



Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique
Université des Sciences et de la Technologie Houari Boumediene

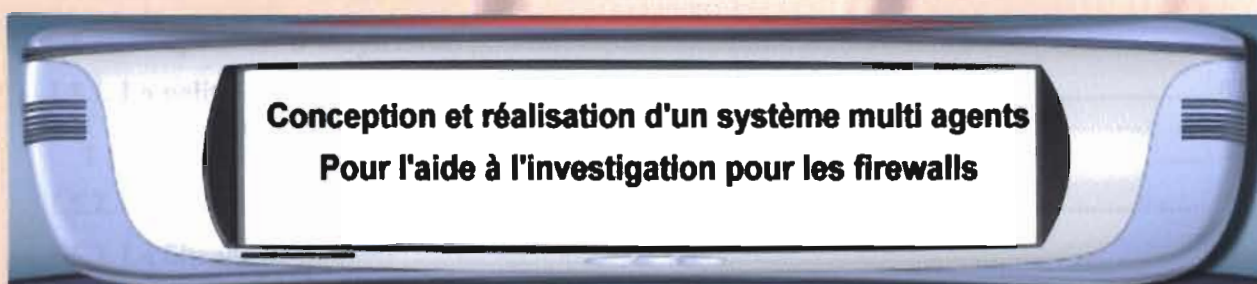


INSTITUT D'INFORMATIQUE

Mémoire du projet de fin d'études
Pour l'obtention du diplôme
D'Ingénieur d'Etat en Informatique

OPTION : Sécurité Réseaux

SUJET



**Conception et réalisation d'un système multi agents
Pour l'aide à l'investigation pour les firewalls**

Devant le jury composé de :
Présidente : Mme Mahdaoui
Examineurs : Mr. Aklouf
Mr. Zaffoune

Dirigé par
Promotrice : Mme H. Mellah

Etudié par :
Mr. Makeri Sofiane
Mr. Gueddah Boumediene

Organisme d'accueil
CERIST

Promotion 2002/2003 (N° 63)

Table des Matières

<u>Titre</u>	<u>Page</u>
--------------	-------------

Introduction Générale.....	5
-----------------------------------	----------

Chapitre I: Les Firewalls

I.1. Introduction.....	6
-------------------------------	----------

I.2. Définition générale.....	6
--------------------------------------	----------

I.3. L'emplacement d'un firewall.....	7
--	----------

I.4. Les catégories de firewall.....	7
---	----------

I.4.1. Le firewall logiciel.....	7
---	----------

I.4.2. Le firewall hardware.....	7
---	----------

I.5. Les composants d'un firewall.....	8
---	----------

I.5.1. La politique de sécurité du réseau.....	8
---	----------

1. Politique d'accès aux services réseau.....	8
---	---

2. La politique de conception du firewall.....	8
--	---

I.5.2. L'authentification Forte.....	9
---	----------

I.5.3. Le filtrage de paquets.....	9
---	----------

1. Les avantages de filtrage de paquets.....	11
--	----

2. Les limitations de filtrage de paquets.....	11
--	----

I.5.4. Les services mandataires (Proxy).....	11
---	-----------

1. Les avantages des services mandataires.....	12
--	----

2. Les limitations des services mandataires.....	12
--	----

I.6. les principales architecture de firewall.....	12
---	-----------

I.6.1 Architecture d'hôte à double réseau.....	12
--	----

I.6.2. Architecture d'hôte à écran.....	13
---	----

I.6.3. Architecture de sous réseau écran.....	14
---	----

I.7. Le fichier journal (log).....	15
---	-----------

I.8. Les avantages d'un firewall.....	15
--	-----------

I.9. Les limitations d'un firewall.....	15
--	-----------

I.10. Conclusion.....	16
------------------------------	-----------

Chapitre II : Les Fichiers Logs

II.1. Introduction.....	17
--------------------------------	-----------

II.2. Définition d'un fichier log.....	17
---	-----------

II.3. Le format d'un fichier log du firewall.....	17
--	-----------

II.4. Les problèmes liés aux fichiers logs.....	20
--	-----------

II.5. La protection des fichiers logs.....	20
---	-----------

II.5.1. Première méthode.....	20
-------------------------------	----

II.5.2. Deuxième méthode.....	20
-------------------------------	----

II.5.3. Troisième méthode.....	20
--------------------------------	----

II.5.4. Quatrième méthode	21
II.5.5. La rotation des fichiers logs	21
II.6. L'importance des fichiers logs dans l'investigation.....	21
II.7. L'interprétation des fichiers logs.....	21
II.8. Conclusion	22

Chapitre III : Les Systèmes Multi Agents

III.1. Introduction.....	23
III.2. Les systèmes multi agent.....	23
III.2.1. Définition d'un système multi agents	23
III.2.2. Intérêts des systèmes multi agents.....	24
III.2.3. Utilisation des systèmes multi agents	24
III.2.4. Problématique des Systèmes multi agents	25
III.2.5. Modèles de systèmes multi agents	25
1. Les systèmes à tableau noir.....	25
1.1. Les avantages.....	26
1.2. Les inconvénients	26
2. Les systèmes d'acteur.....	27
3. Le système physiquement distribué.....	27
III.2.6. Définition d'un agent.....	27
1. La différence entre agent et objet	28
III.2.7. Modèles d'agent.....	28
1. Agents réactifs	28
2. Agents cognitifs	29
3. Etude comparative.....	30
III.2.8. Environnement des agents.....	31
III.2.9. Organisation d'agents.....	31
1. Définition.....	31
1.1. Structure organisationnelle	32
1.1.1. Réseau contractuel.....	32
1.1.2. Le treillis de production	32
1.1.3. Plan partiel global (P.G.P)	32
1.2. Organisation centralisée	32
1.3. Organisation libre (non centralisée)	32
III.2.10. Coopération	33
1. Définition.....	33
2. Les modes de coopération.....	33
2.1. Le mode " COMMANDE "	33
2.2. Le mode "APPEL D'OFFRE"	33
2.3. Le mode "COMPETITION"	34
2.4. Coopération par partage des tâches.....	34
2.5. Coopération par partage des résultats.....	34
III.2.11. Le contrôle	35
1. Le contrôle dans les systèmes à tableaux noirs	35
1.1. Le contrôle procédural	35
1.1.1. Les avantages	35
1.1.2. Les inconvénients	36
1.2. Le contrôle hiérarchique.....	36
1.2.1. Les avantages	37
1.2.2. Les inconvénients.....	37

1.3. Le contrôle opportuniste (à tableau noir).....	37
1.3.1. Les avantages	38
1.3.2. Les inconvénients	38
1.4. Le contrôle hybride	39
2. Le contrôle dans les systèmes d'acteurs	39
III.2.12. La résolution des conflits	40
1. La négociation.....	40
1.1. La négociation centralisée	40
1.2. La négociation distribuée	40
1.3. Le réseau contractuel.....	40
2. La coordination	40
III.2.13. La communication	41
1. Définition.....	41
2. Les différentes formes de communication	41
2.1. La communication par partage d'information.....	41
2.2. La communication par envoi de message.....	42
2.3. Comparaison des deux modèles de communication.....	42
3. Politique de communication entre les agents	43
3.1. Communication asynchrone	43
3.2. Communication synchrone	43
3.3. Communication directe (monocast).....	43
3.4. Communication en groupe de diffusion (multicast).....	43
III.2.14. Les Langages de communication entre agents.....	44
1. Le langage KQML (Knowledge and Query Manipulation Language).....	44
2. ACL (Agent communication language).....	46
III.3. Conclusion.....	46
Chapitre IV : Conception et Implémentation du système	
IV.1. Introduction	48
IV.2. Introduction à UML (Unified Modeling Language).....	48
IV.2.1. Constituant d'UML	48
1. Diagramme de cas d'utilisation.....	48
2. Diagramme de classe.....	48
3. Diagramme d'objet.....	48
4. Diagramme état de transition	48
5. Diagramme d'activité	49
6. Diagramme de séquence	49
7. Diagramme de collaboration.....	49
8. Diagramme de composants.....	49
9. Diagramme de déploiement	49
IV.3. Conception du système.....	49
IV.3.1. La base de connaissance principale.....	49
IV.3.2. La sous base de connaissance	52
1. Principe de la codification utilisée.....	53
1.1. L'identificateur d'un champ de la base de connaissance.....	53
1.2. L'identificateur d'une règle de la base de connaissance.....	54
2. L'intérêt de la codification.....	54
IV.3.3. Définition de la tâche	54
IV.3.4. Le processus d'interprétation d'une ligne de fichier log.....	54
1. Le rôle des agents.....	55
1.1. Le rôle de l'agent superviseur.....	55
1.1.1. Définition de la priorité.....	55
1.1.2. L'intérêt de la priorité.....	55

1.2. Le rôle de l'agent contractant	56
IV.4. Architecture du système	57
IV.5. Modélisation du système.....	58
IV.5.1. Le diagramme de classe.....	58
1. Description conceptuelle des méthodes	59
1.1. Les méthodes de la classe « Agent superviseur ».....	59
1.1.1. La méthode « division base »	59
1.1.2. La méthode « Lecture log ».....	59
1.1.3. La méthode «Extraire- champs ».....	60
1.1.4. La méthode « Envoi- champs ».....	60
1.1.5. La méthode « Traiter-résultat »	60
1.1.6. La méthode « Sauvegarde »	60
1.2. Les méthodes de la classe « Agent contractant »	60
1.2.1. La méthode « Récupère- champ »	60
1.2.2. La méthode « Recherche-sous base »	60
1.2.3. La méthode « Envoi-résultat »	60
1.3. Les méthodes de la classe « Base de connaissances principale ».....	60
1.3.1. La méthode « Ajouter règle ».....	60
1.3.2. La méthode « Supprimer règle »	60
1.3.3. La méthode « Modifier règle »	60
IV.5.2.Le diagramme d'activité.....	61
IV.5.3. Diagramme de séquence	62
IV.6. Implémentation du système.....	63
IV.6.1.Environment de développement	63
1. Langage de programmation	63
1.1. Langage java.....	63
1.2. Eléments de base utilisés dans la réalisation.....	63
1.2.1. L'API d'accès aux données de java (JDBC)	63
1.2.2. Accès via les sockets	64
IV.6.2. Schéma de communication entre client / serveur.....	64
1. Application client (Agent(s) contractant(s)).....	65
2. Application serveur (Agent superviseur)	65
IV.6.3. Les interfaces du système	65
IV.7. La base de Connaissance principale	72
IV.7.1. Les règles spécifiques aux ports destination.....	72
IV.7.2. Les règles spécifiques aux ports source	75
IV.7.3. Les règles spécifiques aux messages ICMP	76
IV.7.4. Les règles spécifiques aux adresses IP	77
Conclusion Générale.....	78
Annexe.....	80
Bibliographie.....	84