Systèmes IPS (Intrusion Prevention System)

Définition

Un IPS est un dispositif de sécurité réseau qui :

- Surveille le trafic en temps réel.
- Détecte les attaques (comme un IDS).
- Bloque automatiquement le trafic malveillant.

Il agit donc en prévention, contrairement à l'IDS (Intrusion Detection System) qui se limite à l'alerte.

Fonctionnement général

1. Inspection du trafic : analyse des paquets réseau (protocole, contenu, signature).
2. Détection : comparaison avec une base de menaces connues + détection comportementale/anormale.
3. Action préventive :
    - Bloquer ou rejeter le paquet.
    - Réinitialiser la connexion.
    - Modifier la règle du firewall.
    - Isoler l'hôte attaqué.

Méthodes de détection

- Basée sur signatures : comparaison avec une base de données (comme antivirus).
- Basée sur anomalies : détection d'un comportement réseau inhabituel.
- Basée sur politiques : règles définies par l'administrateur (ex : bloquer Telnet).
- Basée sur heuristique / IA : analyse intelligente des comportements suspects.

IPS physique – Logiciel – Host IPS

L'IPS physique est une appliance dédiée (un boîtier matériel) qu'on installe dans le réseau.

- Exemples :
  - Cisco Firepower IPS
  - Palo Alto Threat Prevention
  - Fortinet FortiIPS
- Il ressemble à un switch/pare-feu physique avec ses ports réseau.
- Avantage : très performant (puissance dédiée, support constructeur).
- Inconvénient : coûteux.

L'IPS logiciel :

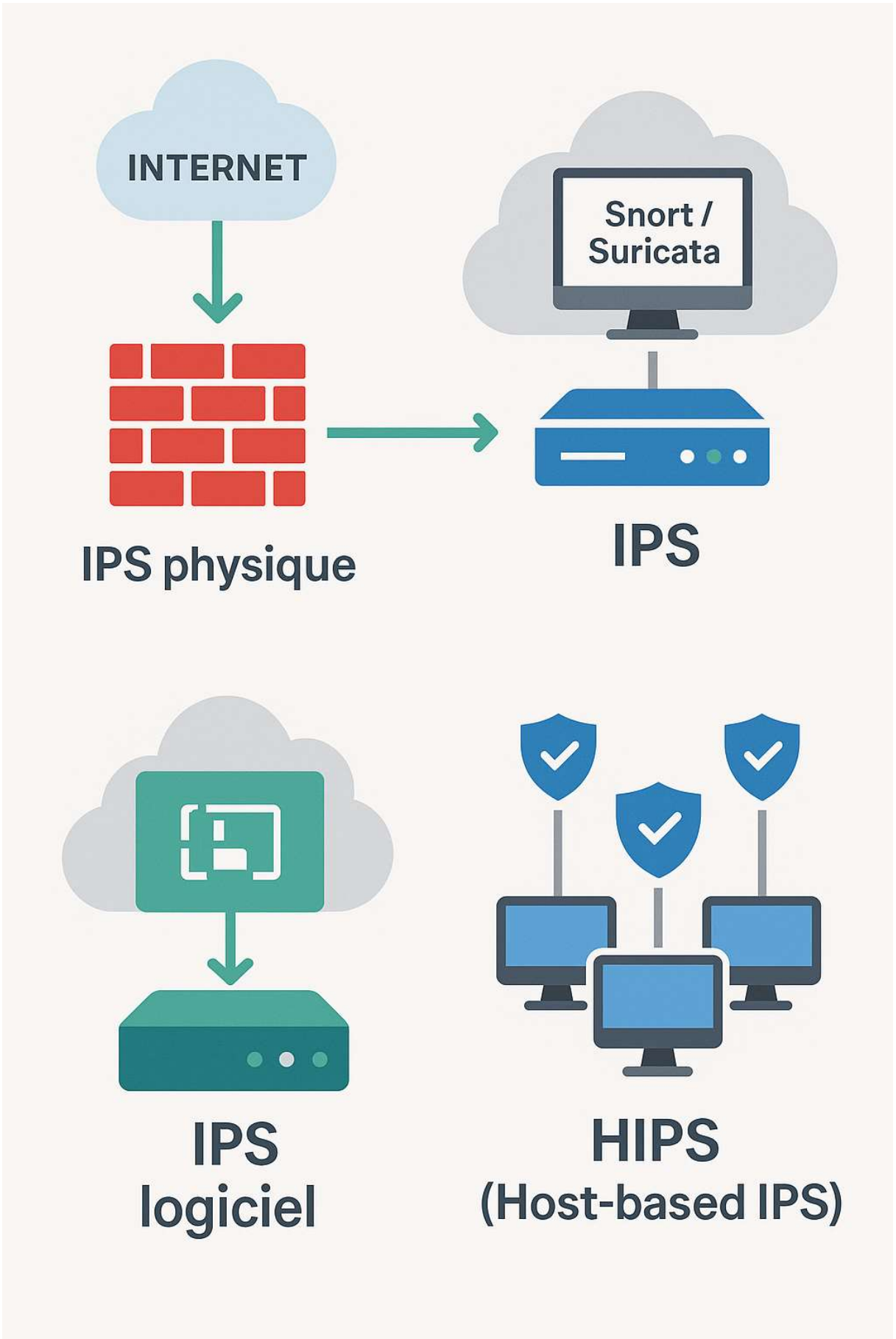
- C'est un programme qui tourne sur un serveur ou une VM.
- Exemples : Snort, Suricata, OSSEC, Wazuh.
- Peut être intégré dans un pare-feu logiciel (ex : pfSense + Suricata).
- Avantage : gratuit ou moins cher, flexible.
- Inconvénient : demande plus de configuration et de ressources CPU.

Et l'HIPS (Host IPS) lui est :

- Installé comme un logiciel agent sur les serveurs/PC.
- Exemple : Symantec Endpoint Protection HIPS, OSSEC.

Types d'IPS

- Network-based IPS (NIPS) : placé sur le réseau (entre switch/routeur).
- Wireless IPS (WIPS) : protège les réseaux Wi-Fi.
- Host-based IPS (HIPS) : installé directement sur une machine (analyse locale).
- Network behavior analysis (NBA) : détecte anomalies de trafic (DoS, scan, botnet).


INTERNET
Snort / Suricata
IPS physique
IPS
IPS logiciel
HIPS (Host-based IPS)

Installation d'un IPS

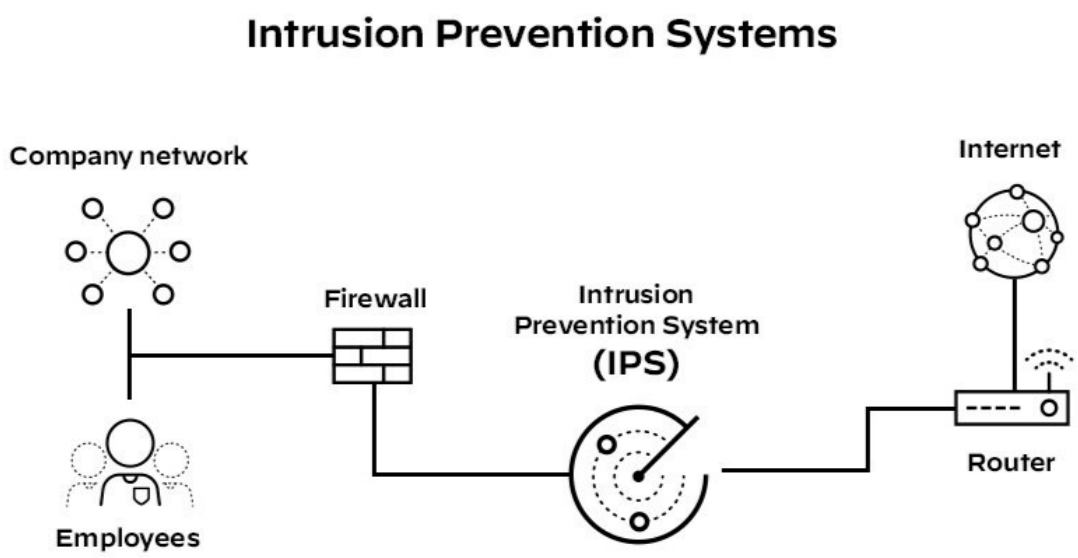
- NIPS (Network-based IPS) → installé dans l'infrastructure réseau.
- HIPS (Host-based IPS) → installé directement sur les serveurs/PC.

Installation d'un NIPS (réseau)

1. Matériel dédié ou appliance virtuelle (Cisco Firepower, Snort, Suricata, Palo Alto, etc.).
2. Placement :
    - En général juste derrière le pare-feu, pour analyser le trafic entrant/sortant.
    - Il doit être en inline mode (dans le chemin du trafic, pas seulement en écoute comme un IDS).
3. Configuration initiale :
    - Définir les zones de réseau protégées.
    - Charger les règles/signatures (ex : Snort rules).
    - Définir la politique d'action (alerter, bloquer, réinitialiser, logguer…).
4. Tests : simuler une attaque (scan Nmap, injection SQL test) pour vérifier la réaction.

Installation d'un HIPS (hôte)

1. Installer un logiciel IPS sur la machine cible (Windows/Linux).
    - Exemples : OSSEC, Wazuh, Symantec HIPS.
2. Configuration :
    - Définir les règles (ex : bloquer exécution de script Powershell inconnu).
    - Surveiller fichiers systèmes, registres, processus.
3. Intégration avec SIEM / logs centralisés.



Points clés à retenir

- IPS réseau → placé stratégiquement (entre firewall et LAN).
- IPS hôte → installé directement sur serveurs ou postes critiques.
- Toujours mettre à jour les signatures.
- Bien régler la sensibilité pour éviter les faux positifs.