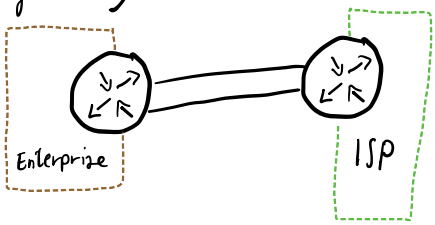
Tűzfalak feladatai

- 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 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.
- Tűzfal generációi
  - Első generáció - Packet Filtering Firewall
    - Döntését ezekre alapozza → • Forrás / cél MAC címe, IP címe, port száma
      → • IP csomagba beágyazott protokoll
    - Működése
      - A csomag fejlécben 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 követi a kapcsolat állapotot
      - Kétirányú forgalmat külön szabályokkal kell megadni.
      - Egész port tartományt engedélyezni kell, mert sok protokoll dinamikusan választ port

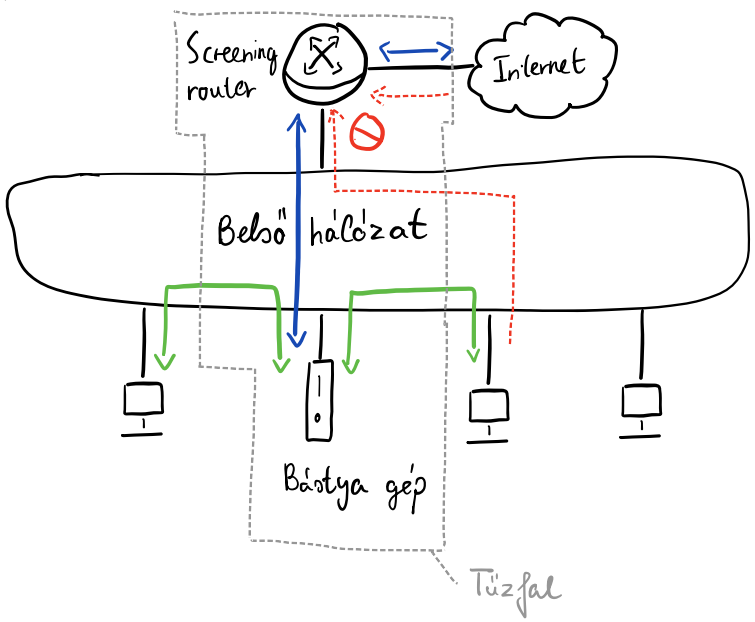
- **Második generáció** - Stateful Firewalls (OSI 5. rétegben dolgozik)
  - Tartalmazat vizsgál és figyelembe veszi a felépített kapcsolatokat.
  - Figyeli az összes áthaladó hálózati csomagot és megállapítja, hogy:
    - melyik már egy meglévő kapcsolat része
    - melyik kezdeményez új kapcsolatot
    - melyik csomag nem része egyik kapcsolatnak sem
  - A felépített kapcsolat információt gyorsítótárban tárolja
  - A kapcsolat csomagjait a gyorsítótárban lévő bejegyzésekkel hasonlítja össze, emiatt hatékony.
  - Előnyei
    - Jobban le lehet írni a szabályokat (állapotokat)
    - Nagyobb biztonságot nyújt, mint a csomagszűrő tűzfalak (sorszámokat folyamatosan figyeli)
  - Hátrányai
    - Állapotok kezelése miatt erőforrás igényes és nem mindig képes megkülönböztetni a biztonságos és a veszélyes adatokat a csomagokban.

- **Harmadik generáció** - Application Level Firewall
  - Két kategóriája van
    1. Proxy Firewalls
    2. Deep Packet Inspection Firewalls
  - Előnye
    - Biztonságos és a puffer túlcsordulásos típusú támadásoknak ellenáll, mert figyeli a protokoll fejléc mezőinek hosszát.
  - Hátrányai
    - Erőforrás igényes, nem megfelelő megvalósításnál gyenge teljesítmény
    - Transzparencia hiánya

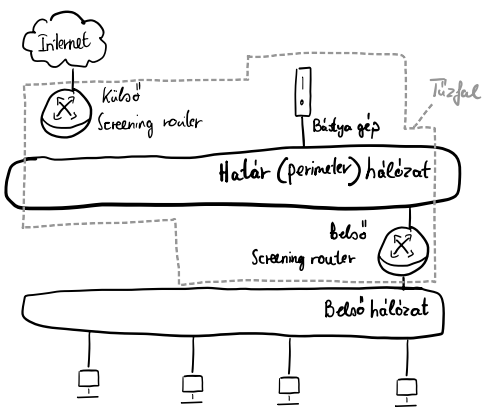
- **Proxy Firewalls**
  - A közvetlen kapcsolat megszakad, a továbbítandó csomagot újraelőállítják, átmásolják az összes protokollréteg szükséges mezőit.
  - Alkalmazás szinten képes a parancsok szűrésére.
- **Deep Packet Inspection Firewalls**
  - Transzparensen működik, nem épít fel külön kapcsolatot a két kommunikáló fél között.
  - Egyszerre szűri az OSI modell mind a 7 rétegét.
  - Figyeli a protokollnak nem megfelelő csomagolást és szűri azokat.
  - Csomagolást 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 szolgáltatót, QoS és sávszélesség menedzsmentet biztosít, hogy a lehető legjobban kielégítse a mai kor igényeit.
- **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)



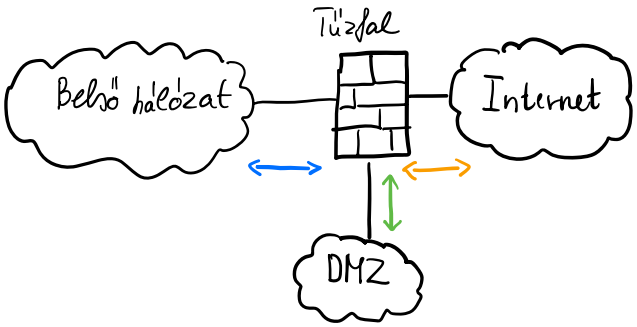
- Single-homed – Screened host
  - A szolgáltatást nyújtó (bástya) gép csak a belső hálózatra csatlakozik.
  - Elsődleges biztonságot a csomagszűrő forgalomirányító adja, ami megakadályozza, hogy a felhasználói gépek közvetlenül hozzáférjenek az internethez.
  - Csomagszűrő routert úgy konfigurálják, hogy az internet gépei csak a bástya géppel léphessenek 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.
  - Hátrányai
    - Screend subnet architektúra biztonságosabb
    - Ha a támadó betört a bástya gépre, onnan már a többi gépet is eléri a LAN hálózaton.



- Single-homed screened subnet
  - 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 router.
  - 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 felé irányuló szolgáltatások két módon kezelhetőek:
      - Belső és a külső routerek 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 szenged a perimeter hálózatról.



- Multi-homed
  - Három vagy több interfésszel rendelkeznek, amik külön hálózatban csatlakoznak és tűzfal szűri a hálózat forgalmát.



- Routeren megvalósítható tűzfalak
  - CBAC – Context-Based access control
    - Stateful Packet Filtering
    - Traffic Inspection
    - IDS
  - 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 nyílászárat hoz létre megadott kapcsolathoz, amik beengedik a blokkolt forgalmat.
    - Az állapottábla automatikusan frissül a forgalom áramlásának megfelelően.
  - ZPF
    - ACL-től független
    - Mindent filtrál, amíg külön nem engedjük
    - Funkciók
      - Inspect, Pass, Drop
    - Zónák
      - Self zone, DMZ, Privát, Publikus / Internet