

# THÈSE DE DOCTORAT

Présentée par :

**Ali KARTIT**

## **Une nouvelle approche de détection d'intrusions et étude des problèmes liés au déploiement de politiques de sécurité dans les réseaux informatiques**

Discipline: Sciences de l'ingénieur

Spécialité : Informatique et Télécommunications

U.F.R. n° : Informatique et télécommunications

Période d'accréditation : 2009/2012

Directeur de l'UFR : Driss ABOUTAJDINE.

Date : 05/11/2011

Heure : 10h30

Lieu : Amphi IBN AL Haytam, Faculté des Sciences Rabat

### **Devant le jury:**

#### **Président:**

M. Driss ABOUTAJDINE, PES (FS, Rabat, Maroc)

#### **Examineurs:**

M. Mohamed EL MARRAKI, PES (FS, Rabat, Maroc)

M. Mohamed RZIZA, PH (FS, Rabat, Maroc)

Mme. Salma MOULINE, PH (FS, Rabat, Maroc)

M. Ahmed HAMMOUCH, PES (ENSET, Rabat, Maroc)

.....

## Résumé :

Actuellement, les politiques de pare-feu (en anglais firewall) peuvent contenir de milliers de règles et ce à cause de la taille énorme et la structure complexe des réseaux modernes. De ce fait, ces politiques nécessitent des outils automatiques fournissant un environnement convivial pour spécifier, configurer et déployer en sûreté une politique cible. Beaucoup de travaux de recherche ont traité de la spécification des politiques, la détection des conflits et le problème d'optimisation, mais très peu de travaux se sont intéressés au déploiement de politiques.

La détection d'intrusions consiste à découvrir ou identifier l'utilisation d'un système informatique à d'autres fins que celles prévues. C'est une technique à multiples facettes, difficile à cerner lorsqu'on ne les manipule pas. Mais la plupart des travaux effectués dans ce domaine restent difficiles à comparer. On peut rarement mettre deux modèles sur un pied d'égalité, et il est peu aisé de mettre à l'épreuve plusieurs modèles, ou encore d'en développer d'autres radicalement différents sans tout reconstruire.

Dans cette thèse, nous avons:

Premièrement, conçu et implémenté un algorithme correct et efficace appelé « *Enhanced Scanning Deployment* » qui nous a permis de déployer une politique de sécurité cible d'une façon exacte. Deuxièmement, adopté et implémenté la solution *VPN/SSH* pour garantir la sécurité lors de déploiement de la politique cible à l'aide de l'algorithme déjà conçu. Troisièmement, proposé une nouvelle approche de détection d'intrusions pour les systèmes informatiques complexes, basée sur une politique de sécurité à trois niveaux appelée « *Système de sécurité à trois niveaux* ». Cette politique globale permettra à l'administrateur des systèmes de sécurité non seulement de détecter les attaques, mais aussi pour l'avertir à propos d'une telle intrusion et en interdire l'accès à l'ensemble des réseaux.

.....

Mots-clefs : Déploiement de Politiques de Sécurité, Sécurité des Réseaux, Système de Détection d'Intrusions (IDS), Corrélation d'Alertes, Division du Trafic, Fusion de Données.