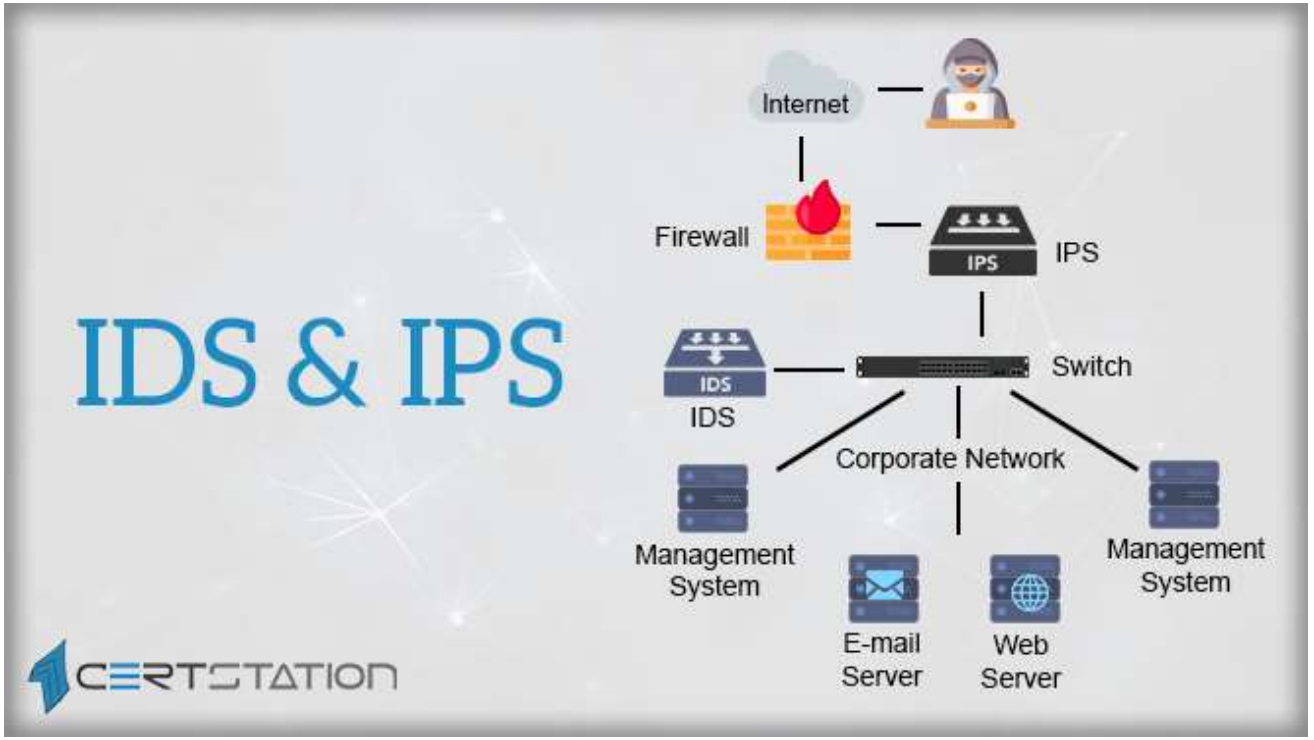
Chapitre 08_Systèmes de Détection d'Intrusions (IDS) & Système de Prévention d'intrusions (IPS)



Professeur Chiba Zouhair

Systèmes de Détection d'Intrusions (IDS)

Définitions :

- En sécurité informatique, la **détection d'intrusion** est l'acte de détecter les actions qui essaient de compromettre la **confidentialité**, **l'intégrité** ou la **disponibilité** d'une ressource.

- La **détection d'intrusion** peut être effectuée **manuellement** ou **automatiquement**. Dans le processus de détection d'intrusion **manuelle**, un analyste humain procède à l'examen de fichiers de logs à la recherche de tout signe suspect pouvant indiquer une intrusion.

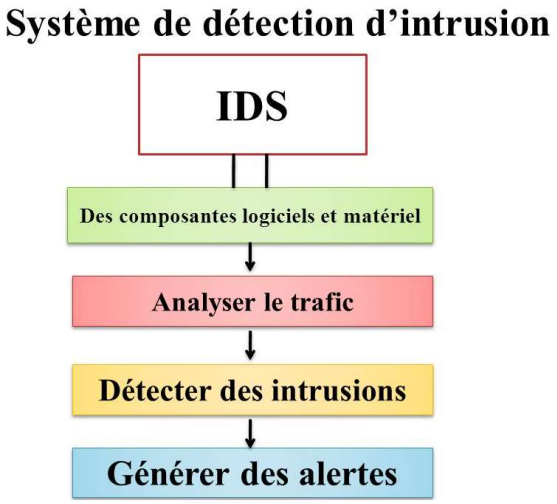
- Un système qui effectue une **détection d'intrusion automatisée** est appelé **Système de Détection d'Intrusion (IDS)**. Lorsqu'une intrusion est découverte par un IDS, les actions typiques qu'il peut entreprendre sont par exemple d'**enregistrer** l'information pertinente dans un fichier ou une base de données, **générer et envoyer** une alerte par e-mail ou un message sur un pager ou sur un téléphone mobile.

Les composants d'un IDS :

1. **Senseur** : Le senseur est responsable de la **collecte** des informations du système, telles que des **paquets d'un réseau** ou des **données de log**.

2. **Analyseur** : L'analyseur reçoit l'ensemble des informations venant des **senseurs**. Il est responsable de les **analyser** et d'indiquer si une **attaque** a lieu ainsi qu'éventuellement sa **réponse**.

3. **Interface utilisateur** : L'interface utilisateur permet aux utilisateurs de l'IDS de **visualiser** ou/et de **définir le comportement du système**.



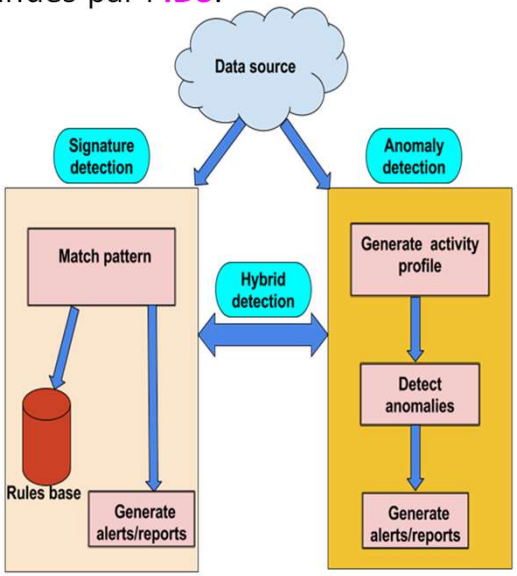
Systèmes de Détection d'Intrusions (IDS)

Les techniques de détection d'intrusion :

L'approche par scénarii :

- Dans cette approche, l'**IDS** analyse l'information recueillie et la compare (**pattern matching**) avec une base de données de signatures (motifs définis, caractéristiques explicites) d'attaques connues (i.e., qui ont déjà été documentées), et toute activité correspondante est considérée comme une attaque (avec différents niveaux de sévérité).

- Ce type d'**IDS** est purement **réactif** ; il ne peut détecter que les attaques dont il possède la signature. De ce fait, il nécessite d**es mises à jour fréquentes**. De plus, l'efficacité de ce système de détection dépend fortement de la **précision** de sa **base de signatures**. C'est pourquoi ces systèmes sont contournés par les pirates qui utilisent des techniques dites "d'évasion''. Ces techniques tendent à faire varier les signatures des attaques qui ainsi ne sont plus reconnues par l'**IDS**.



Systèmes de Détection d'Intrusions (IDS)

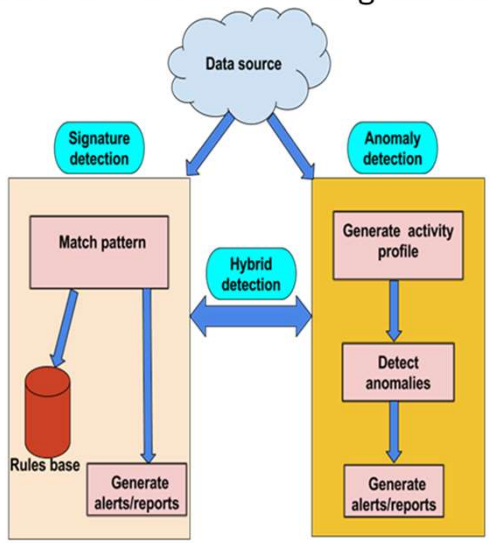
Les techniques de détection d'intrusion :

L'approche comportementale :

- La détection d'anomalie de comportement est une technique assez ancienne (elle est utilisée également pour détecter des comportements suspects en téléphonie, comme le phreaking). L'idée principale est de modéliser durant une période d'apprentissage le comportement "normal" d'un système/programme/utilisateur en définissant une ligne de conduite (dite baseline), et de considérer ensuite (en phase de détection) comme suspect tout comportement inhabituel (les déviations significatives par rapport au modèle de comportement "normal").

- Les **modèles comportementaux** peuvent être élaborés à partir d'analyses statistiques ou via l'Intelligence Artificielle. Ils présentent l'avantage de détecter des nouveaux types d'attaques. Cependant, de fréquents ajustements sont nécessaires afin de faire évoluer le modèle de référence de sorte qu'il reflète l'activité normale des utilisateurs et réduire le nombre de fausses alertes générées.

Chacune de ces deux approches peut conduire à des faux positifs (détection d'attaque en absence d'attaque) ou à des faux négatifs (absence de détection en présence d'attaque)

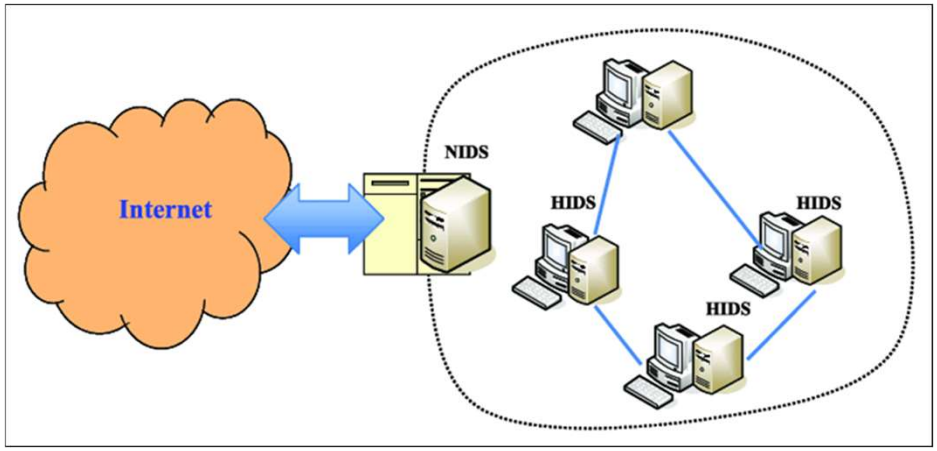


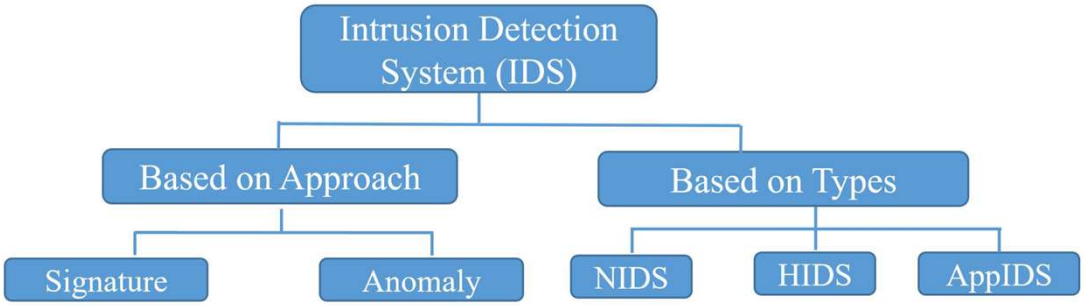
Systèmes de Détection d'Intrusions (IDS)

Classification des IDS :

Les systèmes de détection d'intrusion ou IDS peuvent se classer selon trois catégories majeures selon qu'ils s'attachent à surveiller :

- Le **trafic réseau** : on parle **d'IDS réseau** ou **NIDS (Network based IDS)**
- L'**activité des machines**: on parle **d'IDS Système** ou **HIDS (Host based IDS)**
- Une application particulière sur la machine : on parle **d'IDS Application (Application based IDS)**. Contrairement aux deux IDS précédents, ils sont rares.
- **Les IDS hybrides (NIDS+HIDS)** : Les IDS hybrides rassemblent les caractéristiques de plusieurs IDS différents. En pratique, on ne retrouve que la combinaison de **NIDS** et **HIDS**. Ils permettent, en un seul outil, de surveiller le réseau et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes **ces sondes** remontent alors les alertes à une machine qui va centraliser le tout, et agréger/lier les informations d'origines multiples.



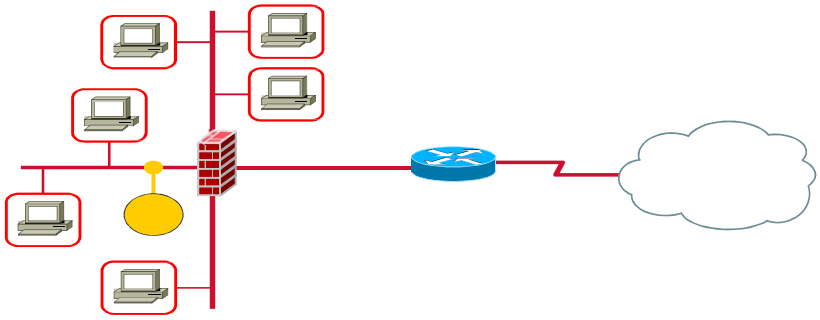


Systèmes de Détection d'Intrusions (IDS)

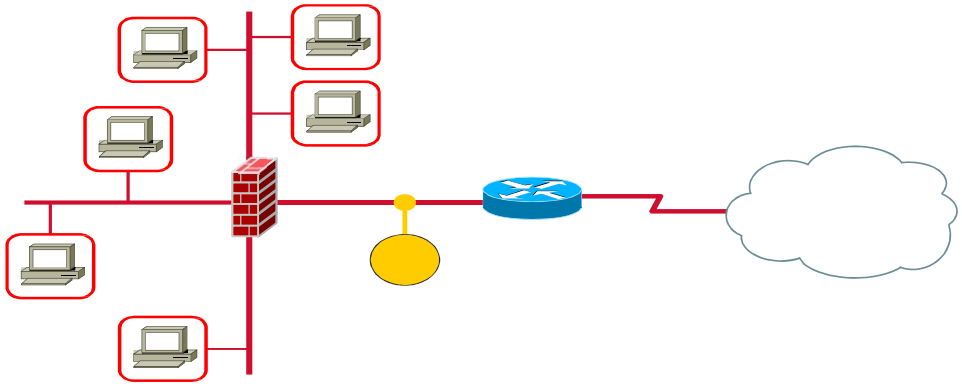
Positionnement des IDS :

Le placement des IDS va dépendre de la **politique de sécurité** menée. Mais il serait intéressant de placer des IDS :

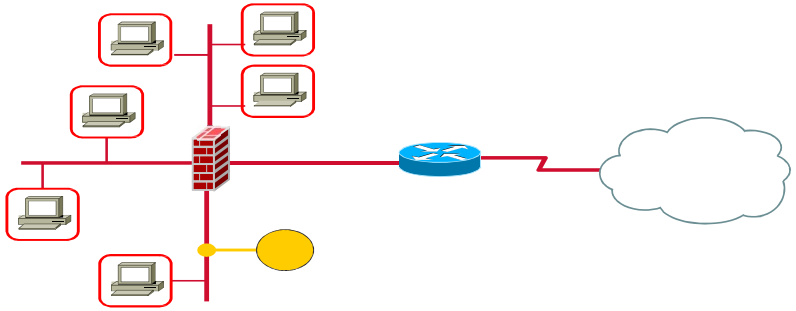
- Dans la zone démilitarisée DMZ (attaques contre les systèmes publics) (**Position 1**) ;
- Dans le (ou les) réseau privé (intrusions vers ou depuis le réseau interne) (**Position 2**) ;
- Sur la patte extérieure du firewall (détection de signes d'attaques parmi tout le trafic entrant et sortant, avant que n'importe quelle protection intervienne) (Position 3) .



Position 2



Position 3



Position 1

Système de Prévention d'intrusions (IPS)

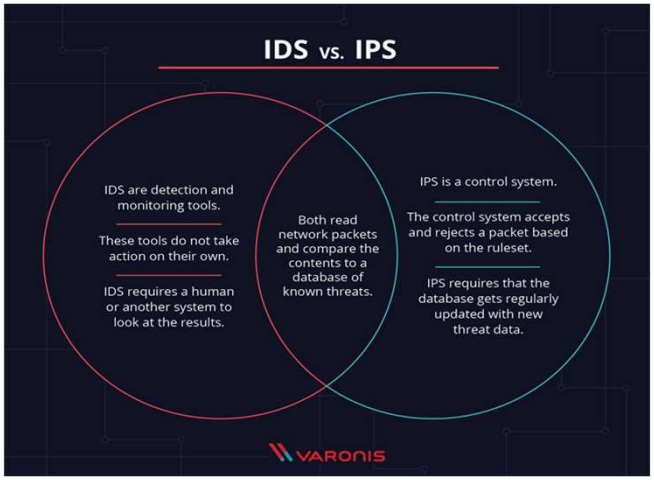
Définitions :

- Un **système de prévention d'intrusion** (ou **IPS**, **intrusion prevention system**) est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement. Les IPS peuvent donc parer les attaques connues et inconnues.

- Les IDS et les IPS lisent tous deux les paquets réseau et en comparent le contenu à une base de menaces connues. La principale différence entre les deux tient à ce qui se passe ensuite. Les **IDS** sont des outils de détection et de surveillance qui n'engagent pas d'action de leur propre fait. Les **IPS** constituent un système de contrôle qui accepte ou rejette un paquet en fonction d'un ensemble de règles.

- Avec l'**IDS**, il est nécessaire qu'un humain ou un autre système prenne ensuite le relais pour examiner les résultats et déterminer les actions à mettre en œuvre, ce qui peut représenter un travail à temps complet selon la quantité quotidienne de trafic généré. L'IDS constitue un très bon outil d'analyse.

- Pour sa part, l'objectif de l'**IPS** est de capturer les paquets dangereux et de les **retirer** avant qu'ils **n'atteignent leur cible**. Il est **plus actif** qu'un **IDS** et exige simplement de mettre régulièrement à jour la base de données pour y intégrer les informations relatives aux nouvelles menaces.



Système de Prévention d'intrusions (IPS)

- Il possède donc généralement soit une base de données de signatures qui peut être régulièrement mise à jour à mesure que de nouvelles menaces sont identifiées, soit un système à approche comportementale qui analyse les différences avec le niveau de fonctionnement normal du réseau qui a été défini par l'administrateur.

Principe de fonctionnement :

- Le concept d'**IPS** vise à anticiper les attaques de pirates informatiques dès lors que leur empreinte est connue. Il ne s'agit plus seulement de réagir à une attaque en cours, mais d'empêcher que celle-ci puisse débuter.

- Un système **IPS** est **placé en ligne** et **examine** en théorie tous les paquets entrants ou sortants. Il réalise un ensemble d'**analyses** de détection, non seulement sur chaque paquet individuel, mais également sur les **conversations et motifs du réseau**, en visualisant chaque transaction dans le **contexte de celles qui précèdent ou qui suivent**

- Si le système **IPS** considère le paquet inoffensif, il le transmet sous forme d'un élément traditionnel de couche 2 ou 3 du réseau. Les utilisateurs finaux ne doivent en ressentir aucun effet. Cependant, lorsque le **système IPS** détecte un trafic douteux il doit pouvoir activer un mécanisme de réponse adéquat en un temps record.

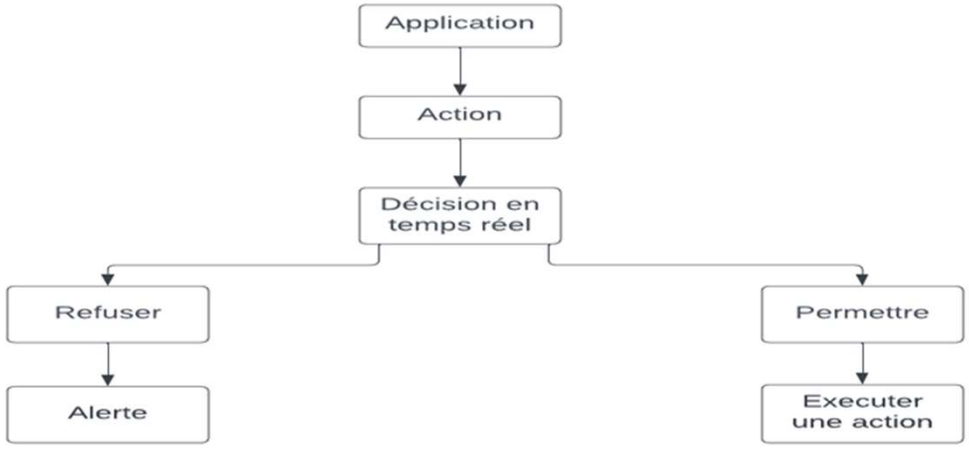


Diagramme de fonctionnement d'un IPS

Système de Prévention d'intrusions (IPS)

Catégories des IPS :

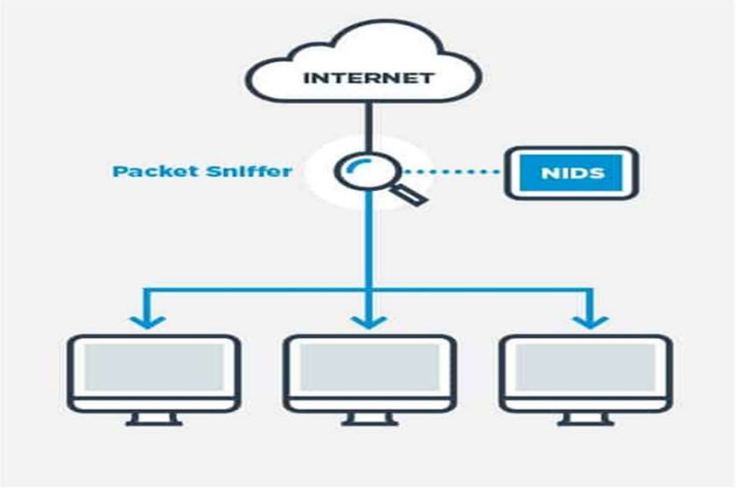
NIPS (Network Intrusion Prevention System)

- Lors de la détection d'une attaque, le système réagit et modifie l'environnement du système attaqué. Cette modification peut être le blocage de certains flux, de certains ports ou l'isolation pure et simple de certains systèmes du réseau.

- Le point sensible de ce genre de dispositif de prévention est qu'en cas de **faux positif**, c'est le trafic du système qui est directement affecté. Les problèmes doivent donc être les moins nombreux possibles car elles ont un impact direct sur la disponibilité des systèmes.

- En cas de détection de trafic dangereux lié à une intrusion potentielle, l'IPS bloque ce trafic comme un **firewall**. Néanmoins, ce même trafic se déroulant dans une configuration non dangereuse (pas d'enchaînement spécifique de trafic signalant une intrusion) ne sera pas bloqué. On pourrait comparer un **IPS** à un firewall « intelligent », qui aurait des règles dynamiques.

Système de prévention d'intrusion réseau



Système de Prévention d'intrusions (IPS)

HIPS (Host Intrusion Prevention System)

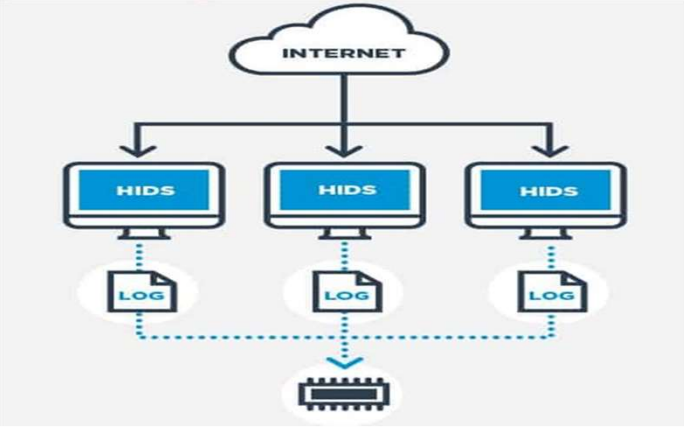
- Aujourd'hui, les menaces évoluent rapidement, il est nécessaire de disposer d'une protection capable d'arrêter les malwares avant la publication d'une mise à jour de la détection spécifique. Un système de prévention d'intrusions sur l'hôte ou HIPS (Host Intrusion Prevention System) est destiné à **arrêter les malwares**, avant qu'une mise à jour de la détection spécifique ne soit publiée, en **surveillant le comportement du code**.

- La majorité des solutions **HIPS** surveillent le code lors de son exécution et interviennent si le code est considéré suspect ou malveillant. **HIPS** précède l'action des **HIDS** en ce sens qu'il est « résident », c'est à dire actif en Permanence, dès le lancement du système et jusqu'à son arrêt.

- Comme un **HIDS**, il se doit de protéger l'intégrité du système d'exploitation, des logiciels applicatifs lancés, des informations stockées, soit en mémoire RAM soit dans le système de fichiers, les fichiers journaux ou ailleurs, et de vérifier que leur contenu demeure intègre, mais en permanence. Il doit contrôler instantanément tout ce qui change dans l'ordinateur et veiller à ce que rien ne contourne la politique de sécurité, que l'agression vienne de l'intérieur ou de l'extérieur (Surveillance des activités en réseau intranet ou internet).

- En plus, un **HIPS** cherche à détecter des anomalies qui indiqueraient un risque potentiel en vérifiant les activités du PC et prend des mesures protectrices.

Système de prévention d'intrusion sur hôte



Différences entre IDS et IPS

Les **IPS** sont souvent considérés comme des **IDS** de deuxième génération. Bien qu'il s'agisse d'un abus de langage, cette expression traduit bien le fait que les **IPS** remplacent petit à petit les **IDS**. Il est pour autant prématuré de dire que les **IDS** sont morts, comme l'avait prétendu Gartner Group.

- En fait, les **IPS** ont avant tout été conçus pour lever les limitations des **IDS** en matière de réponse à des attaques. Alors qu'un IDS n'a aucun moyen efficace de bloquer une intrusion, un **IPS** pourra, de par son positionnement en coupure, bloquer une intrusion en temps réel. En effet, le positionnement en coupure, tel un firewall ou un proxy, est le seul mode permettant d'analyser à la volée les données entrantes ou sortantes et de détruire dynamiquement les paquets intrusifs avant qu'ils n'atteignent leur destination.

- Une autre limite à laquelle devaient faire face les **IDS** il y a quelques années était due à leur incapacité à gérer les hauts débits du fait d'une architecture logicielle. Plusieurs constructeurs ont intégré des circuits spécifiques (ASICs) dans leurs sondes **IPS**, si bien que le débit devient de moins en moins une problématique.