# Tűzfalak
# külső és belső hálózatok

Számítástechnika tanár szak
Rendszertechnika II.
előadás

## Növekvő biztonsági kihívások

- Régebben a fizikai biztonság volt az elsődleges
- Manapság a hálózatok és az Internet jelentik a legnagyobb biztonsági problémát
  - nyílt, szabad közösség, hatalmas populáció
  - szinte mindenki kötődik hozzá
    - potenciális piac
    - a felhasználókkal, vásárlókkal jönnek a támadók is
    - folyamatosan új vírusok, férgek, kémprogramok készülnek
  - Bárki szabadon rákapcsolódhat (vezeték nélküli hálózatok)
  - Letölthető hacker eszközök, útmutatók

## Támadások típusai – külső támadások

- Lopakodók – fizikai biztonság (gépek zárolása)
- DoS – Denial of Service
  - Nehezen kivédhető
  - Nem feltétlenül okoz kárt
- DDoS – DoS sok "zombi gép" felhasználásával
- Támadások az alkalmazási rétegben
  - Ismert és új biztonsági hibák kihasználás
  - A nem frissített operációs rendszerek hibáinak kihasználása
- A hálózat felderítése, figyelése
  - Védtelen vezeték nélküli hálózatok keresése
  - A hálózat, kiszolgálók és kliensek szkennelése
  - Csomagok figyelése, jelszavak, információk keresése

## Támadások típusai – belső támadások

- Fertőzött laptop – egyre gyakoribb probléma
- Nem engedélyezett eszközök
  - Alapértelmezéssel használt hálózati eszközök
    - switch
    - router
    - vezeték nélküli AP
- Nem engedélyezett szolgáltatások
  - Saját fájl és nyomtató megosztások (jelszó nélkül)
- Elbocsátott alkalmazott – Man in the middle
- Vírusok, trójai programok

## A várható támadások típusai

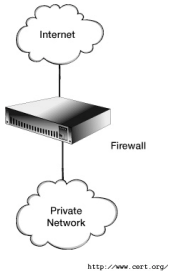
- Web szolgáltatások elleni támadások
- Komplex Web támadás
  - Apache biztonsági rés
  - IE biztonsági rés
- Spyware fenyegetés
- Mobil eszköz elleni támadások
  - Notebook
  - PDA, Telefon
- SPAM
- DoS, DDoS

## Lehetséges védekezési módok

- A megfelelően konfigurált és működő eszközök elégségesek lennének …
- De szükséges a védelem a következők miatt
  - a szoftverek hibái miatt
  - az emberi mulasztás, butaság vagy hozzá nem értés
- Lehetséges megoldások
  - Elosztott, jól koordinálható, több rétegű, független védelem
  - Integrált megoldás (szerverek, routerek, switchek)
  - Önmagát védő hálózatok
  - A hálózat felosztása zónákra
    - a zónák saját szabályrendszer szerint működnek
    - a zónák határán szükséges egy eszköz ami feloldja a konfliktusokat
    - általában tűzfalak látják el ezeket a funkciókat

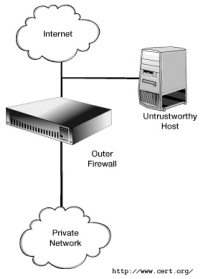
## Egyszerű (határ) tűzfal

- Egyrétegű megoldás
- Egy eszközre van telepítve minden tűzfal funkció
- Elválasztja egymástól a nyilvános és a védett hálózatot
- Egyszerű és olcsó
- A legkevésbé biztonságos



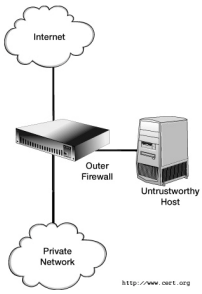

## A megbízhatatlan gép problémája

- A külvilág felé szolgáltatnak
  - WWW, POP3, SMTP, SSH
- A legveszélyeztetettebb elem
- Minimalizálni kell a nyújtott szolgáltatásokat
- A belső hálózat gépei nem tekinthetik megbízhatónak



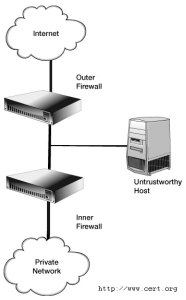

## A DMZ kialakítása

- Feladat a megbízhatatlan kiszolgálók védelme
- Külön hálózatot alakítunk ki ezeknek a gépeknek, szolgáltatásoknak
- Ezáltal növekszik
  - a biztonság
  - a megbízhatóság
  - a rendelkezésre állás



## Kettős tűzfal

- Célja
  - A belső hálózat és a DMZ védelme
  - A belső hálózat elkülönítése a DMZ-től
- Funkciók
  - Külső tűzfal
  - Belső tűzfal
- Védett hálózatok:
  - DMZ
  - Belső hálózat
- Lehetőség szerint eltérő architektúrájú tűzfalak használata javasolt




## Tűzfalak különböző gépeken

- Egygépes rendszer
  - védi a kiszolgálót a a külvilággal szemben
- Többkapcsolatos kiszolgáló
  - több hálózati interfész
  - több egymástól független hálózat
- Útválasztó (router)
  - több hálózati interfész
  - IP továbbítás
  - keresztülhaladó forgalom az egyes hálózatok felé

## Tűzfalak csoportosítása

- Tűzfalak osztályai:
  - Személyes tűzfalak (első osztály)
  - Forgalomirányítók tűzfalai (második osztály)
  - Alsó kategóriás hardver tűzfalak (harmadik osztály)
  - Felső kategóriás hardver tűzfalak (negyedik osztály)
  - Felső kategóriás szerver tűzfalak (ötödik osztály)
- Tűzfalak típusai
  - Csomagszűrő
  - Cím transzformáló
  - Állapottartó
  - Kapcsolat szintű átjáró
  - Proxy
  - Alkalmazásszűrés

## Első osztály - Személyes tűzfalak

- Egyre több otthoni kapcsolat
- Egyre több mobil számítógép, idegen környezet
- Általában PC-n futó szoftveres szolgáltatás
- Kis hálózat védelmére is alkalmas (otthoni hálózat)
- Manapság minden gépen erősen ajánlott a használata
- Minimális tudású megoldások, általában csak csomagszűrést végeznek

## Első osztály - Személyes tűzfalak

| | |
|---|---|
| Alapszolgáltatások | statikus csomagszűrés, NAT |
| Konfigurálás | Automatikus (manuális lehetséges) |
| IP címek engedélyezése vagy blokkolása | Igen |
| Portok vagy protokollok engedélyezése vagy blokkolása | Igen |
| ICMP üzenetek engedélyezése vagy blokkolása | Igen |
| Kimenő folyamatok szabályozása | Igen |
| Alkalmazások védelme | Esetleg |
| Látható vagy hallható riasztások | Esetleg |
| Napló állományok | Esetleg |
| Riasztások valós időben | Esetleg |
| VPN támogatás | Általában nem |
| Távoli felügyelet | Általában nem |
| Gyártói támogatás | Változó |
| Konkurens folyamatok száma | 1-10 |
| Moduláris bővíthetőség (hardver vagy szoftver) | Változó |
| Ár | Alacsony |

## Első osztály - Személyes tűzfalak

- Előnyök
  - Alacsony költség
  - Egyszerű konfigurálás
- Hátrányok
  - Központilag nehezen menedzselhető
    - Minden kliens külön konfigurálást igényel
  - Csak alapvető tűzfal funkciókat lát el
  - Korlátozott teljesítmény
    - Egy gép védelmére vannak tervezve

## Második osztály - Forgalomirányítók tűzfalai

- A routerekbe gyakran integrálnak tűzfal funkciókat is
- Az alsó kategóriás (low-end) routerek
  - forgalomszűrés IP cím alapján
  - forgalomszűrés port alapján
  - NAT szolgáltatás a címek elrejtésére
- A felső kategóriás (high-end) eszközök
  - programozhatóak
  - állapotkövetők
  - támogatják a magas rendelkezésre állást

## Második osztály - Forgalomirányítók tűzfalai

| | |
|---|---|
| Alapszolgáltatások | statikus csomagszűrés, NAT, (alkalmazás szűrés) |
| Konfigurálás | Automatikus (alsó kat.), manuális (felső kat.) |
| IP címek engedélyezése vagy blokkolása | Igen |
| Portok vagy protokollok engedélyezése vagy blokkolása | Igen |
| ICMP üzenetek engedélyezése vagy blokkolása | Igen |
| Kimenő folyamatok szabályozása | Igen |
| Alkalmazások védelme | Esetleg |
| Látható vagy hallható riasztások | Általában igen |
| Napló állományok | Legtöbbször igen |
| Riasztások valós időben | Legtöbbször igen |
| VPN támogatás | Közös (alsó kategória), különálló (felső kategória) |
| Távoli felügyelet | Igen |
| Gyártói támogatás | Korlátozott (alsó kategória), jó (felső kategória) |
| Konkurens folyamatok száma | 10-1000 |
| Moduláris bővíthetőség (hardver vagy szoftver) | Nincs (alsó kategória), korlátozott (felső kategória) |
| Ár | Változó |

## Második osztály - Forgalomirányítók tűzfalai

- Előnyök
  - Alacsony költség (minimális többletköltség)
  - Összevont konfiguráció, kevesebb hibalehetőség
  - Befektetések védelme (nem szükséges újrakábelezni, újabb képzéseket tartani)
- Hátrányok
  - Korlátozott funkciók
  - Csak alapvető tűzfal funkciókat lát el
  - Csökkenő forgalomirányítási teljesítmény
  - Csökkenő teljesítmény naplózáskor (támadás alatt)

## Harmadik és negyedik osztály - hardver tűzfalak

- Low-end hardver tűzfalak
  - Általában plug & play eszközök
  - Minimális konfigurálási igény
  - Integrálhat switch vagy VPN funkciókat is
  - Kis és középvállalatok számára lehet megoldás
- High-end hardver tűzfalak
  - Talán a lehető legjobb megoldás a hálózati teljesítmény csökkenése nélkül
  - Nagyvállalatok, központok védelmére

## Harmadik osztály - Alsó kategóriás hardver tűzfalak

| | |
|---|---|
| Alapszolgáltatások | statikus csomagszűrés, NAT, (alkalmazás szűrés) |
| Konfigurálás | Automatikus (manuális lehetséges) |
| IP címek engedélyezése vagy blokkolása | Igen |
| Portok vagy protokollok engedélyezése vagy blokkolása | Igen |
| ICMP üzenetek engedélyezése vagy blokkolása | Igen |
| Kimenő folyamatok szabályozása | Igen |
| Alkalmazások védelme | Általában nem |
| Látható vagy hallható riasztások | Általában igen |
| Napló állományok | Általában nem |
| Riasztások valós időben | Általában nem |
| VPN támogatás | Néha |
| Távoli felügyelet | Igen |
| Gyártói támogatás | Korlátozott |
| Konkurens folyamatok száma | 10-7.500 |
| Moduláris bővíthetőség (hardver vagy szoftver) | Korlátozott |
| Ár | Alacsony |

## Harmadik osztály - Alsó kategóriás hardver tűzfalak

- Előnyök
  - Alacsony költség (minimális többletköltség)
  - Egyszerű konfigurálás
- Hátrányok
  - Korlátozott funkciók
  - Csak alapvető tűzfal funkciókat lát el
  - Alacsony teljesítmény
  - Korlátozott gyártói támogatás (WEB, e-mail)
  - Korlátozott bővíthetőség (firmware upgrade)

## Negyedik osztály - Felső kategóriás hardver tűzfalak

| | |
|---|---|
| Alapszolgáltatások | statikus csomagszűrés, NAT, alkalmazásszűrés |
| Konfigurálás | Általában manuális |
| IP címek engedélyezése vagy blokkolása | Igen |
| Portok vagy protokollok engedélyezése vagy blokkolása | Igen |
| ICMP üzenetek engedélyezése vagy blokkolása | Igen |
| Kimenő folyamatok szabályozása | Igen |
| Alkalmazások védelme | Lehetőség szerint |
| Látható vagy hallható riasztások | Igen |
| Napló állományok | Igen |
| Riasztások valós időben | Igen |
| VPN támogatás | Lehetőség szerint |
| Távoli felügyelet | Igen |
| Gyártói támogatás | Jó |
| Konkurens folyamatok száma | 7.500-500.000 |
| Moduláris bővíthetőség (hardver vagy szoftver) | Igen |
| Ár | Magas |

## Negyedik osztály - Felső kategóriás hardver tűzfalak

- Előnyök
  - Magas teljesítmény
  - Jó használhatóság
    - összekapcsolható eszközök, terhelés elosztás
  - Moduláris felépítés (HW és SW bővítési lehetőségek)
  - Kifinomult távoli menedzsment
  - Rugalmasság, skálázhatóság
  - Alkalmazásszűrés (L4, L5, L6, L7)
- Hátrányok
  - Magas ár
  - Bonyolult konfiguráció, menedzsment

## Ötödik osztály - Felső kategóriás szerver tűzfalak

| | |
|---|---|
| Alapszolgáltatások | statikus csomagszűrés, NAT, alkalmazásszűrés |
| Konfigurálás | Általában manuális |
| IP címek engedélyezése vagy blokkolása | Igen |
| Portok vagy protokollok engedélyezése vagy blokkolása | Igen |
| ICMP üzenetek engedélyezése vagy blokkolása | Igen |
| Kimenő folyamatok szabályozása | Igen |
| Alkalmazások védelme | Lehetőség szerint |
| Látható vagy hallható riasztások | Igen |
| Napló állományok | Igen |
| Riasztások valós időben | Igen |
| VPN támogatás | Lehetőség szerint |
| Távoli felügyelet | Igen |
| Gyártói támogatás | Jó |
| Konkurens folyamatok száma | >50.000 |
| Moduláris bővíthetőség (hardver vagy szoftver) | Igen |
| Ár | Magas |

## Ötödik osztály - Felső kategóriás szerver tűzfalak

- Előnyök
  - Jól ismert környezet (Linux, FreeBSD, Windows)
  - Magas teljesítmény (megfelelően méretezett szerveren)
  - Nagyfokú integráltság az operációs rendszer szolgáltatásaival
  - Használhatóság, rugalmasság, skálázhatóság
- Hátrányok
  - Felső kategóriás hardver szükséges – magas ár
  - Sebezhető (egy ismert operációs rendszeren fut)

## Csomagszűrők

- Az egyes csomagok eldobása vagy továbbítása
- Szűrési feltételek:
  - Forrás / cél cím
  - Forrás / cél port
- Nem értik és nem vizsgálják az alkalmazásokról szóló információt (csak az IP fejlécet)
- Mivel a különböző hálózatokat leggyakrabban forgalomirányítók kötik össze ezért ezen funkció is leggyakrabban itt található
- Gyors és kis erőforrás igényű megoldás
- Önmagában általában nem elégséges megoldás

## Állapotkövető csomagszűrés

- TCP kapcsolatok nyomon követése
- A kimenő csomagok naplózása az állapot táblában
  - Forrás / cél cím
  - Forrás / cél port
- Bejövő (és kimenő) forgalomnál ellenőrizhető, hogy ki kezdeményezte
- Eldönthető, hogy a csomag része-e egy már létező kapcsolatnak
- Véd a portletapogatással szemben

## Socks Proxyk

- Kommunikáció három vagy több fél között
  - Kliens -> Proxy -> Szerver
- Titkosítatlan esetben a kliens nem látja közvetlenül azokat a csomagokat amelyeket a szerver küldött és fordítva
- Titkosított esetben a proxy ellenőrzi a fejléceket és ha mindent rendben talál akkor továbbítja a csomagot
- Gyorstár funkció
- Köztes megoldás, nem is csomagszűrés de még nem is alkalmazás szűrés
- Nem minden esetben biztosít transzparens átvitelt

## Alkalmazásrétegbeli proxyk

- Alkalmazásszintű intelligencia a közvetített szolgáltatásoknál
- Minden kapcsolatkérést megvizsgálnak
- Értelmezni tudják az adott alkalmazás adatait és ez alapján döntéseket hoznak
- HTTP, FTP, SMTP, DNS kérések, SPAM szűrés
- Pl.: FTP esetén kívülről lehetséges a USER, PASS, DIR, PORT és GET parancsok használat, de tiltott a PUT
- Protokoll validáció
- Bonyolult megoldás, minden protokollt ismernie kell
- Az alkalmazásokra nézve teljesen transzparensek