

Távközlési informatika

Firewall, NAT

Dr. Beinschróth József

Firewall

- Történelem

- Az Internet előtti időszakban az egyes vállalatok hálózatai nem kapcsolódtak össze (kapcsolatok kivételesen léteztek pl. bérelt voltak)
- Az Internet kialakulásakor az egyes vállalatok is rákapcsolódtak: a fenyegetettség megnőtt, a vállalati hálózatokhoz kívülről bárki hozzáférhetett
- Megoldás
 - (Nem veszünk tudomást az Internetről, nem kapcsolódunk hozzá)
 - A vállalat két egymástól teljesen független hálózattal rendelkezik és az egyik nem kapcsolódik az Internethez. A két hálózat közötti adatcsere (pl. floppy-n) szabályzatokkal tiltott.
 - A vállalati hálózat és az Internet között jól definiált felületet határozunk meg és az ezen áthaladó forgalmat szigorúan kontrolláljuk (firewall). A felületen kívüli adatforgalmat tiltjuk ill. megakadályozzuk.

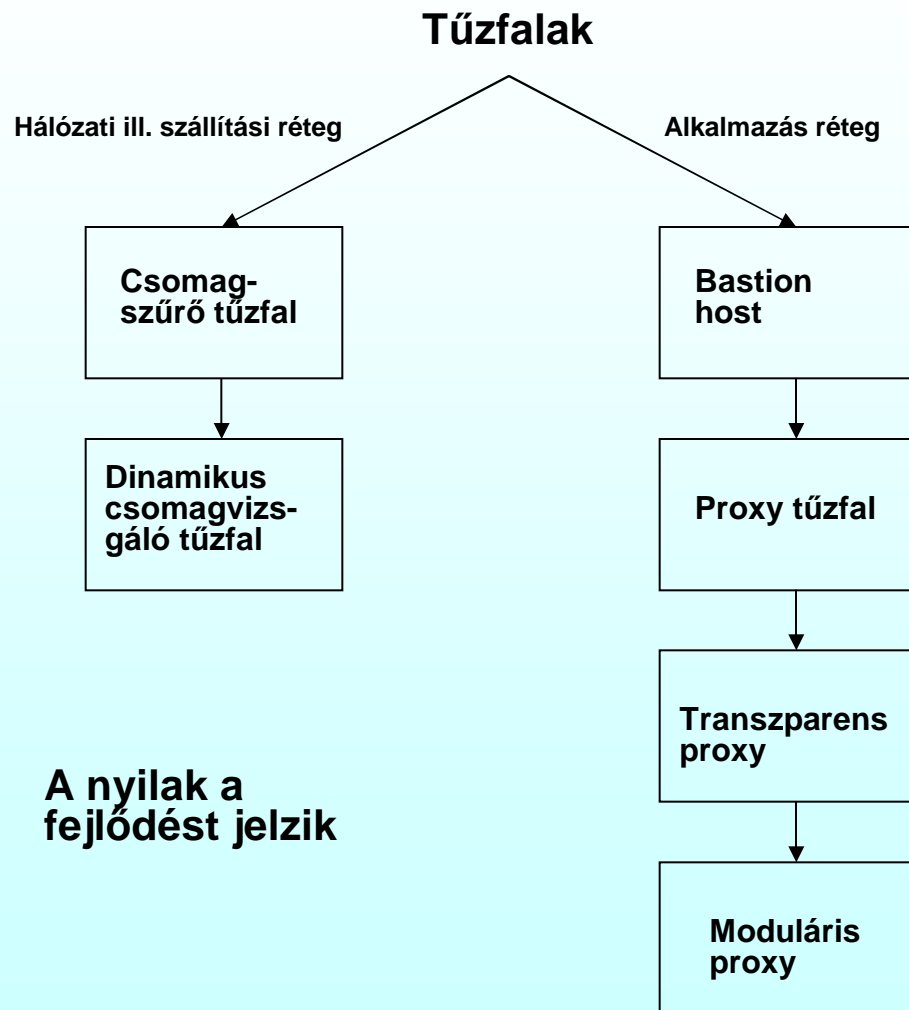
Firewall

- Firewall - tűzfal
 - Gyűjtőnév: Azon módszerek összessége, amelyeket biztonsági megfontolásból alkalmaznak úgy, hogy a hálózatba belépő és onnan kilépő forgalmat naplózzák és korlátozzák – hálózat határvédelmi eszköz
 - A forgalom korlátozás bizonyos, a tűzfalon beállított szabályrendszer alapján történik
 - Forgalomkorlátozás (szűrés): a szabályrendszer alapján dől el, hogy lehetséges a továbbítás ill., hogy milyen intézkedésre van szükség (pl. csomag eldobás)
 - A hálózat minden külső kapcsolódási pontján kell tűzfal, a külvilágból jövő és oda tartó minden forgalomnak át kell haladnia a tűzfalon. (Megkerülési lehetőség pl. telefonos kapcsolat, hordozható gépek...)
 - A routerek a hálózat topológiájában éppen alkalmas helyen szerepelnek, tipikusan rendelkeznek tűzfal funkcióval
 - Alapelv
 - Mindent megtiltunk, azután engedélyezzük, hogy mit engedjen át a tűzfal (és nem fordítva)

Firewall

- Lehetőségek a csomagok vizsgálata után
 - Továbbítás (accept, forward)
 - Eldobás (drop, deny)
 - Eldobás a feladó értesítésével (ICMP reject csomag)
 - Helyi portra történő átirányítás (proxy-hoz)
 - Egyéb, pl. naplózás, riasztás, programindítás stb.)
- Beállítások a tűzfalon
 - Az IBSZ határozza meg!
- Típusok – nem kizárólagosak, együtt is üzemelhetnek
 - Csomagszűrő tűzfal
 - Dinamikus csomagvizsgáló tűzfal
 - Bástya gép (Bastion host)
 - Proxy tűzfal
 - Transzparens
 - Moduláris

Firewall



Optimális megoldás:
többféle tűzfalat alkalmaznak egyszerre – csomagszűrőt is, proxy-t is, sőt különböző gyártmányokat, így a security réseket kihasználó támadások esélye csökken. Továbbá integráljuk a tűzfalat az IDS, antivírus, spamszűrő megoldásokkal

Tűzfal lehet szoftver megoldás: egy op. rendszerrel ellátott gépen egy spec. szoftver valósítja meg, ill. lehet hardver (appliance) megoldás. Persze ebben is van szoftver, sőt op. rendszer is.

Firewall – Packet Filter (Csomagszűrő tűzfal)

- Régi probléma: az Internetre kapcsolódó gépek védtelenek a nekik címzett csomagok ellen
- A Packet Filter IP csomagokat vizsgál és a szabályoknak megfelelően átengedi vagy eldobja azokat (Nem a legerősebb megoldás.)
- Minden kimenő és bejövő csomag külön ellenőrzésre kerül
- Az IP header minden mezője külön ellenőrzésre kerül
- Hamisított címek kiszűrésre kerülnek
- A funkció a router funkcióval könnyen integrálható (gyakran nevezik csomagszűrő routernek is)
- Jellemzően a hálózati rétegben működik (de pl. a port számokat is figyelembe veszi)
- A rendelkezésre álló információ
 - Forrás és cél IP cím
 - Forrás és cél port szám (TCP ill. UDP esetén)
 - Forrás és cél típus (ICMP esetén)
 - A csomagot érkeztető hálózati interface
 - Egyéb protokollspecifikus információk
- Megbízható címtartományok gépeivel engedélyezi a kommunikációt

Csomagszűrő tűzfal

- Tipikus szabályok:
 - A kifelé tartó csomagok közül csak azokat engedjük át, amelyek belső IP címről érkeznek. (Az ettől eltérőek nyilvánvalóan hamisak: pl. valaki belülről magát álcázva küld valamit.)
 - A befelé tartó csomagok közül csak azokat engedjük át, amelyek pl. a 80-as port felé tartanak. (Igy csak a web forgalom engedélyezett.)
 - Nem engedjük át azokat a csomagokat, amelyek kívülről érkeznek, de forrás IP címként valamelyik belső gép IP címét tartalmazzák (IP cím hamisítás.)
- Problémák
 - Viszonylag bonyolult konfiguráció, szabályok kimaradhatnak
 - Bizonyos szolgáltatások számára fenntartott portokat más szolgáltatások is használhatnak
 - Léteznek nyitott portokat kereső alkalmazások (port scan)
 - A csomag eldobásáról vagy megtartásáról szóló döntést kizárólag az adott csomagban szereplő információ alapján hozza meg, nem vizsgálja pl., hogy hol helyezkedik el a csomag az adatfolyamban
 - Csak a csomag fejléce kerül vizsgálatra, a tartalma nem
 - Bonyolult igények kielégítésére nem alkalmasak

Firewall – Stateful Packet Filter

(Dinamikus csomagvizsgáló tűzfal)

- A csomagszűrő tűzfal kizárólag megbízható címtartományok hostjaival engedélyezi a kommunikációt – e-kereskedelem esetén pl. ez nem elégséges megoldás: szükséges ismeretlen hostokkal történő kapcsolat felépítés is
- Nemcsak egy meghatározott csomagot vizsgál, hanem a csomag állapotát is: a tűzfal azonosítja a kapcsolatok kezdetét és befejeződését, számon tartja a létező hálózati kapcsolatokat, a kimenő adatkérelmeket, hogy hol helyezkedik el a csomag az adatfolyamban stb.
- Ezek alapján ki tudja szűrni a kapcsolatokba nem illő csomagokat
- A csomagokat átmenetileg tárolja: addig, amíg a döntést képes meghozni

Firewall – Stateful Packet Filter

(Dinamikus csomagvizsgáló tűzfal)

- Kapcsolatorientált protokollok esetén (TCP) képes a csomagszűrő tűzfalnál többet nyújtani – pl. az adatokat tartalmazó csomag előtt kellett érkeznie olyan csomagnak, amely a kapcsolat kiépülésében játszik szerepet pl. egy ftp csomag akkor továbbítódik, ha korábban már felépült egy ftp kapcsolat
- Bizonyos kapcsolattípusokat képesek hitelesítő szolgáltatásokhoz átirányítani
- Meghatározott típusú csomagokat képesek kiszűrni (pl. futtatható attachementet tartalmazó levelek)
- Problémák
 - A naplózás, az ellenőrzés és elemzés nagyon lelassíthatja a hálózati kapcsolatot (különösen, ha egyidőben sok kapcsolat van és sok, bonyolult szabály él)
 - Csak a csomagok fejléce kerül vizsgálatra, a tartalma nem, a döntés a fejlécek alapján történik meg

Firewall – Bastion Host

- Történelmi kategória: nem igazi tűzfal, a csomagszűrő tűzfalaktól elérő filozófiát követ, nem végez szűrést, de hálózati határvédelmi eszköz – a külső és a belső hálózat határfelületén helyezkedik el
- A bastion host olyan szerver gép, amely több felhasználó párhuzamos távoli hozzáférését támogatja – mind a belső, mind a külső hálózat felé direkt kapcsolattal rendelkezik
- A bastion host másik oldalán elérhető szolgáltatás igénybe vételéhez a felhasználónak először be kell jelentkeznie a bastion hostra és itt el kell indítania egy az illető szolgáltatás igénybe vételéhez szükséges programot
- Megszűnik a kommunikáló felek közötti közvetlen csomagkapcsolat, a a kapcsolatnak két fázisa van (host1-bastion host, bastion host-host2), a bastion host közvetít
- Fő funkciója emiatt nem a szűrés, hanem a hitelesítés
- Probléma: egyidőben sok felhasználó használja ugyanazt az erőforrást (a bastion hostot)

Firewall – Socks tűzfal

- A csomagszűrő és a proxy tűzfalak között helyezkedik el (evolúciós szempontból) – nem elterjedt megoldás
- A kliens gépre telepítésre kerül egy program modul, ami minden hálózati kapcsolat kezelését átveszi az eredeti operációs rendszertől
- Amikor egy program kapcsolódni akar egy szerverhez, akkor a kapcsolódási kérését a modul kezeli, és a program helyett kapcsolódik az előre beállított SOCKS proxyhoz, majd megadja a proxynak, hogy milyen címre szeretne kapcsolódni
- Ezek után a proxy kapcsolódik a kliens program által kijelölt szerverhez
- A kapcsolat kiépülése után az adatforgalmat a kliens program a modul segítségével a SOCKS proxyn keresztül a végzi
- Nem nevezhető csomagszűrőnek, mivel csomagok nem közvetlenül a kliens és a szerver között közlekednek
- Nem tekinthetőek alkalmazásszintű tűzfalnak sem mivel a forgalom nem alkalmazási szinten kerül szűrésre, hanem csak hálózati szinten

Firewall - Proxy tűzfal (proxy szerver)

- Alkalmazás szinten megvalósított szűrés (application gateway)
- Proxy: megbízott – az összes gép nevében a proxy jár el
 - Pl. a routerrel integrált csomagszűrő tűzfal csak a proxy-tól fogad el csomagokat, a proxy viszont alkalmazás szinten elvégzi a szűrést
- Nem engedélyez közvetlen párbeszédet az általa összekapcsolt hálózatok között: minden forgalom rajta halad keresztül, a kliens és a szerver között nem épül ki közvetlen kapcsolat, hanem mindketten a tűzfalon futó proxy alkalmazással kommunikálnak
- A proxy egyik hálózati csatolójával az ismeretlen hálózathoz kapcsolódik, a másikkal pedig a belső hálózatban található kliensekhez
- A kapcsolat kettősségéből kifolyólag a proxy tűzfalak minden különösebb beállítás nélkül képesek kivédeni a csomagszintű támadásokat
- Ez az architektúra képessé tette a tűzfalakat arra is, hogy alkalmazásszinten ellenőrizzék a rajtuk áthaladó információáramot

Firewall - Proxy tűzfal (proxy szerver)

- A proxy alkalmazások már nem csupán a csomagok fejlécét vizsgálták, hanem azok adatairészebe is belenéznek
- Csak meghatározott alkalmazásokhoz tartozó forgalmat enged át
- A belső hálózatban levő kliens nem érheti el közvetlenül a külső hálózaton levő szervert, csak a proxy-n keresztül
- A külső hálózaton levő szerver sem éri el közvetlenül a belső hálózatot
- Bevárják az összes olyan IP csomagot, amelyek alkalmazói szinten összetartozó protokollelemet hordoznak, ezután valósul meg a szűrés funkció
- Általában cache-elnek is (cache proxy – proxy cache)
 - Az áthaladó információ egy ideig tárolódik, újra letöltés esetén a kliens az eltárolt változatot kapja
 - Jelentős sávszélesség megtakarítást eredményez
- Ha nincs telepítve egy meghatározott alkalmazáshoz tartozó alkalmazásproxy, akkor az adott alkalmazást a rendszer egésze nem fogja támogatni
- Probléma: Jelentős erőforrás igény (a finomabb vizsgálatok és a store and forward működés miatt)

Transzparens Proxy Tűzfal

- A tűzfalon - elhelyezkedéséből adódóan - minden forgalom áthalad (a tűzfal, mint a szervezet hálózatának internetes, alapértelmezett átjárója)
- Így lehetőség van a tűzfalon a csomagszűrőkhöz hasonló funkciókat ellátni
- A klienseken semmilyen proxy beállítást nem kell megtenni, azaz a kliensek közvetlenül próbálnak kapcsolódni a szerverhez
- A csomagok nem jutnak át a tűzfalon, hanem a tűzfal a csomagokat, kapcsolatokat - beépített csomagszűrőjének segítségével - "elkapja", és magára irányítja
- Az átirányított kapcsolatokat pedig a proxy program fogadja, és a nem-transzparens proxy-k működéshez hasonlóan kezeli őket
- Kiemelten támaszkodik az alacsonyabb szintű csomagszűrőre
- A csomagszűrő és a hagyományos proxy megfelelő együttműködése eredményezi a sima proxy-knál kényelmesebb használati módot – a klienseken nem kell semmit sem konfigurálni

Moduláris proxy tűzfalak

- A moduláris proxy tűzfalak rendelkeznek a transzparens tűzfalak minden jó tulajdonságával, azaz képesek az átmenő adatfolyam alkalmazásszintű szűrésére, csomagszűrő kiegészítőt tartalmaznak, valamint transzparensnek a kliens számára
- Az alapvető különbség a hagyományos transzparens tűzfalak és a moduláris tűzfalak között, hogy míg a transzparens tűzfalak minden protokoll értelmezésére, elemzésére különálló tűzfal komponenssel rendelkeznek, amelyek nem képesek együttműködésre, valamint sok esetben bizonyos funkciókat mindegyik komponens megvalósít (kapcsolat fogadása, kapcsolódás a szerverhez, stb.), addig a moduláris proxy részei, moduljai képesek együtt működni, valamint a különböző feladatok ellátását más-más modul végzi, csökkentve ezzel a felesleges redundanciát

Moduláris proxy tűzfalak

- Példa: HTTPS
 - Ekkor egy SSL proxy és egy HTTP proxy kerül kombinálásra, ezek együttműködnek
 - Az SSL proxy kapja meg az átmenő forgalmat, azt dekódolja , majd a dekódolt forgalmat átadja a HTTP proxynak
 - A HTTP proxy már a sima HTTP kérést kapja meg, mintha azt egy sima klienstől kapná
 - A kérés feldolgozása után a HTTP proxy a kérést továbbküldi, mintha a szervernek küldené, de a kérés az SSL proxyhoz kerül, amely a kérést újra titkosítja és elküldi a szervernek

Mély-protokollelemzés

- A protokollok betartását alap esetben egy hálózati eszköz sem ellenőrzi!
- Ez nagy teret ad a rosszindulatú támadóknak, hiszen sok hálózati eszközben és alkalmazásban vannak olyan biztonsági rések, amiket, a protokollt sértő metódusokkal ki lehet játszani
- Amennyiben a proxy alkalmazás a teljes szabványt megvalósítja, tehát ismeri az összes utasítást és attribútumot, egyfajta hálózati rendészként minden szabványt sértő kommunikációs próbálkozást megtagadhat
- További előnye a mély protokollelemzésnek, hogy segítségével a tűzfal „élesebben lát”: a hálózati kommunikációban jóval részletesebben tud eseményeket megkülönböztetni egymástól, aminek következtében a reakciója is kifinomultabb lehet
- Példa: web – get ill. header oldal ill. fejléc lekérés, megjön, amit kértük, ezután a kapcsolat normális esetben lezárul, de mi van, ha még jön valami ami egy security rést akar kihasználni – alapesetben ezt senki sem nézi

Firewall – Személyes tűzfal

- Az önálló felhasználói gépek védelmére az egyes gépekre telepített szoftver
- Inkább csak a neve tűzfal, valójában sok köze nincs is hozzá
- MS: Zóna
- Kerio tűzfal

Tartalomszűrési megoldások

- A tűzfalak vizsgálják a rajtuk áthaladó adatokat – egyúttal speciális ellenőrzéseket is végezhetnek: pl. a vállalat dolgozói munkaidőben ne nézzenek irreleváns, pornó stb. oldalakat ill. vírusfertőzött fájlok ne juthassanak be
- A tűzfalakhoz tartozó kiegészítő szoftverek biztosítanak tartalomszűrő funkciókat
- Kulcsszó szerinti keresés
 - Meghatározott tiltólistán szereplő szavak, szavak közötti összefüggések keresése – messze nem tökéletes módszer (Sátoraljaújhely!)
- Képtartalom szerinti keresés
 - Ruha nélküli testfelületek aránya a képben (csecsemő fürdetés!)
- URL szűrés
 - Folyamatosan frissített adatbázis, amely web oldalakat és hozzájuk rendelt kategóriákat tartalmaz (többnyire a tartalomszűrő gyártója tartja karban)
 - A vállalat policy-jának megfelelően az egyes kategóriák tiltottak ill. megengedettek (tiltott web site lekérésekor a felhasználó a kért web oldal helyett figyelmeztető üzenetet kap)

Tartalomszűrési megoldások

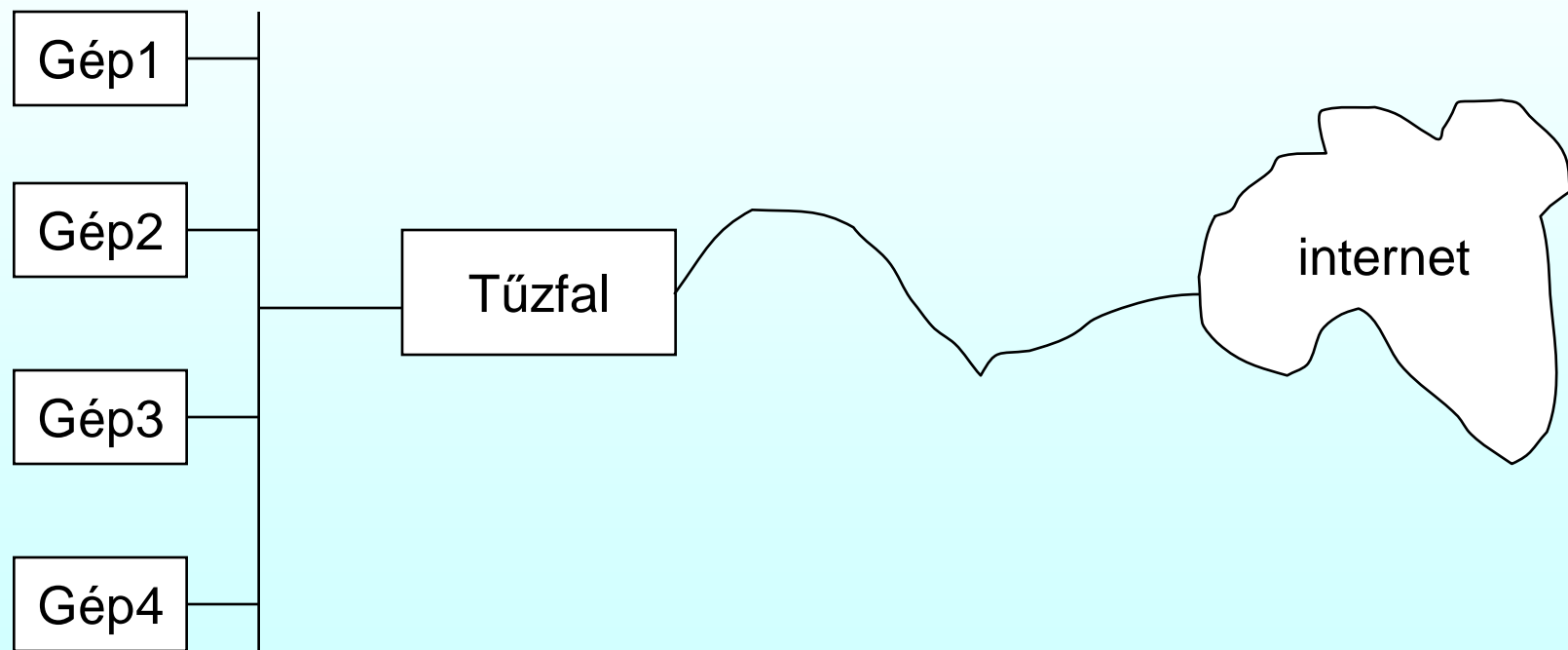
- Víruskeresés
 - A tűzfalat egy speciális víruskeresővel egészítik ki, amely képes a tűzfal által átadott adatok vírusellenőrzésére (a háttérben itt is egy adatbázis van)
 - Fertőzött fájl esetén, akkor a víruskereső megpróbálhatja először fertőtleníteni, illetve ha az nem sikerül, akkor karanténba helyezi, további vizsgálat céljából
 - Többfajta adatforgalom is ellenőrizhető: e-mailek, FTP és HTTP forgalom is szűrhető víruskeresővel
 - Elterjedt víruskereséshez felhasznált protokoll: CVP (Content Vectoring Protocol)

DMZ (Demilitarized Zone)

- Ha egy cég saját SMTP, HTTP és egyéb kiszolgálókat üzemeltet, mindig felmerül az a kérdés, hogy hova tegye a kiszolgálókat
- A DMZ egy olyan hálózati szegmens, ami az Internet felől védett, de nem a belső hálózaton van, hanem egy harmadik alhálózat
- A DMZ a benne elhelyezkedő hálózati eszközökhöz és erőforrásokhoz mind a megbízott belső, mind a megbízhatatlan külső területről engedélyezi a hozzáférést, de megakadályozza, hogy a külső területről bármilyen kérés vagy hozzáférési kísérlet eljusson a belső hálózatra

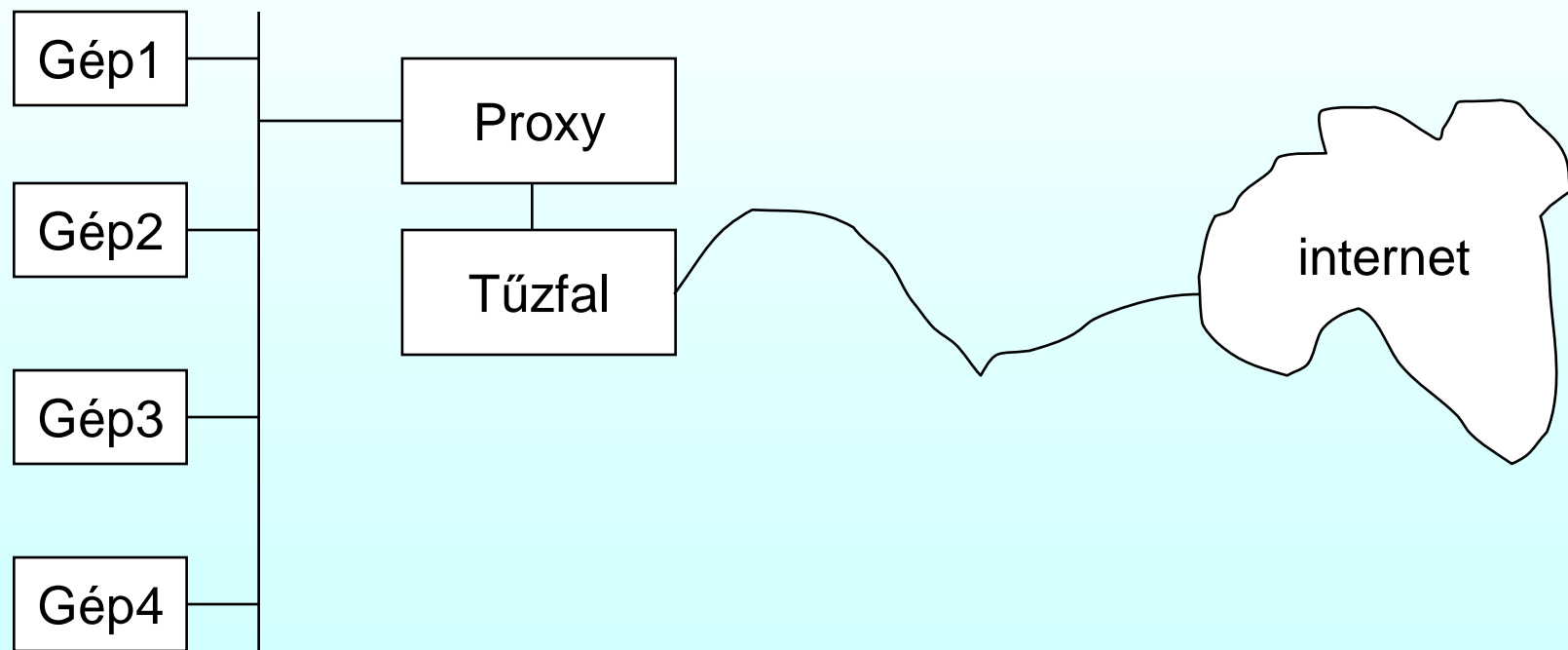
Tűzfal, DMZ, Proxy

- Struktúra



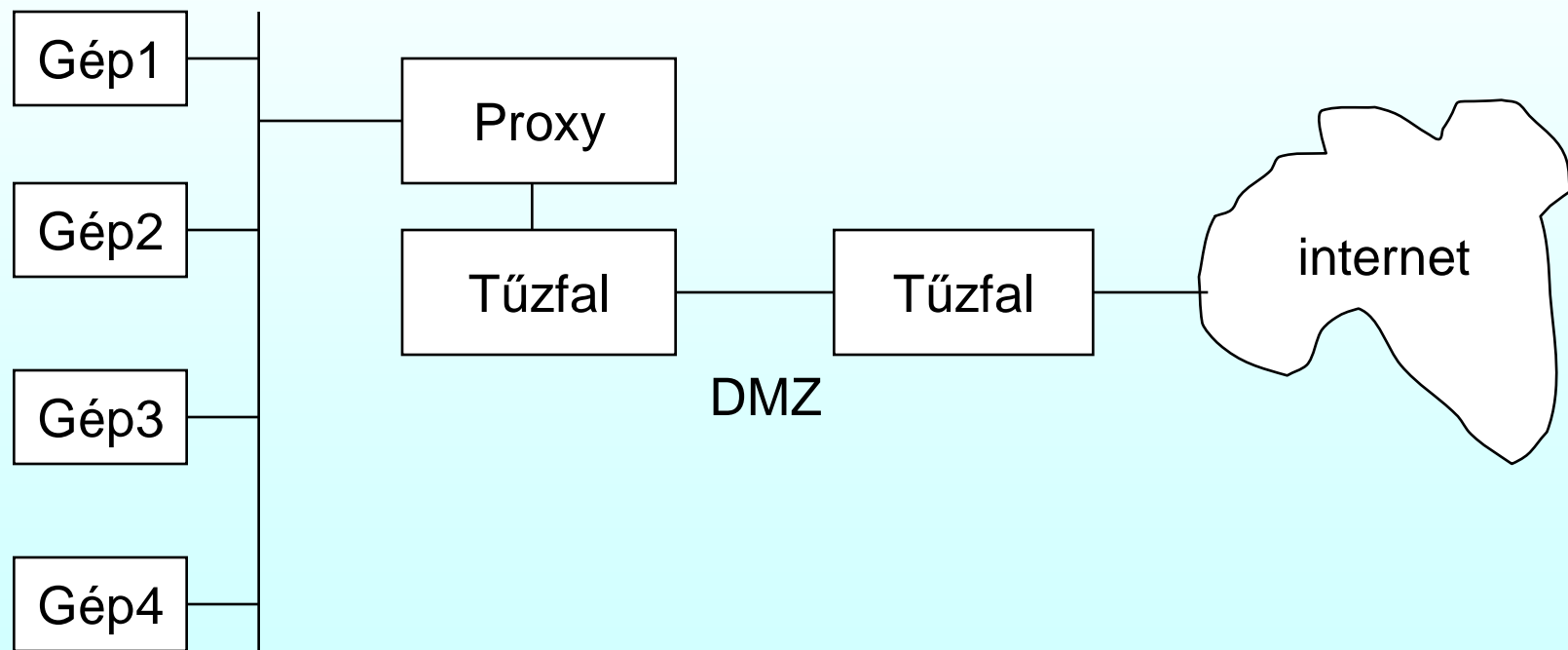
Tűzfal, DMZ, Proxy

- Proxy + Tűzfal



Tűzfal, DMZ, Proxy

- DMZ



Tűzfal – Mire nem jó?

- A belső visszaélésekre alig van hatással
- Az emberi hibák következményeit nem szünteti meg
- A megfelelő szabályozások hiányát nem szünteti meg

NAT (Network Address Translation)

- IPv4 probléma: kevés az IP cím
 - rfc 1631, rfc 3022
 - A címezési rendszer kidolgozásakor nem számítottak ennyi gépre – számuk egyre növekszik
 - 2^{32} gép???
 - (Bizonyos esetekben megoldás a dinamikus IP címkiosztás, pl. betárcsázós kapcsolat)
 - Az IPv6 hosszú távon végleges megoldást jelenthet

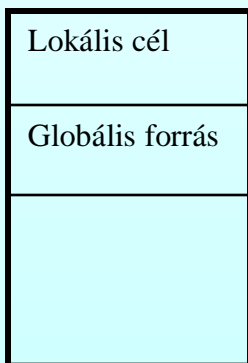
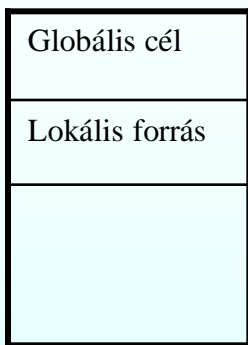
NAT

- **Megoldás**

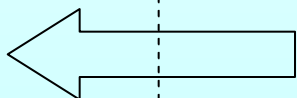
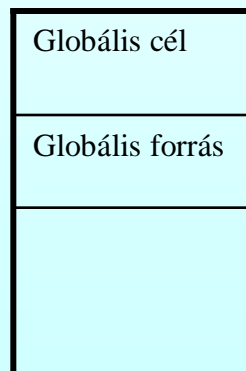
- Külső és belső IP címek: egy szervezet IP hálózata kívülről más címtartományban jelenik meg, mint amit belül valójában használ
- A cégek egy vagy csak néhány IP címet kapnak, ez(ek) látható(k) az Internet felől (globális, külső IP cím)
- Cégen belül az egyes gépek egyedi IP címekkel rendelkeznek, de ezek az Internet felől nem láthatók (lokális, belső IP cím)
- A privát hálózat és az Internet határán a belső címek lecserélődnek a cég külső IP címére (címeire)
- Alkalmazási területek
 - A szolgáltató váltás egyszerűvé válik (nem kell minden gép IP címét átállítani)
 - Több gép érheti el az Internetet, mint ahány IP címmel rendelkezik a szervezet
 - Teherlésmegosztás – virtuális szerver (pl. egy IP cím mögött több azonos tartalommal rendelkező web szerver van)
- Akkor használható célszerűen, ha egyidőben a gépeknek csak viszonylag kis része kommunikál a külső hálózattal

NAT

Belső hálózat



Külső hálózat



NAT

- Eljárás küldéskor
 - Amikor egy IP csomag elhagyja a hálózatot a belső IP címe le lesz cserélve külső IP címre (címfordítás)
 - A csomag TCP(UDP) headerében **a forrás port is le lesz cserélve** egy pointerre, amely egy táblázat egy bejegyzésére mutat
 - (Az headerek control szummáit újraszámolják és az új értékkel helyettesítik)
 - A bejegyzés tartalmazza az eredeti (belső) IP címet és az eredeti forrás port értéket
- Eljárás a válasz visszaérkezésekor
 - A TCP (UDP) header cél port mezőjében pointer szerepel, az IP headerben pedig a külső IP cím
 - A táblázat és a pointer alapján külső IP cím le lesz cserélve a belső IP címre, a cél port pedig az eredeti forrás port értékre
 - (Az headerek control szummáit újraszámolják és az új értékkel helyettesítik)
 - A csomag a belső IP címnek megfelelően továbbításra kerül
- Statikus/dinamikus címfordítás
 - Statikus: Egy-egy értelmű megfeleltetés a belső és külső címek között, ez esetben a csere nincs adminisztrálva a táblázatban (ha bizonyos gépeknek mindig azonos IP címmel kell megjeleníteniük a külső hálózaton)
 - Dinamikus: A belső IP címekhez a külső IP címek egy tartományából (pool) lesz külső IP cím rendelve

NAT

- Kijelölt belső IP címtartományok
 - 10.0.0.0 - 10.255.255.255/8 (>16M host)
 - 172.16.0.0 – 172.31.155.255/12 (>1M host)
 - 192.168.0.0 – 193.168.255.255/16 (>65e host)
- NAT box, router
 - A címfordítást a NAT box végzi, ami gyakran egy egységet alkot a routerrel és a tűzfallal
 - A címfordító router nem hirdeti a belső hálózatot kifelé, de a külső hálózatról jövő routing információt a szokásos módon hirdeti a belső hálózatban
 - Ha a fordítás nem lehetséges (pl. betelt a táblázat), a NAT box eldobja a csomagot és egy ICMP „Host Unreachable” üzenetet küld a forrásnak

NAT

- Problémák
 - Az IP architektúrális modellje sérül
 - Minden IP cím egyértelmű módon kellene, hogy azonosítson egy gépet
 - A k-adik réteg nem tudhat semmit arról, hogy mi van a k+1-edik réteg headerében (pl. nem TCP vagy UDP kapcsolat, továbbfejlesztett TCP header stb.)
 - Összeköttetés nélküli kapcsolat alapelve nem teljesül
 - A NAT box a kapcsolatról információt tárol: a kapcsolatállapot nyilvántartási tulajdonság az összeköttetés alapú hálózatokat jellemzi
 - A NAT box kritikus elem: kiesésével a táblázat elvész, az egész TCP kapcsolat megszűnik
 - A forrás port tartománya (16bit) limitálja a táblázat méretét
 - A fenntartott első 4096 port miatt a táblázat maximális mérete 65535-4096
 - Ennél több gép esetén több külső IP cím szükséges
 - Némelyik alkalmazással nem feltétlenül működik együtt
 - Szabványos FTP
 - H.323