OS/Machine :

L’IPS Appliance peut fonctionner sous n’importe quel OS.

IPS Appliance :

Définition

L’IPS (Intrusion Prevention System) est un outil en sécurité des systèmes d’information similaire aux IDS mais plus actifs que ceux-ci. Il est dédié à une tâche de sécurité spécifique qu'est le blocage des trafics malicieux dans les couches supérieures du modèle OSI. 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...).

Ils existent 3 types d’IPS différent :

* 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 NIPS/WIPS (Network/Wireless Intrusion Prevention System) qui surveillent le trafic réseau, en cas de suspicion, ils peuvent mettre fin à une session TCP.
* Les KIPS (Kernel Intrusion Prevention System) qui détectent les tentatives d’intrusion au niveau du noyau.

Les IPS Appliance sont des solutions de sécurité qui réunissent pare-feu, réseau privé 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 permet aux flux de l’entreprise de circuler. Ils prennent aussi en charge une DMZ pour héberger les serveurs en sécurité tout en garantissant la sécurité du réseau interne de l’entreprise.

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.).

Fonctionnement

L’IPS/IDS analyse les trames dans leurs ensemble et non pas une par une. Ce qui permet, grâce à une base de connaissance sur les attaques connues, de voir si certaine combinaison de trames peuvent être identifié comme une tentative d’intrusion. De plus l’IPS/IDS va garder en mémoire l’évènement afin de conserver une trace du problème et de pouvoir le résoudre plus facilement par la suite.

L’analyse de la trame est complexe. En effet elle s’effectue à l’issue d’une analyse primaire des données, c’est la remonté 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.

A l’inverse de l’IDS, qui fonctionne en mode promiscuité (il réceptionne une copie du trafic sans l’influencer), 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.

Les plus

* Protection contre les attaques/intrusions : le sniffing, l’ip spoofing, le DoS, les virus/vers
* Meilleur sécurité
* Réduction des coûts informatique (moins d’assistance informatique)
* Facile d’utilisation

Les moins

* Risque de faux positifs (ils peuvent bloquer des applications ou des trafics légitimes)
* Ils sont peu discrets et peuvent être découverts lors d’une attaque
* Les bases de connaissance sur lesquels s’appuient les IPS sont incomplètes

Implantation de L’IPS en France :

**Le budget consacré à la sécurité informatique représente encore une part minime des investissements informatiques (estimé à 3%) et ce dans la majeure partie des entreprises françaises, de l’entreprise du CAC 40 à la TPE.** Les entreprises plutôt « inconscientes », qui pensent être sécurisées mais disposent de dispositifs obsolètes, figés ou insuffisants, et les entreprises lucides sur la réalité  des menaces et aux possibles défaillances de leur système, mais qui s’en contentent. **En définitive, toutes les entreprises sont bien protégées, jusqu’à ce qu’elles se fassent attaquer.**

**Cependant beaucoup de grosse entreprise 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 voit 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.**

Le marché Européen :

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

Le marché français :

Il y’a peu d’entreprise française qui se lancent dans la technologie IPS, cependant ils en existent quelques-unes :

* Eliptec
* Afina

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

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