Veille Technologique

Les IDS/IPS, ou Système de détection et de prévention d'intrusion

Problématique

Comment les systèmes de détection et de prévention d'intrusions permettent-ils de protéger un réseau ?

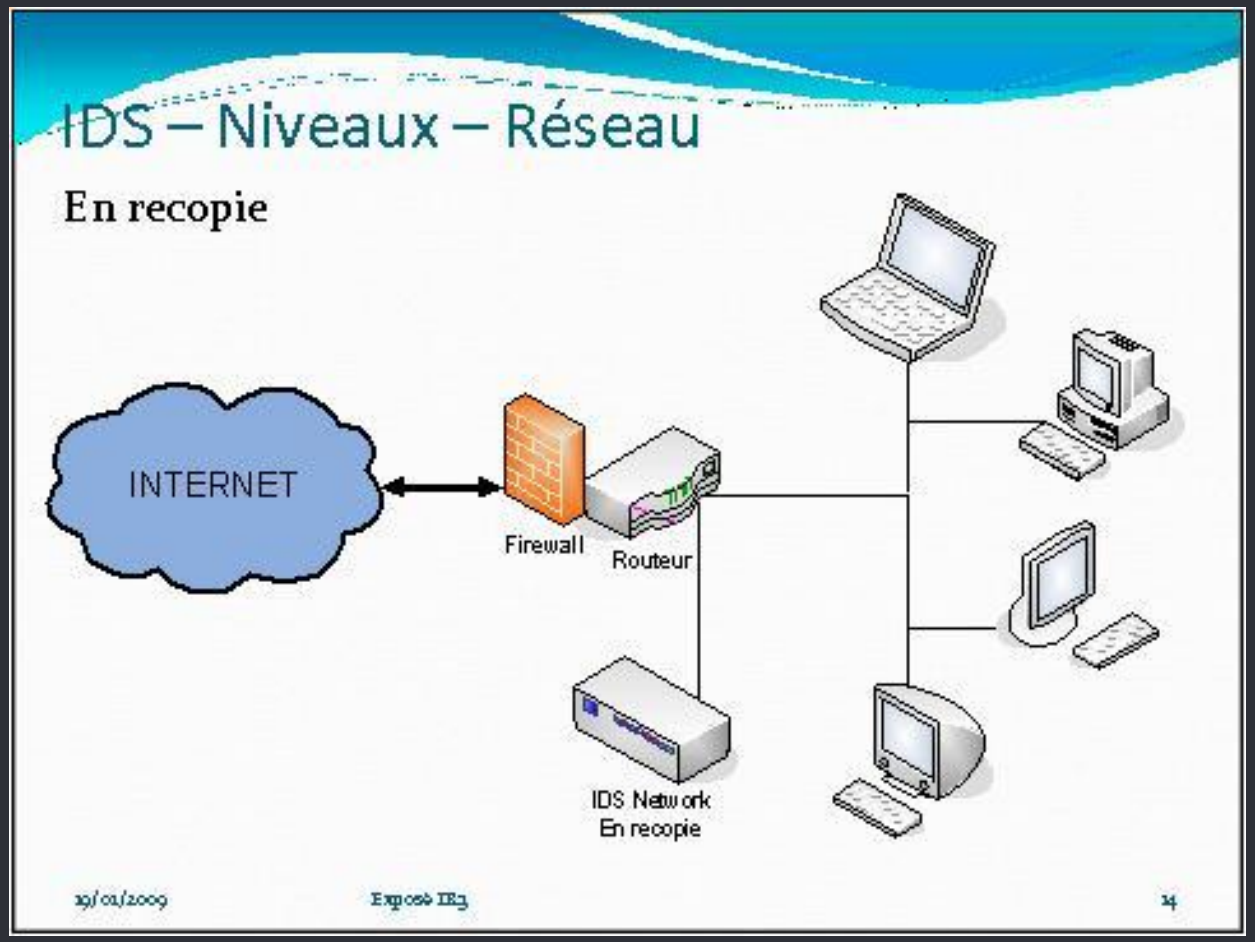
Points abordés

1) Principes généraux des technologies étudiés
2) Les Systèmes de Détection d'intrusions (IDS)
   - 2.1) Le NIDS
   - 2.2) Le HIDS
3) Les Systèmes de Prévention d'intrusion (IPS)
   - 3.1) Le NIPS
   - 3.2) Le HIPS

IDS (Intrusion Detection Système)

Ou système de détection d'intrusion

1



Désigne un mécanisme destiné à repérer des activités suspectes et anormales au sein d'un réseau.

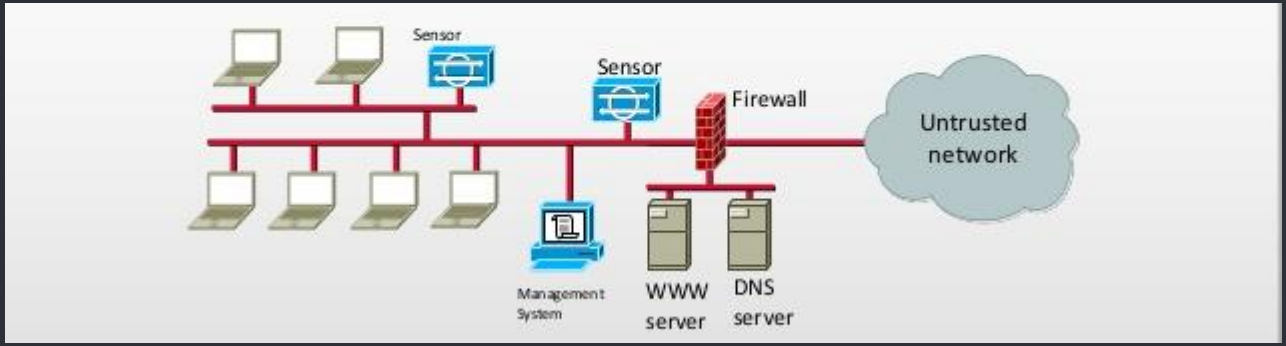
Il existe plusieurs technologies d’IDS :

- NIDS
- HIDS
- IDS Hybride

NIDS

- Sonde les points critiques du réseau

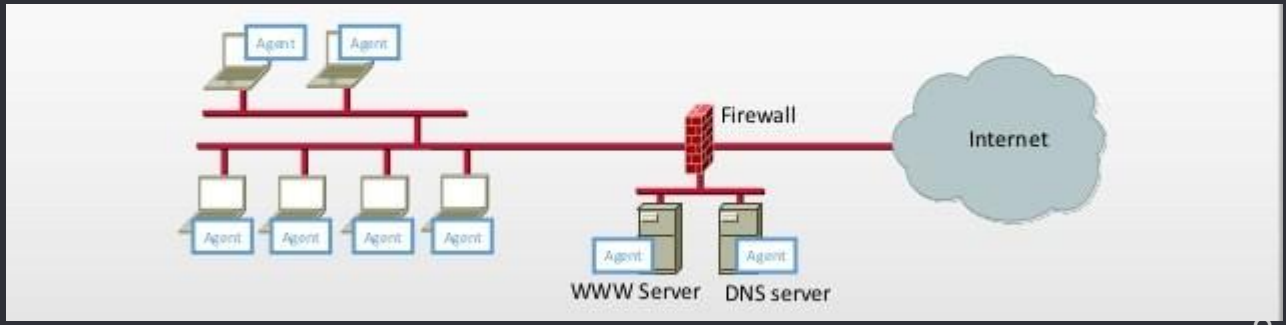
- Ecoute + analyse en temps réel sur le réseau
  - Signatures
  - Patterns



HIDS

- Postes du réseau

- Surveillances des postes :
  - Journaux
  - Intégrité des fichiers
  - Accès au système



IDS Hybrid

Combine les fonctions NIDS et HIDS en effectuant des recherches par signature et par anomalies, sur l'ensemble du réseau (postes et éléments critiques compris)

IPS (Intrusion Prevention Système)

Ou système de prévention d'intrusion

2

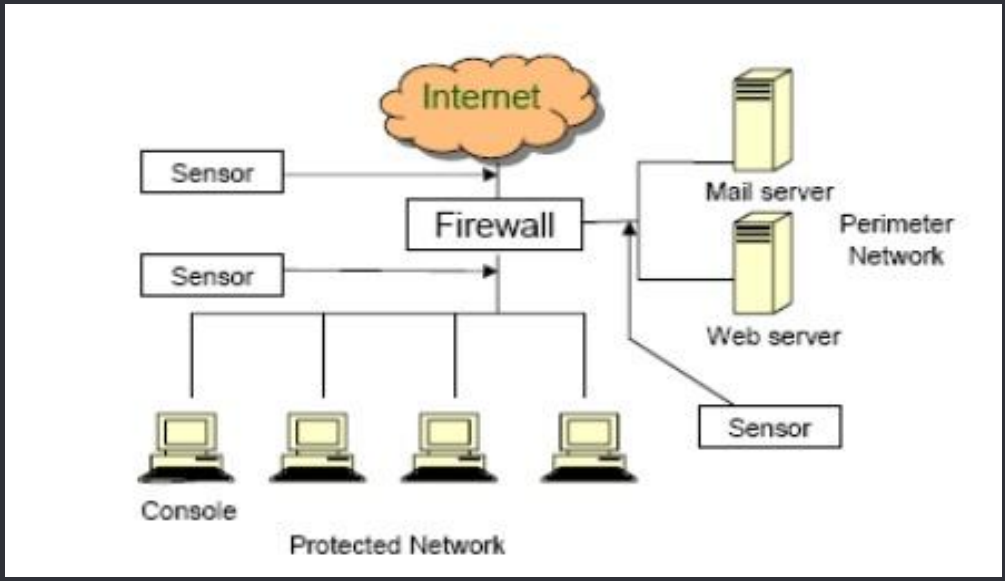
Vu comme un IDS actif, un IPS est capable de prendre des mesures contre les différents attaques signalés par un IDS.

Système de prévention d'intrusion

- Il existe plusieurs technologies d'IPS :
  - NIPS
  - HIPS
  - KIPS

NIPS

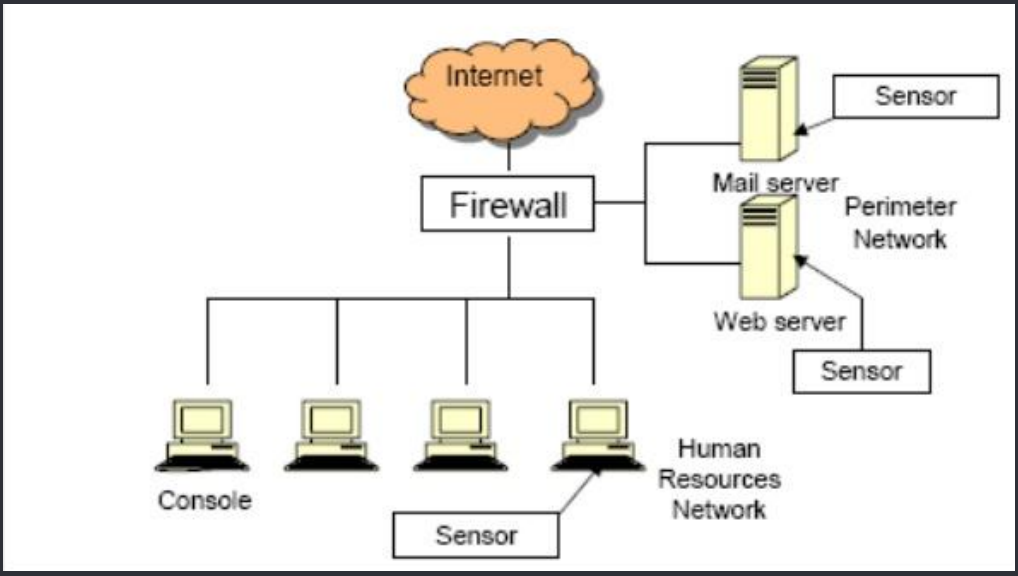
- IPS qui surveille le trafic réseau
  - Termine des sessions suspectes
  - Surveille les connexions aux réseaux wifi (WIPS)



Système de prévention d'intrusion

HIPS

- IPS qui surveille les postes
  - Processus
  - Drivers
  - DLL
- Détruit les processus suspects



KIPS

- IPS qui surveille les tentatives d’intrusions au niveau du noyau des machines.

Sources

- https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_d%C3%A9tection_d%27intrusion
- http://lehmann.free.fr/RapportMain/node10.html
- http://www.iaesjournal.com/online/index.php/IJINS/article/view/1753
- http://www.commentcamarche.net/
- https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_pr%C3%A9vention_d%27intrusion

Des Questions ?