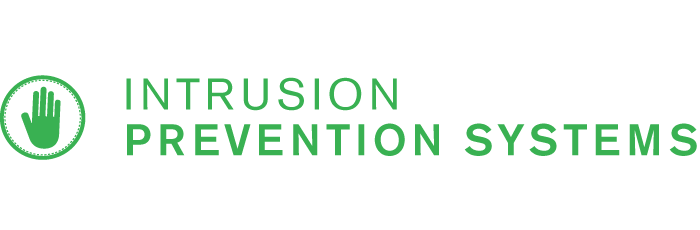


DESZCZ Sébastien

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 |
| […] | Une bibliographie |
|  |  |
|  |  |

Sommaire

[Synthèse 2](#_Toc387148709)

[Préambule 3](#_Toc387148710)

[Sommaire 4](#_Toc387148711)

[1. Présentation 6](#_Toc387148712)

[1.1 Présentation du groupe 6](#_Toc387148713)

[1.2 Gantt 6](#_Toc387148714)

[2. Technologie de l’IPS 7](#_Toc387148715)

[2.1 IPS Appliance 7](#_Toc387148716)

[2.1.1 Définition 7](#_Toc387148717)

[2.1.2 Fonctionnement 8](#_Toc387148718)

[2.1.3 Avantages 8](#_Toc387148719)

[2.1.4 Inconvénients 9](#_Toc387148720)

[2.2 NIPS 9](#_Toc387148721)

[2.2.1 Définition 9](#_Toc387148722)

[2.2.2 Fonctionnement 10](#_Toc387148723)

[2.2.3 Avantages 11](#_Toc387148724)

[2.2.4 Inconvénients 11](#_Toc387148725)

[2.3 HIPS 11](#_Toc387148726)

[2.3.1 Définition 11](#_Toc387148727)

[2.3.2 Fonctionnement 11](#_Toc387148728)

[2.3.3 Avantages 12](#_Toc387148729)

[2.3.4 Inconvénients 12](#_Toc387148730)

[2.4 KIPs 13](#_Toc387148731)

[2.4.1 Définition 13](#_Toc387148732)

[2.4.2 Fonctionnement 13](#_Toc387148733)

[2.4.3 Avantages 13](#_Toc387148734)

[2.4.4 Inconvénients 14](#_Toc387148735)

[2.5 Localisation sur un réseau 14](#_Toc387148736)

[3. Acteurs du marché 15](#_Toc387148737)

[3.1 Identification des constructeurs 15](#_Toc387148738)

[3.2 Identification des produits 16](#_Toc387148739)

[3.3 Identification des OS et machines physiques 18](#_Toc387148740)

[4. Parts de marché 19](#_Toc387148741)

[4.1 Répartition sur le marché Mondial 19](#_Toc387148742)

[4.2 Répartition sur le marché Français 20](#_Toc387148743)

[5. Implantations 21](#_Toc387148744)

[5.1 Mondiale 21](#_Toc387148745)

[5.2 France 21](#_Toc387148746)

[6. Références 22](#_Toc387148747)

[6.1 Identification des types de clients 22](#_Toc387148748)

[6.2 Les grands noms parmi les clients 22](#_Toc387148749)

[Conclusion 23](#_Toc387148750)

[Glossaire 24](#_Toc387148751)

[Bibliographie 25](#_Toc387148752)

[Annexes 26](#_Toc387148753)

[Summary 32](#_Toc387148757)

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) ;

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 ;
* Peut être compliqué à mettre en place.

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

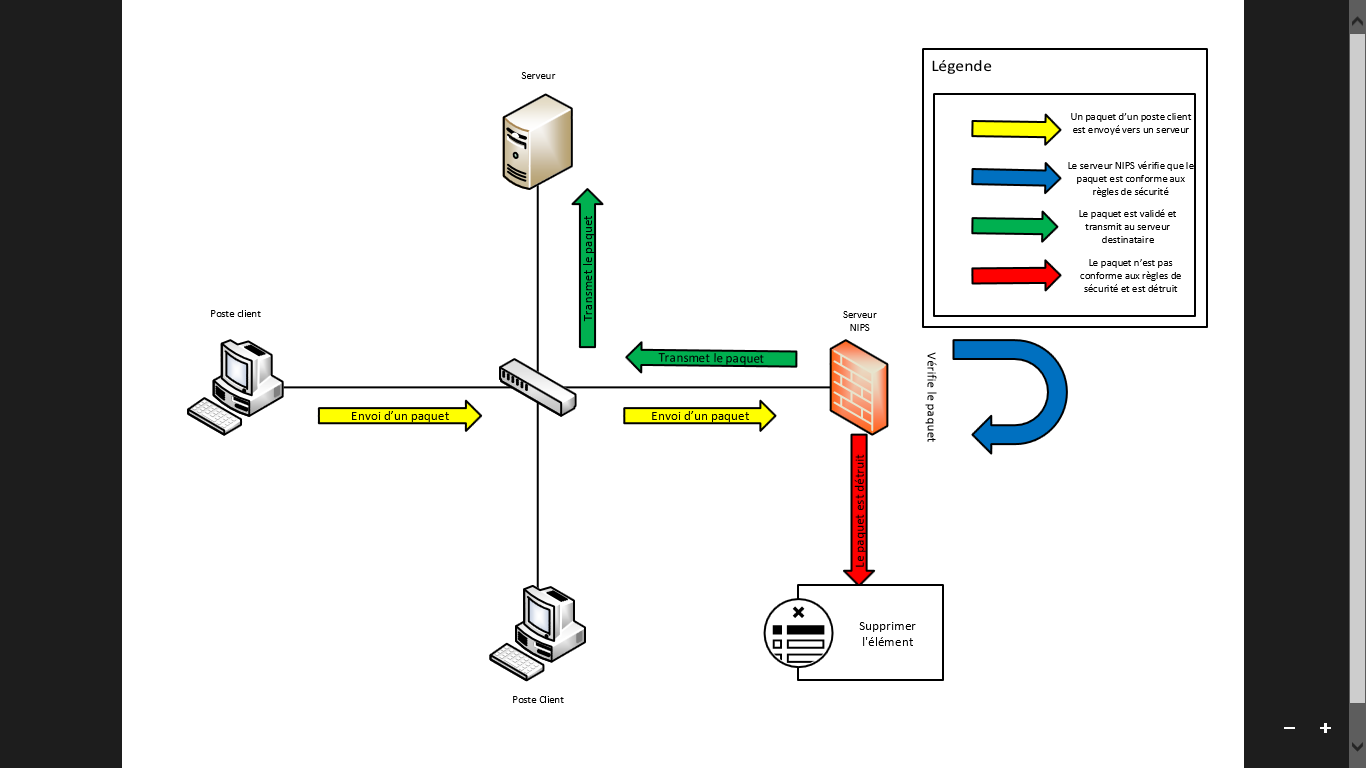
Le NIPS agit au niveau du réseau et vérifie que chaque paquet correspond bien à la politique de sécurité mise en vigueur sur réseau. Puis, si un ou plusieurs d’entre eux ne sont pas conformes, le système NIPS va alors bloquer la source et envoyer une alerte à l’administrateur.

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.

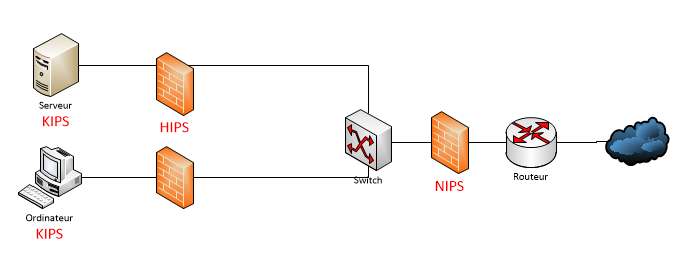
* + 1. Avantages

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]. C’est une entreprise informatique américaine qui vend du matériel réseau. Elle 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). Cisco a de même racheté Sourcefire [FIRE] en 2013, qui propose aussi des offres IPS.

IBM [IBM] est une société présente dans le domaine du matériel informatique, du logiciel et des services informatiques. Celle-ci possède un système de prévention des intrusions, qui inclut les technologies SIEM (Security Information and Events Management), et est dirigé par l'ancien PDG de Q1 Labs, un fournisseur privé de logiciels de sécurité.

Enterasys Networks, dont le siège est dans le Nord-Est des États-Unis, est une société d'infrastructure de réseau, acquis en 2013 par Extreme Networks [EN]. Ses produits de sécurité incluent IPS, couplés à une gestion particulière des événements grâce à SIEM (Security Information and Events Manager).

HP [HP] est une entreprise multinationale américaine, dans le domaine du matériel informatique et du service. Elle possède TippingPoint IPS [TP] dans sa gamme de produits, qu’elle a racheté en 2009. TippingPoint IPS a été le tout premier IPS développé, en 2002.

Huawei [HUA] est un grand fournisseur d'infrastructure de réseau basée à Shenzhen, en Chine. En plus du pare-feu UTM (Unified Threat Management), Huawei a ajouté le NIPS pour garantir la sécurité réseau, depuis 2004.

McAfee [MCAFEE] est une entreprise spécialisée dans la sécurité, avec un large panel de produits réseaux et de sécurité de l’ordinateur. C’est une filiale d'Intel depuis son acquisition en 2011.

* 1. Identification des produits

Cisco dispose d’un large éventail de produits de sécurité de réseau. Par exemple, la solution nommée IPS Manager Express pour les petits déploiements (jusqu’à 10 appareils), et Cisco Security Manager (CSM), pour des déploiements plus importants, comme en entreprise.

Points forts :

* Cisco est le leader du marché en termes d’équipements réseaux. Beaucoup d’entreprises utilisent déjà une infrastructure réseau Cisco. La méthode de gestion et de surveillance est donc assez familière. Les entreprises connaissent en effet déjà la console d’exploitation, qui peut servir pour plusieurs produits Cisco, et pas seulement l’IPS. En outre, l’IPS peut être livré dans le cadre de l’infrastructure.
* Cisco dispose d'un large soutien international et d’une large couverture géographique. Les entreprises qui ont déjà un investissement important dans les produits de sécurité Cisco considèrent souvent Cisco IPS comme la solution la plus envisageable.

Point faible :

* L’innovation des technologies a pris du retard dans le domaine IPS, ce point noir ayant été partiellement corrigé avec le rachat de sourcefire.

La solution IBM Sécurité réseau IPS est disponible en neuf modèles d'appareils au sein de la série GX, avec un débit contrôlé allant de 200 Mbps à 20 Gbps . IBM a récemment publié les XGS 3100, 4100 et 5100 , qui intègrent des capacités NGIPS qui ont jusqu'à 5 Gbps de débit contrôlé . La plate-forme de sécurité réseau virtuel est disponible dans une application virtuelle VMware. IBM ne possède pas son propre portail Web pare-feu ou sécurisé.

Point fort :

* IBM dispose d'un réseau de ventes et de distribution larges, et les clients ayant déjà une relation avec IBM sont généralement satisfaits. On comprend qu’ils préfèreront se diriger vers une solution IPS IBM.

Point faible :

* Dans l'enquête Magic Quadrant pour les fournisseurs, IBM est cité comme possédant l’IPS le plus fréquemment remplacés par une autre solution. [GARTNER]

Le système de prévention des intrusions Enterasys (également connu sous le nom de Dragon IPS) posséde des capteurs en ligne qui vont de 100 Mbps à 10 Gbps de débit.

Pour les grandes ou complexes déploiements , le processeur Enterasys Dragon de flux d'événements (EFP) peut être utilisé pour agréger les informations de l'événement et le signaler à Dragon Enterprise Management Server ( EMS ) . Enterasys ne possède pas son propre pare-feu, ni sa propre passerelle Web sécurisée, ni sa propre passerelle sécurisée de messagerie.

Points faibles :

* Les clients rapportent qu’Entasys donne un taux légèrement plus élevé que prévu de faux positif.
* Le produit Dragon est utilisé plus fréquemment en tant que IDS qu’en tant qu’IPS.

HP inclut désormais la gamme de produits NX NGIPS, qui va jusqu'à un débit de 20 Gbps.

Il contient donc TippingPoint IPS, mais HP ne possède pas son propre portail Web sécurisé ou sa passerelle sécurisé de messagerie.

Points forts :

* Les clients continuent de citer la facilité d'installation comme un élément positif dans l'évaluation de produits, en particulier pour les déploiements avec de nombreux appareils.
* Les produits TippingPoint IPS ont une large gamme de modèles d'appareils spécialement conçus pour, et sont connus pour une faible latence et un débit élevé.

Point faible :

* Les solutions HP sont très facilement remplacées par une autre solution selon les revendeurs.

La plate-forme NIPS de Huawei permet d’inspecter le réseau avec un débit variant de 600 Mbps à 30 Gbps. Plusieurs périphériques peuvent être gérés séparément par le logiciel de gestion NIP. Huawei n’offre pas une passerelle Web sécurisée ou une passerelle de messagerie sécurisé, et n'a aucun appareil IPS virtuel.

Points forts :

* Les produits NIPS de Huawei reçoivent régulièrement de l'utilisateur final des remarques positives. Parmi ces remarques, la facilité d'utilisation et de configuration sont mises en avant.
* Huawei fournit une solution IPS rentable qui permet de faciliter le choix dans les organisations et les entreprises sensibles aux coûts.

Points faibles :

* Ces ventes sont principalement en Asie.
* Huawei a pris des mesures importantes afin de répondre aux inquiétudes des consommateurs concernant les technologies qu’elle développe en Chine. Cependant, pour certains clients potentiels Américains, cela reste un problème.

La plate-forme de sécurité réseau McAfee (PSN) est le seul modèle IPS de la société, avec des appareils possédant un débit allant de 100 Mbps à 40 Gbps. En outre, McAfee a acquis Stonesoft en 2013, qui a fourni un autre produit IPS et un pare feu de nouvelle génération pour entreprise.

Point fort :

* L'ajout de Stonesoft renforce la sécurité du réseau de McAfee.

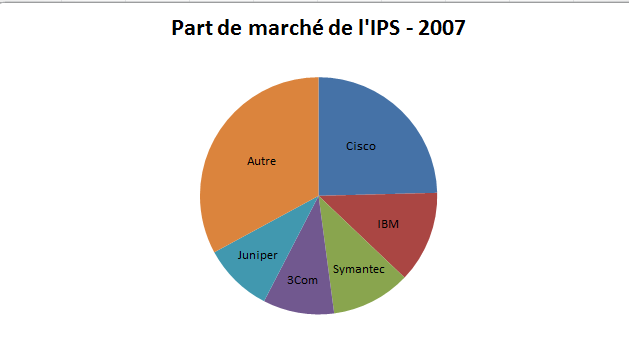
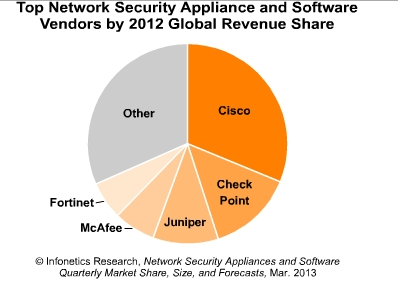
Point faible :

* La marque McAfee est connue plus largement pour les offres de sécurité de bureau, et souvent n'est pas perçu par les entreprises et les partenaires de distribution comme un fournisseur solide de sécurité du réseau.
  1. Identification des OS et machines physiques

L’IPS Appliance peut fonctionner sous n’importe quel OS d’ordinateur, que ce soit Windows, Linux, MacOs,

1. Parts de marché
   1. Répartition sur le marché Mondial

De nombreux éditeurs de solutions de sécurité, dont Sourcefire (Cisco), précurseur sur ce marché, ou encore Check Point, Stonesoft et Fortinet, sont les acteurs de cette technologie sur le marché mondial ainsi qu’européen.

Les deux graphiques qui suivent présentent les parts de marché des différents acteurs, en 2007 d’une part, et en 2012 d’autre part. Ainsi, on peut voir la progression des parts de marché.

* 1. Répartition sur le marché Français

Il y’a peu d’entreprises françaises qui se lancent dans la technologie IPS. Cependant, il en existe quelques-unes :

* Eliptec
* Afina

Malheureusement pour ces entreprises et bien que leur prix soit abordable, elles n’ont pas la même fiabilité que les leaders sur le marché, et ne proposent que peu de produit différents.

Les principaux acteurs sur le marché français sont : Fortinet, Sourcefire (Cisco), checkpoint et Stonesoft (McAfee).

1. Implantations
   1. Mondiale
   2. France

Le budget consacré à la sécurité informatique représente encore une part minime des investissements informatiques (estimé à 3%). Ce fait est avéré dans la majeure partie des entreprises françaises, de l’entreprise du CAC 40 à la TPE.

Les entreprises plutôt « inconscientes » pensent être sécurisées mais disposent de dispositifs obsolètes, figés ou insuffisants.

Les entreprises lucides et conscientes de la réalité  des menaces et des possibles défaillances de leur système se contentent aussi bien souvent de ce qu’elles ont.

En définitive, toutes les entreprises sont bien protégées, jusqu’à ce qu’elles se fassent attaquer.

Cependant beaucoup de grosses entreprises et PME possède un IPS :

* Enterasys a équipé la SNCF, L’EDF ou encore Sanofi Aventis.
* IBM / ISS compte 400 référence clients en France, en majorité des PME.
* Fortinet a réalisé un chiffre d’affaire de 170 millions de dollars en 2006 dont 12 millions pour la France.
* Cyberoam travaille avec 50 partenaires en France et veut continuer de se développer.

L’implantation de IPS en France est assez faible mais est en train d’évoluer, toutes les entreprises ne voient pas encore l’intérêt d’investir dans de la sécurité et pensent être déjà suffisamment sécurisé alors que ce n’est pas toujours le cas. On estime en moyenne que 70% des entreprises françaises ont subi une attaque sur les 12 derniers mois.

1. Références
   1. Identification des types de clients

Comme précisé dans la partie « Implantation en France », peu d’entreprises se sentent réellement concernées par les solutions IPS.

Les petites entreprises n’ont pas les moyens de se fournir un IPS, car c’est un investissement à long terme.

Les grandes entreprises qui ont les moyens ne vont pas le faire systématiquement : certaines sont tout simplement inconscientes des dangers, et ce, pas seulement en France.

Nous avons interviewé une entreprise afin d’apporter une touche concrète à notre projet. Cette dernière, qui souhaite garder l’anonymat, a ressenti le besoin de s’équiper en IPS lors de la mise en place de Data Center au sein de l’entreprise. Un récapitulatif de cet interview est présenté en Annexe.

* 1. Les grands noms parmi les clients

Conclusion

Certains pensent que l’ « Intrusion Prevention System » reste un terme purement marketing, et ne serait qu’une légère évolution de l’ « Intrusion Detection System ». Cependant, il prouve bien sa flexibilité avec les différents services de surveillance de poste, tels que le HIPS ou KIPS, mais aussi avec le NIPS qui se charge de la surveillance du réseau.

De plus, l’IPS s’impose à l’aide de sa popularité avec des grands noms de constructeur comme CISCO (le leader de la sécurité), IBM (l’innovateur) ou McAfee (le protecteur), qui possèdent tous une grande place sur le marché de l’informatique. Enfin, les systèmes IPS s’assurent de leurs places en s’implantant mondialement dans des sociétés-t-elle que la SNCF avec « Enterasys » ou notre entreprise X interviewée, avec Cisco. Ils n’en restent pas moins présents chez les particuliers avec l’anti-virus « Eset Smart Securty » qui sert d’HIPS, par exemple.

Donc nous pouvons affirmer que le système IPS  est bien « LA solution » contre les menaces venant d’internet, mais vu la prolifération des virus en tout genre, nous sommes en droit de nous demander : jusqu’à quand ?

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.

DMZ:

Logiciel de gestion NIP:

Port 80:

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 Extension
* FTP : File Transfer Protocol
* DHCP : Dynamic Host Configuration Protocol

Shell:

SIEM:

Spyware:

Bibliographie

[CISCO] <http://www.cisco.fr/>

[EN] <http://www.extremenetworks.com/>

[FIRE] <http://www.sourcefire.com/fr/security-technologies>

[GARTNER] <http://www.gartner.com/technology/reprints.do?id=1-1OAVJS3&ct=131217&st=sb>

[HP] <http://www.hp.com>

[HUA] <http://www.huawei.com/fr/>

[IBM] <http://www.ibm.com/fr/fr>

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

[MCAFEE] <http://www.mcafee.fr/>

[TP] <http://www.brain-networks.fr/tippingpoint>

[TYAT] <http://igm.univ-mlv.fr/~duris/NTREZO/20032004/Baudoin-Karle-IDS-IPS.pdf>

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.

Sommaire

Annexe 1 : Les types d’attaques

Bon nombre d’attaques, qu’elles soient simples ou complexes, suivent le même schéma :

Tout d’abord, il faut connaitre la cible, c’est-à-dire, récolter le plus d’informations possibles dessus. D’une part, on récolte les informations qu’elle rend publiques sur internet (adresse IP). Puis, un scan est effectué pour récupérer toutes les informations supplémentaires, telles que l’OS de l’ordinateur, le masque de sous réseau, les règles de firewall, etc…).

S’en suit une étape d’identification des failles : à partir des informations que l’on a récupéré, on cherche les failles à exploiter. Elles peuvent être au niveau des protocoles, du système d’exploitation, des applications, …

Enfin, bien sûr, l’attaquant passe à l’action pour contrôler l’ordinateur.

Quels sont les types d’attaques ? [TYAT]

Le sniffing

Grâce à un logiciel appelé "sniffer", il est possible d’intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées. Si quelqu’un se connecte par telnet par exemple à ce moment-là, son mot de passe transitant en clair sur le net, il sera aisé de le lire. De même, il est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Une restriction de cette technique est de se situer sur le même réseau que la machine ciblée.

L’IP spoofing

Cette attaque est difficile à mettre en œuvre et nécessite une bonne connaissance du protocole TCP. Elle consiste, le plus souvent, à se faire passer pour une autre machine en falsifiant son adresse IP de manière à accéder à un serveur ayant une "relation de confiance" avec la machine "spoofée". Cette attaque n’est intéressante que dans la mesure où la machine de confiance dont l’attaquant à pris l’identité peut accéder au serveur cible en tant que root.

Le DoS (Denial of Service)

Le DoS est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d’un système. Cette attaque ne permet pas en elle-même d’avoir accès à des données. En général, le déni de service va exploiter les faiblesses de l’architecture d’un réseau ou d’un protocole. Il en existe de plusieurs types comme le flooding, le TCP-SYN flooding, le smurf ou le débordement de tampon (buffer-overflow).

Les programmes cachés ou virus

Il existe une grande variété de virus. On ne classe cependant pas les virus d’après leurs dégâts mais selon leur mode de propagation et de multiplication. On recense donc les vers (capables de se propager dans le réseau), les troyens (créant des failles dans un système), Les bombes logiques (se lançant suite à un événement du système (appel d’une primitive, date spéciale)).

L’ingénierie sociale (social engineering)

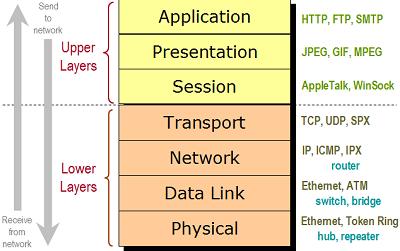
Ce n’est pas vraiment une attaque informatique en soit, mais plutôt une méthode consistant à se faire passer pour quelqu’un que l’on n’est pas afin de recueillir des informations confidentielles.

Le craquage de mots de passe

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s’effectuer à l’aide d’un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu’à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l’appui d’un très grand nombre de machines.

Annexe 2 : Le modèle OSI

L’architecture OSI :



Le modèle ISO définit une structure de référence en 7 couches individualisées pour les systèmes de communication de données.

Deux normes sont définies pour chaque couche:

* + une norme qui spécifie l'interface pour accéder aux services de la couche depuis la couche supérieure;
  + une norme qui définit le protocole par lequel les services sont fournis.
* La couche Physique : Cette couche définit les caractéristiques physiques ;
* La couche Liaison de données : Cette couche est responsable de l'échange de blocs d'information sur une ligne (détection, correction d'erreurs, adressage) ;
* La couche Réseau : Cette couche réalise l'interface utilisateur avec le réseau, et gère l'adressage et le transfert des données vers une machine à travers le ou les réseaux connectés ;
* La couche Transport : Cette couche est responsable du transport des paquets, de son entrée sur le réseau jusqu’à sa réception ;
* La couche Session : Cette couche fournit une interface permettant de synchroniser la communication entre les processus distant ;
* La couche Présentation : Cette couche est responsable de la présentation des données sous un format ;
* La couche Application : Cette couche comprend les programmes d'application avec leurs conventions d'échange et de coopération.

Annexe 3 : Interview d’une entreprise

Par souci d’anonymat, nous l’appellerons l’entreprise « X ».

X possède un IPS sur les Datacenter de ses sites principaux. Ils agissent au niveau de la DMZ, uniquement sur les serveurs accessibles à distance, parmi lesquels ceux contenant le site web grand plus, ou les sites institutionnels…

Le site web de X est devenu un Sandbox (« bac à sable ») où il est normalement impossible d’aller plus loin sur le réseau.

X fait appel à des sociétés externes pour tester la sécurité du réseau, de l’extérieur. Un audit est souvent réalisé en interne pour évaluer le degré de protection des serveurs critiques de la société.

En dehors de cet audit, aucun test n’est effectué de l’intérieur, dans la mesure où le serveur LDAP est déjà un rempart important face aux problèmes internes, grâce aux restrictions d’accès, au système d’authentification…

Ce besoin de protéger le réseau de l’entreprise est apparu aux débuts des années 2000, quand X s’est équipée en data centers. L’entreprise ne peut pas évaluer le coût économique de la mise en place et la maintenance de l’IPS, dans la mesure où cet ajout a été fait uniquement de manière préventive, et non pas en réponse à un éventuel problème.

De ce fait, depuis la mise en place de l’IPS, aucune menace sérieuse n’a infiltré le réseau de X, si ce n’est un virus, transmis par accident par un partenaire, en interne.

L’IPS est donc surtout là à titre informatif, et prévient avec des alertes en cas d’intrusion/d’attaque.

L’équipement IPS est un CISCO. Le choix a été fait après une analyse approfondie du marché, et l’offre de CISCO était la plus intéressante pour l’entreprise, indépendamment du prix.

Summary