Állapotlaró tűzfal

• Tűzfal feladata

- Szoftveres vagy hálózatbiztonsági eszköz.
- Be- és kimenő forgalmat figyelik szabályok alapján.
- Előnyei
  - Nem befolyásolják negatívan a hálózat működését, biztonságot nyújt.
- Hátrányai
  - Általános szabályok alapján működnek.
  - Letilt olyan szolgáltatást, amik nem is veszélyesek.
  - Lehet, hogy lassítja a hálózat működését, így a szolgáltatások minősége romolhat.
  - Nem megfelelő konfiguráció esetén, nem lesz jó a védelem.
  - Nem véd olyan támadásoktól, amik nem mennek rajta keresztül.

• Context-Based Access Control - CBAC

- Fő funkciói
  1. Állapotfelvő szűrés - Stateful Packet Filtering -> Nem csak hálózati és szállítási réteg információk alapján vizsgálja a viszonyok állapotát, hanem alkalmazási réteg információkat is.
  2. Forgalom figyelés - Traffic Inspection -> SYN Flood támadások, TCP sorszámozást figyel és gyanúsakat eldobja.
  3. Behatolás érzékelés - Intrusion Detection -> Syslog üzenetek átvizsgálásával ki lehet szűrni az SMTP támadások és SYN Flood támadások nagyságát, ezeket a kapcsolatokat eldobja és riasztást, értesítést küld a rendszernek.

• CBAC működése

- TCP, UDP és ICMP kapcsolatokról információt tárol az állapot táblában. (state table)
- Állapot tábla alapján dinamikusan ACL-t hoz létre a visszajövő csomagok számára.
- CBAC ideiglenes nyílásokat hoz létre megadott kapcsolathoz, amik beengedik a blokkolt forgalmat.
- Az állapottábla automatikusan frissül a forgalom áramlásának megfelelően.

• CBAC konfigurálása

1. Interfész kiválasztása -> Belső interfész ahonnan indulhat egy viszony felépítés.
2. ACL konfigurálás az interfészen -> Milyen típusú forgalmat engedélyezünk az interfészen
   - Alap konfiguráció, hogy a belső hálózatról a külső hálózatig mindent, de a külső hálózatról a belső hálózatig semmit.
   - Engedélyezzük azt a forgalmat, amit meg kell vizsgálni a CBAC-nak.
   - Implicit deny-t legyük explicitté a naplózás miatt.
3. Inspection rule megadása a vizsgált forgalomra
4. Alkalmazás a megfelelő interfészen.