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

Université Saad Dahlab, Blida
USDB.

Faculté des sciences.
Département informatique .

Mémoire pour l'obtention
d'un diplôme d'ingénieur d'état en informatique.
Option : intelligence artificielle

Sujet :

Etude de mise en œuvre d'une politique de sécurité informatique

Présenté par : BENNAIDJA Billel
BERKANI Hamza

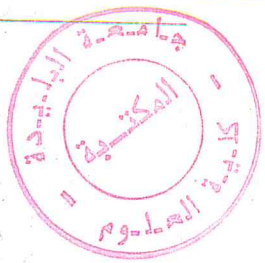
Promoteur : Mr. AKKA Abdelhakim
Encadreur : Mr. AIT KACI Cherif

Organisme d'accueil : SONATRACH
(Direction générale : Activité commerciale)

Soutenue le: 29/06/2005, devant le jury composé de :

Mr	**Bennouar**	**Président**
Melle	**Boustia**	**Examinatrice**
Mr	**Farfera**	**Examinateur**
Mr	**Hamouda**	**Examinateur**

- 2004/2005-



Remerciements

Nous remercions tout d'abord nos parents, les personnes qui nous sont les plus chères au monde.

Nous remercions notre promoteur Mr.AKKA Abdel Hakim pour son aide, sa patience, sa disponibilité et sa compréhension.

Nous remercions aussi :

- Toute l'équipe de SONATRACH, notamment notre encadreur et M. BOUDAI.
- Tous les enseignants de la faculté des sciences surtout ceux du département informatique
- Tout le personnel du département d'informatique
- Nos amis pour leur aide

Dédicace

Je dédie ce modeste travail :

A mes très chers parents qui n'ont cessé de m'encourager et de veiller sur ma réussite.

A « IMMA AZOUZOU » et « KHALTI »

A mon très cher frère MOHAMED et mes sœurs ANISSA et ma petite KENZA

A mon promoteur Mr.AKKA Abdel Hakim

A tous mes oncles maternels et à Ammi AZIZ et ses filles

A mes très cher cousin : RAMTANE, AGHILES,FERIEL MERIEM, TACFA, DIHIA, LILIA, HANNA,FERHAT,SARA,IDIR, MASSI, TINHINAN,ATHMANE,WALID ET TARIK

A Tout le village de « TIZI MEDJBER »

A tous mes amis

HAMZA

RESUME

Notre projet fin d'étude a pour but l'étude de mise en œuvre d'une politique de sécurité informatique au sein d'une entreprise

Il s'agit donc de faire une étude théorique sur le principe du développement d'une politique de sécurité et de l'appliquer au sein de l'entreprise pour élever le degré de sécurité

La mise en œuvre d'une politique de sécurité informatique nous amené en premier lieu a faire un audit de l'entreprise et de recenser tout ce qui existe comme matérielle, logiciel et données pour avoir des informations sur l'état actuel de la politique de sécurité, ensuite on doit analyser les résultats de notre audit tout en rappelant sur risques et les menaces que l'entreprise peut être victime

Notre objectif est de trouver une solution qui offre plus de sécurité à l'entreprise, cette solution peut se résumé dans un logiciel qui offre une protection contre une faille remarqué au niveau de l'étude de l'existant.

Dédicace

Je dédie ce mémoire a :

Ma mère pour sa tendresse et son soutient,

Mon père pour ses conseils et orientations,

Mes frères toufik, ali, ismail, et mes sœurs

Mes cousin samir, abdelkader,

Mes amis

BILLEL

Table des matières

Listes des figures

Chapitre1

Chapitre2

Chapitre 3

Chapitre 4

CHAPITRE 5

Liste des tableaux

Introduction générale

L'informatique, les réseaux et les services associés sont maintenant obligatoires pour Toutes les activités de recherche dans toutes les branches scientifiques. La bonne marche de ces outils est devenue indispensable à la progression de la recherche, même fondamentale.

Si les avantages de ces nouveaux outils sont manifestes en termes de gain de temps, de bonne gestion et d'efficacité (et donc de coût à terme), les outils informatiques et les réseaux présentent des risques et des vulnérabilités inhérents à leur nature. Les atteintes au patrimoine informationnel de l'administration par des attaques informatiques, des erreurs ou des maladresses, ainsi que l'anonymat sur les réseaux et la volatilité des données sont des réalités dont on ne peut faire abstraction.
La pérennité de toute organisation passe par une disponibilité permanente de son système d'information. Les entreprises en sont de plus en plus conscientes.

Mais les efforts de sécurisation ne peuvent avoir d'effet que si ces investissements sont correctement ciblés et étudiés, avec la mise en place de moyens de protection apportant un niveau de sécurité adapté aux enjeux spécifiques de l'entreprise.

La définition d'une politique de sécurité informatique vise ainsi à identifier les besoins de l'organisation en terme de sécurité et à élaborer des stratégies afin de protéger les biens les plus critiques.

L'entreprise nationale SONATRACH est consciente des conséquences de l'absence de sécurité vu q'elle elle dispose d'un réseau vaste, ce qui nécessite d'avoir une sécurité d'un degré élevé pour pouvoir garantir la disponibilité de ses données

Le département commercialisation est l'un des départements le plus important de notre organisme d'accueil puisqu 'il entre en contacte non seulement avec les plus grande compagnie pétrolière du monde mais avec les grand pays consommateur de pétrole au monde. Nous n'allons pas détailler les relations de ce département, mais

ce qui nous intéresse est de savoir le degré d'importance de la base de donnée qu'il possède et l'obligation de suivre une politique de sécurité capable de protéger les biens de toute l'entreprise

Nous nous intéressons dans notre travail à donner une étude de la politique de sécurité actuelle pour la division activité commerciale de notre organisme de la direction générale de l'entreprise SONATRACH

Le présent document est consacré à la présentation détaillée des différentes étapes nécessaires à la mise en œuvre d'une politique de sécurité informatique. Affin d'atteindre ce but nous avons commencé par une étude théorique sur la politique de sécurité informatique, puis en a entamé son application au sein de notre organisme d'accueil en commençant par l'étude de l'existant du département de commercialisation, ensuite en a donné un rappel sur les menaces et les risques que l'entreprise peut avoir en mettant l'accent sur la sécurité des réseaux avec la présentation des différents types de solution.

Le présent document contient à cet effet les chapitres suivants :

Le chapitre 1 présente :
Introduction a la politique de sécurité informatique
Etapes nécessaires pour réaliser une politique de sécurité informatique

Le chapitre 2 présente :
Etude de l'existant matériel et logiciel du département commercial

Le chapitre 3 présente :
Réseaux et sécurité
Les menaces et les risques

Le chapitre 4 présente :
Proposition de solution de sécurité

Le chapitre 5 présente :
Conception et mise en œuvre de la solution proposée.

CHAPITRE 1

POLITIQUE DE SECURITE

I. Introduction

La bonne marche des outils offerte par les réseaux informatiques est devenue indispensable à la progression de la recherche, même fondamentale.
La définition d'une politique de sécurité du système d'information vise ainsi à identifier les besoins de l'organisation en terme de sécurité et à élaborer des stratégies afin de protéger les biens les plus critiques.

II. Définition

Une politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de la sécurité [THO 04].

III Objectifs d'une politique de sécurité :

Pour atteindre des objectifs tel que :

- commerce électronique,
- interconnecter différents sites géographiques de l'entreprise,
- permettre aux collaborateurs d'avoir un accès distant à ses ressources,
- l'entreprise profite de la généralisation de l'Internet et intègre progressivement les progrès réalisés dans les technologies de l'information.
- Protéger l'entreprise de tous ces risques demande un investissement conséquent et peut avoir des répercutions sur les fonctionnalités et la souplesse du système. Il s'agit alors d'aborder la sécurisation du système d'information de manière stratégique. L'objectif d'une politique de sécurité informatique est ainsi de parvenir à concentrer les efforts de sécurité sur les ressources les plus critiques et les plus vulnérables.

Cette ouverture croissante des systèmes d'information est autant de risques pour l'entreprise. Des faits d'actualité démontrent chaque jour la vulnérabilité des systèmes

en l'absence de protections efficaces. Les pertes associées peuvent avoir des conséquences considérables pour l'entreprise [THO 04].

Cette politique repose sur une analyse des risques, visant à évaluer les vulnérabilités des biens vitaux de l'entreprise, les conséquences d'une attaque, et leur probabilité d'occurrence. A partir de cette analyse, les moyens pour assurer la sécurité pourront être mis en place en fonction d'objectifs stratégiques. Ainsi, une architecture, des outils et des procédures seront définis et déployés pour protéger les ressources les plus critiques [THO04].

IV. La portée d'une politique de sécurité

Ce processus vise essentiellement à déterminer l'étendue de la sécurité et la façon dont on devrait définir les exigences en matière de sécurité. Par limites, on entend les parties de l'entreprise que l'on désire protéger. Les limites peuvent comprendre le réseau dans son ensemble ou des segments de celui-ci, comme les volets communications des données, la fonction serveur, les applications logicielles, etc. Si les limites comprennent une partie du réseau qui est contrôlée par une autre partie, cela peut donner lieu à des problèmes de coopération pouvant nuire à l'exactitude des résultats.

Cette possibilité souligne combien est nécessaire la coopération entre les personnes qui possèdent et gèrent les différentes parties du réseau, et qui utilisent des applications et y traitent de l'information [YCH 02].

Une politique de sécurité :

- s'applique au personnel régulier et occasionnel, aux étudiants et aux utilisateurs des services institutionnels offerts à la collectivité. Elle touche également toute personne ou firme externe appelée à utiliser les équipements informatiques ou à traiter l'information appartenant à l'entreprise ou à une de ses constituantes;

- vise tout actif informatique appartenant a l'entreprise, peu importe sa localisation;

- vise tout actif informatique de télécommunication n'appartenant pas a l'entreprise mais utilisé dans ses locaux par les personnes auxquelles s'applique la politique;

- s'applique à toute donnée saisie, traitée ou emmagasinée à l'aide d'équipements, de systèmes ou autres moyens exploitant des technologies de l'information ou des télécommunications que l'entreprise utilise pour ses activités d'enseignement, de recherche, de gestion et de services à la collectivité.

V. Méthodologie d'une Politique de sécurité :

Une politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de la sécurité.

La définition d'une politique de sécurité peut se décomposer en quatre étapes :

1. Evaluation des ressources et analyse des risques
2. Définition des objectifs stratégiques
3. Développement et implémentation d'un plan d'actions
4. Exploitation et évolution de la politique

V.1. Phase d'évaluation

La première étape doit permettre de déterminer les éléments critiques d'une entreprise.

Cette analyse commence par une évaluation des ressources afin d'identifier les biens vitaux de l'entreprises : biens matériels, données, biens logiciels, personnes, etc.

Après avoir identifié ces ressources, il s'agit d'évaluer :

Les conséquences : impact sur l'entreprise de l'exploitation d'une faille de sécurité pouvant affecter chacune de ces ressources [Akk1 04].

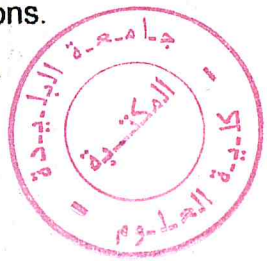
Les menaces et vulnérabilités : Identification et analyse des failles de sécurité pouvant affecter chacune de ces ressources. Définition des probabilités d'occurrence.

Les risques sont ensuite classés de manière graduelle afin de définir leur niveau de «criticité» et déterminer les actions à mettre en œuvre [Akk1 04].

V.2. Définition des objectifs stratégiques

Le rapprochement entre les ressources critiques de l'entreprise et les risques de sécurité associés permet de définir les objectifs stratégiques de la politique de sécurité informatique. Pour chacune des ressources critiques, on visera à garantir :

- La confidentialité : elle assure la protection de l'accès aux informations.
- L'intégrité : elle assure que les informations n'ont pas été modifiées.
- La disponibilité : elle assure l'accès aux informations [Akk2 04].



V.3. Développement et implémentation d'un plan d'actions

L'élaboration des mesures de protection des risques se fait en fonction des objectifs définis précédemment. Dans la limite des contraintes, économiques et politiques, les efforts seront concentrés pour assurer la protection des biens identifiés précédemment.

Une architecture, des outils et des procédures sont alors déployés [THO 04].

Garantir la sécurité consiste généralement à satisfaire les critères d'identification, d'authentification, d'autorisation, de confidentialité, d'intégrité, de disponibilité, de non répudiation de l'information.

V.4. Exploitation et évolution de la politique

Cette phase a pour but d'assurer la sécurité sur le long terme. D'une part, il s'agit de veiller à ce que les actions menées remplissent les objectifs. D'autre part, elle doit permettre de faire évoluer la stratégie au même rythme que son environnement. En effet, les ressources de l'entreprise et les risques liés sont en perpétuelle évolution. Il est ainsi nécessaire de réitérer régulièrement la phase d'évaluation et de réajuster les objectifs de sécurité [THO 04].

VI. Conclusion

Les efforts de sécurisation du système d'information ne peuvent avoir d'effet que si ces investissements sont correctement ciblés et en adéquation avec les besoins spécifiques de l'entreprise.

La définition d'une politique de sécurité vise à élaborer des stratégies et des plans d'actions afin de protéger les biens les plus critiques de l'entreprise.

Une politique de sécurité peut s'établir en 4 phases :

- Evaluer les menaces et les vulnérabilités des biens vitaux de l'entreprise, les conséquences d'une attaque et leur probabilité d'occurrence.
- Définir les orientations stratégiques en fonction des besoins identifiés précédemment.
- Mettre en place des plans d'actions pour atteindre les objectifs de sécurité.
- Assurer la pérennité et l'évolution de la politique de sécurité.

Chaque nouvelle technologie ou nouvelle façon de travailler doit être mise en place en prenant en compte, dès le départ, la composante sécurité.

La planification de la sécurité est complexe et basée sur plusieurs points tel que la sécurité physique, la sécurité de l'information et la sécurité organisationnelle. Dans ce qui suit, on va consacré notre étude sur la sécurité de l'information et en particulier la sécurité des réseaux.

CHAPITRE 2

ETUDE DE L'EXISTANT

I. Introduction

Comme toute activité l'informatique contribue aux objectifs essentiels de l'entreprise. La SONATRACH doit donc assurer la disponibilité constante de son outil informatique dont elle est de plus en plus dépendante. Elle doit aussi assurer l'intégrité de l'information qu'elle a stockée dans son system informatique. Enfin, elle doit conserver la confidentialité et la sécurité de cette information. Tel est l'enjeu, aujourd'hui, qui a pris une importance croissante depuis que le réseau de la SONATRACH a été mis en place avec ses fonctionnalités de partage d'information, de messagerie électronique et de connexion sur le monde extérieur (Email, accès distants, Internet).

II. Architecture Globale Du Siège de la SONATRACH

La direction d'informatique, celle qui gère le réseau global du siége de la SONATRACH, a divisé ce réseau en sous réseaux spécifiant un seul département grâce au SWITCH CISCO qu'elle dispose, cela est fait en créant des VLAN, chaque département tel que :
Direction des finances,
Direction des ressources humaines,
Direction juridique,
Activité commercialisation,
Appartient à un seul VLAN configuré à partir du SWITCH.

II.1. Le routeur

Le routeur est le dispositif de communication le plus important pour la sortie du réseau vers l'extérieur.
Le routeur CISCO dont la SONATRACH dispose, comprend des fonctionnalités de tolérance de pannes, puisqu'il contient les éléments suivants de rechange :

- Bloc d'alimentation
- Carte serial.

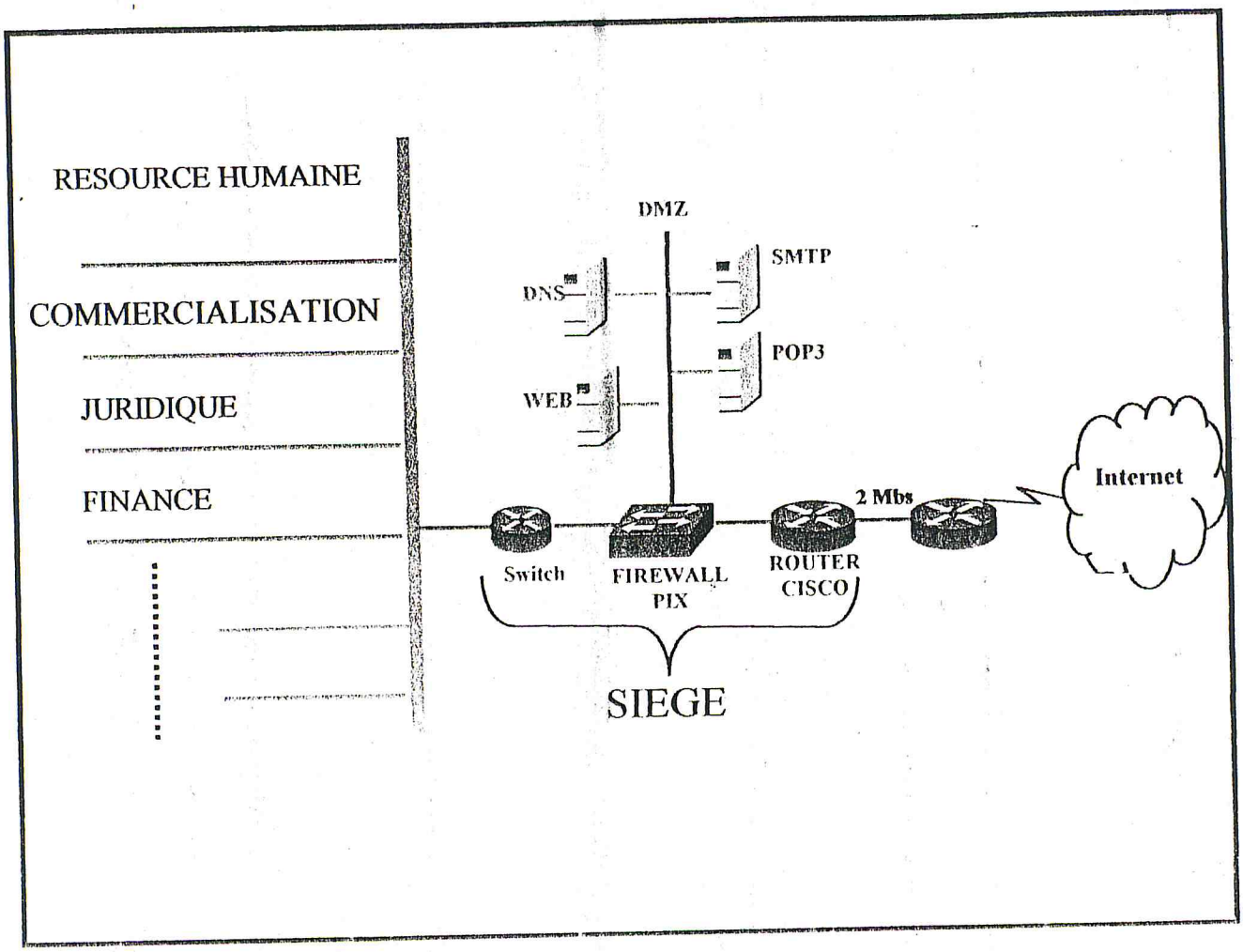


FIG 2.1 RESEAU SONATRACH

La sécurité devient alors un point critique qu'il faudrait prendre en charge. Il faut savoir en effet que l'ouverture Du réseau vers l'extérieur comporte des risques potentiels

Les stratégies de défenses sont :

- Coupe-feu ou pare-feu ou FIREWALL (software + hardware),
- Antivirus,

A) La protection anti-intrusion est généralement réalisée par un système « Firewall » consistant à une protection périmétrique par cloisonnement et contrôle d'accès.

B) la protection virale est assurée par des systèmes anti-virus installés sur le serveur de messagerie ou pour plus d'efficacité en étroite collaboration avec le Firewall.

Cette deuxième configuration sécurise la messagerie (flux SMTP) mais également d'autres services comme le Web (flux HTTP) ou le transfert de fichier (flux FTP).

II.2. Services dans la zone semi-ouverte

Dans la zone semi-ouverte, il faut installer toutes les machines qui assureront les services avec l'extérieur : DNS, messagerie Internet, Web, bases de données publiques, ... Ces machines seront dédiées à ces fonctions, elles ne seront pas utilisées comme stations de travail classique

Avec ces services en dehors du réseau local interne, il y aura peu de communication de l'extérieur vers l'intérieur.
Il est préférable de mettre en place une DMZ entre le routeur et le Firewall où seront connecté les serveurs Web, DNS ...etc. Plus simple à configurer.

Il reste bien sur possible de permettre, grâce au Firewall, à certains utilisateurs d'accéder en TELNET ou en FTP sur leurs postes internes depuis l'Internet ou à certains utilisateurs distants (antenne de chargement) d'accéder aux informations disponibles dans le réseau local interne via une ligne téléphonique.

Sur toutes ces machines de services, les versions des systèmes et des applications devront être régulièrement mises à niveau et les correctifs de sécurité devront être installés dés qu'ils seront diffusés.
La politique du Firewall sera de tous interdire dans le sens entrant sauf certains services connus et maîtrisé, c'est à dire les services vers les machines de la zone semi-ouverte et les accès distants de certains utilisateurs du siège.

III. Architecture du département commercialisation (COM)

Notre but est de mettre en évidence ce qui mérite d'être protégé et d'apporter certaines solutions techniques afin de mettre en place un dispositif efficace de sécurité et d'assurer un fonctionnement continu du réseau.
Pour cela, nous avons déterminé les éléments suivants à protéger

- Le local technique
- Le matériel informatique
- Les données
- Le système d'exploitation et les différents services réseaux
- Les connexions externes

III.1. Protection du local technique

Le local technique est l'endroit ou sont entreposes les serveurs et les différents équipements de connexions internes et externes, nous avons donc dans ce local le « moteur » du réseau. Il est alors primordial de le protéger contre tout accès illicite.

Pour cela, les mesures suivantes sont instaurées:

- Séparer la maintenance et les consommables de ce local,
- Désigner les personnes autorisées à y accéder,
- Avoir un nombre bien déterminé de clés pour l'accès au local et connaître leur possesseur,
- S'assurer des normes de sécurité en matière de climatisation,
- Onduler toutes les prise électrique du local
- Prévoir un coffre anti-incendie pour la protection des copies de sauvegarde des données et des logiciels réseaux (SGBD, Ms Exchange, Win NT, procédures de reprise après incidents,...).

Un onduleur de 650VA est acquis afin d'onduler quelques prises locales.

III.2. Sécurités du matériel

III.2.1. Les serveurs :

Les serveurs existants au niveau du département de commercialisation sont les suivant :

- Serveur de messagerie MS Exchange
- Serveur de base de donnée oracle
- Serveur de fichier
- Serveur de développement sous oracle
- Serveur Web
- Serveur antivirus

Les serveurs sont déjà munis de certaines fonctionnalités de sécurité à savoir :

- Alimentation redondante,
- Ventilation redondante,
- RAID 5,
- Double processeur.

En plus de ces fonctionnalités, il est nécessaire de prévoir d'autres composants redondants afin d'assurer une continuité de service maximum de ces serveurs, tels que

- Disque dur de rechange,
- Blocs d'alimentation,
- Lecteur DAT auto loader de rechange,
- Carte réseau de rechange

Tous les serveurs sont également dotés d'un anti-virus mis à jour régulièrement.

III.2.2. Les postes de travail

Pour chaque poste de travail il est nécessaire de définir une configuration type de base que l'utilisateur doit respecter et ne la modifier en aucun cas sans l'aval du département système et exploitation.

Une configuration type peut être définie pour :

- Les poste connectés en réseau,
- Les poste non connectés,
- Les postes pour les accès distants.

Il faut également savoir que chaque poste de travail est doté d'un antivirus a mettre a jour régulièrement.

III.2.3. Serveur de test

Afin d'anticiper sur les éventuelles problèmes de configuration et de bugs de fonctionnement, le département dispose d'un serveur de test qui permet de tester tout nouveau produit réseau acquit avant son installation de façon permanente.

III.3. Sécurités Windows NT

III.3.1. Sécurisé le BIOS et les lecteurs de disquette de serveurs :

Sur chaque serveur, un mot de passe est demandé pour accéder à la configuration des paramètres BIOS.

Et de plus l'amorçage à partir du lecteur de disquette a été inhibé pour empêcher les personnes étrangères de rebouter le système à partir d'une disquette et donc d'avoir accès au répertoire SystemRoot pour récupérer le fichier des mots de passe.

III.3.2. mise en place d'une stratégie de compte Windows NT :

L'authentification des comptes utilisateurs permet aux utilisateurs de faire partie d'un domaine et d'accéder à ses ressources.
La stratégie de compte concerne les mots de passe et le verrouillage des comptes.
La stratégie de compte mise en œuvre pour le domaine COM est résumée dans le tableau suivant :

Limitation du mot de passe	Durée maximale : expire dans 90 jours Durée minimale : autoriser les modifications immédiates
Longueur minimale du mot de passe	Au moins 7 caractères
Unicité de mot de passe	Se souvenir de 4 mots de passe
Verrouillage des comptes	Verrouillage après 4 tentatives d'accès infructueux Réinitialisation du compte après 30 minutes Le verrouillage est permanent jusqu'à l'intervention de l'administrateur.

Tableau 2.1 stratégies de compte

III.3.3. Mise en œuvre d'une stratégie d'audit :

La fonction d'audit de Windows NT sert à suivre les activités des utilisateurs ainsi que les événements au niveau du system. L'audit permet ainsi de demander la consignation de l'action ou de l'événement dans un journal de sécurité. L'information écrite indique :

- L'action réalisée,
- L'utilisateur ayant réalisé cette action,
- La date et l'heure de l'action.

Tous les événements seront consignés dans le journal de sécurité qu'on pourra consulter par l'utilitaire d'administration observateur d'événement.

III.3.4. Cryptage des mots de passe :

Le service Pack6 pour Windows NT est pourvu d'un utilitaire qui permet de crypter le hachage des mots de passe contenu dans la base de donnée SAM. En effet Windows NT stick des dérivés résultant de la fonction de chiffrement unidirectionnel de NT. Avec cette méthode de stockage, si un intrus procure une copie de la base de registre SAM, il n'obtiendra que le hachage.

III.4. Sécurité des données

En plus du système RAID 5 déjà opérationnel sur les serveurs de bases de données et de messagerie, il est primordial d'instaurer une procédure de sauvegarde périodique des bases de données et des applications.

Pour cela, un logiciel de sauvegarde automatique a été prévu sur le serveur de base de données Oracle ainsi qu'un lecteur DAT auto loader de 6 cassettes de 12/24 GB chacune. Sur le serveur de messagerie, un lecteur de DAT 8/12 a été prévu pour la sauvegarde de la banque d'information du système de messagerie électronique.
Il faut mettre en place une stratégie de sauvegarde c'est à dire la fréquence de sauvegarde des données. Prévoir également les données qui vont être sauvegardées via le réseau.
Et afin de minimiser au maximum le temps des arrêts intempestifs des services offerts sur le réseau, il est nécessaire de prévoir des procédures de restauration et de reprise d'urgence pour :

- La réinstallation et la configuration des systèmes d'exploitation réseau,
- La réinstallation et la configuration du système de gestion de base de données Oracle,
- La réinstallation et la configuration du système de messagerie électronique,
- La restauration des différentes bases de données.

En ce qui concerne les postes clients, chaque utilisateur doit être sensibilisé à effectuer des sauvegardes de ses données locales de manière périodique. Si ces données sensibles sont celles de l'entreprise, il est préférable de mettre en place des dossiers de base pour chaque utilisateur et donc centraliser la sauvegarde.

III.5. Le réseau du département commercialisation (COM)

Le département de commercialisation travail sur deux réseaux :

- Le réseau ouvert.
- Le réseau fermé.

III.5.1. Réseau ouvert

Ce réseau est toujours connecté avec le monde extérieur a travers le routeur (CISCO) qui permet l'accès à Internet pour tout le siége, son architecture est indiquée dans le schéma suivant.

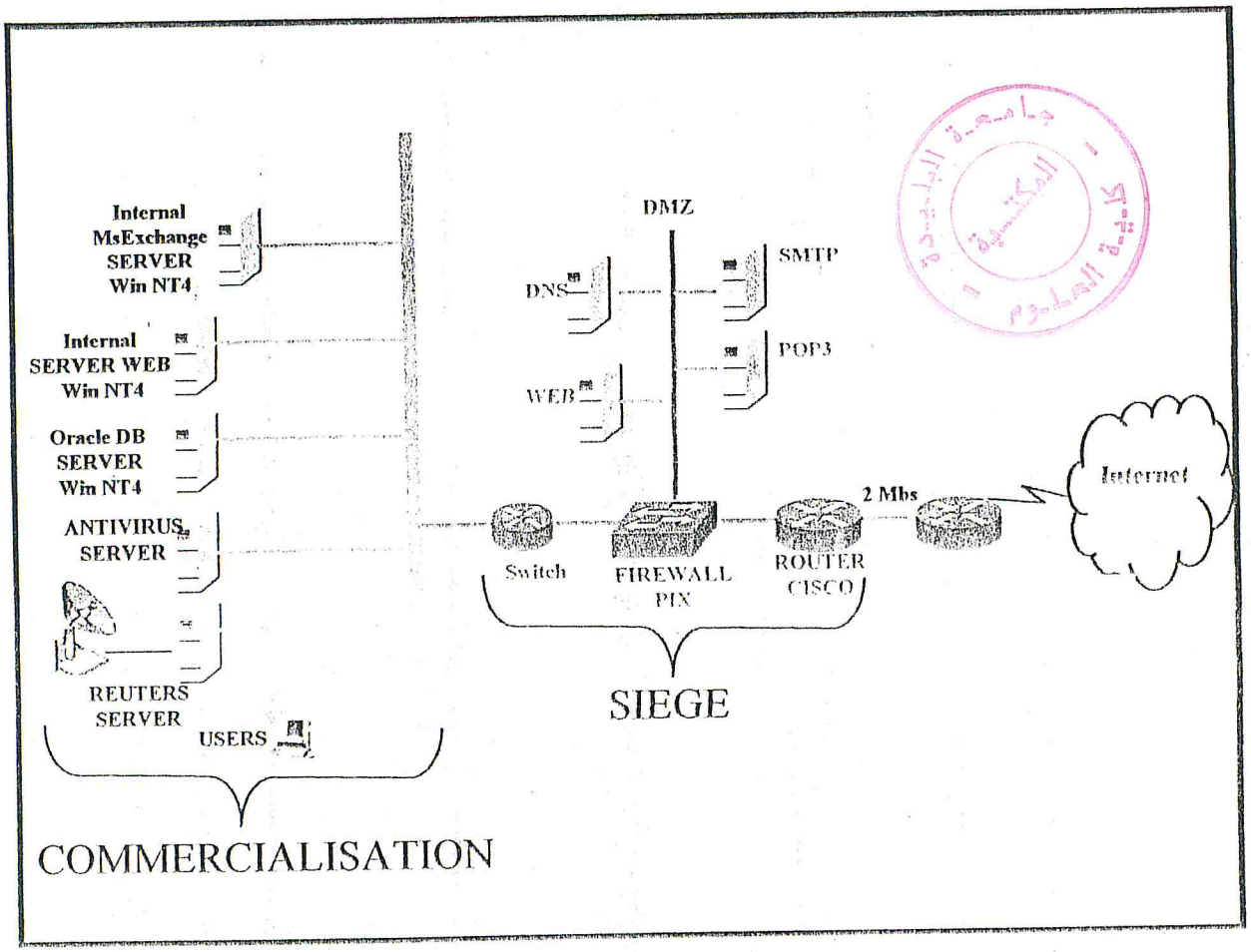


FIG 2.2 RESEAU OUVERT

III.5.2. Réseau fermé

En fait, pour élevé le degré de sécurité du département de commercialisation, ce dernier a séparé toute les ressources confidentielles donc il existe un autre réseau confidentiel appelé réseau fermé, ce réseau n'à aucun contact avec le monde extérieur, son architecture est indiquée dans le schéma suivant.

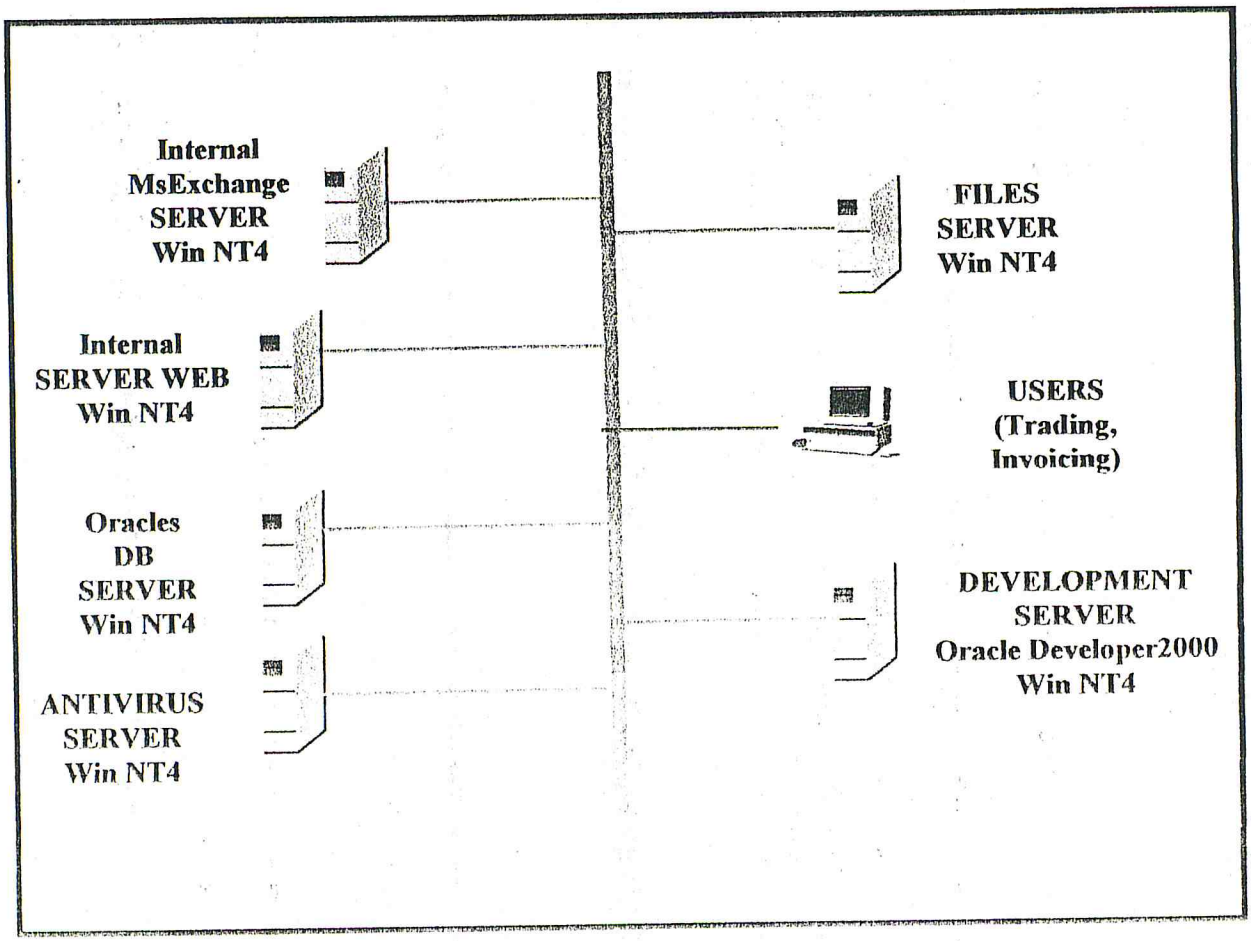


FIG 2.3 RESEAU FERME

III.5.3. Nouvelle architecture souhaitée

L'objectif de suivre une architecture à deux réseaux était de protéger au maximum les ressources confidentielles dans le réseau fermé les intrus externes, mais l'inconvénient majeur de cette approche est :

- Dédoublement de serveurs et de services réseaux
- la difficulté de gérer et d'administrer ces deux réseaux en même temps, ainsi, le département doit gérer deux serveurs Web, deux serveurs de fichier, deux serveurs de base de données...
- Augmentation des coûts.

L'organisme a pensé de prendre en charge les deux réseaux en même temps et pour cela la solution unique est d'interconnecter les deux réseaux pour pouvoir gérer un serveur de chaque type.

L'interconnexion des deux réseaux laisser le réseau fermé comme cible d'attaque a partir de l'extérieur, le département a donc décidé de mettre un dispositif de sécurité afin de protéger les ressource confidentielle, en effet il dispose d'un FIREWALL CISCO (matériel) qui peut répondre a leur exigence.

IV Conclusion

Le travail qui nous a été demandé est de mettre en place une stratégie d'interconnexion sécurisée à l'aide du FIREWALL existant et proposer une solution ciblée plus sécurisée.

CHAPITRE 3

RESEAUX ET SECURITE

I. Introduction

Dans un domaine aussi vaste et complexe que la sécurité, nous étudions en particulier la sécurité dans les réseaux. La première de nos préoccupations a été de définir les terminologies, puis nous nous donnons les exigences en matière de sécurité du réseau, et les menaces et les risques attendus. Et comme la plupart des applications utilisent le modèle TCP/IP, en donnera quelque détail sur les couches de la pile TCP/IP toute en citant leur faille.

II. Définition de la sécurité

« La sécurité informatique est la capacité d'un système de protéger ses objets contre leur modification ou de leur utilisation par ses personnes non autorisées ». [BEN 03]
« Faire de la sécurité sur un réseau consiste à s'assurer que celui qui modifie ou consulte des données du système en a l'autorisation et qu'il peut le faire correctement car le service est disponible. »[LAR 98]

II.1. Autres définitions

Vulnérabilité

C'est une faiblesse, une faille dans la mesure de protection ou encore dans l'absence de mesure de protection[BEN 03].

Attaque

C'est l'action prise par un individu pour modifier l'état d'un système. Une attaque peut réussir si elle exploite une vulnérabilité du système. Elle peut être direct auquel cas elle s'adresse a l'objet en question ou indirecte ou elle obtient des informations d'un autre objet sans attaquer l'objet en question directement [PIL 01].

Pirate

Un pirate peut être :

Hackers

Les Hackers sont des personnes qui s'intéressent de près aux systèmes d'exploitation. Ils cherchent constamment à approfondir leurs connaissances et à les faire partager. Leur but n'est pas de nuire mais au contraire de connaître pour améliorer [BEN 03].

Crachers

Les crashers, par contre, violent des systèmes à distance dans un but de malveillance. Ils détruisent des données, empêchent le fonctionnement de services [PIL01].

II.2. Quelques chiffres

Après un test de 12 000 hôtes du Département de la défense américaine, on retient que 1 à 3% des hôtes ont des ouvertures exploitables et que 88% peuvent être pénétrés par les relations de confiance.

Notons que seules 4% de ces attaques sont détectés et que 5% de ces 4% sont rapportées.

Enfin, notons que le nombre de voleurs d'informations a augmenté de 250% en 5 ans, que 99% des grandes entreprises rapportent au moins un incident majeur et que les fraudes informatiques et de télécommunication ont totalisés 10 milliards de dollars pour seuls les Etats-Unis [THO 04].

1290 des plus grandes entreprises rapportent une intrusion dans leur réseau interne et 2/3 d'entre elles à cause de virus [BEN 03].

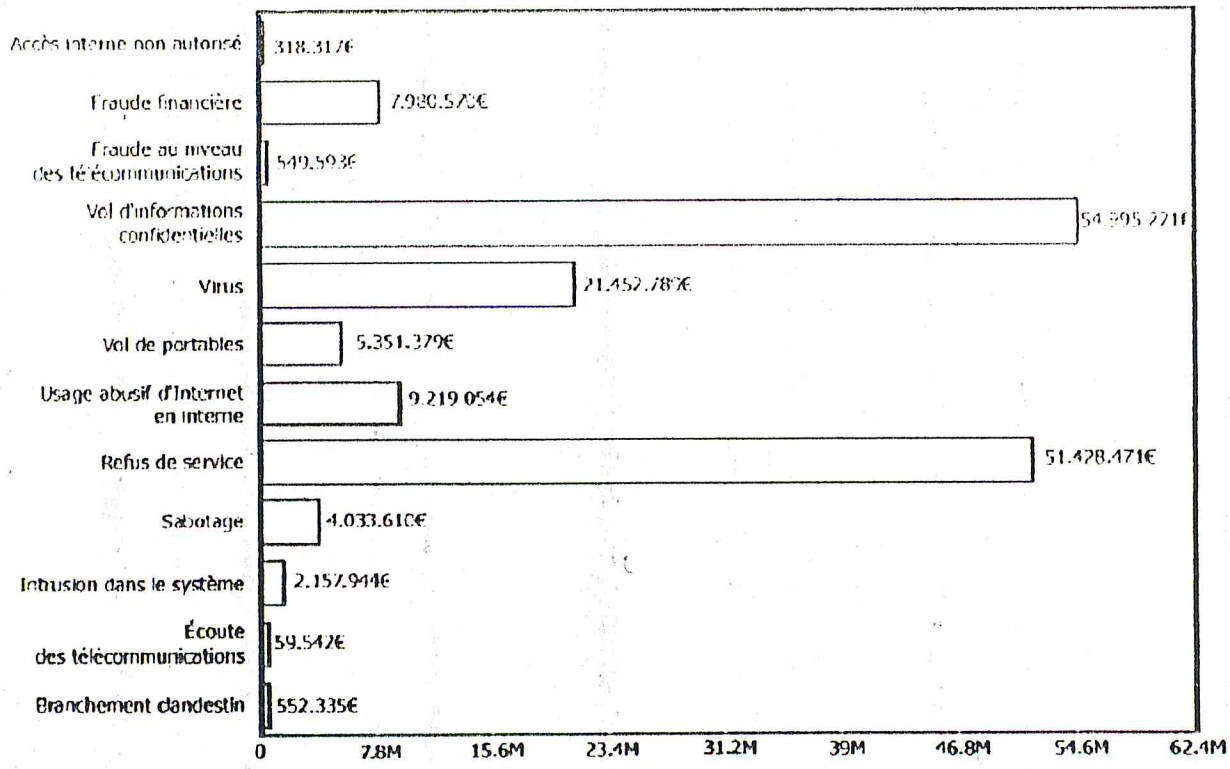


FIG 3.1 Les pertes associées aux failles de sécurité informatique [THO04]

III. Services de sécurité

III.1. Confidentialité

Lorsqu'il faut veiller au caractère privé de l'information, on devrait utiliser des mesures (ou services) de confidentialité. Constituant en quelque sorte une protection de première ligne, ces mesures peuvent comporter des mécanismes utilisés conjointement avec les mesures de contrôle des accès, mais elles peuvent aussi utiliser des techniques de chiffrement afin d'accroître davantage la confidentialité de l'information, qui empêche les personnes ou les systèmes non autorisés d'intercepter ou de perturber les émissions électromagnétiques provenant des composants du réseau.

Le chiffrement de l'information consiste à convertir les données en une forme inintelligible. Par la suite, pour reconvertir l'information dans sa forme originale, on doit utiliser un processus de déchiffrement [Sol 01].
Il existe à l'heure actuelle deux grands principes de chiffrement : le chiffrement symétrique basé sur l'utilisation d'une clé privée et le chiffrement asymétrique qui, repose sur un codage à deux clés, une privée et l'autre publique.

III.1.1. Le chiffrement symétrique

Le chiffrement à clé privé ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. Les algorithmes de chiffrement les plus connus sont : Kerberos, DES (Data Encryption Standard) et RSA.

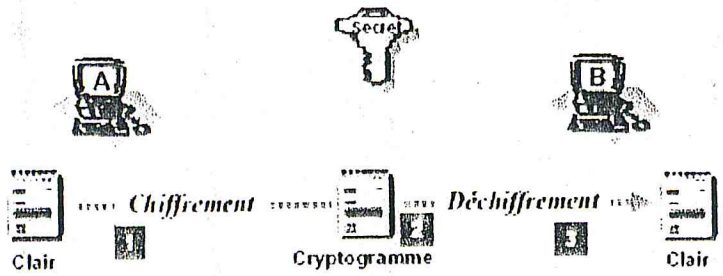


FIG 3.2 Chiffrement symétrique [Sol 01]

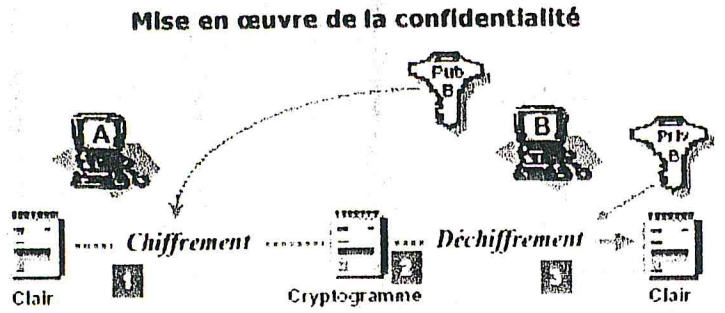
Le principal problème est le partage de la clé : Comment une clé utilisée pour sécuriser peut être transmise sur un réseau insécurisé ? La difficulté engendrée par la génération, le stockage et la transmission des clés (on appelle l'ensemble de ces trois processus le management des clés : Key management) limite le systèmes des clés privées surtout sur Internet [FLO 99].
Pour résoudre ces problèmes de transmission de clés, les mathématiciens ont inventé le cryptage asymétrique qui utilise une clé privée et une clé publique.

III.1.2. Le chiffrement asymétrique

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que de l'utilisateur ; l'autre est publique et donc accessible par tout le monde.
Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage [STA 02].
Ce cryptage présente l'avantage de permettre le placement de signatures numériques dans le message et ainsi permettre l'authentification de l'émetteur.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plupart des cryptages à clé privée il reste préférable pour deux raisons [STA 02] :

- Plus évolutif pour les systèmes possédant des millions d'utilisateurs
- Authentification plus flexible



A veut envoyer un texte à B et ne veut pas qu'un tiers puisse y accéder durant l'échange.

1. A chiffre le texte à l'aide de la clé publique de B (fournie par B ou trouvée dans un annuaire) produisant ainsi un cryptogramme.
2. L'interception du cryptogramme par un tiers est sans conséquence, car il ne pourra pas obtenir le message en clair s'il ne possède pas la clé privée de B.
3. B déchiffre le cryptogramme à l'aide de sa clé privée et obtient le texte en clair que A désirait lui envoyer.

FIG 3.3 Chiffrement asymétrique [Sol 01]

III.2. Intégrité

Les services d'intégrité des réseaux visent à assurer le bon fonctionnement des ressources du réseau, et la transmission ou l'enregistrement sans problème des données sur le réseau. Ces services assurent une protection contre la modification délibérée ou accidentelle et non autorisée des fonctions du réseau (intégrité du système) et de l'information (intégrité des données) [LAR 98].

Un service d'intégrité assure que les messages sont reçus aussitôt qu'envoyés

III.3. Disponibilité

Comme leur nom l'indique, les services de disponibilité assurent à tous les utilisateurs l'accès aux ressources et aux données, comme prévu, on peut diviser ces services en deux groupes principaux. Dans le premier, nous retrouvons des services de contingentement, c.-à-d. les services qui sont requis pour empêcher les personnes, que leurs intentions soient malicieuses ou non [LAR 98], de surutiliser les ressources du réseau, comme l'espace disque, la mémoire, la largeur de bande, etc. de telle sorte que ces ressources ne soient plus disponibles pour les autres utilisateurs. Par ailleurs, un deuxième groupe de services de disponibilité assure le

maintien des fonctions du réseau lorsqu'il y a une panne de matériel ou de logiciel; ce groupe est désigné sous l'appellation «tolérance aux pannes».

III.3.1. Contingentement

Les services de contingentement servent à restreindre l'accès ou l'utilisation des ressources d'un réseau à un certain niveau, afin d'empêcher les utilisateurs d'en abuser, de telle sorte que d'autres utilisateurs ne puissent y avoir accès. La méthode de contingentement la plus commune consiste à imposer des quotas [LAR 98]. Avec des quotas, les utilisateurs ne peuvent utiliser au-delà d'une certaine quantité maximale toute ressource du réseau. Toutes les ressources du réseau ainsi protégées font l'objet d'une surveillance, afin d'assurer que leur utilisation ne dépasse pas les valeurs limites.

III.3.2. Tolérance aux pannes

Les services de tolérance aux pannes permettent aux réseaux de préserver la disponibilité de leurs ressources, même après une panne de composants. Ces services offrent donc au réseau la possibilité de résister aux défectuosités et aux pannes de composants, et de continuer à fonctionner pendant que l'on remplace les composants défectueux et (ou) que l'on récupère les données après une interruption de service.

III.4. Contrôle de l'accès

On peut empêcher la divulgation non autorisée de l'information ou des données en contrôlant l'accès à celles-ci. La plupart des réseaux modernes offrent une telle fonction, habituellement sous forme d'une liste de contrôle de l'accès. Ces listes énumèrent les personnes, les groupes de personnes ou les processus qui sont autorisés à accéder à certains fichiers ou répertoires [PIL 01].

III.5. L'authentification

L'authentification doit assurer que l'accès au système doit être autorisé uniquement au aux sujets habilités.

La phase d'authentification est décomposée en deus parties :

- L'identification lors de laquelle l'utilisateur présente son identifiant
- L'authentification ou l'utilisateur prouve son identité

IV. Différents types d'attaque

Les attaques sur le réseau sont des attaques passives ou des attaques actives :

IV.1. Attaques passives

Les attaques passives sont basées sur l'écoute indiscrète ou de surveillance de transition afin d'obtenir les informations qui ont été transmise. Ces attaques ne produiraient aucune modification d'information contenue dans le système et avec lesquelles ni le fonctionnement ni l'état du système ne changent [KEH 04]

Les attaques passives sont :

Ecoute physique ou capture de contenu de message (une conversion téléphonique, un courrier électronique, un fichier transféré peuvent contenir une information sensible ou confidentielle) [KEH 04].

Analyse de trafique : Elle est plus subtile, supposons qu'un moyen de masquer le contenu du massage de telle manière que les adversaires, même s'ils capturent le massage, ne pourrant pas en extraire l'information contenue. La technique la plus utilisé pour masquer le contenu est le chiffrement.

IV.2. Attaques actives

Ces attaques impliquent certaines modification du flot de données ou la création d'un flot frauduleux, l'altération des informations contenues dans ce système et modification de l'état ou de fonctionnement du système [STA 02].

IV.3. Quelques types d'attaques spécifiques

Dans les paragraphes suivants, en donnera une brève définition de quelque une des attaques particulièrement intéressantes.

IV.3.1 Virus

Un Virus est un programme qui peut « infecter » d'autres programmes en les modifiant afin de pouvoir " vivre " plus longtemps. La modification inclut une copie du programme viral, qui peut alors continuer a infecté d'autres programmes [PIL 01].

Comme son homologue biologique un virus informatique porte dans son code la recette pour fabriquer de parfaite copie de lui même. Logé dans un ordinateur hôte, un Virus prend le contrôle provisoire du système d'exploitation de l'ordinateur [STA 02].

IV.3.2 Cheval de Troie

Un Cheval de Troie est un programme ou une commande utile, ou apparemment utile, contenant un code caché qui, lorsqu' invoque, exécute quelque fonction indésirable ou nuisible [STA 02].
Des programmes de Chevaux de Troie peuvent être employés pour accomplir des fonctions indirectement, qu'un utilisateur non autorisé ne pourrait pas accomplir lui même. Par exemple pour obtenir l'accès aux fichiers d'un autre utilisateur sur un système partagé, un utilisateur pourrait créer un programme de Cheval de Troie qui, lors de son exécution, changerait les permissions de fichiers de l'utilisateur qui l'invoque, pour que ses fichiers soient lisibles par n'importe quel utilisateur.

IV.3.3 Bombe logique

Un des plus vieux types de menace logicielle, antérieur aux virus et aux vers, est la bombe logique. La bombe logique est un code incorporé dans des programmes légitimes et programmer pour « exploser » lorsque certaines causes sont réunies [STA 02]. Des exemples de telles conditions sont la présence ou l'absence de certains fichiers, un jour particulier de la semaine ou une date, un utilisateur particulier exécutant une application

IV.3.4 Sniffer

Un sniffer est un petit dispositif, logiciel ou matériel, qui permet de "voir" les informations qui transite par la machine où il se trouve [PIL 01]. Il ne sert pas seulement à capturer le texte saisi sur la machine mais toutes les informations provenant des machines du réseau passant par la machine en question.
Le sniffer peut ainsi servir à déceler les failles de sécurité, mais il peut aussi être utilisé de façon malveillante (pour intercepter les mots de passe du réseau par exemple).

IV.3.5 Les scanners

Un scanner est un programme qui permet de savoir quels ports sont ouverts sur une machine donnée.

Les scanners servent pour les crackers à savoir comment ils vont procéder pour attaquer une machine.

Leur utilisation n'est heureusement pas seulement malsaine, car les scanners peuvent aussi permettre de déterminer quels ports sont ouverts sur votre machine pour prévenir une attaque.

IV.3.6 Déni de service

Les attaques par Déni de service (souvent abrégé DoS, en anglais Denial Of service) consistent à paralyser temporairement (rendre inactif pendant un temps donné) des serveurs afin qu'ils ne puissent être utilisés et consultés. Elles sont un fléau touchant tout serveurs (Lan, Wan...) mais aussi tous particuliers reliés à l'Internet via les protocoles de la pile TCP/ IP [PIL 01]. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à des sociétés dont l'activité repose sur un système d'information en l'empêchant de fonctionner.

V. Le modèle TCP/IP

Les logiciels TCP/IP sont structurés en quatre couches de protocoles qui s'appuient sur une couche matérielle.

- La couche accès réseau et est constituée d'un driver du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau.

- La couche réseau ou couche IP (Internet Protocol) gère la circulation des paquets à travers le réseau en assurant leur routage. Elle comprend aussi des protocoles tel que ICMP (Internet Control Message Protocol)

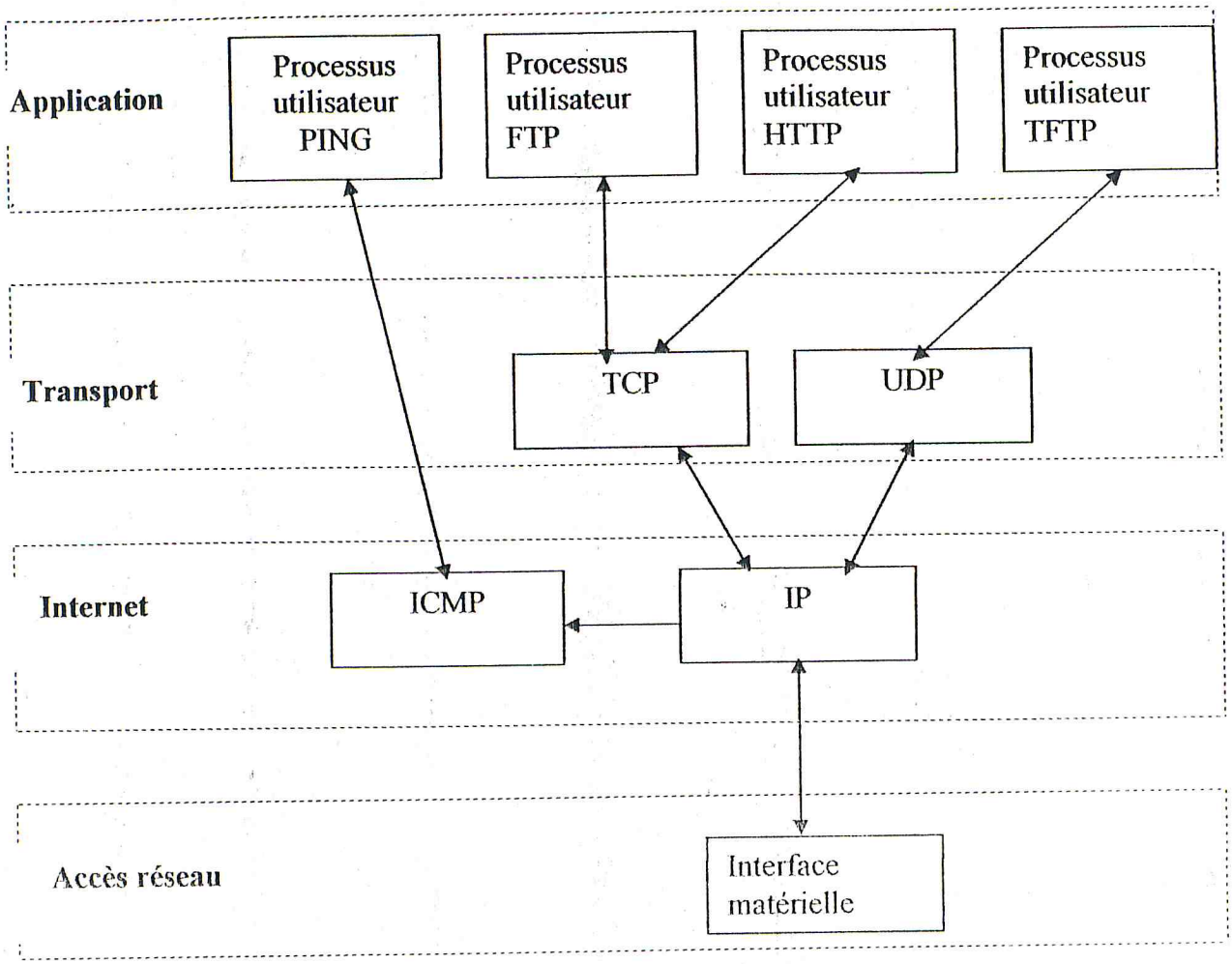


FIG 3.4 Les couches du modèle TCP/IP [BOR 98]

- La couche transport assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP (Transmission Control Protocol) ou non fiable dans le cas de UDP (User Datagram Protocol).

- La couche application est celle des programmes utilisateurs comme tel net (connexion à un ordinateur distant), FTP (File Transfert Protocol), SMTP (Simple Mail Transfert Protocol), etc.

Lorsqu'une application envoie des données à l'aide de TCP/IP, les données traversent de haut en bas chaque couche jusqu'à aboutir au support physique où elles sont alors émises sous forme de suite de bits.
L'encapsulation consiste pour chaque couche à ajouter de l'information aux données en les commençant par des en-têtes, voire en ajoutant des informations de remorque.

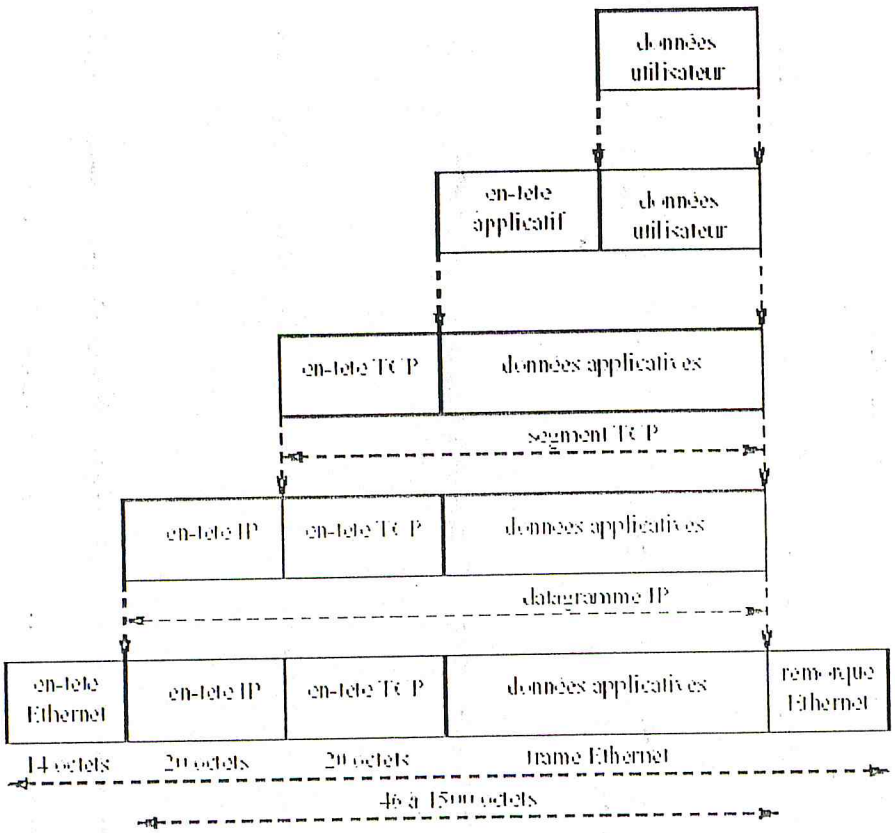


FIG 3.5 Encapsulation des données par la pile des protocoles TCP/IP [BOR 98].

V.1 La couche accès réseau

Cette couche a pour fonction l'encapsulation des datagrammes provenant de la couche IP et la mise en correspondance des adresses IP avec les adresses physiques utilisées sur le réseau. Il y a donc autant de versions de la couche accès réseau qu'il y a de type de moyen de transport des données [BEN 03]. Ainsi, par exemple, la couche physique est différente suivant que l'on est sur un réseau FDDI ou bien ETHERNET.

V.2 La couche Internet (la couche IP)

La couche Internet est au coeur du fonctionnement d'un internet. Il assure sans connexion un service non fiable de délivrance de datagrammes IP [BEN 03]. Le service est non fiable car il n'existe aucune garantie pour que les datagrammes IP arrivent à destination. Certains peuvent être perdus, dupliqués, retardés, altérés ou remis dans le désordre. Le mode de transmission est non connecté car chaque datagramme est traité indépendamment de ceux qui le précèdent et le suivent. Ainsi en théorie, au moins, deux datagrammes IP issus de la même machine et ayant la même destination peuvent ne pas suivre obligatoirement le même chemin [PAS 99]. Le rôle de cette couche est centré autour des fonctionnalités suivantes

- router les datagrammes jusqu'à leur adresse de destination
- transférer les données entre la couche physique et la couche transport
- fragmenter et réassembler les datagrammes

V.3. La couche transport

La couche transport fait le relais entre la couche IP et les applications, On présente ici les deux principaux protocoles de la couche transport d'Internet qui sont les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

V.3.1. User Datagram Protocol

Le protocole UDP utilise IP pour acheminer, d'un ordinateur à un autre, en mode non fiable des datagrammes qui lui sont transmis par une application. UDP n'utilise pas d'accusé de réception et ne peut donc pas garantir que les données ont bien été reçues. Il ne réordonne pas les messages si ceux-ci n'arrivent pas dans l'ordre dans lequel ils ont été émis.

V.3.2. Transmission Control Protocol

Contrairement à UDP, TCP est un protocole qui offre un service de flux d'octets orienté connexion et fiable. Les données transmises par TCP sont encapsulées dans des datagrammes IP en y fixant la valeur du protocole à 6 [BOR 98].

Le terme orienté connexion signifie que les applications dialoguant à travers TCP sont considérées l'une comme un serveur, l'autre comme un client, et qu'elles doivent établir une connexion avant de pouvoir dialoguer (comme dans le cas de l'utilisation du téléphone). Les ordinateurs vérifient donc préalablement que le

transfert est autorisé, que les deux machines sont prêtes en s'échangeant des messages spécifiques. Une fois que tous les détails ont été précisés, les applications sont informées qu'une connexion a été établie et qu'elles peuvent commencer leurs échanges d'informations [PAS 99]. Il y a donc exactement deux extrémités communiquant l'une avec l'autre sur une connexion TCP.

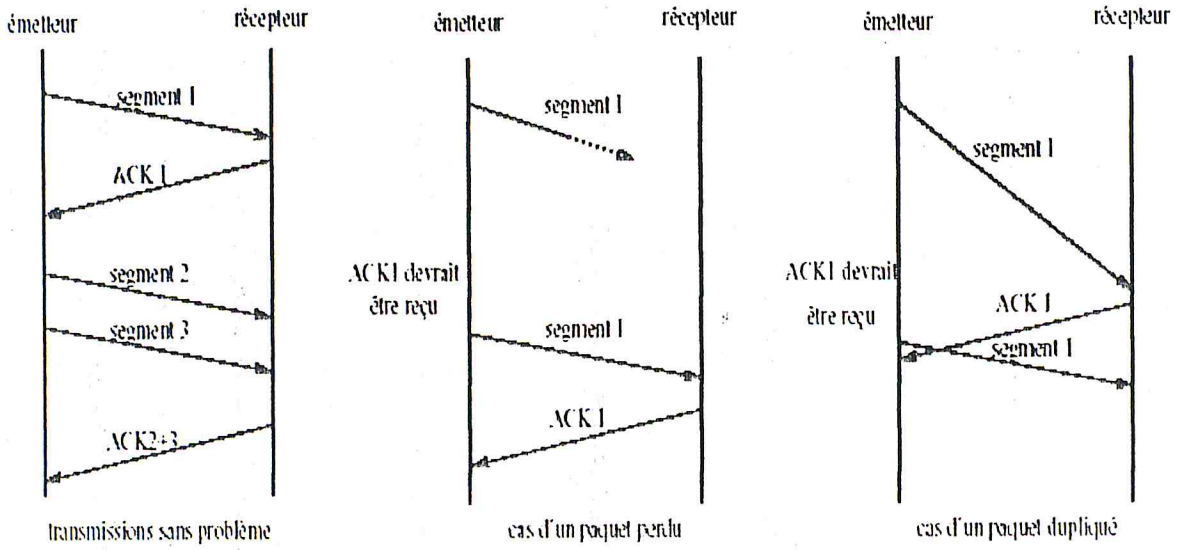


FIG 3.6 Échanges de segments TCP [PAS 99].

La fiabilité fournie par TCP consiste à remettre des datagrammes, sans perte, ni duplication, alors même qu'il utilise IP qui lui est un protocole de remise non fiable. Ceci est réalisé à l'aide de la technique générale de l'accusé de réception (ACK).

V.4. La couche Application

La couche application prend en charge les détails de communication d'une application particulière. Certains protocoles de cette couche sont des applications intégrables qui gèrent des requêtes réseau comme FTP. D 'autres protocoles fournissent un support aux applications sous forme de service comme SNMP

V.4.1. TELNET et Rlogin

Telnet et Rlogin sont deux applications qui permettent à un utilisateur de se connecter à distance sur un ordinateur, pourvu que cet utilisateur y dispose d'un accès autorisé. Ces deux applications permettent toutes les deux de prendre le contrôle (du moins partiellement) d'un ordinateur distant, mais Rlogin ne permet de le faire qu'entre deux machines Unix, tandis qu'il existe des clients Telnet pour

nombreuses plate formes (Unix, Windows, MacOs, ...). Tel net et Rlogin sont tous les deux bâtis sur TCP.

V.4.2. Transfert de fichier : TFTP et FTP

TFTP (Trivial File Transfert Protocol) et FTP (File Transfert Protocol) permettent tous les deux de transférer des fichiers d'une machine à une autre.. L'utilisation de FTP depuis un poste client pour aller chercher ou déposer un fichier sur un serveur nécessite de la part de l'utilisateur de se connecter avec un nom et un mot de passe. Donc, si l'utilisateur n'est pas reconnu la connexion FTP ne sera pas établie.

V.4.3. Le Protocole SMTP (Simple Mail Transfer Protocol)

Le courrier électronique au sein d'Internet est géré par le protocole SMTP (Simple Mail Transfer Protocol) bâti sur TCP (port 25). Il permet d'échanger des messages entre un expéditeur et un (ou plusieurs) destinataire pourvu que leurs adresses soient connues. Une adresse de courrier électronique se présente sous la forme nom@domaine est doit être composée de lettres (minuscules ou majuscules sont indifférenciés), de chiffres, de _ (souligné) et de . (point). Il est à noter qu'un mécanisme d'alias permet de définir des équivalences entre adresses, notamment de préciser quelle machine parmi toutes celles d'un même domaine gère réellement le courrier de chaque utilisateur.

V.4.4. World Wide Web: http.

HTTP (Hyper Text Transfer Protocol) est le protocole de communication du Web permettant d'échanger des documents hypertextes contenant des données sous la forme de texte, d'images fixes ou animées et de sons [DON 00].
Tout client Web communique avec le port 80 d'un serveur HTTP par l'intermédiaire d'une, ou plusieurs, connexions TCP simultanées, chacune des connexions TCP ouvertes servant à récupérer l'un des composants de la page web.
Trois types de requêtes sont disponibles :

- GET url renvoie l'information spécifiée par l'url.
- HEAD url renvoie l'en-tête de l'information demandée et non pas le contenu du document.

- POST pour envoyer du courrier électronique, des messages de news, ou des formulaires interactifs remplis par l'utilisateur.

La requête du client se compose de lignes de texte ASCII terminées par les caractères CR/LF et organisées comme ci-après :

requête	client	serveur
format	Requête/ url demandé /HTTP version En-têtes (0 ou plus) <Ligne blanche>	HTTP version code-réponse phrase-réponse En-têtes (0 ou plus) <Ligne blanche> Corps de la réponse
	Get / www.yahoo.fr 80 / http 1.0 Accept: text/html Accept: image/gif	HTTP/1.0 200 OK Date: Wed, 02Feb97 23:04:12 GMT LastModified:Mon,26Oct1998 19:13:02 Content-Type: text/html Content-Length: 13163 <Head> <Title>Yahoo! France</title> <base href="http://www.yahoo.fr/"> </Head> <Body> .... </Body> </Html>

Tableau 3.1 formats d'une requête http [DON 00].

Les codes de réponses sont des nombres de 3 chiffres rangés en 5 catégories comme décrits dans la table

Code	Description
1yz	non utilisé
200 201 202 204	succès OK, requête réussie OK, nouvelle ressource créée (commande POST) requête acceptée mais traitement incomplet OK, mais pas de contenu à envoyer
300 301 302 304	redirection (à gérer par le client) le document demandé a été définitivement déplacé vers une autre url le document demandé a été temporairement déplacé vers une autre url le document n'a pas changé (dans le cas d'un GET conditionnel)
400 401 403 404	erreur du client requête mal formulée interdit, la requête nécessite une certification interdit sans raison spécifique document non trouvé
500 501 502 503	erreur du serveur erreur interne du serveur non implanté mauvaise passerelle, réponse invalide d'une passerelle service temporairement indisponible

Tableau 3.2 Codes de réponses d'un serveur Web [DON 00]

VI Vulnérabilités et attaques dans la pile de protocole TCP/IP

VI.1 Attaque sur IP :

- **Ping o'death** : cette attaque crée un déni de service en utilisant un système de ping pour créer un paquet IP, les données vont arriver sur la machine destinataire sous la forme de petits paquets qui respectent la norme. Ce n'est qu'une fois rassembler que ces paquets dépassent la taille maximale des datagrammes IP, ce qui peut entraîner le crash de la machine [PIL 01].

- **l'IP spoofing** est dangereux car cette technique permet au pirate de se faire passer pour un utilisateur authentifié en changeant son adresse sur le réseau.

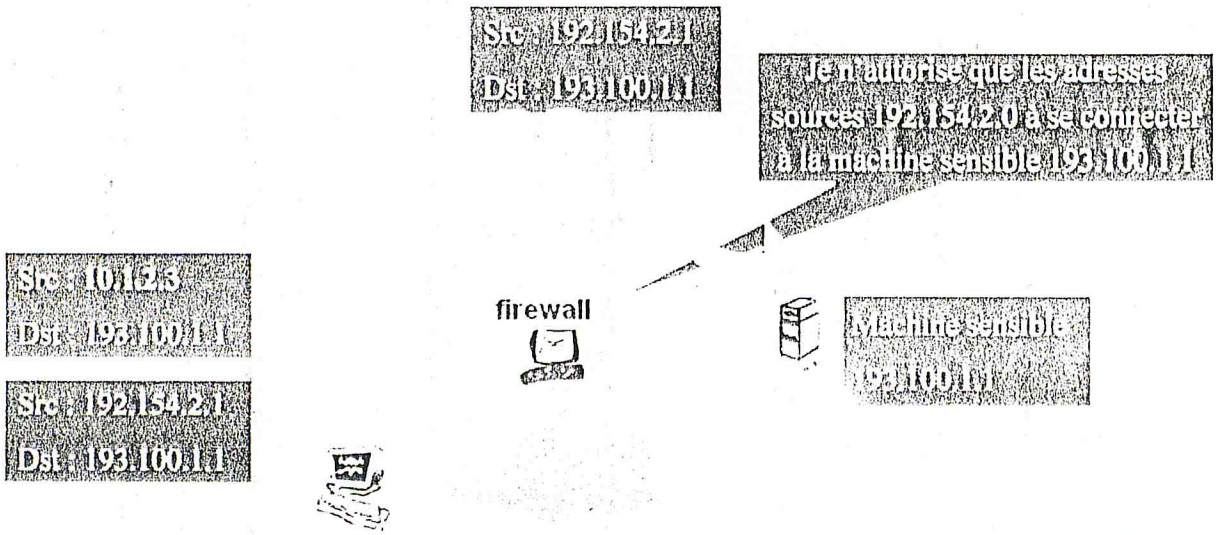


FIG 3.7 L'IP SPOOFING [YCH 02]

VI.2 Attaque sur TCP

- **Le TCP/SYN (flooding)**

Lors d'une connexion TCP, le client et le serveur échangent des données et des accusés de réception pour établir la connexion. On appelle ce mécanisme la poignée de main en trois temps.

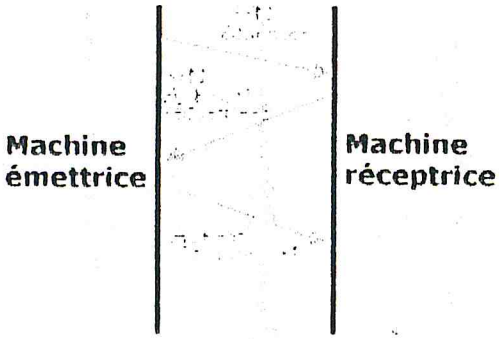


FIG 3.8 attaque sur une connexion TCP [PAS99]

Toutefois ce mécanisme possède une faiblesse lorsque le serveur renvoie un accusé de réception (*SYN-ACK*) mais ne reçoit aucun accusé (*ACK*) en provenance du client. Dans ce cas le serveur crée une structure de données contenant toutes les connexions ouvertes (et occupant de la place en mémoire). S'il est vrai qu'il existe un mécanisme d'expiration permettant de fermer des connexions ouvertes pendant un temps trop long, et ainsi libérer de la mémoire, il est possible pour un agresseur de saturer la mémoire rapidement en envoyant suffisamment rapidement des paquets *SYN*.

D'autre part, le système agresseur fournit généralement une adresse de retour d'un ordinateur n'étant pas capable de répondre. Il est ainsi très difficile de savoir d'où provient l'attaque [PIL 01].

VI.3 Attaque sur HTTP :

- **Bad HTTP request**, vise tous les systèmes et consiste à envoyer des requêtes

HTTP mal formaté. Le serveur peut alors planté [BEN 03].

VII. La sécurité dans les couches TCP/IP

Il existe de nombreuses technologies offrant des services de sécurité aux diverses couches de la pile TCP/IP. La couche application et la couche transport utilisent des protocoles de bout en bout, les systèmes doivent assurer la sécurité aux deux extrémités

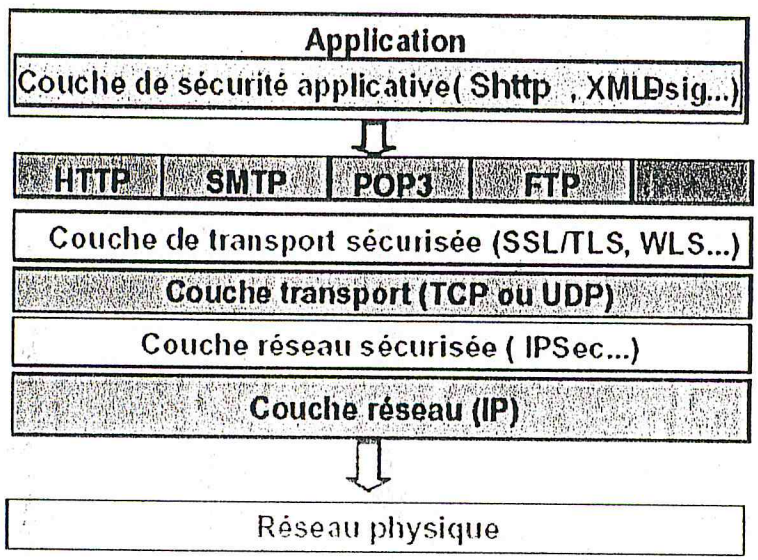


FIG 3.9 **Sécurisation des couches réseaux, transport et application** [Sol 01]

VII.1 Protocole SHttp

Secure http a été conçu pour sécuriser les messages qui utilisent le protocole http en permettant aux messages de requête et de réponse d'être authentifié, cryptés

Il supporte plusieurs mécanismes de gestion de clé.

Il peut vérifier l'intégrité des messages de l'authenticité de l'émetteur en calculant un code d'authentification de message [Sol 01].

VII.2 Protocoles de sécurité de la couche Transport

Ces protocoles sécurisent la couche Transport et fournissent des méthodes assurant la confidentialité, l'authentification et l'intégrité.

Protocole SSL

SSL (Secur Sockets Layer) est un protocole ouvert développé par Netscape. Il fournit un mécanisme pour garantir la sécurité des données implémentée entre les protocoles de niveau application (http, Telnet, Ftp) et TCP/IP. Il assure le chiffrement des données, l'authentification de serveur, l'intégrité des messages. L'objectif

principal de SSL est d'assurer la confidentialité et la fiabilité entre deux applications communicantes [KEH04].

VII.3 Protocoles de sécurité de la couche Réseau

La sécurité de ce niveau est gérée par les services au niveau de la couche IP de la pile de protocoles TCP/IP

Protocoles IP Security

IPSec s'applique au niveau IP, il est utilisé pour sécuriser n'importe quel type de trafic sur IP .IPSec comprend un ensemble de standards qui fournissent des services de confidentialité et d'authentification pour la couche IP. L'ensemble des services de sécurité IPSec peut assurer le contrôle d'accès, l'intégrité en mode non connecter, l'authentification de l'origine des données, le rejet de paquets redondants, la confidentialité (chiffrement) [KEH 04].

VIII. Conclusion

Nous Avon montré dans ce chapitre les risques et les menaces qu'un réseau peut être victime, nous essayons dans le chapitre suivant de donner les différentes solutions pour protéger un réseau et faire une barrière qui peut contrer les différentes attaques.

CHAPITRE 4

SOLUTIONS DE SECURITE

I. Introduction

Il existe plusieurs approches pour la prise en charge du problème de sécurité d'un réseau connecté à un réseau externe tel que les VPN (virtual private network), les IDS (système de détection d'intrusion) et les FIREWALLS.
Les FIREWALLS est L'approche la plus utilisée car elle permet la mise en place de mécanisme de sécurité limité à un seul niveau d'accès au réseau. Il composé d'une ou plusieurs fonctions de sécurité pour protéger le réseau contre les différentes menace possibles.

II. Les FIREWALLS

II.1. Définition d'un FIREWALL

Un FIREWALL (coupe feu en langue française) est essentiellement un dispositif de protection qui constitue un filtre entre un réseau local et un autre réseau non sûr tel que l'Internet ou un autre réseau local [BEL 03].

Le FIREWALL est en fait un mur entre l'Internet et le réseau local [CHA01].

Un coupe-feu peut-être considéré comme un sas permettant de réduire la zone vulnérable d'un réseau local à un seul point [BEL 03].

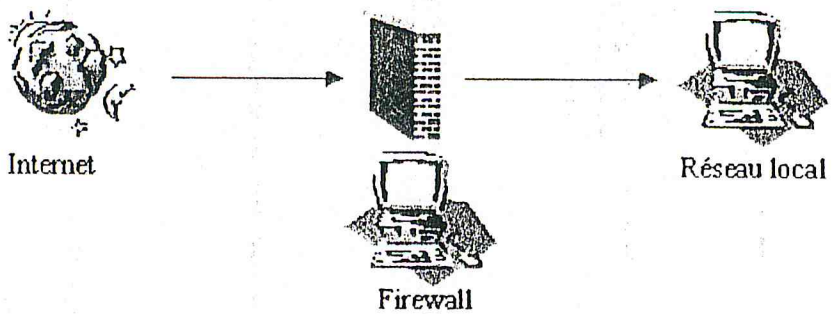


FIG 4.1 LE FIREWALL [FIRE]

Un coupe-feu est l'assemblage d'une partie matérielle (un ordinateur) et d'un logiciel installé sur celui-ci. L'installation d'un coupe-feu repose presque toujours sur la

nécessité de protéger un réseau de l'intrusion. Dans la plupart des cas, il devra interdire l'accès aux ressources matérielles et logicielles aux utilisateurs non autorisés [SAU].

Les coupe-feu visent, au niveau de la sécurité, deux objectifs :

1) Contrôler et protéger les hôtes du réseau local :
   - Contre la divulgation non autorisée d'informations sensibles
   - Contre les virus de toutes sortes

2) Protéger les serveurs
   - contre des commandes jugées dangereuses associées à des services du type "tel net " et "sendmail "
   - contre la modification ou la suppression non autorisée de fichiers vitaux pour le système vocation

II.2. Fonctionnement de base d'un FIREWALL

Le FIREWALL étant un mécanisme de sécurité, il implémente selon la politique de sécurité les fonctions de contrôle d'accès adéquates deux niveaux de contrôle d'accès possible :

- Le contrôle d'accès des paquets échangés
- Le contrôle d'accès des utilisateurs participants aux échanges de données [SAU]

Le contrôle d'accès des paquets doit considérer la nature du paquet, les machines sources et destination du paquet, ainsi que la direction du service demandé auquel appartient le paquet. En utilisant la terminologie du client serveur, on définit deux direction de service comme suit :

- Un service entrant ; dans ce cas le client est à l'extérieur du réseau et le serveur offrant le service est à l'intérieur du réseau.
- Un service sortant ; dans ce cas le client est à l'intérieur du réseau et le serveur est à l'extérieur du réseau [KEH 04]

La politique de sécurité peut autoriser les services entrants à des utilisateurs connus. Ils doivent être authentifiés avant d'utiliser les services internes. Les services sortants sont très souvent autorisés par les politiques de sécurité car on fait souvent confiance aux utilisateurs internes du réseau.

Les fonctions de filtrage du FIREWALL suivent le raisonnement exprimé par l'algorithme suivant :

Pour chaque paquet faire

a. si la politique de sécurité autorise le paquet

Alors

Établir la connexion en prenant les mesures de sécurité nécessaires. Aller a b

b. si le paquet appartient à la connexion autorisée

Alors

Autorisé le paquet

Sinon rejeter le paquet

Fait

Algorithme du fonctionnement du FIREWALL [CHA 01]

II.3. Notions de filtrage de paquets IP

Chaque ordinateur d'un réseau local relié à l'Internet est doté d'une adresse "IP" qui permet son identification sur le réseau, chaque adresse est unique et propre à une machine, elle est constituée d'une partie correspondant au numéro du réseau et d'une étant le numéro de la machine dans ce réseau.

Seule l'en-tête IP d'une trame peut laisser des traces lors de son passage, les rubriques utiles pour le filtrage de paquets sont :

- types de paquets (TCP, UDP, ...)
- adresse IP d'origine
- adresse IP de destination
- le port de destination, d'origine (TCP, UDP, ...)

FIG 4.2 le filtrage [FIRE]

Les filtres de paquets travaillent en triant les paquets d'après leur adresse ou leur port d'origine ou de destination. En général, aucun contexte n'est conservé ; les décisions sont prises seulement d'après le contenu du paquet en cours de traitement. L'administrateur fait une liste de services et machines acceptables et une liste de services ou machines irrecevables. Il est facile de permettre ou de refuser l'accès au niveau du réseau ou des machines avec un filtre de paquets [BEL 03]. Par exemple, on peut permettre tout accès IP entre les machines A et B ou refuser l'accès a B de toute machine excepte de A,

II.4. Configurations des FIREWALL

Le FIREWALL regroupe en fait tous les systèmes de sécurité qui fonctionnent en connexion avec un réseau. Il en existe différents types de philosophie de base du coupe-feu ; en effet, chaque type repose en quelque sorte sur celle-ci.
Cette philosophie est la suivante :

Tout ce qui n'est pas expressément interdit est autorisé
OU
Tout ce qui n'est pas expressément autorisé est interdit

Dans le premier cas, le coupe-feu est conçu pour bloquer le trafic. Tout est étudié au cas par cas après une analyse fine de tous les risques. Dans cette configuration, la protection peut-être ressentie comme une gêne par l'utilisateur.

Dans le deuxième cas, c'est l'administrateur du réseau qui doit réagir en temps réel. Il doit prévoir les attaques afin de les contrer. Cette méthode implique une "course à l'armement " entre les pirates et les responsables de la sécurité du réseau local.

II.5. Méthodes de filtrage

II.5.1. FIREWALL statique

Le filtrage statique est une des premières solutions FIREWALLS à avoir été mise en oeuvre. Ce système inspecte les paquets IP (en-tête et données) des couches réseau et transport afin d'en extraire l'adresse et le port source et l'adresse et le port de destination et le protocole utilisé. Ces quatre valeurs identifient la session en cours [BEL 03]. Cette solution permet de déterminer la nature du service demandé et de définir si le paquet IP doit être accepté ou rejeté en fonction des règles définies.

Exemple [BEL 03]

Posons que l'adresse IP de notre hôte est 172.16.1.1, et que quelqu'un essaye de nous envoyer du courrier électronique depuis sa machine distante à partir de l'adresse IP 192.168.3.5, le client SMTP de l'expéditeur utilise le port 1234 pour parler à notre serveur SMTP qui se trouve sur le port 25.

Règle	direction	Adresse source	Adresse destination	protocole	Port destination	action
1	Entrant	192.168.3.5	172.16.1.1	TCP	25	Permis
2	Sortant	172.16.1.1	192.168.3.5	TCP	1234	Permis

Tableau 4.1 table de filtrage

Le principal intérêt du filtrage statique réside dans sa transparence vis-à-vis des postes utilisateurs, ainsi que dans la vitesse des traitements.

Par exemple, une première règle indique que toutes les machines peuvent se connecter à un serveur Web sur Internet sur le port 80, et la suivante autorise le serveur Web à répondre à tous les clients du service (sur un port supérieur à 1024). Ces règles permettent à toutes les machines du réseau local d'accéder au Web.

Cet exemple est celui d'un service reposant sur TCP, La différenciation entre appel entrant et appel sortant repose sur une information de l'en-tête (le bit ACK) qui caractérise une connexion établie.
Ce type de distinction n'existe pas pour le protocole de data gramme UDP. Différencier un paquet valide d'une tentative d'attaque s'avère donc irréalisable. Cette problématique se retrouve également avec certaines applications qui répondent aux requêtes des clients sur des ports alloués dynamiquement. C'est le cas, notamment, pour FTP qui utilise un port pour les commandes et un port pour les données.
Il est généralement impossible de gérer de façon satisfaisante ce type de protocole sans ouvrir l'accès à un plus grand nombre de ports, et donc de rendre le réseau plus vulnérable. Le FIREWALL dynamique répond à ces limites.

II.5.2. FIREWALL dynamique

Le filtrage dynamique reprend le principe de travail du filtrage statique au niveau de la couche réseau, ainsi que la transparence de sa mise en place. Or, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement un port de manière aléatoire afin d'établir une session entre la machine faisant office de serveur et la machine cliente. Ainsi, il est impossible de prévoir les ports à laisser passer ou à interdire. Pour y remédier, on a breveté un système de filtrage dynamique de paquets ou basé sur l'inspection des couches réseau et transport du modèle TCP/IP. Cette technologie permet d'effectuer un suivi des transactions entre le client et le serveur et donc d'assurer la bonne circulation des données de la session en cours [BEL 03].

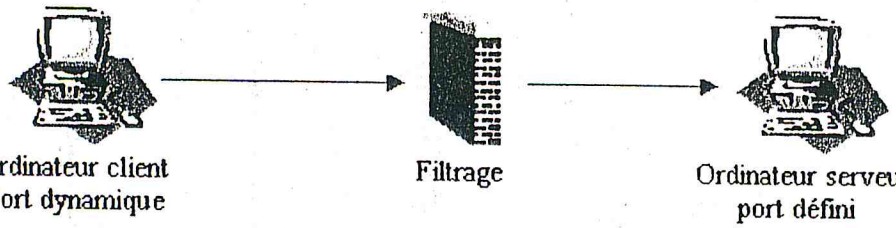


FIG 4.3 FIREWALL dynamique [FIRE]

Le filtrage dynamique tient donc à jour une table des connexions ouvertes par les clients pour certaines applications. C'est pour cette table gérée de manière dynamique qu'il porte son nom [KEH 04].
Si le filtrage dynamique est plus performant que le filtrage statique de paquets, il ne protège pas pour autant de failles applicatives, c'est-à-dire les failles liées aux logiciels, représentant la part la plus importante des risques en terme de sécurité.

II.5.3. FIREWALL applicatif

Un FIREWALL effectuant un filtrage applicatif permet de relayer des informations entre deux réseaux en effectuant un filtrage fin au niveau du contenu des paquets échangés. Il travaille sur la dernière couches du modèle TCP/IP, la couche application. Il s'agit donc d'un dispositif performant assurant une bonne protection du réseau, pour peu qu'il soit correctement administré.
En contrepartie une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications [BEN 03].
Le FIREWALL applicatif permet de vérifier l'intégrité des données et d'authentifier les échanges. Ce type de filtrage apporte une sécurité accrue puisqu'il permet de déceler les tentatives d'attaques sur la couche la plus haute du modèle TCP/ IP. A ce stade, le FIREWALL apporte les mêmes fonctionnalités en terme de filtrage qu'un proxy.

III. Le Proxy

Le but d'un Proxy est d'isoler une ou plusieurs machines pour les protéger, comme indiqué sur le schéma [GUI 00]

Les machines A doivent se connecter au réseau par l'intermédiaire du Proxy. Ce dernier sert de relais entre le réseau et les machines à cacher. Ainsi, les machines du réseau B auront l'impression de communiquer avec le Proxy, et non les machines A.

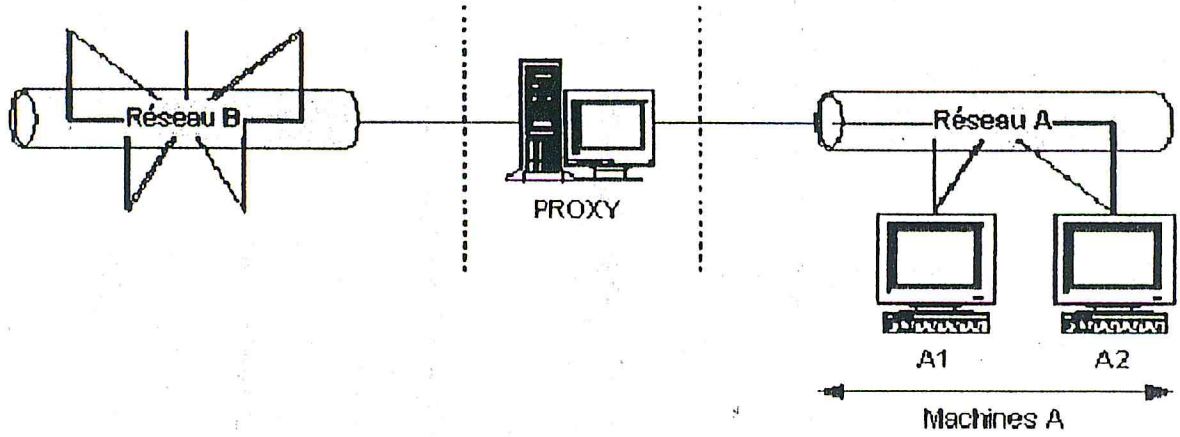


FIG 4.4 Placement du Proxy

III.1. Serveur Proxy

Le Proxy est un logiciel « serveur », acceptant des connexions « clientes » sur un ou plusieurs ports. Il se destine généralement à un protocole. Son but est, lors de la réception de requête de la part du réseau local, d'aller chercher l'information à la place du client pour la lui retransmettre. Ce système permet tout d'abord de rendre invisible les machines du réseau local pour le réseau externe. Pour les machines externes, les requêtes proviennent toujours de la même source : du serveur Proxy [PAU 03]. Ce système permet également de contrôler toutes les requêtes émanant des clients ainsi que les réponses des serveurs et donc, de les autoriser ou non selon certaines règles de la politique de la sécurité. Pour que cela fonctionne, il est évident que seul le Proxy doit pouvoir accéder au réseau externe. Les machines du réseau privé doivent passer par le Proxy pour atteindre Internet. Pour cette raison, un Proxy sera souvent couplé à un FIREWALL ou un routeur.

III.2. Fonctions d'un Proxy

Ce serveur agit sur les protocoles de la dernière couche du modèle TCP/IP, On trouve des Proxies applicatifs pour différents protocoles, les plus fréquents étant HTTP et HTTP , FTP, Tel net , Rlogin , Mail.

- Le FIREWALL n'est efficace que pour le trafic y transitant. Si un autre moyen est utilisé par accéder à un réseau externe, le FIREWALL ne sera d'aucune utilité. C'est le cas lors des communications par modem.
- La mise en place d'un FIREWALL ne change en rien la veille sécuritaire et la mise à niveau des logiciels par les correctifs fournit par les éditeurs. En effet, les modes d'intrusion des pirates utilisent souvent des failles de sécurité provenant des applications ou du système d'exploitation. En appliquant les correctifs, on comble ces failles de sécurité [CHA01].
- Un FIREWALL ne protège pas non plus des attaques au sein du réseau local. Si un pirate à l'intérieur du réseau local veut attaquer une machine au sein du même réseau local, le FIREWALL (étant donné que les messages n'y transitent pas) ne sera d'aucune utilité. C'est en paramétrant chaque machine qu'on améliore la sécurité globale.
- Le FIREWALL rentre dans le cadre d'une politique globale de sécurité. Cette politique globale se doit de définir les différentes zones et leur niveau de sécurité, les équipements du réseau et leur niveau de protection (routeur, pont, passerelle), les règles de filtrage pour le FIREWALL et le Proxy, la sécurité des machines au sein du réseau local, la sécurité des serveurs, la sauvegarde des données, etc. Tous ces choix sont à définir et à appliquer afin de garantir une qualité de service informatique au sein d'une entreprise [THO 04].
- La mise en place et la maintenance d'un FIREWALL est assez longue, complexe et nécessite un personnel qualifié. Il est nécessaire de disposer de bonnes compétences sur le réseau et sur le logiciel utilisé pour l'administrer. De plus, chaque nouveau service souhaité par les utilisateurs implique un changement des règles du FIREWALL. Un système sécurisé implique forcément une certaine rigidité [BEL 03].
- La mise en place d'un système de FIREWALL est assez coûteuse en terme de matériel, de logiciel et de personnel.

V. Les VPN

V.1. Définition d'un VPN

Les réseaux privés virtuels (VPN : Virtual Private Network) permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le

En plus de mandater les requêtes des clients, le serveur Proxy offre d'autres fonctionnalités :

III.2.1. Le cache

La plupart des Proxies ont la capacité de garder en mémoire les pages les plus souvent visitées par les clients. Lorsqu'une page "cachée" est demandée, le Proxy vérifie si la page a été mise à jour sur le serveur, si ce n'est pas le cas, il transmet sa copie. Cela limite le trafic sortant et permet de servir les clients plus rapidement. C'est une solution intéressante si l'on est limité par la bande passante et que l'on souhaite améliorer la qualité du réseau interne. Le cache offre également la possibilité de présenter la copie locale des pages lorsque les serveurs sur Internet sont inaccessibles[PAU 03].

III.2.2. Le filtrage

Il permet d'améliorer la bande passante en rationalisant l'utilisation des ressources. Il est en effet fréquent d'utiliser la connexion à Internet pour télécharger des ressources non professionnelles. Le filtrage permet d'interdire le téléchargement de certains fichiers et l'accès à certains sites jugés non professionnels. Les règles de filtrage doivent faire l'objet d'une réflexion philosophique et éthique faisant partie de la politique globale de sécurité qu'une entreprise doit se fixer. En plus de filtrer les requêtes sur les ports et les méthodes utilisées par le client, certaines fonctionnalités permettent de filtrer la réponse du serveur (en recherchant des mots-clés) et également effectuer une vérification en fonction de l'heure ou du jour de la semaine. On peut ainsi interdire l'utilisation d'Internet pendant certaines heures de la journée par exemple.

Certaines fonctionnalités avancées permettent également d'améliorer la navigation au sein des pages Web en supprimant les messages de publicité[PAU 03].

III.2.3. L'authentification

Il est possible de demander un identifiant ainsi qu'un mot de passe avant de servir les clients. Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire.

IV. Limites et inconvénients des FIREWALLS et des PROXIES

Le fait d'installer un FIREWALL n'est bien évidemment pas signe de sécurité absolue.

développement d'Internet, il est intéressant de permettre ce processus de transfert de données sécurisé et fiable. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffré.
Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet [BUT 00].

V.2. Principe des VPN

Le principe du VPN est basé sur la technique du tunnelling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Ensuite la source chiffre les données et les achemine en empruntant ce chemin virtuel [GUI 00].

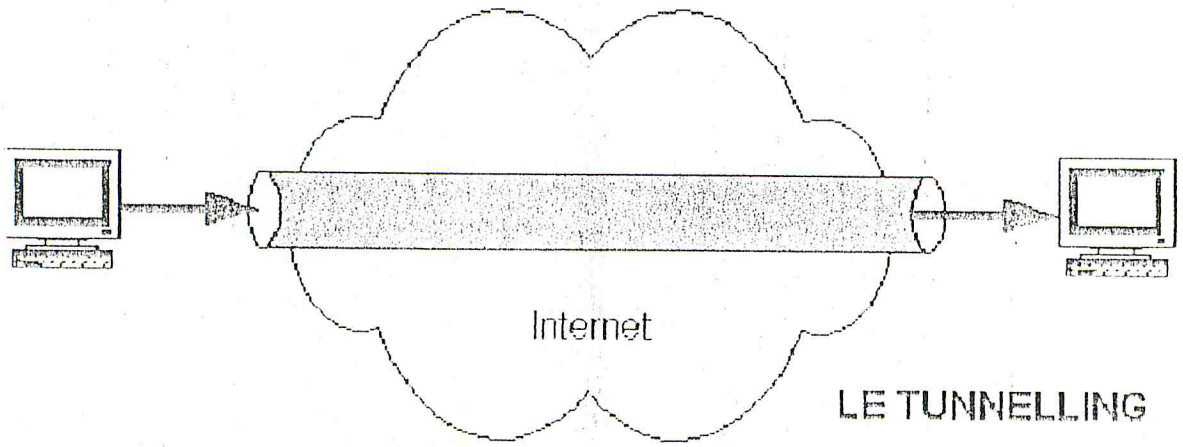


FIG 4.5 principe des VPN

V.3. Application des VPN

Auparavant pour interconnecter deux LANs distants, il n'y avait que deux solutions, soit les deux sites distants étaient reliés par une ligne spécialisée permettant de réaliser un WAN entre les deux sites soient les deux réseaux communiquaient par le RTC.
Une des premières applications des VPN est de permettre à un hôte distant d'accéder à l'intra net de son entreprise ou à celui d'un client grâce à Internet tout en garantissant la sécurité des échanges. Il utilise la connexion avec son fournisseur d'accès pour se connecter à Internet et grâce aux VPN, il crée un réseau privé virtuel entre l'appelant et le serveur de VPN de l'entreprise.

Cette solution est particulièrement intéressante même pour des entreprises : elles peuvent se connecter de façon sécurisée et d'où ils veulent aux ressources de l'entreprise. Cela dit, les VPN peuvent également être utilisé à l'intérieur même de l'entreprise, sur l'intra net, pour l'échange de données confidentielles [GUI 00].

VI. Les systèmes de détection d'intrusions :

La détection d'intrusion est une technologie de sécurité complémentaire des autres mécanismes mis en œuvre dans le cadre sécurité globale (authentification, chiffrement, outils de test de vulnérabilités, FIREWALL).
Les systèmes de détection d'intrusions ont pour but d'analyser tout ou partie des actions effectuées sur le système afin de détecter d'éventuelles anomalies de fonctionnement [BEN 03].

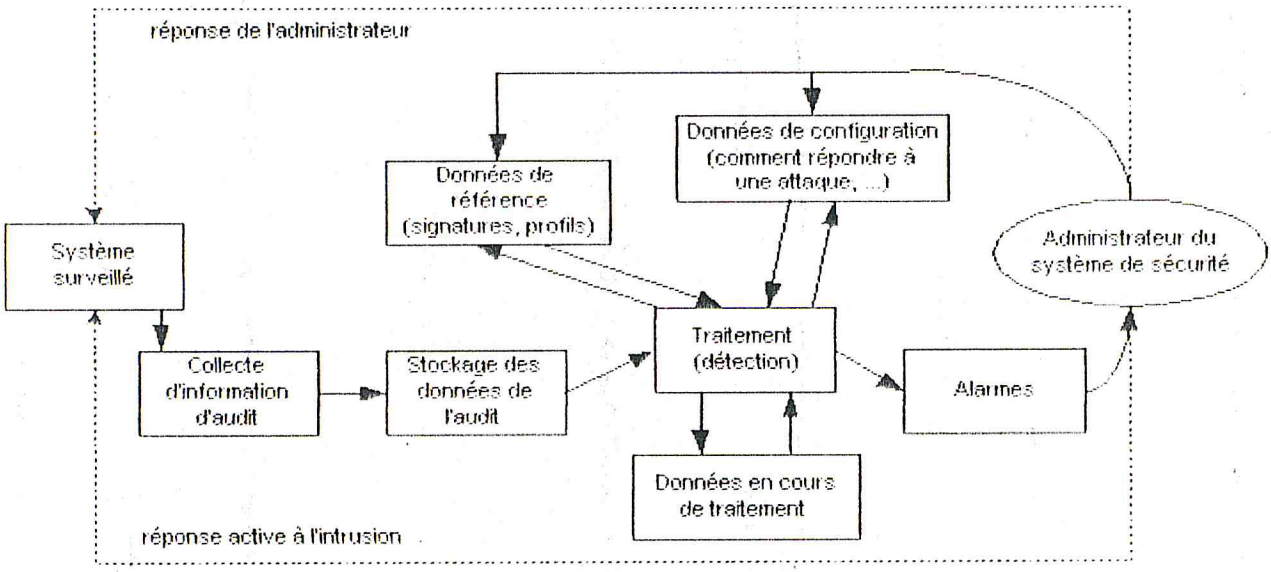


FIG 4.6 Modèle d'architecture de base pour Un système de détection d'intrusions [GUI 00]

L'audit de sécurité :

L'audit de sécurité permet d'enregistrer tout ou partie des actions effectuées sur le système. L'analyse de ses informations permet de détecter d'éventuelles intrusions. Les différents événements du système sont enregistrés dans un journal d'audit qui devra être analysé fréquemment.

Pour permettre la détection d'intrusions. On y trouve les informations sur les accès au système (qui y a accédé, quand et comment), les informations sur l'usage fait du système (utilisation du processeur, de la mémoire ou des entrées/sorties) et les informations sur l'usage fait des fichiers [GUI 00]

VI.1. Classification des systèmes de détection d'intrusions :

La classification des systèmes de détection d'intrusion est un sujet difficile à cerner. La raison principale est que la plupart des IDS sont basés sur plus d'une approche. La principale approche la plus utilisée, peut être soit comportementale, soit par scénarios [BEN 03].

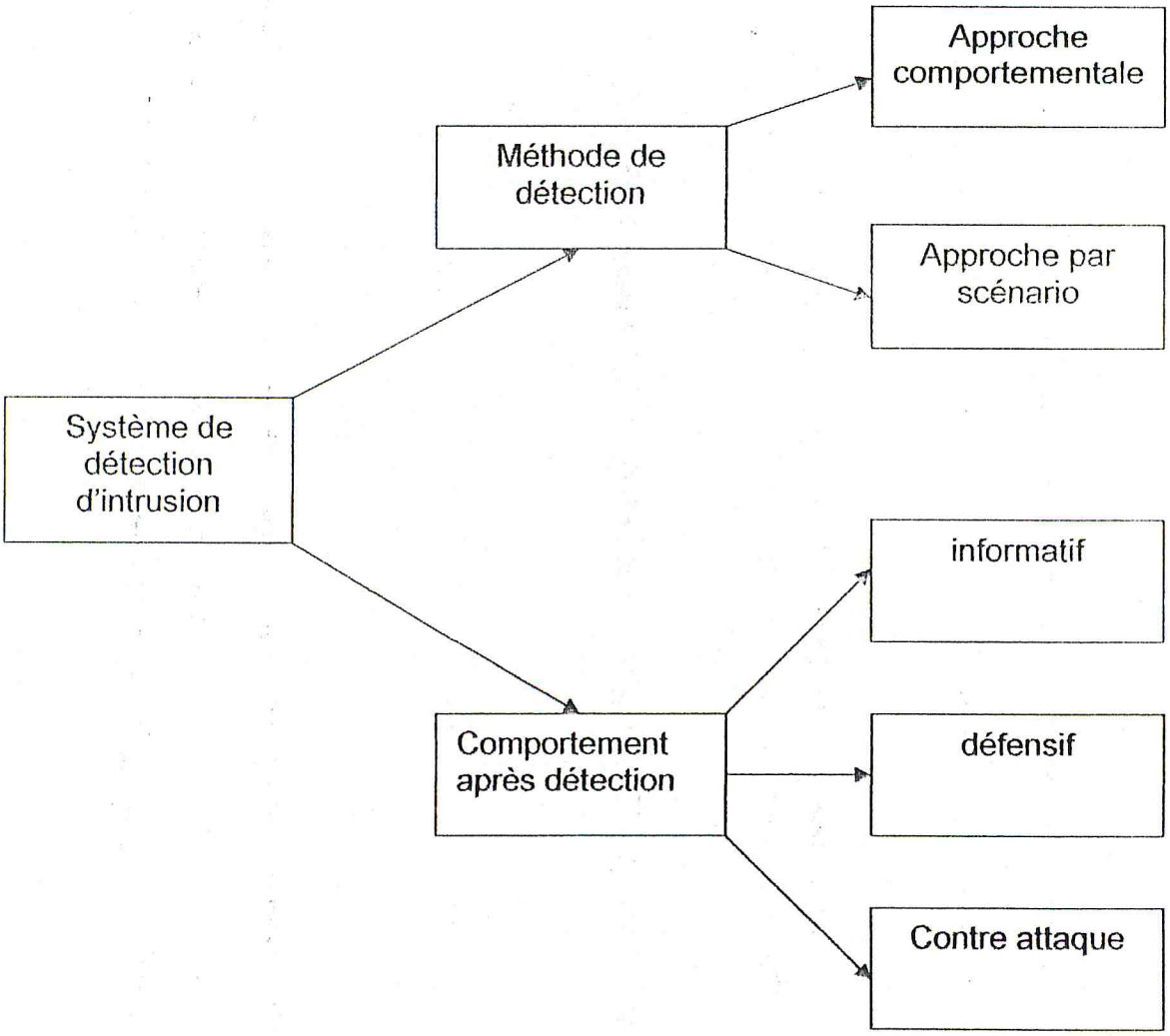


FIG 4.7 Classification Des IDS [GUI 00]

VI.1.1. Approche comportementale et approche par scénarios :

Dans les traces d'audit, on peut chercher deux choses différentes. La première correspond à l'approche comportementale, c'est-à-dire qu'on va chercher à savoir si un utilisateur a eu un comportement déviant par rapport à ses habitudes. Ceci signifierait qu'il essaye d'effectuer des opérations qu'il n'a pas l'habitude de faire. On peut en déduire, soit que c'est quelqu'un d'autre qui a pris sa place, soit que lui même essaye d'attaquer le système en abusant de ses droits. Dans les deux cas, il y a intrusion.

La deuxième chose que l'on peut chercher dans les traces d'audit est une signature d'attaque. Cela correspond à l'approche par scénarios. Les attaques connues sont répertoriées et les actions indispensables de cette attaque forment sa signature. On compare ensuite les actions effectuées sur le système avec ces signatures d'attaques. Si on retrouve une signature d'attaque dans les actions d'un utilisateur, on peut en déduire qu'il tente d'attaquer le système par cette méthode [BEN 03].

VII. Conclusion

Nous avons présenté dans ce chapitre les différentes solutions pour sécuriser un réseau. Ce marché est toujours en pleine progression, pour évaluer un produit qui répond aux contraintes qu'on a cité reste une chose extrêmement difficile vu que le niveau de complexité des attaques au système évolue lui aussi et impose aux produits de sécurité d'être toujours plus puissants.

CHAPITRE 5 :

CONCEPTION ET MISE-EN ŒUVRE DE LA SOLUTION

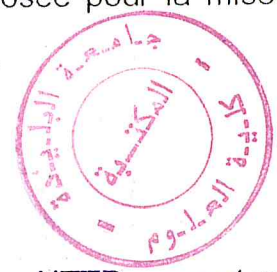
I. Introduction

La phase la plus importante dans l'élaboration des applications est la conception. La conception d'une application produit une architecture simple et nette d'un programme résolvant un problème donné.

Ainsi, notre conception, basée essentiellement sur l'étude effectuée dans les chapitres précédents, notamment celui des solutions de sécurité existantes, consiste à trouver des solutions qui répondront éventuellement au travail qui nous a été confié, pour finalement bâtir la structure du programme final.

Après avoir étudier l'état actuel de la politique de sécurité appliqué dans le département de commercialisation à SONATRACH et vu le nombre de connexions important à Internet, nous allons poursuivre notre plan d'action en concevant un serveur Proxy qui réalise un filtrage applicatif permettant à l'administrateur du réseau d'enrichir sa politique de sécurité.

Dans ce chapitre, nous allons décrire notre conception proposée pour la mise en œuvre d'un serveur proxy.



II. Objectifs et besoins

L'objectif du développement était de réaliser un serveur Proxy HTTP supportant la norme HTTP/1.0 qui permet donc au client de l'application, de naviguer sur Internet de façon transparente.

Seul le rôle de mandataire et celui de filtrage par adresse sont visés. Le rôle de cache et celui d'authentification sont des fonctions annexes qui ne sont pas fondamentales pour le fonctionnement du proxy, le filtrage est réalisé En fonction de l'Url et du port saisi par l'utilisateur.

Le serveur Proxy doit également pouvoir supporter plusieurs clients de façon simultanée.

Par ailleurs, le support des règles peut être dans une base de donnée.

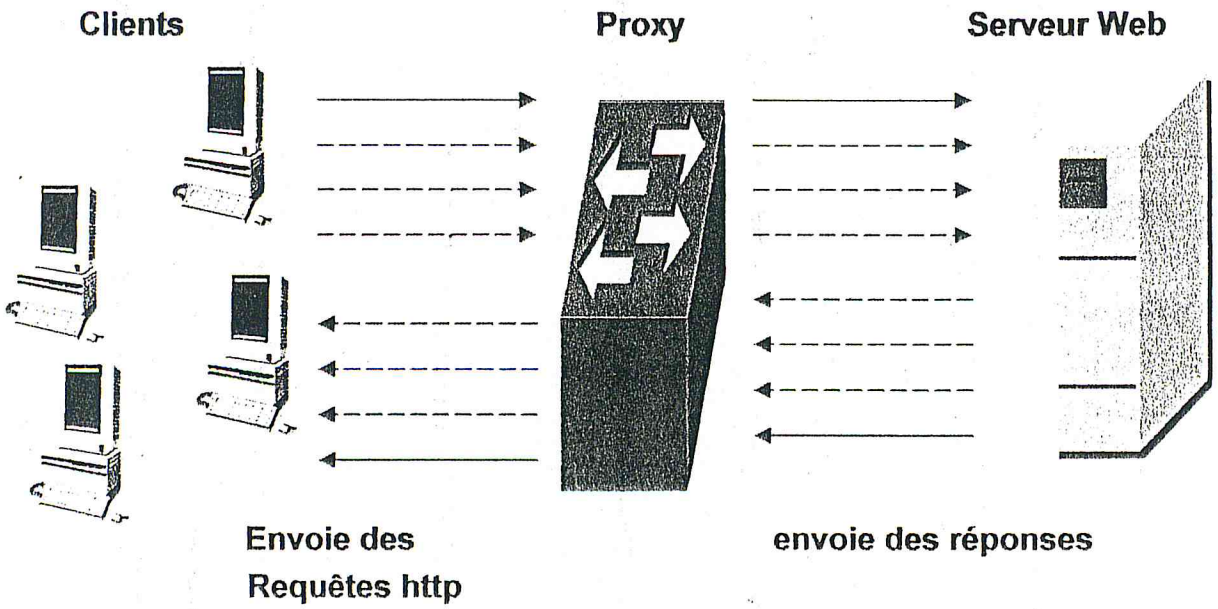


FIG 5.1 proxy http

III. Méthode de conception

La technique de modélisation par objet (OMT) est le nom qui a été donné à la méthode qui associe trois vues de modélisation des systèmes. Le modèle objet représente les aspects statiques, structurels et de données d'un système. Le modèle dynamique représente les aspects temporels, comportementaux et de contrôle d'un système. Le modèle fonctionnel représente les aspects de fonctions et de transformation.

III.1. Le modèle objet

Le modèle objet décrit la structure des objets dans un système : leur identité, leurs relations avec les autres objets, leurs attributs et leurs opérations. Le modèle objet fournit le cadre majeur dans lequel les modèle dynamique et fonctionnel peuvent être placé. Les modifications et transformations et modifications n'ont pas de signification. Les objets sont des unités utilisées pour diviser le monde [RUM 97].

III.2. Le modèle dynamique

Le modèle dynamique décrit les aspects du système en relation avec le temps et le séquencement des opérations : les événements qui marquent le changement, les séquences d'événement les état qui définissent le contexte des événement, et

l'organisation des états et des événements le modèle dynamique modélise le contrôle,

Le modèle dynamique est représenté graphiquement par des diagrammes d'état chaque diagramme d'état met en évidence les séquence d'état et d'événement permis dans un système pour une classe d'objet, les diagrammes d'état sont également en relation avec les autres modèle[RUM 97].

III.3. Le modèle fonctionnel

Le modèle fonctionnel décrit les aspects relatifs aux transformations des valeurs : fonctions, correspondances, le modèle fonctionnel modélise ce que fait un système sans s'occuper de la façon ou du moment ou il le fait.

Le modèle fonctionnel est représenté par des diagrammes a flots de données. Les diagrammes à flots de données montrent les dépendances entre les valeurs et le calcul des valeurs de sorties a partir des valeurs d'entrée et des fonctions sans tenir compte du moment de l'exécution des fonctions [RUM 97].

III.4. Les relations entre les modèles

Chaque modèle décrit un aspect du système mais contient des références aux autres modèles. Le modèle objet décrit les structures des données sur lesquelles les modèles dynamiques et fonctionnels opèrent. Les opérations du modèle objet correspondent aux événements du modèle dynamique et aux fonctions du modèle fonctionnel [RUM97]

IV. Description des cas d'utilisations

L'utilisation de notre application est très simple, elle est exprimée par les cas suivant :

VI.1. Coté client

Demande de connexion : pour que le client puisse transmettre une requête, notre serveur Proxy doit accepter sa connexion.

Effectuer une requête : quand la connexion est accepter, le client peut transmettre une requête sur un site de son choix.

VI.2. coté administrateur :

Consulter le journal des connexions : il permet a l'administrateur de contrôler les postes clients et d'avoir des informations sur leur connexions.
Modifier la politique de sécurité : c'est a l'administrateur de décider et de choisir sa politique, il a le privilège d'autoriser des sites et d'interdire des autres en modifiant les règles de filtrage

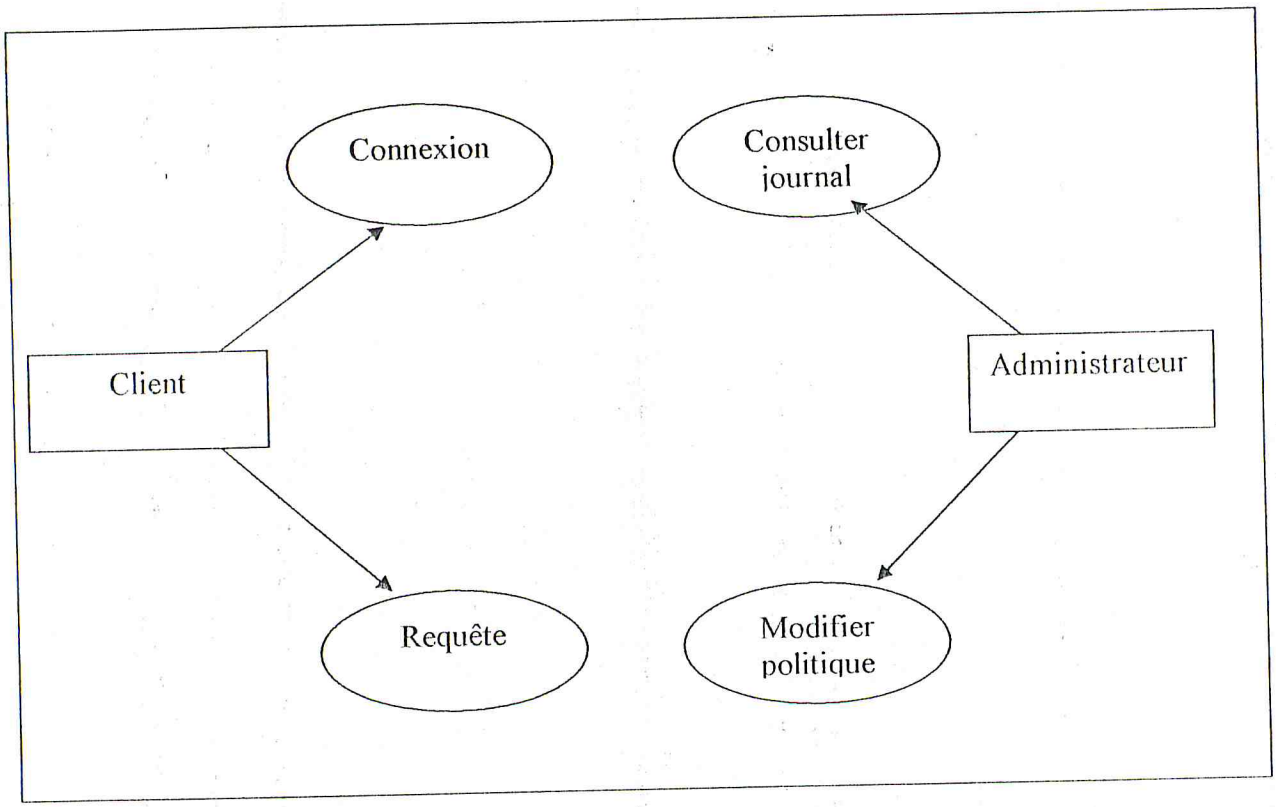


FIG 5.2 Cas d'utilisations

V. Dictionnaire de données

La première étape dans la modélisation objet consiste à définir les entités qui entrent en jeu dans la modélisation. Chaque classe d'objet doit être décrit dans un paragraphe ainsi la description de son cadre d'utilisation et ses relations avec les autres classes avant d'être assemblé dans le diagramme objet

PROXY serveur tournant sur un port précis en attente de connexion cliente, capable d'accepter et de traiter plusieurs demandes de la part de plusieurs clients simultanément, son rôle est de récupérer les informations sur les requêtes de ses clients et de les transmettre à **PROXYREQUETE** pour les traitements et le renvoie de la réponse.

PROXYREQUETE processus chargé de traiter les requêtes acceptées par le serveur, il utilise les détaille fournies par **TRAITEMENT** pour appliquer le filtrage des adresses en utilisant les règles fournies par **REGLE**, il s'occupe aussi de la communication entre le client et le serveur Web a travers les flux d'entrée et de sortie.

TRAITEMENT utilisé par le **PROXYREQUETE**, détermine les détaille des connexions des clients en analysant l'entête envoyé par le **PROXYREQUETE** en ce qui concerne le protocole http utilisé, l'adresse demandée et le port utilisé.

INTERFACE adresse réseau utilisé par le client pour de connecter a Internet, le client peut utiliser une carte réseau on un modem, elle détecte l'adresse interne du client ainsi que l'adresse pour se connecté a l'Internet.

REGLES ensembles de règles définies par l'administrateur selon la politique de sécurité choisies par ce dernier, charge les règles en consultant les fichiers des règles

CLIENT est l'entité qui demande une connexion pour transmettre une requête à un serveur Web, cette demande est prise en considération par la classe Proxy pour la traiter.

SERVEUR WEB c'est le serveur qui héberge les pages Web, il répond à chaque requête en lui transmettant la page nécessaire si elle existe.

LECTURE permet la lecture dans un fichier, elle est utilisée par l'administrateur pour la consultation des journaux de connexions

ADMINISTRATEUR la personne qui gère le réseau, il peut effectuer plusieurs taches tel que la modification de la politique de sécurité, il a le privilège d'ajouter ou de supprimer des règles

Dictionnaire de données pour les classes du serveur Proxy

VI. Diagramme objet

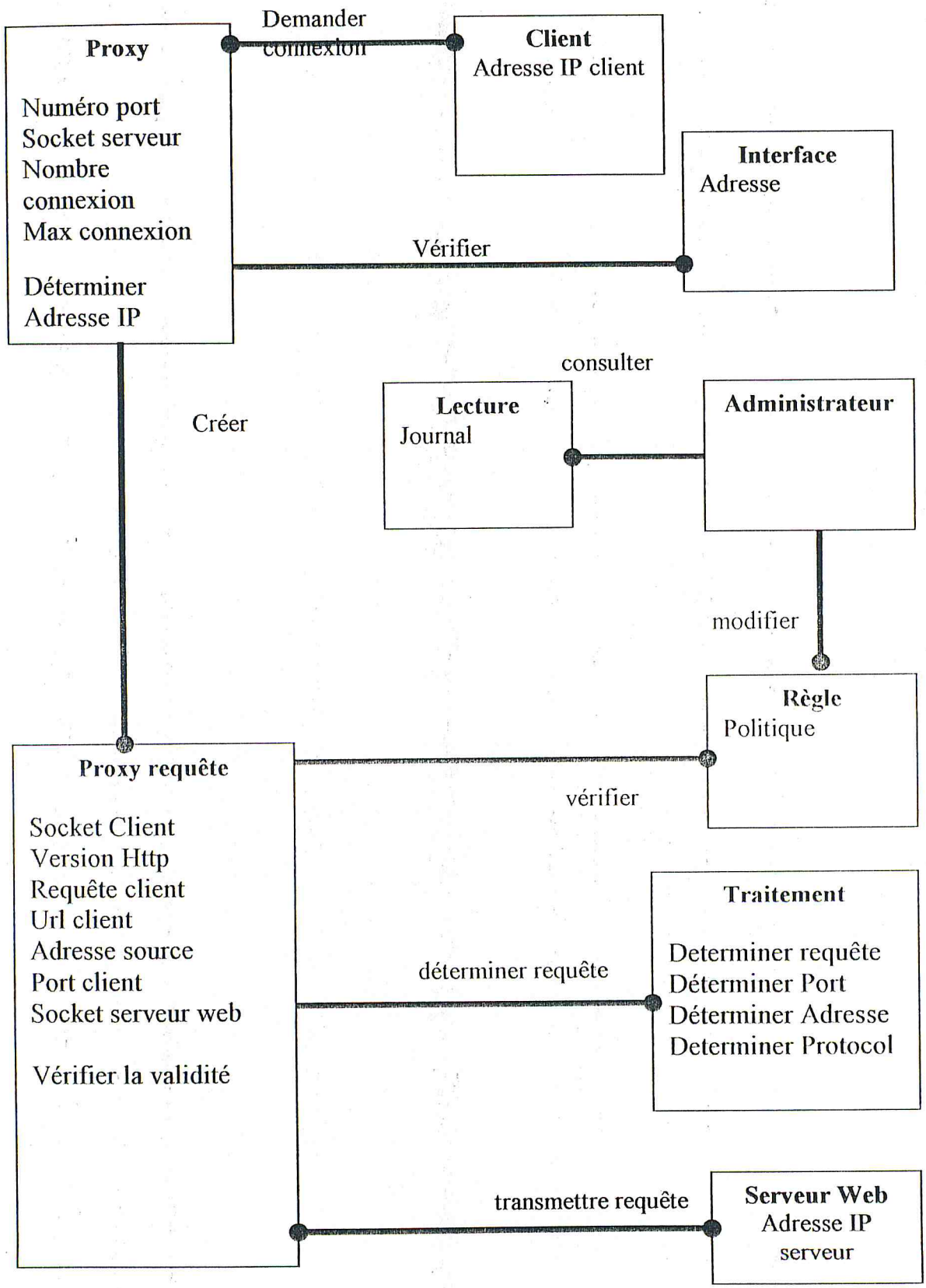


FIG 5.3 Modèle objet du serveur Proxy

VII. Modèle dynamique

V.1. Les scénarios d'événements

a) Scénario d'une requête validée

Nous présentons dans ce scénario le suivi d'événement d'une requête qui sera validé par le filtrage

Le Proxy vérifie les interfaces réseaux,
Interface trouvée, pré à accepter des connections
Le client demande une connexion et transmet une requête :www.google.com
Le Proxy accepte la connexion
Le PROXYREQUETE Détermine la requête
La requête est : GET : http: // Www.google.com : 80
Le PROXYREQUETE Détermine l'adresse,
L'adresse est www.google.com
Le PROXYREQUETE Détermine Le port
Le port utilisé est 80
Le PROXYREQUETE Détermine Le protocole
Le protocole utilisé est http 1.0
Le PROXYREQUETE Détermine le mode de filtrage a utilisé
Le mode utilisé est : allow ;
Vérifie la validation de l'adresse et du port dans le fichier dény :
La requête est autorisée
Ouverture du flux d'entrées et de sorties du serveur
Envoie la requête au serveur
Réception de la requête du serveur
Envoie de la requête au client et affichage de la page demandé
Fermeture des flux d'entrées et de sorties
Fin de la connexion
Le serveur attend éventuellement de nouvelle connexion

Cette séquence est représentée par le diagramme de suivi d'événement d'un déroulement normal du Proxy

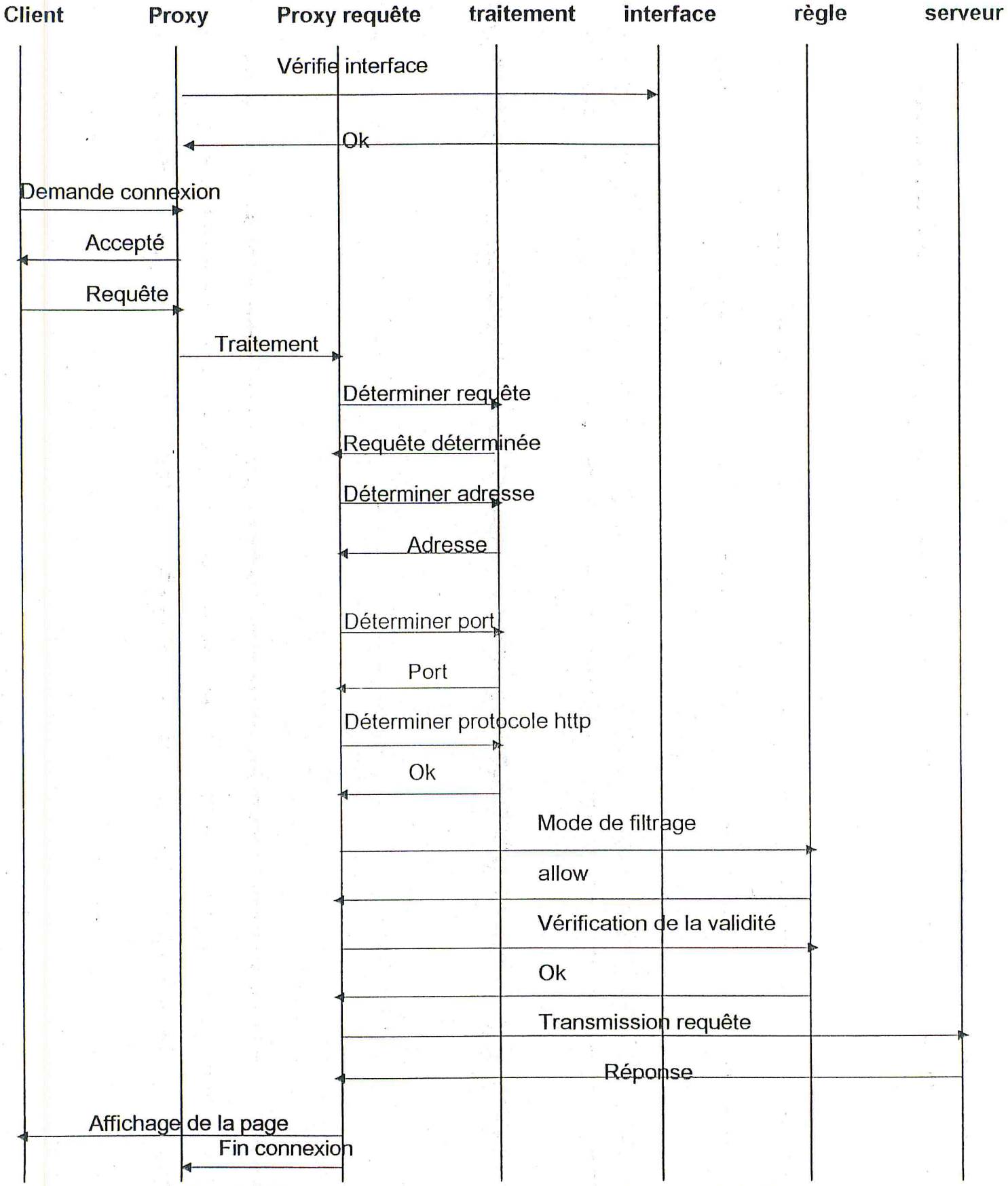


FIG 5.4 Suivi d'événement pour un scénario normal du Proxy

b) Scénario d'une requête refusée

Ce deuxième scénario explique la transmission d'une requête qui sera rejeté par le Proxy, son filtrage indique que l'accès a ce site est interdit, donc sa transmission au serveur Web est inutile

Le Proxy vérifie les interfaces réseaux,
Interface trouvée, pré à accepter des connections
Le client demande une connexion
Le Proxy accepte la connexion
Le client demande l'ouverture du flux d'entrées et de sorties et transmet une requête :www.microsoft.com
Le PROXYREQUETE Détermine la requête
La requête est : GET : http:// Www.microsoft.com :80
Le PROXYREQUETE Détermine l'adresse,
L'adresse est www.microsoft.com
Le PROXYREQUETE Détermine Le port
Le port utilisé est 80
Le PROXYREQUETE Détermine Le protocole
Le protocole utilisé est http 1.0
Le PROXYREQUETE Détermine le mode de filtrage a utilisé
Le mode utilisé est : allow
Vérifie la validation de l'adresse et du port dans le fichier dény
La requête est refusée
Envoie de la requête au client et affichage de la page indiquant le message : « vous n'étés pas autorisé a afficher cet page »
Fermeture des flux d'entrées et de sorties
Fin de la connexion
Le serveur attend éventuellement de nouvelle connexion

Cette séquence est représentée par le diagramme de suivi d'événement elle est considérer toujours comme un déroulement normal du Proxy.

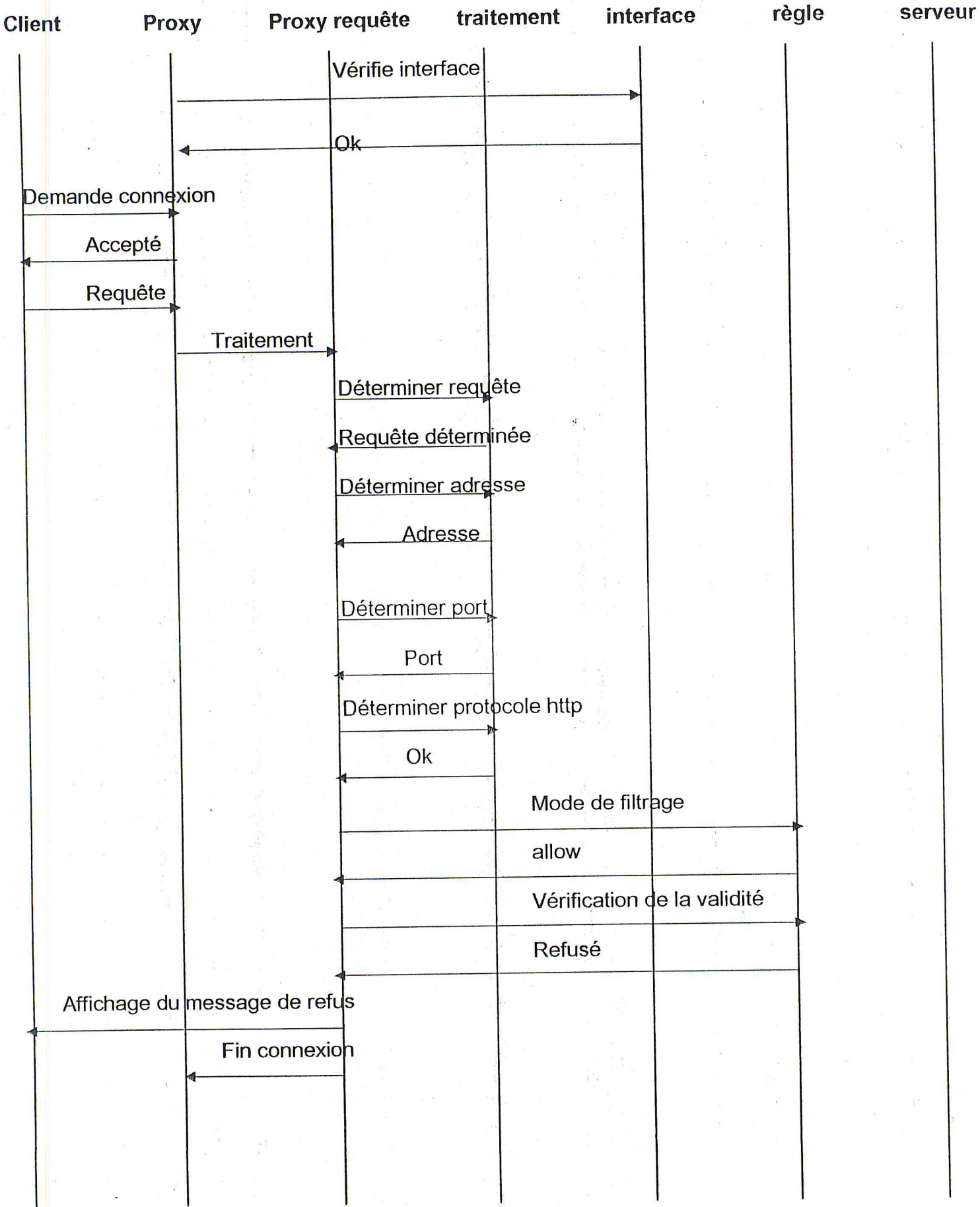


FIG 5.5 Suivi d'événement pour un scénario normal du Proxy

c) Scénario de l'administrateur

Ce scénario explique le rôle de l'administrateur dans le choix de la politique de sécurité, a partir du journal des connexions, il a le privilège d'ajouter ou de supprimer des règles

L'administrateur demande la consultation du fichier contenant le journal
L'administrateur Remarque l'abus sur quelque adresse Internet
L'administrateur décide de modifier la politique de sécurité pour bloquer ces accès
La politique est modifiée

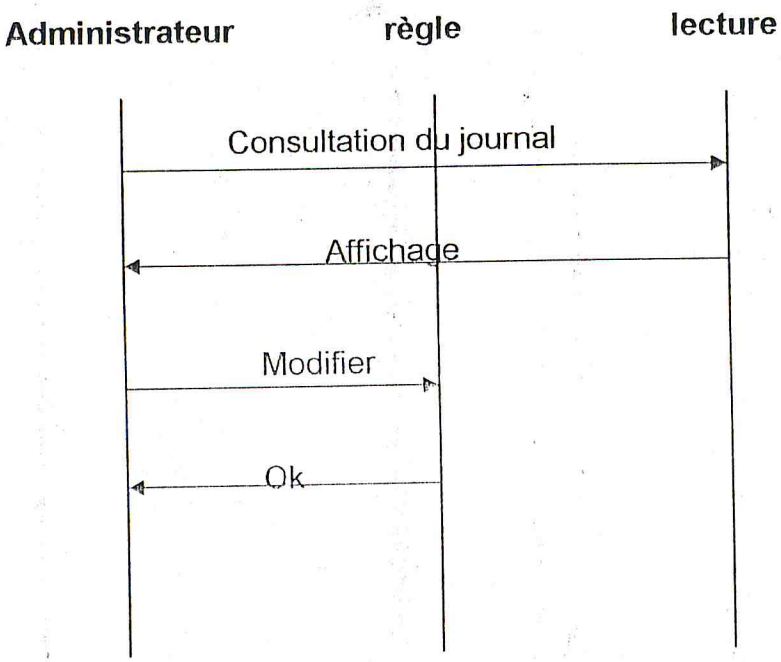


FIG 5.6 Suivi d'événement pour un scénario de l'administrateur

d) Scénario avec échec

La séquence suivante montre le cas ou la raquette du client n'est pas valide,

Le Proxy vérifie les interfaces réseaux,
Interface trouvée, pré à accepter des connections
Le client demande une connexion
Le Proxy accepte la connexion
Le client demande l'ouverture du flux d'entrées et de sorties et transmet une requête : www.google.com
Le **PROXYREQUETE** Détermine la requête
La requête est : GET : http:// Www.google.com :80
Le **PROXYREQUETE** Détermine l'adresse,
L'adresse est www.google.com
Le **PROXYREQUETE** Détermine Le port
Le port utilisé est 80
Le **PROXYREQUETE** Détermine Le protocole
Le protocole utilisé est http 1.0
Le **PROXYREQUETE** Détermine le mode de filtrage a utilisé
Le mode utilisé est : dény ;
Vérifie la validation de l'adresse et du port dans le fichier allow :
La requête est autorisée
Ouverture du flux d'entrées et de sorties du serveur
Envoie la requête au serveur
Réception de la réponse du serveur indiquant « l'adresse IP n'a pas pu être déterminé »
Fermeture des flux d'entrées et de sorties
Fin de la connexion
Le serveur attend éventuellement de nouvelle connexion

Le diagramme suivant présente le déroulement de cette séquence, il représente du suivi d'événement avec un cas d'échec

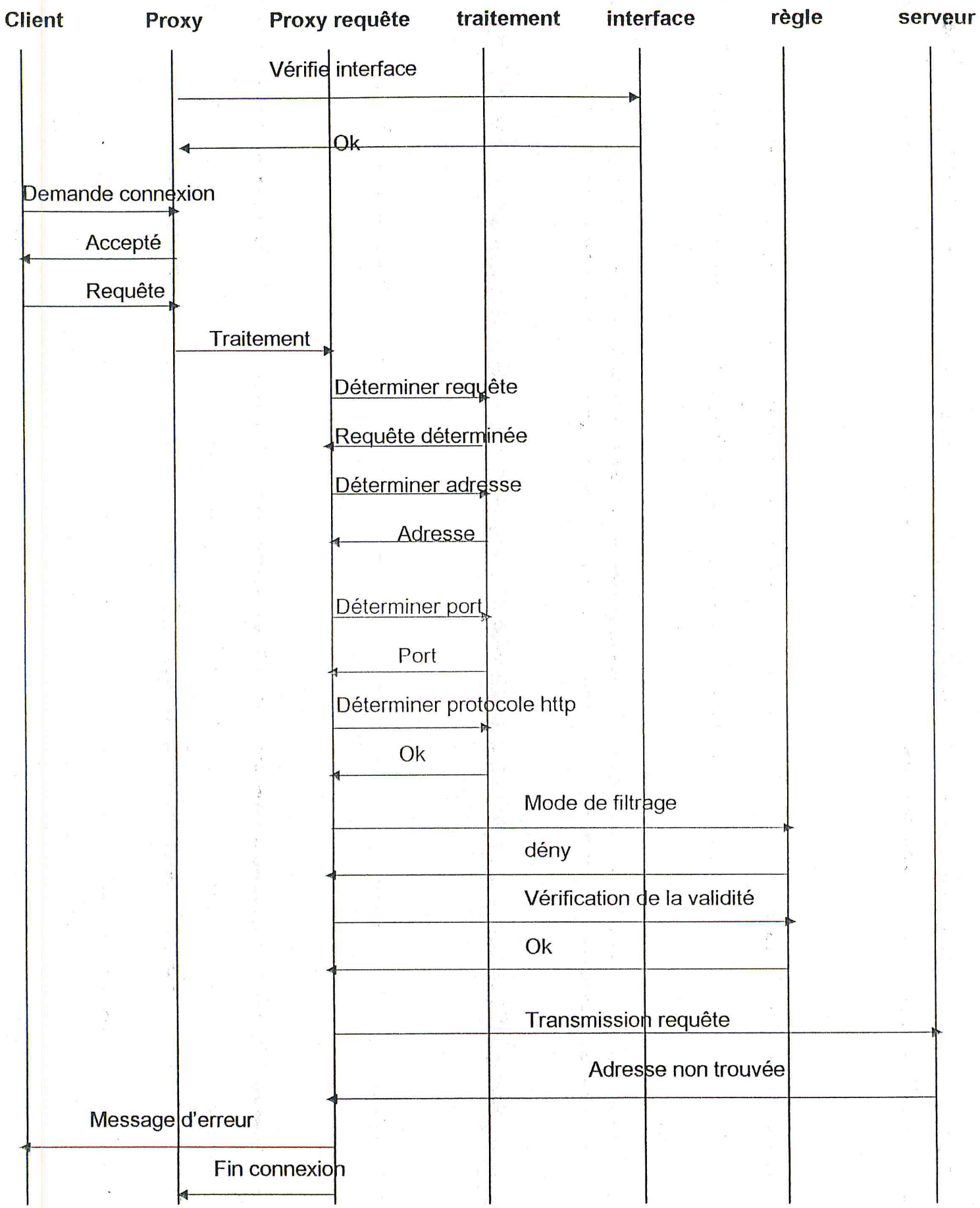


FIG 5.7 Suivi d'événement pour un scénario du Proxy avec un cas d'échec

VII.2. Diagrammes d'état

Le diagramme d'état sera construit pour chaque objet dont le comportement dynamique a de forte interaction, en indiquant les événements que l'objet reçoit et ce qu'il émet. Chaque scénario ou suivi d'événement correspond à un chemin dans le diagramme d'état.

Dans notre cas, il nécessaire de construire un diagramme d'état pour la classes Proxy qui reçoit des demande de connexion, ainsi que interface qui est nécessaire pour une connexion, Proxy requête qui traite les demandes et la classe règles qui nécessaire pour le traitement

Les autres classes ne nécessitent pas de diagramme d'état tel que client et serveur Web, ces deux derniers sont des objets externe au serveur Proxy et ne nécessite pas l'implémentation.

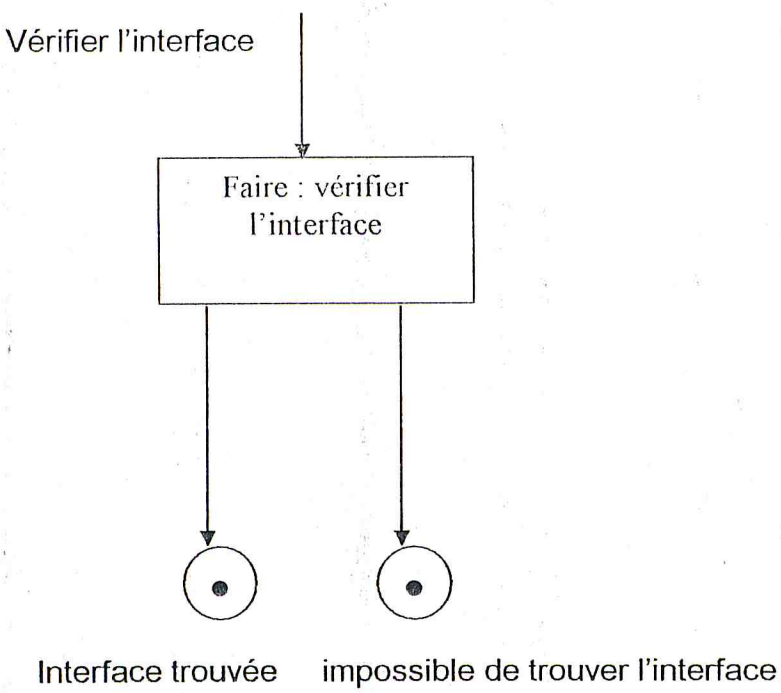


FIG 5.8 Diagramme d'état de la classe interface

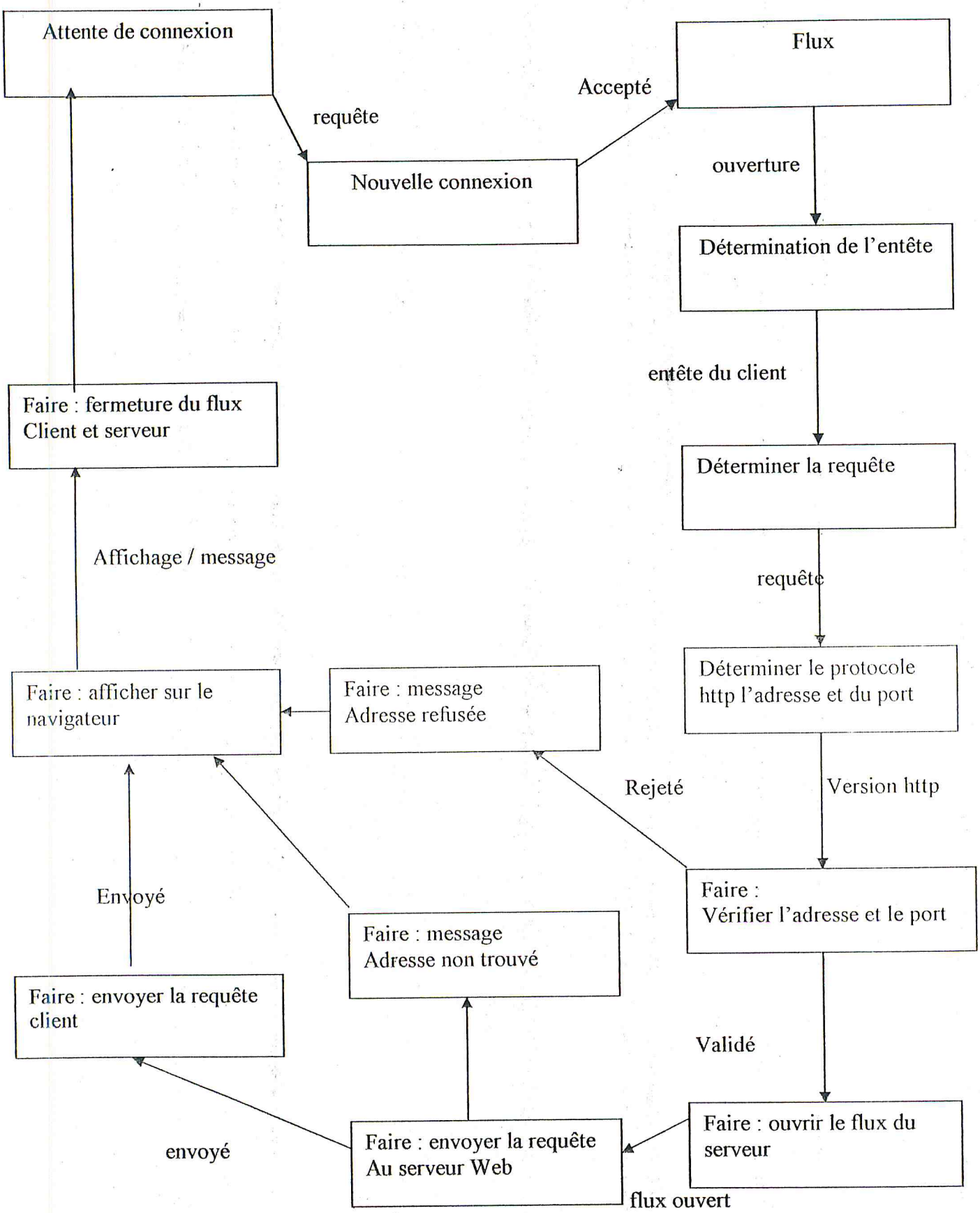


FIG 5.9 diagramme d'état de la classe Proxy requête

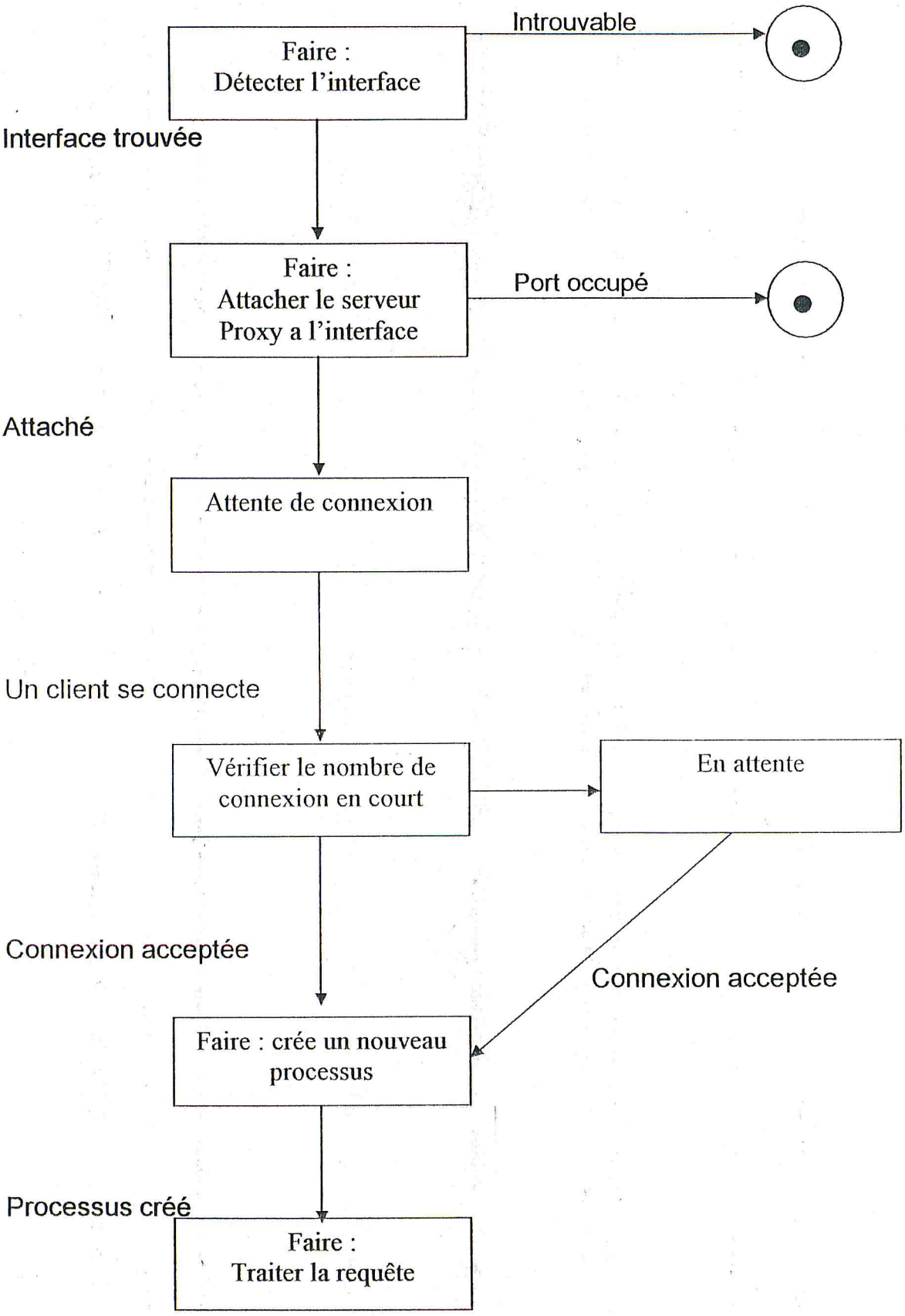


FIG 5.10 Diagramme d'état pour la classe Proxy

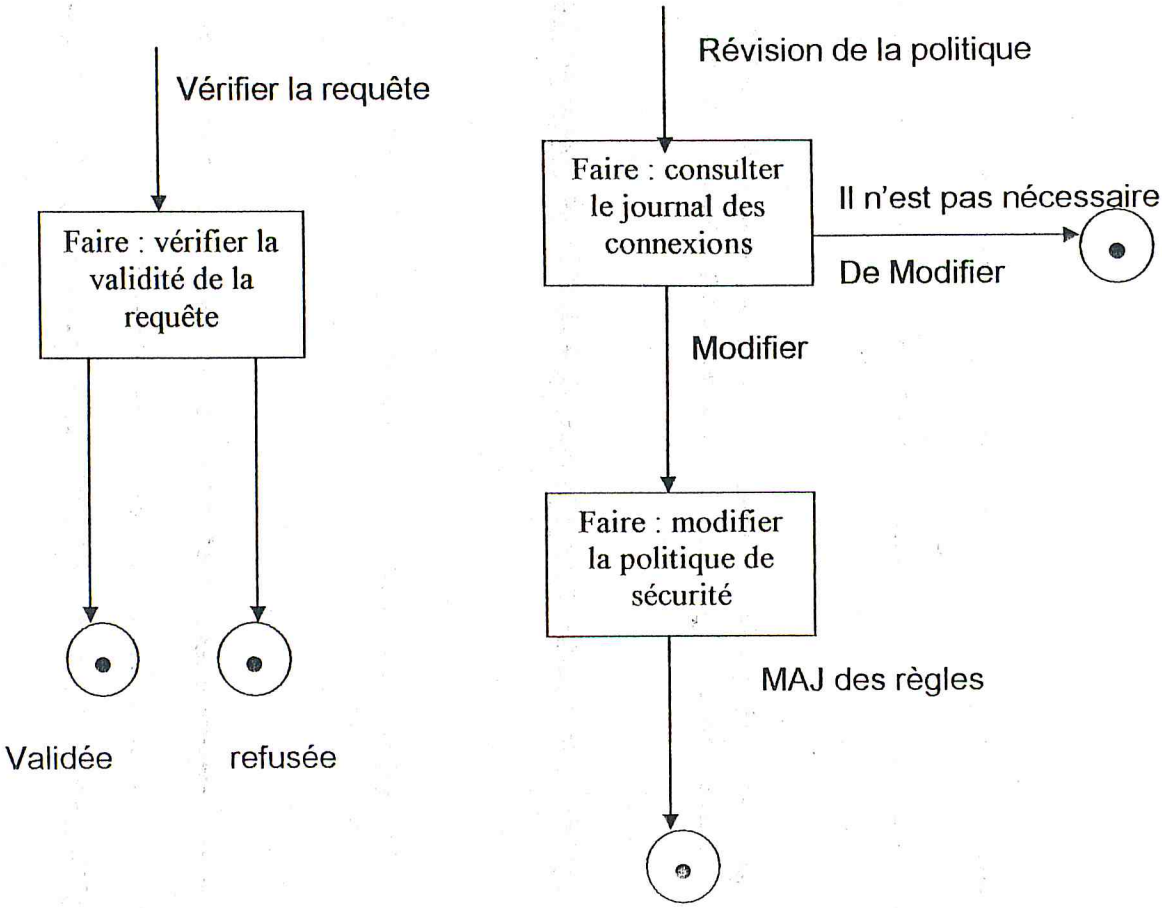


FIG 5.11 Diagramme d'état pour la classe règles

VII.3. Le modèle fonctionnel

Le modèle fonctionnel s'intéresse au traitement des données sans tenir compte du séquencement.

Le diagramme a flot de données est un moyen de montrer les dépendances fonctionnelles, les traitements sur un diagramme à flot de données correspondent aux activités ou aux actions sur un diagramme d'état de classes, les flots, dans un diagramme à flot de données correspond au objets ou au valeur d'attribut.

La première étape dans la construction du diagramme à flot de données est de dresser une liste des valeurs d'entrées et de sortie pour construire un diagramme de premier niveau. Un diagramme à flot de données est généralement constitué de couches.

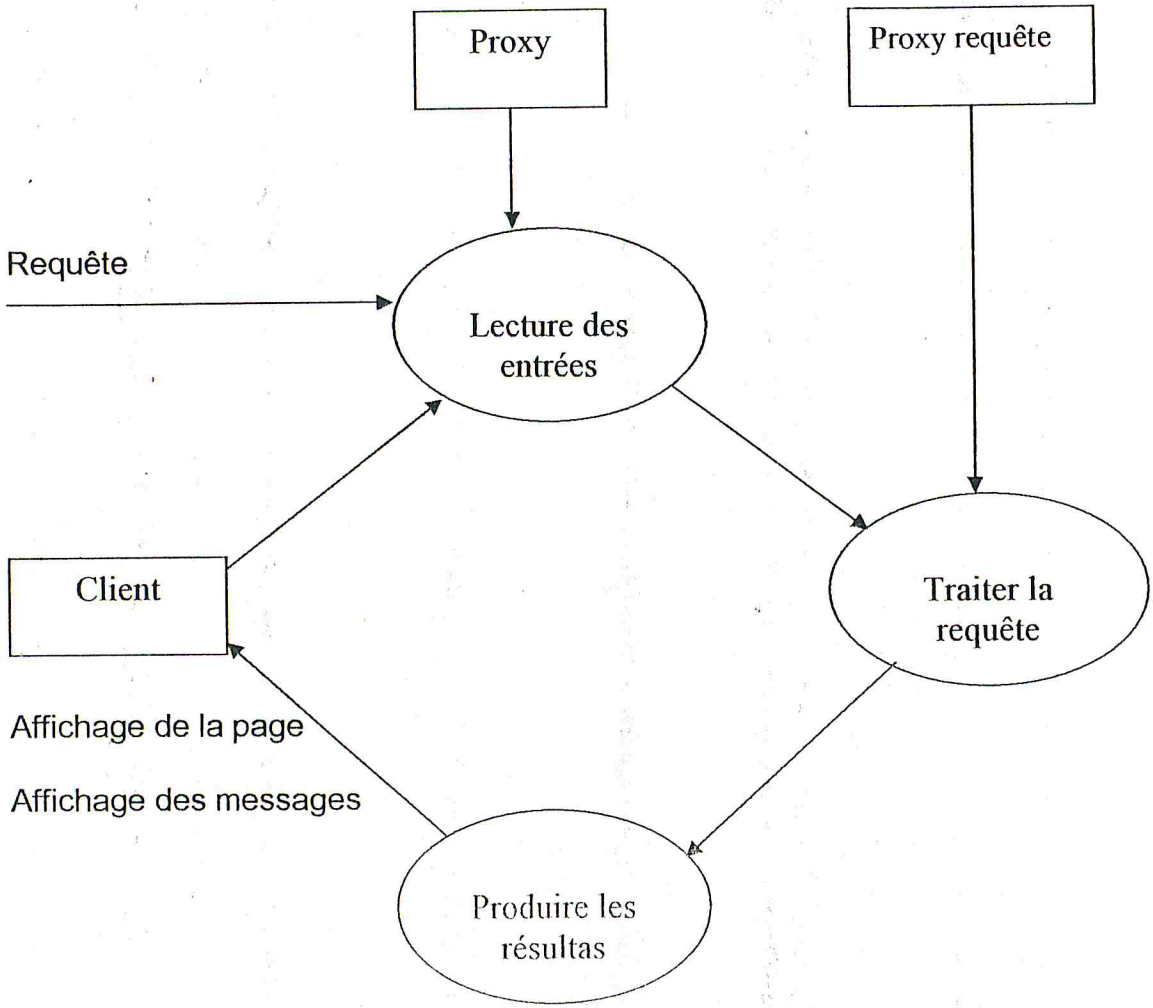


FIG 5.12 DFD du Proxy

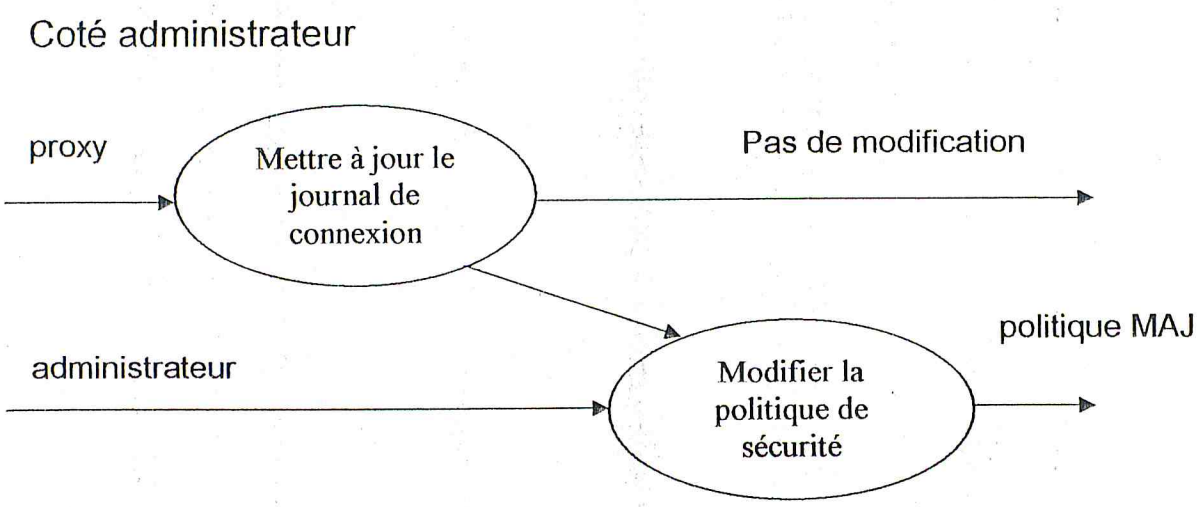


FIG 5.13 DFD la configuration de la politique de sécurité

Nous développerons dans Le diagramme à flot de données suivant une fonction qui existe dans le diagramme général : le traitement d'une requête

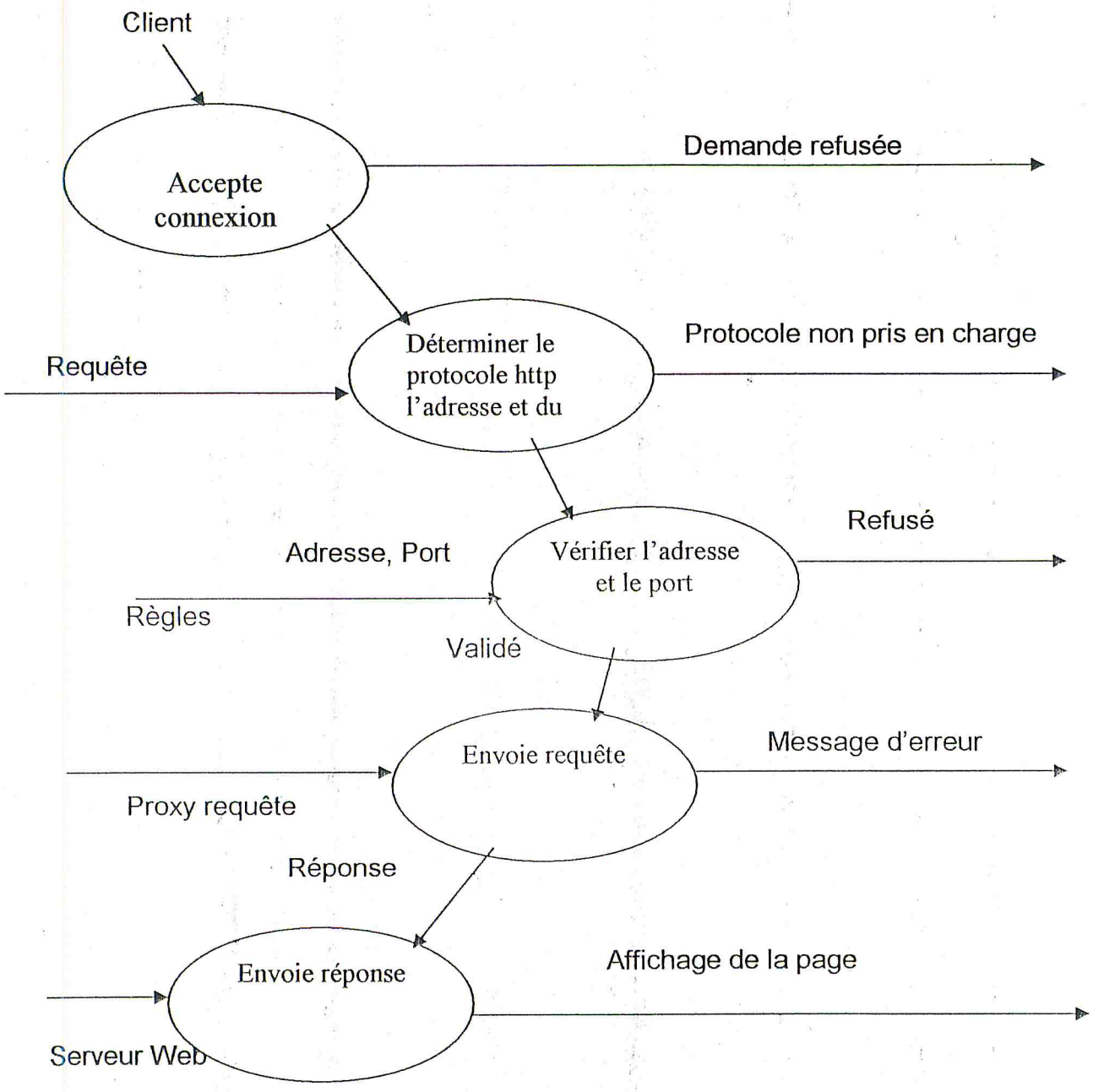


FIG 5.14 D.F.D du traitement d'une requête

VIII. Environnement de développement

VIII.1. Environnement matériel

La réalisation de notre logiciel nécessite un serveur Web ainsi qu'un serveur DNS ou bien d'avoir une connexion à Internet, ainsi pour l'exploitation de notre logiciel, notre application peut s'exécuter dans un environnement réseau ou bien en monoposte.

VIII.2 Environnement logiciel

Notre logiciel Proxy http peut être supporté par tous les systèmes d'exploitation Windows existant :

- Windows 98
- Windows NT
- Windows XP
- Windows 2000 professionnel ainsi que les différentes version récentes de Windows.

Linux

VIII.3. Environnement de programmation

Tout développement de logiciel passe par une étape délicate : le choix du langage adéquat. Effectivement, afin de développer le Proxy http qui est un serveur et doit répondre a des demandes de différents clients, donc on doit mettre en œuvre une communication client serveur fiable avec un traitement simultané des requêtes des clients. Il nous fallait aussi choisir un multi plateforme qui sera compatible avec chaque plate forme des clients. Il nous fallait choisir un langage qui répond à ces besoins.

L'implémentation en Java était notre choix puisque le langage fournit tous les objets nécessaires à ce genre de développement. Les vastes possibilités de java font le langage le plus passionnant qui soit apparu depuis une dizaine d'année. Ainsi :

- Il permet de créer une communication fiable en mode TCP entre deux applications client serveur
- Il offre la possibilité de travailler en parallèle avec la création des threads
- Il nous permet aussi d'effectuer les différents types d'entrée et de sortie entre deux objets
- Il permet de créer des programmes avec une interface graphique.
- Création d'une application multi plateforme

IX. Principe de fonctionnement

Le principe de fonctionnement est le suivant :

- chargement des règles,
- attachement à un port précis (8080 par défaut), attente de connexion clientes,
- Pour chaque connexion, création d'un thread distinct s'occupant de la requête du client.

La gestion de chaque requête implique :

- l'analyse de l'adresse IP source, de l'adresse de destination et du port et de la version du protocole HTTP,
- la vérification de la validité de l'adresse et du port en fonction des règles définissant l'abandon ou la poursuite de la requête,
- si la requête est validée, la transmission de la requête au serveur Web, sinon, la fermeture de la connexion,
- la réception de la réponse du serveur Web et sa retransmission au client,
- Et enfin, la fermeture de la connexion.

X. Les bibliothèques de java utilisées

Pour la programmation de notre application, on à utilisé les bibliothèques décrites dans le tableau suivant :

package	classe	objectif
Java.io	InputStream OutputStream	Création du flux d'entrée pour le client et pour le serveur Web Création du flux de sortie pour le client et pour le serveur Web
Java.net	ServerSocket Socket InetAddress	Création du serveur Proxy pour le traitement des requêtes des clients Création du client demandant une connexion au serveur Rechercher l'adresse réseau
Java.lang	Thread	Création d'un processus de traitement de la requête client lorsque elle est accepté par le serveur

Tableau 5.1 bibliothèques utilisées

XI. Implémentation en java du Proxy http

Une première classe nommé PROXY contient la méthode public static void main ().

La seconde est la classe TRAITEMENT, celle qui traite la requête du client.

XI.1. Lancement de l'application

La classe PROXY lance l'application en invoquant :

- La méthode public void init () qui fixe les paramètres en fonction des arguments de la ligne de commande ou les fixe à des paramètres par défaut.
- Ensuite, on appelle public void run () qui contient la boucle principale. Celle-ci, pour chaque connexion, crée un nouvel objet, qu'elle encapsule dans un thread et qu'elle lance.

XI.1.1. La méthode public void init ()

Il s'agit dans un premier lieu d'identifier l'interface réseau existante, Le résultat est un objet qu'on peut utiliser pour construire un SOCKET,

a) Identifier une machine

L'adresse IP est représentée en interne comme un nombre sur 32 bits (et donc chaque nombre du quadruplet ne peut excéder 255), et il existe un objet spécial Java pour représenter ce nombre dans l'une des formes décrites ci-dessus en utilisant la méthode de la bibliothèque java.net.
Le résultat est un objet du type InetAddress qu'on peut utiliser pour construire un SOCKET,

```
... ... ...
Public static InetAddress getInterface (int type) {
        InetAddress     ia_adr [];
    Try {
    Ia_adr = InetAddress.getAllByName (InetAddress.getLocalHost (). get
Hostname ());
... ... ...
```

b) Création des SOCKETS

La finalité d'un réseau est de permettre à deux machines de se connecter et ainsi de se « Parler » Une fois que les deux machines se sont trouvées l'une l'autre, elles peuvent entamer une agréable conversation bidirectionnelle.

La machine qui attend est appelée serveur, celle qui cherche client. Cette distinction n'est importante que tant que le client cherche à se connecter au serveur. Une fois les machines connectées, la communication se traduit par un processus bidirectionnel et on n'a plus à se préoccuper de savoir qui est le serveur et qui est le client.
Le rôle du serveur est donc d'être en attente d'une demande de connexion, ceci est réalisé par l'objet serveur qu'on crée dans ce but. Le rôle du client est de tenter d'établir une connexion avec un serveur, ceci est réalisé avec un objet client qu'on crée pour cela.
Les sockets offrent des Communications fiables en mode connecté utilisant le protocole TCP.

La classe Socket définit un canal de transmission entre machines. Après avoir créé deux objets de type Socket, un sur chacun des sites communicants

Une fois la connexion établie, aussi bien du côté serveur que du côté client, elle se transforme en un objet flux d'entrée et sortie, et dès lors on peut traiter cette connexion comme une lecture ou une écriture dans un fichier. Ainsi, une fois la connexion établie, il ne reste qu'à utiliser les commandes d'entrée et sortie.
Les communications se font au moyen de canaux d'entrées/sorties de type InputStream et OutputStream.
Apres la détection de l'interface, on crée notre serveur a l'aide de la classe ServerSocket qui sera attaché sur le port déjà déclaré auparavant. Son rôle est de traiter des requêtes reçues et accepter de la part du client.

```
try {
                    // On attache le serverSocket à l'interface interne
                    svrSocket     = new ServerSocket( portNumber, 0,
ia_internalInterface );
```

XI.1.2 La méthode public void run ()

Cette méthode permet à notre serveur d'accepter des connexions que les clients demandent. Le client est créé en utilisant la classe Socket.

```
.....
                    Try {

                        clSocket = svrSocket.accept();
.....
```

XI.2 Traitement de la requête par Proxy requête

Dès qu'une connexion est acceptée, on crée un nouvel objet ProxyRequete qui traite la requête. Ce fonctionnement permet la gestion de clients multiples.
Le constructeur récupère le socket de connexion et l'approprie à une variable privée.
Il appelle ensuite la méthode public void run(). Cette méthode ouvre les différents

Stream qui permettront de communiquer avec le client. Elle affecte notammement un BufferedReader à partir du Stream entrant. Ceci permettra de découper la requête ligne par ligne. Enfin, la méthode traite la requête du client. La méthode public void run() est le corps de l'application. Une fois que la connexion est terminée, la méthode public void stop () s'occupe de la fermeture du flux d'entrée et de sortie.

XI.2.1 Utilisation des threads

Dans notre application, nous ne nous sommes pas contentés de traiter un client à la fois, ceci diminuera dans le rendement de notre serveur, la solution était donc de traiter en même temps plusieurs demandes de connexions.

Dans ce cadre, java propose la solution des Threads et permet de créer des processus qui peuvent s'exécuter simultanément, donc chaque client sera traité dans un processus.

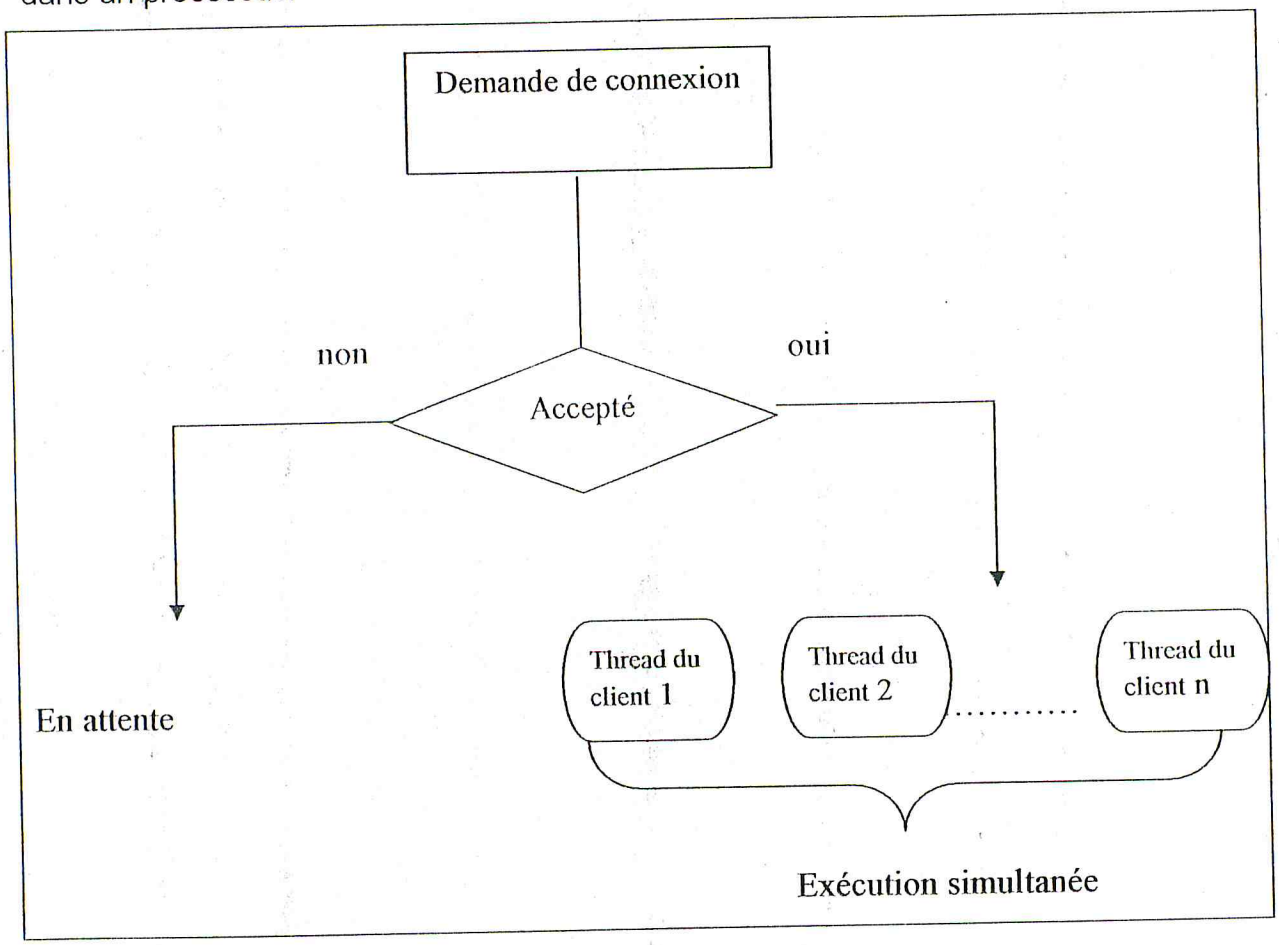
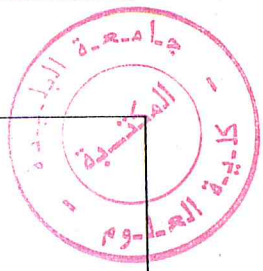


FIG 5.15 Création des thread

Quand la demande de connexion est acceptée par le serveur, on crée un nouveau thread qui va se charger du traitement de la requête.



```
.....
// On crée l'objet ProxyRequete qui traitera la demande

                poolRequete[i]      = new ProxyRequete(clSocket);
                    poolThread[i]       = new Thread(poolRequete[i]);
                poolThread[i].start();

.....
```

XI.2.2. Les flux de communication

Pour effectuer une entrée ou une sortie de données en Java, le principe est simple et se résume aux opérations suivantes :

- Ouverture d'un moyen de communication.
- Écriture ou lecture des données.
- Fermeture du moyen de communication.

En Java, les moyens de communication sont représentés par des objets particuliers appelés (en anglais) stream. Ce mot, qui signifie courant, ou flot, a une importance particulière.

Au moment où le serveur accepte la connexion du client, on a réellement établi une connexion Socket à Socket et on peut traiter les deux extrémités de la même manière, car elles sont alors identiques. On utilise alors les méthodes getInputStream( ) et getOutputStream( ) pour réaliser les objets InputStream et OutputStream correspondants à partir de chaque Socket.
Les entrées et les sorties du client sont réalisées par le biais des classes du package java.io :

- **InputStream**, pour les entrées de données
- **OutputStream**, pour les sorties

```
.....
.....
try {
//On crée et on ouvre le flux d'entrée et de sortie de la part du client
 ClInputStream          = clSocket.getInputStream ();
 ClOutputStream    = clSocket.getOutputStream ();
```

XI.2.3. Récupérations des informations sur la connexion (coté client)

Pour traiter une requête du client, on doit récupérer

a) la requête qui nous informe sur les détails suivants :

- **Requête**
- **url demandé**
- **HTTP version**

b) l'adresse IP du client

Ceci nous permet donc de récupérer l'adresse IP du client la version du protocole http utilisé, l'adresse recherchée par le client ainsi que le port a l'aide des méthodes décrites dans le tableau suivant :

méthode	rôle
private void détermine Protocole ()	Déterminer la version du protocole http utilisé
private void détermine Addresse ()	Déterminer l'adresse que le client tente a accédé
private void determine Port()	Déterminer le port utilisé

Tableau 5.2 méthodes utilisées pour le traitement d'une requête

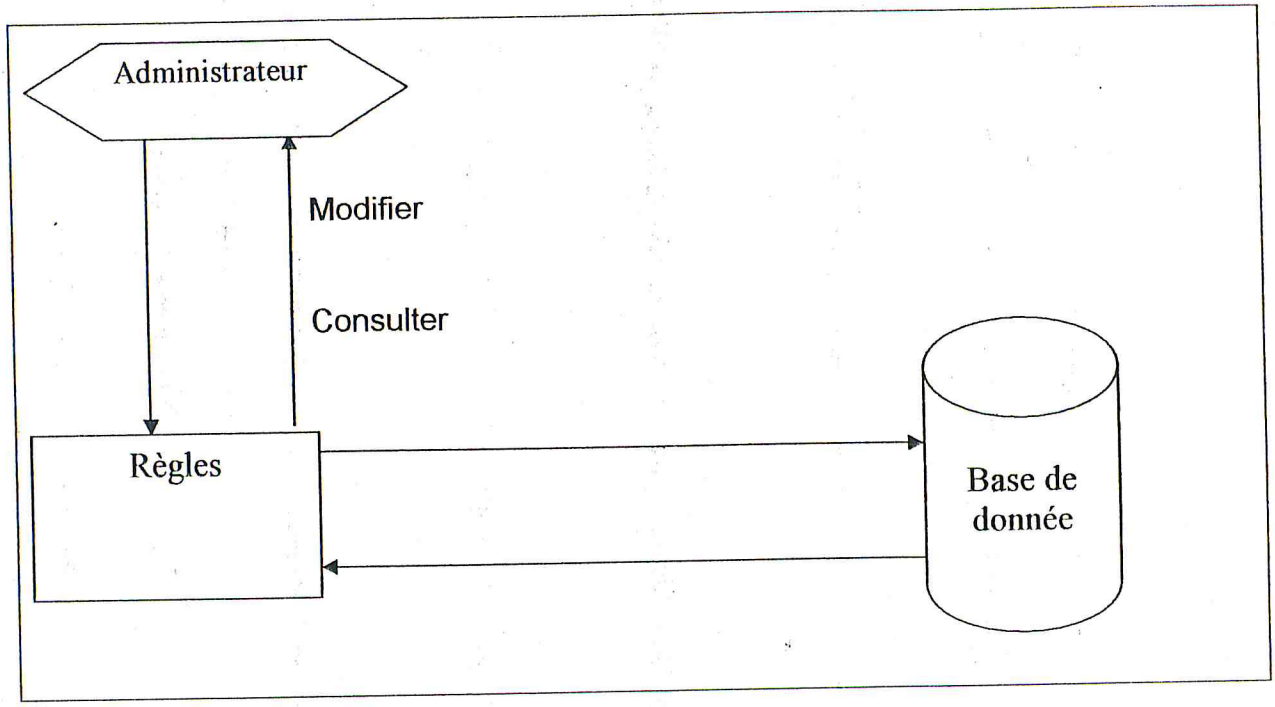


FIG 5.16 relations entre l'administrateur et les règles

Les deux fichiers « allow » et « deny » représente donc la politique de sécurité, leur configuration bien sur, consiste à étudier ce qui devrait ou pas être permis.
Les règles de filtrage sont tirées à partir des deux fichiers et chargées dans un tableau contenant l'adresse source, l'adresse de destination et le port lors de l'exécution de notre Proxy qui va nous faciliter la tache de filtrage.

XI.2.5. Envoi de la requête au serveur Web :

Comme on l'a vu déjà avec le client, on crée un flux de communication au profit du serveur Web pour permettre de récupérer la réponse.

La transmission de la requête n'est effectuer que si cette dernière est validée lors du filtrage, des que la requête est validée, on crée le SOCKET de serveur et on ouvre les flux d'entrée et de sortie du serveur pour recevoir les informations envoyées par le SOCKET client.

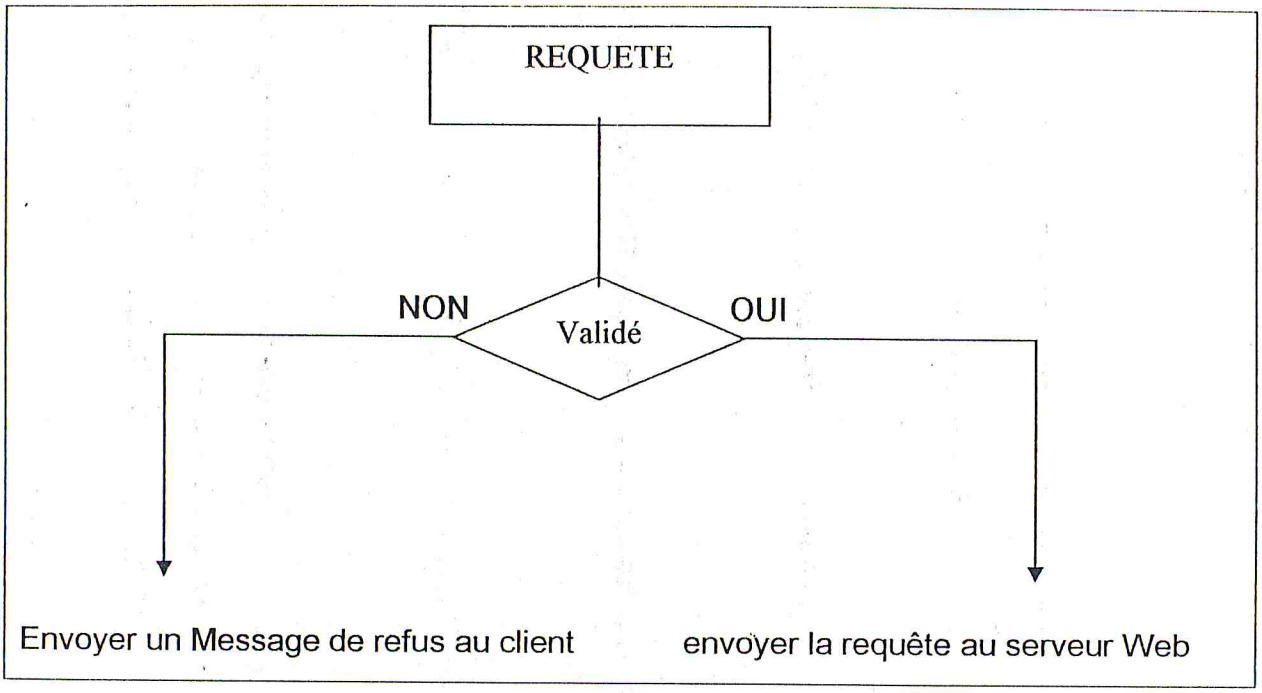


FIG 5.17 envoie de la requête au serveur web

Dans le cas ou la requête du client est refusée, elle ne sera pas transmise au serveur Web, et on lui envoi le message de refus a travers son flux d'entrée à partir de notre Proxy indiquant le refus de la requête.

XI.2.6. Réception de la réponse

En utilisant toujours les flux d'entrée et sortie la réponse est renvoyée au client.
Une réponse peut être en deux cas :

a) réponse positive

C'est le cas ou la requête est acceptée lors du filtrage, la réponse sera la page Web celle qu'a demandé le client.

b) réponses négatives

C'est le cas ou la requête est refusée lors du filtrage, la réponse sera donc un message de refus provenant du serveur Proxy.

XI.2.7. Fin de la connexion

Comme toute connexion en mode TCP, notre connexion doit être fermée après l'obtention de la réponse. La fermeture est réaliser des que la réponse est transmis au client a partir de la méthode public void stop (). Cette dernière sert à

XI.2.4. Le filtrage des adresses

Une fois que les informations sur le client sont déterminées, celles ci seront comparées aux règles définit par l'administrateur dans les deux fichiers « allow » et «deny » qui sont accessible par la classe règle afin de décider si la requête sera acceptée ou rejetée.

Pour cela nous avons laissé le choix à l'administrateur de prendre une méthode de filtrage parmi les deux proposés, ces méthodes sont inspirées du principe général du fonctionnement des FIREWALL.

Mode	principe
allow	Tout ce qui n'est pas explicitement interdit est autorise
deny	Tout ce qui n'est pas explicitement autorise est interdit

Tableau 5.3 Mode de filtrage

A/ la méthode allow

Le principe de La méthode « permit » est d'autorisé les adresses qui ne sont pas interdites, donc si l'administrateur opte pour cette méthode, les comparaisons des adresses se feront par rapport à la liste décrite dans le fichier des adresses interdites, cela veut dire que si la requête du client se trouve dans « deny » elle sera rejetée si non elle est valide.

B/ la méthode deny

Le principe de La méthode «deny » est le contraire de la première, il s'agit d'interdire les adresses qui ne sont pas autorisées, donc si l'administrateur choisi cette méthode, les comparaisons des adresses se feront par rapport a la liste décrite dans le fichier des adresses autorisé, cela veut dire que si la requête du client se trouve dans «allow » elle sera validée si non elle sera rejetée.

- ✓ fermer les flux d'entrée et de sortie
- ✓ fermer le socket client et du serveur Web

XII. Interface graphique

En premier lieu, en doit signaler que notre application est destinée pour deux genres d'utilisateur :

- ➢ Utilisateur normal : il s'agit des postes clients
- ➢ Administrateur

L'interface que nous avons conçue, n'est destinée qu'a l'administrateur chargé de la configuration de la politique de sécurité.

L'utilisateur normal aura l'affichage de la réponse sur son navigateur :

- ➢ Page Web demandé
- ➢ Messages

XII.1. Lancement du serveur Proxy

A partir de l'onglet général, le serveur Proxy peut être lancé pour traiter les requêtes de ces clients. Ce lancement va bien sur prendre en charge la dernière configuration mise en en place par l'administrateur.

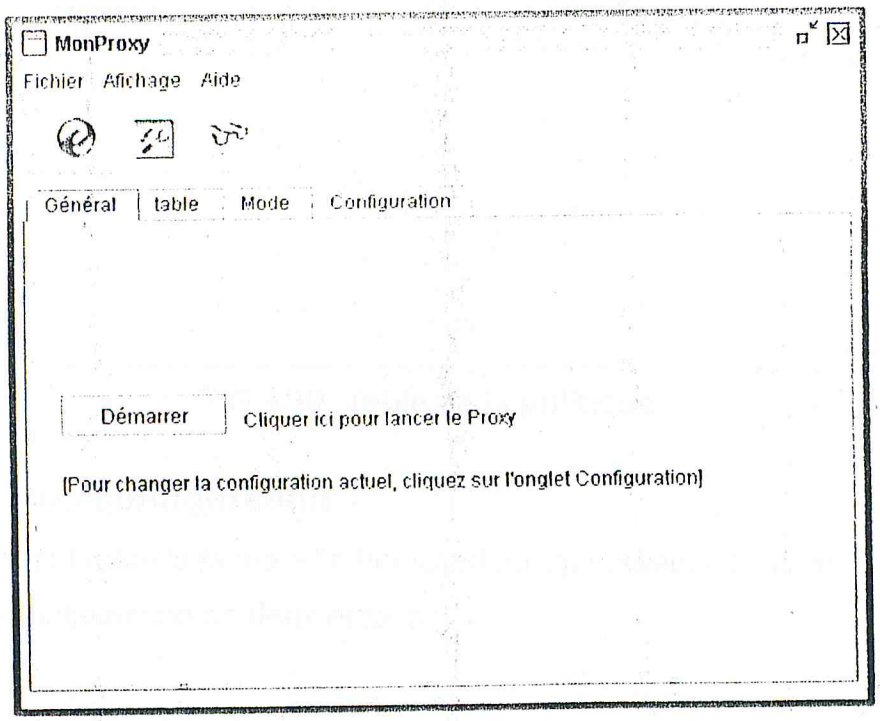


FIG 5.18 Lancement du serveur Proxy

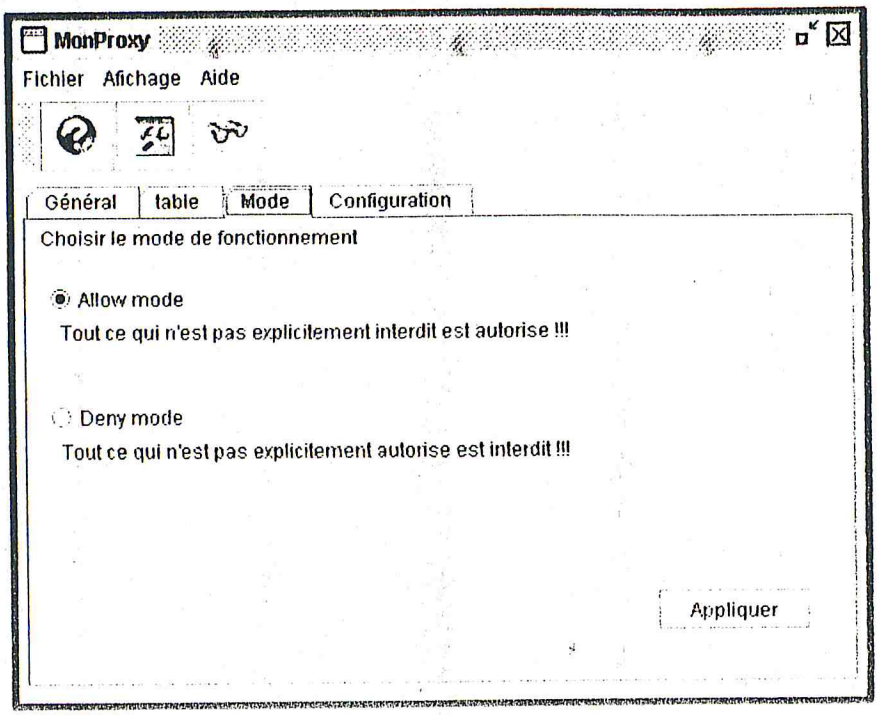


FIG 5.20 modes de filtrage

XII.3.2 Configuration des adresses

Dans cette étape, l'administrateur affecte a chaque poste client une politique selon les besoins de ce dernier, il a la possibilité de modifier les règles de filtrage

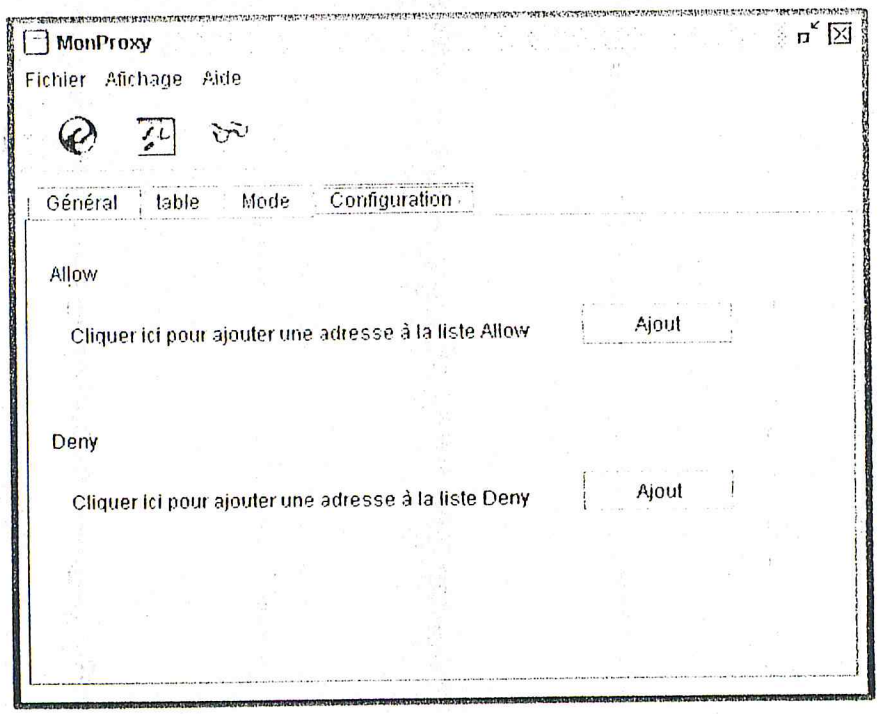


FIG 5.21 Configuration de la politique

XII.2 La politique de sécurité

L'onglet table indique la configuration actuelle du serveur Proxy, les facteurs principaux de la politique de sécurité sont :

- L'adresse IP source
- Port local
- L'adresse de destination
- Emplacement de la règle (mode d'application)

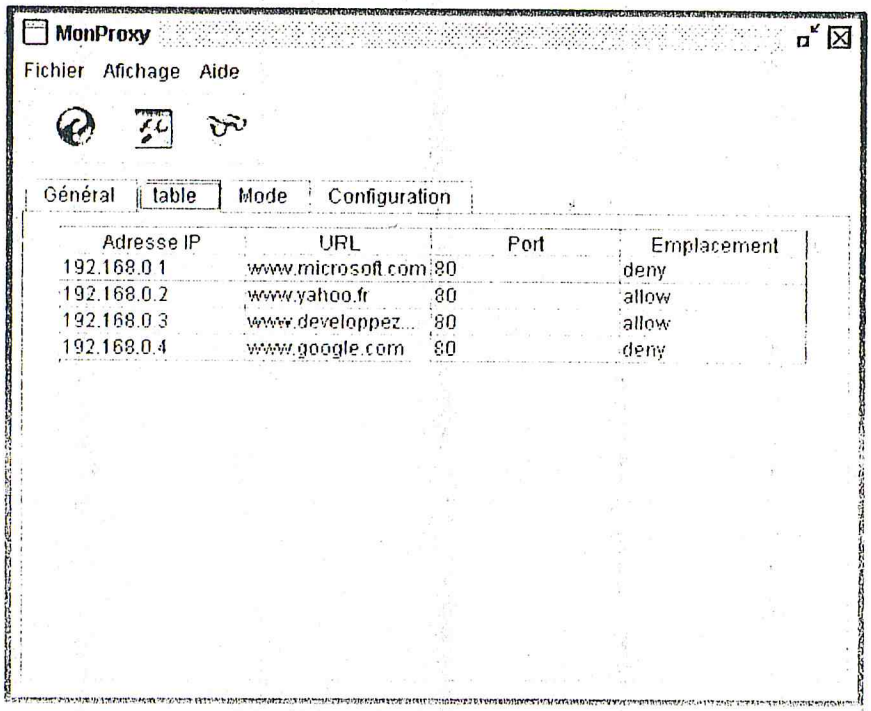


FIG 5.19 Table de la politique

XII.3 Étapes de configuration

Notre application facilite la tache à l'administrateur du réseau, elle lui offre une possibilité de configuration en deux étapes :

XII.3.1 Mode de filtrage

L'administrateur a le choix entre deux modes pour le fonctionnement du filtrage

- Allow Tout ce qui n'est pas explicitement interdit est autorise
- Deny Tout ce qui n'est pas explicitement autorise est interdit

Une modification dans la politique de sécurité implique l'ajout ou la suppression des règles dans les deux modes de filtrage

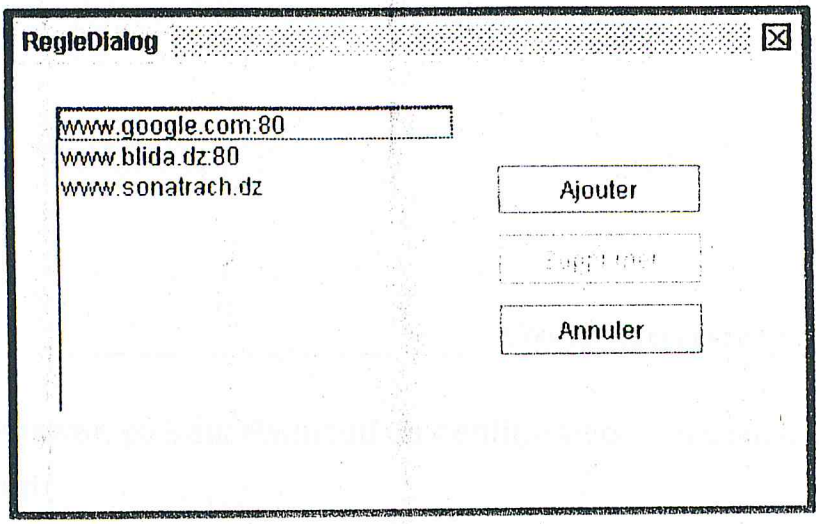


FIG 5.22 Ajout ou suppression des règles

Pour que l'administrateur reste toujours informé sur les connexions des postes clients et pour qu'il soit aidé dans le choix de la configuration, il peut consulter le journal des connexions qui est en mise à jour régulière par le serveur Proxy.

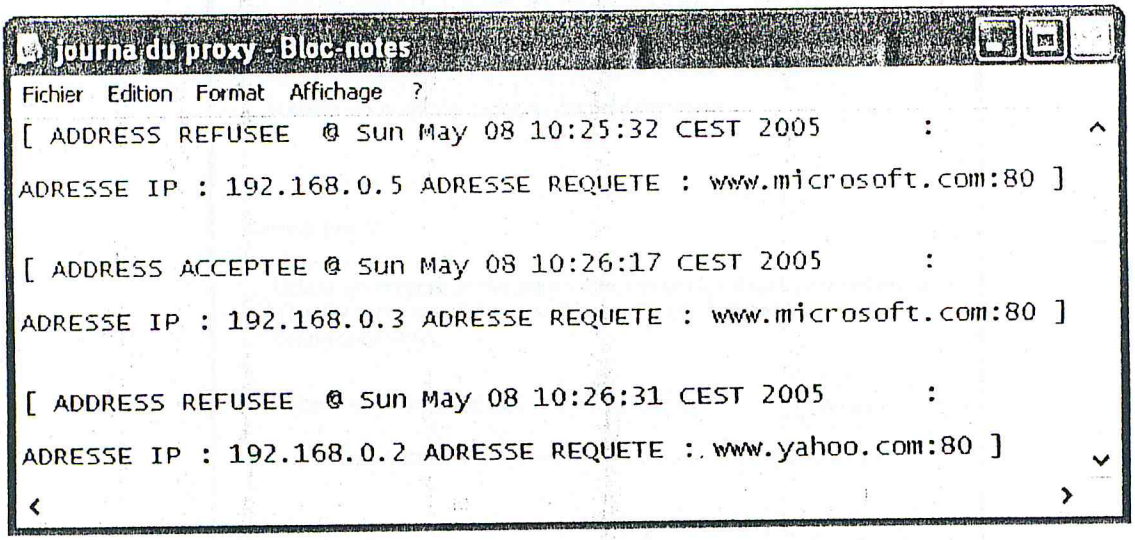


FIG 5.23 Journal des connexions

XII.4. Test de l'application

Avant le lancement du serveur Proxy, tous les postes concernés (client, administrateur) doivent suivre une configuration.

Cette configuration est la même pour tous les postes, il s'agit d'accéder au paramètre du réseau local

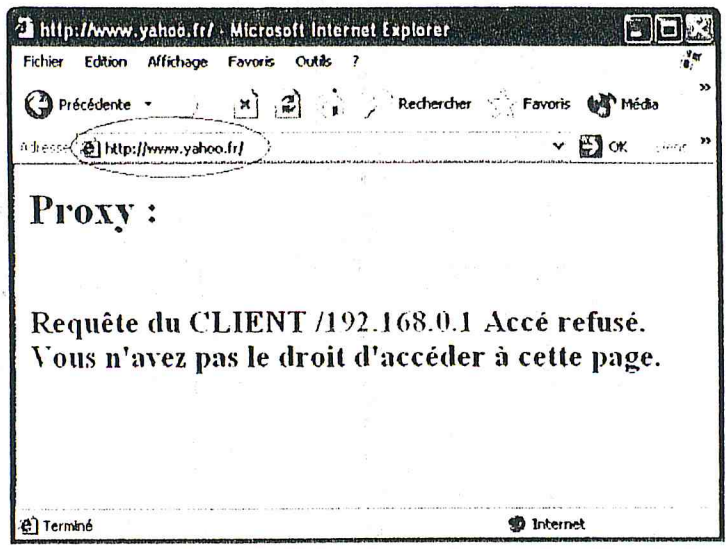


FIG 5.25 Requête refusée

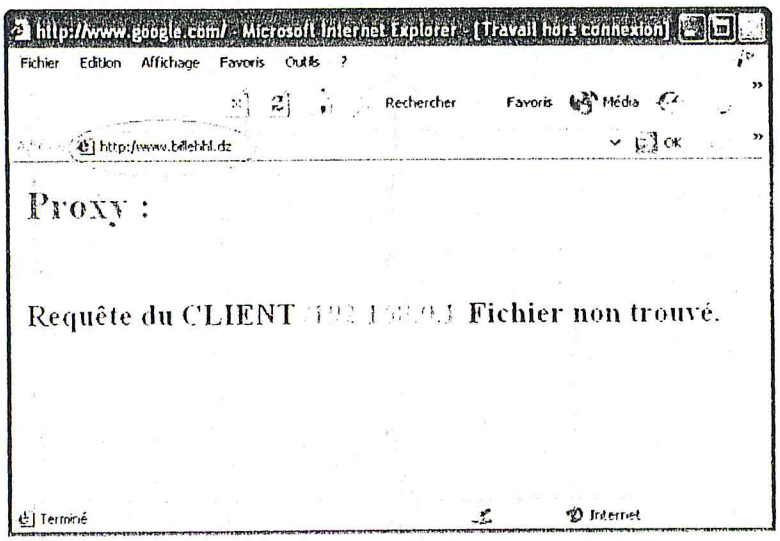


FIG 5.26 Adresse non valide

XIII. conclusion

Nous avons présenté dans ce chapitre la conception et la mise en œuvre de notre solution qui est le serveur proxy.

Pour notre conception et modélisation nous avons choisi une méthode orientée objet

Notre application vise deux genres d'utilisateur : le client qui se connecte à Internet et l'administrateur qui a le privilège d'exiger une politique sur les clients.

Cliquez sur **Démarrer**, puis sur **Panneau de configuration**, puis double-cliquez sur **Options Internet**

Dans Options Internet cliquer sue l'onglet **connexion**, puis sur **paramètres du réseau local**

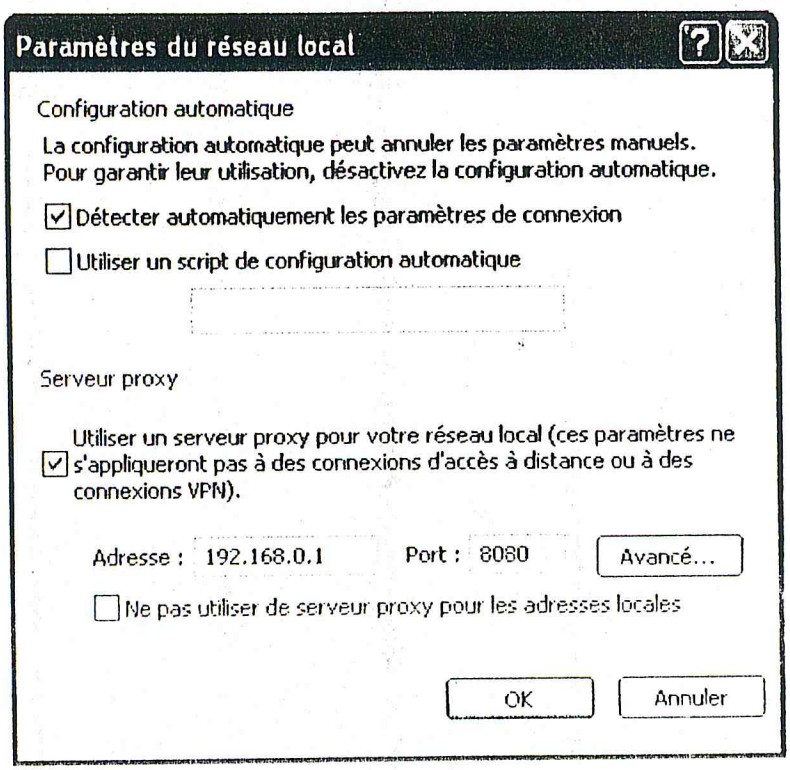


FIG 5.24 paramètres du réseau local

- Cocher la case du serveur Proxy
- Mettre dans le champ « adresse » l'adresse IP du serveur
- Mettre dans le champ « port » le port ou l'application est en train de s'exécuter

Dès maintenant chaque client peut transmettre sa requête avec l'intermédiaire d'un navigateur Web (Internet explorer, Netscape,...) qui va être pris en charge par notre serveur Proxy.

Conclusion générale

Dans ce mémoire, nous avons mis en œuvre la démarche proposée dans le premier chapitre qui consiste à mettre en œuvre une politique de sécurité au sein d'une entreprise, nous avons appliqué la démarche suivante :

- Etude de l'existant
- Les risque et les menace prévu
- Proposition des solutions de sécurité
- Mettre en œuvre une solution qui permet d'enrichir la politique de sécurité

Notre stage nous a permet de développer nos connaissances sur l'ensembles des ressource que la SONATRACH possède :

- Matériel: SWITCH, ROUTEUR et FIREWALL...
- Logiciel : antivirus, SGBD oracle ...

Notre solution offre a l'administrateur la possibilité d'avoir des statistiques sur les connexions des différents poste client a l'Internet, a partir de la il peut choisir sa propre politique de sécurité en ajoutant des règles ou bien en supprimant d'autres, et ce ci peut ce faire non seulement dans un cadre d'une politique globale mais dans une politique qui réagie avec le comportement de chaque utilisateurs du réseau.

L'avantage de notre solution est qu'elle est standard, c'est à dire qu'elle peut détecter les connexions de n'importe quel client dans un réseau TCP/IP et d'avoir des statistiques sur n'importe machine du réseau, d'autre part, L'interface que nous avons proposée permet à l'administrateur d'introduire les règles de la politique de l'entreprise.

Enfin, nous pouvons affirmer que l'expérience vécue dans le cadre de notre mémoire a été fructueuse. Elle constitue une solide base de départ qui nous permet d'aborder des travaux plus complexes dans un domaine aussi vaste que la sécurité informatique.

Annexe

EXISTANTS SECURITE

Cadre de l'étude

La prise de connaissance détaillée de l'environnement est indispensable, en revanche il n'est pas prévu de rédiger un document répertoriant toutes les informations collectées (sauf demande spécifique). Cependant une documentation de synthèse vous sera remise avec les principaux points relatifs aux règles de sécurité

Questions préliminaires

Quels sont les éléments qui entrent en considération d'un point de vue de la sécurité (au yeux du client) ?

Les ressources à protéger par ordre d'importance.

IDENTIFICATION DES INTERLOCUTEURS SECURITE

Avez-vous une équipe chargée de la sécurité ?

De combien de personnes cette équipe est-elle constituée ?

Quelles sont les tâche affectées à cette équipe ?

Comment sont réparties les responsabilités ?

De quels types d'habilitation et de droit disposent les différents interlocuteurs ?

EXISTANTS SECURITE

Accès au locaux

Comment le matériel informatique est-il déployé ? Salles spéciales ?

Y a t-il un contrôle d'accès ?

Y a t-il des restrictions aux accès des personnes ? Comment ?

Prestataires externes ?

Alimentation électrique

Vos systèmes sont-ils bien alimentés en courant électrique ? Puissance suffisante ?

Vos systèmes sont-ils secourus en courant électrique ? Puissance et autonomie Suffisante ?

Périodicité d'entretien des systèmes de secours ?

Dispositifs incendie
Quels sont les dispositifs existants ?
Sont-ils suffisants ?
Périodicité d'entretien des systèmes ?

Responsabilisation du personnel
Quels sont les formations sécurité mises en place actuellement ?
Comment gérez-vous les déchets papiers ? Broyeur, double poubelle ?
Qui est habilité à donner des réponses au téléphone ?

EXISTANT RESEAU PHYSIQUE
Câblage
Y a-t-il des têtes de réseaux partagées avec d'autres sociétés ?
Y a-t-il des prises dans les salles de réunions ?
Qui assure son exploitation ? Sa maintenance ?

Équipements LAN
Avez-vous un schéma de principe de votre réseau ?
Redondance des équipements de concentration ?
Gestion de VLAN ? Avec quelles règles de sécurité ?
Qui assure son exploitation ? Sa maintenance ?

EXISTANT MACHINES

station de travail
Utilisation du lecteur de disquette ?
Gestion des mots de passe locaux ?
Chiffrement des données locales ?
Sauvegarde des configurations ?
Accès WorkGroup ou Domain pour les environnements NT

Serveurs Micro
OS utilisés (et services packs appliqués) ?
Gestion des mots de passe
Sauvegarde des configurations
Technologie de sauvegarde des données
Utilisez-vous un schéma RAID ? Si oui, lequel ?

Est-il systématique ?
Comment est-il défini ?

SYSTEMES UTILISES

Vos systèmes sont-ils à jours en fonction des applications ? Service packs appliqués ?
Utilisez-vous des services inutiles sur vos machines ?
Un inventaire des logiciels installés par machine est-il disponible ?
Un utilisateur peut-il installer des applicatifs ?

GESTION DES DROITS D'ACCES

Management des utilisateurs

Comment les utilisateurs qui arrivent dans l'entreprise sont-ils traités?
Comment les utilisateurs qui quittent l'entreprise sont-ils traités?
Comment les utilisateurs qui changent de services, de locaux, d'unités, de lieux dans l'entreprise sont-ils traités?

Gestion des mots de passe

Comment sont gérés les mots de passe et les noms de compte ?
Quelles sont les périodes de renouvellement des mots de passe ?
Quels sont les limites en cas d'échec sur la saisie du mot de passe ?
Qui déverrouille les comptes utilisateurs ?

Droits des utilisateurs –accès aux applications et aux données

Comment sont affectés les droits des utilisateurs ? Sur quels critères ?
Segmentation des droits d'accès – réseau, serveurs, applications, disques réseaux ?
Comment sont gérés les droits à utiliser les applications ?

DONNEES STRATEGIQUES

Quelle est la localisation de ces données ?
Quels sont les risques, déjà répertoriés, liés à la divulgation, l'altération, le détournement des données ?

ANTIVIRUS

Quels sont les dispositifs utilisés aujourd'hui ?
Etes-vous à jour ?

Quels sont les menaces traitées (FTP, smtp, ...) ?
Avez vous souscrit des contrats des mise à jour des logiciels ?
Etes-vous sujet à des problèmes ?
Comment purgez-vous les zones de quarantaines ?
Quels sont les types de machines concernés par les anti-virus : Poste de travail ?
Serveurs micro ? Firewall ?

PROTOCOLES UTILISES

Quels sont les protocoles que vous utilisés ?
TCP/IP
Avez-vous un plan d'adressage ?
Utilisez-vous des adresses officielles Internet pour l'interne ?
Quels sont les besoins de translation ?
Quels sont les services TCP/UDP déjà utilisés (Telnet, SMTP, SNMP, HTTP...)
IPX
Utilsez vous des gateway IPX/IP?
Quel type de matériel ou logiciel utilisez-vous ?

ACCES EXTERNES

Quels sont les modems utilisés dans l'entreprise (nombre, utilisation...) ?

Routeurs

Quels sont les routeurs déjà installés dans l'entreprise ?
Quelles sont les versions d'OS ?
Qui en assure l'exploitation et la maintenance ?
Comment sont gérés les mots de passe d'accès à ces routeurs ?Depuis quels équipements sont-ils atteignables ?
Sont-ils administrables SNMP ?

EXISTANT INTERNET

Disposez-vous d'accès Internet ?
De quelle nature ?
Disposez-vous d'un firewall ou d'un proxy ? Quel type ? Est-il à jour ?
Analysez-vous les informations fournies par les applications ? (Firewall, anti-virus, Etc..)
Quels sont les services Internet permis aux utilisateurs ?
Comment savez-vous que votre protection est efficace ?Avez-vous déjà été attaqué ?
Comment le savez-vous ?

Bibliographie Et Références

[PAS 99] Pascal Nicolas, Cours de réseaux Maîtrise d'informatique U.F.R. Sciences de l'Université d'Angers, 1999

[BOR 98] *François Borderies, Olivier Châtel, Jean-christophe Denis, Didier Reis.* ADMINISTRATION RESEAU *spéciale informatique, 1998*

[DON00] Didier DONSEZ ,Le protocole http Université de Valenciennes Institut des Sciences et Techniques de Valenciennes,2000

[Sol 01] SoluCom , Les PKI : Vers une Infrastructure Globale de Sécurité 2001

[FLO 99] Gérard FLORIN LES TECHNIQUES DE CRYPTOGRAPHIE 1999

[Akk1 04] Abdel Hakim AKKA. Stratégies de sécurité,Meilleures pratiques pour la sécurité d'entreprise, 2004

[Akk2 04] AKKA Abdel Hakim, Étude existant sécurité, 2004

[THO 04] THOMAS.*jacob,* Définir une politique de sécurité informatique des systèmes d'information, www.voirin-consultants.com, mai 2004

[STA 02] William stallings,Sécurité des réseau application et standard Septembre 2002

[Ych 02] Jean- Pierre YCHE, STAGE RSSI Stage du Responsable de la sécurité du système d'information, 2002

[PIP 00] Donald L. PIPKIN, *Sécurité des systèmes d'information,* CampusPress, 2000

[GUI 00] Guillaume Des George, La sécurité des réseaux http://www.guill.net/ 2000

[LAR 98] Marc Laroche, SÉCURITÉ DES RÉSEAUX Analyse et mise en oeuvre Janvier 1998

[PIL 01] Jean-françois pilou Vulgarisation informatique, http://www.commentcamarche.net/, 2001

[RUM 97] James Rumbaugh Modélisation et conception orientées objet, 1997

[BEN 03] BENCHIBANE MOHAMED, Université de BLIDA, Réalisation d'un scanneur réseau, 2003

[KEH 04] Kehliche widad, Conception et réalisation d'un FIREWALL 2004

[CHA01] CHAOUKI AMEL, Conception d'un outil intelligent d'aide au choix de FIREWALL, USTHB,2001

[BEL 03] Stephen M. Bellovin, bill Cheswick FIREWALL et sécurité Internet, 2003
C'est quoi un FIREWALL

[PAU 03] Paul Grégory, réalisation d'un FIREWALL,30 mars 2003

[BUT 00] f. butelle Note d'information sur Les réseaux privés virtuels sécurisés (VPN), 2000.

[SAU] www.sebsauvage.net

[FIRE] www.firewall.com, des pare-feu pour protéger le poste de travail