NIPS « 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 car elle a un comportement anormal. Autrement dit, cet outil permet aux administrateurs de vérifier l’état de leur réseau et de vérifier que tout se déroule normalement

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

Il arrive aussi que les services NIPS soient plus utilisés sous forme de « NIDS » (Network Intrusion Detection) qui permet simplement de détecter les intrusions et les comportements anormaux sur le réseau et d’en informer les administrateurs. C’est ce que le groupe Gartner estime à 25 % sur l’ensemble des installations. Et cela à pus ce confirmer lorsque nous avons interrogé notre interlocuteur lors d’un entretient. En effet, celui-ci nous précisé qu’ils utilisé un IDS et non pas un IPS car cela leur apporte une certaine sécurité et sérénité.

Comment ça marche ?

1. Un appareil envois un des paquets
2. Le NIPS intercepte les paquets
3. Le NIPS Analyse les paquets
4. Le NIPS vérifie la conformité des paquets (tailles, nombres, destination, …) dans sa base de règles.

Maintenant il existe 2 possibilités :

1. A) Le paquet est validé et continue sa route.

B) Le paquet est refusé et l’appareil est bloqué en fonction des règles mise en place.

Les Avantages :

* Détectes et bloque les intrusions
* Envois des alertes
* Possibilité de configurations très nombreuses
* Analyse les paquets et les logs

Les Inconvénients :

* Possibilité de faux-positif
* Très complexe à configurer
* Possibilité de ralentir le réseau
* La fiabilité n’est pas de 100%
* Machine dédié à ce service car énormément d’information à traiter