# 1.a Ismertesse a határforgalomirányítók védelmének különböző területeit, majd mutassa be az egyes területeken alkalmazható megoldásokat!

# Határforgalomirányító

* Hálózat külső és belső rendszerének határán található eszköz.
* **Célja**
  + Adatintegritás és adatvédelem megvalósítása.
* **Védelme**
  + Legelső szenzitív pont
  + Hálózatnak az első védelme

# Védekezés

## Eszköz védelem - Router hardening

* Jelszavas védelem
* AAA – (Authentication, Authorization, Accounting)
* Privilege level

## Fizikai védelem

* Zárt, jól szellőző terem
* Port védelem
  + IDS/IPS

## Szoftver védelem

* Nem használt szolgáltatások letiltása

# AAA

## Authentication

* Hitelesítés megvalósítható felhasználónév jelszó párokkal, kihívás és válasz üzenetekkel,

token, smart cards

## Authorization - Jogosultságkezelés

* Mely erőforrásokhoz férhetnek hozzá a felhasználók, milyen műveleteket végezhetnek

## Accounting – Könyvelés

* Naplózza → mit csinált/változtatott a felhasználó, milyen erőforrást és mennyi ideig ért el

## AAA Authentication

* Felhasználónevek és jelszavak tárolása
  + Local
    - lokálisan a Cisco forgalomirányítókon tárolja, ez alapján hitelesíti a felhasználókat.
    - Kis hálózatokban
  + Server-based
    - központi AAA szerveren
    - Több hálózati eszközt tartalmazó hálózat esetén

# Szerver alapú AAA megvalósítására használható protokollok

|  |  |  |
| --- | --- | --- |
|  | TACACS+ | RADIUS |
| Funkcionalitás | AAA-t részekre osztja, modularitást  lehetővé teszi | Kombinálja az hitelesítést és a jogosultságkezelést, külön  könyvelés. Ezáltal nem olyan  rugalmas, mint a TACACS+ |
| Támogatottság | Cisco | Nyitott/RFC standard |
| Szállítási protokoll | TCP | UDP |
| CHAP | Kétirányú hívás és válasz, mint a  Challenge Handshake Authentication Protocol (CHAP) | Egyirányú a RADIUS szerver és kliens között |
| Bizalmasság | Egész csomag titkosított | Csak a jelszó titkosított |
| Testreszabhatóság | biztosítja az útválasztó parancsok jogosultságkezelését felhasználónként  vagy csoportonként | nem biztosítja |
| Könyvelés | Limitált | Széleskörű |

# IPS és IPS rendeltetése

* Behatolás érzékelő eszközöknek a hálózat kritikus forgalmat átbocsátó pontjaira helyezésével a nem kívánt vagy jogosulatlan forgalom érzékelése és valós idejű beavatkozás is elvégezhető.

## IDS és IPS alapfunkciók

* **Érzékelik**
  + Gyanús csomagokat
  + Illegális tevékenységre utaló adattartalmakat
  + Normálistól eltérő forgalom mintákat
  + Küszöb értékeket meghaladó mennyiségű csomagokat
  + IDS jelzi a behatolás tényét
  + IPS valós időben ellenintézkedéseket tesz a támadás megelőzésére

## Tervezési megfontolások

* **Védelem:** Biztonsági politika kialakítása és megvalósítása megfelelő technológia alkalmazásával.
* **Érzékelés:** Támadások észlelése
* **Elhárítás:** Válaszlépés megtétele
* **Értékelés:** Kockázatelemzés, ellenintézkedések és költség/haszon elemzés
* **Javítás:** Kiválasztott ellenintézkedések megvalósítása

## Szolgáltatások és lehetőségek

### IDS

* **Előnyei:** Nem érinti negatívan a hálózati forgalmat.
* **Hátrányai:** Nem skálázható és a rosszindulatú csomag célba juttatását nem akadályozza meg.

### IPS

* **Előnyei:**
  + Single-packet támadásokat megállítja
  + Real-time figyeli a forgalmat
  + Harmadik és negyedik rétegben figyel
* **Hátrányai:**
  + Negatívan érinti a hálózati teljesítményt (latency, jitter)
  + Kieséskor megszakad a forgalom