



# A hálózati határvédelem eszközei

Kovács Bálint

# Miről lesz szó?

---

- A hálózati határvédelem értelmezése
- Hálózati alapfogalmak
- Tűzfal típusok
- Határvédelmi technológiák
- Speciális határvédelmi megoldások
- Kérdések és válaszok

# Mi a biztonság?

- Kedvező állapot
  - Nincsenek fenyegetések
  - Nem is valószínű, de nem zárható ki
- Maradék kockázat
  - Mindig van
  - Nem mindegy, hogy ismert-e
- Folyamat és nem termék
- Biztonság menedzsment: az állapot fenntartás folyamata

# Az IT biztonság elemei

- Az IT biztonsági elemei:
  - **Érték:** Bármilyen, ami a szervezet számára jelentőséggel bír (adatok, tudás, védjegy, receptek, eljárások, know-how stb).
  - **Fenyegetés:** Olyan negatív esemény, amelynek esetleges bekövetkezése veszteséget okozna.
  - **Sérülékenység:** A fenyegetettség bekövetkezését lehetővé tevő hiba.
  - **Ellenintézkedések:** Minden olyan eszköz, tevékenység, amely az fenyegetések minimalizálását szolgálja.
  - **Kompromisszumok:** Minden intézkedés, védelmi eszköz hordoz magával valamilyen hátrányt.
  - **Maradék kockázat:** nincs tökéletes (100%-os) védelem!

# Az információ tulajdonságai

- **Bizalmasság:** az információ megtekintésének korlátozása
- **Sértetlenség:** az objektum védelme nem kívánt módosítás ellen
- **Hitelesség:** az információ forrásának hiteles megjelölése
- **Rendelkezésre állás:** az információ elérhetősége a kívánt időben
- **Letagadhatatlanság:** az információ forrásának hiteles megőrzése a jövőben

# Ellenintézkedések típusai

- Ellenintézkedések típusai (Control intézkedések):
  - **Preventív**: megelőző intézkedések
  - **Detektív**: érzékelő intézkedések (megfigyelés)
  - **Korrektív**: korrigáló intézkedések

# IT biztonsági eszközök

---

- **Adminisztratív**, pl. belső szabályzás;
- **Fizikai**, pl. záruk, beléptető rendszerek, kamerák;
- **Logikai**, pl. szoftveres és hardveres megvalósítások;

# Mit értünk hálózati határvédelem alatt?

- Bejövő és kimenő hálózati forgalom monitorozása és szabályozása előre meghatározott biztonsági szabályok alapján
- Tipikusan különböző biztonsági szintű hálózatok közötti elválasztást valósít meg (pl a biztonságosnak tekintett belső hálózat és az internet)
- Logikai kontroll
- Preventív és detektív kontroll
- Olyan ellenintézkedés, ami az érték elérhetőségének fenntartása mellett a fenyegetések és sérülékenységek számát minimalizálja



# Mit értünk hálózati határvédelem alatt?

- Azon fizikai és logikai eszközök összessége, melyek az IT Biztonsági Szabályzat („IBSZ”) hálózati határvédelemre vonatkozó követelményeit megvalósítják.
  - Az az eszköz, ami két fizikai hálózat között csak az (IBSZ-ben) engedélyezett szabályok szerinti adatáramlást (CC: FDP\_IFC és IFF) kényszeríti ki.

# Az IT biztonság tervezésének lépései

- A tervezés során felmerülő kérdések (Beyond Fear, Bruce Schneier):
  - Milyen értéket védünk?
  - Milyen kockázati tényezők vannak jelen?
  - A megoldás mennyire hatékonyan csökkenti a kockázatot?
  - Milyen új kockázatot jelent a megoldás?
  - Milyen költségeket és kompromisszumokat jelent a megoldás bevezetése?

# A hálózati határvédelem eszközei

- Szabályzatok, eljárásrendek (IBSZ)
- Házirend (policy) karbantartás és a hozzájuk tartozó folyamatok
- Autentikációs adatbázis karbantartása
- Hibajavítás (security patch, nem új verzió telepítés!)
- Monitorozás
- Naplógyűjtés és elemzés (on-line és periodikus)

# Kontrollok a hálózati határvédelemben

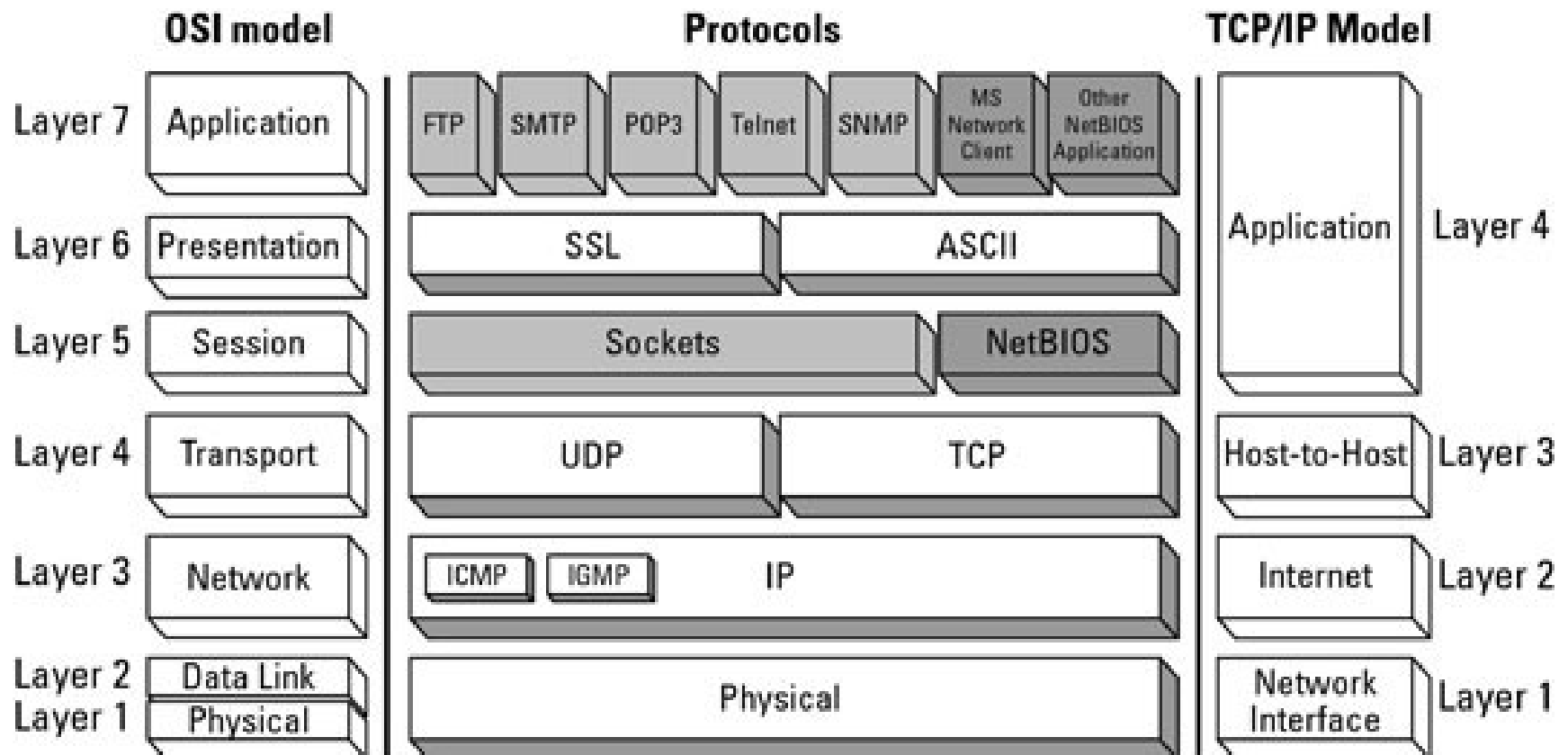
	Bizalmasság (C)	Sértetlenség (I)	Rendelkezésre állás (A)	Hitelesség	Letagadhatatlanság
<b>Preventív (Pre)</b>	<ul style="list-style-type: none"><li>•Hozzáférés korlátozása</li><li>•Rejtjelezés</li><li>•Fizikai szeparáció</li><li>•User autentikáció</li></ul>	<ul style="list-style-type: none"><li>•Rejtjelezés</li><li>•MITM védelem</li><li>•Protokoll elemzés</li><li>•IPS</li><li>•Vírus szűrés protokollban</li></ul>	<ul style="list-style-type: none"><li>•HA</li><li>•fail-over kapcsolódás</li></ul>	<ul style="list-style-type: none"><li>•Korrekt tanúsítvány ellenőrzés</li><li>•Subject naplózás</li><li>•Issuer naplózás</li></ul>	<ul style="list-style-type: none"><li>•Subject naplózás</li><li>•Issuer naplózás</li><li>•URL naplózás</li><li>•Accounting</li></ul>
<b>Detektív (De)</b>	<ul style="list-style-type: none"><li>•Napló feldolgozás</li><li>•ACL ellenőrzés</li></ul>	<ul style="list-style-type: none"><li>•Napló feldolgozás</li><li>•IPS/IDS</li></ul>	<ul style="list-style-type: none"><li>•Host monitorozás</li><li>•FailOver riasztás</li></ul>	<ul style="list-style-type: none"><li>•Napló feldolgozás</li></ul>	<ul style="list-style-type: none"><li>•Napló feldolgozás</li></ul>
<b>Korrektív (Co)</b>	<ul style="list-style-type: none"><li>•Szabály audit</li><li>•Szabály módosítás</li></ul>	<ul style="list-style-type: none"><li>•CRL frissítés</li></ul>	<ul style="list-style-type: none"><li>•Node bővítés</li></ul>	<ul style="list-style-type: none"><li>•CA adatbázis karbantartás</li><li>•CRL lista frissítés</li></ul>	<ul style="list-style-type: none"><li>•Szabály audit</li><li>•Szabály módosítás</li></ul>

# Hálózati alapfogalmak

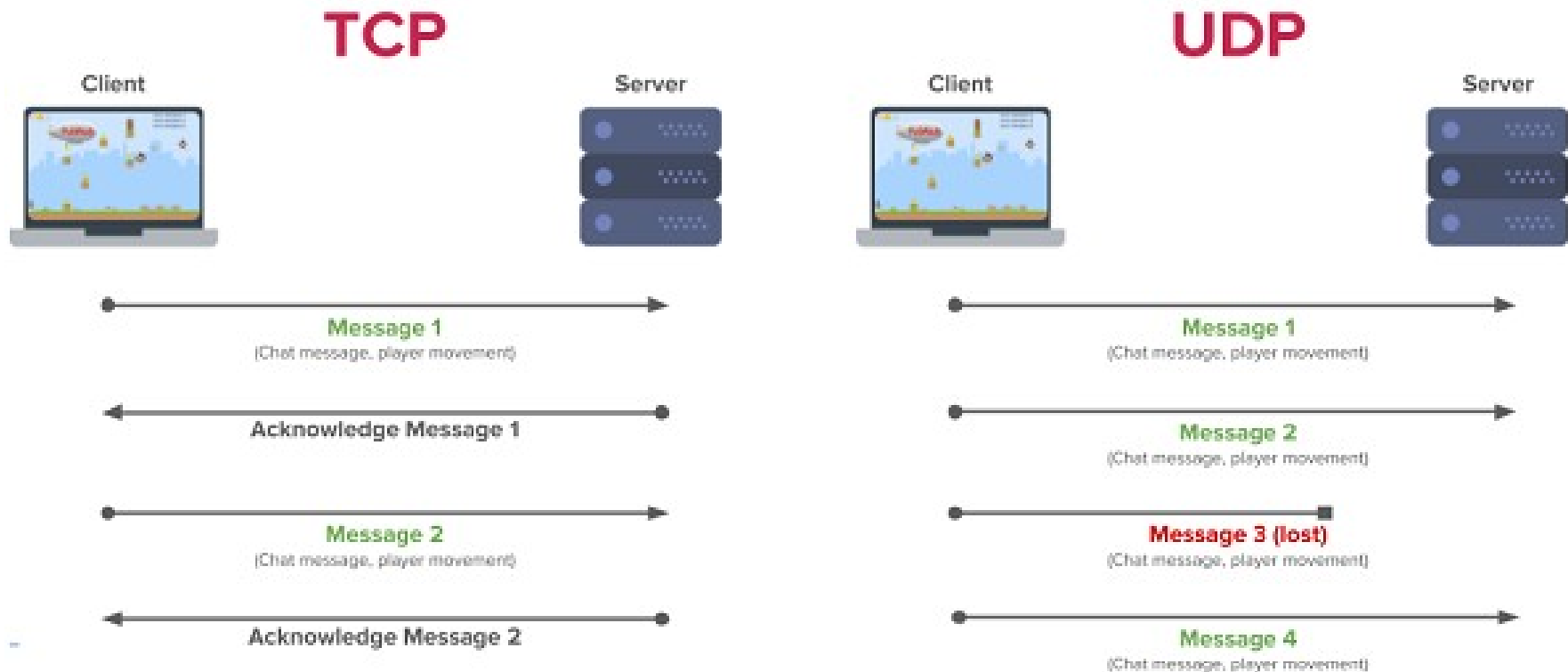
---

- ISO/OSI modell
- TCP vs UDP
- Hogy néz ki egy kommunikáció

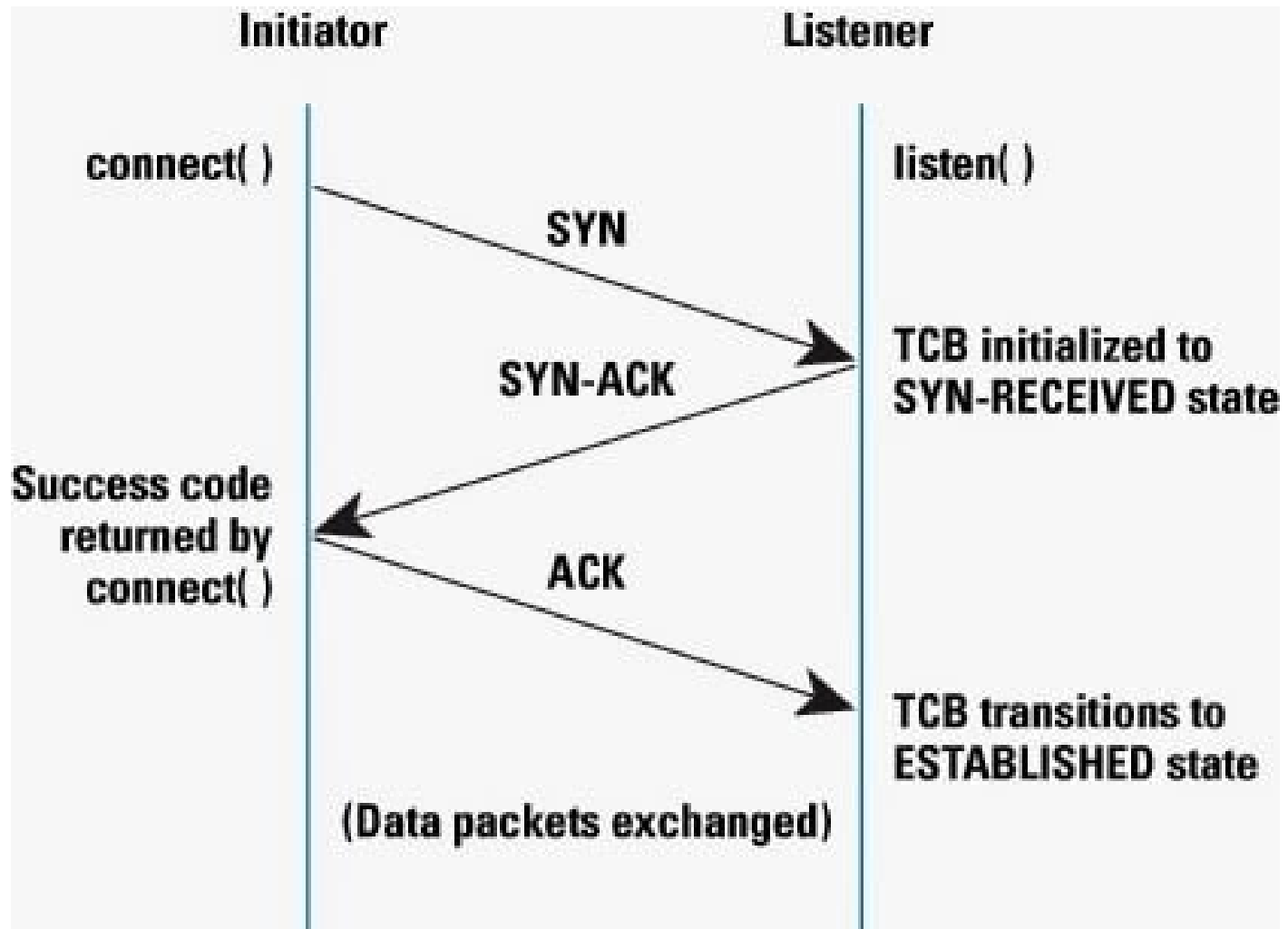
# ISO/OSI layer-ek és protokollok



# TCP vs UDP

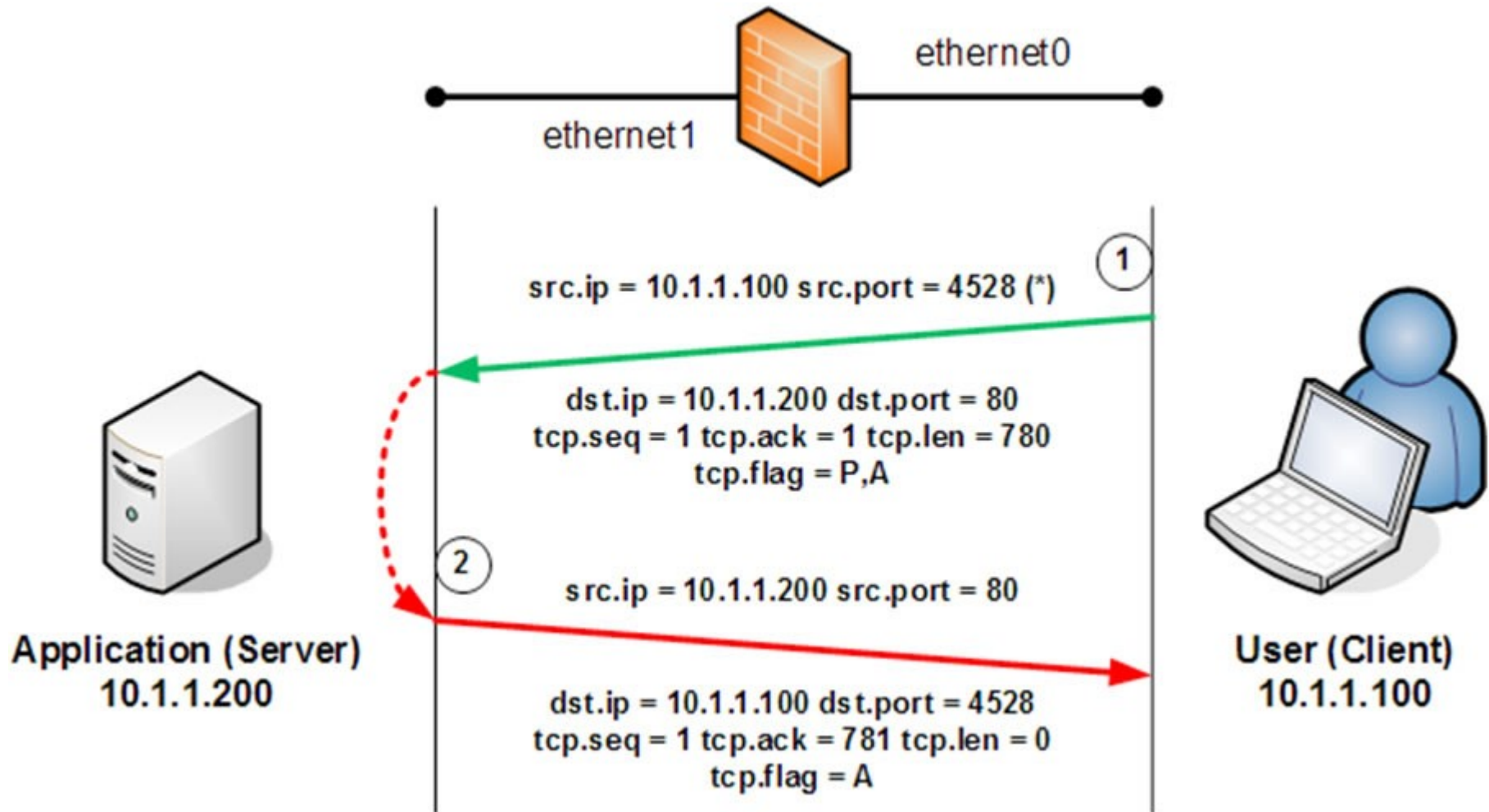


# TCP 3-way handshake





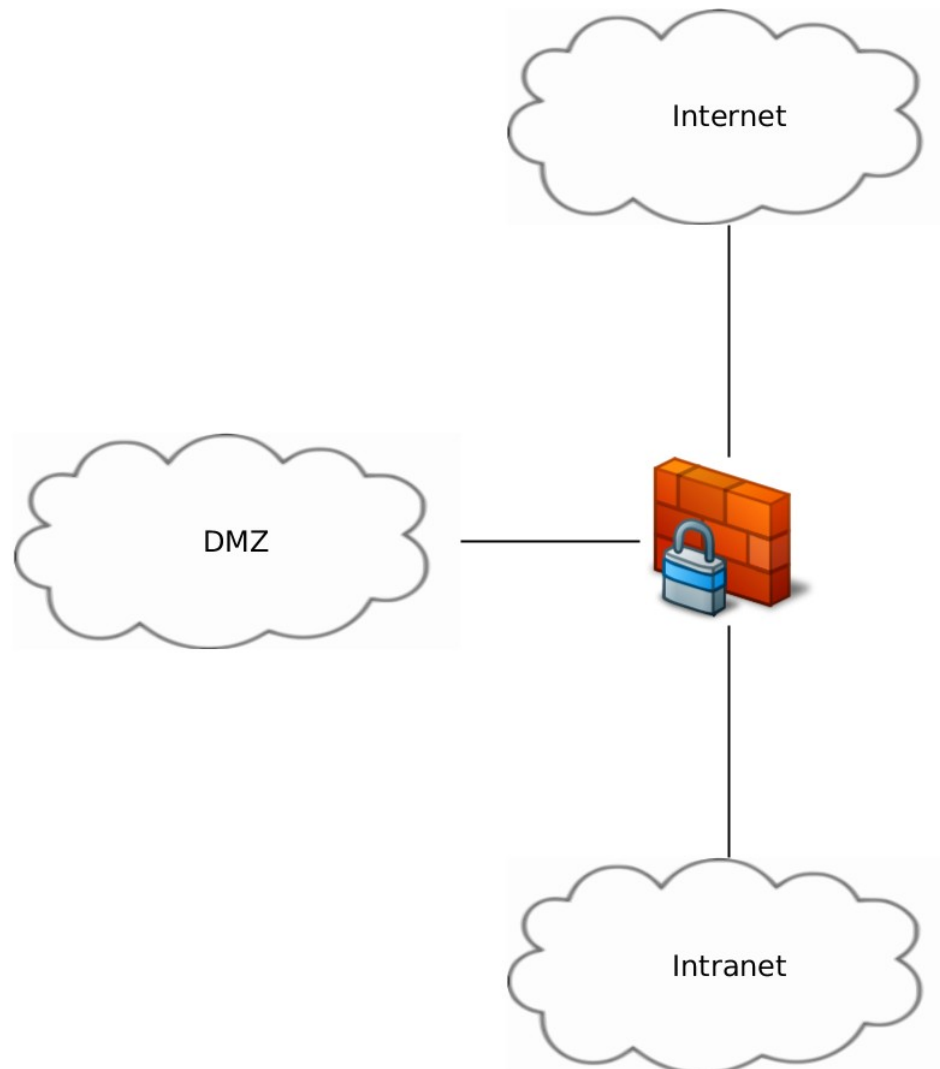
# Packet flow routing megtartással



- Routing megtartása:
  - Packet Filter
  - Stateful Packet Filter
  - Transzparens proxy
  - Moduláris, transzparens proxy
- Routing nélkül:
  - Bastion host
  - Proxy
  - SOCKS

- **Működési elv:** A bejövő csomagokat tulajdonságaik alapján elfogad (továbbít, routingot végez), elvet vagy eldob illetve naplóz
- **Döntés alapja:** A csomagok forrása és célja (port és IP), bizonyos flag-ek. Ezért a szabályok csak a csomagokra vonatkoznak (Packet Filter).
  - Működési réteg: IP és transzport
- **Megvalósítás:** Minta illesztés

# Routing tartó tűzfalak



# A házirend tárolása

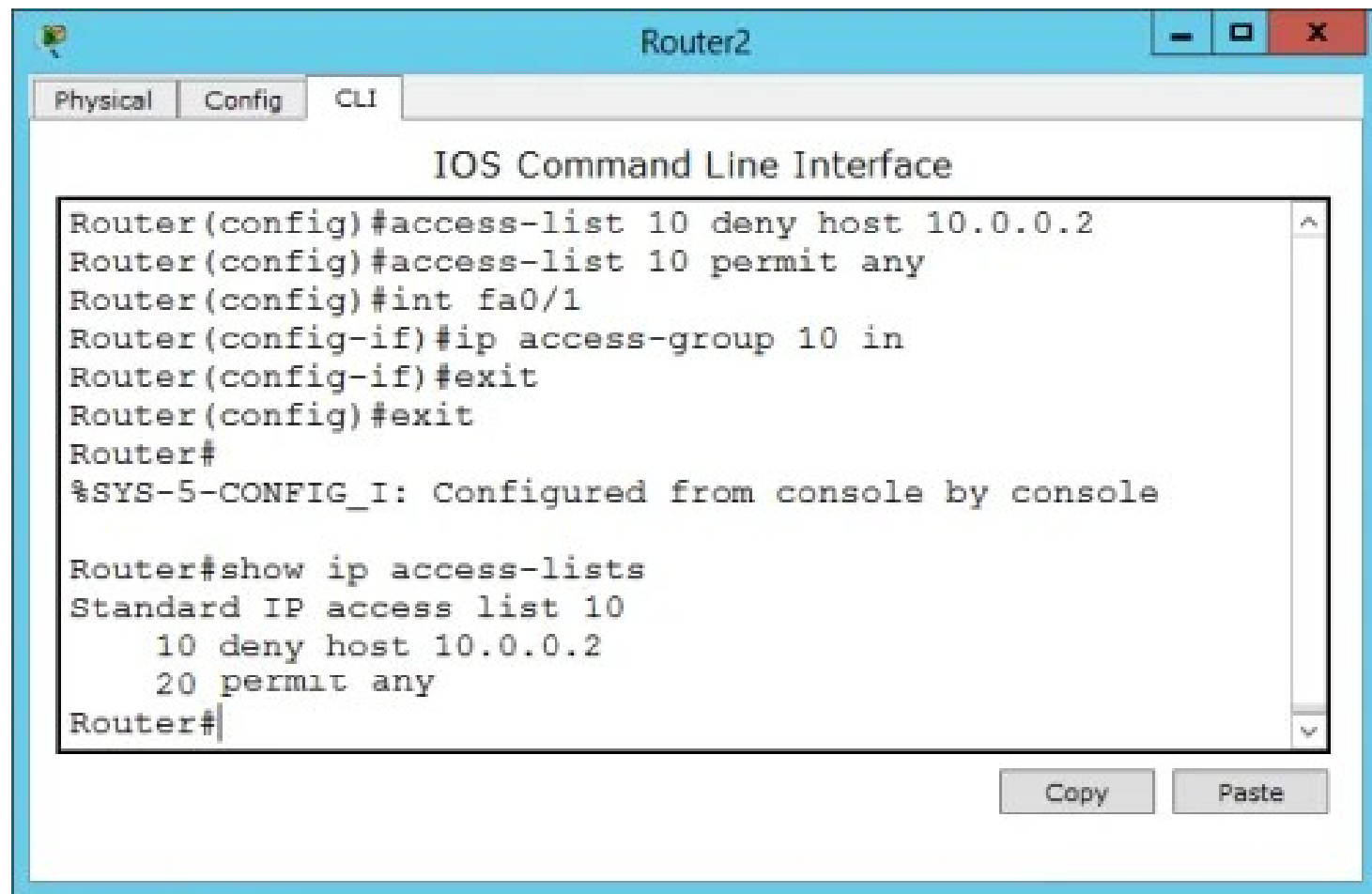
- A házirend (policy vagy szabályrendszer) tárolására szolgáló leggyakoribb eszköz, a hozzáférési lista (ACL - Acces Control List):
  - A minta (pattern) feladata a cél (döntés) kiválasztása;
  - A szabály feladata az illeszkedő (packet) sorsának eldöntése (policy verdict):
    - Engedélyezés vagy tiltás;
    - Ugrás másik szabályra;
    - Naplózás és ugrás másik szabályra;
  - Az ACL-ek feldolgozása általában az első illeszkedésig tart, ezért a számít sorrend (specifikus szabályok előre, átfogók a lista végére).

# A házirend tárolása

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

# A házirend tárolása



The screenshot shows a Cisco Packet Tracer window titled "Router2". It has three tabs: "Physical", "Config", and "CLI". The "CLI" tab is active, displaying the "IOS Command Line Interface". The command history is as follows:

```
Router(config)#access-list 10 deny host 10.0.0.2
Router(config)#access-list 10 permit any
Router(config)#int fa0/1
Router(config-if)#ip access-group 10 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip access-lists
Standard IP access list 10
  10 deny host 10.0.0.2
  20 permit any
Router#
```

At the bottom right of the CLI window, there are "Copy" and "Paste" buttons.

# Csomagszűrő routerek értékelése

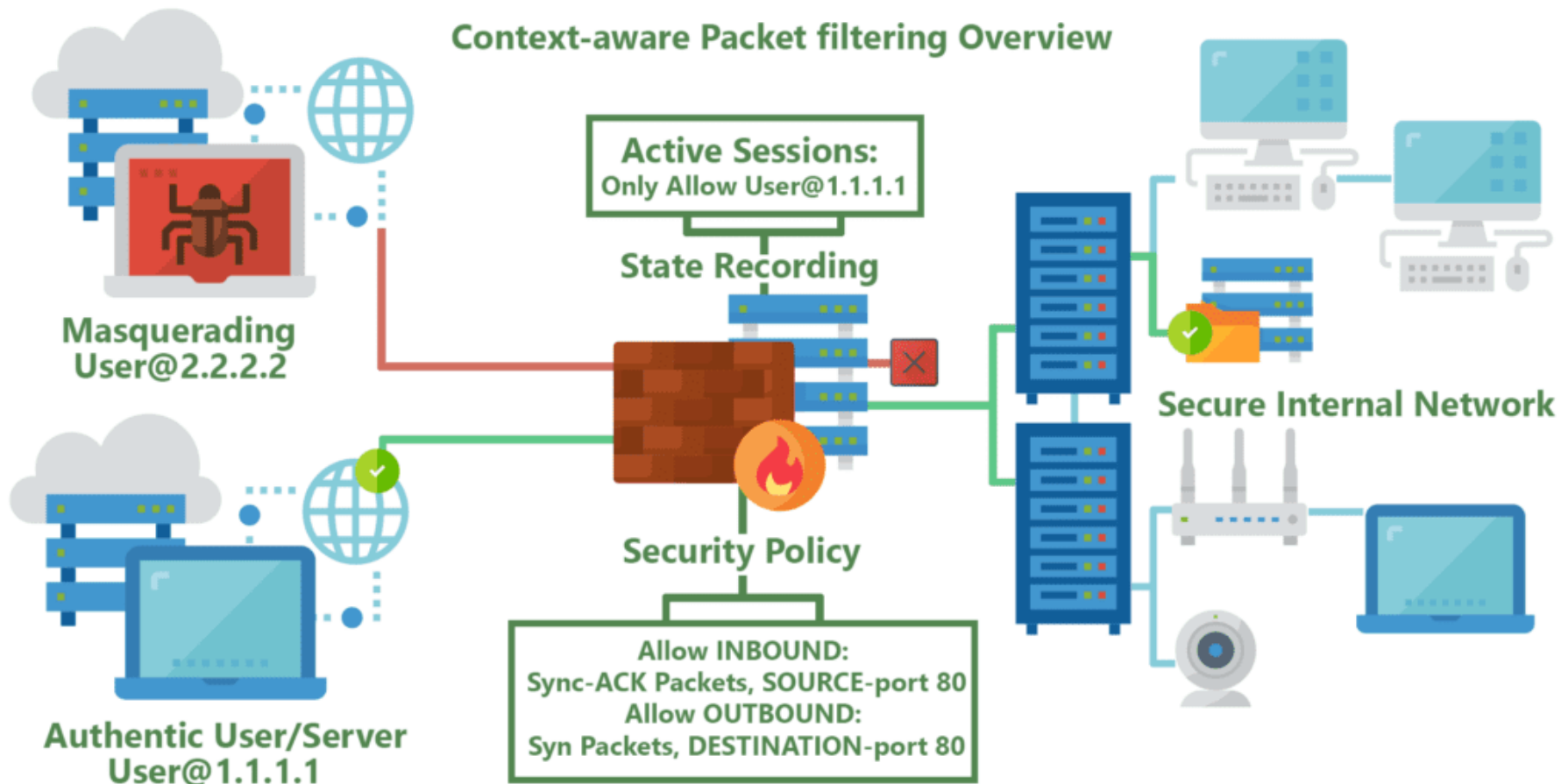
- **Előnyök:**
  - gyors
  - egyszerűen kezelhető szabályrendszer
- **Hátrányok:**
  - az alkalmazás szintre nem lát
  - többcsatornás protokollok kezelése nem megvalósítható
  - sok szabály szükséges (válasz packetek kezelése)
- **Ismeretlen elemek kezelése:**
  - Az ismeretlen elemeket szűrés nélkül engedik át.



# Állapot tartó csomagszűrők

- **Működési elv:** A bejövő csomagokat tulajdonságaik alapján elfogad, továbbít vagy eldob.
- **Döntés alapja:** A teljes TCP és IP rétegek, (forrás, cél port és IP, seq és ack, csomagok sorrend illetve helye) tehát a kapcsolatok (Ezért állapot tartó – Stateful Packet Filter - SPF).
- **Megvalósítás:** Mintaillesztés és elemzés
- **Többcsatornás protokollok kezelése:** Valamilyen modul segítségével felismeri az alkalmazás szintből, hogy hová kell nyitni a további kapcsolatot, majd azt RELATED-nek jelöli.

# Állapot tartó csomagszűrők

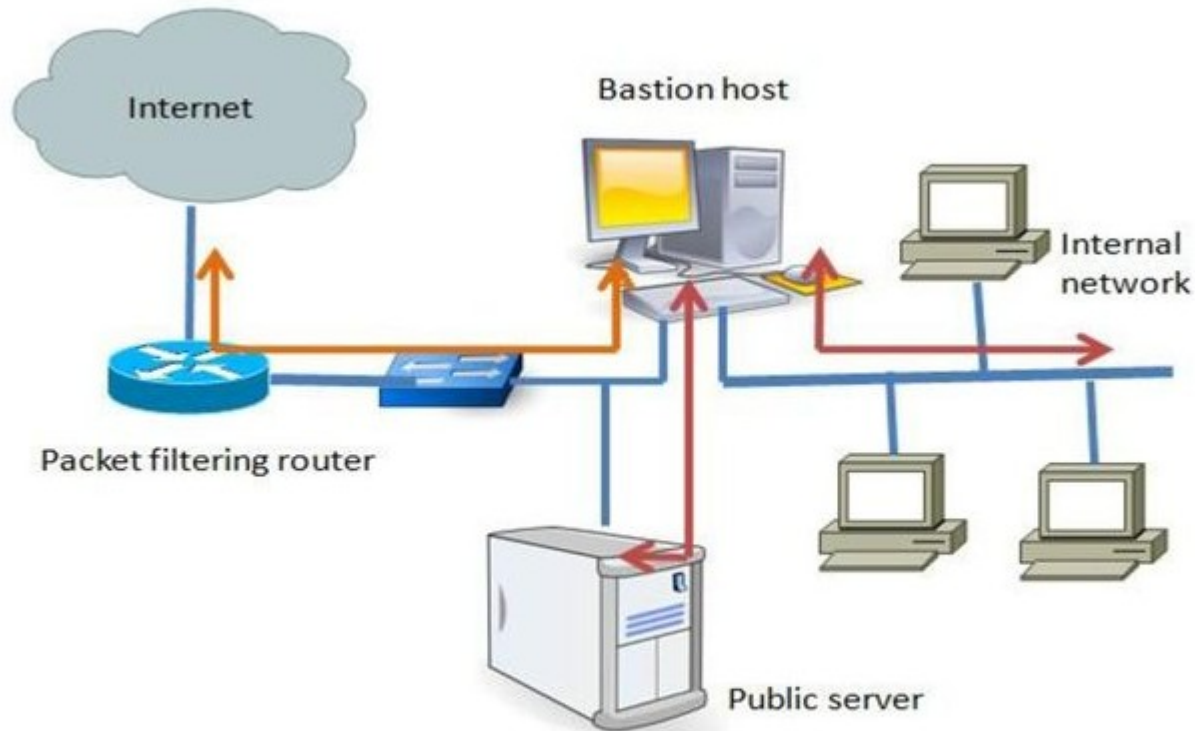


# Állapot tartó értékelése

- **Előnyök:**
  - gyors
  - kevesebb szabály (nem kell kezelni a válaszokat)
- **Hátrányok:**
  - alkalmazás szintre nem lát
  - többcsatornás protokollok kezelése nehezen megvalósítható
- **Ismeretlen elemek kezelése:**
  - Az ismeretlen elemeket szűrés nélkül engedik át.

- **Működési elv:** A több hálózathoz csatlakozó (dual home vagy multi home) hoszton a bejelentkezett felhasználók szolgáltatásokat vehetnek igénybe (kombinálható csomagszűréssel).
- **Döntés alapja:** A felhasználók autentikációján alapszik.

# Bastion hostok



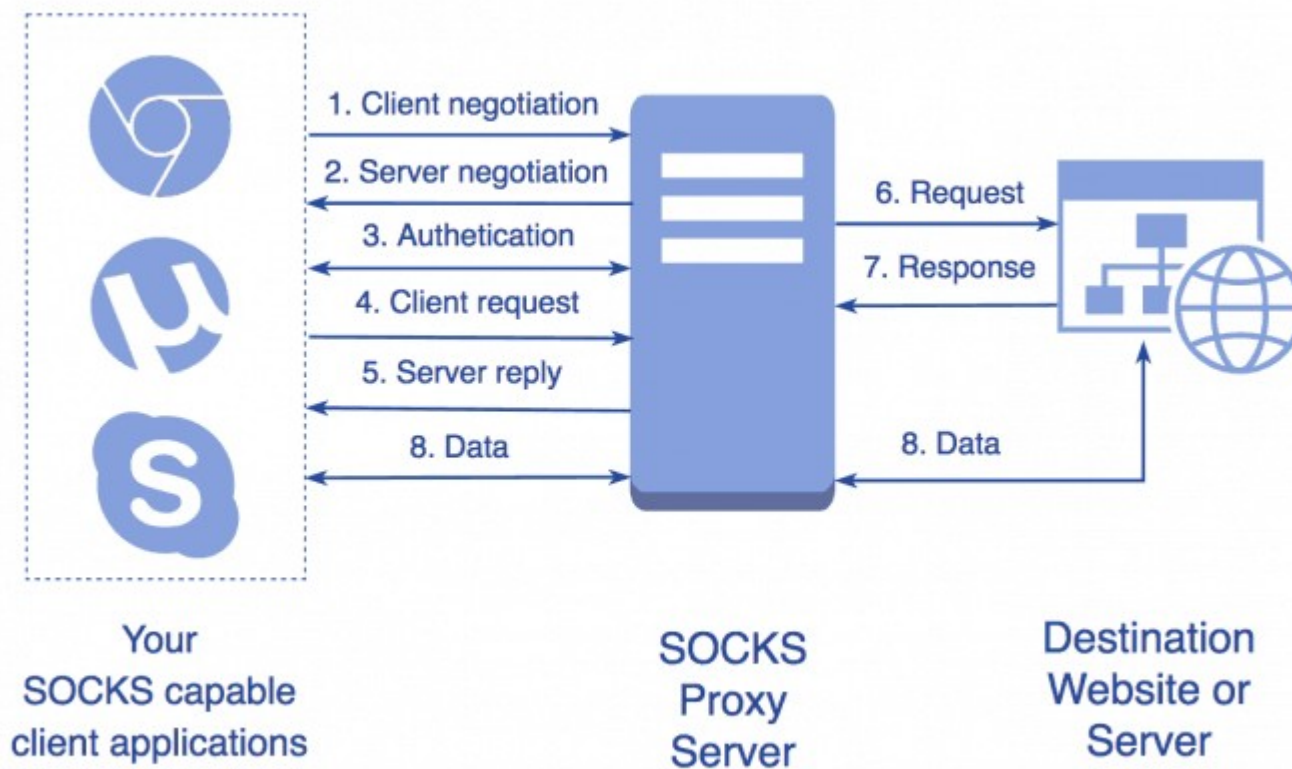
Screened host firewall ( Dual-homed bastion host)

# Bastion hostok értékelése

- **Előnyök:**
  - Felhasználói autentikáció általában van
  - A kliens alkalmazás ellenőrizhető, kézben tartható
- **Hátrányok:**
  - Elavult, de felhasználói szolgáltatásokra újra népszerű
  - nehezen karbantartható (pl. eltérő verziók felhasználónként)
  - erőforrás igényes
  - a felhasználó potenciális veszélyforrást jelent
  - az alkalmazások sérülékenységei ellen nem nyújt védelmet
- **Ismeretlen elemek kezelése:**
  - Nem értelmezhető

- **Működési elv:** Egy speciális, a kliensre telepített alkalmazás elveszi a kapcsolatot az operációs rendszertől és a tűzfalnak adja át.
  - Kicseréli az API hívásokat (beépül az alkalmazás és a TCP réteg közé, fixen a SOCKS szerverhez kapcsolódik) bár létezik olyan alkalmazás ami natívan beszéli a protokollt.
  - Csak kliens védelemre alkalmas (a SOCKS proxy szerver oldalán csak 1 kapcsolat lehet, tehát nem tud sok klienst kiszolgálni).
- **Döntés alapja:** A csomagok forrása és célja (port és IP) illetve megvalósítás függően az alkalmazási réteget is elemezheti.

# SOCKS tűzfalak





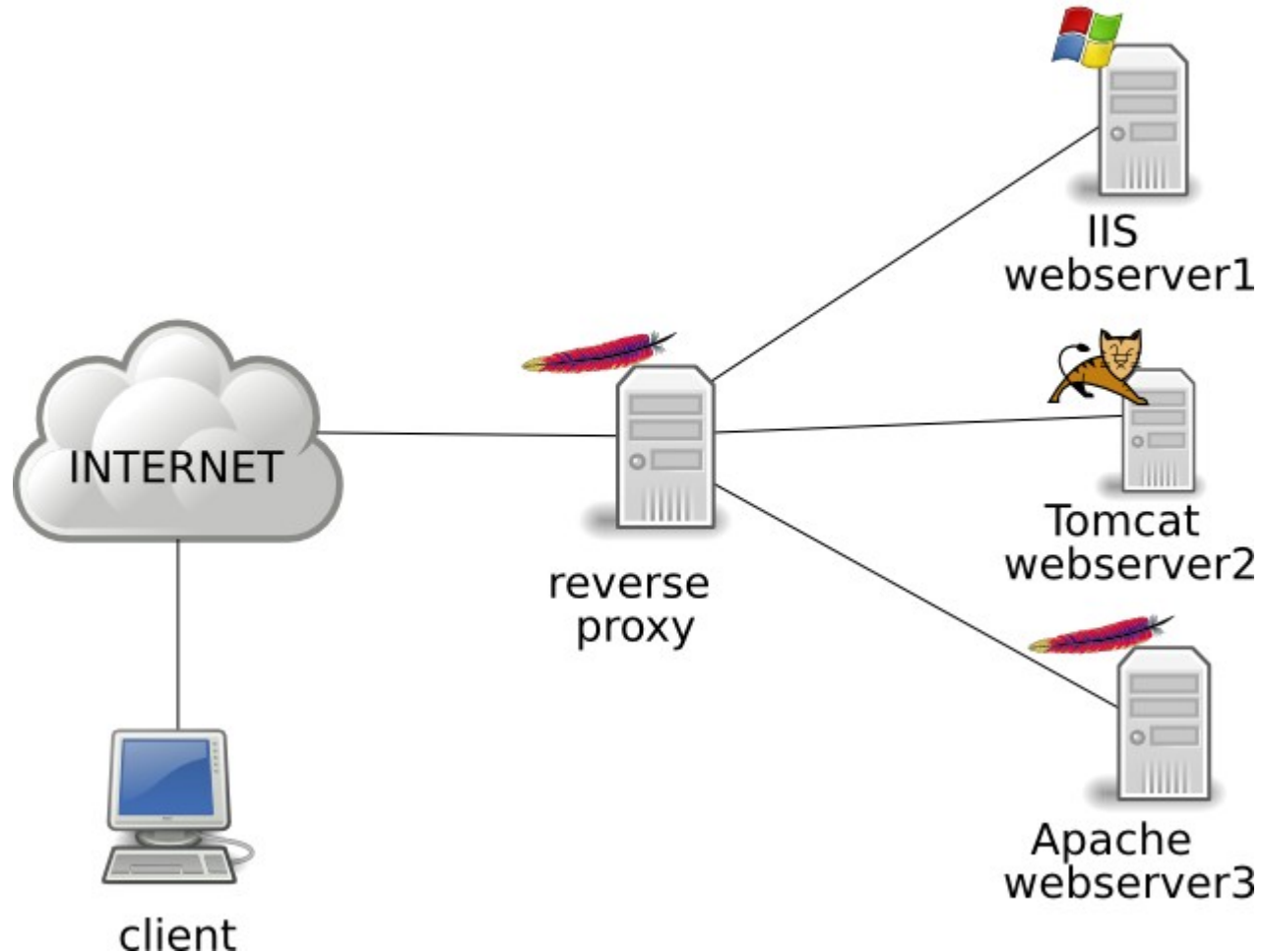
# SOCKS tűzfalak értékelése

- **Előnyök:**
  - SOCKSv5-től felhasználói autentikáció megvalósítható (pl. Kerberos SSO)
- **Hátrányok:**
  - A kliens alkalmazások általában nem támogatják a SOCKS protokollt.
  - Az OS-re telepíteni kell a SOCKS klienst (API csere).
  - Szerver nem védhető.
- **Ismeretlen elemek kezelése:**
  - Megvalósítás függő, alapvetően nincs alkalmazás szintű védelem.

# Alkalmazásszintű tűzfalak

- **Működési elv:** A kliens a tűzfalon futó alkalmazással (**proxy**) tart kapcsolatot, az alkalmazás pedig a szerverrel. Fontos hogy ezek a proxyk gyorsítótár (cache) funkcióval nem rendelkeznek.
- **Döntés alapja:** Az alkalmazási réteg protokollja.
- **Megvalósítás:** Összetett. Mintaillesztés a hálózati rétegekben valamint mintaillesztés és **értelmezés** az alkalmazási rétegben. Az értelmezés mélysége függ a megvalósítástól.

## Apache Reverse Proxy.



# Proxy tűzfalak értékelése

- **Előny:**
  - Alkalmazás szintű védelem
  - Protokoll értelmezés, kifinomultabb szűrés
  - Többcsatornás protokollok elemzése lehetővé válik
- **Hátrány:**
  - Proxy használatára felkészített kliens szükséges illetve azt támogató protokoll
  - Lassabb, bonyolultabb a konfigurálás
- **Ismeretlen elemek kezelése:**
  - Megvalósítás függő, az ismeretlen elemek eldobása lehetséges

- **Transzparens működés:** A kliens és a szerver azt hiszi, hogy közvetlenül egymással kommunikálnak.
- **Nem transzparens működés:** A kliens a tűzfallal kommunikál (eltérő protokoll használat lehetséges!).
- **A transzparencia értelmezhető:**
  - Hálózati szinten (TCP/IP)
  - Alkalmazási szinten
  - Kliens vagy szerver oldalon
    - Lehet szimmetrikus vagy asszimmetrikus
- A hálózati és alkalmazásszintű transzparencia lazán kötődik

# Hálózati szintű transzparencia

---

- **Kliens oldali:**

- A kliensek a valódi célszerver IP-jét címzik
- A kliensek a tűzfal IP-jét címzik

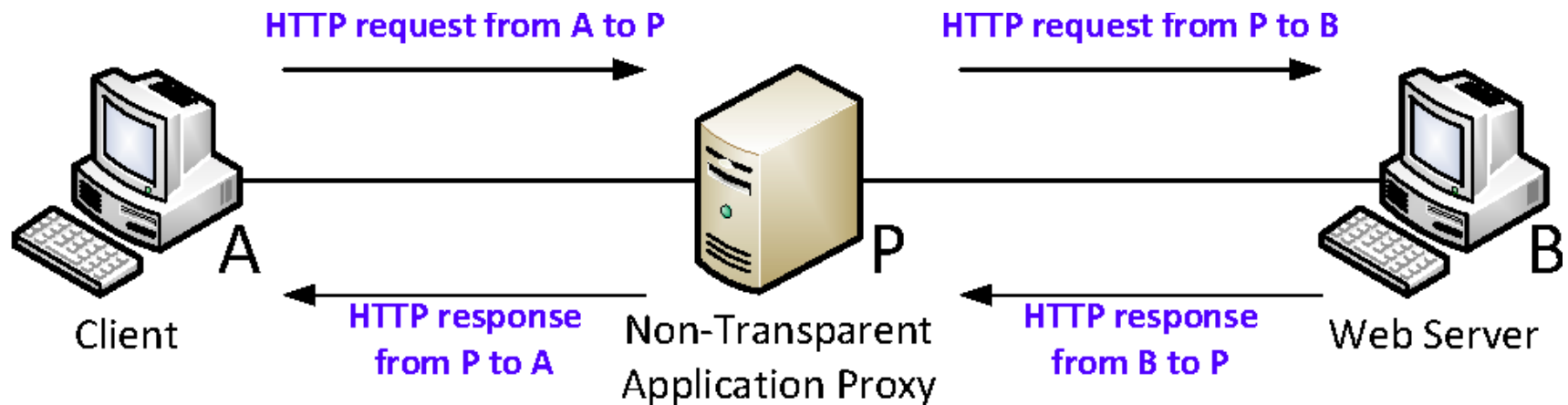
- **Szerver oldali:**

- A szerverek a valódi kliens IP-jéről vagy a tűzfal IP címéről látják a kapcsolatot

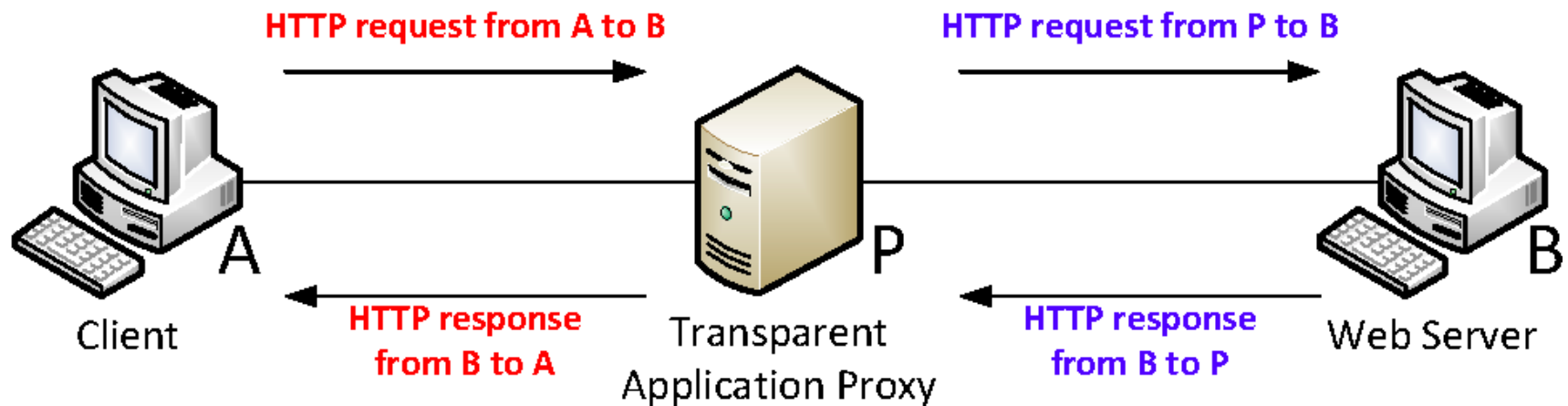
# Alkalmazásszintű transzparencia

- Szerver típusú kérés (protokoll) használata, pl.:  
GET / HTTP/1.0  
Host: www.balasys.hu  
Connection: Keep-Alive
- Proxy típusú kérés (protokoll) használata, pl.:  
GET http://www.balasys.hu HTTP/1.0  
Proxy-Connection: Keep-Alive
- Szimmetrikus vagy aszimmetrikus transzparencia:  
mindkét oldalon ugyanolyan, vagy különböző  
protokoll használat

# Alkalmazásszintű transzparencia



(a) Access network services via a non-transparent proxy.



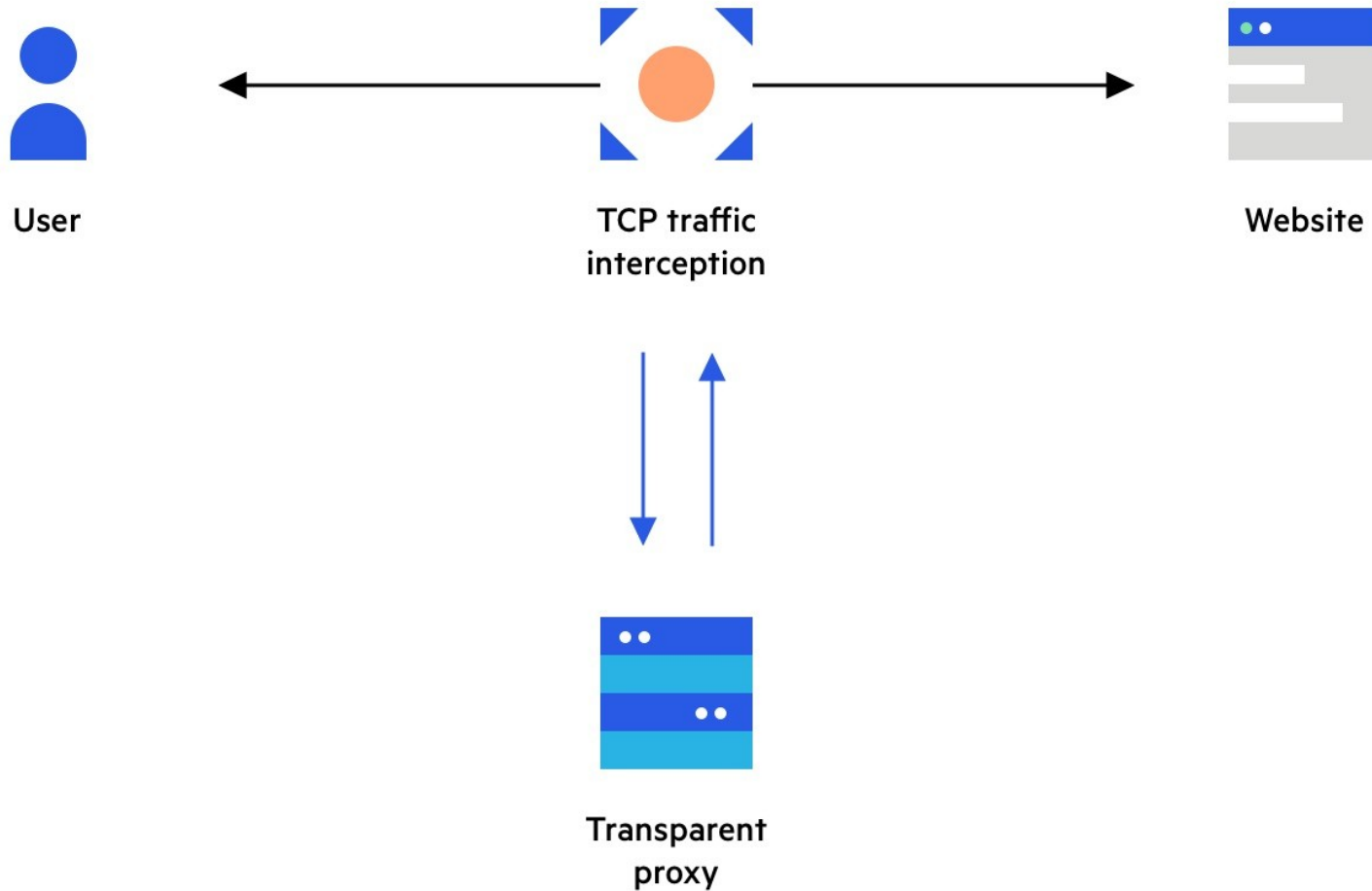
(b) Access network services via a transparent proxy.



# Transzparens proxyk

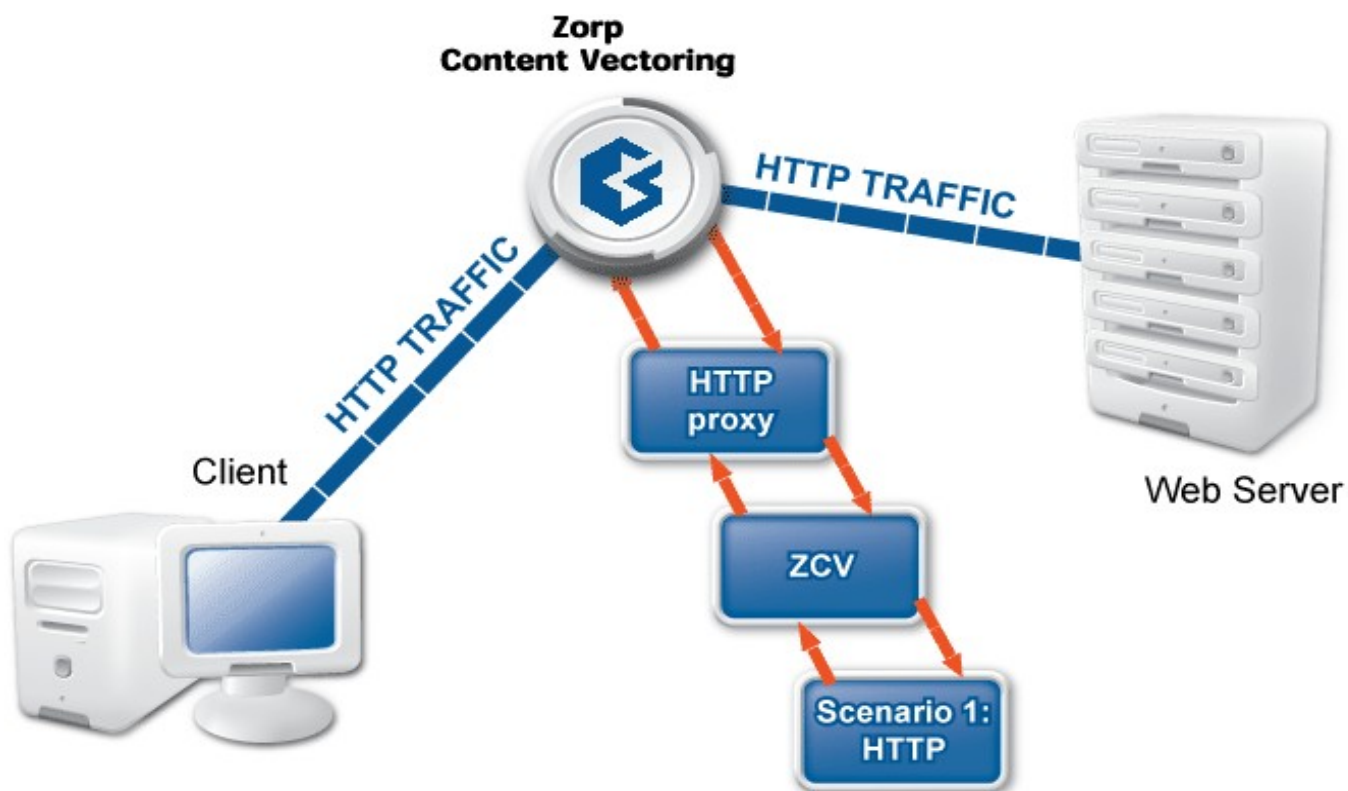
- **Működési elv:** A kapcsolatot valamilyen módon eltérítik eredeti céljától a proxyhoz (Ehhez gyakran csomagszűrőt használnak). A kliens és a szerver számára a kommunikáció transzparens.
- **Döntés alapja:** A kliens és a protokoll minden eleme alkalmazás szinten és az azt hordozó többi réteg (TCP/IP)
- **Megvalósítás:** Összetett. Mintaillesztés a hálózati rétegekben valamint mintaillesztés és **értelmezés** az alkalmazási rétegben. Az értelmezés mélysége függ a megvalósítástól.

# Transzparens proxy



- **Működési elv:** A feladatokat modulokra osztják és a modulokat kapcsolják egymáshoz. Funkcionalításban egyezik a transzparens proxykkal.
- **Döntés alapja:** A transzparens proxykkal egyező
- **Megvalósítás:** A transzparens proxykkal egyező

# Moduláris proxy



# Moduláris proxyk értékelése

- **Előnyök:**
  - Összetett és többcsatornás protokollok elemzése lehetővé válik
  - Nagyobb rugalmasság, stabilitás (KISS elv), mélyebb elemzés, skálázhatóság
- **Hátrány:**
  - Nagyobb CPU igény
- **Ismeretlen elemek kezelése:**
  - Megvalósítás függő, az ismeretlen elemek eldobása lehetséges

- Az a technológia, mely az eszközön (router vagy tűzfal) áthaladó csomagok forrás vagy cél címét megváltoztatja (NAT: Network Address Translation)
- Fajtái:
  - Egy-egy NAT
  - Sok-egy NAT
  - Forrás és cél NAT (SNAT vagy DNAT)
  - PAT (Port Address Translation)

# Címfordítás csomagszűrőkkel

- Csomagszűrők az adott szabályrendszer (minta) illesztik csomagról-csomagra, majd végrehajtják az ott előírt feladatot, ami engedély esetében a routing:
  - Alapvetően **ugyanazt az IP csomagot továbbítják**
- Címfordításkor a csomagszűrő az áthaladó csomag forrását (esetleg célját) módosítják
  - A válaszok esetében pedig vissza fordítanak

# Címfordítás proxy tűzfalakkal

- A proxyk a kliens oldali kapcsolatokat végződtetik, majd a protokoll értelmezés után független kapcsolatot építenek a szerver oldalon, ezért:
  - A szerver oldali kapcsolatának forrása a tűzfal címe (tehát a proxyk natívan végzik a csomagszűrők NAT funkcionalitását)
- Címfordításkor a szerver oldali kapcsolat forrása nem a tűzfal címe (hanem pl. a kliens IP-je).



# További határvédelmi funkciók

---

- Autentikáció
- nIDS és IPS funkciók
- Tartalomszűrés
- Naplózás
- VPN végződtetés (terminálás)

# Autentikáció tűzfalakon

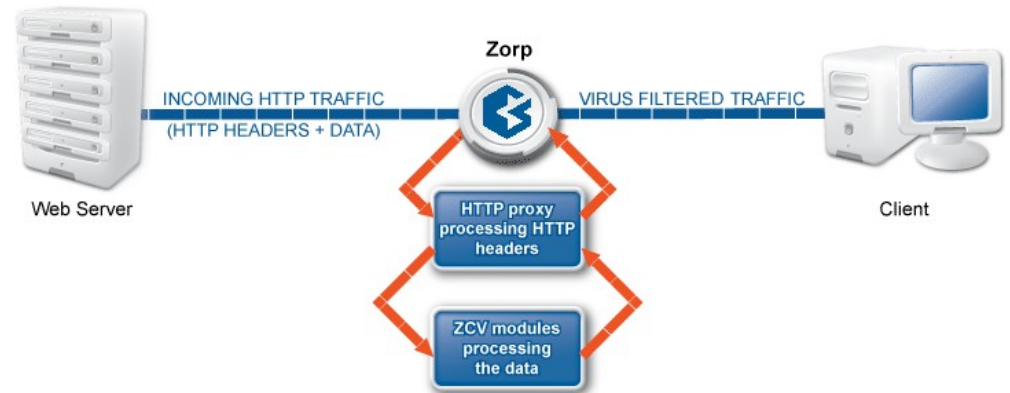
- Célja a felhasználó identitásának pontos meghatározása, majd felhasználói jogok hozzárendelése.
- **Protokollon belüli (inband):** egyes protokollok (pl. ftp és http) támogatják a kliens autentikációját a proxyn, tűzfalon.
- **Protokollon kívüli (outband):** valamilyen külső eszközzel, független csatornán azonosítjuk a klienst (így a protokoll nem befolyásolja az autentikációs mechanizmust).

# nIDS és IPS funkcionalitás tűzfalakon

- **Működési elv:** az eszközön áthaladó, engedélyezett forgalomban rossz szándékú aktivitás érzékelése és blokkolása
- Csomagszűrők esetében ez csak kiegészítő eszközzel (modullal) megvalósítható
- Proxyk esetében, amennyiben az ismeretlen protokollelemeket az tiltja, több IPS funkcionalitás megvalósítható

# Tartalomszűrés

- Vírusszűrés
- Spam szűrés
- Egyéb tartalom szűrés
  - URL
  - HTML, XML, SOAP (XML validáció)

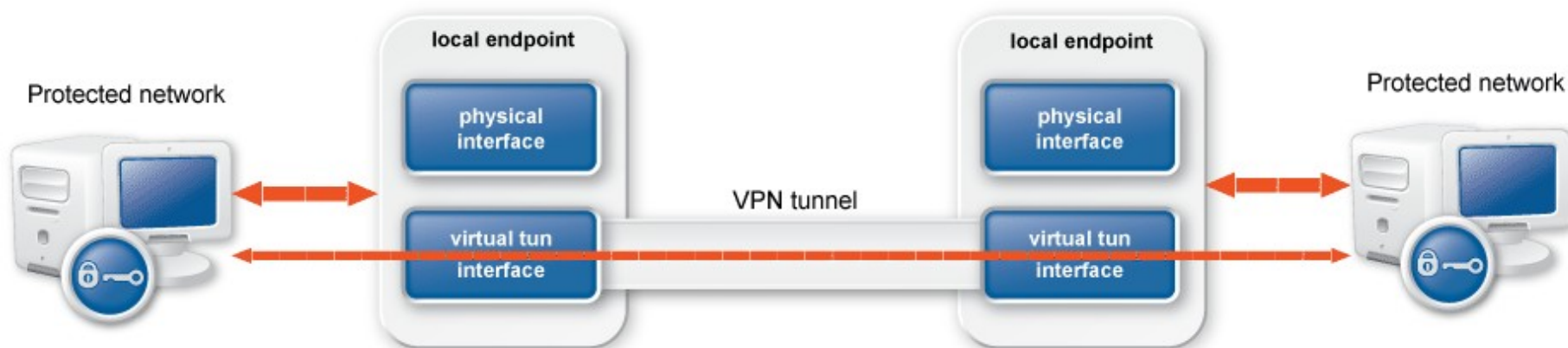


- Minden tűzfal megoldás az által értelmezett protokoll elemekkel kapcsolatos naplózási funkciókat képes megvalósítani.
- Csomagszűrők csak TCP/IP szinten naplóznak
- Proxyk esetében ez akár a teljes kapcsolat és minden protokoll elem naplózását is jelentheti (erőforrás igényes).
- Accounting információk naplózása lehetséges.

# Virtuális Magánhálózatok

- Olyan technológiák összessége, mely egymástól távol eső eszközöket és hálózatokat kötnek össze úgy, hogy a köztük megvalósult kommunikáció bizalmassága, sértetlensége és hitelessége ne sérüljön.
- Megvalósítás: általában valamilyen autentikált, rejtjelezett csatornát használnak.
- Alkalmazás szinten: OpenVPN, SSTP, IP over HTTPS és gyártó-specifikus implementációk
- Transzport szinten: IPSec, Teredo, 6to4

# Virtuális Magánhálózatok



# VPN megvalósítás tűzfalon

- A kikényszerített házirend a VPN csatornákon is érvényes.
- Rejtjelezett kapcsolatokban is lehetséges protokoll ellenőrzés, vírus és tartalom szűrés (melynek feltételeit az IBSZ-ben rögzíteni kell).
- VPN-ek autentikációja a központi PKI rendszerhez.



# Integrált határvédelmi megoldások

---

- Unified Threat Management
- User-based Firewall

# Unified Threat Management

---

- Packet filter + mintaillesztés
- Alkalmazás felismerés signature database segítségével
- Alap TLS inspection
- URL szűrés
- Tartalom szűrés
- Authentikáció
- VPN

Leánykori nevén Next-generation Firewall

- Előnyök:
  - Több technológiát egyesít
  - Egy felületről állítható
  - Nagy rugalmasság
- Hátrány:
  - SPF (Single point of failure)
  - Állandó frissítés
  - „checkbox security” - a pontos működése az adminisztrátor számára nem ismert
- Ismeretlen elemek kezelése:
  - Megvalósítás és szignatúra függő

# User-based Firewall

---

- Packet filter + beépített autentikáció
- User felismerés több forrásból
- Szabályok a felismert felhasználó alapján lépnek érvényre

# User-based Firewall értékelése

- Előnyök:
  - IBSZ-ben megfogalmazott szabályokhoz közeli a konkrét tűzfal konfiguráció
- Hátrány:
  - Nem kiforrott user felismerés (agent nélkül)
  - Rugalmatlan szabályrendszer konfiguráció
- Ismeretlen elemek kezelése:
  - Eldobásra kerülnek

# Speciális határvédelmi megoldások

---

- Threat Intelligence
- Software-defined Networking
- Speciális kiegészítő megoldások
  - Web Application Firewall
  - XML firewall
  - API Firewall
  - Dinamikus malware elemzés
  - Terheléselosztók
  - Privileged access monitoring
  - User behaviour analytics

# Threat Intelligence

- A hálózaton található biztonsági eszközök együttműködnek és információforrásként szolgálnak egymás számára
- A detektív kontrollok által felismert fenyegetésekre preventív kontrollt léptet életbe

Példa:

Végponti víruskereső által felismert fertőzés alapján a határvédelmi eszköz lezárja a hoszt hozzáféréseit

# Threat Intelligence értékelése

- Előnyök:
  - Kiegészítő megoldásként nagyban növeli akár egy csomagszűrő hatékonyságát
- Hátrány:
  - Bonyolult infrastruktúra
  - Gyártó specifikus megvalósítások (változóban, STIX/TAXXI)
- Ismeretlen elemek kezelése:
  - Eldobásra kerülnek



# Software-defined Networking

- Hálózati eszközök konfigurációját teljesen új alapokra helyezi, központosított, pluginelhető, teljesen rugalmas architektúra kialakításával
- A hálózati döntések elszeparálása négy, jól elkülöníthető rétegre (síkra): menedzsment, szolgáltatás, vezérlés és továbbítás
- Vezérlés (kontroller) és továbbítás (switchek, routerek tűzfalak) valósítja meg a határvédelemet és hálózat szegmentálást
- A továbbítási réteg minden kapcsolatra döntést kér a vezérlési rétegtől
- A vezérlés akár alkalmazást is kérdezhet a döntéshez

# Software-defined Networking értékelése

- Előnyök:
  - Dinamikus (pl felhő) infrastruktúrák könnyű kezelése
  - Emberi hiba kiküszöbölése nagy hálózatokban
  - Bevált elemekből építkezik (VLAN, GRE, stb)
- Hátrány:
  - A kontroller Single Point of Failure a hálózaton
  - A kontroller biztonsága határozza meg minden eszköz biztonsági szintjét
  - Az első csomag latency-je nem determinisztikus
  - Nehéz hibakeresés, komplex generált konfiguráció
  - Önmagában nem hálózatbiztonsági technológia
  - Nem kiforrott

# Speciális kiegészítő megoldások

- Web Application Firewall
  - elterjedt webes sebezhetőségek elhárítása (OWASP Top10)
  - szignatúra alapú
  - széles körben használt alkalmazások hibáira külön ruleset
- XML Firewall
  - biztosítja az XML üzenetek megfelelőségét
  - parzolás és séma validálás, XML signature ellenőrzés
- API Firewall
  - biztosítja az API (SOAP és REST) request és response megfelelőségét
  - Parzolás, séma validálás, API endpoint alapján
  - Naplózás, transzformáció, aggregálás

# Speciális kiegészítő megoldások

- Dinamikus malware elemzés
  - 0-day és ismeretlen malware-ek felismerése
  - minták futtatása sandboxban és a footprint elemzése
  - viselkedés alapú
- Terheléselosztók
  - szerepük egyre növekszik és változik
  - alkalmazás szintű tűzfal funkciókat kezdenek megvalósítani
  - scriptelhető

# Speciális kiegészítő megoldások

- Privileged access monitoring
  - privilegizált felhasználók hozzáféréseinek rögzítése
  - munkamenetek 4-szem elv alapú autorizálása
  - másodlagos azonosítás hozzáadása a munkamenethez
- User behaviour analytics
  - felhasználói viselkedés anomáliáinak felismerése
  - machine learning alapú megoldás, baseline építés után automatikus felismerés
  - semi-biometrikus adatok (gépelési dinamika, egérmozgás) drámaian növelik a megbízhatóságát

# Hálózatbiztonság a felhőben

- Szolgáltatófüggő megoldások
  - általában állapotartó csomagszűrő (security groups)
  - Identity-aware proxy
  - minden cloud szolgáltatónál más feature set ÉS túl sok eszköz, nem egyértelmű céllal
- Kihívások
  - a cloud szolgáltatón belüli forgalom integritása, sértetlensége és hitelessége nem biztosított
  - orchestration megoldások nem foglalkoznak a biztonsággal
  - bonyolult hálózati architektúra nehezíti a kockázatok felmérését és hibakeresést

# Hálózatbiztonság a felhőben

- On-premise virtualizációs infrastruktúra
  - VMware Virtual Distributed Switch – ACL-ek (proprietary)
  - OpenStack Nova – FwaaS (csomagszűrő), CNI (tunneling)
- Konténer orchestration
  - Kubernetes – Ingress Controller (csomagszűrő, proxy és alkalmazásszintű proxy), CNI (tunneling)
- Serverless :D
- Felkészül: Industry4.0 és IoT

# Kérdések?

---

**Kovács Bálint**

Chief Technology Officer

[kovacs.balint@balasys.hu](mailto:kovacs.balint@balasys.hu)



# Miről volt szó?

---

- A hálózati határvédelem értelmezése
- Hálózati alapfogalmak
- Tűzfal típusok
- Határvédelmi technológiák
- Speciális határvédelmi megoldások
- Kérdések és válaszok