude-et-optimisation-du-reseau-local-de-inova-si.html

[13]: https://www.editions-eni.fr/open/mediabook.aspx?idR=f2ea566d827e896b7a64ba97710f771c

[14]: https://www.cases.lu/knowhow/glossary/SecurityCharter_fr.html

Chapitre IV:

BIBLIOGRAPHIE :

[4] : C. Pernet. – Sécurité et espionnage informatique

WEBOGRAPHIE :

[1] : https://www.techno-science.net/definition/3741.htm

[2]: https://shms-prod.s3.amazonaws.com/media/editor/143832/Comparison_Between_Network_Simulation_Software.pdf

[3]: http://www.siloged.fr/cours/docs/manuels/doc_packettracer.pdf

[5]: http://www.mustbegeek.com/configure-site-to-site-ipsec-vpn-tunnel-in-cisco-ios-router/

[6]: https://www.coursehero.com/file/42446154/tp-vpn-ipsec-packet-tracerpdf/

[7]: http://e-biblio.univ-mo-sta.dz/bitstream/handle/123456789/15648/M%C3%89MOIRE%20CORRIG%C3%89E%20FINALE.pdf?sequence=1&isAllowed=y

[8]: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

VIDEOTHEQUE:

- Server, DSL Modem, Cloud configuration en Cisco Packet Tracer

https://youtube.com/watch?v=JumX9bXUXak&feature=share

https://youtube.com/watch?v=AFhTp2Bq6Xg&feature=share