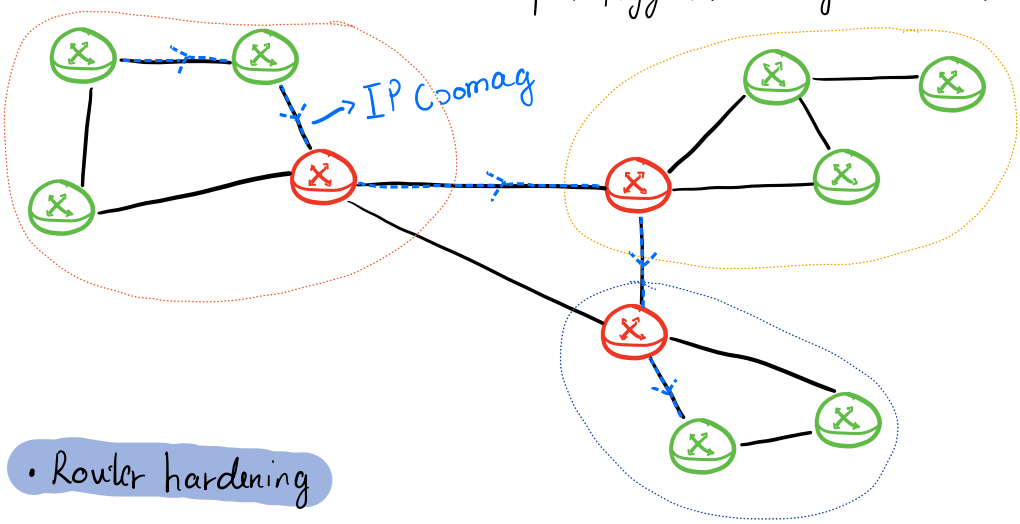
Határforgalomirányítók védelme

• Védelme

- Ha nem lenne, a csomagok oda-vissza "patognának".
- Hálózat gerince, "első" szenzitív pont, így rendkívül fontos a védelme.



• Router hardening

- AAA
- Jelszavas védelem
- Privilege level

• Fizikai védelem

- Zárt, jól szellőző terem
- Port védelem -> IDS/IPS

• Szoftveres védelem

- Nem használt portokat és szolgáltatásokat ki kell kapcsolni

• AAA

- 3 komponensből tevődik össze
  - Authentication → Bejelentkeztetés, adatbázis alapján
  - Authorization → Jogosultságkezelés, ki, mit érhet el
  - Accounting → Könyvelés/naplózás, ki, mit csinál
- Konfigurálható lokálisan és szerver alapon
  - Lokálisan általában kis hálózatokban használják
  - Szerver alapon több eszközös, nagyobb hálózatokban
- Nagy előnye, hogy szálazható, ezáltal tudunk "fallback" eszközöket használni, mint backup.
- Autentikáció folyamata:
  1. Router kéri a belépési adatokat.
  2. Felhasználó megadja
  3. AAA szerver ellenőrzi adatbázisban
- Autorizáció folyamata:
  1. Felhasználó csinál valamilyen tevékenységet
  2. AAA ellenőrzi az engedélyt
  3. Visszatér egy "PASS/FAIL" üzenettel
- AAA hálózati protokollok
  1. Tacacs+
  2. RADIUS

Tacacs+	RADIUS
• Modularizálható	• Authentication-t és Authorization-t kombinálja, Accounting-ot külön
• TCP szállítási protokoll	• UDP szállítási protokoll
• Csomagot titkosítja	• Jelszót titkosítja
• Könyvelés limitált	• Könyvelés ragalmas

• IDS/IPS

- Hálózat kritikus pontjaira elhelyezett behatolás érzékelés és való idejű beavatkozás.
- Képes észlelni
  - gyanús csomagokat
  - normálistól eltérő forgalom mintázat
  - IDS -> Behatolás érzékelés
  - IPS -> Valós idejű ellenintézkedések

• Tervezési megfontolások

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

• IDS

- Előnye
  - Nincs negatív hatással a hálózati forgalomra
- Hátrányai
  - Nem skálázható és a rosszindulatú támadásoknak a célba juttását 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)
  - Kiesésnél megszakad a hálózati forgalom.