République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaia

Faculté des Sciences Exactes
Département d'Informatique


# MÉMOIRE DE FIN D'ÉTUDES

En vue de l'obtention du diplôme d'un Master en Informatique
**Option :** Administration et Sécurité des Réseaux

Thème

---

# Renforcer la sécurité des reseaux avec le serveur ISA 2006

## Cas d'étude : NAFTAL Bejaia

---

**Soutenu devant le jury composé de :**

**Président** : Mr YAZID Mohand
**Examinateur :** Mr AKILAL Abedllah
**Examinateur :** Mr MOKTEFI Mohand
**Encadreur :** Mr ATMANI Mouloud

**Réalisé par :**

$M^{elle}$AIT MOKRANE Safia
$M^{elle}$LAMRANI Sounia

**Promotion : 2015/2016**

# Remerciements

*Tout d'abord, nous remercions Dieu le tout-puissant qui nous a donné le courage, la force et la volonté pour mener ce travail.*

*Nous tenons à présenter nos expressions de reconnaissance envers notre promoteur* ***Mr ATMANI Mouloud***

*A notre maitre de stage* ***Mr AIT SALAH Yazid****, pour leurs précieuses assistances et leurs orientations*

*A tout le corps professoral et administratif de département informatique de l'Université Abderrahmane MIRA de Bejaia pour la richesse et la qualité de leurs enseignements*

*Aux membres du jury pour l'honneur qu'ils nous feront en acceptant de juger ce modeste travail*

*Enfin, Nous remercions vivement toutes personnes ayant contribuées d'une manière ou d'une autre à l'élaboration de ce mémoire.*

# Dédicaces

*Avec l'aide de DIEU tout puissant, qui trace le chemin de notre vie, nous avons pu arriver à réaliser ce modeste travail que nous dédions :*

*A nos très chers parents qui nous ont beaucoup aidés au long de notre vie et durant notre cursus, que DIEU préserve leur santé et longue vie.*

*A nos sœurs, frères, familles nous leurs souhaitons un avenir plein de succès, et à toutes les personnes qui nous ont apporté de l'aide.*

# Table des matières

# Table des figures

# Liste des abréviations

| | |
|---|---|
| **CPU** | **C**entral **P**rocessing **U**nit |
| **IP** | **I**nternet **P**rotocol |
| **LAN** | **L**ocal **A**rea **N**etwork |
| **VPN** | **V**irtual **P**rivate **N**etwork |
| **TCP** | **T**ransmission **C**ontrol **P**rotocol |
| **UDP** | **U**ser **D**atagram **P**rotocol |
| **FTP** | **F**ile **T**ransfer **P**rotocol |
| **http** | **H**yper **T**ext **T**ransfer **P**rotocol |
| **OSI** | **O**pen **S**ystems **I**nterconnexion |
| **PPTP** | **P**oint- **T**o-**P**oint **T**unneling **P**rotocol |
| **SMTP** | **S**imple **M**ail **T**ransfer **P**rotocol |
| **IDS** | **I**ntrusion **D**etection **S**ystem |
| **HIDS** | **H**ost **I**ntrusion **D**etection **S**ystem |
| **NIDS** | **N**etwork **I**ntrusion **D**etection **S**ystem |
| **CPU** | **C**entral **P**rocessing **U**nit |
| **IP** | **I**nternet **P**rotocol |
| **LAN** | **L**ocal **A**rea **N**etwork |
| **VPN** | **V**irtual **P**rivate **N**etwork |
| **TCP** | **T**ransmission **C**ontrol **P**rotocol |
| **UDP** | **U**ser **D**atagram **P**rotocol |
| **FTP** | **F**ile **T**ransfer **P**rotocol |
| **http** | **H**yper **T**ext **T**ransfer **P**rotocol |
| **OSI** | **O**pen **S**ystems **I**nterconnexion |
| **PPTP** | **P**oint- **T**o-**P**oint **T**unneling **P**rotocol |
| **SMTP** | **S**imple **M**ail **T**ransfer **P**rotocol |

| | |
|---|---|
| **IDS** | **I**ntrusion **D**etection **S**ystem |
| **HIDS** | **H**ost **I**ntrusion **D**etection **S**ystem |
| **NIDS** | **N**etwork **I**ntrusion **D**etection **S**ystem |
| **UND** | **U**nité **N**AFTAL **D**istribution |
| **CPL** | **C**arburants **L**ubrifiants **P**eneumatiques |
| **RSI** | **R**esponsable de la **S**écurit **I**ndustrielle |
| **AMG** | **A**dministration **M**oyen **G**énéraux |
| **OSC** | **O**euvres **S**ociales **C**ulturelles |
| **R.H** | **R**essources **H**umaines |
| **BOG** | **B**ureau **O**rdre **G**eneral |
| **ING** | **I**nformation **G**estion |
| **ISA** | **I**nternet **S**ecurity **A**cceleration |
| **VLAN** | **V**irtual **L**ocal **A**rea **N**etwork |
| | |
| **RAM** | **R**andom **A**ccess **M**emory |
| **DNS** | **D**omain **N**ame **S**ystem |

# Introduction générale

L'outil informatique fait partie intégrante du métier de l'entreprise et l'évolution d'Internet lui a permis d'émettre, de recevoir, de rechercher des informations, et de mettre en place un travail coopératif totalement efficace, mais il est indiscutable qu'il nous a également son corolaire de problèmes.

Les attaques des systèmes informatiques sont de plus en plus automatisées et les mesures de sécurité deviennent de plus en plus compliquées. Ainsi, elles doivent être étudiées de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

Les administrateurs de réseau de l'entreprise de NAFTAL semblent avoir compris la nécessité de sécuriser leurs systèmes d'informations, car son réseau expose une absence de contrôle des connexions sortantes et entrantes.

La configuration actuelle d'ISA server ne dispose d'aucun filtrage sortant, ce qui laisse les employés a utilisé l'internet en dehors le cadre de travail, ceci cause le ralentissement de la vitesse de la connexion, ni d'aucun filtrage entrant, ceci laisse libre court aux potentielles d'attaques et vols d'informations dont peut être victime les ordinateurs de l'administration.

Notre objectif est de fournir la meilleure configuration de ISA server 2006 en mode pare feu, C'est la raison essentielle pour laquelle ce dernier n'acceptent que des communications déterminées à l'avance dans notre politique de sécurité.

Nous avons partagé notre travail en trois grands chapitres :

- **Chapitre 1 :** Sécurité des réseaux informatiques ;
- **Chapitre 2 :** Analyse et critique du réseau informatique existant ;
- **Chapitre 3 :** Instalation et configuration de serveur ISA.

Chapitre 1

# Sécurité des réseaux informatiques

## 1.1 Introduction

La sécurité des systèmes d'information permet aux entreprises et organisations, dont ils constituent de plus en plus un moteur essentiel, de résister à des atteintes en disponibilité, intégrité ou confidentialité.
Certes, le réseau devient le principal outil du système d'informations [1] de l'entreprise, pour favoriser le développement des échanges. Il est donc important, de définir une politique de sécurité pour ces réseaux et veiller à leur respect.
Avant de passer à l'étude du réseau existant dans l'entreprise NAFTAL, nous reprendrons ici, quelques notions théoriques sur les principales menaces pesant sur la sécurité des réseaux, ainsi que les mécanismes de défense.

## 1.2 Securite des réseaux

La sécurité d'un réseau est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires, et mis en place pour réduire la vulnérabilité d'un système informatique contre les menaces accidentelles ou intentionnelles auxquelles il peut être confronté [1].

[1]Ensemble matériel et immatériel des entités (ressources, données, traitements, relation, procédures).

## 1.3 Objectifs de la sécurité

La sécurité d'un réseau peut s'évaluer sur la base d'un certain nombre de critères de sécurité. On distingue généralement trois principaux critères de sécurité [2].

- **Disponibilité :** assure que le système est en bon fonctionnement et ses informations sont toujours disponibles aux personnes autorisées.
- **Confidentialité :** assurai que seulement les personnes autorisées qui ont l'accès aux informations [2] échanges.
- **Intégrité :** assurai que seulement les personnes autorisées qui peuvent altère au changer les informations sur le système.
- **Non répudiation :** assure que l'auteur d'un acte ne peut ensuite dénier l'avoir commis [4].

## 1.4 Terminologie de la sécurité informatique

Avant de traiter ce qu'est une attaque informatique, il convient de présenter quelques définitions.

### 1.4.1 Vulnérabilités

C'est une faiblesse dans la protection du système, telles que les failles de sécurité dans les actifs [3], les contrôles de sécurité technique, les procédures d'exploitation ou d'administration utilisées dans l'entreprise [3].

### 1.4.2 Menace

Une menace est un danger qui peut exploiter une vulnérabilité en vue d'obtenir, modifier ou empêcher l'accès à un actif ou encore le compromettre [4].

On distingue deux grandes catégories :

- menaces intentionnelles.
- menaces non intentionnelles.

a) **Menaces intentionnelles :** c'est un ensemble d'actions malveillantes qui constituent la plus grosse partie du risque, et qui doivent être l'objet principal

[2]Ensemble cohérent de données incluant lors d'une transmission : l'émetteur, le message, le récepteur.

[3]C'est la partie d'un bien qui compose le patrimoine et présentant de la valeur pour l'entreprise.

de mesures de protection.

On définit deux types de menaces :

- menaces passives.
- menaces actives.

**Menaces passives :** le but dece type de menace n'est pas la modification des informations mais, les écouter seulement, il porte essentiellement sur la confidentialité.

**Menaces actives :** dans ce type de menace c'est le contenu de l'information qui va être modifiée, donc elles portent sur l'intégrité des données.

b) **Menaces non intentionnelles :** ces menaces qui se produisent sans le vouloir, concernent les pannes et les erreurs. Parmi les menaces non intentionnelles, citons : les erreurs de transmission, les erreurs de conception des applications, les erreurs de manipulation d'informations.

### 1.4.3 Risque

Le risque est la possibilité qu'une chose critique apparaisse. Son évaluation, permet d'établir des actions pour réduire et maintenir la menace à un niveau raisonnable et acceptable [2].

On distingue deux grandes catégories :

- les risques physiques.
- les risques logiques.

a) **Risques physiques :** il s'agit de toutes les atteintes physiques directes dont peut-être victime un système d'informations, tels que les défaillances matérielles, les dommages électriques ou les événements naturels. . .etc [1].

b) **Risques logiques :** il s'agit d'un événement perturbant les données qui ont acquis une importance plus grande avec le développement fulgurant de l'informatique distribuée [4] ou des erreurs de conception, de programmation, de paramétrage ou de manipulation de données.

Le développement du Cloud Computing [5] est l'une des illustrations les plus expressives de cette tendance [1].

[4] L'informatique distribuée correspond à la structure de la société humaine, en réseau, où chacun est différent et avance à son rythme.

[5] Informatique dans les nuages.

### 1.4.4 Attaque

Les hackers utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois familles différentes :

- les attaques directes ;
- les attaques indirectes par rebond ;
- les attaques indirectes par réponses .

Nous allons voir en détail ces trois familles [3].

a) **Attaques directes :** c'est la plus simple des attaques. Le hacker attaque directement sa victime, à partir de son ordinateur.
Cette technique est utilisée généralement par les scripts kiddies. En effet, les programmes de hack qu'ils utilisent, ne sont que faiblement paramétrables, et un grand nombre de ces logiciels envoient directement les paquets à la victime. Dans ce type d'attaque il ya une grand chance de remonter à l' origine de l'attaque et de trouver l'identité de l'attaquant [4].

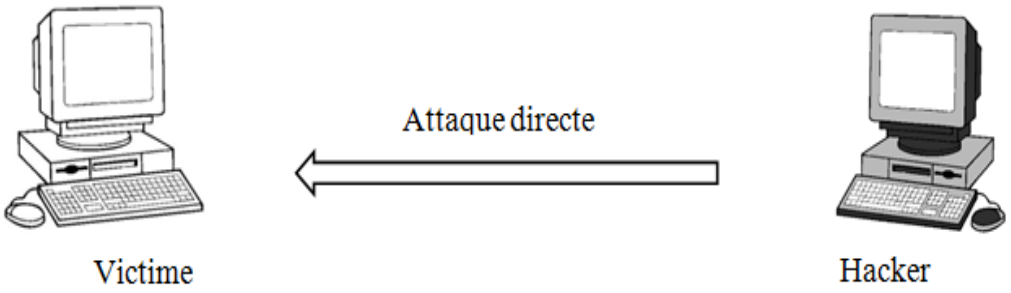


FIG. 1.1 – Attaque directe

b) **Les attaques indirectes par rebond :** le principe de cette attaque c'est d'envoyer des paquets à un (ou plusieurs) ordinateur ou serveur intermédiaire, ce dernier répercute l'attaque vers la victime. D'où le terme de rebond. Dans ce genre d'attaque il n'est pas facile de remonter à la source. Au plus simple, on peut remonter jusqu'à l'ordinateur intermédiaire.
L'attaque indirecte par rebond à deux avantages :

- masquer l'identité (l'adresse IP) du hacker ;
- éventuellement, utiliser les ressources de l'ordinateur intermédiaire, car il est plus puissant (CPU, bande passante...) pour attaquer [4].

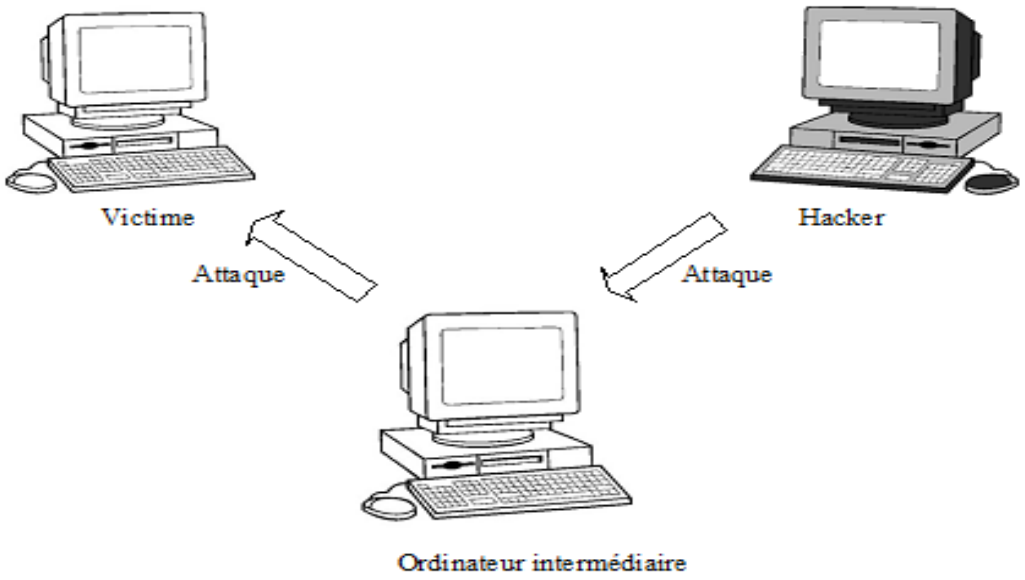


FIG. 1.2 – Attaque indirecte par rebond

c) **Les attaques indirectes par réponse :** cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages mais, au lieu d'envoyer une attaque à l'ordinateur ou le serveur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime [4].

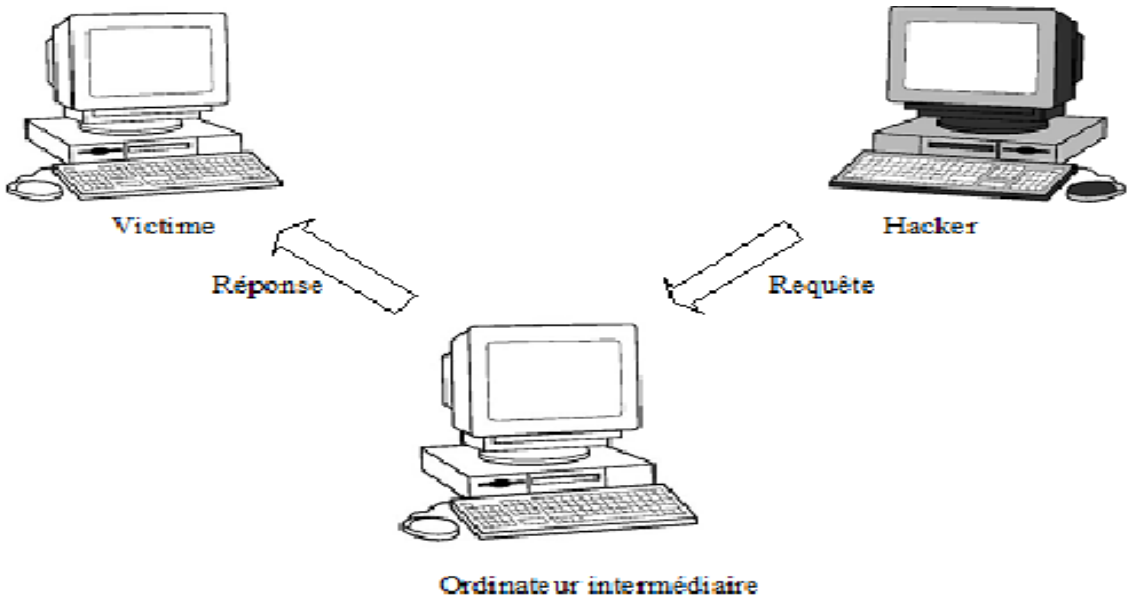


FIG. 1.3 – Attaque indirecte par réponse

## 1.5 Les pirates

### 1.5.1 Script kiddes

Ce sont des jeunes pirates néophytes qui réutilisent des codes ou des programmes prêts à l'emploi, il les exécute sur des machines sans comprendre les enjeux, dans le but de provoquer des pannes volontaires. Malgré leur faible niveau mais parfois leurs attaques présentent une menace réelle pour un système [5].

### 1.5.2 Hacker

Ils introduisent dans les systèmes d'information sans autorisation, dans le but de provoquer des dégradations dans les données ou les applications au pire des cas. Ses vacations peuvent s'effectuer à partir de l'intérieur, ou de l'extérieur de l'entreprise. Toutefois, il n'est pas toujours facile de détecter sa présence sur les systèmes ni de connaître ce qu'il a provoqué comme dégâts [2].

### 1.5.3 cracker ou casseur

C'est un pirate informatique qui est spécialisé dans le cassage de système de sécurité informatique, il est plus dangereux que le hacker, car il cherche à nuire et montrer qu'il est le plus fort. Souvent il est mal dans sa peau ou son environnement donc il cherche à venger de ce qui il a rejeté ou détesté [6].

## 1.6 Motivations d'attaques

Chaque attaquant à un but pour son attaque. Dans ce qui suit nous allons définir quelques buts.

### 1.6.1 L'espionnage

Celui-ci va tenter d'enfreindre les mesures de sécurité qui protègent la confidentialité des informations, cette menace concerne particulièrement les informations stratégiques d'une entreprise [4].

### 1.6.2 Le sabotage

Il a pour but de mettre hors service un système d'informations ou une de ses composantes [4].

### 1.6.3 Les accès illégitimes

Cette menace est le fait d'une personne qui se fait passer pour une autre, en usurpant son identité. Les accès illégitimes portent atteinte à la confidentialité des informations [4].

### 1.6.4 La fraude physique

Elle peut consister à récupérer les informations oubliées ou non détruites par l'adversaire ou le concurrent. L'attaquant portera une attention particulière aux supports physiques usagés (bandes magnétiques, disquettes, disques classiques ou optiques, etc.) [6].

### 1.6.5 Le vol

Visible quand l'objet du délit est matériel mais, le vol de ressources est plus insidieux, car il se peut qu'il soit réalisé sans porter atteinte à la confidentialité, l'intégrité ou la disponibilité des informations et des services [6].

## 1.7 Mécanismes d'attaque

### 1.7.1 Logiciels malveillants

Un logiciel malveillant est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté. Plusieurs types de logiciels malveillants ont été proposés, nous citons les plus répandus :

- **Virus (malware) :** c'est un programme de petite taille qui se reproduit grâce à une vulnérabilité logicielle ou avec l'aide des usages [6]. Il peut être transmis à un autre ordinateur par les réseaux ou les supports d'informations amovibles.

[6]La reproduction de virus se fait lorsque nous activons le fichier ou le programme ou il est attaché.

- **Vers (worm) :** un ver est une variété de virus qui a une vitesse de propagation très élevée sur les réseaux, parce qu'il se duplique automatiquement sans action humaine. A ce titre, les vers sont plus dangereux que les virus [7].
- **Cheval de Troie (Trojan horse) :** programme ou un sous-programme à apparence légitime. Une fois installé sur un ordinateur, il effectue des actions cachées et pernicieuses, sans l'autorisation de l'utilisateur [8].
- **Bombe logique :** une bombe logique est une fonction, cachée dans un programme en apparence honnête, qui se déclenchera à retardement, lorsque sera atteinte une certaine date, ou lorsque surviendra un certain événement [8].

### 1.7.2 Mécanismes d'attaque sur messagerie électronique

- **Pourriel (spam) :** c'est un courrier électronique indésirable, qui est transmis à une multitude de destinataires n'ayant solliciter aucune demande de la part de l'émetteur. A cet effet, ils encombrent le réseau, et font perdre du temps à leurs destinataires [6].
- **Hameçonnage (phishing) :** c'est une technique qui utilise un courrier électronique, dont l'expéditeur se fait généralement passer pour un organisme financier, et demandant au destinataire de fournir des informations confidentielles, comme le mot de passe ou d'autres informations privées [9].
- **Canular informatique (hoax) :** un courrier électronique incite généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes, dans le but d'encombrer le réseau, et font perdre du temps à leurs destinataires [9].

### 1.7.3 Mécanismes d'attaque sur le réseau

- **Écoute (sniffing) :** c'est une technique qui utilise un logiciel sniffer, afin de récupérer toutes les informations transitant sur un réseau LAN. Elle est généralement utilisée pour récupérer les mots de passe des applications et pour identifier les machines qui communiquent sur ce réseau [9].
- **Usurpation d'identité (spoofing) :** c'est une technique consistante à prendre l'identité d'une machine autorisée [7] et qui fait croire que la requête provient de cette machine [9].
- **Déni de service (denial of service) :** c'est une activité qui consiste à

[7] C'est une machine qui fait partie de réseau sécurisé LAN .

paralyser un service ou un réseau complet, dont le but d'empêcher quelqu'un de les utiliser [8].

## 1.8 Mécanismes de sécurité

À cause des menaces et les risques de la sécurité informatique, il faut mettre en place des mécanismes pour s'assurer la confidentialité, l'intégrité et la disponibilité des services. Parmi ces mécanismes, on peut citer :

### 1.8.1 Cryptage

C'est une procédure de la cryptographie, consiste à traiter une information par un algorithme mathématique, de sorte que seules les personnes possédant la clé appropriée, puissent accéder à l'information et la traiter [2].

### 1.8.2 Antivirus

Les antivirus sont des programmes capables de détecter et éliminer des logiciels malveillants sur un ordinateur. Une mise à jour sera effectuée périodiquement, en fonction des exigences et spécificités de la politique de sécurité [10].
On dénombre deux composants d'un antivirus : les scanners et moniteurs.

#### 1.8.2.1 Scanners

Le scanner examine un ordinateur à la demande : un fichier, un dossier ou tous les fichiers de disque. Un scanner complet consomme beaucoup de ressources matérielles et de temps, mais il est conseillé de le faire de temps à autre.

#### 1.8.2.2 Moniteurs

Le moniteur analyse en temps réel les fichiers au cours de leurs utilisations et stoppe immédiatement une exécution virale.

### 1.8.3 VPN

C'est un tunnel sécurisé assurant des connexions confidentielles entre des sites distants, tout en utilisant le réseau public. Les VPN ont deux applications princi-

pales :

- la connectivité site-à-site qui permet de joindre deux réseaux de type LAN, distants, de manière à faire en sorte qu'ils puissent communiquer comme s'ils étaient sur le même réseau ;
- la connectivité à accès distant permettant de relier un utilisateur avec le réseau local [10].

### 1.8.4 Pare-feu (firewall)

Un firewall est une solution mise en place dans une architecture réseau, afin de renforcer la politique de sécurité de l'entreprise. A cet effet, ils surveillent les liaisons entrantes ou sortantes depuis l'intérieur, mais également entre les entités éloignées [8]de l'entreprise, mais reliées par un réseau de type extranet. Il existe différents types de pare-feu, selon leur typologie ou leur fonction. Ils peuvent opérer sur chacun des niveaux 3 (IP), niveau 4 (TCP, UDP) ou niveau 7 (FTP, HTTP...) du modèle OSI [2].

#### 1.8.4.1 Fonctionnalités de pare-feu

Les principales fonctionnalités d'un pare-feu sont résumées comme suit [2] :
Au niveau de paquets

- filtres statiques et dynamiques ;
- filtrage à partir de l'analyse des données ;
- possibilité de suppression des paquets.

Au niveau de circuits (protocoles)

- filtrage basé sur les sessions ;
- contrôle et analyse de la connexion du client vers le serveur ;
- association de connexion .

Au niveau d'applications

- inspection des données ;
- analyse du contenu (action de blocage, modification, redirection) ;
- filtrage pour les protocoles HTTP (HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), etc.

[8]Une station qui fait partie de réseau local et connecté à distance (VPN).

#### 1.8.4.2 Type de pare-feu

Il existe trois types de pare-feu [3] :

- pare-feu à filtrage de paquet ;
- pare-feu state full inspection ;
- pare-feu applicatif (proxy).

**Pare-feu à filtrage de paquet (Stateless) :** appelé on générale les ACL. Son rôle consiste à analyse les paquets échangés entre une machine du réseau interne et une machine extérieure de manière totalement indépendante. Ces firewalls interviennent sur les couches réseau et transport, selon des règles de filtrages qui s'appliquent par rapport à :

- l'adresse IP sources ou destination ;
- le port source ou destination ;
- le type des paquets (TCP, UDP...).

**Pare-feu state full inspection :** ce type de pare-feu verifie que les parquets apportionment à une session régulière, ilposséde une table d'états ou est stocké un suivi de chaque connexion établie, ce qui permet au pare-feu de prendre des decisions adaptées à la situation.

**Pare-feu applicatif (proxy) :** le pare-feu s'intercale dans la session et analyse l'information afin de vérifier que les échanges protocolaires sont conformes aux normes.

### 1.8.5 Les systèmes de détection d'intrusion (IDS)

Afin de se protéger des risques et vulnérabilités auxquels les pare-feu ne peuvent faire face, les IDS surveillent l'identité des requêtes circulant sur le réseau, comme il empêche les utilisateurs non autorisés, d'accéder à leurs réseaux. A ce titre, les IDS ont pour but de compléter les fonctions du pare-feu [10].

On distingue principalement deux catégories de détection d'intrusion [2] :

- HIDS (host intrusion detection system) ;
- NIDS (network intrusion detection system) ;

**HIDS (host intrusion détection system) :** ces types d'IDS sont prévus pour la détection des menaces à un haut niveau de sécurité. En général, il est intégré au système d'exploitation qu'il protège, donc il doit être installé sur chaque machine.

**NIDS (network intrusion détection system) :** ces types d'IDS implémentés en tant qu'analyseurs intelligents de protocole. Ses composants surveillent le trafic réseau au niveau physique.

## 1.9 Conclusion

Dans ce chapitre nous avons étudié les définitions théoriques nécessaires à la compréhension des notions fondamentales de la sécurité dans les réseaux de l'entreprise. L'objectif général de cette recherche, c'est de faciliter l'analyse du réseau de l'entreprise de NAFTAL vu leur efficacité ainsi que leur rendement dans la pratique.

Chapitre 2

# Analyse et critique du réseau informatique existant

## 2.1 Introduction

Dans ce deuxième chapitre, nous allons présenter l'entreprise d'accueil NAFTAL de Bejaia, et faire une description détaillée de son système architectural d'informations, en y décrivant les ressources matérielles et logicielles qui le composent. Enfin, notre solution va être présentée après une critique de l'existant.

## 2.2 Présentation de l'organisme d'accueil

### 2.2.1 Historique de NAFTAL

Issue de SONATRACH, (société nationale pour la recherche, transport, production, transformation, la commercialisation des hydrocarbures), l'entreprise nationale de raffinage et de distribution de produits pétroliers (ERDP) a été créé par le décret N°80-101 du 06 avril 1980.

Entrée en activité le 01 janvier1982, elle est chargée de l'industrie de raffinage et de la distribution de produits pétroliers. Le 04 mars 1985, les anciens districts (Carburants, lubrifiants, pneumatique et bitume) ont été regroupés sous le nom UND (unité NAFTAL de distribution).

En 1987, l'activité raffinage est séparée de la distribution, conformément au

Décret n° 87- 189 du 25 Août 1987 modifiant le décret n°80-101 du 6 Avril 1980, modifié, portant création de l'Entreprise nationale de raffinage et de distribution de produits pétroliers, il est créé une Entreprise nationale dénommée :

«Entreprise nationale de commercialisation et de distribution de produits pétroliers », sous le sigle de «NAFTAL ». A partir de 1998, elle change de statut et devient société par action filiale à 100% de SONATRACH, en intervenant dans les domaines suivants :

- de l'enfûtage GPL ;
- de la formulation des bitumes ;
- de la distribution, stockage et commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatique, GPL /produits spéciaux ;
- du transport des produits pétroliers.

Elle est chargée, dans le cadre du plan national de développement économique et social, de la commercialisation et de la distribution des produits pétroliers et dérivé.

Le 01 janvier 2000 l'activité GPL enfûtage est séparée de l'activité CLP.

Par décision n° S 554 du 29 mars 2000, il a été procédé à l'organisation générale de la division CLP et l'identification des zones de distribution «CLP»(carburants, lubrifiants et pneumatiques).

Par décision n° S 555 du 29 mars 2000, il a été procédé à la création des zones de distribution CLP.

Par décision n° S 606 du 10 Février 2001, il a été procédé à l'organisation et la classification des centres Bitumes de la Division Bitume.

Par décision n° S 705 du 17 Juin 2002, il a été procédé à la dénomination des zones de distribution CLP et GPL en District.

Par décision n° S 766 du 22 Décembre 2003, il a été procédé à la dissolution de la Branche CLPB.

Par décision n° S 770 du 03 Janvier 2004, il a été procédé à la dissolution des Districts CLP et création des Districts Commercialisation.

A partir du 01.12.2006 l'activité Carburants est séparée de l'activité commercialisation.

### 2.2.2 Présentation de la branche carburant de NAFTAL

NAFTAL est une société par actions, filiale de SONATRACH, ayant pour mission la commercialisation et la distribution des produits pétroliers.

La branche carburant est l'une des trois branches de NAFTAL. Elle est chargée des activités d'approvisionnement, de stockage et de livraison des carburants par airs, mer et terre ; de même que pour les lubrifiants et graisses par airs et mer. L'organigramme ci-dessous retrace une représentation schématique des liens fonctionnels.

### 2.2.3 Organigramme

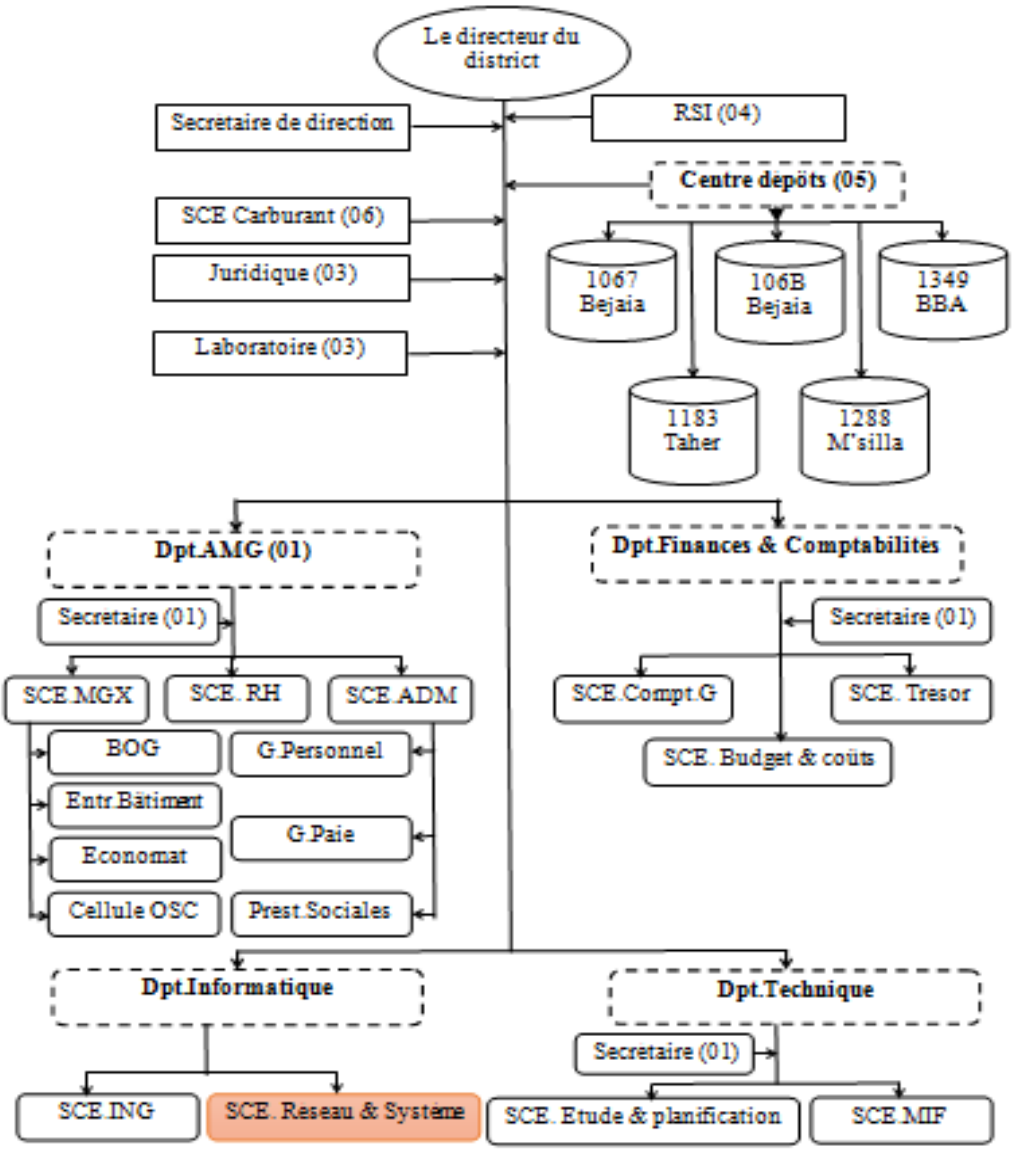


FIG. 2.1 – L'organigramme général de NAFTAL

a) **Directeur :** il est rattaché aux : responsable de la sécurité industrielle (RSI), la secrétaire, le laboratoire, le service carburant, la cellule juridique, la chargée de communication, et les différent départements et dépôts carburants.

b) **Département Informatique :** le département Informatique est assuré par un chef de département, son rôle principal est de garantir la continuité de service des systèmes informatiques déployés au niveau des districts et centres opérationnels ; et veiller à la mise à disposition des informations de gestion aux structures du district, des branches et des structures centrales.

Le département informatique est divisé en deux services :

- service système et réseaux ;
- service informations de gestion (ING).

1. **Service système et réseaux :** le rôle principal de ce service est de prendre en charge :
   - les infrastructures réseaux filaires et wifi ;
   - l'exploitation des systèmes opérationnels ;
   - la maintenance des équipements informatiques.

   Le service système et réseaux se présente comme suit :

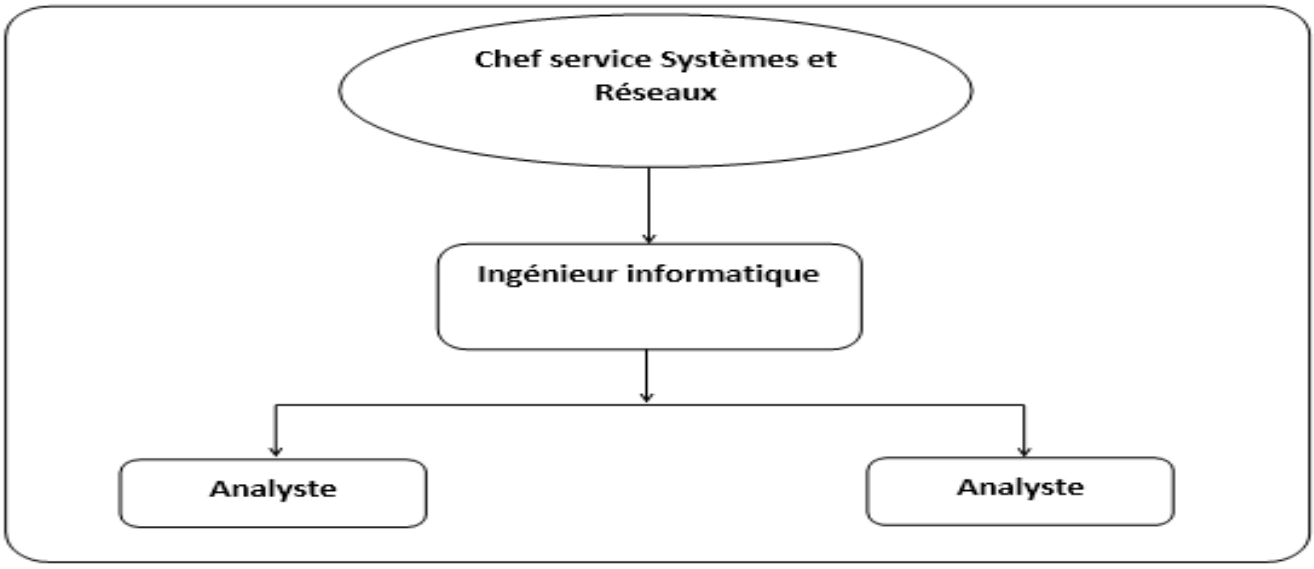


Fig. 2.2 – Organigramme du service Système et Réseau

Ce service est composé d'un (1) chef de service système et réseau, d'un (1)

ingénieur informatique et de deux (2) analyste ; il assure deux tâches principales :

a) **La maintenance informatique :**

- assure la maintenance corrective de tous types de matériels informatiques ;
- analyse les causes des pannes et y apporter la solution adéquate dans des meilleures délais ;
- installe les matériels neufs.

b) **L'infrastructure réseau :** mise en place et configure le réseau informatique de l'entreprise, il intervient à chaque étape de la mise en place d'un réseau local, il s'occupe généralement de fournir le matériel nécessaire est faire

- la pose du câblage informatique ;
- la configuration des postes utilisateurs, système d'exploitation, messagerie, internet. . .etc ;
- assure aussi la gestion des domaines et ressource du réseau ;
- administrer les serveurs de réseau (serveur FTP, messagerie . . .).

En plus de ces deux tache le service système et réseau assure des services généraux : la sécurité, distribution logicielle et gestion des postes de travail.

2. **Service information de gestion (ING) :** le rôle principal de ce service c'est de gérer et mettre à jour une banque de données de toutes les activités du district.

   Ce service est composé d'un chef de service ING et d'un cadre d'étude comme on le vois dans la figure si dessous :

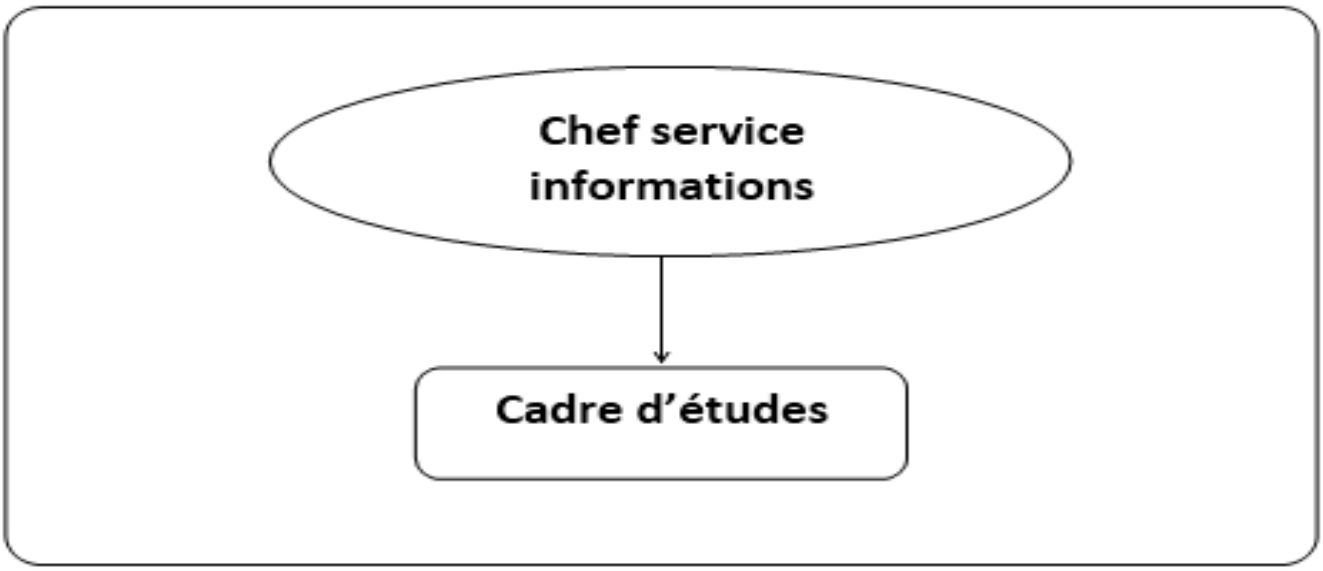


FIG. 2.3 – Organigramme du service information de gestion

## 2.3 Étude de l'existant

### 2.3.1 Problématique et travail demandé

Le réseau de NAFTAL possède un accès à Internet. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps.

L'utilisation massive de l'internet par les employés de l'entreprise ralenti la vitesse de la connexion ce qui engendre un ralentissement dans leurs taches.

Le serveur d'ISA est mis place, mais aucun filtrage entrant et sortant, alors après la reconfiguration de serveur ISA l'accès vers Internet doit être accessible le plus rapidement possible, afin d'optimiser les performances de travail. De plus, nous nous intéresserons à sécuriser le réseau en filtrant certain site soit ces derniers sont malveillant ou il ne correspond pas au domaine d'activité de l'entreprise.

### 2.3.2 Présentation du réseau NAFTAL

Le réseau actuel de l'entreprise NAFTAL est un réseau Ethernet commuté à 100 Mbps et d'une connexion internet ANIS d'une bande passante de 2Mo : constitué de 93 postes interconnectés entre eux par une cascade de 14 commutateurs , essen-

tiellement basés sur une topologie en étoile.

Le bloc administratif de l'entreprise de NAFTAL comporte un câblage réseau normalisé : des câbles fibre optique et des câbles paires torsadés ; le bloc en question, ne comporte malheureusement pas de subdivision, ni en sous-réseau, ni en celle de VLAN, et le plan d'adressage de réseau privé est basé sur cette adresse 192.168.168.0/24 avec un maque 255.255.255.0, toutes les machines clientes DHCP recevront une adresse dans cette plage, avec comme passerelle par défaut 192.168.168.1.

Le serveur ISA sépare le réseau privé du réseau externe, afin d'assurer les fonctions de proxy (options de cache Web) dont l'objectif est d'améliorer les performances des requêtes WEB et pour que les utilisateurs sentent suivis et restent sages dans leurs recherches.

### 2.3.3 Architecture du réseau existant

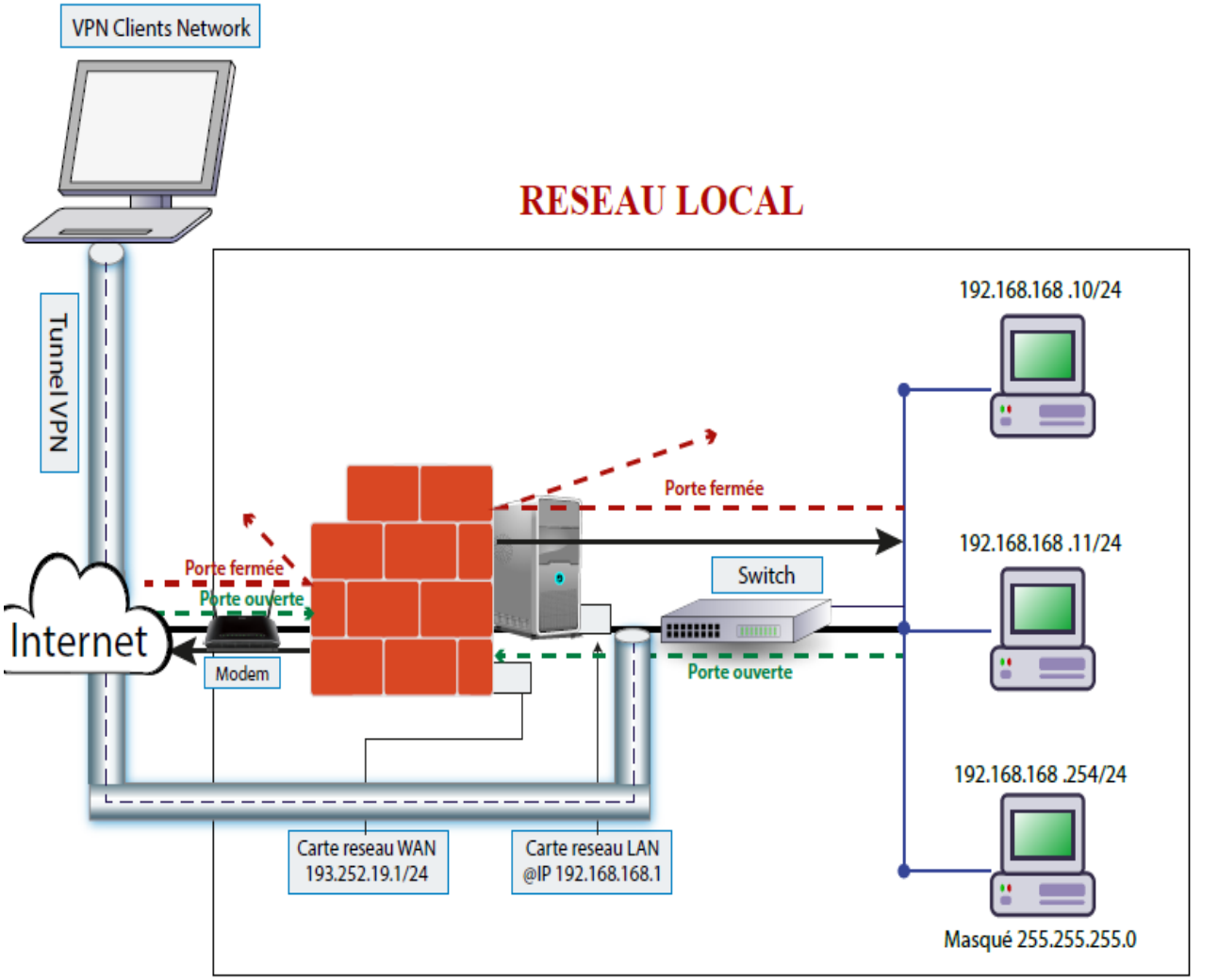


FIG. 2.4 – Architecture du réseau existant

### 2.3.4 Analyse de parc informatique

#### 2.3.4.1 Unités Centrales

Le parc informatique de NAFTAL compte environ 93 ordinateurs, de marque ACER, HP, FUJITSU, IBM, la configuration est généralement comme suit :

- CPU : Core 2 Duo, I3 et I7.
- mémoire RAM : entre 02 et 04 GO.
- disque dur entre 160 et 500 GO.

- système d'exploitation installé au niveau des différents postes de travail est : Windows7
- office version 2013.

Tous les postes de travail disposent d'un antivirus installé (Kaspersky) qui vérifie en permanence les fichiers de l'ordinateur. La mise à jour de l'antivirus est paramétrée, et un scan se fait régulièrement à chaque démarrage.

On constate que la configuration matérielle répond aux exigences minimales :

- configuration des applications ;
- exploitation facile ;
- assurance d'une rapidité des traitements ;
- protection maximale des ordinateurs contre les verus informatique ;

#### 2.3.4.2 Imprimantes

L'entreprise possède 13 imprimantes de différentes marque HP, EPSON, CANON, LEXMARK, ou l'on distingue deux types : celles dotées d'une interface réseau et d'autres ne possédant pas. Chaque service possède une imprimante soit configurée et reliée directement sur une prise réseau, soit partagée sur un poste de travail.

#### 2.3.4.3 Les commutateurs

Les différents postes de travail sont interconnectés via des switches en cascade, les switch envoient uniquement le trafic vers la destination voulue, l'utilisation de ce dernier réduit les risques d'intrus et attaques d'écoute. Tous les postes de travail connectés au réseau sont placés sur le même segment.

#### 2.3.4.4 Câblage Informatique

Le système de câblage informatique, installé dans l'entreprise de NAFTAL, est conçu et installé dans les normes, et cela, pour éviter les déconnexions. Tous les équipements informatiques existant dans la société sont interconnectés via le câblage de type paire torsadé catégorie 6 et fibre optique.

Les boitiers des prises murales «prise Rj45» sont identifiés par des étiquettes portant un numéro unique sur le réseau, et qui est répété également dans le panneau de brassage pour l'interconnexion avec les commutateurs.

#### 2.3.4.5 Serveur ISA 2006

actuellement ISA server est installé uniquement dont l'objectif est d'améliorer les performances des requêtes WEB : Un client du proxy Web envoi directement les demande vers l'ordinateur ISA server.

L'environnement de l'installation d'ISA server 2006 : ISA server est installé sur un Windows Server 2003 dont la configuration système de server ISA est comme suit :

- un processeur à 3.0 gégahertz (GHz) ;
- système d'exploitation de l'ordinateur est un Microsoft Windows 2003 Server avec le Service Pack 1 ;
- 6 GO de mémoire vive ;
- 500 GO d'espace disque disponible ;
- deux cartes réseaux ;

## 2.4 Critique de l'existant

Durant notre stage, nous avons pu constater une réelle nécessité d'apporter des améliorations au niveau de la sécurité malgré que le parc informatique de l'entreprise NAFTAL répond à la plupart de leurs besoins, et comme ce dernier ne cessent d'évoluer, l'internet est devenu une ressource importante, et l'accès vers ces ressources doivent être accessibles le plus rapidement possible, afin d'optimiser les performances de travail.

La configuration actuelle d'ISA server ne dispose aucun filtrage sortant, ce qui laisse les employés à utiliser l'internet en dehors le cadre de travail ce qui cause le ralentissement de la vitesse de la connexion, ni d'aucun filtrage entrant, ce ci laisse libre court aux potentielles d'attaques et vols d'informations dont peut être victime les ordinateurs de de l'administration.

Pour toutes ces raisons, nous avons opté pour la reconfiguration d'ISA Server de façon fiable et irréprochable, afin de résoudre la problématique déjà signalée.

## 2.5 Solutions proposées

Le serveur ISA est mis en place doit être assuré les fonctions de filtrages avancés, en garantissant une protection plus efficace du réseau privé et une navigation Inter-

net plus rapide.

Après la reconfiguration de serveur ISA le premier mécanisme de sécurité qui serait appliqué pour contrôler les accès au réseau de l'entreprise NAFTAL est l'authentification des utilisateurs. La politique mise en place aura pour rôle d'assurer l'accès à des ressources uniquement aux personnes autorisées.

Le deuxième mécanisme est d'appliquer les mêmes interdictions et autorisations à tous les utilisateurs comment suit :

- autoriser les navigations Web ;
- autoriser les téléchargements des fichiers ;
- bloquer les téléchargements dans l'extension (.MP4, .FLV) ;
- bloquer le téléchargement TORENT (Peer-To-Peer) ;
- l'autorisation de la messagerie (courriel électronique) ;
- bloquer tous les ports inutiles.

Maintenant que tous les droits d'accès du réseau LAN au réseau WAN selon le besoin sont définis, ne reste qu'à définir les numéros de port correspondant aux règles de passage du firewall.

## 2.6 Méthodes et Techniques

### 2.6.1 Méthodes

Dans un premier temps nous traitons l'installation d'un système d'exploitation serveur «Windows 2003 Server Entreprise Edition», recommandé par Microsoft pour la mise en place du serveur ISA 2006 edition entreprise. Puis la configuration des éléments système contributeurs au bon fonctionnement du serveur :

- **Configuration de service d'annuaire Active Directory :** ISA Server 2006 peut être configuré pour filtrer l'application des règles selon des ensembles d'utilisateurs. Ces derniers peuvent être entre autres des utilisateurs ou des groupes du domaine Active Directory ;
- **Configuration de serveur DNS :** le DNS dans Windows server 2003 offre la résolution de noms de domaine.
- **Configuration de DHCP :** le DHCP dans Windows Server offre des fonctionnalités de paramétrages valides pour tous les clients sur le réseau de manière

dynamique. Les clients DHCP renouvellent automatiquement leur allocation d'adresse en arrière-plan. Avec le basculement DHCP. Dans un second temps nous traitons l'installation de serveur ISA 2006 Entreprise Edition, et l'installions de service pack 1 d'ISA server 2006, par la suite il nous faut donc installer ISA server 2006.

Enfin nous traitons la configuration d'ISA server 2006 en exploitant les deux cartes réseaux du serveur, une pour le réseau interne et l'autre pour le réseau externe. Nous allons voire cette configuration en détail dans le chapitre de réalisation.
Afin d'assurer les règles de filtrage, deux mesures doivent être prises :

- toutes les requêtes http, https du réseau local doivent passer par le serveur ISA ;
- protocoles autorisés pour la messagerie : SMTP, POP3, IMAP3 ;
- protocole autorisé pour le téléchargement : FTP ;

### 2.6.2 Techniques

Après avoir vu les méthodes de résolution choisies, nous allons présenter les outils nécessaires utilisés pour qu'elle soit élaborée.

### 2.6.3 Virtual Box

Virtual Box ou machine virtuelle est un logiciel de ritualisation de systèmes d'exploitation. En utilisant les ressources matérielles de l'ordinateur (système hôte), Virtual Box permet la création d'un ou de plusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation (systèmes invités).

Les systèmes invités fonctionnent en même temps que le système hôte, mais seul ce dernier a accès directement au véritable matériel de l'ordinateur. Les systèmes invités exploitent du matériel générique, simulé par un " faux ordinateur " (machine virtuelle) créé par Virtual Box.

Virtual Box permet de faire fonctionner plus d'un système d'exploitation en même temps en toute sécurité. En effet, les systèmes invités n'interagissent pas directement avec le système hôte, et n'interagissent pas entre eux. Le champ d'action des systèmes invités est confiné, limité à leur propre machine virtuelle [11].

### 2.6.4 Serveur Windows 2003 Server Entreprise Edition

Windows Server 2003 est un système d'exploitation orienté serveur développé par Microsoft. Il est considéré par Microsoft comme étant la pierre angulaire de la ligne de produits serveurs professionnels system. Les versions évoluées de ce système intitulé comme suit [12] :

- Windows Server 2003 R2 ;
- Windows Server 2008 ;
- Windows Server 2008 R2 ;
- Windows Server 2012 ;
- Windows Server 2012 R2 ;
- Windows Server 2016.

Les fonctionnalités qui sont apportées par les services de Windows Server 2003 incluent :

1. **Assistant de configuration de la Sécurité :** un outil qui permet aux administrateurs d'effectuer plus facilement des recherches et modifications relatives aux stratégies de sécurité.
2. **Hot Patching :** cette fonctionnalité permet d'étendre la capacité de Windows Server 2003 à mettre à jour des fichiers **DLL**, des **pilotes**, et des **patches non-kernel** sans avoir à effectuer un redémarrage.
3. **IIS 6.0 Metabase Auditing :** cette fonctionnalité permet d'auditer les modifications apportées au méta base IIS.
4. **Les Autres améliorations réseaux :** concernent le support des Services de Fournisseurs Sans-fil (Wireless Provisioning Services), un meilleur support de l'IPv6, et de nouvelles protections contre les attaques réseaux de type SYN flood TCP.
5. **Mises à jour de sécurité post-installation :** il s'agit du mode qui est activé par défaut lorsqu'un serveur démarre pour la première fois après l'installation du Service Pack 1. Il configure le pare-feu pour qu'il bloque toutes les connexions entrantes et invite l'utilisateur à appliquer les mises à jour de sécurité.

### 2.6.5 Active directory

Active directory sert d'annuaire des objets du réseau, utilisé pour stocker des informations relatives aux ressources réseau sur un domaine. Il fournit des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows [13].

### 2.6.6 ISA server 2006

ISA signifie Internet Security and Accélération Server, il est disponible en édition Standard mais aussi en édition Entreprise [14] :

- ISA Server standard edition : limitée à 4 processeurs, les stratégies de configurations sont définies localement, intégration à active directory limitée.
- ISA Server Entreprise Edition : mise en cache distribuée, aucune limite d'exploitation du nombre de processeurs, gestion centralisée des stratégies de configuration.

Différents modes d'installation sont disponibles sous ISA afin d'adapter ISA au rôle qui lui a été confié :

- **Mode Cache :** le mode cache permet d'améliorer les performances d'accès à Internet en stockant localement les fichiers les plus consultés par les utilisateurs ce qui permet d'optimiser la bande passante d'accès à Internet.
- **Mode pare-feu :** permet de sécuriser le trafic réseau à l'aide de règles et d'identifier différentes attaques connues.
- **Mode intégré :** le mode intégré cumule les fonctionnalités du mode cache et du mode pare-feu.

### 2.6.7 Nouvelle architecture du réseau proposé

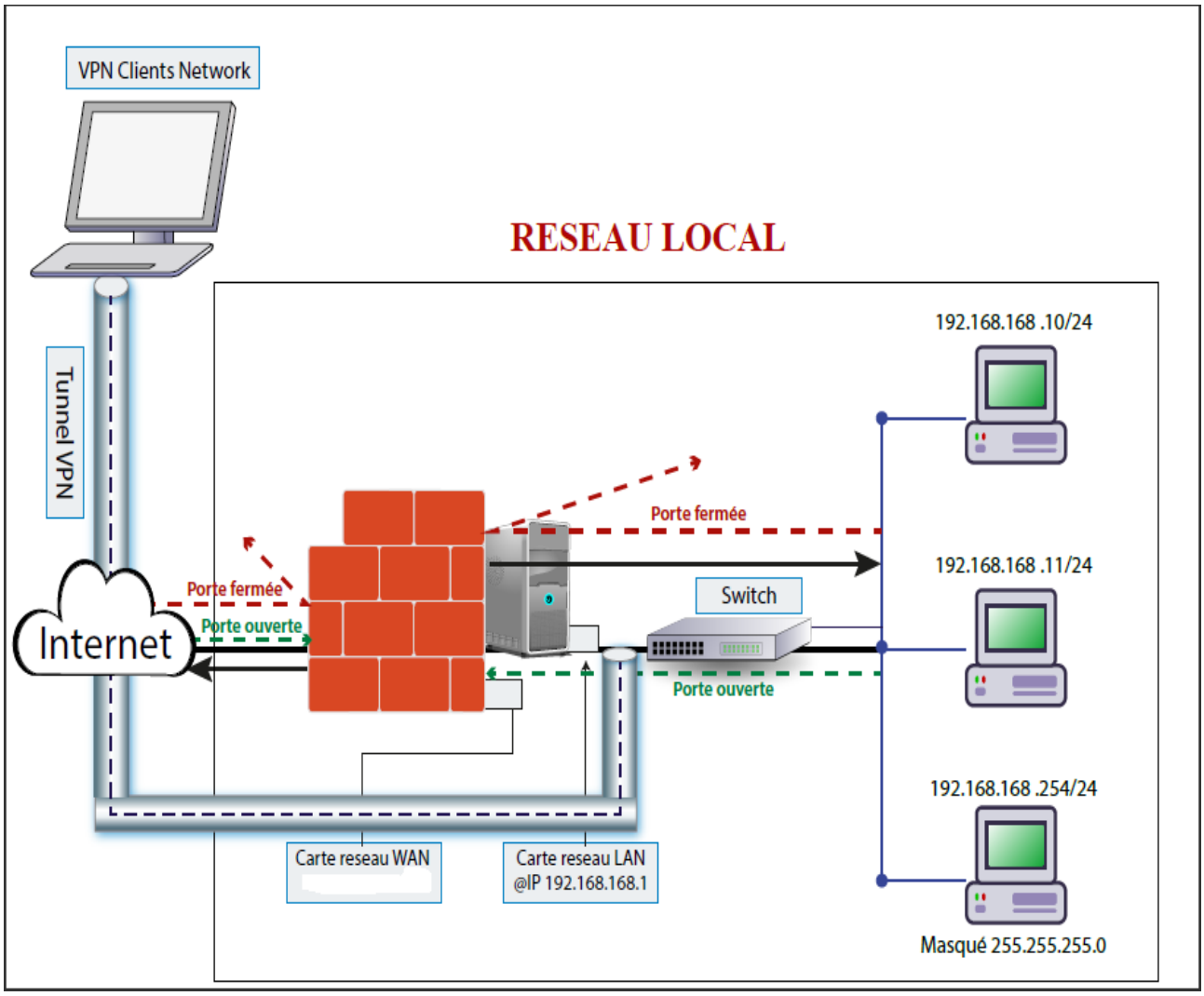


FIG. 2.5 – architecture du réseau proposé

## 2.7 Conclusion

Dans ce chapitre nous avons présenté l'entreprise et les problèmes découverts dans son réseau qui exposent une absence de contrôle des connexions sortantes et entrantes, ainsi le problème lié au manque de débit en bande passante. Dont l'objectif de notre projet est de renforcer la sécurité en reconfigurant le logiciel ISA SERVER 2006 .

Chapitre 3

# Instalation et configuration de serveur ISA

## 3.1 Introduction

Ce chapitre a pour objectif majeur de présenter le notre solution. C'est la phase de l'installation et la configuration du serveur ISA 2006. Ce chapitre est composé de deux parties principales : la première présente l'environnement d'installation alors que la seconde partie concerne la l'installation et configuration de ISA serveur.

## 3.2 Installation et configuration d'un serveur Windows 2003

Pour que nous puissions installer le serveur ISA on doit d'abord installer un serveur Windows, dans notre cas on veux installer Windows serveur 2008, mais malheureusement après leur installation et configuration on a découvert qu'il n'est pas compatible, donc on les a installé sur Windows serveur 2003.

Premièrement on a installes le serveur Windows 2003. Une fois notre serveur est installé on doit le configurer et le paramétrer pour le rendre fonctionnel sur notre réseau Windows serveur 2003 nous offre plusieurs rôles de base mais dans notre cas on a choisi la configuration suivante :

- configure le service active directory afin de gère les utilisateurs ; pour les faire on a choisi de créé un nouveau domaine racine que nous a nommée NAFTAL.LOCAL sur ce domaine on ajoute les utilisateurs.
- installer et configurer le serveur DHCP pour qu'il attribue automatiquement les adresses IP aux utilisateurs.

- installer et configurer le serveur DNS afin qu'il gère le nom du domaine sur Internet .

Avant de passe a l'installation de ISA on doit configura les deux carte réseau comme suit :

La première carte réseau on la configure en mode pont, pour quel pont a la carte réseau physique de l'hôte.

La deuxième carte réseau on la configure en mode réseau local ce mode permet à plusieurs machine d'être dans un réseau isolé, comme un VLAN.

## 3.3 Installation et configuration de serveur ISA 2006

### 3.3.1 l'installation d'ISA

Après l'installation et la configuration du serveur Windows 2003 on passe à l'installation du serveur ISA 2006 Edition Entreprise.

1. On premier lieu nous avons lancé le programme d'installation qui nous a affiché la fenêtre ci-dessous. Pour commencer l'installation on a cliqué sur «installer ISA serveur 2006 »

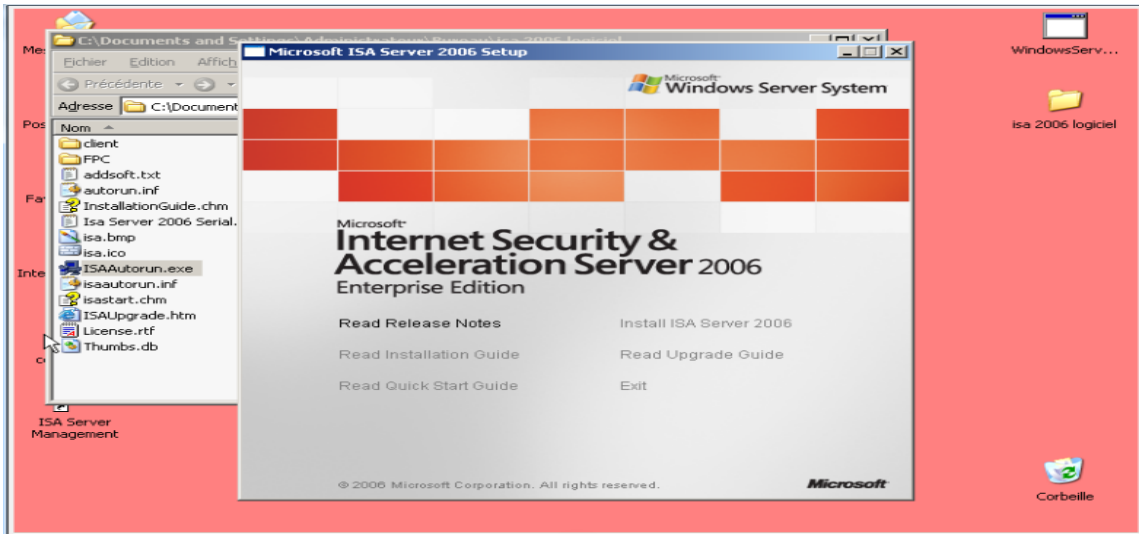


FIG. 3.1 – L'étape 1 d'installation d'ISA serveur 2006

2. La fenêtre suivante nous apparait dans cette étape on séléctionné «*I accept the terms in the license agreement*».


FIG. 3.2 – L'étape 2 d'installation d'ISA serveur 2006

3. Cette interface nous donne l'accès pour nommer notre machine (Naftal), et de saisir la clé de la licence. Donc on doit cliquer sur "*NEXT*" pour passer à l'étape suivante.

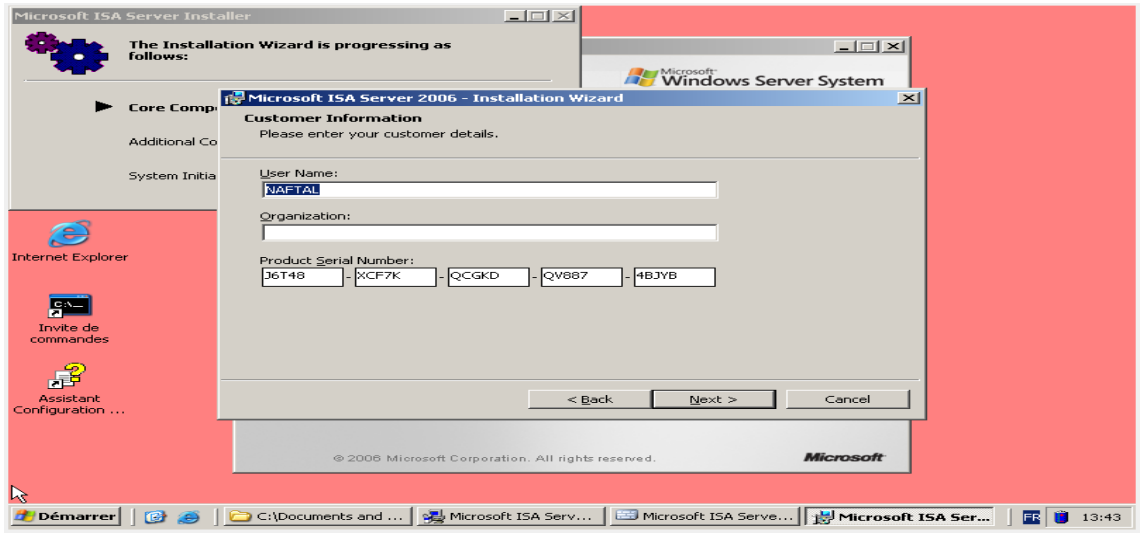


FIG. 3.3 – L'étape 3 d'installation d'ISA serveur 2006

4. Sur la page scénarios d'installation, nous avons choisi le troisième choix " *Install both ISA server services and configuration storage server* ". Pour avoir

la base de données de configuration ainsi que les services d'ISA.

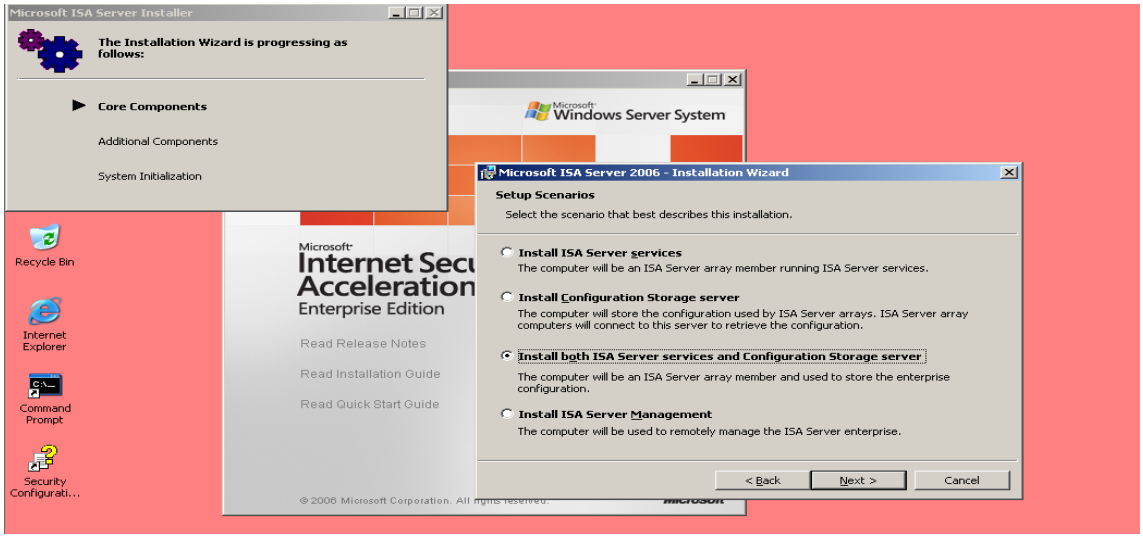


FIG. 3.4 – L'étape 4 d'installation d'ISA serveur 2006

5. Sur la fenêtre suivante on active tous les icones pour avoir tous les modes l'installation.

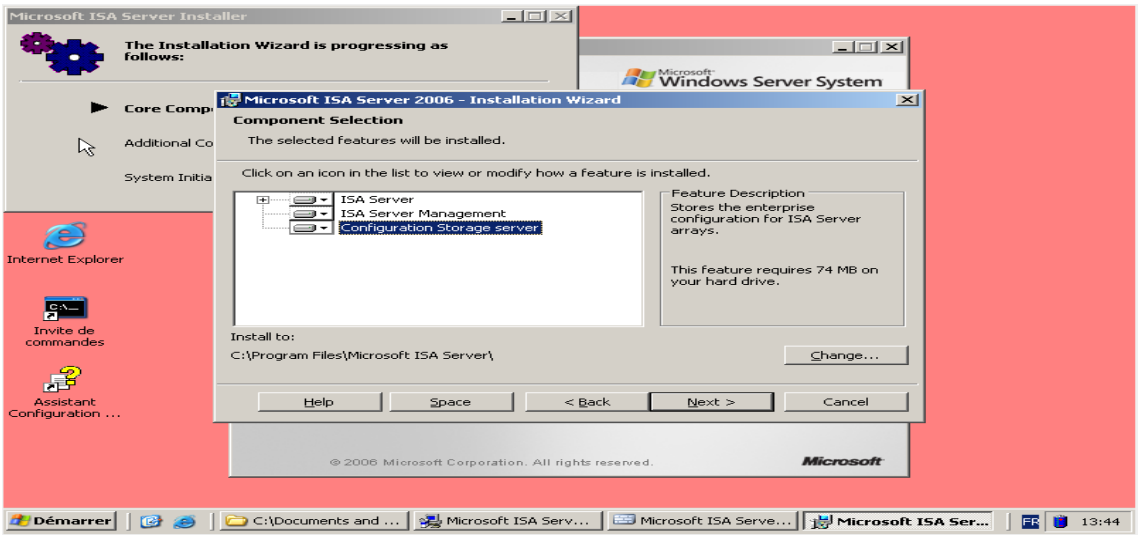


FIG. 3.5 – L'étape 5 d'installation d'ISA serveur 2006

6. Sur la page Options d'installation de l'entreprise, nous avons choisi " *create a new ISA Server entreprise* " car notre serveur et le seul serveur ISA dans l'entreprise.

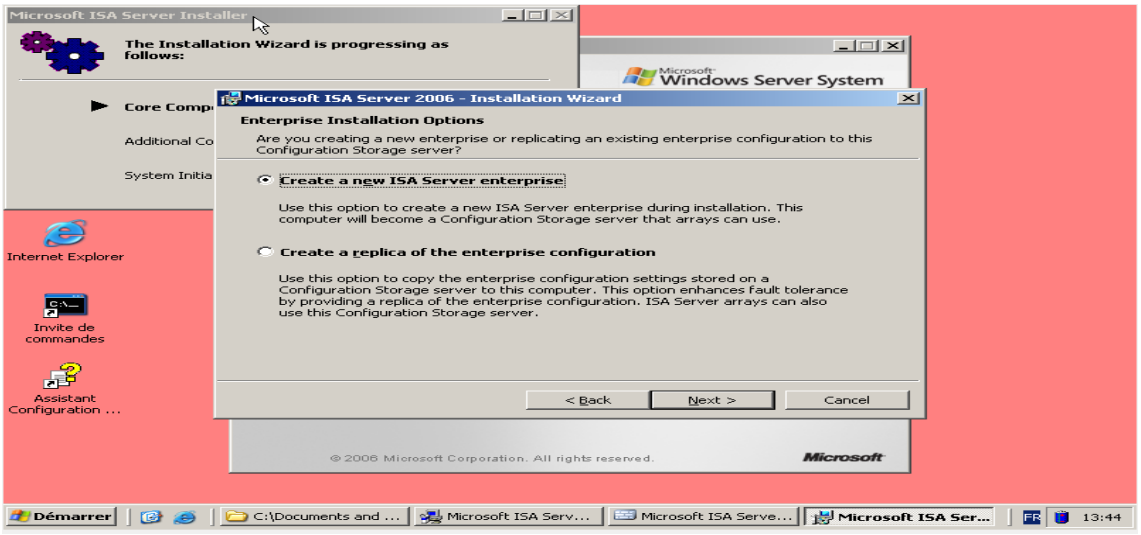


FIG. 3.6 – L'étape 6 d'installation d'ISA serveur 2006

7. Dons cette interface nous allons donner un nom et un mot de passe pour l'administrateur de réseau. Nous on a nomme notre utilisateur par administrateur et on lui affecter un mot de passe. Puis on clique sur "*NEXT*".

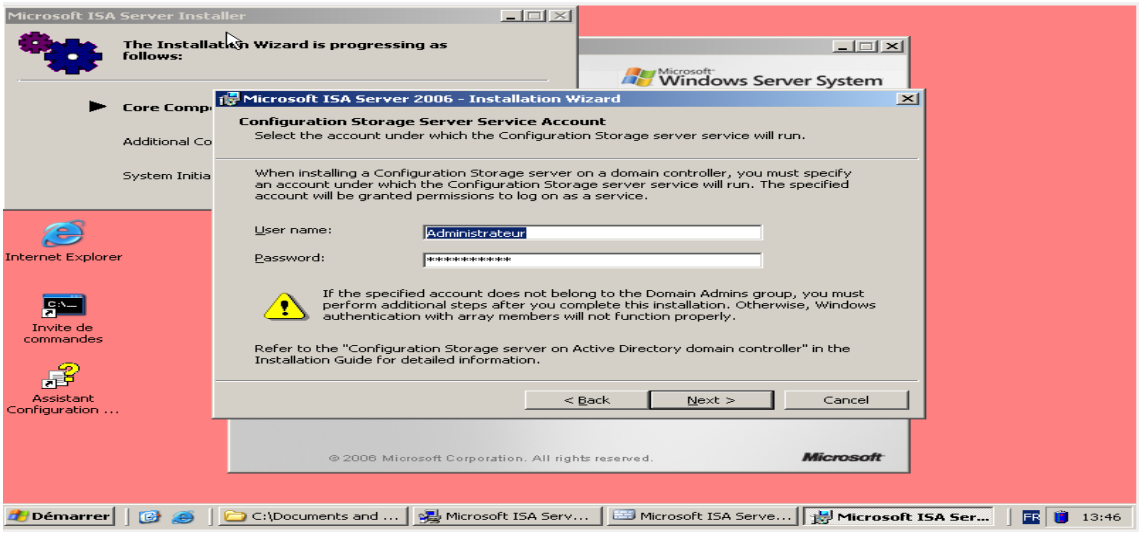


FIG. 3.7 – L'étape 7 d'installation d'ISA serveur 2006

8. Etape suivante nous donne l'accès pour selectioner une carte reseau. En cliquant sur ajouter pour avoir la fenetre au dessous on a selectionné la carte réseau interne pour filtrer le trafic sortant de l'entreprise .

9. Dans cette etape nous allons specifier la plage d'adressage que nous avons

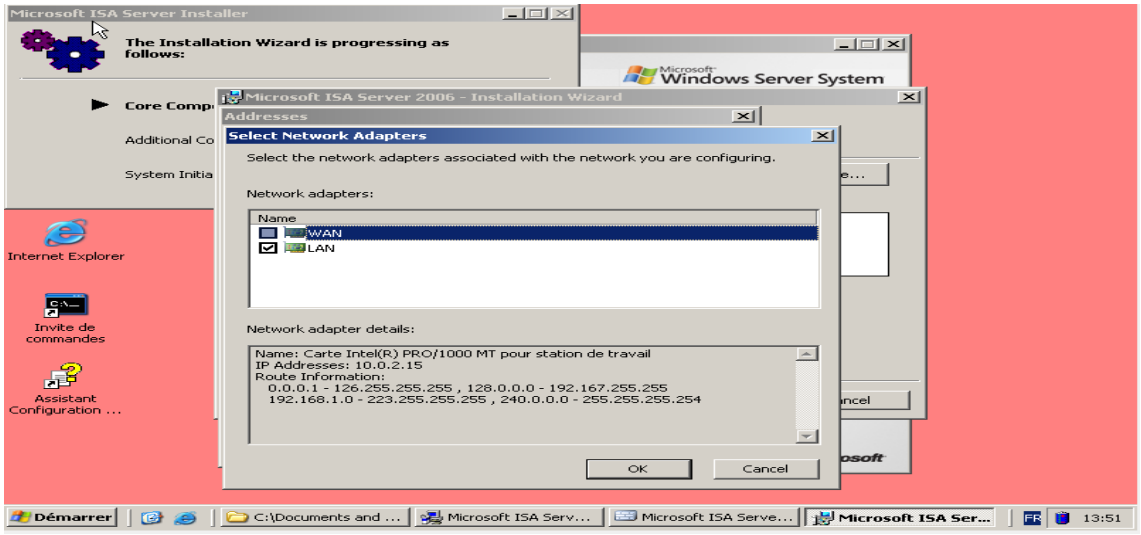


Fig. 3.8 – L'étape 8 d'installation d'ISA serveur 2006

affecter pour notre carte reseau.

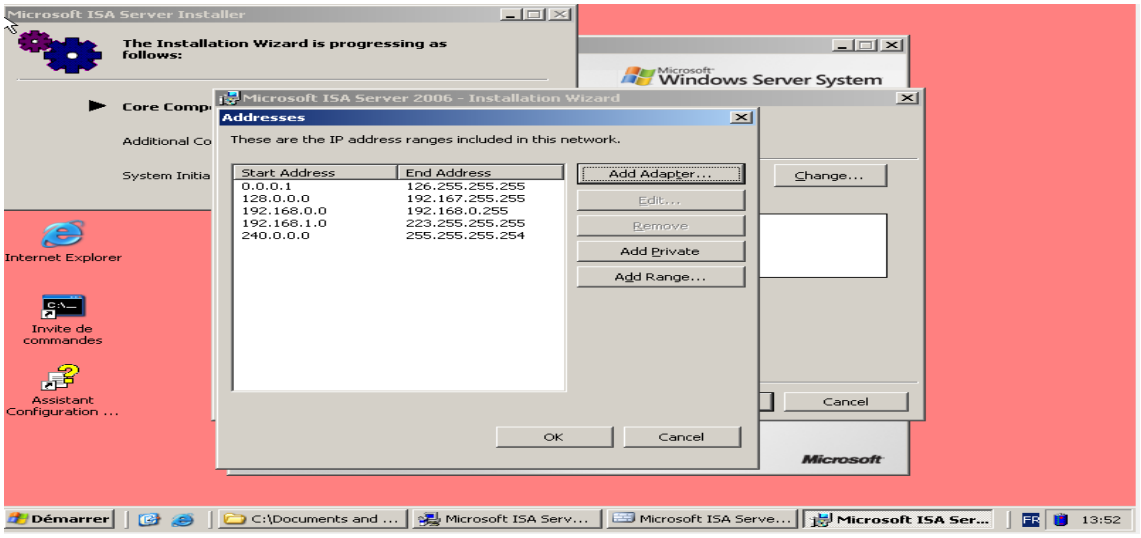


Fig. 3.9 – L'étape 9 d'installation d'ISA serveur 2006

10. Finalement, le processus d'installation a commencé on patiente un peu pour qu'il termine.

11. On cliquesur "*Finish*" pour terminé l'instalation .

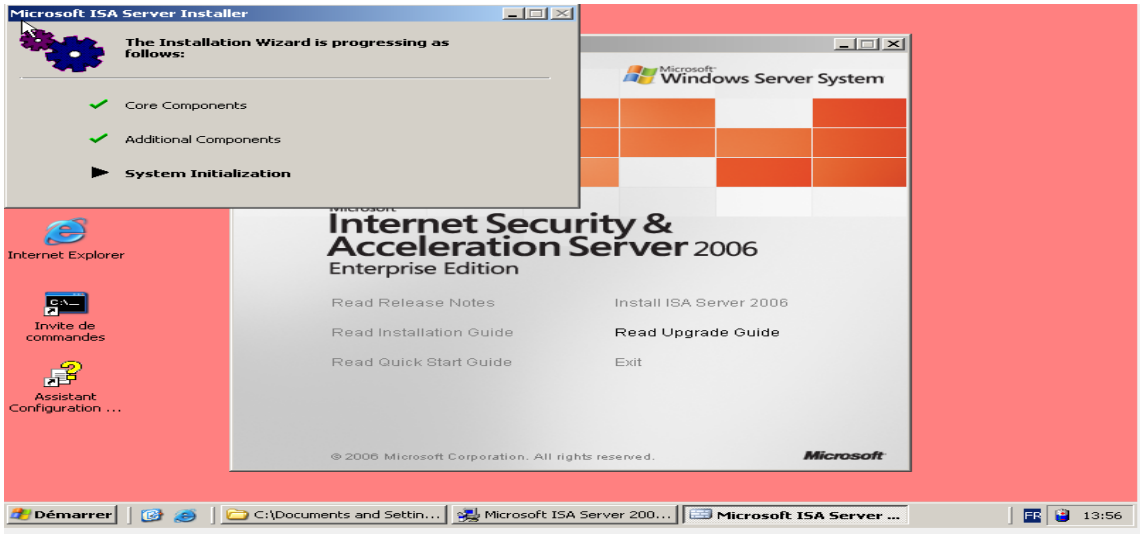


FIG. 3.10 – L'étape 10 d'installation d'ISA serveur 2006

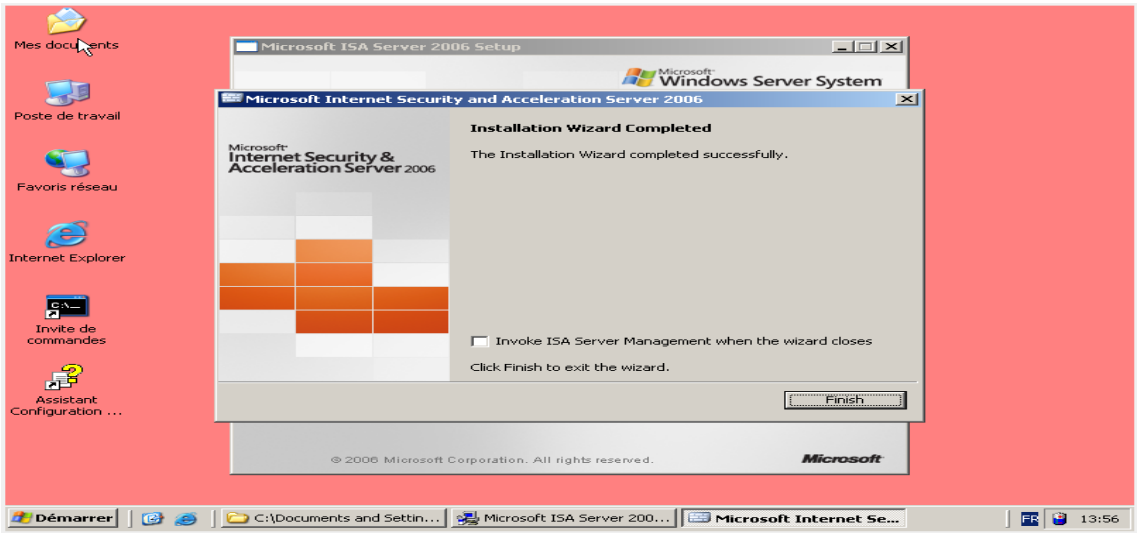


FIG. 3.11 – L'étape 11 d'installation d'ISA serveur 2006

## 3.4 La configuration

a) La configuration de la règle 1 "autoriser la navigation web" :
la première règle nous permet d'autoriser la navigation web (HTTP et HTTPS),et le téléchargement des fichiers (FTP). Pour la configurer procède comme ceci :
après l'installation d'ISA et son exécution l'interface ci dessous nous apparait :

1. On clique sur stratégie des pare-feu puis créer une règle et on obtient la fenêtre suivante :

Dans l'espace on donne le nom de la règle d'accès que nous avons nomme

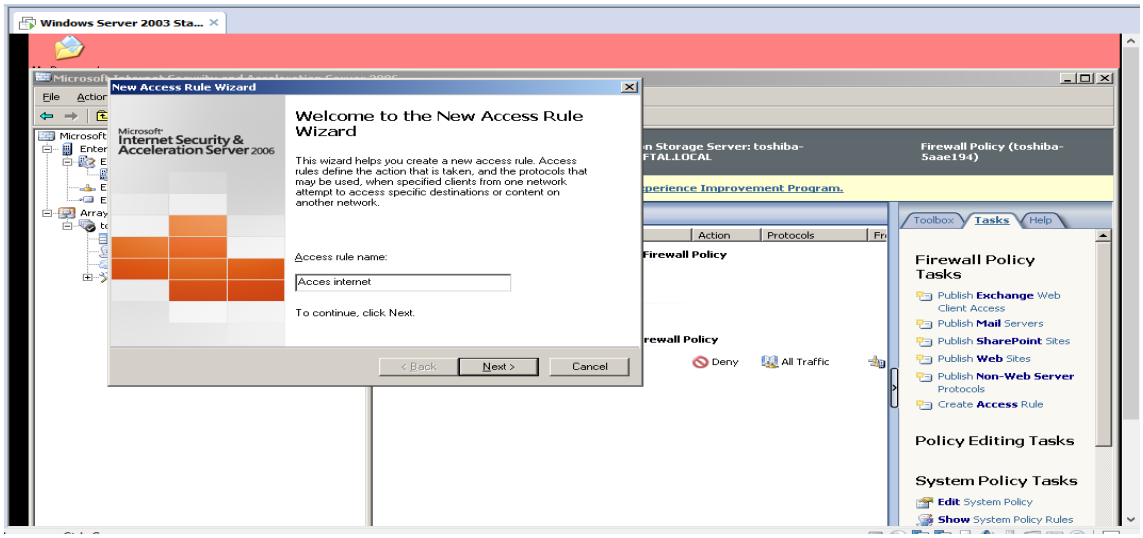


FIG. 3.12 – L'étape 1 de la configuration de la régle 1

Accès internet et on clique sur " next " pour avoir l'interface suivante.

2. Dans l'étape suivante, l'assistant nous donne deux actions sur la règle soit : d'autoriser ou de refuser l'accès. Nous on autorise l'accès on sélectionne " *Allow* ".

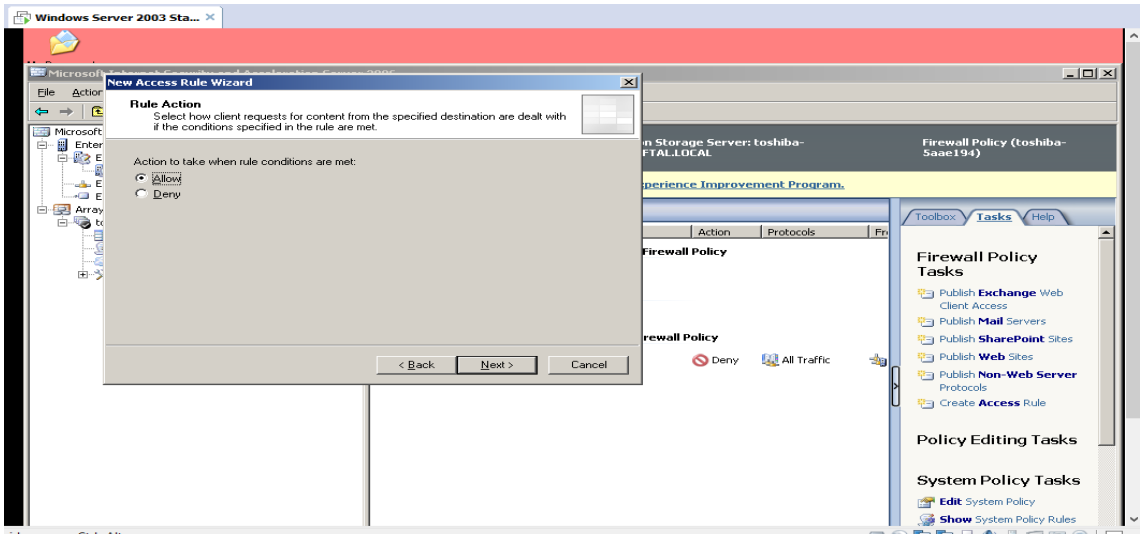


FIG. 3.13 – L'étape 2 de la configuration de la régle 1

3. On clique sur " *next*" l'interface ci-dessus nous apparaisse. Cette fenêtre nous donne l'accès d'ajouter, modifier et supprimer les différents type de protocole par exemple protocole mail, protocole web ...etc. Donc en clique sur " *add* " et on sélectionne web pour avoir les protocoles web, ainsi on

ajoute les protocoles : FTP, http et https.

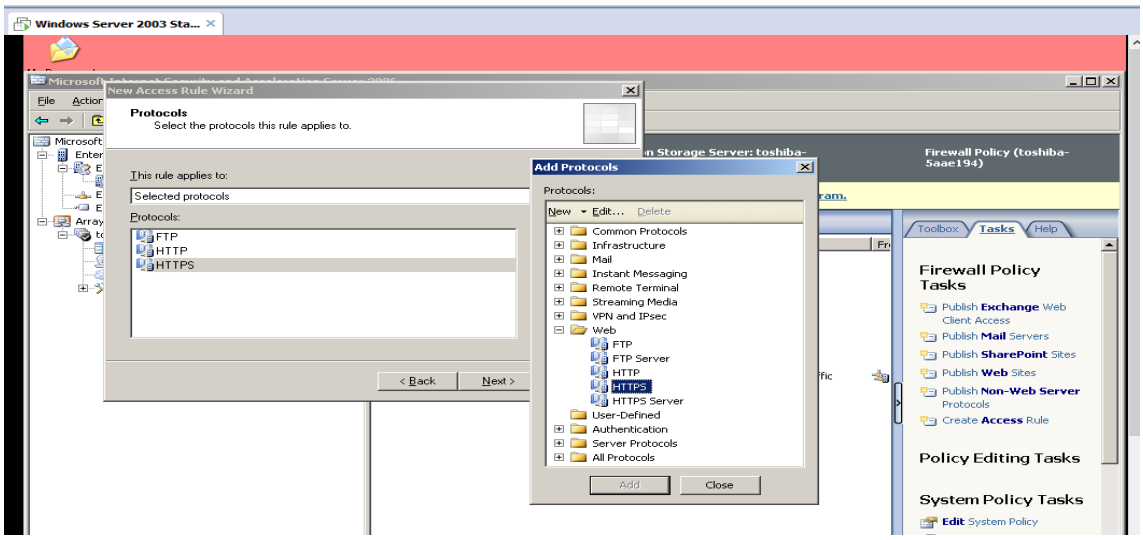


FIG. 3.14 – L'étape 3 de la configuration de la régle 1

4. Apre la fermeture de la liste des protocoles on aura la fenêtre suivante qui nous donne tout les accès cites auparavant dans notre cas on clique sur "*next*" pour avoir l'étape suivante.

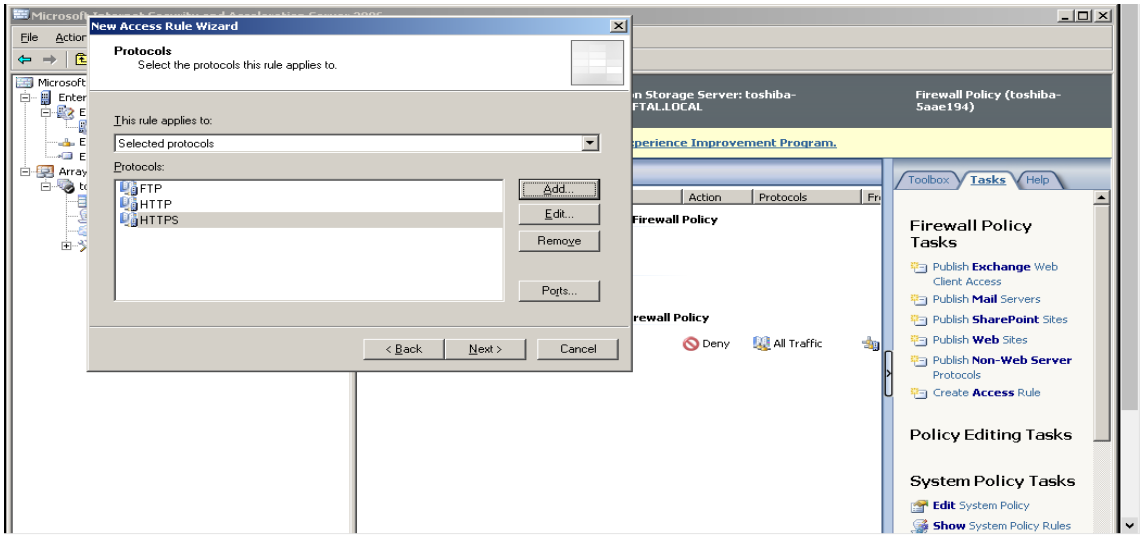


FIG. 3.15 – L'étape 4 de la configuration de la régle 1

5. Dans l'étape suivante, on choisi de bloquer ou d'autoriser l'accès de l'intérieur vers l'extérieur ou le contraire. Dans notre cas on autorise l'accès du réseaux

local vers le réseau externe donc on ajoute " *internal* " pour dire qu'on autorise l'accès depuis le réseau interne (figure5) et " *external* " pour autoriser ver le réseau externe ( figur6) .

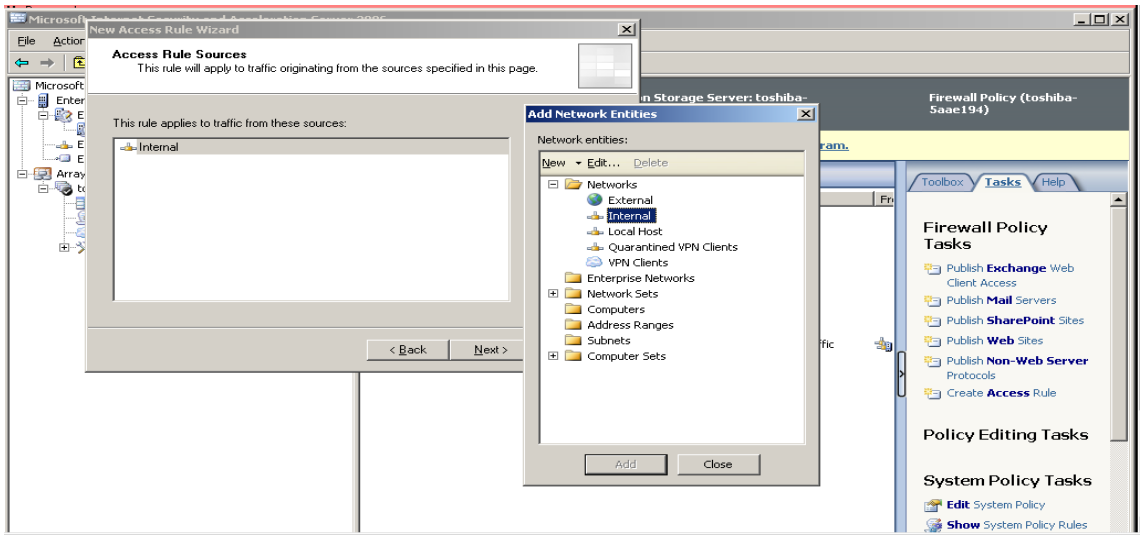


FIG. 3.16 – L'étape 5 de la configuration de la régle 1

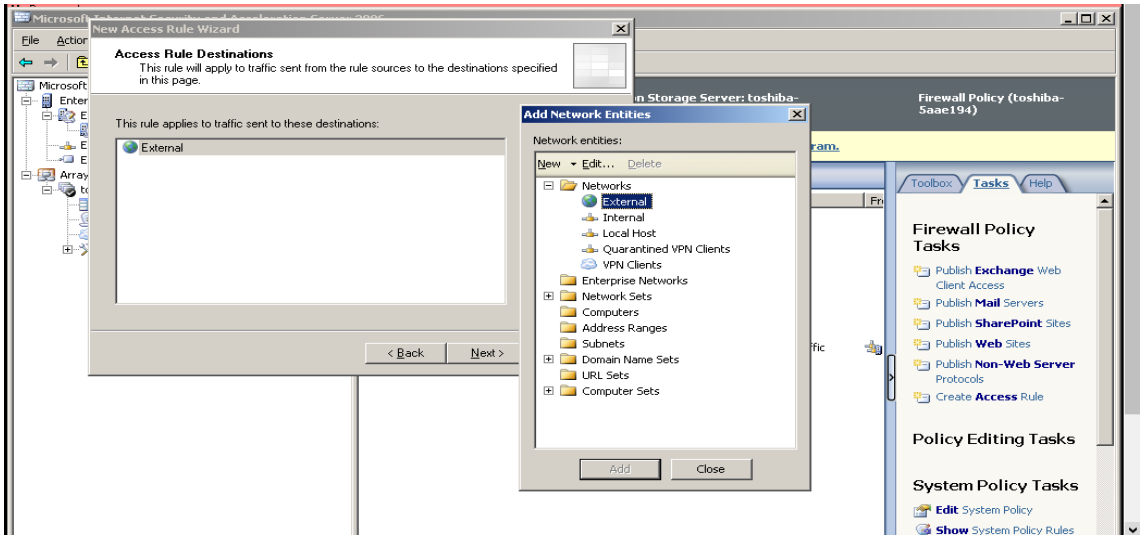


FIG. 3.17 – L'étape 6 de la configuration de la régle 1

6. Dans cette fenêtre on ajoute les utilisateurs sur lesquels on applique la règle. Nous on ajoute tout les utilisateurs car dans notre entreprise les droits d'accès sont les même pour tout les utilisateurs.

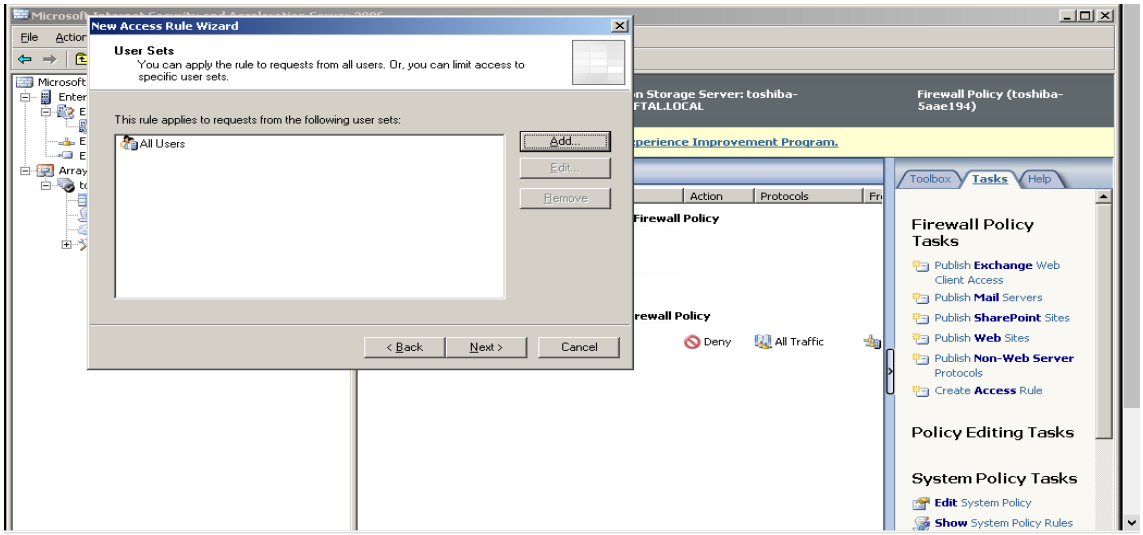


FIG. 3.18 – L'étape 7 de la configuration de la régle 1

7. Finalement, on a la fenêtre suivante qui nous résume notre configuration. On clique sur "*Finish* " pour terminer la configuration

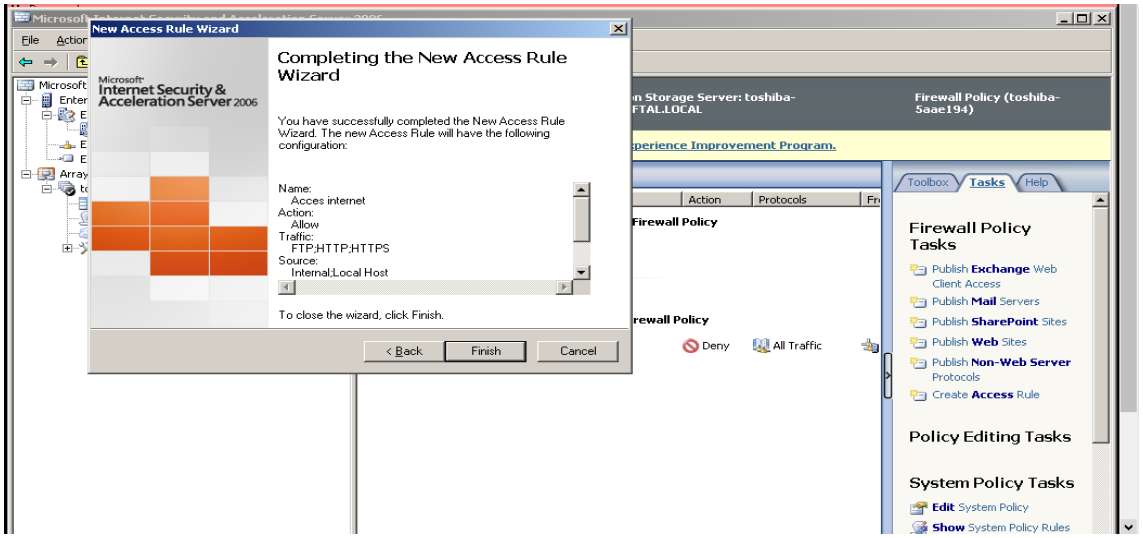


FIG. 3.19 – L'étape 8 de la configuration de la régle 1

8. Une fois la règle créee, il faut cliquer sur " *Appliquer* " pour qu'elle soit prise en compte.

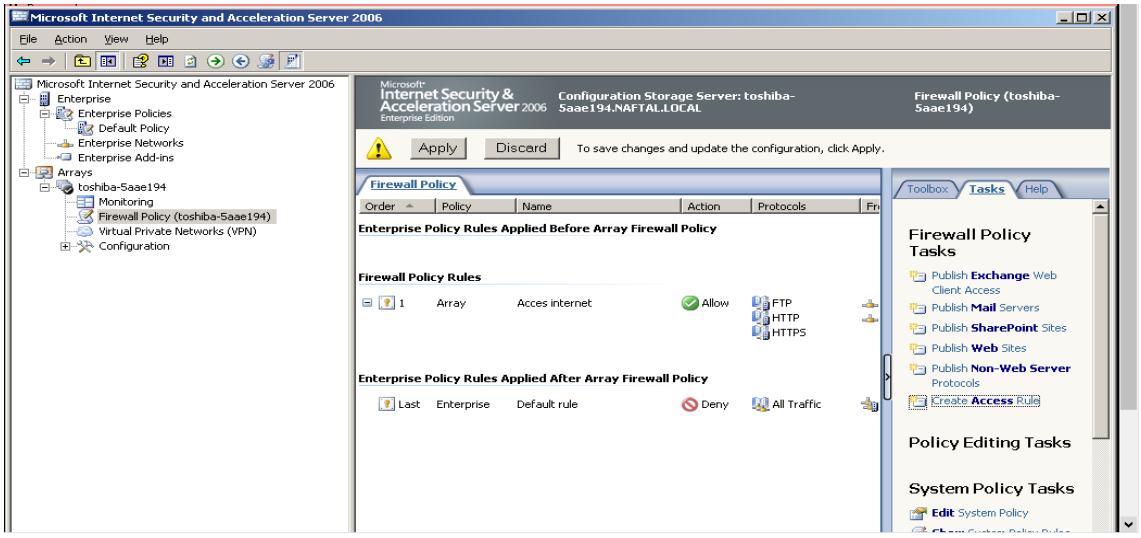


FIG. 3.20 – L'étape 9 de la configuration de la régle 1

b) La configuration de la règle 2 "Autoriser le ping" :

Pour configurer la règle 2 on suit les mêmes étapes de la règle 1 mais dans cette règle la différence est dans les étape 3 et 5.

1) Dans cette étape on nomme notre règle "Ping".

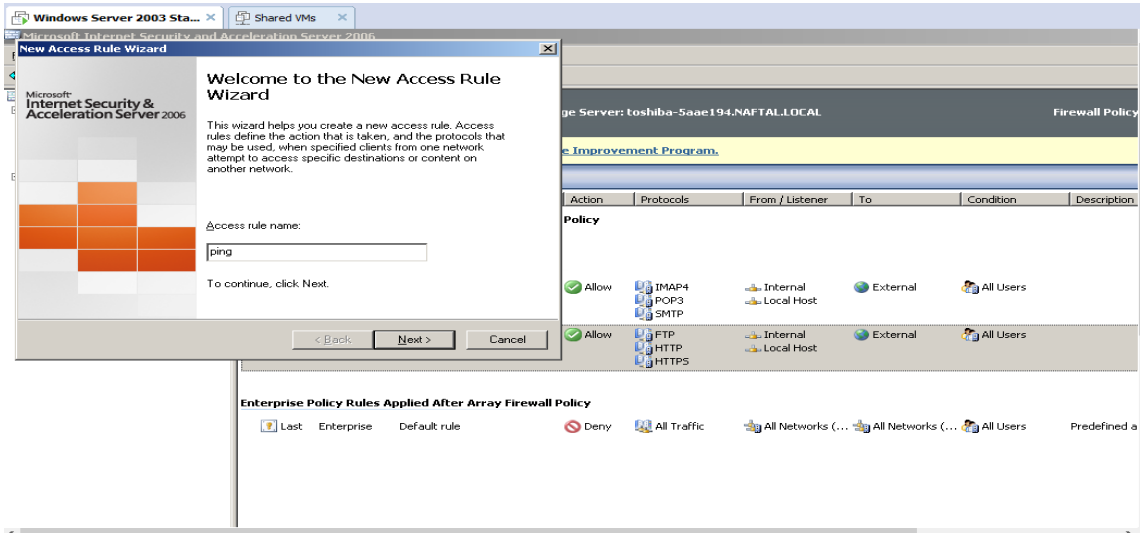


FIG. 3.21 – L'étape 1 de la configuration de Ping

2) On sélectionne Ping sur la liste des protocoles.

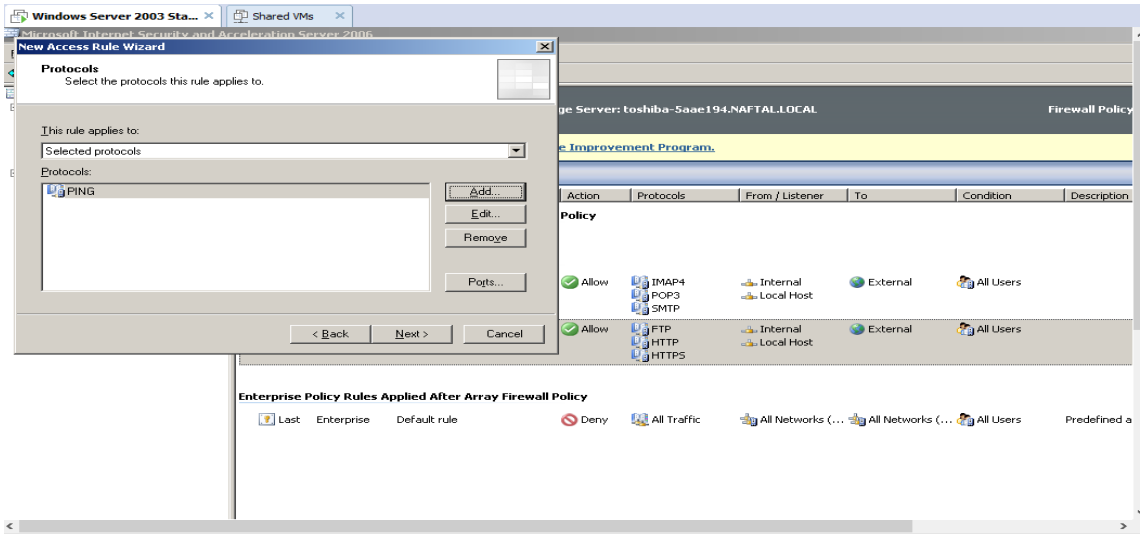


FIG. 3.22 – L'étape 2 de la configuration de Ping

3) L'étape 5 on choisi d'autoriser le Ping de l'intérieur ver l'intérieur.

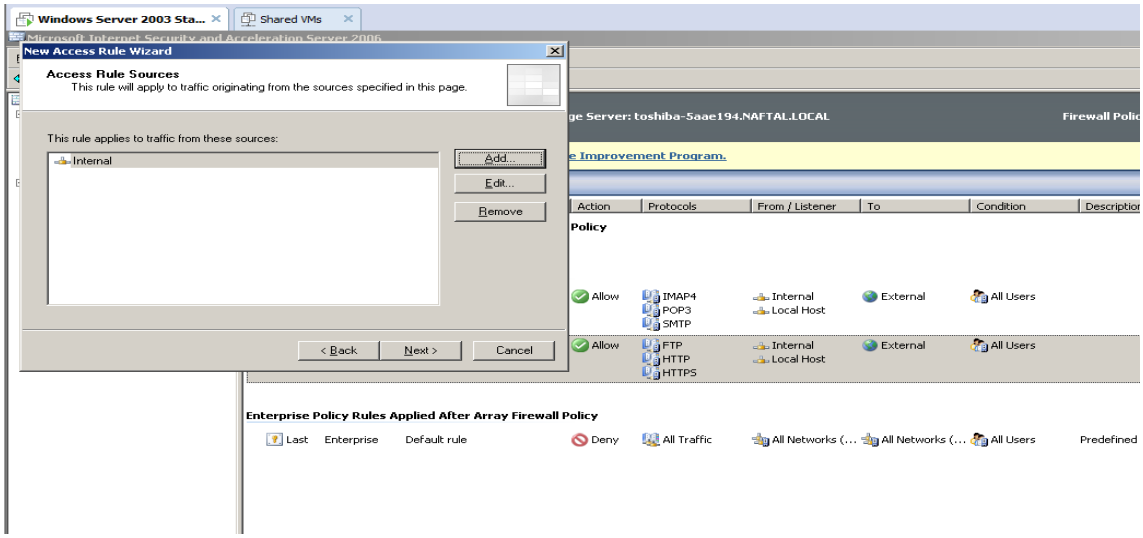


FIG. 3.23 – L'étape 3 de la configuration de Ping

c) La configuration de la règle 3 "interdire le site you tube" :

Cette configuration est comme les autres, sauf que ya un peut de changement que nous allons montrer ci-dessous : a la fin de cette configuration on doit s'assurer l'ordre suivant : le site youtube doit être le premier, puis les règles de l'autorisation, sinon le site youtube va pas être bloqué.

1. Premièrement nous avons nome notre règle "Interdire Youtube".

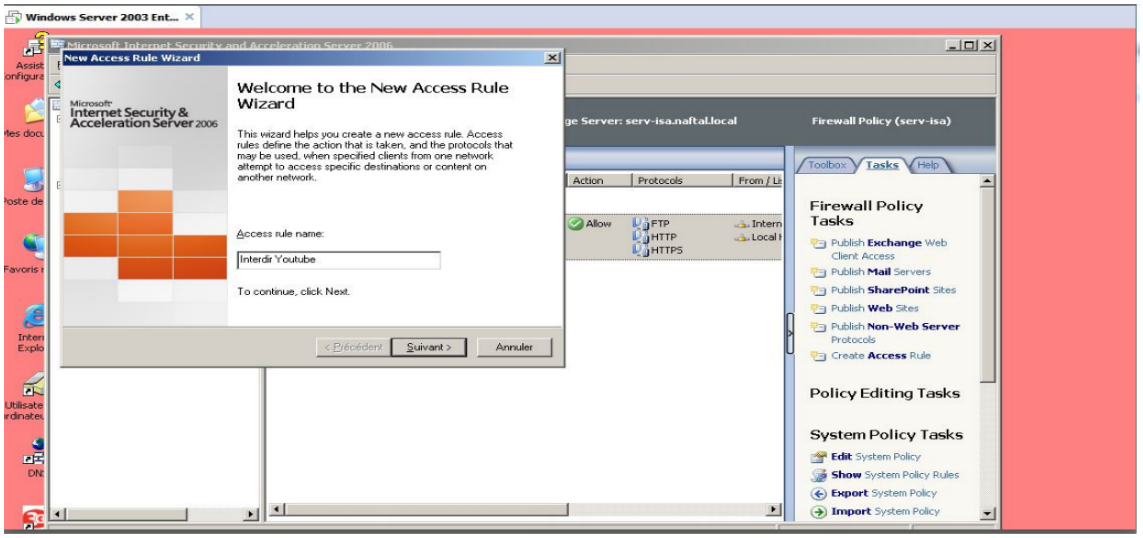


FIG. 3.24 – L'étape 1 de la configuration du site Youtube

2. Deuxièment, nous avons choisi "*Deny* " pour bloquer l'accès vers le site youtube.

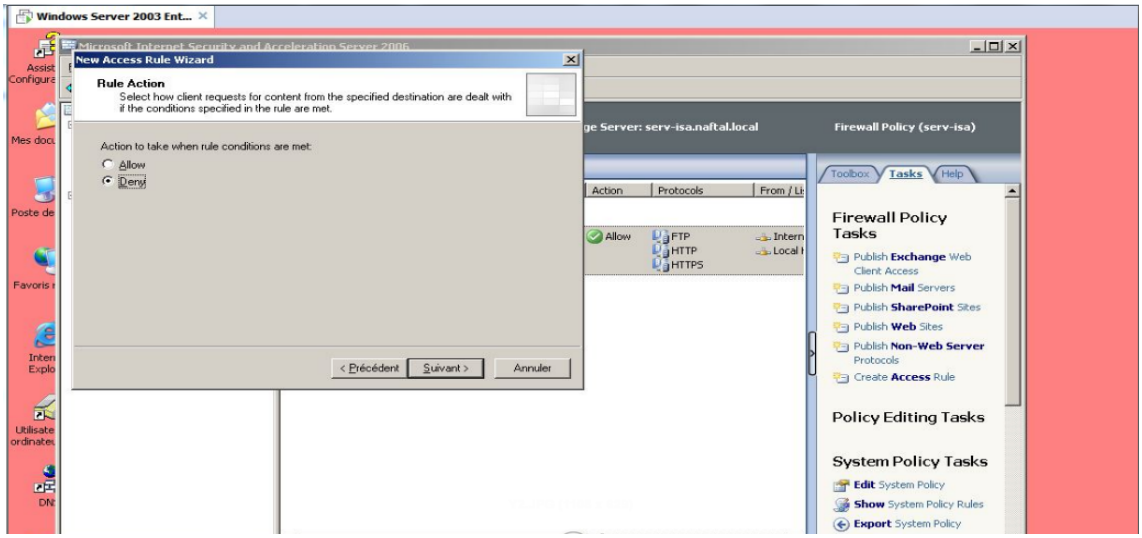


FIG. 3.25 – L'étape 2 de la configuration du site Youtube

3. Sur la fenêtre suivante, on clique sur " *all outbond trafic* " pour bloquer tout les méthodes du site youtube.

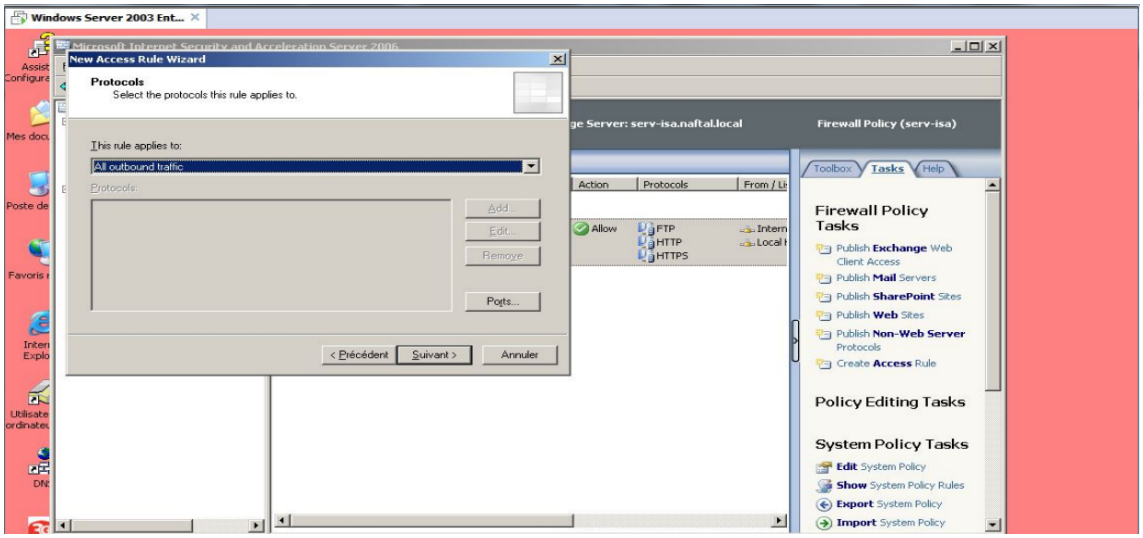


FIG. 3.26 – L'étape 3 de la configuration du site Youtube

4. Dans l'étape suivant, on sélectionne la destination de trafic qui est le site youtube.

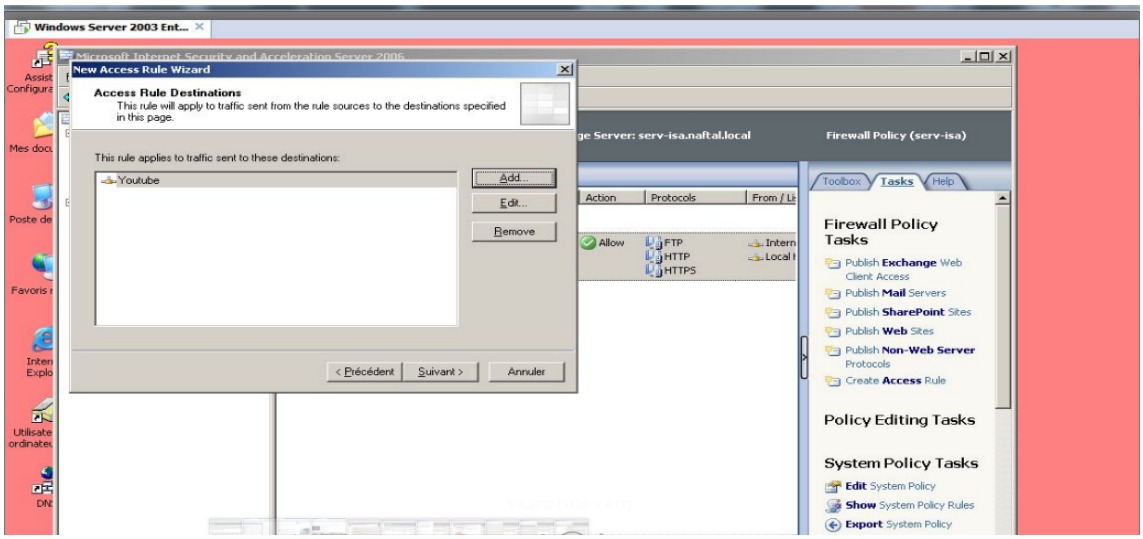


FIG. 3.27 – L'étape 4 de la configuration du site Youtube

d) Activer le mode en cache :

1. Pour configurer du mode en cache, on sélectionne le cache puis créer un cache. Une autre interface apparait sur la- quelle on précise la taille de notre cache, nous on lui a affecté 2048 MB.

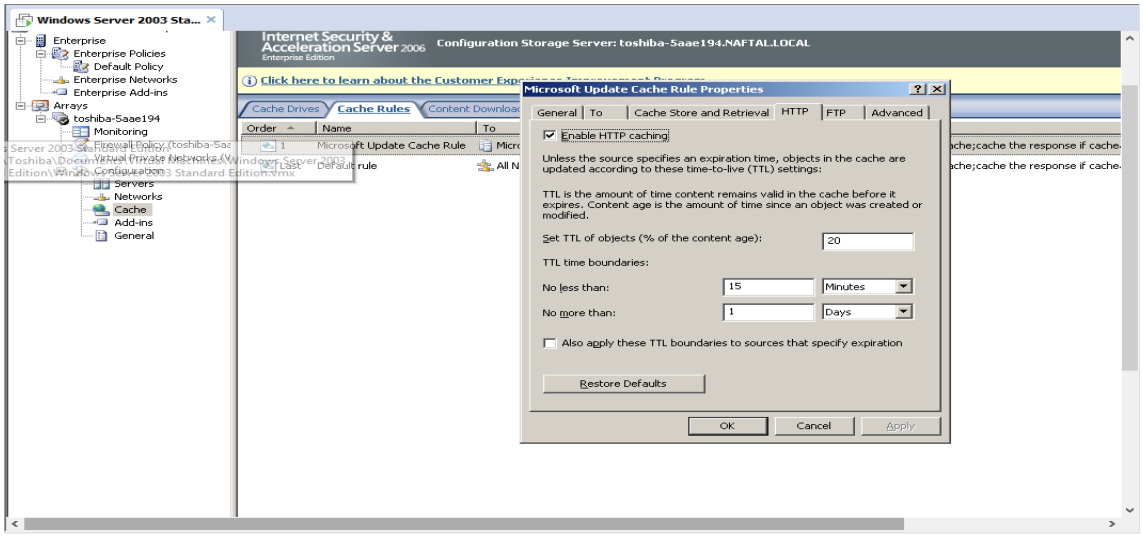


FIG. 3.28 – L'étape 1 d'activation de mode en cache

2. On l'active pour le protocole http et FTP mais on laisse les paramètres par défauts.

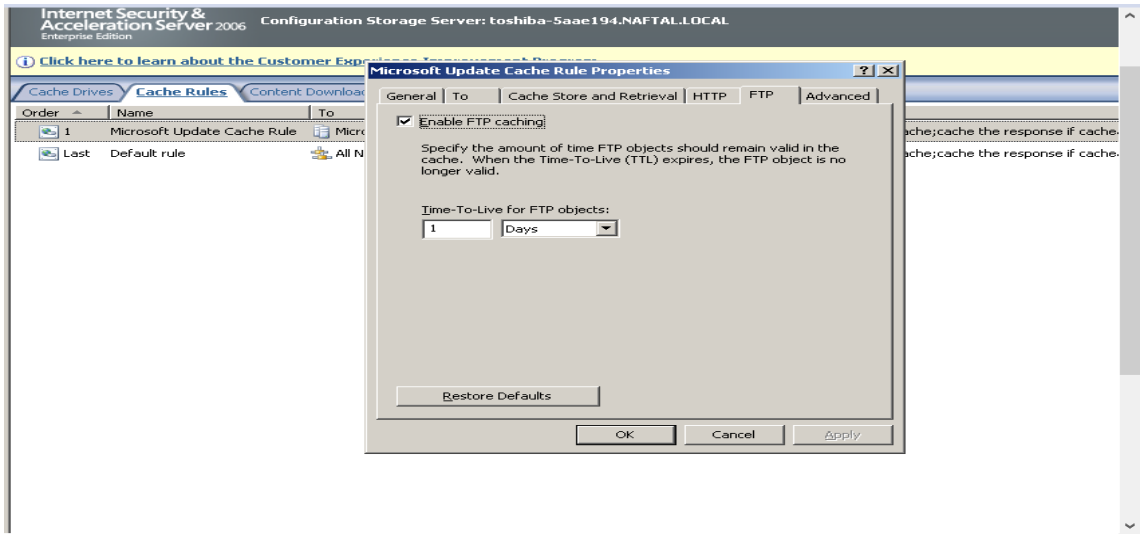


FIG. 3.29 – L'étape 2 d'activation de mode en cache

De la même façon nous avons réalisé le reste de scénario de notre politique de sécurité

## 3.5 Conclusion

La sécurité des systèmes d'information prend tout son sens dans un contexte. La connaissance des principes de base de la sécurité,ainsi que la mise en place d'une bonne politique de sécurité a contribuée,dans ce cadre nous avons configuré le serveur ISA, et les exigences de la problématique ont été satisfaites.

newpage

# Conclusion générale

Ce projet de fin d'étude de Master à concevoir une configuration d'ISA server 2006 qui permettra le filtrage de trafic entrant et sortant de réseau de l'entreprise de NAFTAL de Bejaia.
Dans ce présent travail, nous avons présenté premièrement le cadre de ce projet, puis nous avons fait l'étude de l'existant. En second lieu nous avons montré la nouvelle architecture de notre politique de sécurité. Finalement, nous avons traité toutes les phases nécessaires à la réalisation de cette configuration.
Notre travail s'agitd'une configuration presque finalisée et elle répond aux exigences de la problématique : Les utilisateurs ne peuvent pas accéder aux sites gourment en bande passante, ni aux sites qui sont malveillants, ainsi aux sites qui ne correspond pas au domaine d'activité de l'entreprise, mais on n'a pas pu faire l'authentification des utilisateurs vu a le temps limité, car ce dernier pour le réaliser il faut utiliser un serveur RADIUS afin d'effectuer l'authentification, l'autorisation et la gestion des clients RADIUS.

Par ailleurs, l'objectif principal de stage que nous avons effectué au sein de l'entreprise de NAFTAL, était la découverte du monde de l'entreprise, et dans cette optique, ce stage a totalement répondu à nos attentes. En perspective, notre configuration peut être améliorée encréant des sous-réseaux, et chaque sous-réseau reconnaissent en tant que réseau distinct, Une plage d'adressage permet de regrouper un ensemble d'utilisateurs, qui pourront ensuite être utilisés dans des règles pour autoriser ou bloquer selon les besoins de groupes.

# Bibliographie

[1] V.AMAN. " Concevoir la sécurité informatique en entreprise" . Ouvrage, France, 2014.

[2] J.M.Lamare. " Sécurité des systèmes d'information ". Livre, Edition DUNOD, paris, France, 1991.

[3] J.M.Lamare. " Sécurité des systèmes d'information ". Livre, Edition DUNOD, paris, France, 1991.

[4] A.BOUADJEMI. "Conception er réalisation d'un AGL pour la sécurisation d'intranet sécurisé selon un CDC pré-défini". Thèse, université d'Oran, 2009.

[5] ACISSI. " La sécurité informatique Ethical hacking". Livre. Editions ENI. France. Octobre 2009.

[6] Direction des opérations Bureau conseil de la DCSSI. " Menaces sur les systèmes informatiques ". Livre. PARIS. 12 septembre 2006.

[7] L. BLOCH, C.WOLFHUGEL. "Sécurité informatique Principes et méthode".Ouvrage. ÉDITIONS EYROLLES61, bld Saint-Germain 75240 Paris, 2007.

[8] Jean-Marc Robert. " Malware - Logiciels malveillants " . Article sur internet. Pp 05-15, 21 Juillet 2014.

[9] P-F Bonnefoi. "Cours de Sécurité Informatique" Support de cours. Edition SafeNet.2014

[10] Cisco Systems Europe. "Guide des solutions sécurité et VPNCiscoSystems". article sur internet .pp 5-7.29-06-2015

[11] https ://doc.ubuntu-fr.org/virtualbox

[12] https ://fr.wikipedia.org/wiki/Windows-Server-2003

[13] https ://fr.wikipedia.org/wiki/Active-Directory

[14] https ://fr.wikipedia.org/wiki/Microsoft-Internet-Security-and-Acceleration-Server

## Résumé

Le mémoire que nous avons présenté en vue de l'obtention du diplôme fin d'études de master, porte sur le renforcement de la sécurité de réseaux locale de l'entreprise NAFTAL de Bejaia avec le serveur ISA qui est mis en place à l'heure actuelle. Cette évolution est nécessaire pour remédier aux problèmes de l'insuffisance de la bande passante disponible et aux différentes menaces intentionnelles venant de l'internet.

Pour implémenter les besoins au paravent on s'est orienté vers l'Analyse et critiques de réseau existant afin d'analyser le niveau de sécurité actuelle de réseau de l'entreprise. Nous avons pu constater une réelle nécessité d'apporter des améliorations au niveau de cette dernière.

Pour ce qui de la réalisation, il est clair qu'on doit aboutir une reconfiguration d'ISA server sous Windows 2003 Server de façon fiable et irréprochable, en exploitant la partie pare-feu qui filtre les accès entrants et sortantes.



## Abstract

The memoire we submitted for the graduation in master studies is about strengthening the Security of the local network of the company NAFTAL Bejaia with the ISA server. This improvement is necessary to address the problems of inadequate bandwidth and different intentional threats from the Internet.

To implement the requirements before we focused on on the analysis and criticism of the existing network in order to analyze the current security level company network. We have noticed the need to make improvements at this latter.

In terms of implementation, it is clear that we must achieve a reconfiguration of ISA Server in Windows 2003 Server to reliably and flawlessly , exploiting the firewal that filters the incoming and outgoing acceses.