

Hálózati határvédelem eszközei (kivonat)

Scheidler Balázs

2000.09.16.

Napjainkban sajnos egyre kevésbé „biztonságos” hely a Net. Míg néhány évvel ezelőtt az Internet még félig-meddig bizalmi alapon működött, ma már mindenki gyanakvással figyel a „külvilágba”. Gyakran hallani tizenévesek „akcióiról”, mely során nagynevű cégek hálózataiba hatolnak be látszólag különösebb probléma nélkül. Ezen csínyek során súlyos milliók kerülhetnek, kerülnek veszélybe.

Az írott és iratlan sajtó persze igyekszik nagy lufit varázsolni mindenből, a sikerek legnagyobb oka viszont általában az elégtelen, rosszul kivitelezett vagy rosszul üzemeltetett hálózati határvédelem.

Előadásomban igyekszem bemutatni a rendelkezésre álló védelmi technológiákat:

- bastion host: egy egyszerű munkaállomás, két hálózati interfésszel, a külső hálózatot a belső hálózatról közvetlenül nem-, csak a bastion hostra való belépéssel lehet elérni.
- csomagszűrő router: olyan számítógép (vagy célszámítógép), mely a fejlc-re vonatkozó szabályok alapján enged át, vagy tilt meg csomagokat.
- állapottartó csomagszűrő (stateful packet filter): olyan csomagszűrő, mely képes a csomagok között állapotot tartani, azaz megvizsgálni a csomagok tartalmát, és ez alapján döntést hozni.
- proxy tűzfal: csomagok továbbítása helyett kapcsolatok továbbítását végzi, és biztosítja, hogy egy kapcsolaton csak megadott protokoll haladhasson át, és annak is csak az engedélyezett részei.

A BalaBit IT Biztonságtechnikai Kft jelenlegi fejlesztése, a GNU/GPL alatti Zorp proxy tűzfalrendszer ez utóbbi csoportba tartozik, és célja, hogy minden területen felvegye a versenyt a jelenleg kapható tűzfalszoftverekkel.

A Zorp keretrendszerének felépítése lehetővé teszi az átengedett protokoll finomhangolását, a beágyazott protokollok kezelését, valamint az outbound autentikációt. Ezeket a lehetőségeket mutatom be egy életszerű példán keresztül, mely egy képzeletbeli cég hálózati határvédelmét mutatja be.

