# **4.a** Milyen feladat elvégzésére alkalmasak a tűzfalak? Ismertesse a különböző tűzfal architektúrákat és típusokat!

# Tűzfalak feladata és rendeltetése

* Szoftveres vagy hardveres hálózatbiztonsági eszköz.
* A tűzfalak a hálózatba be és kimenő kapcsolatokat figyelik, és csak azokat engedélyezik, amik megfelelnek a beállított szabályoknak.
* **Előnyei:** 
  + Nem befolyásolják negatívan a hálózat működését és biztonságot nyújt
* **Hátrány:**
  + Általános szabályok alapján működnek.
  + Letilt olyan kapcsolatokat, 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 kapcsolatoktól, amik nem mennek rajta keresztül

# Tűzfalak generációi és fejlődésük

## Első generáció – Packet Filtering Firewall

* **Döntését ezekre alapozza:**
  + Forrás / Cél MAC címe, ip címe és port száma
  + IP csomagba beágyazott protokoll

### Működése

* A csomag fejlécben lévő információt **összeveti a tűzfalban megadott szabályokkal.**
* A hálózati és szállítási rétegben működik, adattartalmat nem figyel.
* Alacsony szintű biztonságot nyújt, mert nem vizsgálja a csomag tartalmát.
* Nem kezeli a kapcsolatállapotot
* Kétirányú forgalmat külön szabályokkal kell megadni
* Egész port tartományt engedélyezni kell, mert sok protokoll dinamikusan választ portot kliens oldalon.

## Második generáció – Stateful Firewalls (OSI 5. rétegben dolgozik)

## Tartalmakat vizsgál és figyelembe veszi a felépített kapcsolatokat.

* Figyeli az összes áthaladó hálózati csomagot és megállapítja, hogy:
  + melyik már egy meglévő kapcsolat része
  + melyik kezdeményez új kapcsolatot
  + melyik csomag nem része egyik kapcsolatnak sem
* A felépített kapcsolat információt gyorstárolóban tárolja.
* A kapcsolat csomagjait a gyorsítótárban lévő bejegyzésekkel hasonlítja össze (hatékony)

### Előnyei

* Jobban le lehet írni a hálózati szabályokat (állapotokat).
* Nagyobb biztonságot nyújt, mint a csomagszűrő tűzfalak (sorszámokat folyamatosan követi)

### Hátrányai

* Állapotok kezelése miatt erőforrás igényes és nem mindig képesek megkülönböztetni a biztonságos és a veszélyes adatokat a csomagokban.

## Harmadik generáció – Application Level Firewall

* **Két kategóriája van:** Proxy tűzfalak – Proxy Firewalls, Mély csomag ellenőrző – Deep Packet Inspection

### Előnyei

* Biztonságos, és a puffer túlcsordulás típusú támadásoknak ellenáll, mert figyeli a protokoll fejléc mezőinek hosszát.

### Hátrányai

* Erőforrás igényes, nem megfelelő megvalósításnál gyenge teljesítmény
* Transzparencia hiánya

### Proxy firewalls

* A közvetlen kapcsolat megszakad, a továbbítandó csomagot újraelőállítják, átmásolják az összes protokollréteg szükséges mezőit.
* Alkalmazás szinten képes a parancsok szűrésére.

### Deep Packet Inspection Firewalls

* Transzparensen működik, nem épít fel külön kapcsolatot a két kommunikáló fél között.
* Egyszerre szűri az OSI modell mind a 7 rétegét.
* Figyeli a protokollnak nem megfelelő csomagokat és szűri azokat.
* Csomagokat az alkalmazásoknak megfelelően osztályozza.

### Next Generation Firewalls

* Több hálózatbiztonsági technológia együttes integrációja.
* Olyan megoldás, ami DPI tűzfalat, IDS/IPS eszközöket, antivirus átjárót, proxy megoldást, VPN kiszolgálót, QoS és sávszélesség menedzsmentet biztosít, hogy a lehető legjobban kielégítse a mai kor igényeit.

# Lehetséges Tűzfal topológiák

### Dual-Homed

* Két interfésszel rendelkezik, amik külön hálózatba csatlakoznak és közöttük szűri a hálózati forgalmat.
* Speciális esete, amikor a router a tűzfal (screening router)

### Single-Homed - Screened host

* A szolgáltatást nyújtó (bástya) gép csak a belső hálózatra csatlakozik.
* Elsődleges biztonságot a csomagszűrő forgalomirányító adja, ami megakadályozza, hogy a felhasználói gépek közvetlenül hozzáférjenek az internethez.
* Csomagszűrő forgalomirányítót úgy konfigurálják, hogy az internet gépei csak a bástya géppel léphetnek érintkezésbe.
* Bástya gép biztonsága fontos és proxy-ként működik.
* **Előnyei:**
  + A screened host architektúra nagyobb biztonságot nyújt, mint a dual-homed host architektúra és nincs Single Point Of Failure
* **Hátránya**
  + Screened subnet architektúra biztonságosabb
  + Ha a támadó betört a bástya gépre, onnan már a többi gépet is eléri a LAN hálózaton.

### Single-Homed - Screened subnet

* Screened subnet architektúra újabb biztonsági réteget helyez el az internet és a belső hálózat felé, ez a határ (perimeter) hálózat.
* **Bástya gép sebezhető**
  + Ha a támadó bejut a bástya gépre, még mindig útját állja a belső forgalomirányító.
* **Perimeter hálózat**
  + Ha a támadó bejut a bástya gépre, csak a perimeter hálózat forgalmát lehallgatja, a belső hálózat forgalmát nem láthatja.
  + A perimeter hálózaton megy keresztül a bástya gép és az internetre irányuló forgalom, de két belső gép egymás közötti forgalma nem.
* **Bástya gép**
  + A bejövő forgalom kezelésének helye
  + **A kifelé irányuló szolgáltatások két módon kezelhetők:**
    - Belső és a külső forgalomirányítók csomagszűrő szabályainak beállításaival.
    - Proxy szerverek futtatásával a bástya gépen.
* **Belső router (Choke router)**
  + Szabályozza, hogy a belső hálózatról melyik szolgáltatások érhetőek el közvetlenül.
  + Szabályozza a belső hálózat és a bástya gép közötti forgalmat.
* **Külső router (Access router)**
  + Védi a perimeter és a belső hálózatot az internet felől.
  + Minden forgalmat kienged a perimeter hálózatról.

### Multi-Homed

* Három vagy több interfésszel rendelkezik, amik külön hálózatban csatlakoznak és közöttük szűri a hálózat forgalmát.

# Routereken megvalósítható tűzfalak

### CBAC – Context-based access control

* **Állapottartó szűrés – Stateful Packet Filtering**
  + Nem csak hálózati és szállítási réteg információk alapján vizsgálja a viszonyok állapotát, hanem alkalmazási réteg információkat is.
* **Forgalom figyelés – Traffic Inspection**
  + SYN flood támadások, TCP sorszámozást figyel és gyanúsakat eldobja.
* **Behatolás érzékelés – Intrusion Detection**
  + A syslog üzenetek átvizsgálásával ki lehet szűrni az smtp támadások és SYN flood támadások sajátosságait, 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.
* 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.

### ZPF

* ACL-től független
* Mindent tiltunk, amíg külön nem engedjük
* Könnyen értelmezhető
* Házirend minden forgalom hatással van, így nem kell több ACL/ellenőrzési művelet.

### ZPF funkciói

* **Inspect**
  + Automatikusan beengedi a válasz forgalmat.
  + Támogatja azokat a protokollokat, amik több párhuzamos kapcsolat felépítését igénylik.
* **Pass**
  + Hasonló az ACL permit-hez.
  + Nem követi a kapcsolat állapotát
  + Csak egy irányban engedi át a forgalmat
  + Megfelelő szabványt kell alkalmazni a válaszforgalom beengedésére
* **Drop**
  + Hasonló egy ACL deny-hoz
  + Blokkolt csomagok naplózása

### ZPF, ZBF szabályok

* Egy zónát először konfigurálni kell.
* Egy interfész egy biztonsági zónához rendelhető.
* Egy zónához tartozó interfészek közötti forgalom engedélyezett.
* Különböző zónák közötti forgalom engedélyezéséhez policy-t kell konfigurálni.
* Egy zónabeli és egy nem zónabeli interfész közötti forgalom nem engedélyezett.
* Zónák között: **pass, inspect, drop** események definiálhatóak.
* Nem zónához tartozó interfészen CBAC-ot lehet konfigurálni.

### Zónák

* Self zone
* DMZ
* Privát
* Publikus/Internet