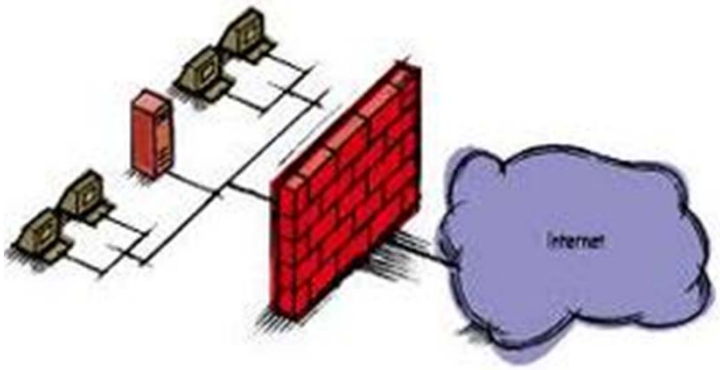
Fábián Zoltán – Hálózatok elmélet

Firewalls - Tűzfalak

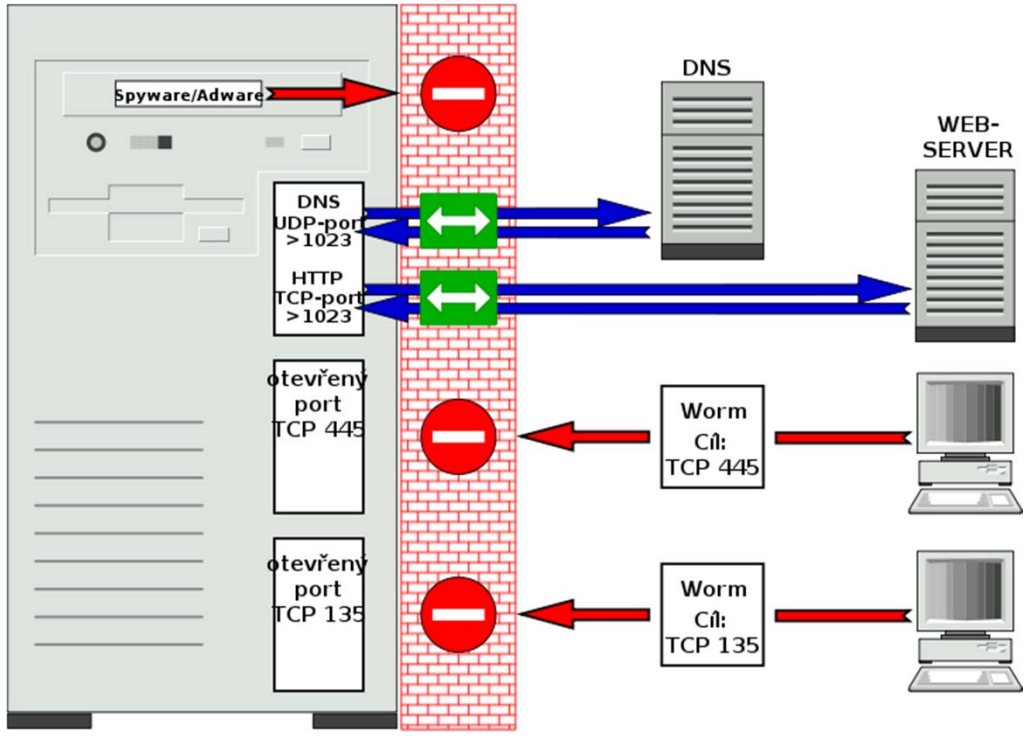
Tűzfal fogalma

- Tűzfal fogalma
  - Olyan alkalmazás, amellyel egy belső hálózat megvédhető a külső hálózatról (pl. Internet) érkező támadásokkal szemben
- Vállalati tűzfal
  - Olyan tűzfal, amely teljes hálózati struktúrát véd



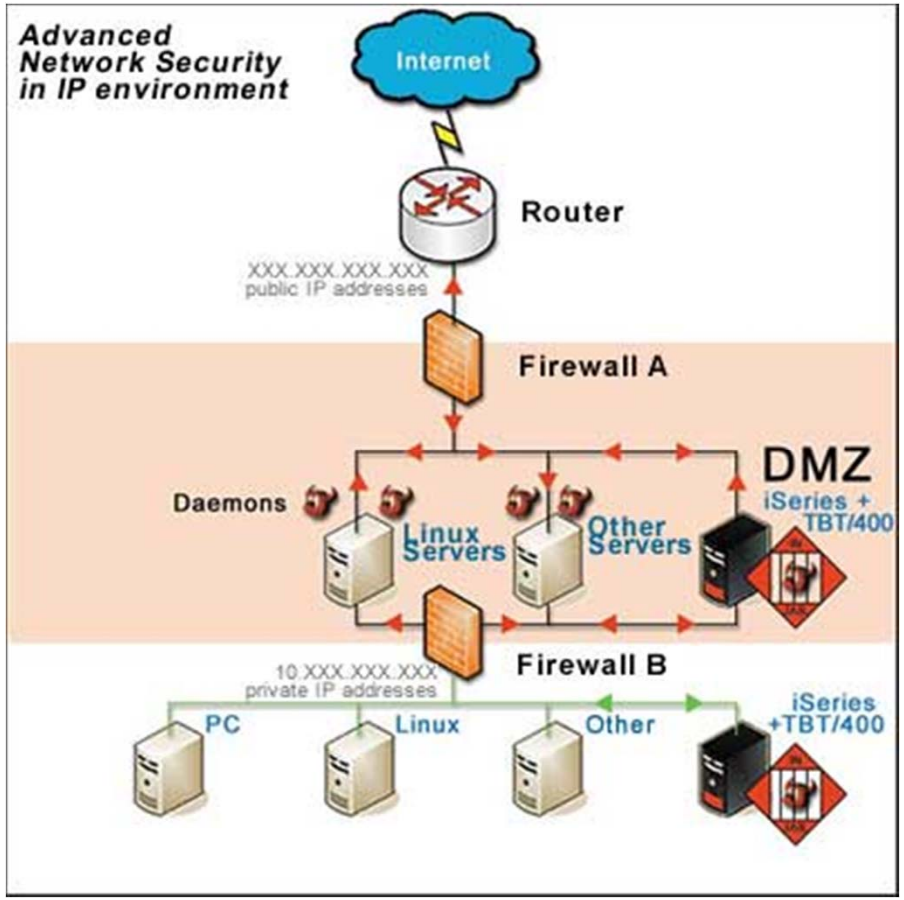
Személyes (Personal) tűzfal

- Olyan tűzfal, amely egy számítógépet véd



Demilitarizált Zóna – Demilitarized Zone - DMZ

- A vállalati hálózat része – általában szervereket helyeznek el benne
  - Kívülről a tűzfalon keresztül el lehet érni
  - Belülről is csak tűzfalon keresztül lehet elérni
  - Célja:
    - Biztonságos publikus szolgáltatások biztosítása
    - A hálózatba való behatolás megnehezítése



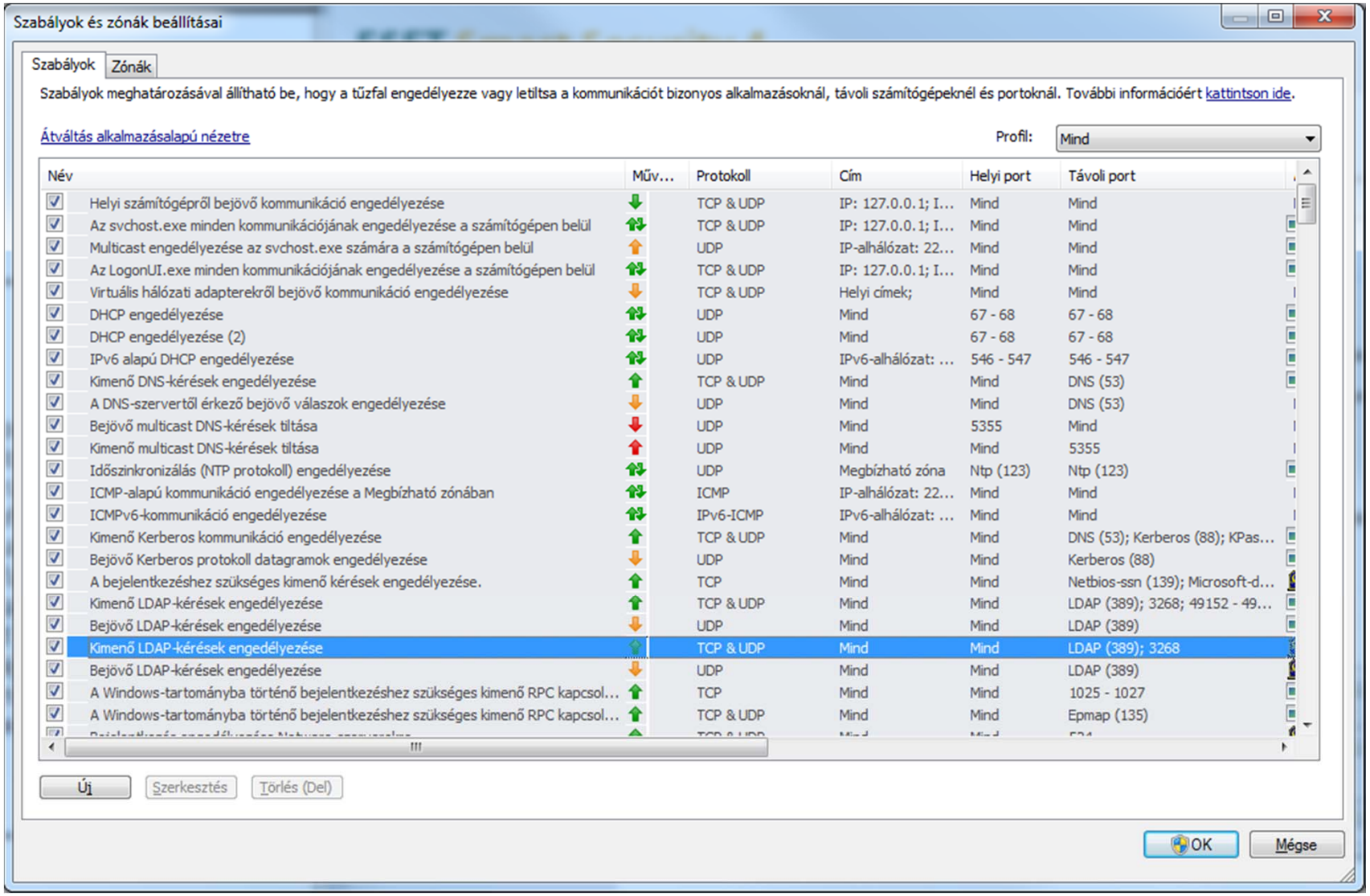
Tűzfalak működési módjai

- Csomagszűrés
- Állapot szerinti szűrés (Personal tűzfal esetén)
- Alkalmazás szintű tűzfal
- Tartalomszűrés
- Behatolás felismerő és megelőző rendszer
- NAT
- Portszűrés, port kezelés

Csomagszűrés

- Az adatcsomagokra szabályokat állítunk be
  - Forráscím:port
  - Cél cím:port
  - A csomagforgalom iránya (Ki, Be, mindkét irány)
  - Az csomag fajtája: TCP, UDP, ICMP
- A szabályokat fentről lefelé hajtja végre a tűzfal
- Ha egy szabályra illik a csomag tulajdonsága, akkor nem vizsgálja tovább
- Alapvető működési mód
- A szabályok beállításához ismerni kell a hálózaton használt protokollokat
- Az ún. bújtatott protokollokkal nem tud mit kezdeni

ESET Smart Security 4.x beépített personal tűzfal szabályai



Portszűrés beállítása példa

- Vállalati hálózati tűzfal beállítása
  - Ki, forrás IP: *,Forrásport port: *, Cél IP:*, cél port:80, csomag: TCP/UDP, enged
  - Ki, forrás IP: *,Forrásport port: *, Cél IP:*, cél port:443, csomag: TCP/UDP, enged
  - Ki, forrás IP: *,Forrásport port: *, Cél IP:*, cél port:21, csomag: TCP/UDP, enged, protokol:FTP
  - Be, forrás IP:*, Forrás port:*, Cél IP:*, Cél Port: 80, csomag: TCP
  - .....
  - **Ki, forrás IP: *,Forrásport port: *, Cél IP:*, cél port:*, csomag: *, tilt, default szabály**

A szabályok beállításának elve

- Vannak baráti vagy (trusted) IP tartományok – ott minden forgalom szabad
- Windows portokat nem engedünk ki, csak ha kell
- Szabályok sorrendje
  - Az engedélyek kifelé
  - Engedélyek befelé a DMZ felé (NAT-olással irányítjuk a forgalmat a DMZ felé)
  - A végén a minden tilt szabály (default)
- A szabályokat lehetőleg általánosan fogalmazzuk meg

Állapot szerinti szűrés

- A csomagszűrés kibővített formája
- A 7. OSI-rétegen vizsgálja a csomagokat és minden hálózati-csomagról állapottáblát hoz létre, így felismeri a csomagok közti összefüggéseket és az aktív kapcsolathoz tartozó munkafolyamatokat leállíthatja. Így szűri ki mikor kommunikál a gép külső hálózattal és ha olyan adatot talál akkor a tűzfal blokkolja az átvitelt.

Alkalmazás szintű tűzfal

- Az adatok tartalmát is figyeli
- Malware, Trójai tartalomelemzéssel összeköthető
- Víruskeresővel összeköthető

Alkalmazás proxy

- A forgalmat tárolja, és továbbítja
- Elemzi a tartalmat
- Alkalmazás specifikus
- Hátrány
  - Csak a megadott protokollokra működik
  - A tartalom átvizsgálása sokáig tarthat
- Célszerű használat
  - Vállalati tűzfal esetén a http és https forgalom szabályozására és ellenőrzésére alkalmas

Tartalomszűrés problémái

- Nem elegendő csak csomagokat figyelni, hanem csomagok sorozatát is figyelni kell
  - Összerakja az adatfolyamot => megvizsgálja => szétszedi csomagokra
- Lassú, memóriaigényes, processzorigényes

Behatolás felismerő és megelőző rendszerek

- Intrusion Detection System – IDS
- Intrusion Prevention System - IPS
- A kommunikáció mintái alapján felismeri a behatolási kísérletet
  - Portscan tipikus mintái
    - Ugyanarról az IP egyesével címről pásztázzuk végig a portokat
    - Ugyanarról az IP címről véletlenszerűen több portra érkezik a kérés
      - El kell dönteni, hogy több kliens alkalmazás akar elérni bizonyos erőforrásokat, vagy portscan
    - TCP, vagy UDP connect – Kapcsolódási kisérlet
    - Syn Scan – Nem befejezett kapcsolódási kisérlet
- A hamis forrás IP címeket felismeri és letiltja

Riasztások

- Naplózás – alapfeltétel
  - A naplókat a rendszergazdának rendszeresen kell ellenőriznie
- A behatolási kísérlet észlelése
  - Manuálisan észleli a rendszergazda
  - A tűzfal automatikusan észleli a beállított minták alapján
- Behatolás kísérlet észlelése utáni tevékenység
  - Automatikus észlelés esetén
    - A megadott forgalom ideiglenes tiltása
    - Email küldése az adminisztrátornak
    - A rendszergazda módosít a szabályokon
  - Manuális észlelés esetén
    - A rendszergazda módosít a szabályokon
  - Dokumentálja a behatolási kísérletet
    - Mikor, honnan, milyen módon, Sikeres vagy sikertelen
    - Ha sikeres, akkor milyen anyagi, vagy egyéb károk érték a rendszert, üzemeltetőt
    - Milyen tevékenységet végzett utána a rendszergazda

Biztonsági kérdések

- Kell-e DMZ?
  - A törési kísérletek 70-80% a vállalaton belülről érkezik
- A tűzfal a bizalmatlanságra épül
- Ha magát a tűzfalat feltörik, akkor is legyen védve a belső hálózat
  - Vállalati tűzfal különálló gép
  - Más biztonsági beállításokkal, jelszavakkal, platformmal, mint a többi gép
- A bújtatott és/vagy titkosított protokollokat is szűrni kell
  - VPN, HTTPS
- Távoli elérés kérdése HTTP protokollon keresztül
  - A HTTP-t mindenhol engedik – azon át lehet-e vinni törést?

Elterjedt tűzfalak

- Microsoft megoldása
  - Vállalati tűzfal: Forefront család
  - Personal tűzfal: Windows XP, 2003, Vista, Win7, Server 2008 (komolyabb)
- Más cégek
  - Víruskereső cégek: ESET Smart Security, ZoneAlarm
  - KERIO WinRoute Firewall, Personal Firewall
  - GFI Sunbelt Personal Firewall
- Linux
  - pfSense – FreeeBSD

Fontosabb personal tűzfal tulajdonságok

- Csomagszűrés
- Fájl integritás ellenőrzés
- Alkalmazások kommunikációjának ellenőrzése
- Hálózati behatolás érzékelés
- IP alapú behatolás érzékelés
- Azonosítási kísérletek érzékelése
- Tartalomszűrés
  - Cookie érzékelés
  - Reklám blokkolás
  - POP-Up Windows blokkolás
  - Víruskereső integráció (Antivirus, antispyware)
- Statisztikák készítése
- Adminisztrálás
  - Távoli elérés lehetősége
  - Jelszóvédett adminisztráció