

8.a Milyen állapotartó tűzfal konfigurálható a forgalomirányítókön? Mutassa be a működés elvét, jellemzőit és a beállítás lépéseit!

Tűzfalak feladata és rendeltetése

- Szoftveres vagy hardveres hálózatzbiztonsági eszköz.
- A tűzfalak a hálózatba be és kimenő kapcsolatokat figyelik, és csak azokat engedélyezik, amik megfelelnek a beállított szabályoknak.
- **Előnyei:**
 - o Nem befolyásolják negatívan a hálózat működését és biztonságot nyújt
- **Hátrány:**
 - o Általános szabályok alapján működnek.
 - o Letilt olyan kapcsolatokat, amik nem is veszélyesek.
 - o Lehet, hogy lassítja a hálózat működését, így a szolgáltatások minősége romolhat.
 - o Nem megfelelő konfiguráció esetén, nem lesz jó a védelem.
 - o Nem véd olyan kapcsolatokról, amik nem mennek rajta keresztül

Context-Based Access Control – CBAC

- CBAC csak azokat a protokollokat szűri, amiket az adminisztrátor konfigurált
- Csak azokat a csomagokat szűri, amik áthaladnak a routeren.

Fő funkciói

- **Állapotartó szűrés (Stateful packet filtering)**
 - o Nem csak hálózati réteg, szállítási réteg információk alapján, hanem alkalmazási réteg információt is vizsgál, hogy megállapítsa a viszonyok állapotát.
- **Forgalom figyelés (Traffic inspection)**
 - o SYN flood támadások, TCP sorszámozást figyel és gyanúsakat eldobja.
- **Behatolás érzékelés (Intrusion detection)**
 - o Syslog üzenetek átvizsgálásával bizonyos SMTP támadások, SYN Flood támadások, sajátosságait ki lehet szűrni, ezeket a kapcsolatokat eldobja és riasztást, értesítést küld a rendszernek.
 - o CISCO IOS tűzfal 3 küszöbértéket is figyel a TCP DoS támadások kivédésére:
 - Félig megnyitott TCP kapcsolatok száma.
 - Félig megnyitott TCP kapcsolatok száma adott intervallumban.
 - Félig megnyitott TCP kapcsolatok száma egy adott host-tól.

CBAC működése

- **TCP, UDP és ICMP kapcsolatokról információt tárol az állapot táblában (state table).**
- Amikor a hálózaton belüli eszköz munkamenetet kezdeményez, egy dinamikus bejegyzés kerül az állapottáblába és a kimenő forgalom áthaladhat a routeren.
- Ennek a bejegyzésnek a segítségével a kimenő forgalom válasza áthaladhat a routeren, mivel a hálózaton belül kezdeményezett forgalomra is van bejegyzése.
- Ideiglenes lyukakat nyit a bejövő forgalomra alkalmazott hozzáférési listán, hogy engedélyezze a reply csomagokat.

CBAC konfigurálása

1. Interfész kiválasztása

- a. Belső interfész ahonnan indulhat egy viszony felépítés.

2. ACL konfigurálás az interfészen

- a. Milyen típusú forgalmat engedélyezünk az interfészen
 - i. Alap konfiguráció, hogy a belső hálózattól a külső hálózatig mindent, de a külső hálózattól a belső hálózating semmit.
 - ii. Engedélyezzük azt a forgalmat, amit meg kell vizsgálni a CBAC-nak.
 - iii. Implicit deny-t tegyük explicitté a naplózás miatt.

3. Inspection rule megfogalmazása a vizsgált forgalomra

4. Alkalmazás a megfelelő interfészen