Kommunikációs rendszerek programozása

Tűzfalak

Tűzfalak

- Internet
  - Hatalmas lehetőségek ↔ hatalmas veszélyek, azaz „se veled, se nélküled”
  - Bárki ill. bármelyik cég célpontja lehet az Internetes támadóknak
- Támadások az Internet felől
  - Web alapú, IP spoofing
  - Denial of Services (DoS), Distributed DoS (DDoS)
  - SYN flood, Sniffer
  - Bővebben: http://www.cert.org/

Tűzfalak

- Védekezés lehetőségei
  - Nem használunk Internetet
  - Elszigeteljük ill. leválasztjuk az Internetet használó gépeket
  - Szabályozzuk a hozzáférést (külső, belső) a védendő gépekhez, információkhoz ⇒ **Tűzfal**
- Tűzfalak működésének alapelvei
  - Hálózatok közötti forgalom szabályozása a biztonsági szintek, előírások figyelembe vételével
  - **Mindenhonnan mindenhova minden szolgáltatás tiltott!**

Tűzfalak

- Alkalmazásának céljai
  - Bizalmas adatok védelme ⇒ **bizalmasság**
  - Kritikus információk sértetlenségének biztosítása ⇒ **sértetlenség (integritás)**
  - Adatok és erőforrások bármikor elérhetők ⇒ **üzemkészség, rendelkezésre állás**
- Alkalmazásának előnyei
  - Intranet védett a támadókkal szemben
  - Szabályozott hozzáférés a kritikus, bizalmas adatokhoz az Intraneten belülről is
  - Hálózati biztonsági rendszer menedzselése központosítható
  - Átmenő hálózati forgalom monitorozható
  - Felhasználói hitelesítés lehetősége
  - Virtuális magánhálózatok (VPN) hozhatók létre

Tűzfalak

Alapvető típusok

- Csomagszűrő tűzfalak
  - Csomagok fejrészét hasonlítják össze az ACL-lel
  - Monitorozható fejrész adatok
    - Forrás ill. cél IP cím és portszám
    - ICMP üzenettípus, protokoll
    - Csomagméret, különböző fejrész flag-ek
  - Általában a hálózati réteg szintjén működnek
  - Hátrányai
    - Nagy terheléseknél jelentősen lecsökken a teljesítménye
    - Felsőbb szintű protokollok adatait tartalmazó csomagokat nem tudja értelmezni
    - Könnyen átverhető: darabolt csomagokkal, hamis vagy érvénytelen IP címmel

Tűzfalak

- Alapvető típusok
  - Alkalmazás szintű proxy tűzfalak
    - Minden egyes új kapcsolatot két kapcsolatra bontanak, ha átengedhető a forgalom
    - Nagyon biztonságosak, de intelligens működésük miatt viszonylag lassúak
    - Cache-léssel gyorsíthatják pld. a weblapok letöltését
    - Nagy forgalmú hálózatokban szűk az áteresztőképessége

Tűzfalak

- Alapvető típusok
  - „Stateful Inspection” tűzfalak
    - Csomagszűrő tűzfalak hátrányait küszöböli ki
    - Dinamikus állapottáblákat használnak a döntésekhez
      - Segítségükkel alsóbb szinteken már eldönthető egy csomag átengedhetősége
      - Azaz, a kapcsolat „ellenkapcsolata” újabb felső szintű vizsgálat nélkül átengedhető (FTP,Telnet)
    - Felsőbb szinteken korlátozott szűrési képességekkel rendelkezik

Tűzfalak

- Egyéb alkalmazási területek, funkciók
  - Network Address Translation ⇒ NAT
  - Port Address Translation ⇒ PAT
  - Authentication (felhasználói hitelesítés)
  - Virtual Private Network ⇒ VPN
  - Content Screening
  - Monitoring, logging (monitorozás, naplózás)
- Tűzfalakkal szembeni követelmények
  - Magas rendelkezésre állás
  - Skálázhatóság
  - Nagy áteresztőképesség
  - Központosított menedzsment