

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'enseignement supérieur et de la recherche scientifique

Centre de Recherche de l'Information Scientifique et Technique

C.E.R.I.S.T

MEMOIRE

Pour l'obtention du Diplôme de Post-Graduation Spécialisée en

Sécurité Informatique

THEME

In té g r a t i o n e t d é p l o i e m e n t d ' u n e a r c h i t e c t u r e d e F i r e w a l l
d a n s u n e i n f r a s t r u c t u r e r é s e a u a c a d é m i q u e

Présenté par :

Mr : Smail BOUSSAADI

Encadré par :

Mme : Hassina BENSAFIA

Devant le jury :

D. Omar NOUALI

Mme Souad BENMEZIANE

D. Djamel TANDJAOUI

Président

Examineur

Examineur

MAI 2006

TABLES DES MATIERES

INTRODUCTION GENERALE.....	1
-----------------------------------	----------

CHAPITRE 1 : LA SECURITE DES RESEAUX INFORMATIQUE

I. INTRODUCTION.....	5
II. LE MODELE TCP/IP.....	6
III. L'IMPORTANCE DE LA SECURITE.....	8
IV. LES MENACES.....	8
IV.1. les acteurs d'une menace.....	9
IV.2. Les vecteurs d'une menace et attaques.....	10
IV.3. les nouvelles menaces.....	12
V. POLITIQUE DE SECURITE.....	13
V.1. analyse de la situation.....	14
V.2. analyse du risque.....	14
V.3. établissement de la politique de sécurité.....	15
VI. LES COMPOSANTES DE LA SECURITE.....	15
VI.1. les firewalls.....	15
VI.2. contrôle d'accès : authentification.....	15
VI.3. cryptage et réseau VPN.....	15
VI.4. détection d'intrusion (IDS).....	16
VII. CONCLUSION.....	17

CHAPITRE 2 : TECHNOLOGIE & ARCHITECTURE DES FIREWALLS

I. INTRODUCTION.....	19
II. GENERALITES SUR LES FIREWALLS.....	20
III. DEFINITIONS D'UN FIREWALL.....	20
IV. EMBLACEMENT D'UN FIREWALL.....	21
V. LES FONCTIONS DE SECURITE D'UN FIREWALL.....	21
V.1. contrôle d'accès	21
V.2. isolement du réseau et authentification des utilisateurs.....	22
V.3. chiffrement des données et VPN.....	22
V.4. le NAT ou translation d'adresses.....	22

VI. AVANTAGES ET LIMITES DES FIREWALLS.....	23
VII. TECHNOLOGIE DES FIREWALLS.....	24
VII.1. les filtre de paquets.....	24
VII.1.1. principe.....	24
VII.1.2. fonctionnement.....	25
VII.1.3. avantages et limites des filtres de paquets.....	26
VII.2. les passerelles applicatives.....	27
VII.2.1. principe.....	27
VII.2.2. fonctionnement.....	28
VII.2.3. les passerelles de niveau applicatif.....	28
VII.2.4. les passerelles de niveau circuit.....	28
VII.2.5. avantages et limites des passerelles applicatives.....	30
VII.3. les firewalls a inspections d'états.....	31
VII.3.1. principe.....	31
VII.3.2. fonctionnement.....	32
VII.3.3. avantages et limites des firewalls a inspections d'états.....	33
VIII. AUTRES FONCTIONNALITES DE FIREWALLS.....	33
IX.1. la gestion de NAT.....	33
IX.2. l'authentification des utilisateurs.....	34
IX.3. la gestions des VPN.....	35
IX. COMPARAISON DES PERFORMANCES DES TROIS TECHNOLOGIES.....	35
X. ARCHITECTURES DES FIREWALLS.....	36
X.1. ARCHITECTURE MONO COUCHE.....	36
X.1.1. architecture routeur filtrant.....	36
X.1.2. avantages et limites.....	37
X.1.2. architecture hote a double réseau.....	37
X.2.3. avantages et limites.....	38
X.1.3. architecture hote a écran.....	39
X.3.3. avantages et limites.....	40
X.2. ARCHITECTURE MULTI COUCHE.....	40
X.2.1. concept d'une DMZ.....	40
X.2.2. avantages d'une DMZ.....	41
X.2.3. architecture sous réseau filtré.....	42
X.2.4. avantages et limites.....	43
X.2.5. variation sur les architectures sous réseau filtré.....	43
X.2.6. architecture dual DMZ.....	44
X.2.7. structure d'une architecture dual DMZ.....	44
XI. CONCLUSION.....	46
CHAPITRE 3 : LE MARCHE DES FIREWALLS & CRITERES DE CHOIX	
I. INTRODUCTION.....	48
II. FIREWALL LOGICIEL.....	48

II.1. avantages d'une solution logicielle.....	48
II.2. limites d'une solution logicielle.....	49
III. FIREWALL MATERIEL.....	49
III.1. avantages d'une solution matérielle.....	49
III.2. limites d'une solution matérielle.....	49
IV. LES PRODUITS DU MARCHE.....	50
IV.1. Check Point.....	50
IV.2. Cisco.....	51
IV.3. NetFilter.....	52
IV.4. Clavister.....	52
IV.5. SonicWall.....	53
V. CRITERES DE CHOIX.....	54
V.1. les deux niveaux de sécurité.....	55
V.2. choix des équipements.....	57
V.3. architecture de l'ensemble.....	57
V.4. compétences humaines.....	58
VI. CONCLUSION.....	60

CHAPITRE 4 : GESTION DU RISQUE D'UN RESEAU ACADEMIQUE & INTEGRATION D'UNE SOLUTION DE FIREWALL

I. INTRODUCTION.....	62
II. LE RESEAU ACADEMIQUE DE L'INI.....	63
II.1. infrastructure du réseau de l'INI.....	63
II.2. schéma du réseau locale de l'INI.....	65
III. GESTION DU RISQUE ASSOCIE AU RESEAU DE L'INI.....	65
III.1. les risques externes.....	65
III.2. les facteurs aggravants du risque.....	66
IV. POLITIQUE DE SECURITE.....	66
V. PROPOSITION D'UNE ARCHITECTURE.....	67
V.1. LES COMPOSANTES DE L'ARCHITECTURE PROPOSEE.....	68
V.1.1. les filtres.....	68
V.1.2. choix des composantes de l'architecture.....	69
V.2. PERSPECTIVE D'UNE SOLUTION DUAL DMZ.....	71
V.2.1. les services de la deuxième DMZ.....	71
V.2.2. choix des composantes de l'architecture.....	74

VI. CONCLUSION.....	75
CONCLUSION GENERALE.....	76
REFERENCES BIBLIOGRAPHIQUES.....	78