IDS/IPS

IDS/IPS

- Hálózat kritikus pontjaira elhelyezett behatolás érzékelés és való idejű beavatkozás.
- Képes érzelni
  - gyanús csomagolzat
  - normálistól eltérő forgalom mintázat
  - IDS -> Behatolás érzékelés
  - IPS -> Való idejű ellenintézkedések

Tervezési megfontolások

- Védelem -> Biztonsági politika kialakítása
- Érzékelés -> Támadások észlelése
- Elhárítás -> Válaszlépés megtétele
- Értékelés -> Kockázatelemzés, haszonelemzés
- Javítás -> Megfelelő technológia alkalmazásával ellenintézkedések megvalósítása

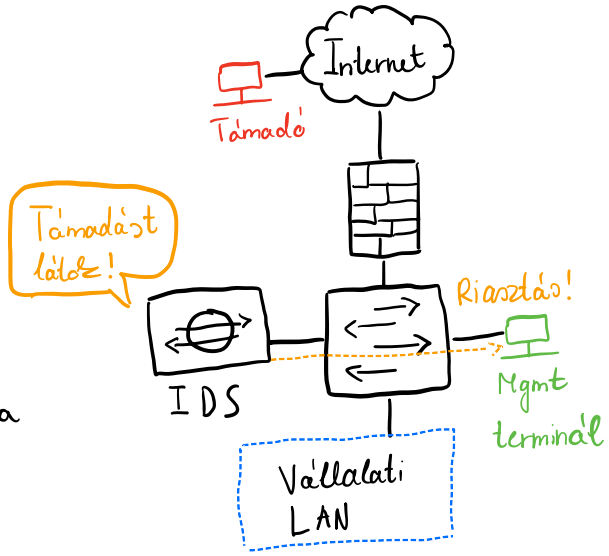
IDS

- Előnye
  - Nincs negatív hatással a hálózati forgalomra
- Hátrányai
  - Nem skálázható és a rosszindulatú támadásoknak a célba jutását nem tudja megakadályozni.

IPS

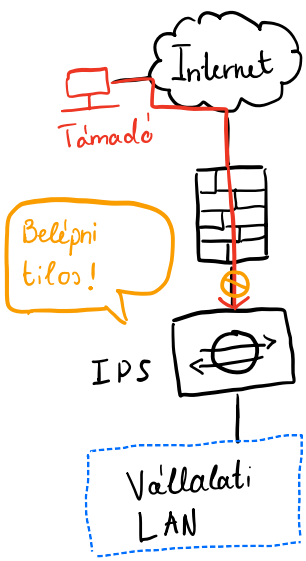
- Előnye
  - Single-Packet támadásokat megállítja
  - Real-time figyeli a forgalmat
  - 3. és 4. rétegben figyel
- Hátrányai
  - Negatívan érinti a hálózati teljesítményt (latency, jitter)
  - Kieséskor megszakad a hálózati forgalom.

• Host-alapú IPS megoldások



- Lényege, hogy a kliensre egy szoftvert telepítenek, ami monitorozza a gépen végzett tevékenységeket.
- Előnyei
  - OS-re tipikus támadásokat figyeli
  - Szokásostól eltérő műveleteket is detektálja
- Hátrányai
  - Csak lokális
  - Minden gépen implementálni kell
  - Nem ismeri az egész hálózatot, mivel a hálózat végén van

• Hálózat alapú IPS megoldások



- Host-alapú szenzorok nem tudják megvédeni a hálózatot!
- Ezeket a szenzorokat a hálózat megfelelő pontjaira kell telepíteni a maximális biztonság eléréséhez
- Előnyei
  - Költséghatékony
  - Hálózaton transzparens
  - Alacsony szintű hálózati eseményeket is látja
- Hátrányok
  - Titkosított forgalmat nem látja
  - Nem tudja a támadás sikerességét
- Port mirroring → Port analizáló (Cisco SPAN

- signature alapú IPS rendszerek
  - Olyan biztonsági megoldások, amik a hálózati forgalom ellenőrzésére használnak aláírásokat.
  - Ezek az aláírások egyedi azonosítók, amik a hálózati támadásokra jellemző mintákat és jellemzőket tartalmazzák.
  - Figyelik a hálózati forgalmat és ha találnak egy aláírást, akkor riasztanak.
  - Gyors reakcióideje van
  - Magas fokú pontosság és könnyű kezelhetőség
  - Javasolt olyan környezetekben használni, ahol a hálózati forgalom ellenőrzése és szabályozása fontos szempont.
- Minta alapú
  - Előre definiált mintázat keres a forgalomban.
  - Atomi és összetett mintázatot is felismer.
  - Előnye -> Könnyen konfigurálható és kevesebb hibás pozitív eredmény.
  - Hátrányai
    - Eddig nem ismert hibákat nem tudja felismerni.
    - Kezdetben sok a hibás pozitív eredmény.
    - Mintákat folyamatosan frissíteni kell.
- Anomália
  - Normál profilt kell létre hozni, ahol meg kell határozni mi a normál működés és minden ami attól eltér, az negatív.
  - Előnyei
    - ismeretlen támadási fajta detektálható.
    - Elég normális mintát meghatározni, nem kell minden támadási fajtára.
  - Hátrányai
    - Nem mondja meg, hogy pontosan milyen támadás történik
    - Normál működést meg kell határozni.
    - Tanulási időszakban támadásmentesnek kell lennie a hálózatnak, különben az lesz a normális.

- Policy alapú
  - Nem mintázat határoz meg, hanem viselkedéseket.
  - Riaszt, ha történik valami.
  - Mindenre alkalmazkodik
  - Előnye -> Ismeretlen támadások detektálása
  - Hátrányai
    - Nehéz nagy profilokba kategorizálni a hálózati forgalmat nagy hálózaton
    - Nem változhat a hálózati forgalom profilja.
- Honeypot
  - Álszervereket állít a hálózatba, hogy azt támadják
  - Adatokat gyűjt a támadásokról, így finom hangolva az IDS/IPS szenzorait.
  - Biztonsági cégek alkalmazzák kutatás céljából.
  - Előnyei
    - Megléveszti, klasszifikálja a támadókat.
    - Információkat gyűjt a támadásról.
  - Hátrányai
    - Dedikált szervert, erőforrást igényel.
- Riasztások típusai
  - False positive -> Elvárt, de nem kívánt riasztás.
  - False negative -> Rendszer nem ismeri fel a támadást.
  - True positive -> Helyesen ismeri fel a támadást.
  - True negative -> Helyes működésnél nem riaszt.
- Riasztások kezelése
  - Figyelmeztetés
  - Logolás
  - TCP kapcsolat reset
  - Aktivitás megszakítás
  - Jövőbéli kapcsolat blokkolása