Az informatikai biztonság alapjai

Pintér-Huszti Andrea

2020. szeptember 7.

Tartalom

1. Szolgáltatásmegtagadással járó támadások
2. Tűzfalak

Szolgáltatásmegtagadással járó támadások

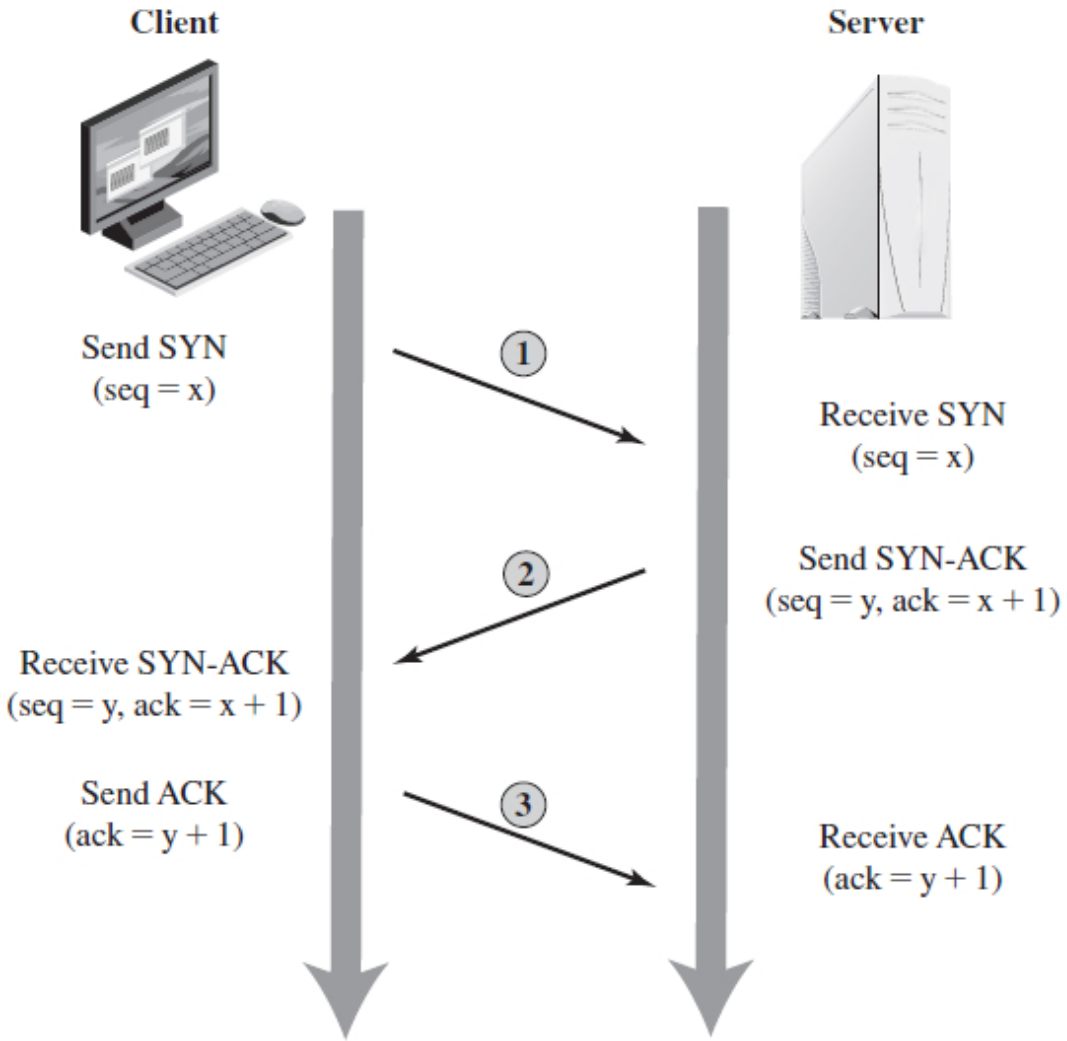
Szolgáltatásmegtagadással járó támadás (Denial-of-service attack)

- A támadás valamely szolgáltatás **rendelkezésre állását** veszélyezteti.
- Kategóriák:
  - **Sávszélesség elleni támadás**: A sávszélesség elleni támadás az Internet és a szerver közötti hálózati kapcsolat szűk kapacitását használja ki. A támadónak nagyobb sávszélességgel kell rendelkeznie, mint amilyen az áldozaté.
  - **Rendszer erőforrások elleni támadás**: A rendszer erőforrásait célozza, úgy túlterhelik, hogy **a hálózat kezelő rendszer összeomlik**. pl. SYN flood támadás a memóriát terheli
  - **Alkalmazási rétegbeli támadás**: Speciális alkalmazásokat célozza meg. Pl.: SMTP (email) szerver nagy mennyiségű e-mailt kap, megtöltve a háttértárat, amely a további levelek fogadását lehetetlené teszi (email bomb). Másik lehetőség a Web szerver terhelése jónéhány valós kéréssel (pl. adatbázis lekérdezések)

DoS támadások

- **Ping of death támadás**: Pingen alapul, melynél 65353 bájt csomag lehet a legnagyobb méretű csomag. A támadó ettől nagyobb csomagokkal bombázza az áldozatot, megtelik a memóriaterület (Buffer), és ez összeomláshoz vezet.
- **Elárasztásos (flooding) támadások**:
  - **ICMP Flood**: A ICMP (Internet Control Message Protocol) Echo (ping) parancson alapul. Csomagokat küldünk hamis forráscímekkel addig, míg az áldozat válaszolni tud. Egy idő után nem tud válaszolni.
  - **SYN Flood**: Syn(synchronization). A TCP protokoll három-utas kézfogásos üzenet visszaigazolási rendszerét használja ki. A célpont kapcsolatok állapotát tároló memóriája megtelik, így nem lesz képes új TCP kapcsolatot létrehozni.
- **IP forrás cím spoofing**: Hamis forrás cím megadásával a válasz csomagok nem térnek vissza a támadóhoz. Vannak hamis forrás címek, melyek válaszolnak error csomaggal, illetve a célt nem érő csomagok visszaküldődnek, növelve a forgalmat.

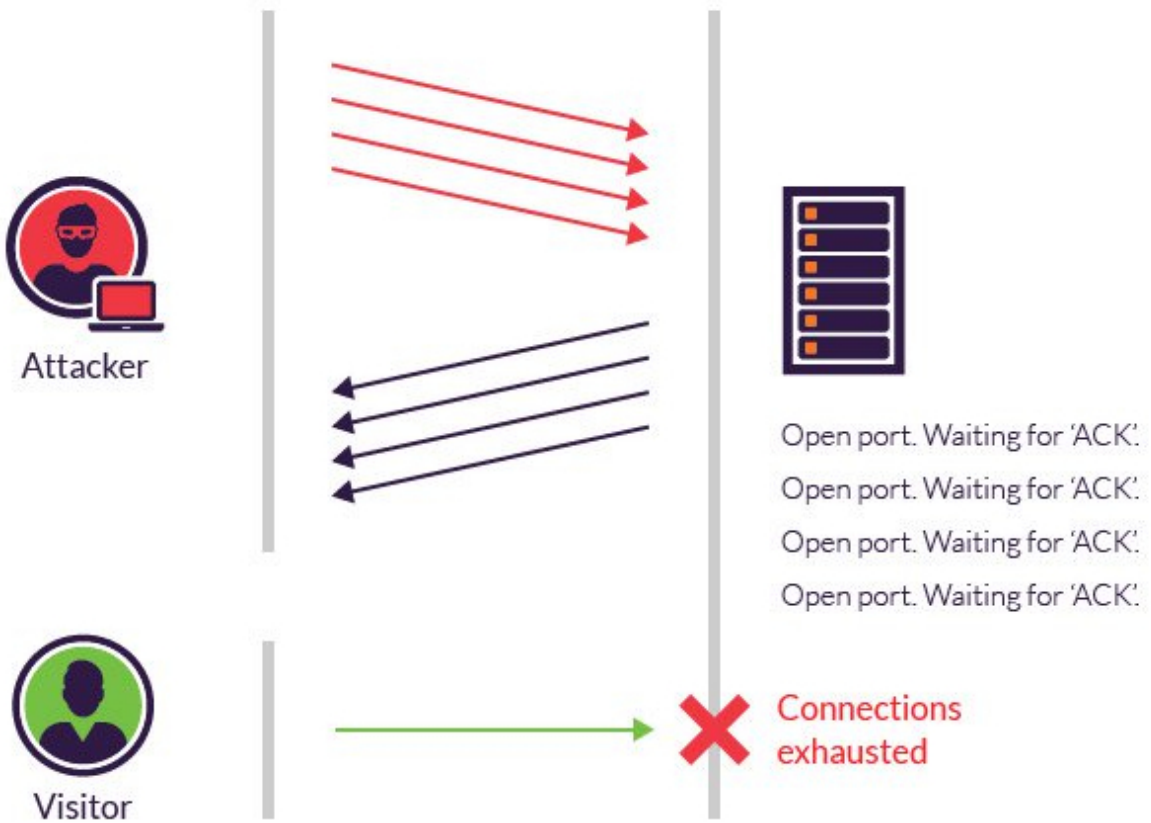
Három-utas kézfogás



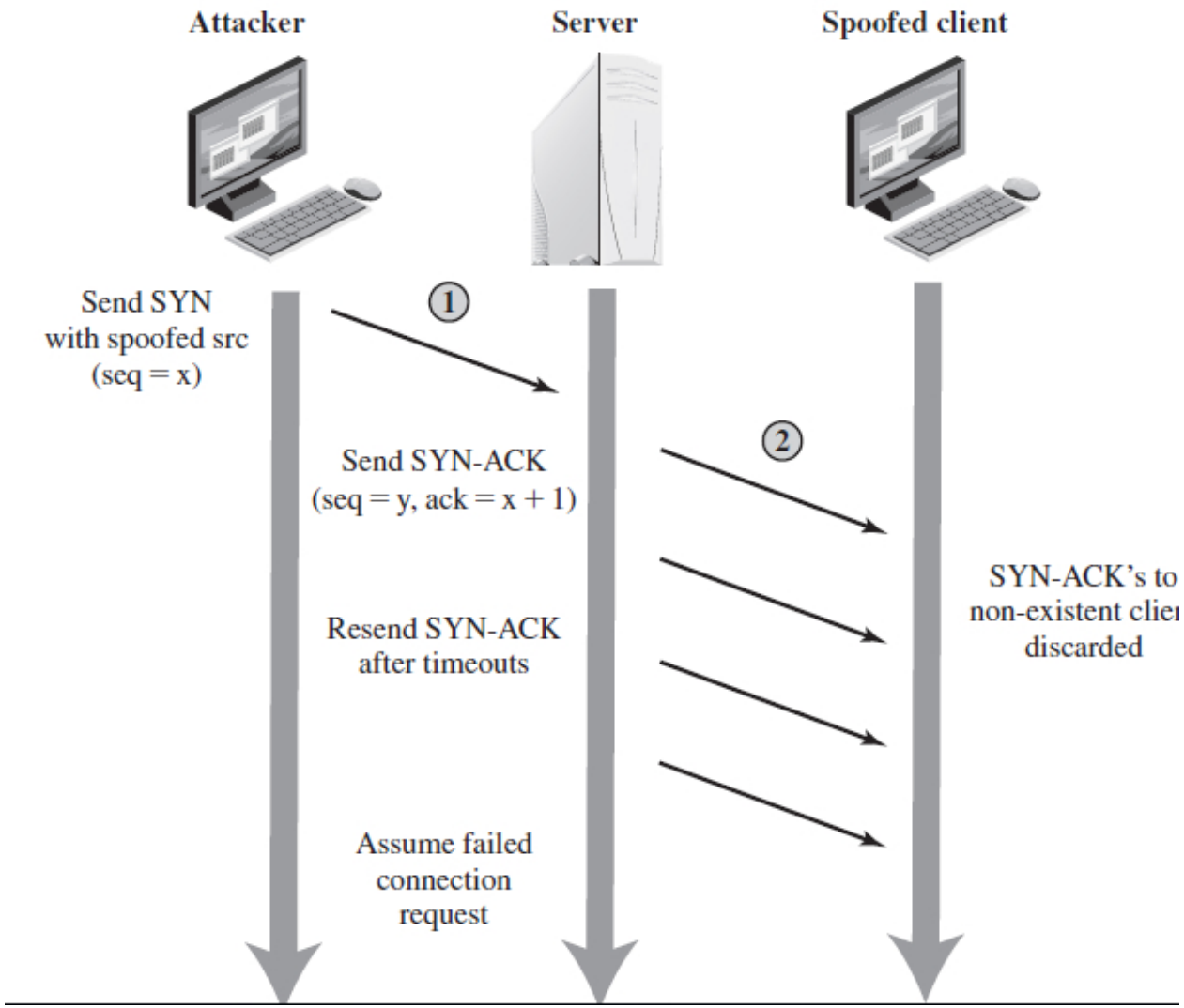
Három-utas kézfogás

- A kliens TCP kapcsolatot kezdeményez a szerverrel a **SYN csomag** elküldésével.
- Ez a csomag tartalmazza a kliens címét, portját, valamint egy kezdősorszámot. A szerver kezdeményezés valamennyi adatát tárolja egy **TCP kapcsolat táblában**. **SYN-ACK csomag** tartalmazza a szerver új **sorszámát** és **növeli a kliens sorszámát**.
- Ahogy a kilens megkapja a csomagot, küld egy **ACK csomagot** a szervernek a megnövelt szerver sorszámmal és a kapcsolatot létrejöttnek állítja be.
- Amikor a szerver megkapja az ACK csomagot, a kapcsolatot létrejöttnek állítja be.
- Mind a kliens, mind a szerver nyomon követi mely csomagokat küldte el, ha nem kap választ, újraküldi a csomagokat.

Syn flood támadás



Syn flood támadás (részletesen)



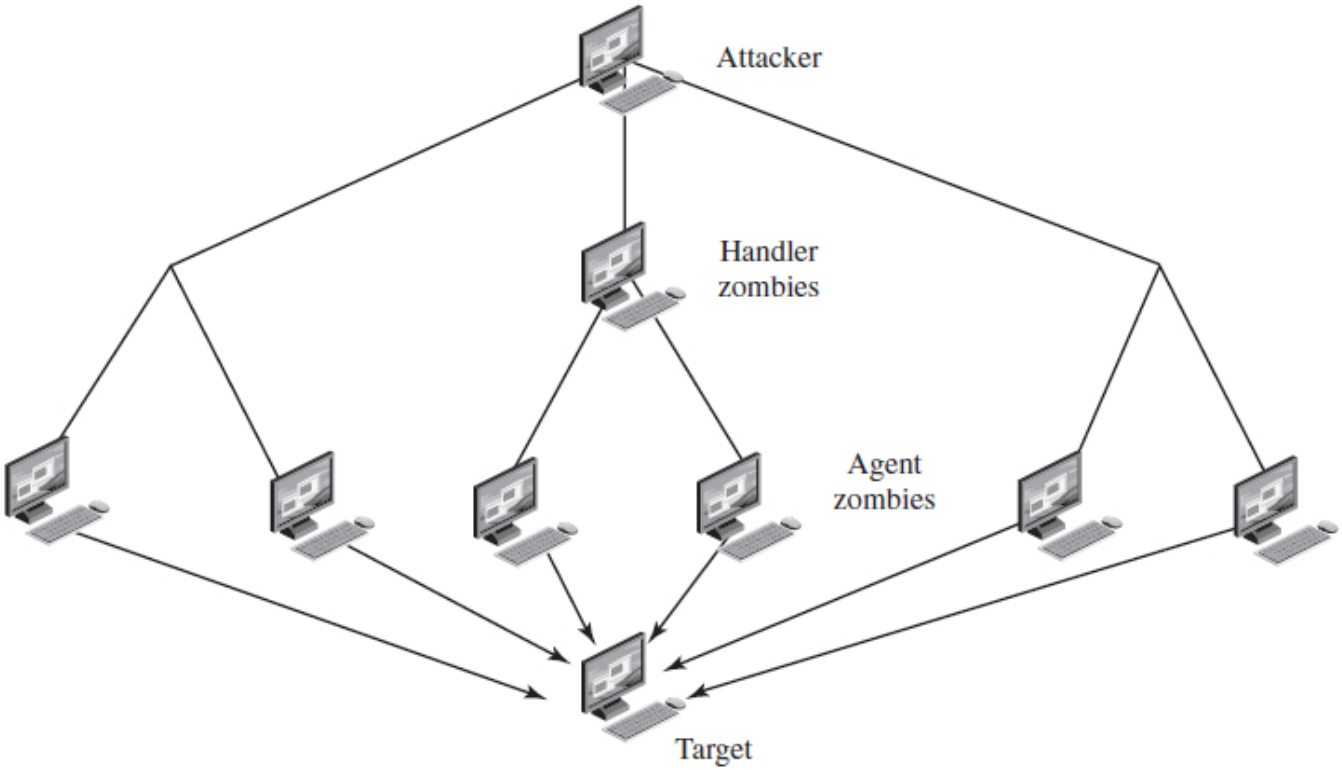
Syn flood támadás

- A támadó számos SYN kapcsolat kezdeményező csomagot generál, melyben hamis forrás IP-címek vannak. (spoofing)
- Minden egyes kérésre a szerver eltárolja az adatokat és küld egy SYN-ACK csomagot a megadott forrás címre.
- Ha forrás című rendszer elfoglalt, vagy ha nincs, akkor a szerver nem kap válasz csomagot és újra elküldi a SYN-ACK csomagot, jó néhányszor. Végezetül, feltételezve, hogy a kezdeményezés sikertelenné vált törli a kezdeményezés adatait.
- A támadó nagy mennyiségű hamis kapcsolat kezdeményezést küld a szerver felé. Ahogy a tábla telítődik, a valós kezdeményezéseket visszautasítja.

Elosztott DoS (Distributed Denial-of-Service) támadás

- A támadó egyetlen rendszer helyett, több rendszert is használ a támadáshoz.
- Ezek a rendszerek tipikusan fertőzött rendszerek: zombigépek, melyek botnetet alkotnak.
- A támadók egy kontrollált hierarchiát alkotnak. Kevés számú kezelő zombi irányítja a nagyobb számú ügynök zombikat.
- Ahogy egy ügynök szoftver feltöltődött egy fertőzött gépre, egy-két kezelő géppel egyből közli, hogy rendelkezésre áll.
- A legjobb védekezés a megelőzés.

DDoS Attack Architecture



Védelmi intézkedések

- **Tűzfalak használata:** Amennyiben a tűzfalat lehet úgy konfigurálni, hogy a lehető legtöbb rosszindulatú forgalmat eldobja, akkor legalább maga a szerver visszakaphatja kiszolgáló és feldolgozó teljesítményének egy részét. A tűzfal alkalmasságát a rosszindulatú forgalom a többitől való megkülönböztetésének képessége adja. Lehetnek bizonyos körülmények a támadás szerkezetében, amik aktív szerepet játszhatnak a rosszindulatú és szabályszerű forgalom szétválasztásában.
- Célszerű létrehozni **tükör másolatot**. Igen hatékonyan lehet egy szerver tartalmának formáját visszaállítani és azt tetszőleges sebességgel elérhetővé tenni.
- **Megosztott tartalom:** Az adatok terjesztés (elosztás) szempontjából mindig rendelkezésre állnak megosztott módon. Nem egy szerver, hanem több szerver is válaszol a kérésekre.

Tűzfalak

Kerecsendi András: Hálózatbiztonság

Miért van szükség tűzfalakra?

- A tűzfalak védik a helyi hálózatunkat hálózat-alapú támadásoktól.
- Elhelyezkedésük alapján:
  - Személyes (szoftveres) tűzfal: Egyedi számítógépekre telepített tűzfal alkalmazás, amely szoftveresen fog védeni, de csak azt az egy gépet.
  - Központi (hardveres) tűzfal: Nem egy számítógépen fut a szolgáltatás, hanem egy speciális hardveren(router), ezért ezt a módszert hívjuk hardveres tűzfal szolgáltatásnak is. A teljes belső hálózatunkat védhetjük.
- Központi tűzfal jellemzői: olcsóbb, egyszerűbb hálózatmenedzsment, központi kezelhetőség
- Személyes tűzfal jellemzői: operációs rendszer része, alapbeállítással is hatékonyak, minden számítógépen külön el kell végezni a beállításokat

Tűzfal

- Tűzfal alatt olyan biztonsági rendszert értünk, amely a számítógépes hálózatok kapcsolódási pontján helyezkedik el, és minden átmenő (kimenő és bejövő) hálózati forgalom figyelésével, szűrésével nyújt védelmet.
- A teljes hálózati forgalmat képes figyelni, akár csomagonként átvizsgálva azt, hogy átengedje-e azokat, vagy veszélyesnek minősítse, és megakadályozza a továbbításukat.
- A kimenő csomagok ellenőrzésére is sor kerülhet, így egyszerűen lehet megakadályozni a belső hálózatunkból induló támadásokat, vagy a nem kívánt hálózati helyek elérését. (pl. nem lehet a közösségi oldalakat elérni)

Mit várhatunk egy tűzfaltól?

- Jogosulatlan felhasználókat a védett hálózaton kívül tarthatjuk, kockázatos szolgáltatások be- és kikerülésétmegakadályozza, védelmet nyújt IP spoofing és routing támadások ellen.
- Biztonsággal kapcsolatos események monitorozása (audits, figyelmeztetések).
- Nem biztonsággal kapcsolatos finkcionalitás biztosítása: NAT (network address translator) hálózati cím átalakítása, hálózatmenedzsment funkciók: Internet használat figyelése audit vagy log fájlok alapján.

Tűzfalak korlátai

- A központi tűzfal nem véd a belső, tűzfal mögötti támadástól, ha a hálózatunkon belül található már fertőzött, feltört számítógép, esetleg rosszindulatú felhasználó, aki belülről támad. (Megoldás: személyes tűzfal)
- Kintről behozott fertőzött laptop, PDA, vagy hordozható tároló eszköz használata esetén szintén nem véd a központi tűzfal.

Tűzfalak típusai: Csomagszűrő tűzfalak

Packet Filtering Firewall: A csomagszűrő tűzfalak szabályok halmazát(házirendet) alkalmazzák minden egyes bejövő és kimenő IP csomagra, mely alapján vagy továbbítják vagy eldobják a csomagot. (pl. forrás és cél IP cím, port száma)

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Tűzfalak típusai: Állapot szerinti szűrés

Állapot szerinti szűrés: Ez a módszer alapvetően a kapcsolatorientált protokollok esetén nyújt újabb lehetőségeket. A tűzfal azonosítani tudja egy kapcsolat kezdetét és végét, valamint a kettő között zajló adatforgalmat. Csomagokat tárolja átmenetileg, amíg a szolgáltatás a döntéshez szükséges adatokat össze nem gyűjti. Néhányuk tárolja a TCP sorszámot, hogy megelőzze a session hijacking támadást.

Table 9.2 **Example Stateful Firewall Connection State Table**

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Tűzfalak típusai: Alkalmazásszintű (proxi) tűzfal

- **Alkalmazásszintű tűzfal**: Egy alkalmazás-szintű tűzfal a tisztán csak a forgalomhoz tartozó, mint a forrás, cél és szolgáltatás adatokon kívül a hálózati csomagok tartalmát is figyeli.
- A proxy megoldások azzal a céllal készültek, hogy kiküszöböljék a felhasználók kiszolgálókra való bejelentkezésből adódó kényelmetlenségeket, illetve az ebből fakadó veszélyeket.
- A kliensek és a kiszolgálók között nem épül fel közvetlen kapcsolat, hanem mindketten a tűzfalon futó proxy alkalmazással kommunikálnak.