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 Master professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Simulation d'un pare-feu d'entreprise
Cas de SONATRACH de Béjaïa

Réalisé par :

M^elle^ BOUNOUNI Sara.
M^elle^ MECHEROUH Katia.

Devant le jury composé de :

Présidente :	M^me^ GHANEM Souhila.
Examinatrice :	M^me^ SABRI Salima.
Promotrice :	M^me^ KHALED Hayette.

Soutenu le 28 Juin 2016

Promotion 2015/2016

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AAA	Authentification Autorisation Acounting.
ACL	Access List Control.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection.
DHCP	Dynamic Host Configuration Protocol.
DMZ	Demilitarized Zone.
DNS	Doman Name Server.
HTTP	Hyper Text Transfer Protocol.
IP	Internet Protocol.
LAN	Local Area Network.
MAC	Medium Access Control.
MAN	Metropolitain Area Network.
MAU	Multi Access Unit.
NAT	Network Address Translation.
OSI	Open System Interconnexion.
VNC	Virtual Network Computing.
VPN	Virtual Private Network.
VLAN	Virtual Local Area Network.
WAN	Wide Area Network.

Introduction générale

De nos jours, la plus part des entreprises possèdent de nombreux postes informatiques qui sont en général reliés entre eux par un réseau local. Ce réseau permet d'échanger les données entre les divers collaborateurs internes à l'entreprise et ainsi de travailler en équipe sur des projets communs.

Une entreprise n'est jamais complètement fermée sur elle même. Il est par exemple nécessaire de pouvoir partager des informations avec les clients de l'entreprise, ce qui signifie laisser une porte ouverte a divers acteurs étrangers. Cette porte peut être utilisée pour des actions qui, si elles ne sont pas contrôlées, peuvent nuire à l'entreprise (piratage et destruction de données).

Pour parer à ces attaques, une architecture de réseau sécurisée est nécessaire. L'architecture devant être mise en place doit comporter un composant essentiel qui est le pare-feu. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut également permettre de restreindre l'accès interne vers l'extérieur et inversement.

En plaçant un pare-feu limitant ou interdisant l'accès à ses services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Dans ce cadre s'inscrit notre projet de fin d'études qui consiste à mettre en place un pare-feu d'entreprise, cas de SONATRACH de Béjaïa. Pour mener à bien notre travail, nous le répartissons en quatre chapitres.

Nous allons préluder par « Généralités sur les réseaux et sécurité informatique » où nous allons définir les réseaux, leurs rôles ainsi que leurs différents type d'une part et définir la sécurité informatique et retracer quelques attaques d'autre part.

Dans le chapitre suivant « Organisme d'acceuil » nous allons faire une présentation de la SONATRACH de Béjaïa RTC (Région Transport Centre) et dégager la problématique de l'entreprise et de proposer une solution à cette dernière.

Dans le prochain chapitre nommé « Les pare-feu » nous allons expliquer c'est quoi un pare-feu et ses différents types.

Le dernier chapitre « Réalisation » sera consacré à la réalisation de notre travail qui est une simulation sous Packet-Tracer.

Chapitre 1

Généralités sur les réseaux et sécurité informatique

1.1 Introduction

Aujourd'hui, les réseaux informatiques sont devenus incontoutnables. Ils sont omniprésents dans toutes les entreprises. Ils servent à mettre en oeuvre des applications très diverses, des plus simples aux plus sophistiquées. La plus connue est la navigation sur le Web qui permet le partage d'informations grâce à Internet. Les réseaux obéissent à des principes de structuration qu'il est indispensable de comprendre. Ils utilisent une architecture en couches, dans laquelle la communication entre ordinateurs obéit à des règles précises définies par des protocoles de communication. Les protocoles les plus connus sont TCP et IP ; ils ont donnée leur nom à l'architecture TCP/IP.

Ce chapitre sera décomposé en deux parties, la première consiste à retracer les rôles, les types et le fonctionnement des réseaux. Dans la deuxième partie nous aborderons les différents concepts de la sécurité informatique, ses objectifs, les différentes attaques et les statégies de sécurité.

1.1.1 Généralités sur les réseaux

1.1.2 Rôles des réseaux

Avant de rentrer dans le détail de l'architecture des réseaux, il semble nécessaire de réfléchir sur ce que peut amener un réseau à un système d'information.

L'une des raisons justifiant très souvent l'installation d'un réseau est le partage des ressources (imprimantes, copieurs, lecteurs DVD) entre plusieurs utilisateurs. Il est en effet particullièrement intérressant d'accéder à des données à distance et de réaliser sur ces dernières toutes les opérations qui seraient disponibles en travaillant réellement sur l'ordinateur distant.

De même, il est possible de mettre des programmes à la dispostion de l'ensemble des utilisateurs connectés. Dans ce cas, le nombre d'installation d'un logiciel peut par exemple être réduit à une seule, ce qui facilite de manière évidente la tâche d'un administrateur du système.

Enfin, de nombreux périphériques peuvent être partagés sur un réseau. C'est alors souvent l'aspect financier qui est intéressant, il est évident que le partage de périphériques entraîne directe-

ment une réduction des coûts. L'interconnexion de plusieurs ordinateurs facilite aussi la poursuite du travail en cas de problème sur l'une des machines.

La toile (le web) est aujourd'hui une source mondiale de l'information de tous types directement utilisables par chaque utilisateur et basée sur l'interconnexion physique d'un trés grand nombre de réseaux locaux [1].

1.1.3 Différents types de réseaux

Les caractéristiques principales qui vont permettre de differencier les grandes familles de réseaux sont la taille et le mode de transmission de l'information utilisé. Dans ce qui suit nous présentons les différentes familles [5] :

1. Les réseaux locaux

Un réseau local ou LAN (Local Area Network) permet de connecter des éléments (ordinateurs et périphériques) distants de quelques mètres à quelques centaines de mètres. On recense donc sous cette appellation la plupart des réseaux informatiques présents dans les entreprises.

La notion de surface géographique limitée n'implique pas un nombre faible de postes de travail interconnéctés : un réseau local peut en effet compter jusqu'à plusieurs centaines de machines.

La transmission des données est réalisé par un support simple auquel chaque ordinateur accède selon des méthodes d'accès définies par des normes établies.

Lorsqu'un poste de travail désire emettre des données vers un second, le mode de transmission est la diffusion. Les débits proposés par les réseaux locaux s'étalent de 1 Mbit/s à plus de 1 Gbit/s, en fonction des normes et de l'évolution matérielle. Les délais de transmission sur de tels réseaux sont très courts.

2. Les réseaux métropolitains

Un réseau métropolitain ou MAN (Metropolitain Area Network) est un réseau dont la géographie peut aller jusqu'à couvrir une ville. Il sert généralement à interconnecter des réseaux locaux distans de quelques kilomètres.

Le fonctionnement d'un MAN est similaire à celui des réseaux locaux. Avec l'interconnexion des réseaux locaux à Internet, en particulier par les VPN (Virtual Private Network) ou réseau privé virtuel, le terme de MAN tend de plus en plus à être intégré dans la famille des réseaux longues distance et devrait disparaître prochainement. Dans la plupart des cas, le grand public simplifie la terminologie en interconnectant des LAN par des réseaux longue distance.

3. Les réseaux longue distance

Dans son rôle, un réseau longue distance ou WAN (Wide Area Network) se rapproche d'un réseau MAN. Il est en effet utilisé pour permettre des échanges entre des réseaux locaux, mais qui sont séparés par des distances plus importantes, de plusieurs centaines à plusieurs milliers de kilomètres.

Sa structure est par contre plus complexe. Les ordinateurs, indépendants ou regroupés en réseau LAN constituent les extrémités du réseau. A la différence des réseaux locaux ou métropolitains, la transmission des données entre ces ordinateurs n'est plus laissée à la seule charge du support de transmission, mais d'un sous-réseau de communication. Ce sous-réseau possède les lignes physiques ainsi que des éléments actifs (commutateurs) qui vont aiguiller l'information de l'emetteur vers le destinataire à travers le maillage. La complexité de ce maillage varie avec la taille géographique et le nombre de commutateurs présents sur le parcours des données. On parle aussi dans ce cas de réseau maillé.

Le mode de transmission des données dans un réseau longue distance est généralement le point à point. Chaque commutateur est un noeud qui possède une capacité de réflexion : lorsqu'il reçoit de l'information sur l'un de ses ports de communication, il détermine sur quel port emettre cette information pour qu'elle parvienne au plus vite au destinataire.

Le plus grand réseau longue distance est aujourd'hui Internet. D'un point de vue physique, le réseau mondial n'est autre que l'interconnexion d'un très grand nombre de réseaux locaux. Notons qu'un intranet est un réseau local utilisant les technologies d'Internet et proposant les mêmes services aux utilisateurs. La figure (Fig 1.1) résume les types de réseaux.

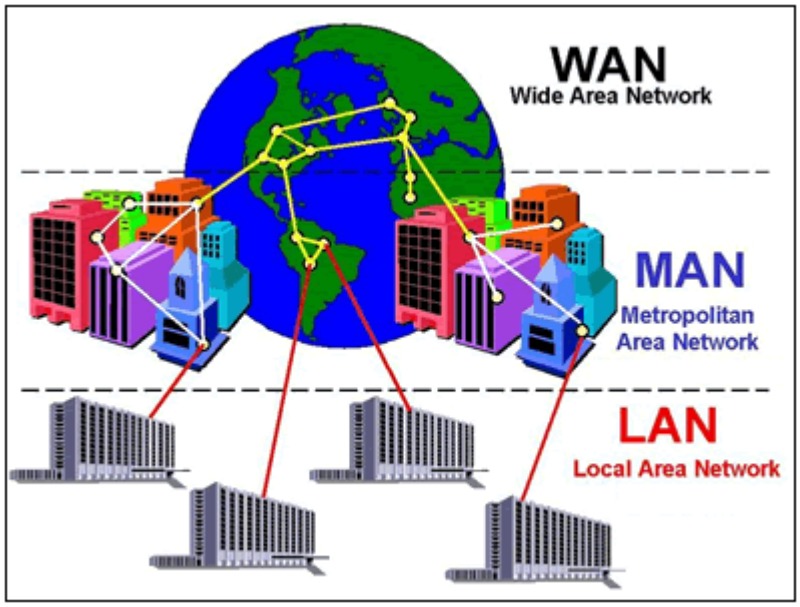

FIG. 1.1: Les types de réseau.

1.1.4 Topologies des réseaux

Pour pouvoir utiliser un réseau, il ne suffit pas de brancher le matériel aléatoirement. Il faut définir, en plus du type de réseau, une méthode d'accès entre les ordinateurs ce qui permettra de connaître la manière dont les informations sont échangées.

Il existe deux types de topologies : topologie physique et topologie logique [5].

1. **Topologie physique :** Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique du réseau est appelé topologie physique.

   La topologie physique est en réalité la façon dont les ordinateurs sont connectés physiquement les uns aux autres. On distingue généralement les topologies suivantes [5] :

   1.1 Topologie en bus : Il s'agit de l'organisation la plus simple d'un réseau. Cette topologie relie tous les ordinateurs par un même câble réseau comme nous la montre la figure (Fig 1.2). Ce n'est pas la topologie la plus pratique s'il y a plus de deux, ou trois ordinateurs connectés. Puisque le câble servant à la transmission est commun à toute les machines, il est impossible d'en avoir deux communiquant en même temps pour éviter les collisions. Si la ligne est déjà occupée, il va falloir attendre qu'elle se libère pour pouvoir l'utiliser. Ce n'est pas non plus la topologie la plus sûre, s'il y a un problème avec le câble plus aucune machine ne pourra communiquer vu qu'elles partagent le même [5].

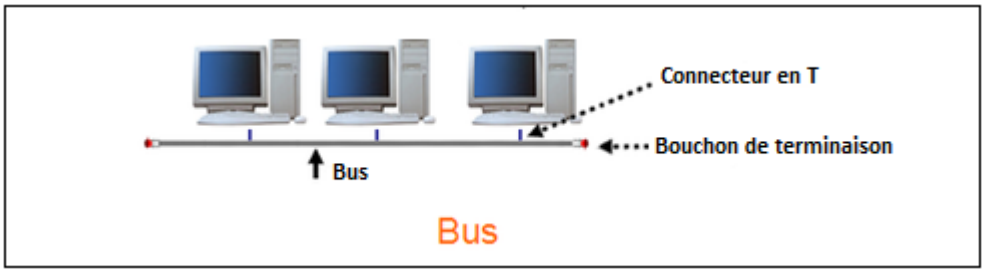

FIG. 1.2: Topologie en bus.

   1.2 Topologie en étoile : Dans une topologie en étoile, les machines sont reliées à un appareil comme un hub ou un switch qui est au centre du réseau, la figure (Fig 1.3) nous illustre cette topologie.
   Pour communiquer à une autre machine, le message envoyé par l'ordinateur est obligé de passer par ce point central ce qui permet d'éviter les collisions entre les paquets. Cette topologie est plus coûteuse que la topologie en bus (dû à l'achat de l'appareil central) mais il est plus rapide et plus sûr. Le risque est que si l'appareil central n'est plus en état de marche, le réseau ne fonctionne plus [5].

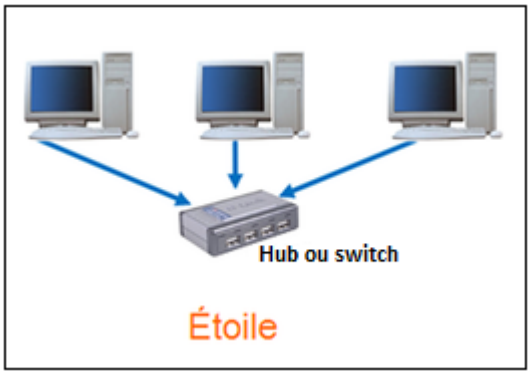

FIG. 1.3: Topologie en étoile.

1.3 Topologie en anneau : Dans ce type de topologie, les machines communiquent chacune leur tour ce qui permet d'éviter le problème majeur de la topologie en bus : la collision des données !
Pour simplifier les schémas, on dispose les ordinateurs en cercle comme nous la montre la figure (Fig 1.4) mais dans la réalité les machines sont connectées à répartiteur qu'on appelle aussi MAU (Multistation Access Unit) qui gère la communication en attribuant à chacun un temps de parole. Les deux principales topologies logiques utilisent cette topologie physique [5].

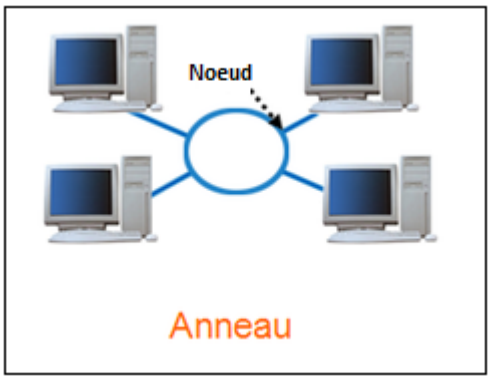

FIG. 1.4: Topologie en anneau

1.4 Topologie maillée : Cette topologie n'est pas la plus pratique ni la plus facile à mettre en place. L'idée est de relier tous les ordinateurs entre eux ce qui permet d'éviter une panne générale mais le nombre de liaisons peut devenir rapidement très élevé.
On trouve cette topologie dans les grands réseaux de distribution comme Internet. L'information parcours le réseau en passant par les différentes machines [5].

2. **Topologie logique :** Une topologie logique est une structure logique d'une topologie physique. Elle définit comment la communication se passe. Il en existe deux principales :

2.1 Ethernet : Dans un réseau Ethernet, tous les ordinateurs sont reliés à une même ligne de transmission. La communication est gérée par un protocole appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detection. Avec ce protocole chaque machine peut émettre sur la ligne de transmission à n'importe quel moment et sans notion de priorité. Avant d'émettre un message, la machine vérifie qu'il n'y a aucune communication sur la ligne, s'il y a deux machine qui communiquent en même temps, il y a alors une collision, les machines vont interrompre leur envoi de message et attendre aléatoirement un temps avant de réessayer d'envoyer leur données [5].

2.2 Token ring : Appelé en français l'anneau à jeton. Le principe de l'anneau à jeton est de donner le droit de parole à chaque machine chacune son tour.
Le jeton représente un paquet de données qui circule en boucle d'une machine à une autre. Lorsqu'un ordinateur est en possession de ce jeton, il peut émettre des informations durant un temps donné, à la fin du temps déterminé le jeton passe à un autre ordinateur. Les machines sont reliées à un MAU (Multistation Access Unit) qui gère la parole dans le réseau [5].

1.1.5 Fonctionnement d'un réseau (le modèle OSI)

Les architectures de réseaux, comme toutes les architecture de systèmes ouverts, sont fondées sur une hiérarchie en couches. Le modèle OSI (Open System Interconnexion) présente une structure en couches, ces dernières sont repérés par le niveau dans la hiérarchie. Chacune d'entre elles a pour rôle de fournir des services à la couche qui lui est immédiatement supérieure. La nature de ces services diffère en fonction du niveau de la couche et doit être adaptée au mieux à son rôle.

La couche de niveau n d'un ordinateur ne peut communiquer qu'avec la couche de niveau n d'un autre ordinateur.

Une communication entre deux couches de niveau n est soumise à un certain nombre de règles définies par un protocole. Le protocole fixe, de manière parfaitement claire et détaillée, toutes les caractéristiques de l'échange qui est effectué entre les deux entités de niveau n. Le modèle OSI est composé de sept couches qui sont les suivantes [1] :

1. La couche physique

La couche physique regroupe toutes les caractéristiques de la transmission de données binaire au niveau matériel. Ses caractéristiques sont de deux ordres : elle concernent d'une part le média lui même, et d'autre part les techniques qui vont être utilisées pour qu'une machine puisse émettre un bit sur ce média.

L'éventail des supports de transmission utilisés est très large. Parmis les plus communs, on citera les câbles électriques ou les fibres optiques, mais de nouvelles technologies sont aujourd'hui disponibles, telles que les liaisons radio ou laser.

La couche physique propose des techniques de transmission binaire propre à chacun de ces supports.

2. La couche liaison de données

La couche liaison de données a pour rôle global d'utiliser les services que lui fournit la couche physique pour émettre des ensembles de bits sur un support de transmission. Les bits sont regroupés en trames binaire. La construction de ces trames suit un format précis définissant par exemple la taille de la chaîne binaire à envoyer, les champs de contrôle sur ces données, la forme des adresses de l'émetteur et du récepteur.

Le contrôle d'erreur réalisé par cette couche permet de détecter si une trame arrivée au récepteur n'a subi aucune modification sur le média de transport. Certaines méthodes de détection d'erreurs permettent de les corriger ; pour cela des informations supplémentaires sont ajoutées aux données lors de la construction de la trame. Les protocoles de niveau liaison de données sont aussi chargés de la gestion des acquittements des trames reçues.

Une fois la trame construite et le contrôle d'erreur mis en place, la couche liaison doit gérer l'accès au support de transmission commun à toutes les machines connectées. Ce support étant physiquement unique, les algorithmes d'accès au média devront être optimisés, justes et équitables pour que cet accès soit transparent à l'utilisateur. Les fonctions propores à cette tâche particulière sont regroupés au sein de la sous-couche d'accès au média MAC (Medium Access Control).

3. La couche réseau

La couche réseau a pour rôle général de faire transiter des données entre deux points d'un réseau (émetteur et récepteur) à travers un maillage dont la compléxité peut être élevée. Ses fonctions principales concernent l'adressage, la constitution des trames de niveau 4 et les techniques de routage.

Des trames de niveau réseau sont constituées à partir des données fournies par la couche transport. En plus des données à transmettre sont ajoutées diverses informations nécessaire au cheminement de la trame sur le réseau, telles que par exemple l'adresse du récepteur, un numéro permettant la bonne restauration des données après réception.

Le transport de la trame de l'émetteur au récepteur nécessite une réflexion sur le chemin à emprunter : il existe pour cela de nombreux algorithmes de routage. La couche réseau est aussi chargé de gérer le réseau d'un point de vue plus golobal : des problèmes peuvent survenir, du fait d'avoir des trames trop nombreuses sur un segment à un instant donné ou du disfoncionnement d'une ligne physique qui modifie directement le maillage du réseau. Si un émetteur envoie plusieurs trames à un même destinataire, toutes n'emprunteront pas forcément le même chemin.

4. La couche transport

La couche transport est la première couche entièrement logicielle. En effet, les couches de niveau inférieurs sont liés au matériel : la couche physique met le support de transmission à disposition des interlocuteurs, les fonctions de la couche liaison de données sont réalisés par les composants électroniques de la carte réseau ou du modem et celles de la couche réseau par des éléments actifs (routeurs, passerelles). La couche transport fournit un ensemble de fonctions logicielles destinées à préparer le travail que devra effectuer la couche réseau, indépendamment du matériel utilisé pour l'acheminememt des trames sur le réseau.

Les données traitées par cette couche sont des messages provenant des couches supérieures. Ces messages sont d'abord scindés en paquets de taille fixée qui sont traités individuellement par la couche réseau. A la réception, ces paquets sont ré-assemblés puis mis à la disposition de la couche session.

5. La couche session

La couche session permet d'établir une liaison entre deux utilisateurs distants, indépendamment de la connexion physique, elle a pour tâche de gérer les échanges, de manière à synchroniser le dialogue et éviter les confusions. Certains protocoles proposent pour cela la création d'un jeton de gestion du dialogue. L'utilisateur qui possède ce jeton a le droit temporaire d'utiliser la connexion et il le cède lorsqu'il n'a plus besoin d'émettre.

La couche session dispose de mécanismes de reprise de l'échange en cas de problème sur la connexion. La transmission doit reprendre au point le plus proche de celui auquel elle s'est interrompue.

6. La couche présentation

Il est évident qu'un message reçu doit pouvoir être traité par le récepteur quelle que soit la nature de la machine émetrice, c'est à dire indépendamment du système d'exploitation en place d'une part et de l'application utilisée pour créer le message d'autre part.

La couche présentation a donc pour rôle d'adapter toutes les données à émettre à un format standard épuré de tous les aspects liés à l'environnement de travail et en particulier au système d'exploitation.

7. La couche application

Propose à l'utilisateur des outils d'utilisation et de gestion du réseau. Les utilisations qui peuvent être offertes par un réseau sont nombreuses et variées : messagerie électronique, transfert de fichiers, connexion distante, World Wide Web, etc. Les protocoles de niveau application ont été conçus afin de garantir pour chaque famille d'application une entière compatibilité entre les différents environnements logiciels, on cite comme exemple : HTTP(Hyper Text Transfer Protocol), SMTP et

SSL. La figure (Fig 1.5) nous résume la nature des données échangés entre chaque couche de deux hôtes communiquants.

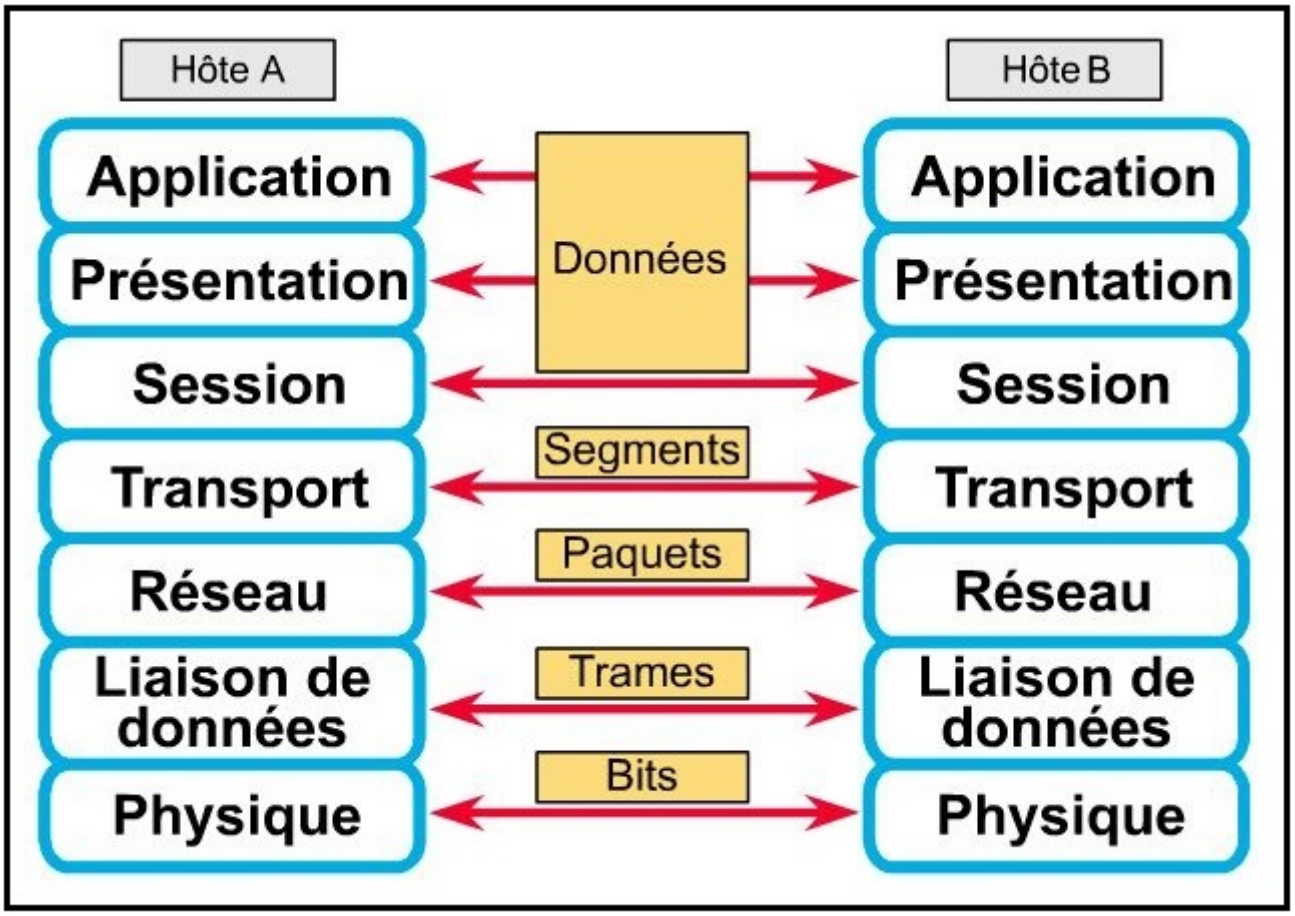

FIG. 1.5: Communication en couches.

1.1.6 Le modèle TCP/IP

Les systèmes d'information ont beaucoup évolué depuis la création du modèle OSI. Avec l'apparition de nouvelles technologies matérielles et logicielles, le modèle de référence n'est plus aujourd'hui adapté aux nouvelles architectures de réseaux. Des évolutions ont été proposées, mais même si le modèle était particulièrement bien conçu au départ, il semble de plus en plus difficile de faire référence aux 7 couches OSI.

L'apparition d'Internet a encore compliqué le problème : la diversité des solutions présentes, tant d'un point de vue matériel que d'un point de vue logiciel, a entraîné le besoin d'outils de conversion à chaque niveau : les convertisseurs au niveau physique, les passerelles au niveau données, des protocoles ouverts voire universels au niveau réseau et des application multi-plateformes.

Parmi ces évolutions, la principale est la généralisation de l'usage des protocoles TCP et IP comme standatds en matière d'interconnexion de réseau. C'est donc naturellement que s'est construit un nouveau modèle directement basé sur ces deux protocoles, nommé le modèle de réference TCP/IP.

Ce dernier définit une architecture de réference en quatre couches permettant au diverses applications réseau d'accéder à un support de transmission [1].

1. La couche interface réseau

Elle regroupe toutes les fonctions des couches de niveaux 1 et 2 du modèle OSI. C'est donc une couche qui abrite un nombre important d'entités nécessaires pour fournir tous les services liés au support physique et à l'interface réseau.

Les tâches réalisées par la couche interface réseau sont :
- Constitution de trames ;
- Mise en place d'un gestion d'erreurs sur les trames fournies par la couches supérieure : détection des erreurs de transmission et correction de celles-ci si c'est possible ;
- Accès au média selon les techniques d'accès définies par les différentes normes de réseaux ;
- Transmission sur les divers supports physiques utilisables.

2. La couche Internet

Les rôles de la couche Internet sont similaire à ceux de la couche réseau du modèle OSI. Elles ont la particularité d'être réalisées par un protocole universel : IP (Internet Protocol). Elles sont donc entièrement indépendantes de l'environnement matériel et permettent l'interconnexion de structures différentes de manière transparente. Les trames crées par cette couche portent le nom de trames IP, elle suivent un format défini par le protocole IP.

3. La couche transport

Les couches Internet et transport pourraient aisément être regroupées en une seule couche chargée de la gestion d'une communication.

4. La couche application

De nombreuses applications sont disponibles pour utiliser les réseaux. Elles sont basées sur des protocoles de haut niveau conçus spécifiquement afin de compatrimenter les rôles bien distincts at ainsi de gérer diverses familles d'applications.

Citons les types d'applications les plus communs, accompagnés de leur protocole de référence :
- Le courrier électronique (SMTP) ;
- La téléphonie IP et la VoIP (SIP) ;
- Les connexion à distance (TELNET, SSH) ;
- Le Web (HTTP) ;
- L'administration réseau (PING) ;
- La sécurité (SSL)

La figure suivante (Fig 1.6) nous résume les différentes couches du modèle OSI ainsi que le modèle TCP/IP.

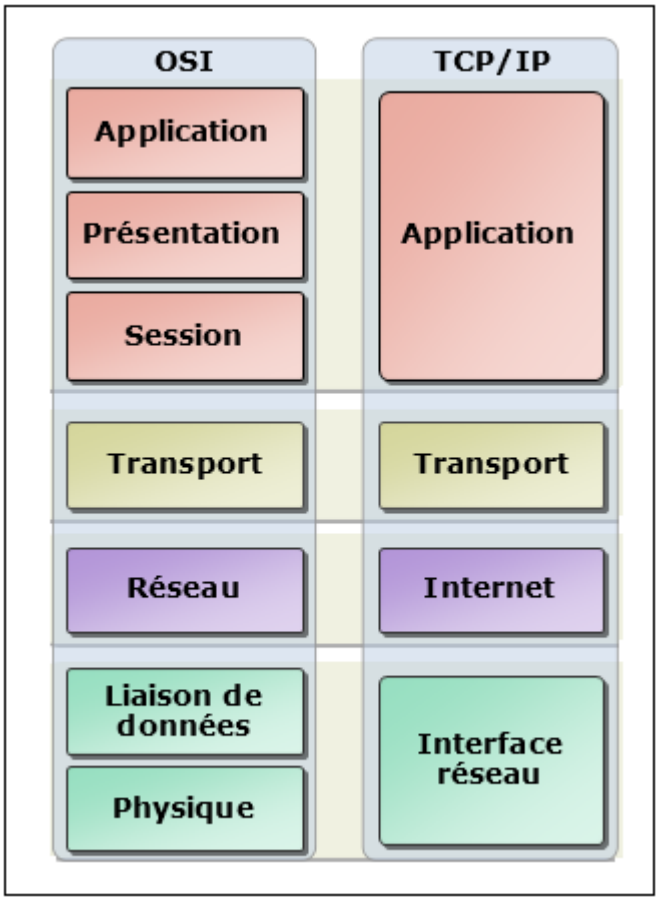

FIG. 1.6: Modèle OSI / Modèle TCP/IP

1.1.7 Les transmissions et les supports

Un réseau suppose plusieurs équipements informatiques (ordinateurs fixes ou portables, divers équipements électroniques, télephones...) situés à distance les uns des autres. La première chose à mettre en oeuvre pour constituer le réseau est la transmission des informations d'un équipement à l'autre : on utilise des supports de transmission. A chaque nature de support correspond une forme particulière du signal qui se propage. Les techniques de transmission et l'interface entre ordinateur et modem sont normalisées pour assurer l'intéropérabilité des équipements [2].

1. Supports de transmission

Les supports de transmission sont nombreux. Nous distinguons : les supports métalliques, non métalliques et immatériels. Les supports métalliques, comme les paires torsadées et les câbles coaxiaux, sont les plus anciens et les plus largement utilisés ; ils transportent des courants électriques. Les supports non métalliques de verre ou de plastique, comme les fibres optiques, transmettent la lumière, tandis que les supports immatériels des communication sans fil propagent des ondes électromagnétiques et sont en plein essor [2].

2. Caractéristiques globales des supports de transmission

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

3. Techniques de transmission

Selon les techniques de transmission, un équipement spécifique est placé à chaque extrémité du support : soit un modem (modulateur-démodulateur), soit un codec (codeur-décodeur). Cet équipement fabrique avec les données binaires à émettre, un signal dont les caractéristiques sont adaptées au support de transmission. Inversement, à la réception, il extrait la suite des données binaires du signal reçu. Le support et les deux modems placés à ses extrémités constituent le circuit de données [2].

1.2 Sécurité informatique

1.2.1 Principe de la sécurité informatique

La sécurité informatique c'est l'ensemble des moyens mis en oeuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelle [7].

1.2.2 Objectifs de la sécurité

La sécurité vise à assurer plusieurs propriétés :

La confidentialité : C'est la propriété qui garantie que les informations transmises ne sont compréhensibles que par les entités autorisées.

L'authentification : C'est la propriété qui consiste à vérifier l'identité d'un utilisateur avant de lui donner l'acccès à une ressource.

L'intégrité : C'est la propriété qui consiste à vérifier si les informations n'ont pas été modifiées durant la transmission.

La disponibilité : c'est la propriété qui permet de garntir l'accès aux données.

La non-répudiation : C'est la propriété qui permet d'avoir une preuve comme quoi un utilisateur a envoyé (ou reçu) un message particulier. Cette propriété permet d'empêcher l'utilisateur de nier l'envoie (ou réception) du message en question.

1.2.3 Les attaques

Les attaques représentent les moyens d'exploiter une vulnérabilité. Ils s'appuient sur divers types de faiblesses telles que les faiblesses des protocoles, faiblesses d'authentification, faiblesses d'implémentation ou bogues et les Mauvaises configurations.

Dans ce qui suit, nous décrivons brièvement la classification des attaques ainsi qu'une description de quelques attaques basées sur ces faiblesses.

1. Les scènarios d'attaques

Les scènarios d'attaques peuvent être classées en deux grandes catégories :

a) Attaque passive

Dans ce genre d'attaques, les informations ne sont pas modifiées. L'attaquant collecte seulement les informations qui circulent sur le réseau.

b) Attaque active

Il y a trois cas possible pour mener une attaque active [15] :

L'interruption : L'intrus intercepte le message envoyé par l'utilisateur A pour B et l'interrompt, ceci illustré par la figure (Fig 1.7).

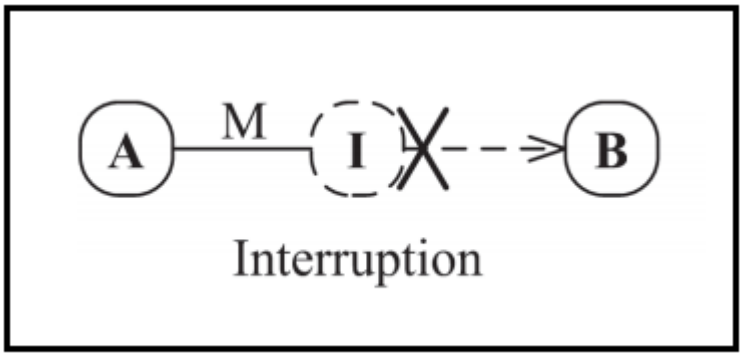

FIG. 1.7: L'interruption.

La modification : L'intrus intercepte le message envoyé par l'utilisateur A et le modifie avant de le faire suivre à l'utilisateur B, ceci présenté par la figure (Fig 1.8).

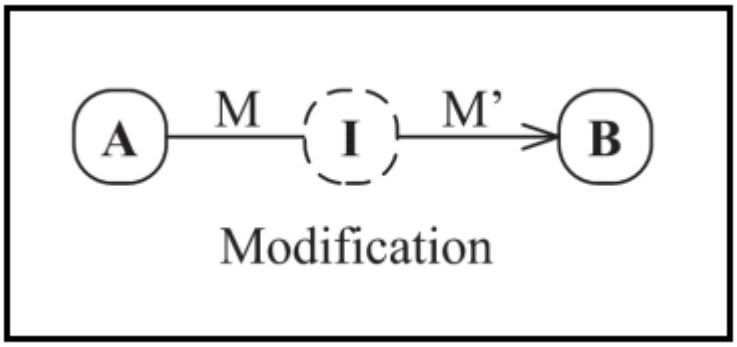

FIG. 1.8: La modification.

La fabrication : L'intrus fabrique un message et l'envoie à l'utilisateur B en se passant pour l'utilisateur A, ceci exposé par la figure (Fig1.9).

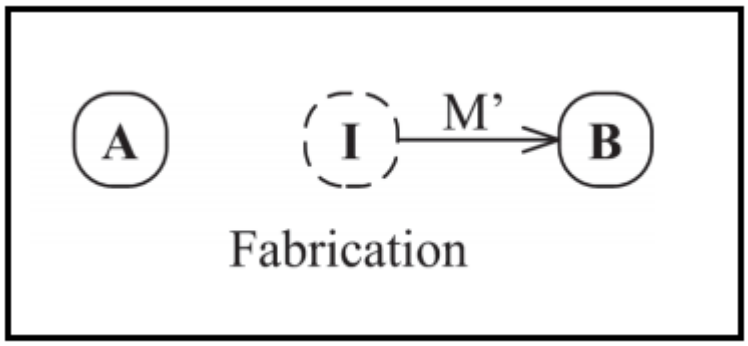

FIG. 1.9: La fabricationtion.

2. Description de quelques attaques

Les attaques réseaux sont aujourd'hui nombreuses, elles touchent généralement les trois composants suivants d'un système : la couche réseau, le système d'exploitation et la couche application.

De plus, beaucoup d'attaques peuvent infecter le réseau, voici quelques-une [7] :

1. **Attaque par déni de service (DoS) :** Le but d'une telle attaque n'est pas de dérober des informations sur une machine distante, mais de paralyser un service ou un réseau complet, c'est à dire, le rendre indisponible pendant un temps indeterminé. De ce fait, les utilisateurs ne peuvent plus accéder aux ressources.
   Les deux exemples principaux sont ; le « ping flood » ou l'envoie massif de courrier électronique pour saturer une boîte aux lettres (mailbombing). La meilleure parade est le firewall ou la répartition des serveurs sur un réseau sécurisé.

2. **Ecoute du réseau (sniffer) :** Il existe des logiciels qui permettent d'intercepter certaines informations qui transistent sur un réseau local, en transcrivant les trames dans un format plus lisible (Network packet sniffing). C'est l'une des raisons qui font que la topologie en étoile autour d'un hub n'est pas la plus sécurisée, puisque les trames qui sont émises en «broadcast» sur le réseau local peuvent être interceptées. De plus, l'utilisateurn'a auccun moyen de savoir qu'un pirate a mis son réseau en écoute.
   La meilleure solution est l'utilisation de mot de passe non rejouable, de carte à puce ou de calculette à mot de passe.

3. **Intrusion :** L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace et est donc une attaque. Le principal moyen pour prévenir les intrusions est le coupe-feu (Firewall en anglais). Il est efficace contre les fréquentes attaques de pirates amateurs, mais d'une efficacité toute relative contre des pirates expérimentés et bien informésne

politique de gestion des accès et des mots de passe est complémentaire.

4. **Cheval de troie :** Dans ce type d'attaque, le pirate, après avoir accédé à votre système ou en utilisant votre crédulité, installe un logiciel qui va à votre insu, lui transmettre par Internet les informations de vos disques durs. Un tel logiciel, aussi appelé troyen, peut aussi être utilisé pour générer de nouvelles attaques sur d'autres serveurs en passant par le votre. Certains d'entre eux sont des «key logger» c'est à dire qu'ils enregidtrent les frappes faites au clavier. La première mesure de protection face aux attaques est de sécuriser au maximum l'accès à votre machine et de mettre en service un antivirus régulièrement mis à jour. Un nettoyeur de troyens peut aussi s'avérer utile.

5. **Man in the middle :** Lorsqu'un pirate prend le contôle d'un équipement du réseau, se place au milieu d'une communication, il peut écouter ou modifier celle-ci, il peut falcifier les échanges afin de se faire passer pour l'une des parties communicantes. On parle de «l'homme du milieu» (man inthe middle en anglais).

6. **L'attaque IP spoofing :** Est une technique consistant à remplacer l'adresse IP de l'éxpediteur par l'adresse IP d'une autre machine. Le pirate commence par choisir le système qu'il veut attaquer, ensuite, après avoir obtenu le maximum de détails sur le système cible, il determine les adresses IP autorisés à se connecter au système cible.

1.2.4 Stratégies de sécurité

Pour faire face aux attaques citées ci-dessus, citons quelques solutions à ces dernières :

1. Cryptographie

La cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages. Elle utilise l'arithmétique pour chiffrer et déhiffrer les données, donc elle permet la protection des données stockées ou transmises à travers un réseau non sûr (comme Internet).

2. Antivirus

Principale cause de désagrément en entreprise, les virus peuvent être combattus à plusieurs niveaux. La plupart des antivirus sont basés sur l'analyse de signature des fichiers, la base des signtatures doit donc être très régulièrement mise à jour sur le site de l'éditeur [7].

3. Zone démilitarisée

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web ou un serveur de messagerie), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de «zone démilitarisée».

Une zone démilitarisées (ou DMZ en anglais demilitarized zone) est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet. Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité et les services susceptibles d'être accédés depuis Internet seront situés en DMZ.

La politique de sécurité mise en oeuvre sur la DMZ est généralement la suivante :
- Trafic du réseau externe vers la DMZ **autorisé** ;
- Trafic du réseau externe vers le réseau interne **interdit** ;
- Trafic du réseau interne vers la DMZ **autorisé** ;
- Trafic du réseau interne vers le réseau externe **autorisé** ;
- Trafic de la DMZ vers le réseau interne **interdit** ;
- Trafic de la DMZ vers le réseau externe **refusé** ;

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour stocker des données critiques pour l'entreprise.

Il est à noter qu'il est possible de mettre en place des zones dilitarisées en interme afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi les intrusions venant de l'intérieur.

4. La technologie AAA

Nous vivons dans un monde ou presque tout doit être protégé contre utilisation abusive ou impropre et/ou rien n'est gratuit. Que vous soyez administrateur système, responsable, ingénieur réseau ou étudiant, lorsque vous accédez à un réseau, vous êtes toujours confronté aux trois aspects suivant :

Authentification (Authentification) : C'est la procédure qui consiste, pour un système informatique à vérifier l'identité d'une personne ou d'un ordinateur afin d'autoriser l'accès de cette entité à des ressources (système, réseaux, application...). L'authentification permet donc de valider l'authenticité de l'entité en question.

Autorisation (Autorisation) : C'est la fonction spécifiant les droits d'accès vers les ressources liées à la sécurité de l'information et la sécurité des systèmes d'information en général et au contrôle d'accès en particulier.

Comptabilité (Accounting) : Elle permet de collecter des informations sur les utilisateurs et les actions qu'ils accomplissent lorsqu'ils sont connectés aux équipements du réseau.

5. Les VLANs (Virtual Area Network)

Un VLAN ou Virtual LAN, en français, réseau local virtuel, est un réseau local regroupant un ensemble de machine de façon logique et non physique.

Parmis les raisons d'utilisation des VLANs ; l'optimisation de l'utilisation de la bande passante, l'augmentation de la sécurité et l'administration des réseaux.

Dans un réseau local, la communication entre différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce aux critères (adresse MAC, numéros de port,etc).

Selon ces derniers, plusieurs types de VLANs sont définis :

VLAN par port : Les VLANs de niveau 1, définissent un réseau virtuel en fonction des ports de raccordement sur le commutateur. On peut donc regrouper les systèmes en fonction du port sur lequel ils sont connectés ;

VLAN par adresse IEEE : Les VLANs de niveau 2 aussi appelé VLAN MAC, consiste à définir un réseau virtuel en fonction des adresses MAC ;

VLAN par protocole : Les VLANs de niveau 3 permettent de créer un réseau virtuel par type de protocole (TCP/IP, IPX...). Dans ce cas, la communication ne se fera qu'entre les machines qui utilisent le même protocole ;

VLAN par sous-réseau : Les VLANs de niveau 3, associent des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure ou la configuration des commutateurs se modifient automatiquement en cas de déplacement d'une station.

6. Pare-feu

C'est une machine dédiée au routage entre LAN et Internet, le trafic est analysé au niveau des datagrammes IP (adresse, utilisateur, contenu...). Un datagramme non autorisé sera simplement détruit.

1.3 Conclusion

Ce chapitre a été constitué de deux parties ; la première s'intitulant «Généralités sur les réseaux» qui nous a permis de définir les réseaux, leur rôles, leur fonctionnement et leur différents types. La deuxième partie «Sécurité informatique» consiste à dégager quelques définitions basiques sur la sécurité, les attaques d'une part et les solutions contre ces dernières d'autre part.

Parmis les solutions proposées, on trouve les pare-feu (Firewalls en anglais) que nous allons détailler dans le chapitre qui suit.

Chapitre 2

Les pare-feu

2.1 Introduction

Tout ordinateur connecté à Internet ou à n'importe quel réseau informatique est susceptible d'être victime d'une intrusion, donc le besoin de le sécuriser est sans doute fondamentale, de ce fait, mettre en place un pare-feu est nécessaire car il est conçu pour protéger les données d'un réseau, que se soit protéger un ordinateur personnel relié à Internet ou protéger un réseau d'entreprise. Dans ce présent chapitre, nous allons présenter la notion des pare-feu d'une manière générale.

2.2 Définition d'un pare-feu

Un pare-feu ou Firewall en anglais est parfois appelé coupe-feu, garde-barrière où barrière de sécurité. En informatique l'usage du terme «pare-feu» est métaphorique : il évoque une porte empêchant les flammes d'Internet d'entrer chez soi et/ou de « contaminer » un réseau informatique [3].

C'est un logiciel ou un matériél qui vérifie les informations provenant d'Internet ou d'un réseau, puis les empêche d'accéder à l'ordinateur ou les y autorise, selon la configuration qui lui a été donné. Il gère les flux entrants et les flux sortans [7].

2.3 Rôle des pare-feu

Le pare-feu consiste à protéger le réseau de l'entreprise des intrusions extérieures. Ces dispositifs filtrent les trames (contenant des données) des différentes couches du modèle OSI (Open System Interconnection) afin de contrôler ler flux et de les bloquer en cas d'attaques, celles-ci pouvant prendre plusieurs formes. Le filtrage réalisé par le pare-feu constitue le premier rempart de la protection du système informatique.

Un pare-feu est installé le plus souvent en périphérie du réseau local de l'entreprise ce qui lui permet de contôler l'accès aux ressources externes depuis l'intérieur mais également entre les entités éloignées de l'entreprise mais reliées par un réseau de type extranet. Il existe différents types de pare-feu selon leur fonction. Ils peuvent opérer sur les niveaux 3, 4 et 7 du modèle OSI.

Indépendamment ou en complément d'une architecture utilisant ces dispositifs, il existe des services additionnels tel que : la traduction d'adresses réseau (Network Address Translation ou NAT), le protocole DHCP (Dynamis Host Configuration Protocol) et les réseaux privés virtuels (Virtual Private Networks ou VPN).

Les pare-feu permettent le filtrage de l'accès au réseau interne, afin d'empêcher l'accès non autorisé à l'ensemble des serveurs du réseau de l'entreprise. Il s'agit de contôler les flux entrants et sortants sur le réseau, la figure (Fig 2.1) nous montre les connexions autorisées avec une ligne de couleur verte et les connexions interdites en couleur rouge. Ils sont considérés comme la première ligne de défense et la principale dans le cadre de la protection du réseau d'une entreprise [8].

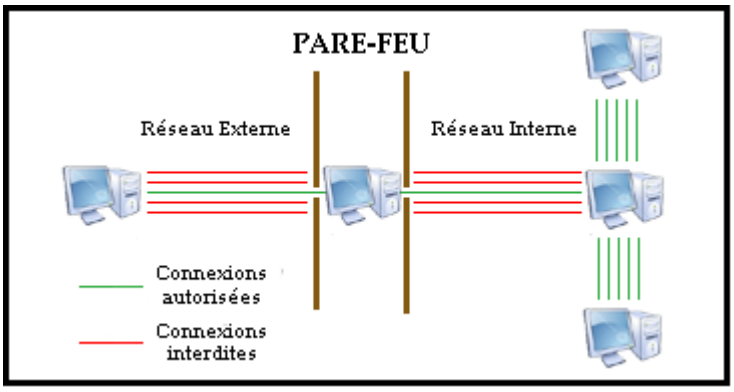

Fig. 2.1: Connexions autorisées et interdites par le pare-feu.

2.4 Fonctionnement d'un pare-feu

Lorsqu'on est connecté à Internet, notre ordinateur peut-être à tout moment la cible d'une attaque. Hormis le mythe du hackeur qui pirate notre ordinateur, sachons que nous pouvons tout simplement infecter notre machine en cliquant sur un lien WEB ou en ouvrant un mail.

Le filtrage peut se faire sur les adresses IP, les ports ou les applications. Le pare-feu fonctionne avec des règles, concrètement, si nous donnons pas explicitement le droit à une application d'accéder à internet, celle-ci sera bloquée.

Lorsque des connexions sont établies, le pare-feu va examiner ces dernières. Selon les règles établies, il autorisera ou bloquera les connexions. Nous avons la possibilité de créer des règles sur les ports. Par exemple, nous pouvons créer une règle qui accepte les connexions vers le port 20 et 21 si nous avons un serveur FTP sur notre machine. Ainsi, n'importe qui pourra se connecter à notre serveur FTP.

Nous avons aussi la possibilité de combiner un filtrage sur les ports et sur les adresses IP. Cela peut être intéressant si par exemple, nous installons une application sensible comme VNC (Virtual Network Computing) qui permet de partager notre bureau. Ainsi, nous pouvons filtrer les

connexions sur le port ET sur l'adresse IP de la personne qui aura accès à notre bureau partagé. Ce qui permet de garder énormément en sécurité puisqu'une seule personne (de confiance !) aura accès à VNC, dès lors même si une faille sur VNC est publiée, le risque de se faire hacker est réduit [9].

2.5 Scénarios d'attaques (Pénétrations de réseaux)

Qu'est-ce qu'une backdoor ? Une backdoor est un accès <caché> sur votre système qui permet à un pirate d'en prendre le contrôle à distance. Il existe une multitude de sortes de backdoor, et en général dans ce domaine, l'imagination des pirates rivalise avec l'incrédulité des utilisateurs. Voici quelques scénarios d'attaques [6] :

2.5.1 Premier cas (Pas de protection)

Considérons un ordinateur victime sur lequel on a installé une backdoor en exploitant une des failles du système. L'attaquant a alors la possibilité d'utiliser tous les services présents sur cet ordinateur. Il lui suffit d'envoyer ses ordres à la backdoor et de récupérer les réponses.

2.5.2 Deuxième cas (Filtrer les flux entrants illégaux)

La sécurité de notre système ne nous semblant pas infaillible, nous décidons alors d'installer un pare-feu avec états (Un Firewall sans état nous semblant quelque peu léger). Le trafic entrant est maintenant stoppé comme il se doit. Malheureusement, le pirate étant rusé et malicieux, il a pris soin de s'arranger pour que sa backdoor initie elle-même les sessions. Du coup le Firewall laisse passer les requêtes de l'attaquant qui sont considérées comme des réponses par celui-ci.

2.5.3 Troisième cas (Bloquer les flux entrants et sortants)

Dans le cas précédent, le problème était dû aux flux sortants qui permettait au cheval de Troie d'initier les sessions avec la machine de l'attaquant. Il s'agit donc de bloquer les flux sortants. Pour cela la défense insère donc un proxy afin de contrôler ce qui sort du réseau. Malheureusement le trojan peut encore sortir, certes avec plus de difficultés puisqu'il devra se renseigner sur les flux autorisés à sortir par le proxy, et les utiliser pour passer le proxy. Par exemple on peut encapsuler des ordres dans du HTTP, dans du SSL, DNS.

2.6 Les techniques et outils de découvertes de pare-feu

Il existe beaucoup d'outils et beaucoup de techniques permettant d'identifier un pare-feu. Il est évident que la plupart des outils utilisés par les pirates pour découvrir les pare-feu sont utilisables pour une activité tout aussi louable telle que la vérification du bon fonctionnement du firewall et de la robustesse du réseau.

Dans un premier temps il convient de localiser le ou les pare-feu, ensuite l'attaquant cherchera à identifier le pare-feu, soit en espérant exploiter une faille même du pare-feu, soit il cherchera à identifier les règles du pare-feu afin d'y détecter une faille dans le filtrage de paquet. Pour identifier les règles d'un pare-feu, il faut utiliser un scanner de port. Il existe de nombreux scanner de ports, les plus connus sont Firewalk, Nmap et Hping2 [6].

2.7 Configuration théorique des défenses

Il existe deux politiques de configurations différentes en ce qui concerne le pare-feu ; la première consiste à tout autoriser sauf ce qui est dangereux : cette méthode est beaucoup trop laxiste. En effet, cela laisse toute latitude à l'imagination des intrus de s'exprimer. Et à moins d'avoir tout prévu de façon exhaustive, on laissera forcément des portes ouvertes, des failles béantes dans notre système. A éviter absolument.

La deuxième consite à tout interdire sauf ce dont on a besoin et ce en quoi on a confiance : cette politique est beaucoup plus sécuritaire. En effet, les services sont examinés avant d'être autorisés à passer le firewall, et sont donc tous soumis à un examen plus ou moins approfondi. Ainsi, pas de mauvaise surprise sur un service que l'on pensait ne pas avoir installé, plus d'oubli : tout service autorisé est explicitement déclaré dans le firewall. Cette politique s'accompagne de la création de deux zones : une zone interne et l'extérieur. On peut considérer que tout ce qui est dans notre réseau local est autorisé, sans prendre de trop gros risques : le firewall est là pour nous protéger des attaques extérieures [6].

2.8 Les différents types de filtrages

Il existe trois types de filtrage, le filtrage simple de paquets, le filtrage de paquet avec état et le filtrage applicatif [6].

2.8.1 Le filtrage simple de paquet

Le filtrage simple de paquet ou Stateless en anglais est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accoder ou refuser le passage de paquet d'un réseau à un autre en se basant l'adresse IP Source/Destination, le numéro de port Source/destination et le protocole de niveau 3 ou 4.

Ce type de filtrage ne résiste pas à certaines attaques de type IP-Spoofing et les attaques de type DoS.

2.8.2 Le filtrage de paquets avec état

Le filtrage de paquets avec état ou Stateful en anglais, l'amélioration par rapport au filtrage simple est la conservation de la trace des sessions et des connexions dans des tables d'états internes au pare-feu. Ce filtrage permet de se protéger face à certains types d'attaques DoS.

La limite de ce filtrage est que lorsque l'accès à un service a été autorisé, il n'y a aucune contôle effectué sur les requêtes et les réponses des clients et serveurs.

2.8.3 Le filtrage applicatif

Le filtrage applicatif ou pare-feu de type proxy est comme son nom l'indique réalisé au niveau de la couche application. pour cela, il faut bien-sûr pouvoir extraire les données du protocole de niveau

7 pour les étudier. Les requêtes sont traités par des processus dédiés, par exemple une requête de type HTTP sera filtrée par un processus proxy HTTP. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

Le problème qui se pose dans ce type de filtrage est la finesse du filtrage réalisé par le proxy, c'est à dire qu'il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7. En outre, le fait de devoir connaître les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles. Mais il est indéniable que le filtrage applicatif apporte plus de sécurité que le filtrage de paquet avec état.

2.9 Les différents types de pare-feu

Il existe trois type de pare-feu qui sont les suivants :

2.9.1 Les pare-feu bridge

Les pare-feu bridge agissent comme des câbles réseau avec la fonction de filtrage en plus, leurs interfaces ne possèdent pas d'adresse IP et ne font que transférer les paquets d'une interface à une autre. Cette absence d'adresse IP est particulièrement utile, car cela signifie que le pare-feu est indétectable pour un haker lambda.

En effet, quand une requête est émise sur la câble réseau, le pare-feu bridge ne répondra jamais, car ses adresses MAC ne circulerontjamais sur le réseau, et comme il ne fait que transmettre les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirrigé contre le pare-feu. Parmi ses avantages on trouve qu'il est impossible de l'éviter puisque les paquets passeront par ses interfaces et il est peu coûteux, par contre sa configuration est souvent contraignante [6].

2.9.2 Les pare-feu matériels

Les pare-feu matériels se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco. Intégrés directement dans la machine. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau, ils sont intégrés au matériel réseau avec une administration relativement simple et ils ont un bon niveau de sécurité mais ils dépendent du constructeur pour les mises à jour [6].

2.9.3 Les pare-feu logiciels

Les pare-feu logiciels sont présents à la fois dans les serveurs et les routeurs, nous pouvons les classer en deux catégories ; les pare-feu personnels et les pare-feu plus sûr.

Les pare-feu personnels sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés.

Les pare-feu nommé plus-sûr tournent généralement sous linux, car ils offrent une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les pare-feu matériels des routeurs. Le plus courant est iptables (anciennement ipchains), qui utilise directement le noyau linux. Toute fonctionnalité des firewalls de routeurs est potentiellement réalisable sur une telle plateforme [6].

2.10 Conclusion

Après avoir fait une étude approfodie sur les pare-feu, nous arrivons à conclure qu'à l'heure où les infections se multiplient, accouplé à un antivirus, l'utilisation d'un pare-feu filtrant les connexions entrantes et sortantes devient incontournable.

Chapitre 3

Organisme d'acceuil

3.1 Introduction

Actuellement la puissance d'un pays se mesure essentiellement par sa part de participation au marché internationnal. Ainsi, Sonatrach est considérée comme l'un des paliers les plus importants de l'industrie.

Dans ce chapitre, nous allons présenter le groupe Sonatrach ainsi que sa structure hiérarchique, ensuite nous exposerons la problèmatique suivie de la solution proposée, puis nous allons concevoir les architectures LANs tout en désignant les équipements et les interfaces que nous utiliserons.

3.2 Présentation de Sonatrach

Sonatrach(Société Nationale pour la Recherche, la Production, le Transport, la Transformation, et la Commercialisation des Hydrocarbures) est une entreprise publique algérienne d'envergure internationale et un acteur majeur de l'industrie pétrolière, c'est la clé de voûte de l'économie algérienne.

Le groupe pétrolier et gazier Sonatrach intervient dans l'exploration, la production, le transport par canalisation, la transformation et la commercialisation des hydrocarbures et de leurs dérivés.

3.3 Structure de Sonatrach

Pour un bon fonctionnement de SONATRACH, celle-ci a été divisée en cinq branches principales, représentées par l'organigramme suivant (Fig 3.1) :

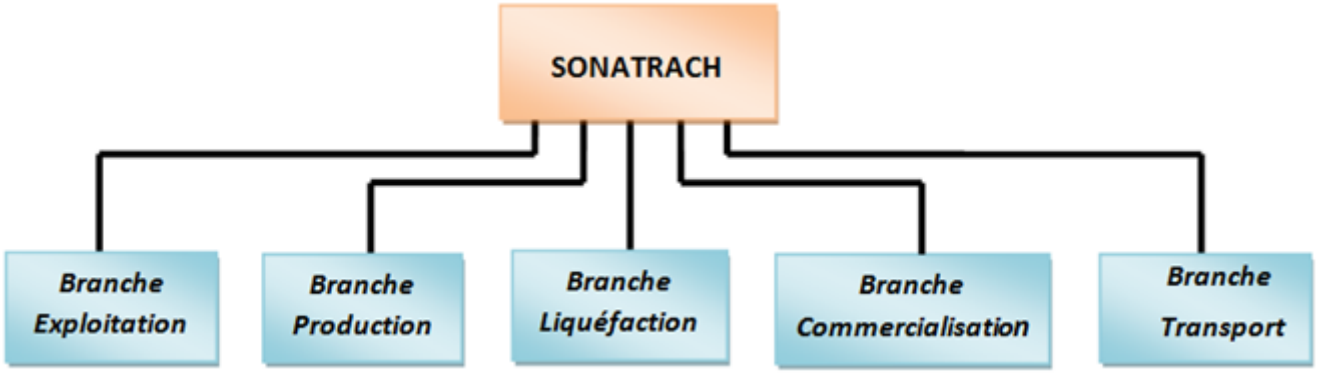

FIG. 3.1: Branches de Sonatrach

3.4 Directions régionales de Sonatrach

La Sonatrach possède cinq directions régionales de transport des hydrocarbures :

1. RTO : Région Transport Ouest(Arzew) ;
2. RTH : Région Transport Haoud El Hamra (Centre distribution) ;
3. RTE : Région Transport Est(Skikda) ;
4. RTC : Région Transport Centre(Béjaia) ;
5. RTI : Région Transport In Amenas.

3.5 Présentation de l'activité transport par canalisation (TRC)

L'activité de transport par canalisation (TRC) est en charge de l'acheminement des hydrocarbures (pétroles brut, gaz et condensat) vers les ports pétroliers, les zones de stockages et les pays d'exploitation.

Les différentes tâches de la branche de transport par canalisation sont :

- Stockage d'hydrocarbures liquides et gazeux en amont et en aval ;
- Le chargement des navires pétroliers ;
- Transport par canalisation d'hydrocarbures liquides gazeux, depuis les lieux de la production primaires, à travers le réseau secondaire et principal ;
- La coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation ;
- La maintenance, l'entretien et la protection des ouvrages et canalisation ;
- L'exécution des révisions générales, des machines tournantes et équipements ;
- La conduite des études, la réalisation et la gestion des projets de développement des ouvrages et canalisations.

3.6 Direction régionale de transport de Bejaia (DRGB)

La direction régionale de transport de Bejaia (DRGB) est l'une des cinq directions régionales de transport des hydrocarbures de la SONATRACH (TRC). Sa structure générale est défini dans la figure suivante :

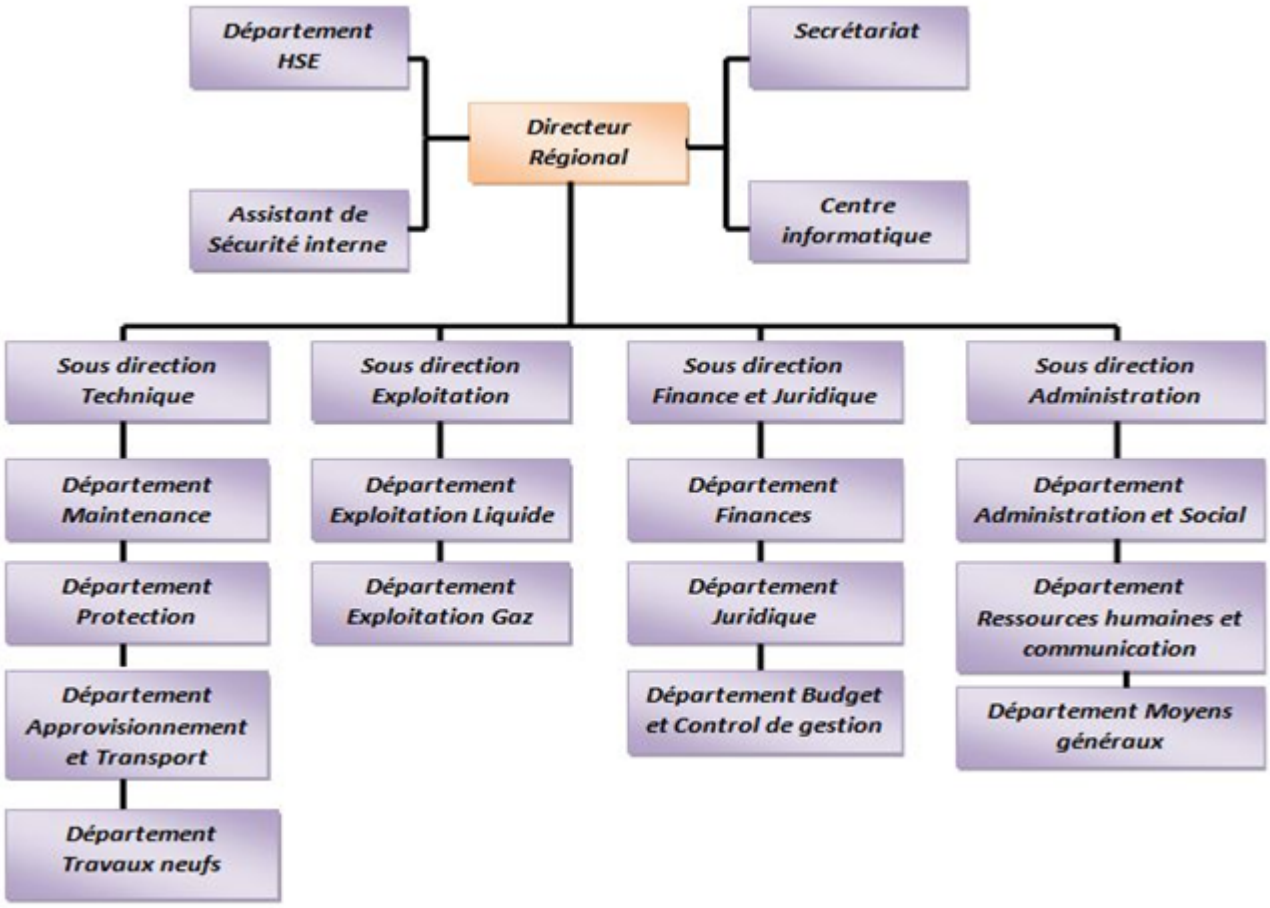

Fig. 3.2: Structure de la DRGB.

Direction régionale : Dirigée par un directeur régional aidé par des assistants et un secrétaire.

Département HSE : Il est composé de trois services ; service prévention, service intervention et service environnement et santé du travail.

Secrétariat : Il s'agit du sercrétariat de la direction (directeur).

Assistant de sécurité interne : A pour rôle d'assurer la sécurité et la sauvegarde du patrimoine humain et matériel de la DRGB.

Centre informatique : Il regroupe les moyens d'exploitation et de développement des applications informatiques ainsi que la gestion du réseau informatique interne.

Sous direction Technique : Elle a pour mission d'assurer la maintenance et la protection des ouvrages ainsi que l'approvisionnement, l'étude et le suivi de projets de réalisation de travaux neufs. Elle est constitué en quatre départements : département maintenance, département

protection des ouvrages, département approvisionnement et transport et département des travaux neufs.

Sous direction Exploitation : Elle est chargée de l'exploitation des installations de la région, et la maintenance du fonctionnement des trois ouvrages en effectuant des réparations en cas de fuite, de Sabotage ou de panne pour les stations de pompage. Elle comporte deux départements : le département exploitation liquide et le département exploitation gaz.

Sous direction Finances et juridique : Elle a pour mission d'effectuer la gestion financière, le budget et le contrôle de gestion et de prendre en charge les affaires juridiques de la DRGB. Elle est constituée de trois départements : département finances, département juridique, département budget et contrôle de gestion.

Sous direction Administration : Elle a pour mission la gestion des ressources humaines et les moyens généraux. Elle est organisée en trois départements : département administration et social, département ressources humaines et communication, département moyens généraux.

3.7 Présentation du centre informatique

Le centre informatique est chargé du développement et de l'exploitation des applications informatiques afin d'assurer la gestion de la direction régionale de Bejaïa (DRGB) et des autres régions.

3.7.1 Structure du centre informatique

La structure du centre informatique n'a cessé de connaitre des changements et ceux ci sont du à l'évolution du domaine informatique qui exige d' apporter de nouvelles fonctionnalités afin d'assurer les besoins de l'entreprise. Actuellement, l'organisation du centre informatique est la suivante :

Fig. 3.3: Structure du centre informatique.

3.7.2 Tâches des différents serivces informatiques

Chaque service a sa propre fonction, nous allons définir et citer les différentes taches de chacun comme suit :

Service système et réseaux

Le service système et réseaux assure les tâches suivantes :
- Choix des équipements informatiques et logiciels de base ;
- Mise en oeuvre des solutions matériels et logicielles retenues ;
- Installation et configuration des systèmes ;
- Orienter les travaux de l'équipe de développement par une bonne utilisation des ressources de l'ordinateur ;
- Assure le bon fonctionnement, la fiabilité des communications, l'administration du réseau et organise l'évolution de sa structure ;
- Conduite de l'étude pour le choix de l'architecture du réseau à installer ;
- Participer à la mise en place des réseaux ;
- Définir les droits d'accès à l'utilisation du réseau ;
- Assurer la surveillance permanente pour détecter et prévenir les pannes ;
- Traitement des dysfonctionnements et incidents survenant sur le réseau.

Service bases de données et logiciels

Ce service à son tour assure les tâches suivantes :
- Conçoit les bases de données et assure l'optimisation et le suivi de la gestion des données informatiques ;
- Installer, configurer et exploiter le SGBD et ses bases ;
- Mise en oeuvre et gestion des procédures de sécurité (accès, intégrité) ;
- Gérer la sauvegarde, la restauration et la migration des données ;
- Assurer la cohérence et la qualité des données introduites par les utilisateurs ;
- Etude et conception de système d'information ;
- Développement et maintenance des applications informatiques pour TRC ;
- Déploiement des applications et formation des utilisateurs.

Service support technique

Ce service garantie les tâches suivantes :
- Assistance aux utilisateurs en cas de problèmes software et hardware ;
- Installation des logiciels de gestion, technique et bureautique ;
- Formation aux nouveaux produits installés .

3.8 Problématique

Aujourd'hui, les réseaux informatiques sont devenus incontournables, ils sont omniprésents dans toutes les entreprises. Sonatrach est une entreprise constituée de plusieurs sites distants permettant l'échange des données qui doit être de façon sécurisée sans qu'un intrus puisse altérer l'information interne du réseau. Actuellement Sonatrach se base sur les adresses MAC afin de sécuriser son réseau.

La question qui se pose est : est-ce qu'il existe une autre solution pour protéger un réseau informatique des intrusions indésirables ?

3.9 Solution proposée

L'objectif de notre projet est la simulation d'un pare-feu d'entreprise dans le but de filtrer les communications autorisées ou non entre deux sites informatiques de l'entreprise Sonatrach.

Pour cela nous avonçu une architecture qui sera présenté dans le chapitre suivant, cette dernière est composé de huit sites distants. Pour notre cas, nous nous sommes localisé sur le site de Bejaia que nous avons munis d'un pare-feu pour le sécuriser.

Un pare-feu est un élément du réseau informatique, logiciel et/ou matériel qui est aujourd'hui incontournable dans la sécurité de tout système informatique car il permet d'appliquer une politique d'accès aux ressources informatiques. Il a pour principale tâche de contrôler le trafic entre les différentes zones de confiance en filtrant les flux de données qui y transitent.

3.10 Présentation générale du modèle

Notre modèle type se compose de huit réseaux locaux ou chacun représente un site de Sonatrach.Chaque site est consitué d'un serveur, d'un nombre de machines reliées à un switch qui est connécté à un routeur, chaque routeur de chaque site est lié au routeur coeur du réseau.

3.11 Présentation des équipements utilisés pour la simulation

Les équipements réseau utilisés sont presentés dans le tableau (Tab 3.1).

Les équipements	**La marque et le type**
Switch	Cisco catalyst 2960
Routeur	cisco Router-PT
Sécurité (pare-feu)	ASA 5505

Tab. 3.1: Présentation des équipements.

3.12 Nomination des équipements utilisés

Nous nominons les équipements par des noms significatifs pour faciliter la conception de l'architecture de chaque site. Les switchs d'accès seront nominé avec des abréviations des différentes station de pompage de la Sonatrach, par exemple : Station de pompage numéro 1 (050-SP1-SW). Le tableau (Tab 3.2) résume les noms des équipements utilisés pour effectuer l'architecture réalisée.

Sonatrach de Béjaia	Routeur	Switch	Stations
Sonatrach PP	002-PP-RO	002-PP-SW	002-PP-ST1 / 002-PP-ST2 / 002-PP-ST3
Sonatrach BBM	010-BBM-RO	010-BBM-SW	010-BBM-ST1 / 010-BBM-ST2 / 010-BBM-ST3
Sonatrache El-Oued	050-SP1Bit-RO	050-SP1Bit-SW	050-SP1Bit-ST1 / 050-SP1Bit-ST2 / 050-SP1Bit-ST3
Sonatrach Biskra1	041-SPB-RO	041-SPB-SW	041-SPB-ST1/041-SPB-ST2/041-SPB-ST3
Sonatrach Biskra2	040-SP2-RO	040-SP2-SW	040-SP2-ST1 / 040-SP2-ST2 / 040-SP2-ST3
sonatrach M'sila	030-SP3-RO	030-SPB-SW	030-SPB-ST1 / 030-SPB-ST2 / 030-SPB-ST3
Sonatrach Bouira	020-SBM-RO	020-SBM-SW	020-SBM-ST1 / 020-SBM-ST2 / 020-SBM-ST3

Tab. 3.2: Nomination des équipements.

3.13 Désignation des interfaces et la table d'adressage

Les interfaces des différents routeurs des différents sites sont indiqués dans le tableau suivant (Tab3.3).

Dispositif	**Interface**	**Adresse IP**	**Subnet Mask**	**Passerelle**	**Serveur DNS**
Routeur-Béjaia	Se 2/0	209.165.200.226	255.255.255.252	/	/
Routeur-Béjaia	Fa 0/0	209.165.200.254	255.255.255.240	/	/
Routeur-Internet	Se 2/0	209.165.200.225	255.255.255.252	/	/
Routeur-Internet	Se 3/0	192.31.4.1	255.255.255.252	/	/
Routeur-Internet	Se 4/0	192.31.5.1	255.255.255.252	/	/
Routeur-Internet	Se 5/0	192.31.6.1	255.255.255.252	/	/
Routeur-Internet	Se 6/0	192.31.7.1	255.255.255.252	/	/
Routeur-Internet	Se 7/0	192.31.8.1	255.255.255.252	/	/
Routeur-Internet	Se 8/0	192.31.9.1	255.255.255.252	/	/
Routeur-Internet	Se 9/0	192.31.10.1	255.255.255.252	/	/
Routeur-Internet	Fa 0/0	192.135.250.1	255.255.255.0	/	/
Routeur 002-PP-RO	Se 2/0	192.31.4.2	255.255.255.252	/	/
Routeur 002-PP-RO	Fa 0/0	192.31.4.62	255.255.255.224	/	/
Routeur 010-BBM-RO	Se 2/0	192.31.5.2	255.255.255.224	/	/
Routeur 010-BBM-RO	Fa 0/0	192.31.5.62	255.255.255.224	/	/
Routeur SP1bit (El-Oued)	Se 2/0	192.31.6.2	255.255.255.252	/	/
Routeur SP1bit (El-Oued)	Fa 0/0	192.31.6.62	255.255.255.224	/	/
Routeur SPB (Biskra1)	Se 2/0	192.31.7.2	255.255.255.252	/	/
Routeur SPB (Biskra1)	Fa 0/0	192.31.7.62	255.255.255.224	/	/

Routeur SP2 (Biskra)	Se 2/0	192.31.8.2	255.255.255.252	/	/
Routeur SP2 (Biskra)	Fa 0/0	192.31.8.62	255.255.255.224	/	/
Routeur SP3 (M'sila)	Se 2/0	192.31.9.2	255.255.255.252	/	/
Routeur SP3 (M'sila)	Fa 0/0	192.31.9.62	255.255.255.224	/	/
Routeur SBM (Beni-Mansour)	Se 2/0	192.31.10.2	255.255.255.252	/	/
Routeur SBM (Beni-Mansour)	Fa 0/0	192.31.10.62	255.255.255.224	/	/
Serveur web (Site-Béjaia)	Fa 0/2	192.168.20.2	255.255.255.0	192.168.20.1	192.168.20.5
Serveur web (Site-Port Pétrolier)	Fa 0/2	192.31.4.35	255.255.255.224	192.31.4.62	192.135.250.5
Serveur web (Site-El-Oued)	Fa 0/2	192.31.6.35	255.255.255.224	192.31.6.62	192.135.250.5
Serveur web (Biskra1)	Fa 0/2	192.31.7.35	255.255.255.224	192.31.7.62	192.135.250.5
Serveur web (Biskra2)	Fa 0/2	192.31.8.35	255.255.255.224	192.31.8.62	192.135.250.5
Serveur web (M'sila)	Fa 0/2	192.31.9.35	255.255.255.224	192.31.9.62	192.135.250.5
Serveur web (Beni-Mansour)	Fa 0/2	192.31.10.35	255.255.255.224	192.31.10.62	192.135.250.5
Serveur web (BBM)	Fa 0/2	192.31.5.35	255.255.255.224	192.31.5.62	192.135.250.5
Serveur DNS (Public)	Fa 0/2	192.135.250.5	255.255.255.0	192.135.250.1	/

TAB. 3.3: Indication des interfaces des routeurs.

3.14 Conclusion

A travers ce chapitre, nous avons tout d'abord fait un aperçu sur l'entreprise d'acceuil qui est Sonatrach, par la suite nous avons exposé la problématique de cette dernière. Pour finir, nous avons présenté et nominé les équipements et les interfaces qu'on utilisera dans la phase réalisation qui est le chapitre suivant.

Chapitre 4

Réalisation

4.1 Introduction

Dans ce chapitre, nous allons passer à la dernière étape de notre travail qui est la réalisation de notre projet. Cette dernière est une cruciale pour la mise en place de tout ce que nous avons fait dans les précédents chapitres.

Nous implémenterons la solution précédemment proposée et conçu, pour ce faire, nous commencerons par la présentation du simulateur utilisé, puis nous expliquerons en détail les différentes étapes suivies pour la réalisation des réseaux LANs et nous finirons par la configuration du pare-feu.

4.2 Présentation de simulateur Cisco Packet Tracer

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipement tels que les routeurs, les commutateurs, les ordinateurs. Ces équipements doivent ensuite être reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc.

Le but de Packet Tracer est d'offrir aux étudiants et aux professeurs un outil permettant de créer des réseaux virtuellement [11].

La figure ci-dessous (Fig 4.1) montre un aperçu général de Packet Tracer. La zone (1) est la partie dans la quelle le réseau est construit. Les équipements sont regroupés en catégories accessibles dans la zone (2). Une fois la catégorie sélectionnée, le type d'équipement peut être sélectionné dans la zone (3), la zone (4) permet de passer du mode temps réel au mode simulation, la zone (5) permet d'ajouter des indications dans un réseau et la zone (6) contient un ensemble d'outils qui sont les suivants :

Select : Permet de déplacer ou d'éditer des équipements ;

Move layout : Permet de déplacer le plan de travail ;

Place note : Permet de placer des notes sur le réseau ;

Delete : permet de supprimer un équipement ou une note ;

Inspect : Permet d'ouvrir une fenêtre d'inspection (table ARP, routage) sur un équipement.

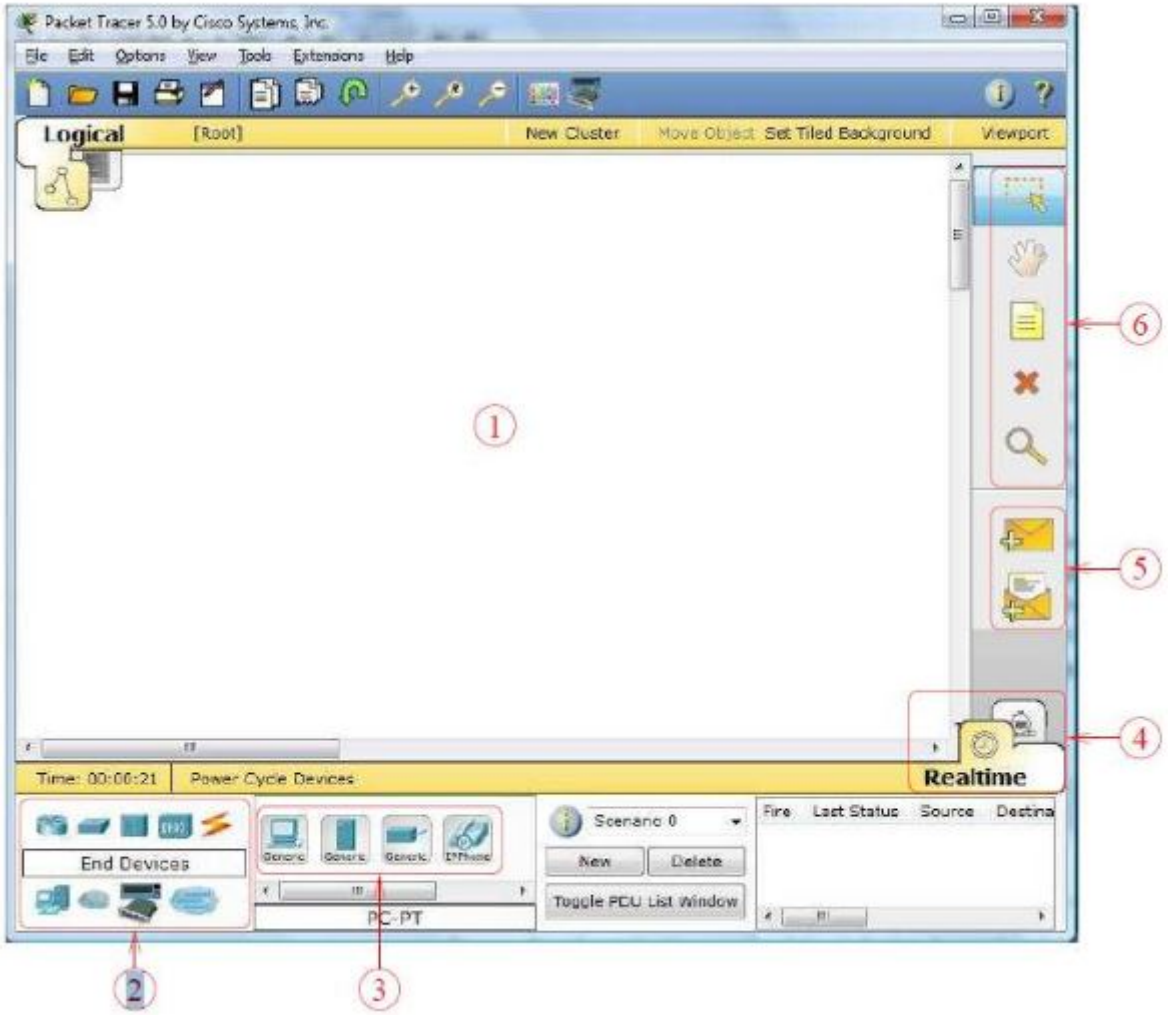

FIG. 4.1: Interface Cisco Packet Tracer.

4.3 Réalisation des architectures LANs

Avant de configurer le pare-feu qui est l'objectif de notre mémoire, nous sommes obligé de créer d'abord les architectures LANs. Ceci dit qu'à présent, nous allons lancer une série de configuration (la configuration des routeurs, des PCs et des serveurs), pour réaliser les neuf réseaux locaux de Sonatrach et une interconnexion de ces derniers.

4.3.1 Configuration des équipements

La configuration des équipements du réseau sera faite au niveau des commutateurs (niveau 2), et au niveau des routeurs (niveau 3), ainsi qu'au niveau des PCs et serveurs. En effet, une série de configuration sera réalisée sur ces équipements, en montrant des exemples de chaque configuration.

1. Configuration des commutateurs

Pour la configuration des commutateurs nous avons besoin de configurer des hostname et des mots de passe.

1. **Configuration des hostname :** Le but de cette configuration est de renommer les commutateurs par des noms significatifs comme le montre la figure ci-dessous (Fig 4.2). Nous prendrons comme exemple de configuration le switch du port pétrolier de Bejaia. Sachant que c'est la même chose pour tout les autre switchs.

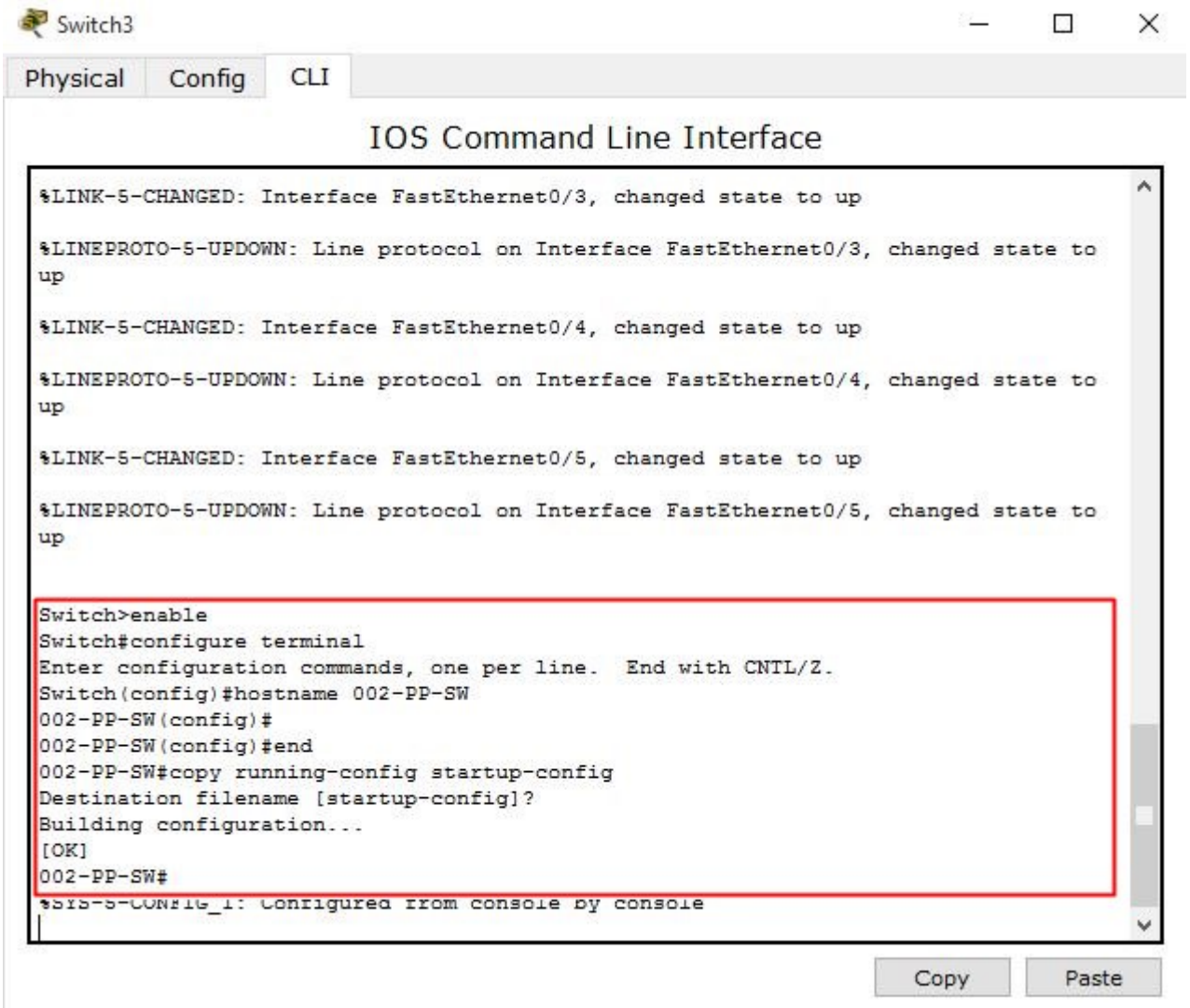

Fig. 4.2: Nomination du Switch de port pétrolier de Bejaia.

2. **Configuration des mots de passe :** Nous avons choisi "sonatrach" comme mot de passe via la console. L'exemple que nous prendrons est le switch de port pétrolier de Bejaia. La figure (Fig 4.3) montre les commandes de mise en place du mot de passe. La même chose sera faite pour tous les autres switchs.

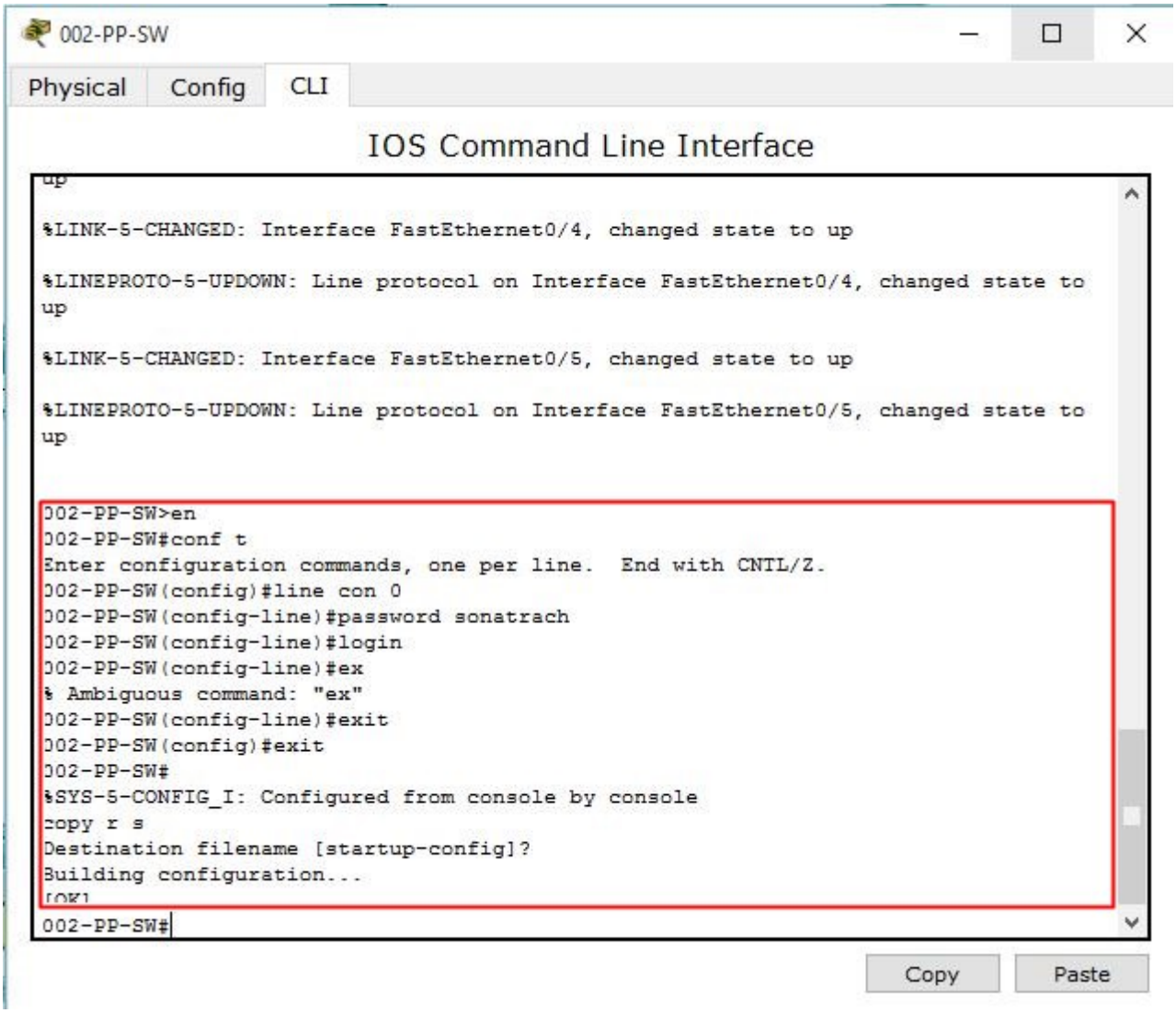

FIG. 4.3: Attribution des mots de passe.

2. Configuartion des routeurs

Pour la configuration des routeurs, nous allons commencer par la configuration des interfaces ensuite la configuration de routage EIGRP. Les hostnames et les mots de passe sont configurés de la même façon que les commutateurs.

1. **Configuration des interfaces :** Dans cette étape nous allons attribuer les adresse IP aux interfaces des routeurs et les activer par la suite. La figure (Fig 4.4) illustre cette configuration.

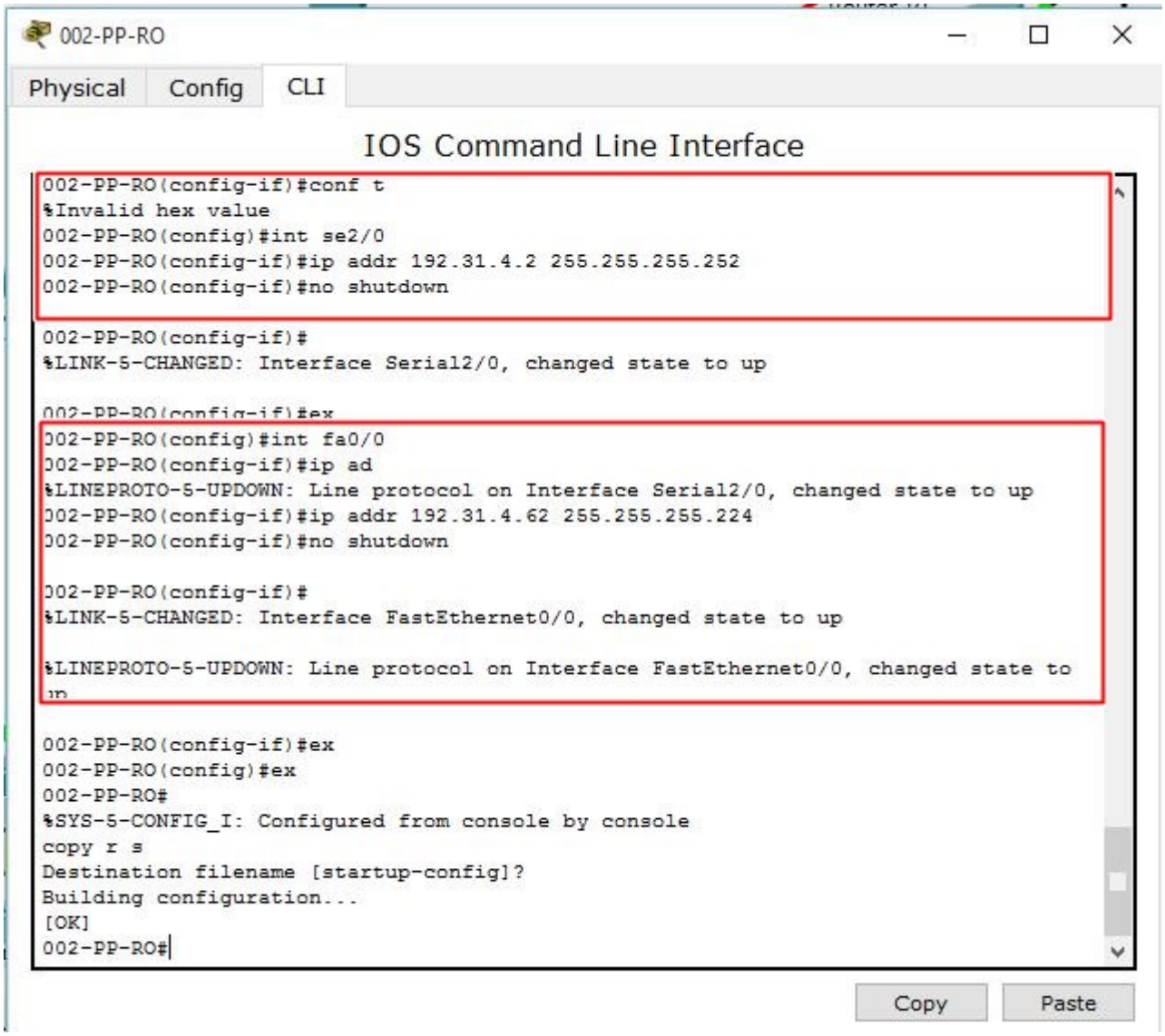

FIG. 4.4: Adressage et activation des interfaces du routeur port pétrolier.

2. **Configuration de routage EIGRP :** A présent, nous allons configurer le protocole de routage EIGRP au niveau des routeurs, on prend par exemple la configuration de routage EIGRP sur le routeur de port pétrolier de Bejaia comme l'illustre la figure (Fig 4.5). La même chose sera faite pour tous les autres switchs.

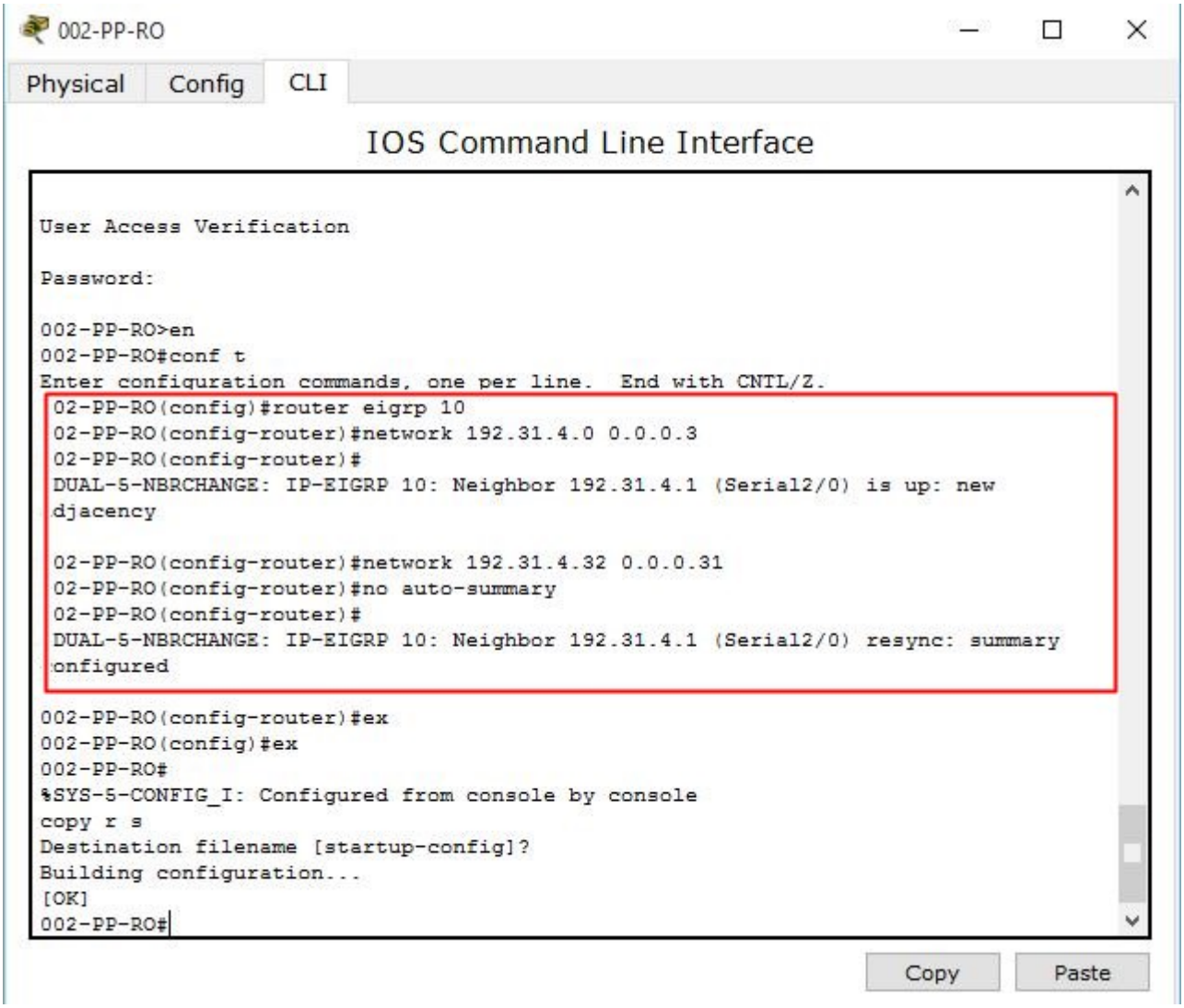

FIG. 4.5: Activation de protocole EIGRP sur le routeur port pétrolier.

3. Configuration des serveurs et des PCs

Dans cette étape de configuration, nous allons configurer les serveurs web, les serveurs DNS, ainsi que les PCs.

1. **Configuration des serveurs DNS :** Un serveur DNS assure la résolution de noms des réseaux TCP/IP. En d'autres termes, il permet aux utilisateurs d'ordinateurs clients d'adopter des noms à la place des adresses IP numériques pour identifier les hôtes distants [12]. Les étapes de configuration de serveur DNS sont illustrées par les figures (Fig 4.6) et (Fig 4.7) qui représentent l'attribution d'une adresse au serveur et les étapes de configuration du serveur DNS numérotées de 1 jusqu'à 6 respectivement. Nous prenons l'exemple d'un seul serveur, sachant que la même chose sera appliquée pour les autres serveurs.

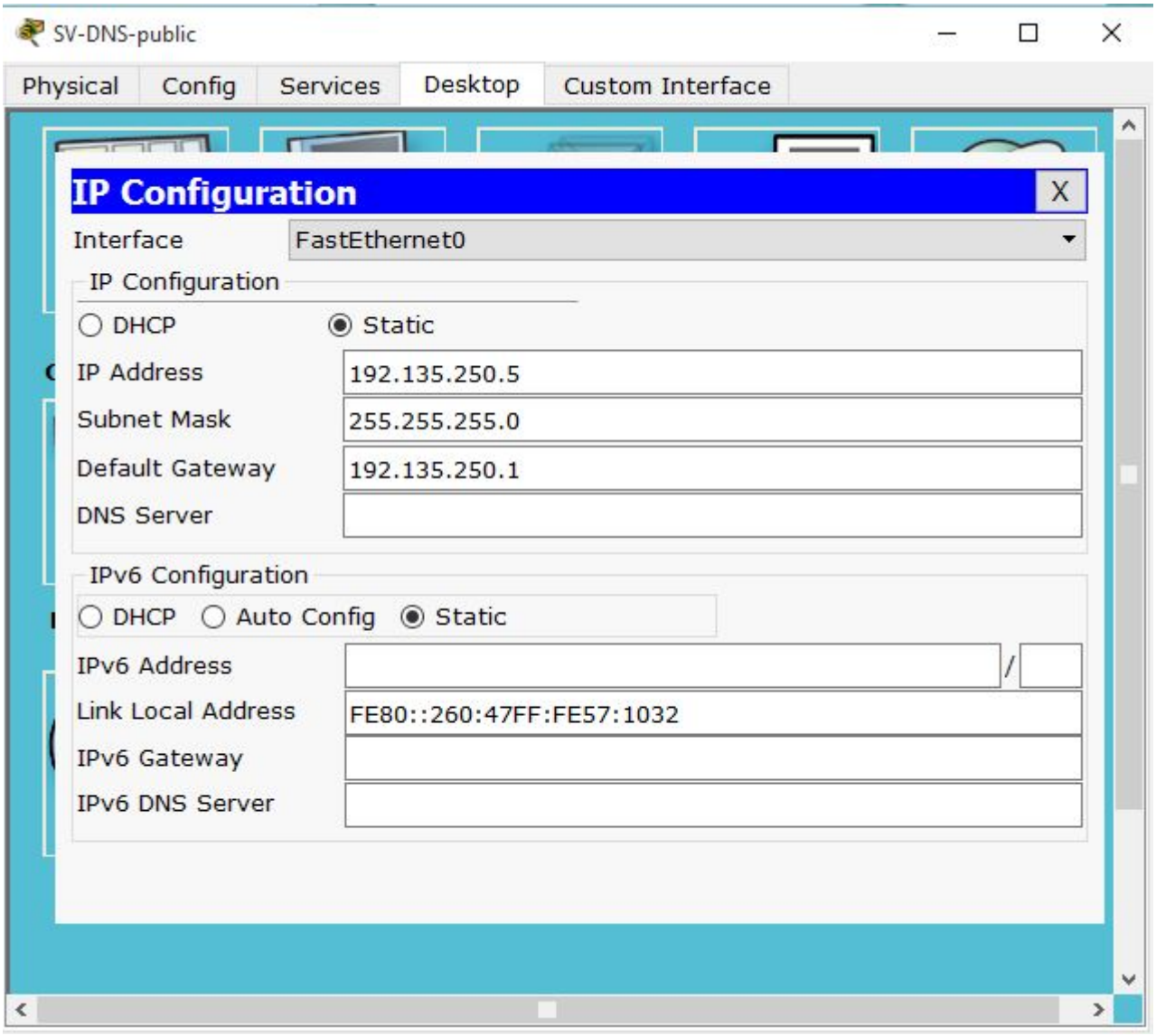

FIG. 4.6: Attribution d'une adresse au serveur.

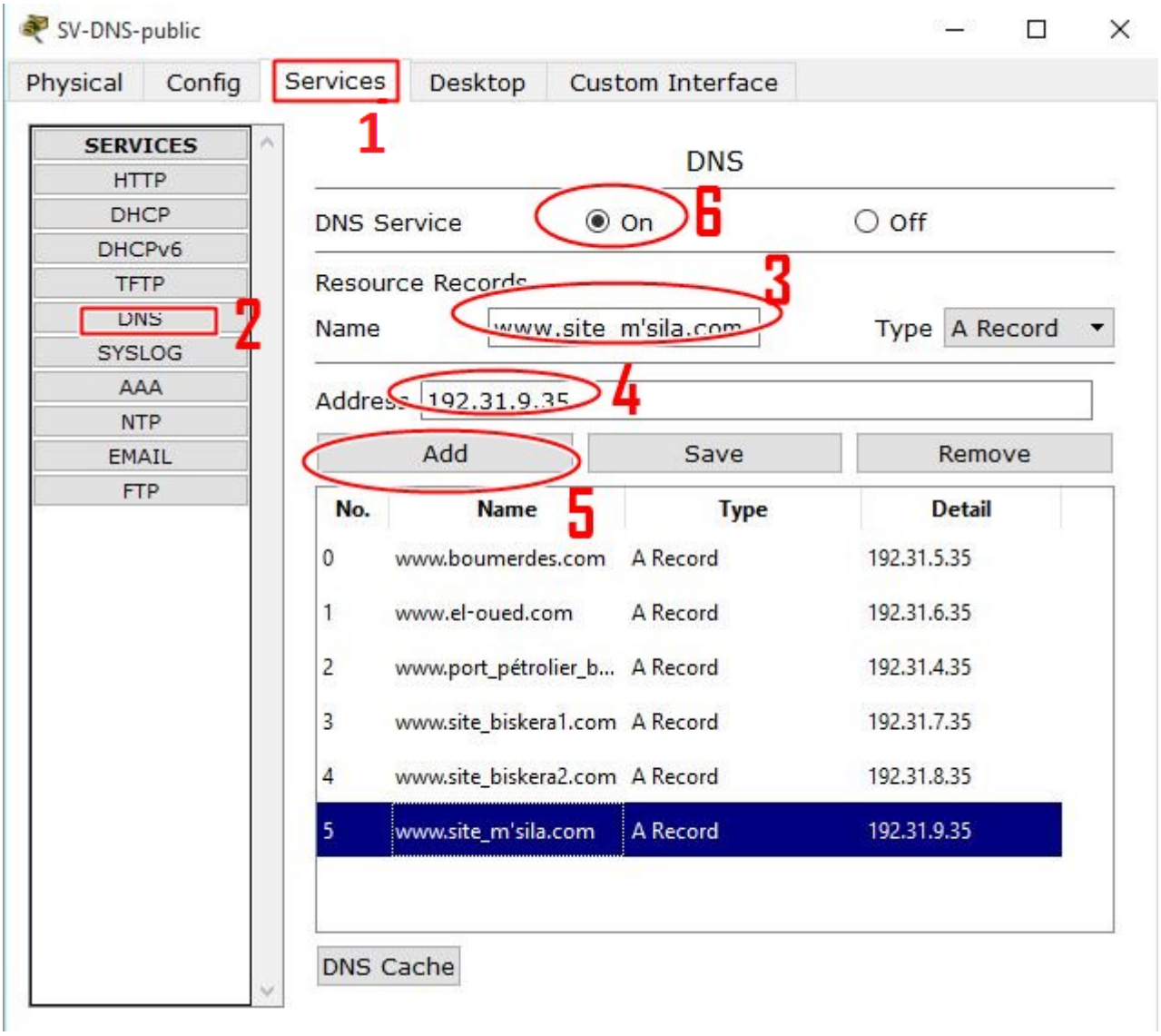

FIG. 4.7: Configuration du serveur DNS.

2. **Configuration des serveurs Web :** Un serveur web est un serveur informatique utilisé pour publier des sites web sur internet[13]. Pour configurer ces derniers, nous devons d'abord configurer l'adresse IP et l'adresse du serveur DNS, puis nous allons l'activer. Les figures (Fig 4.8) et (Fig 4.9) montrent les étapes de configuration. D'abord, l'atribution d'une adresse IP et l'adresse du serveur DNS au serveur Web. Ensuite l'activation du serveur Web avec ses étapes numérotées de 1 jusqu'à 4. Nous prenons l'exemple d'un seul serveur, sachant que sa sera la même chose pour les autres serveurs.

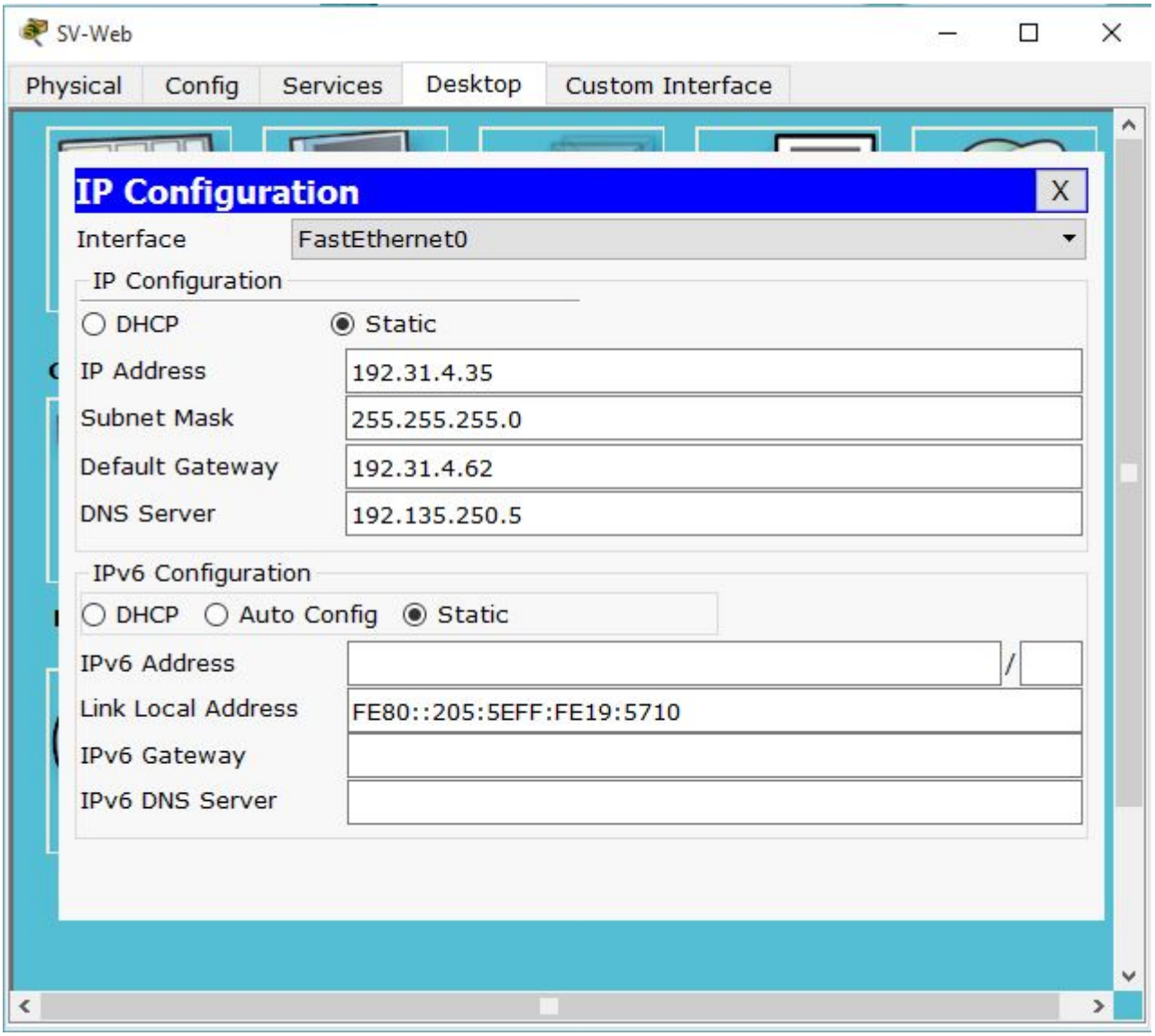

FIG. 4.8: Attribution d'une adresse IP et l'adresse du serveur DNS au serveur web.

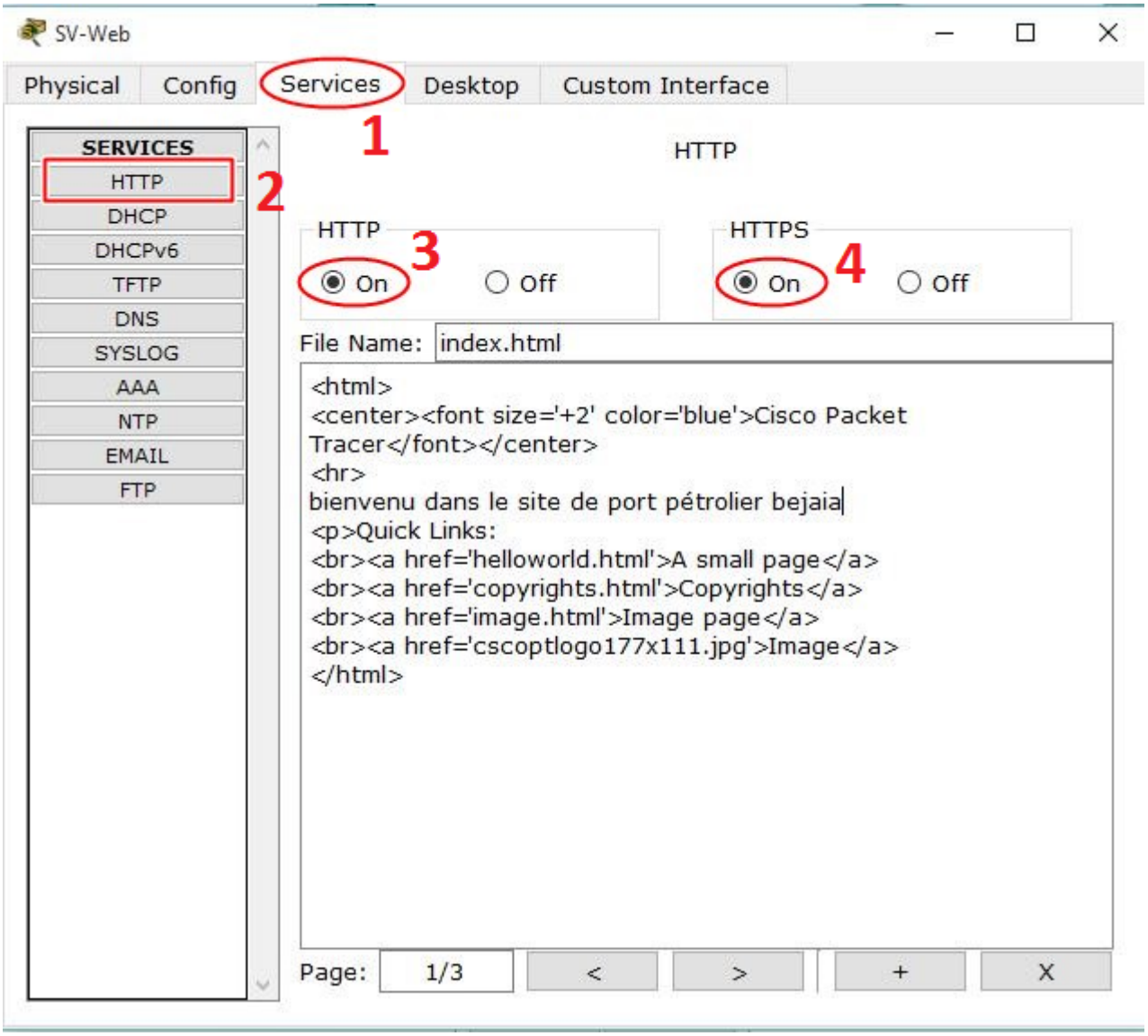

Fig. 4.9: Activation du serveur web.

3. **Configuration des PCs :** La configuration des PCs se fait par l'attribution des adresses IP, des passerelles ainsi que l'adresse du serveur DNS, la figure (Fig 4.10) montre les étapes de configuration de pc, sachant que la même chose sera appliqué pour tous les autres PCs.

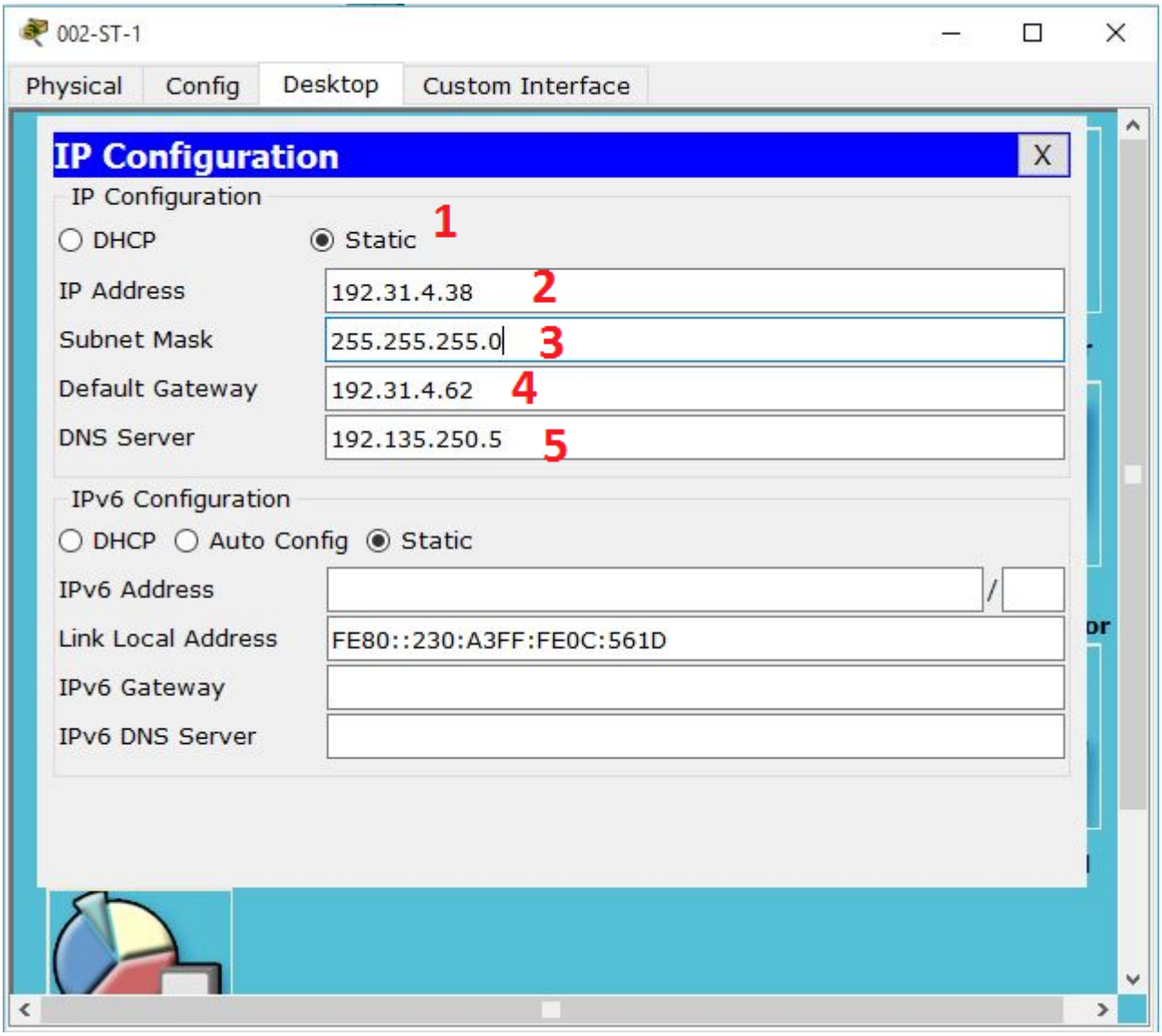

FIG. 4.10: Configuration des PCs.

4.3.2 Tests et validation de la configuration

Dans cette partie nous allons vérifier d'abord la communication entre tous les équipements en utilisant la commande Ping. Ensuite, nous allons vérifier l'accès aux différents sites.

1. Teste entre les différents sites

Après avoir configuré les différents équipements de l'architecture, nous allons testé le bon fonctionnement des échanges de données et cela grâce à la commande Ping.

Nous avons lancé un Ping entre le PC 002-PP-ST3 ayant l'adresse IP (192.31.4.36) qui se situe au port pétrolier de Béjaia et le PC 020-SBM-ST1 ayant l'adresse (192.31.10.38) se situant à Bouira, ceci illustré par la figure suivante (Fig 4.11).

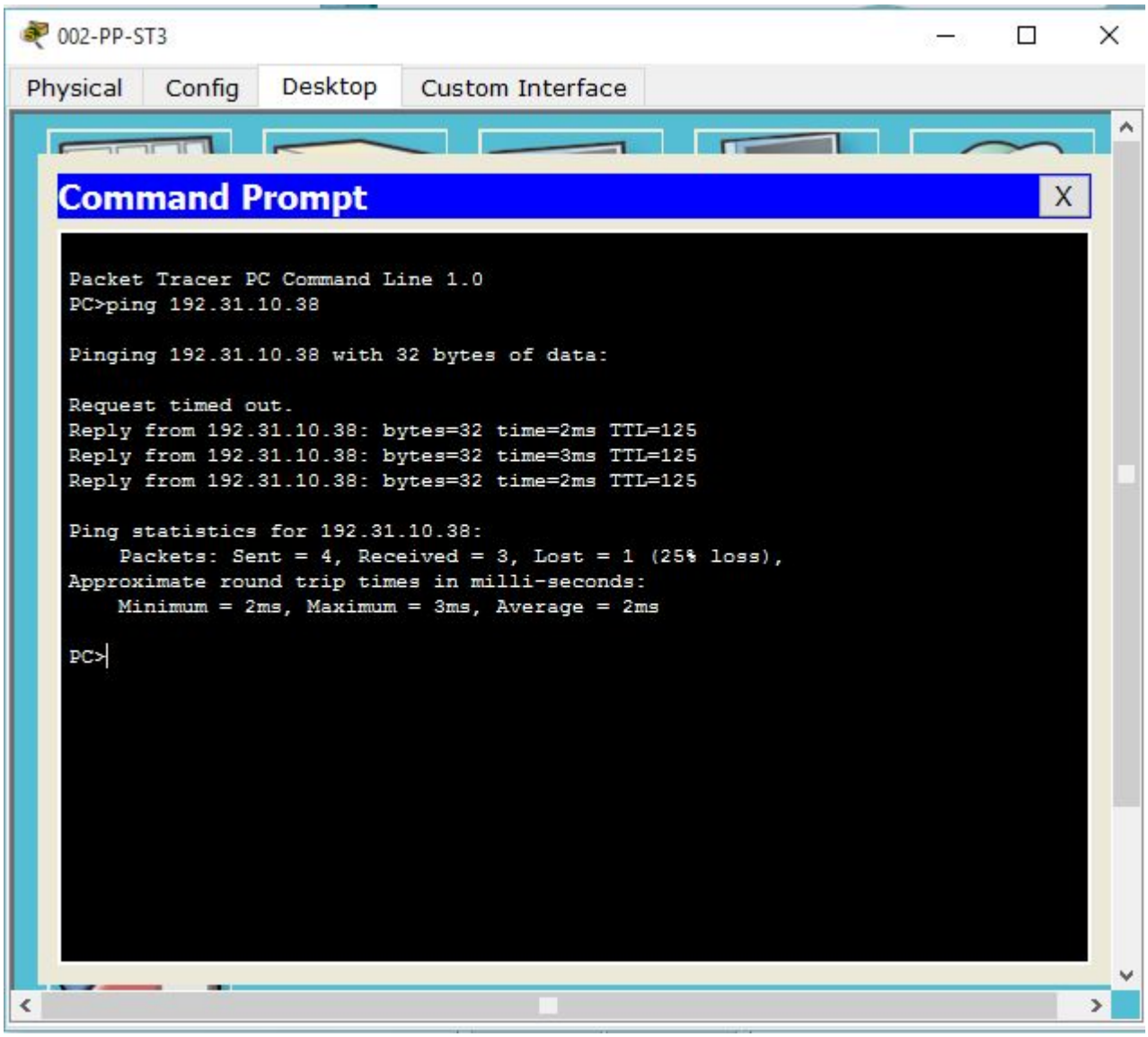

Fig. 4.11: Résultat de ping entre pc 002-PP-ST3 et le pc 020-SBM-ST1.

2. Vérification de l'accès au site web

A présent, nous allons tester l'accès au site du port pétrolier de Béjaia à partir d'une machine se situant au site de Boumerdes comme nous montre la figure (Fig 4.12) .

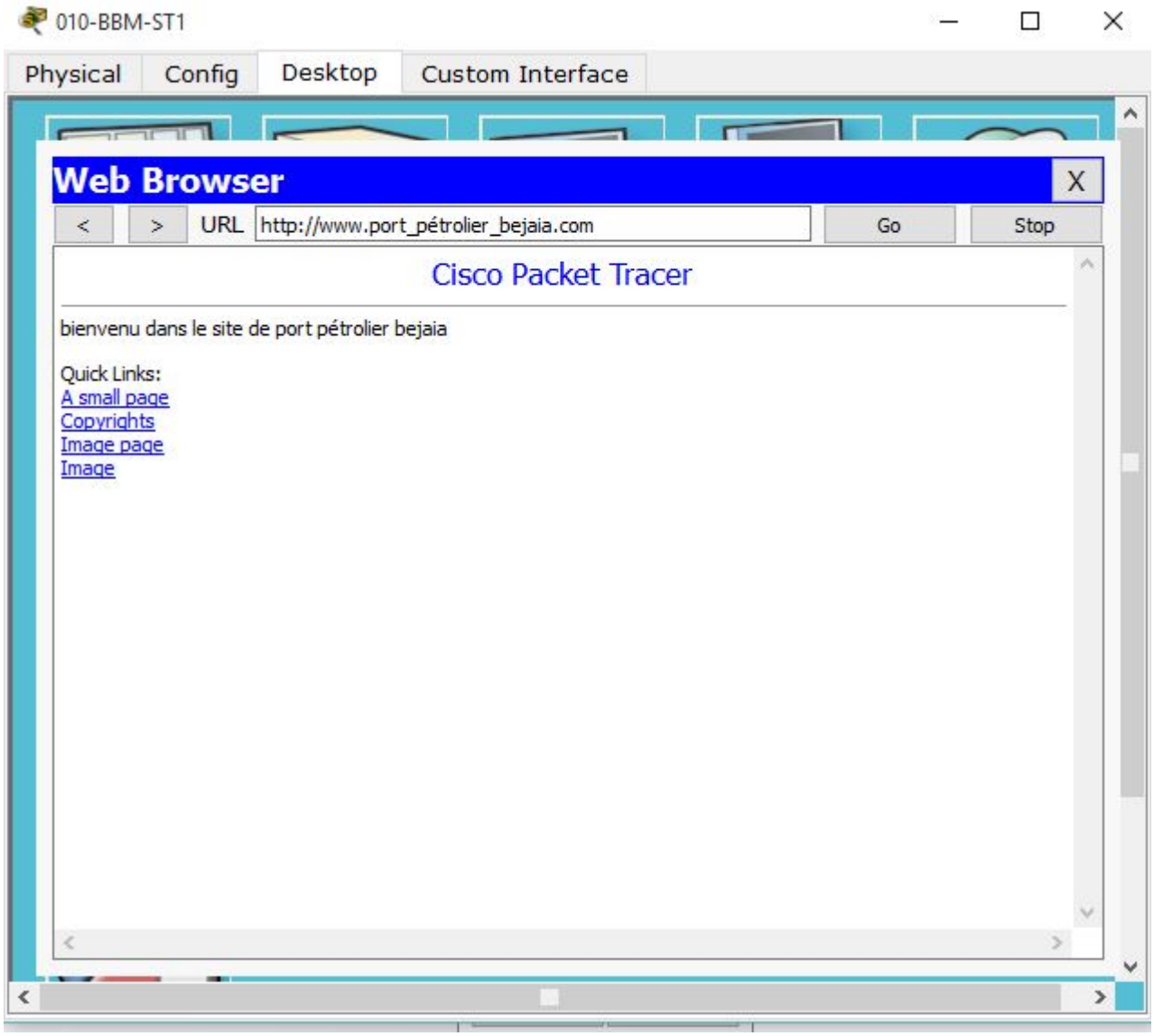

FIG. 4.12: Accès au site port pétrolier de Bejaia.

4.3.3 Architecture réalisée

Dans ce qui suit (Fig 4.13) sera présentée l'architecture LAN que nous avons réalisé.

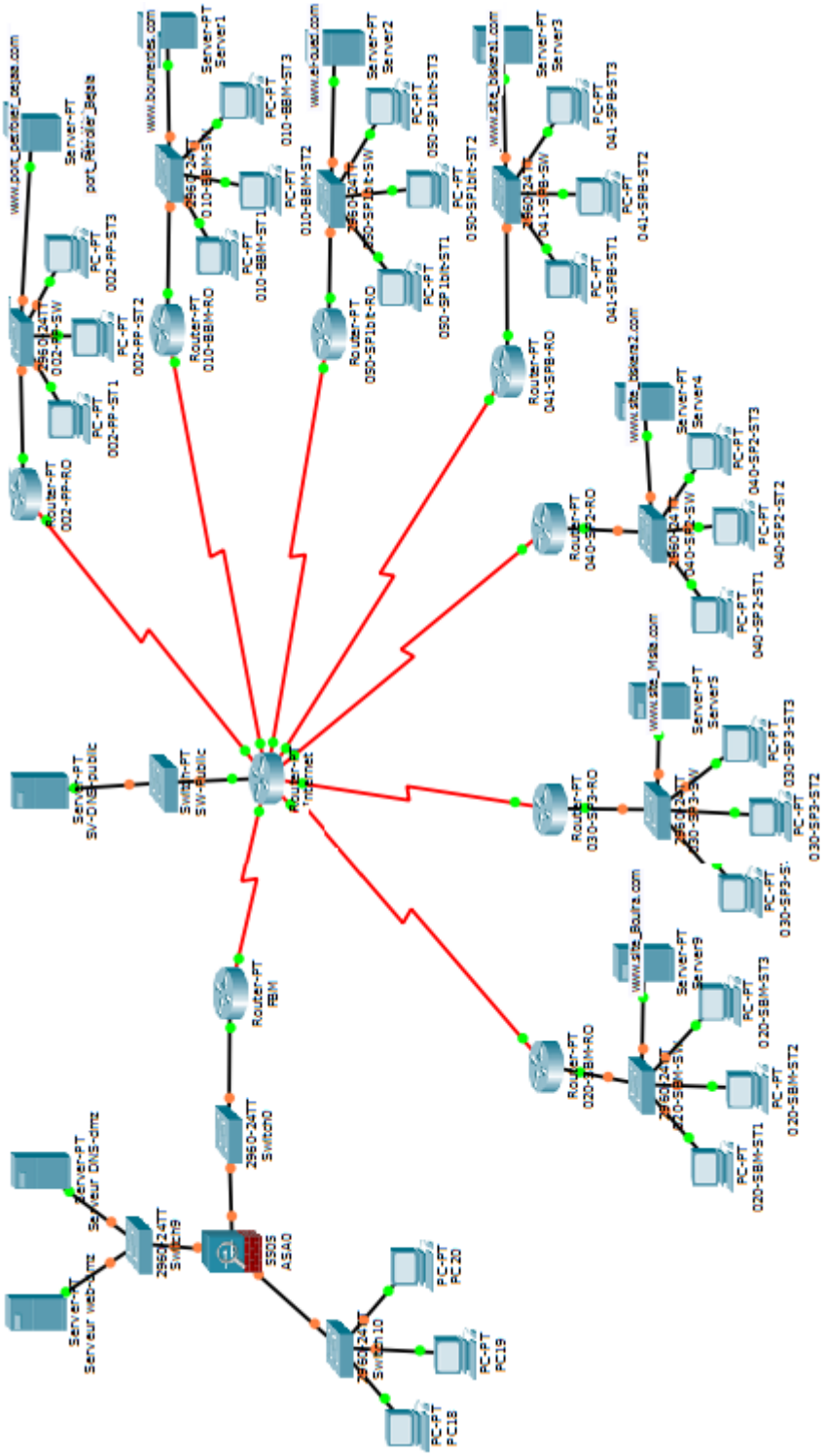

FIG. 4.13: L'architecture LAN réalisée.

4.4 Configuration de pare-feu

Après avoir réalisé l'architecture LAN, nous passons à la configuration des interfaces du pare-feu.

4.4.1 Configuration des interfaces de pare-feu

Le pare-feu est livré avec une configuration de base qui comporte deux interfaces routées qui sont des interfaces VLAN identiques à celle des commutateurs. Les deux interfaces vlan de la configuration de base sont nommées inside et outside. Chacune d'elle est associée à un niveau de sécurité. La figure (Fig 4.14) montre la configuration des VLANs INSIDE et OUTSIDE.

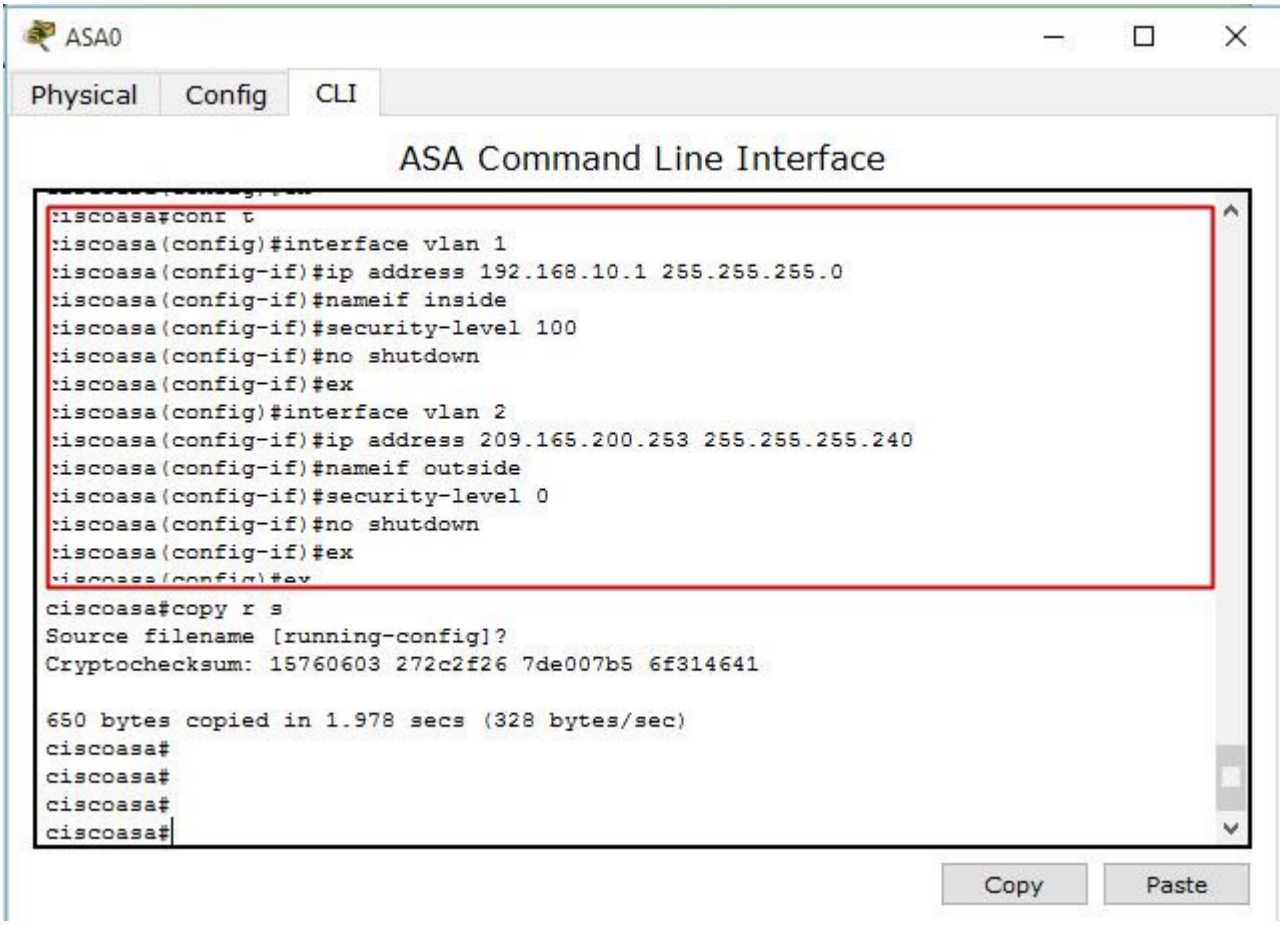

Fig. 4.14: Configuration des VLANs INSIDE et OUTSIDE.

Dans cette figure(Fig 4.14), nous remarquons la commande <nameif> qui donne son appellation aux deux interfaces. La commande <security-level> suivie d'une valeur indique son niveau de sécurité. Plus le chiffre est grand plus l'interface est digne de confiance. Il faut retenir que par défaut, le trafic transite uniquement entre deux interfaces du niveau le plus élevé vers le niveau le moins élevé. Dans la figure suivante (Fig 4.15) l'interface vlan 3 est configurée de telle sorte qu'elle ne puisse pas initialiser de communication vers l'interface vlan1. D'autre part, son niveau de sécurité est de 70 ce qui la situe entre les deux valeurs des deux autres interfaces.

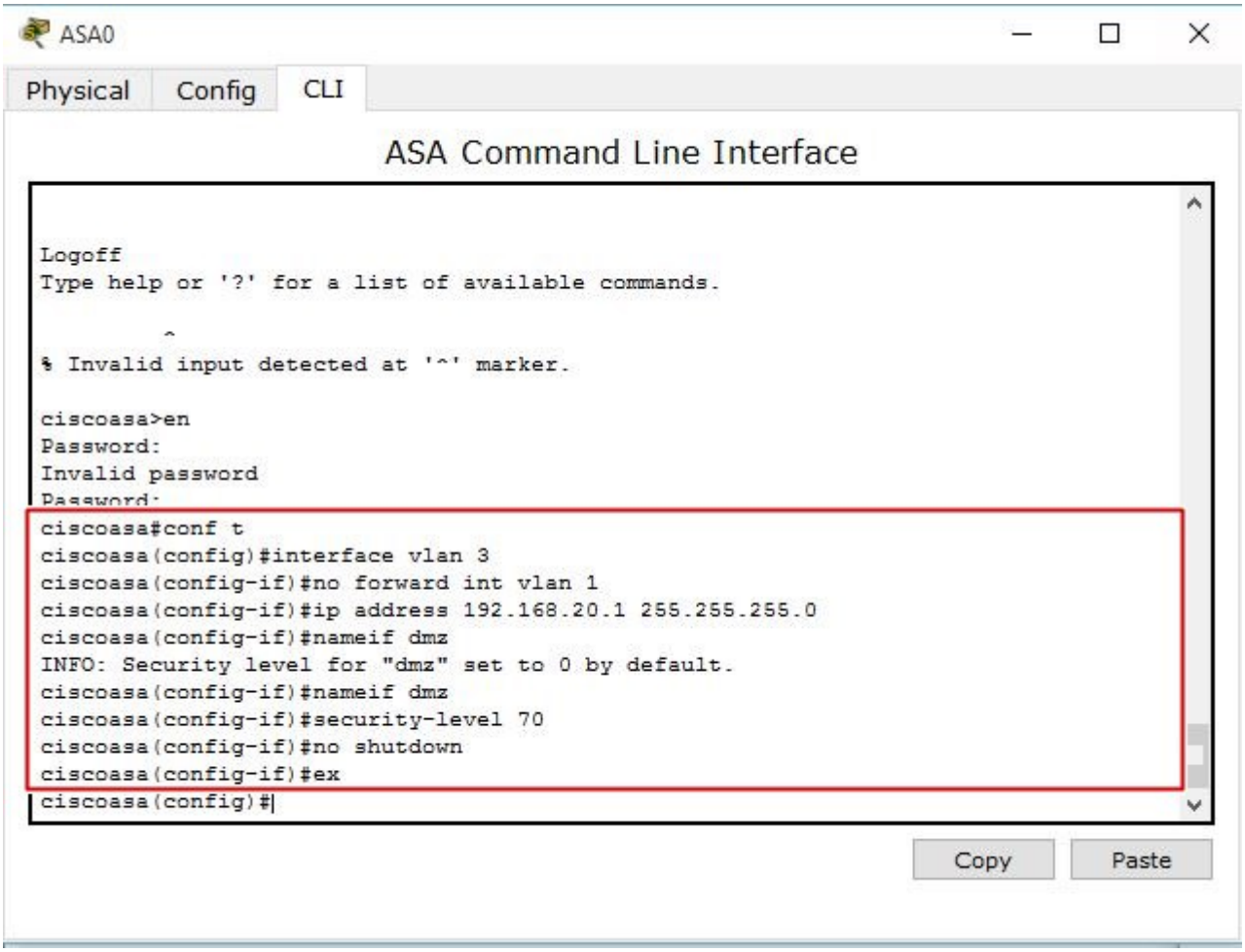

FIG. 4.15: Configuration des DMZ.

Les interfaces physiques du pare-feu sont au final raccordées aux divers VLAN en utilisant la commande switchport access vlan suivie d'un numéro de VLAN. la figure (Fig 4.16) montre la configuration des interfaces de pare-feu.

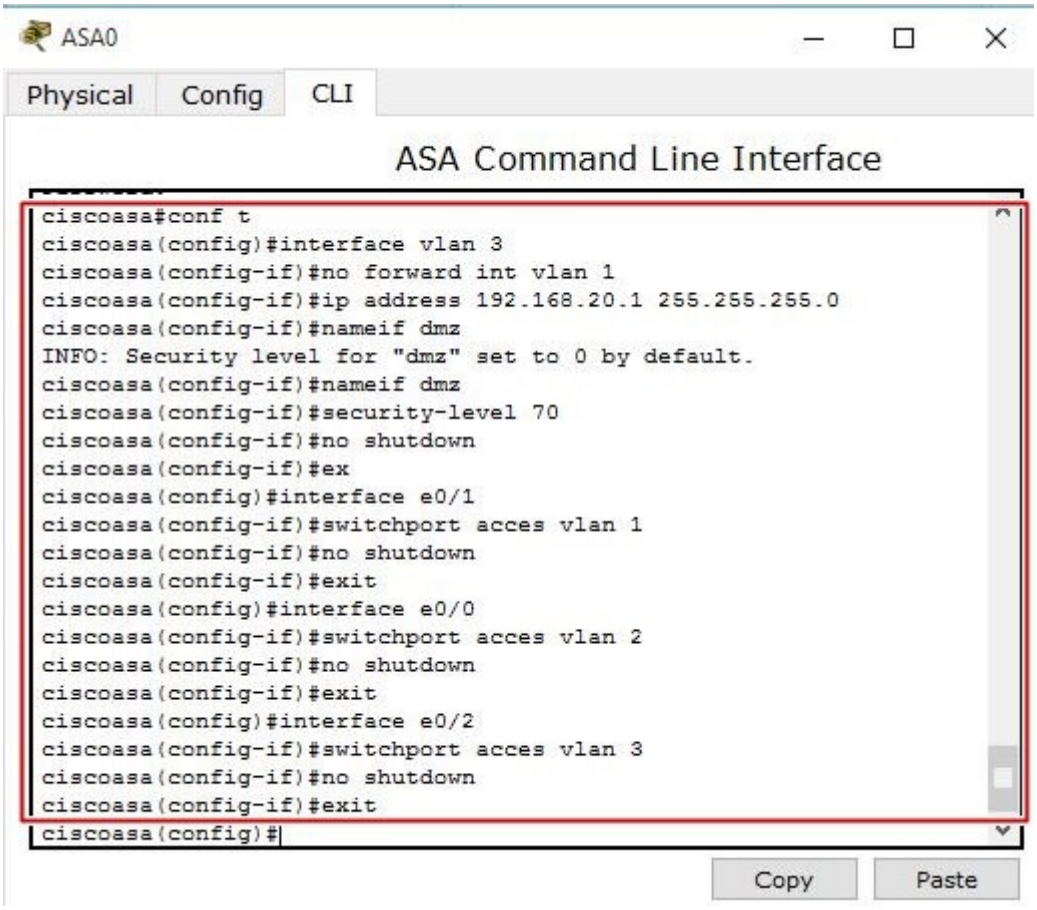

FIG. 4.16: Configuration des interfaces de pare-feu.

4.4.2 Configuration du service NAT pour le pare-feu et pour le réseau DMZ

Pour la configuration du service NAT (Network Address Translation) pour le pare-feu, nous avons deux cas :

1er cas : l'intérieur du réseau Nous allons créer la règle NAT pour que le réseau INSIDE puisse accéder au réseau OUTSIDE, pour ce faire nous allons préciser l'adresse de NAT ainsi que l'adresse de sortie de façon dynamique et ceci illustré par la figure (Fig 4.17).

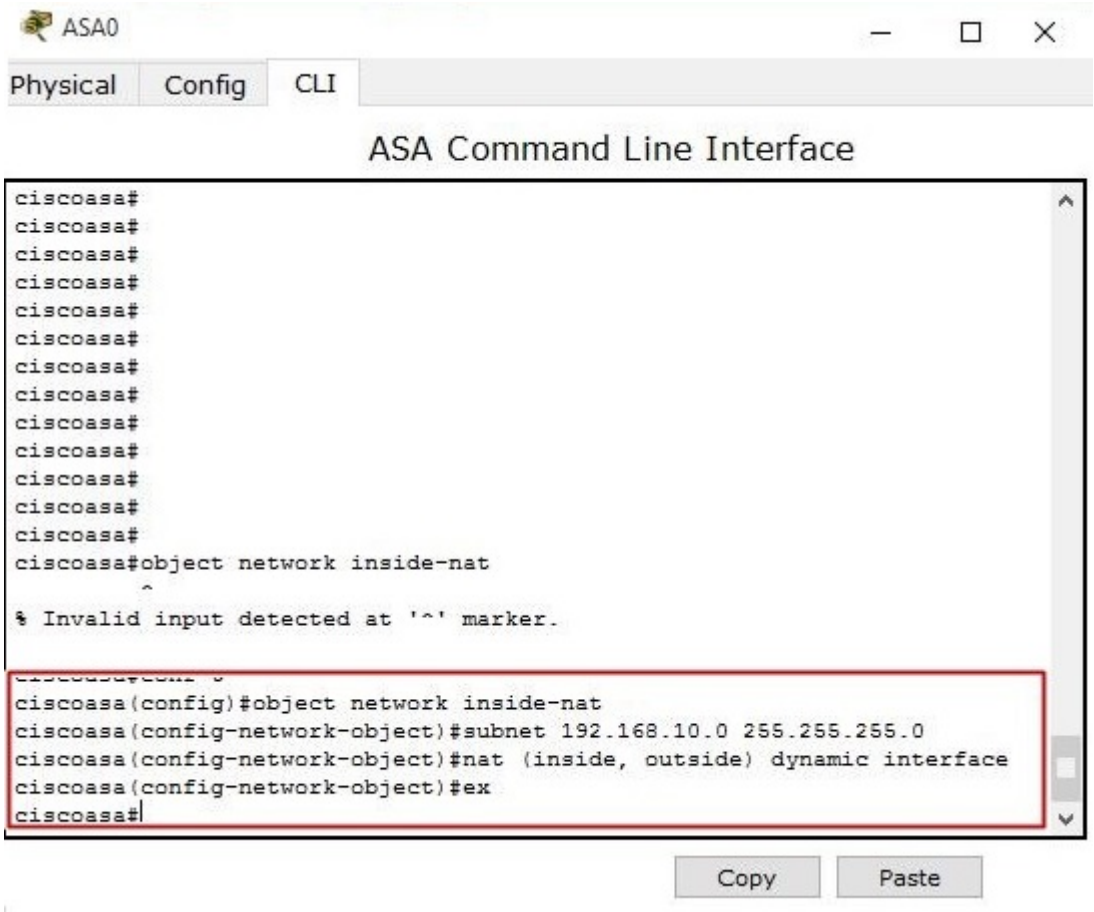

FIG. 4.17: Configuration du service NAT pour l'intérieur du réseau.

2ème cas : DMZ Les services offerts au public sont généralement installés sur des zones démilitarisées afin de bénéficier de la protection offerte dans ces espaces. La traduction d'adresse est l'une de ces protections. Il faut que le serveur dans le réseau DMZ soit accessible de l'extérieur par son adresse publique, la configuration de cette traduction d'adresse et illustré dans la figure (Fig 4.18).

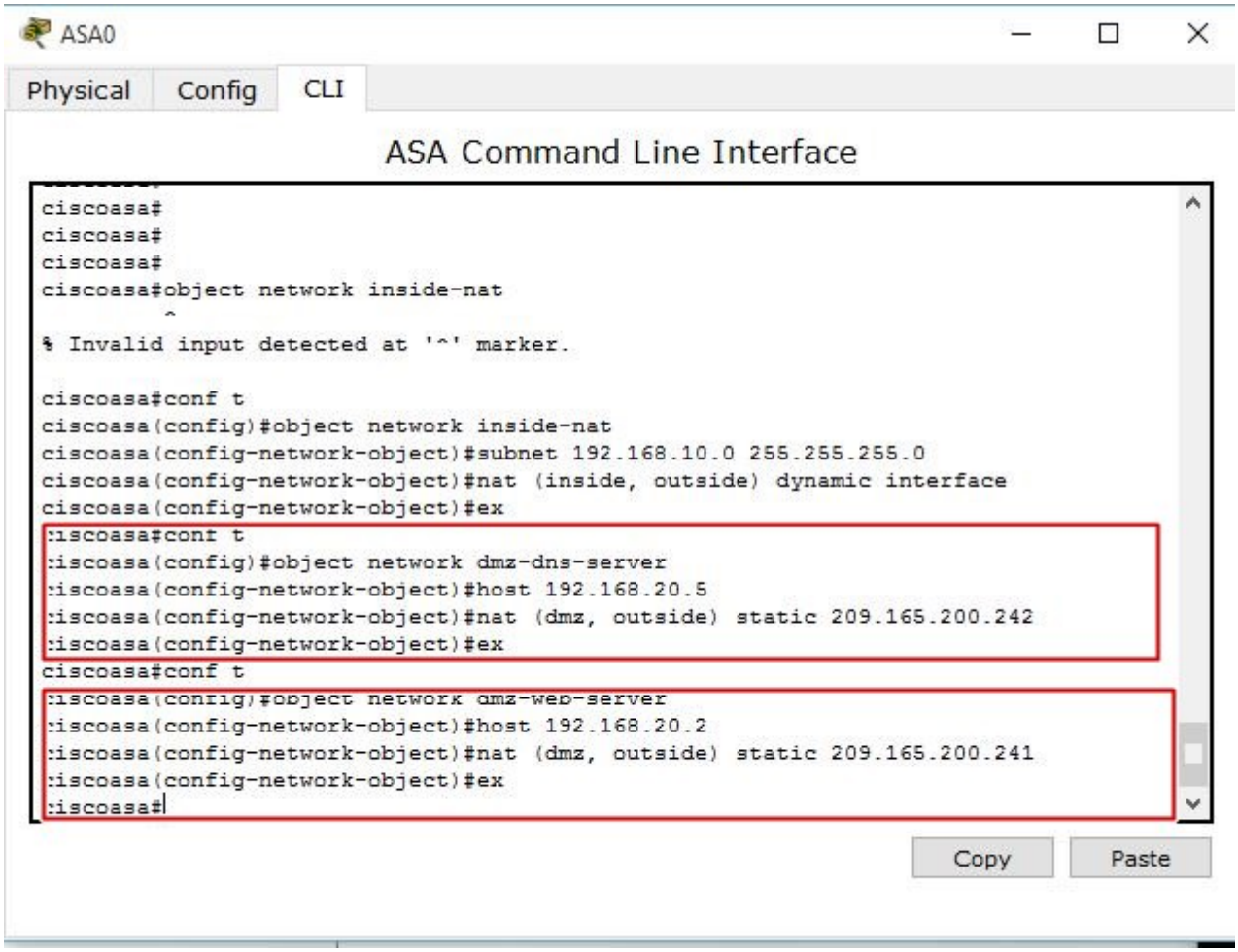

FIG. 4.18: Configuration du service NAT pour la DMZ.

4.4.3 Modification de la class-map pour indiquer le trafic

Dans cette étape nous allons modifier la politique par défaut MPF inspection d'application de service globale pour permettre aux hôtes du réseau interne pour accéder aux serveurs web sur Internet, on va d'abord créer une classe inspection-default qui correspond à défaut d'inspection du trafic. Ensuite, créer une politique-carte global-policy et l'inspecter avec DNS, FTP, HTTP et ICMP. Enfin, on fixe la carte politique globalement à toutes les interfaces, voir la figure (4.19).

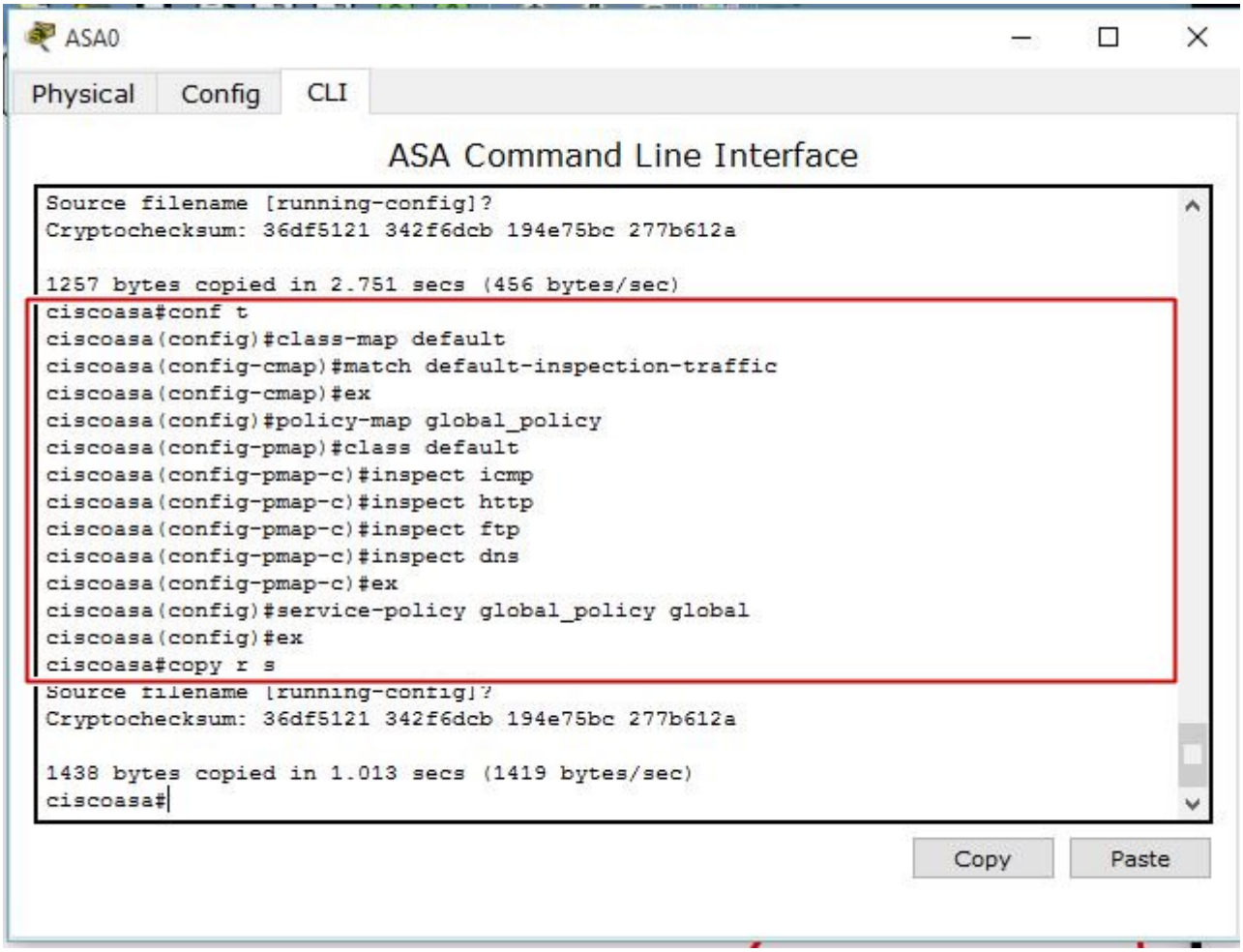

FIG. 4.19: Modification de la politique par défaut MPF.

4.4.4 Configuration des ACL(Access Control List)

Pour permettre l'accès aux serveurs DMZ à partir d'Internet il suffit de créer, appliquer et vérifier une ACL nommée outside-to-dmz pour filtrer le trafic entrant vers le pare-feu.

L'ACL doit être créé dans l'ordre spécifié dans les lignes directrices suivantes :
- Le trafic HTTP est autorisé à DMZ Web serveur ;
- Le trafic DNS (TCP et UDP) est autorisé au serveur DMZ DNS.

La figure suivante (Fig 4.20) montre les étapes de configuration des ACL.

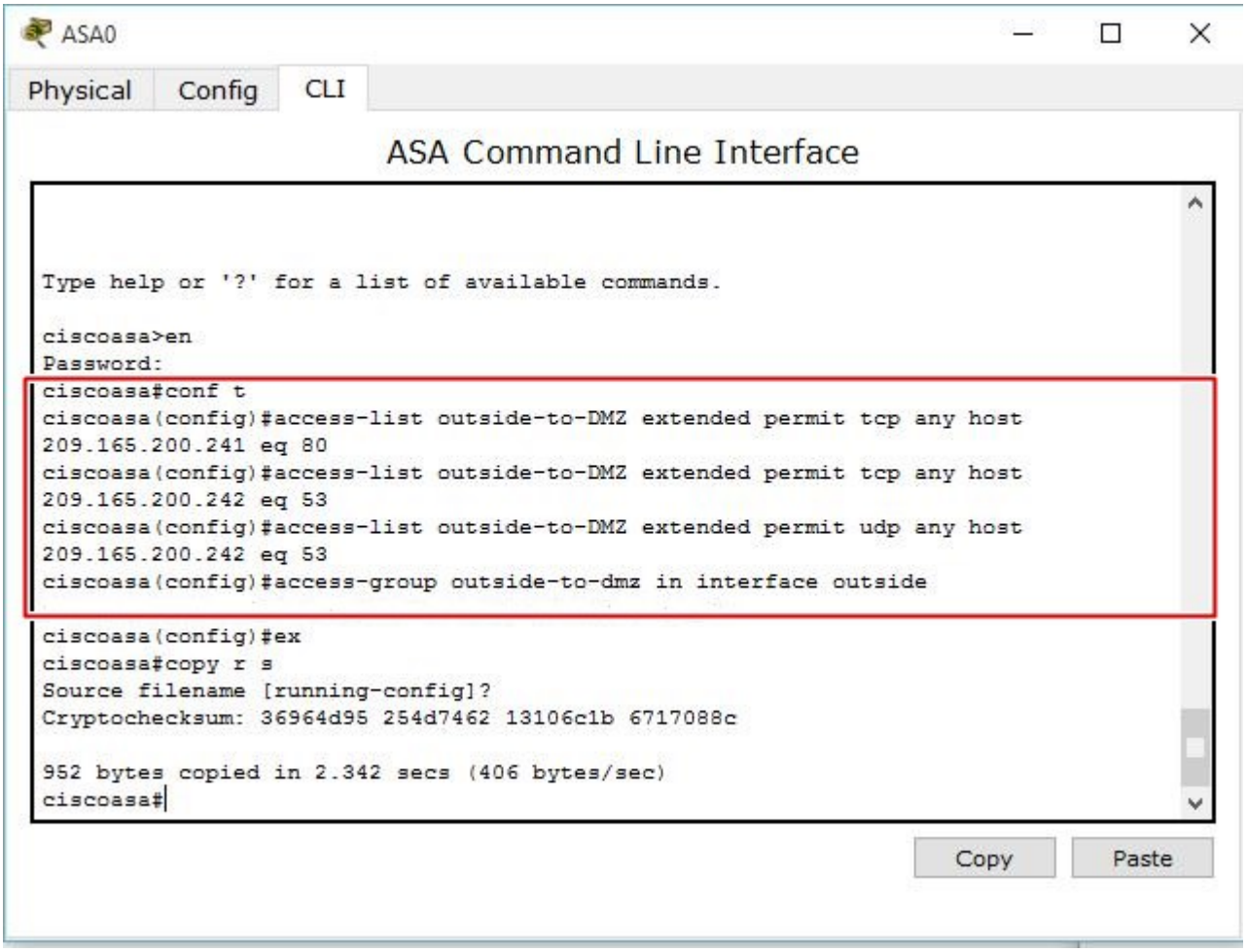

Fig. 4.20: Configuration des ACL.

4.4.5 Vérification de la configuration de pare-feu

– Le serveur web-dmz peut accéder un n'importe quelle site web. En prend un exemple de teste de serveur web-dmz au site de biskera1 (Fig 4.21).

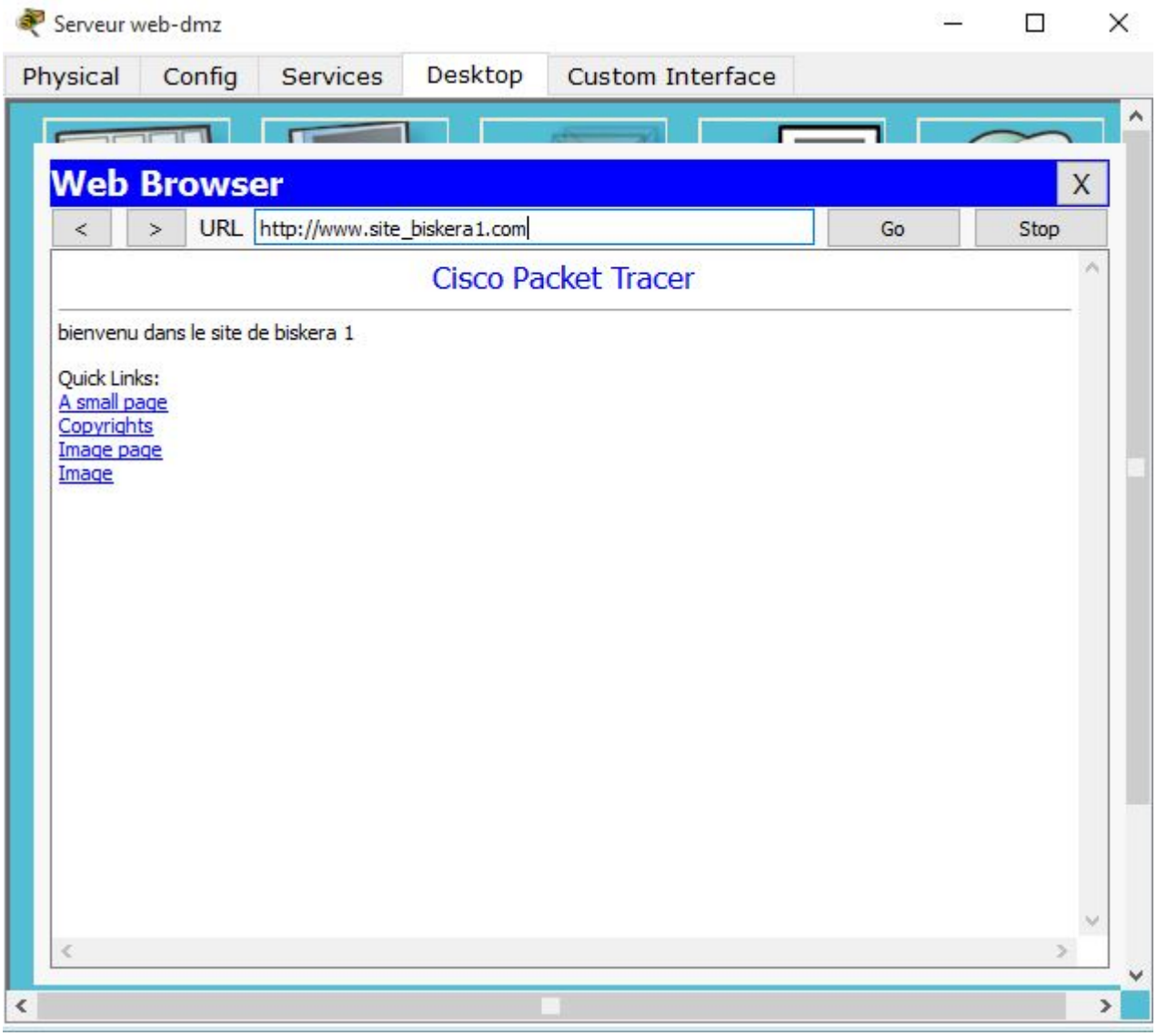

FIG. 4.21: Test de l'accès au site de biskera1 a partir de serveur web-dmz.

– N'importe quelle machine d'outside peut accéder au site web de Bejaia (Fig 4.22).

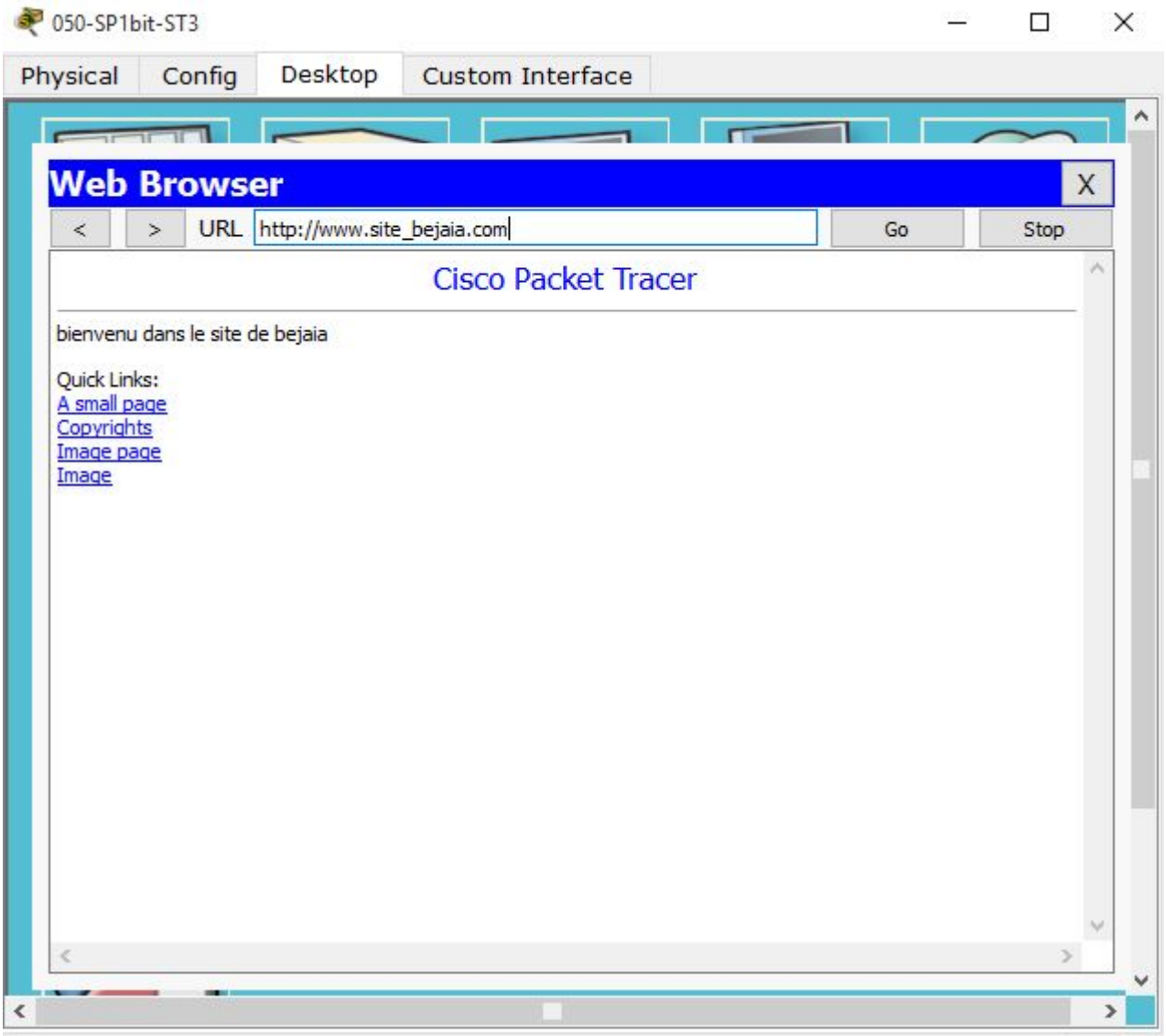

FIG. 4.22: Test l'accès au site de bejaia a partir de la machine de site de el-oued.

4.5 Conclusion

Dans ce chapitre, nous avons commencé par introduire le simulateur Packet tracer, nous avons par la suite décri la configuration de nos architectures réseaux dans les deux parties.

Dans la première, nous avons configuré les réseaux LANs ainsi que des testes de vérification, et dans la deuxième partie nous sommes passé à la configuration du pare-feu illustré par une présentation des différentes commandes de mise en place.

Conclusion générale et perspectives

A travers ce mémoire, nous avons apporté une nouvelle solution pour sécuriser le réseau intranet de SONATRACH de Béjaia. Comme nous l'avons constaté, SONATRACH est constitué de neuf sites distants et situés dans différentes régions de l'Algérie. Alors il y a lieu de sécuriser le réseau intranet de l'entreprise en organisant chaque site dans un sous réseau distinct.

Notre démarche consiste à implémenter une solution basée sur les pare-feu pour filtrer les données qui circulent dans le réseau.

Dans un premier temps, nous avons présenté les concepts fondamentaux des réseaux locaux, dans lequel nous avons fait un petit aperçu sur les différentes topologies et les équipements d'interconnexion des réseaux locaux. puis, nous avons mis un accent sur le modèle de référence OSI qui est la base de référence pour les réseaux locaux.

Ensuite, une étude sur la sécurité informatique nous à permis d'exposer un large panorama sur les différente attaques qui peuvent affecter notre réseau, sans oublier les stratégies de sécurité, à savoir les pare-feu et leurs fonctionnement, la cryptographie, les zones démilitarisées DMZs, Systèmes de détection d'intrusion ainsi les réseaux virtuels VLANs.

En effet, la mise en place d'un pare-feu d'entreprise a permi d'assurer la sécurité des informations du réseau de Sonatrach en filtrant les entrées et en contôlant les sorties selon des règles définies par l'administrateur du réseau.

Ce projet nous a permis d'acquérir une expérience personnelle et professionnelle et ne peut être que bénéfique. Ce fut une occasion pour se familiariser avec l'environnement du travail et de la vie professionnelle ainis que d'élargir et d'approfondir nos connaissances sur l'administration des réseaux informatiques.

Dans ce présent projet, nous n'avons fait qu'une simulation avec le simulateur packet-tracer, dans l'avenir, nou souhaitons faire une vraie réalisation sur des équipemennts réels, des équipements matériel afin d'appliquer concrétement ce que nous avons fait au cours de ce mémoire.

Bibliographie

[1] B.PETIT, Architecture des réseaux, Ellipses, 2013, 4ème édition.

[2] D.DROMARD, D.SERET, Architecture des réseaux, Pearson, 2010, 2ème édition.

[3] https ://www.eisti.fr, dernier accès Mai 2016.

[4] https ://www.wikipédia.fr, dernier accès Mai 2016.

[5] M.AUBERT, Introduction aux technologies de l'information et de la communication, Les topologies des réseaux.

[6] A.JAQUEMIN, A.MERCIER, Les firewalls.

[7] Le pare-feu https ://www.commentcamarche.net/faq/22304-le-pare-feu-ou-firewall.

[8] J-F.CARPENTIER, La sécurité informatique dans la petite entreprise, état de l'art et bonnes pratiques.

[9] Fonctionnement et utilité de pare-feu www.malekal.com/le-fonctionnement-et-lutile-dun-firewall-2, dernier accès Juin 2016.

[10] Fonctionnement et importance de pare-feu forum.malekal.com/fonctionnement-importance-pare-feu-t7601 dernier accès Juin 2016.

[11] Packet-Tracer https ://fr.wikipedia.org/wiki/Packet-Tracer, dernier accès Juin 2016.

[12] Rôle de serveur DNS https ://technet.microsoft.com/fr-fr/library/cc753635(v=ws.10).aspx, dernier accès Juin 2016.

[13] Serveur-web https ://fr.wikipedia.org/wiki/Serveur-web, dernier accès Juin 2016.

[14] G.FLORIN, Cours de sécurité, Pare-feu (Firewalls), Laboratoire CEDRIC.

[15] Inspiré du cours de troisième année module de sécurité par le professeur Omar Mawloud, 2014