ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 32436 B1

(43) Date de publication :
03.07.2011

(51) Cl. internationale :
G06F 21/00; G06F 12/14; G06F 15/16

(21) N° Dépôt :
32471

(22) Date de Dépôt :
31.12.2009

(71) Demandeur(s) :
UNIVERSITE HASSAN II AIN CHOCK, PRESIDENCE 19 RUE TARIK BNOU ZIAD CASABLANCA (MA)

(72) Inventeur(s) :
MEDROMI HICHAM

(74) Mandataire :
MEDROMI HICHAM

(54) Titre : **PLATEFORME DISTRIBUEE HARD/SOFT DE SECURITE ET DE DETECTION D'INTRUSION**

(57) Abrégé : LA PLATEFORME DE DÉTECTION D'INSTRUSIONS PROPOSÉE, COMPREND : - UN CAPTEUR CHARGÉ DE COLLECTER DES INFORMATIONS SUR L'ÉVOLUTION DE L'ÉTAT DU SYSTÈME SURVEILLÉ; - UN ANALYSEUR MATÉRIEL NIVEAU 1 CARACTÉRISÉ PAR UN AUTOMATE PROGRAMMABLE, UN DSP, FPGA, UN MICROCONTRÔLEUR. SON RÔLE EST D'ANALYSER LE FLUX D'INFORMATION CAPTURÉ ET SELON LE DEGRÉ DE MENACE QUE PEUT REPRÉSENTER L'INSTRUSION ET LES RÈGLES ET PROCÉDURES QUI LUI ONT ÉTÉ APPLIQUÉES, IL VA DÉCIDER DE BLOQUER OU LAISSER LE TRAFIC CONSTINU SON CHEMIN VERS L'ANALYSEUR NIVEAU2. - UN ANALYSEUR LOGICIEL NIVEAU 2 CHARGÉ D'EFFECTUER UN EXAMEN PLUS APPROFONDI DU FLUX ET QUI VA SE SERVIR DE L'INTELLIGENCE DES AGENTS POUR DÉCIDER DE BLOQUER OU PAS LE TRAFIC ET GÉNÉRER UNE ALERTE PERTINENTE. - UN MANGER QUI COLLECTE LES ALERTES PRODUITS PAR LES DEUX ANALYSEURS. IL EST CHARGÉ DE LA PRÉSENTATION DES ALERTES À L'ADMINISTRATEUR DE SÉCURITÉ ET AUSSI, DE LA RÉACTION ADOPTÉE PAR LES DEUX ANALYSEURS.

Abrégé du contenu technique de l'invention

La plateforme de détection d'intrusions proposée, comprend :

- un **capteur** chargé de collecter des informations sur l'évolution de l'état du système surveillé ;
- un **analyseur matériel niveau 1** caractérisé par un automate programmable, un DSP, FPGA, un microcontrôleur. Son rôle est d'analyser le flux d'information capturé et selon le degré de menace que peut représenter l'intrusion et les règles et procédures qui lui ont été appliquées, il va décider de bloquer ou laisser le trafic continu son chemin vers l'analyseur niveau 2.
- un **analyseur logiciel niveau 2** chargé d'effectuer un examen plus approfondi du flux et qui va se servir de l'intelligence des agents pour décider de bloquer ou pas le trafic et générer une alerte pertinente.
- un **manager** qui collecte les alertes produites par les deux analyseurs. Il est chargé de la présentation des alertes à l'administrateur de sécurité et aussi, de la réaction adoptée par les deux analyseurs.

32436

Plateforme distribuée Hard/Soft de Sécurité et de Détection

Description de l'invention

01 JUIL 2011

Etat de la technique antérieur

Un système de détection d'intrusions, appliance ou logiciel, actuel est formé d'un seul moteur d'analyse utilisant une technique de détection d'intrusions à base du soft. Ces solutions existantes dépendent fortement des systèmes d'exploitation ce qui facilite les attaques et les intrus et une forte indépendance à l'environnement du travail.

Description du problème technique

Les systèmes de détection d'intrusions existants ont été conçus pour des environnements connus et bien définis et n'offrent pas une solution à certaines caractéristiques des réseaux telles que la variation des comportements des utilisateurs et des services offerts, la complexité et l'évolution croissantes des types d'attaques auxquelles ils peuvent être sujets, la rapidité des attaques qui peuvent survenir simultanément sur plusieurs machines. Ils ne sont donc pas adaptés à des environnements dynamiques.
Il manque toujours des méthodes et des mécanismes permettant de détecter les scénarios d'attaques complexes et d'outils efficaces pouvant faire coopérer différents systèmes d'intrusions.

Solution apportée

L'architecture du système de détection d'intrusions comprend un nouveau modèle de détection constitué de deux analyseurs indépendants utilisant une nouvelle approche fonctionnelle.

Cette approche est basée sur l'intelligence du **S**ystème **M**ulti-**A**gent (SMA) pour réagir contre les attaques complexes. L'efficacité de cette approche repose sur un analyseur matériel pour analyser les informations et donner le type, le degré d'intrus et la politique utilisée. Aussi l'existence d'un deuxième analyseur soft qui pousse la recherche et renforce le degré de sécurité apportée à la cible surveillée.

Les agents intelligents, répartis sur deux analyseurs, coopèrent et communiquent pour détecter efficacement des attaques suivant des schémas d'attaques définis dans leur base de connaissances. Ainsi la capacité d'intervenir en temps réel pour bloquer, détruire, filtrer et exploiter l'information.

La figure 1 caractérise la plateforme temps réel de sécurité et de détection d'intrusions distribuée à base des systèmes multi-agents. Cette plateforme est caractérisée par deux niveaux d'analyses, le premier est un matériel et le second est un logiciel.

La figure 2 caractérise le fonctionnement de la plateforme par l'indication du passage de l'information entre les différents éléments dans le cas d'une détection d'intrusion.
La figure 3 présente l'Architecture pratique de la plateforme distribuée temps réel de sécurité et de détection d'intrusions.

Revendications

1. L'architecture du système de détection d'intrusions distribuée comprend un nouveau modèle de détection constitué de deux analyseurs indépendants utilisant une nouvelle approche fonctionnelle
2. La plateforme comprend deux parties : matériel et logiciel
3. La plateforme comprenant un automate programmable ou un DSP ou un microcontrôleur ou un FPGA et un serveur à base d'un logiciel fonctionnel distribué.
4. La plateforme comprend n'importe quelles marques des automates, DSP, FPGA, Microcontrôleurs ou des serveurs
5. La plateforme matériel-logiciel est caractérisée par le critère temps réel au niveau collecte d'information, au niveau de l'analyseur matériel pour l'analyse du flux d'information selon le degré de menace, au niveau de l'analyseur logiciel pour approfondir d'une manière intelligente sans perdre l'information l'examen du flux d'information et au niveau du manager pour déclencher les alertes à l'administrateur.
6. La plateforme matériel-logiciel est caractérisée par le critère distribué et multi-agents pour faciliter la maintenance de chaque partie (capteur, analyseur matériel, analyseur logiciel et manager soft) d'une manière indépendante sans perdre le fonctionnement des autres parties.
7. La plateforme matériel-logiciel est caractérisée par le critère de supervision dans les deux niveaux d'une manière indépendante. Ce critère permet l'intervention à n'importe quel moment pour bloquer un intrus dans le cas d'un risque très fort.

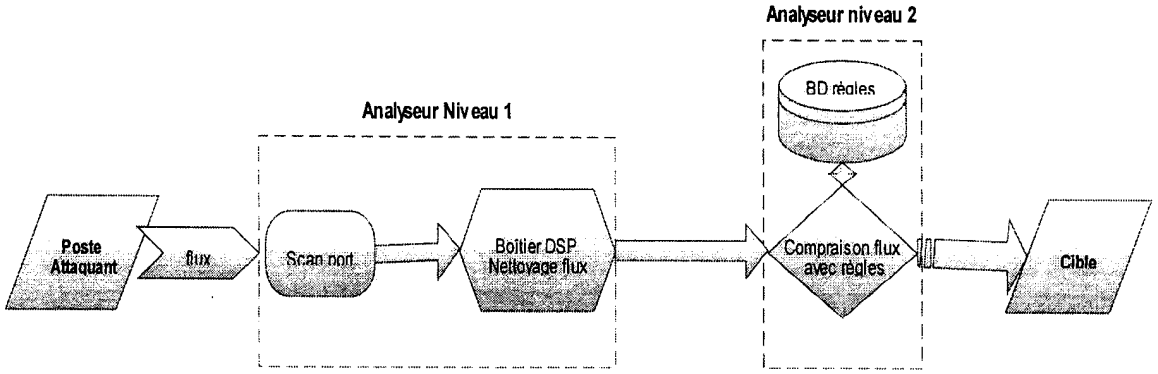

Figure1

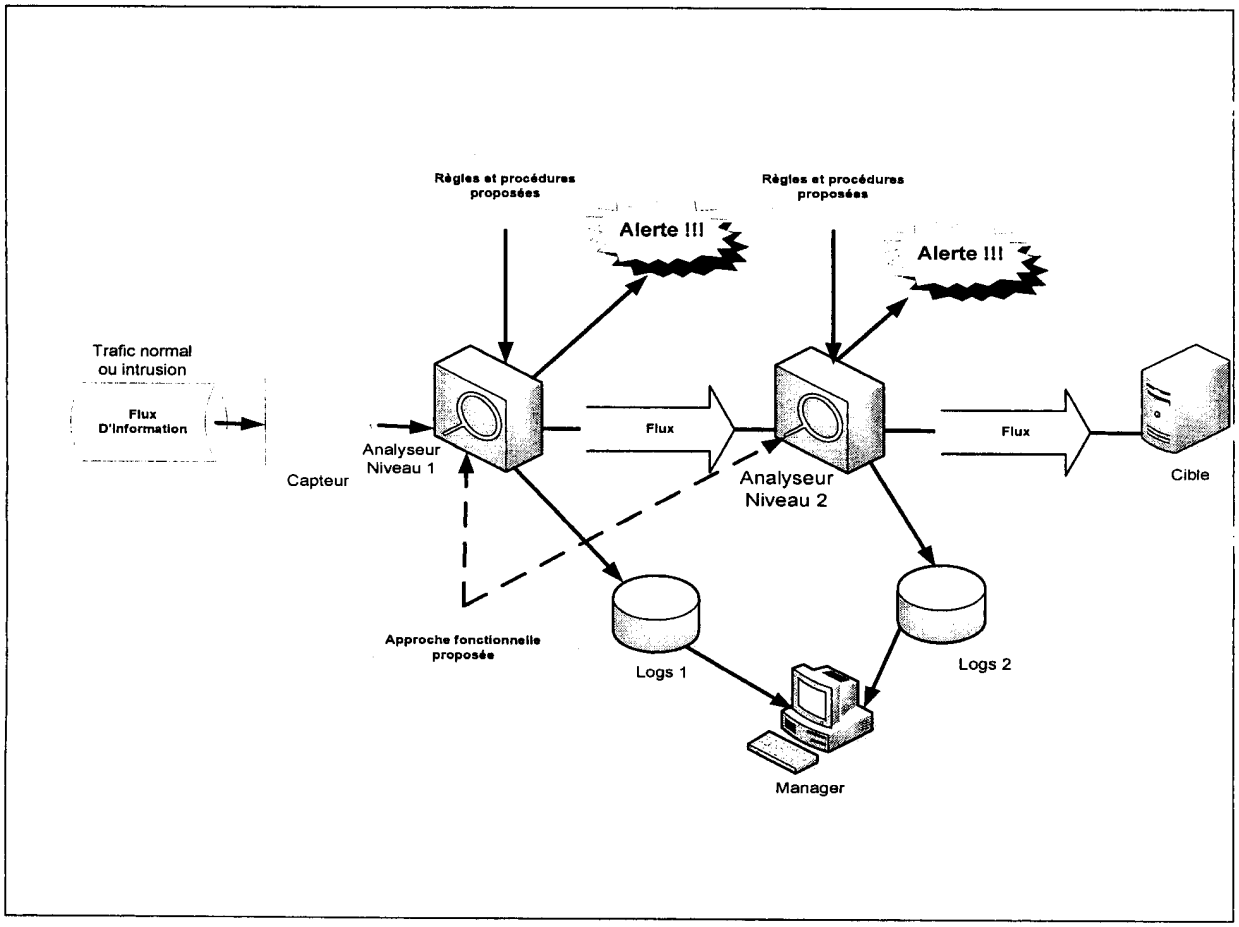

Figure2

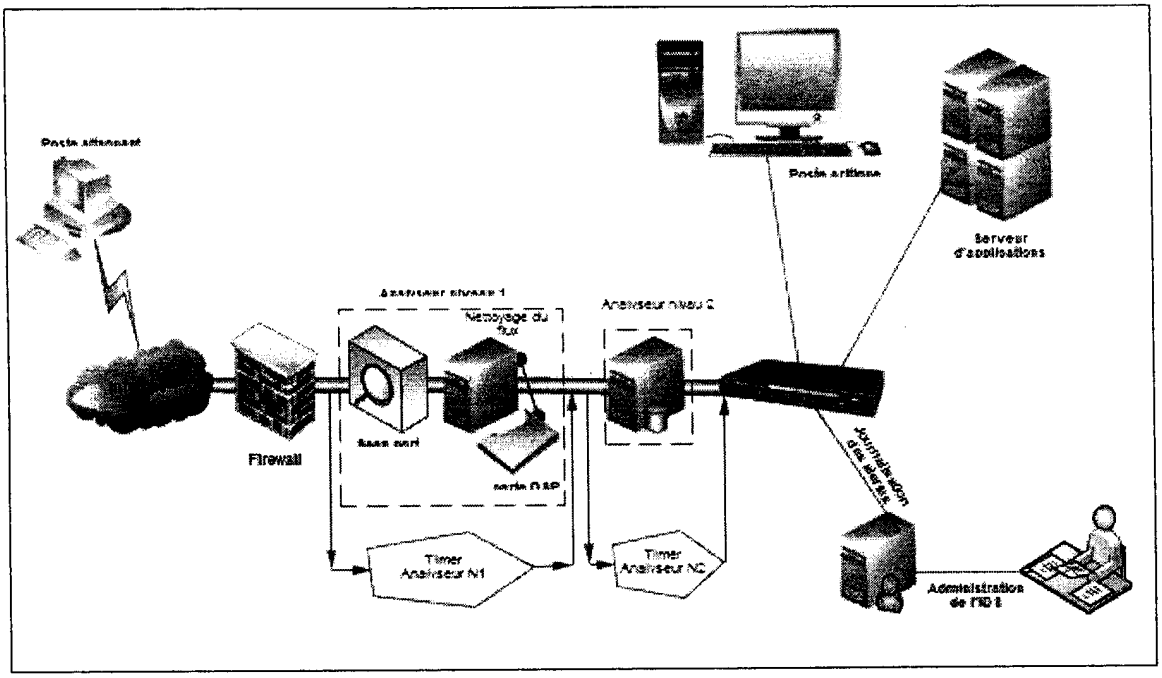
Poste attaquant
Poste victime
Serveur d'applications
Analyseur niveau 1
Nettoyage du flux
Analyseur niveau 2
Firewall
Sans sort
sortie NIDS
Journalisation des alertes
Timer Analyseur N1
Timer Analyseur N2
Administration de l'IDS

Figure3