République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A. Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Fin de Cycle

En vue de l'obtention du diplôme de Master professionnel en Informatique

Option : Administration et sécurité des réseaux

Thème

Les outils d'administration et sécurité des réseaux informatiques : cas d'étude Sonatrach

Réalisé par

M^{lle} BENNACER Yasmina
M^{lle} MOKRANI Yasmine

Devant le jury composé de

Présidente :	Mme. AIT ABDELOUHAB Karima	M.C.B	Université de Béjaïa
Encadrant :	Mr. YAZID Mohand	M.C.A	Université de Béjaïa
Co-Encadrant :	M^{lle} BRAHMI Saloua	Doctorante	Université de Béjaïa
Examinatrice :	M^{lle}. MAMMERI Souhila	M.A.B	Université de Béjaïa

promotion 2020-2021

Remerciements

Au terme de ce travail, nous tenons à exprimer notre profonde gratitude et nos sincères remerciements.

Nous remercions le dieu le tout puissant de nous avoir donné la force, la volonté de donner le meilleur de nous-même et le courage de mener ce travail.

Nous tenons en premier lieu à exprimer notre profonde reconnaissance à notre encadreur Mr **YAZID Mohand** , pour son encadrement , puis pour nous avoir fait confiance , encouragé et conseillé au cours de notre cursus .
Comme on exprime notre reconnaissance pour le directeur de la RTC Bejaïa pour nous avoir autorisé à effectué notre stage .
Nous remerciements les plus vifs vont tout particulièrement à notre encadreur de stage Mr **SOUADIH kamel** pour son encadrement et orientation avec toute rigueur tout le long de notre stage inspirant en nous curiosité et passion pour promouvoir la réalisation de ce travail.
Nous tenons à remercier très chaleureusement notre Co-ecadrante Mme **BRAHMI Saloua** pour sa collaboration importante pendant la rédaction de ce mémoire, ses encouragements et ses conseilles.
Nous tenons également à remercier les membres du jury d'avoir consacré leurs temps à la lecture et à la correction de ce mémoire .
Nous remerciements les plus particuliers à nos parents, en qui nous avons puisé tout le courage, la volonté et la confiance, nous leur serons éternellement reconnaissants.
Enfin, Nous n'omettrons jamais d'exprimer toute notre gratitude à tous les membres du département d'Informatique de l'Université de Béjaia, que ce soit enseignants ou cadres administratifs, qui de près ou de loin n'ont épargné aucun effort pour que notre formation et nos travaux se terminent dans de bonnes conditions.

Dédicaces

Une spéciale dédicace pour ma grand-mère BOUAKLI Zohra qui a tant attendu le jour de ma soutenance et qui nous a quitté quelques jours avant de réaliser sa joie d'assister , qui m'a beaucoup encourager pour bien faire, paix à ton âme .

A **ma chère mère ISSADOUNANE Karima**

tes prières et ta bénédiction m'ont été d'un grand secours pour mener à bien mes études. Je te dédie ce travail pour t'exprimer ma reconnaissance pour tous les sacrifices que ta mené depuis ma naissance .

A **mon chèr père Louanas**

symbole de sacrifice, de tendresse, et qui m'a donné un magnifique modèle de labeur et de persévérance.

A **mes chèrs frères et sœurs : Lyas , Azdine, Souad et Nadjet** pour leur soutient et encouragement.

A **mon chèr fiancé Dr MEHELLEB Sofiane** qui ma accompagné pendant toutes ces longues années dans les bons comme dans les mauvais moments , pour son amour, confiance ,soutient et encouragements .

A **mes chères nièces Emilie , Malak et Farah** ma source de tendresse.

A mon chèr beau frère **BAGHEZOUZ Lyakin** et A ma chère belle sœur **HARATI Besma** .

Je tiens également à exprimer ma profonde gratitude à toute ma famille , ma belle famille , mes amies et toutes celles et ceux qui ont participés du pré ou du loin à la réalisation de ce travail.

Yasmina.B

Dédicaces

A mes parents MOKRANI BOUZIDE et SAHKI ZAKIA

Rien au monde ne vaut vos efforts fournis jour et Nuit pour mon éducation et mon bien être. Ce travail est le fruit de vos sacrifices. Aucune dédicace ne saurait exprimer l'amour, L'estime, et le respect que j'ai toujours eu Pour vous. Vous qui êtes pour moi un exemple

A mon frère bien aimer« OUASSIM » et mes sœurs« Lydia et Ikrame », et à mon amour «Lyazid.M».

A toute la famille MOKRANI spécialement «ma grande mère MARBOHA, Mes deux tante NADIA et HALIMA » et la famille SAHKI spécialement «ma cousine ZINA»

Ils vont trouver ici l'expression de mes sentiments de respect et de reconnaissance pour le soutien qu'ils n'ont cessé de me porter.

A tous mes professeurs :

Leur générosité et leur soutien m'oblige de leurs témoigner mon profond respect et ma loyale considération.

A mes chères ami(e)s exceptionnellement : AIT MANSOUR. A, AMAOUZE.Y, ATMAOUI.I, BERABZE. K, CHEURFA.S, IHADDADEN.S, NACERDDINE.Y, SEGHIRI.S.

Je ne peux trouver les mots justes et sincères pour vous exprimer mon affection et mes pensées, vous êtes pour moi des frères, sœurs et des amis sur qui je peux compter. En témoignage de l'amitié qui nous uni et des souvenirs de tous les moments que nous avons passés ensemble, je vous dédie ce travail et je vous souhaite une vie pleine de santé et de bonheur.

YASMINE.M

Table des matières

Table des figures

Liste des abréviations

ACL	Access Control List
ARP	Adress Resolution Protocol
CLI	Command Line Interface
FTP	File Transfer Protocol
GNS3	Graphical Network Simu-lator
GUI	Graphical User Interface
HTTPs	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IPSec	IPSec Internet Protocol Security
IP	Internet Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
NAT	Network Address Translation
OSI	Open Systems Interconnection, Interconnexion des systèmes ouverts
PAN	Personale Area Network
POP3	Port Office Protocole version 3
RARP	Reverse Adress Resolution Protocol
RTC	Région Transport Centre, Bejaia
SNMP	Simple Network Management Protocol
SONATRACH	Société Nationale de Transport et Commercialisation des Hydrocarbure
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

Introduction générale

De nos jours, le développement industriel et les réseaux informatiques invoquent le développement des infrastructures réseaux utilisées, ainsi qu'ils rendent la sécurité de ces équipements plus complexes. L'administration et la sécurité des réseaux informatiques n'est réalisable qu'à avec l'aide d'outils appropriés.

L'entreprise SONATRACH de Bejaia fait partie de celles qui utilisent les outils informatiques les plus robustes pour la gestion et la sécurisation de leur réseau d'entreprise. Nous avons pu observer lors de notre stage au sein de cette entreprise le rôle des administrateurs et les ingénieurs spécialisés dans le domaine de l'administration et sécurité des réseaux et les moyens utilisés au fil des années dans cette entreprise. Nous avons constaté que le problème d'administration et sécurité des réseaux ne met pas en question seulement la qualité du service rendue aux utilisateurs mais aussi la réactivité due aux changements et à l'évolution rapide du secteur informatique. Cette gestion des réseaux se définit comme étant l'ensemble des moyens mis en œuvre (connaissances, techniques, méthodes, outils, ...) pour superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes de coût, de qualité et de matériel.

L'objectif de notre travail est de réaliser une application qui va mettre en pratique la mission d'un administrateur réseau dans le but de répondre aux objectifs suivants :

- Superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes de coût, de qualité et de matériel.
- Collecter les outils d'administration des réseaux informatiques.
- Collecter les outils de sécurité des réseaux informatiques.

Le reste de notre travail est organisé comme suit : Dans le premier chapitre, nous présentons des généralités sur les réseaux informatiques et leurs systèmes de sécurité. Puisque le domaine d'étude concerne le réseau et la sécurité informatique, le chapitre sera divisé en deux parties ; dans la première nous allons parler uniquement sur les réseaux informatiques d'une façon théorique et la deuxième sera consacrée pour la sécurité informatique.

Dans le deuxième chapitre qui s'intitule «étude préalable» , nous allons présenter l'organisme d'accueil, la société nationale des hydrocarbures (SONATRACH) généralement et la RTC de Bejaia. Notamment pour arriver à décrire le domaine d'étude qui est traité par le centre informatique, nous allons présenter ce dernier et expliquer ses bases. En dernier lieu nous établirons un cahier des charges qui exprime les spécifications de notre projet. Puisque nous allons travailler sur les outils d'administration des réseaux le troisième chapitre « les outils d'administration des réseaux informatiques », sera consacré pour la collecte des différents outils logiciels de gestion des réseaux informatiques qu'on pourra utiliser sur le terrain professionnel.

Le quatrième chapitre « les outils de sécurité des réseaux informatiques » va traiter les différentes méthodes, logiciel et protocoles utilisés dans une entreprise pour garantir les objectifs de la sécurité.

Le cinquième chapitre concernera « contexte de travail et implémentation » de notre application,

nous présentons les outils utilisés ainsi que des captures pour les différentes interfaces de notre application. En dernier lieu nous terminerons par une conclusion et quelques perspectives.

Chapitre 1

Généralités sur les réseaux informatiques et leurs systèmes de sécurité

1.1 Introduction

De plus en plus que les réseaux se développent en fonction de leurs caractéristiques et besoins, ils deviennent aujourd'hui une infrastructure indispensable dans tous les domaines de la vie, Cependant, les menaces et les attaques sur les réseaux prennent de nouvelles mises à jour représentant les pires ennemis de cette évolution. Pour cela, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises.

Dans ce chapitre nous allons présenter les réseaux informatiques leurs significations , objectifs , classifications ainsi le modéle OSI pour terminer le chapitre avec une presentation générale de la sécurité informatique .Pour l'objectif de bien identifier le domaine dans lequel nous souhaitons travailler.

1.2 Les réseaux informatiques

1.2.1 Que signifie un réseau

Un réseau informatique en général est le résultat de la connexion de deux à plusieurs machines entre elles, afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations. Le terme réseau en fonction de son contexte peut désigner plusieurs choses[1] :

- Il peut désigner l'ensemble des machines, ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés, ce qui est le cas lorsque l'on parle de Internet.
- Le terme réseau peut également être utilisé pour décrire la façon dont les machines d'un site sont interconnectées. C'est le cas lorsque l'on dit que les machines d'un site (sur un réseau local) sont sur un réseau Ethernet, Token Ring, réseau en étoile, réseau en bus,...
- Le terme réseau peut également être utilisé pour spécifier le protocole qui est utilisé pour que les machines communiquent .

1.2.2 Objectifs des réseaux informatiques

Nous appelons réseau un ensemble d'ordinateurs interconnectés entre eux et réalisant des tâches différentes. Ceci étant posé, les objectifs d'un réseau sont classiquement les suivants :

- Partage des ressources : Rendre accessible à chacun les données, les programmes et équipements indépendamment de leur situation physique par rapport à l'utilisateur.
- Augmenter la fiabilité : Permettre des copies d'un même fichier sur plusieurs machines augmente la fiabilité face aux pannes d'une machine.
- Réduction des coûts : Plusieurs petits ordinateurs revient moins cher que de gros serveurs à performance égale.
- Médium de communications : Des personnes éloignées géographiquement peuvent travailler ensemble plus facilement.

1.2.3 Classification des réseaux informatiques selon leur étendu géographique

Nous pouvons classifier les réseaux informatiques de la manière suivante [2] :

PAN (Personale Area Network)

La plus petite étendue de réseau . Deux autres appellations de ce type de réseau sont : réseau individuel et réseau domestique.

LAN (Local Area Network)

De taille supérieure de pan, en français Réseau Local d'Entreprise (RLE), relie entre eux des ordinateurs, des serveurs.

MAN (Metropolitan Area Network)

Le réseau métropolitain ou Metropolitan Area Network (MAN) est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN.

WAN (Wide Area Network)

Les étendues de réseaux les plus conséquentes sont classées en Wide Area Network (WAN). Constitués de réseaux de type LAN, voire MAN, les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau public Internet dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux.

1.2.4 Classification des réseaux informatiques selon leur topologie

Les réseaux informatiques ont une architecture particulière qui présente des caractéristiques et des propriétés , On appelle cela la topologie d'un réseau. Il faut distinguer la topologie physique qui est donc la forme que prend le réseau selon les nœuds et leurs connexions et la topologie logique qui est la manière dont les entités communiquent. Dans le cas des réseaux informatiques, on peut

distinguer entre autres les cas suivants [3] :

Topologie en bus : Tous les nœuds sont connectés en parallèle et chaque message est reçu par tous les nœuds. Le mot bus désigne littéralement la ligne physique qui relie les machines, comme celui montré dans la figure ci-dessous. .

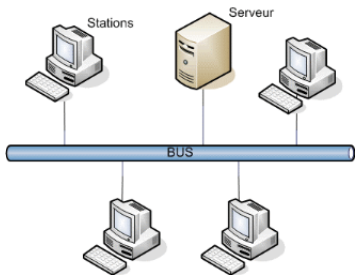

FIGURE 1.1 – Topologie en bus

Topologie en étoile : Est une topologie dans laquelle tous les nœuds sont connectés à un périphérique central, formant ainsi une étoile. Deux types de périphériques fournissant un point de connexion central commun aux nœuds du réseau sont un Hub et un Switch. Toutes les données transférées d'un nœud à un autre passent par le Hub ou le Switch. Les réseaux en étoile sont assez faciles à installer et à entretenir. Les nœuds peuvent être ajoutés et supprimés du réseau avec peu ou pas d'interruption du réseau. Sur réseau en étoile, si un nœud tombe en panne, seul ce nœud est affecté. Les autres nœuds continuent à fonctionner normalement. Pourtant, si le Hub ou le Switch tombe en panne, le réseau entier est inutilisable jusqu'à ce que l'appareil soit réparé continuent à fonctionner normalement (voir la figure ci-dessous).

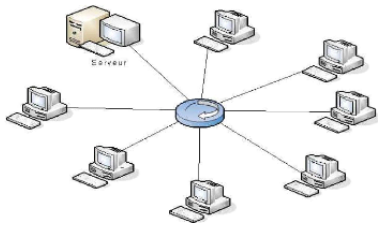

FIGURE 1.2 – Topologie en étoile

Topologie en anneau : Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour. En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole (voir la figure ci-dessous).

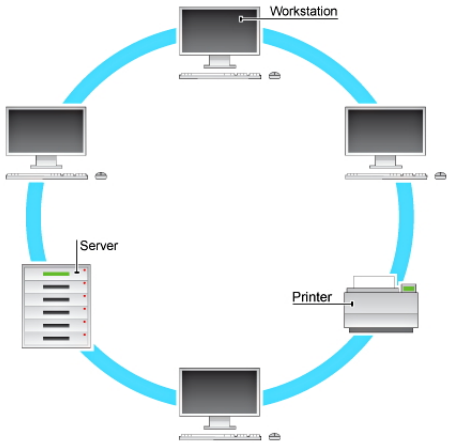

FIGURE 1.3 – Topologie en anneau

1.2.5 Architecture des réseaux

Les réseaux sont structurés du point de vue fonctionnel en deux catégories [4] :

Les réseaux postes à postes (Peer to Peer) : Les réseaux postes à postes ne comportent en général que peu de postes, moins d'une dizaine de postes, parce que chaque utilisateur fait office d'administrateur de sa propre machine, il n'y a pas d'administrateur central, ni de super utilisateur, ni de hiérarchie entre les postes, ni entre les utilisateurs.

Les réseaux Client/serveu : Comportent en général plus de dix postes. La plupart des stations sont des « postes clients », c'est à dire des ordinateurs dont se servent les utilisateurs, les autres stations sont dédiées à une ou plusieurs tâches spécialisées, on dit alors qu'ils sont des serveurs.

1.2.6 Architectures protocolaires

1.2.6.1 modèle OSI (Open System Interconnection) [5]

Est une norme établie par L'International Standard Organisation, afin de permettre aux systèmes ouverts (ordinateur, terminal, réseau, ...) d'échanger des informations avec d'autres équipements hétérogènes. Cette norme est constituée de 7 couches, dont les 4 premières sont dites basses et les 3 supérieures dites hautes. Le principe est simple, la couche la plus basse (directement au dessus du support physique) ne peut communiquer directement avec une couche n+l : chacune des couches est composée d'éléments matériels et/ou logiciels chargés de « transporter » le message à la couche immédiatement supérieure .

- ***La Couche physique***
  Cette couche définit les caractéristiques techniques, électriques, fonctionnelles et procédurales nécessaires à l'activation et à la désactivation des connexions physiques destinées à la transmission de bits entres deux entités de liaisons de données.
- ***La Couche de liaisons de données***

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l'activation et à l'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de données entre les entités du réseau. Cette couche détecte et corrige, quand cela est possible, les erreurs de la couche physique et signale à la couche réseau les erreurs irrécupérables.

- ***La Couche Réseau***
  Cette couche assure toutes les fonctionnalités de relais et d'amélioration de services entre les entités du réseau, c'est à dire : l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche 2 (liaison) pour préparer le travail de la couche .

- ***La Couche Transport***
  Cette couche définit un transfert de données transparent entre les entités en les déchargeant des détails d'éxecution (contrôle entre l'OS et le support de transmission). Son rôle est d'optimiser l'utilisation des services de réseau disponibles afin d'assurer à moindre coût les performances requises par la couche 5 (session).

- ***La Couche Session***
  Cette couche fournit aux entités de la couche présentation les moyens d'organiser et de synchroniser les dialogues et les échanges de données. Il s'agit de la gestion d'accès, de sécurité et d'identification des services.

- ***La Couche présentation***
  Cette couche assure la transparence du format des données à la couche 7 (application).

- ***La Couche Application***
  Cette couche assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tous les services directement utilisables par l'application (transfert de données, allocation de resources, intégrité et cohérence des informations, synchronisation des applications).

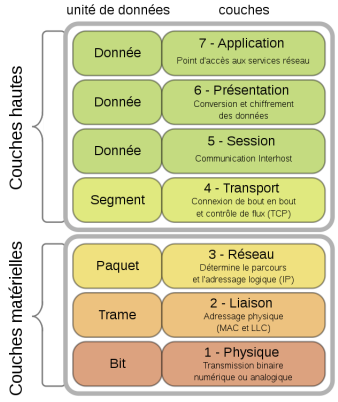

FIGURE 1.4 – les couche du modèle OSI

1.2.6.2 Modèle TCP/IP (Transmission Control Protocol/Internet Protocol)

Le modèle OSI plutôt théorique a été remplacé par un(- modèle plus pratique, le modèle TCP/IP. A la différence du modèle OSI, qui a d'abord été normalisé avant d'être appliqué, le modèle TCP/IP, a tout d'abord été déployé avec succès avant d'être normalisé. TCP/IP ou la « pile TCP/IP » est une suite de protocoles. Le sigle TCP/IP signifie « Transmission Control Protocol/Internet Protocol ». Il provient des noms des deux protocoles majeurs de la suite de protocoles, c'est-à-dire les protocoles TCP et IP [6] .

Architecture en couche du modèle TCP/IP

est une suite de protocoles de communication utilisés pour interconnecter des périphériques réseau sur Internet. Il sp´ecifie comment les données sont échangées sur Internet en fournissant des communications de bout en bout qui identifient comment elles doivent etre divisées en paquets, adressées, transmises, acheminées et reçues à destination .

- ***Couche Accès réseau***
  Cette couche est regroupée les couches physique et liaison de données du modèle OSI. Il assure la bonne gestion du médium (détection de collisions) et permet l'acheminement des informations entre émetteur et destinataire au niveau des adresses MAC.

- ***Couche Internet***
  Ce sont ici des protocoles de haut niveau de la couche réseau. IP permet le routage des informations entre réseaux, c'est ici que l'adresse IP est utilisée. ICMP est un protocole de contrôle il met à disposition des outils de dépistage d'erreur et de signalisation. C'est un protocole important qui mérite que l'on s'y arrête. Nous en reparlerons plus en détail. Ne pas oublier le protocole ARP.

- ***Couche Transport***
  La couche transport permet d'identifier les applications qui communiquent. Pour faciliter la communication on a défini non pas des noms d'applications, mais des ports de communication spécifiques à chaque application. La couche transport gère 2 protocoles de livraison des informations : UDP est dit "sans connexion" et TCP est dit "avec connexion".

- ***Couche application***
  C'est la couche de haut niveau, elle correspond directement avec l'utilisateur, elle englobe les couches OSI d'application, de présentation et de session. Elle s'assure que les données soient correctement "empaquetées" pour qu'elles soient lisibles par la couche suivante.

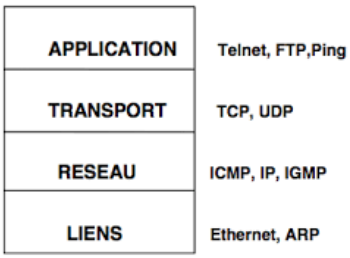

FIGURE 1.5 – les couche du modèle TCP/IP

1.2.7 Protocoles réseaux

Définition d'un protocole

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines), c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau .

Différents types de protocoles [7]

Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (le FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (c'est le cas du protocole ICMP).

Le Protocole TCP (Transmission Control Protocols)
Protocole utilisé sur le réseau Internet pour transmettre des données entre deux machines. Protocole de transport, TCP prend à sa charge l'ouverture et le contrôle de la liaison entre deux ordinateurs.

Protocole UDP (User Datagram Protocol)
Est un protocole permettant l'envoi sans connexion de datagrammes dans des réseaux basés sur le protocole IP. Afin d'atteindre les services souhaités sur les hôtes de destination, le protocole utilise des ports qui constituent un élément essentiel de l'entête UDP.

Le protocole IP
Ce protocole permet de gérer l'acheminement des paquets d'une machine à une autre ainsi que l'adressage. Au plus bas niveau (physique), on dispose alors d'interfaces pour communiquer d'un point à un autre.

Protocole DHCP (Dynamic Host Configuration Protocol)
Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau).

Protocole HTTP (HyperText Transfer Protocol)
Désigne dans le langage informatique un protocole de communication entre un client et un serveur pour le World Wide Web, le protocole http établit une liaison entre un ordinateur (client) et un serveur Web.

Protocole ARP (Adress Resolution Protocol)
Le protocole ARP a un rôle important parmi les protocoles de la couche internet de la suite TCP/IP, car il permet de connaitre l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle protocole de résolution d'adresse. Le protocole ARP interroge les machines du réseau pour connaitre leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses. Physiques dans une mémoire cache. Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance. Si

jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête sur le réseau. Les machines du réseau vont comparer cette adresse logique à la leur, si l'une d'entre s'identifie à cette adresse, la machine va répondre à ARP qui va stocker le couple d'adresse dans la table de correspondance et la communication va pouvoir avoir lieu.

Protocole RARP (Reverse Adress Resolution Protocol)

Le protocole RARP est beaucoup moins utilisé, il signifier protocole ARP inversé, il permet à une station de connaitre son adresse IP à partir d'une adresse table de correspondance entre adresse physique (MAC) et adresse IP hébergée par une passerelle située sur le même réseau.

Protocole ICMP

Le protocole ICMP permet d'envoyer des messages de contrôle ou d'erreur vers d'autre machines ou passerelles. ICMP rapporte les messages d'erreurs à l'émetteur initial. Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dues à des problèmes d'interconnexions rencontrées sur l'Internet : machine destination déconnectée, durée de vie des datagrammes expirée, congestion de datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial. Les messages ICMP sont véhiculés à l'intérieur de datagramme IP et sont routés comme n'importe quel datagramme IP sur l'Internet. Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP.

TFTP (Trivial File Transfer Protocol)

Est un transfert de fichier protocole similaire à Ftp, mais est beaucoup plus limité. Contrairement à FTP, TFTP ne supporte pas l'authentification et ne peut pas changer répertoires ou liste le contenu du répertoire. Par conséquent, il est le plus souvent utilisé pour transférer des fichiers individuels sur un réseau local. TFTP peut également être utilisé pour botte un système informatique à partir d'un réseau connecté périphérique de stockage.

Protocole POP3 (Port Office Protocole version 3)

Occupe le port 110, il est nécessaire pour les personnes n'étant pas connectées en permanence à internet de pouvoir consulter les mails reçus hors connexion.

1.2.8 Equipement d'interconnexion

La mise en place d'un réseau soulève de nombreuses questions sur les contraintes d'utilisation. Comment faire si le réseau à créer dépasse les distances maximales imposées par le type de câble utilisé ? Comment faire parvenir les informations a d'autres réseaux que le sein ? Comment relier des réseaux utilisant des protocoles de communication différents ? Toutes ces questions peuvent être résolus grâce à différents types de matériels qui sont [8] :

Répéteur (repeater)

C'est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Il travaille uniquement au niveau de la couche physique du modèle OSI, c'est-à-dire qu'il ne travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'informations.

FIGURE 1.6 – Le répéteur (repeater)

Concentrateur (Hub)

C'est un élément matériel tout comme le répéteur, opère au niveau de la couche physique du modèle OSI, permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. Il est ainsi une entité possédant un certain nombre de ports (il possède autant de ports qu'il peut connecter de machines entre elles, généralement 4,8 ,16 ou 32). Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports, c'est pour cela il est parfois appelé répéteurs multiports.

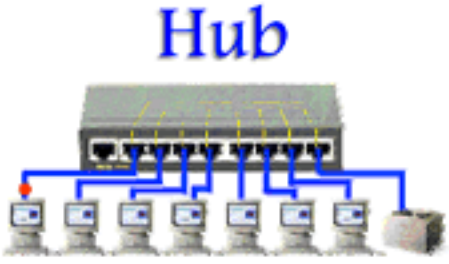

FIGURE 1.7 – Concentrateur (Hub)

Pont (bridge)

Le pont travaille au niveau logique (couche 2) de modèle OSI, c'està-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont. Ainsi le pont permet de segmenter un réseau en concevant au niveau du réseau local les trames destinées à ce dernier, et en transmettant les trames destinées aux autres réseaux. Cela permet de réduire le trafic (collision) sur chacun des réseaux et d'augmenter la confidentialité.

FIGURE 1.8 – Pont (bridge)

Le commutateur (switch)

C'est un pont multiport, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI, il analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (commutation). Le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité.

FIGURE 1.9 – Le commutateur (switch)

Routeur

C'est un pont multiport, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI, il analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (commutation). Le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité.

FIGURE 1.10 – routeur cisco serie 1921

1.2.9 Médias réseaux

Afin que les informations circulent au sein d'un réseau, il est nécessaire de relier les différentes unités de communications à l'aide d'un support de transmission. Celui-ci est un canal physique qui permet de relier des ordinateurs et leurs périphériques sur un réseau [9] .

Les câbles réseau

Les plus utilisés dans les environnements domestiques ou les environnements de bureau. Deux types de câbles existant : les câbles coaxiaux et les câbles Ethernet.

Fibre optique

Les réseaux de fibre optique utilisent des signaux optiques pour conduire l'information, ils sont chargés de transporter les signaux au travers de fibre de verre ou de plastique..

Transmission sans fil

Aucun support filaire n'est utilisé, il s'agit des réseaux sans fil. Des ondes sont utilisées pour transporter l'information.

1.3 Sécurité informatique

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité [10] .

1.3.1 Objectifs de la sécurité

La sécurité informatique vise généralement l'objectif de protéger les informations contre toutes divulgation, altération ou destruction, alors on peut sélectionner trois objectifs principaux de la sécurité d'un réseau [11] :

La Confidentialité

Garantit aux utilisateurs qu'aucune donnée n'a pu être lue et exploitée par un tiers malveillant c'est à dire empêcher la divulgation d'informations à des entités(sites, organisations, personnes, etc.) non habilitées à les connaître.

L'integrité

Garantir que les données sont bien celles que l'on croit être ,et assurer aux utilisateurs que leurs données n'ont pas été indûment modifiées au cours de la transmission dans le réseau ;

La Disponibilité

L'accès aux ressources du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues. Les services et ressources sont accessibles rapidement et régulièrement.

1.3.2 Terminologie de la sécurité informatique

- ***Une ressource*** : tout objet qui a une valeur pour une organisation et qui doit être protégé.
- ***Une vulnérabilité :*** c'est la faiblesse d'un système qui pourrait être exploitée par une menace.
- ***Une menace*** : est un danger potentiel pour une ressource ou pour le fonctionnement du réseau.
- ***Une attaque*** : c'est une action prise pour nuire à une ressource
- ***Un risque*** : c'est la possibilité de perte, altération, destruction ou autres conséquences négatives de la ressource d 'une organisation. Le risque peut naitre d'une seule ou de plusieurs menaces ou de l'exploitation d'une vulnérabilité : Un risque =une ressource + une menace + une vulnérabilité
- ***Une contremesure :*** une protection qui atténue une menace potentielle ou un risque.

1.3.3 Typologie des menaces

Les différentes catégories de menaces qui pèsent sur le système d'information ou sur un réseau peuvent être classées comme illustré à la figure 1.11 Les menaces non intentionnelles ou imprévisibles, comme les catastrophes naturelles, ne mettent pas en œuvre d'outils ou de techniques particulières et n'ont évidemment pas d'objectif déterminé. À l'inverse, les menaces intentionnelles

mettent généralement en œuvre des outils et des techniques d'attaque très variés. Des études ont montré que, dans les trois quarts des cas, les menaces réelles de sécurité viennent de l'intérieur de l'entreprise. Face aux menaces identifiées lors de la première étape, des stratégies de sécurité proactives ou réactives doivent être définies pour tous les cas [12] .

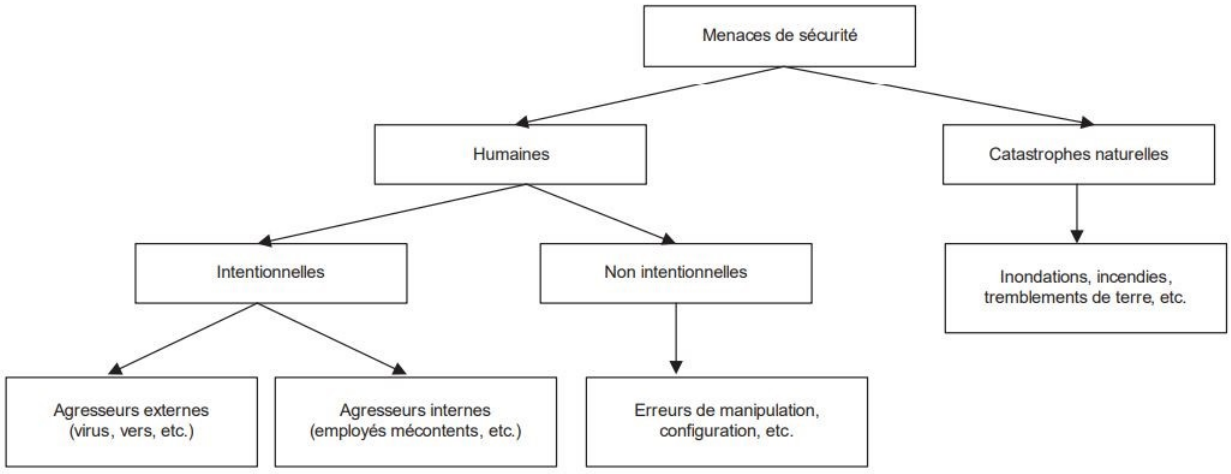

FIGURE 1.11 – typologie des menaces

1.3.4 Codes malveillants

L'Internet et les réseaux informatiques ont longtemps été infesté par du code malveillant et ses effets néfastes.

1.3.4.1 Définition

Un code malveillant est un code informatique ou script Web dangereux qui crée des vulnérabilités pouvant entraîner des backdoors, violations de la sécurité, vols d'informations et de données ainsi que d'autres dommages potentiels sur des fichiers et systèmes informatiques Les types des codes malveillants (malware) qui peuvent être utilisés par les pirates sont les suivants [13] :

Les vers

Les vers ciblent les vulnérabilités des systèmes d'exploitation pour s'installer dans les réseaux. Plus faciles à programmer qu'un virus, ils utilisent internet sous toutes ses formes pour se propager via des emails, des sites web ou des serveurs FTP. Une fois en place, les vers peuvent être utilisés par les cybercriminels pour lancer des attaques DDoS, voler des données sensibles ou mener des attaques de ransomware [14] .

Worms

ce sont des programmes autonomes qui exploitent des vulnérabilités connues dans le but de ralentir un réseau. Ils ne nécessitent pas l'activation de l'utilisateur, ils se dupliquent et tentent d'infecter d'autres hôtes dans le réseau .

Spyware

ce sont des logiciels espions qui sont généralement utilisés dans le but d'influencer l'utilisateur pour acheter certains produits ou services. Les spywares, en général, ne se propagent pas automatiquement, mais ils s'installent sans autorisation. Ils sont programmés pour :

- recueillir des informations personnelles sur les utilisateurs .
- surveiller l'activité de navigation sur le Web pour détecter les caprices de l'utilisateur .
- la redirection des requêtes HTTP vers des sites de publicité préétablis .

Adware

réfère à tout logiciel qui affiche des publicités, sans l'autorisation de l'utilisateur, parfois sous la forme de fenêtres pop-up.

scaryware

réfère à une classe de logiciels utilisés pour convaincre les utilisateurs ayant leurs systèmes infectés par des virus, et leur proposer une solution dans le but de vendre des logiciels .

trojan horse (cheval de troie)

c'est un programme ayant deux caractéristiques :

- un comportement apparemment utile à l'utilisateur .
- un comportement caché, malveillant conduisant, généralement, à un accès à la machine sur laquelle il est exécuté .

ransomwares

est un programme conçu pour bloquer l'accès à un système informatique, par le chiffrement de contenu, jusqu'à ce qu'une somme d'argent soit payée.

1.3.5 Types de sécurité

on peut citer plusieurs catégories de la sécurité réseau tel que :

La sécurité physique

La sécurité physique concerne tous les aspects liés à l'environnement dans lequel les Ressources sont installées. Elle peut inclure :

- La sécurité physique des salles de serveurs, des périphériques réseau, etc.
- La prévention des accidents et des incendies .
- Les systèmes de l'alimentation ininterrompue .
- La Surveillance vidéo, etc.

La sécurité logique

La sécurité logique fait référence à la mise en œuvre d'un système de contrôle d'accès, par logiciel, pour sécuriser les ressources. Elle peut inclure :

- L'application d'une stratégie de sécurité fiable pour les mots de passe .
- L'instauration d'un modèle d'accès s'appuyant sur l'authentification, l'autorisation et la traçabilité, la configuration correcte des pare-feux de réseau .
- L'installation des IPS (systèmes de prévention d'intrusion) .
- L'utilisation des VPN (réseau privé virtuel), etc.

1.3.6 Politique de la sécurité

Une politique de sécurité informatique est une stratégie visant à maximiser la sécurité informatique d'une entreprise. Elle est matérialisée dans un document qui reprend l'ensemble des enjeux, objectifs, analyses, actions et procédures faisant parti de cette stratégie.

- À distinguer de la charte informatique, qui est un document de recommandations concernant la bonne utilisation des technologies informatiques, et qui est destiné aux employés de l'entreprise
- Ce document est unique et personnalisé, car établi en tenant compte du fonctionnement, de l'environnement, de la composition du système d'information de l'entreprise et des enjeux et des risques informatiques qui lui sont propres

1.3.7 Mise en place d'une politique de la sécurité informatique

Les meilleures pratiques à observer lors de l'élaboration de la politique de sécurité informatique :

- Désigner un responsable informatique, qui sera en charge de l'élaboration et de la mise en place de cette politique de sécurité.
- Définir le périmètre et les objectifs de la politique de sécurité informatique, à des fins d'efficience et de mesure des résultats.
- Effectuer une analyse de l'existant, matériel et logiciel, et tenir à jour un registre de l'ensemble des éléments qui composent le système d'information. Ce registre est important lors des modifications des composants de la configuration informatique. En cas d'incident, il peut permettre aux équipes IT de trouver l'origine du problème.
- Effectuer une analyse des risques informatiques, au regard du préjudice possible et de la probabilité d'occurrence de l'incident.
- Déterminer les moyens nécessaires pour la réduction des risques et la prise en charge des incidents, qu'il s'agisse de moyens matériels ou humains.

- Définir les procédures adaptées, notamment en matière de gestion des incidents, ou de gestion de la continuité d'activité.

- Rédiger une charte informatique, à l'attention des collaborateurs.

- Communiquer sur la politique de sécurité informatique auprès de l'ensemble de l'entreprise.

1.4 Conclusion

Dans ce chapitre nous avons présenté les réseaux et la sécurité informatique d'une façon générale, nous avons cité les critères basiques qui montrent le rôle d'un réseau informatique et la nécessité de le sécurisé, pour l'objectif de bien définir le concept d'administration et la sécurité d'un réseau au sein d'une entreprise. Le chapitre suivant sera consacré pour la présentation de l'organisme d'accueil et l'étude approfondie des notions de l'administration et sécurité d'un réseau d'entreprise.

Chapitre 2

Etude Préalable

2.1 Introduction

Afin de comprendre le cœur de travail du centre informatique et son role d'administartion et sécurisation de réseaux informatiques , Une présentation globale de l'organisme d'accueil SONATRACH, notamment la RTC de Bejaia et le centre informatique indispensable, pour donner une approche sur le domaine et le milieu ou nous souhaitons travailler. Ce chapitre sera consacré à l'étude globale de l'existant.

2.2 Présentation de l'Organisme d'Accueil

2.2.1 Historique de la SONATRACH

SONATRACH est l'acronyme de « Société Nationale de Transport et Commercialisation des Hydrocarbures », est une entreprise publique algérienne qui a été créé le 31/12/1963 par le décret N° 63/491. Ses activités principales étaient le transport et la commercialisation des hydrocarbures.

SONATRACH est créée pour objectif principal le transport et la commercialisation des hydrocarbures et se déployer progressivement dans les autres segments de l'activité pétrolière.

Le 24/02 /1971, arriva la nationalisation du secteur des hydrocarbures, qui a conduit à une restructuration et une réorganisation efficace de la société qui a donné naissance à 18 entreprise parmi elles : NAFTAL, ENIP, ENGTP, ENAC, ASMIDAL,... etc.

En 1986, la SONATRACH adopta une politique plus ouverte aux relations d'association avec des partenaires étrangers, et affiche l'ambition de devenir un groupe pétrolier de dimension internationale.

C'est un acteur majeur de l'industrie pétrollière surnommé la major africaine.SONATRACH est classée la première entreprise d'afrique.

2.2.2 Objectifs et missions de l'entreprise

Pour atteindre ses objectifs et consolider sa position sur le marché international en recentrant sur ses activités de base, on cite quelque objectifs et missions :

- Le doublement du rythme de la production.
- Le développement des activités en international.
- Le renforcement de ses capacités technologiques.

- La commercialisation des hydrocarbures.
- La transformation du gaz.

2.2.3 Organigramme de SONATRACH

La figure 1 présente un organigramme global de l'entreprise nationale SONATRACH avec ces différentes branches sur le terrain national.

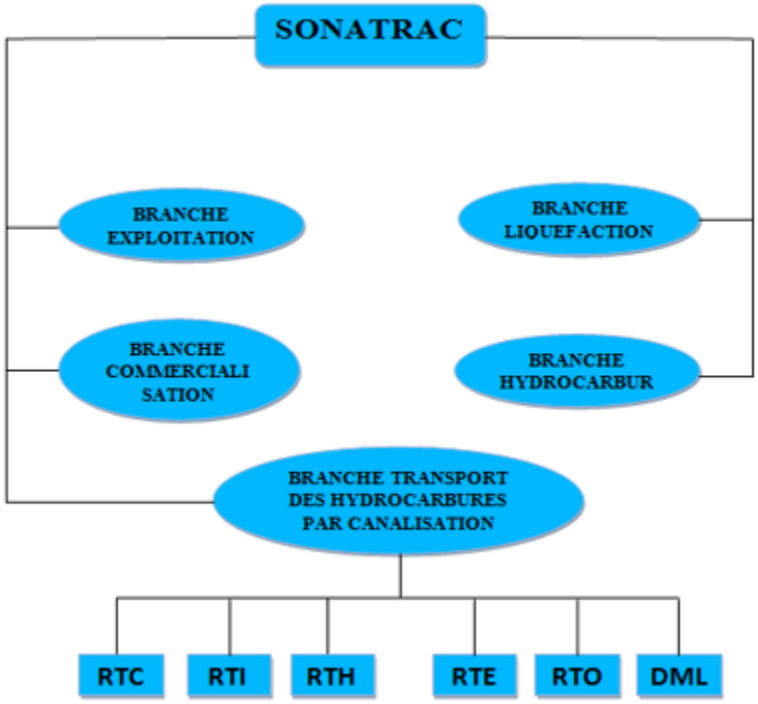

FIGURE 2.1 – Direction Régionale Transport Centre(RTC)

2.3 Direction Régionale Transport Centre(RTC)

La Direction Régionale Transport Centre(RTC) est l'une des cinq régions couvrant l'activité de la branche transport par canalisations.

La RTC est composée de plusieurs sous directions : technique, administration et finances, exploitation oléoducs /Gazoducs, Exploitation des installations portuaires et bouées de chargement.

2.3.1 Sous-direction technique

Elle est composée de sept départements

- Département Maintenance : Sa mission est d'assurer la maintenance des équipements industriels de l'entreprise (pompes, groupes électrogènes, etc.. . .).
- Département entretien lignes et bacs de stockage.
- Département méthodes.
- Département Protection des cathodique.

- Département passation des marchés
- Département Approvisionnement et transport : Ce département alimente la RTC en matériel nécessaire à son fonctionnement et assure aussi le transport du personnel de l'entreprise.
- Département Travaux Neufs : Il est chargé de l'étude et du suivi des projets d'investissement de la RTC dans les différents domaines.

2.3.2 Sous-direction administration et finances

Elle est composée de cinq départements :

- Département Ressources Humaines : Il a pour rôle la recherche et l'acquisition du potentiel humain, sa présentation et son développement qualitatif.
- Département Administratif et Social : Ce département veille au respect des lois en vigueur régissant les relations de travail et gère le personnel de la RTC.
- Département Moyens Généraux : Ce département fournit le soutien logistique à l'entreprise.
- Département Finances .
- Département budget et contrôle de Gestion

.

2.3.3 Sous-direction exploitation des installations portuaires et bouées déchargement

Elle est composée de deux départements qui sont chargées de l'exploitation ouvrages (Gazoduc et Oléoducs) :

- Département Exploitation et installation portuaires et bouées de chargement
- Département Entretient Installations

2.3.4 Sous-direction exploitation Oléoducs gazoducs

Elle est composée de deux départements :

- Département Exploitation Oléoducs
- Département exploitation gazoducs

2.3.5 Autres structures

On trouve :

- Secrétaire
- Département HSE : Cette structure doit assurer la protection du patrimoine humain et matériel de la RTC et le bon acheminement des hydrocarbures.
- Centre Informatique : Il représente le support d'exploitation et de développement des applications informatiques pour le compte de la RTC et des autres directions régionales.
- Département juridique.
- Sureté interne d'établissement.

2.3.6 Organigramme de la RTC

Notre travail concerne le centre informatique, dont l'organigramme est présenté par la figure 2 :

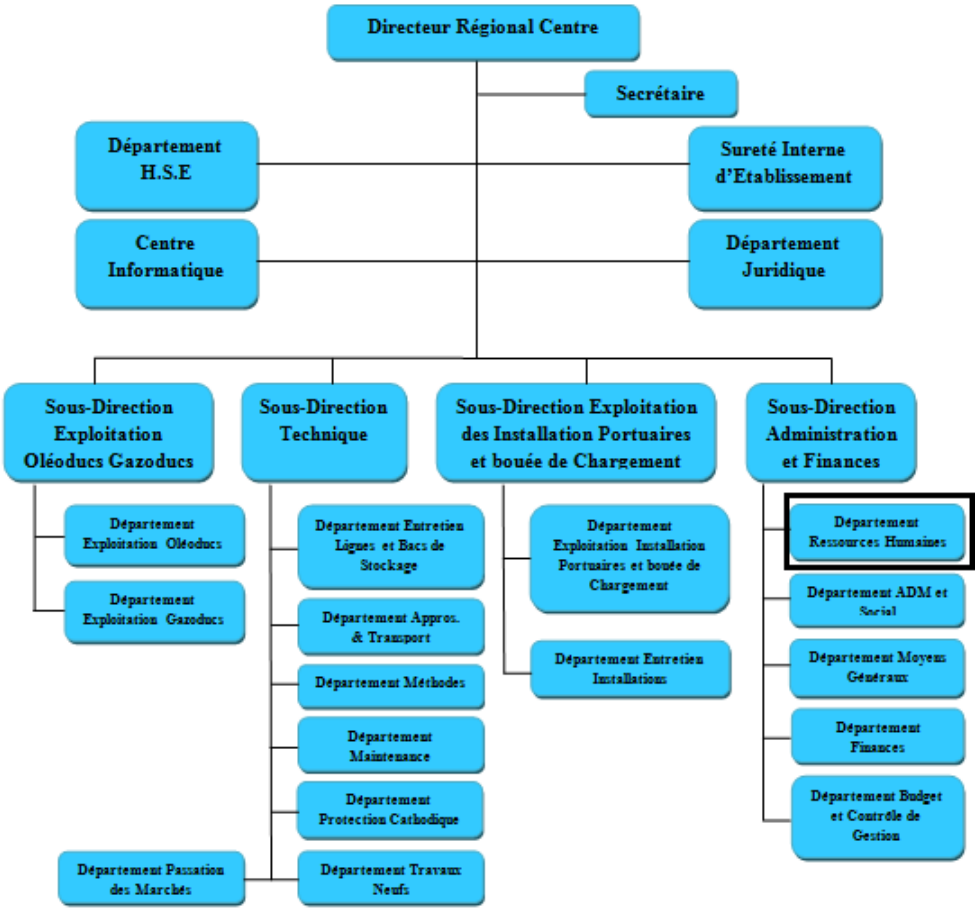

FIGURE 2.2 – Organigramme de la RTC

2.4 Description du domaine d'étude

2.4.1 Présentation du centre informatique

Le centre informatique sert a regrouper les moyens d'exploitation et de développement des applications informatiques pour les différents structures de RTC il gère le réseau informatique interne. Il constitue de trois services :(service système et réseau, service base de donnée et logiciel et service support technique) géré par un chef de centre .

2.4.2 Organigramme du centre informatique

Les services informatiques sont illustrés dans la figure suivante :

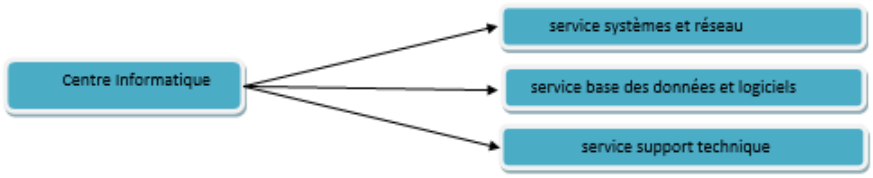

FIGURE 2.3 – Les services du centre informatique de RTC

2.4.3 Définition du chaque service

2.4.3.1 Service systèmes et réseau

Ce service est dirigé par un chef (ingénieur système (SIQ)), un ingénieur système distribué (SPD) et un ingénieur d'informatique industriel (SIQ), qui assure le bon fonctionnement, la fiabilité des communications, l'administration du réseau, organise l'évolution de sa structure, et la surveillance permanente pour détecter et prévenir les pannes. Il oriente des travaux de l'équipe de développement pour une bonne utilisation des ressources matérielles et logicielles et il sert à définir les droits d'accès pour l'utilisation du réseau.

2.4.3.2 Service de base de données et logiciels

Ce service est dirigé par un chef (ingénieur SI) et quatre ingénieurs systèmes d'information .il mit en œuvre l'étude et la conception des systèmes d'information et assure l'optimisation et le suivi de la gestion de cohérence et la qualité des données numériques introduites par les utilisateurs . il sert à installer , configurer et exploiter le SGBD et ses bases de données qui gèrent la sauvegarde ,la restauration et migration des données .

2.4.3.3 Service de support technique

Ce service est dirigé par un chef de support technique (ingénieur SI) .Il sert à installer les logiciels de gestion, technique et bureautiques et il sert aussi à assister les utilisateurs en cas des problèmes matériels ou logiciels .

2.4.4 Présentation du réseau RTC

Le réseau informatique de la RTC de Bejaia est constitué de deux bâtiments, l'ancien bâtiment qui dispose de topologie physique en étoile étendue et le nouveau bâtiment dont la topologie physique est hybride (en étoile et en annaux). Le type de lien entre ces deux derniers est la fibre optique.

2.5 Cahier des charges

Un cahier des charges est un document qui doit être respecté lors de la réalisation d'un projet, cet outil est indispensable pour définir les spécifications d'un projet.

2.5.1 Présentation du sujet

Le projet que nous présentons dans ce mémoire traite le thème de « les outils d'administration et sécurité des réseaux informatiques » qui consiste à réaliser une application pour présenter l'évolution des méthodes d'administration et de supervision des réseaux informatiques.

2.5.2 Problématique

Le plus grand souci d'un administrateur n'est pas seulement la qualité de service rendu aux utilisateurs, Mais la réactivité due aux changements et à l'évolution rapide du secteur informatique aussi l'efficacité des moyens mis en œuvre (connaissances, technique, méthodes outils...) pour administrer , superviser, surveiller son réseau d'entreprise et également planifier son évolution en respectant les contraintes de coût, de qualité et de matériel.

2.5.3 Objectifs de notre travail

Objectifs visé par ce travail sont :

- Superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes de coût, de qualité et de matériel.
- Mettre en œuvre nos connaissances théoriques au sein d'une entreprise.
- Collecter les outils d'administration des réseaux informatiques
- Collecter les outils de la sécurité des réseaux informatiques.

2.6 Conclusion

Sachant que Sonatrach est une grande entreprise et ses activités sont multiples elle dispose de plusieurs types de matériaux réseaux elle utilise de nouvelle technologie d'administration et de sécurité de leurs réseaux . Au cours de notre stage dans cette dernière nous avons essayé de collecter un maximum d'outils utilisés sur le terrain profesionnel dans le domaine de notre étude qu'on présentera dans les chapitres qui Suits, ou nous allons présenter les outils les plus utilisés dans le milieu professionnel pour Administrer et sécuriser un réseau d'entreprise.

Chapitre 3

Outils d'administration des réseaux informatiques

3.1 Introduction

En raison de la complexité des infrastructures réseau modernes et de la complexité des composants qu'elles contiennent, l'administration réseau n'est faisable qu'avec l'aide d'outils appropriés. Parmi ceux-ci il y a d'abord les commandes et utilitaires fournis par les systèmes d'exploitation. Dans ce chapitre nous allons définir le domaine de l'administration réseau et présenter les outils utilisés dans l'entreprise pour gérer leur réseau informatique.

3.2 Administration réseau

L'administration d'un réseau est une discipline informatique qui sert à gérer les comptes et les machines d'une entreprise ça peut concerner notamment les concentrateurs, commutateurs, routeurs, modems, pare-feu, proxy, connectivité Internet, les réseaux privés virtuels (VPN) .

3.2.1 Objectifs d'administration des réseaux

On peut citer plusieurs Objectifs pour mettre en place l'administration des réseaux dans les entreprises [15] [16] :

- La supervision et la surveillance des systèmes.
- Visualisation de l'architecture du système.
- permission l'évolution du système en incluant de nouvelles fonctionnalités.
- Optimisation pour l'utilisation des ressources.
- Détection et prévision des erreurs.
- Signalisation des pannes.
- Calculs de facturations à l'utilisation des ressources
- Le support technique pour utilisateurs

3.3 Un administrateur réseau

L'Administrateur Réseau est une personne chargée de la gestion du réseau et les machines du réseau de son entreprise. Il gère les gestions à distance,le bon fonctionnement,garante la qualité du service du réseau informatique et participe dans la mise en place de son architecture et ça sécurité.

3.3.1 Rôles d'un administrateur des réseaux informatiques :

L'administrateur réseau est responsable de ce qui peut se passer dans un réseau administré ; ainsi les rôles d'un administrateur réseau consiste à [16] :

- Mettre en place et maintenir l'infrastructure du réseau (organisation, ...) .
- Installer et maintenir les services nécessaires au fonctionnement du réseau .
- Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures) .
- S'assurer que les utilisateurs n'outrepassent pas leurs droits .
- Gérer les « logins » (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...) .
- Gérer les systèmes de fichiers partagés et les maintenir.

3.4 Outils d'administration d'un réseau informatique

En fonction des besoins et les tâches demandées, les administrateurs réseau utilisent plusieurs moyens pour assurer une bonne gestion de leur réseau d'entreprise tel que :

Port Console

Il s'agit d'un port de gestion permettant un accès hors réseau à un périphérique Cisco. L'accès hors bande désigne l'accès via un canal de gestion dédié qui est utilisé uniquement pour la maintenance des périphériques. L'avantage d'utiliser un port de console est que le périphérique est accessible même si aucun service réseau n'a été configuré, par exemple en effectuant la configuration initiale du périphérique réseau. Un ordinateur exécutant un logiciel d'émulation de terminal et un câble de console spécial pour se connecter à l'appareil sont nécessaires pour une connexion à la console [17] .

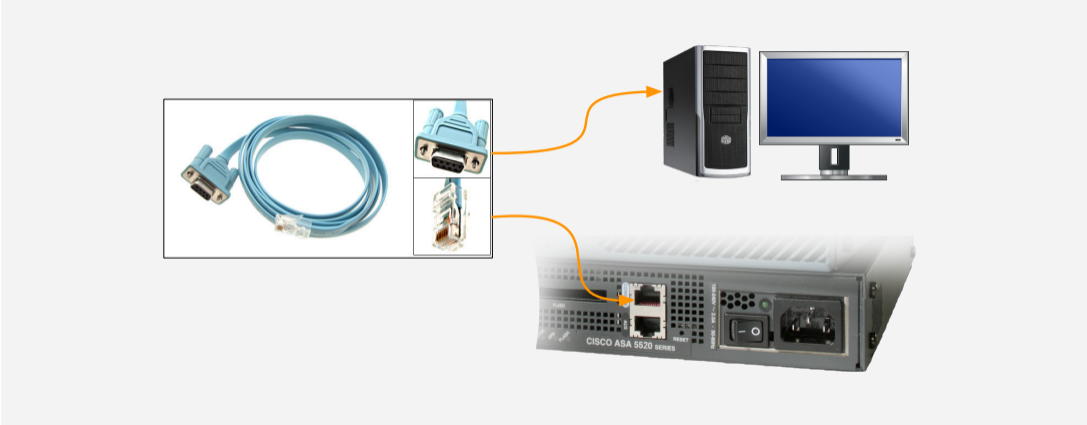

FIGURE 3.1 – Le cable console

Interfaces CLI(Command Line Interface)

Le mode d'administration le plus basique, mais parfois le plus efficace pour un équipement réseau se présente via une interface minimaliste permettant d'entrer des lignes de commandes, on parle de CLI (Command Line Interface). Ces commandes CLI dépendent de l'équipement en question et du constructeur. Chaque constructeur défini et implémente ses propres commandes ; rappelons en effet que la majorité des systèmes d'exploitation des éléments actifs d'un réseau sont propriétaires [18] .

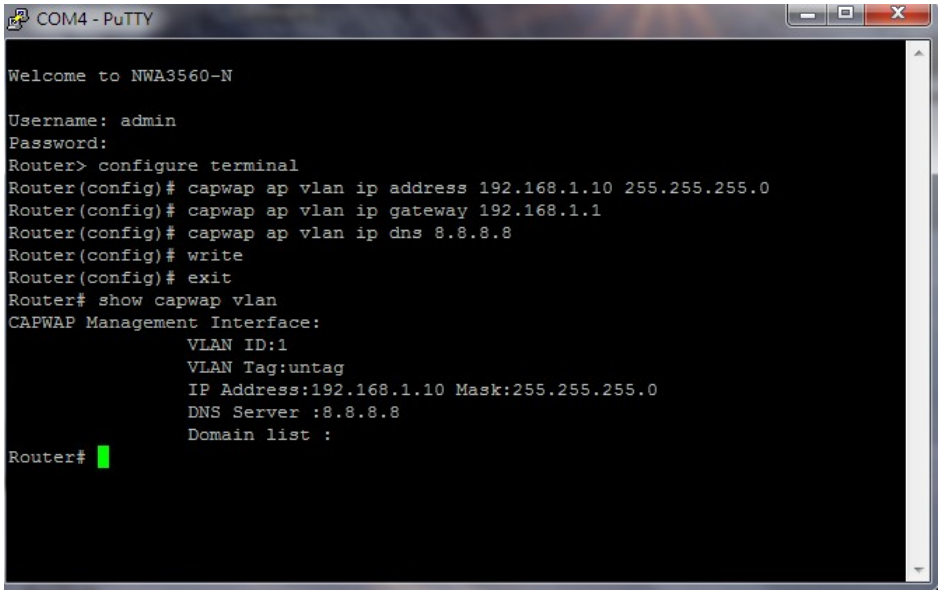

FIGURE 3.2 – L'interface en ligne de commande CLI

Interfaces GUI(Graphical User Interface)

La GUI, pour Graphical User Interface, désigne en français une interface graphique. Il s'agit de la manière selon laquelle un logiciel est présenté à un utilisateur sur un écran. Pour faire simple, l'interface graphique, ou GUI, se résume à l'affichage des commandes permettant d'effectuer des

actions dans un logiciel, comme des menus, des boutons, des fonctionnalités, etc., sans avoir à saisir des lignes de commandes. Apparues dans les années 1970 et développées dans les années 1990, les interfaces graphiques ont en effet progressivement remplacé les interfaces en lignes de commandes que l'on retrouvait par exemple sur le Macintosh d'Apple dans les années 1980. Lorsqu'une GUI est bien conçue et ergonomique, elle devient intuitive pour l'utilisateur, qui parvient alors à utiliser un logiciel, un système d'exploitation, etc., en toute simplicité [19] .

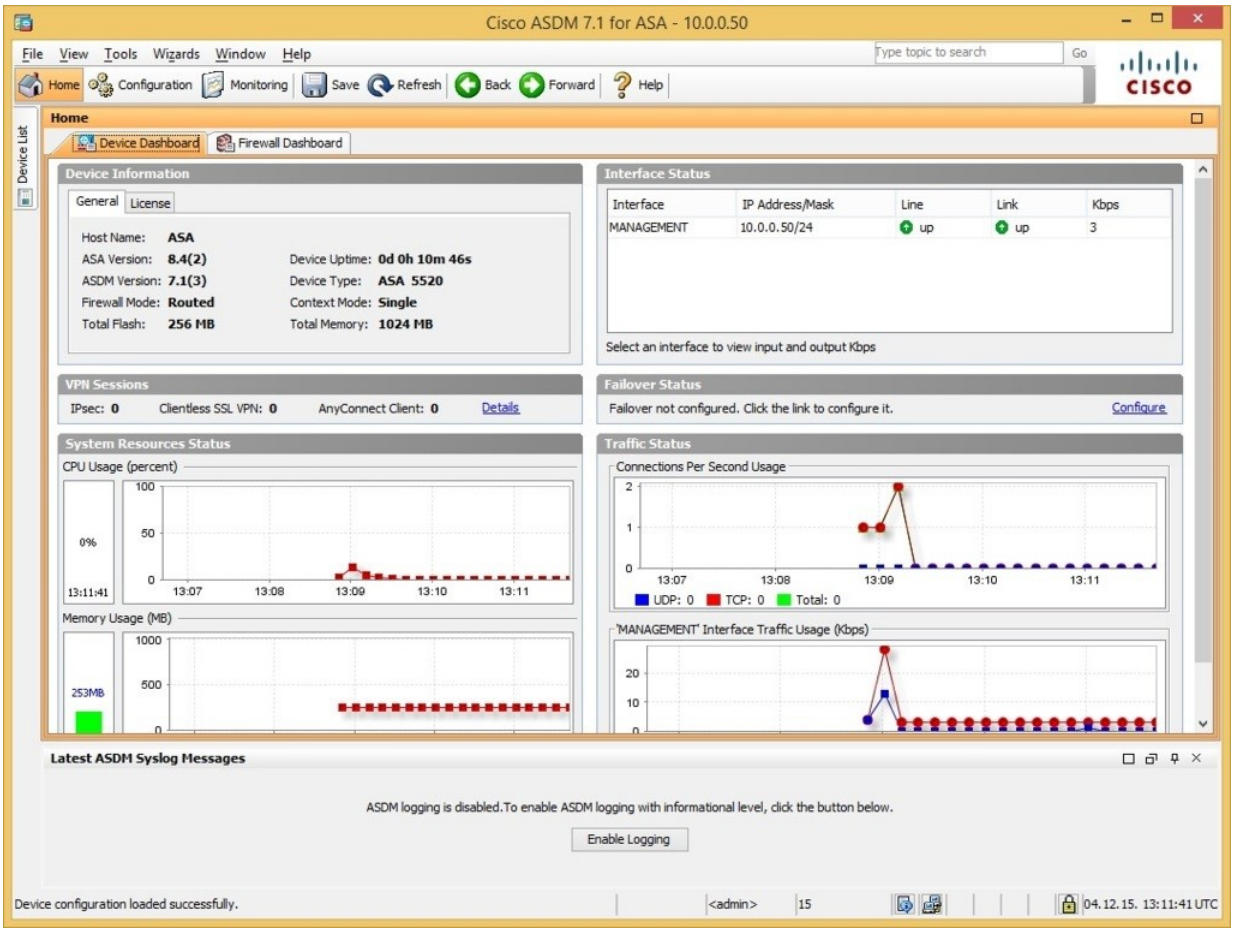

FIGURE 3.3 – Interface GUI

Interface Web
La gestion réseau par une interface Web s'est développée durant ces dernières années, car celle-ci fournit une interface plus intuitive et plus agréable à utiliser que l'interface Telnet. Toutefois, à l'instar de Telnet, l'interface reste propre à chaque matériel réseau et ne permet aucune homogénéisation de la gestion. De plus, la gestion peut vite s'avérer fastidieuse s'il y a un grand nombre de nœuds au sein de notre réseau et qu'il soit nécessaire d'appliquer plusieurs modifications. Enfin, les serveurs Web consomment souvent un important nombre de ressources sur le matériel, apportant un risque de baisse de performances.

3.4.1 Protocoles d'administration

SNMP (Simple Network Management Protocol)
Abrégé SNMP, en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance. Le noyau de SNMP est un ensemble simple d'opérations qui donne aux administrateurs la possibilité de changer l'état de certains SNMP Appareil basé. Par exemple, vous pouvez utiliser SNMP pour fermer une interface sur votre routeur ou vérifiez la vitesse à laquelle votre interface Ethernet fonctionne. SNMP peut surveiller même la température de votre interrupteur et vous avertir lorsqu'elle est trop élevée. SNMP est généralement associé à la gestion des routeurs, mais il est important de comprendre qu'il peut être utilisé pour gérer de nombreux types d'appareils. Alors que le prédécesseur de SNMP, le Simple Gateway Management Protocol (SGMP), a été développé pour gérer Internet routeurs, SNMP peut être utilisé pour gérer les systèmes Unix, les systèmes Windows, les imprimantes et Tout appareil exécutant un logiciel qui permet la récupération des informations SNMP peut être gérée. Cela inclut non seulement le physique périphériques mais aussi des logiciels, tels que des serveurs Web et des bases de données.

Telnet
Est un moyen non sécurisé d'établir une session CLI à distance via une interface virtuelle sur un réseau. Contrairement à SSH, Telnet ne fournit pas de connexion sécurisée et cryptée et ne doit être utilisé que dans un environnement de travaux pratiques. Les informations d'authentification des utilisateurs,
les mots de passe et les commandes sont envoyés sur le réseau en clair. La meilleure pratique consiste à utiliser SSH au lieu de Telnet. Cisco IOS inclut à la fois un serveur Telnet et un client Telnet [17] .

SSH (Secure Shell) Est un moyen d'établir à distance une connexion CLI sécurisée via une interface virtuelle sur un réseau. À la différence des connexions de console, les connexions SSH requièrent des services réseau actifs sur le périphérique, notamment une interface active possédant une adresse. La plu Partie des versions de Cisco IOS incluent un serveur SSH et un client SSH qui peuvent être utilisés pour établir des sessions SSH avec d'autres périphériques.

3.5 Conclusion

Dans ce chapitre nous avons présenté les outils d'administration des réseaux informatiques que nous avons constaté au sein de l'entreprise ,Dans ce qui suit nous allons présenter également leurs méthodes et outils de sécurité réseau pour l'objectif de simuler et montrer les déférents outils dans une architecture de notre travail.

Chapitre 4

Outils de la sécurité des réseaux informatiques

Pour protéger les données sensibles d'une entreprise, il est indispensable d'installer une solution de sécurité informatique qui permet de s'assurer que les ressources matérielles et logicielles sont uniquement utilisées dans le cadre prévu, nous allons présenter dans ce chapitre les différents outils utilisés dans les entreprises pour mettre en place la sécurité de leurs infrastructures.

4.1 Définition

La sécurité d'un réseau informatique d'une entreprise c'est mettre en action plusieurs taches dont : planifier, concevoir, optimiser, mettre en œuvre, auditer, superviser et dépanner le système de sécurité réseau pour améliorer l'efficacité de l'organisation

4.2 Ouitils de la sécurité

Pour sécurisé l'infrastructure réseau d'une entreprise nous avons besoins de plusieurs systèmes , logiciels et matériels dont on présente dans ce qui suit :

4.2.1 VLAN (Virtual Local Area Network)

En français Réseau Local Virtuel est un réseau local regroupant un ensemble de machines de façon logique et non physique [20] .

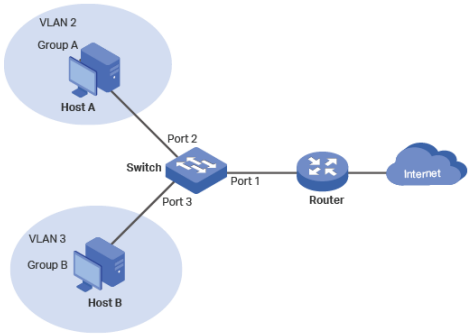

FIGURE 4.1 – Le fonctionnement de VLAN

4.2.2 VPN (Virtual Private Network)

Un réseau privé virtuel est une connexion sécurisée et chiffrée entre deux réseaux ou entre un utilisateur individuel et un réseau. Ils permettent de masquer l'identité en ligne, Le trafic internet passe à travers un tunnel chiffré à l'intérieur duquel personne ne peut voir, que ce soient les hackers, les gouvernements ou votre fournisseur d'accès internet.

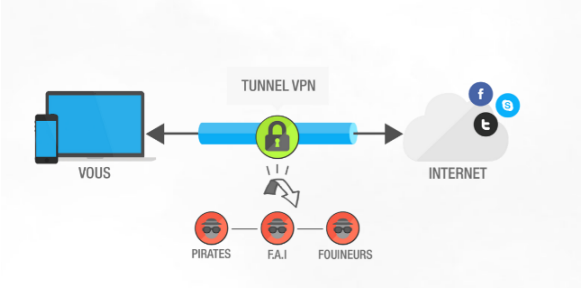

FIGURE 4.2 – Le fonctionnement de VPN

4.2.3 IDS (Intrusion détection System)

Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblent suspectes. Plus communément appelé IDS , les systèmes de détection d'intrusions conviennent parfaitement pour réaliser cette tâche [21].

4.2.4 IPS (intrusion prevention system)

l'IPS est un outil de protection et sécurité des systèmes d'information contre les intrusions, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque. C'est un IDS actif, il empêche toute activité suspecte détectée au sein d'un système [22] .

4.2.5 NAT (Network Address Translation)

Dans les entreprises de grandes tailles, différents réseaux interconnectés peuvent utiliser les mêmes adresses IP. Pour que la communication soit possible entre nœuds des deux coté, il est nécessaire de modifier les références de l'émetteur de paquets afin qu'il n'y ait pas de conflits et que la transmission soit fiable. Des équipements de translation d'adresse NAT (Network Address Translation) sont chargés d'adopter cette fonctionnalité. Ils permettent le changement d'une adresse IP par une autre. Trois types d'adresse sont possibles :

- Gérer les systèmes de fichiers partagés et les maintenir.
- La conversion dynamique d'adresses (NAT dynamique) change à la volée d'adresse IP par rapport à une externe disponible dans une liste.
- La conversion statique d'adresse (NAT statique), effectue également un changement d'adresse IP, mais une table est maintenue, permettant à une adresse IP interne de toujours être remplacée par la même adresse IP externe [23] .

4.2.6 ACL (Access Control List)

Une ACL est une liste de règles permettant de filtrer ou d'autoriser du trafic sur un réseau en fonction de certains critères (IP source, IP destination, port source, port destination, protocole, ...). · Une ACL permet de soit autoriser du trafic (permit) ou de le bloquer (deny). Il est possible d'appliquer au maximum une ACL par interface et par sens (input/output). · Une ACL est analysée par l'IOS de manière séquentielle. · Dès qu'une règle correspond au trafic, l'action définie est appliquée, le reste de l'ACL n'est pas analysé. · Toute ACL par défaut bloque tout trafic. Donc tout trafic ne correspondant à aucune règle d'une ACL est rejeté. Remarque : Les ACLs servent également à identifier un trafic afin d'être traité par un processus, dans ce cas le trafic correspondant à un « permit » est traité, et celui correspondant à un « deny » est ignoré [24].

4.2.7 Proxy

Un serveur proxy (traduction française de «proxy server», appelé aussi «serveur mandataire») est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...)[25].

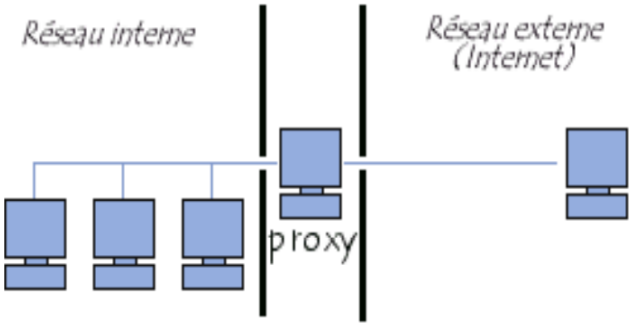

FIGURE 4.3 – Architacture de proxy

4.2.8 Par-feux

Un pare-feu est un système logiciel ou matériel placé entre un réseau fiable et un autre non fiable. L'objectif principal de son implémentation est de filtrer et d'empêcher le trafic indésirable de traverser la limite du pare-feu. Pour ce faire, un pare-feu doit assurer les recommandations suivantes [11] :

- être résistant aux attaques .
- être le seul point de transit entre deux réseaux ,
- assurer l'application de la stratégie de contrôle d'accès de I 'organisation

4.2.8.1 Types des parfeux

Il existe différents types de pare-feux, dont nous pouvons citer, parmi d'autres, les suivants :

- **pare-feu NAT :** permet de cacher une adresse IP privée en la traduisant par une adresse IP publique .

- **pare-feu de filtrage de paquets :** permet de cacher une adresse IP privée en la traduisant par une adresse IP publique .
- **pare-feu de filtrage de paquets :** Permet de cacher une adresse IP privée en la traduisant par une adresse IP publique .
- **pare-feu de filtrage de paquet avec état :** Assure la même fonction que les pare-feux de filtrage de paquets, mais conserve également le suivi de l'état des connexions réseau (c'est-à-dire les numéros de séquence TCP et UDP), ce qui le rend plus sécurisé .
- **pare-feu applicatif (pare-feu proxy) :** C'est généralement, un serveur qui assure ce type de filtrage des informations situées aux couches 3, 4, 5 et 7. .

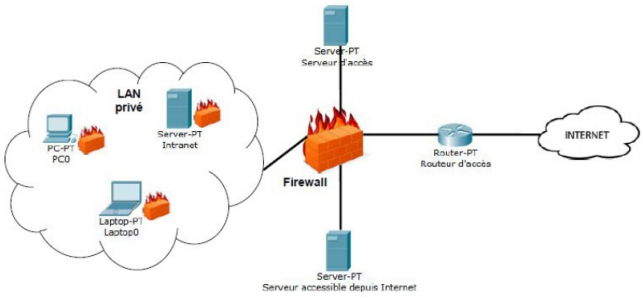

FIGURE 4.4 – Le pare-feu

4.2.9 Protocoles de sécurité

IPSec (Internet Protocol Security)
Est un protocole ou une technique assurant la sécurité de la couche réseau. IPSec est conçu pour prendre en charge un environnement TCP/IP sécurisé sur Internet en tenant compte de la flexibilité, de l'évolutivité et de l'interopérabilité. IPSec prend principalement en charge la sécurité entre les hôtes plutôt que les utilisateurs, contrairement aux autres protocoles de sécurité. Récemment, IPSec est mis en évidence comme l'une des infrastructures de sécurité importantes de la prochaine génération d'Internet. Il dispose également de fonctionnalités

adaptées pour mettre en œuvre efficacement un VPN (Virtual Private Network) et ses domaines d'application devraient se développer rapidement [26].

SSL((Secure Sockets Layer)
Ce protocole permet la transmission de données chiffrées sur le réseau Internet.

TLS (Transport Layer Security) Est le successeur du protocole SSL.Est une nouvelle version de SSL. Cela fonctionne plus ou moins comme le SSL, utilisant le chiffrement pour protéger le transfert des données et de l'information. Les deux termes sont généralement utilisés de façon interchangeable dans l'industrie bien que SSL soit toujours largement utilisé [27] .
.

HTTPs (HyperText Transfer Protocol Secure)
Littéralement « protocole de transfert hypertextuel sécurisé » est la combinaison du HTTP avec une couche de chiffrement comme SSL ou TLS. HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification

SSH (Secure Shell)
Désigne à la fois un protocole de communication et un programme informatique. Il permet la connexion d'une machine distante (serveur) via une liaison sécurisée dans le but de transférer des fichiers ou des commandes en toute sécurité [28] .

4.2.10 DMZ

Une zone démilitarisée (ou DMZ, DeMilitarized Zone) est une zone de réseau privée ne faisant partie ni du LAN privé ni de l'Internet. À la manière d'une zone franche au-delà de la frontière, la DMZ permet de regrouper des ressources nécessitant un niveau de protection intermédiaire. Comme un réseau privé, elle est isolée par un firewall mais avec des règles de filtrage moins contraignantes [29] .

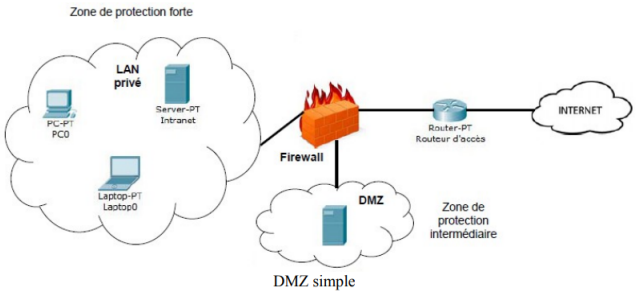

FIGURE 4.5 – Le DMZ

4.3 conclusion

A l'issue de cette étape nous avons pu exprimer clairement les outils de la sécurité des réseaux informatiques les plus utilisés au sein des entreprises . Nous avons pu collecter les différents systèmes , logiciels , matériels et méthodes de la sécurisation des infrastructures réseaux . Le chapitre suivant sera consacré à la conception de notre travail étudié dans les deux chapitres précédant.

Chapitre 5

Contexte de travail et implementation

5.1 Introduction

Ce chapitre sera dédié à la partie de la réalisation de notre application et la mise en œuvre de l'ensemble des techniques dans le but d'atteindre notre objectif. Par la suite, nous allons montrer quelques captures d'écran de notre application.

5.2 Materiel utilisé

Pour pouvoir configurer l'architecture souhaitée dont la nécessité de mettre en place une gestion de par feu ASA nous avons travaillé avec un pc de marque HP avec une RAM de 8Go et pour assurer la compatibilité des environnement on a choisi de travailler avec le système d'exploitation Windows 10.

FIGURE 5.1 – Pc utilisé

5.3 Présentation de la machine virtuelle

5.3.1 VMware Workstation 16

Est la norme de l'industrie pour l'exécution de plusieurs systèmes d'exploitation en tant que machines virtuelles (VM) sur un seul ordinateur Linux ou Windows. Pour les professionnels de l'informatique, les développeurs et les entreprises qui construisent, testent ou démontent des logiciels pour n'importe quel appareil, plate-forme ou cloud.

5.3.2 Téléchargement de VMware Workstation 16

- On pourrait toutefois télécharger une version d'évaluation de VMware Workstation 15 Pro via deux façons : Le premier moyen consiste à se connecter sur son compte « my vmware » à l'adresse www.vmware.com. Si on ne dispose pas de compte, on pourrait le créer gratuitement sur le site web de VMware. Une fois connectée à son compte, se rendre à la section « VMware Workstation 15Pro for Windows » choisir la version du produit à télécharger via un menu déroulant à la version et cliquer sur le bouton «Télécharger maintenant» pour démarrer le téléchargement du produit.

- Le deuxième moyen de télécharger la VMware Workstation 14 Pro sans disposer de compte VMware, est de se rendre sur le lien ci-dessous : https ://goo.gl/5SyGWT. Une fois sur la page « Try VMware Workstation Pro », cliquez juste sur le lien « Télécharger maintenant ».

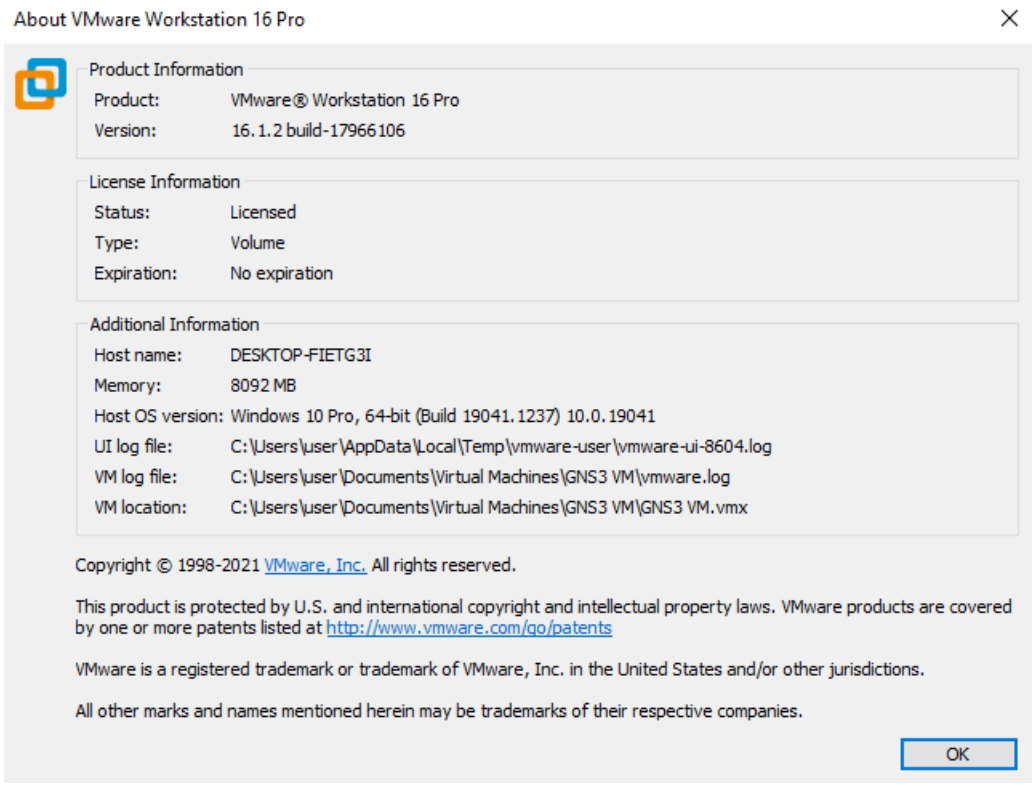

FIGURE 5.2 – La machine virtuelle

5.4 Présentation de GNS3 (Graphical Network Simulator)

Est une solution open-source qui permet d'émuler des équipements informatiques (routeur, switch, PC...) et qui permet de simuler leurs fonctionnements. Cet outil est très utile pour maquetter avant une mise en production.

5.4.1 Installation de GNS3 sous windows

Pour installer GNS3, il faut tout d'abord télécharger le fichier exécutable, ensuite le lancer et suivre les étapes d'installation :

1. Téléchargez l'installeur Windows depuis le lien fourni (www.GNS3.com).

2. Lancer l'exécution de linstallateur.

3. Lorsque la fenêtre de bienvenue s'affiche, appuyez sur « next ».

4. Acceptez les termes de la licence.

5. Ne modifiez pas le répertoire du menu démarrer au travers duquel GNS3 est accessible.

6. Laissez la liste des composants à installer inchangée.

7. A l'apparition de l'écran de bienvenue de Wireshark, appuyez sur « next ».

8. Acceptez les termes de la licence.

9. Laissez la liste des composants à installer inchangée et validez.

10. Laissez la liste des taches additionnelles inchangée et validez.

11. Ne modifiez pas le répertoire dans lequel Wireshark sera installé et validez.

12. l'apparition de l'écran de bienvenue de Winpcap, appuyez sur « OK ».

13. Acceptez les termes de la licence.

14. Autorisez le module winpcap à s'exécute au démarrage.

15. Lorsque l'installation se termine, cliquez sur « Finish ».

16. Après l'installation de GNS3, cliquez sur « Next ».

17. A la demande d'inscription à la mailing-list de GNS3,, cliquez sur « next » puis sur « No » à la fenêtre demandant de confirmer.

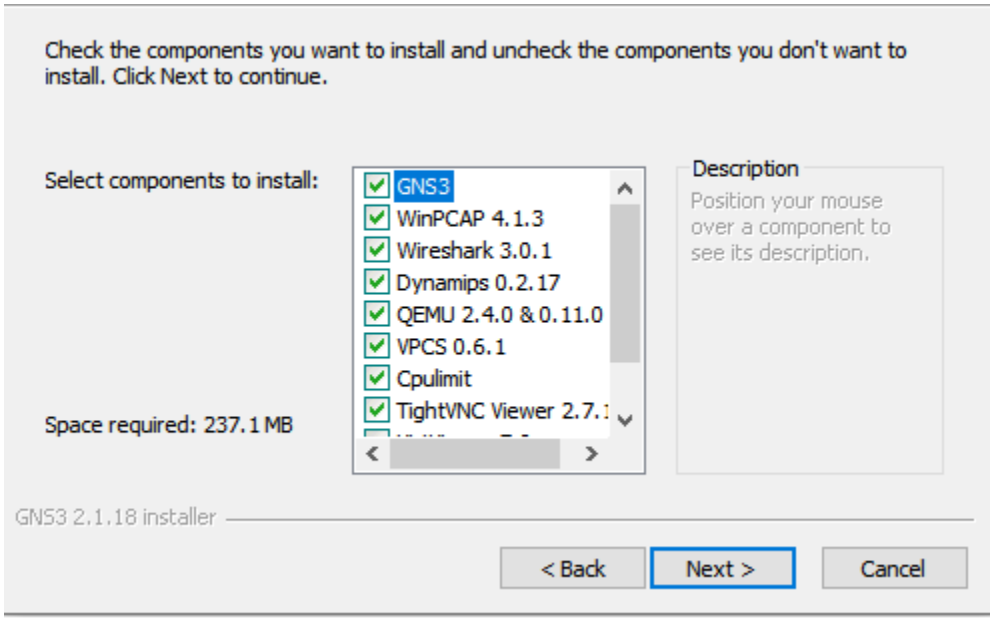

FIGURE 5.3 – Répertoire de GNC3

18. Décochez « Start GNS3 » et cliquez sur « Finish ».

19. L'installation est terminée.

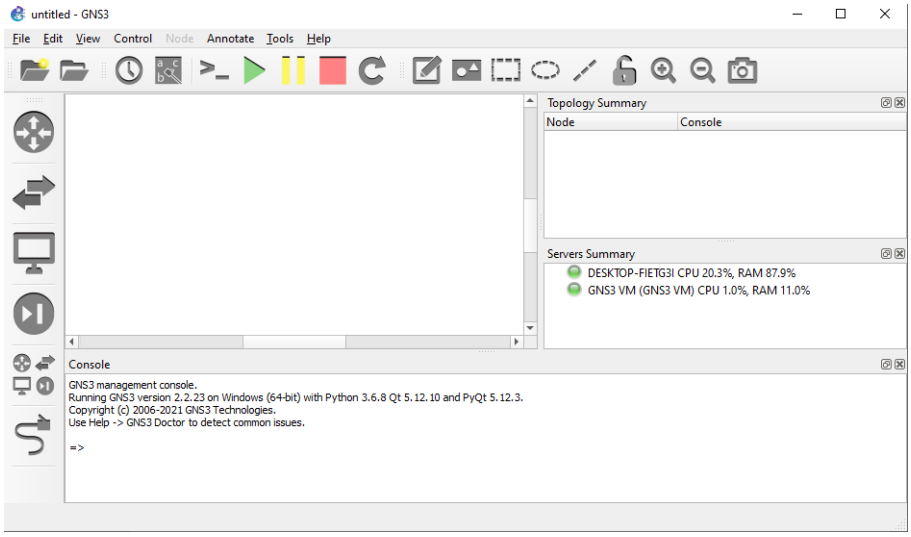

FIGURE 5.4 – l'inteface de GNS3

5.5 Architecture de configuration

Afin de bien présenter les outils d'administrations et sécurité les plus connus sur le terrain professionnel des entreprises au cours de développement de la technologie des réseaux informatiques, nous nous sommes évertués à configuré une architecture hiérarchique à trois couches (la couche cœur de réseau , la couche distribution et la couche d'accès). Chaque couche apporte ses impératifs et ses besoins , influençant le matériel mis en place ainsi que les configurations et/ou solutions. Plus compliqué au premier abord à mettre en place mais totalement plus efficace , retable , réfléchi et économe sur le long terme.

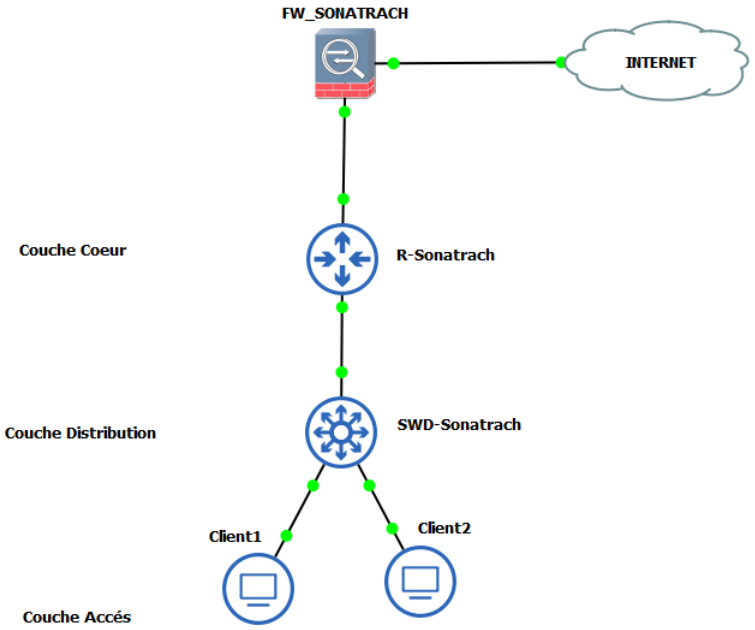

FIGURE 5.5 – Architecture de teste

5.6 Présentation de par feu ASA

Le par feu ASA est l'un des outils de sécurité les plus utilisés au sein des entreprises afin de garantir plusieurs fonctionnalités dont :

- Supervision et de système .
- Filtrage des paquets.
- Filtrage et inspection applicative.
- Network Adressa Translation (NAT).
- DHCP.
- Routage.

- Implémentation Layer 3 ou Layer 2.
- Support VPN.
- Groupe d'objets (Object groups).
- Filtrage du trafic de botnets.
- Haute disponibilité.
- Support AAA.

5.6.1 Configuration de par feu ASA

Commandes	Explication
Ciscoasa >	Mode EXEC utilisateur
Ciscoasa >enable	Mode EXEC privilégie
Password :	Pas de mot de passe
Ciscoasa #configure terminale	Mode de configuration globale
Ciscoasa(config) #interface GigabitEthernet0/0	Accès à la configuration de l'interface G0/0
Ciscoasa(config-if) #ip addresse 8.8.8.1 255.255.255.0	Adresse IP et masque de sous réseau de G0/0
Ciscoasa(config-if) #nameif outside	Réseau externe
Ciscoasa(config-if) #no shutdown	Activation de l'interface G0/0
Ciscoasa(config-if) #exit	Routeur au mode EXEC privilégie
Ciscoasa(config) #interface GigabitEthernet0/1	Accès à la configuration de l'interface G0/1
Ciscoasa(config-if) #ip addresse 10.10.10.2 255.255.255.0	Adresse IP et masque de sous réseau de G0/1
Ciscoasa(config-if) #nameif inside	Réseau interne
Ciscoasa(config-if) #no shutdown	Activation de l'interface G0/1
Ciscoasa(config-if) #exit	Routeur au mode EXEC privilégié
Ciscoasa(config) #write|memory	Sauvegardé la configuration

FIGURE 5.6 – Configuration de firewall ASA

Dimenstration de la configuration valideé sur les interfaces du par feu avec la commande "show interface ip brief" :

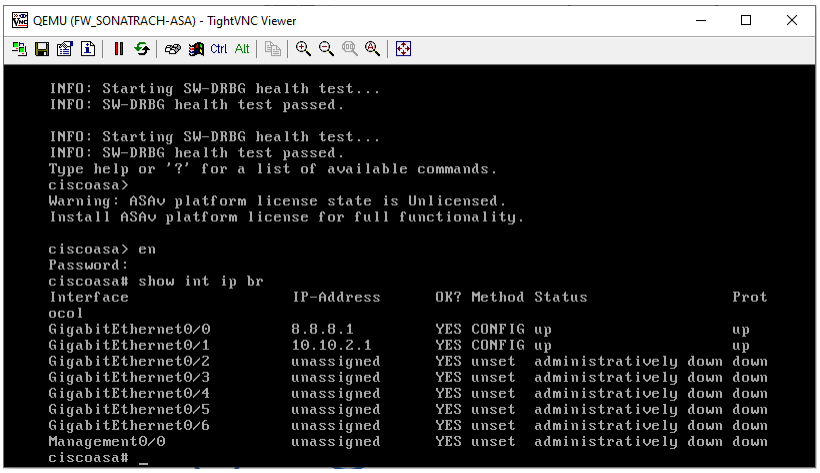

FIGURE 5.7 – Aperçu des interface de firewall ASA.

5.7 Configuration de routeur

Commandes	Explication
R>	
R1>enable	Mode EXEC privilégie
R1# configure terminale	Mode de configuration globale
R1(config)#interface Ethernet0/0	Accès à la configuration de l'interface E0/0
R1(config-if) #ip address 10.10.2.2 255.255.255.0	Adresse IP et masque de sous réseau de E0/0
R1(config-if)# no shutdown	Activation de l'interface F0/0
R1(config-if)# exit	Routeur au mode EXEC privilégie
R1(config)#interface Ethernet0/0	Accès à la configuration de l'interface E0/1
R1(config-if) #ip address 10.10.2.1 255.255.255.0	Adresse IP et masque de sous réseau de E0/1
R1(config-if)# no shutdown	Activation de l'interface 0/1
R1(config-if)# exit	Routeur au mode EXEC privilégie

FIGURE 5.8 – Configuration de routeur

La première étape consiste à donner une adresse IP pour chaque interface de routeur, Puis on doit les configurés :

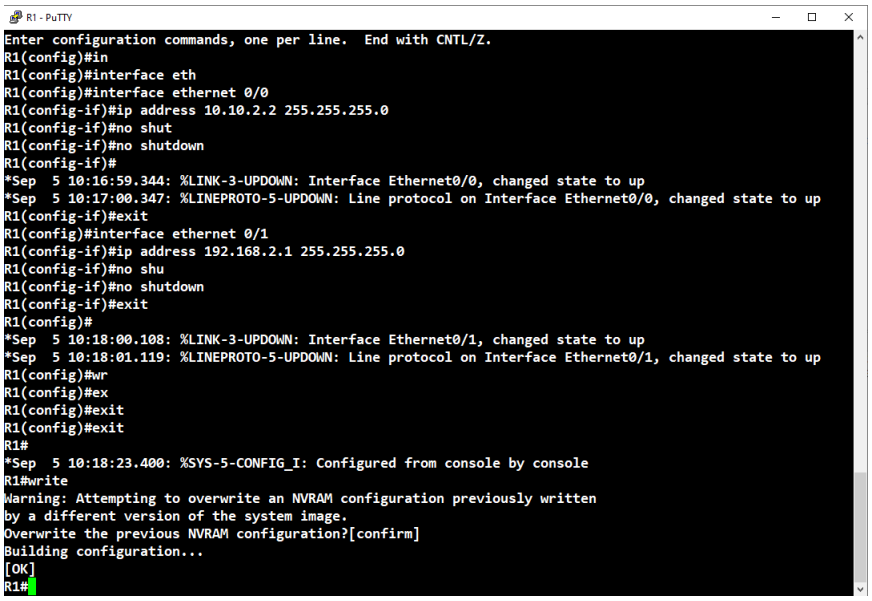

FIGURE 5.9 – Configuration de routeur

Dimenstration de la configuration valideé sur les interfaces du routeur avec la commande "show interface ip brief" :

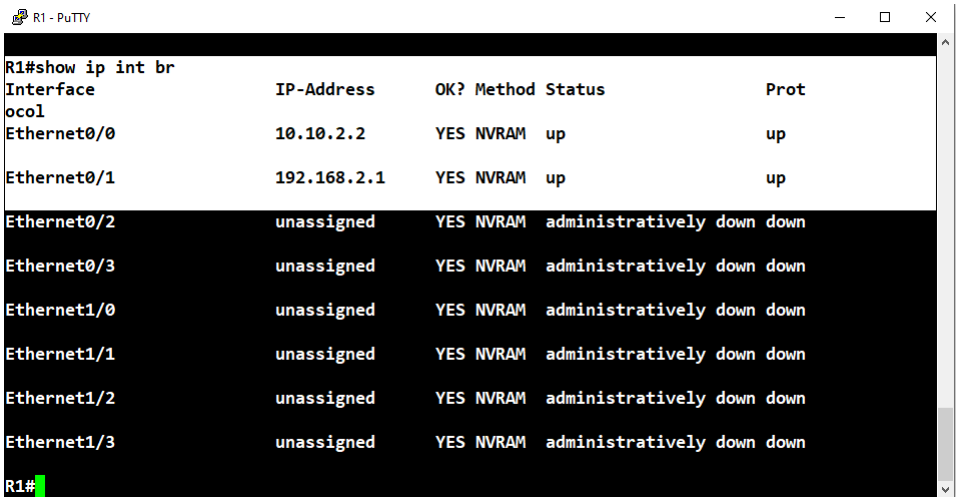

FIGURE 5.10 – Aperçu des interfaces de routeur

5.8 Présentation de client 1

Le client 1 représente l'ordinateur de l'administarteur avec lequel nous allons accéder à distance pour gérer le réseau il s'agit d'une machine vertuelle avec le système d'exploitation windows 10, bien configuré pour son usage .

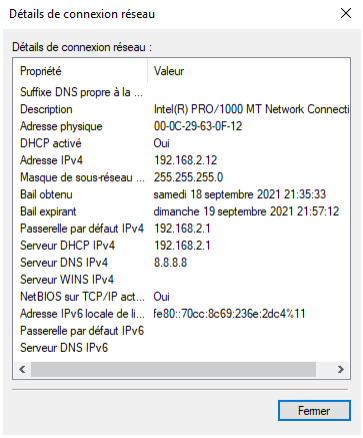

FIGURE 5.11 – Configuration de la machine client 1

5.9 CLI

L'interface en lignes de commande (CLI) bien qu'ancienne offre encore de nombreux avantages c'est la principale méthode de configuration et de gestion elle permet de bien maitriser et familiariser avec les commandes de configurations c'est l'outil le plus basique pour s'intégrer dans le monde des réseaux informatiques. La gestion à distance de notre par-feu se fais à tarvers de la CLI et à base d'un autre outil PUTTY qui est un émulateur de terminal pour Windows permettant la connexion à une machine distante par protocole telnet ou ssh. Avec ce logiciel, nous pourrons travailler, depuis notre ordinateur client 1, en mode ligne de commandes. pour l'utiliser il suffet juste de t'apper l'addresse ip de linterface d'enterer ASA , lui donner un nom et puis cliquer sur save et open pour ouvrir l'interface CLI de ASA voir les figures ci-dessous :

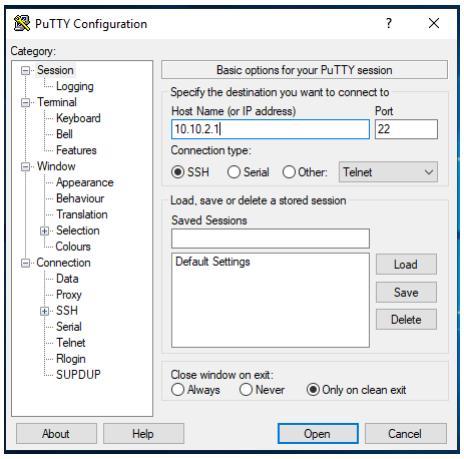

FIGURE 5.12 – Présentation de l'interface PUTTY

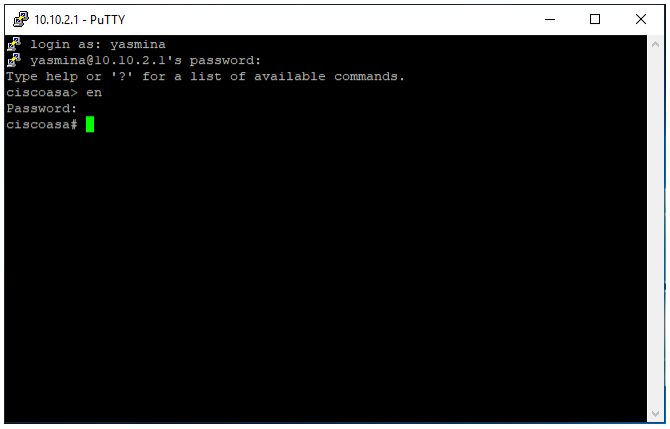

FIGURE 5.13 – CLI de ASA à travers putty

5.10 ASDM (Cisco Adaptive Security Device Manager)

ASDM Nous permet de gérer les pare-feux Cisco Adaptive Security Appliance (ASA) et le client Cisco AnyConnect Secure Mobility via une interface Web locale il nous permet d'appliquer tout les objectifs de l'administration des réseaux comme la supervision et la surveillance du systeme , visualisation de l'architecture du systeme...

5.10.1 Etapes d'installation de ASDM

le ASDM est installé à partir d'une configuration dans la cli de ASA dont :

- activer le http avec la commande (http server enable).

FIGURE 5.14 – Activation de serveur HTTP

- Autoriser le réseau de l'interface inside de n'importe quel réseau vers n'importe quel réseau avec la commande (http 0.0.0.0.0.0.0.0 inside)
- De la machine client 1 on test ping.
- Finir par télécharger le asdm par google chrome de la machine client 1.

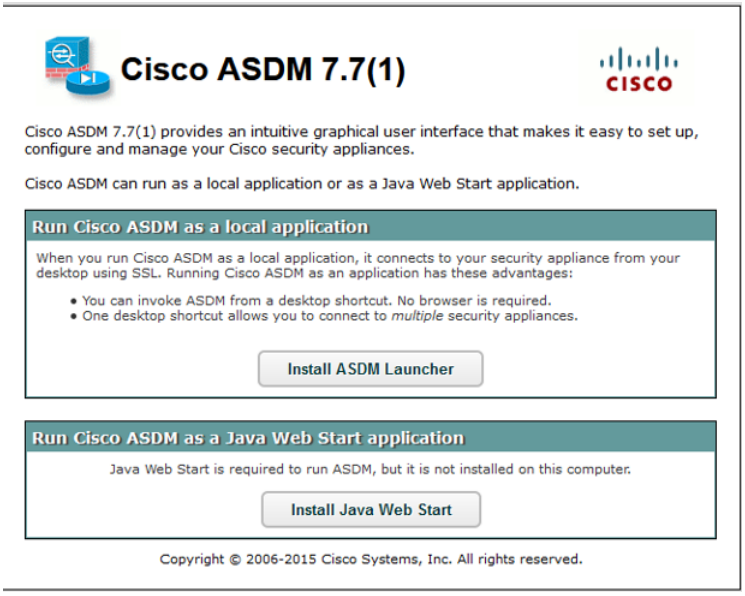

FIGURE 5.15 – Installation de l'ASDM

5.10.2 Utilisation de ASDM

Nous allons présenter les interfaces de ASDM qui sont pretes à utiliser sans avoir besoin aux commandes :

5.10.2.1 Interface d'authentification

Pour qu'un utilisateur puisse accéder à l'interface, il lui faut tout d'abord passer par l'interface d'authentification et s'authentifier pour se connecter ou bien annuler.

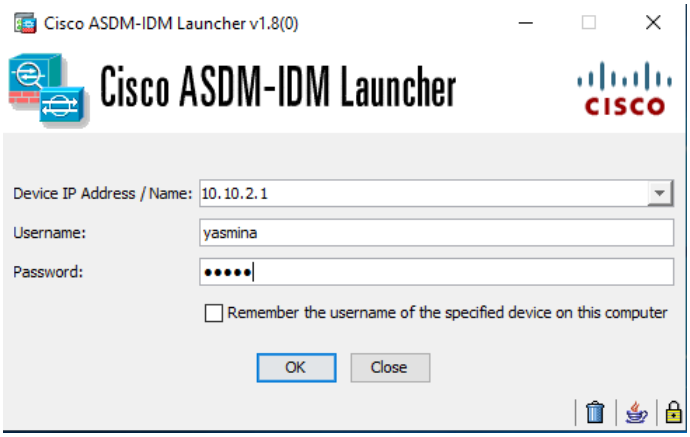

FIGURE 5.16 – L'interface d'authentification

5.10.2.2 Interface initiale de ASDM

Aprés l'authentification l'interface initiale doit apparaitre et contenir toute les informations du parfeu ASA ainsi que les paramètres de configuration et modification.

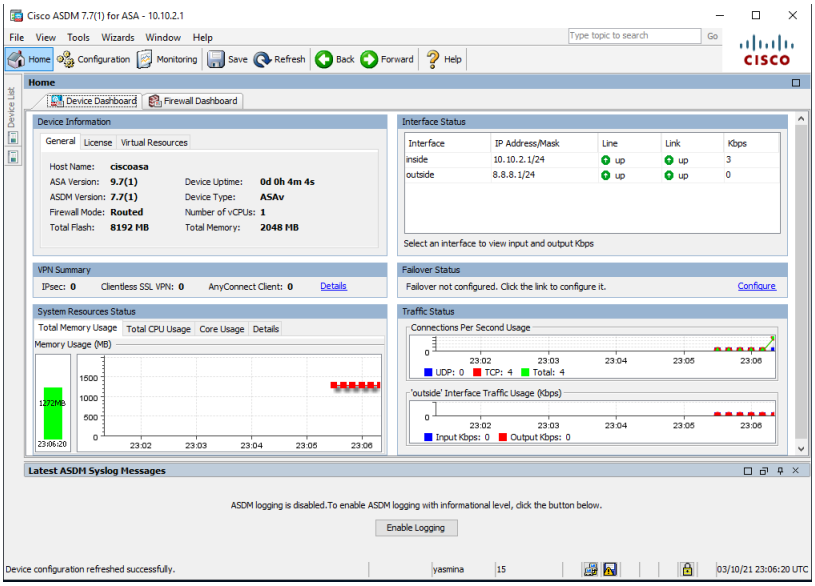

FIGURE 5.17 – L'interface initiale de ASDM

5.10.2.3 Interface de la configuration

Cette interface permet à l'administrateur de gérer le parfeu ASA à distance. Elle contient des boutons vers d'autres interfaces qui nous permettent d'effectuer les différentes conféigurations.

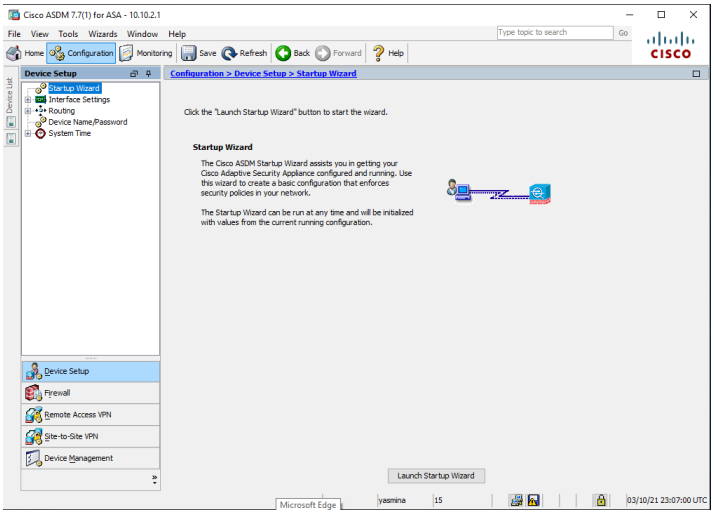

FIGURE 5.18 – L'interface de la configuration

5.10.2.4 Interface de la configuration de http et ssh

L'interface "Administrative access" permet à l'administrateur de spécifier les addresses de tous les hôtes ou réseaux qui sont autorisés à accéder au parfeu asa en utilisant HTTP/ASDM, SSH ou TELNET.

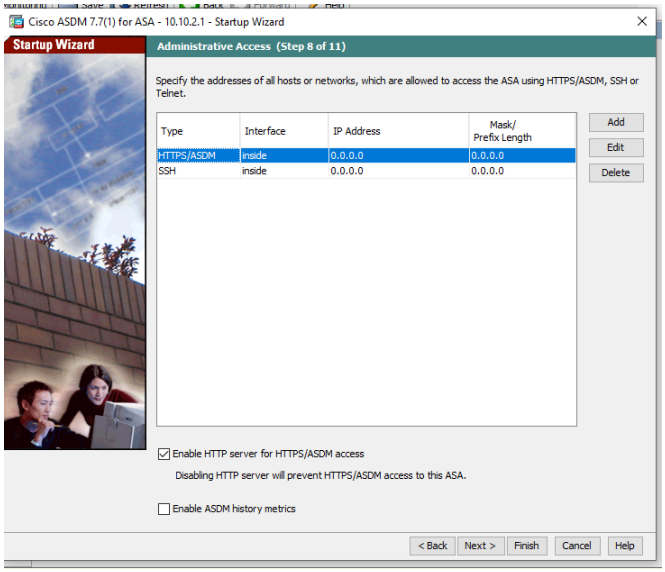

FIGURE 5.19 – L'interface de la configuration de http et ssh

5.11 Tests d'accessibilité

Nous allons tester l'accessibilité des machines et équipements à travers un réseau IP voir les images ci-dessous :

```
ciscoasa# ping 10.10.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/10 ms
ciscoasa#
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.
```

FIGURE 5.20 – Ping ASA vers le routeur

FIGURE 5.21 – Ping Client 1 vers ASA

5.12 Conclusion

Dans ce chapitre concernant la partie implémentation, nous avons présenté les différents outils ainsi qu'une présentation de quelques interfaces de notre application en montrant son bon fonctionnement avec l'illustration de quelques exemples sur les interfaces présentées, ainsi qu'à la fin de ce chapitre nous avons montré l'atteint de tous les objectifs visé au début de ce travail.

Conclusion générale et perspectives

Ce projet de fin d'études consiste à collecter les outils d'administration et sécurité des réseaux informatiques, et mettre en pratique les connaissances théoriques à travers des méthodes professionnelles utilisées Dans l'entreprise SONATRACH.

Notre stage nous a permis de mieux comprendre le domaine de l'administration et sécurité des réseaux au sein d'une entreprise. Les dimensions de cette gestion commencent d'abord par bien comprendre le rôle d'un administrateur et la valeur d'une bonne gestion dans le domaine, ainsi que l'importance de bien exploiter les outils d'administration et sécurité, afin d'arriver à définir les méthodes et les outils de cette gestion.

Pour la réalisation de ce travail, nous avons utilisé le GNS 3 avec le VMWARE WORKSTATION PRO pour reproduire et simuler l'architecture étudiée. Aussi nous avons présenté notre environnement de travail et les outils qui nous ont servi pour implémenter notre simulation et vérifier son bon fonctionnement.

La réalisation de ce modeste travail nous a mené à atteindre nos objectifs fixés dès le début, nous a permis d'enrichir et développer nos connaissances et compétences en terme de gestion professionnelle des réseaux informatiques, et s'habituer à régler les problèmes et les difficultés de la simulation et de la réalisation des projets. De plus, cela nous a permis de nous familiariser avec l'environnement de travail et aussi la vie professionnelle, tout en essayant de satisfaire notre besoin pour intégrer dans le travail de l'entreprise.

En perspective, nous souhaitons enrichir notre application, en lui rajoutant plus de fonctionnalités, aussi enrichir nos connaissances et nos compétences en vue de s'intégrer prochainement dans le milieu professionnel.

Bibliographie

[1] https://d1n7iqsz6ob2ad.cloudfront.net, Consulté le 28 Avril 2021.

[2] José Dordoigne. *Réseaux informatiques : Notions fondamentales [4e édition]*. 2013.

[3] https://www.commentcamarche.net/contents/512-topologie-des-reseaux, Consulté le 24 Avril 2021.

[4] http://hautrive.free.fr/reseaux/architectures/organisation-des-reseaux.html, Consulté le 28 Avril 2021.

[5] Yann Ducheminé. *Indroduction à l'interconnexion de réseaux [1e édition]*. 2001.

[6] Frédéric Jacquenodé. *« Normalisation des réseaux [1e 1édition]*. 2008.

[7] https://cisco.goffinet.org/ccna/services-infrastructure/protocole-resolution-noms-dns, Consulté le 12 mai 2021.

[8] Lila Adouane, Aicha Touahri, A Boukerram, et al. *Proposition d'une solution firewall pour les r´ eseaux locaux d'entreprise*. PhD thesis, 2016.

[9] R. LEGRAND et A. VAUCAMPS é. *« Notions de base sur les réseaux[1e 1édition]*. 2009.

[10] ACISSIé. *sécurité informatique Ethical Hacking apprendre l'attaque pour mieux se défendre [3e édition]*. 2012.

[11] Ali Sadiqui. *Sécurité des réseaux informatiques*. ISTE Group, 2019.

[12] Cédric Llorens, Laurent Levier, Denis Valois, and Benjamin Morin. *Tableaux de bord de la sécurité réseau*. Editions Eyrolles, 2011.

[13] https://www.kaspersky.fr/resource-center/definitions/malicious-code, Consulté le 02 juin 2021.

[14] https://www.pandasecurity.com/fr/mediacenter/mobile-news/differents-types-de-malware/, Consulté le 02 juin 2021.

[15] https://docuri.com/download/snmp_59bf3b56f581716e46c56166_pdfJuly17,2016|Author:NawalBohi|Category:N/A, Consulté le 04 juin 2021.

[16] HALId:cel-01995184https://hal.archives-ouvertes.fr/cel-01995184Submittedon25Jan2019, Consulté le 02 juin 2021.

[17] https://contenthub.netacad.com/itn/2.1.4, Consulté le 03 juin 2021.

[18] https://www.lemagit.fr/conseil/CLI-ou-interface-graphique-quels-sont-les-avantages-et-
Consulté le 09 juillet 2021.

[19] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203287-gui-graphical-user-interface-definition-traduction/, Consulté le 09 juillet 2021.

[20] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203479-ssh-secure-shell-definition-traduction/, Consulté le 01 juillet 2021.

[21] David Burgermeister and Jonathan Krier. Les systèmes de détection d'intrusions, 2006.

[22] Keltouma Belkhatmi, Ouarda Benamara, et al. *Mise en place d'un systéme de détection et de prévention d'intusion*. PhD thesis, Universite de bejaia, 2016.

[23] `https://kupdf.net/download/firewall_5afd89f5e2b6f563688f1551_pdf`, Consulté le 10 mai 2021.

[24] `www.ciscomadesimple.be/wp-content/uploads/2011/06/CMSBE_F04_ACL.pdf`, Consulté le 10 mai 2021.

[25] `http://n.grassa.free.fr/cours/proxy.pdf`, Consulté le 12 Avril 2021.

[26] `https://www.researchgate.net/publication/320357573_What_is_IPsec`, Consulté le 3 juin 2021.

[27] `https://www.websecurity.digicert.com`, Consulté le 3 juin 2021.

[28] `https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203479-ssh-secure-shell-definition-traduction/`, Consulté le 1 juillet 2021.

[29] `http://projet.eu.org/pedago/sin/ISN/8-securite_reseaux.pdf`, Consulté le 1 juillet 2021.

RÉSUMÉ

Dans ce travail nous nous focalisons sur la collecte des outils d'administration et de sécurité des réseaux informatiques, ainsi que nous mettons en évidence la supervision et l'administration du réseau informatique au sein de l'entreprise SONATRACH de Bejaia, dans laquelle on a fait notre stage pratique. Pour la réalisation de ce travail, notre simulation est faite à base du simulateur GNS 3 version 2.2.23 et VMWARE aussi WORKSTATION PRO version 16.

Mots clés : Administration, sécurité, réseau informatique, GNS 3, VMWARE, WORKSTATION PRO.

ABSTRACT

In this work we focus on the collection of administration and security tools for computer networks, as well as we highlight the supervision and administration of the computer network within the company SONATRACH of Bejaia, in which our practical internship. For this work, our simulation is based on GNS 3 version 2.2.23 and VMWARE simulator also WORKSTATION PRO version 16.

Key words : Administration, security, computer network, GNS 3, VMWARE, WORKSTATION PRO.