Ministère de l'Enseignement Supérieur de la Recherche et de l'Innovation

Université Assane Seck de Ziguinchor

UFR Sciences et Technologies

Département d'Informatique

Mémoire de Fin d'études

Pour l'obtention du diplôme de Master

Mention : Informatique

Spécialité : Génie Logiciel

Sujet :

Conception et implémentation d'une architecture sécurisée d'un réseau d'entreprise sur plusieurs sites

présenté et soutenu par : **M. Serigne Mbacké DIENE**

le lundi 20/12/2021

Sous la direction de :

Youssou FAYE — Maître de Conférences à UASZ

Devant le jury composé de :

Youssou DIENG	Maître de Conférences	Président	UASZ
Youssou FAYE	Maître de Conférences	Encadreur	UASZ
Marius DASYLVA	Enseignante-Chercheur	Rapporteur	UASZ
El Hadji Malick NDOYE	Maître Assistant	Rapporteur	UASZ

Année Universitaire 2020-2021

Remerciements et Dédicaces

Je tiens tout particulièrement à remercier mon encadreur, **M. Youssou FAYE**, Professeur à l'Université Assane SECK de Ziguinchor, pour sa disponibilité, sa patience et son efficacité tout au long de ce travail. Je le remercie également de la confiance qu'il a mise en moi en me donnant ce sujet. Je vous remercie sincèrement Professeur, de m'avoir accordé votre confiance depuis le tout début et surtout pour l'atmosphère de sérénité que vous m'avez octroyée. Grâce à vous, j'ai bénéficié des conditions de travail exceptionnelles et d'un soutien constant. Merci !!! pour la patience que vous avez eue avec moi, pour le temps que vous m'avez toujours consacré et pour vos remarques qui m'ont permis d'améliorer ce document.

Je remercie tous les membres du jury d'avoir accepté de juger ce travail,

M. Youssou DIENG, Maître de Conférence à l'université Assane SECK de Ziguinchor pour le temps qu'il a bien voulu consacrer à l'appréciation de ce travail mais aussi de m'avoir honoré en présidant le jury de ma soutenance.

Mme Maruis Dasilva MENDY, Enseignante-chercheur à l'université Assane SECK de Ziguinchor, pour son ouverture mais aussi pour m'avoir fait l'honneur d'être rapporteur du jury de ma soutenance.

M. EL Hadji Malick NDOYE, Maître Assistant à l'université Assane SECK de Ziguinchor pour l'honneur qu'il m'a fait en acceptant de faire partir du jury de ma soutenance comme rapporteur.

Je remercie l'ensemble du corps professoral de l'UFR Sciences et Technologies particulièrement celui du département d'Informatique, tous mes amis du département et tous mes camarades de la promotion MPI 2015-2016 et surtout ceux de la promotion Génie Logiciel de 2019 du département au sein duquel j'ai trouvé du soutien, des conseils et un cadre de travail exceptionnel : **M. Ndiassé MBENGUE**, **M. Ass DIANE**, **M. Assane GUEYE** et **Mlle Arame GUEYE** à qui j'ai trouvé une disponibilité, une expertise technique et une gentillesse.

J'adresse un remerciement tout particulier à **M. Kéba Badiane**, compagnon de route et ami, qui a partagé toutes mes joies, mais aussi tous mes doutes, tous mes moments de fatigue, toutes mes galères tout au long de ce travail.

Je remercie tous mes confrères mourides du **DAHIRA MATLLBOUL FAWZAYNI** de l'Université Assane SECK de Ziguinchor (DMF/UASZ) et tous les membres de l'entreprise **DBE** et **B2C** pour la solidarité, l'aide et les conseils que vous m'avez toujours confiés.

Ma gratitude et mes remerciements les plus sincères vont également à **M. Bassirou DIENE**, **M. Alioune Badara DIENG** et **M. Ousmane DIALLO**, pour être les grands frères et tuteurs les plus inconditionnels, les plus exceptionnels, et bien plus encore.

Je remercie également ma famille, en particulier mes frères, sœurs, oncles, neveux, nièces, cousins et cousines, de m'avoir permis d'être ce que je suis, d'oser avoir envie, d'entreprendre et de réussir, grâce à leur soutien constant et leur affection permanente.

Enfin, mes pensées les plus émues vont, avec une tendresse et une affection sans limite, à mes mères chéries **Fatou FAYE** et **Mbacké NDIAYE**, qui donnent simplement et entièrement à ce mémoire tout son sens.

J'adresse une toute dernière pensée à tous mes amis de mon cher village natal, NGATHIE NAOUDE et ***tous ceux que j'aime et que je n'ai pas cité***.

Je dédie ce mémoire à tous ceux que j'ai déjà cités, à mon défunt père ***Ibrahima DIENE et*** à mon amie, frère et camarade ***Mamour DIOUF,*** mais aussi à toi que j'avais promis cette dédicace.

Résumé

Aujourd'hui, on assiste de plus en plus à de nouveaux types d'attaques et de menaces, et les réseaux d'entreprise doivent implémenter tous les mécanismes de sécurité pour se protéger.

La protection d'un réseau implique la protection de son architecture et de ses services. Les réseaux d'entreprise se caractérisent généralement par une infrastructure avec un grand nombre d'équipements répartis sur plusieurs sites interconnectés par un réseau généralement publique (Internet). Dans ce mémoire, notre objectif principal a été de sécuriser les infrastructures sur site, mais aussi les liaisons d'interconnexion entre sites. C'est ainsi que dans un premier temps, nous nous sommes intéressés à la configuration de l'architecture en plusieurs couches, sur lesquelles nous avons appliqué des techniques de segmentation en VLAN pour le regroupement et l'isolation des utilisateurs. Un focus sur le VLAN gestion, la sécurité des ports de switch et l'usage de protocole sécurisé (SSH) permettra un accès local et distant plus sécurisé des administrateurs. Afin de mieux contrôler l'accès aux services hébergés dans le réseau depuis l'extérieur, nous avons par la suite déployé des firewalls à des endroits stratégiques mettant ainsi en œuvre des zones démilitarisées et contrôlant les flux d'entrées/sorties à travers des règles de filtrage sur différentes couches réseau. Des mécanismes de redondance sur les équipements et liaisons seront également mis en œuvre pour assurer une haute disponibilité. Une interconnexion publique sécurisée avec des services et protocoles de sécurité permettra d'assurer la liaison entre sites. Enfin nous avons fait une implémentation sur Packet tracer qui sera plus tard suivi d'un déploiement réel et d'une couche supervision en perspective.

Table de Matières

Liste des Figures

Liste des Tableaux

Glossaire

***IP** : Internet Protocol*

***IPv4** : Internet Protocol version 4*

***IPv6** : Internet Protocol version 6*

***CIDR**: Classless Inter-Domain Routing*

***NAT**: Network Address Translation*

***FAI** : Fournisseurs d'Accès à Internet*

***RIP** : Routing Information Protocol*

***OSPF**: open Shortest Path First*

***ID**: Identificateur*

***MAC**: Media Access Control*

***WLAN**: Wireless Local Area Network*

***DHCP**: Dynamic Host Configuration Protocol*

***DNS**: Domain Name Server*

***UDP**: User Datagram Protocol*

***CPU**: Central Processing Unit*

***LAN**: Local Area Network*

***FTP** : File Transfer Protocol*

***Dos** : Denial of Service*

***DDos** : Distributed Denial of Service*

***VLAN** : Virtual Local Area Network*

***SSH**: Secure Shell*

***VPN**: Virtual Private Network*

***BNC:** Bayonet Neill–Concelman connector*

***Http**: Hypertext Transfer Protocol*

***DMZ**: demilitarized zone*

***WAN**: wide area network*

***URL**: Uniform Resource Locator*

***MITM**: man-in-the-middle*

***TCP**: Transmission Control Protocol*

***MD5**: Message Digest #5*

***SHA-1**: Secure Hash Algorithm #1*

SGBD : Système de Gestion de Base de Données

SSL : *Secure Socket Layer*

MPLS *: MultiProtocol Label Switching*

IPsec*: Internet Protocol Security*

MLS*: Multilayer Switch*

MLS1*: Multilayer Switch 1*

MLS2*: Multilayer Switch 2*

MLS3 *: Multilayer Switch 3*

MLS4 *: Multilayer Switch 4*

Introduction Générale

Aujourd'hui, on assiste de plus en plus au développement des réseaux d'entreprise qui dans certains cas se trouvent sur plusieurs sites interconnectés par des liaisons généralement publiques. Ce qui expose ces dernières à des menaces internes mais surtout externes. De jour en jour, les entreprises doivent faire face à de nouveaux types d'attaques et de menaces, et leurs réseaux doivent implémenter tous les mécanismes de sécurité pour se protéger. C'est ainsi que nous nous intéressons à la conception et au déploiement d'une infrastructure d'un réseau d'entreprise se trouvant sur plusieurs sites interconnectés par l'internet.

Au prime abord nous avons compris que la protection physique du site est la première ligne de défense pour mettre en œuvre un périmètre de sécurité, et que les pratiques actuelles montrent que la sécurité d'un réseau commence par la sécurité de son architecture ou topologie physique. Les réseaux d'entreprise se caractérisent généralement par une infrastructure avec une variété et un grand nombre d'équipements répartis sur plusieurs sites interconnectés par une réseau généralement publique (Internet). Dans ce mémoire, notre objectif principal a été de mettre en place une architecture d'un réseau d'une grande entreprise se trouvant sur des sites distants, de sécuriser l'infrastructure sur site, mais aussi d'assurer des liaisons d'interconnexion sécurisées entre sites. C'est ainsi que nous nous sommes intéressés à la configuration de l'architecture en trois couches : couche d'accès, couche distribution et couche cœur. Dans un premier temps, nous avons appliqué sur la couche d'accès des techniques de segmentation en réseaux locaux virtuels (ou VLAN : Virtual Local Area Network) pour le regroupement et l'isolation des utilisateurs mais aussi pour la fluidité du trafic. Un focus sur le VLAN de gestion, la sécurité des ports de switch et l'usage de protocole sécurisé comme SSH permettront un accès local et distant plus sécurisé des administrateurs. Afin de mieux contrôler l'accès aux services hébergés dans le réseau depuis l'extérieur, nous avons par la suite déployé sur les couches distribution et cœur des firewalls à des endroits stratégiques mettant ainsi en œuvre des zones démilitarisées et contrôlant les flux d'entrées/sorties à travers des règles de filtrage. Nous avons également mis des mécanismes de redondance sur les équipements (switchs niveau 3, firewalls, et routeurs) et sur les liaisons (etherchannel) pour assurer une haute disponibilité à travers la tolérance aux pannes. Une interconnexion publique via les réseaux privés virtuel (ou VPN : Virtual Private Network) avec des services et protocoles de sécurité permettra d'assurer une liaison sécurisée entre les sites. Par manque d'un cadre de déploiement, nous avons enfin fait une implémentation sur Packet Tracer et tester toutes les fonctionnalités et services mis en

œuvre. En perspectives, un déploiement réel et une couche supervision sont prévus pour assurer la prévention et la détection d'intrus.

Ce document est organisé en quatre chapitres :

- Chapitre 1 : Généralités sur les réseaux d'entreprises, chapitre qui nous a permis de comprendre les concepts fondamentaux, les technologies de base (équipements, topologies, communication etc..) des réseaux d'entreprise.
- Chapitre 2 : Généralités sur la sécurité, ce chapitre nous a permis de mieux mettre en exergues les risques, les vulnérabilités, les attaques et les mécanismes généraux de sécurité.
- Chapitre 3 : Sécurité des architectures réseau, dans ce chapitre, nous avons examiné les modèles d'architectures sécurisées, les différents équipements et interfaces sécurisés, les stratégies et techniques de sécurisation avant d'en concevoir une.
- Chapitre 4 : Implémentation de l'architecture sécurisée, dans ce chapitre nous avons d'abord conçu l'architecture, puis implémenté sur Packet Tracer toutes les fonctionnalités de sécurité.

Chapitre I :
Les Réseaux d'entreprise : Technologies, Architectures et Services

Introduction

Le réseau d'entreprise permet de relier les ordinateurs entre eux via un serveur qui va gérer l'accès à Internet, les e-mails, les droits d'accès aux documents partagés et le travail collaboratif. Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe et est authentifié par le serveur. En entreprise, le réseau permet à l'entreprise de centraliser ses données, les sécuriser et de travailler en équipe de manière productive. Dans ce chapitre nous allons parler en premier lieu des technologies utilisées, en deuxième lieu des architectures et en troisième lieu des services dans des réseaux d'entreprises. Avant le développement de ce chapitre nous présentons ci-après le schéma type d'un réseau d'entreprise et ses différents rôles[1].

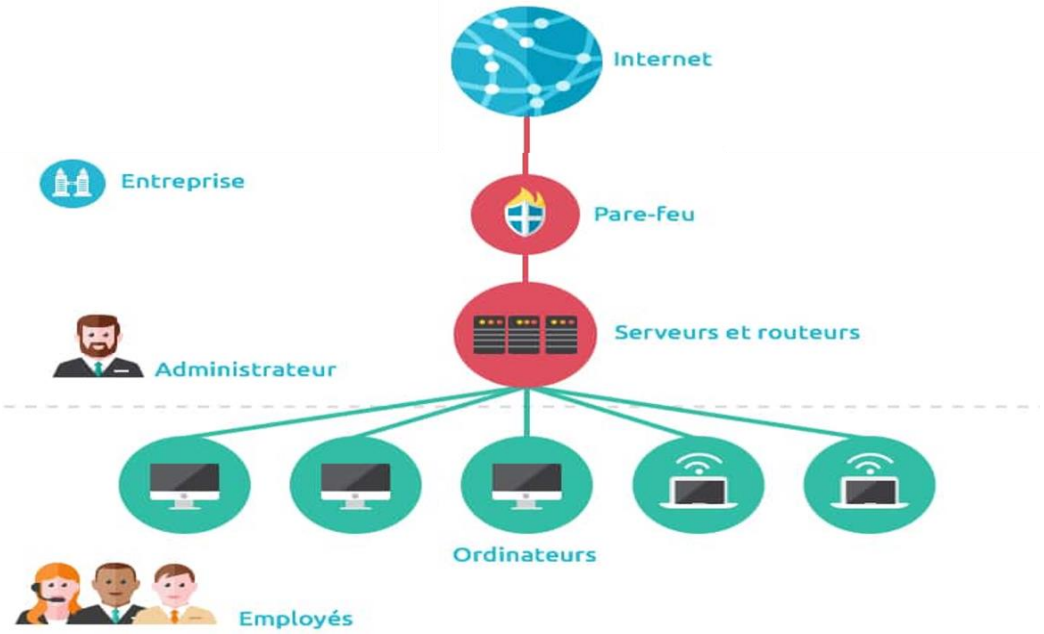

Figure 1 : Réseau d'entreprise

1.1 Les technologies utilisées

La technologie est un mot grec « Tekhnologia », le préfixe « Tekhnê » signifie « Métier ou Procédés ». Le suffixe « Logia » renvoie à « Théorie ».

Par définition, la technologie est un ensemble des connaissances théoriques et pratiques nécessaires à la conception et la fabrication des objets techniques. En informatique, la technologie facilite la communication entre les personnes et entre les pays à travers les réseaux. Dans les réseaux d'aujourd'hui, les technologies utilisées sont des supports physiques d'interconnexions et des équipements d'interconnexions. Ils permettent l'interconnexion et la communication des utilisateurs dans un réseau.

1.1.1 Les Supports physiques d'interconnexions

Le support physique d'interconnexion est un support généralement filaire, c'est-à-dire sous forme de câble permettant de relier les équipements d'un réseau comme des ordinateurs, switch, routeurs, etc. Parmi ces supports physiques utilisés dans les réseaux on peut citer le câble coaxial, le câble à paire torsadée et la fibre optique.

1.1.1.1 Câble coaxial

Le câble coaxial est largement utilisé comme moyen de transmission. Ce type de câble est constitué de deux conducteurs concentriques : un conducteur central, le cœur, entouré d'un matériau isolant de forme cylindrique, enveloppé le plus souvent d'une tresse conductrice en cuivre. L'ensemble est enrobé d'une gaine isolante en matière plastique. Il est utilisé pour les transmissions numériques en bande de base sur quelques kilomètres avec une impédance[1] caractéristique de 50 Ohm. On fait également usage de ce support pour les transmissions analogiques en mode large bande avec une impédance caractéristique de 75 Ohm. On distingue deux types supports[2]:

1.1.1.1.1 Le câble coaxial 10B5

Le câble coaxiale **10B5** est une norme Ethernet spécifiant une couche physique du modèle OSI utilisant une topologie réseau en bus, d'une longueur maximale de 500 mètres avec 100 connexions espacées de plus de 2,50 m et une vitesse de 10 Mbit/s.

Le nom scientifique donné à ce câble est **10B5** dont chaque élément a un signifiant.

- Le **10** indique le débit en Mbps (mégabits par seconde)
- Le **B** indique la façon de coder les 0 et les 1, soit ici la bande de Base
- Le **5** indique la taille maximale du réseau qui est 500, exprimé en mètre et divisé par 100

Le **10B5** est le plus ancien et le plus difficile à utiliser. Le principe est de poser le câble partout dans les salles à informatiser. Ensuite, on peut brancher des machines sur le câble, mais seulement à certains endroits. La connexion se fait à l'aide de prise vampire.

1.1.1.1.2 Le câble coaxial 10B2

Le câble coaxial 10B2 possède la même structure que le 10B5, mais en plus fin. La connectique utilisée est aussi très différente, car la propagation de l'information ne se fait pas de la même façon.

- Des câble **10B2** équipés de prises BNC

[1] L'**impédance** est une caractéristique physique d'un système physique, définie comme le rapport d'une grandeur caractérisant une excitation à laquelle il est soumis à celui d'une grandeur caractérisant sa réponse.

- Des **tés BNC** ;
- Des **bouchons**

Même si, cette connexion est plus simple et plus solide que le 10B5, tout débranchement individuel du réseau, coupe le réseau en entier, ce qui est anormale pour les réseaux d'entreprises d'aujourd'hui.

Heureusement, on a noté l'évolution des réseaux avec l'arrivé des câbles paires torsadées.

1.1.1.2 Câble paire torsadée

Celui-ci est un ancien support de transmission utilisé depuis très longtemps pour le téléphone ; il est encore largement utilisé aujourd'hui. Il n'y a pas un unique fil dans le câble mais huit, pour faire passer de l'information dans tous les sens. Le câble à paires torsadées est donc composé de huit fils, torsadés deux à deux par paire, d'où le nom qui lui est donné, la paire torsadée.

Mais pourquoi utilise-t-on les huit fils dans ce câble ?

Comme nous ne savons pas ce que l'avenir nous réserve avec l'avancé rapide de la technologie des réseaux, et peut être que demain nous voudrons faire passer plusieurs informations sur un même câble. Ces constructeurs ont pensé à mettre 8 fils (deux à deux). Ainsi, le câble à paire torsadée a été créée avec 8 fils, alors que deux seulement suffisent, pour la transmission de l'information.

Aujourd'hui, dans la plupart des d'entreprise, nous utilisons deux (2) paires, soit quatre (4) fils, car nous utilisons une paire pour envoyer les données, et une paire pour les recevoir. On utilise que quatre fils sur huit (4 fils sur 8) pour la transmission et la réception des données. Comme il existe déjà des technologies qui utilisent plus de quatre fils, les constructeurs ont eu raison de mettre huit fils dans le câble à paires torsadée.

En plus, pour une meilleure protection du signal électrique, les fils ont été torsadé. En effet, on s'est rendu compte qu'en torsadant les fils de la sorte, le câble serait moins sujet à des perturbations électromagnétiques.

Comme le **10B5**, la paire torsadée a un nom scientifique qui est **10BT** ou **100BT** ou **1000BT** selon le débit utilisé (**10Mbps, 100Mbps, 1000Mbps**), le **T** étant là pour « torsadé ». On ajoute parfois un x derrière, pour dire que le réseau est cumulé.

L'utilisation de la paire torsadée nécessite des connecteurs RJ45. Son câblage universel (informatique et téléphone), son faible coût et sa large plage d'utilisation lui permettent d'être le support physique le plus utilisé aujourd'hui.

A priori, même si cela coute encore très cher, la fibre optique est amenée à remplacer le câble à paire torsadée, notamment en raison des débits qu'elle peut offrir.

1.1.1.3 La fibre optique

Avec la fibre optique, nous transportons des 0 et des 1, non plus avec de l'électricité mais avec de la lumière. On envoie de la lumière dans le fil, et elle ressort quelques mètre/kilomètre plus loin. Son intégration dans le système de câblage est due au fait que la fibre optique résout les problèmes d'environnement grâce à son immunité aux perturbations électromagnétiques ainsi qu'à l'absence d'émission radioélectrique vers l'environnement extérieur. La fibre optique est composée d'un cylindre de verre mince : le noyau, qui est entourée d'une couche concentrique de verre : la gaine optique, et son nom scientifique est communément le **1000BF**. Du gigabit avec le **F** pour **Fibre**.

Il existe aujourd'hui globalement deux types de fibre :

- La fibre multimode **:** La fibre multimode fonctionne avec de la lumière blanche, et donc toutes les longueurs d'ondes (la lumière blanche étant la somme de toutes les lumières possibles, comme la lumière du soleil). Elle est composée d'un cœur de diamètre variant entre 50 et 62.5 microns[2]. Elle est aussi utilisée sur les réseaux locaux et sa longueur maximale est de deux kilomètres. Elle supporte de très larges bandes passantes et offre un grand débit d'environ 2.4Gbps. Cette fibre peut connecter plusieurs équipements contrairement aux autres. Mais son inconvenant est onéreux et difficile à installer.
- La fibre monomode **:** La fibre monomode fait passer une seule longueur d'onde lumineuse, soit une seule couleur. Elle fonctionne donc avec du laser qui peut être vert, bleu, rouge, …. Elle a un cœur extrêmement fin de diamètre 9 microns. Dans ce type de fibre, la transmission des données est assurée par des lasers optiques émettant des longueurs d'onde lumineuses de 1300 à 1550 nanomètres. Contraire au fibre multimode, la fibre monomode peut s'étendre sur une distance de 60 km environ. C'est celle que l'on utilise sur les liaisons à longue portée car elles peuvent soutenir les hauts débits même si son câblage est onéreux et difficile à mettre en place.

Mais la circulation des données informatiques s'effectue essentiellement par le biais de liaisons filaires. Cependant, dans certains cas la nécessité d'un autre support de communication se fait sentir. Ainsi, on peut utiliser :

- ✓ **Une liaison radio LAN** (R-LAN-WIFI) qui utilise une bande de fréquence de 2.4Ghz. Ce lien est utilisé dans des architectures en étoile et dans le concentrateur d'une antenne (borne sans fil), est connecté au réseau câblé.

[2] **Microns :** le micron (aujourd'hui dénommé micromètre) est une unité de longueur du système métrique. C'est un sous-multiple du mètre, qui est équivalent à un millionième de mètre, soit un millième de millimètre (0,001 mm)

- ✓ **Une liaison laser** : elle permet d'implémenter des liaisons point à point (interconnexion des réseaux), la distance entre les sites peut varier de 1 à 2 km sans obstacles ; les débits pouvant aller de 2 à 10 Mbits/s. Elle n'est pas soumise à des conditions météorologiques par contre le réglage de la direction des faisceaux reste problématique.

Dans un réseau d'entreprise, pour qu'il est une bonne communication entre les utilisateurs et la transmission des données dans le réseau, il faut utiliser des support physique d'interconnexion dans le réseau. A priori, même si on a des supports physiques d'interconnexion, les équipements d'interconnexion sont indispensables dans un réseau.

1.1.2 Les équipements d'interconnexion

C'est l'ensemble des matériels connectés dans un réseau d'entreprise, mais qui ne sont pas des hôtes. Leur appellation est différente selon leur niveau d'intelligence ou le rôle qu'ils jouent. Parmi ces équipements on peut citer : le répéteur, hub, pont, switch, routeur, …

1.1.2.1 Un répéteur

Un répéteur est un équipement qui permet d'étendre la portée du signal sur le support de transmission en générant un nouveau signal à partir du signal reçu. Le but de cet élément est d'augmenter la taille du réseau. Le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI), c'est-à-dire qu'il ne travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'informations. Il est transparent pour les stations de travail car il ne possède pas d'adresse Ethernet. Il offre un débit de 10 Mbits/s ; l'avantage de cet équipement est qu'il ne nécessite pas (ou très peu) d'administration. Par contre il ne diminue pas la charge du réseau, ne filtre pas les collisions, n'augmente pas la bande passante et n'offre pas de possibilité de réseau virtuel[3].

1.1.2.2 Un concentrateur ou hub

Un concentrateur est un élément matériel permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. C'est un répéteur qui transmet le signal sur plus d'un port d'entrée-sortie. Lorsqu'il reçoit un signal sur un port, il le retransmet sur tous les autres ports. Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé répéteur multiports, il est utilisé en extrémité du réseau et doit être couplé en un nombre maximum de 4 entre deux stations de travail. Il présente les mêmes inconvénients que le répéteur.

1.1.2.3 Un pont

Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Ainsi, contrairement au répéteur, qui travaille au niveau physique, le pont travaille également au niveau logique (couche 2 du modèle OSI), c'est-à-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont. Il est aussi appelé répéteur filtrant ou **bridge** en anglais. Ils transmettent des trames de données en fonction de l'adresse MAC, lisent l'adresse MAC de l'émetteur des paquets de données reçus sur les ports entrants pour découvrir les équipements de chaque segment. Les adresses MAC sont ensuite utilisées pour créer une table de commutation qui permet au point de bloquer les paquets qu'il n'est pas nécessaire de transmettre à partir du segment local.

1.1.2.4 Un commutateur ou switch

Un commutateur (en anglais switch) est un pont multiport, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI. Il relie les hôtes qui sont connectés à un port en lisant l'adresse MAC comprise dans les trames et ouvre un circuit virtuel unique entre les nœuds d'origine et de destination, ce qui va limiter la communication entre ces deux ports sans affecter le trafic des autres ports. Le switch utilise un mécanisme de filtrage et de commutation consistant à diriger les flux de données vers les machines les plus appropriées, en fonction de certains éléments présents dans les paquets de données.

A part ce commutateur de niveau 2, d'autres type de commutateurs existent.

Le switch de niveau 3, agissant au niveau de la couche transport du modèle OSI, inspecte les adresses de source et de destination des messages, dresse une table d'adresse MAC qui va lui permettre de savoir quelle machine est connectée sur quel port du switch avant d'envoyer le paquet.

Le switch de niveau 7, sont les commutateurs les plus évolués correspondant à la couche application du modèle OSI, sont capables de rediriger les données en fonction de données applicatives évoluées contenues dans les paquets de données, telles que les cookies pour le protocole HTTP, le type de fichier échangé pour le protocole FTP, …. Ainsi, un switch de niveau 7, peut par exemple permettre un équilibrage de charge en dirigeant les flux de données entrant dans l'entreprise vers les serveurs les plus appropriés.

1.1.2.5 Un routeur

Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter à travers sa table de routage. Un routeur possède plusieurs interfaces

réseau, chacune connectée sur un réseau différent. Il possède ainsi autant d'adresses IP que de réseaux différents sur lesquels il est connecté. Cet équipement est qualifié de fiable car il permet de choisir une autre route en cas de défaillance d'un lien ou d'un routeur sur le trajet qu'empreinte un paquet.

1.1.2.6 Un firewall ou pare-feu

Chaque ordinateur connecté à internet est susceptible d'être victime d'une attaque d'un pirate informatique. Ce qui favorise l'utilisation des pare-feu dans les réseaux d'entreprise. Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), 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.**

1.1.3 Les topologies physiques

La topologie physique d'un réseau est l'agencement géométrique réel des postes de travail. Il existe plusieurs topologies physiques : topologie en bus, topologie en étoile, topologie en anneau et topologie maillée.

1.1.3.1 Topologie en bus

Dans une topologie en bus, chaque poste de travail est connecté à un câble principal appelé bus. Par conséquent, chaque poste de travail est connecté directement aux autres postes du réseau. Elle est caractérisée par :

- Connexion multipoints
- Câble défectueux => réseau paralysé
- Relatif à la couche 1 (la couche 2 permet de faire le tri parmi les signaux transmis)
- Longueur de câble optimisé

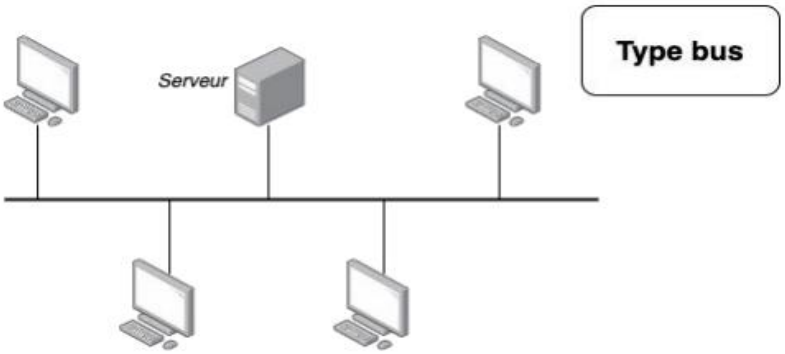

Figure 2 :Topologie en BUS

1.1.3.2 Topologie en étoile

Dans une topologie en étoile (Star) tous les postes de travail sont directement connectés à un ordinateur ou un serveur central. Chaque poste de travail est indirectement connecté aux autres via l'ordinateur central. Elle se caractérise par :

- Nœud central (hub ou switch)
- Un hub (concentrateur) travaille en diffusion
- Un switch travaille en commutation
- Réduction des conflits (par rapport au bus)
- Longueur de câble plus importante

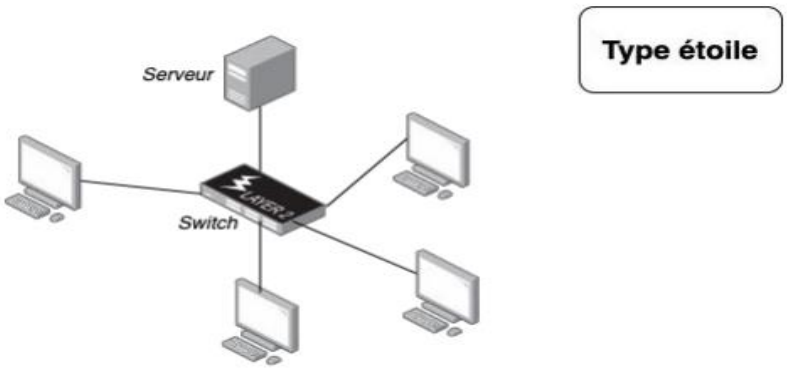

Figure 3 : Topologie en étoile

1.1.3.3 Topologie en anneau

Dans une topologie en anneau (Ring), les postes de travail sont connectés dans une configuration en boucle fermée. Les paires adjacentes de postes de travail sont directement connectées. Les autres paires sont connectées de manière indirecte, les données transitant par un ou plusieurs nœuds intermédiaires, caractérisée par :

- Sens de parcours déterminé (évitement de conflits)
- Système de fonctionnement par jeton

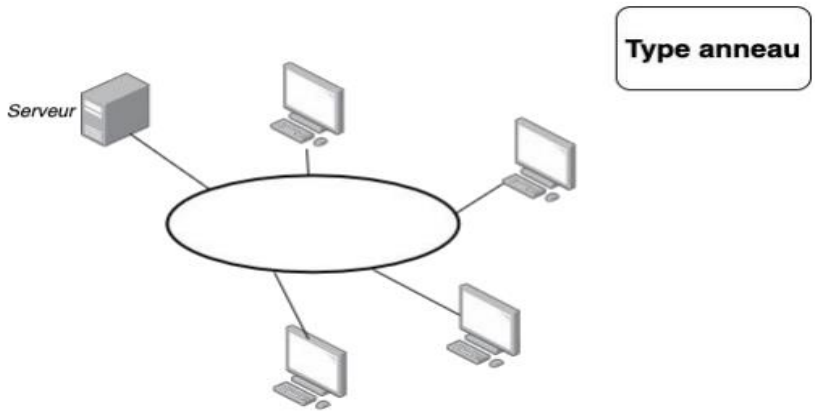

Figure 4 : Topologie en anneau

1.1.3.4 Topologie maillée

Une topologie maillée est une topologie de réseau dans laquelle tous les nœuds de réseau sont connectés les uns avec les autres. Il n'existe pas de concept de commutateur(Switch) central, de hub ou d'ordinateur qui serve de point de communication central pour la transmission des messages.

Contrairement aux autres topologies de réseau, elle peut être divisée en deux types :

- Topologie maillée entièrement connectée
- Topologie maillée partiellement connectée

Dans la topologie maillée entièrement connectée, tous les nœuds sont connectés les uns aux autres. Si vous connaissez la théorie des graphes, alors il s'agit d'un graphe entièrement connecté dans lequel tous les nœuds sont connectés à tous les autres nœuds.

Tandis qu'une topologie maillée partiellement connectée n'a pas tous les nœuds connectés les uns aux autres.

- **Avantages de la topologie maillée** :
  - ✓ Chaque connexion peut porter sa propre charge de données
  - ✓ Il est robuste
  - ✓ Une faute est diagnostiquée facilement
  - ✓ Assure la sécurité et la confidentialité
- **Inconvénients de la topologie maillée** :
  - ✓ L'installation et la configuration sont difficiles si la connectivité devient plus importante
  - ✓ Le coût de câblage est de plus en plus élevé dans le cas d'une topologie maillée entièrement connectée
  - ✓ Le câblage en masse est requis

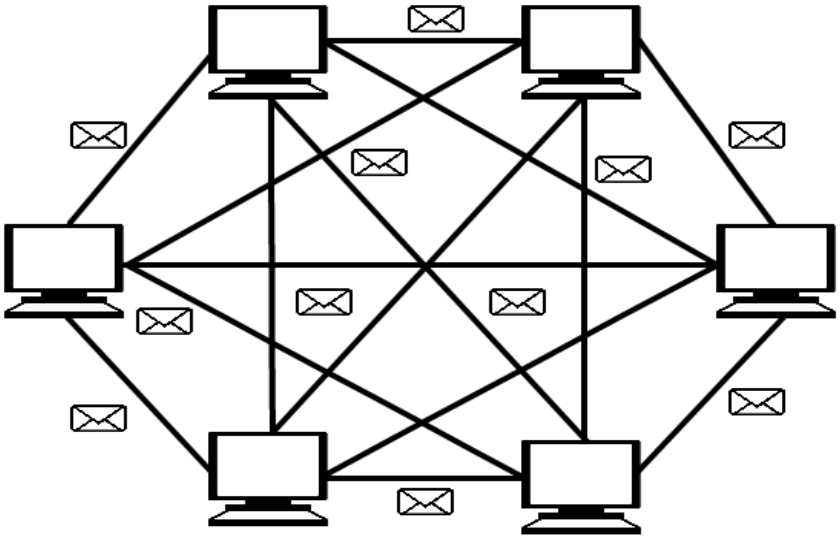

Figure 5 : Topologie en Maille

L'interconnexion de ces équipements par les supports de transmissions n'est utile que lorsqu'on les applique dans une architecture réseau d'une entreprise, pour les faire communiquer.

1.2 Les architectures réseaux

Une architecture est un édifice ou un ensemble fonctionnel composé d'équipements de transmission, de logiciels et protocoles de communication et d'une d'infrastructure filaire ou radioélectrique permettant la transmission des données entre les différents composants.

Il existe différentes types d'architectures réseaux en informatique et parmi celle-ci on a les architectures réseaux d'une petite, moyenne et grande entreprise. En premier lieu, nous allons parler de l'architecture d'une petite entreprise, ensuite l'architecture d'une entreprise moyenne et enfin l'architecture d'une grande entreprise.

1.2.1 Architecture réseau d'une petite entreprise

Comme définit précédemment, une architecture réseau est un élément incontournable pour la mise en place d'un réseau d'entreprise ou autres. Dans une petite entreprise, on a moins d'utilisateur qui constitue le réseau. L'architecture réseau d'une petite entreprise peut être définie comme un réseau local c'est-à-dire un LAN. Et que les LAN 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, …). L'étendue géographique de ces réseaux locaux ne dépasse pas 10 km (ex. : pour un immeuble ou un campus). Le débit, ou la vitesse de communication, varie de quelques Mbps à 100 Mbps. Le nombre de stations ne dépasse généralement pas 1 000. Dans cette architecture nous avons des utilisateurs qui partagent une imprimante, connectés directement à un commutateur de niveau 3 assurant la liaison des trois commutateurs de niveau 2 dans le réseau (voir ***Figure 6***). Or,

d'autre types d'architectures plus étendues du point de vue géographique existent, exemple l'architecture des entreprises moyennes.

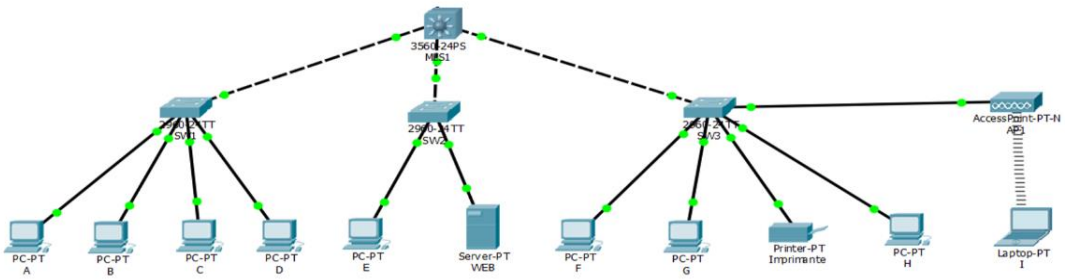

Figure 6: Architecture réseau d'une petite entreprise

1.2.2 Architecture réseau d'une entreprise moyenne

Plus étendue que la précédente, l'architecture réseau d'une entreprise moyenne est l'interconnexion de plusieurs LAN pour mettre en place un réseau plus grand. Elle peut aussi contenir des réseaux locaux virtuels (VLAN) qui est un groupe logique d'unités ou d'utilisateurs qui peut être regroupé par fonction, service ou application peu importe l'emplacement de leur segment physique. Elle contient un nombre plus important d'utilisateurs repartis en groupes logiques d'unité pour interdire certaines communications entre des utilisateurs d'un même réseau. Pour mettre en place ce genre d'architecture réseau, on a besoin un nombre important d'utilisateurs, des commutateurs de niveau 2 pour connecter les utilisateurs dans les différents switches du réseau.

Pour la sécurisation de l'architecture ; on peut mettre les utilisateurs dans des VLAN en limitant les communications dans le réseau. Après cette répartition dans des VLAN, leurs communications entre eux peut être assurées par des commutateurs de niveau 3 qui jouent parfois le rôle DHCP. Et comme les utilisateurs sur les VLAN séparés sont, par défaut, incapables de se communiquer. Donc pour autoriser cette communication entre ces VLANs, il faut faire du routage inter-VLAN. C'est un processus qui permet de transférer du trafic réseau d'un VLAN à un autre à l'aide d'un périphérique de couche 3 comme un routeur. Parfois dans ces réseaux, on déploie des serveurs (exemple : serveur web, messagerie, DNS, DHCP, …), pour protéger l'accès à ces serveurs aux utilisateurs du réseau, on utilise ce qu'on appelle les zones démilitarisées appelées **DMZ**. Elle est un réseau d'ordinateur ou serveur qui sert de zone tampon entre deux réseaux et qui dispose de sa propre adresse IP. Les serveurs qui se trouvent à l'intérieur d'une **DMZ** sont physiquement dans l'entreprise mais ne sont pas directement liés

aux machines connectées au LAN. La fonction de protection la plus performante a une architecture où la zone démilitarisée fait écran aux réseaux voisins entre le LAN et Internet via un pare-feu séparé.

Pour une prévention de ces réseaux d'entreprises contre les accès provenant du réseau public (WAN, Wide Area Network) c'est-à-dire internet, il est recommandé d'utiliser des pare-feu. Il peut s'agir de composants matériels indépendants ou d'un logiciel pare-feu sur un routeur. Le pare-feu qui est connecté entre le DMZ et le réseau de l'entreprise va protéger ces derniers contre le réseau public. Grace à ce pare-feu toutes les communications venant de l'extérieur ou intérieur peuvent être autoriser ou interdire (voir **Figure 7**). Par ailleurs, à côté de cette architecture réseau on a l'architecture réseau des grandes entreprises.

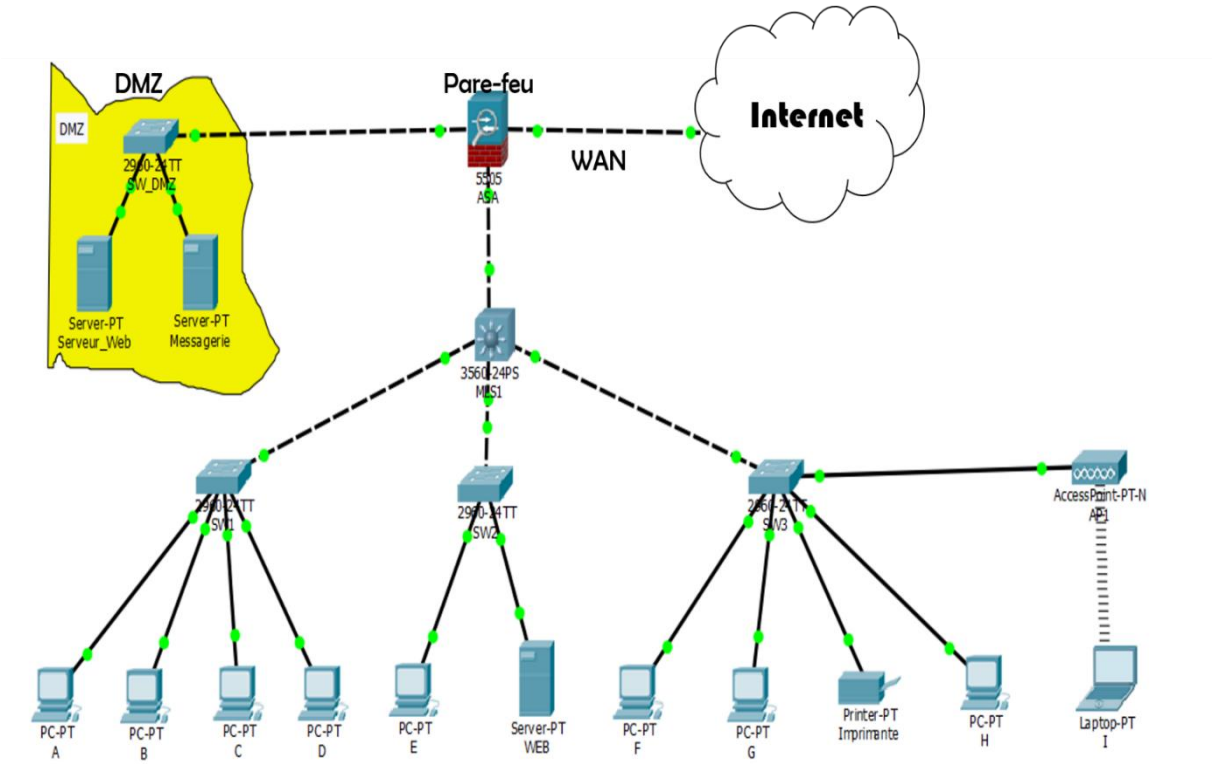

Figure 7 :Architecture réseau d'une entreprise Moyenne

1.2.3 Architecture réseau d'une grande entreprise

L'architecture des grandes entreprises est beaucoup plus importante que celle des entreprises moyennes en terme d'utilisateurs et de services, c'est-à-dire l'entreprise peut contenir plus ou moins 5000 employés. Ces types d'architectures peuvent composer de différents compartiments comme illustré dans la **Figure 8,** elle est composée d'un site principal appelé aussi la maison mère et deux succursales (Succursale 1 et succursale 2). En retour ils sont connectés par le réseau publique Internet.

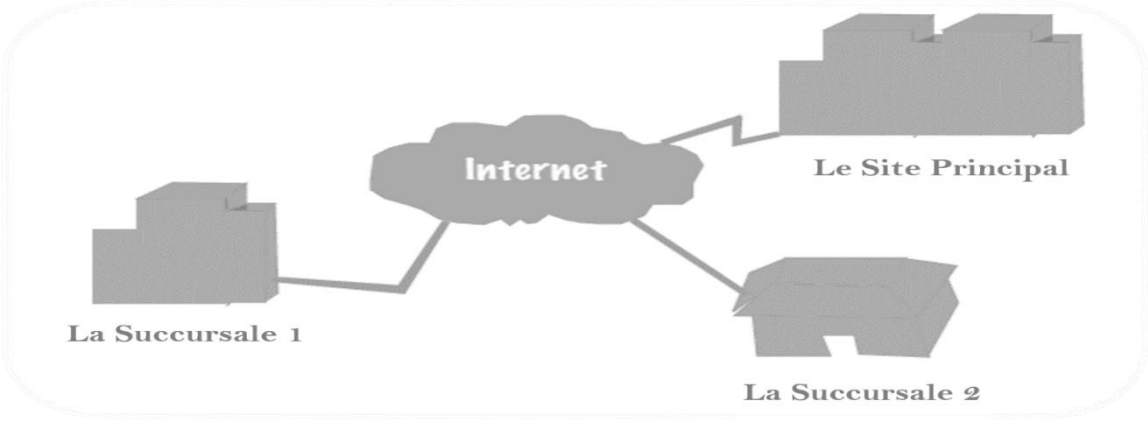

Figure 8 : Architecture réseau globale d'une grande entreprise

- **La maison mère**

Dans une architecture réseau d'une grande entreprise, les sites principaux sont constitués d'infrastructures différentes. Ces infrastructures peuvent être des utilisateurs des terminaux, des commutateurs (switchs niveau 2 et 3), des routeurs, des pare-feu, des serveurs, … comme illustré par la **Figure 9.**

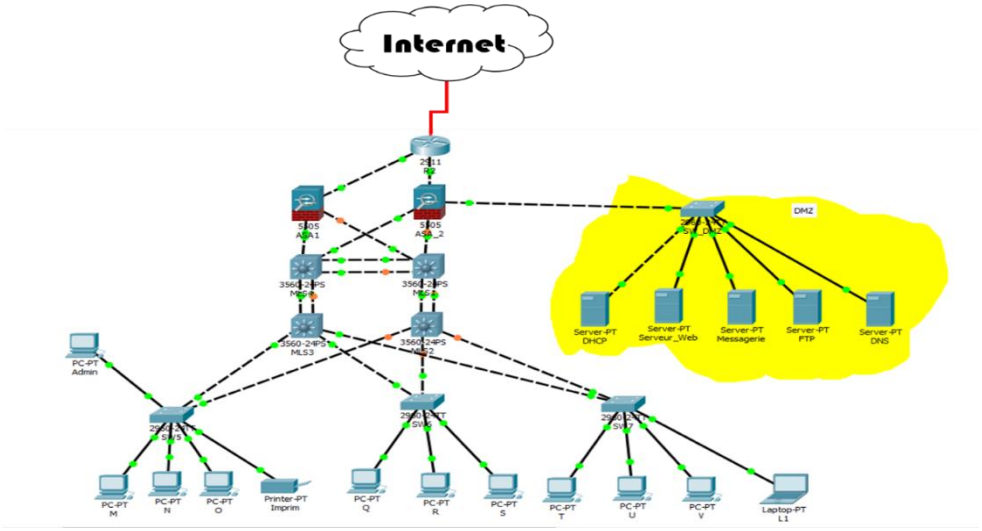

Figure 9 : Architecture Réseau d'une grande entreprise: Maison mère

- **La succursale 1** : Infrastructure de la succursale 1 est composée des terminaux des utilisateurs, des switch (SW), des points d'accès (AP) et d'un routeur R.RS1 (Routeur de la succursale 1) qui assure la passerelle vers internet (**voir Figure 10**).

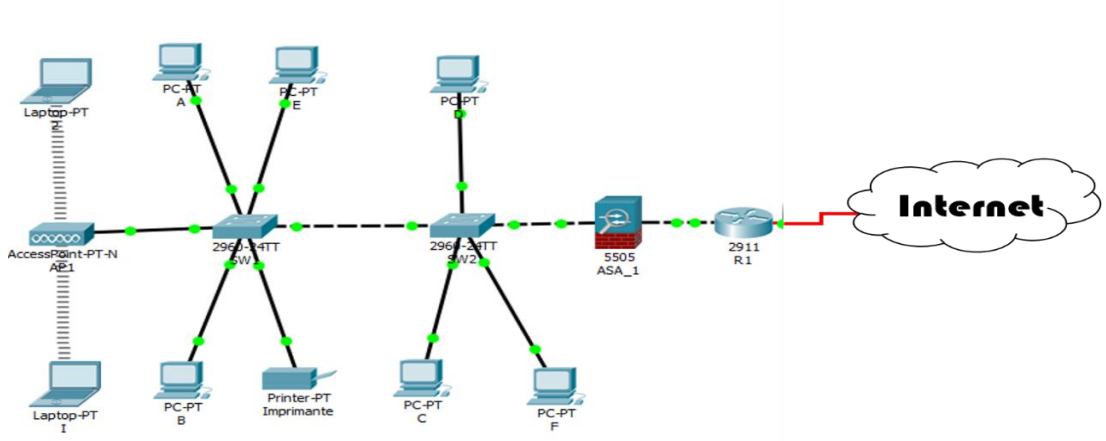

Figure 10: Architecture Réseau d'une grande entreprise : Succursale 1

- **La succursale 2 :** elle est comme la précédente par rapport aux infrastructures, mais leurs différences peuvent être le nombre de terminaux d'utilisateurs et des services configurés dans la succursale. Tous sont connectés par internet (voir **Figure 11**)

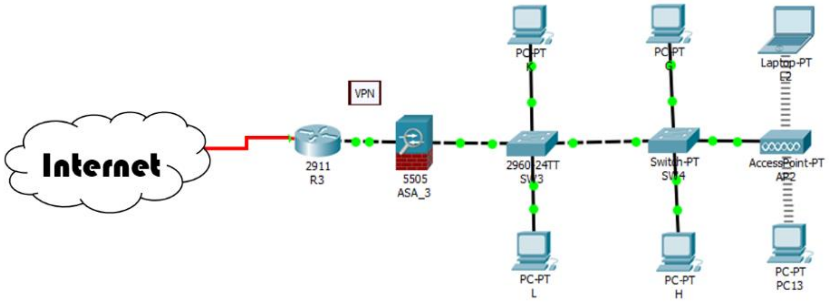

Figure 11: Architecture Réseau d'une grande entreprise : Succursale 2

L'internet : est le réseau public qui interconnecte les 3 sites. Il est composé de réseaux autre que celui de l'entreprise. En guise d'exemple qui ne le décrit pas parfaitement, son interconnexion avec les trois sites est illustrée par la **Figure 12**.

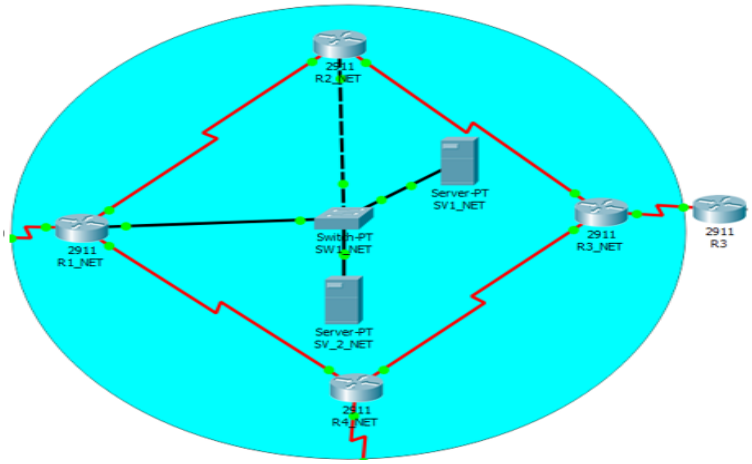

Figure 12: Architecture Réseau d'une grande entreprise : Internet

1.3 Les services réseaux

Un service réseau est une fonctionnalité assurée par un ordinateur, fournissant des informations à d'autres ordinateurs via une connexion réseau normalisée. Les services réseaux se basent sur des protocoles pour fournir des fonctionnalités qui sont accessibles par l'utilisateur au niveau de la couche application. Comme services réseaux, on a le service de résolution de noms (machines : DNS), l'attribution d'adresse (DHCP), la messagerie, le web, le FTP ...

1.3.1 Domain Name System (DNS)

Le **DNS** (Système de noms de domaine en français) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP. Autrement dit, le **DNS** est un service qui permet d'associer à un site web (ou un ordinateur connecté ou un serveur) une adresse IP, comme un annuaire téléphonique permet d'associer un numéro de téléphone à un nom d'abonné. Ce principe de fonctionnement suscite une unicité des noms et le respect d'un nommage hiérarchique avec des domaines existants (.com, .edu, .org, ...). Chaque fournisseur d'accès à internet dispose notamment de ses propres serveurs **DNS**, avec des adresses IP qui prennent souvent la forme d'une succession de nombres de chiffres (194.158.122.10 par exemple).
Pour déployer un serveur DNS dans un réseau, il faut définir l'adresse du réseau ; pour des organisations désirant donner un accès public à leur domaine, il faut acheter un nom de domaine chez un fournisseur d'accès à internet tout en assurant son unicité sur internet[2].

1.3.2 Attribution d'adresse (DHCP)

Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau chargé de la configuration automatique des adresses IP d'un réseau informatique. Il est défini aussi comme un protocole de communication ou protocole réseau parfaitement indispensable. On le traduit généralement par protocole de configuration dynamique des hôtes. Il assure une configuration automatique et dote les autres appareils du réseau d'adresses IP. Donc son rôle principal est de distribuer des adresses IP à des clients, en réduisant considérablement l'intervention humaine c'est-à-dire l'administrateur ou le technicien réseau. Il passe en paramètres au client toutes les informations nécessaires. Mais le serveur DHCP peut configurer à la fois et automatiquement l'adresse de la passerelle par défaut et le serveur DNS[2].

1.3.3 Messagerie

Le courrier électronique est aujourd'hui l'une des applications les plus populaires du réseau. Il est utilisé pour des applications très variées : personnelles, professionnelles, politiques, …. En fait, pour fonctionner, la messagerie électronique s'appuie principalement sur des serveurs de messagerie, des protocoles de transport. Le serveur de messagerie est un logiciel de courrier

électronique ayant pour vocation de transférer les messages électroniques d'un serveur à un autre.

Pour son implémentation, service de messagerie, il est nécessaire de faire le choix de la forme des adresses, de répartir les serveurs (entrant/sortant), de définir les méthodes d'accès aux boites aux lettres et le format des messages [2]:

- **Choix de la forme d'adresse** : il s'agit de définir la stratégie pour la forme des adresses email. Il est possible d'avoir une forme canonique (ex : prenom.nom@...), soit faire apparaître le sous-domaine ou non (ex : nom.prenom@zig.univ.sn ou nom.prenom@zig.sn), soit utiliser des adresses génériques.
- **Répartition des serveurs** : vu le double service (relais de message et hébergement de boîtes aux lettres) offert, le serveur entrant (serveur qui rapatrie les mails en local) peut assurer ces deux services ou uniquement le service de relayage de messages dans ce dernier cas les boîtes aux lettres sont sur des serveurs internes non accessibles sur internet. Le serveur sortant quant à lui passe de préférence par un seul serveur relais.
- **Méthodes d'accès aux boîtes aux lettres** : il est possible d'utiliser soit une connexion interactive sur le serveur (commande mail unix...), soit POP (l'utilisateur accède au serveur via un client de messagerie tel qu'un navigateur et la boîte aux lettres est transférée sur la station du client), soit IMAP (l'accès client est pareil à celui de POP mais la boîte aux lettres reste sur la station du client).
- **Format de messages** : MIME, S/MIME (MIME sécurisé)

1.3.4 Service web

Dans l'informatique, le mot "serveur web" désigne à la fois une machine physique et un logiciel. Dans le premier cas, il s'agit d'un ordinateur relié à Internet et hébergeant des ressources. Ces ressources peuvent être des fichiers, des programmes ou des bases de données. C'est une technologie qui permet à des applications de communiquer à travers le réseau internet. Dans les entreprises, l'accès aux serveurs web externes (Internet) fait très souvent l'objet d'une décision de la direction et non de l'administrateur réseau afin d'attribuer des autorisations aux utilisateurs. Dans ce cas on peut implémenter un proxy pour réglementer l'accès à Internet et la sécurité. Pour un déploiement d'un serveur web en interne (Intranet) au sein d'une organisation, le serveur doit héberger les informations internes, être placé dans un sous-réseau et non accessible depuis l'extérieur. Contrairement à un serveur web externe (Extranet), les informations sont hébergées dans un sous-réseau public et accessible par tout internaute[2].

1.3.5 FTP

Le **FTP** veut dire « File Transfert Protocol » ou Protocole de transfert de Fichier. C'est donc un langage qui va permettre l'échange de fichiers entre 2 ordinateurs, et plus exactement entre un serveur et un client.

On parle alors de **serveur FTP** et **client FTP**

Dans un échange **FTP** il y a deux intervenants à savoir le **client** et le **serveu**r.

- **Le serveur FTP** : Le serveur FTP est un logiciel qui va répondre aux demandes des clients. Lorsque le serveur reçoit une demande, il vérifie les droits et si le client à les droits suffisants, il répond à cette demande sinon la demande est rejetée. Il passe son temps à attendre. Si les demandes ne sont pas nombreuses, les ressources utilisées par le serveur FTP sont quasi-nulles.
- **Le client FTP** : il initie de toutes les transactions et se connecte au serveur FTP, effectue les commandes (récupération ou dépôt de fichiers) puis se déconnecte. Toutes les commandes envoyées et toutes les réponses seront en mode texte. C'est-à-dire un humain peut facilement saisir les commandes et lire les réponses).

Et le protocole FTP n'est pas sécurisé : les mots de passe sont envoyés sans cryptage entre le client FTP et le serveur FTP. Chacun de ces éléments présentent des logiciels marchant sur les différents systèmes d'exploitations[2].

Conclusion

Les technologies utilisées, les architectures réseaux et les services jouent un rôle primordial pour la mise en place d'un bon réseau d'entreprise. Une fois ce réseau existe, il faut penser à sa sécurité en évitant des failles de sécurité dans le réseau. C'est pour cette raison que nous tenterons au chapitre suivant d'étudier la sécurité informatique dans les réseaux.

Chapitre II :

Généralité sur la sécurité informatique

Introduction

De nos jours, Le monde connaît des avancées très significatives dans le domaine informatique ; les besoins en matière de sécurité surtout informatique, sont un peu plus irrésistibles, et la prédisposition n'est forcément pas à la baisse. Depuis quelques années déjà, on assiste à un changement constant des techniques, qu'il s'agisse des techniques visant à sécuriser l'échange des données informatiques ou des techniques de mises au point pour contourner les systèmes sécurisés informatiques. Ainsi, dans ce chapitre nous allons d'abords définir quelques concepts primordiaux de la sécurité informatique, ensuite faire un développement sur les vulnérabilités, les risques, les attaques informatiques, les services de sécurités proposés et les mécanismes de sécurités, enfin terminer avec une conclusion du chapitre.

2.1 Définitions

- **La sécurité informatique :** Elle est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Et que son objectif principal est de garantir que les ressources matérielles et/ou logicielles d'un système informatique sont uniquement utilisées dans le cadre prévu et par des personnes autorisées.
- **La sécurité des réseaux :** Elle englobe toutes les activités visant à protéger la fonctionnalité et l'intégrité d'un réseau d'entreprise et des données qui y trouvent. Elle comprend des technologies matérielles et des technologies logicielles. Elle empêche aussi les hackeurs de pénétrer dans le réseau ou de s'y propager en prenant des mesures efficaces de sécurité. La sécurité des réseaux combine de nombreuses couches de défenses en périphérie et dans le réseau. Chaque couche de sécurité du réseau met en œuvre des politiques et des contrôles. Les utilisateurs autorisés obtiennent un accès aux ressources de réseau, tandis que les intervenants malveillants sont bloqués et ne peuvent pas accomplir leurs exploitations et menaces.
- **La cryptanalyse :** Ensemble des méthodes et procédés de décryptage visant à rétablir en clair un cryptogramme, sans connaissance préalable de la clé de chiffrement. Plus généralement, elle étudie la sécurité des procédés de chiffrement utilisés en cryptographie. La cryptanalyse est alors utilisée pour mettre à l'épreuve des fonctions cryptographiques existantes, de manière à démontrer leur efficacité. Parmi les méthodes utilisées par la cryptanalyse, on peut citer : l'attaque en force, l'analyse de trafic et l'analyse statistique.
- **La cryptographie :** La cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre

inintelligibles sans une action spécifique (protéger des messages). Grâce à son évolution, la cryptographie ; on a vu naitre deux types de cryptages : la cryptographie symétrique (clé secrète) et la cryptographie asymétrique (clé publique).

- **Le chiffrement :** Le chiffrement est un procédé de la cryptographie qui consiste à protéger des données qui sont alors incompréhensibles pour celui qui ne dispose pas de la clef du chiffrement. Mais en informatique, le chiffrement a pour objectif de garantir la confidentialité et l'intégrité des données stockées sur des Systèmes Informatiques (SI) ou des données en transition. Les données sont chiffrées à l'aide d'un algorithme et d'un jeu de clefs de chiffrement. Comme la cryptographie, on a le chiffrement symétrique, le chiffrement asymétrique et le chiffrement hybride.
- **Une menace :** c'est un danger potentiel pour un actif tel que les données ou le réseau lui-même.

D'ailleurs, dans le domaine de la sécurité informatique on note un taux très élevé de menaces. Ces dernières essayent parfois d'exploiter les faiblesses ou les failles d'un système informatique (Vulnérabilités) ouvrant des portes aux hackers.

2.2 Les vulnérabilités dans l'informatique

2.2.1 Définition

Une vulnérabilité ou faille informatique est une faiblesse d'un système informatique(SI) permettant à un attaquant de porter atteinte à l'intégrité, la confidentialité et la disponibilité des données ou des services dans un système. Elle provient également d'une faiblesse dans la conception d'un système d'information (SI), d'un composant matériel ou d'un logiciel. Mais toutes les vulnérabilités ne mènent pas nécessairement à une attaque au système. Comme illustré dans le schéma ci-après, une vulnérabilité est une porte d'entrée des attaquants dans un réseau informatique. La liste des vulnérabilités informatiques est exhaustive, mais nous allons prendre quelques exemples de ces vulnérabilités et leurs causes[4].

2.2.2 Les types de vulnérabilités informatiques

En informatique, on distingue plusieurs types de vulnérabilités, parmi lesquelles on peut citer :

- **Failles au niveau des protocoles d'administration :** Pour ce type de faille, les faiblesses en matière de sécurité se trouvent au niveau des éléments actifs comme les switchs, les routeurs ou encore les imprimantes. Souvent, les mots de passe d'administration par défaut pour accéder à ces types d'équipement restent inchangés. Elle est souvent exploitée par les hackers pour porter atteinte à l'entreprise[5].

- **Failles au niveau du partage de fichiers :** La plupart des entreprises ou des structures, pour ne pas dire toutes, utilisent le partage de fichiers. Le plus souvent, la restriction est rarement préconisée. Pourtant le partage de fichiers non sécurisés représente une porte sans serrure pour les hackers et leur permettant d'obtenir des informations sensibles, voire confidentielles du lieu (entreprises, structures). Par exemple, les imprimantes les plus récentes ont des failles qui permettent aux pirates (hackers) de récupérer des données numérisées ou photocopiées des données à l'intérieur de l'entreprise ou de la structure, si aucune mesure de sécurité informatique adaptée n'a été prise en compte[5].
- **Failles au niveau de la gestion des droits d'accès :** Dans certaines d'entreprises, les restrictions d'accès au locaux sont parfois trop faciles, et parfois même inexistantes. D'après nos recherches, des études en sécurité informatique ont montrés que 50% des menaces proviennent directement des employés de l'entreprise c'est-à-dire les menaces internes. Non pas parce qu'ils sont malintentionnés, mais souvent ils ne sont conscients des risques que représente leur laxisme en matière de sécurité informatique. Bref, ils constituent le maillon faible de la chaine de sécurité informatique. Par exemple, en permettant à un stagiaire d'utiliser la session de son encadreur au sein de la boîte, donc l'entreprise est exposée à des risques comme le **vol d'informations stratégiques** ou **confidentielles**.
- **Faille au niveau du web :** Les vulnérabilités web représentent des risques non négligeables en matière de sécurité informatique**.** La majeure partie des entreprises ou des structures utilisant le web sont exposées aux attaques et même plus dangereusement que les autres.

Bref, quand un système informatique est vulnérable aux attaques, donc ce système court énormes risque qui peut porter préjudice en son entreprise ou son réseau informatique.

2.3 Les risques dans un système Informatique

Le risque informatique peut être définit comme étant la probabilité qu'une menace exploite la vulnérabilité particulière d'un actif (serveur informatique, ordinateurs, …) et entraine une ou des conséquences indésirables, c'est-à-dire occasionner un dommage à l'entreprise ou à la structure. Ces risques peuvent parfois être d'origine humaine, technique ou juridique. Dans cette partie du chapitre, nous essayerons en premier lieu de parler de l'origine des risques informatiques, en deuxième lieu montrer les conséquences des risques informatiques et en troisième et dernier lieu parler de la gestion des risques informatiques dans un système informatique.

2.3.1 L'origine des risques informatiques

Dans une entreprise ou une structure informatique, les risques peuvent provenir de n'importe où c'est-à-dire plusieurs origines. Parmi ces origines on peut citer :

- ✓ **Les risques accidentels**
- ✓ **Les erreurs**
- ✓ **La malveillance.**

2.3.1.1 Les risques accidentels

Dans les risques accidentels, on peut faire allusion aux risques matériels, aux pannes et au dysfonctionnement d'un matériel ou d'un logiciel de base.

2.3.1.1.1 Les risques matériels

C'est la destruction totale ou partielle d'un ou plusieurs composants d'un système d'information (des équipements informatiques ou de communication, supports de données, environnement tels que locaux, conditionnement d'air, alimentation électrique, installation téléphonique, serveurs …) suite à des événements comme un choc, la coupure de câbles électriques ou téléphoniques, l'incendie, l'inondation, la foudre, la tempête, ...

2.3.1.1.2 Pannes et dysfonctionnement d'un matériel ou de logiciel de base

Généralement, les interruptions de service informatiques consécutives à des pannes sont de courte durée mais ce n'est pas toujours le cas. Des défaillances de matériel ou de logiciels de base ont provoqué des arrêts de fonctionnement de serveurs importants s'étendant sur plusieurs jours ouvrables. Ces interruptions peuvent aussi résulter de pannes dont l'origine est externe à l'entreprise ou à une organisation qui utilise les réseaux informatiques (réseau téléphonique, alimentation électrique, …). L'impossibilité d'accéder au réseau Internet peut empêcher une organisation de recevoir ou d'émettre du courrier électronique ou faire en sorte qu'un site de commerce électronique ne puisse plus recevoir de commandes ou parfois empêcher une université de faire ces tâches administratives par exemple les inscriptions en ligne ou les délibérations des examens.

2.3.1.2 Les erreurs

Parfois dans les entreprises, l'administrateur réseau ou les employés de l'entreprise peuvent commettre des actes malintentionnés dans un matériel ou dans le réseau espérant qu'il a bien faite alors qu'il s'est trompé. Ces erreurs sont nombreuses aujourd'hui dans les entreprises, on prend l'exemple comme :

2.3.1.2.1 Les erreurs de saisie, de transmission et de l'information

On a tendance à sous-estimer les erreurs de saisie de données dans les entreprises. Même après vérification, elles atteignent couramment un taux très important de dégâts au sein de l'entreprise. A tort, on les considère comme une conséquence inéluctable de l'activité humaine, alors qu'elles sont à l'origine d'un nombre élevé de problèmes et de pertes pouvant être importantes. Donc le contrôle des données saisies est une mesure indispensable pour prévenir un danger.

Quant à la transmission de données, qu'elle se fasse par transport de supports ou par télécommunications, elle est sujette à altération de données ou détournements, sans compter les transmissions de mauvais fichiers.

D'une manière générale, les erreurs humaines de tous types sont une grande source de préoccupation. Comme les défauts organisationnels ou de communication interne (la non-suppression d'un mot de passe attribué à une personne licenciée), peuvent être lourds de conséquences pour l'entreprise ou l'organisation.

Comme il est souvent à l'origine d'un certain nombre de ces erreurs humaines, l'informatique peut venir « à son propre secours », notamment si l'on a le bon sens de prévoir certains choses :

- Des contrôles de robustesse (limite d'un champ de saisie évitant un débordement dans les champs suivants),
- Des filets de sécurité (« une date d'expiration » qui suspend automatiquement un utilisateur dont le contrat se termine à une date précise), ….

2.3.1.2.2 Les erreurs d'exploitation

Les erreurs d'exploitations prennent des formes variées : effacement accidentel de fichiers, supports ou copies de sauvegarde, chargement d'une version incorrecte de logiciel ou de copie de sauvegarde, lancement d'un programme inapproprié, … II est souvent difficile d'identifier la cause exacte de ces problèmes : faute professionnelle, malveillance, erreur, négligence, laxisme, … Une analyse pointue des processus et des éléments endogènes ou exogènes, qui ont provoqué l'erreur, prendra du temps et risque d'être coûteuse pour l'entreprise. Donc pour réduire les erreurs provoquées par les interventions humaines, on fait recours à des systèmes automatisés de gestion des applications pour baisser le nombre de ces erreurs.

2.3.1.2.3 Les erreurs de conception et de réalisation

Alors que le nombre d'erreurs des deux catégories précédentes a tendance à se stabiliser et même à diminuer, les erreurs de conception et de réalisation sont en forte augmentation. D'après

nos recherches dans les revues et des articles, ces erreurs de conception et de réalisations provoquent par chaque semaine une dizaine de vulnérabilités dans les entreprises.

D'une part, des logiciels conçus et réalisés il y a bon nombre d'années sont toujours utilisés de manière opérationnelle. Leur documentation est souvent inexistante, incomplète ou mauvaise et n'est plus à jour. Leurs auteurs ne sont plus disponibles pour assurer la maintenance. La qualité de la programmation est généralement médiocre voire mauvaise. Toute évolution ou correction sur ces logiciels devient dès lors très difficile, et entraîne fréquemment des dysfonctionnements graves et imprévisibles dans ces logiciels.

D'autre part, on développe chaque jour de nouveaux logiciels de grande taille et d'une complexité sans cesse croissante. Les ambitions dépassent quelquefois l'état de l'art ou la compétence de leurs auteurs. Les développements s'appuient souvent sur des bibliothèques de composants ou de logiciels de base eux-mêmes truffés d'erreurs.

Les défaillances des logiciels résultent souvent des lacunes de la maintenance. Chaque nouveau développement entraîne des charges de mise à jour du logiciel pendant toute sa durée de vie. Les conséquences de ces erreurs de développement et de conception sont souvent dramatiques et peuvent mettre en péril aussi bien la survie du client que du fournisseur.

Les erreurs de conception dans la configuration et le paramétrage des systèmes de protection engendrent de grosses vulnérabilités. Il y va par exemple d'ordinateurs coupe-feu (« firewalls ») ne filtrant rien ou encore qui soient mal placés dans le réseau.

Des faiblesses dans la conception de la protection logique, telles que des mots de passe communs à plusieurs personnes ou trop faciles à découvrir (par raisonnement logique, par « craquage » ou piratage, par observation illicite, …) créent également des brèches dans la sécurité.

2.3.1.3 La malveillance

Les actes malveillants à l'encontre des systèmes d'information, sont fréquents de nos jours dans le milieu des réseaux et provoquent d'énormes dégâts dans les entreprises. Pour protéger les acteurs du réseau, ces actes malveillants ont été criminalisés leurs auteurs encourent des sanctions. Par ailleurs, ces actes malveillants dans les systèmes informatiques sont divers et variés.

2.3.1.3.1 Vol et sabotage de matériel

Les vols portent principalement sur les petits matériels, tels que les ordinateurs portables et les supports informatiques (disques dure, serveurs, …). La disparition d'un PC ou d'un serveur peut être de conséquences lourdes au cas où celui-ci n'a pas fait l'objet d'une copie de

sauvegarde récente et complète ou encore lorsque celui-ci contient des données ou programmes confidentiels de l'entreprise. Le vol d'un portable peut également permettre de prendre connaissance des mots de passe et des informations nécessaires pour se connecter au réseau interne de l'entreprise et prendre des informations confidentielles.

Mais le sabotage va de l'endommagement d'un appareil isolé de l'entreprise en détruisant toute les infrastructures ou faire des actes de vandalismes au sein des locaux de l'entreprise.

L'utilisation de matériels hors standards du réseau principal aggrave les conséquences d'un vol ou d'un sabotage dans la mesure où l'obtention de matériels de remplacement peut s'avérer plus difficile.

2.3.1.3.2 Sabotage immatériel

Le sabotage immatériel concerne la destruction, totale ou partielle, des données, des programmes ou de leurs sauvegardes. Ses conséquences peuvent également être graves et parfois même non-avantageuse, car il peut provoquer des destructions en profondeur et avoir pour effet de neutraliser pendant un temps long le fonctionnement du système informatique dans tout le réseau de l'entreprise.

Le sabotage immatériel recouvre diverses notions comme la modification non autorisée de programmes, le cheval de Troie, les bombes logiques, les virus et vers.

Mais l'Internet et le courrier électronique ont fourni des voies de propagation dans les réseaux par exemple les logiciels espions (« spyware ») qui sont dangereux sur l'échanges des mails de l'extérieur vers l'intérieur d'un réseau.

2.3.1.3.3 Grève, départ de personnel stratégique

Le personnel ou l'employé est un maillon indispensable dans la chaîne qui assure le bon fonctionnement d'un système d'information dans une entreprise. L'indisponibilité, l'absence, une épidémie ou la disparition d'un membre de personnel-clé peut provoquer l'arrêt total ou partiel du système et par voie de conséquence celle de toute l'activité de l'entreprise. Donc pour diminuer ces genres de risques, il est préférable soit d'automatisées certaines taches ou de chercher des suppliants à ces genres de personnes importantes, pour que leurs absences ne puissent pas impacter l'entreprise entière.

Par ailleurs, l'origines de ces risques informatiques peut entrainer des dommages néfastes dans un système d'information ou dans un réseau total d'une entreprise, en y laissant des conséquences irréparables. Peut aller même plus loin, jusqu'à la fermeture de l'entreprise avec des dettes importantes.

2.3.2 Les conséquences des risques informatiques

Les conséquences des risques informatiques aux systèmes d'informations sont nombreuses aujourd'hui, elles peuvent être des pertes directes ou des pertes indirectes.

2.3.2.1 Les pertes directes

Elles correspondent de manière directe à une disparition d'actifs. Ces pertes directes correspondant à des pertes financières de l'entreprise, entraînent des écritures de redressement comptable s'il s'agit d'actifs appartenant à l'entreprise c'est-à-dire détournement de fonds ou de biens mais aussi un décaissement s'il s'agit d'actifs appartenant à des tiers (collaborateurs) c'est-à-dire des comptes clients ou de dépôts, ...

Egalement ces pertes directes peuvent être **des pertes directes matérielles** (équipements informatiques, équipements télématiques), environnement (électricité, eau, climatisation, …), bâtiments, logiciels, données ou **des pertes directes immatérielles** (le contenu des logiciels, le contenu des données).

2.3.2.2 Les pertes indirectes

Les conséquences indirectes d'un incident dépassent généralement de loin les pertes directes. Comme les pertes directes, les pertes indirectes peuvent être des pertes indirectes matérielles ou des pertes indirectes immatérielles.

Dans les pertes indirectes matérielles, on trouve des postes tels que :

- Les frais de reconstitution de données et d'archives ;
- Les frais financiers ;
- Les intérêts sur comptes à recevoir ;
- Les pertes d'exploitation ;
- Le manque à gagner (reconstitution du bénéfice normal en l'absence de sinistre) ;
- La perte de matières périssables ;
- Les frais d'étude et d'expertise ;
- Les frais supplémentaires

Les pertes indirectes immatérielles contiennent aussi des postes tels que :

- L'atteinte à l'image de marque (et donc le risque de fuite de la clientèle, etc.)
- La perte de marchés potentiels ;
- L'affaiblissement de la capacité concurrentielle ;
- Le retard technologique

Bref, lorsqu'un système d'information vulnérable est exposé à des menaces en courant des risques, est susceptible d'être attaqué par des attaquants. Donc dans partie qui suit nous allons parler des attaques informatiques et ces différents types.

2.4 Les attaques informatiques

C'est l'ensemble des actions qui peuvent compromettre la sécurité des informations ou des ressources. En outre elles représentent les moyens d'exploiter une vulnérabilité d'un réseau ou d'un système informatique à des fins non connues par l'exploitant du réseau ou du système et généralement préjudiciables.

Ainsi les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système ;
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- Chercher des informations personnelles sur un utilisateur ;
- Récupérer des données bancaires ;
- Troubler le bon fonctionnement d'un service ;
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée

Il existe plusieurs types d'attaques informatiques dans le domaine de la sécurité des informations. On peut donner par exemple les attaques d'accès, les attaques de reconnaissances, les attaques par déni de service (Dos) et DDos, les attaques d'ingénierie sociale et les attaques des logiciels malveillants.

2.4.1 Attaques d'accès

Les attaques d'accès exploitent des vulnérabilités connues dans les services d'authentification, les services FTP et les services Web pour accéder à des comptes en ligne, à des bases de données confidentielles ou à toute autre information sensible d'une entreprise. C'est-à-dire accéder à des comptes ne disposant pas d'un compte ni un mot de passe pour y accéder. Parmi ces attaques d'accès, on a les attaques de mot de passe, les attaques d'usurpation d'identité, les attaques par débordement de tampon, les attaques de l'homme au milieu, la redirection de port et l'exploitation de confiance.

2.4.1.1 Attaques de mot de passe

Les attaques de mot de passe peuvent se faire à l'aide d'un analyseur de paquets pour glaner les comptes et les mots de passe utilisateur transmis en clair. Les attaques de mot de passe se rapportent en général aux tentatives de connexion répétées à une ressource partagée, comme un

serveur ou un routeur, afin d'identifier un compte utilisateur, un mot de passe. Ces tentatives répétées s'appellent attaques par dictionnaire ou attaques en force, qui sont des types d'attaques de mots de passe.

2.4.1.2 Attaques d'usurpation d'identité

Une attaque d'usurpation d'identité est une attaque d'accès qui se définit par l'appropriation de l'identité ou de toute autre donnée permettant d'identifier la victime par un tiers. Elle comprend donc le vol:

- de Nom, prénom, surnom, pseudonyme, identifiants électroniques
- des adresses IP, URL, e-mails, mots de passe, SMS, logos, images, ...

L'usurpation d'identité (ou spoofing) est une attaque d'usurpation qui se produit lorsqu'une personne malveillante fait semblant d'être une source de confiance pour accéder à des données ou des informations importantes.

L'objectif principal de l'usurpation d'identité est d'accéder à des informations personnelles, de voler des données personnelles, de contourner les contrôles d'accès à un réseau ou de propager des logiciels malveillants via des pièces jointes ou des liens infectés.

2.4.1.3 Attaques par débordement de tampon

Les attaques par « débordement de tampon » (en anglais « Buffer overflow », parfois également appelées dépassement de tampon) est une attaque très efficace et assez compliquée à réaliser. Elles visent à exploiter une faille, une faiblesse dans une application (navigateur, logiciel de mail, …). Elles ont pour principe l'exécution de code arbitraire par un programme en lui envoyant plus de données qu'il n'est censé en recevoir.

Le fonctionnement général de cette attaque est de faire détruire un programme en écrivant dans le buffer plus de données pour surcharger son contenu (un buffer est un zone mémoire temporaire utilisée par une application), dans le but d'écraser des parties du code de l'application et d'injecter des données utiles pour exploiter le crash de l'application. Cela permet donc en résumer d'exécuter du code arbitraire sur la machine où tourne l'application vulnérable dans le système.

2.4.1.4 Attaques de l'homme du milieu

L'attaque man-in-the-middle (MITM) ou (littéralement « attaque de l'homme du milieu ») est une technique de piratage informatique consistant à intercepter des échanges cryptés ou no-cryptés entre deux personnes à distance ou deux ordinateurs d'une entreprise pour décoder les messages. L'attaquant doit donc être capable de recevoir les messages des deux parties communicantes et d'envoyer des réponses à une partie en se faisant passer pour l'autre. La

couche la plus utilisée pour ce type d'attaque est une connexion Internet entre des ordinateurs et/ou des terminaux mobiles à distance.

L'objectif principal d'une attaque MITM est de pouvoir espionner les communications voire, dans certains cas, modifier des contenus. Il existe différents types d'une attaque MITM, parmi lesquels :

2.4.1.4.1 Détournement de session

Le détournement de session est une attaque de l'homme au milieu, connu également sous le nom de « détournement de session TCP », est une méthode visant à prendre possession de la session Web d'un utilisateur en obtenant clandestinement son identificateur de session afin de se faire passer pour l'utilisateur autorisé. Après avoir obtenu l'identificateur de session de l'utilisateur, l'attaquant peut se faire passer pour lui et effectuer toutes les tâches à sa disposition sur le réseau.

2.4.1.4.2 Usurpation d'IP

Une usurpation d'adresse IP se produit lorsqu'un acteur malveillant construit un paquet IP qui semble provenir d'une adresse valide à l'intérieur de l'intranet de l'entreprise. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

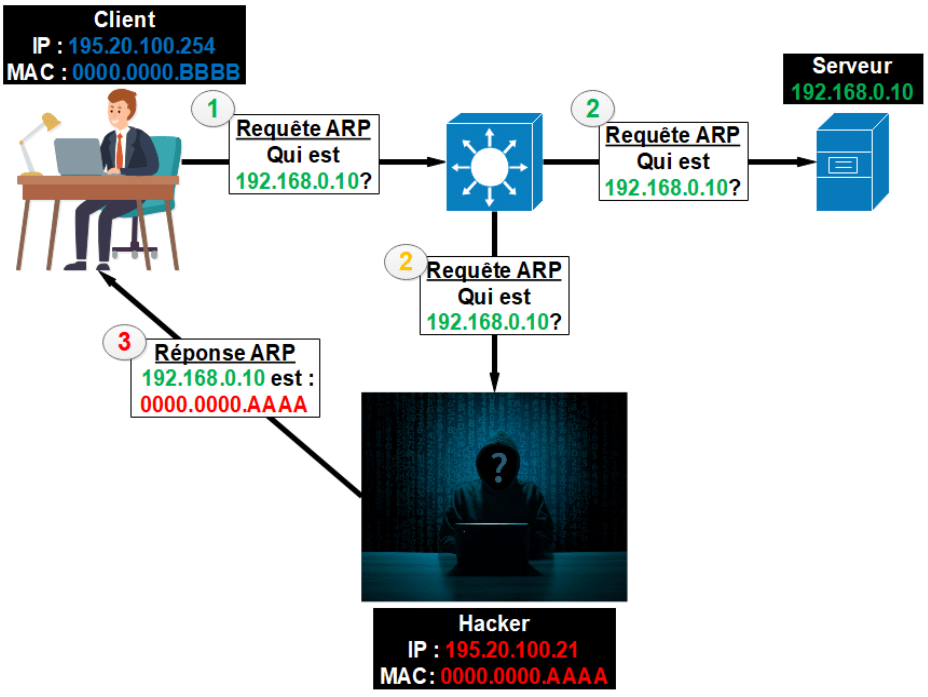

Figure 13 : Attaque par l'homme du milieu[6]

2.4.2 Attaques de reconnaissance

La reconnaissance est la collecte d'informations, les attaques par reconnaissance ont pour but de récupérer un maximum d'informations en vue d'attaques futures. Les attaques de type reconnaissance recherchent des faiblesses ou des vulnérabilités dans les défenses du réseau d'une entreprise. C'est analogue à un voleur dans un quartier en faisant du porte-à-porte en faisant semblant de vendre quelque chose ou chercher quelque chose. Ce que le voleur est en train de faire, c'est de chercher des maisons vulnérables dans lesquelles s'introduire, telles que des résidences inoccupées, des résidences avec des portes ou des fenêtres faciles à ouvrir et des résidences sans système de sécurité ni caméras de sécurité.

Donc les hackeurs utilisent des attaques de reconnaissance (ou de reconnaissance) pour effectuer une découverte et une cartographie non autorisées de systèmes, de services ou de vulnérabilités. Lorsque des vulnérabilités ou failles sont trouvées, elles ne sont pas directement exploitées par les attaquants, mais ils ont besoin des informations à sorties de ces vulnérabilités afin de mieux organiser des attaques futures, qui elles, vont cibler spécifiquement ces vulnérabilités collectées. Un bon attaquant cherche à obtenir un maximum d'informations sur l'infrastructure qu'il souhaite attaquer, avant de se lancer sur une attaque qu'il n'a pas assez d'informations.

2.4.3 Attaques par déni de service (Dos) et Attaques par déni de service Distribué (DDos)

Appelées parfois attaques par saturation, une attaque par Déni de service (Denial of Service) est une attaque qui empêche l'utilisation normale d'un ordinateur ou d'un réseau par des utilisateurs valides. Une attaque DoS peut inonder un ordinateur ou l'ensemble du réseau de trafic jusqu'à ce qu'un arrêt se produise en raison de la surcharge. Une attaque DoS peut également bloquer le trafic, ce qui entraîne une perte d'accès aux ressources du réseau par les utilisateurs autorisés. Son objectif principal est d'affecter un service en ligne ou le réseau total d'une entreprise en saturant le ou les ressources du système. C'est-à-dire la bande passante, l'espace de stockage, la capacité de traitement d'une base de données, les ressources de calcul des processeurs, la mémoire vive, …[7].

Figure 14: Attaque par Déni de service

Différente de l'attaque par déni de service, l'attaque par déni de service distribuée (DDos ou Distributed DoS en anglais) est une attaque de DoS émise depuis plusieurs origines distinctes (***Figure 14***). Ce type d'attaque est extrêmement complexe à bloquer, car il est souvent impossible de différencier une vraie requête d'une requête de DDos. L'attaque par DDos utilise très souvent une multitude de PC zombies (un ensemble de machine infecté) pour infecter tout le réseau. Et que les serveurs de messagerie sont les principales victimes des d'attaques de DDos.

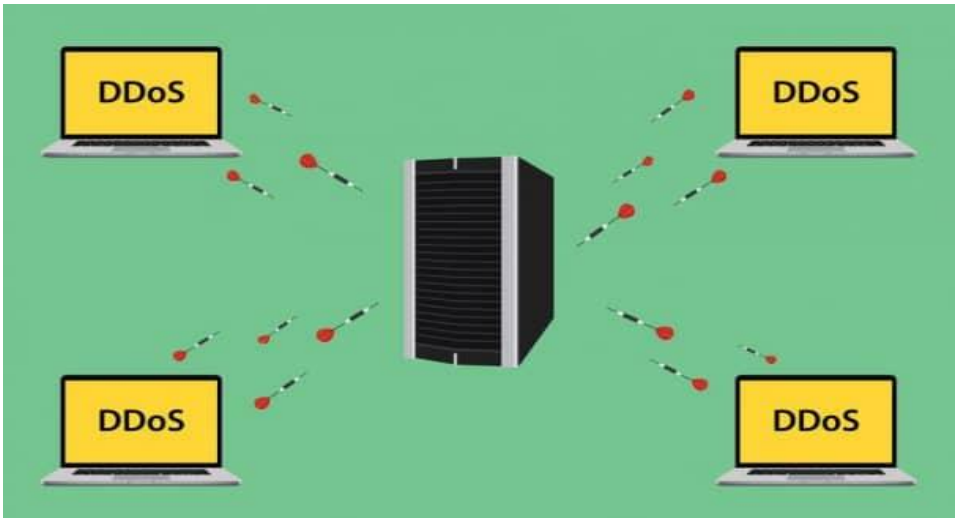

Figure 15 : Attaque par Déni De service Distribuée*[6]*

2.4.4 Attaques par des logiciels malveillants

Un logiciel malveillant (ou malware) désigne un logiciel destiné à nuire à un système informatique ou à un utilisateur. Une attaque par logiciel malveillant est capable d'infecter un ordinateur ou un appareil, et éventuellement tous les appareils avec lesquels ils communiquent. Il s'agit d'une expression générique qui englobe les logiciels espions, les chevaux de Troie, les vers et les virus informatiques.

2.4.4.1 Logiciels espions (spyware)

Un logiciel espion est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter des informations au niveau cette machine ou du système avant de les transmettre à d'autres ordinateurs ou systèmes. Il peut s'agir de dispositifs qui surveillent vos actions sur Internet ou encore d'outils d'espionnage très perfectionnés. Les logiciels espions violent la vie privée des utilisateurs, et peuvent aussi ralentir votre système et engorger le réseau de l'entreprise.

Les logiciels espions sont souvent inclus dans des logiciels gratuits et s'installent généralement à l'insu de l'utilisateur. Et ils ne sont généralement actifs qu'après redémarrage de l'ordinateur.

2.4.4.2 Cheval de troie

Un cheval de Troie est un programme qui a l'air utile mais qui contient également du code malveillant. Les acteurs malveillants les utilisent pour compromettre les hôtes ou un réseau. Les chevaux de Troie sont souvent fournis avec des programmes en ligne gratuits tels que des jeux informatiques et souvent sur les logiciels de publicités. Parfois des utilisateurs peu méfiants téléchargent et installent le jeu, ainsi que le cheval de Troie sans en rendre compte.

Il existe plusieurs types de cheval de Troie, comme illustré dans le tableau :

Type de cheval de Troie	Description
Accès à distance	Le cheval de Troie permet un accès à distance non autorisé
Envoie de données	Le cheval de Troie fournit à l'acteur de la menace des données sensibles, telles que des mots de passe
Destructeurs	Le cheval de Troie de corrompt ou supprime des fichiers
Procuration	Le cheval de Troie utilisera l'ordinateur de la victime comme périphérique source pour lancer des attaques et effectuer d'autres activités illégales
FTP	Le cheval de Troie active les services de transfert de fichiers non autorisés sur les terminaux
Désactivation du logiciel de Sécurité	Le cheval de Troie empêche les programmes antivirus ou les pare-feu de fonctionner
Déni de service (Dos)	Le cheval de Troie ralentit ou arrête l'activité du réseau
Enregistreur de frappe	Le cheval de Troie tente activement de voler des informations confidentielles, telles que des numéros de carte de crédit, en enregistrant les frappes de touches saisies dans un formulaire Web lors d'un achat en ligne.

Tableau 1 : Les types de cheval Troie

2.4.4.3 Vers informatiques

Un ver est un programme auto-répliquant qui se propage automatiquement sans action de l'utilisateur en exploitant les vulnérabilités des logiciels légitimes. Il utilise le réseau pour rechercher d'autres victimes présentant la même vulnérabilité. Et son intention, un ver est généralement de ralentir ou de perturber les opérations du réseau.

2.4.4.4 Virus informatiques

Le virus informatique est l'un des logiciels malveillants le plus couramment utilisé sur les attaques informatiques. Les virus nécessitent une action humaine pour se propager et infecter d'autres ordinateurs. Par exemple, un virus peut infecter un ordinateur lorsqu'une victime ouvre une pièce jointe à un e-mail, ouvre un fichier sur une clé USB ou télécharge un fichier.

Il se cache en s'attachant à un code informatique, un logiciel ou des documents sur l'ordinateur. Lorsqu'il est ouvert, le virus s'exécute et infecte l'ordinateur ou tout le réseau.

Les virus informatiques peuvent :

- Modifiez, corrompre, supprimez des fichiers ou effacez des lecteurs entiers ;
- Provoque des problèmes de démarrage de l'ordinateur et des applications corrompues ;
- Capturez et envoyez des informations sensibles aux acteurs de la menace ;
- Accédez aux comptes de messagerie et utilisez-les pour diffuser ;
- Rester en sommeil jusqu'à ce qu'il soit convoqué par l'acteur menaçant ;

Les virus, les chevaux de Troie, les vers, … ne sont pas les seuls logiciels malveillants utilisés par les acteurs malveillants. Il existe de nombreux autres types de logiciels malveillants conçus à des fins spécifiques.

2.4.5 Attaque d'ingénierie sociale

L'ingénierie sociale est une attaque d'accès qui tente de manipuler des individus pour qu'ils effectuent des actions ou divulguent des informations confidentielles.

Certaines techniques d'ingénierie sociale sont réalisées en personne tandis que d'autres peuvent utiliser le téléphone ou Internet. Les ingénieurs sociaux (acteur de menace) comptent souvent sur la volonté des gens d'être utiles. Ils s'attaquent également aux faiblesses des gens. Par exemple, un acteur malveillant pourrait appeler un employé autorisé avec un problème urgent nécessitant un accès immédiat au réseau. L'acteur de la menace peut faire appel à la vanité de l'employé, invoquer l'autorité en utilisant des techniques de suppression de nom ou faire appel à la cupidité[3] de l'employé. On prend quelques exemples d'attaques d'ingénierie social comme :

[3] **Cupidité :** Désir immodéré de l'argent et des richesses.

2.4.5.1 Spam (courrier indésirable)

Également connu sous le nom de courrier indésirable, il s'agit d'un courrier électronique non sollicité qui contient souvent des liens nuisibles, des logiciels malveillants ou du contenu trompeur.

2.4.5.2 Talonnage(Tailgating)

Un talonnage est un type d'attaque d'ingénierie sociale qui consiste à accéder dans un endroit réservé au personnel de l'entreprise dont tu n'as fait pas parti. C'est-à-dire lorsque qu'une personne malveillante entre dans l'entreprise et suit rapidement une personne autorisée dans un endroit sécurisé pour accéder à une zone sécurisée sans problème.

2.4.5.3 Plongée en Benne (Dumpster diving)

C'est un type d'attaques très fréquentes, dont les personnelles de la sécurité ignorent. Cette attaque permet au acteurs de la menace de fouiller dans les poubelles pour recueillir ou de découvrir des documents confidentiels pour porter préjudice l'entreprise. Don pour éviter ces types d'attaques dans les entreprises, il faut prendre toutes ces précautions avant de les mettre dans des poubelles.

Donc en sécurité informatique, pour gardes en toute sécurité les données, les informations qui sont au repos ou qui transitent dans le réseau ; des services de sécurités ont été mise en place.

2.5 Les services de sécurité en informatique

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources logiciels et matériels d'un réseau d'entreprise, d'un parc informatique ou d'une organisation sont uniquement utilisés dans le cadre prévu et aux ayants droits. Pour son application, des services de sécurités ont été proposés comme :

2.5.1 La confidentialité

La confidentialité est un service de sécurité qui assure que les données échangées dans le réseau ont été lues seulement par les personnes autorisées. Elle rend l'information inintelligible à d'autres personnes que les seules personnes de la transaction. C'est-à-dire l'émetteur et le récepteur sont les seuls à comprendre le message. La confidentialité est proposée par certaines mécanismes de sécurité comme les deux chiffrements.

Le chiffrement symétrique nécessite une échange sûr préalable de la clé entre les entités **M. FAYE** et **DIENE (*Figure 16*).**

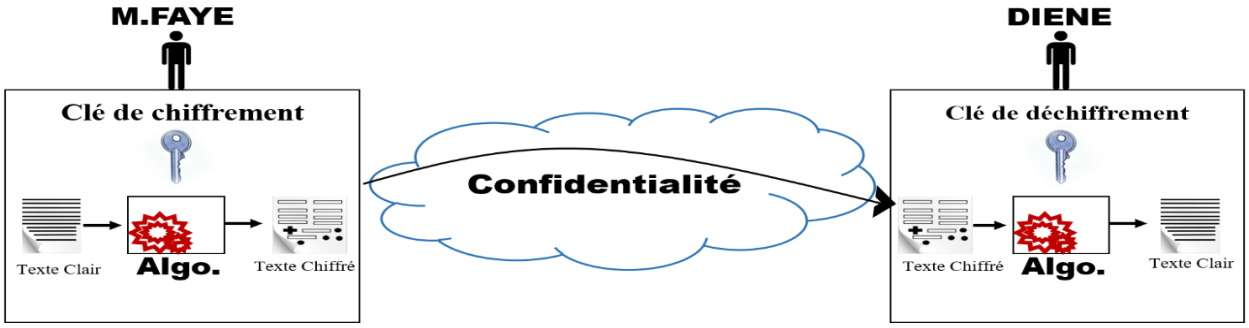

Figure 16 : La confidentialité avec le chiffrement symétrique

Donc dans ce type de chiffrement, la confidentialité ne peut pas être employée pour confirmer ni l'intégrité ni l'authenticité.

Mais elle est aussi proposée par l'autre type de chiffrement qui est le chiffrement asymétrique (**Figure 17**).

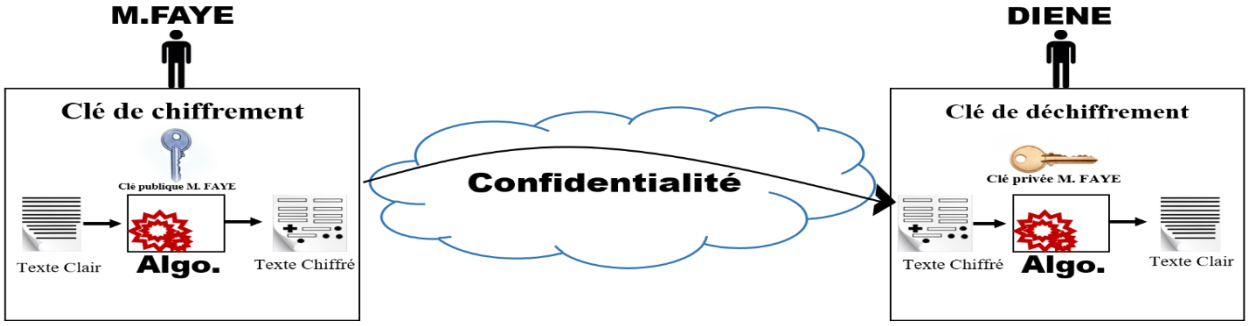

Figure 17 : la confidentialité avec le chiffrement asymétrique

2.5.2 L'intégrité

L'intégrité consiste à assures aux utilisateurs qui communiquent que leurs données n'ont pas été indûment modifiées au cours de la transmission dans le réseau. C'est-à-dire garantir que les données sont bien celles que l'on croit être.

2.5.3 La disponibilité

La disponibilité, permet aux utilisateurs d'un réseau informatique d'utiliser les services du réseau en cas de besoin. Son objectif principal est de garantir l'accès à un service, à une application, au réseau ou à une donnée et que cela soit possible en tout temps, afin de garantir le bon fonctionnement du système d'information.

2.5.4 L'authentification

L'authentification consiste à s'assurer que seules les personnes dûment autorisées aient accès aux données et/ou aux ressources souhaitées. Son but est d'identifier de manière unique et sans équivoque qu'un individu est bien celui qu'il prétend être. L'authentification consiste donc à

demander à un utilisateur de prouver son identité en fournissant un mot de passe ou des données biométriques par exemple (**Figure 18**).

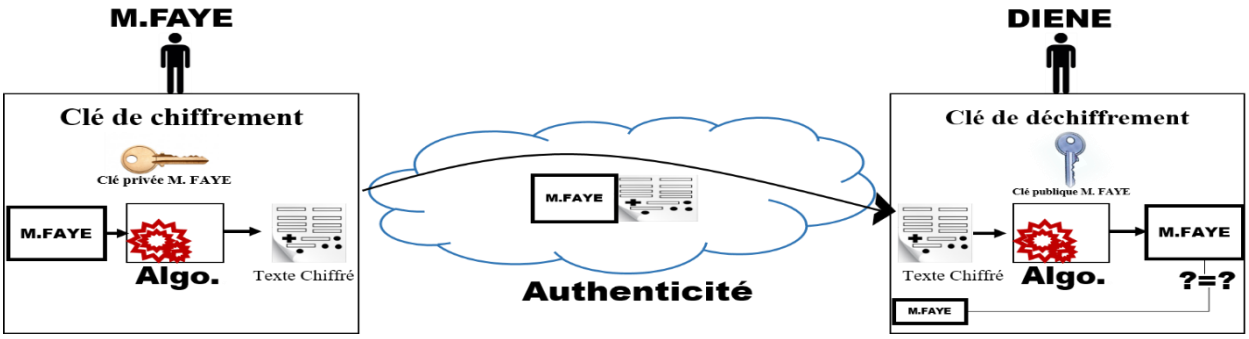

Figure 18 : Authentification

2.5.5 La non-répudiation

La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction. Elle a pour objectif de s'assurer que l'émetteur d'une information ne puisse pas nier qu'il est bien à l'origine de celle-ci. Par exemple, la signature d'un email, d'un document ou d'un certificat. Seule la personne possédant la clé privée correspondant à la signature, déposée sur un email, serait en mesure d'émettre cet email signé. Il ne lui est donc pas possible de nier en être l'émetteur, sauf dans le cas où il aurait partagé cette clé privée (censée être personnelle) à un tiers.

2.6 Les mécanismes de sécurité

2.6.1 La cryptographie

La cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique (protéger des messages). Les premières traces de la cryptographie remontent au XVIème avant J-C. Depuis cette époque, la cryptographie n'a fait qu'évoluer. Cette évolution de la cryptographie a donné naissance à deux types de cryptages : le chiffrement symétrique (clé secrète) et le chiffrement asymétrique (clé publique).

2.6.1.1 La cryptographie symétrique

La cryptographie symétrique (ou cryptographie à clé secrète) est la forme la plus ancienne de la cryptographie mais plus rapide que les autres types de chiffrements.

2.6.1.1.1 Objectifs

Ce chiffrement fonctionne en principe avec une paire de clé secrète, appelé parfois clé pré-partagée pour chiffrer et déchiffrer les données.

2.6.1.1.2 Fonctionnement

Dans ce cas de chiffrement, le principe est le suivant : L'émetteur du message chiffre les données grâce à une clé. Cette clé est généralement une chaine de caractère. Le message est chiffré et sans la clé il est quasi impossible de retrouver le message d'origine. L'émetteur doit donc transmettre la clé aux personnes à qui il désir transmettre le message s'il veut que son message puisse être lu (**Figure 19**). Les algorithmes symétriques utilisent la même clé pour chiffrer et déchiffrer le texte en claire et que ces algorithmes de chiffrement sont plus simples et nécessite moins de calcul.

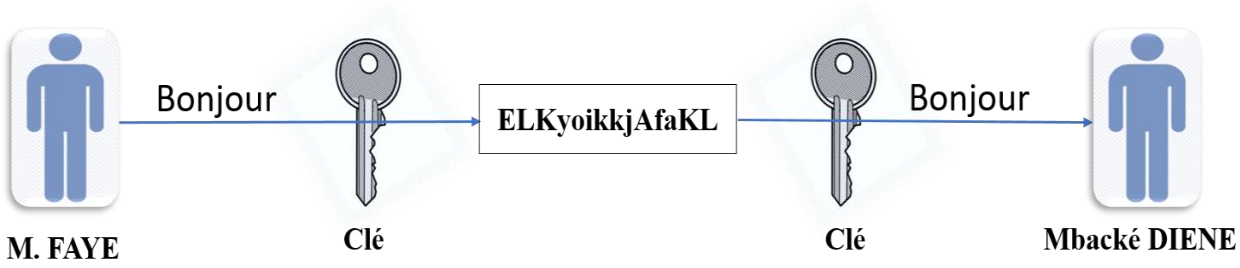

Figure 19 : Schéma de fonctionnement de la cryptographie Symétrique

Pour le chiffrement symétrique, il en existe deux méthodes de chiffrement à savoir : le chiffrement de flux (ou chiffrement par flot) et le chiffrement par blocs.

- **Le chiffrement de flux (ou chiffrement par flot) :** les algorithmes basés sur le principe de chiffrement de flux chiffrent ou déchiffrent un message à la volée. Le chiffrement de flux chiffre du texte en clair, à raison d'un bit à la fois. Ce chiffrement correspond à un chiffrement par bloc avec taille de bloc d'un seul bit. Avec le chiffrement de flux, la transformation de ces plus petites unités de texte dépend de leur position dans le processus de chiffrement. Le chiffrement de flux peut se révéler beaucoup plus rapide que le chiffrement par bloc.

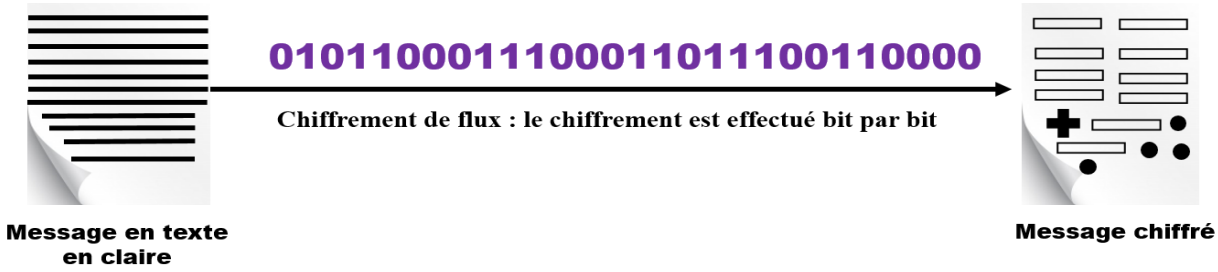

Figure 20 : Chiffrement par flux

- **Le chiffrement par blocs :** il fonctionne différemment que le chiffrement précédent. Au lieu de prendre les bits un par un, les messages sont découpés en blocs (la taille des blocs dépend des clés). Le chiffrement par bloc transforme un bloc de texte en claire

d'une longueur fixe en bloc de texte crypté de 64 bits ou 128 bits. La taille du bloc correspond à la quantité de données chiffrées à un moment donné. Pour déchiffrer ce texte crypté, appliquons la transformation inverse ou bloc de texte crypté en utilisant la même clé secrète. En générale, le chiffrement par bloc génère des données de sorties plus volumineuses que les données d'entrées, car le texte chiffré doit être un multiple de la taille du bloc. On peut prendre l'exemple de l'algorithme DES (Data Encryption Standard), qui est un algorithme symétrique qui chiffre les blocs en segment de 64bits à l'aide d'une clé de 56bits. Pour ce faire, l'algorithme prélève les données par segment (des segments de 8bits, par exemple) ; jusqu' à ce que tout le bloc soit rempli. Si la quantité de données d'entrée est inférieur à un bloc complet, l'algorithme ajoute des données artificielles, ou de blancs jusqu' à ce que les 64bits soient utilisés.

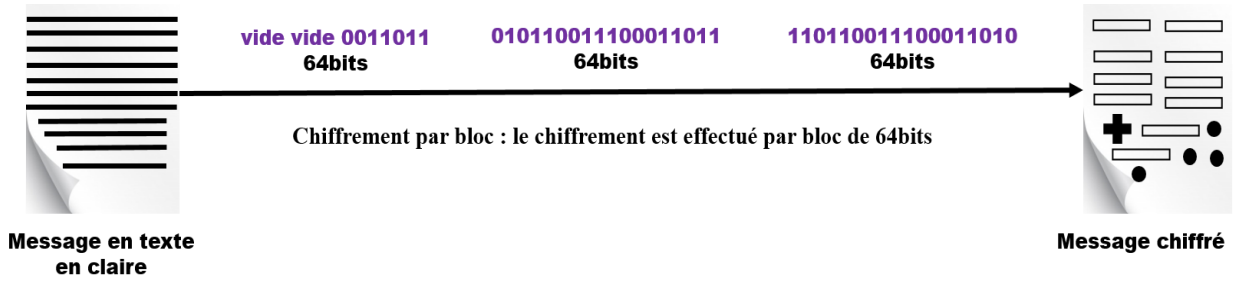

Figure 21 : Chiffrement par bloc

2.6.1.1.3 Algorithmes de chiffrement symétrique

Pour faire le chiffrement symétrique, il y' a différents algorithmes de chiffrement symétrique. Parmi ces algorithmes de chiffrement, on peut en citer :

- **3DES (Triple DES) : DES (Digital Encryption Standard) ;**
- **DES (Data Encryption Standard) ;**
- **IDEA (International Data Encryption Algorithme) ;**
- **AES (Advanced Encryption Standard) ;**
- **Skipjack (développé par NSA) ;**
- **Blowfish ;**
- **Twofish, ….**

2.6.1.2 La cryptographie asymétrique

La cryptographie asymétrique ou cryptographie à clé publique fonctionne de façon totalement différente celle de la cryptographie symétrique. Si on peut comparer la cryptographie symétrique à un coffre-fort auquel seul les personnes possédant la clé peuvent accéder, la cryptographie asymétrique pourrait être comparé à une boite aux lettres dans laquelle on peut

déposer des informations, et seule la personne possédant la clé peut accéder au contenu de la boite.

2.6.1.2.1 Objectifs

Dans un système de chiffrement asymétrique (ou système de chiffrement à clés publiques), les clés existent par paires (le terme de bi-clés est généralement employé) :

- **Une clé publique pour le chiffrement**
- **Une clé secrète pour le déchiffrement**

2.6.1.2.2 Fonctionnement

Dans un système de chiffrement à clé publique, un utilisateur peut chiffrer un message à l'aide de la clé publique du destinataire, qui est le seul à pouvoir le déchiffrer au moyen de sa clé privée (**Figure 22**). Les nombres premiers sont les éléments clé pour rendre les algorithmes de cryptographie asymétrique indéchiffrable (ou presque). C'est sur cette difficulté de factorisation que se reposent les algorithmes asymétriques.

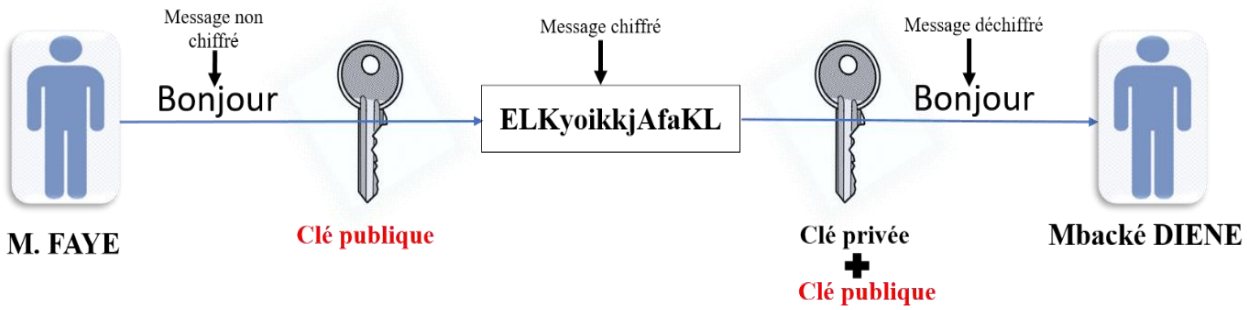

Figure 22 : Schéma de Fonctionnement de la cryptographie asymétrique

2.6.1.2.3 Algorithmes de chiffrement asymétrique

Le chiffrement asymétrique a des algorithmes de chiffrements aussi comme le chiffrement symétrique, qui sont plus complexe en termes de calcule et demandent beaucoup de ressources. Les algorithmes sont les suivants :

- **RSA (Revest-Shamir-Adleman) ;**
- **Diffie-Hellman ;**
- **ElGamal ;**
- **Cryptographie sur les courbes elliptiques (ECC) ;**

2.6.2 Le hachage

Comme la cryptographie, le hachage est un mécanisme de sécurité qui vérifie l'intégrité des informations ou des données envoyées dans un réseau. Cette vérification de l'intégrité des données se fait via des fonctions appelées fonctions de hachage. Une fonction de hachage est une méthode permettant de caractériser une information ou une donnée. En faisant subir une

suite de traitements reproductibles à une entrée, elle génère une empreinte servant à identifier la donnée initiale. Elle prend donc en entrée un message de taille quelconque, applique une série de transformations et réduit ces données. Et on obtient à la sortie une chaîne de caractères hexadécimaux, le condensé, qui résume en quelque sorte le fichier.

Cette sortie a une taille fixe varie selon les algorithmes de hachages :

- **MD5** : (Message Digest #5) est une fonction de hachage très répandue qui produit un condensé de 128 bits ;
- **SHA-1 :** (Secure Hash Algorithm) crée par NIST, est une autre fonction de hachage qui renvoie un résumé de 160 bits ;
- **SHA-256**, qui génère un hachage d'une longueur fixe de 256 bits ;

De manière générale, une fonction de hachage est une fonction mathématique qui, à partir d'un texte fixe quelconque, génère une empreinte. Donc toute modification du texte d'entré entraîne la modification de l'empreinte.

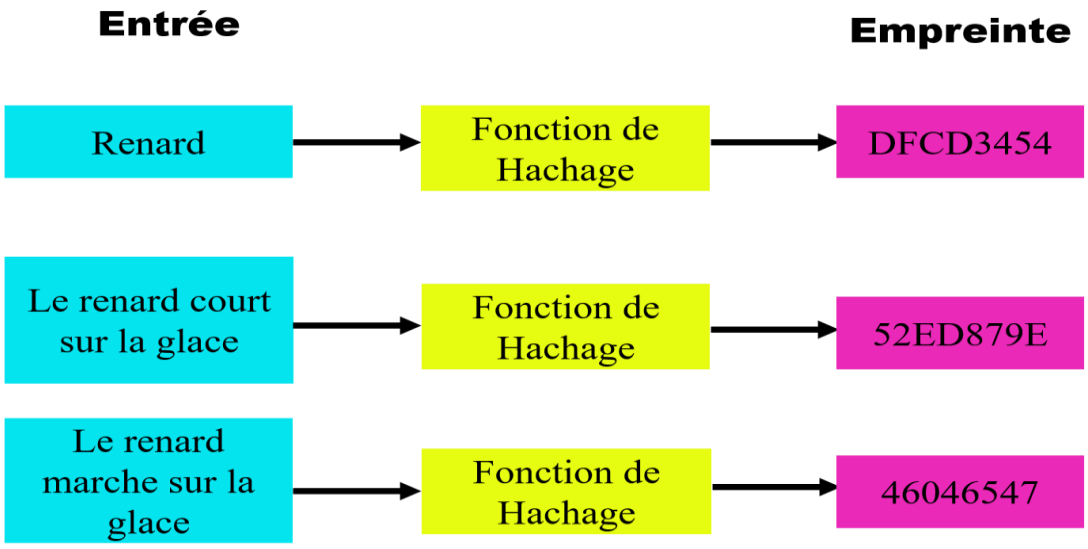

Figure 23 : Fonction de hachage

2.6.3 La signature numérique

La signature numérique est un mécanisme de sécurité permettant de garantir l'intégrité, la non-répudiation d'un document électronique et d'en authentifier l'auteur. Cette authentification du signataire (auteur) se fait, par utilisation des signatures numériques basée sur des certificats. Ce certificat du signataire est lié au document par cryptage c'est à dire une clé privée dont le signataire ou l'auteur du document est le seul détenteur. Durant le processus de validation, la clé publique correspondante à la clé privée est extraite de la signature et permet à la fois d'authentifier l'identité du signataire à l'aide de l'autorité de certification à qui on a confiance et de confirmer qu'aucune modification n'a été apportée au document depuis sa signature.

Dans une signature numérique, on assiste toujours la combinaison de la cryptographie asymétrique et les fonctions de hachages. Donc elle implique le respect strict de certaines conditions :

- **Authentique** : l'identité du signataire doit pouvoir être retrouvée de manière certaine ;
- **Infalsifiable** : la signature ne peut pas être falsifiée. Quelqu'un ne peut se faire passer pour un autre ;
- **Non réutilisable** : la signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document ;
- **Inaltérable** : un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier ;

  Irrévocable : la personne qui a signé ne peut le nier ;

Comme illustré dans la figure suivante, une signature numérique suis ce processus pour donner les données signées numériquement qui seront par leur tour vérifiées si les données en entrée ne sont pas modifiées lors de la sortie.

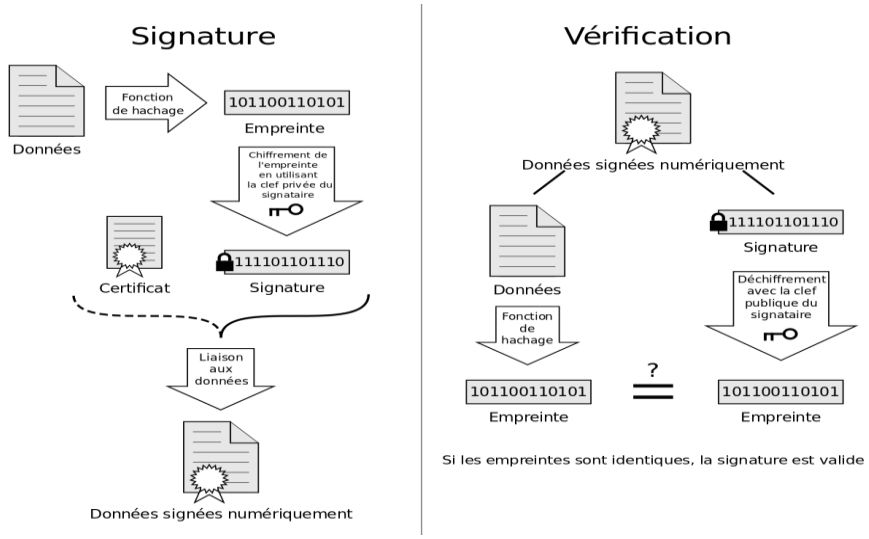

Figure 24 : Signature Numérique

Conclusion

Dans ce chapitre, nous avons assimilé les aspects de la sécurité informatique qui nous a permis de comprendre les méthodes pour assurer la sécurité des données en circulation. En sécurité informatique, si une vulnérabilité est détectée alors il court des risques. Ces derniers vont aboutir à des attaques, pour prévenir ces attaques il faut des mécanismes de sécurité comme la cryptographie. Comme nous connaissons les étapes de la sécurité informatique avec ses mécanismes proposés, nous allons étudier dans le chapitre suivant de la sécurité des architectures réseaux.

Chapitre III :
Sécurité des architectures réseaux

Introduction

L'architecture est la façon dont les composants d'une chose s'organisent. S'agissant d'un système d'information en réseau, l'objectif est d'organiser et d'exploiter ce système de manière à pouvoir contrôler le système et à détecter des activités inattendues, indésirables et malveillantes. Pour une telle protection, il y a des outils adéquats et des mécanismes pour protéger les architectures réseaux. Ainsi dans ce chapitre, vous allons parler d'abord de l'architecture et de la topologie de réseaux et enfin parlé des architectures sécurisées de réseaux.

3.1 Architecture et topologies des réseaux

3.1.1 Les réseaux Locaux

Un réseau local ou LAN (Local Area Network) est un système de communication permettant d'interconnecter des ordinateurs et d'autres équipements informatiques dans un domaine géographiquement limité. Il utilise des supports physiques de types paires filaires, câble coaxial, fibre optique, ondes électromagnétiques ou autres. Les dispositifs reliés entre eux sont de tous types : ordinateurs, imprimantes, modems, switch niveau 2, serveurs, ... Ils permettent de :

- Rendre disponibles à tous, les équipements ne pouvant pas être affectés à chaque poste de travail (imprimantes, modems, serveurs...)
- Centraliser les applications disponibles pour l'entreprise afin d'en faciliter l'utilisation et la mise à jour.
- Centraliser les données sur des dispositifs sécurisés aussi bien au niveau de l'accès qu'au niveau de la fiabilité.
- Permettre l'interconnexion de stations de travail d'origines différentes et de systèmes d'exploitation différents (PC, MAC, Stations Unix, ...).
- Permettre l'usage de bases de données centralisées (SGBD).
- Faciliter la circulation des informations (transferts de fichiers, messagerie, images...).
- Assurer l'interconnexion rationnelle avec des équipements distants.

3.1.1.1 Les caractéristiques des réseaux locaux

Sur le plan physique, les principales caractéristiques permettant de définir un réseau local dans une entreprise sont :

- **La Topologie**

La topologie des réseaux informatiques définie la manière dont sont interconnectées les machines. On distingue en informatique deux types de topologies des réseaux : la topologie physique et la topologie logique.

- **La topologie physique (Architecture physique)** : La topologie physique définit la manière dont le câblage réseau interconnecte les nœuds entre eux.
- **La topologie logique (Architecture Logique)** : La topologie logique définit la manière dont circulent les informations sur le réseau. Les informations véhiculées sur un réseau local le sont en utilisant des bits envoyés en mode série sur un support.

En topologie des réseaux informatiques, il existe également d'autres types de topologies physiques : la topologie en bus, la topologie en étoile, la topologie maillée, la topologie en arbre et la topologie en anneau.

- **La Méthode d'accès au Support**

En informatique, chaque type de réseau local possède une méthode d'accès au support qui lui est propre. Elle détermine la manière dont chaque nœud peut envoyer des trames sur le réseau sans créer de collision entre les trames émises dans le réseau. Elle est souvent conditionnée par la topologie utilisée. Ainsi, sur un bus série, 2 stations ne peuvent émettre en même temps sans provoquer une collision entre les 2 signaux électriques émis. D'où la nécessité de définir une politique d'accès au support.

- **La Technique de transmission**

Sur les réseaux locaux ; on a principalement deux méthodes de transmission possibles :

- La méthode Large Bande (Signal Analogique)
- La méthode Bande de Base (Signal Numérique)

En pratiques, seule cette dernière est vraiment utilisée. Les données sont envoyées en mode série et sous forme numérique sur le support de transmission.

Pour des raisons tenant à la synchronisation du récepteur et à la largeur de bande du signal à transmettre, les données sont toujours envoyées de façon codée sur le support

- **Les Supports de transmissions**

Les supports de transmission sont nombreux. Parmi ceux-ci, on distingue : les supports métalliques, non métalliques et immatériels. Les supports métalliques, comme les paires torsadées et les câbles coaxiaux, sont les plus anciens et les plus largement utilisés ; ils transportent des courants électriques. Les supports de verre ou de plastique, comme les fibres optiques, transmettent la lumière, tandis que les supports immatériels des communications sans fil propagent des ondes électromagnétiques et sont en plein essor.

Cette partie du **chapitre 3** est développée au niveau du **chapitre 1** voire **1.1 Les technologies utilisées.**

o Caractéristiques globales des supports de transmission

Quelle que soit la nature du support, le signal désigne le courant, la lumière ou l'onde électromagnétique transmis. Certaines caractéristiques des supports (bande passante, sensibilité aux bruits, limites des débits possibles) en perturbent la transmission. Leur connaissance est nécessaire pour fabriquer de « bons » signaux, c'est-à-dire les mieux adaptés aux supports utilisés.

➢ Bande passante

La bande passante est la bande de fréquences dans laquelle les signaux appliqués à l'entrée du support de transmission ont une puissance de sortie supérieure à un seuil donné après traversée du support. Le seuil fixé correspond à un rapport déterminé entre la puissance du signal d'entrée et la puissance du signal trouvé à la sortie (voir **Figure 25**). En général, on caractérise un support par sa bande passante à 3 dB (décibels), c'est-à-dire par la plage de fréquences à l'intérieur de laquelle la puissance de sortie est, au pire, divisée par deux. Si on note Ps la puissance de sortie et Pe la puissance d'entrée, l'affaiblissement A en décibels est donné par la formule :

A = 10 × log10 Ps/Pe ; pour Ps /Pe= 0,5, on trouve : 10 × log10 Ps/Pe= 3 dB

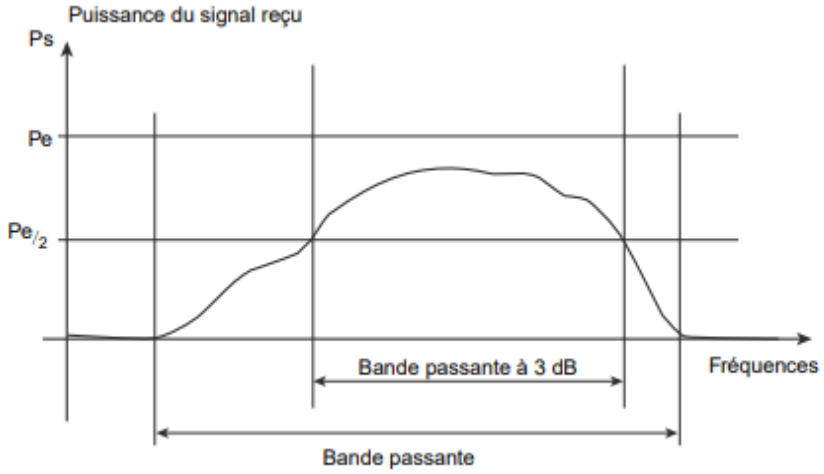

Figure 25 : Notion de la bande passante

➢ Bruits et distorsions

Les supports de transmission déforment les signaux qu'ils transportent, même lorsque leurs fréquences sont adaptées, comme l'illustre la figure 20. Diverses sources de bruit perturbent les signaux : parasites, phénomènes de diaphonie… Certaines perturbations de l'environnement introduisent également des bruits (foudre, champs électromagnétiques dans des ateliers…).

Par ailleurs, les supports affaiblissent et retardent les signaux. La distance est un facteur d'affaiblissement, très important pour les liaisons par satellite. Ces déformations, appelées

distorsions, sont gênantes pour la bonne reconnaissance des signaux en sortie, d'autant qu'elles varient avec la fréquence et la phase des signaux émis.

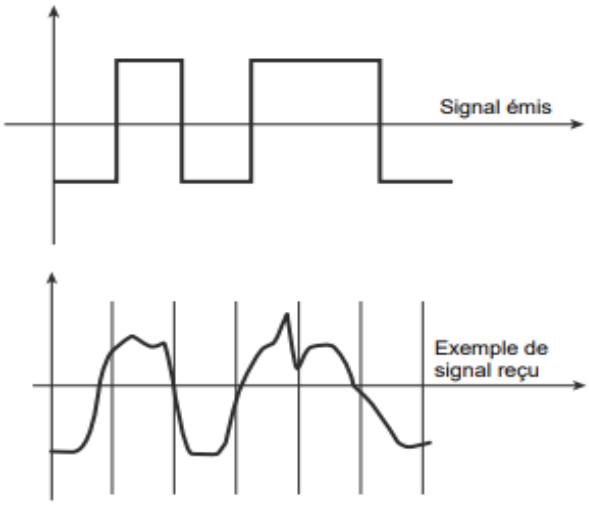

Figure 26 : Signal émis et exemple de signal reçu

- **Le Débit Binaire**

Le débit binaire est une mesure utilisée pour déterminer la quantité de données transmises dans un intervalle de temps fixé. Cette mesure sert principalement pour des transmissions audio ou vidéo. Par exemple, lorsque vous regardez une vidéo sur YouTube ou écoutez une émission de radio, les informations du fichier sont lues et interprétées par l'ordinateur. La vitesse à laquelle ces informations sont traitées et appelée le débit binaire. Plus le volume de données transmises par seconde est élevé, meilleure est la qualité finale de l'image ou du son.

D'ailleurs, pour une bonne gestion des réseaux locaux d'une entreprise en matière de sécurité, il est primordial d'intégrer les vlan dans le réseau pour regrouper des machines de façon logique et non physique.

3.1.2 Les VLANS

3.1.2.1 Qu'est-ce qu'un réseau virtuel ? VLAN

De nos jours, les réseaux physiques sont généralement basés sur un ou plusieurs commutateur(s) (« switch(es) »), des appareils gérant le trafic de données entre les équipements. Pour ce faire, tous les câbles réseau sont raccordés au commutateur permettant ainsi à différents ordinateurs de communiquer. Il est alors possible que ces commutateurs relient entre eux des centaines d'appareils tout en assurant une communication relativement fluide. Il peut toutefois s'avérer pertinent de fragmenter d'aussi vastes réseaux sans pour autant changer quoi se soit à l'installation physique en utilisant la technologie des VLAN.

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

Donc on peut définir un réseau local virtuel comme étant un regroupement virtuel d'au moins deux périphériques dans un réseau. Ce regroupement virtuel des machines peut s'étendre au-delà de plusieurs commutateurs. Les périphériques sont regroupés sur la base d'un certain nombre de facteurs suivant la configuration du réseau. Le VLAN permet de gérer et de maintenir plusieurs réseaux locaux (LAN), soit séparés par du routage, sur une seule et même infrastructure physique commutée.

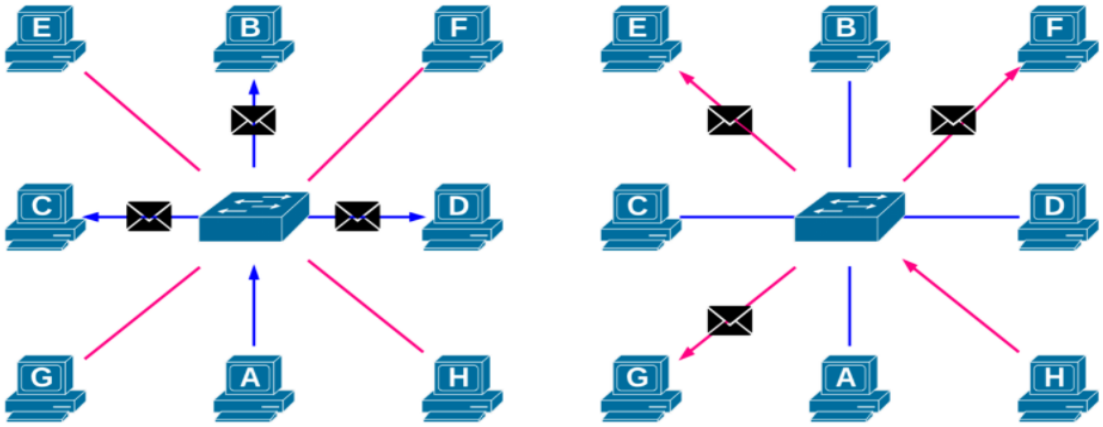

Figure 27 : Réseau Local Virtuel (VLAN)

Comme illustré par la Figure 1, les hôtes A, B, C et D appartiennent au VLAN 66 et les hôtes E, F, G et H appartiennent au VLAN 33. Donc la Figure 1 illustre le trafic de broadcast d'A à D et de E à H.

Concrètement, les ports du commutateur prennent un identifiant VLAN. Cet identifiant logique définit l'étendue du domaine de diffusion : le trafic de diffusion ne sera transféré que sur les ports ayant le même identifiant. Autrement dit, par exemple, le trafic de diffusion venant d'un port appartenant au VLAN 66 ne se sera transféré que sur les ports ayant pour attribution le VLAN 66.

3.1.2.2 Pourquoi créer un réseau virtuel ?

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLAN) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, adressage, ...).

Egalement il existe d'autres intérêts qui nous pousse à avoir des VLAN dans une entreprise. Par contre, il n'est pas nécessaire d'avoir des vlan si on a une petite entreprise avec peu de fonctionnalités. Parmi ces intérêts on peut citer :

- Améliorer la gestion du réseau

- Optimiser la bande passante
- Séparer les flux
- Fragmentation : réduire la taille d'un domaine de broadcast
- Sécurité : permet de créer un ensemble logique isolé pour améliorer la sécurité. Le seul moyen de communiquer entre des machines appartenant à des VLAN différents est alors de passer par un routeur.

3.1.2.3 Principes de fonctionnement des VLANs

Dans le principe de fonctionnement des VLAN, on distingue en général deux (2) méthodes pour regrouper les utilisateurs connectés dans le réseau local en VLAN :

- Le filtrage des trames
  - Un examen de chaque trame permet d'élaborer pour chaque commutateur une table de filtrage afin de permettre de prendre les décisions appropriées.
  - Cela suppose qu'une table de filtrage par commutateur, a donc des temps de mise en jour lents ainsi que des problèmes d'évolutivité.
- L'identification des Trames
  - Chaque trame dispose d'un code d'identification VLAN (TCI=Tag Control Information) définit par la norme IEEE 802.1q
  - L'identificateur est utilisé lors du transfert des paquets sur le réseau.
  - Il est enlevé lorsque le paquet quitte le réseau pour atteindre les hôtes ou les routeurs.

Cette dernière méthode est la plus utilisée aujourd'hui sur les vlan. Elle est identifiée de manière claire au niveau des commutateurs par le support de cette norme.

Exemple de Trame 802.1q :

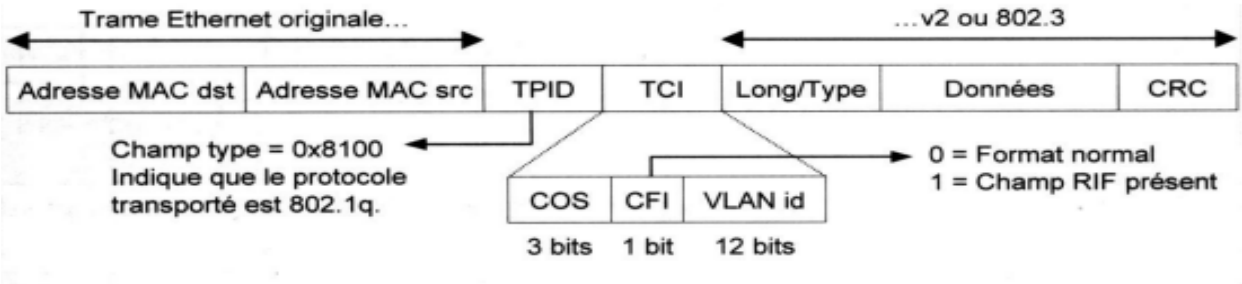

Figure 28:Trame 802.1q

TPID = Tag Protocol Identifier : correspond au champ type d'une trame Ethernet v2

TCI = Tag Control Information : le label 802.1q inséré dans la trame Ethernet v2

COS = Class of Service : utilisé par la norme 802.1q

CFI = Common Format Identifier : permet de transporter le champ RIF dans le cas d'un

tunnel source routing.

VLAN id = numéro de VLAN (4 096 possibilité)

Donc l'objectif fondamental d'un VLAN est de rendre la fonction d'un LAN indépendante de l'architecture physique.

De plus la fonctionnalité des VLAN peut être étendues sur des ports du commutateur distant à travers toute l'architecture. Dans ce cas, les commutateurs devront transporter entre eux du trafic appartenant à plusieurs VLAN sur une ou plusieurs liaisons spécifiques, comme les liaisons Trunk ou liaisons d'agrégation.

3.1.2.4 TRUNK ou liaison d'agrégation

Un trunk ou liaison d'agrégation est un lien entre deux équipements, le plus souvent entre deux switch, configuré de telle sorte que l'on peut y faire circuler des trames Ethernet modifiées comportant des informations relatives au VLAN sur lequel elles transitent.

Le but ici est que le trafic du VLAN 33 de gauche puisse circuler sur le VLAN 33 de droite et idem pour le VLAN 66. Afin que cela soit possible, il faut configurer la liaison entre les deux switches en « trunk » … ou plus précisément configurer une encapsulation (**3.1.2.5**) des trames lorsqu'elles transitent sur le lien de sorte que le switch qui la reçoit peut ensuite la relayer dans le bon VLAN.

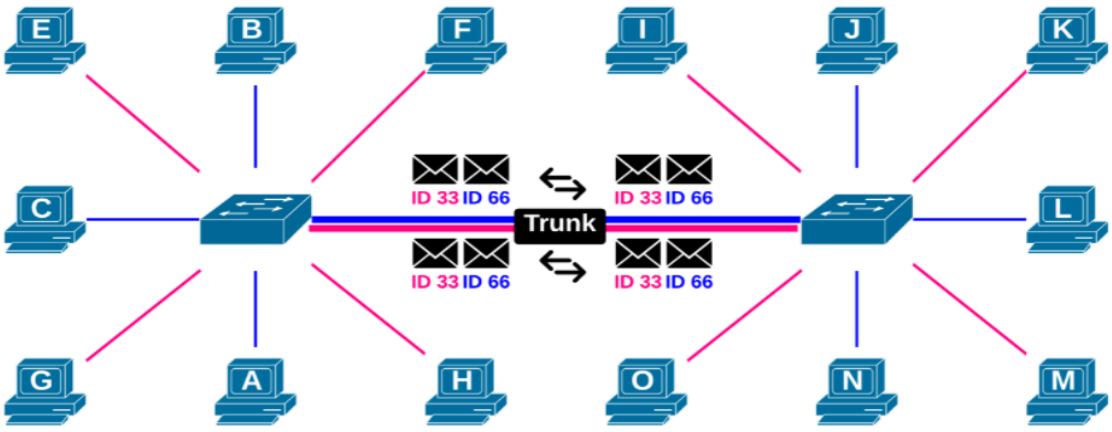

Figure 29 : Trunk ou Liaison d'agrégation

Les machine **A, B, C, J, L** et **N** appartiennent au **VLAN 66 ;** les machines **E, F, G, H, I, K L, M** et appartiennent au **VLAN 33.**

Les commutateurs isolent toujours le trafic entre les VLANs distincts mais transfèrent le trafic de plusieurs VLANs sur une liaison Trunk ou liaison d'agrégation.

Mais les ports d'une liaison qui agrègent le trafic de plusieurs VLANs s'appellent un "Trunk" chez le constructeur Cisco Systems et "liaison d'agrégation" chez d'autres. Sur ce type de liaison, le commutateur ajoute des champs supplémentaires dans ou autour de la trame Ethernet.

Ils servent notamment à distinguer le trafic de VLANs différents car ils contiennent entre autres le numéro d'identification du VLAN (illustré dans l'exemple de trame 802.1q).

Une liaison "Trunk" transporte les trames de plusieurs VLANs. La liaison doit être dimensionnée avec des capacités supérieures (bande passante) à celles des hôtes qui placent du trafic. Enfin, sauf exception, une liaison "Trunk" se monte entre des ports de commutateurs.

3.1.2.5 Encapsulation VLAN

Lorsqu'un port de commutateur est configuré pour fonctionner comme un port de jonction, il ajoute des balises d'identification uniques, des balises 802.1Q ou des balises Inter-Switch Link (ISL) aux trames lorsqu'elles se déplacent entre les commutateurs.

La norme IEEE 802.1Q, souvent appelé DOT1Q ou 1Q, est la norme de mise en réseau qui prend en charge les réseaux locaux virtuels (VLAN) sur un réseau Ethernet IEEE 802.3. Il s'agit de la méthode d'encapsulation la plus utilisée pour le balisage VLAN. Mais la norme IEEE 802.3 est une norme qui spécifie les caractéristiques de la couche physique et de la couche MAC (Media Access Control) pour les connexions Ethernet filaires, généralement appelées LAN. Elle est également appelée norme Ethernet.

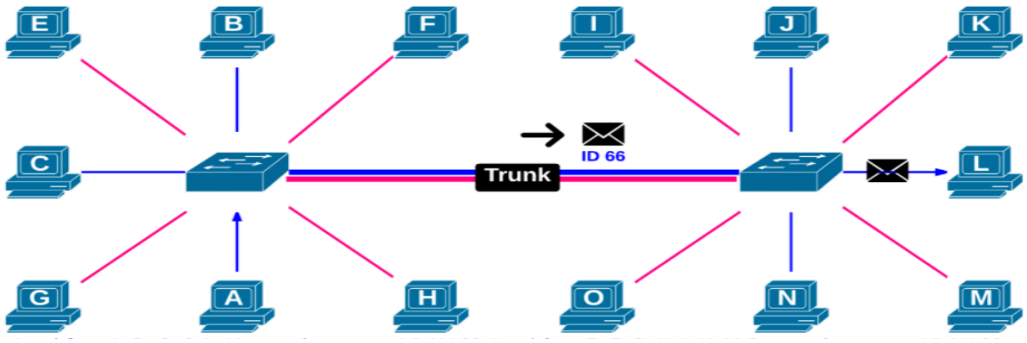

Figure 30 : Encapsulation 802.1q

Les machine **A, B, C, J, L** et **N** appartiennent **au VLAN 66 ;** les machines **E, F, G, H, I, K L, M** et appartiennent au **VLAN 33.**

La machine A veut joindre la machine L connecté à un commutateur distant.

La machine A veut joindre la machine L connecté à un commutateur distant. Les commutateurs (switchs) sont interconnectés par une "liaison d'agrégation" ou "Trunk". La trame sera étiquetée (**voir exemple de trame 802.1q**) seulement si elle quitte le commutateur sur un port qui connecte une "liaison d'agrégation" ou "Trunk" (voir **Figure 29**). Lors de la livraison locale de la trame à la station destinataire, elle sort du port du commutateur de destination sans étiquette.

3.1.2.6 Routage inter-VLAN

Chaque VLAN est un domaine de broadcast unique. Les ordinateurs sur des VLAN séparés sont, par défaut, incapables de communiquer. Pour autoriser une communication entre vlan, il faut faire du routage inter-VLAN. Ce routage est faisable avec un périphérique de couche 3. Par exemple un routeur ou un switch de niveau 3. Pour faciliter le routage inter-VLAN, il faut soit utiliser un routeur soit utiliser un switch de niveau 3, car ces interfaces peuvent être connectées à des VLAN séparés.

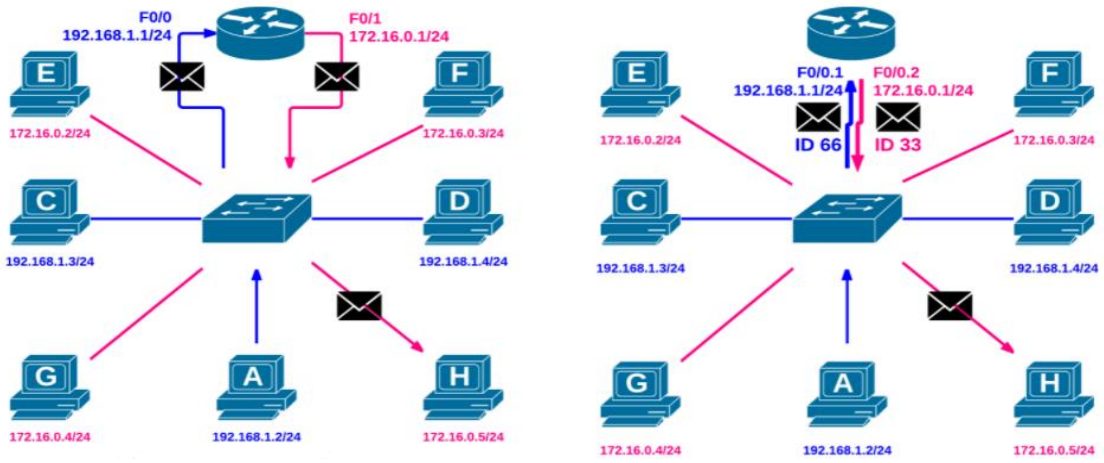

Figure 31 : Routage Inter-VLAN

Les machine **A, C** et **D** appartiennent au **VLAN 66 ;** les machines **E, F, G** et **H** appartiennent au **VLAN 33.**

Dans cet exemple, une seule interface du routeur est nécessaire. Elle sera configurée en mode "trunk" en créant pour chaque VLAN une sous-interface logique différente. Et que, l'interface physique ne prend pas d'adresse IP.

3.1.2.7 Les différents niveaux des VLAN

Afin d'identifier les différents VLAN dans un réseau, on attribue un niveau à chaque type de VLAN. Les réseaux locaux virtuels (VLAN) permettent de créer des domaines de diffusions gérés par des commutateurs. Une trame ne peut être associée qu'à un VLAN et cette trame ne peut être diffusée que sur les ports du commutateur associés à ce vlan. Il existe différentes façons d'associer des ports à un VLAN, les principes sont les suivantes :

- **VLAN de niveau 1** ou **VLAN par port** : On y définit les ports du commutateur (switch) qui appartiendront à tel ou tel VLAN. Cela permet entre autres de pouvoir distinguer physiquement quels ports appartiennent à quels VLAN, ainsi chaque port du commutateur est affecté à un VLAN, donc chaque carte réseau est affectée à un VLAN en fonction de son port de connexion.

- **VLAN de niveau 2** ou **VLAN d'adresses MAC** : On indique directement les adresses MAC des cartes réseaux contenues dans les machines que l'on souhaite voir appartenir à un VLAN, cette solution est plus souple que les VLAN de niveau 1, car peu importe le port sur lequel la machine sera connectée, cette dernière fera partie du VLAN dans lequel son adresse MAC sera configurée (mais présente tout de même un inconvénient, car si le serveur contenant les adresses MAC tombe en panne, tout le réseau est alors affecté). De plus, il est possible de tricher sur son adresse MAC (spoofing). Donc chaque port du commutateur se voit affecter dynamiquement à un VLAN en fonction de l'adresse MAC de la carte réseau qui y est connectée.
- **VLAN de niveau 3** ou **VLAN d'adresses IP** : c'est le même principe que pour les VLAN de niveau 2 sauf que l'on indique les adresses IP (ou une plage d'IP) qui appartiendront à tel ou tel VLAN. Donc chaque port du commutateur se voit affecter dynamiquement à un VLAN en fonction de l'adresse IP de la carte réseau qui y est connectée.

Donc dans un réseau, chaque VLAN peut être géré par un ou plusieurs commutateurs, un commutateur peut gérer plusieurs VLAN. Et que les commutateurs identifient le VLAN auquel appartient une trame grâce au protocole 802.1q, ils échangent ces trames via des ports d'interconnexion. En pratique, un port de commutateur ne sera associé qu'à un seul VLAN (à l'exception des ports d'interconnexion).

3.1.2.8 Les Avantages du VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées
- Réduction de la diffusion du trafic sur le réseau

3.1.3 Les sous réseaux et adressage dans IP

Au début de l'informatique, chaque constructeur d'ordinateurs utilisait ses propres standards. Il était virtuellement impossible, ou extrêmement difficile, d'interconnecter des machines de marques différentes. Alors pour remédier à ce problème des pays ou des organisations ont décidé de créer un protocole permettant l'interconnexion de toutes ces machines. D'où la naissance du protocole TCP/IP et internet

3.1.3.1 Adressage IP

Une adresse IP est une adresse logique attribuée à un équipement. Elle permet de l'identifier de façon unique dans un réseau logique. Cette adresse est la base sur laquelle repose la transmission des informations de l'expéditeur au bon destinataire. Elle s'agit en fait d'un simple numéro qui doit être unique sur l'entièreté du réseau.

Dans un souci de manque de performance, un réseau TCP/IP sera subdivisé en sous-réseaux. Ainsi, elle possédera deux parties : une partie réseau situé au début de l'adresse et une partie hôte située à la fin de l'adresse.

Exemple : NN...NNHH...HH

N : représente un bit d'adresse réseau

H : représente un bit d'adresse hôte

Les machines se trouvant sur un même sous-réseau communiqueront entre elle de manière directe. Les machines se trouvant sur des sous-réseaux différents devront passer par des routeurs pour se communiqués.

En adressage IP, nous avons deux types d'adresses IP : les adresses IPv4 et les adresses IPv6

3.1.3.1.1 Les adresses IPv4

Une adresse IPv4 (**Internet Protocol version 4**) est une adresse attribuée à un équipement. L'adresse IP est représentée en décimal, c'est une suite de 4 nombres décimaux compris entre 0 et 255 et séparés par des points : on parle de notation décimale pointée[8].

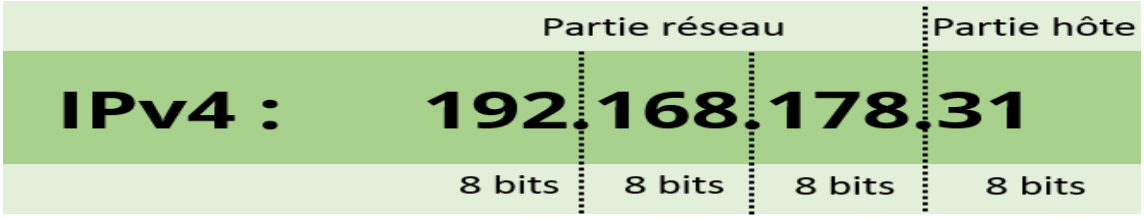

Figure 32 : Représentation IPv4*[9]*

Exemple : **176.26.142.26**

En binaire l'adresse IP est codée sur 32 bits car chaque nombre de 0 à 255 sera représenté sur 8 bits

Exemple : 18. 230. 5. 46

18	230	5	46
00010010	11100110	00000101	00101110

Toutes les adresses IP sont réparties sous différentes classes. À chaque classe correspond un nombre déterminé de bits pour le réseau et pour la machine. C'est pourquoi la partie réseau et

la partie machine varient selon la classe de l'adresse IP. On distingue 5 classes d'adresse IP : A, B, C, D, E.

- **Classe A**

Les adresses dont le premier bit est **0** sont de la classe A. En binaire, nous aurons les adresses du type suivant :

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

Les **8** premiers bits correspondent à la partie réseau et les autres à la partie machine. Les valeurs du premier octet de la classe A iront donc de **0** à **127**. Avec des adresses de classe A, nous aurons ainsi peu de réseaux mais de très grande taille.

Exemple : **114.50.49.13**

- **Classe B**

Les adresses dont les deux premiers bits sont **10** sont de la classe B. En binaire, nous aurons les adresses du type suivant :

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Les **16** premiers bits correspondent à la partie réseau et les autres à la partie machine. Les valeurs du premier octet de la classe B iront donc de **128** à **191**.

Exemple : **176.26.142.26**

- **Classe C**

Les adresses dont les trois premiers bits sont **110** sont de la classe C. En binaire, nous aurons les adresses du type suivant :

110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

Les 24 premiers bits correspondent à la partie réseau et les autres à la partie machine. Les valeurs du premier octet de la classe C iront donc de **192** à **223**. Avec des adresses de classe C, nous aurons ainsi beaucoup de réseaux de petite taille.

Exemple : **192.168.1.34**

- **Classe D**

Les adresses dont les quatre premiers bits sont **1110** sont de la classe D. En binaire, nous aurons les adresses du type suivant :

1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

Les valeurs du premier octet de la classe D iront donc de **224** à **239**. Ces adresses sont réservées pour les communications multicast.

Exemple : **226.26.12.126**

- **Classe E**

Les adresses dont les quatre premiers bits sont **1111** sont de la classe E. En binaire, nous aurons les adresses du type suivant :

1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

Les valeurs du premier octet de la classe D iront donc de **240** à **255**. Ces adresses sont réservées à des usages particuliers (indéterminé).

Exemple : **246.168.1.34**

A part ces adresses de classe nous avons également des adresses particuliéres définies par le protocole IP. Par exemple l'adresse zéro.

En IP v4, l'adresse zéro (**0.0.0.0**) signifie "**tout le réseau**". Il s'agit en fait d'une adresse réseau.

3.1.3.1.2 Les adresses IPv6

Avec l'essor d'internet, nous nous sommes vite retrouvé à cours d'adresses IP v4. Ainsi, il a fallu trouver des solutions. Dans la version 6 du protocole IP, les adresses IP sont maintenant codées sur 128 bits au lieu de 32. Nous avons considérablement augmenté le nombre d'adresses et chaque appareil peut maintenant recevoir la sienne[8].

- **Représentation des adresses**

Le format des adresses est un peu différent dans la version 6 que dans la version 4. Ici, elles sont formées de 8 nombres hexadécimaux de 4 chiffres séparés par des deux-points.

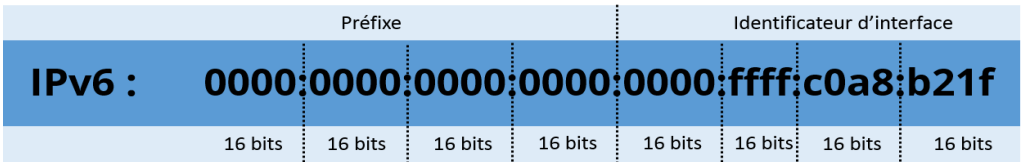

Figure 33: Représentation adresse IPv6*[9]*

Exemple : **abcd:ef01:2345:6789:abcd:ef01:2345:6789**

Il existe un certain nombre de règles pour la représentation des adresses IP v6.

Les symboles hexadécimaux **a** à **f** doivent être représentés par des minuscules.

Les premiers zéros de chaque nombre doivent être omis (mais pas les derniers).

Ex : **0123:0078:9abc:def0:1234:5678:9abc:def0** = **123:78:9abc:def0:1234:5678:9abc:def0**

Une suite de plusieurs nombres égales à zéros (et une seule) doit être omise. S'il est possible de supprimer plusieurs suites de zéros, la suite la plus longue sera supprimée. S'il n'y a qu'un seul nombre égale à zéro, il sera représenté par un seul zéro.

Ex : **a123:0:0:def0:1234:0:0:def0** = **a123::def0:1234:0:0:def0** ou **a123:0:0:def0:1234::def0**

Exemple : **a123:0:0:0:def0:1234:0:def0** doit s'écrire **a123::def0:1234:0:def0**

Exemple : **abcd:ef01:0:6789:abcd:ef01:2345:6789**

- **Les types d'adresse**

Dans l'IP v6, la notion de classe de l'IP v4 est abandonnées. Les adresses sont réparties suivant leur usage. La partie réseau de l'adresse est constituée des 64 premiers bits et la partie hôte des 64 derniers.

Adresses unicast

Il s'agit d'une adresse "normale". Elle désigne une seule machine.

Adresses anycast

Une adresse **anycast** représente un ensemble de machines. Lorsqu'un message sera envoyé sur cette adresse, la machine la plus proche le recevra.

Adresses multicast

Comme pour les adresses **anycast**, une adresse **multicast** représente un ensemble de machines. Toutefois, lorsqu'un message sera envoyé sur cette adresse, toutes les machines du groupe le recevront. Les huits (8) premiers bits de ces adresses sont à 1. Ce sont donc le adresses qui vont de **ff00**:: à **ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff**

On a aussi une adresse zéro en IPv6. En IP v6, l'adresse zéro (**::**) indique une adresse indéfinie, c'est à dire une absence d'adresse.

3.1.3.2 Les sous-réseaux

Comme nous l'avons expliqué en haut, l'adresse IP possède une partie réseau et une partie hôte. Pour ce qui est de l'IP v4, les adresses ont une partie réseau de 8, 16 ou 24 bits suivant la classe d'adresse. Pour ce qui est de l'IP v6, les adresses ont une partie réseau de 64 bits.

Ces masques par défaut ne permettent pas toujours de coller aux besoins particuliers de tout le monde. C'est pourquoi, il est possible de subdiviser les réseaux par défaut au moyen d'un masque de sous-réseau[8].

Un masque de sous-réseau est un nombre de la même taille que l'adresse. Les premiers bits sont à **1** et désignent la partie réseau. Les derniers bits sont à **0** et désignent la partie hôte.

Exemples : **111111...111111000000...000000**

- **Notation**

En IP v4, les masques de réseau peuvent se représentés comme une adresse réseau.

Exemples : **11111111111111111111111111100000** peut s'écrire **255.255.255.224** en IP v4

Une autre notation utilisée en IP v4 et seule valable en IP v6 est de faire suivre l'adresse IP d'une barre oblique **/** et ensuite du nombre de bit du masque de réseau.

Exemples : **11111111111111111111111111100000...** peut s'écrire **/27**

- **Subdivision de réseaux**

Lorsque nous avons à subdiviser des réseaux, il y a deux approches possibles. Soit nous essayons de déterminer le nombre de sous-réseaux que nous voulons obtenir, soit nous essayons de déterminer le nombre de machines par sous-réseaux.

- **Subdivision sur base du nombre de sous-réseaux**

Dans ce cas-ci, nous allons agrandir le masque réseau (bits à 1) d'autant de bit qu'il est nécessaire pour obtenir le nombre de subdivisions voulu. Dans le tableau suivant nous avons pris quelques exemples montrant le nombre de subdivisions qu'on veut par rapport au nombre de bits empreintes.

Nombre de subdivisions	Nombre de bits
2	1
3 à 4	2
5 à 8	3
9 à 16	4
17 à 32	5

Tableau 2: Subdivisions sur base du nombre de sous-réseaux

- **Subdivision sur base du nombre d'hôtes**

Dans ce cas-ci, nous allons garder pour la partie machine (bits à 0) autant de bit qu'il est nécessaire pour obtenir le nombre de machine moins deux (l'adresse réseau et l'adresse de diffusion). Voir **Tableau *3***.

Nombre de subdivisions	Nombre de bits
2	2
3 à 6	3
7 à 14	4
15 à 30	5
31 à 62	6

Tableau 3 : Subdivisions sur base du nombre de hôtes

Comme nous venons de voir la notion adressage IP et les sous-réseaux du protocole IP, donc pour qu'il est échange de paquet entre deux machines se trouvant dans le même réseau mais séparés par un équipement intermédiaire (routeur), on doit faire du routage. Ainsi nous allons parler dans la partie suivante le routage IP et l'interconnexion de réseaux.

3.1.4 L'interconnexion de réseaux et le routage dans IP

3.1.4.1 L'interconnexion de réseaux

L'interconnexion de réseaux permet à deux réseaux ou plus de communiquer et offre par conséquent un moyen d'échange d'informations aux équipements terminaux qui y sont connectés. La mise en œuvre d'interconnexions fait appel à une multitude de technologies et de protocoles qui interviennent à différents niveaux. Elle peut impliquer plusieurs organisations dans le même réseau caractérisant les différentes types d'architectures réseau qui existent[10].
L'interconnexion réseau peut s'appliquer à différents niveaux dans les réseaux d'entreprises.
Nous avons l'interconnexion de niveau 3, dans le chapitre I nous avons montré l'utilisation d'équipements d'interconnexion jouant un rôle essentiellement dans les niveaux physique et liaison de données.
Donc en reprenant rapidement le cas des réseaux locaux de type Ethernet, deux grandes classes d'équipements intervenant à ces niveaux ont été évoquées :

- les **répéteurs** et les **concentrateurs** (ou hubs ou répéteurs multi-ports) interviennent au niveau de la couche physique en régénérant le signal qui transite par eux. Ils permettent d'étendre le domaine de collision en interconnectant des segments physiques.
- les **ponts** (bridges) et les **commutateurs** (switches) réduisent quant à eux le domaine de collision en séparant logiquement des segments d'un même réseau. Ils opèrent au niveau 2 en analysant les adresses physiques (MAC) contenues dans les trames qui y transitent. L'objectif est ici de gagner en performances globales du réseau, le domaine de diffusion restant inchangé.

Ces équipements impliquent l'utilisation d'un même protocole MAC sur chacun de leur port. (Certains, qualifiés de multimédia, peuvent permettre l'interconnexion de supports de transmission hétérogènes (exemple : paire torsadée et fibre optique)). Enfin, ils ont capables de commuter des trames transportant n'importe quel protocole de niveau 3 (IP, IPX, …).
Mais l'interconnexion de niveau réseau, comme son nom l'indique, va s'appuyer sur des informations propres à cette couche : il s'agit plus précisément d'exploiter l'adressage logique qui y est mis en place.
On peut prendre l'exemple du routeur qui est un équipement dédié à la commutation de niveau 3. Le relayage d'un paquet, entrant sur une interface d'un routeur vers l'interface de sortie appropriée, s'opère à partir des informations de la couche réseau. En fonction de l'adresse du réseau de destination contenue dans le paquet et des informations de routage stockées, l'équipement pourra prendre sa décision de relayage vers l'interface appropriée permettant

d'acheminer le paquet vers une prochaine étape, intermédiaire ou finale, sur un chemin menant à sa destination.

Et qu'un routeur est dit « multi-protocoles » dans la mesure où il est capable de router du trafic lié à plus d'un protocole routé. Pour ces protocoles, routage et adressage sont donc intimement liés. Les adresses de niveau réseau sont des adresses logiques. Ainsi, une adresse de réseau logique peut être associée à une infrastructure physique (niveaux 1 et 2). Ce système d'adressage permet l'introduction d'une hiérarchie dans le réseau.

Contrairement aux adresses physiques, les adresses logiques peuvent être modifiées (Une carte Ethernet possèdera durant toute sa durée de vie la même adresse MAC attribuée par le constructeur lors de sa fabrication. L'adresse IP attribuée à l'interface d'un équipement associée à cette carte Ethernet pourra varier dans le temps : elle représente l'accès d'un équipement à un réseau logique dans ce cas mis en œuvre par un LAN Ethernet.

Le routeur est par excellence l'équipement dédié à l'interconnexion de liaisons hétérogènes. On doit le choisir en fonction des besoins d'interconnexion et devra disposer de ports lui permettant de s'interfacer sur les liaisons à interconnecter et donc présenter des interfaces à des technologies de transmission LANs et/ou WANs concernées. Un routeur peut donc relier entre eux des réseaux à accès multiple, basés ou non sur de la diffusion, des liaisons point à point…

Dans les routeurs, on a un point essentiel concernant la fonctionnalité de routage et plus particulièrement la constitution de l'information servant à la prise de décision. Les techniques de constitution de ces tables de routage varient de la simple configuration manuelle. On parle alors de routage statique et dynamiquement pour l'alimentation des tables de routage.

Dans la suite de cette partie nous parlerons les bases du routage dans IP et décrit comment se présentent les tables de routage.

3.1.4.2 Le routage dans IP

Le protocole IP fournit un service non fiable et sans connexion. Le routage IP consiste à définir la manière dont les paquets IP doivent être achemines à travers les divers réseaux. Un routeur IP est un équipement permettant aux paquets IP de circuler entre des réseaux hétérogènes ou des réseaux de même type mais comportant un grand nombre de machines. Il comporte des buffers (mémoires tampons) lui permettant notamment de relier des réseaux de vitesses différentes. Il extrait et insère des paquets (ou datagrammes) dans les trames. Il est en quelque sorte un relais qui "travaille" au niveau de la couche réseau : il analyse l'adresse IP de destination de chaque paquet reçu et décide, grâce à sa table de routage, sur quelle ligne de sortie il doit l'envoyer[11].

Nous avons deux types de routages : routage statique, routage dynamique.

- **Le routage statique (manuellement)**

Les entrées de la table de routage sont créées par défaut lorsqu'une interface est configurée ou par la commande **ip route** et les tables sont remplies manuellement. Ce type de routage fonctionne bien lorsque le réseau est de petite taille ou sur des réseaux d'extrémité.

Mais dans les routages statiques on a le routage statique par défaut. Pour ce routage le réseau de destination et le masque de sous-réseau est 0.0.0.0 suivi de la passerelle voire la commande ci-dessous.

```
R4(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

Pour le routage statique, le réseau à atteindre est le réseau 192.168.2.0/24 et l'interface utilisée pour joindre le réseau est ethernet 1/0 voir **Figure 34**.

On peut aussi utiliser l'adresse IP du prochain routeur c'est-à-dire la passerelle du réseau.

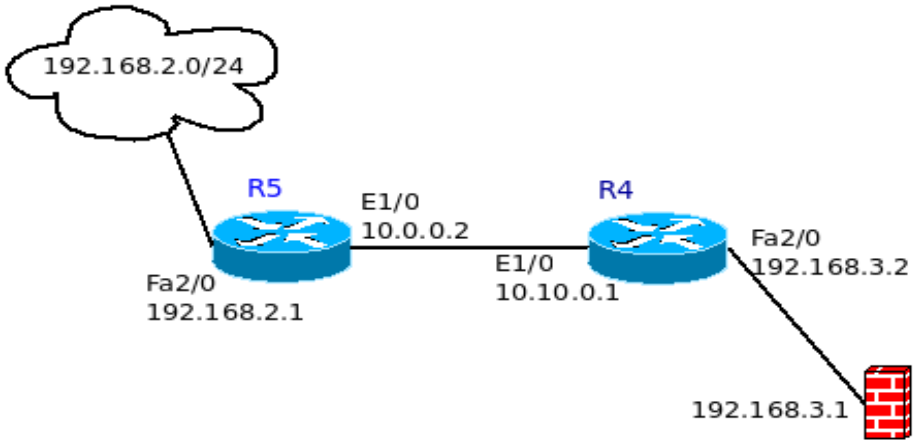

Figure 34 : Routage Statique et par défaut

Pour afficher les tables de routage des routeur R4 et R5 et tape la commande **show running-config.** Voici en image les tables de routages des deux routeurs

```
R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.3.1 to network 0.0.0.0

10.0.0.0/24 is subnetted, 1 subnets
C 10.0.0.0 is directly connected, Ethernet1/0
S 192.168.2.0/24 [1/0] via 10.0.0.2
C 192.168.3.0/24 is directly connected, FastEthernet2/0
S* 0.0.0.0/0 [1/0] via 192.168.3.1
R4#
```

Table e routage du routeur R4

```
R5(config)#do show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

10.0.0.0/24 is subnetted, 1 subnets
C 10.0.0.0 is directly connected, Ethernet1/0
C 192.168.2.0/24 is directly connected, FastEthernet2/0
S* 0.0.0.0/0 [1/0] via 10.0.0.1
R5(config)#
```

Table de routage du routeur R5

- **Le routage dynamique (dynamiquement)**

Le routage dynamique met en œuvre un protocole de communication entre les routeurs, chacun d'eux informant son voisin des réseaux auxquels il se trouve connecté. Dans ce type de routage, les tables sont remplies automatiquement. On configure un protocole qui va se charger d'établir la topologie et de remplir les tables de routage. On utilise un protocole de routage dynamique sur des réseaux plus importants. Le routage dynamique permet également une modification automatique des tables de routage en cas de rupture d'un lien sur un routeur. Il permet également de choisir la meilleure route disponible pour aller d'un réseau à un autre.

Il existe quelques protocoles routage dynamique : BGP (utilisé sur l'Internet), RIP, OSPF, IS-IS[12].

3.2 Les architectures sécurisées de réseaux

3.2.1 Le Pare-Feu (Firewall)

3.2.1.1 Définition

Un pare-feu est un mur ou une partition conçue pour prévenir la propagation du feu d'une partie du bâtiment vers une autre. En informatique, il est considéré comme un appareil de sécurité des réseaux qui contrôle le trafic entrant et sortant et décide s'il bloque ou autorise le trafic selon la définition de la politique de sécurité de l'administrateur. Egalement, 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.

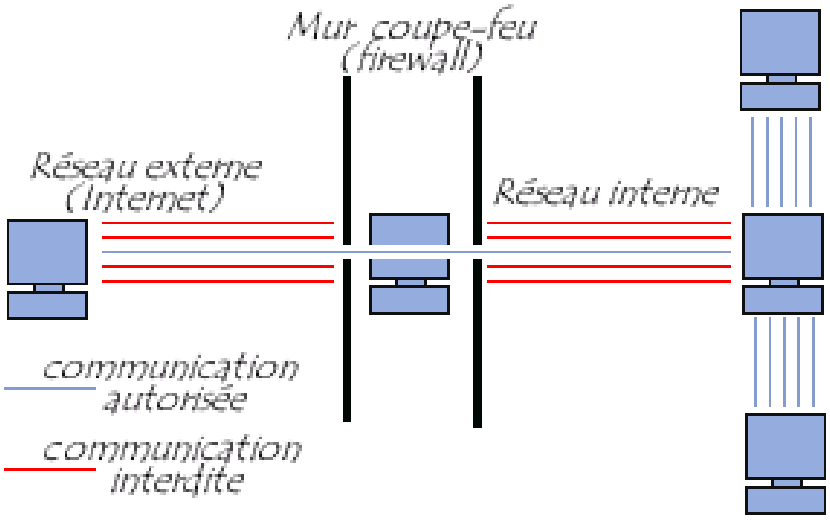

Figure 35 : Pare-Feu ou Firewall

C'est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (LAN) et un ou plusieurs réseaux externes (succursales). Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quelle position dans le réseau de l'entreprise interdisant ou autorisant le trafic entre l'extérieur et l'intérieur.

3.2.1.2 Emplacement de Pare-feu dans un réseau

Pour une bonne gestion des trafics venant de l'extérieur et de l'intérieur, l'emplacement des pare-feu est primordiale. Les pare-feu doivent occuper des positions stratégiques dans le réseau afin de bien jouer leur rôle.

- **Un pare-feu unique :** une approche plus modeste de l'architecture réseau consiste à utiliser un pare-feu unique incluant au moins trois interfaces réseau. La zone démilitarisée sera alors placée à l'intérieur de ce pare-feu. Le fonctionnement de ce pare-feu est le suivant : le périphérique réseau externe établit la connexion à partir du FAI (**Fournisseur Access Internet**), le réseau interne est connecté par le deuxième périphérique, puis le troisième périphérique du pare-feu est connecté la DMZ si cette dernière doit exister dans le réseau de l'entrepris, si cette sous-réseau n'existe pas, alors le troisième périphérique du pare-feu ne sera pas utilisé dans le réseau de l'entreprise.

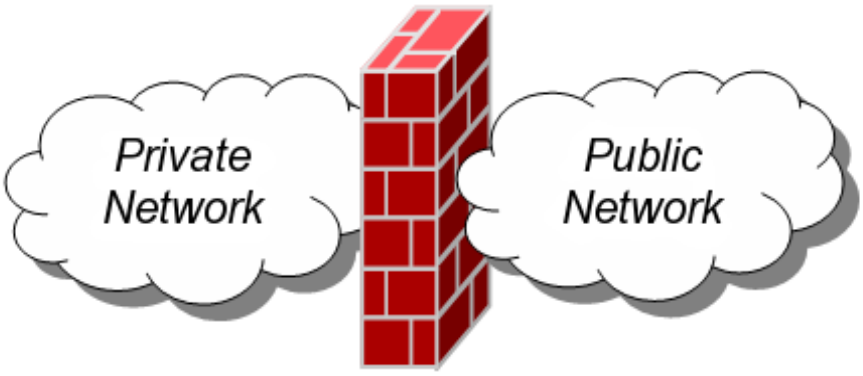

Figure 36 : Emplacement d'un pare-Feu Unique

- **Deux ou plusieurs Pare-Feu :** L'approche la plus sécurisée dans un réseau, consiste à utiliser deux pare-feu pour créer la DMZ. Le premier pare-feu (appelé pare-feu « frontal ») est configuré de façon à n'autoriser que le trafic destiné à la DMZ. Le second pare-feu (appelé pare-feu « principal ») est uniquement responsable du trafic entre la DMZ et le réseau interne. Pour renforcer le niveau de protection, il est possible d'utiliser des pare-feu développés par deux fournisseurs distincts, qui seront alors moins susceptibles de présenter les mêmes vulnérabilités. S'il est plus performant, ce modèle peut toutefois s'avérer plus coûteux à mettre en œuvre dans un réseau étendu.

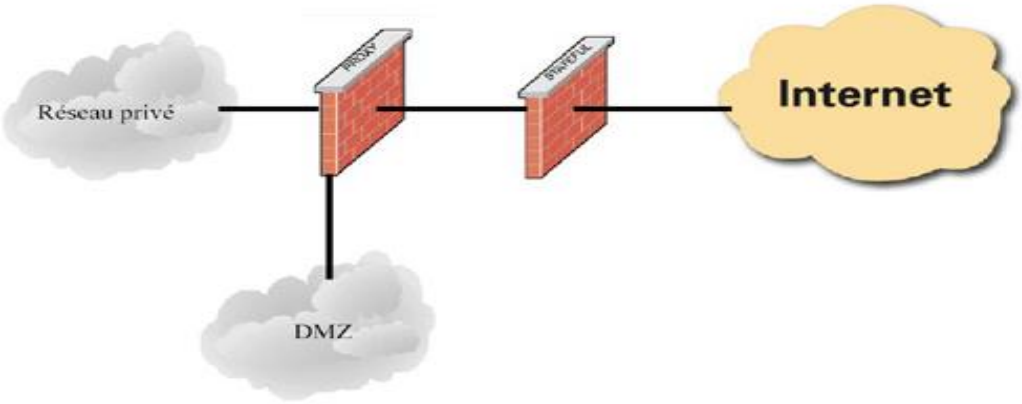

Figure 37 :Emplacement de deux pare-Feu

3.2.1.3 Fonctionnement d'un système de Pare-Feu

Un système pare-feu contient un ensemble de règles prédéfinies 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 œuvre une méthode de filtrage dépendant de la **politique de sécurité** adoptée par l'administrateur du réseau. On distingue habituellement deux types de politiques de sécurité permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées (c'est le Principe du moindre privilège) ;
- Soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

Pour un bon fonctionnement d'un système de pare-feu, on assiste à différents types de filtrages au niveau du firewall :

3.2.1.3.1 Le Filtrage simple de paquets

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « stateless packet filtering »). Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- ✓ Adresse IP de la machine émettrice ;
- ✓ Adresse IP de la machine réceptrice ;
- ✓ Type de paquet (TCP, UDP, etc.) ;
- ✓ Numéro de port (rappel : un port est un numéro associé à un service ou une application réseau).

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

Règle	Action	IP source	IP destination	Protocol	Port source	Port destination
1	Accept	192.168.10.20	194.154.192.3	Tcp	any	25
2	Accept	any	192.168.10.3	Tcp	any	80
3	Accept	192.168.10.0/24	any	Tcp	any	80
4	Deny	any	any	Any	any	any

Tableau 4: Filtrage simple de paquets

Les ports reconnus (dont le numéro est compris entre 0 et 1023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web). La plupart des dispositifs pare-feu sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue).

Le port 23 est par exemple souvent bloqué par défaut par les dispositifs pare-feu car il correspond au protocole Telnet, permettant d'émuler un accès par terminal à une machine distante de manière à pouvoir exécuter des commandes à distance. Les données échangées par Telnet ne sont pas chiffrées, ce qui signifie qu'un individu est susceptible d'écouter le réseau et de voler les éventuels mots de passe circulant en clair. Les administrateurs lui préfèrent généralement le protocole SSH, réputé sûr et fournissant les mêmes fonctionnalités que Telnet.

3.2.1.3.2 Le Filtrage dynamique

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente.

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. Le terme anglo-saxon est « stateful inspection » ou « stateful packet filtering », traduisez « filtrage de paquets avec état ».

Un dispositif pare-feu de type « stateful inspection » est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu ; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Si le filtrage dynamique est plus performant que le filtrage de paquets basique, il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en terme de sécurité.

3.2.1.3.3 Le Filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application.

Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau, et notamment de la manière dont elle structure les données échangées (ports, etc.).

Un firewall effectuant un filtrage applicatif est appelé généralement « passerelle applicative » (ou « proxy »), car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

Il s'agit d'un dispositif performant, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.

Par ailleurs, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et de connaître les failles afférentes pour être efficace. Enfin, un tel système peut potentiellement comporter une vulnérabilité dans la mesure où il interprète les requêtes qui transitent par son biais. Ainsi, il est recommandé de dissocier le pare-feu (dynamique ou non) du proxy, afin de limiter les risques de compromission.

3.2.1.4 Les types de Pare-Feu

Il existe deux principaux types de pare-feu : les pare-feu de type client et les pare-feu de type Appliance.

- Un pare-feu client est un logiciel qui réside dans lui-même et contrôle la totalité du trafic réseau sur cet ordinateur.
- Un pare-feu de type Appliance est matériel qui est connecté entre internet et votre ordinateur.

Au fil des années, comme les attaques informatiques et les attaques du réseau sont devenus plus sophistiques, de nouveaux types de pare-feu ont été élaborés pour répondre à différents objectifs dans la protection d'un réseau.

Voici une liste des types pare-feu utilisés aujourd'hui dans les réseaux d'entreprise :

- ✓ Pare-feu de la couche réseau : filtrage basé sur les adresses IP sources et de destinations ;
- ✓ Pare-feu de la couche transport : filtrage basé sur les ports de données sources et de destinations et filtrage basé sur les états de connexions ;
- ✓ Pare-feu de la couche application : filtrage basé sur les applications, les programmes ou les services ;
- ✓ Serveur proxy : filtrage des demandes de contenu web comme l'URL, les domaines les médias ;
- ✓ Service proxy inverse : placé à l'avant des serveurs web, les serveurs proxy inverse protègent, masquent, déchargent et distribuent l'accès aux serveurs web ;
- ✓ Pare-feu NAT (traduction d'adresses de réseau) : cache ou masque les adresses privées des hôtes du réseau ;
- ✓ Pare-feu propre à un hôte unique : filtrage des ports et des appels de services du système sur le système d'exploitation d'un seul ordinateur.

A part ces pare-feu cités en haut, il existe d'autres pare-feu de types logiciels des différents systèmes d'exploitations installés dans les ordinateurs. Parmi ces pare-feu on prend l'exemple du pare-feu dans le système d'exploitation Ubuntu qui est aujourd'hui le plus sécurisé et plus utilisé pour protéger les machines dans un réseau.

Ubuntu, comme tous les systèmes GNU/Linux, dispose de base d'un pare-feu logiciel. Celui-ci n'est toutefois pas activé par défaut après l'installation du système. Il inclut aussi de nombreuses interfaces pour gérer ce pare-feu logiciel. Il s'agit d'un empilement plus ou moins complexe pour lequel l'utilisateur final n'interagit réellement qu'avec les dernières couches. Ce pare-feu logiciel sous Ubuntu se nomme **NetFiltre.** Ce dernier agit directement au niveau du noyau Linux, ce qui permet une bonne sécurité. **NetFiltre** prend en charge aussi IPv6 ainsi le suivi de connexions. Mais, Netfiltre a une interface de configuration par défaut depuis le noyaux linux 2.6 appelée **Iptable**. Son utilisation est néanmoins complexe, fonctionnant uniquement en ligne de commande et requérant des commandes aux structures bien précises. Donc Iptables est une interface en ligne de commande permettant de configurer Netfilter.

Comment fonctionne Iptable ?

En général, Iptable pour Linux est déjà pré-installé. Si ce n'est pas le cas, ou si vous voulez vous assurer d'utiliser la dernière version du programme, vous pouvez l'installer ou le mettre à jour grâce au gestionnaire de paquets de votre distribution.

Il existe différentes interfaces graphiques pour iptables, comme notamment **Webmin**, grâce auxquelles le contrôle du programme avec la ligne de commande est relativement simple et rapide à apprendre. Et qu'Iptables requiert des privilèges de système étendus et ne peut donc être utilisé qu'avec un compte root ou des droits d'administrateur. Les tables chargées avec le programme et générées par le noyau contiennent des chaînes de règles, fournissant des informations sur la façon dont les paquets de donnés envoyés et reçus doivent être traités. Ces paquets sont propagés de règle en règle au sein de la chaîne, dans laquelle chaque règle peut induire une action ou un changement vers une autre chaîne. Alors qu'Iptable est composé de trois (3) table et que chaque table contient des chaines. Les tables d'iptable sont :

- **FILTER** :
  - **ACCEPT** : le paquet est accepté ;
  - **DROP** : le paquet est rejeté ;
  - **QUEUE** : le paquet est déplacé dans les processus utilisateurs. Ceci nécessite un intermédiaire (queue handler), qui transfère le paquet à une application ;
  - **RETURN** : le paquet est renvoyé à la chaîne précédente s'il s'agit d'une chaine personnalisée par l'utilisateur. Dans les chaînes standard, le règlement (policy) est exécuté (sans configuration par défaut : ACCEPT).
- **NAT :** correspond à des fonctions de routage et s'occupe de la conversion ou la transcription d'adresse réseau**.**
- **MANGLE** : est utilisée pour la manipulation des paquets c'est à dire modifier les paquets à la volée.

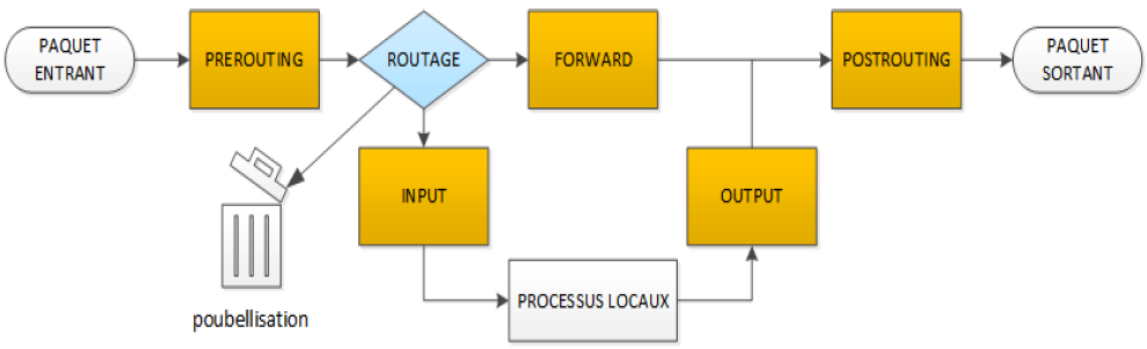

Figure 38 : Fonctionnement du Pare-Feu Iptable

Tables	Chaines
FILTER	INPUT, FORWARD, OUPUT
NAT	PREROUTING, POSTROUTING, OUTPUT
MANGLE	PREROUTING, INPUT, FORWARD, OUTPUT, PORTROUTING

Tableau 5: Résumé IPTable

Les chaînes standard mentionnées dans l'action **RETURN** sont spécifiées dans les tables **filter iptables**. Il s'agit des trois chaînes **INPUT, FORWARD** et **OUTPUT**. **INPUT** est en charge de livrer les paquets au système, tandis que **FORWARD** traite les paquets arrivants en attente d'être transmis. La chaîne **OUTPUT**, au contraire, contrôle le trafic de données généré par votre ordinateur.

Malgré leurs importances dans les réseaux d'entreprises en matières de sécurités, les pare-feu ont des limites.

3.2.1.5 Les limites des Pare-Feu

Un système pare-feu n'offre bien évidemment pas une sécurité absolue, bien au contraire. Les pare-feu n'offrent une protection que dans la mesure où l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. Ainsi, les accès au réseau extérieur par contournement du pare-feu sont autant de failles de sécurité. C'est notamment le cas des connexions effectuées à partir du réseau interne à l'aide d'un modem ou de tout moyen de connexion échappant au contrôle du pare-feu.

De la même manière, l'introduction de supports de stockage provenant de l'extérieur sur des machines internes au réseau ou bien d'ordinateurs portables peut porter fortement préjudice à la politique de sécurité globale.

Enfin de garantir un niveau de protection maximal, il est nécessaire d'administrer le pare-feu et notamment de surveiller son journal d'activité afin d'être en mesure de détecter les tentatives d'intrusion et les anomalies. Par ailleurs, il est recommandé d'effectuer une veille de sécurité afin de modifier le paramétrage de son dispositif en fonction de la publication des alertes.

3.2.2 La Zone démilitarisée (DMZ)

En sécurité informatique, une zone démilitarisée (ou DMZ) fait référence à un sous-réseau qui héberge les services exposés et accessibles de l'extérieur d'une entreprise. Elle agit comme une zone tampon avec les réseaux non sécurisés tels qu'Internet.

Les DMZ ont pour objectif de renforcer le niveau de sécurité du réseau local de l'entreprise. Dans ce système de réseau, un nœud de réseau protégé et surveillé, tourné vers l'extérieur, a

accès aux éléments exposés au sein de la zone dématérialisée tandis que le reste du réseau est protégé par un pare-feu.

Lorsqu'elles sont correctement mises en œuvre, les DMZ aident les entreprises à détecter et corriger les failles de sécurité avant qu'elles n'atteignent le réseau interne, où sont stockées les ressources les plus précieuses.

- ✓ **Objectif des zones démilitarisées**

Les DMZ visent avant tout à protéger les hôtes les plus exposés aux attaques. Parmi ces hôtes, on trouve généralement des services accessibles aux utilisateurs en dehors du réseau local, tels que la messagerie, les serveurs Web et les serveurs DNS. En raison de leur vulnérabilité, ceux-ci sont placés dans un sous-réseau surveillé, afin que le reste du réseau soit protégé en cas d'attaque.

Les hôtes hébergés dans la DMZ peuvent uniquement posséder des autorisations d'accès extrêmement restreintes aux autres services du réseau interne, car le niveau de sécurité des données transmises dans cette zone fait parfois défaut. Par ailleurs, les communications entre les hôtes hébergés dans la DMZ et le réseau externe sont également limitées afin d'étendre autant que possible cette zone tampon. Cette pratique permet aux hôtes situés dans le réseau protégé d'interagir avec les réseaux interne et externe tandis que le pare-feu se charge de répartir et de gérer le trafic partagé entre la DMZ et le réseau interne. En général, un pare-feu complémentaire sera utilisé pour protéger la DMZ de toute menace émanant du réseau externe. Tous les services accessibles aux utilisateurs depuis un réseau externe devront être placés dans la zone DMZ. Parmi les services les plus souvent rencontrés, on retrouvera : les serveurs Web, les serveurs de messageries, les serveurs FTP, …

- ✓ **Types de DMZ**

Pour renforcer la sécurité du réseau, on a de deux types de DMZ chacune connectée à un pare-feu ou les deux connectées à un même pare-feu pour filtrer les paquets entrantes ou sortantes. Nous avons une DMZ privée et une DMZ publique.

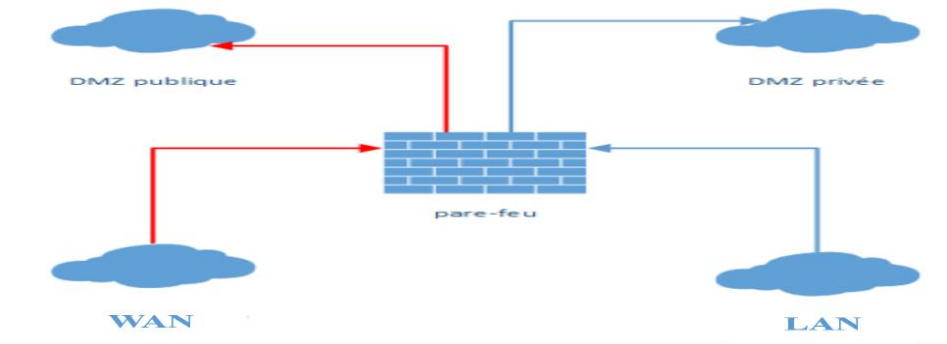

Figure 39 : Les Types De DMZ

- **DMZ privée** : il doit contenir tous les services qui sont joignables depuis le réseau LAN à savoir : DNS, DHCP, SQL, …
- **DMZ publique :** quant à cette DMZ, on doit mettre tous les services joignables depuis internet ou le réseau WAN.

Dans ces zones démilitarisées certains flux sont permis comme illustré dans la figure ci-dessus parlant des types de DMZ.

Donc les flux autorisés sont :

- **WAN → DMZ publique ;**
- **LAN → DMZ privée ;**
- **DMZ privée → DMZ publique ;**

✓ **Emplacement des zones démilitarisées**

Dans une architecture réseau d'une entreprise, la position de la zone démilitarisée dépend parfois du nombre de pare-feu présent dans le réseau pour faire le filtre des trafics entre le réseau local et l'internet. On distingue en générale deux emplacements majeurs des DMZ :

❖ **DMZ avec un Pare-Feu**

Il est plus rentable de réaliser une DMZ via un seul pare-feu performant (par exemple un routeur incluant un pare-feu) avec trois connections réseaux séparés : une pour Internet, une pour le réseau local et une troisième pour la zone démilitarisée. En ce qui concerne les DMZ protégées (Tout est relié à un seul pare-feu accompagné de trois terminaux distincts), toutes les connexions sont surveillées par le même pare-feu indépendamment les unes des autres, ce qui peut entraîner un point unique de défaillance dans le réseau (de l'anglais Single point of Failure). Par ailleurs, le pare-feu doit, dans une telle architecture, être capable gérer tant le trafic provenant d'Internet que les accès qui viennent du réseau local.

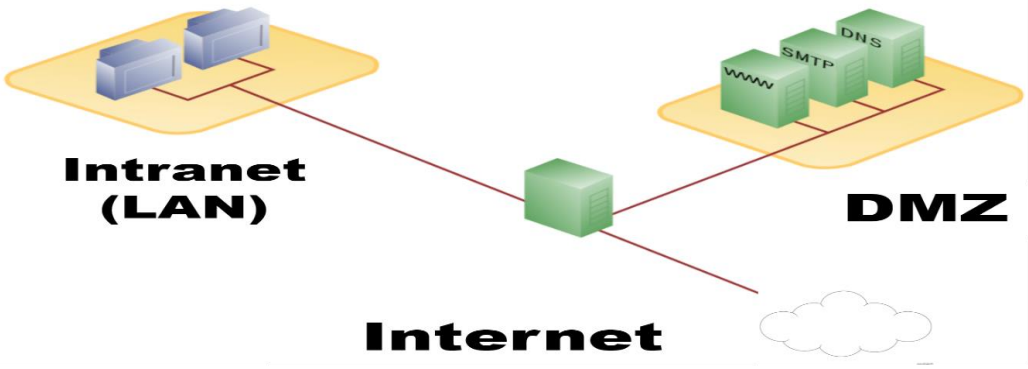

Figure 40 : Zone démilitarisée avec un Pare-Feu

Avec une zone démilitarisée protégée, un seul pare-feu surveille les connexions réseau et contrôle ainsi le trafic Internet et l'accès au réseau local.

❖ **DMZ avec deux Pare-feu**

Pour prévenir les réseaux d'entreprises contre les accès provenant du réseau public (WAN, Wide Area Network soit le réseau "dispersé", Internet), il convient de mettre en œuvre les concepts de zones démilitarisées en utilisant deux pare-feu. Il peut s'agir de composants matériels indépendants ou d'un logiciel pare-feu sur un routeur. Le pare-feu externe protège la zone démilitarisée du réseau public, le pare-feu interne est quant à lui connecté entre le DMZ et le réseau de l'entreprise.

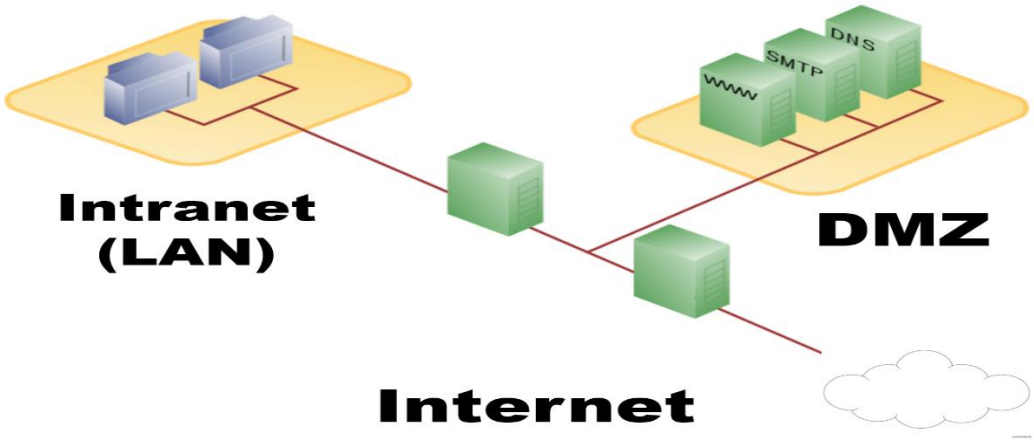

Figure 41 : Zone démilitarisée avec deux Pare-Feu

Dans une architecture réseau d'une entrepris, il n'est pas conseillé d'utiliser les pare-feu du même constructeur. En effet, des hackers peuvent détecter des failles de sécurité et ainsi franchir sans problèmes les deux pare-feu. Pour empêcher les attaques d'un serveur compromis sur d'autres machines de la DMZ, il est possible d'éloigner ces dernières en utilisant d'autres logiciels pare-feu ou via une segmentation dans le réseau local virtuel (de l'anglais Virtual Local Area Network ou VLAN).

3.2.3 Les réseaux privés virtuels VPN

3.2.3.1 Définition

Un réseau privé virtuel (VPN) est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de « tunnel ». Il est le moyen le plus simple et plus efficace pour les gens de protéger leur trafic internet et de garder leur identité privée en ligne[13].

La technique consiste à utiliser internet comme support de transmission en utilisant un protocole de VPN ou tunneling, c'est-à-dire encapsulant les données à transmettre de façon chiffré. On parle de VPN pour désigner le réseau artificiellement créé. Un VPN est virtuel en ce sens qu'il transporte des informations au sein d'un réseau privé, mais ces informations sont en fait

transportées sur un réseau public. Un VPN est privé dans la mesure ou le trafic est crypté pour garder les données confidentielles pendant leur transport sur le réseau public.

Le tunnel permet aux sites distant et aux utilisateurs d'accéder en toute sécurité aux ressources réseau du site principale.

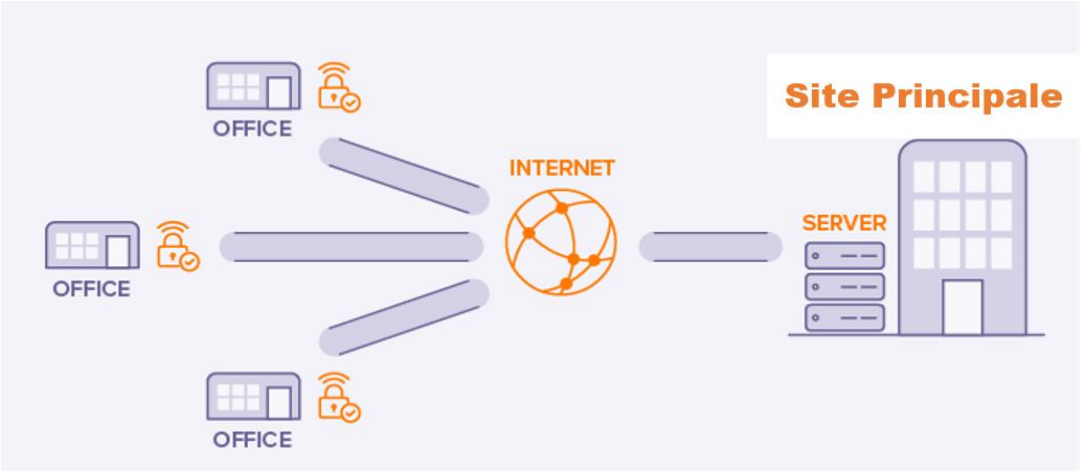

Figure 42 : Réseau Privé Virtuel (VPN)

3.2.3.2 Fonctionnement des réseaux Privés Virtuels (VPN)

Comment fonctionne un réseau privé virtuel (VPN) ?

Pour comprendre le bon fonctionnement d'un réseau privé virtuel, il est utile de comprendre d'abord comment fonctionne une connexion internet avec un VPN et celle sans VPN.

- **Sans VPN**

Lorsque vous accédez à un site web sans VPN, vous êtes connecté à un ce site via votre fournisseur de services internet ou **FAI**. Le **FAI** vous attribue une adresse IP unique qui peut être utilisée pour vous identifier sur le site web. Etant donné que votre **FAI** gère et dirige votre trafic, il peut voir les sites web que vous visitez. Et votre activité peut vous être liée par cette adresse IP unique.

- **Avec un VPN**

Lorsqu' on se connecte à internet avec un VPN, l'application VPN de notre appareil (également appelée client VPN) établit une connexion sécurisée avec un serveur VPN. Le trafic effectué va toujours passer par le FAI, mais le FAI ne peut plus le lire ou voir sa destination finale. Les sites web visités via l'adresse IP d'origine seront invisible pour le FAI. Il peut voir seulement et uniquement l'adresse du serveur VPN, qui est protégée par de nombreux autres utilisateurs et changes régulièrement.

Pourquoi utiliser un VPN ?

Il existe de nombreuses raisons d'utiliser un VPN :

- Sécurité en ligne : pour protéger vos e-mails et vos connexions sur différents appareils, il devient quasiment indispensable d'utiliser un VPN pour sécuriser les données. De cette façon, aucun hacker ne peut décrypter les données qui transitent via le VPN, ce qui vous offre une sécurité optimum dans le transfert des données.
- Liberté d'accès à des données géo-localisés
- Anonymat : l'anonymat du VPN est aussi utile pour les téléchargements sécurisés des activités P2P et de partage de fichiers.

Mais également il est important dans les VPN de comprendre le fonctionnement des deux configurations de VPN à savoir le VPN de site à site et le VPN d'accès à distance pour comprendre les VPN.

- **VPN de Site à site et d'accès à distance**

Les VPN sont généralement déployés dans l'une des configurations suivantes :

➢ **VPN de site à site**

Un VPN de site à site est créé lorsque les périphériques de terminaisons VPN, également appelés passerelles VPN, sont préconfigurés avec des informations pour établir un tunnel sécurisé. Le trafic VPN n'est chiffré qu'entre ces appareils. Les hôtes internes ne savent pas qu'un VPN est utilisé.

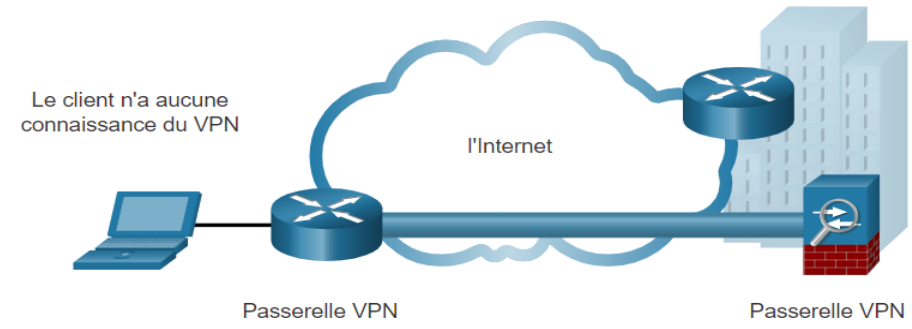

Figure 43 : Réseau Privé virtuel de Site à Site

➢ **VPN d'accès à distance**

Un VPN d'accès à distance est créé dynamiquement pour établir une connexion sécurisée entre un client et un terminal VPN. Par exemple, un VPNSSL est utilisé lorsque vous vérifiez des informations bancaires en ligne.

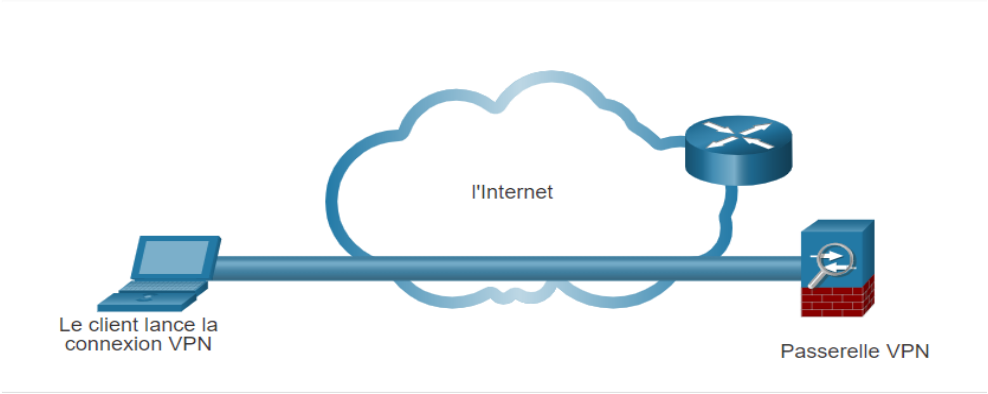

Figure 44 : Réseau Privé Virtuel d'accès à distance

Et voici quelque concepts clés liés au VPN qui nous aiderons à bien comprendre le fonctionnement d'un VPN.

- **Proxying**

Le serveur VPN agit comme un proxy ou un remplaçant de votre activité web : au lieu de votre adresse IP et votre emplacement réel, les sites visités ne verront que l'adresse IP et l'emplacement du serveur VPN. Cela vous rend plus anonyme sur internet.

- **Authentification**

L'établissement d'une connexion sécurisée est un problème délicat résolu par des mathématiciens intelligents dans un processus appelé authentification.

Une fois authentifié, le client VPN et le serveur VPN peuvent être sûr qu'ils se parlent entre eux et avec personne d'autre.

- **Tunneling**

Les VPN protègent également la connexion entre le client et le serveur avec un tunnel et un cryptage. Le tunneling est un processus par lequel chaque paquet de données est encapsulé dans un autre paquet de données. Cela rend la lecture par des tiers plus difficile.

- **Chiffrement**

Les données à l'intérieur du tunnel sont également chiffrées de telle sorte que seul le destinataire concerné peut les déchiffrées. Cela garde le contenu du trafic internet complétement privé. Même le FAI ne les verras pas.

3.2.3.3 Les Types de réseaux privés virtuels (VPN)

Dans la sécurité d'une entreprise, plusieurs options sont disponibles pour sécuriser le trafic dans l'entreprise. Ces solutions varient en fonction de la personne qui gère le VPN.

Ils peuvent être gérés et déployés en tant que :

- **VPN d'entreprise :** les VPN gérés par l'entreprise sont une solution courante pour sécuriser le trafic d'entreprise sur internet. Les VPN de site à site et d'accès à distance sont créés et gérés par l'entreprise à l'aide des VPN IPsec et SSL**.**
- **VPN des fournisseurs de services :** les VPN gérés par les fournisseurs de services sont créés et gérés sur le réseau du fournisseur. Le fournisseur utilise la communication multi-protocole par étiquette (MPLS) au niveau de la couche 2 ou couche 3 pour créer des canaux sécurisés entre les sites d'une entreprise. MPLS est technologie de routage que le fournisseur utilise pour créer des chemins virtuels entre les sites. Cela sépare efficacement le trafic des autres trafics clients.

Les deux figures suivantes répertorient les différents types de déploiements VPN l'un gérés par l'entreprise et l'autre gérés par les fournisseurs de services.

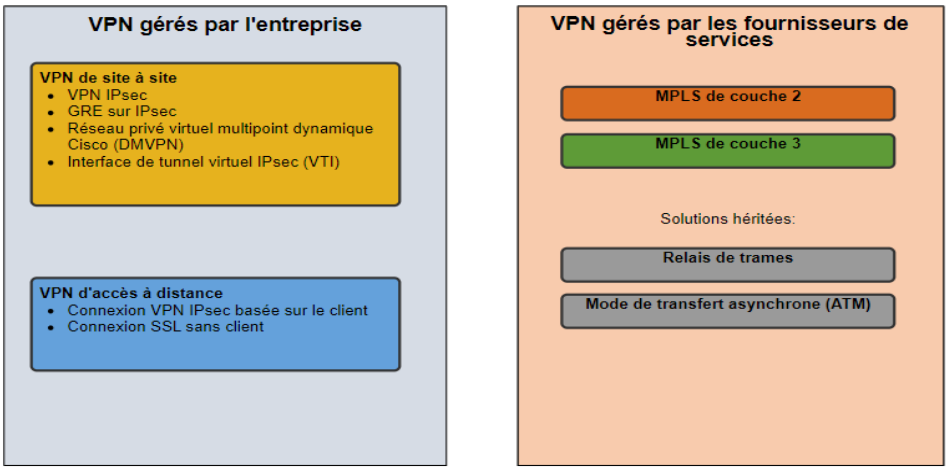

Figure 45 : Différence entre VPN d'entreprise et VPN des Fournisseurs de Services

3.2.3.4 Les protocoles VPN

Les protocoles VPN sont les méthodes par lesquelles un appareil se connecte au serveur VPN. Certains protocoles sont meilleurs pour la vitesse, certains sont meilleurs pour la sécurité et certains fonctionne simplement mieux dans certaines conditions de réseau.

Les protocoles VPN les plus populaires utilisés aujourd'hui sont :

- **OpenVPN ;**
- **IKEv2 ;**
- **L2TP/IPsec ;**
- **PPTP ;**
- **WireGuard ;**
- **SSTP ;**

- **Lightway ;**

3.2.3.5 Les avantages des réseaux privés virtuels (VPN)

Les réseaux privés virtuels modernes prennent désormais en charge les fonctionnalités de cryptage, telles que la sécurité du protocole internet (IPsec) et les VPN SSL (Secure Sockets Layer) pour sécuriser le trafic réseau entre les sites.

Les principaux avantages de VPN sont regroupés dans le tableau suivant :

Avantage	Description
Économies de coûts	Avec l'avènement de technologies rentables à large bande passante, les entreprises peuvent utiliser des VPN pour réduire leurs coûts de connectivité tout en augmentant simultanément la bande passante de connexion à distance.
Sécurité	Les VPN offrent le plus haut niveau de sécurité disponible, en utilisant des protocoles de cryptage et d'authentification avancés qui protègent les données contre tout accès non autorisé.
Évolutivité	Les VPN permettent aux organisations d'utiliser Internet, ce qui facilite l'ajout de nouveaux utilisateurs sans ajouter d'infrastructure significative.
Compatibilité	Les VPN peuvent être mis en œuvre sur une grande variété d'options de liaison WAN, y compris toutes les technologies haut débit populaires. Les travailleurs distants peuvent profiter de ces connexions haut débit pour obtenir un accès sécurisé à leurs réseaux d'entreprise.

Tableau 6:les Avantages des réseaux privés virtuels

3.2.4 Les serveurs proxy

3.2.4.1 Définition

Il semble très important de préciser que le terme « proxy » peut être traduit par mandataire, procuration, intermédiaire. Donc un serveur proxy est alors un serveur servant d'intermédiaire (ou mandataire) pour accéder à un autre réseau, généralement internet.

3.2.4.2 Rôle du serveur proxy http (ou proxy web)

Dans la vie courante, si on surfe sur internet, un ordinateur est directement connecté. C'est l'ordinateur qui va chercher les pages directement sur internet comme dans le schéma ci-dessous.

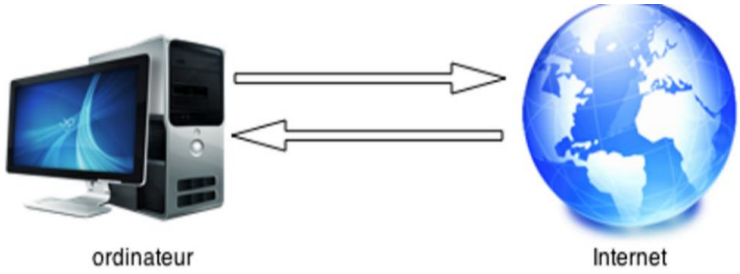

Figure 46: Connexion Internet sans serveur Proxy

Comme vous le voyez l'ordinateur va chercher directement les pages sur l'internet. Mais l'inconvénient principal de ce fonctionnement est que l'ordinateur est directement exposé sur internet, même s'il y a d'autres inconvénients.

Si maintenant, on place un serveur proxy entre l'ordinateur et l'internet, on obtient les événements suivants :

1. **L'ordinateur est connecté au serveur proxy**
2. **Et c'est lui qui est connecté à internet**
3. **L'ordinateur demande des pages (via son navigateur) à ce serveur**
4. **Il va chercher les pages demandées sur internet**
5. **Et renvoie les pages demandées à l'ordinateur.**

Figure 47: Connexion Internet avec serveur Proxy

Pour que tout cela fonctionne, il faut prendre en compte les paramètres proxy, en indiquant deux informations importantes au navigateur pour lui dire d'utiliser un serveur proxy :

1. L'adresse du serveur proxy
2. Le port utilisé pour échanger les données.

Donc le navigateur ne connait alors qu'une seule adresse : celle du serveur proxy.

3.2.4.3 Le Filtrage d'URL

En entreprise, il est facile pour l'administrateur de filtrer les pages puisqu'elles passent toutes par un point unique qui est le serveur proxy. Donc suivant les politiques des entreprises sur la sécurité, la direction peut décider de filtrer les pages qui peuvent nuire à la production : comme

les jeux, les réseaux sociaux, …. Donc le serveur proxy peut servir de filtrage des pages pour ne surcharger le réseau ou lutter contre des attaques.

3.2.4.4 L'anonymat avec un proxy

Un serveur proxy peut garantir l'anonymat (sauf pour un proxy transparent) en cachant l'adresse IP de l'ordinateur et laisse apparaitre celle du serveur proxy.

Mais cet anonymat peut être de deux niveaux :

1. Le proxy anonyme va interroger pour le navigateur de l'ordinateur les serveurs distants mais indiquera qu'il est mandaté (il ne donnera pas l'adresse IP de l'ordinateur).
2. Le proxy hautement anonyme (high Anonymous) va interroger les serveurs distants et n'indiquera rien. Il se fera passer pour un client classique.

Comment utiliser un serveur proxy ?

On peut utiliser un serveur proxy de deux façons :

1. En saisissant directement son adresse dans le navigateur de votre ordinateur. Vous arrivez alors sur une page qui vous demande de saisir la page sur laquelle vous voulez aller, et à partir de ce moment vous pouvez surfer directement.
2. Soit en modifiant les paramètres de votre navigateur. Dans ce cas, vous utilisez votre navigateur comme avant.

3.2.4.5 Les autres types de serveurs proxy

Dans la partie précédente, on parlait sur le fonctionnement des serveurs proxy plus particulièrement le proxy web, mais à part ce dernier il existe d'autres types de proxy. On peut en citer :

- **Le proxy Cache** : le proxy sert de cache, c'est-à-dire qu'il va conserver sur son disque dur les pages web les plus utilisés et pouvoir les renvoyer aux navigateurs qui les demandent sans aller les chercher sur internet. Cela permet d'accélérer la mise à disposition des pages et d'éviter au proxy d'aller sur internet.
- **Le proxy transparent** : On le trouve le plus souvent en entreprise, un proxy transparent. Comme un proxy classique, celui-ci a pour rôle d'envoyer les flux à destination d'internet mais à la différence d'un proxy classique, les utilisateurs ne le voient pas. C'est pour cela qu'il est appelé proxy transparent. Cela fonctionne car il est placé entre le post client et la sortie vers internet, ce qui fait que les flux sont obligés de passer dedans.

  Attention, avec un proxy transparent , fini l'anonymat : la demande passe à travers le proxy, mais c'est toujours votre adresse IP qui est vue (pas celle du proxy).

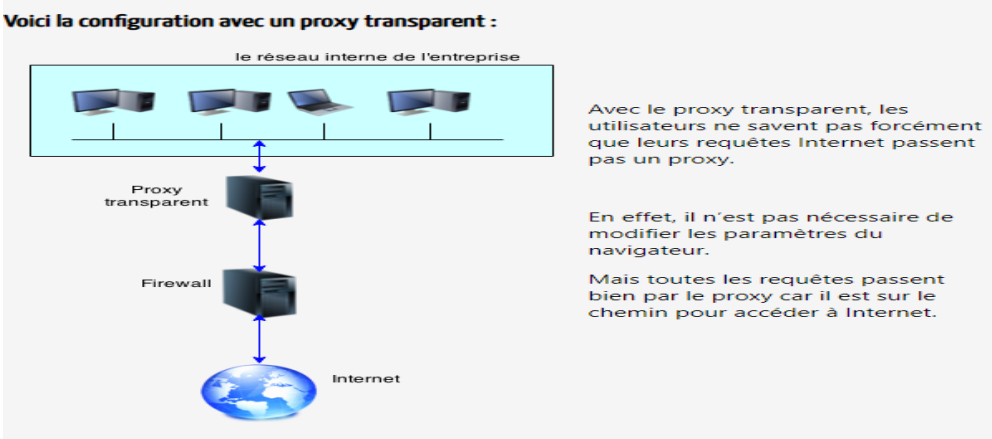

Figure 48 : Le Proxy Transparent

- **Le reverse proxy** : nous venons de voir que le proxy (http) était le prote de sortie vers l'internet. Le reverse proxy est comme son nom l'indique l'inverse de proxy. Le reverse proxy est donc la porte d'entrée du web vers le réseau interne. Le reverse proxy peut éventuellement équilibrer la charge qui arrive en la répartissant sur les différents serveurs web. Le reverse proxy est le point d'entrée des demandes, c'est qu'il peut les traiter et donc les aiguiller. Ainsi avec l'avancé de la technologie, on peut avoir un reverse proxy sur lequel on peut se connecter en http, https, ftp, …. C'est lui qui reçoit les demandes et les envois vers les bons serveurs. Enfin, un autre avantage du reverse proxy, c'est le cache. Comme les autres proxys, le reverse proxy peut mettre en cache les informations les plus demandées et les fournir sans avoir à interroger à nouveau les serveurs.

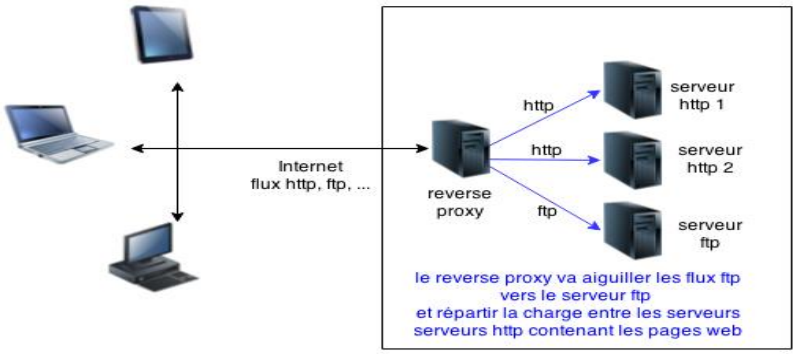

Figure 49 : Le reverse Proxy

- **Le proxy FTP** : C'est un proxy qui supporte le protocole FTP. Il fonctionne exactement comme un serveur http. Bien que certains proxys soient spécialisés pour ne faire que du FTP. Mais la plupart des proxys récents sont capables de faire du http, https, et ftp (squid, nginxf, …). Egalement, on peut trouver des proxy FTP transparent.

3.2.4.6 Les exceptions proxy

Une exception proxy est une adresse IP ou une URL pour laquelle un navigateur ne va pas utiliser le proxy comme intermédiaire, mais se connecter directement à internet.

3.2.4.7 Les avantages et les inconvénients

- **Les avantages**

Les avantages sont nombreux :

- **Le surf anonyme** : Ce n'est pas votre adresse qui est vue sur les sites, mais l'adresse du proxy. Vous êtes ainsi "quasiment anonyme" ou "complètement anonyme" (voir un peu plus bas).
- **La protection de votre ordinateur** : Ce n'est pas vous qui êtes en première ligne sur Internet, vous êtes donc mieux protégé.
- **Le masquage de votre lieu de connexion** : Le proxy peut être dans un pays différent du votre. Lorsqu'il se connecte à un site, c'est la géolocalisation du proxy qui est vu, pas là votre. Cela peut être utile sur certains sites qui filtre les connexions suivants les lieux d'où elles proviennent.
- **Le cache** : le serveur va conserver les pages web dans son disque dur pour une réutilisation rapide, sans une nouvelle des serveurs.
- **Le filtrage** : comme toutes les requêtes et les réponses passent par le proxy, il est possible de filtrer ce que l'on autorise à sortir ou à entrer, c'est le cas dans de nombreuses entreprises lorsqu'ils veulent interdire les connexions sur les réseaux sociaux, YouTube.

- **Les inconvénients**

Qui dit avantages, dit également inconvénients. Comme nous l'avons vu au-dessus, c'est lui qui fait l'intermédiaire entre vous et le web, donc il voit et peut enregistrer tout ce qui circule entre votre ordinateur et le web, cela peut être risqué ! Imaginez juste que la personne qui gère ce serveur soit mal intentionné. Il a accès à l'ensemble de votre historique de navigation.

Si vous utilisez un proxy, il doit être irréprochable car lorsque vous vous connectez à votre banque, votre proxy pourrait très bien enregistrer vos codes (même si ceux-ci sont émis dans des flux https).

Il faut donc utiliser un proxy, donc vous êtes sûr, ou alors ne pas l'utiliser : c'est à dire mettre des exceptions à l'utilisation de celui-ci. Sur certains sites, certains préconisent absolument d'utiliser des proxys pour être cachés, mais ces mêmes personnes oublient de parler de la sécurité des données confidentielles que vous envoyez sur Internet.

Un autre inconvénient des proxys est la technologie utilisée sur les sites web. En effet, certains sites peuvent utiliser des technologies de connexion directes entre votre ordinateur et le serveur Web, dans ce cas, il peut être impossible de se connecter à ce genre de sites si vous êtes caché derrière un proxy.

Mais n'oubliez jamais que même si vous vous cachez dernière un proxy, celui-ci enregistrera dans ses logs toutes vos actions sur internet. Si voulez vraiment vous cachez, utilisez plutôt une connexion sécurisée.

3.2.5 Sécurité et VLAN

Dans les réseaux informatiques d'aujourd'hui, la sécurité des informations est importante, pour cela il faut toujours veiller à la sécurité des employer et de l'entreprise en mettant en place des politiques de sécurités fiables et robustes. Nous allons parler dans ce document précisément dans cette partie la sécurité qu'apporte les réseaux locaux virtuels et la sécurité des ports dans un réseau.

3.2.5.1 Le VLAN de gestion

Comme définie dans la partie des réseaux locaux virtuels, cette virtualisation des LAN consiste à séparer l'infrastructure physique des services de transports rapide fournis par les commutateurs. Et que son objectif est de rendre la fonction d'un LAN indépendante de l'infrastructure physique.

Donc pour créer un réseau local virtuel, les équipements réseau, tels que les points d'accès, les routeurs et les commutateurs doivent prendre en charge la configuration VLAN. Le VLAN de gestion (management VLAN) est utilisé à des fins de gestion (c'est-à-dire pour accéder à l'interface utilisant la gestion du commutateur).

Qu'est-ce qu'un VLAN de Gestion ?

Le VLAN de gestion est un VLAN spécifique attribué aux commutateurs pour qu'ils soient accessibles via une adresse IP (ICMT, Telnet, SNMP, http). C'est une pratique courante utilisée par les administrateurs réseau pour empêcher les utilisateurs finaux d'accéder aux périphériques réseau clé de leur infrastructure réseau. Cela ajoute une couche supplémentaire de protection au sein du réseau.

Ceci est effectué en configurant chaque périphérique réseau avec un ID de VLAN unique, tout en s'assurant que les utilisateurs finaux entrent dans le réseau à partir d'un VLAN différent.

Dans les bonnes pratiques de configuration, on le distinguera du VLAN par défaut d'un VLAN utilisateur ou du VLAN natif. On changera donc le numéro du VLAN de gestion.

Aussi, une bonne raison de séparer le VLAN de gestion des autres VLAN tient au fait évident de séparer logiquement les périphériques « digne de confiance » des autres. Il s'agit alors d'appliquer les règles de sécurité nécessaires afin d'éviter, par exemple que des utilisateurs classiques ou tout simplement « non autorisés » n'accèdent pas aux matériels.

Pour configurer le vlan de gestion dans un réseau, il faut suivre ces différentes étapes (voir **Figure 50**) une fois entré dans le commutateur en ligne de commande.

```
Switch>
Switch>
Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#interface vlan 1
Switch(config-if)#
Switch(config-if)#ip address 10.1.1.8 255.255.255.0
Switch(config-if)#
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#
Switch(config)#ip default-gateway 10.1.1.254
Switch(config)#
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Figure 50: Configuration du VLAN de Gestion

3.2.5.2 La sécurité des Ports

3.2.5.2.1 Fonction Switchport Security

Cette fonction permet de contrôler les **adresses MAC** autorisées sur un port. En cas de "violation", c'est-à-dire en cas **d'adresses MAC** non autorisées sur le port, une action est prise. Dans les infrastructures **LAN** modernes, on trouvera un port de commutateur dédié par station de travail. Dans ce cadre, les ports ne devraient recevoir de trafic que d'une seule **adresse MAC** autorisée. On y trouvera alors une utilité pour empêcher la connexion de commutateurs pirates par exemple. Par contre, la mesure uniquement configurée sur un nombre minimal d'adresses à 1 (qui est la configuration par défaut), n'empêche personne de déconnecter un hôte et d'y connecter son ordinateur pirate. Il serait nécessaire d'indiquer au commutateur quelle est l'adresse MAC à autoriser.

Mais comment "autoriser" une adresse MAC spécifique autrement qu'en tenant un registre central ? Par contre dans un réseau, il est possible que le commutateur Cisco apprenne les adresses MAC à un moment déterminé (où seules les stations autorisées seraient connectées par hypothèse) et de les inclure en dur dans la configuration du commutateur. Combinée à un maximum d'une seule adresse, la fonction **switchport port-security mac-address sticky**

autorise en dur dans la configuration courante uniquement la première adresse connectée au port.

3.2.5.2.2 Contre-mesures face aux attaques sur le réseau local

Switchport-Port Security permet donc de contrôler au plus bas niveau les accès au réseau. Elle fait partie de l'arsenal disponible pour contrer des attaques de bas niveau sur les infrastructures commutées. Parmi d'autres :

- **BPDU Guard ;**
- **Deep ARP Inspection ;**
- **IPv6 First Hop Security ;**
- **DHCP Snooping ;**
- **IEEE 802.1X / EAP + Radius ;**
- **Bonne pratique VLAN ;**

3.2.5.2.3 Mise en œuvre sur des commutateurs Cisco

Par défaut, cette fonction est désactivée.

Si elle est simplement activée, par défaut :

- Une seule **adresse MAC** est apprise dynamiquement et elle la seule autorisée.
- En cas de "**violation**", le port tombe en mode **shutdown**.

3.2.5.2.4 Activation de port-security

La fonction s'active en encodant une première fois la commande **switchport port-security** en configuration d'interface dans un commutateur de Cisco

```
(config)#interface G0/1
(config-if)#switchport mode access
(config-if)#switchport port-security
```

3.2.5.2.5 Définition des adresses MAC autorisées

Lorsqu'on configure un port dans un commutateur, on peut fixer le nombre d'adresse MAC autorisée à connecté au niveau du port pour la gestion du réseau. Mais exemple suivant, on fixe le nombre d'adresse MAC autorisée à 10 :

```
(config-if)#switchport port-security maximum 10
```

Les adresses MAC apprises peuvent être **inscrites dynamiquement dans la configuration courante (running-config) avec le mot clé "sticky"** :

```
(config-if)#switchport port-security mac-address sticky
```

Les adresse MAC autorisée peuvent être fixées dans le port qu'il est connecté :

```
(config-if)#switchport port-security mac-address 0000.0000.0003
```

3.2.5.2.6 Mode de "violation"

Une "Violation" est une action prise en cas de non-respect d'une règle **port-security**.

```
(config-if)#switchport port-security violation {protect | restrict | shutdown}
```

- **Mode protect** : dès que la "violation" est constatée, le port arrête de transférer le trafic des adresses non autorisées sans envoyer de message de log.
- **Mode restrict** : dès que la "violation" est constatée, le port arrête de transférer le trafic des adresses non autorisées et transmet un message de log.
- **Mode shutdown** : dès que la "violation" est constatée, le port passe en état **err-disabled** (**shutdown**) et un message de log est envoyé.

En somme, dans un réseau d'entreprise la sécurité des ports particite aussi à la bonne gestion du réseau. Donc l'administrateur du réseau lui seule peut être autorisé à se connecter sur le commutateur via le port dont son adresse MAC est autorisée à connecter. Autre que cette machine va faire ce que l'on appelle une violation du réseau à partir du port.

3.2.6 La haute disponibilité par la redondance des liens et des équipements

La haute disponibilité désigne le fait qu'un service ou une architecture matérielle possède un taux de disponibilité compris entre 99,99% et 100%, c'est-à-dire qui résiste à une panne pour ne pas affecter l'entreprise. Plusieurs techniques permettent d'améliorer la disponibilité des services dans un réseau, en fonction du niveau où l'on se situe :

- Équipements
- Les Liens d'interconnexion

Afin d'éviter toute panne causée par un arrêt de service d'un équipement (Switch, routeur, pare-feu, …), on suggère de mettre en place une réplication des équipements suivants :

- **Switch niveau 3 ;**
- **Pare-feu ;**

- **Routeur ; …**

Donc cette manière de faire, la redondance des équipements permet d'assurer la disponibilité des services lorsqu'un équipement tombe en panne les services continuerons de marcher.
Mais également il y' a la redondance d'accès qui raccordent ces différents équipements. Aussi nommée redondance de liens, elle consiste à fournir plusieurs connexions Internet pour assurer une continuité de service. Si le premier lien tombe, les flux sont redirigés vers le second lien. La redondance d'accès permet d'assurer une plus grande disponibilité. Dans les équipements de Cisco on l'appelle les liens Etherchannel qui crée des liaisons logiques en regroupant tous les liens physiques dans un seul lien logique pour transmettre les paquets. Donc la redondance des liens et celle des équipements permettent d'assurer une haute disponibilité des services dans un réseau d'entreprise et la tolérance aux pannes.

Conclusion

La protection de l'architecture réseau ou les données de l'entreprise passe par une politique de sécurité capable de résister à toutes menaces extérieures. La sécurité doit être prise en compte aussi bien pour les équipements réseaux que pour les systèmes. Même si l'administrateur d'un réseau n'est pas expert du domaine, ne doit pas ignorer les risques accourus et doit être capable de mettre en œuvre une architecture de sécurité répondant aux exigences de l'entreprise en faisant appel aux équipements de sécurité (Porxy, Pare-feu, etc.) et aussi les réseaux virtuels et les VPN. Connaissant les bonnes méthodes de la sécurité des architectures réseau, nous allons dans le chapitre suivant implémenté et déployé une architecture sécurisée d'un réseau d'entreprise.

Chapitre IV :

Implémentation d'une architecture sécurisée d'un réseau d'entreprise

Introduction

Dans cette partie, nous mettons en place une architecture sécurisée d'un réseau d'entreprise qui sera déployée dans le simulateur Packet Tracer. L'architecture est composée de deux sites interconnectés avec le réseau publique Internet : l**e site principal (maison mère) et** l**a succursale (client vpn ou site distant).** Afin de mieux comprendre les fonctionnalités de sécurité qui seront implémentées dans notre architecture sécurisée, nous présentons d'abords une architecture non sécurisée pour ensuite y ajouter les modules de sécurité.

4.1 Architecture du réseau (non sécurisée)

Nous présentons d'abord une architecture globale sans modules de sécurité à la base. Celle-ci sera composé de deux sites reliés par le réseau publique Internet comme le montre la **Figure 51**.

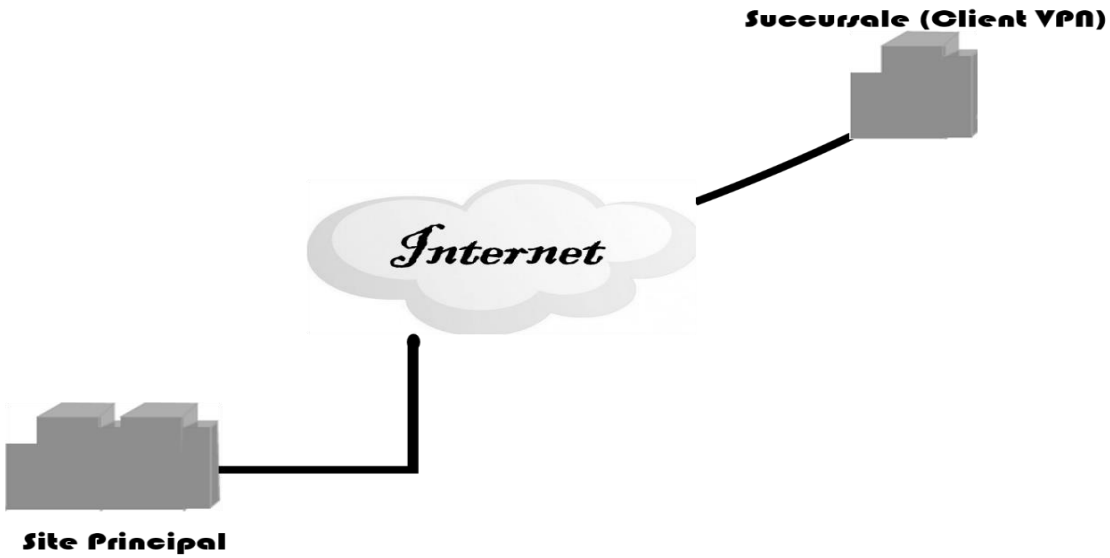

Figure 51 : Topologie Global du réseau

Le site principal ou la maison mère héberge l'ensemble des serveurs de l'entreprise et la succursale (client VPN) qui constitue un point relai stratégique de l'entreprise.

Le personnel informatique est composé d'un ingénieur et un technicien supérieur répartis sur les 2 sites. L'ingénieur basé à la maison mère, a le rôle d'administrer toute l'infrastructure aussi bien le site principale (directement) que la succursale (à distance). Le technicien au sein de la succursale, permet d'effectuer les tâches basiques, et pour les tâches avancées, il va se servir de support à l'ingénieur surtout quand il a besoin d'accès direct au matériel.

4.1.1 La maison mère

Pour une architecture traditionnelle, l'infrastructure est principalement constituée des terminaux des utilisateurs, de switchs de niveau deux (2), de switchs de niveau trois (3) et routeurs. Une architecture globalement non sécurisée interconnecterait les switchs de niveau 2

aux switchs de niveau 3 qui leurs serviraient de passerelles ; vers les routeurs qui vont feraient office de passerelle vers Internet. Et ce dernier est directement connecté à un routeur. La **Figure 52** montre une architecture non sécurisée qui pourrait être déployée pour l'entreprise.

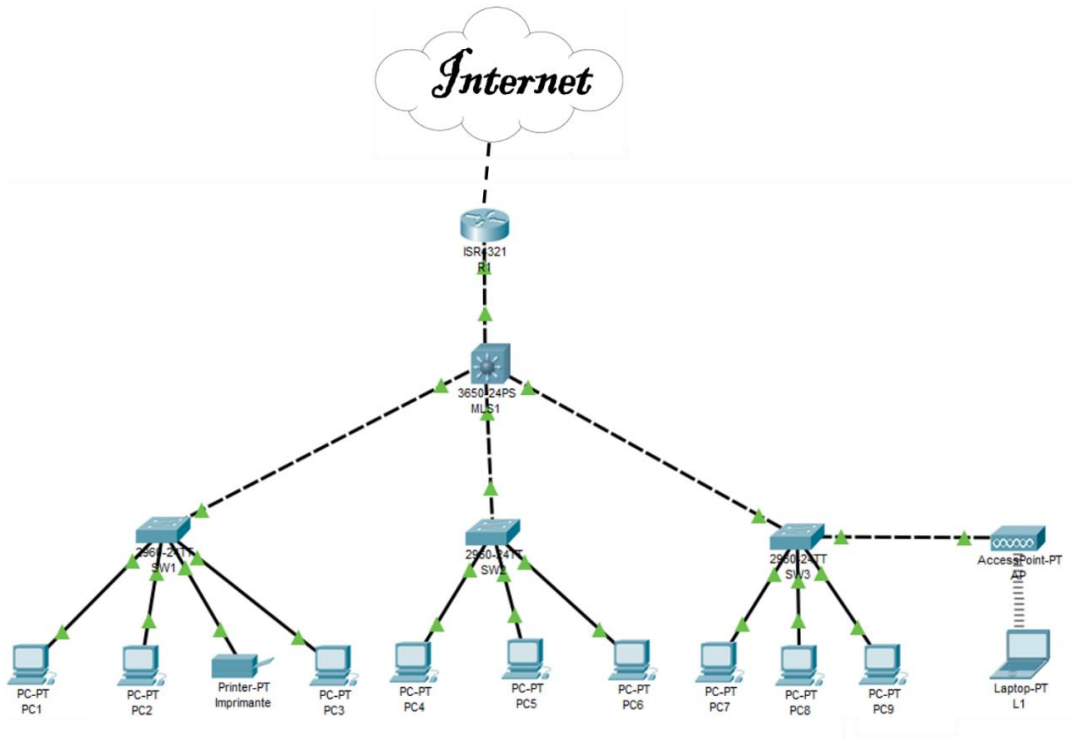

Figure 52 : Infrastructure de la maison mère (Architecture non sécurisée)

Du point de vue physique, cette topologie est non sécurisée, et du point de vue logique, les différents utilisateurs peuvent être regroupés en sous réseaux et seront interconnecté par les switch de niveau 3.

4.1.2 La succursale

Du point de vue physique, cette topologie est non sécurisée, et du point de vue logique, les différents utilisateurs peuvent être regroupés en sous-réseaux et seront interconnecté par les switch de niveau 2.

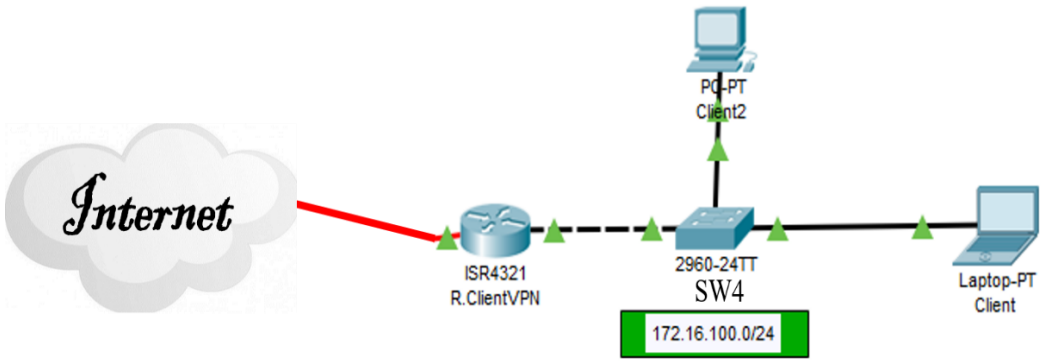

Figure 53 : Infrastructure de la Succursale (Architecture non sécurisée)

L'internet est le réseau public qui interconnecte les deux sites (la maison mère et la succursale du client vpn). Il est composé de réseaux autre que celui de l'entreprise. En guise d'exemple, ce schéma ne le décrit pas parfaitement, il peut être constituer de différents fournisseurs accès à internet (FAI).

4.2 Les différentes couches et fonctions de sécurité à mettre en œuvre

Dans cette partie, nous allons proposer un modèle d'architecture sécurisée et des fonctionnalités à mettre en œuvre. Afin de mieux segmenter les différentes fonctionnalités de sécurité et les rendre plus transparentes, nous avons d'abord travaillé sur un modèle d'architecture sécurisée.

4.2.1 Choix du modèle d'architecture en couches (accès, distribution, cœur)

Le modèle hiérarchique à trois couches proposées par Cisco Systems est celui que nous implémentons : couche d'accès, couche de distribution et couche cœur de réseau. Dans ce modèle, chaque couche apporte ses impératifs et ses besoins, influençant le matériel mis en place ainsi que les configurations et/ou solutions. Même s'il est difficile à mettre en œuvre, un de ces avantages majeurs est que non seulement il intervient lors de la segmentation logique du réseau, mais efficace, rentable, et passe à l'échelle.

- **La Couche d'accès** permet de fournir des points d'extrémités et c'est sur cette couche que les utilisateurs ont un accès direct du réseau. Elle fournit également une connectivité filaire et sans fil, et contient aussi des fonctionnalités et services qui garantissent la **sécurité** et le bon fonctionnement du réseau. La couche d'accès donne aussi une connectivité avec une très grande bande passante, afin de pouvoir prendre en charge un pique de Traffic quand les utilisateurs effectuent plusieurs tâches sur le réseau. Ça peut être par exemple, un envoi de mail avec de grosses pièces jointes ou bien l'ouverture d'un fichier sur un serveur distant. C'est aussi celle qui s'assure l'efficacité de la bonne livraison du trafic.
- **La Couche de distribution** quant à elle regroupe la couche d'accès et fournit en plus une connectivité aux services. C'est dans cette couche qu'on implémente le routage IP aussi bien en statique qu'en dynamique et permet de fournir une évolutivité d'un réseau. La couche de distribution sert de point d'agrégation pour les switchs de la couche d'accès. Ce qui permet de réduire les coûts d'exploitation en rendant le réseau plus efficace. Elle augmente aussi la disponibilité du réseau en enfermant les risques de

pannes dans des zones plus petites. Avec des liaisons redondantes ; elle garantit une haute disponibilité des services et une tolérance aux pannes

- **La Couche Cœur (Couche Core)**, donne une connectivité pour les couches de distribution. Elle est très utilisée dans des environnements LAN de grande taille de certaines entreprises.

Il faut noter que dans le cas d'une petite ou moyenne entreprise moyenne, il n'est préférable d'utiliser l'architecture à trois couches. On peut même utiliser l'architecture à deux couche en sous entendant que la couche cœur et la couche de distribution forment une seule couche dans l'architecture à deux couches.

Donc dans notre projet de mémoire, nous ne sommes mis dans une étude de cas d'une moyenne ou grande entreprise. Ainsi sur le modèle d'architecture hiérarchique à trois couche, nous avons une segmentation en VLAN au niveau de la couche d'accès pour diminuer le domaine de diffusion, séparer les utilisateurs par groupe et permettre un accès sécurisé des administrateurs. La redondance des liens et des équipements sur les couches distributions et cœur permettra d'atteindre une haute disponibilité et d'accroitre la tolérance aux pannes. La mise en place de DMZs, des Pare-feu (Firewalls) au niveau de la couche de distribution permettra d'isoler et de faciliter le déploiement des fonctionnalités des équipements qui hébergeurs de services et des données. Ainsi nous présentons dans la prochaine section, notre proposition d'architecture sécurisé.

4.2.2 Présentation de l'architecture

Ici nous présentons l'architecture en commençant par la segmentation de vlan au niveau de la couche d'accès en suite les zones démilitarisées, les firewalls installés au niveau de la couche de distribution, les choix des liens redondants dans l'architecture pour enfin terminer avec le choix des équipements redondants.

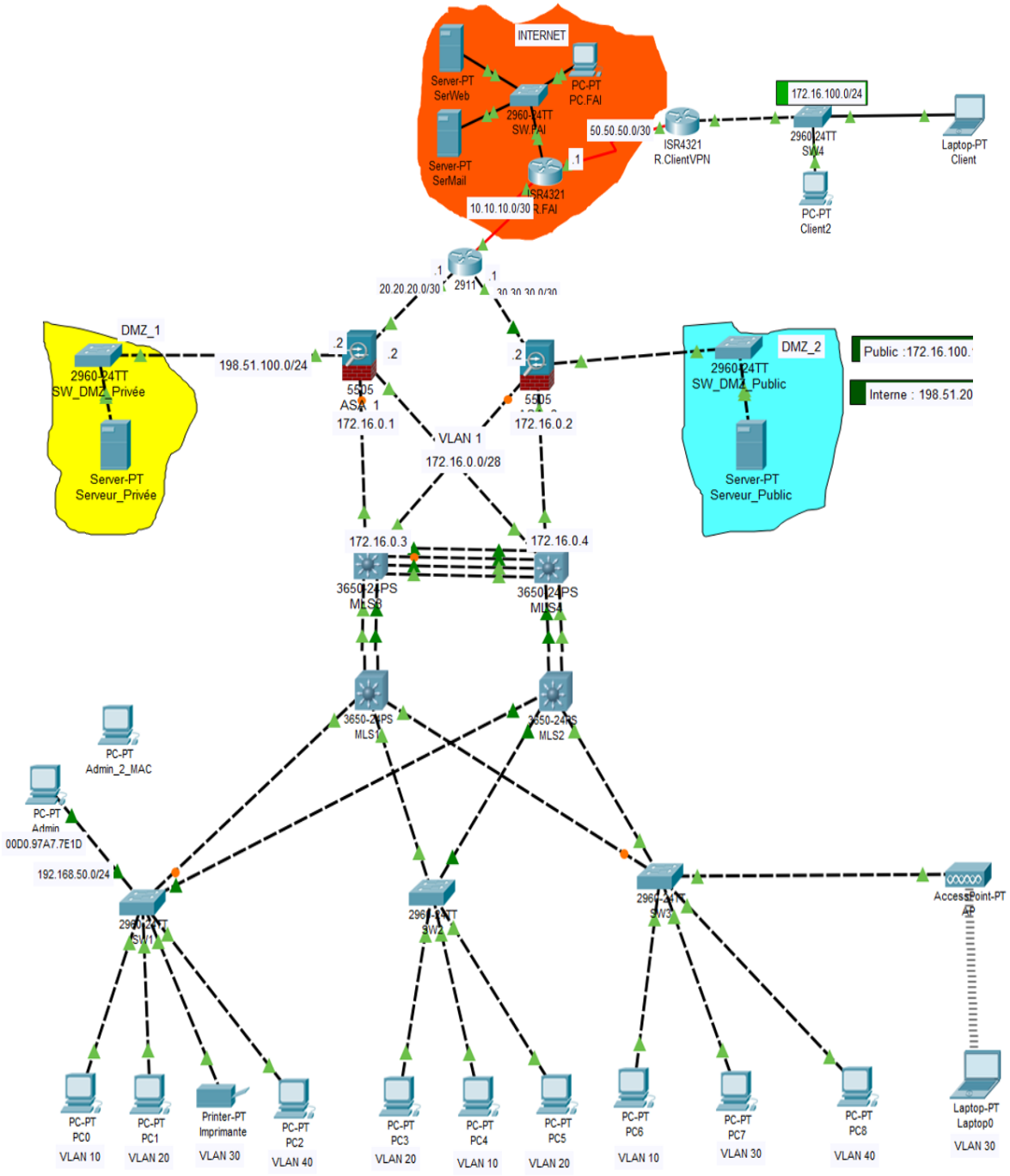

Figure 54 : Architecture Globale

4.2.2.1 La maison mère

En plus des infrastructures citées dans la section **I.1,** le site principal est décomposé en vlans connectés aux pare-feu par l'intermédiaire de switchs de niveau 3 qui en assure l'interconnexion inter-vlans. Ces pare-feu connectés au réseau publique (Internet) via des routeurs assurent le filtrage des paquets entre trois zones : la zone privée qui hébergent les serveurs intranets, la zone publiques ou zone démilitarisée qui hébergent les serveurs extranets, et le réseau publique internet (voir **Figure 55**).

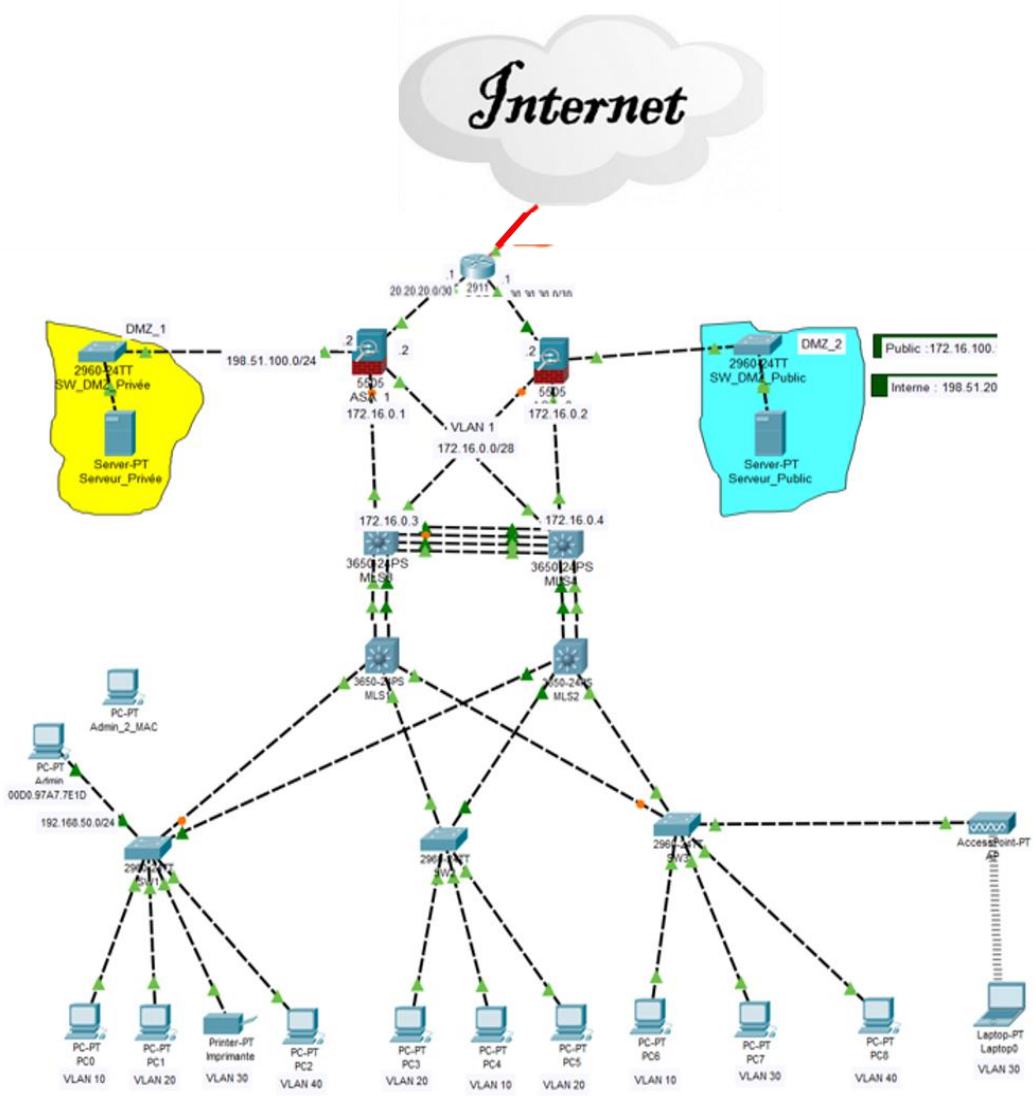

Figure 55 : Infrastructure Maison Mère (Architecture sécurisée)

4.2.2.2 La succursale

La succursale comporte en nombre réduit des switchs d'accès, et une passerelle vers l'Internet (voir **Figure 53**)

4.2.3 Les fonctionnalités de sécurités

4.2.3.1 La Segmentation en VLAN (couche d'accès)

Pour éviter la communication ou l'échange directe entre les utilisateurs dans un LAN et éviter un domaine de broadcast large, nous avons fait une segmentation de la couche d'accès Réseaux locaux Virtuels qui constituent les premiers périmètres de sécurité. Ainsi le réseau a été segmenté en VLAN 10, VLAN 20, VLAN 30, VLAN 40, VLAN 99 et VLAN 100 selon les types d'utilisateurs et la façon dont le réseau doit être géré comme le montre la **Figure 56***Figure 54*. Ci-après la liste nominative des différents VLANs.

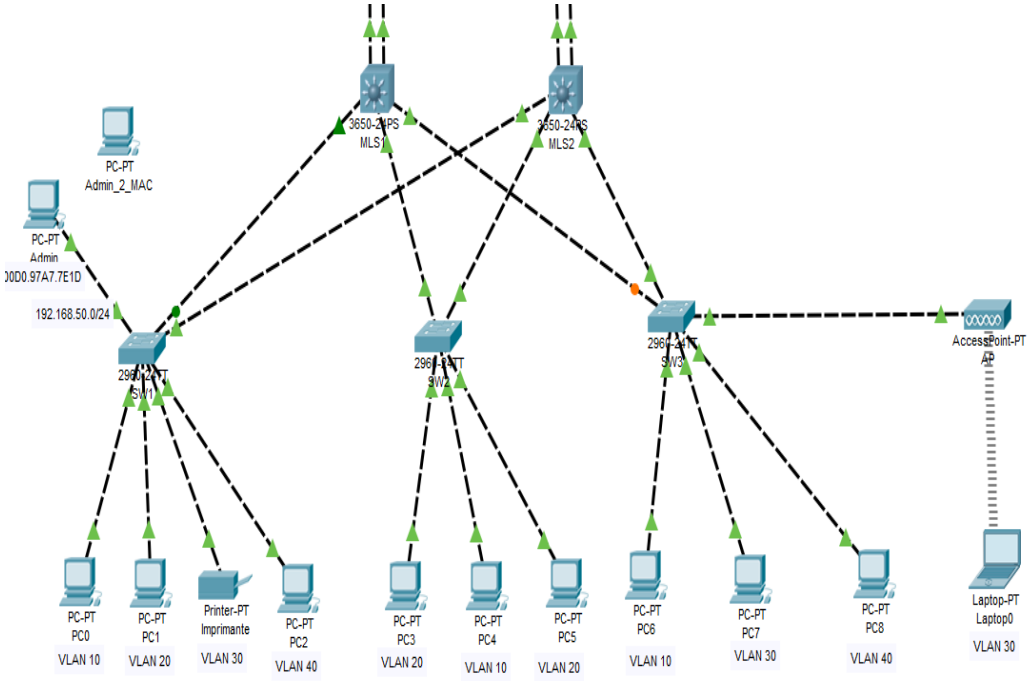

Figure 56 : Segmentation de VLAN

Dans ce réseau on a différents réseaux virtuels :

- VLAN 10 : Service commerciale 192.168.10.0/24
- VLAN 20 : INFORMATIQUE 192.168.20.0/24
- VLAN 30 : AC (Agence Comptable) 192.168.30.0/24
- VLAN 40 :SEC (SECURITE) 192.168.40.0/24
- VLAN 100 : GESTION 192.168.50.0/24
- VLAN 99 : NATIVE

Les VLANs utilisateurs : qui regroupe les utilisateurs par catégories et dont la fonction principale de sécurité est d'isoler les utilisateurs les uns des autres. Ainsi les employés des services critiques comme l'agence comptable se verront détachés des employés des autres services comme celui commercial, ce qui impose aux utilisateurs une communication intra-vlan.

Le VLAN de gestion

Dans les réseaux de grandes tailles, l'administrateur réseau peut parfois manager les équipements du réseau par exemple les commutateurs sans se déplacer Nous nous sommes mis dans une étude de cas d'une moyenne ou grande entreprise. Comme les commutateurs ont un vlan 1 qu'est le vlan par défaut connu par tout le monde, donc il préférable de créer un autre vlan pour manager les commutateurs du réseau en créant un vlan de management, appelé souvent VLAN de GESTION. Nous savons créer un vlan de gestion pour manager tous les

équipements intermédiaires (switchs, routeurs, pare-feu, …) du réseau en leurs attribuant chacun une adresse IP sur le port dont on doit manager l'équipements à distance. On l'a nommé **VLAN GESTION** dont le numéro du VLAN est 100**.** Donc pour manager ces équipements, chaque commutateur aura un vlan 100 qu'est le vlan de gestion ensuite on lui attribue une adresse IP dans l'adresse réseau du VLAN de GESTION.

4.2.3.2 Choix des ports sécurisés

Pour mieux contrôler la gestion des équipements dans le réseau d'une entreprise, l'administrateurs du réseau doit choisir les ordinateurs qu'on doit autoriser à se connectés sur le port de gestion du commutateur. Pour se faire l'administrateur réseau doit fournir les adresses MAC des ordinateurs autorisés à se connecter sur le port. Ici on a pris le port 24 du commutateur comme le port de gestion du réseau et on a mis les Adresses de deux machines. Donc seulement ces deux ordinateurs peuvent connecter sur le port et manager le commutateur et tous les autres commutateurs du réseau.

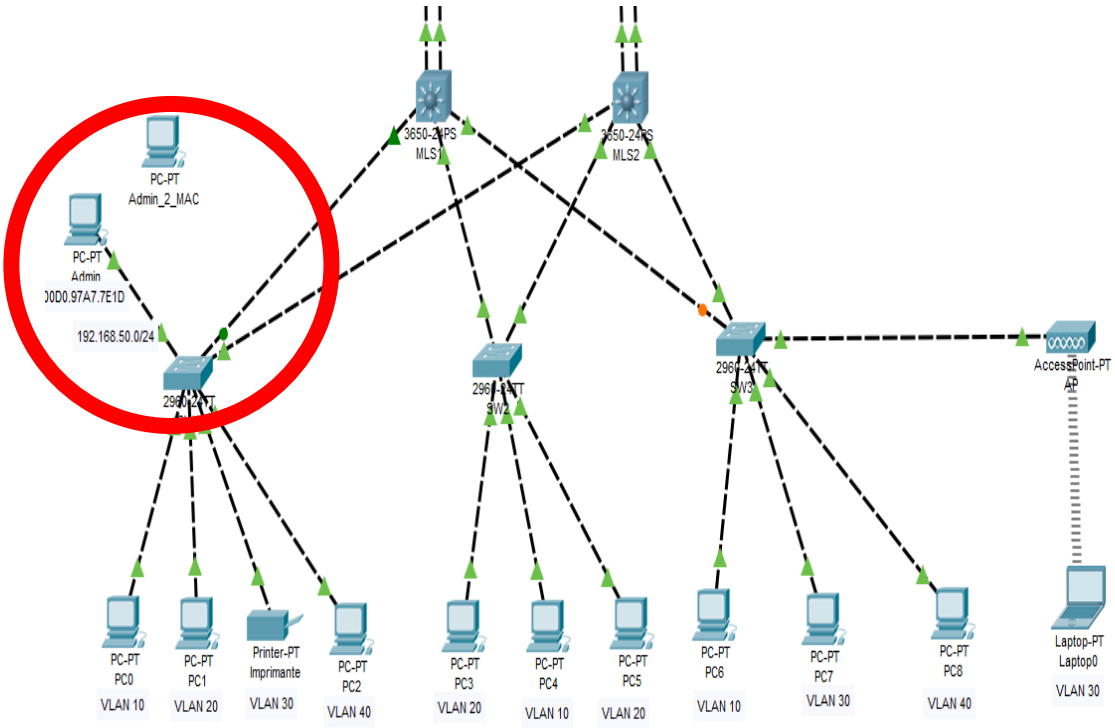

Figure 57 : Sécurité des Ports et Vlan de Gestion

4.2.3.3 Les ports protégés

Comme les terminaux des utilisateurs n'hébergent pas de service, donc une communication entre utilisateurs n'est pas nécessaire. Dans ce cas pour éviter la propagation de virus entre deux terminaux du même VLAN, nous avons mis la fonctionnalité de ports protégés entre VLAN au niveau des switchs de niveau 2.

Exemple de commande de la configuration des ports protégés sur le commutateur SW1 connecté à **MLS1** et **MLS2** pour interdire le trafic entre les PCs du **Vlan 10** (voir **Annexe 1**).

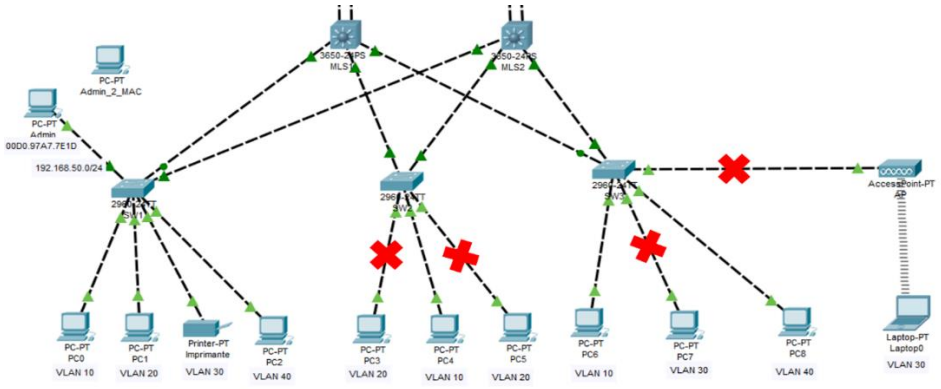

Figure 58 : Ports Protégés

4.2.4 La DMZ (distribution et/ou cœur)

Situées au niveau de la couche de distribution, les DMZ (DMZ_Privée et DMZ_Public) sont reliées chacune par un pare-feu pour le filtrage des trafics entre le LAN privé, le LAN public, l'Internet et la succursale du client vpn. Chacune de ces DMZ héberge des serveurs (serveur web, FTP, DNS, …) et sont accessible soit de l'extérieur et de l'intérieur du réseau. Pour le DMZ_Privée, elle héberge un serveur web et ce dernier n'est accessible qu'à l'intérieur du réseau. C'est-à-dire seuls les utilisateurs interne du réseau peuvent accéder au serveur hébergés dans la DMZ_Privée. Quant à la DMZ_Public, elle héberge des serveurs qui sont accessibles aussi bien de l'extérieur et de l'intérieur. Ainsi les utilisateurs de l'extérieur peuvent directement se connecter aux serveurs de cette DMZ au même pied que les utilisateurs du réseau local. En plus chacune de ces DMZ a une adresse réseau dont les adresse IP que prend les serveurs pour accéder aux serveurs qu'elles hébergent.

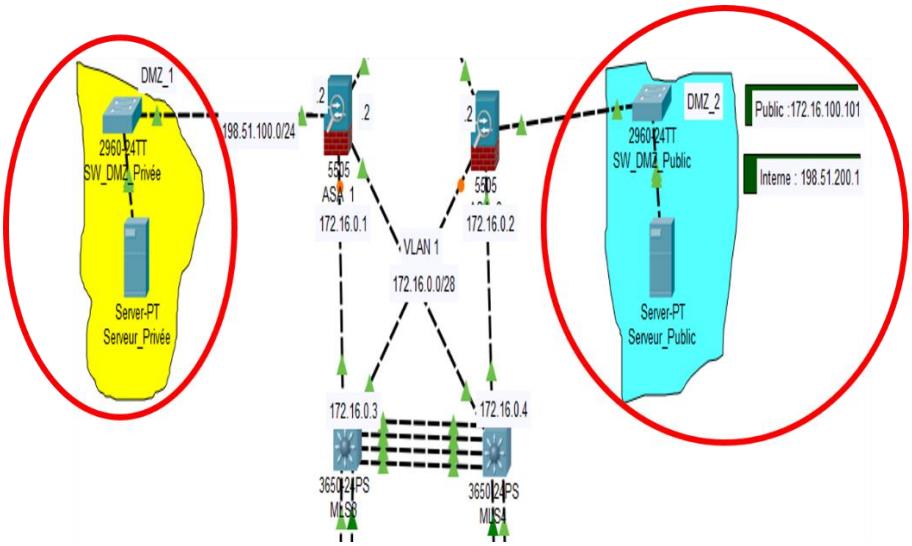

Figure 59 : Les Zones Démilitarisées (DMZ)

4.2.5 Les firewalls et leur position stratégique (distribution et/ou cœur)

Tout comme les antivirus, les firewalls sont en première ligne de défense pour protéger le réseau d'une entreprise. Il contrôle véritablement le trafic réseau de l'entreprise, l'analyse, le sécurise et l'optimise pour la performance des applicatifs métiers

Installés au niveau de la couche de distribution du réseau, les firewalls permettent de filtrer les trafics entres deux réseaux en autorisant ceux qui doivent entrer ou sortir du réseau local ou de les interdire. Comme on a des succursales et que les utilisateurs externes peuvent accéder au LAN. Donc il est mieux d'utiliser les pare-feu pour protéger le réseau local de l'entreprise, en mettant en place un politique de sécurité solide. Pour ce faire on a branché deux firewalls entre le site principal et la succursale pour empêcher les paquets de quitter l'extérieur vers l'intérieur c'est-à-dire accéder au réseau local sans autorisation mais aussi d'accéder au niveau de la zone démilitarisée privée. Chaque pare-feu (Firewall) a trois vlan (vlan 1,2 et 3).

- ✓ Sur le **vlan 1** est connecté le réseau local c'est-à-dire le réseau du site principal et ont comme adresse réseau 172 .16.0.0/24.
- ✓ Sur le **vlan 2** est toujours branché le câble qui va vers internet qui a comme adresse l'adresse du réseau qui est connecté à internet.
- ✓ Sur le **vlan 3** est branché les différentes DMZ que ce soit dmz privée ou dmz public.

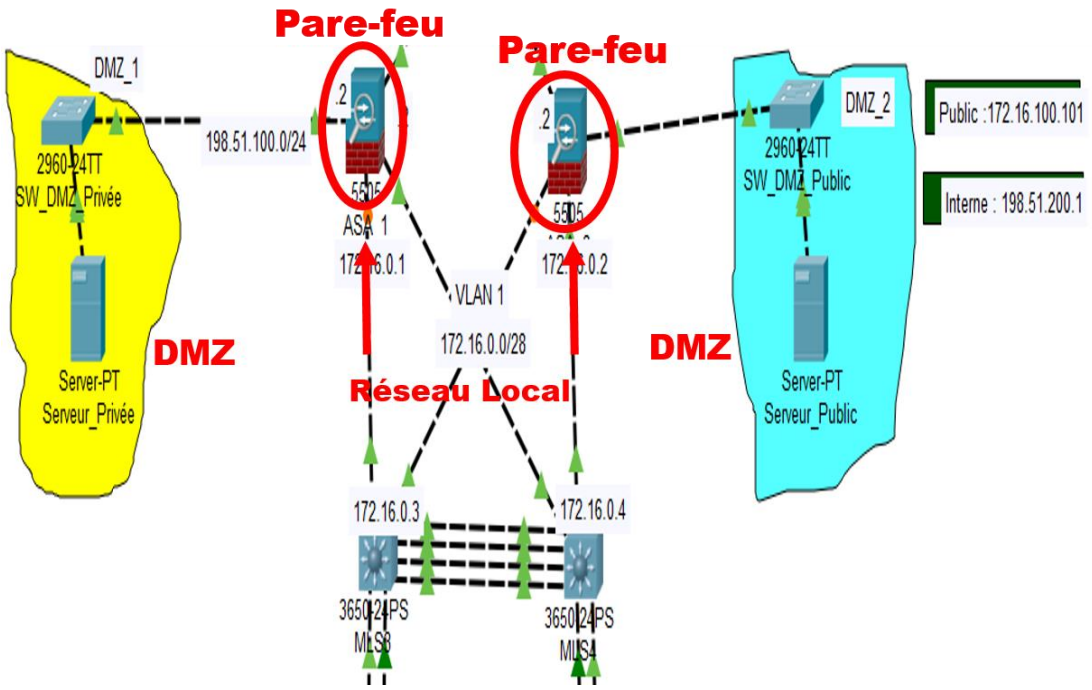

Figure 60 : Les Firewalls (Pare-feu)

4.2.6 Le choix des lien redondants (distribution et/ou cœur)

La redondance de liens, aussi appelée redondance d'accès consiste à fournir plusieurs connexions pour assurer une continuité de service. Si le premier lien tombe, les flux sont redirigés vers le second lien ainsi de suite. La redondance de liens permet d'assurer une plus grande disponibilité. Comme on utilise le simulateur Packet tracer, nous les avons implémentés avec EtherChannel (IEEE 802.3ad) qu'est une technologie d'agrégation de liens qui permet d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique. On l'appelle aussi bonding, LAG, etherchannel, ou encore portchannel.

Son objectif est d'augmenter la vitesse et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs. Elle permet de simplifier une topologie Spanning-Tree en diminuant le nombre de liens. Donc ces liens redondants permettent d'assurer la haute disponibilité des services dans un réseau d'entreprise.

Au niveau de l'architecture, on a créé des liens redondants situés dans la couche de distribution du réseau. Cela nous permet d'éviter la panne du réseau entier quand un lien tombe en panne. Donc la redondance des liens est importante pour que les services soient disponibles en cas de besoin.

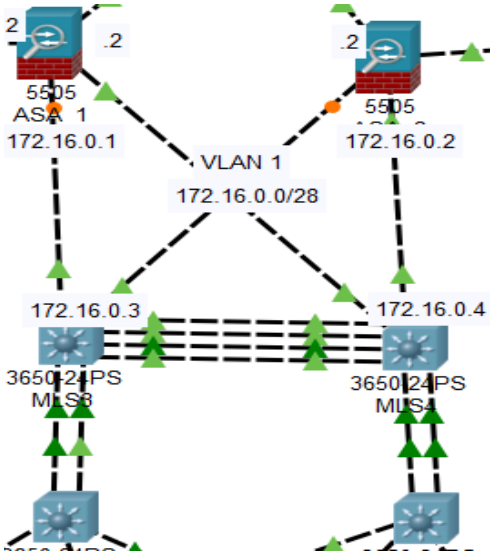

Figure 61 : La redondance des Liens

4.2.7 Choix des équipements redondants (distribution et/ou cœur)

Un réseau d'une entreprise doit fonctionner 24 sur 24 ; 7jours sur 7 jours pour éviter des pertes lourdes qui peuvent affecter l'entreprise. Pour cela, il faut penser à la redondance de certains équipements pour assurer la disponibilité des services demandés même si un équipement tombe en panne. Ces équipements redondants, placés dans des endroits stratégiques permettent

d'assurer la haute disponibilité des services demandés par les utilisateurs d'une entreprise. Ainsi nous avons mis quatre switch de niveau 3 pour éviter qu'en cas de panne que le réseau soit paralysé. De ce fait, si le **MLS3** tombe en panne, le **MLS4** va continuer à fonctionner en attendant la réparation du **MLS3**. C'est la même chose que les deux pare-feu, si l'un tombe en panne l'autre assure le filtre des paquets non autorisées d'entrer ou de sortir du réseau local. Et que tous ces équipements sont logés ou installés dans la couche de distribution du réseau.

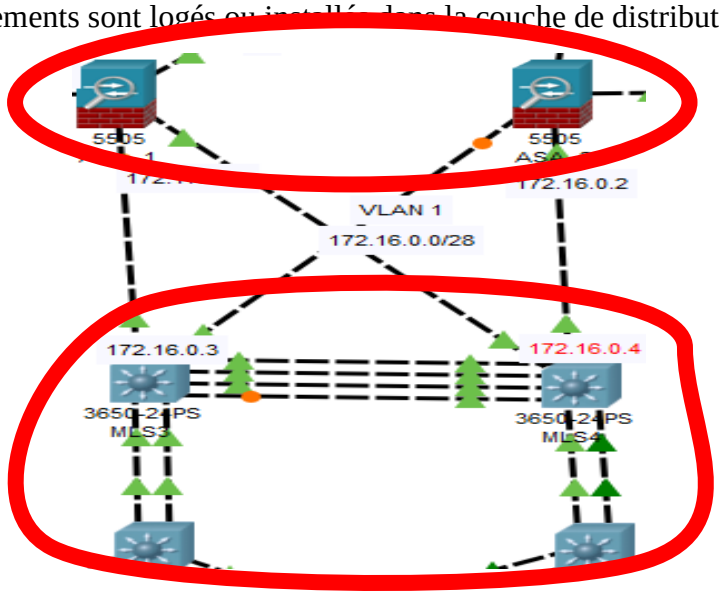

Figure 62 : la redondance d'équipements

4.3 Mise en œuvre

4.3.1 Déploiement de l'architecture sur Packet Tracer

Nous avons déployé l'architecture sécurisé de la **Figure 54** dans l'environnement Packet tracer. Packet Tracer est un outil de simulation visuelle multiplateforme conçu par l'académie de Cisco qui permet aux utilisateurs de créer des topologies de réseau et d'imiter les réseaux informatiques modernes. Le logiciel permet aux utilisateurs de simuler la configuration des routeurs et des commutateurs Cisco à l'aide d'une interface de ligne de commande simulée. Nous avons utilisé la version **8.0.0.211** pour Windows.

Nous avons mis en œuvre notre architecture avec les équipements suivants :

- **Switch Niveau 2 de 2960-24TT :** pour connecter les utilisateurs et les deux DMZ aux pare-feux
- **Switch Niveau 3 de 3650-24PS :** les deux premiers pour connecter les switchs de la couche d'accès des utilisateurs, et les deux derniers sont connectés directement aux pare-feux de la couche de distribution.
- Un point d'accès **AccessPoint-PT** pour connecter un utilisateur sans fil dans le réseau local

- Serveur **server-PT** utilisés ici pour configurer soit les protocols FPT, http, DNS, site web, …
- Pare-feu **ASA-5505** pour autoriser ou interdire les trafics entrants ou sortants entre le site principal et la succursale
- Routeur **ISR4321** utilisé au niveau de la succursale du client vpn

4.3.2 Configuration et implémentation des fonctionnalités de sécurité

4.3.2.1 La couche d'accès

Nous avons créé des VLAN (voir **2.1 la segmentation des VLAN** et **Figure 6**).

Exemple de commande sur les switchs SW1, SW2 et SW3 pour la création du **VLAN 10 (**voir **Annexe 2)**.

Dans cette même couche, nous avons attribué les ports de switch à chaque vlan configuré dans le commutateur. Exemple de commande sur les switch SW1, SW2 et SW3 pour l'attribution des ports au **VLAN 20 (**voir **Annexe 2).**

Nous avons aussi configuré les ports trunk dans chacun des commutateurs de la couche d'accès pour faciliter la circulation des différents vlan.

Exemple de commande de la configuration du port trunk pour le switch 1 de la couche d'accès vers le MLS1 **(**voir **Annexe 2)**.

Par rapport à la sécurité pour les configurations des commutateurs, nous avons mis des mots de passes pour l'utilisateur privilégier et simple.

Exemple de commande pour configurer le mot de passe **enable secret et enable password** du **SW1 (**voir **Annexe 3)**.

4.3.2.1 La couche de distribution

Dans cette couche, nous avons créé des vlan en tapant les mêmes commandes comme la création des vlan dans la couche d'accès sur les switch (SW1, SW2, SW3), la configuration des ports Trunk et les mots de passes **enable** et **eanable password**.

A part ces configurations précedantes, nous avons créé des liens Etherchannel dans les switchs de niveau 3 (**2.4 les Liens redondants**).

Exemple de création des liens Etherchannal (**voir Annexe 4**) sur le switch **MLS1** dans la ligne de commande de Cisco (**Figure 62**).

Après la création du port-channel, on doit le configurer en mode trunk et l'encapsulé pour faciliter l'échange entre les différents vlan du réseau. Exemple de commande pour l'activation du port-channel 1 du commutateur MLS1 de la couche de distribution (**voir Annexe 4**).

Sur cette même couche de distribution, nous avons créé d'autre ports-channel dans les commutateurs qui servent de passerelle au réseau local (**MLS3 et MLS4**). Pour la création du port-channel dans ce switch, c'est les mêmes commandes que la précédente : mais sur ces équipements on aura deux port-channel (port-channel1 et port-channel2), nous avons aussi configuré les ports trunk et l'encapsulation.

Nous avons configuré les autres ports connectés aux pare-feu en mode access au lieu de trunk comme ils serviront de passerelles au réseau local.

Comme ils servent de passerelles, les switch MLS3 et MLS4 détient chacun les différents VLAN du réseau local (**2.1 la segmentation de VLAN**) pour acheminer les trafics venant du LAN vers le réseau publique Internet. Exemple de commande de la céreation des VLAN et l'attribution des adresse IP au différents VLAN créés dans le switch **MLS4** (voir **Annexe 5**).

4.3.2.2 La couche cœur (Core)

Dans cette dernière couche de l'architecture, la couche cœur ; nous avons connecté les deux pare-feu à un routeur qui est à son tours connecté à l'internet. Donc nous avons configuré les deux ports de connexions aux pare-feu à leurs attribuant des adresses IP chacun. Et le port connecté à l'internet, nous avons fait du routage par défaut vers internet.

4.3.2.3 VPN entre site

Pour établir une connexion sécurisée entre le réseau local et la succursale, on doit créer des réseaux privés virtuel appelé aussi le phénomène de tunneling. C'est-à-dire le chemin que va prendre le ou les paquets sera sécurisé de la source à la destination du paquet. Pour cela on a créé un VPN entre la succursale et le réseau local. Exemple de commandes de création d'un réseau privé virtuel au niveau du routeur de la succursale (R.clientVPN) du réseau (**Annexe 6**).

Ce réseau privé virtuel est aussi créé au niveau de chaque pare-feu pour faciliter la mise en place du chemin entre les deux sites et l'autorisation du trafic de paquets.

Sur ce nous allons essayer de tester l'ensemble des fonctionnalités configurées sur les différents équipements du réseau mis en place.

4.3.3 Tests des fonctionnalités

Dans cette partie, nous testons quelques fonctionnalités de sécurité mis en œuvre à travers différents scénarios relatifs au filtrage des paquets. Pour les VLAN, les ports de sécurité, les ports protégés, le VLAN de gestion, les liaisons ether-channel etc.., la visualisation de quelques fichiers de configuration en Annexe permet de bien les mettre en exergue. L'ensemble des communications ont testées avec la commande ping du protocole ICMP.

- **Pour une communication du LAN privé vers le LAN public**

Entre **PC2** et le pare-feu **ASA_1 :** le paquet passe par le **vlan 40,** le Switch de niveau 3 **MLS1,** puis **MLS3** et atteint le pare-feu **ASA_1.** En réponse le même chemin est emprunté au retour.

- **Pour une communication du LAN public vers l'Internet**

Entre **PC0** et le routeur **R.ClientVPN** : le paquet passe par le **vlan 10**, le Switch de niveau 3 **MLS2** et celui du **MLS4,** passe aussi par le pare-feu **ASA_2**, le routeur **R.RE** et attient le **R.ClientVPN**. Le paquet prendra le chemin inverse pour la réponse, mais sera bloqué au niveau du pare-feu **ASA_2** à cause du filtrage.

- **Pour une communication de l'internet vers le LAN privé**

Entre le routeur **R.ClientVPN** et le Switch de niveau 3 **MLS3** : le paquet passe par le routeur **R.CleintVPN**, le routeur de l'entreprise **R.RE** et bloqué par le pare-feu **ASA_1**.

- **Pour une communication de la succursale vers le LAN privé**

Entre le **ClientVPN** et **PC2** : le paquet passe le **ClientVPN**, le Switch de niveau 2 **SW4,** le routeur **R.ClientVPN**, **Internet**, et passe encore par le routeur de l'entreprise **R.RE** avant d'être bloqué par le pare-feu **ASA_2** à cause du filtrage des paquets entrants.

- **Pour une communication du LAN privé vers la succursale**

Entre le **PC1** et **ClientVPN** : le paquet passe par le **vlan 20,** le Switch de niveau 3 **MLS1,** puis **MLS3,** après passe au niveau du pare-feu **ASA_1,** le routeur **R.RE**, **Internet**, ensuite le routeur **R.ClientVPN**, puis le Switch **SW4** avant d'atteindre l'utilisateur **ClientVPN.** En réponse, le paquet prend le chemin inverse pour le retour et bloqué au niveau du pare-feu **ASA_1**.

- **Pour une communication du LAN public vers la succursale**

Entre le Switch niveau 3 **MLS4** et le **ClientVPN** : le paquet quitte le **MLS4**, puis le pare-feu **ASA_2**, passe par le routeur **R.RE**, **Internet**, passe ensuite sur le routeur **R.ClientVPN**, le Switch de niveau 2 **SW4**, et attient le **ClientVPN**. Pour la réponse, le paquet va prendre le même chemin au retour ; mais est bloqué par le **ASA_2**.

4.3.4 Limites et perspectives

Lors de la mise en place de cette architecture, limites liées à certains équipements de Cisco. Nous avons voulu mettre en place deux fournisseurs d'accès à internet dans le réseau pour que l'autre prend le relai en cas de panne. Mais cela présente d'interconnexion, car au niveau des pare-feu de Cisco nous ne pouvons mettre que trois VLANs dont un pour le réseau local, un pour l'internet et le troisième peut-être soit branché au niveau du LAN dans une DMZ qui est le cas dans notre réseau, soit au niveau de l'internet pour un autre fournisseur d'internet. Comme cette possibilité de connexion n'est pas offerte nous n'avons pas été en mesure de respecter la

redondance au niveau des fournisseurs d'accès à l'Internet. Comme nous n'avions pas le cadre pour un déploiement réel, nous avons simulé avec Packet Tracer, l'utilisation de GNS3 serait une étape de transition vers le déploiement réel, cependant nous manquions aussi de PC aussi performant avec des caractéristiques qui pourrait supporter un tel déploiement sur GNS3.
Aujourd'hui, les réseaux d'entreprise sont exposés à des attaques, et deviennent de plus en plus courants, il est important d'avoir des bonnes pratiques de déploiement et d'administration des réseaux. Il est donc important de se tenir informé des failles qui se trouvent dans le réseau afin de prendre des décisions avant que l'entreprise soit affecté.
Et dans le futur, nous comptons nous pencher dans une phase de supervision qui permettra la veille ou la surveillance du réseau, Mais également endurcie la sécurité.

Conclusion

Dans ce chapitre, nous avons mis en place une architecture sécurisée en présentant ces différents compartiments (maison mère et la succursale) avant d'appliquer les fonctionnalités de sécurités. D'abord nous avons fait une présentation de l'architecture sécurisée avant de parler sur le choix des modèles de couches. Ensuite nous avons montré toutes les fonctionnalités de sécurités existantes dans l'architecture que ce soit les pare-feu, les DMZ, les ports protégés, etc… avec leurs positions stratégiques dans une architecture. Enfin nous avons parlé de la mise en œuvre de l'architecture déployé sur Packet Tracer afin de tester les fonctionnalités mis en place.

Conclusion Générale

Dans ce mémoire, nous avons mis en place une architecture sécurisée d'un réseau d'entreprise se trouvant sur plusieurs sites interconnectés avec le réseau publique Internet. Nous avons aussi sécurisé une infrastructure d'un réseau d'entreprise sur plusieurs sites tout en assurant des liaisons d'interconnexion sécurisées entre les sites.

D'abord nous nous sommes intéressés à la configuration de l'architecture en trois couches, sur laquelle nous avons appliqué des techniques de segmentation en VLAN pour le regroupement et l'isolation des utilisateurs. Le VLAN de gestion, la sécurité des ports de switch et l'usage du protocole SSH a permis un accès local et distant plus sécurisé des administrateurs. Afin de mieux contrôler l'accès aux services hébergés dans le réseau depuis l'extérieur, nous avons mis des zones démilitarisées pour contrôler les flux d'entrées/sorties. Les mécanismes de redondance mis sur les équipements et liaisons assurent une haute disponibilité. Enfin, nous avons mis en place un VPN pour assurer une interconnexion sécurisée entre les sites.

La conception de l'architecture en tant que telle nous a permis de comprendre que les réseaux d'entreprise évoluent en fonction des technologies et équipements sous-jacents. Et à l'heure actuelle nous constatons de plus en plus des changements majeurs notamment en termes de fonctionnalités sur les équipements (routeurs, switchs, pare-feu etc…), mais aussi sur les technologies liées aux supports de transmission pour accroitre surtout le débit. Avec de telles évolutions, les modèles d'architectures sécurisées en couche sont appelés peut-être à subir des évolutions.

Pour garantir l'accès aussi bien sur les équipements que sur les services, nous avons mis en place des mécanismes de contrôle d'accès basés sur des règles de filtrage et des points de déploiement sur des endroits stratégiques du réseau. Cela dépend des services dont dispose l'entreprise mais aussi de son implantation sur un ou plusieurs sites.

La tolérance aux pannes et la haute disponibilité n'ont pas été en reste dans nos travaux et dépendent des types de services hébergés au sein de l'entreprise.

En perspectives, nous comptons mettre en œuvre un système de supervision pour prévenir et détecter les intrus. La disponibilité d'un cadre de déploiement nous permettra aussi de faire les tests en situation réelle.

Bibliographie et Webographie

[1] « Réseau d'entreprise », Xyoos. https://cours-informatique-gratuit.fr/cours/reseau-informatique-entreprise/ (consulté le nov. 25, 2021).

[2] « Memoire Online - Conception et déploiement d'une architecture réseau sécurisée : cas de SUPEMIR - Angeline Kone ». https://www.memoireonline.com/11/11/4952/Conception-et-deploiement-dune-architecture-reseau-securisee--cas-de-SUPEMIR.html#_Toc303858730 (consulté le nov. 25, 2021).

[3] « Equipements réseau - Le répéteur ». https://web.maths.unsw.edu.au/~lafaye/CCM/lan/repeteurs.htm (consulté le nov. 25, 2021).

[4] « Vulnérabilités informatiques : quelles sont-elles, quelles sont leurs causes et comment les résoudre ? », Informatique Mania. https://www.informatique-mania.com/linformatique/vulnerabilites-de-informaticas/ (consulté le déc. 14, 2021).

[5] sekurigi, « Les failles informatiques les plus courantes », @Sekurigi, avr. 17, 2018. https://www.sekurigi.com/2018/04/les-failles-informatiques-les-plus-courantes/ (consulté le déc. 14, 2021).

[6] « Les attaques d'usurpation d'identité - FORMIP FORMIP », FORMIP, mars 01, 2020. https://formip.com/les-attaques-dusurpation-didentite/ (consulté le déc. 14, 2021).

[7] « Les 10 types de cyberattaques les plus courants », https://blog.netwrix.fr/. https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-plus-courants/ (consulté le déc. 14, 2021).

[8] S. Adam, « Cours et tutoriels sur les réseaux et l'informatique - Sébastien Adam, un développeur hors du commun... » https://www.sebastienadam.be/connaissances/cours.php (consulté le nov. 27, 2021).

[9] « Adresses IP : tout ce que vous devez savoir », IONOS Digitalguide. https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-quune-adresse-ip/ (consulté le déc. 14, 2021).

[10] D. Seba, CISCO : interconnexion des réseaux à l'aide des routeurs et commutateurs. Editions ENI, 2003.

[11] P. Materne et O. Bonaventure, « 1 Routage IP », 2000.

[12] « Configuration du routage statique - routeur Cisco ». https://routeur.clemanet.com/routage-statique-cisco.php (consulté le déc. 01, 2021).

[13] « Memoire Online - Mise en place d'un réseau VPN au sein d'une entreprise. Cas de la BRALIMA Sarl en RDC - Eric BAHATI - SHABANI », Memoire Online.

https://www.memoireonline.com/01/13/6733/Mise-en-place-dun-reseau-VPN-au-sein-dune-entreprise-Cas-de-la-BRALIMA-Sarl-en-RDC.html (consulté le janv. 04, 2022).

[14] D. Seba, CISCO : interconnexion des réseaux à l'aide des routeurs et commutateurs. Editions ENI, 2003.

[15] B. Martin, Codage,cryptologie et application. pressesPolytechniques et Universitaires Romandes.

[16] J.-L. Montagnier, Construire son réseau d'entreprise. Eyrolles, 2001.

[17] R. Dumont, Cryptographie et Sécurité Informatique INFO0045-2. Université de Liége, 2009.

[18] « Définition Réseau d'entreprise — Dictionnaire informatique », Xyoos. https://cours-informatique-gratuit.fr/dictionnaire/reseau-dentreprise/ (consulté le nov. 01, 2021).

[19] V. Remazeilles, La sécurité des réseaux avec Cisco. Editions ENI, 2009.

[20] J.-F. Carpentier, La sécurité informatique dans la petite entreprise : état de l'art et bonnes pratiques. Editions ENI, 2009.

[21] Sécurité informatique : pour les DSI, RSSI et administrateurs, 5e éd. Paris : Eyrolles, 2016.

[22] P. Atelin et J. Dordoigne, TCP/IP et les protocoles Internet. Editions ENI, 2006.

Annexes

Annexe 1 : Configuration des ports protégés

SW2>

SW2>en

Password:

SW2#config t

Enter configuration commands, one per line. End with CNTL/Z.

SW2(config)#interface fastEthernet 0/1

SW2(config-if)#switchport protected

SW2(config-if)#end

SW2#

SW2#config t

Enter configuration commands, one per line. End with CNTL/Z.

SW2(config)#interface fastEthernet 0/3

SW2(config-if)#switchport protected

SW2(config-if)#end

SW2#

SW2#config t

Enter configuration commands, one per line. End with CNTL/Z.

SW2(config)#interface gigabitEthernet 0/1

SW2(config-if)#switchport protected

SW2(config-if)#end

SW2#

Annexe 2 : Segmentation des VLANs

SW1(config)#
SW1(config)#vlan 10
SW1(config-vlan)#name INFORMTIQUE

SW1(config)#
SW1(config)#int Fastehernet 0/1
SW1(config-if)#switchport access vlan 20

SW1(config)#int Fastehernet 0/24
SW1(config-if)#switchport mode trunk

Annexe 3 : configurer le mot de passe enable secret et enable password

SW1(config)#enable secret mbacke
SW1(config)#enable password diene
SW1(config)#service password-encryption
SW1(config)#service timestamps log datetime msec

Annexe 4 : Création et configuration des liens Etherchannal

MLS1(config)#interface range gigabitEthernet 1/0/4-5
MLS1(config-if-range)#channel-group 1 mode active
MLS1(config-if-range)#
Creating a port-channel interface Port-channel 1
MLS1(config-if-range)#no shut

MLS1(config)#interface port-channel 1
MLS1(config-if)#switchport trunk native vlan 99
MLS1(config-if)#switchport tru
MLS1(config-if)#switchport trunk en
MLS1(config-if)#switchport trunk encapsulation do
MLS1(config-if)#switchport trunk encapsulation dot1q
MLS1(config-if)#switchport mode trunk

Annexe 5 : Création des VLAN et attribution d'adresse IP

MLS4 (config)#int vlan 10
MLS4 (config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
MLS4 (config-if)#ip ad
MLS4 (config-if)#ip address 192.168.10.2 255.255.255.0

Annexe 6 : Configuration de VPN entre sites

R.clientVPN(config)#crypto isakmp policy 10
R.clientVPN(config-isakmp)#encryption aes
R.clientVPN(config-isakmp)#authentication pre-share
R.clientVPN(config-isakmp)#group 2
R.clientVPN(config)#
R.clientVPN(config)#crypto isakmp key ciscocisco address 20.20.20.2
R.clientVPN(config)#crypto isakmp key ciscocisco address 30.30.30.2
R.clientVPN(config)#crypto ipsec transform-set VPN_SET esp-aes esp-sha-hmac
R.clientVPN(config)#crypto map VPN_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R.clientVPN(config-crypto-map)#set peer 20.20.20.2
R.clientVPN(config-crypto-map)#set peer 30.30.30.2
R.clientVPN(config-crypto-map)#set transform-set VPN_SET
R.clientVPN(config-crypto-map)#match address VPN_ACL
R.clientVPN(config)#ip access-list extended VPN_ACL
R.clientVPN(config-ext-nacl)# permit ip 172.16.100.0 0.0.0.255 192.168.0.0 0.0.255.255