IDS & IPS

Par Patrick Sentinel – 29a.ca

🕵️‍♂️🔔 IDS & IPS : ces potins de réseau qui te sauvent la vie

Tu as enfin sécurisé ton pare-feu, mis un mot de passe de 27 caractères, et désactivé ton Wi-Fi invité. Tu es prêt. Invincible. Mais voilà… tu entends un bruit bizarre dans ton réseau. Un petit "ping" de trop. Un "port scan" suspect. Un trafic étrange à 3 h du matin. Félicitations, tu viens de découvrir que ton réseau a **besoin d'un détective**.

Bienvenue dans le monde merveilleux des **IDS** et **IPS** : les commères numériques qui surveillent, dénoncent et (parfois) frappent les intrus sans pitié comme dans les villages reculés du Québec (ne vous inquiétez pas ça n'arrive pas que les gens des villages frappent les intrus, c'est juste une bulle qui m'a montée au cerveau).

👀 IDS vs IPS : la différence entre regarder… et frapper

🧠 IDS (*Intrusion Detection System*)

C'est le gars assis avec des jumelles, qui note tout ce qui bouge et t'envoie un message style : « Heu… quelqu'un essaie de s'introduire chez toi. Je dis ça, je ne dis rien. » Il détecte. Il alerte. Il ne réagit pas. Il est passif, mais informé. Comme un concierge de film qui dit "j'avais prévenu" ou ta belle-maman qui te dit « Je te l'avais dit que ça arriverait ».

💪 IPS (*Intrusion Prevention System*)

Lui, il ne rigole pas et il est sérieux. Il surveille **ET** intervient. Il voit un paquet bizarre? Il le bloque. Un comportement étrange? Il bannit l'IP. Il agit avant que tu comprennes ce qui se passe. C'est un IDS… sous stéroïdes (comme *Ben Johnson* dans les années 80 pour ceux qui sont d'un certain âge 😉).

🤼 Comment ces systèmes détectent les méchants

1. *Signature-Based*

Comme un antivirus. Il reconnaît les modèles connus de vilains (exemple : « si ça ressemble à un cheval de Troie… c'est probablement un cheval de Troie »).

2. *Anomaly-Based*

Il surveille le comportement "normal" de ton réseau. Et dès qu'il voit un truc étrange, il dit : « Pourquoi le frigo essaie-t-il de contacter la Chine à 4 h du matin? »

3. *Heuristic-Based*

Un genre de mix intelligent. Il tente de deviner si un truc est bizarre, même s'il n'a jamais vu ce type d'attaque.

🔧 Concrètement, où on installe ça?

- Sur un **pare-feu *Next-Gen***;
- Dans un **réseau d'entreprise** qui ne veut pas se faire chiffrer par un ransomware;
- Chez toi, si tu es très sérieux… ou très parano 😅;
- Dans une VM, pour tester si ce que tu installes est un gentil pingouin ou un loup déguisé en .deb.

🧩 Les problèmes classiques

- **Trop d'alertes** : Ton IDS devient une alarme incendie de parano, qui sonne pour *chaque miette*. Ça c'est ce qu'on appelle des 'Faux positifs' dans notre jargon;
- **Faux positifs** : Tu bloques ton propre imprimante *Wi-Fi*. Merci champion;
- **Faux négatifs** : Tu penses que tout va bien… alors qu'un botnet est déjà en train de chanter *Thriller* dans ton NAS.

🛡️ Astuces pour utiliser un IDS/IPS sans devenir fou :

- Apprends à lire les logs sans pleurer;
- Ajoute des règles progressivement;
- N'ignore pas les alertes, même si elles te réveillent à 2 h (dans un contexte d'entreprise bien sûr);
- Ne laisse pas ton système tout bloquer automatiquement (à moins que tu veuilles bannir ta propre montre connectée).

🧘 Conclusion :

L'IDS/IPS, c'est le commis du dépanneur de ton réseau. Il te regarde avec suspicion, note tout, et appelle la police si quelqu'un met un *hoodie*. Mais entre toi et le chaos numérique, parfois il est la seule chose qui te sépare d'un ransomware qui danse dans ton salon. Alors installe un IDS. Ou un IPS. Ou les deux. Et rappelle-toi :

Un bon système d'intrusion, c'est comme une belle-mère vigilante : parfois envahissant, mais toujours à l'affût du moindre faux pas.
