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 34415 B1

(51) Cl. internationale :
H04L 29/06

(43) Date de publication :
01.08.2013

(21) N° Dépôt :
34481

(22) Date de Dépôt :
22.12.2011

(71) Demandeur(s) :
UNIVERSITE MOHAMMED V-AGDAL, AVENUE DES NATIONS UNIES, AGDAL, RABAT, B.P. 554 RABAT-CHELLAH (MA)

(72) Inventeur(s) :
ALI RADI ; DRISS ABOUTAJEDINE

(74) Mandataire :
Mouloud EL MOUDDANE

(54) Titre : **système de prévention d'intrusion basé sur une politique de sécurité à trois niveaux**

(57) Abrégé : LA SOLUTION PROPOSÉE, DANS LE PRÉSENT DOCUMENT CONSISTE EN LA MISE EN PLACE D'UN SYSTÈME DE PRÈVENTION D'INTRUSION (IPS) BASÈ SUR UNE POLITIQUE DE SECURITÉ À TROIS NIVEAUX. CHAQUE NIVEAU CONTRIBUE À LA FOIS PROTECTION DU SYSTÈME D'INFORMATIONS (SI) DES ATTAQUES INTERNES AINSI QUE DES ATTAQUES EXTERNES, LE PREMIER NIVEAU DE DÉTECTION CONSISTE EN L'UTILISATION D'UN SYSTÈME DE DÉTECTION D'INTRUSIONS AXÉ RÉSEAU (NIDS), LE DEUXIÈME NIVEAU, CONSISTE EN L'IMPLÉMENTATION D'UNE POLITIQUE DE SÉCURITÉ FONCTIONNELLE PERMETTANT AUX USAGERS D'ACCÉDER STRICTEMENT AUX APPLICATIONS ET AUX DONNÉES NÉCESSAIRES VIA DES RÈGLES DE SÉCURITÉS. ENFIN, LE TROISIÈME NIVEAU CONSISTE EN L'IMPLÉMENTATION D'UNE POLITIQUE DE SÉCURITÈ OPÉRATIONNELLE VIA UN MÉCANISME DE CORRÉLATION DE DONNÉES DE LA LISTE DE CONTRÔLE D'ACCÈS PHYSIQUE ET LA LISTE DE CONTRÔLE D'ACCÈS LOGIQUE AUX MACHINES COMPOSANT LE SI.

Système de prévention d'intrusion basé sur une politique de sécurité à trois niveaux

Résumé

La solution proposée, dans le présent document consiste en la mise en place d'un système de prévention d'intrusion (IPS) basé sur une politique de sécurité à trois niveaux.

Chaque niveau contribue à la fois à la protection du système d'informations (SI) des attaques internes ainsi que des attaques externes. Le premier niveau de détection consiste en l'utilisation d'un système de détection d'intrusions axé réseau (NIDS), le deuxième niveau, consiste en l'implémentation d'une politique de sécurité fonctionnelle permettant aux usagers d'accéder strictement aux applications et aux données nécessaires via des règles de sécurités. Enfin, le troisième niveau consiste en l'implémentation d'une politique de sécurité opérationnelle via un mécanisme de corrélation de données de la liste de contrôle d'accès physique et la liste de contrôle d'accès logique aux machines composant le SI.

Système de prévention d'intrusion basé sur une politique de sécurité à trois niveaux

Description

Domaine technique

L'invention concerne la mise en place d'un système permettant l'amélioration de la protection et la détection d'intrusions dans les réseaux informatiques contre les attaques à la fois des utilisateurs non-autorisés (attaques externes) et de celles des utilisateurs autorisés (attaques internes).

Etat de la technique

La conception et la mise en œuvre des IDS restent un enjeu de recherche important pour maintenir la sécurité des réseaux informatiques appropriée. Malgré les progrès indéniables dans le domaine de la sécurité des SI (SSI), il y a encore beaucoup à faire pour l'améliorer. Pour cela, de nombreux mécanismes et systèmes ont été développés pour assurer et améliorer la SSI. Ces systèmes sont vulnérables aux attaques à la fois externes et internes.

Comme résultat et conséquence de la crise économique mondiale, le nombre d'employés insatisfaits ou licenciés augmente considérablement, entraînant ainsi, l'instabilité du marché d'emploi et l'augmentation du taux de chômage à l'échelle mondiale. Certains de ces employés insatisfaits tentent d'abuser des privilèges qu'ils avaient lors de leur période d'activité, et essaient parfois de voler des informations méritant d'être vendues ou pour simplement nuire à la SSI de leur actuel ou ancien établissement. S'ajoute à tout cela, la concurrence acharnée entre les établissements et les sociétés multinationales. De ce fait, plusieurs études réalisées [Mag Securs, Nov 05] ont prouvé que (70%) des attaques des réseaux informatiques, en particulier celles qui causent des dommages très importants, proviennent de l'intérieur des SI. Aussi, la grande vitesse des réseaux actuels étrangle des IDS existants par l'énorme quantité d'événements et alertes générés. Cette vulnérabilité est très utilisée par les attaquants pour réaliser des attaques par dénis de service (DoS; Denis of Service). En plus, les outils

d'attaques sont de plus en plus sophistiqués et disponibles gratuitement sur internet, et même échangés via des forums dédiés aux hackers.

Pour se protéger, des stratégies basées sur différents IDS sont mises en œuvre, à la fois, pour un effet dissuasif et pour mettre fin à l'utilisation abusive et non autorisée du SI. Les approches traditionnelles, se basant sur un profit de comportement normal ou une base de scénarii d'attaques, ont montré leurs insuffisances pour la protection des SI, en particulier, de l'intérieur. Dans les meilleurs cas, elles permettent de sécuriser le réseau uniquement sur son point d'entrée contre les attaques provenant du réseau externe. D'autres systèmes de protection ont été aussi étudiés.

L'invention concernant le brevet FR 2875981 (Butti Laurent, Duffau Roland et Veyesst Franck), a consisté en la proposition d'un système de détection d'usurpation d'adresse réseau par un dispositif de filtrage d'adresse réseau et une vérification du système d'exploitation. De même, concernant le brevet français FR 2596179 (Philippe Blanc), il a été proposé, un IDS dans un local par un dispositif de détection de variation de pression de l'air, applicable à un système d'alarme. Par ailleurs, dans le brevet FR 287648 (Cusin Nicolas, Crevoulin Roland et Badel Christian), il a été proposé, un IDS dans un local par un dispositif transducteur transformant une force en une grandeur électrique mesurable. Dans le brevet FR 2675602 (Larvoire Jean-François, Ribollet Thierry et Hays Bertrans), il a été proposé, un système de protection d'un système informatique comprenant des périphériques via la comparaison d'un mot de passe saisi au moment de la mise sous tension avec un autre prédéfini stocké dans une mémoire non volatile reprogrammable. Dans la publication FR 2842000 (Rodrigo Fernandez et Kodjaba-Chian Jérôme), il a été proposé, un IDS dans un réseau informatique par une analyse du comportement actuel des utilisateurs comparé à celui de référence prédéfini par apprentissage. De même dans le brevet KR 20040109985, il a été proposé, Une méthode pour prévenir automatiquement une attaque ARP/IP spoofing pour réduire les dommages dus à ce type d'attaque et renforcer ainsi la sécurité du réseau informatique par la surveillance des adresses IP attribuées aux hôtes.

La solution technique proposée consiste en la mise en place d'un IPS basé sur une politique de sécurité à trois niveaux via :

- La segmentation du réseau informatique, tenant compte des tâches attribuées aux utilisateurs au sein de l'entreprise, en réseaux locaux virtuels « ou VLAN: Virtuel Local Area Network» et l'utilisation des LCA (listes de contrôle d'accès).
- L'implication des utilisateurs dans la politique sécurité globale.
- Un mécanisme de corrélation de données de la liste de contrôle d'accès physique au locaux de l'entreprise, et la liste de contrôle d'accès logique aux machines composants le SI, appartenant aux utilisateurs exerçants au sein de l'entreprise.

Objet de l'invention

L'invention a pour objet la mise en place d'un IPS basé sur une politique de sécurité à trois niveaux. C'est une approche qui peut être implémentée pour les SI simples ou complexes,

dans laquelle chaque niveau contribue à la fois à la protection du SI des attaques internes ainsi que des attaques externes.

Cette politique globale de sécurité permettra, aussi, aux administrateurs et aux responsables de la SSI (RSSI) non seulement de détecter les attaques, mais de les avertir des intrusions en cours et interdire l'accès à l'ensemble des réseaux au cas où une partie du SI a été déjà contaminée. Donc, des actions proactives seront possibles dans notre approche, ce qui n'est pas le cas avec la majorité des IDS, énoncés auparavant.

Description de l'invention

La mise en œuvre des IDS reste un enjeu de recherche important pour maintenir la sécurité des réseaux informatiques appropriés. Malgré les progrès indéniables dans le domaine de la SSI, il y a encore beaucoup à faire pour améliorer la sécurité de ces systèmes aujourd'hui. Pour cela, de nombreux mécanismes et systèmes ont été développés pour assurer et améliorer la SSI. Ces systèmes sont vulnérables aux attaques à la fois des utilisateurs non-autorisés (attaques externes) ainsi que des attaques des utilisateurs autorisés (attaques d'internes) qui abusent des privilèges qui leurs sont octroyés. D'où l'importance de la mise en place de ce nouvel IPS.

Le premier niveau de détection consiste en l'utilisation d'un NIDS. Ce système sera capable de détecter des intrusions à la base de scénarii d'attaques et sera placé à l'entrée du réseau. Ce niveau à pour objectif principal de protéger le réseau interne des attaquants externes, par la détection des tentatives de connexion malicieuses de parties tierces non autorisées situées à l'extérieur du réseau. La base de scénarii des attaques sera améliorée et mise à jour grâce aux niveaux 2 et 3 du système que nous proposons.

Le deuxième niveau de détection consiste en l'implémentation d'une politique de sécurité fonctionnelle tenant compte des tâches attribuées aux utilisateurs du département par la segmentation du réseau en VLAN et l'utilisation des LCA. Ainsi, les machines des utilisateurs seront configurées dans le même VLAN. De même pour les machines Gateway des différents VLANs, elles seront configurées avec des LCA définissant la liste des actions autorisées pour les utilisateurs appartenant au VLAN ou par la liste des actions interdites pour ce "sous-ensemble" d'utilisateurs. Aussi, l'utilisation des VLAN, vu leur fonction de blocage des broadcasts, permettent au pire des cas, si l'attaquant a réussi à prendre le contrôle sur une machine appartenant à un VLAN (tel que : lancement de virus, vert, ...), de la restreindre à ce petit segment du réseau (VLAN) et ne pas contaminer l'ensemble du réseau tout entier.

Ce niveau sert à protéger le réseau des attaquants internes qui peuvent abuser des droits et privilèges qui leur sont octroyés durant leur période d'activité. En plus, ce niveau va servir pour protéger aussi le réseau interne des attaquants externes qui réussissent à s'infiltrer au réseau informatique par usurpation. Même s'ils arrivent à prendre le contrôle sur une machine d'un sous-réseau, au pire des cas, leurs attaques ne dépasseront nullement ce sous-réseau auquel appartient cette machine, le cas échéant, ces actions intrusives seront confrontées aux LCA et seront ainsi détectées par l'administrateur du SI.

Cette configuration permet à l'administrateur du réseau informatique d'enregistrer toutes ou une partie des actions intrusives effectuées sur le SI par chaque utilisateur ou groupe d'utilisateurs, qu'elles soient internes ou externes. L'administrateur peut aussi, via des scripts implémentés, être alerté à distance sur différents types de terminaux. L'analyse ultérieure des événements enregistrés dans des journaux d'événements « log » permettra de détecter l'origine de l'attaque à l'aide de la méthode de reconstruction des événements, afin de savoir ce qui s'est exactement passé, et mettre en œuvre des contre-mesures adéquates pour ce nouveau type d'attaques et, par la suite, mettre à jour la base des scénarii d'attaques de notre NIDS implémenté pour le premier niveau. Aussi, et afin d'impliquer les utilisateurs dans la politique de sécurité interne, on peut leur offrir, une marge de techniques et paramètres spécifiques de protection à exécuter localement et à leur demande.

Les figures 1 et 2, illustrent la structure d'un réseau composé de trois domaines de broadcast distincts (03 VLAN) créés par 02 commutateurs et un routeur.

Le routeur achemine le trafic entre les VLANs à l'aide du routage de la couche 3 et contrôle l'accès aux VLANs. Ce qui apporte plus de sécurité et améliore la gestion du réseau.

D'après la figure-2, représentant la structure en couches de notre système, si la station de travail B3 du VLAN n°3 veut envoyer des trames de trafic à la station de travail B2 du VLAN n°2, (simulation de cas de collaborateurs travaillant dans des départements différents) celles-ci sont envoyées à l'adresse MAC de l'interface Fa0/0 du routeur qui vérifie les droits d'accès de la station de travail B3 du VLAN n°3, si elle est autorisée, le routage est effectué via l'adresse IP (@IP3) sur l'interface de routeur Fa0/0 pour le VLAN n°3. Dans le cas contraire, la requête sera rejetée.

Par contre, si la station de travail A1 du VLAN n°1 souhaite envoyer des données à la station de travail B1 du même VLAN n°1 (simulation de cas de collaborateurs travaillant au sein du même département), l'adresse MAC de destination de la trame est l'adresse MAC de la station de travail B1, et la transmission se fait sans passage via le routeur.

Les LCA doivent être configurées sur les routeurs périphériques situés aux frontières du réseau pour tirer le plus parti de leurs avantages en matière de sécurité. Cela permettra de fournir une protection de base contre le réseau externe, les utilisateurs externes et contre les utilisateurs internes qui abusent parfois des privilèges qui leurs sont octroyés ou de mettre à l'abri une zone plus privée du réseau d'une zone moins contrôlée.

Le troisième niveau de détection désigné « politique de sécurité opérationnelle » consiste en la définition d'une politique de sécurité opérationnelle via un mécanisme de corrélation de données de la liste de contrôle d'accès physique et la liste de contrôle d'accès logique aux machines composants le système d'informations. C'est-à-dire, ne permettre l'accès au réseau informatique qu'aux utilisateurs qui sont réellement opérationnels au sein de l'établissement. Ce contrôle a pour but principal de limiter l'usurpation d'identité de l'intérieur ou de l'extérieur de l'établissement sur les machines du SI.

Ce niveau de détection d'intrusions, en interaction avec les deux niveaux précités, permet de détecter automatiquement les violations de la politique de sécurité globale du SI, au lieu de se contenter seulement d'une base de scénarii d'attaques ou de profils empiriques. L'analyse

du comportement du SI dans cette approche permet de connaître le trafic anormal d'une machine sur le réseau informatique.

La détection de ce genre d'attaques est alors automatiquement réalisée et des contre-mesures peuvent être paramétrées (blocage du trafic en provenance ou vers la machine victime, ou carrément l'isolement total de cette machine victime) ce qui améliore les performances de notre IDS en se transformant en un IPS. Ainsi, l'analyse des fichiers « log » permettra de comprendre comment l'intrus à pu pénétrer dans le SI et la modélisation de ce scénario servira, par la suite, à la mise à jour de la base des scénarii utilisée au premier niveau de détection de notre système global.

La plupart des outils de détection d'intrusions sont passifs lorsqu'ils détectent des attaques. Dans les meilleurs des cas, les alertes sont générées et exigent de l'administrateur du réseau informatique de les analyser manuellement, s'il le peut, et prendre les décisions appropriées. Par conséquent, il peut y avoir un retard important dans le processus de traitement d'une intrusion durant lequel l'attaquant, s'il y a lieu, a déjà obtenu les informations souhaitées ou détérioré les équipements ciblés, et ceci avant que l'administrateur du réseau informatique ne s'en rende compte.

Pour bénéficier d'une protection efficace, une action immédiate est nécessaire pour minimiser la marge d'exploitation d'une vulnérabilité et réduire le temps d'exposition du SI à une attaque, de même pour minimiser les dégâts et les coûts associés.

Dans le cas de notre système, un certain nombre de fonctionnalités proactives peuvent être mises en œuvre. Par exemple, modifier les autorisations d'accès à des fichiers, arrêter un processus, couper une connexion au réseau et ajouter ou modifier les règles de protection d'un pare-feu.

Les figures-3 & 4 résument les étapes importantes de notre système IPS. Les événements générés des trois niveaux seront regroupés, filtrés et corrélés afin de réduire leur volume et faciliter ainsi l'analyse et l'optimisation du temps de traitement à la recherche des intrusions.

Dans le cas d'une intrusion provenant du niveau-2 ou du niveau-3, l'administrateur du SI peut, à travers un diagnostic détaillé des événements agrégés, savoir comment les événements se sont exactement passés. Ce qui permettra à l'administrateur du SI:

- D'avoir une meilleure compréhension des besoins du SI,
- D'identifier les faiblesses du SI et améliorer les politiques de sécurité appliquées,
- De prévenir l'abus de ces vulnérabilités par des attaquants internes ou externes du SI,
- De mettre à jour la base de connaissances des scénarii d'attaques au niveau-1,
- D'être capable de résoudre, totalement ou partiellement, le problème des faux positifs et des faux négatifs.
- De réduire le nombre d'alertes et accélérer le traitement,
- D'améliorer en permanence les performances du système.

Comme le montre le diagramme de la figure-5, lorsque le paquet de trafic arrive, il passe en premier lieu à travers le premier niveau, où on a implémenté un NIDS. Le paquet sera confronté à la base des scénarii d'attaques. Si le paquet est un intrusion, et son scénario est

inclus dans la base des scénarii de notre NIDS, le paquet sera rejeté. S'il n'existe pas dans la base des scénarii, il passe pour le deuxième niveau où on vérifie le type de service demandé par l'utilisateur, s'il est autorisé ou pas. Si cet utilisateur n'a pas le droit d'accéder aux services et/ou ressources demandés, la demande sera rejetée et l'administrateur du réseau informatique sera notifié par une alerte pour lancer les diagnostics nécessaires. S'il a le droit le paquet passe pour le troisième niveau. Dans ce 3ème niveau, on vérifie si l'utilisateur est présent dans l'établissement ou pas. Si oui, l'utilisateur aura un accès complet, s'il est absent, et s'il n'a pas le droit d'accéder à distance, le paquet sera rejeté et l'administrateur du réseau informatique sera notifié par une alerte pour lancer les diagnostics nécessaires. L'analyse de ce genre de paquets intrusifs permet à l'administrateur du réseau informatique de déterminer l'origine et le chemin de l'attaque afin de savoir ce qui s'est exactement passé, pour mettre en œuvre des contre-mesures adéquates pour ce nouveau type d'attaque et par la suite, mettre à jour la base des scénarii d'attaques de notre système NIDS dans le premier niveau.

Les résultats expérimentaux concernent la validation de notre nouvelle approche, sont regroupés dans les tableaux 1à 3. Ils ont été obtenus par application de la Méthode des Séparateurs à Vaste Marge (SVM) couplée avec la technique validation croisée (CV) sur un échantillon de données trafic de la base KDD99 (KDD: Knowledge Discovery in Database), développée par le laboratoire Lincoln de l'institut de technologie du Massachusetts et qui est utilisée pour validation des IDS. Nos résultats sont comparés avec d'autres approches publiées dans la littérature [Bouzida, 06] utilisant la même base des données trafic KDD99.

Les chiffres présentés dans les tableaux sus-indiqués sont extraits des matrices de confusion fournies par l'outil WEKA après chaque lancement de l'application. La précision de chaque expérience est basée sur le PICC «pourcentage des instances correctement classifiées ou prédites sur l'ensemble de données de test».

Le troisième niveau de détection d'intrusion consiste en la définition d'un système de politique de sécurité opérationnelle, à savoir refuser l'accès au réseau informatique aux utilisateurs qui ne sont pas réellement opérationnels au sein de l'établissement. En général, un intrus qui veut voler des informations dans un SI, tentera de réussir un accès à distance sur l'un des hôtes dont l'utilisateur est absent. Ainsi, il utilisera des attaques de la catégorie U2R (user to root) et R2L (remote to local). Par conséquent, pour simuler ce niveau, nous avons fusionné les deux classes d'attaques U2R et R2L, de la base KDD99, dans une seule classe que nous avons appelé « Abs », faisant référence à « l'utilisateur absent ». Ainsi, dans nos expériences, à l'étape « D » nous avons utilisé seulement quatre catégories de classes (Normal, Probing, DOS, et ABS) au lieu de cinq catégories de classes utilisées à l'étape « C » (tableaux 1&2).

Mode de Test	Nombre des attributs d'entrée pour sélection	% des Instances Correctement Classifiées	Nombre des attributs sélectionnés	% de réduction en attributs
B- Sélection des attributs pertinent à partir de 23 Classes & 41 attributs	41	100%	14	66
C- Sélection des attributs pertinent à partir de 5 Classes & 41 attributs	41	100%	6	85
D- Sélection des attributs pertinent à partir de 4 Classes & 41 attributs	41	100%	6	85

Tableau 1: Résumé des résultats de sélection des attributs par la méthode CV dans SVM

Mode de Test	Nombre des attributs d'entrée sélectionnés	Temps mis pour la construction du modèle (s)	% des Instances Correctement Classifiées	% de réduction en attributs	% de réduction en temps
A- Modèle de classification à partir de 23 Classes & 41 attributs	41	16,72	93,68%	-	-
B- Modèle de classification à partir de 23 Classes & 14 attributs	14	15,61	93,28%	66	7
C- Modèle de classification à partir de 5 Classes & 06 attributs	6	2,31	98,78%	85	85
D- Modèle de classification à partir de 04 Classes & 06 attributs	6	1,91	97,84%	85	88

Tableau 2: Résultat de classification par la méthode CV dans SVM

Prédite / Actuel	% Normal	% DoS	% Probing	% Abs
normal	99,11	0,89	0,00	0,00
dos	0,16	99,76	0,08	0,00
probe	4,41	1,76	92,65	1,18
Abs	43,23	0,00	0,00	56,77
PICC=97,86%				

Tableau 3: Matrice de confusion relative notre approche

Le tableau 4 illustre une comparaison des résultats relatifs à notre approche avec d'autres existant dans la littérature et ayant utilisé la méthode PCA (analyse en composantes principales) combinée aux arbres de décision à travers l'algorithme C4.5, puis aux réseaux de neurones.

L'analyse de ces résultats, montre clairement que notre approche a apporté une bonne amélioration de la performance des résultats, soit sur le PICC, soit sur la prédiction des différentes catégories des classes d'attaques, en particulier les deux dernières classes U2R (7,02%) et R2L (2,85%), alors que le taux de notre nouvelle classe Abs (qui est une fusion des deux classes) est de 61,54%. Aussi, le taux de faux négatifs de cette classe diminue considérablement en passant de 21, 93% à 2,12% et le PICC est passé de 92,87% à 97, 86%.

classes / Algorithmes & approches	% Normal	% Probing	% DoS	% U2R	% R2L	% PICC
Approche NN sans PCA	99.50	72.01	97.01	6.60	1.21	92,05
Approche NN & PCA	99,5	74.40	97.14	7.91	0.80	92,22
Approche C4.5 sans PCA	99,42	78.80	96.96	5.26	5.27	92,35
Approche C4.5 & PCA	98.99	66.30	97.25	8.33	2.30	92,16
Approche C4.5 amélioré & PCA	99.43	72.73	97.14	7.02	2.85	92.87
Approche d'IPS à trois niveaux	99,11	99,76	92,65	Abs=56,77		97,86

Tableau -4: Résultats expérimentaux des différentes approches

REVENDICATIONS

1. Système de prévention d'intrusion basé sur une politique de sécurité comprenant trois niveaux, le niveau 1 implémente une politique de sécurité externe, le niveau 2 implémente une sécurité fonctionnelle et le niveau 3 implémente une sécurité opérationnelle.
2. Système de prévention selon la revendication 1 caractérisé en ce que le niveau 1 utilise NIDS permettant la protection du réseau des attaques externes et dont la base des scénarii est mise à jour.
3. Système de prévention selon la revendication 1 caractérisé le niveau 2 utilise une segmentation en VLAN en fonction des tâches attribuées aux utilisateurs.
4. Système de prévention selon la revendication 1 caractérisé en ce que le niveau 3 implémente un système de corrélation entre la liste d'accès physique et la liste d'accès logique.
5. Système de prévention selon les revendications 1 à 4 caractérisé en ce que la base des scénarii du système NIDS sera mise à jour à travers les nouvelles attaques détectées par les niveaux 2 et 3.

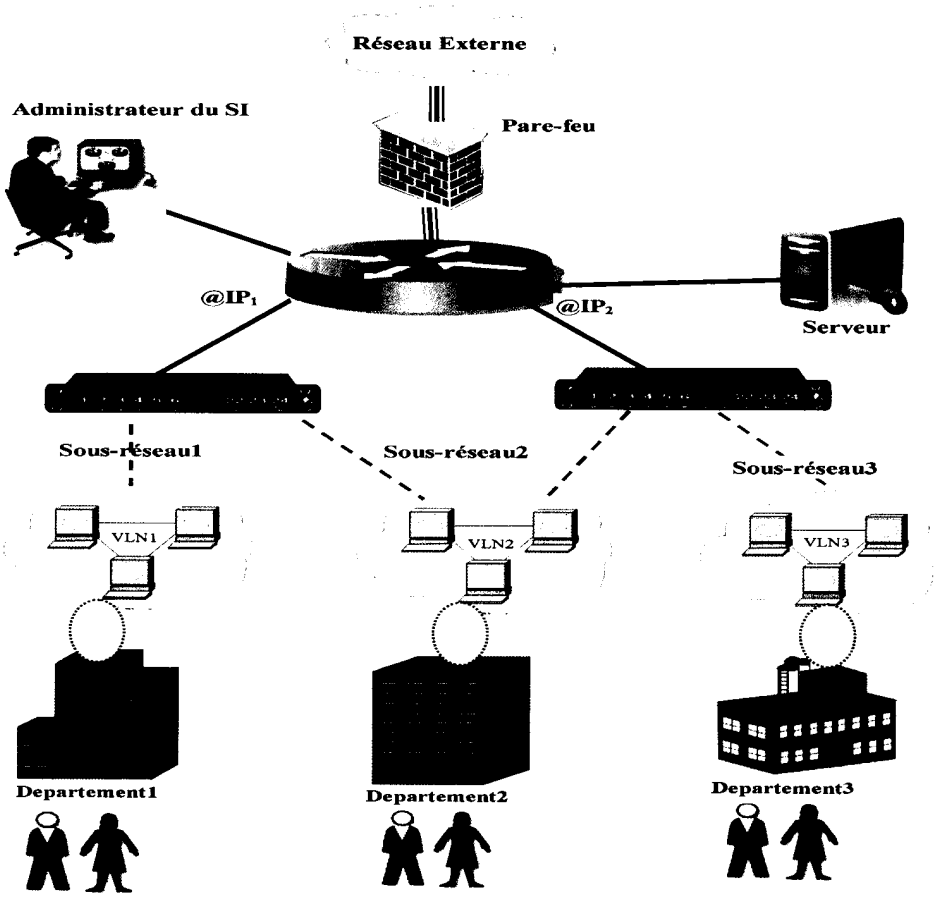

Figure 1: Architecture de réseau avec 03 VLAN en utilisant 2 commutateurs un routeur

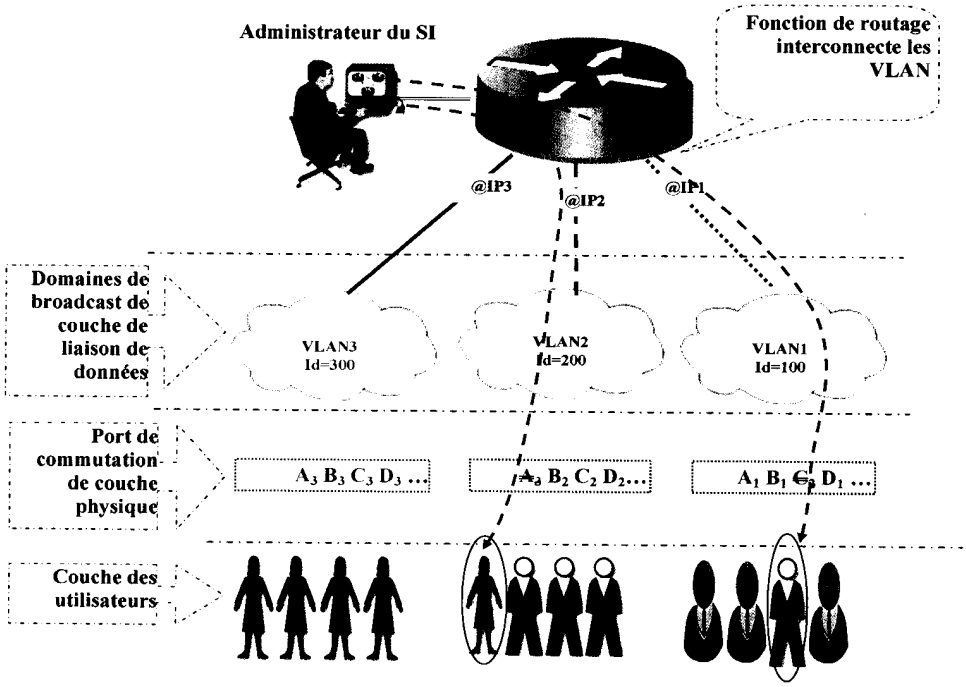

Figure-2: Structure en couches de l'architecture d'un réseau avec des VLAN

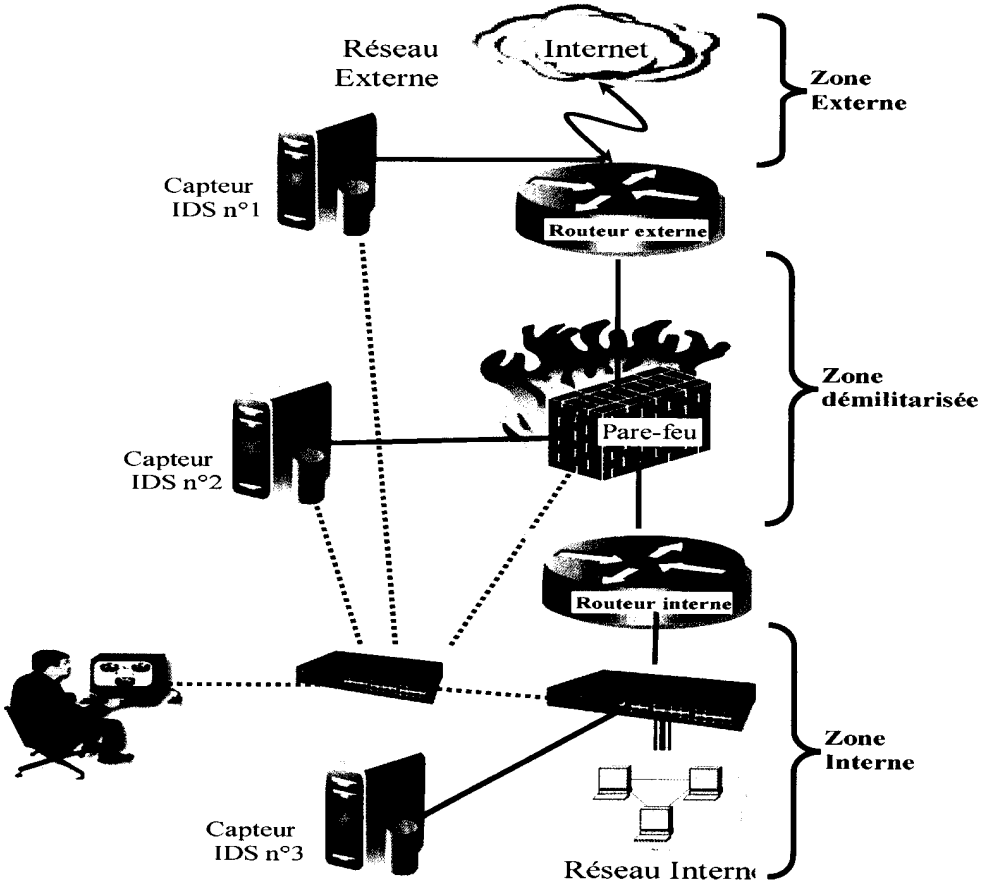

Figure-3: Architecture d'un système IPS à trois Niveaux

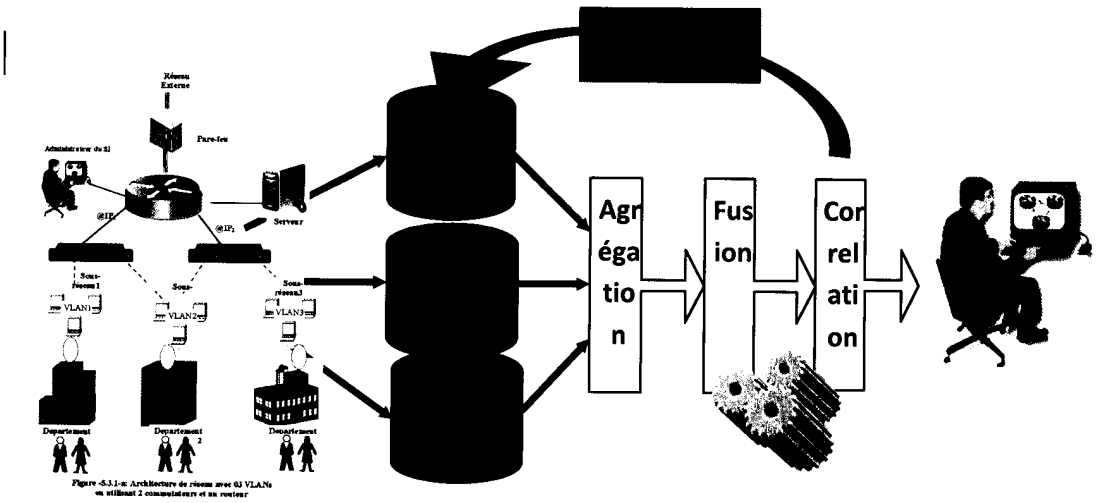

Figure-4: Architecture fonctionnelle d'un système IPS à trois Niveaux

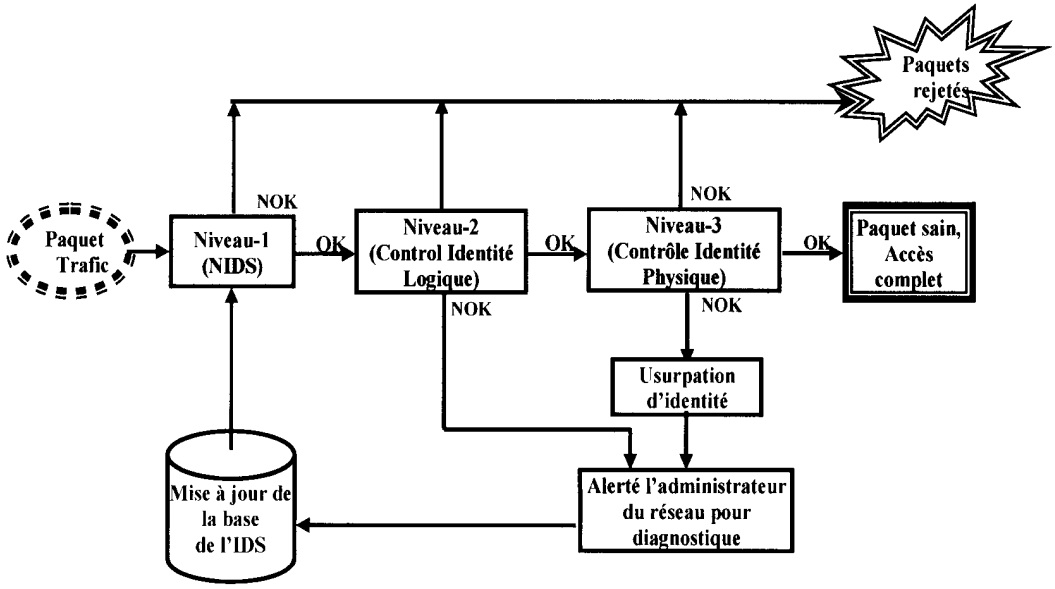

Figure-5: Diagramme de notre IPS basé sur une politique de sécurité à trois niveaux