

INFORMATIKAI BIZTONSÁG ALAPJAI

7. előadás

Göcs László

főiskolai tanársegéd

Neumann János Egyetem GAMF Műszaki és Informatikai Kar

Informatika Tanszék

TÁMADÁSOK ÉS VÉDEKEZÉSEK AZ IT RENDSZEREKBEN

2016. május. 13. 15:33 · MTI · VILÁG

Berlin Oroszországot vádolja egy tavalyi hackertámadásért

Egy az orosz állam által irányított csoport állhatott egy tavalyi Bundestag elleni kibertámadás mögött a német hírszerzés szerint.

2016. április. 02. 21:06 · MTI · ITTHON

Bakondi: Még támadás alatt áll a kormányzati hálózat

Szombaton este azt mondta Orbán Viktor belbiztonsági tanácsadója, hogy nem tudja, ki támadta meg a kormányzati honlapokat, de a támadás még tart.

2016. április. 27. 14:01 · hvg.hu · TECH

Vírust találtak az egyik német atomerőműben

Két rosszindulatú programot is talált az üzemeltető a bajor létesítményben. Konkrét veszély most nincs, de innentől már tényleg csak egy lépés, hogy legyen.

2014. február. 12. 23:10 · MTI · TECH

Kína beismerte, hogy vannak kiberháborús kommandói

Kína mindeddig visszautasította azokat a vádakát, hogy amerikai cégeknél kémkedne vagy képes lenne kibertámadásokra, most azonban egy amerikai kutató szerint egy hivatalos kiadványban ismerte be, folytat ilyen tevékenységet.

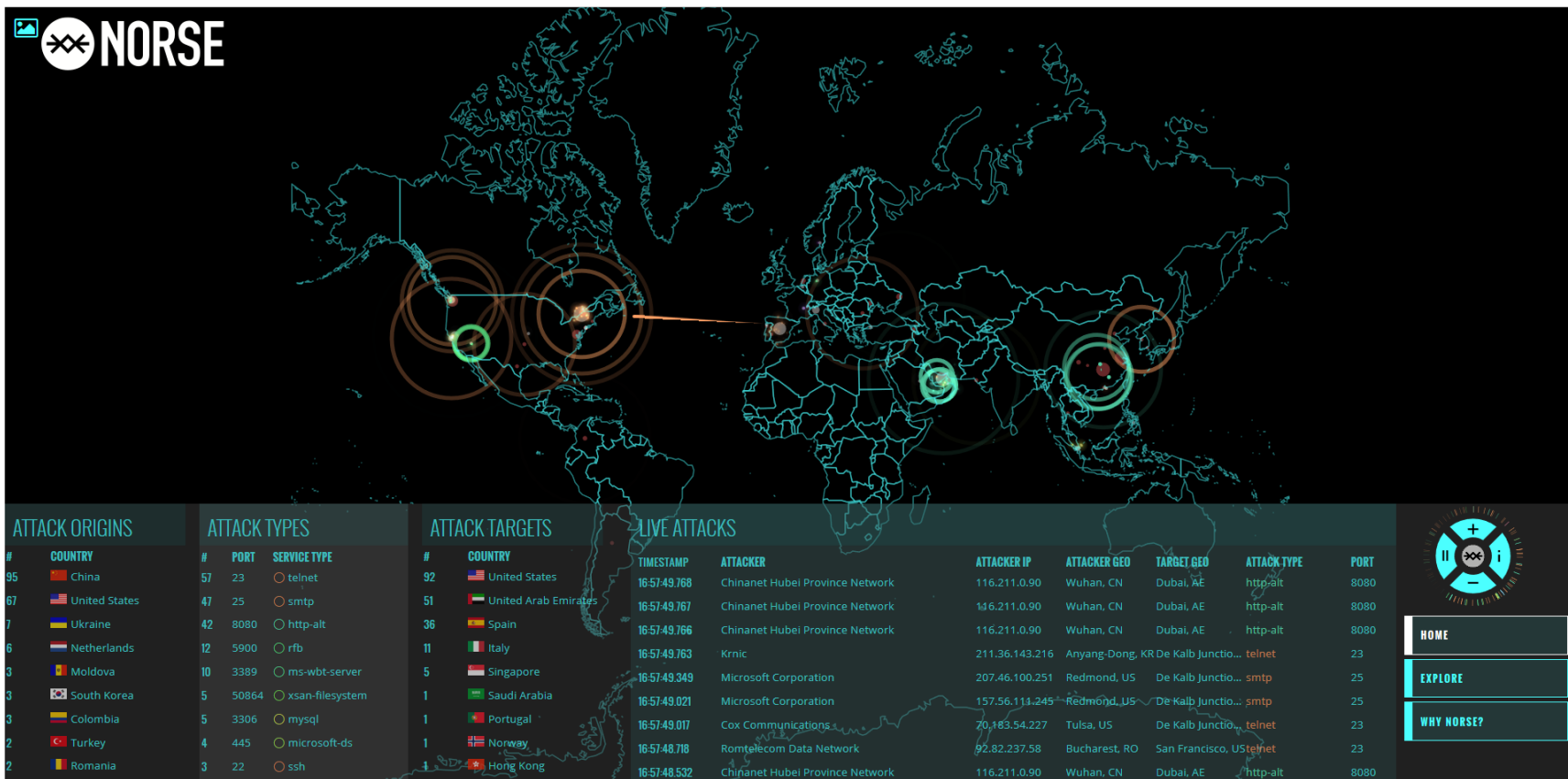
2014. február. 12. 23:10 · MTI · TECH

Megtámadtak egy magyar számítógépgyárat, lopott mobilokat akartak legalizálni

Öt ember, köztük két román állampolgár ellen emelt vádat a Zalaegerszegi Járási Ügyészség, amiért a Flextronics zalaegerszegi gyárában behatoltak a cég számítógépes rendszerébe, majd azon keresztül a kanadai cégközpontba, hogy egyebek mellett lopott mobiltelefonokat legalizáljanak.

TOP 10 (Balabit felmérés)

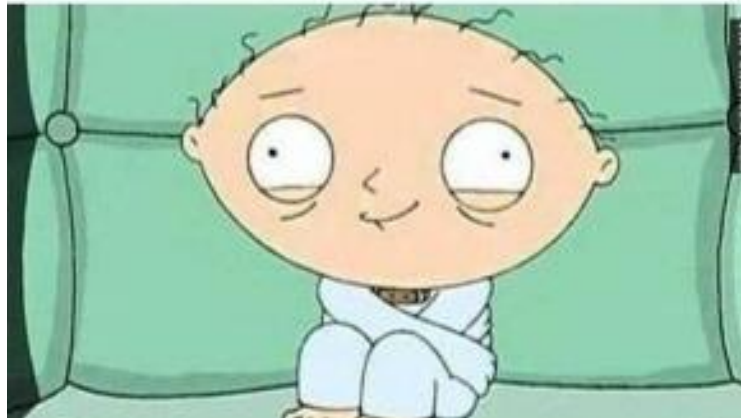
- Social engineering (például adathalászat)
- Kompromittált hozzáférések (gyenge jelszó)
- Web alapú támadások (SQL/command injection)
- Kliens oldali támadások (például dokumentum olvasó, web böngésző)
- Szerverfrissítésekre írt exploit-ok (például OpenSSL, Heartbleed)
- Nem menedzselt privát eszközök (például rossz BYOD szabályzat)
- Fizikai behatolás
- Árnyék informatika
- Külső szolgáltatók igénybevétele (kiszervezett infrastruktúra)
- Felhő infrastruktúrába kihelyezett adatok megszerzése (például IAAS, PAAS)



<http://map.norsecorp.com/#/>

Legbiztosabb módszer a védekezésre?

LIFE WITHOUT
INTERNET



Tűzfal

- A tűzfal **két vagy több hálózat között** helyezkedik el és ellenőrzi a közöttük zajló forgalmat, valamint segíti a jogosulatlan hozzáférés elleni védelmet.
- A tűzfal az egyik leghatékonyabb olyan biztonsági eszköz, mely a **belső hálózati felhasználók külső veszélyektől való megvédésére** rendelkezésre áll.
- A tűzfal-termékek akár többféle szűrést is támogathatnak.
- Ezen kívül a tűzfalak gyakran hálózati címfordítást (Network Address Translation, **NAT**) is végeznek.

Tűzfal

- Csomagszűrés - az **IP** vagy **MAC-cím** alapján **akadályozza meg vagy engedélyezi** a hozzáférést.
- Alkalmazás/Webhely szűrés - Az **alkalmazás** alapján **akadályozza meg vagy engedélyezi** a hozzáférést.
- A webhelyek, egy meghatározott weblap **URL címe** vagy **kulcsszavak** alapján blokkolhatók.

SPI

- Állapot-alapú csomagvizsgálat (Stateful Packet Inspection, SPI) - A bejövő csomagok csak a belső hálózat állomásairól kezdeményezett kérések válaszcsomagjai lehetnek.
- A **nem kívánatos csomagokat** külön engedély hiányában kiszűri. Az SPI felismerhet és kiszűrhet bizonyos típusú támadásokat is (pl.: DoS).

Tűzfal megvalósításai

- Eszköz-alapú tűzfal
- Kiszolgáló-alapú tűzfal
- Integrált tűzfal
- Személyes tűzfal

Eszköz alapú tűzfal

- Egy biztonsági készülékként ismert **célhardverbe** van beépítve.
- Nem rendelkezik perifériával és merevlemezzel.
- **Gyors**abban képes a forgalmat megvizsgálni.



Kiszolgáló alapú tűzfal

- Egy tűzfalalkalmazás, amely valamilyen hálózati **operációs rendszer alatt fut** (Network OS: UNIX, Windows, Novell).
- SPI tűzfalat és az IP cím vagy alkalmazás alapú hozzáférést kombinálja.
- **Kevésbé biztonságos** az általános célú OS biztonsági hiányosságai miatt.



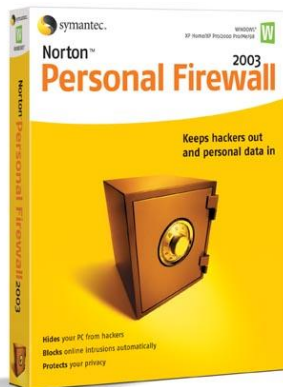
Integrált tűzfal

- Egy meglevő eszköz (pl.: forgalomirányító) **tűzfalszolgáltatással kiegészítve.**
- Az integrált forgalomirányítók rendelkeznek alapvető tűzfal szolgáltatással (csomag, alkalmazás, webhely szűrés)
- A nagy teljesítményű forgalomirányítók is rendelkeznek tűzfal szolgáltatással.



Személyes tűzfal

- A **munkaállomáson** helyezkedik el, nem LAN megvalósításra tervezték.
- Lehet az operációs rendszer **beépített** szolgáltatása, vagy származhat **külső gyártótól** is.



Személyes tűzfal

- A személyes tűzfal külön álló asztali rendszerek védelmére kifejlesztett alkalmazás, mely **hálózati csatoló** és az azt igénybe vevő **operációs rendszer**, illetve annak alkalmazásai között a beállított szabályok szerint vizsgálja a hálózati forgalmat.

Személyes tűzfal

- A személyes tűzfalak általában háromféle feladatot látnak el:
 - A **beérkező** forgalmat blokkolni tudják szolgáltatás/program, port és protokoll (TCP/UDP) szerint.
 - A **kimenő** forgalmat blokkolni tudják program, port és protokoll szerint.
 - A bejövő forgalomra általában valamilyen **tartalom szerinti szűrést** is végeznek (scriptek, cookie-k, ... stb blokkolása).

Személyes tűzfal

- A személyes tűzfalak, egy "tanulási" folyamattal jutnak el ahhoz, hogy mely kommunikációt engedélyezzenek, ezért konfigurálásuk lényegében nem szükséges.
- Minden egyes új kommunikáció kezdeményezésekor megkérdezik, hogy azt engedélyezzük-e? (permit - deny) És ha igen, hogy ezt általános szabályként akarjuk-e, emlékezzék-e erre?
- Amennyiben ezt általános szabályként akarjuk, többet nem kérdeznek arra a programra. Így az elindulás után sokat kérdez(het)nek, de utána már csendben vannak.
- A konfigurálásuk ezért meglehetősen egyszerű. Mindegyiknél van mód a szabályok későbbi megtekintésére és azokat akkor módosíthatjuk is.

A tűzfal használata

- A tűzfalnak mint határkészüléknek, a belső hálózat (intranet) és az Internet közé helyezésével minden **kifelé és befelé irányuló Internet forgalom** megfigyelhető és ellenőrizhető.
- Mindemellett néhány külső ügyfélnek szüksége lehet a belső erőforrások használatára. Ennek biztosítására lehet kiépíteni a **demilitarizált zónát (DMZ)**.

Demilitarizált zónát (DMZ)

- Azt a területet írja le, amely a belső és külső hálózat (internet) **között** helyezkedik el.
- Ide kerülhetnek a webkiszolgálók, FTP kiszolgálók, SMTP kiszolgálók, DNS kiszolgálók.
- Mind a belső, mind a külső felhasználók számára **hozzáférhető**.
- A belső hálózatot, a DMZ-t és a külső hálózatot egy vagy több tűzfallal különítik el.

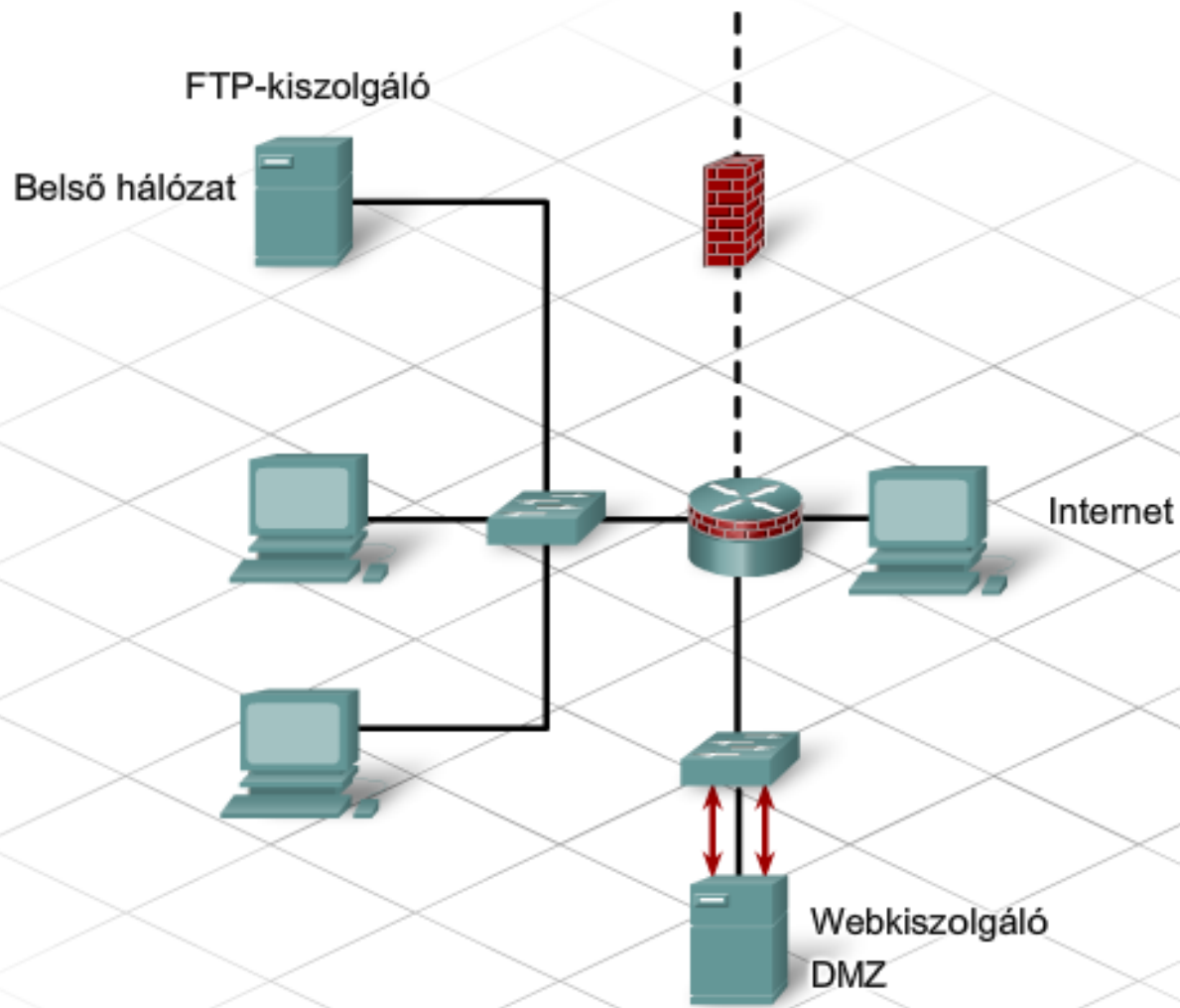
Egytűzfalas konfiguráció

- Az egyedüli tűzfal három területtel rendelkezik, egy-egy területtel a külső hálózat, a belső hálózat, és a DMZ számára.
- **Minden külső** hálózatból származó forgalom a tűzfalhoz kerül elküldésre.
- A tűzfallal szembeni elvárás az is, hogy **ellenőrizze** a forgalmat és határozza meg, hogy mely forgalmat kell a DMZ-be, melyet kell a belső hálózatba továbbítani és melyet kell végképp elutasítani.

Egytűzfalas konfiguráció

- Az egytűzfalas konfiguráció a **kisebb**, kevésbé terhelt hálózatokhoz megfelelő.
- Az egytűzfalas konfiguráció **egyetlen meghibásodási** ponttal rendelkezik és **túlterhelhető**.

Egy tűzfalas konfiguráció

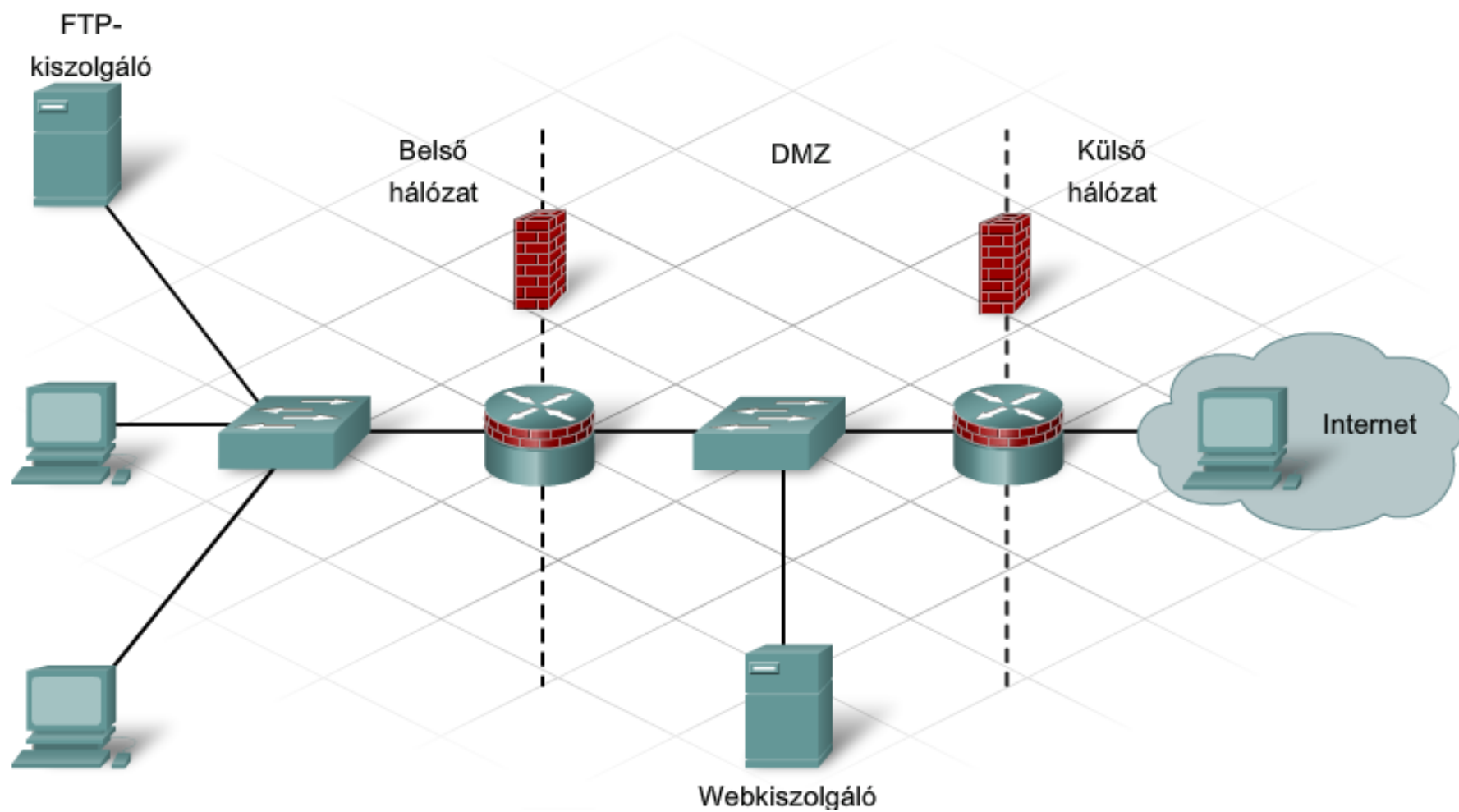


Kéttűzfalas konfiguráció

- A két tűzfalas konfigurációnál **egy belső és egy külső** tűzfal található a kettőjük között elhelyezkedő DMZ-vel együtt.
- A külső tűzfal kevésbé korlátozó és megengedi, hogy az **Internet** felhasználók **hozzáférjenek a DMZ-ben levő** szolgáltatásokhoz valamint megengedi, hogy bármely **belső felhasználó** által kért forgalom **áthaladjon rajta**.

Kéttűzfalas konfiguráció

- A belső tűzfal **jóval korlátozóbb** és védi a belső hálózatot a jogosulatlan hozzáféréstől.
- A kéttűzfalas konfiguráció inkább az olyan nagyobb, összetettebb hálózatok számára alkalmas melyek jóval **nagyobb forgalmat** bonyolítanak le.



Tűzfalak használata

- Sok otthoni eszköz, mint például egy integrált forgalomirányító, gyakran többfunkciós tűzfalszoftvert tartalmaz.
- Az ilyen tűzfal jellemzően:
 - Hálózati címfordítás (**NAT**),
 - Állapot alapú csomagvizsgálat (Stateful Packet Inspection, **SPI**),
 - IP, alkalmazás és webhely **szűrő** képességgel rendelkezik.
 - Támogatja a **DMZ** lehetőségét is.

A Tűzfal használata

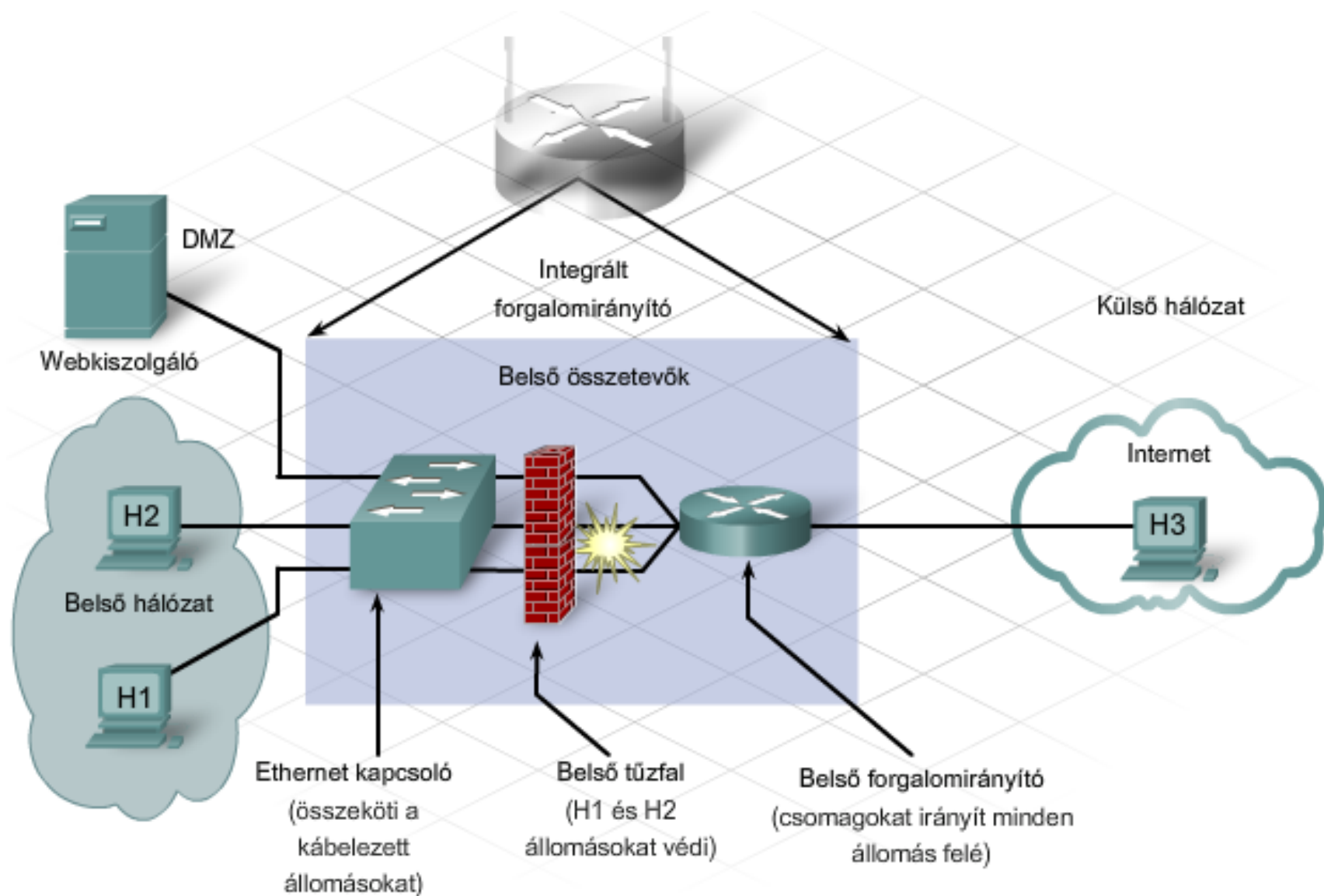
- Az integrált forgalomirányítóval egy olyan egyszerű DMZ állítható be, amely megengedi hogy egy belső kiszolgáló a külső állomások számára hozzáférhető legyen.
- Ennek megvalósítása érdekében a **kiszolgálónak statikus IP-címre** van szüksége, melyet a DMZ konfigurációban meg kell határozni.
- Az integrált forgalomirányító elkülöníti a meghatározott cél IP-című forgalmat.
- Ez a forgalom csak ahhoz a **kapcsoló-porthoz** lesz továbbítva amelyhez a kiszolgáló kapcsolódik.
- Az összes többi állomást így még inkább védi a tűzfal.

A tűzfal használata

- A **port-alapú továbbítás** használatával jóval korlátozóbb DMZ állítható be.
- A port-alapú továbbítás esetén meg vannak határozva azok a portok melyek a kiszolgálón elérhetők.
- Ebben az esetben **csak az adott célportokra irányuló** forgalom engedélyezett, minden más forgalom tiltott.

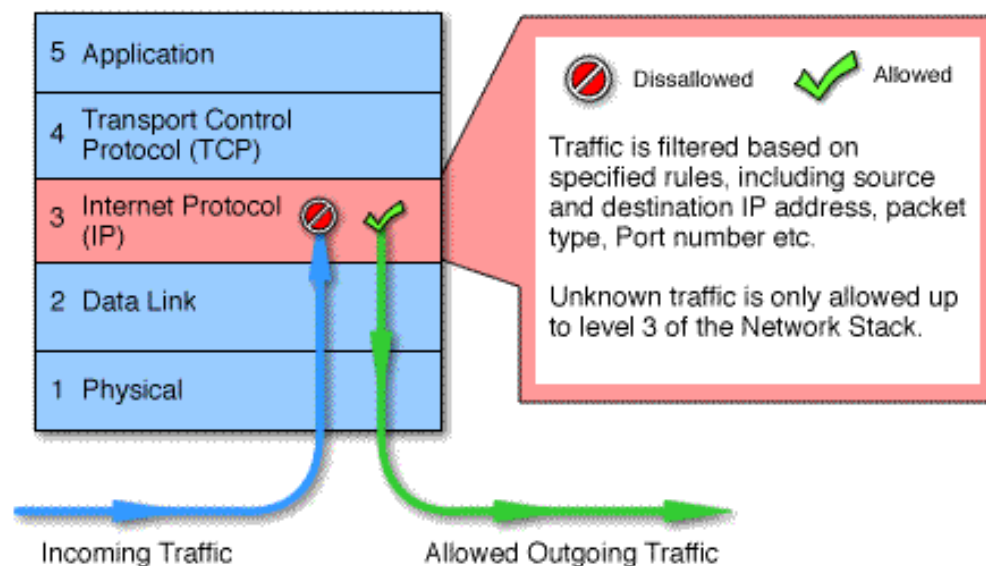
A tűzfal használata

- Az integrált forgalomirányítón belüli **vezeték nélküli** elérési pont a **belső hálózat** részének tekintendő.
- Fontos annak megértése, hogy ha a vezeték nélküli elérési pont **nem biztonságos**, bárki, aki ahhoz csatlakozik a belső hálózat védett részére, a **tűzfal mögé** kerül.
- A hekkerek (hacker) így a biztonsági szolgáltatások kikerülésével juthatnak a belső hálózatba.



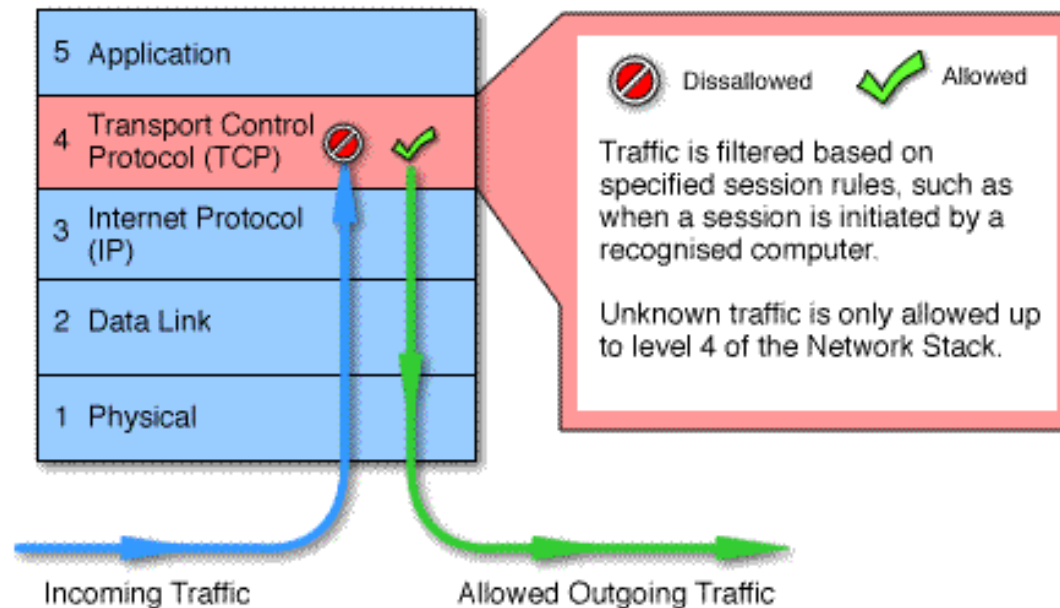
TŰZFAL KATEGÓRIÁK

Csomagszűrős tűzfal (Packet Filtering)



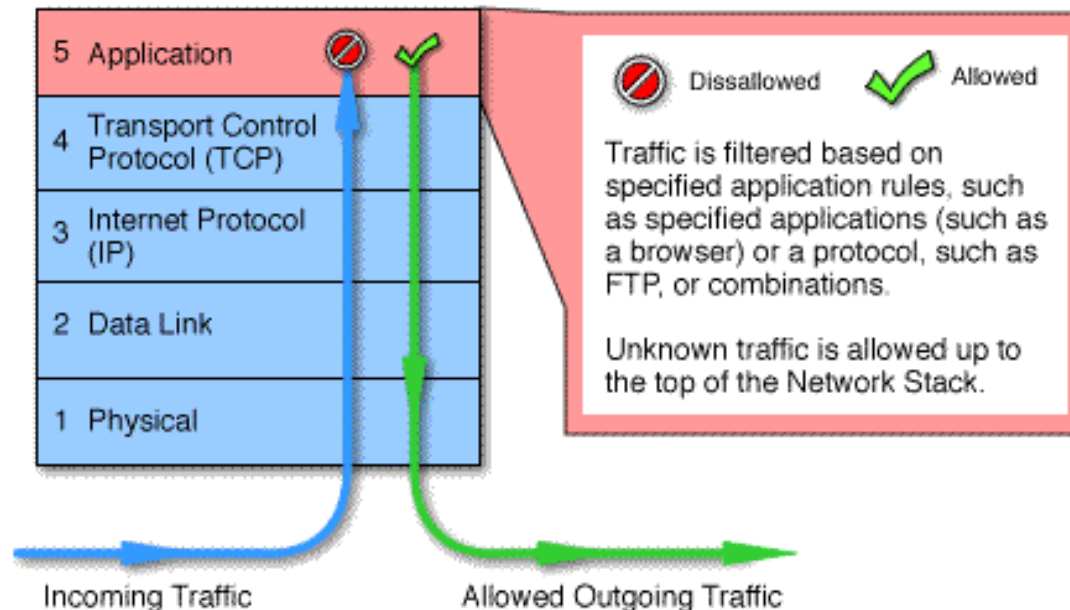
- A továbbküldés előtt minden csomag eleget kell tegyen egy bizonyos kritériumnak: forrás és cél IP, csomag típus, port szám.

Circuit-Level gateway



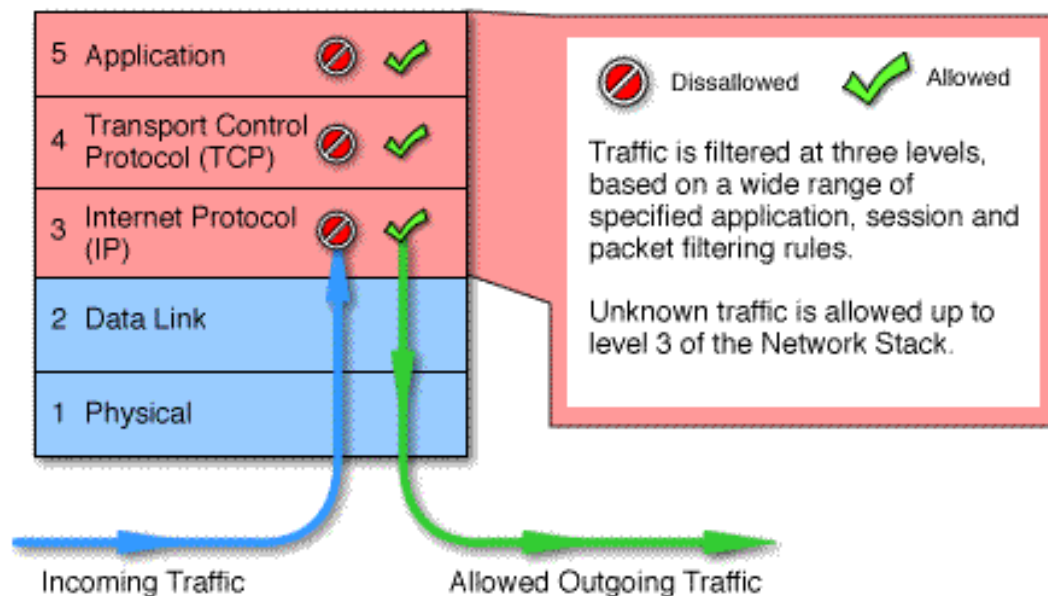
- A csomagok közötti kapcsolat felépítésére vonatkozó ajánlatokat felügyelik.

Application Level Gateway



- Amikor csomagok kívülről érkeznek, megvizsgálja és értékeli, hogy a csomag bekerülhet-e a belső hálózatra. A szerver kiértékeli az IP-címét, de emellett értékeli az adatokat és a csomagokat, hogy ne legyenek hackerek támadják az információkat, a csomagokat.

Stateful Inspection



- Az előző három tűzfal tulajdonságait egyesíti. Kliens és gazda között direkt összeköttetést létesít, ezáltal megoldja a többi hibáit. Felismeri és kezeli az alkalmazás szintű adatokat. Nagy sebesség, magas biztonság.

PROXY SZERVER

Mi a PROXY?

- Speciális tűzfal-típus, amely a közvetlen kommunikációt a külső és a védett hálózat között nem teszi lehetővé.
- E helyett a **belső hálózatról érkező kéréseket** feldolgozza, majd azokkal azonos értelmű kérést küld a külső szerver felé, az azokra érkező válaszokat pedig ismét a belső hálózat felé továbbítja.
- A proxy szerverek sok esetben **tartalmi gyorsítótárat** is magukban foglalnak, így bizonyos esetekben jelentős mértékben **csökkenthetik a kifelé irányuló forgalmat**.

Mi a PROXY?

- Az Interneten arra használják, hogy a szolgáltatások elérésére irányuló kéréseket **ne saját maga válaszolja** meg, hanem irányítsa azokat egy közeli (innen a név: proxy -- **közelben lévő**) kiszolgálóhoz, amely az adott szolgáltatással rendelkezik és nagyobb teljesítményt produkál.
- A proxyk biztonsági szerepet is játszhatnak (pl. tűzfalak), de gyakran a cél csupán az **ellenőrizhetőség** és **naplózhatóság** (pl. egy cégnél lévő alkalmazottak HTTP proxy-n át érhetik el az internetet, így tevékenységeiket ellenőrizni és megfigyelni is lehet).

Gyorsító tárazás

- Másik igen jelentős felhasználási terület a rendelkezésre álló **sávszélesség kihasználtságának javítása** illetve annak kímélése a végfelhasználótól egészen a kiszolgáló webszerverig.
- Az igény szerinti **gyorsító tárazási modell** intelligens módon, felhasználói kérések alapján **tárolja a letöltött adatokat**. Mindezt annak érdekében, hogy a lehető leghatékonyabb módon végezze a tartalom változásának követését, annak frissítését és az adatok szolgáltatását.

Gyorsító tárazás

- Több felhasználós környezetben (hálózatban kötött gépek) gyakran előfordulhat **ugyanazon oldalak ismétlődő látogatása**.
- A proxy szerver letölti és elmenti az oldalak tartalmát egy **átmeneti tárolóban**, majd újabb kérés esetén a tartalom egyezőségét illetve annak változását több előre beállított szempont szerint is megvizsgálja.
- Végezetül eldönti hogy újratölti az **egészet**, az oldal **egy részét**, illetve a tartalom **megegyezik** az átmeneti tárban lévővel így azt továbbítja a felhasználó felé.

Proxy

- A kis, a közép és a nagyvállalati környezetben is alapvető elvárás a különböző hálózati protokollokon alkalmazott **tartalomszűrési lehetőség**:
- **HTML Tag Filters** (OBJECT, EMBED, APPLET, SCRIPT, IMG illetve adott a lehetőség tetszőleges számú és tartalmú szűrő létrehozására).
- **MIME Filters** ebben az esetben a rendelkezésünkre áll a teljes MIME táblázat tartalma (pl: application/zip, video/mpeg, audio/x-wav).
- **URL** alapján történő szűrés” (előre elkészített lista vagy reguláris kifejezések alapján).

ROUTEREK HOZZÁFÉRÉSI LISTÁJA

Biztonság

- A vállalati hálózaton belül a biztonság alapvető fontosságú.
 - Illetéktelen felhasználók belépésének megakadályozása.
 - Hálózat védelme a különféle támadásokkal (pl.: DoS támadás) szemben.
- Mindkét eset idő- és pénzveszteséggel jár a vállalat számára.

Forgalomszűrés

- Segítségével a hálózati rendszergazda felügyelheti a hálózat különböző részeit.
- A szűrés a csomagtartalom elemzésének folyamata, amely alapján eldönthető, hogy egy adott csomagot átengedünk vagy blokkolunk.
- A forgalomszűrés javítja a hálózat teljesítményét.

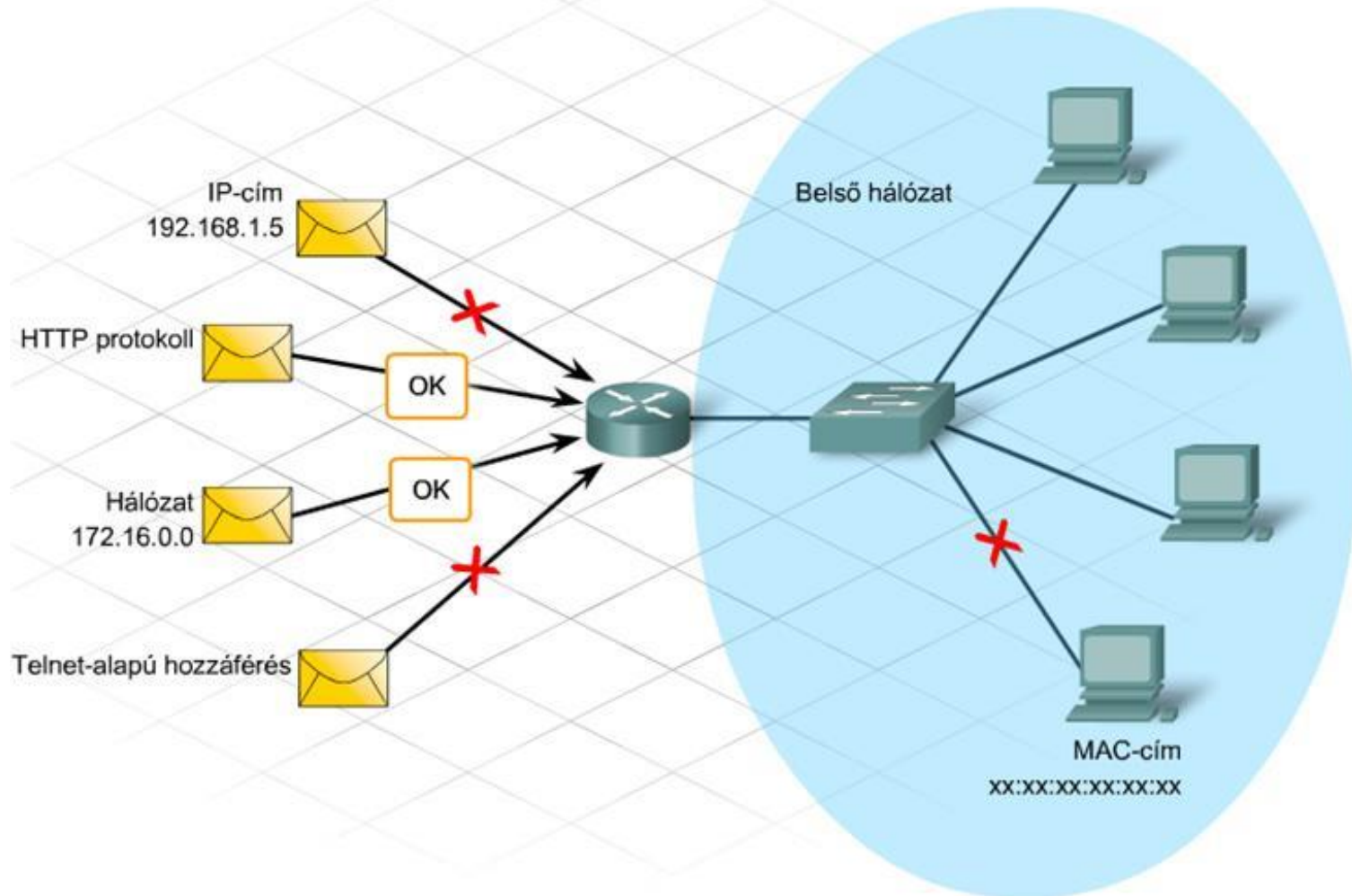
Forgalomszűrés

- A forgalom engedélyezése vagy tiltása az alábbiak szerint történhet:
 - Forrás IP-cím
 - Cél IP-cím
 - MAC-cím
 - Protokollok
 - Alkalmazástípus

Forgalomszűrés menete

- Be kell állítani a forgalomirányítót a nemkívánatos forgalom azonosítására.
- A nemkívánatos forgalom forráshoz közeli tiltásával a forgalom nem halad keresztül a hálózaton, és nem pazarol el értékes erőforrásokat.

Forgalomszűrés



Forgalomszűréshez használt eszközök

- Integrált forgalomirányítóba épített tűzfalak
- Adatbiztonsági funkciókat ellátó célkészülékek
- Kiszolgálók

Forgalomirányító forgalomszűrés

- Szinte minden forgalomirányító képes a
 - Forrás és cél IP-cím alapján történő csomagszűrésre.
 - Meghatározott alkalmazások és protokollok (pl. IP, TCP, HTTP, FTP és Telnet) szerinti szűrésre.

ACL - Access Control List

- A forgalomszűrés legáltalánosabb módja.
- A hálózatba belépő és az onnan távozó forgalom ellenőrizhető és szűrhető.
- Lehet egy adott forrásból érkező forgalmat engedélyező vagy tiltó egyetlen parancs,
- Lehet több száz parancsból álló lista is, ami különböző forrásból érkező csomagok átengedéséről vagy tiltásáról dönt.

ACL további használata

- A belső állomások meghatározása címfordításhoz.
- A speciális funkciókhoz (pl. QoS) tartozó forgalom azonosítása és csoportosítása.
- A forgalomirányítási frissítések tartalmi korlátozása.
- A hibakeresési üzenetek korlátozása.
- A forgalomirányítók virtuális terminálról történő elérésének szabályozása.

ACL-ek használatából eredő problémák

- Az összes csomag ellenőrzése terhelést jelent a forgalomirányítónak.
- A rosszul megtervezett ACL-ek még nagyobb terhelést okoznak, ami zavart okozhat a hálózat használatában.
- A nem megfelelően elhelyezett ACL-ek blokkolhatják az engedélyezni kívánt, és engedélyezhetik a blokkolni kívánt forgalmat.

ACL típusok

- Normál ACL
- Kiterjesztett ACL
- Nevesített ACL

Normál ACL (Standard ACL)

- Forrás IP-cím alapján végzi a szűrést
- A teljes (pl. IP) protokollműködés alapján engedélyezi vagy tiltja a forgalmat
- Adott PC vagy LAN számára engedélyezheti vagy tilthatja az összes szolgáltatás elérését
- Azonosítási száma 1-99, 1300-1999

| | | |
|--------|---|-------------------------------------|
| Normál | Router(config)#access-list 1 permit host 172.16.2.88 | • Egy bizonyos IP-címet engedélyez. |
|--------|---|-------------------------------------|

Kiterjesztett ACL (Extended ACL)

- Forrás IP-cím, cél IP-cím, protokoll és portszámok alapján szűrhet.
- Elterjedtebb, mivel specifikusabbak és jobb ellenőrzést tesznek lehetővé.
- Azonosítási száma 100-199, 2000-2699

| | | |
|---------------|---|---|
| Kiterjesztett | <pre>Router(config)#access-list 100 deny tcp 172.16.2.0 0.0.0.255 any eq telnet</pre> | <ul style="list-style-type: none">• Tiltja a 172.16.2.0/24 alhálózat számára bármely más állomás elérését, amennyiben telnetkapcsolatot próbálnak létesíteni. |
|---------------|---|---|

Nevesített ACL (Named ACL, NACL)

- Szám helyett névvel hivatkozunk
- Normál vagy kiterjesztett hozzáférési lista
- NACL üzemmód

| | | |
|------------|---|--|
| Nevesített | <pre>Router(config)#ip access-list standard permit-ip Router(config-ext-nacl)#permit host 192.168.5.47</pre> | <ul style="list-style-type: none">• Létrehoz egy permit-ip nevű normál hozzáférési listát.• Engedélyezi a hozzáférést a 192.168.5.47 IP-címről.• Az első parancs a forgalomirányítót NACL konfigurációs almódba helyezi. |
|------------|---|--|

ACL felépítése

- A hozzáférési listák egy vagy több utasításból állnak.
- A forgalmat minden egyes utasítás a megadott paraméterek alapján engedélyezheti vagy tilthatja.
- Az ACL utolsó utasítása mindig implicit tiltás.
 - Automatikusan odakerül mindegyik ACL végére.

ACL felépítése

- Az engedélyező utasítást nem tartalmazó ACL minden forgalmat tilt, mivel minden ACL végén szerepel az implicit tiltás.
- Az ACL tehát minden olyan forgalmat tilt, ami nincs konkrétan engedélyezve.

ACL felépítése

- A forgalmat sorban össze kell vetni az ACL-ben található utasításokkal míg egyezést nem találunk vagy el nem érjük az utasításlista végét (implicit tiltás).
 - Az implicit tiltás semmilyen forgalmat nem engedélyez.
 - Az implicit tiltás funkció megakadályozza a nemkívánatos forgalom véletlen áthaladását.

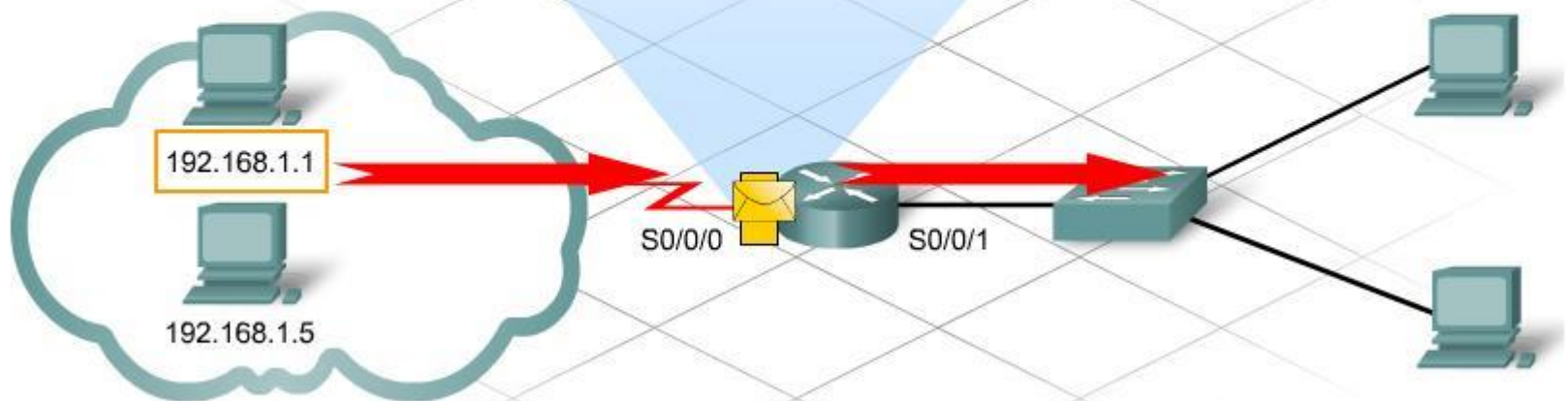
ACL elhelyezése

- A hozzáférési lista akkor lép működésbe ha elkészítése után hozzárendeljük a megfelelő interfészhez.
- Az ACL az interfészen vagy a bejövő vagy a kimenő forgalmat figyeli.
 - Az irányt mindig a forgalomirányító szemszögéből nézzük.


ACL működése

- Létezik-e az interfészhez rendelt ACL lista?
- Az ACL lista a bejövő vagy a kimenő forgalomra vonatkozik?
- A forgalomra teljesül-e valamely engedélyező vagy tiltó feltétel?
 - Az összes csomag címrészét össze kell hasonlítani az ACL-utasítások megfelelő címrészével.

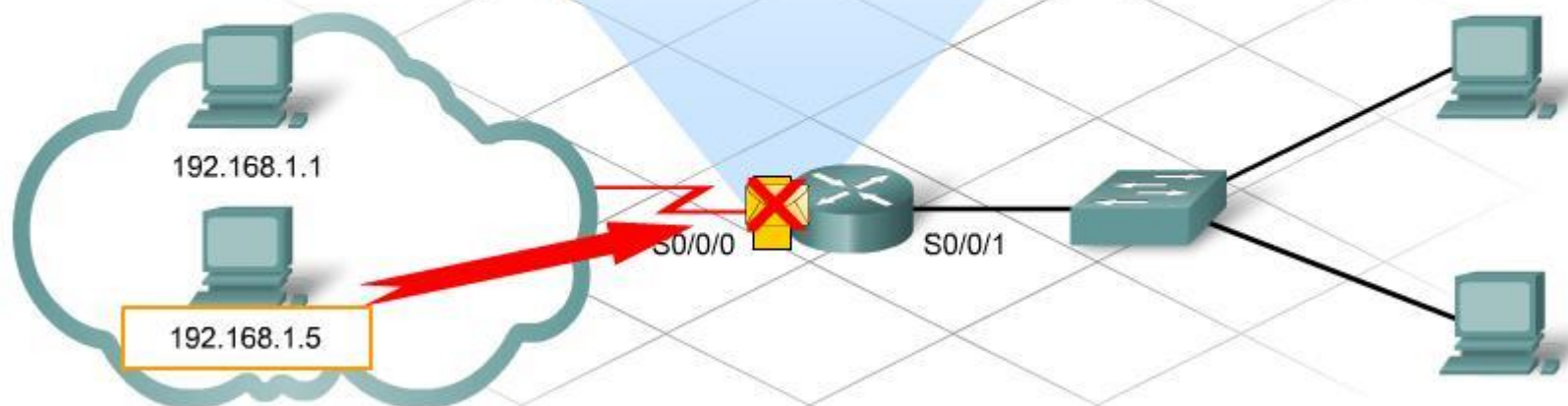
```
access-list 1 permit host 192.168.1.1  
access-list 1 deny any (implied)
```




Az ACL-ben lévő IP-cím egyezik a csomag forrás IP-címével.

 = hozzáférési lista

```
access-list 1 permit host 192.168.1.1  
access-list 1 deny any (implied)
```



Implicit elutasítás

 = hozzáférési lista

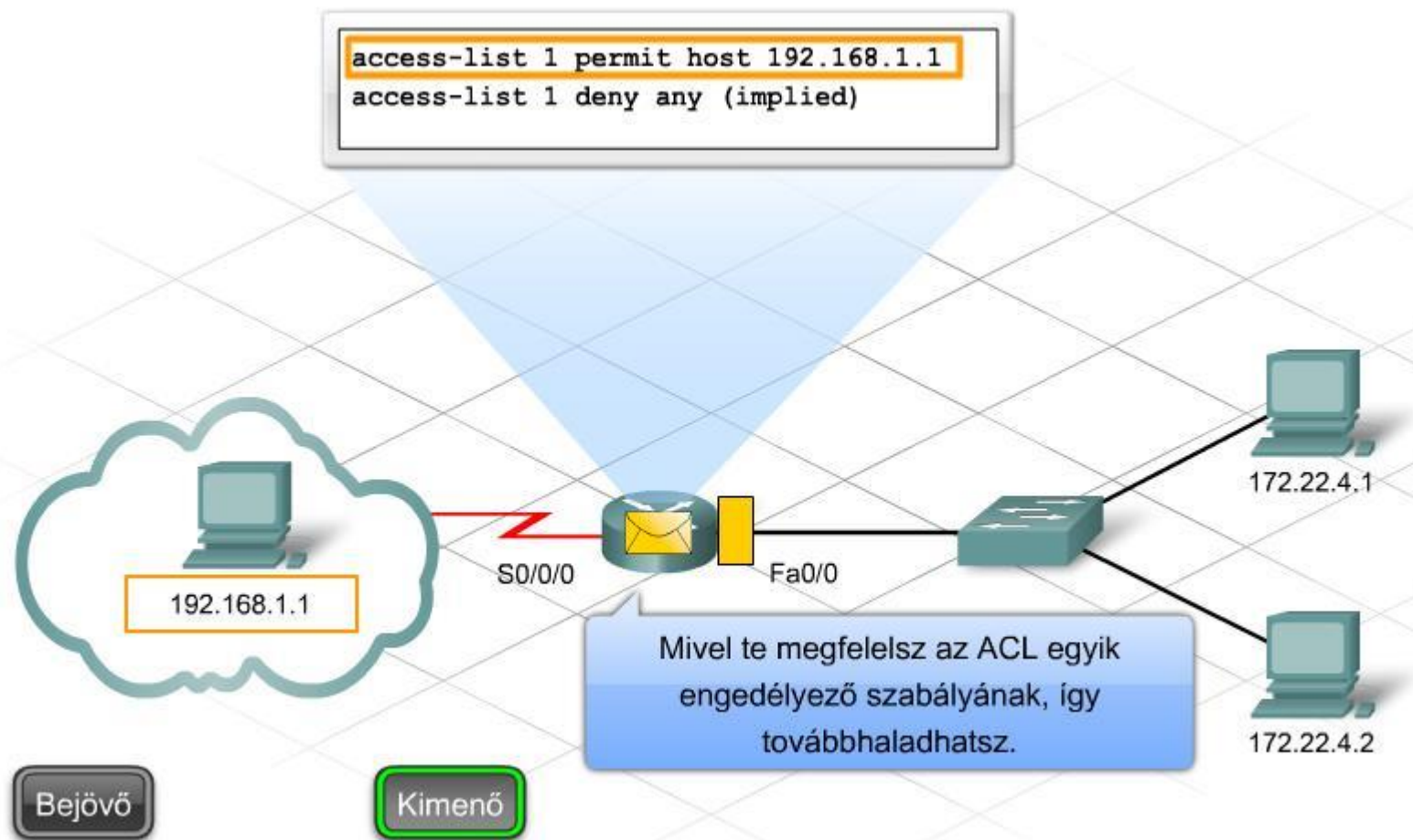
ACL-ek hatása

- A forgalomirányító interfészekhez protokollonként és irányonként egy-egy ACL adható meg.
- Az interfészhez hozzárendelt ACL-ek végrehajtása késlelteti a forgalmat.
- Akár egyetlen hosszú ACL is észrevehető hatással lehet a forgalomirányító teljesítményére.

Bemenő forgalom



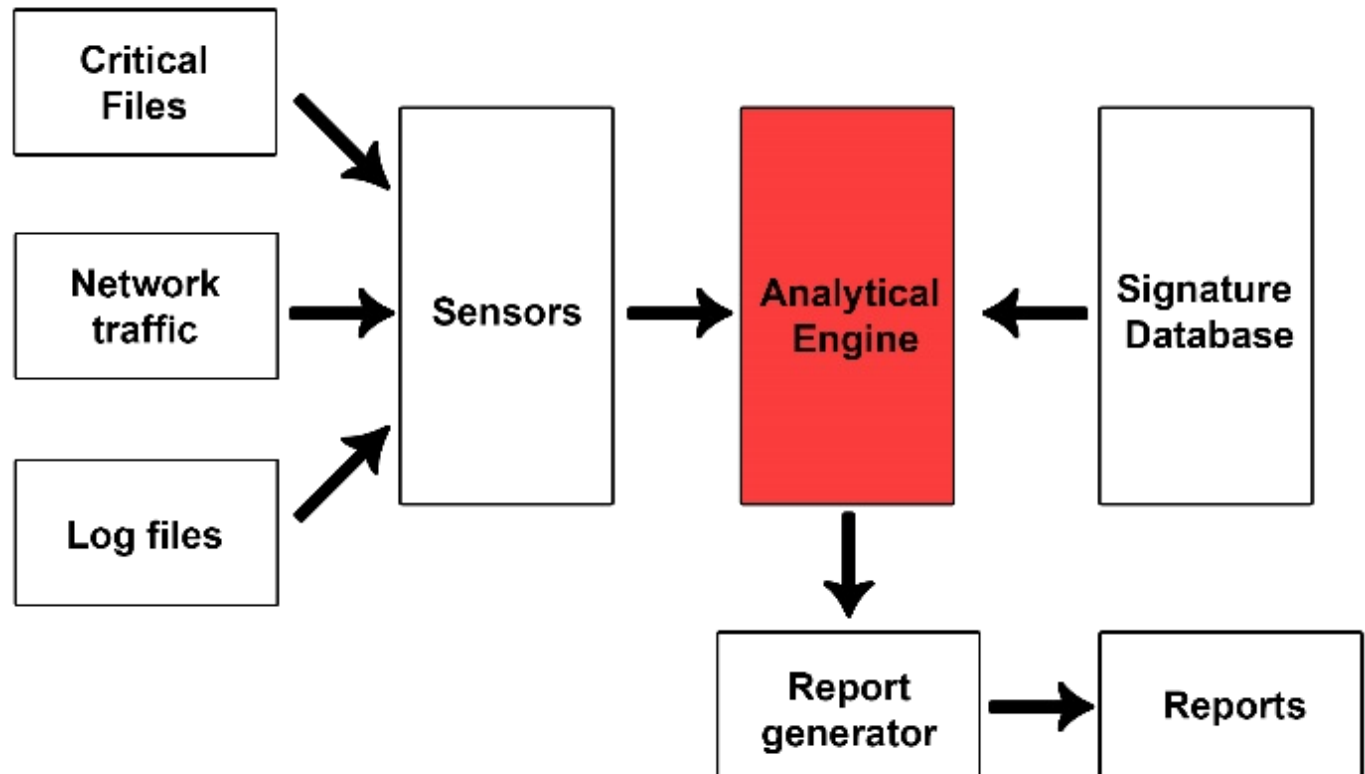
Kimenő forgalom



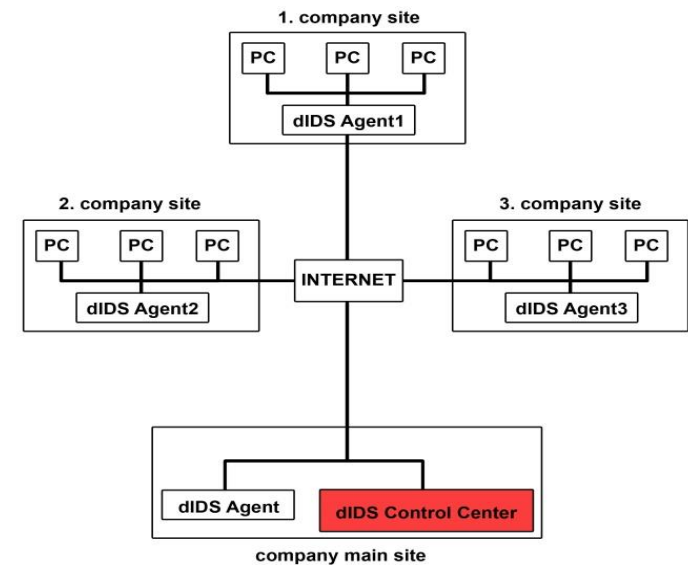
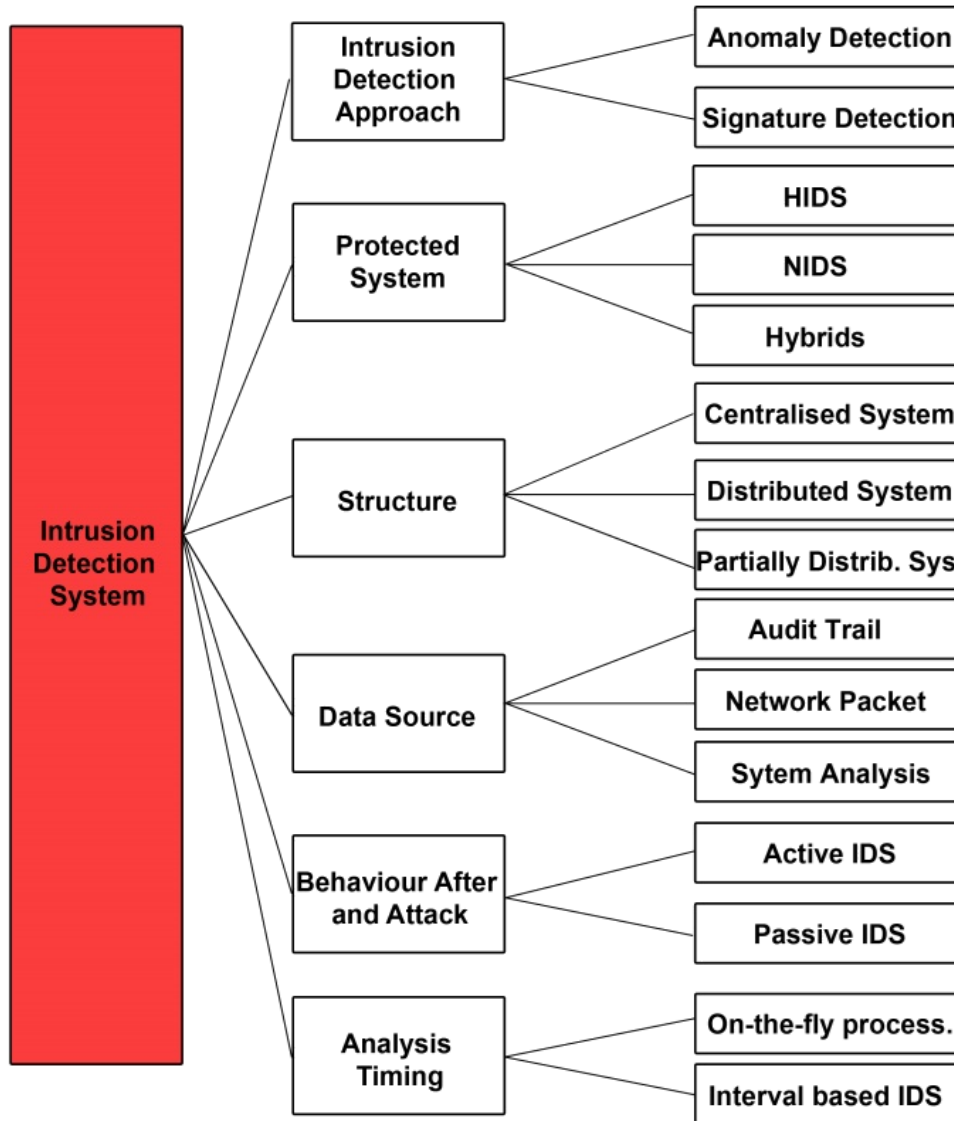
Behatolás érzékelő rendszerek

Intrusion Detection System (IDS)

IDS



http://gocslaszlo.hu/kutatas/G_J_Survey_on_Intrusion_TEAM_2015.pdf



Types of IDS systems

IDS

- **Aktív IDS**

A behatolás megelőző rendszerként (Intrusion Prevention System – IPS) ismert aktív IDS emberi beavatkozás igénye nélkül, automatikusan blokkolja a gyanúsak vélt rendszer-hozzáférési kísérleteket. Az IPS-t a hálózat határain kell elhelyeztetni, aminek következtében maga az IPS is érzékennyé válik a támadásokra. Még az is megtörténhet, hogy saját tevékenységét véli illetéktelen behatolásnak. Az IPS megfelelő konfiguráció hiányában könnyen tilthatja a rendszer használatára felhatalmazott felhasználókat és alkalmazásokat is. Az IPS típusú megoldás érzékenyebb egy memória túlterhelést irányzó támadásra (Denial of Service – DOS) mint egy passzív IDS. A DOS támadás különböző hálózati címekről indít kérelmeket a rendszer felé egészen addig, amíg a rendszer memória puffere túl nem terhelődik. Az IPS ugyan képes ennek kivédésére, viszont mellékhatásként letilthatja az adott portot, vagy akár a teljes hálózati forgalmat is.

- **Passzív IDS**

A passzív IDS nem képes automatikus válaszlépésekre, csak a háttérben működve vizsgál, és támadásgyanús esetben riasztja a rendszergazdát. Előnye, hogy mivel csak passzív megfigyelő a hálózatban, ezért nem válik támadás célpontjává, és az a veszély sem fenyegeti, hogy saját tevékenységét érzékelje támadásként. Hátránya, hogy mire a rendszergazda az megkapja értesítést, elemzi azt, majd döntést hoz a válaszlépésről, addigra nagy valószínűséggel a támadás már lezajlott.

IDS

- **Hálózati behatolást jelző rendszer (Network intrusion detection system - NIDS)**

Egy NIDS általában egy hálózati megfigyelő eszközt tartalmaz, ami mögött egy hálózati interfész kártya dolgozik. Ez az IDS típus a hálózat egy szegmensében vagy annak határa mentén helyezkedik el, és vizsgálja a hálózati forgalmat. Képes egy, vagy akár több rendszert és eszközt is megfigyelni a hálózaton belül, és védeni a hálózatot a támadások ellen.

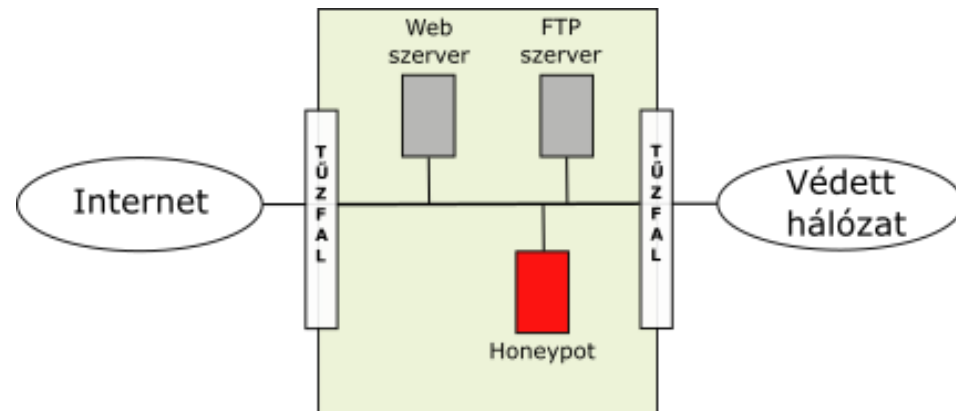
- **Host Intrusion Detection System – HIDS**

A HIDS egy önálló számítógép megfigyelésére szolgál. Telepíteni és konfigurálni kell az adott gépre. A HIDS-nek szüksége van kisebb, beleépített vizsgáló mechanizmusokra, amelyek az adott rendszer napló fájljaiból szerzik be a szükséges információt a behatolási kísérletek elleni fellépéshez. Képes a rendszert fenyegető hálózati és fizikai támadások jelzésére és kivédésére is egyaránt.

CSALIK A HÁLÓZATON

Honeypot

- Egy olyan információs rendszer (erőforrás), mely értéke az erőforrás engedély nélküli felhasználásában rejlik.
- Csaliként használunk olyan számítógépes rendszereket, hogy hackereket, kárt okozó embereket vagy szoftvereket tudjunk beazonosítani.
- Csak szimulálnak működő rendszereket
- Nincs normális funkciójuk, tehát minden tevékenység ami kapcsolatba van velük az támadási kísérlet.



Honeypot

- Csak a támadásokat naplózza – könnyű feldolgozás
- Támadások, betörések érzékelésére és nyomon követésére
- Kutatási célokra: új támadási módszerek, eszközök felderítésére, statisztikák készítésére
- Wormok és spamek elleni védekezésre

Honeypot – alacsony kölcsönhatású

- Az alacsony kölcsönhatású honeypot nem egy önálló gép (virtuális gép), hanem csak egy emulátor program, ami egy operációs rendszer szolgáltatásait utánozza.
- Előnyös tulajdonsága, hogy egyszerű telepítés és konfigurálás jellemzi. Az emulált szolgáltatással minimális a kockázat.
- Ezen megoldás nagy előnye, hogy a támadó nem szerzi meg az irányítást az operációs rendszer fölött, mivel az csak emulált.
- A támadó csak korlátozott mennyiségű információt szerez, főként tranzakciós adatokat, néhány kisebb kölcsönhatást gyűjt.
- Ezeket leginkább a vállalati rendszerekben, termelési iparágakban használják.

Honeypot – magas kölcsönhatású

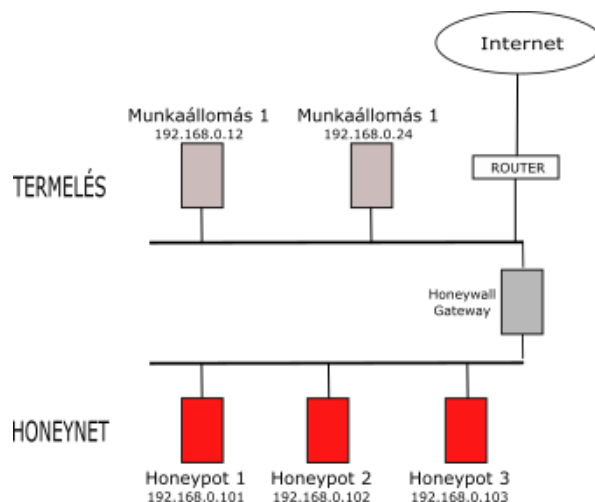
- A magas kölcsönhatású honeypotok nem emulált, hanem valós operációs rendszert és szolgáltatásokat futtatnak.
- Az ilyen típusú honeypotok mögé tűzfalat kell helyezni a kockázatok csökkentése érdekében.
- Telepítésük és karbantartásuk nehézkes, de hatalmas mennyiségű információt tudnak nyújtani a hackerek viselkedéseiről, motivációiról.
- Ezeket leginkább kutatásokhoz használják.

Honeynet

A honeynet több számítógépből álló hálózat, ami a honeypotokéval megegyező funkciókkal rendelkezik.

Ha egy hálózaton konfigurálunk egy honeypotot, amelyen csaliként több ismert szolgáltatást futtatunk vagy emulálunk egyszerre, a támadó számára gyanús lehet, hogy egy sebezhető szervert több módon is meg tud támadni.

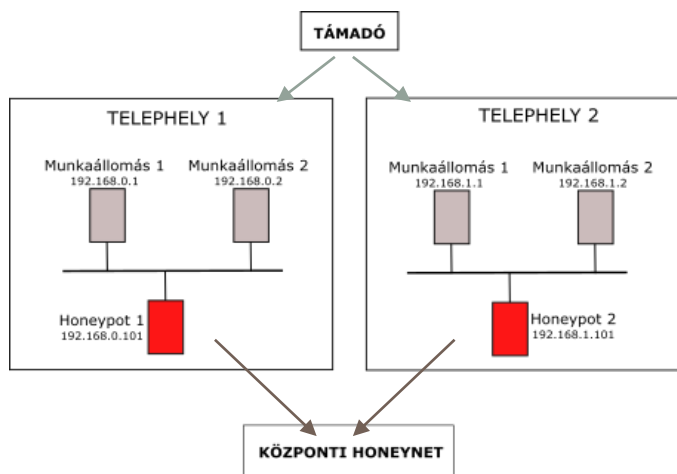
Ennek elkerülése érdekében érdemes egy hálózaton több honeypotot tartalmazó honeynet-et kialakítani, ahol a különböző szolgáltatások más és más honeypoton futnak.



Honeyfarm

Azon vállalatoknál, melyek telephelyei földrajzilag távol esnek egymástól, problémát okozhat, hogy ezen az egyes telephelyeken telepített honeynet-ek túl sok erőforrást igényelnek, és az üzemeltetéshez is külön adminisztratív személyzet szükséges.

Ebben az esetben egy honeyfarm megvalósítása jelenti a megoldást. Működésének lényege, hogy egy központi helyre kell telepíteni egy csali hálózatot (honeynet), a telephelyekre pedig egy-egy honeypot-t, melyeknek az a szerepe, hogy a gyanús tevékenységeket azonnal átirányítja az adatokat a központi honeynet-re.



Honeynet Project

<https://www.honeynet.org/>

