

REPUBLIQUE ALGERIENNE DEMOCRATE ET POPULAIRE  
UNIVERSITE DE SCIENCE ET DE TECHNOLOGIE  
HOUARI BOUMEDIENNE

**USTHB**

MEMOIRE DE FIN D'ETUDE POUR L'OBTENTION D'UN DIPLOME  
D'INGENIEUR D'ETAT EN INFORMATIQUE

**THEME**

**UN SYSTEME DE FILTRAGE  
DES ACCES A UN  
RESEAU CONNECTE A  
INTERNET**

**Réalisé par :**

*Mr AKLOUF YOUCEF  
Mr DAAS OMAR*

**JURY :**

*Mr RAHAOUAL (PRESIDENT)  
Mr REZGHI (EXAMINATEUR)  
Melle AKLI (EXAMINATRICE)*

**Encadrés par :**

*Promotrice : Mme NOUALI*

*Organisme d'accueil :*

*Centre de recherche sur l'information scientifique et technique  
CERIST*

**PROMOTION 1998 N° 27/98**

# RESUME

Lorsque le réseau interne d'une entreprise est connecté sur un réseau externe (tel que Internet) sans avoir tenu compte des mécanismes pour contrôler les accès à ses systèmes, il peut subir des attaques contre la confidentialité, l'intégrité et la disponibilité de ses informations et des services qu'il délivre. Les conséquences de ces attaques peuvent être très graves voir même désastreuses.

Plusieurs mécanismes ont été élaborés par les experts de la sécurité informatique[CHA96]. Le filtrage des accès réseau en constitue une solution très utilisée dans ce domaine. Et c'est à ce mécanisme que nous nous intéressons dans le cadre de ce projet.

Le filtrage peut être utilisé pour bloquer certaines demandes de connexion ou pour n'en autoriser que quelques-unes sur un sous-ensemble des systèmes appartenant au site que l'on désire sécuriser.

Dans ce mémoire, il est question de filtrer les accès réseau en se basant sur deux mécanismes : Le filtrage des paquets au niveau réseau, réalisable sur un routeur, et le filtrage au niveau application réalisable grâce à des serveurs mandataires jouant le rôle d'intermédiaire entre les serveurs réels de l'application et les utilisateurs désirant y accéder.

## *Mots Clés :*

Filtrage des accès, Proxy server, Routeur, Politique de sécurité, FTP, TCP/IP.

# SOMMAIRE

<b><u>INTRODUCTION</u></b> .....	1
----------------------------------	---

## **CHAPITRE 1 : LES RESEAUX TELEINFORMATIQUES**

1.1- INTRODUCTION.....	4
1.2- SYSTEME TELEINFORMATIQUE.....	4
1.3- EVOLUTION DES SYSTEMES TELEINFORMATIQUE.....	4
1.4- RESEAU TELEIFORMATIQUE.....	5
1.5- COMMUTATION.....	5
1.6 – MODE DE TRANSFERT DE DONNEES.....	6
1.7- LES GRANDES CLASSES DES RESEAUX.....	6
1.8- TOPOLOGIE DES RESEAUX.....	7
1.9- DECOMPOSITION EN COUCHE DU MODELE OSI.....	9

## **CHAPITRE 2 : LE PROTOCOLE TCP/IP**

2.1- INTRODUCTION.....	14
2.2- QU'EST CE QUE TCP/IP.....	14
2.3- CARACTERISTIQUE DE TCP/IP.....	14
2.4- ARCHITECTURE DE TCP/IP.....	15
2.5- TCP/IP EST LE MODELE OSI.....	16
2.6- LES DIFFERENTES COUCHES DU TCP/IP.....	16
2.6.1- COUCHE D'ACCES RESEAU.....	16
2.6.2- COUCHE INTERNET.....	17
2.6.2.1- LE PROTOCOLE IP.....	17
2.6.2.2- LE PROTOCOLE ICMP.....	20
2.6.3- COUCHE TRANSPORT.....	20
2.6.3.1- LE PROTOCOLE TCP.....	20
2.6.3.2- LE PROTOCOLE UDP.....	22
2.6.4- COUCHE APPLICATION.....	23
2.6.4.1- LES SERVICES ORIENTES CONNEXION.....	23
2.6.4.2- LES SERVICES SANS CONNEXION.....	24
2.7- ARCHITECTURE GLOBALE DU PROTOCOLE TCP/IP.....	24
2.8- LE MULTIPLEXAGE.....	26

## **CHAPITRE 3 : APERCU SUR LA SECURITE DES RESEAUX**

3.1- INTRODUCTION.....	28
3.2- MECANISMES DE SECURITE.....	29

3.2.1- AUTHENTIFICATION D'UN SUJET.....	29
3.2.2- SECURITE DE COMMUNICATION.....	29
3.2.3- CONTROLE D'ACCES.....	29
3.2.4- CONTROLE DE FLUX DES INFORMATIONS.....	30
3.3- DIFFERENTS TYPES DES ATTAQUES CONTRE LA SECURITE.....	30
3.4- QUELQUE EXEMPLES D'INTRUSIONS.....	32
3.5- NECESSITE D'UNE POLITIQUE DE SECURITE.....	33
3.6- MISE EN PLACE D'UNE POLITIQUE DE SECURITE.....	35
3.7- LA POLITIQUE DE SECURITE ET LE FILTRAGE DES ACCES RESEAU...	37

## **CHAPITRE 4 : LES SERVICES DE BASE D'INTERNET**

4.1- INTRODUCTION.....	39
4.2- LE MODELE CLIENT/SERVEUR.....	39
4.3- FILE TRANSFERT PROTOCOL (FTP).....	40
4.3.1- DEFINITIONS.....	40
4.3.2- LES CONNEXIONS FTP.....	40
4.3.3- LE MODELE DE PROCESSUS CLIENT/SERVEUR DE FTP.....	41
4.3.4- LES MODES DE CONNEXIONS DE FTP.....	42
4.3.5- LES TRANSFERTS FTP PAR TIERS INTERPOSE.....	44
4.3.6- EXEMPLE D'UNE SESSION FTP.....	45
4.4- LE PROTOCOLE TELNET (TELECOMMUNICATION NETWORK).....	47
4.5- LE PROTOCOLE SMTP (SIMPLE MAIL TRANSFERT PROTOCOL).....	48
4.6- LA VULNERABILITE DE CES SERVICES.....	49

## **CHAPITRE 5 : LE FILTRAGE DES ACCES RESEAUX**

5.1- INTRODUCTION.....	52
5.2- LE FILTRAGE PAR PAQUETS.....	52
5.2.2- LES INFORMATIONS NECESSAIRES AU ROUTAGE.....	53
5.2.3- FONCTIONNEMENT DU FILTRAGE DE PAQUETS.....	54
5.2.4- CHOIX D'UN ROUTEUR A FILTRAGE DE PAQUETS.....	55
5.2.5- CLASSIFICATION DES METHODES DE FILTRAGE PAR PAQUETS.....	56
5.2.5.1- LES REGLES DE FILTRAGE.....	56
5.2.5.2- FILTRAGE PAR ADRESSE.....	57
5.2.5.3- FILTRAGE PAR LE SERVICE.....	57
5.2.5.4- FILTRAGE PAR L'INTERFACE.....	59
5.2.5.5- CONVENTIONS CONCERNANT LES ROUTEURS CISCO.....	59
5.2.5.6- EXEMPLE PRATIQUE (CAS D'UN ROUTEUR CISCO)....	62
5.2.6- RENVOIE DES CODES D'ERREURS ICMP.....	64
5.2.7- AVANTAGE DU FILTRAGE DE PAQUETS.....	64
5.2.8- INCONVENIENTS DE FILTRAGE DE PAQUETS.....	65
5.3- FILTRAGE AU NIVEAU APPLICATION (OU PROXY SERVER).....	67
5.3.2- QU'EST QU'UN BASTION(PASSERELLE).....	67
5.3.3- QU'EST QU'UN PROXY.....	68
5.3.4- L'ARCHITECTURE D'UN PROXY.....	69
5.3.5- TERMINOLOGIE DES PROXIES.....	71
5.3.6- AVANTAGES DES PASSERELLES APPLICATION.....	72

