

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENNE
INSTITUT DE L'INFORMATIQUE

MEMOIRE DU PROJET DE FIN D'ETUDES POUR L'OBTENTION
DU DIPLOME D'INGENIEUR D'ETAT EN INFORMATIQUE

Option
SYSTEME D'INFORMATION

Thème

APPORT DE XML POUR LES SYSTEMES
D'AIDE A L'INVESTIGATION POUR LES
FIREWALLS

Organisme d'accueil : CERIST
Encadré par : M^{me} H.Mellah

Réalisé par : M^{elle} Afrit Siham
M^{elle} Rahim Samia

Devant le jury composé de:

M^{me} Akli
M^{me} Gharbi
M^r Aklouf

Présidente
Examinatrice
Examinateur

N°79 - Promotion 2003

Résumé:

Un Firewall est un système permettant de protéger un réseau local des attaques provenant d'Internet, en contrôlant l'accès au réseau et en limitant le trafic entrant et sortant. Les Firewalls installés sur les machines sont de type divers, ce qui engendre une différence de format au niveau des journaux de bord des connexions qui sont générés par les Firewalls. Ces journaux (plus communément appelés fichiers log) sont dans la majorité des cas difficilement interprétés par l'administrateur réseau.

L'objectif de notre travail est dans un premier temps d'homogénéiser les formats des fichiers log en utilisant la norme XML pour générer un format standard directement exploitable par un interpréteur automatique, en proposant certaines solutions aux points de défaillances des Firewalls, et dans un second temps essayer d'étudier ce que le langage de définition des interfaces (IDL) de CORBA peut faire dans ce genre de situation.

Mots clés : Firewalls, Log, XML, DTD, XSL, IDL, CORBA, Filtrage.

Abstract:

Firewall is a system permitting to protect a local network of the attacks coming from Internet, while controlling the access to the network and while limiting the incoming and retiring traffic. The Firewall installed on the machines is of various types, what generates a difference of format of the connections' newspapers that is generated by the Firewalls. The administrator network in the majority of the cases difficulty interprets these newspapers (more commonly named files log).

The objective of our work is in a first time to homogenize the format of log file while using the XML norm to generate a standard format directly exploitable by an automatic interpreter, while proposing some solutions to the points of failings of the Firewalls, and in a second time to try to study what the language of definition of the interfaces (IDL) CORBA can make in this kind of situation.

Key words: Firewalls, Log, XML, DTD, XSL, IDL, CORBA, Filtering.

Table des matières

	page
INTRODUCTION GENERALE	1
CHAPITRE I: LES FIREWALLS	
Introduction.	4
1. Qu'est-ce-qu'un firewall ?	4
2. Objectifs des firewall.	5
3. Firewall réseau et firewall individuel.	5
3.1. Firewall individuel.	6
3.2. Firewall réseau.	6
4. Types des firewalls.	6
4.1. Les firewalls matériels.	6
4.2. Les firewalls logiciels.	7
5. Politique de sécurité.	7
6. Classification des firewalls.	8
6.1. Firewalls niveau paquet.	8
6.1.1. Avantage du filtrage de paquets.	8
6.1.2. Inconvénients du filtre des paquets.	9
6.2. Firewalls niveau session.	9
6.3. Firewalls niveau application.	9
7. Architecture des firewalls.	10
7.1. Firewall avec routeur de filtrage.	10
7.1.1. Avantages.	11
7.1.2. Inconvénient.	11
7.2. Passerelle double -Le réseau du bastion-.	11
7.3. Firewall avec filtrage du réseau.	11
7.4. Firewall avec filtrage de sous réseau.	12
7.4.1. Avantages.	13
7.4.2. Inconvénients.	13
8. Filtrage de paquets.	13
8.1. Introduction.	13
8.2. Fonctionnement du filtrage de paquets.	14
8.3. Les méthodes de filtrage de paquets.	14
8.3.1. Filtrage de paquets avec TCP.	14
8.3.2. Filtrage de paquets avec UDP.	14
8.3.3. Filtrage de paquets par adresse IP.	15
8.3.4. Filtrage de paquets par service.	15
9. Spécification des règles de filtrage.	15
10. Journalisation.	15
10.1. La définition de fichier log.	16
10.2. Les fichiers logs d'un Firewall.	16
10.3. Le Format d'un fichier log.	17

10.4. Les critères de création de fichier log.	18
10.5. L'utilisation des fichiers logs.	19
10.6. L'importance des fichiers logs.	19
11. Avantages et inconvénient des firewalls.	20
11.1. Avantages des firewalls.	20
11.2. Inconvénient des firewalls.	21
12. Les solutions aux points de défaillances des firewalls.	21
Conclusion.	23

CHAPITRE II: LA NORME XML

Partie I: Concepts Généraux Sur Les Documents

Introduction.	24
1. Définition.	24
1.1. Qu'est ce qu'un document?	24
1.2. le document électronique.	24
1.3. modèles et formats de documents électroniques.	24
2. le modèle de documents structurés.	25
3. Formats normalisés des documents.	26
3.1. SGML.	27
3.2. ODA.	28
3.3. HyTime.	28
3.4. XML.	29
Conclusion.	29

Partie II: XML(eXtensible Markup Language)

Introduction.	30
Origine.	30
1. SGML.	31
1.1. Avantages.	32
1.2. Inconvénients.	32
2. HTML.	32
2.1. Avantages.	32
2.2. Inconvénients.	32
3. XML.	33
3.1. Définition.	33
3.2. Avantages.	33
3.3. Outils et Logiciels.	34
3.3.1. Parseur (Analyseur).	34
3.3.2. Le processeur de feuilles de style.	35
3.3.3. Des logiciels généraux.	35
3.3.4. Les standards.	35
4. XML le langage.	36
4.1. Q'est ce que le XML ?	36
4.2. Les documents XML.	36
4.3. Documents bien formés et documents valides.	37
4.4. Structure d'un document.	37
4.4.1. Prologue.	38
4.4.1.1. Déclaration XML.	38
4.4.1.2. Instruction de traitement.	38

4.4.1.3. Déclaration de type de document.	39
4.4.2. Arbre des éléments.	39
4.4.3. Les commentaires.	39
4.5. Eléments et Attributs.	39
4.5.1. Les balises.	39
4.5.2. Eléments.	39
4.5.3. Les attributs.	41
4.5.4. Entités.	42
4.5.4.1. Entités générales internes.	43
4.5.4.2. Entités générales externes.	43
4.5.4.3. Référence à des entités prédéfinies.	44
4.5.4.4. Références à des caractères.	44
4.5.5. Section littérale.	45
4.5.6. Entités non XML (Notation).	45
4.6. La définition de type de document.	46
4.6.1. Contenu d'une DTD.	48
4.6.1.1. Déclaration d'éléments.	48
4.6.1.1.1. Elément fils.	48
4.6.1.1.2. Données.	49
4.6.1.1.3. Modèle mixte.	49
4.6.1.1.4. Contenu libre (ANY).	49
4.6.1.1.5. Elément vide.	49
4.6.1.2. Déclaration de type d'attributs.	50
4.6.1.3. Les entités paramètres.	51
1- Interne.	51
2- Externe.	51
4.6.2. Sections conditionnelles.	51
5. Les schémas XML.	52
5.1. Définition.	52
5.2. Objectifs.	53
5.3. Description des éléments.	53
5.4. Description des attributs.	53
5.5. Les différents types de schémas XML.	53
5.5.1. Type simple.	53
5.5.2. Type complexe.	54
6. Les liens XML.	55
6.1. Xlink.	55
6.2. Xpointer.	56
7. Feuilles de style.	56
7.1. CSS (cascading Style Sheet).	57
7.1.1. Principe de base.	57
7.2. XSLT.	59
7.2.1. Principe de fonctionnement.	59
7.2.2. La structure de document XSL.	60
8. Les API.	60
8.1. Les API utilisant une approche hiérarchique.	61
8.1.1. Introduction à DOM.	61
8.1.2. Les caractéristiques de l'API DOM.	61
8.1.3. La structure de l'API DOM.	61
8.1.4. Le fonctionnement de l'API DOM.	62

8.2. Les API basés sur un mode événementiel.	62
8.2.1. Introduction à SAX.	62
8.2.2. Structure d'une application fondée sur SAX.	63
8.2.3. Le fonctionnement d'un API SAX.	63
Conclusion.	64

CHAPITRE II: L'IDL DE CORBA

Introduction.	65
1. Présentation de CORBA.	65
2. Le modèle objet client/serveur.	66
3. Architecture CORBA.	68
3.1. L'OMG.	68
3.2. L'OMA.	68
3.2.1. L'Object Request Broker.	69
3.2.1.1. Le rôle de l'ORB.	69
3.2.1.2. Les composants de l'ORB.	70
3.2.2. Les services objets "CORBAServices".	73
3.2.3. Les utilitaires communs "CORBAFacilities".	74
3.2.4. Les interfaces de domaine " Domain Interfaces".	74
3.2.5. Les objets applicatifs "Application Interface".	74
4. Les avantages et limites de CORBA.	74
4.1. Avantages.	74
4.2. Les limites.	75
5. IDL de CORBA.	75
5.1. Définition.	75
5.2. Les éléments du langage IDL.	75
5.2.1. Le module.	75
5.2.2. L'interface.	75
5.2.2.1. Les attributs.	76
5.2.2.2. Les opérations.	76
5.2.3. Les types complexes.	77
5.2.3.1. Enumération.	77
5.2.3.2. Structure:	77
5.2.3.3. Union.	77
5.2.3.4. Tableau.	78
5.2.3.5. Sequence.	78
5.2.4. Exceptions.	78
5.2.5. Types de méta-données.	78
5.2.5.1. TypeCode.	78
5.2.5.2. Type any.	78
6. Projection vers un langage.	79
7. La mise en place d'une application CORBA.	81
8. Les limites actuelles de l'IDL.	83
Conclusion.	84
CORBA et XML, conflit ou coopération?	85

CHAPITRE IV: CONCEPTION

Introduction.	88
1. Les Firewalls.	88
1.1. ZoneAlarm.	88

1.2. Sygate.	89
2. Première approche en utilisant la norme Xml.	90
2.1. Architecture du système.	90
2.2. Description des différentes phases de l'application.	91
2.2.1. La phase Traitement.	91
2.2.1.1. les différentes couches de Traitement.	91
2.2.1.1.1. Couche Détection de Type.	92
2.2.1.1.2. La couche Extraction.	93
2.2.1.1.2.1. Description des entités de la couche Extraction.	94
2.2.2. La phase Insertion.	99
2.2.2.1. Création de la Table Standard.	100
2.2.3. La phase Génération XML.	100
2.2.3.1. Fonctionnement de la phase Génération XML.	101
2.2.3.2. Association d'une feuille XSL au document XML.	102
3. Deuxième approche en utilisant la norme CORBA.	103
3.1. Architecture Générale du système.	104
3.2. Description du système à développer.	104
1. L'application serveur.	105
2. L'application client.	105
3.3. Phase Implémentation.	105
3.4. Exécution de l'application.	112
Conclusion.	113

Chapitre V: MISE EN OEUVRE

Introduction.	114
1. Les outils utilisés.	114
1.1. Le langage Java.	114
1.2. JdataStoreExplorer.	114
1.2.1. Création d'une nouvelle table.	115
1.2.2. Requêtes SQL.	115
2. Présentation de l'application.	116

CONCLUSION GENERALE.	107
-----------------------------	-----

ANNEXES

Annexe A.
Annexe B.
Annexe C.

BIBLIOGRAPHIE