IDS a IPS (Systémy detekce a prevence průniku)

IDS a **IPS** jsou bezpečnostní technologie, které monitorují síťový provoz a hledají v něm škodlivou aktivitu nebo porušení bezpečnostních pravidel. Často jsou integrovány přímo do moderních firewallů (tzv. Next-Generation Firewalls - NGFW).

Základní rozdíl: IDS vs. IPS

Hlavní rozdíl spočívá v tom, jak systém reaguje na nalezenou hrozbu:

IDS (Intrusion Detection System)

* **Role:** Pasivní pozorovatel (detekce). * **Funkce:** Monitoruje provoz a v případě detekce hrozby odešle varování (alert) správci. Samotný provoz však **neblokuje**. * **Umístění:** Obvykle připojen k zrcadlenému portu (SPAN/TAP), aby neovlivňoval propustnost sítě.

IPS (Intrusion Prevention System)

* **Role:** Aktivní ochránce (prevence). * **Funkce:** Monitoruje provoz a v případě detekce hrozby **automaticky zasáhne** (zahodí pakety, ukončí spojení). * **Umístění:** Musí být zapojen „v cestě“ (inline) – veškerý provoz přes něj fyzicky protéká.

Metody detekce hrozeb

Oba systémy využívají k odhalení útočníka několik metod:

1. **Signatury (Signature-based):** Porovnává provoz s databází známých vzorků útoků (podobně jako antivirus). Je velmi přesný na známé hrozby, ale neumí odhalit nové (Zero-day) útoky.
2. **Anomálie (Anomaly-based):** Učí se, jak vypadá „normální“ provoz v síti. Pokud dojde k náhlé změně (např. obrovský nárůst UDP provozu), vyhodnotí to jako útok.
3. **Analýza protokolů:** Kontroluje, zda pakety dodržují standardy (RFC). Např. pokud se v HTTP provozu objeví nečekané binární znaky, může jít o pokus o Buffer Overflow.

Umístění v síti

Podle toho, co systémy chrání, je dělíme na:

- **NIDS / NIPS (Network-based):** Chrání celou síť nebo segment. Jsou umístěny na strategických bodech (např. za hraničním firewallem).

- **HIDS / HIPS (Host-based):** Instalovány přímo na konkrétním zařízení (serveru, endpointu). Sledují logy, systémové volání a integritu souborů.

Srovnání v tabulce

Vlastnost	IDS	IPS
Akce	Pouze upozorní (Alert).	Upozorní a zablokuje (Block).
Vliv na síť	Žádný (běží kopie dat).	Může způsobit zpoždění (latenci).
Riziko chyby	Žádné (jen falešný poplach).	Kritické (může zablokovat legitimní provoz – False Positive).
Vhodné pro	Monitoring, analýzu, forenziku.	Aktivní obranu v reálném čase.

> **Pozor na False Positives:** Největší výzvou pro správce IPS je odladění pravidel tak, aby systém neblokoval běžnou práci uživatelů. Pokud je IPS nastaveno příliš přísně, může omylem odstavit důležitou podnikovou službu.

— **Viz také:** SIEM, Firewall, SOC, Honeypot