République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. Mira-Béjaia

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Faculté de Technologie
Département d'Automatique,Télécommunication et d' Électronique(ATE)

Mémoire de fin d'étude

En vue de l'obtention du diplôme en MASTER télécommunications.

Option : Réseaux et télécommunications.

Thème

Configuration et administration d'un réseau de campus sécurisé

Présenté par :
M^r DERGUINI Redha
M^lle TALEB Céline

Devant le jury composé de :

Présidente :	*M^me GHERBI* Meriem	Université de Béjaia.
Encadreur :	*M^r BENAMIROUCHE* Nadir	Université de Béjaia.
Examinatrice :	*M^me GHENNAM* Souhila	Université de Béjaia.

Année universitaire 2021/2022

Remerciment

Par-dessus tout, nous remercions Dieu tout-puissant de nous avoir accordé la vigueur, le courage et la patience pour accomplir notre projet.

Nous exprimons notre profonde gratitude à nos chers parents et familles pour leur soutien et leurs encouragements.

Nous présentons tous nos respects et nos sincères remerciements aux membres du jury Mme Gherbi et Mme Ghennam pour nous avoir fait l'honneur d'accepter de juger notre modeste travail.

Nous remercions notre superviseur de l'université Mr. BENNAMIROUCHE Nadir pour sa confiance, ses encouragements et ses conseils pour mener à bien notre travail.

Nous tenons à remercier Mr. AZNI Mohammed pour sa présence et sa disponibilité .

Nos sincères remerciements au personnel de l'entreprise SONATRACH Bejaia, en particulier à Mr. HANANE Abdelhamid, notre maître de stage, pour sa patience, son sérieux et sa grande disponibilité tout au long de notre stage au sein de l'entreprise.

Nous adressons nos sincères remerciements à toutes les personnes qui nous ont aidé de près ou de loin à élaborer notre projet.

Dédicace

C'est avec une immense gratitude que je dédie ce modeste travail

À **mes très chers parents** pour leurs indéfectibles soutient, leurs patiences et leurs confiances en moi tout le long de mon parcours dans les bons moments comme dans les mauvais, pour que je puisse atteindre mes objectifs, qu'ils puissent trouvé dans ce travail toute ma reconnaissance et mon amour et que dieu les protéges et que dieu leurs réserve la bonne santé et une longue vie inchallah.

À **mon frère, Mustapha**

À **mes oncle**

À **mes tantes**

Pour leurs soutiens et leurs conseils.

À **Toute personne** qui m'a aidé de prés ou de loin durant mes études.

Du fond du cœur merci.

Redha

Dédicace

C'est avec un énorme plaisir que je dédie ce travail

A la mémoire de mon défunt oncle Abderrahmane, qui m'a été un deuxième père ,qu'il repose en paix , puisse Allah le miséricordieux lui ouvre les portes de son paradis.

A Mes très chers parents pour leurs sacrifices leurs amours et leurs confiances en moi ,ils ont tout fait pour mon bonheur et ma réussite ,qu'ils trouvent dans ce modeste travail toute ma reconnaissance et mon amour et que dieu leur réserve la bonne santé et une longue vie inchallah.

À mon frères **Krimou**
À ma soeur **Feryel** et son mari **Salim**
À mes deux neveux adorés **Cécile** et **Salas**
Je vous aime
À ma **famille** et mes **amis**

À Toute personne qui m'a aidé et encouragé de prêt ou de loin toute au long de mes études qu'ils trouvent ici toute ma gratitude.

Céline

Table des matières

Liste des tableaux

Table des figures

Listings

Liste des abréviations

ACL : Access Control List.
ARP : Address Resolution Protocol.
AES : Advanced Encryption Standard.
CIA : Confidentiality, Integrity, Availability.
DHCP : Dynamic Host Configuration Protocol.
DMZ : Zone démilitarisée.
DNS : Domain Name Service.
HSRP : Hot Standby Router Protocol.
ICMP : Internet Control Message Protocol.
IEEE : Institute of Electrical and Electronics Engineers.
ISO : International Standard Organisation.
IP : Internet Protocol.
IPsec : Internet Protocol SECurity.
LAN : Local Area Network.
MAC : Media Access Control.
MAN : Metropolitan Area Network.
MITM : Man In The Middle.
NAT :Network Address Translation.
NOS : Network Operating System.
OSI : Open Systems Interconnection.
OSPF : Open shortest Path First.
PAN : Personnel Area Network.
PPP : Point to Point Protocol.
PPTP : Point To Point Tunneling Protocol.
QOS : Quality Of Service.
RARP : Reverse Address Resolution Protocol.
RSA : Rivest–Shamir–Adleman.
SNMP : Simple Network Management Protocol.
SSL : Secure Socket Layer.
SSH : Secure SHell.
STP : Spanning-Tree Protocol.
TCP : Transmission Control Protocol.
TLS : Transport Layer Security.
UDP : User Datagram Protocol
VRRP : Virtual Router Redundancy Protocol
VLAN : Virtual Local Area Network

VPN : Virtual Private Networl
VTP : Virtual Trunking Protocol
WAN : Wide Area Network
WLAN : Wireless LAN

Introduction générale

Aujourd'hui, PME ou GAMAM (ex-Gafam) ne peuvent se passer d'outils informatiques qui leur permettent d'échanger des informations et des ressources au niveau local ou même entre sites distants. Le besoin de transmettre des informations entre l'entreprise et ses différents sites distants à donner lieu à son ouverture à internet. Cependant cette dépendance des entreprises à internet les a rendues plus exposées aux attaques ciblées ou non, généraliser et véhiculer par les réseaux. Cette atmosphère malveillante peut aboutir à de graves conséquences Professionnelles et financières, ce qui pousse les entreprises à imposer des politiques de sécurité afin de garantir l'intégrité, la confidentialité et la disponibilité de l'information..

La sécurité est devenue un domaine d'étude à part entière, s'imposant comme étant l'élément essentiel et clé de toute entreprise qui veulent protéger ces ressources réseaux quelle que soit sa taille, son domaine d'activité et sa répartition géographique. Et ce par l'application d'une stratégie de sécurité efficace qui repose sur le choix et la capacité des administrateurs du réseau à déployer les solutions adéquates.

Dans le cadre de notre projet de fin d'étude, l'entreprise Sonatrach RTC de Bejaia nous a permis d'effectuer un stage dans lequel ils nous ont proposé l'étude d'une architecture réseau. L'objectif de cette étude et de proposer une nouvelle architecture plus sécurisée en cas de panne ou de potentielle attaque contre leurs réseaux, en mettant des solutions sûres afin d'améliorer la sécurité de la topologie proposée et en assurant un bon fonctionnement de cette dernière.

La réalisation de ce projet a été organisée en 4 chapitres, à savoir :

- Le premier chapitre sera dédié aux généralités des réseaux informatiques, en présentant les différents types de réseau, les modèles, et certains protocoles.
- Le deuxième chapitre sera axé sur l'administration des réseaux et sur l'aspect sécuritaire de ces derniers.
- Le troisième chapitre sera conçu à la présentation de l'organisme d'accueil et l'étude de la topologie proposée, dans lequel nous allons exposer les problématiques et proposer des solutions fiables.
- Le quatrième chapitre sera consacré à la réalisation et la configuration des solutions envisagées.

Enfin, notre mémoire sera clôturé par une conclusion générale qui décrit les connaissances acquises lors de la réalisation de notre projet de fin d'étude.

Chapitre I

Gènèralité sur les réseaux

I.1 Introduction

De nos jours, les réseaux informatiques sont devenus indispensables pratiquement dans tous les domaines de la vie, ils ont pris une importance majeure dans le fonctionnement des entreprises, ces dernières sont dotées d'un réseau afin d'être plus efficientes.

Les besoins d'échanges de données informatiques entre systèmes plus ou moins éloignés sont multiples : transmission de messages (messagerie), partage de ressources, transfert de fichiers, consultation de base de données, gestion de transactions, et l'exécution de programmes à distance.

Dans ce premier chapitre, nous allons mettre en revue quelques notions de base sur les réseaux, que nous jugeons nécessaires de les rappeler très brièvement pour une meilleure compréhension de l'avancement du notre travail.

I.2 La définition d'un réseau

Nous pouvons définir un réseau informatique comme étant un ensemble d'équipements informatiques (ordinateurs, périphériques... etc.) interconnectés entre eux via des supports de communication afin de réaliser le partage des différentes ressources matérielles et/ou logicielles existantes.Il existe deux types de réseaux :

- **Le réseau filaire :** c'est un réseau qui utilise des câbles(Ethernet, cuivre (RJ45)...) pour relier les ordinateurs et les périphériques.
- **Le réseau sans fil :** c'est un réseau numérique qui connecte les différents postes entre eux par des ondes radio. c'est une technique utilisée par des entreprises afin de limiter l'utilisation de câbles entre diverses localisations.

I.3 Les types de réseaux

Il existe quatre types de réseaux en fonction de la localisation, de la distance et du débit :

1. **Réseau PAN :** est un réseau personnel. IL a pour objectif de faire communiquer des appareils qui se trouvent dans la même pièce (souris, clavier, imprimante, etc). Il s'étend sur une dizaine de mètres.
2. **Réseau LAN :** c'est un ensemble d'ordinateurs et d'équipements informatiques reliés les uns aux autres dans un même bâtiment, site ou dans des sites différents ayant un air géographiquement proche ne dépassant pas 10 Km. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s et 1 Gbit/s.
3. **Réseau MAN :** est un réseau qui couvre une métropole (ville), interconnectant plusieurs LAN géographiquement proche à des débits supérieurs à 100 Mbit/s, il assure la liaison entre deux ou plusieurs sites. Dans ce type de réseau, la distance entre les sites ne dépasse pas 200 Km.
4. **Réseau WAN :** réseau étendu à longue distance constituée par l'interconnexion de plusieurs réseaux LANs et MANs. sur des distances à l'échelle d'un pays, voire d'un continent ou encore toute la planète à des débits importants, supérieur à 100 Mbits/s, Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus

approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

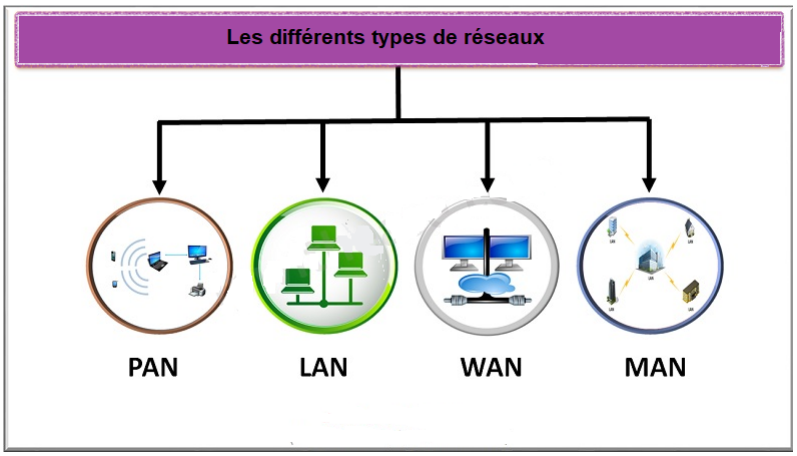

FIGURE I.1 – les types de réseaux

I.4 la topologie d'un réseau

La topologie désigne la manière dont les équipements sont interconnectés en réseau. On distingue généralement les topologies suivantes :

- **Topologie en bus :** c'est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire des câbles, généralement de type coaxial tel qu'il est illustré dans la figure (I.2). Une seule station émet en même temps. À chaque extrémité, le réseau est terminé par un bouchon, qui empêche l'apparition de signaux parasites. Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, si l'une des connexions est défectueuse, l'ensemble du réseau est affecté.

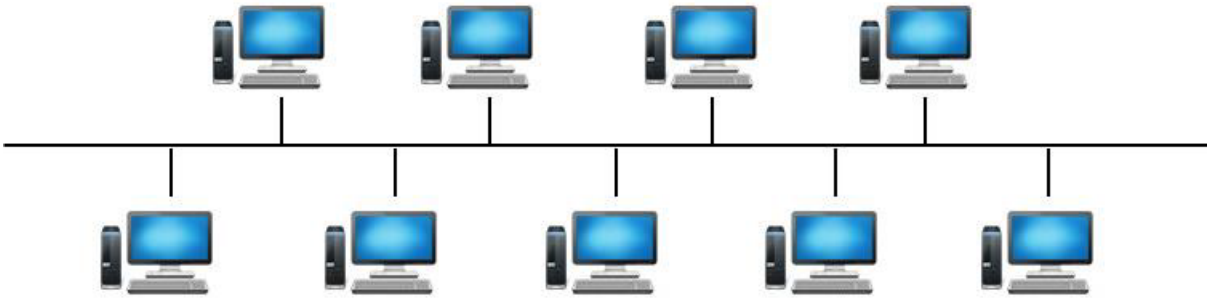

FIGURE I.2 – la topologie en bus

- **Topologie en étoile :** la topologie en étoile qui est la topologie la plus utilisée dans les réseaux locaux, dans cette topologie les ordinateurs du réseau sont raccordés à un point central appelé concentrateur (hub) tel qu'il est montré dans la figure (I.3). Le concentrateur a pour rôle d'assurer la communication entre les différentes jonctions. Les réseaux de cette topologie sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau.

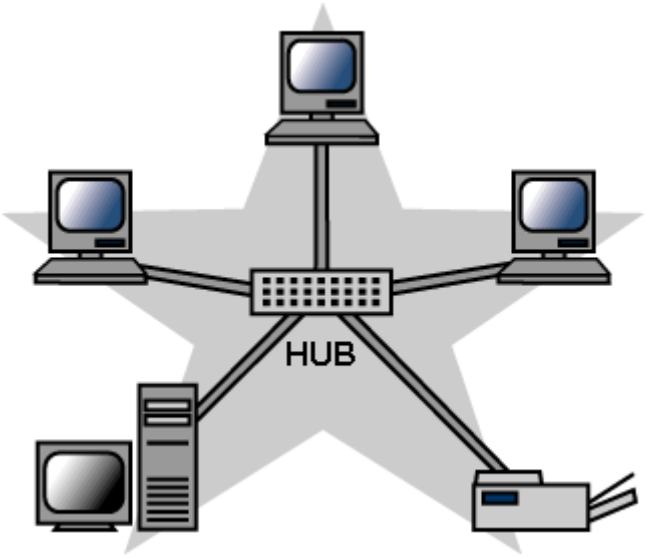

FIGURE I.3 – la topologie en étoile

- **Topologie en anneau :** Dans un réseau possédant une topologie en anneau, les ordinateurs sont théoriquement situés sur une boucle comme le démontre la figure(I.4) et communiquent chacun à leur tour. Les deux principales topologies logiques utilisant cette topologie physique sont Token Ring (anneau à jeton) et FDDI (Fiber Distributed Data Interface).

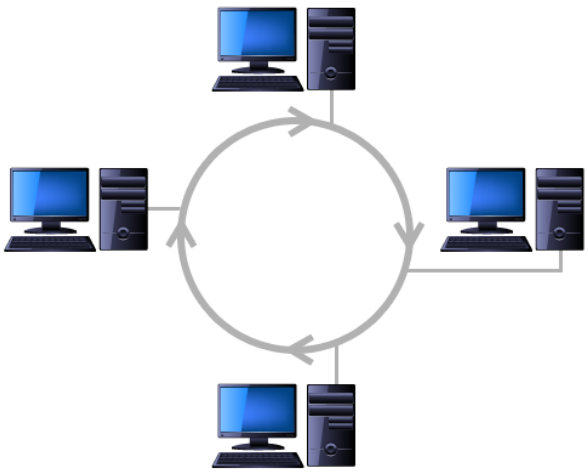

FIGURE I.4 – la topologie en anneau

I.5 Les modèles de référence d'un réseau

La transmission d'informations entre deux programmes informatiques sur deux machines différentes passe par deux modèles :

- Le modèle OSI,
- Le modèle TCP/IP.

I.5.1 Le modèle OSI

Le modèle OSI est le standard en matière de normalisation de tous les systèmes ouverts normalisés par ISO, les produits proposés par les fournisseurs pour les réseaux sont conçus d'après les spécifications (règles) de modèle OSI.

Le modèle OSI est un modèle en 7 couches comme l'illustre le schéma de la figure (I.5). Chaque couche fournit des services directement à la couche supérieure. Le rôle de chacune des couches est :

1. **La couche Physique** : Elle définit les spécifications mécaniques (connecteur), électriques (niveau de tension), et fonctionnelles pour établir les connexions physiques.

2. **La couche Liaison de données** : Elle est responsable de l'acheminement sans erreur des blocs d'informations appelés trame.

3. **La couche Réseau** : Elle permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau.

4. **La couche transport** : Elle est chargée du transport des données, de leur découpage en paquets et de la gestion des éventuelles erreurs de transmission.

5. **La couche session** : Elle définit l'ouverture et la destruction des sessions de communication entre les machines du réseau.

6. **La couche présentation** : Elle définit le format des données manipulées par le niveau applicatif (leur représentation, éventuellement leur compression et leur chiffrement) indépendamment du système.

7. **La couche application** : Elle assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.

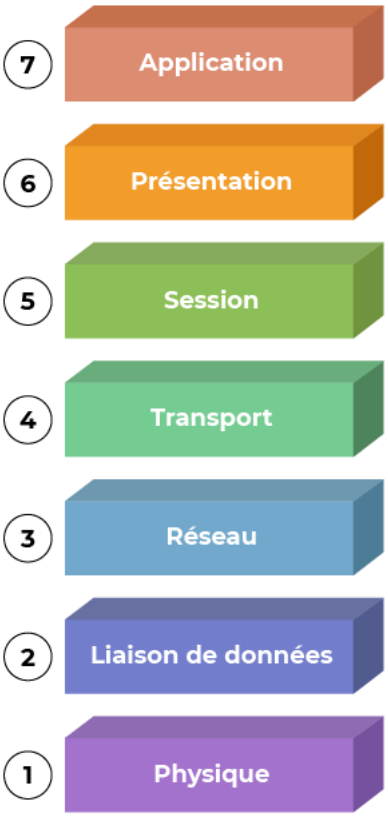

FIGURE I.5 – les couches du modele OSI

I.5.2 Le modèle TCP/IP

Le modèle TCP/IP désigne une architecture réseau à quatre couches, illustré par la figure(I.6) ci-dessous , dans laquelle les protocoles TCP et IP jouent un rôle prédominant, constituant ainsi la structure la plus courante. Les tâches de chacune des couches sont :

1. **La couche accès réseau** :Elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé .

2. **La couche Internet** : Elle est chargée de fournir le paquet de données (datagramme).

3. **La couche transport** : Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.

4. **La couche application** : Elle englobe les applications standard du réseau (Telnet, SMTP, FTP, ...).

FIGURE I.6 – les couches du modele TCP/IP

I.6 Les équipements de base d'un réseau informatique

I.6.1 Les unités hôte

L'hôte est une unité directement connectée au segment réseau, on les retrouve sous la forme d'un ordinateur, serveur, scanner ou imprimante. Pour les relier, il faut des équipements intermédiaires.

I.6.2 Switch (Commutateur)

est un appareil qui relie les hôtes qui y sont connectés au réseau en lisant leurs adresses MAC comprises dans les trames. Intervenant au niveau de la couche 2 OSI et au niveau 1 du modèle TCP/IP. Les commutateurs dirigent des informations vers des destinations spécifiques sur le réseau.

I.6.3 Routeur

est l'élément intermédiaire qui relie deux ou plusieurs réseaux. Il fournit le routage des paquets de données d'une interface à une autre. Il fonctionne sur la troisième couche du modèle OSI (couche réseau), grâce à des protocoles de routage, il peut choisir le meilleur ou le plus court chemin par lequel faire transiter le paquet.

I.6.4 Pont

est élément actif qui assure l'interconnexion de deux réseaux. Un pont filtre les trames et laisse passer les blocs destinés au réseau raccordé. En général, un pont permet de passer d'un réseau vers un autre réseau de même type, mais il est possible d'avoir des ponts qui transforment la trame pour l'adapter au réseau raccordé. Par exemple, un réseau Ethernet peut être connecté à un réseau Token-Ring par un tel pont.

I.6.5 Le hub

c'est un concentrateur capable de récupérer le signal arrivant d'une entrée et de le dupliquer vers l'ensemble des portes de sortie. Le signal est en général réamplifié, car les données sont enregistrées dans des mémoires du type registre à décalage. Dans ce cas, les hubs sont dits actifs, c'est-à-dire qu'ils possèdent des éléments qui doivent être alimentés électriquement.

I.7 L'adressage IP

L'adresse IP est un numéro unique de 32 bits utilisés pour identifier chaque ordinateur connecté au réseau. Le numéro est divisé en 4 par 8 chiffres, allant de 0 à 255, séparés par des points. L'adresse IP est divisée en deux parties, la partie réseau et la partie hôte. Le premier identifie le réseau auquel la machine est connectée et le second identifie la machine connectée à ce réseau. Pour identifier ces deux parties, chaque adresse est liée à un masque de sous-réseau qui vous permet de définir le réseau sur lequel elle se trouve. Les adresses IP sont divisées en plusieurs catégories :

Classes des adresses	Plages	Masque
A	0.0.0.0 à 127.255.255.255	255.0.0.0
B	128.0.0.0 à 191.255.255.255	255.255.0.0
C	192.0.0.0 à 223.255.255.255	255.255.255.0
D	224.0.0.0 à 239.255.255.255	240.0.0.0
E	240.0.0.0 à 255.255.255.255	non défini

TABLE I.1 – Classes et masques réseaux

Certaines adresses réseau sont réservées aux réseaux privés :

- Classe A : 10.0.0.0 à 10.255.255.255.
- Classe B : 172.16.0.0 à 172.31.255.255 .
- Classe C : 192.168.0.0 à 192.168.255.255 .

I.8 Types de Routage

Il existe deux types de routage qui sont les suivants :

I.8.1 Le routage statique

Dans le routage statique, la table est remplie manuellement par l'administrateur réseau, ce dernier doit gérer le routage de chaque unité du réseau. Il est utilisé pour les petits réseaux ou les réseaux terminaux. Dans le routage statique, les informations de routage sont mises à jour manuellement.

I.8.2 Le routage dynamique

Avec le routage dynamique, la table sera automatiquement remplie, et les informations sont automatiquement mises à jour à l'aide des protocoles.

I.9 Les protocoles

Les protocoles qui seront décrits dans ce qui suit seront classés selon les couches du modèle OSI :

I.9.1 Protocoles d'application

I.9.1.1 Le DNS

C'est le service informatique distribué utilisé pour traduire les adresses IP utilisés pour l'adressage des équipements informatiques en noms de domaines.

I.9.1.2 Le protocole DHCP

C'est un protocole réseau dont son rôle est d'assurer la configuration automatique des adresses IP d'une entité informatique adressable, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.

I.9.1.3 Le protocole SNMP

C'est un protocole de la couche application qui facilite l'échange d'informations de gestion entre les dispositifs d'un réseau. Le SNMP permet à des administrateurs réseaux de contrôler l'état du réseau, détecter et résoudre les problèmes du réseau, et de prévoir le développement du réseau, si jamais celui-ci arrive à saturation.

I.9.1.4 Le protocole SSH

Est le protocole le plus sécurisé ; grâce aux algorithmes cryptographiques robustes inclus dans ce protocole, il est souvent utilisé pour protéger des communications de type console ou transferts de fichiers.

I.9.2 Protocoles de transport

I.9.2.1 Le protocole TCP

C'est un protocole de type session responsable du service de transmission fiable de données avec détection et correction d'erreurs.

I.9.2.2 Le protocole UDP

C'est un protocole de transmission peu fiable, il n'établit pas de session entre deux machines et il n'intègre aucun système de correction d'erreurs.

I.9.3 Protocoles réseaux

I.9.3.1 Le protocole IP

C'est un protocole de communication de réseau informatique par commutation de paquets, il est de niveau réseau, et il assure un service d'adressage unique pour l'ensemble des terminaux connectés.

I.9.3.2 Le protocole ICMP

C'est un protocole qui assure un dialogue IP/IP ; il est utilisé par la commande PING qui permet de savoir si un ordinateur est bien connecté au réseau.

I.9.3.3 Le protocole OSPF

C'est un protocole de routage IP interne de type protocole à état de liens (link-state protocol). Ce protocole n'envoie pas aux routeurs adjacents le nombre de sauts qui les sépare, mais l'état de la liaison qui les sépare, [1].

I.9.4 Protocoles de laision de données

I.9.4.1 Le protocole ARP

C'est un protocole qui permet d'associer une adresse logique (IP) à une adresse physique (MAC) dans un réseau local.

I.9.4.2 Le protocole RARP

Signifie Protocole ARP inversé, il permet à une station de connaître son adresse IP à partir d'une table de correspondance entre adresse MAC (adresse physique) et adresses IP hébergée par une passerelle (gateway) située sur le même réseau local (LAN).

I.9.4.3 Le protocole STP

STP est un protocole adapté aux ponts et aux commutateurs. Le but de ce protocole est de construire un arbre qui recouvre tout le réseau, pour que tout point du réseau soit accessible à partir de toutes les feuilles de l'arbre. Sa principe fonctionnalité est de détecter les boucles et de les supprimer en désactivant certaines interfaces de certains ponts afin d'obtenir une architecture arborescente du réseau local, [2].

I.9.4.4 Le protocole VTP

VTP est un protocole utilisé pour configurer et administrer les VLANs sur les périphériques CISCO. VTP permet d'ajouter, renommer ou supprimer, un ou plusieurs réseaux locaux virtuels sur un seul commutateur qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau. VTP permet ainsi d'éviter toute incohérence de configuration de VLANs sur l'ensemble d'un réseau local, [2].

I.10 Conclusion

Ce chapitre était un passage sur la présentation de tout ce qui concerne les réseaux en général à savoir les différents types et topologies, les équipements de base, les modèles de référence OSI, et TCP/IP, ainsi que les protocoles. Nous détaillerons l'administration et la sécurité des réseaux dans le chapitre qui suit.

Chapitre II

Administration et Sécurité des réseaux

II.1 Introduction

L'administration des réseaux informatiques est l'une des discipline clés dans la mise en place d'un réseau de toute entreprise, à l'aide des outils d'échange des données qui fournissent une confidentialité maximale et une sécurité à toute épreuve.

La sécurité des réseaux se place au premier plan de la mise en œuvre et de l'administration réseau dans une entreprise, cette dernière applique une stratégie de sécurité efficace afin de protéger son réseau. L'autorisation d'accès aux données est prise en charge par la sécurité du réseau, qui est contrôlée par les administrateurs.

Dans ce chapitre, nous consacrerons une section à la présentation de l'administration des réseaux, qui reposera sur les éléments de base qui contribuent à sa mise en œuvre, de même nous effectuerons un tour d'horizon sur les principes de la sécurité des réseaux ainsi que quelques solutions proposées.

II.2 L'administration des réseaux informatiques

L'administration des réseaux informatiques (ou Network management) désigne les activités, les méthodes, les procédures qui permettent de gérer au mieux sa mise en oeuvre opérationnelle, et sa surveillance grâce à la mise en place d'outils par l'administrateur. Ces outils (Nagios XI, Wireshark, Putty, Traceroute, Nmap, Ping, ...) sont liés à l'exploitation, l'administration, la maintenance des réseaux informatiques. La gestion des réseaux informatiques est une problématique dont le défi est de garantir au moindre coût, non seulement la qualité du service fournit aux utilisateurs mais aussi la réactivité liée aux mutations et à l'évolution fulgurante du secteur informatique. La qualité de service se décline sur plusieurs axes, en particulier la disponibilité, la performance (temps de réponse), la fiabilité, la sécurité... La gestion des réseaux est habituellement répertoriée en 3 activités, [3] :

II.2.1 supervision

La supervision est la surveillance des systèmes et la collecte d'informations sur leur état et leur comportement, ce qui peut se faire au moyen d'une interrogation régulière ou d'un feed-back non sollicité de l'équipement du réseau lui-même.

Plus le réseau est étendu et complexe, plus la supervision devient délicate sans les outils appropriés. Une large majorité des outils de supervision se base sur le protocole SNMP, qui est présent depuis de longues années. La majorité de ces outils offrent de nombreuses fonctions, dont les plus importantes sont les suivantes :

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

II.2.2 Administration

L'administration se rapporte plus particulièrement aux activités de contrôle du réseau avec la gestion de la configuration et de la sécurité. De façon générale, l'administration de réseau est destinée à englober un éventail de techniques de gestion mises en œuvre pour :

- Fournir aux usagers une certaine qualité de service ;
- Permettre le développement du système en intégrant de nouvelles fonctionnalités ;
- Mise en service d'un système ;

II.2.3 Exploitation

Désormais, les systèmes d'exploitation tels qu'UNIX, MacOs et Windows prennent tous en charge les aspects liés au fonctionnement du réseau, aux procédures et aux fonctions associées. Un système de gestion de réseau est une combinaison de divers outils de surveillance et de contrôle du réseau qui sont intégrés dans le sens où ils impliquent :

- Une interface opératrice unique comportant un ensemble de commandes à la fois performantes et conviviales pour effectuer toutes les tâches d'administration du réseau ;
- Un nombre réduit de dispositifs distincts constitués habituellement de composants matériels et logiciels requis pour la gestion du réseau, et incorporés dans l'équipement existant de l'utilisateur.
- Rendre opérationnel un système ;

L'objectif de l'administration des réseaux pour un administrateur :

- Supervision du fonctionnement des réseaux ;
- Optimiser l'utilisation des ressources ;
- Détecter et prévoir les erreurs ;
- Signalisation des pannes ;
- Calculs de facturation basé sur l'utilisation des ressources ;
- Assistance technique aux utilisateurs.

II.3 Réseaux campus

La gestion d'un réseau implique l'existence d'un système d'information qui décrit le réseau de l'entreprise et répertorie les données et les éventuels événements concernant chaque équipement du réseau administré.

Un réseau local est un ensemble de ressources informatiques indépendantes (micro-ordinateurs, stations de travail,...) liées entre elles pour échanger des informations et partager des ressources matérielles ou logicielles. Le qualificatif de LAN, définit un réseau comme un système de communication entre unités centrales sur une zone géographique restreinte, est restrictif, [4].

II.3.1 Constituants d'un réseau local

Un réseau local est essentiellement constitué de :

- Un câblage reliant les différents nœuds selon une certaine topologie ;
- Une méthode d'accès au support pour assurer son partage ;
- Une méthode d'adressage pour identifier chaque nœud ;
- Un ensemble cohérent de protocoles pour permettre la communication ;
- Un système d'exploitation particulier (NOS) permettant de supporter des dispositifs distants communs et de contrôler leur utilisation (administration et sécurité) ;
- Un ensemble de programmes utilisant les ressources mises en commun.

II.3.2 Standard IEEE

Le comité IEEE 802, composé essentiellement de représentants des firmes américaines, s'est penché sur l'architecture des LAN. De nombreux documents ont été rédigés pour définir l'architecture proposée, [4] :

- Le standard 802.1 définit le contexte général des réseaux locaux informatiques.
- Le standard 802.2 définit la couche Liaison de données.
- Les standards 802.3, 802.4, 802.5 et 802.6 définissent différents protocoles d'accès au support, pour plusieurs types de supports physiques : paire métallique, câble coaxial ou fibre optique.
- Le standard 802.11 définit un protocole d'accès pour les réseaux locaux sans fil (WLAN).

II.4 Sécurité des réseaux

La sécurité des communications est désormais une source de préoccupation considérable pour les utilisateurs et les entreprises. Tout le monde cherche à se prémunir contre tout usage frauduleux de leurs données ou contre toute intrusion malintentionnée dans les systèmes informatiques. Par ailleurs, une multitude de virus se répandent à l'insu des utilisateurs et ils sont ainsi capables de provoquer la destruction de documents, voire la fuite des informations contenues dans les machines. La tendance actuelle est de définir des mécanismes de contrôle d'accès et d'utiliser des protocoles sécurisés garantis :

- L'authentification ;
- la confidentialité ;
- L'intégrité ;
- la non-répudiation.

II.4.1 Les principes de la sécurité informatique

II.4.1.1 Terminologie de la sécurité informatique

- **Vulnérabilité** : Désigne une brèche (faille) de sécurité dans un ou plusieurs systèmes, qui peut être exploité ou non, [5].
- **Attaque (exploit)** : Représente la démarche à suivre pour parvenir à exploiter une vulnérabilité. Il peut exister différentes attaques pour une même vulnérabilité, [5].

- **Contre-mesure** : Est une disposition définie par une procédure ou une technique permettant soit résoudre une vulnérabilité ou de se prémunir d'une attaque spécifique, [5].
- **Menace** : Se rapporte à tout ce qui est susceptible de causer des dommages à un système informatique. Les menaces peuvent conduire à des attaques sur des systèmes informatiques, des réseaux, [5].
- **Politique de sécurité** : Est une stratégie permettant d'optimiser la sécurité informatique d'une entreprise. Elle est synthétisée dans un document qui comprend tous les enjeux, objectifs, analyses, actions et procédures qui font partie de cette stratégie, [5].

II.4.1.2 Les objectifs de la sécurité

La sécurité de l'information est fondée sur, [6] :

- **La confidentialité** : a pour but de s'assurer qu'une information n'est accessible qu'aux entités autorisées.
- **L'intégrité** : garantie que les données reçues n'ont subi aucune modification lors du transport dans le réseau.
- **L'authentification** : lors d'un échange garantit que les données reçues proviennent bien de l'entité émettrice. Mais dans un réseau permet de vérifier l'identité d'une entité et de l'autoriser ou pas à accès à des ressources.
- **La non répudiation** : permet de garantir que l'échange entre des entités ne peut être nié par ces dernières.
- **La disponibilité** : assure que les infrastructures, les informations, les services sont accessibles aux personnes autorisées quand elles en ont besoin.

II.4.2 Malveillance informatique

De nos jours, une simple navigation sur l'internet ou l'ouverture d'un courrier électronique expose l'utilisateur à des logiciels malveillants qui sont des programmes informatiques nuisibles tels que les virus, les vers, les ransomware... Mais aussi de par l'importance qu'a pris internet dans le monde et l'hétérogénéité des équipements qui le constitue, ses derniers peuvent eux-mêmes présenter des défauts de construction dans leurs systèmes internes, ou potentiellement des défauts de configurations lors de leurs installations générant ainsi des brèches qui peuvent être exploitées. Malgré cette diversité des champs d'attaques contre les systèmes d'information, une attaque suit généralement les mêmes étapes, se procéder et appeler « anatomie d'une attaque » [5].

II.4.2.1 Anatomie d'une attaque

Cette anatomie d'une attaque décrit les phases par laquelle un attaquant passe afin d'attendre l'objectif défini. Cette anatomie définie généralement 5 étapes mais qui peut être réduite à 4 ou 3 étapes, elle est appelée par les anglophones « The 5 P » Probe, Penetrate, Persist, Propagate, Paralyze, représentant ainsi le squelette de toute attaque informatique. Le rôle de chaque étape, [7] :

- **Probe** : Appelé aussi reconnaissance c'est la phase primordiale de toutes attaques, car elle permet de collecter des informations, de manière passive et active, afin de détecter potentiellement une ou plusieurs failles sur une entité.
- **Penetrate** : Connu en français sous le nom de gain d'accès, elle consiste à exploiter les informations récoltées afin d'accéder au réseau.
- **Persist** : Également connu comme étant le processus de maintien d'accès. Il permet de se réinfiltrer ultérieurement si nécessaire, et ce en utilisant une backdoor ou porte dérobée.
- **Propagate** : Cette étape permet d'infiltrer d'autres équipements dans l'objectif de gagné de nouveau privilège dans le réseau en observant ce qui est accessible et disponible sur le réseau local.

  Le processus d'attaque peut généralement s'arrêter à cette étape, permettant ainsi a un attaquant de récolter des informations confidentielles, mais parfois ces attaques visent à entrainer des préjudices c'est pour quoi une dernière phase est définie.
- **Paralyse** : cette étape, est utilisée afin de détruire des données ou encore endommager le système dans le but de planter le serveur et rendre le service qu'il offre inaccessible ou dans le but de mener des attaques de plus grande envergure en passe par un réseau intermédiaire afin que le pirate puisse protéger son identit.

II.4.2.2 Les techniques d'attaques réseaux

A ce jour ;les pirates ne cessent d'innover des attaques qui leur permettant de contourner les différentes protections mises en place. Ces attaques peuvent être classées généralement en 2 grandes familles les attaques directes et les attaques indirectes, certains d'entre sont plus complexes à mettre en place que d'autres. Parmi ces attaques on retrouve, [5] :

- **Les virus** : C'est un programme informatique capable de s'installer sur un ordinateur à l'insu de son utilisateur légitime, ils appartiennent à la famille des attaques directes car ce dernier ne se propage pas sur internet mais c'est une attaque ciblée.
- **Virus réticulaire (botnet)** : Appartient à la famille des attaques indirectes. Ce virus une fois déployée sur internet il se propage d'ordinateur à autre, créant ainsi un réseau d'ordinateurs appelé zombie qui peut être utilisé pour des attaques de grande ampleur, ou tout simplement récolter le maximum d'informations sensibles.
- **DDoS** : Cette attaque permet d'engendrer une saturation d'un serveur rendant son service inaccessible pendant un certain temps, et ce en donnant l'ordre aux ordinateurs zombies de se connecter au serveur simultanément.
- **Cheval de Troie (Trojan horse)** :souvent transmis via des e-mails, il se cache derrière des pièces jointes mais une fois installée sur un ordinateur y effectue des actions cachées et pernicieuses.
- **MITM (Man In The Middle)** : Consiste à intercepter les paquets envoyés d'un utilisateur à un autre sans qu'aucun d'entre eux n'ait connaissance que le support de transmission utilisé est compromis. Elle permet également de modifier, injecter des codes sur les paquets interceptés.
- **IP Spoofing** : Cette attaque consiste à émettre des paquets IP portants comme adresses IP sources différentes que celle de l'attaquant. Cette stratégie d'attaque est utilisée pour des raisons de sécurité, afin que l'émetteur de ses paquets ne puisse pas être trouvé et elle est employée dans plusieurs des attaques.

- **Ingénierie Sociale** : C'est une attaque qui se base sur la manipulation des personnes peu consciencieuses, ignorantes afin de contourner les dispositifs de sécurité.

II.4.3 Lutte contre les malveillances informatiques

II.4.3.1 Pare-feu

Le firewall est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique, il protège le système en prenant des décisions de routage après avoir filtré les paquets en se basant sur l'information contenue dans l'en-tête d'un paquet IP, [6].

Le pare-feu permet donc de filtrer les paquets de données échangés avec le réseau, donc il représente une passerelle filtrante comme l'illustre la figure (II.1) comportant au minimum les interfaces réseau suivantes :

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

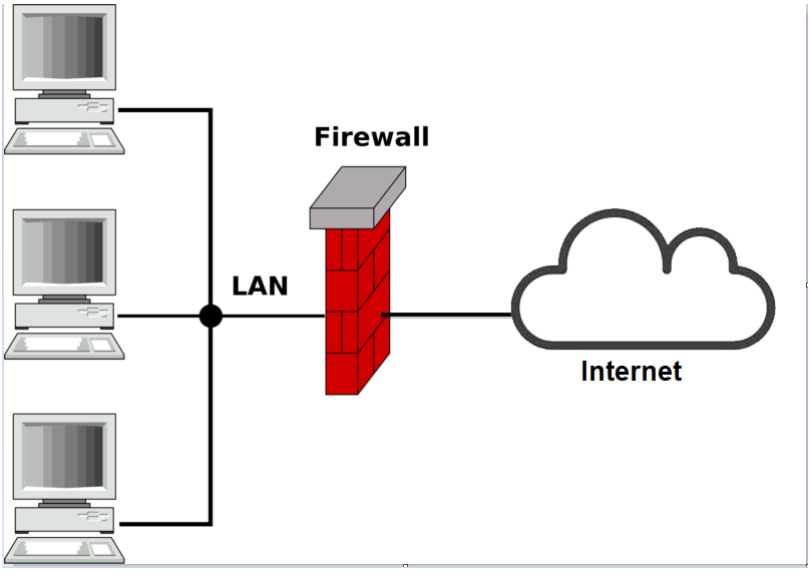

FIGURE II.1 – L'architecture d'un Pare-feu

II.4.3.1.1 Le fonctionnement d'un Pare-feu

Un système firewall 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).

On distingue habituellement deux types de politiques de sécurité permettant :

- soit d'autoriser uniquement les communications ayant été explicitement autorisées,
- soit d'empêcher les échanges qui ont été explicitement interdits.

II.4.3.1.2 Les systémes de filtrages

- **Filtrage de paquets** : Opérant au niveau de la couche réseau et transport du modèle OSI, il est mis en place par des ACL, il permet de rejeter ou d'accepter le passage de paquet en fonction de nombreux critères :
  - L'adresse destination ;
  - L'adresse source ;
  - Le protocole transporté (TCP, ICMP... etc.) ;
  - Le numéro de port ;
  - La valeur des flags (ACK, RST, SYN... etc.).

  Mais ce type de firewall reste peu efficace contre des attaques de type DoS si un accès vers internet doit être autorisé, ce dernier doit accepter les connexions TCP provenant de l'extérieur avec un port supérieur à 1024.
- **Filtrage de paquets avec état (firewall stateful) :** Il effectue une sauvegarde des sessions et des connexions dans des tables d'états internes au Firewall, qui lui permet de réagir dans le cas de situations protocolaires anormales en fonction des états de connexions. Ainsi seuls les paquets correspondant à une connexion active connue seront autorisés. Mais peut-être contourné si un utilisateur sollicite une connexion externe.
- **Proxy :** Le proxy est utilisé en couche applicative selon le modèle OSI, il analyse le trafic de données, et applique une politique de sécurité spécifique de chaque application selon le protocole utilisé. Cependant de part la diversité des règles protocolaires des protocoles de la couche 7, empêchant une adaptabilité de nouveaux protocoles ou des protocoles locaux.

II.4.3.2 Architecture DMZ

La zone démilitarisée est un sous-réseau isolé situé entre le réseau extérieur(internet) considérer moins sécurisé et le réseau interne séparé par un pare-feu comme le montre la figure ci-dessous. Ce sous-réseau héberge des équipements (serveur de messagerie, web, ...) accessible depuis internet. Elle joue le rôle d'une zone tampon entre le réseau à protéger et le réseau hostile. Les serveurs du LAN ne sont jamais exposés directement à internet et à l'inverse les utilisateurs extérieurs n'ont jamais à accéder directement à des ressources du LAN, toutes communications entre internet et le LAN doivent passer par la DMZ afin d'être analysé et l'information sera transmise au LAN si aucun problème n'a été détecté, ce processus permet en cas de compromission d'empêcher qu'un pirate aura accès aux machines de réseau privé. Pour résumer la DMZ permet :

- D'autorisation du trafic du réseau externe vers la DMZ,
- D'interdire le trafic externe vers le réseau interne,
- D'autorisation du trafic du réseau interne vers la DMZ.

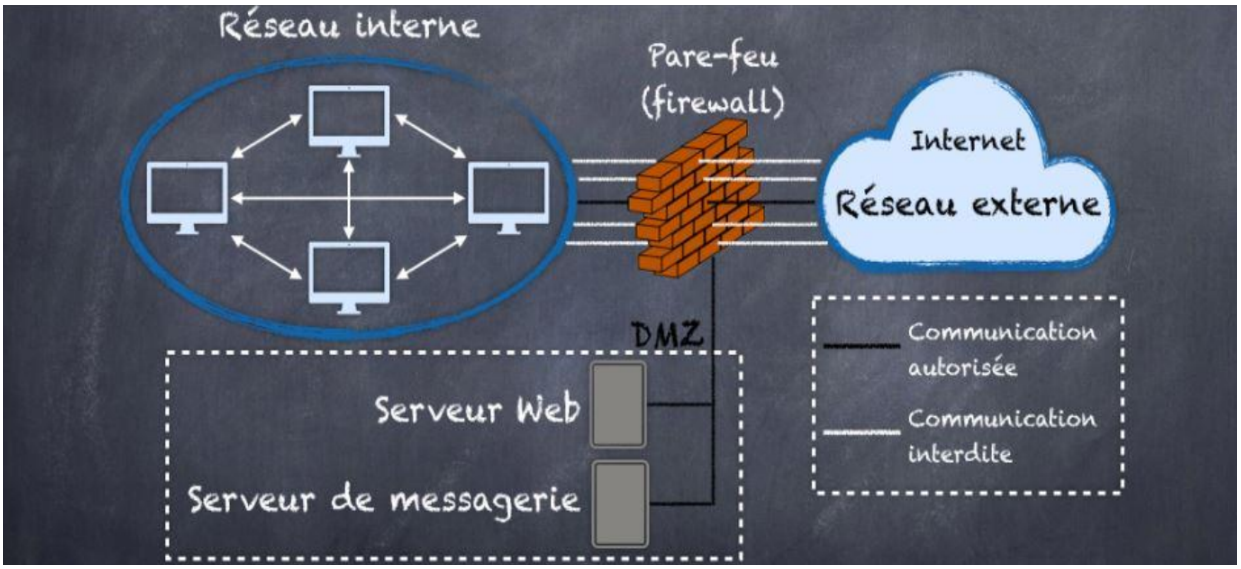

FIGURE II.2 – Zone démilitarisée.

II.4.3.3 La cryptographie

Réservée aux militaires et aux états développés, la cryptographie, est une méthode qui permet d'envoyer des messages de manière secrète, ce domaine s'est démocratisé devenu ainsi une science accessible pour le grand public afin d'assurer la CIA de leurs communications informatiques, ou celle des données stockées sur des serveurs, [8].

II.4.3.3.1 La cryptographie Symétrique

Son principe est fondé sur une unique clé secrète utilisée par l'émetteur pour crypter les données, et par le récepteur, afin qu'il puisse décrypter les données reçues (exemple : **AES**). Mais ce système est peu sûr car il implique l'existence d'un canal sûr afin de transmettre cette clé évitant ainsi des attaques de type MITM.

II.4.3.3.2 La cryptographie Asymétrique

La cryptographie Asymétrique quant à elle se base sur 2 clés différentes : la première clé doit rester secrète(privée) et donc ne jamais être publié, car elle permet de déchiffrer les messages reçus qui sont cryptés par la deuxième clé qui sera publiée et donc connue de tous (exemple :**RSA**).

II.4.3.4 Les VLANs

Est Un réseau local regroupe un ensemble de machines de manière logique et non physique, il a été normalisé selon la spécification IEEE 802.1Q.

Un VLAN est assimilable à un domaine de diffusion (Broadcast Domain). Ceci signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN. Ces derniers n'ont été réalisables qu'avec l'apparition des commutateurs (Switches).

II.4.3.4.1 L'avantage des Vlans

Les VLANs permettent de définir de nouveaux réseaux au-dessus du réseau physique et à ce titre offrent 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 encapsulés dans un niveau supplémentaire et éventuellement analysé ;
- Réduction de la diffusion du trafic sur le réseau.

II.4.3.5 Les ACLs

Est une liste séquentielle de critères utilisée pour du filtrage du trafic réseau en commandant aux interfaces d'un routeur d'acheminer ou de bloquer des paquets qui y transitent, que ce soit en entrée ou en sortie selon quelques critères :

- l'adresse source pour les access-lists standards (Numéro d'access-list de 1 à 99) ;
- l'adresse source, l'adresse de destination, le protocole ou le numéro de port pour les access-lists étendues (Numéro d'access-list : de 100 à 199).

Les ACLs servent à : Contrôler et gérer le flux de trafic en déterminant le type de trafic qui sera acheminé ou bloqué au niveau des interfaces du routeur, améliorer les performances réseau ,et fournir un niveau de sécurité d'accès réseau.

II.4.3.6 Le fonctionnement d'une ACL

Le principe de fonctionnement d'une ACL est donné par la figure(II.3).

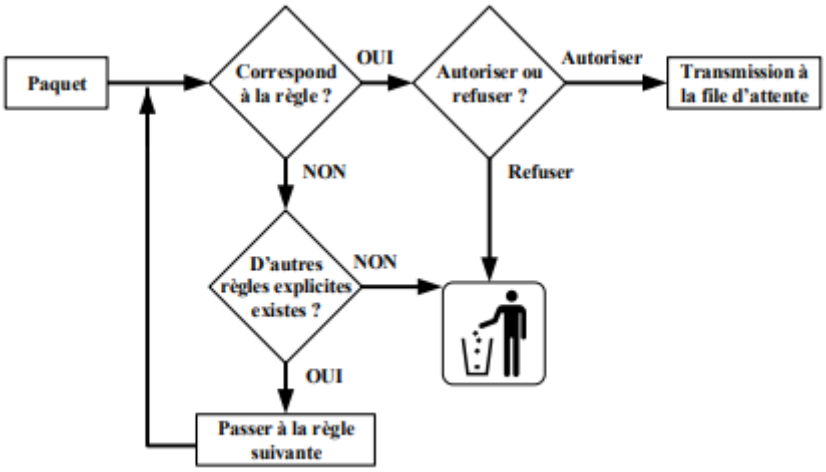

FIGURE II.3 – Le fonctionnement d'une ACL

- Le paquet sera analysé par l'ACL entrante ;
- Si le paquet matche avec une règle Deny, alors il sera supprimé ;
- S'il matche avec une règle permit, alors il pourra passer et le routeur le prendra en charge ;
- Le routeur décide de router ce paquet vers l'interface ;
- Là aussi il y'a une ACL, mais cette fois-ci, elle est placée en sortie ;
- Si le paquet est autorisé alors il continuera son chemin ;
- Sinon il sera supprimé, [9].

II.4.3.7 Le VPN

Le réseau privé virtuel (noté RPV ou VPN) est une technique permettant à deux ou plusieurs postes distants de communiquer de manière sûre. C'est un environnement de communication, dans lequel l'accès est contrôlé, afin de permettre des connexions entre une communauté d'intérêt seulement.

Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données. Les VPN ont aujourd'hui pris une place importante dans les réseaux informatiques et l'informatique distribuée.

II.4.3.6.1 Le fonctionnement d'un VPN

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunneling qui permet aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie, entre l'entrée et la sortie du VPN, les données sont chiffrées (cryptées) et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel, la figure(II.4) ci-dessous montre le fonctionnement d'un VPN, [6].

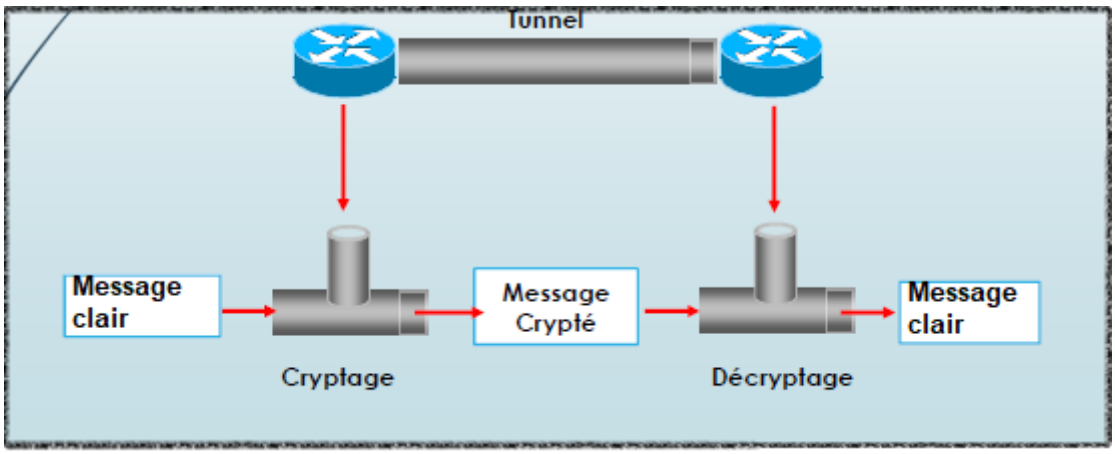

FIGURE II.4 – Le fonctionnement d'un VPN

II.4.3.6.2 Les avantages des VPN

Les réseaux privés virtuels offrent les avantages suivants :

- **Sécurité** : assure des communications sécurisées et chiffrées entre les différents sites.
- **Simplicité** : utilise les circuits de télécommunication classiques.
- **Économie** : utilise Internet en tant que média principal de transport, ce qui évite les coûts liés à une ligne dédiée.
- **Évolutivité** : Les réseaux privés virtuels utilisent l'infrastructure Internet dont les opérateurs, facilitant l'ajout de nouveaux utilisateurs pour les entreprises. Ces dernières, quelle que soit leur taille, peuvent augmenter leur capacité sans élargir sensiblement leur infrastructure.

II.4.3.6.3 Les principaux protocoles utilisés :

- **PPTP et PPP** : sont des protocoles d'encapsulation des datagrammes IP, ils assurent la délimitation des trames, identifient le protocole transporté et la détection d'erreurs.
- **IPSec** : Est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. IPsec est basé sur deux mécanismes :
  - **AH** (Authentification Header) : C'est un protocole réseau, de couche 3 du modèle OSI, vise à assurer l'intégrité et l'authenticité des datagrammes IP.
  - **ESP** (Encapsulating Security Payload) : C'est un protocole de couche 4 du modèle OSI, peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations.
- **TLS/SSL** : Est un protocole de niveau transport utilisé pour l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.

II.5 Représentation des attaques et leurs solutions

Attaque	**Solution**
Les virus et botnet	- Antivirus - Création d'une DMZ empêchant les paquets infectés de joindre directement leurs correspondants ou de se propager dans le réseau (protection par honeypot)
DDOS	- Pare-feu (Firewall) - Augmenter le niveau de sécurité des équipements connectés au réseau.
Cheval de Troie	- Antivirus - Logiciels anti-Spam et anti-Trojan
MITM	- Utilisation de protocoles de communication chiffrés comme SSH (SFTP, SCP), SSL (HTTPS ou FTPS) et non des protocoles ouverts comme HTTP, FTP, Telnet
IP Spoofing	- Utiliser un VPN afin de cacher l'adresse IP ; - Authentifier l'utilisateur en utilisant des systémes de cryptage pour comme IPsec, TLS, SSH et pas se baser sur les adresses IP.
Ingénierie Sociale	- Sensibilisation des utilisateurs aux problèmes de sécurité ; - Vérifiez la provenance des demandes surtout lorsque cette derniere demande des informations sensibles ou personnelles. - Ne jamais répondre rapidement, si cela est demandé. C'est une des ruses les plus répandues pour pousser à agir avant de réfléchir.

Table II.1 – Représentation des attaques et leurs solutions

II.6 Conclusion

Dans ce chapitre on a pu constater que la sécurité d'un système d'information d'une entreprise représente l'élément fondamental pour son bon fonctionnement, afin de lutter contre les menaces qui pèsent sur lui. L'administrateur a pour tâche d'évaluer continuellement ces menaces et lutter contre en mettant en place des solutions, cela nécessite des compétences et des connaissances qui doivent être enrichies.

Dans le chapitre qui suit nous allons introduire l'organisme d'accueil, et représenter sa topologie qui va nous permettre d'effectuer une étude du réseau.

Chapitre III

Etude du réseau existant

III.1 Introduction

Ce chapitre sera consacré pour présenter d'abord l'organisme d'accueil SONATRACH , ensuite on va faire une étude détaillée sur l'architecture proposée de son réseau afin de déterminer les failles de sécurité et les problématiques de ce réseau, puis on va proposer des suggestions pour améliorer sa sécurité et de rendre le trafic plus efficace , et enfin on procédera à la proposition d'une nouvelle topologie plus sécurisée.

III.2 Présentation de l'organisme d'accueil SONATRACH

SONTARACH (acronyme de société nationale pour la recherche, la production, le transport, la transformation, et la commercialisation des hydrocarbures) est une entreprise pétrolière et gazière surnommé la major africaine. Elle contient cinq directions régionales de transport des hydrocarbures et celle de Bejaïa est la région de transport centrale (RTC) ; Cette dernière est composée d'un centre informatque et de trois sous-directions chaque sous-direction contient des différents départements et services afin d'assurer le transport, la sécurité et la commercialisation des hydrocarbures, le schéma de la figure (III.1) illustre l'organisme de la RTC.

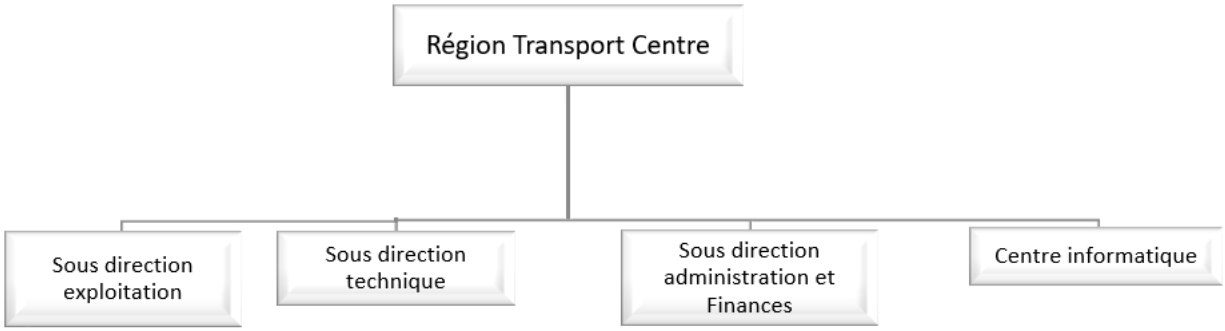

FIGURE III.1 – l'organisme de la RTC

Le rôle de chaque sous-direction est :

- **Sous-direction Technique** : Elle a pour mission d'assurer la maintenance et la protection des ouvrages.

- **Sous-direction Exploitation** : Elle est chargée de l'exploitation des installations, elle effectue des réparations en cas de fuite, de sabotage ou de panne pour les stations de pompage.

- **Sous-direction Administration et Finance** : Elle a pour mission la gestion des ressources humaines et les moyens généraux,et aussi d'effectuer la gestion financière, le budget et le contrôle de gestion.

- **Centre Informatique** : Il regroupe les moyens d'exploitation et de développement des applications informatiques pour l'ensemble des structures de la RTC, ainsi que la gestion du réseau informatique interne.

III.3 Topologie du réseau proposée par l'entreprise :

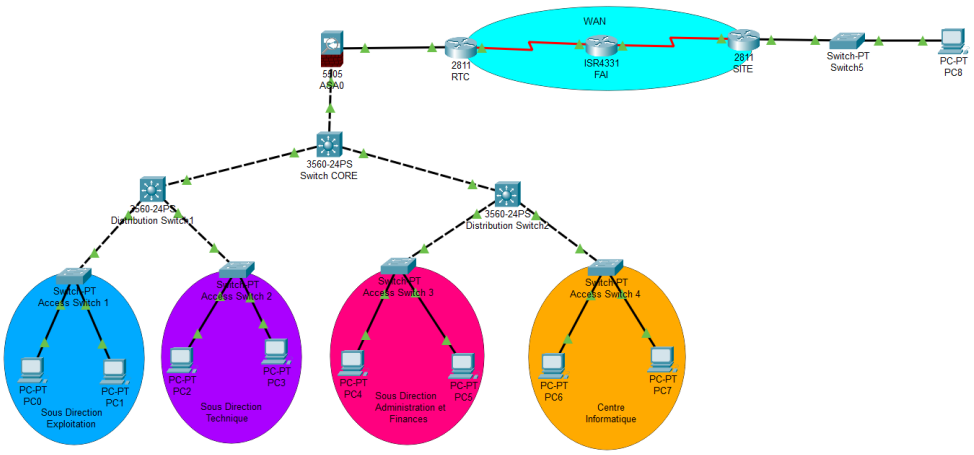

FIGURE III.2 – Réseau de l'entreprise

III.3.1 Etude de la topologie :

III.3.1.1 Modèle de conception hiérarchique à trois couches :

Le modèle hiérarchique à trois couches est un ensemble de recommandations qui décrivent comment un réseau LAN de campus doit être conçu. Il définit trois couches : cœur, distribution et accès. Ce modèle rend plus facile la gestion et le dépannage du réseau, en offrant une flexibilité au réseau permettant aux administrateurs d'ajouter, remplacer, supprimer facilement des composants individuels du réseau.

- **La couche d'accès :** La couche d'accès permet aux utilisateurs finals d'accéder au réseau. Les principales fonctions de cette couche sont les suivantes :
  - Connexion de divers types de dispositifs finaux au réseau LAN.
  - Fournir une commutation de couche 2 et mettre en œuvre divers services de commutation de couche 2 tels que spanning tree, contrôle d'accès virtuel, QoS et ARP...
  - Empêcher les périphériques non autorisés de se connecter au réseau local en appliquant diverses politiques de sécurité telles que la sécurité des ports, le snooping DHCP et la configuration statique des adresses MAC.
- **La couche de distribution :** Situé entre la couche d'accès et cœur, contrairement aux commutateurs d'accès, les commutateurs de distribution ne fournissent aucun service aux périphériques finaux. Les principales fonctions de cette couche sont les suivantes :
  - Assurer la connectivité entre les commutateurs de la couche d'accès ;
  - Agrégation des liens et du trafic LAN et WAN ;
  - Contrôler et filtrer le trafic en mettant en œuvre des listes de contrôle d'accès (ACL) ;
  - Contrôle de la diffusion par le biais des VLAN ;
  - Assurer la redondance et l'équilibrage des charges.

- **La couche cœur :** Appelé backbone, elle réduit les besoins en câblage et les ports de commutation tout en permettant aux périphériques l'échanger des données avec l'extérieur. Contrairement aux couches d'accès et de distribution, la couche centrale ne fournit pas beaucoup de services parmi eux on retrouve :
  - Transmission du trafic à la vitesse la plus rapide possible ;
  - Le maintien de la liaison entre différents segments du réseau.

III.3.2 Problématique

L'architecture du réseau illustrée précédemment est utile à l'entreprise présente quelques problèmes et failles de sécurité comme :

- L'absence d'une zone démilitarisée (DMZ) qui rend les hôtes les plus exposés aux attaques vulnérables ;
- L'absence de la redondance qui rend le réseau non tolérant aux pannes et qui obstruera la continuité et le bon fonctionnement du réseau ;
- L'accès aux ressources de l'infrastructure depuis l'extérieur ne se fait pas d'une façon sécurisée et ce par l'absence d'utilisation de VPN.

III.3.3 La solution proposée

Pour remédier les problèmes cités précédemment, nous proposons les solutions suivantes :

- Afin de sécuriser le réseau du RTC , on a opté pour la création d'une zone démilitarisée (DMZ) pour renforcer le niveau de sécurité du réseau local de l'entreprise.en visant à protéger les hôtes les plus exposés aux attaques. Cette zone contient 2 serveurs :
  - **Le serveur web** qui protège la base de données interne qui contient des informations sensibles ;
  - **Le serveur de messagerie** qui permet l'accès à la base de données de messagerie et d'interagir avec sans qu'elle ne soit exposée à un trafic susceptible de représenter un danger.
- Pour une meilleure sécurisation de l'information et l'échange des données entre RTC et le site distant ; on a proposé la configurer une connexion VPN site-à-site pour garantir la confidentialité des données.
- Utiliser une architecture redondante en utilisant deux backbones interconnectés en redondances.

III.3.4 c'est quoi la redondance ?

Ce que les entreprises recherchent de nos jours, c'est un réseau fiable et disponible à tout moment. Une telle solution n'est pas forcément très simple à mettre en place, de plus elle peut être relativement coûteuse pour l'entreprise. Le mieux est d'avoir un réseau qui supporte la charge sans interruption d'utilisation et une redondance en cas de pannes. Cela signifie avoir plusieurs appareils qui remplissent la même fonction, tout en étant aussi transparent que possible pour les utilisateurs.

III.3.4.1 Les protocoles de redondance

- **HSRP** : HSRP est un protocole propriétaire Cisco. Il permet de gérer la redondance de routeur, lorsqu'un routeur tombe en panne un autre routeur de secours prend le relais. Il permet d'augmenter la tolérance de panne sur un réseau en créant un routeur virtuel à partir de 2 routeurs physiques (ou plus), une élection déterminera le routeur actif et les autres routeurs seront en "attente" (standby). L'élection du routeur actif est réalisée grâce à la priorité configurée sur chaque routeur, [10].
- **VRRP** : À l'instar de HSRP, VRRP fournit une solution de continuité de service principalement pour la redondance de passerelles par défaut.
  VRRP est un standard ouvert d'élection qui assigne les responsabilités d'un routeur virtuel à l'un des routeurs VRRP présents dans le LAN. Le nombre de routeurs dans un groupe agit comme un routeur logique virtuel qui sera la passerelle par défaut de tous les hôtes locaux. Si un routeur tombe en panne, l'un des autres membres du groupe peut prendre la responsabilité de transférer le trafic, [1].

III.4 Nouvelle topologie

La figure (III.3) ci-dessous montre la nouvelle topologie du réseau RTC après avoir appliqué les différentes solutions proposées telles que : la DMZ, la redondance et le VPN.

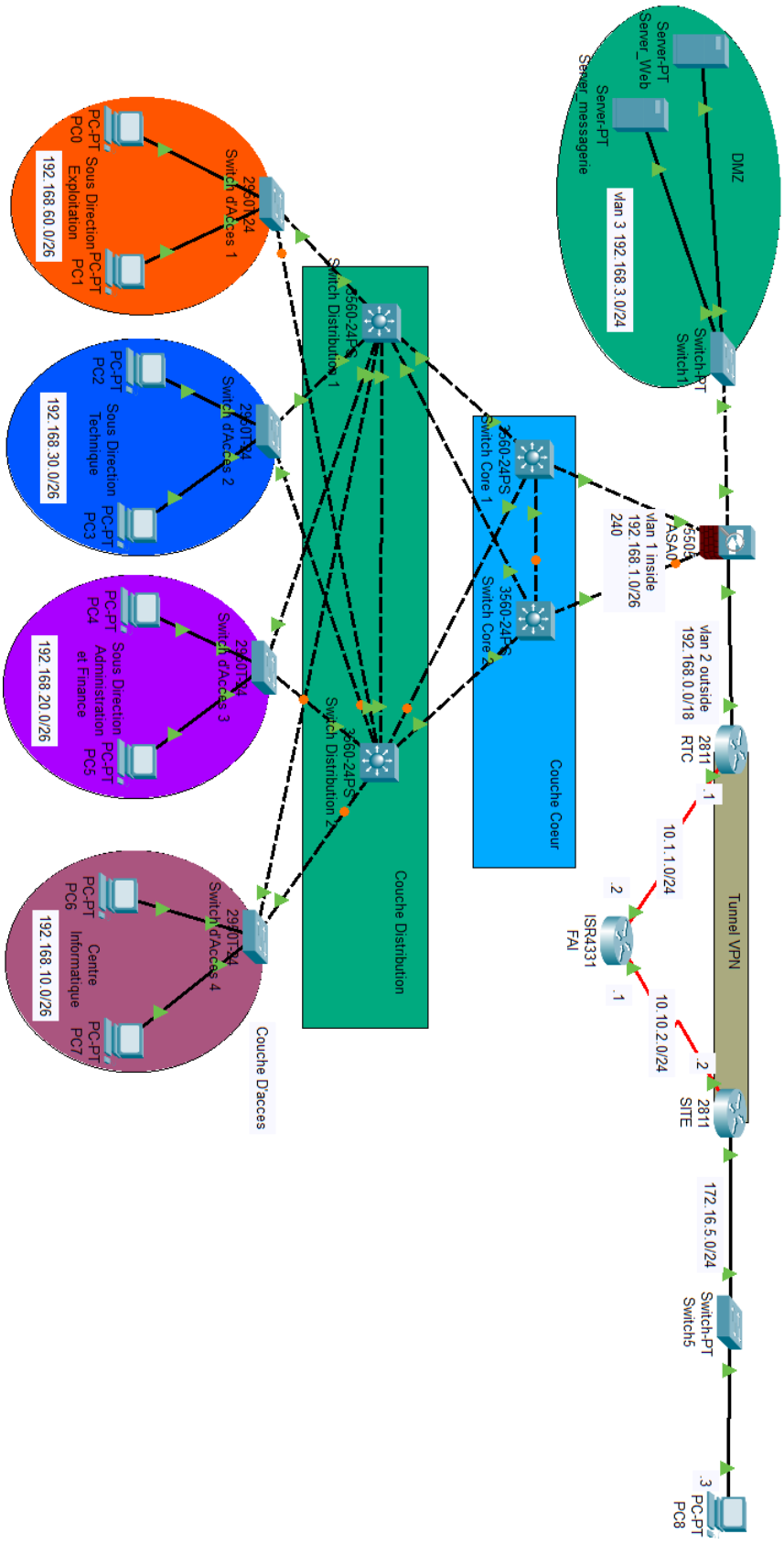

FIGURE III.3 – La nouvelle architecture

III.4.1 Équipements utilisés

III.4.1.1 Switch

- **c2950** : La gamme Catalyst 2950 de Cisco offrant des performances, une souplesse et une facilité d'administration. Cette gamme de commutateurs de niveau 2 offre de nombreuses fonctionnalités avancées de QoS et de traitement des flux multicast, [11].

FIGURE III.4 – Switch Catalyst 2950T-24

- **c3560** :La gamme Cisco Catalyst 3560 est une ligne de commutateurs à configuration fixe, de niveau 3, idéal pour les réseaux locaux d'entreprise ou aux succursales. Il remplit des fonctions de switching classiques et les fonctions de routeur à la fois en offrant un maximum de productivité qui permet le déploiement des services réseaux intelligents tels que la limitation de débit, le filtrage par ACLs, la gestion multicast, et le routage IP haute performance tout en conservant la simplicité de la commutation traditionnelle des réseaux locaux, [12].

FIGURE III.5 – Switch Catalyst 3560

III.4.1.2 Routeur

- **Router 2811** : La gamme Cisco 2800 apporte une importante valeur ajoutée,parmi les principales caractéristiques différenciatrices on retrouve, [13] :
  - Accroît par cinq les performances sécurité ;
  - Augmentation considérable en terme de capacités et de densité d'emplacements d'interfaces ;
  - Embarque des fonctions de cryptage matérielles sur la carte mère ;
  - Offre en option d'un système de prévention des intrusions (IPS) et de fonctions de pare-feu à inspection d'état.

FIGURE III.6 – Routers Cisco 2811

III.4.1.3 Pare-feu

- **ASA 5500** : Le modèle Cisco ASA 5500 est une gamme de serveurs de protection de réseaux polyvalents et efficaces, en mesure de protéger de manière complète les réseaux des petites, moyennes et grandes entreprises, tout en limitant les dépenses de déploiement et d'exploitation et en facilitant les tâches associées à ce niveau de sécurité. Parmi cette gamme on retrouve le modèle Cisco ASA 5505, permet de mettre en place un pare-feu hautes performances, un VPN SSL et I Psec, Un service de prévention des intrusions et d'atténuation des vers et d'autres services sont disponibles en activant les fonctions de la licence sécurité plus, [14].

FIGURE III.7 – Pare-Feu ASA 5505

III.5 Conclusion

À l'issue de ce chapitre, nous avons conçu une partie pour la présentation de l'organisme d'accueil, en l'occurrence RTC-SONATRACH- Bejaia, ensuite on a effectué une étude critique sur la topologie proposée dont nous avons mis en avant des failles qui nous ont amenés à la proposition des solutions et une nouvelle topologie du réseau RTC qui va contribuer à l'amélioration de la sécurité de ce réseau et de se protéger contre les attaques et les accès non autorisés. Ces solutions sont mises en œuvre sous CISCO Packet Tracer, dans le chapitre qui suit.

Chapitre IV

Etude du réseau existant

IV.1 Introduction

Après avoir défini tous les concepts nécessaires dans les chapitres précédents ; ce chapitre sera conçu pour réaliser ; configurer et mettre en pratique les solutions qu'on a envisagées auparavant au réseau de l'entreprise SONATRACH, en utilisant le simulateur « Cisco Packet Tracer », et au final, nous allons tester si les problèmes ont été bel et bien disparus.

IV.2 Présentation de simulateur « Cisco Packet Tracer »

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel. Il est possible de créer, visualiser et de simuler le comportement des protocoles des réseaux informatiques avec ce simulateur. L'utilisateur après avoir construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou les ordinateurs en les reliant via des câbles (câbles divers, fibre optique) peuvent configurer les adresses IP, les services disponibles, etc. . . . pour chacun d'entre eux..

Cisco Packet Tracer est un moyen d'apprentissage de la réalisation de divers réseaux et permet de découvrir le fonctionnement des différents éléments constituant un réseau informatique.

IV.2.1 L'interface principale du simulateur Packet Tracer

La figure ci-dessous (IV.1) est un aperçu général de l'interface principale de Packet Tracer, dont on définit les zones :

- Zone 1 : la partie dans laquelle le réseau est construit ;
- Zone 2 : la partie où les équipements sont regroupés en catégories ;
- Zone 3 : la partie où on choisit le type d'équipement dont on a besoin ;
- Zone 4 : permet de passer du mode réel au mode simulation et vice-versa ;
- Zone 5 : contient un ensemble d'outils (sélection, inspection, suppression et redimensionner la forme) ;
- Zone 6 : regrouper les outils permettant de créer des formes et des commentaires ;
- Zone 7 : concerne les tests de communication (envoie de la trame et la personnalisation de la trame) ;
- Zone 8 : la partie qui affiche les résultats des tests (successful /failed).

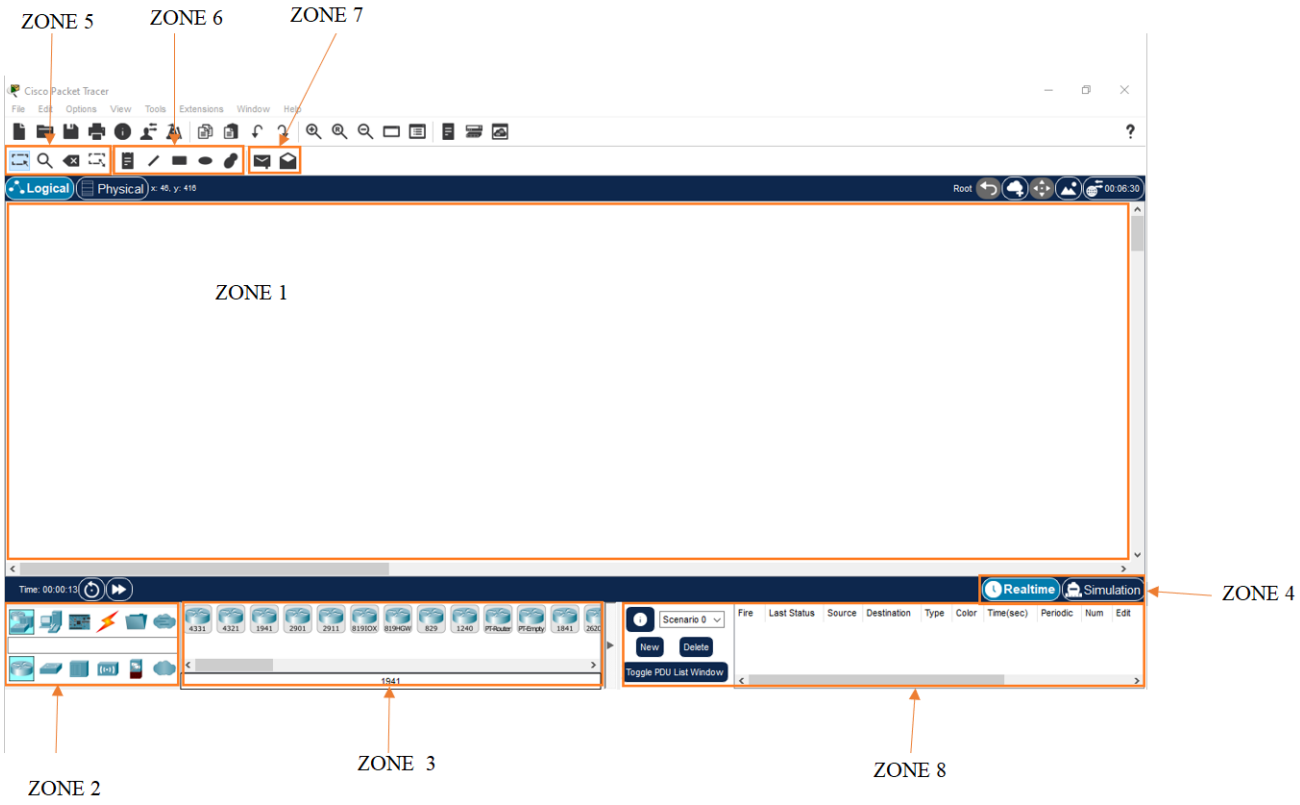

FIGURE IV.1 – l'interface principale du simulateur Cisco Packet Tracer.

IV.3 Réalisation

IV.3.1 Configuration des switchs

Durant cette partie nous allons présenter le processus de configuration courant aux switchs pour qu'ils puissent être fonctionnels.

IV.3.1.1 Attribution d'un nom au switch cœur

Afin d'attribuer un nom pour les différents équipements, il faudra accéder au mode configuration golobale identifier par "nom(config)#" en passant au mode d'exécution privilégier identifier grâce à un "#" depuis le mode utilisateur défini par ">". Grâce à la commande "enable" exécuter depuis le mode utilisateur on accède au mode enable puis enfin on exécute la commande "configuration terminal" afin d'accéder au mode de configuration globale. On utilise la commande "hostname" afin de changer le nom du switch tel qu'il est illustré dans le code IV.1.

Listing IV.1 – Attribution d'un nom au switch cœur (cas Switch cœur 1)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SwC1
SwC1(config)#
```

IV.3.1.2 Création et configuration des VLANs

Les tableaux (IV.1) et (IV.2) ci-dessous est une représentation des noms des VLANs existants au sein de l'entreprise et leurs adresses de sous-réseau.

Nam VLAN	ID VLAN	Adresse de sous-réseau	gateway
Centre_Informatique	10	192.168.10.0/26	192.168.10.1
Sous_Direction_Administration_et_Finances	20	192.168.20.0/26	192.168.20.1
Sous_Direction_Technique	30	192.168.30.0/26	192.168.30.1
Sous_Direction_Exploitation	60	192.168.60.0/26	192.168.60.1

Table IV.1 – Organisation des VLANs (cas SwC1)

Nam VLAN	ID VLAN	Adresse de sous-réseau	gateway
Centre_Informatique	10	192.168.10.0/26	192.168.10.30
Sous_Direction_Administration_et_Finances	20	192.168.20.0/26	192.168.20.30
Sous_Direction_Technique	30	192.168.30.0/26	192.168.30.30
Sous_Direction_Exploitation	60	192.168.60.0/26	192.168.60.30

Table IV.2 – Organisation des VLANs (cas SwC2)

Le code (IV.2) montre les commandes utilisées pour créer puis attribuer les adresses aux VLANs au niveau du premier switch cœur.

Listing IV.2 – Creation et configuration des interfaces VALNs (cas Switch cœur 1)

```
SwC1(config)#vlan 10
SwC1(config-vlan)#name Centre_Informatique
SwC1(config)#vlan 20
SwC1(config-vlan)#name Sous_direction_Administration_et_Finance
SwC1(config)#vlan 30
SwC1(config-vlan)#name Sous_Direction_Technique
SwC1(config)#vlan 60
SwC1(config-vlan)#name sous_Direction_Exploitation
SwC1(config-vlan)#exit
SwC1(config)#interface vlan 10
SwC1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

SwC1(config-if)#ip address 192.168.10.1 255.255.255.192
SwC1(config-if)#interface vlan 20
SwC1(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

SwC1(config-if)#ip address 192.168.20.1 255.255.255.192
SwC1(config-if)#interface vlan 30
```

```
SwC1(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

SwC1(config-if)#ip address 192.168.30.1 255.255.255.192
SwC1(config-if)#interface vlan 60
SwC1(config-if)#
%LINK-5-CHANGED: Interface Vlan60, changed state to up

SwC1(config-if)#ip address 192.168.60.1 255.255.255.192
SwC1(config-if)#exit
SwC1(config)#
```

On pourra vérifier que tous les VLANs ont été créé, et chaque adresse correspond au VLAN a été assignée grâce à la commande "show IP interface brief" exécuter en mode enable, tel qu'il est montré par le listing (IV.3).

Listing IV.3 – Vérification des VLANs (cas Switch ccœur 1)

```
SwC1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
...
Vlan10                 192.168.10.1    YES manual up                    down
Vlan20                 192.168.20.1    YES manual up                    down
Vlan30                 192.168.30.1    YES manual up                    down
Vlan60                 192.168.60.1    YES manual up                    down
SwC1#
```

IV.3.1.3 Configuration du protocole VTP

Le protocole VTP définit trois mode d'utilisation :

- **Serveur** : Défini comme étant le mode par défaut de tous les commutateurs niveau 2 de CISCO. Les commutateurs serveurs transmettent les VLANs et leurs paramètres aux commutateurs 'client' du même domaine VTP via des paquets 'vtp avertissement'. Ce mode permet la création, suppression et le renommage des VLANs tout en propageant ces modifications aux autres commutateurs du réseau.
- **Client** : Les commutateurs configurés en mode client ne supportent pas la création, suppression ni renommage des VLANs . Les informations des VLANs lui sont propagées et ne sont pas enregistrées dans sa NVRAM.
- **Transparent** : Les commutateurs en mode 'transparent' sont en mode passive au protocole VTP. Ils acheminent les paquets 'vtp avertissement' aux autres clients VTP. Dans ce mode on peut créer, renommer ou supprimer des VLANs mais ils seront liés à ce commutateur uniquement.

Les étapes de configuration décrit dans (IV.4) et (IV.5) qui suit illustrent le processus de configuration du protocole VTP sur le commutateur coeur et accès.

Listing IV.4 – Configuration du VTP (cas SwC 1)

```
SwC1(config)#vtp domain RTC
Changing VTP domain name from NULL to RTC
```

```
SwC1(config)#vtp password SOnAtrAcH06RTC
Setting device VLAN database password to SOnAtrAcH06RTC
SwC1(config)#vtp mode SERVER
Device mode already VTP SERVER.
SwC1(config)#vtp version 2
SwC1(config)#
```

Listing IV.5 – Configuration du VTP (cas SwA 1)

```
SwA1(config)#vtp domain RTC
Changing VTP domain name from NULL to RTC
SwA1(config)#vtp password SOnAtrAcH06RTC
Setting device VLAN database password to SOnAtrAcH06RTC
SwA1(config)#vtp mode client
Setting device to VTP CLIENT mode.
```

On pourra vérifier la configuration du protocole VTP grâce à la commande "show vtp status", il a noté que les commandes du mode d'exécution privilégié peuvent étre éxécuter dans le mode configuration globale en ajoutant l'instruction "do", comme le montre les listings (IV.6) et (IV.7).

Listing IV.6 – Vérification du statu VTP (cas SwC1)

```
SwC1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : RTC
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 000C.CF05.3C00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 192.168.1.2 on interface Vl1 (lowest numbered VLAN
interface found)

Feature VLAN :
--------------

VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
Configuration Revision          : 333
MD5 digest                      : 0xFF 0x78 0x70 0xB0 0xF0 0x6D 0x96
                                  0x6C 0xE6 0xC1 0xDD 0x32 0x4A 0x18
                                  0xCF 0xBE
```

Listing IV.7 – Configuration du VTP (cas SwA1)

```
SwA1#show vtp status
VTP Version                     : 2
Configuration Revision          : 333
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Client
```

```
VTP Domain Name                 : RTC
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xFF 0x78 0x70 0xB0 0xF0 0x6D 0x96 0x6C
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
```

Avec cette configuration les VLANs créés précédemment seront présents dans les switchs d'accès et même dans les switchs de distributions, pour vérifier cela on utilise la commande "show vlan brief" comme illustré dans la figure (IV.2).

```
SwA1#show vlan bri

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                Gig0/1, Gig0/2
10   Centre_Informatique              active
20   Sous-direction_Administration_et_Finance active
30   Sous-Direction_Technique         active
60   Sous-Direction_Exploitation      active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

FIGURE IV.2 – Vérification de la présence des VLANs (cas SwA1)

IV.3.1.4 Configuration des interfaces

Les interfaces fonctionnent selon deux modes différents : Trunk et Access.

- **Access** : Le mode access est destiné à la connexion terminale d'un périphérique (PC, imprimante, serveur, ...) faisant partie d'un seul vlan.
- **Trunk** : Le mode trunk permet de véhiculer sur une même liaison des paquets provenant de différents VLANs.

Le tableau (IV.3) indique les ports qui seront en mode access et ceux qui seront en mode trunk selon les switchs.

Switch	Interface	Mode
switch cœur 1 et 2	Fa0/1-3	Trunk
	fa0/4	Access
switch distribution 1 et 2	Fa0/1-7	Trunk
switch d'accés	Fa0/3-4	Trunk
	Fa0/1-2	Access

TABLE IV.3 – Mode des différents ports utilisés selon les switchs

Les interfaces qui raccordent les équipements finaux au réseau sont configurées en mode accès, tel qu'il est montré dans le listing (IV.9), contrairement aux autres interfaces qui permettant de véhiculer les paquets et par conséquent ils seront configurés en mode trunk, illustré par le listing (IV.8).

Listing IV.8 – Configuration des Interfaces du switch cœur (cas SwC1)

```
SwC1(config)#interface range FastEthernet0/1-3
SwC1(config-if-range)#switchport trunk encapsulation dot1q
SwC1(config-if-range)#switchport mode trunk
```

```
SwC1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
```

Listing IV.9 – Configuration des Interfaces du switch d'accès (cas SwA3)

```
SwA3(config)#interface range fastEthernet 0/1-2
SwA3(config-if)#switchport mode access
SwA3(config-if)#switchport access vlan 20
```

On finalise la configuration des interfaces trunk en autorisant que les VLANs créés de pouvoir transmettre sur ces interfaces, tel qu'il est illustré par le listing (IV.10).

Listing IV.10 – Allouer les VLANs aux interfaces trunk (cas SwC1)

```
SwC1(config)#interface range fastEthernet 0/1-3
```

```
SwC1(config-if)#switchport trunk allowed vlan 10,20,30,60
```

IV.3.1.5 Configuration du protocole DHCP

Nous allons ici réaliser la configuration du DHCP au niveau des switchs,afin que le DHCP puisse distribuer des adresses aux différents VLANS existants,nous allons devoir configurer les points suivants :

- Pour chaque VLAN configurer un pool DHCP dans lequel on spécifiera les options (passerelle, nom, adresse réseau, ...).
- Exclure les adresses qu'on souhaite ne pas distribuer (celle de la passerelle, ou de machines ayant des adresses fixes).

Le listing (IV.11) montre le processus de mise en service du serveur DHCP dans l'un des switchs coeur (SwC1).

Listing IV.11 – Configuration du DHCP (cas SwC1)

```
SwC1(config)#ip dhcp pool Centre_Informatique
SwC1(dhcp-config)#network 192.168.10.0 255.255.255.192
SwC1(dhcp-config)#default-router 192.168.10.1
SwC1(dhcp-config)#exit
SwC1(config)#ip dhcp pool Sous_direction_Administration_et_Finance
SwC1(dhcp-config)#network 192.168.20.0 255.255.255.192
SwC1(dhcp-config)#default-router 192.168.20.1
SwC1(dhcp-config)#exit
SwC1(config)#name Sous_Direction_Technique
SwC1(dhcp-config)#network 192.168.30.0 255.255.255.192
SwC1(dhcp-config)#default-router 192.168.30.1
SwC1(dhcp-config)#exit
SwC1(config)#sous_Direction_Exploitation
SwC1(dhcp-config)#network 192.168.60.0 255.255.255.192
SwC1(dhcp-config)#default-router 192.168.60.1
SwC1(dhcp-config)#exit
SwC1(config)#ip dhcp-excluded-address 192.168.10.1
SwC1(config)#ip dhcp-excluded-address 192.168.20.1
SwC1(config)#ip dhcp-excluded-address 192.168.30.1
SwC1(config)#ip dhcp-excluded-address 192.168.60.1
```

Une fois configuré il faudra activer le protocole DHCP au niveau de chaque PC, et ce en se rendant dans le « Desktop> IP Configuration » comme indiqué par les figures (IV.3) et (IV.4).

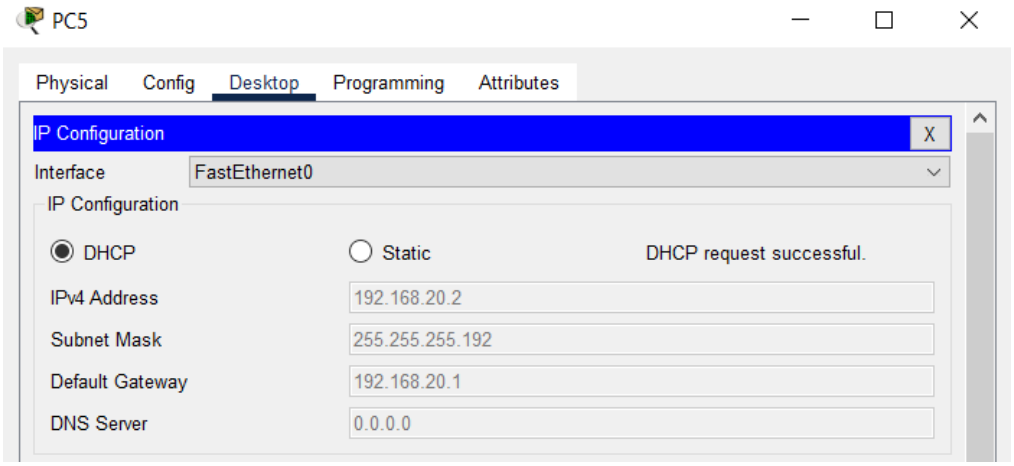

FIGURE IV.3 – Activation du DHCP (cas PC5)

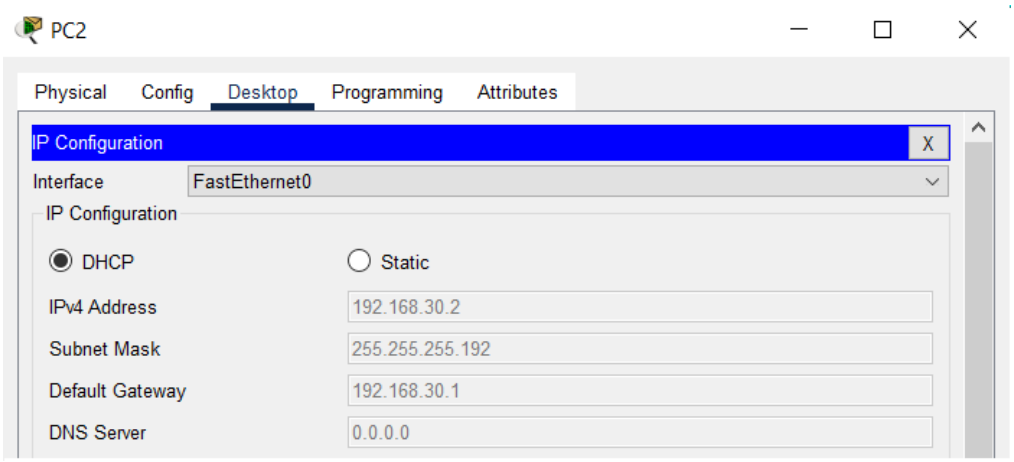

FIGURE IV.4 – Activation du DHCP (cas PC2)

IV.3.1.6 Configuration du protocole STP

Nous allons prendre le switch-cœur 1 comme switch-serveur en lui introduisant la plus grande priorité, illustré par le listing (IV.12) et le switch cœur 2 aura une priorité inférieure comme le montre le listing (IV.13) afin que seuls les chemins uniques vers le SwC1 soient actifs.

Listing IV.12 – Configuration du STP (cas SwC1)

```
SwC1(config)#spanning-tree vlan 10 priority 61440
SwC1(config)#spanning-tree vlan 20 priority 61440
SwC1(config)#spanning-tree vlan 30 priority 61440
SwC1(config)#spanning-tree vlan 60 priority 61440
SwC1(config)#spanning-tree vlan 10 root primary
SwC1(config)#spanning-tree vlan 20 root primary
SwC1(config)#spanning-tree vlan 30 root primary
SwC1(config)#spanning-tree vlan 60 root primary
```

Listing IV.13 – Configuration du STP (cas SwC2)

```
SwC2(config)#spanning-tree vlan 10 priority 57344
SwC2(config)#spanning-tree vlan 20 priority 57344
SwC2(config)#spanning-tree vlan 30 priority 57344
SwC2(config)#spanning-tree vlan 60 priority 57344
SwC2(config)#spanning-tree vlan 10 root secondary
SwC2(config)#spanning-tree vlan 20 root secondary
SwC2(config)#spanning-tree vlan 30 root secondary
SwC2(config)#spanning-tree vlan 60 root secondary
```

Pour le switch de distribution 1 nous allons les configurer comme switch-client en lui introduisant la priorité 0, dont le principe est donné par la listing (IV.14).

Listing IV.14 – Configuration STP (cas SwD1)

```
SwC1(config)#spanning-tree vlan 10 priority 0
SwC1(config)#spanning-tree vlan 20 priority 0
SwC1(config)#spanning-tree vlan 30 priority 0
SwC1(config)#spanning-tree vlan 60 priority 0
SwC1(config)#spanning-tree vlan 10 root primary
SwC1(config)#spanning-tree vlan 20 root primary
SwC1(config)#spanning-tree vlan 30 root primary
SwC1(config)#spanning-tree vlan 60 root primary
```

Pour augmenter le niveau de sécurité physique nous allons assigner aux ports des switchs d'accès utilisé l'adresse mac du Pc connecté, en lui indiquant la procédure à suivre si un autre Pc se connecte au même port. Ce processus est illustré par les figures (IV.5) et (IV.15).

L'adresse MAC d'un pc est obtenue on se rendant dans Desktop > Command Prompt puis on exécute la commande « ipconfig /all ».

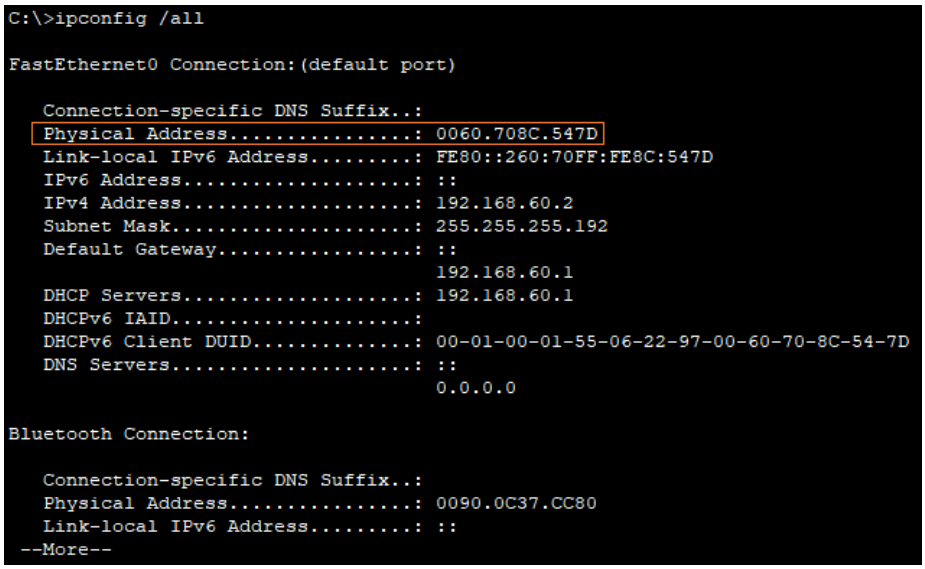

FIGURE IV.5 – Obtention de l'adresse MAC (cas PC0)

Listing IV.15 – Sécurisé les ports d'accès (cas : SwA1)

```
SwA1(config)#interface fastEthernet 0/1
SwA1(config-if)#switchport port-security maximum 1
SwA1(config-if)#switchport port-security mac-address 0060.708C.547D
SwA1(config-if)#switchport port-security violation shutdown
SwA1(config-if)#exit
SwA1(config)#interface fastEthernet 0/2
SwA1(config-if)#switchport port-security maximum 1
SwA1(config-if)#switchport port-security mac-address 0060.2A1D.ACCB
SwA1(config-if)#switchport port-security violation shutdown
```

IV.3.1.7 Sécurisation des lignes vty et console

Le port console est destiné à connecter un ordinateur à un switch/routeur et à gérer ce dernier, car il n'existe pas de dispositif d'affichage pour le switch, et les line vty représentent les lignes d'accès distantes, de par les services qu'ils offrent leurs sécurités sont indispensables, le tableau (IV.4) ci-dessous indique les mots de passe utilisés et le listing (IV.16) qui suit montre comment les sécurisés.

Switch	Service	Mots de passe
Switch cœur 1 et 2	Line consol	SoNaTracH06RTC
	Line vty	SoNaTracH06RTC
	Mode config terminal	rtc06RTC
Switch de distribution 1 et 2	Line consol	sOnAtRaCh06RtC
	Line vty	sOnAtRaCh06RtC
	Mode de configuration globale	RtC06rTc
Switch d'accès	Line consol	sOnaTRacH06RTc
	Line vty	sOnaTRacH06RTc
	Mode config terminal	rtC06RtC

TABLE IV.4 – Liste des mots de passe utilisés dans les différents switchs

Listing IV.16 – Sécuriser les accès d'un switch (cas SwD1)

```
SwD1(config)#line console 0
SwD1(config-line)#password sOnAtRaCh06RtC
SwD1(config-line)#logging synchronous
SwD1(config-line)#exec-timeout 5
SwD1(config-line)#login
SwD1(config-line)#exit
SwD1(config)#line vty 0 15
SwD1(config-line)#password sOnAtRaCh06RtC
SwD1(config-line)#logging synchronous
SwD1(config-line)#exec-timeout 5
SwD1(config-line)#login
SwD1(config-line)#exit
SwD1(config)#enable secret RtC06rTc
SwD1(config)#service password-encryption
```

La commande « logging synchronous » permet d'éviter que les messages IOS émettent vers la console ou vers les lignes Telnet interrompent la saisie sur le clavier.

La commande « exec-timeout » définit le temps d'inactivité d'une ligne de console ou de terminal virtuel avant l'interruption de la session encourt. La syntaxe est la suivante : exec-timeout minutes [secondes].

Listing IV.17 – Création d'un message de sécurité (cas SWC1)

```
SwC1(config)#banner motd "Authorized access only. Unauthorized access
is prohibiyrd and violators will be prosecuted to the full extent of
the law."
```

IV.3.1.8 Test de connectivité

La commande « ip routing » permet d'activer le routage inter-vlans sur le swtich cœur. Cette commande est exécutée en mode privilège. Les figures (IV.6) et (IV.7) montrent que les équipements sont joignables entre eux en interne.

```
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

FIGURE IV.6 – Test de connectivité du PC0 vers le PC4

```
C:\>ping 192.168.60.3

Pinging 192.168.60.3 with 32 bytes of data:

Reply from 192.168.60.3: bytes=32 time<1ms TTL=127
Reply from 192.168.60.3: bytes=32 time=12ms TTL=127
Reply from 192.168.60.3: bytes=32 time<1ms TTL=127
Reply from 192.168.60.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.60.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

FIGURE IV.7 – Test de connectivité du PC5 vers PC1

IV.3.2 Mise en place de la redondance

Les figures (IV.18), (IV.19), (IV.20), (IV.21) et (IV.22) illustrent les commandes qui nous permettent de configurer le protocole STP au niveau des switchs cœur, et de configurer la root primaire et secondaire à des VLAN. Nous avons fait en sorte que :

- SwC1 sera le root primaire pour les VLANs et le SwC2 le root secondaire ;
- SwD1 sera le root primaire pour les VLANs et le SwC2 le root secondaire.

Listing IV.18 – Configuration du mode actif pour le vlan 10 (cas SwC1)

```
SwC1(config)#interface vlan 10
SwC1(config-if)#standby 10 ip 192.168.10.1
SwC1(config-if)#standby 10 priority 200
SwC1(config-if)#standby 10 preempt
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
```

Listing IV.19 – Configuration du mode actif pour le vlan 20 (cas SwC1)

```
SwC1(config)#interface vlan 20
SwC1(config-if)#standby 10 ip 192.168.20.1
SwC1(config-if)#standby 10 priority 200
```

```
SwC1(config-if)#standby 10 preempt
%HSRP-6-STATECHANGE: Vlan20 Grp 10 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan20 Grp 10 state Standby -> Active
```

Listing IV.20 – Configuration du mode actif pour le vlan 30 (cas SwC1)

```
SwC1(config)#interface vlan 30
SwC1(config-if)#standby 10 ip 192.168.30.1
SwC1(config-if)#standby 10 priority 200
SwC1(config-if)#standby 10 preempt
%HSRP-6-STATECHANGE: Vlan30 Grp 10 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan30 Grp 10 state Standby -> Active
```

Listing IV.21 – Configuration du mode actif pour le vlan 60 (cas SwC1)

```
SwC1(config)#interface vlan 60
SwC1(config-if)#standby 10 ip 192.168.60.1
SwC1(config-if)#standby 10 priority 200
SwC1(config-if)#standby 10 preempt
%HSRP-6-STATECHANGE: Vlan60 Grp 10 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan60 Grp 10 state Standby -> Active
```

Listing IV.22 – Configuration du mode standby (cas SwC2)

```
SwC1(config)#interface vlan 10
SwC1(config-if)#standby 10 ip 192.168.10.1
SwC1(config-if)#standby 10 priority 150
SwC1(config-if)#standby 10 preempt
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby

SwC1(config)#interface vlan 20
SwC1(config-if)#standby 10 ip 192.168.10.1
SwC1(config-if)#standby 10 priority 150
SwC1(config-if)#standby 10 preempt
%HSRP-6-STATECHANGE: Vlan20 Grp 10 state Speak -> Standby

SwC1(config)#interface vlan 30
SwC1(config-if)#standby 10 ip 192.168.10.1
SwC1(config-if)#standby 10 priority 150
SwC1(config-if)#standby 10 preempt
%HSRP-6-STATECHANGE: Vlan30 Grp 10 state Speak -> Standby

SwC1(config)#interface vlan 60
SwC1(config-if)#standby 10 ip 192.168.10.1
SwC1(config-if)#standby 10 priority 150
SwC1(config-if)#standby 10 preempt
%HSRP-6-STATECHANGE: Vlan60 Grp 10 state Speak -> Standby
```

À ce stade le SwC1 est en mode actif et le SwC2 en standby, cela peut être vérifié grâce à la commande « show standby brief », illustré par la figure (IV.8) et (IV.9).

```
SwC1(config)#do sh stand bri
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   200 P Active   local           192.168.10.30   192.168.10.1
Vl20        10   200 P Active   local           192.168.20.30   192.168.20.1
Vl30        10   200 P Active   local           192.168.30.30   192.168.30.1
Vl60        10   200 P Active   local           192.168.60.30   192.168.60.1
```

FIGURE IV.8 – Vérification de l'activation (cas SwC1)

```
SwC2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   150 P Standby  192.168.10.1    local           192.168.10.1
Vl20        10   150 P Standby  192.168.20.1    local           192.168.20.1
Vl30        10   150 P Standby  192.168.30.1    local           192.168.30.1
Vl60        10   150 P Standby  192.168.60.1    local           192.168.60.1
```

FIGURE IV.9 – Vérification de la mise en standby (cas SwC2)

IV.3.3 Configuration des routeurs

Le tableau (IV.5) ci-dessous résume les interfaces utilisées et les adresses.

Périphérique	Interface	Adresse IP	Masque de sous-réseau
RTC	Fa0/0	192.168.0.0	255.255.192.0
	Se0/2/0	10.1.1.1	255.255.255.0
FAI	Se0/2/0	10.1.1.2	255.255.255.0
	Se0/2/1	10.10.2.1	255.255.255.0
SITE	Se0/2/0	10.10.2.2	255.255.255.0
	Fa0/0	172.16.5.1	255.255.255.0

TABLE IV.5 – Table d'adressage

IV.3.3.1 Configuration des interfaces

Les figures (IV.23), (IV.24) et (IV.25) illustrent la configuration des interfaces des routeurs RTC, FAI et SITE respectivement.

Listing IV.23 – Configuration des interfaces du routeur RTC

```
RTC(config)#interface FastEthernet0/0
RTC(config-if)#ip address 192.168.2.2 255.255.255.192.0
RTC(config-if)#no shutdown

RTC(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

RTC(config-if)#exit
RTC(config)#interface serial 0/2/0
RTC(config-if)#ip address 10.1.1.1 255.255.255.255.0
RTC(config-if)#clock rate 64000
RTC(config-if)#no shutdown

RTC(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to down
```

Listing IV.24 – Configuration des interfaces du routeur FAI

```
FAI(config)#interface Serial 0/2/0
FAI(config-if)#ip address 10.1.1.2 255.255.255.255.0
FAI(config-if)#no shutdown

FAI(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed
state to up

FAI(config-if)#exit
FAI(config)#interface serial 0/2/1
FAI(config-if)#ip address 10.10.2.1 255.255.255.255.0
FAI(config-if)#clock rate 64000
FAIT(config-if)#no shutdown

FAI(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/1, changed state to down
```

Listing IV.25 – Configuration des interfaces du routeur SITE

```
SITE(config)#interface FastEthernet0/0
SITE(config-if)#ip address 172.16.5.1 255.255.255.255.0
SITE(config-if)#no shutdown

SITE(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

SITE(config-if)#exit
SITE(config)#interface serial 0/2/0
SITE(config-if)#ip address 10.10.2.2 255.255.255.255.0
SITE(config-if)#no shutdown
```

```
SITE(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed
state to up
```

IV.3.3.2 Mise en place du NAT

Dans cette partie nous allons mettre en place le NAT dans les différents routeurs existants comme les listings (IV.26),(IV.27) et (IV.28) l'indiquent. Le NAT est un processus de modification des adresses IP source et destination, ce qui signifie qu'une seule adresse IP unique est requise pour représenter un groupe entier d'ordinateurs à quoi que ce soit en dehors de leur réseau.

Listing IV.26 – Signaler la configuration de la NAT aux interfaces (cas : RTC)

```
RTC(config)#interface FastEthernet 0/0
RTC(config-if)#ip nat inside
RTC(config-if)#exit
RTC(config)#interface serial 0/2/0
RTC(config-if)#ip nat outside
RTC(config-if)#exit
RTC(config)#
```

Listing IV.27 – Configuration de la NAT (cas : routeur RTC)

```
RTC(config)#access-list 100 deny ip 192.168.0.0 0.0.63.255 172.16.5.0
0.0.0.255
RTC(config)#access-list 100 permit ip 192.168.0.0 0.0.63.255 any
RTC(config)#ip nat inside source list 100 interface Serial 0/2/0
overload
```

Listing IV.28 – Configuration de la NAT (cas : routeur SITE)

```
RTC(config)#access-list 100 deny ip 172.16.5.0 0.0.0.255 192.168.0.0
0.0.63.255
RTC(config)#access-list 100 permit ip 172.16.5.0 0.0.0.255 any
RTC(config)#ip nat inside source list 100 interface Serial 0/2/0
overload
```

IV.3.3.3 Mise en place du routage dynamique

Le déploiement du routage dynamique est illustré par les figures (IV.29), (IV.30) et (IV.31) ci-dessous .

Listing IV.29 – Configuration du protocole OSPF (cas : routuer RTC)

```
RTC(config)#router ospf 1
RTC(config-router)#network 10.1.1.0 0.0.0.255 area 10
RTC(config-router)#network 192.168.0.0 0.0.63.255 area 10
RTC(config-router)#exit
```

Listing IV.30 – Configuration du protocole OSPF (cas : routeur FAI)

```
FAI(config)#router ospf 1
FAI(config-router)#network 10.1.1.0 0.0.0.255 area 10
FAI(config-router)#network 10.10.2.0 0.0.0.255 area 10
FAI(config-router)#exit
```

Listing IV.31 – Configuration du protocole OSPF (cas : routeur SITE)

```
SITE(config)#router ospf 1
SITE(config-router)#network 172.16.5.0 0.0.0.255 area 10
SITE(config-router)#network 10.10.2.0 0.0.0.255 area 10
SITE(config-router)#exit
```

À partir d'un certain délai, un message est partagé entre les différents routeurs afin qu'ils puissent avoir connaissance des réseaux voisins. La figure (IV.10) illustre la table de routage du routeur FAI.

```
FAI#show ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, 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 not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Serial0/2/0
L       10.1.1.2/32 is directly connected, Serial0/2/0
C       10.10.2.0/24 is directly connected, Serial0/2/1
L       10.10.2.1/32 is directly connected, Serial0/2/1
     172.16.0.0/24 is subnetted, 1 subnets
O       172.16.5.0/24 [110/65] via 10.10.2.2, 00:03:57, Serial0/2/1
O    192.168.0.0/18 [110/65] via 10.1.1.1, 00:03:57, Serial0/2/0
```

FIGURE IV.10 – Table de routage (cas : routeur FAI)

Afin que le routeur RTC puisse joindre les différents réseaux internes, des routes statiques doivent être configurées comme le démontre le listing (IV.32) ci-dessous.

Listing IV.32 – Configuration des routes statiques

```
RTC(config)#ip route 192.168.10.0 255.255.255.192 192.168.2.1
RTC(config)#ip route 192.168.20.0 255.255.255.192 192.168.2.1
RTC(config)#ip route 192.168.30.0 255.255.255.192 192.168.2.1
RTC(config)#ip route 192.168.60.0 255.255.255.192 192.168.2.1
RTC(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.1
```

IV.3.3.4 Sécurisation du Routeur RTC

En clôture la configuration du routeur RTC par la sécurisation des accès physiques et distants tels qu'il est montré par le listing (IV.33).

Listing IV.33 – Sécuriser les accès du routeur RTC

```
RTC(config)#line console 0
RTC(config-line)#password rtc06
RTC(config-line)#logging synchronous
RTC(config-line)#exec-timeout 5
RTC(config-line)#login
RTC(config-line)#exit
RTC(config)#line vty 0 15
RTC(config-line)#password rtc06
RTC(config-line)#logging synchronous
RTC(config-line)#exec-timeout 5
RTC(config-line)#login
RTC(config-line)#exit
RTC(config)#enable secret rtc06
RTC(config)#service password-encryption
```

IV.3.4 Mise en fonction du tunnel VPN IPsec

IV.3.4.1 Configuration de la négociation des clés

Le listing (IV.34) illustre la procédure d'activation du protocole «IKE» et la configuration du protocole «ISAKMP».

Listing IV.34 – Configuration de la négociation des clés (cas : router RTC)

```
RTC(config)#crypto isakmp enable
RTC(config)#crypto isakmp policy 10
RTC(config-isakmp)#encryption aes
RTC(config-isakmp)#authentication pre-share
RTC(config-isakmp)#hash sha
RTC(config-isakmp)#group 2
RTC(config-isakmp)#lifetime 86400
RTC(config-isakmp)#exit
RTC(config)#crypto isakmp key RTCVPN06 address 10.10.2.2
```

IV.3.4.2 Configuration de la méthode de chiffrement de données

Le chiffrement de données représente le point central de la sécurité dans un échange sur internet sa mise en place est donnée par le listing (IV.35).

Listing IV.35 – Configuration de la méthode de chiffrement de données (cas : routeur RTC)

```
RTC(config)#crypto ipsec transform-set VPNRTC esp-aes esp sha-hmac
RTC(config)#crypto ipsec security-association lifetime seconds 86400
RTC(config)#ip access-list extended VPN
RTC(config-ext-nacl)#permit ip 192.168.0.0 0.0.63.255 172.16.5.0 0.0.0.255
RTC(config-ext-nacl)#exit
```

```
RTC(config)#crypto map CARTEVPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured
RTC(config-crypto-map)#match address VPN
RTC(config-crypto-map)#set peer 10.10.2.2
RTC(config-crypto-map)#set transform-set VPNRTC
RTC(config-crypto-map)#exit
RTC(config)#interface serial 0/2/0
RTC(config-if)#crypto map CARTEVPN
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

IV.3.5 Configuration du firewall

Dans cette étape, nous allons créer des interfaces VLAN internes, externes et DMZ tel qu'il est montré dans les figures (IV.36) et (IV.41), on va leurs attribuer des adresses IP et définir le niveau de sécurité de l'interface. Enfin, nous allons affectez les ports utilisés aux interfaces correspondantes comme il est décrit dans les figures (IV.37) et (IV.42).

Listing IV.36 – Création des VLANs inside et outside

```
FWRTC(config)#interface vlan 1
FWRTC(config-if)#nameif inside
FWRTC(config-if)#ip address 192.168.1.1 255.255.255.240
FWRTC(config-if)#security-level 100
FWRTC(config-if)#interface vlan 2
FWRTC(config-if)#nameif outside
FWRTC(config-if)#ip address 192.168.2.1 255.255.192.0
FWRTC(config-if)#security-level 0
FWRTC(config-if)#exit
```

Listing IV.37 – Configuration des interfaces

```
FWRTC(config)#interface ethernet 0/1
FWRTC(config-if)#switchport access vlan 1
FWRTC(config-if)#interface ethernet 0/2
FWRTC(config-if)#switchport access vlan 1
FWRTC(config-if)#interface ethernet 0/3
FWRTC(config-if)#switchport access vlan 2
FWRTC(config-if)#exit
```

Listing IV.38 – Configuration de la NAT

```
FWRTC(config)#object network INSIDE-NET
FWRTC(config-network-object)#subet 192.168.0.0 255.255.255.240
FWRTC(config-network-object)#nat (inside,outside) dynamic interface
FWRTC(config-network-object)#end
```

Nous allons configurer une liste d'accès nommée (OUTSIDE-NET) qui autorise tout paquet IP depuis le site distant vers le réseau RTC, cette condition sera appliquée à la liste d'accès de l'interface extérieure de l'ASA dans le sens IN. Le principe est donné par le listing

(IV.39).

Listing IV.39 – Mise en place d'une accés liste

```
FWRTC(config)#access-list OUTSIDE-NET extended permit ip 172.16.5.0
 255.255.255.0 192.168.0.0 255.255.192.0
FWRTC(config)#access-group OUTSIDE-NET in interface outside
FWRTC(config)#
```

Afin que les paquets du site distant puissent être orientés vers le réseau interne, des routes statiques doivent être configurées tel que le lisnting (IV.40) l'illustre.

Listing IV.40 – Configuration des routes inside et outside

```
FWRTC(config)#route outside 0.0.0.0 0.0.0.0 192.168.2.2
FWRTC(config)#route inside 192.168.10.0 255.255.255.192 192.168.1.2
FWRTC(config)#route inside 192.168.20.0 255.255.255.192 192.168.1.2
FWRTC(config)#route inside 192.168.30.0 255.255.255.192 192.168.1.2
FWRTC(config)#route inside 192.168.60.0 255.255.255.192 192.168.1.2
FWRTC(config)#route inside 192.168.10.0 255.255.255.192 192.168.1.3
FWRTC(config)#route inside 192.168.20.0 255.255.255.192 192.168.1.3
FWRTC(config)#route inside 192.168.30.0 255.255.255.192 192.168.1.3
FWRTC(config)#route inside 192.168.60.0 255.255.255.192 192.168.1.3
FWRTC(config)#
```

IV.3.5.1 Configuration de la DMZ

À cette étape nous allons attribuer un nom et une adresse ip pour le VLAN 3 de la DMZ et nous lui définirons un niveau de sécurité,tel qu'il est illustré dans le listing (IV.41) en-dessous.

Listing IV.41 – Création du VLAN DMZ

```
FWRTC(config)#interface vlan 3
FWRTC(config-if)#ip address 192.168.3.1 255.255.255.0
FWRTC(config-if)#security-level 70
FWRTC(config-if)#nameif DMZ
FWRTC(config-if)#exit
```

Le listing (IV.42) montre l'attribution de l'interface qui relie la DMZ au pare-feu et sa configuration en mode access.

Listing IV.42 – Configuration de l'interface reliant le réseau DMZ

```
FWRTC(config)#interface ethernet 0/0
FWRTC(config-if)#switchport access vlan 3
FWRTC(config-if)#exit
```

Enfin on va rajouter une condition à l'accès liste (OUTSIDE-NET) qui stipule que tout réseau pourra joindre la DMZ, et qui sera appliquée à l'interface extérieure de l'ASA dans le sens IN, puis on va créer une nouvelle liste d'accès (ENTRER) qui autorise la DMZ de communiquer avec le réseau interne de l'entreprise si et seulement si une communication TCP est initialisée avec cette dernière et de répondre à la sollicitation ICMP du réseau interne, ces conditions seront appliquées à l'interface intérieure de l'ASA dans le sens OUT, tel que

le montre le listing (IV.43).

Listing IV.43 – Configuration de l'accès liste

```
FWRTC(config)#access-list OUTSIDE-NET extended permit ip 0.0.0.0
0.0.0.0 192.168.3.0 255.255.255.0
FWRTC(config)#access-group OUTSIDE-NET in interface outside
FWRTC(config)#access-list ENTRER extended permit icmp 192.168.3.0
255.255.255.0 192.168.0.0 255.255.192.0 echo-reply
FWRTC(config)#access-list ENTRER extended permit tcp 192.168.3.0
255.255.255.0 192.168.0.0 255.255.192.0
FWRTC(config)#access-group ENTRER out interface inside
```

IV.3.5.2 Configuration du SSH

Listing IV.44 – Mise en service du SSH

```
FWRTC(config)#crypto keu generate rsa general-key modulus 2048
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>

Do you really want to replaxe them? [yes/no]: yes
Keypair generation process begin. Please wait...

FWRTC(config)#username RTCadmin password RTC06ADMIN
FWRTC(config)#ssh 192.168.10.0 255.255.255.192 inside
FWRTC(config)#ssh timeout 20
FWRTC(config)#aaa authentication ssh console LOCAL
```

Dans le listing (IV.44) au-dessus on commence par augmenter le niveau de cryptage de la clé qui sera utilisé pour autoriser que les ordinateurs appartenant au centre informatique d'accéder au firewall via le ssh.

On clôtura la configuration de firewall par la sécurisation de l'accès au firewall par le mot de passe RTCASA06, décrit dans le listing (IV.45).

Listing IV.45 – Activation du mot de passe sur le firewall

```
FWRTC(config)#enable password RTCASA06
```

IV.3.5.3 Test de la connectivté

Afin que le réseau de l'entreprise puisse joindre les différents réseaux (DMZ, SITE) des routes statiques doivent être configurées au niveau des switchs cœur. Le principe est donné par le listing (IV.46).

Listing IV.46 – Configuration des routes statiques vers les réseaux externes

```
SwC1(config)#ip route 192.168.3.0 255.255.255.0 192.168.1.1
SwC1(config)#ip route 172.16.5.0 255.255.255.0 192.168.1.1
```

Afin de tester le bon fonctionnement du réseau et de s'assurer qu'il est opérationnel, nous allons simuler des Ping continus d'un des Vlans vers le site distant, puis un ping depuis un des serveurs de la DMZ vers le réseau interne afin de vérifier que ce dernier ne puisse initier une communication avec les équipements internes, tel qu'il est illustré dans la figure (IV.11), et (IV.12), et enfin du site vers le réseau interne illustré par la figure (IV.13) pour ces tests nous allons prendre le serveur web et le PC 2 du VLAN 30.

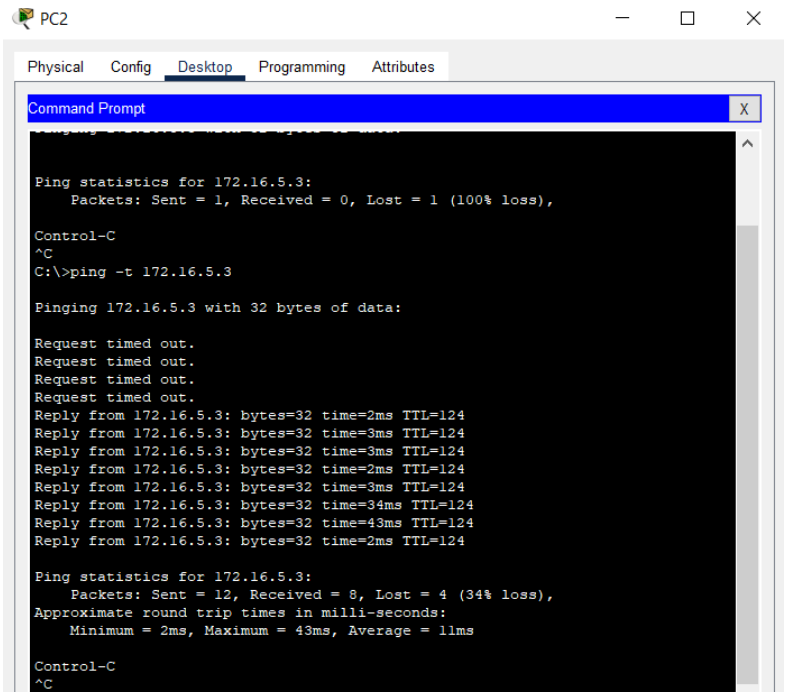

FIGURE IV.11 – Test de connectivité du réseau interne (PC2) vers le site

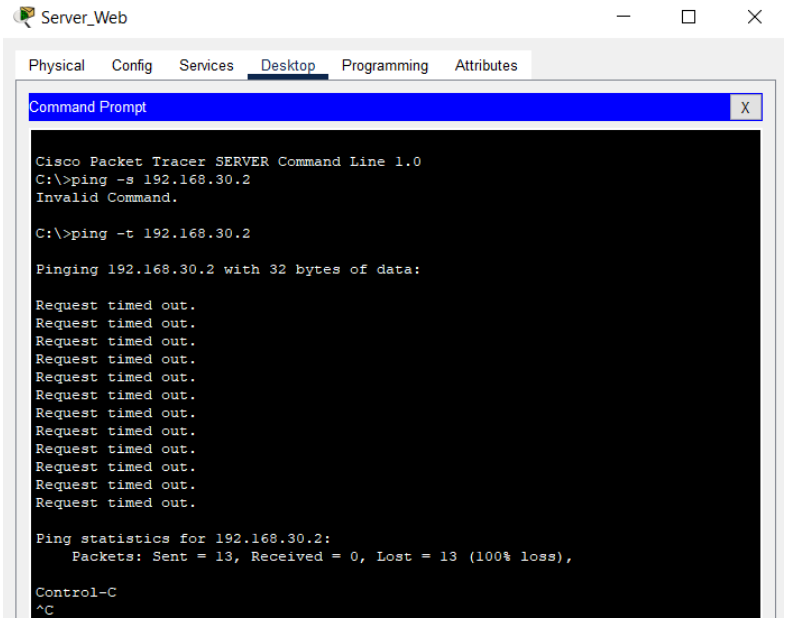

FIGURE IV.12 – Test de connectivité de la dmz vers le réseau interne (PC2)

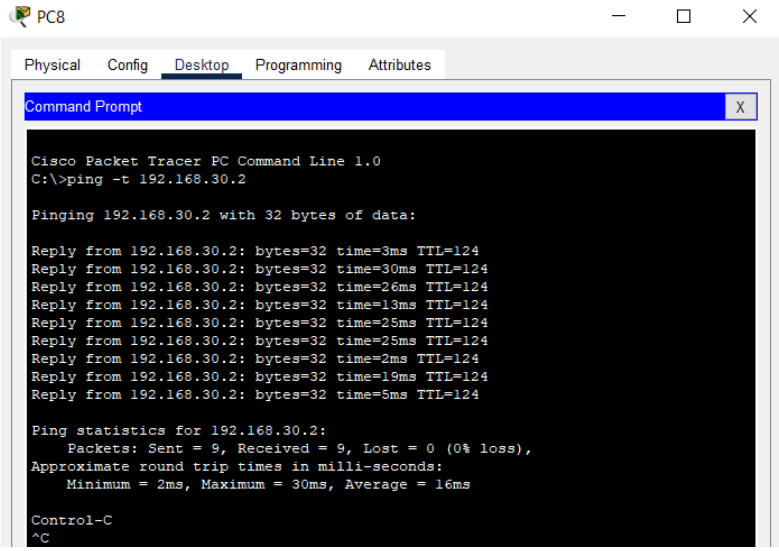

FIGURE IV.13 – Test de connectivité du site vers le réseau interne (PC2)

Enfin, nous allons simuler un accès vers un site web depuis le réseau interne et le pc du site distant tel qu'il est illustré par les figures (IV.16) et (IV.15), et ce en activant le service HTTPS dans le serveur web de la DMZ tel qu'il est montré par la figure (IV.14).

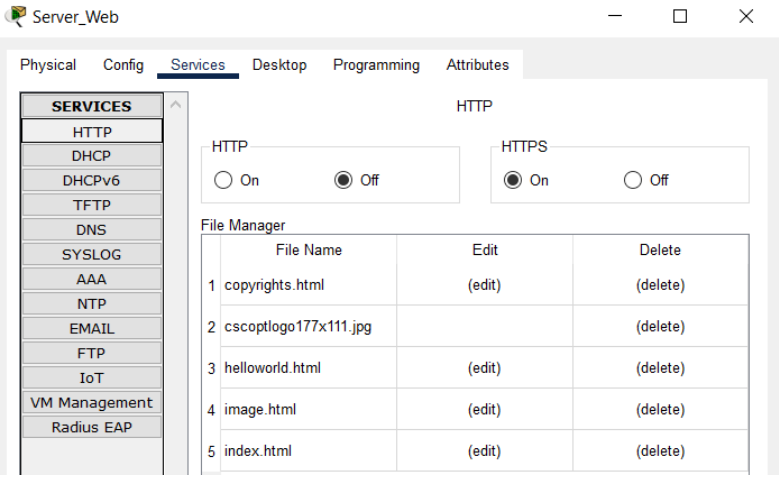

FIGURE IV.14 – Activation du protocole https

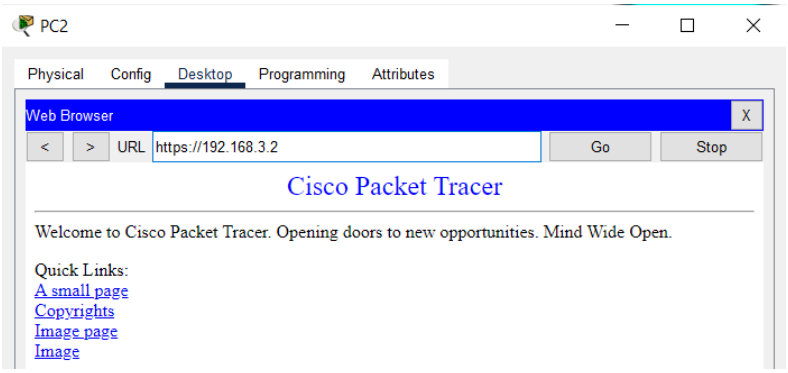

FIGURE IV.15 – Test de connectivité du réseau interne (PC2) vers la DMZ

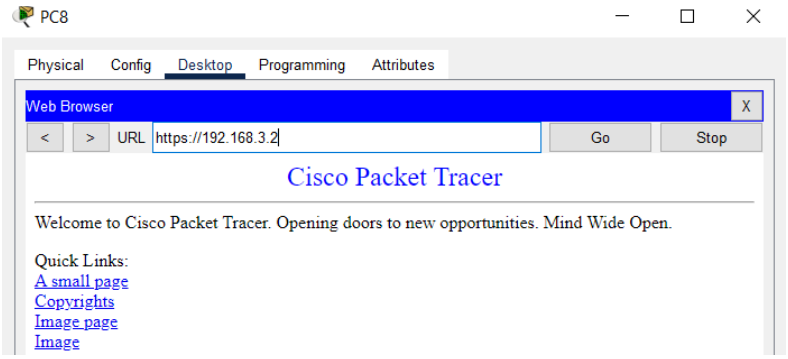

FIGURE IV.16 – Test de connectivité du site distant vers la DMZ

IV.4 Conclusion

Dans ce chapitre, nous avons pu décrire toutes les configurations effectuées au niveau du réseau local concernant les VLANs, DHCP, VTP, STP, sécurité des ports, ainsi que le HSRP, ensuite nous avons configuré tout ce que sont en relation avec le réseau externe, le pare-feu et la DMZ ; OSPF et le VPN. Les solutions proposées apportent une sécurisation des données échangées entre les différents services de l'entreprise RTC et entre le site de Bejaïa et un autre site distant, et améliorent la gestion de manière dynamique en évitant des collisions, et en assurant la continuité du son réseau.

Conclusion générale

Dans ce présent projet de fin d'étude nous avons pu approfondir nos connaissances théoriques et les mettre en pratique durant notre stage au sein de l'entreprise RTC SONATRACH BEJAIA ,nous avons proposé une nouvelle topologie réseau dont l'objectif est d'améliorer le niveau de la sécurité de celui-ci.

Cette nouvelle topologie consiste à mettre une politique de sécurité qui empêche tout accès indésirable au sein du réseau, et qui protège ce dernier de toutes menaces et attaques qui peuvent intervenir de la connexion avec le réseau extérieur et même du réseau interne

D'abord nous avons sécurisé le réseau interne en utilisant des VLANS qui représentent le cœur de la configuration des LAN pour réduire les domaines de collisions et éviter les congestions, ce qui permet de renforcer la sécurité au niveau du réseau interne.Ensuite nous avons mis en place de la redondance pour assurer la tolérance aux pannes et augmenter la capacité et améliorer la fiabilité du réseau.

Dans ce cadre-là, et pour améliorer le niveau de sécurité des architectures réseaux en plus de pare-feu ; on a inclus une passerelle entre la zone Inside et la zone outside appelée zone démilitarisé DMZ.

Concernant la partie extérieure et les menaces peuvent parvenir d'elle ; nous avons solutionné par l'utilisation d'un VPN site-à-site qui consiste à mettre au point une liaison permanente, distante et sécurisée entre le site du Bejaia RTC et un autre site distant ; et par l'utilisation des listes de contrôle d'accès ACL, qui se basent sur le filtrage des paquets entrants ou sortants, par l'utilisation des adresses IP source et IP destination selon le besoin.

La variété des tâches que nous avons accomplies ; nous a permis d'améliorer nos connaissances dans le domaine de la sécurité des réseaux tels que la manipulation du matériel et la configuration des différentes solutions.

L'intérêt principal que nous avons tiré de ce travail est que nous avons pu voir la complexité de la mise en route d'un nouveau projet dans des durées de temps exactes, et de sa rapide évolution qui nous a appris à mieux nous organiser afin d'être capable de finaliser notre travail.

Bibliographie

[1] Claude Servin. *Réseaux & télécoms : cours avec 129 exercices corrigés*. Dunod, 2009.

[2] Richard Froom, Balaji Sivasubramanian et Erum Frahim. *Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide : Foundation learning for SWITCH 642-813*. Cisco press, 2010.

[3] Raphael Yende. "COURS D'ADMINISTRATION DES RÉSEAUX INFORMATIQUES". In : (2019).

[4] Danièle Dromard et Dominique Seret. *Architecture des réseaux*. Pearson Education France, 2013.

[5] Laurent Bloch et al. "Sécurité informatique". In : *Edition EYROLLES* (2007).

[6] N BENAMIROUCHE. "Cours de sécurité de l'information". In : (2017).

[7] Albert de Mereuil et Annabel-Mauve Bonnefous. "Anatomie d'une cyber-attaque contre une entreprise : comprendre et prévenir les attaques par déni de service". In : *Annales des Mines-Gerer et comprendre*. 1. FFE. 2016, p. 5-14.

[8] Gilles Dubertret. "Initiation à la cryptographie". In : (1998).

[9] Mohammed EL HARFAOUI. "Listes de Contrôle d'Access". In : (2018).

[10] T Li et al. *RFC2281 : Cisco Hot Standby Router Protocol (HSRP)*. 1998.

[11] *Commutateurs de Gamme Cisco Catalyst 2950*. Cisco Systems, Inc. 2003.

[12] *Commutateurs Cisco Catalyst 3560*. Cisco Systems, Inc.

[13] *ROUTEURS A SERVICES INTÉGRES DE LA GAMME CISCO 2800*. Cisco Systems, Inc.

[14] *Cisco ASA 5500*. Cisco Systems, Inc. 2009.

Résumé

Notre projet a pour objectif de remédier aux problématiques de sécurité, disponibilité et intégrité des ressources informatiques de la société Sonatrach que pose l'ouverture à internet. Dans ce but, le projet propose une nouvelle architecture plus sur en utilisant des protocoles de redondances, et un autre protocole qui permet de centraliser la gestion des réseaux locaux virtuels (VTP), la mise en place d'un DMZ et l'utilisation d'une politique de filtrage des paquets au niveau du firewall. Pour mettre en pratique nos solutions, nous nous sommes servis du simulateur "PACKET TRACER", qui nous offre la possibilité de réaliser un réseau physique virtuel et de reproduire le fonctionnement des différents protocoles sur ce réseau.

Mots clés : VLAN, VTP, DMZ, firewall, PACKET TRACER.

Abstract

Our project aims to remedy the problems of security, availability and integrity of computer resources of the company Sonatrach that poses the opening to the Internet. To this end, the project proposes a new architecture more secure by using redundancy protocols, and another protocol that allows to centralize the management of virtual local networks (VTP), the establishment of a DMZ and the use of a packet filtering policy at the firewall. To put our solutions into practice, we used the "PACKET TRACER" simulator, which allows us to create a virtual physical network and to reproduce the functioning of the different protocols on this network.

Key words : VLAN, VTP, DMZ, firewall, PACKET TRACER.