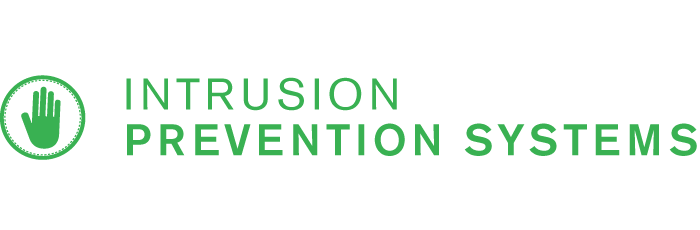


DESZCZ Sébastien

DURAK Thomas

MEURILLON Grégoire

STALTER Marianne



**Années 2013-2014**

**B3**

Projet de Veille Technologique

Sujet : IPS Appliance

Synthèse

Dans un monde de plus en plus informatisé et connecté, l’IPS devient indispensable pour tout système informatique. En effet, devant la prolifération des virus informatiques et des hackers, il convient de protéger toutes les informations sensibles d’une structure, d’autant plus lorsqu’il s’agit d’une entreprise.

L’outil présenté dans ce document s’appelle IPS (« Intrusion Prevention System »).

Il permet à un utilisateur de contrôler tous les flux réseaux d’un système informatique. En cas d’actions anormales sur le réseau, l’IPS en informe l’utilisateur. Il peut tout aussi bien nettoyer le problème, s’il s’agit de logiciels malveillants.

Mots clés : système, informatique, sécurité, prévention, alerte, quarantaine, intrusions, hackers, virus, nettoyage.

Préambule

De notre sujet, nous y en avons retiré une problématique, qui est la suivante :

**L'IPS : LA solution pour lutter contre les menaces venant d'Internet ?**

De ce fait, on évoque tous les sujets importants : les acteurs du marché, ainsi que la technologie, en abordant aussi bien les points positifs que les points négatifs. Le terme « LA » a été choisi pour couvrir l’étude des parts de marché et l’implantation du logiciel.

En effet, on suppose dans cette problématique que l’IPS serait la meilleure solution pour répondre aux besoins des entreprises, notamment à la vue des statistiques concernant l’usage de l’IPS dans le monde.

Le guide de lecture suivant aidera le lecteur à se repérer dans le document :

|  |  |
| --- | --- |
| Le pictogramme ci-après… | …fait référence à : |
| http://thumbs.dreamstime.com/m/bulb-vector-illustration-icon-36622935.jpg | Une remarque |
| http://the.pmol.free.fr/kraland/pictogrammes/jeuxoccupations/loupe.gif | Une annexe |
|  |  |
|  |  |
|  |  |

Sommaire

Sommaire

1. Présentation
   1. Présentation du groupe
   2. Gantt
2. Technologie de l’IPS

Dans cette partie, nous expliquerons les différentes technologies liées à l’IPS. Comme énoncé précédemment, il existe différentes sortes d’IPS, positionnées à différents endroits d’un réseau.

Chacune de ces technologies a des propriétés bien spécifiques. De même, chacun d’entre elles possède des avantages, comme des inconvénients. De ce fait, nous parlerons d’abord de l’IPS en général. Puis, nous évoquerons les trois types d’IPS, qui sont le NIPS, l’HIPS et le KIPS.

* 1. IPS Appliance
     1. Définition

IPS signifie « Intrusion Prevention System ». Il s’agit d’un outil basé sur la sécurité des systèmes d’information. Il s’inspire en fait de la technologie IDS. Cependant il est bien plus actif que cette dernière.

Il est dédié à une tâche de sécurité spécifique qu'est le blocage des trafics malicieux. Il agit principalement dans les couches supérieures du modèle OSI (Transport, Session, Présentation, Application).

Les types de protocoles surveillés par les solutions d'IPS peuvent être de différentes natures : réseaux (IP, TCP, UDP, ICMP, MPLS...) ou encore systèmes et applicatifs (HTTP, MIME, FTP, DHCP...).



Retrouvez la signification de ces acronymes dans le glossaire.

Ils existent donc 3 types d’IPS différents :

* Les NIPS/WIPS (« Network/Wireless Intrusion Prevention System ») qui surveillent le trafic réseau. En cas de doute, ils peuvent mettre fin à une session TCP.
* Les HIPS (Host-based Intrusion Prevention System) qui permettent de surveiller le poste de travail. Ils surveillent le processus, les driver, les .dll et en cas de détection de processus suspect, ils peuvent le détruire.
* Les KIPS (Kernel Intrusion Prevention System) qui détectent les tentatives d’intrusion au niveau du noyau de l’ordinateur.

Les IPS Appliance sont des solutions de sécurité qui réunissent pare-feu, réseaux privés et toutes les fonctionnalités de prévention des intrusions et de sécurité web.

Les IPS bloquent les menaces avant qu’elles ne pénètrent sur le réseau et endommagent les activités de l’entreprise.

Ils bloquent les visiteurs indésirables et permettent aux flux de l’entreprise de circuler. Ils prennent aussi en charge une DMZ pour héberger les serveurs importants. Ils garantissent de ce fait la sécurité du réseau interne de l’entreprise.

De même, ils permettent de contrôler l’accès aux ressources du réseau (protection des données et optimisation du temps de disponibilité du réseau). Les IPS permettent aussi d’accroitre la productivité des employés tout en sécurisant et en contrôlant l’accès au web (blocage des courriers indésirables, du phishing, des intrusions, des virus, etc...).

* + 1. Fonctionnement

L’IPS analyse les trames dans leur ensemble et non pas une par une. Il possède par ailleurs une base de connaissances sur les attaques connues. Cela permet, grâce à cette base, de voir si les combinaisons de trames reçues peuvent être identifiées comme une tentative d’intrusion.

L’analyse de la trame est complexe. En effet, elle s’effectue à l’issue d’une analyse primaire des données : la « remontée d’informations ». Ces informations sont ensuite analysées par le SIM (Security Information Management), qui les confronte à sa base de connaissances et génère une alerte ou non.

Ce type de fonctionnement est bien différent de celui de l’IDS (Intrusion Detection System). Ce dernier fonctionne en mode promiscuité : il réceptionne une copie du trafic, mais sans l’influencer.

Au contraire, l’IPS fonctionne en mode coupure de port : il ne va pas juste recenser les problèmes, mais il va les bloquer en empêchant le trafic de circuler. L’IPS ne va donc pas juste détecter le problème mais il va aussi le supprimer.

De plus, l’IPS va garder en mémoire l’évènement afin de pouvoir s’occuper de cette intrusion plus facilement par la suite.

* + 1. Avantages

Globalement, l’IPS présente des avantages non négligeables, qui pourraient pousser une entreprise à s’orienter vers ces solutions :

* Forte protection contre les attaques/intrusions : le sniffing, l’ip spoofing, le DoS, les virus/vers ;



Voir annexe « Les attaques »

* Meilleur sécurité ;
* Réduction des coûts informatique (moins d’assistance informatique) ;
* Facilité d’utilisation.

L’utilisation d’un IPS est si rentable que de nos jours, de plus en plus de particuliers désirent en posséder chez eux. [IPSHOME]

* + 1. Inconvénients

Comme toute technologie, il existe bien évidemment des inconvénients. On en dénombre trois principaux :

* Risque de faux positifs : l’IPS peut bloquer des applications ou des trafics légitimes ;
* Il est peu discret : il est donc facilement découvert lors d’une attaque ;
* Les bases de connaissance sur lesquels s’appuient les IPS sont parfois incomplètes.

Heureusement, pour palier à ce dernier inconvénient, on peut rappeler que l’IPS garde en mémoire les attaques qu’il a reçues. Connecté à Internet, il peut automatiquement les rajouter dans la base de connaissances.

* 1. NIPS
     1. Définition

NIPS signifie « Network Intrusion Prevention System ».

Cette forme d’IPS permet de scanner en permanence un réseau et d’en détecter tout comportement suspect. Ainsi, il est possible d’interdire, à une machine l’accès à un service du réseau si elle présente un comportement anormal.

Par ailleurs, cet outil permet aux administrateurs de vérifier l’état de leur réseau et de vérifier qu’il fonctionne normalement. C’est en général ainsi qu’est utilisé le NIPS. On appelle alors cela un NIDS, qui ne permet que la supervision et l’enregistrement des actions et non l’application de règles.

* + 1. Fonctionnement

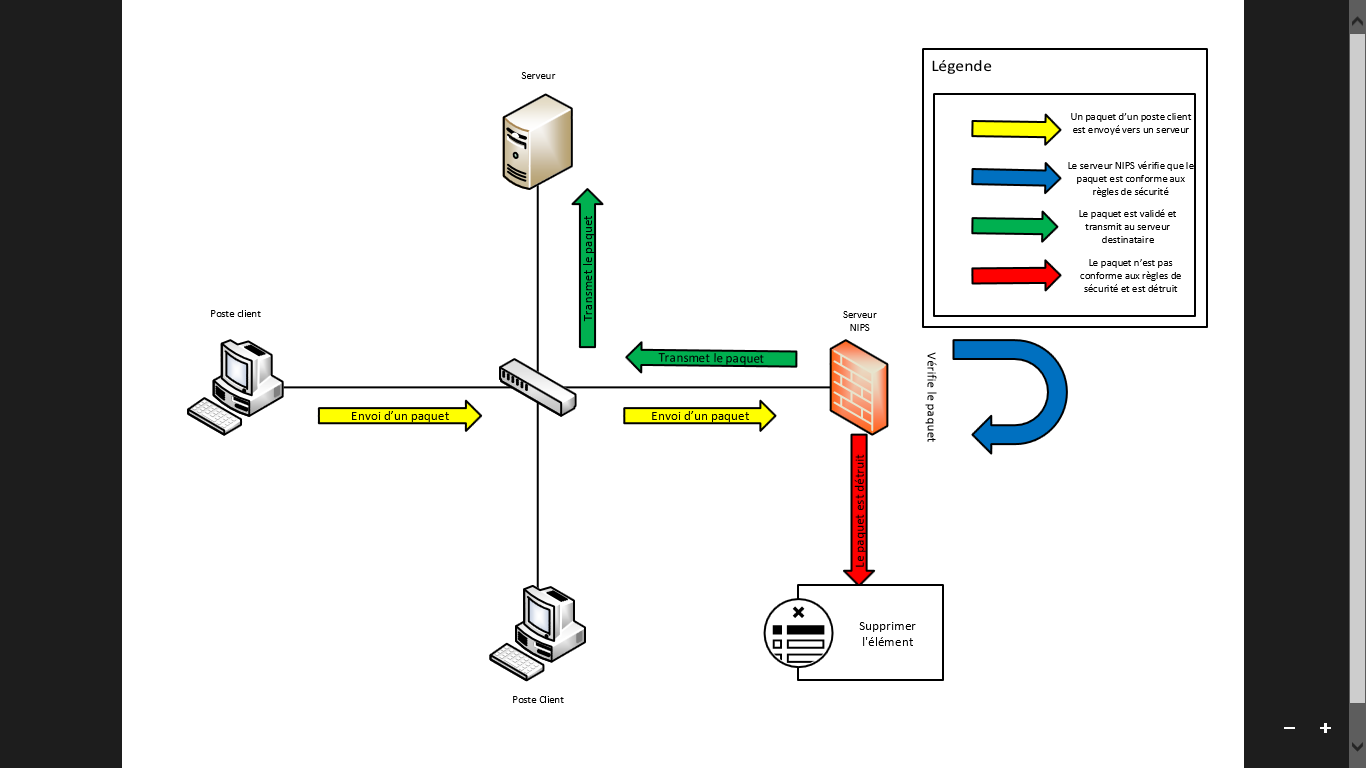
Le NIPS agit au niveau du réseau et vérifie que chaque paquet correspond bien à la politique de sécurité mise en vigueur sur réseau. Puis, si un ou plusieurs d’entre eux ne sont pas conformes, le système NIPS va alors bloquer la source et envoyer une alerte à l’administrateur.

Comment ça marche ?

1. Un appareil quelconque envoie des paquets. En général, il viendra d’Internet. Mais attention, une menace peut aussi venir du réseau interne ;
2. Le NIPS intercepte les paquets ;
3. Le NIPS analyse les paquets ;
4. Le NIPS vérifie la conformité des paquets (tailles, nombre, destination, …) dans sa base de règles ;

Puis, 2 possibilités :

A) Le paquet est validé et continue sa route.

B) Le paquet est refusé et on coupe les accès au réseau de l’appareil responsable, en fonction des règles mise en place. Si l’ordinateur est en interne, le NIPS peut aller jusqu’à directement l’éteindre.

* + 1. Avantages

Nous pouvons observer un certain nombre de points forts pour ce système :

* Détection et blocage les intrusions ;
* Envoi d’alertes ;
* Possibilités de configurations sont très nombreuses et variées ;
* Analyse des paquets et enregistrement.
  + 1. Inconvénients

Mais cette sécurité n’offre pas que des bienfaits pour le réseau. On retrouve les mêmes inconvénients que dans le chapitre « IPS Appliance » :

* Possibilité de faux-positif ;
* Très complexe à configurer ;
* Possibilité de ralentir le réseau ;
* La fiabilité n’est pas de 100% ;
* Il faut une machine dédiée à ce service, car il y a énormément d’informations à traiter.
  1. HIPS
     1. Définition

HIPS signifie « Host-based Intrusion Prevention System »/

Contrairement au simple IPS qui agit au niveau du réseau et sous réseau, l’HIPS agit directement au niveau du poste de travail de chaque utilisateur.

Il s’agit en fait d’une sorte de firewall croisé avec un anti-virus. En effet, son rôle est de contrôler les actions de l’utilisateur, lorsqu’il clique sur un lien, lorsqu’il essaye d’ouvrir un logiciel, …

Attention, le mot « firewall » est à nuancer. Un firewall n’est pas nécessairement un HIPS. En effet, le principe du firewall repose sur le blocage des ports TCP/IP. En revanche, un HIPS est capable de détecter tous types de menaces et, contrairement au firewall, il peut aussi bien le détecter avant qu’il n’arrive dans l’ordinateur, qu’au moment où il est déjà bien ancré dedans.

* + 1. Fonctionnement

Le fonctionnement de l’HIPS est similaire à celui du NIPS.

Pareillement, il possède une base de connaissances des intrusions. Lorsque l’utilisateur parcourt Internet, consulte ses mails, installe un logiciel…. Il y a de fortes probabilités qu’un virus/cheval de troie/spyware(cf glossaire) tente d’accéder à l’ordinateur.

Un antivirus classique va alerter l’administrateur, et éventuellement supprimer/mettre en quarantaine le fichier. Il arrive tout de fois que l’antivirus ne détecte pas la menace.

L’HIPS, lui, va aussi détecter et supprimer la menace. En revanche, il peut aussi demander à bloquer automatiquement tous les flux venant de l’adresse IP fautive.

Dès lors que l’action est considérée comme étant suspecte, l’HIPS ouvre une fenêtre d’alerte en signalant un danger potentiel. Libre à l’utilisateur de poursuivre son action ou non.

* + 1. Avantages
* Le logiciel ne requiert aucune mise à jour régulière, dans la mesure où il calcule des valeurs de danger en fonction du trafic, qui devient inhabituel : en fonction de ce qu’il « connait », il va tout de suite suspecter quelque chose.
* Il n’a pas besoin de connaitre les virus précisément, il lui suffit de détecter qu’un paquet inhabituel tente d’accéder au PC.
* Il fait office d’outil de supervision, qui permet de consulter les informations d’activité et d’état de l’HIPS (à jour, …)
  + 1. Inconvénients
* L’utilisateur peut se trouver envahi par les alertes. L’HIPS étant très complexe, le nombre d’alertes est largement supérieur à celui proposé par un Firewall. Ce dernier est prévu pour protéger l’ordinateur, sans pour autant faire couler l’utilisateur sous les alertes. De ce fait, l’HIPS est plutôt destiné à un utilisateur averti.
* Comme toutes les autres technologiques IPS, il peut lui arriver de refuser l’arrivée d’un paquet qui est pourtant tout à fait légitime.
  1. KIPs
     1. Définition

KIPS signifie « Kernel Intrusion Prevention System ».

Cet outil permet aux administrateurs réseaux de configurer une ou plusieurs réactions permettant de bloquer des évènements d’une partie du système d’exploitation d’une machine.

Le KIPS agit directement sur le « Noyau » d’un système. Cela permet de réguler les actions et de prévenir toute défaillance ou attaque. En effet, le KIPS va vérifier chaque appel vers le système et va ainsi détecter un comportement anormal et en stopper les actions.

Le KIPS permet par exemple de protéger un serveur web en restreignant la lecture et l’écriture des fichiers (port 80 - cf glossaire). Ainsi, il empêche toute possibilité d’ouverture de « shell » de commande (cf glossaire) et de lecture sur le reste du serveur.

L’outil KIPS peut aussi détecter toutes les modifications de performance de la machine, tel qu’une utilisation trop importante de mémoire. Il peut alors stopper le logiciel ou l’outil entrainant cette perte de performance.

* + 1. Fonctionnement

Le KIPS fonctionne sur le système d’exploitation d’une machine. Il analyse toutes les actions entrantes et sortantes de celui-ci, tout en vérifiant qu’elles apparaissent bien dans sa base de règles de sécurité. Si elles sont autorisées, le système les laisse s’effectuer. Sinon elles sont bloquées et enregistrées en mémoire.

Comment ça marche ?

1. La machine initialise une action système ;
2. L’outil KIPS analyse la commande ;
3. KIPS vérifie dans sa base de règle si la commande est autorisée ;

A présent deux possibilités :

A) L’action est autorisée et exécutée ;

B) L’action est refusée et enregistrée dans la mémoire du KIPS.

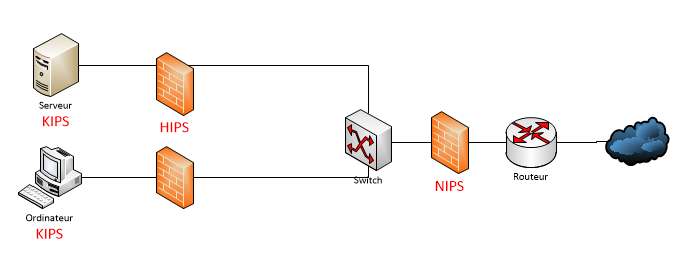
* + 1. Avantages

Comme pour tout outil IPS, le KIPS possède certains avantages :

* Détecte et bloque les commandes douteuses ;
* Envoie une alerte en cas de problème ;
* Possibilités de configuration nombreuses ;
* Ajoute des règles de sécurité supplémentaires ;
  + 1. Inconvénients

Et bien entendu, cet outil possède des inconvénients :

* Ralenti la machine car vérifie chaque action et dépendance ;
* Possibilité de faux-positif ;
* Rarement utilisé sur des serveurs déjà beaucoup sollicités ;
* Complexe à configurer.
  1. Localisation sur un réseau

Globalement, la seule différence notable entre les trois technologies, est leur emplacement dans un réseau. De ce fait, leurs actions sont différentes.

Le KIPS agit donc directement à l’intérieur du système d’exploitation du PC.

Le HIPS agit sur le PC, mais en communication avec l’extérieur.

Le NIPS agit au niveau du réseau.

On peut se poser la question suivante : Est-ce utile de posséder les trois types d’IPS différents ?

Pour garantir la plus grande sécurité possible, la réponse serait oui. Mais avec autant d’alertes et de contrôles, le débit à l’intérieur du réseau est nettement diminué, et l’utilisateur trouvera désagréable de devoir en permanence accepter/refuser qu’une action se déroule.

1. Acteurs du marché
   1. Identification des constructeurs

On dénombre principalement 6 grands acteurs du marché de l’IPS, jugés selon les critères suivants :

* Produit ou service proposé
* Satisfaction du client
* Viabilité globale de l'entreprise
* Revenus
* Taille moyenne des transactions
* Réactivité du marché.

Tout d’abord Cisco Systems [[Cisco]](http://www.cisco.fr) qui est une entreprise informatique américaine qui vend du matériel réseau. Celui ci dispose de plusieurs offres de solutions IPS qui peuvent être mises en œuvre par l'intermédiaire de son logiciel de capteur IPS ainsi que par du matériel autonome (avec des modules add-on). Cette entreprise ayant acquis sourcefire en 2013.

IBM [[IBM]](http://www.ibm.com/fr/fr/‎) qui est une société présente dans le domaine du matériel informatique, du logiciel et des services informatiques. Celle-ci possède système de prévention des intrusions sur le réseau de sécurité IBM est placé dans une unité de sécurité d'entreprise plus large, qui inclut les technologies SIEM , et dirigé par l'ancien PDG de Q1 Labs .

Enterasys Networks , dont le siège est dans le Nord-Est des États-Unis et qui est une société d'infrastructure de réseau , acquis en 2013 par Extreme Networks [[Extreme Networks]](http://www.extremenetworks.com/) , avec des produits de sécurité qui incluent IPS , les informations de sécurité et de gestion des événements ( SIEM ) , une identité mobile et solution de gestion des accès et le contrôle d'accès réseau ( CNA ) .

HP [[HP]](http://www.hp.com/‎) qui est une entreprise multinationale américaine, à large base informatique et service fournisseur. Qui a conservé le nom de la marque TippingPoint IPS (racheté en 2009) dans sa gamme de produits.

Huawei [Huawei] est un grand fournisseur d'infrastructure de réseau basée à Shenzhen, en Chine. En plus de pare-feu, UTM, sa sécurité contre les attaques par déni de service (DDoS) et de solutions de sécurité mobile, Huawei a livré sa protection réseau intelligent (NIPS) de la gamme de produits depuis 2004.

McAfee [[McAfee]](http://www.mcafee.fr/‎) qui est une entreprise spécialisé dans la sécurité avec un large panel de produits à travers le réseau et la sécurité de bureau, et est une filiale d'Intel depuis son acquisition en 2011.

* 1. Identification des produits
  2. Identification des OS et machines physiques

1. Parts de marché
   1. Répartition sur le marché Mondial
   2. Répartition sur le marché Européen
   3. Répartition sur le marché Français
2. Implantations
   1. Mondiale
   2. Europe
   3. France
3. Références
   1. Identification des types de clients
   2. Les grands noms parmi les clients

Conclusion

Bien organisée, dénoue l’étude écrite et le retour d’expérience permet de comprendre le choix des sources, la méthodologie et l’intérêt pour l’entreprise d’accueil de chaque membre du binôme. Cette conclusion en français précède la même conclusion en anglais. Cette conclusion est le résultat de la réflexivité clairvoyante et éveillée du binôme (auteur dudit document).

ICI : Version anglaise !

Glossaire

Seuls les mots et acronymes utilisés dans le document sont cités dans le glossaire. Ce glossaire doit être rédigé dans l’ordre alpha.

Protocoles :

IP : Internet Protocol

TCP : Transmission Control Protocol

UDP : User Datagram Protocol

ICMP : Internet Control Message Protocol

MPLS : MultiProtocol Label Switching

HTTP : Hypertext Transfer Protocol

MIME : Multipurpose Internet Mail Extensions

FTP : File Transfer Protocol

DHCP : Dynamic Host Configuration Protocol

Bibliographie

[IPSHOME] http://eatingsecurity.blogspot.fr/2008/01/idsips-placement-on-home-network.html

Annexes

Les annexes peuvent être un autre document non relié au document lui mêmes. Ces annexes paginées doivent avoir un lien avec l’étude du sujet et doivent être organisées dans l’ordre d’utilisation dans le texte du doc. Un sommaire des annexes est nécessaire.

Annexes – Sommaire

Summary