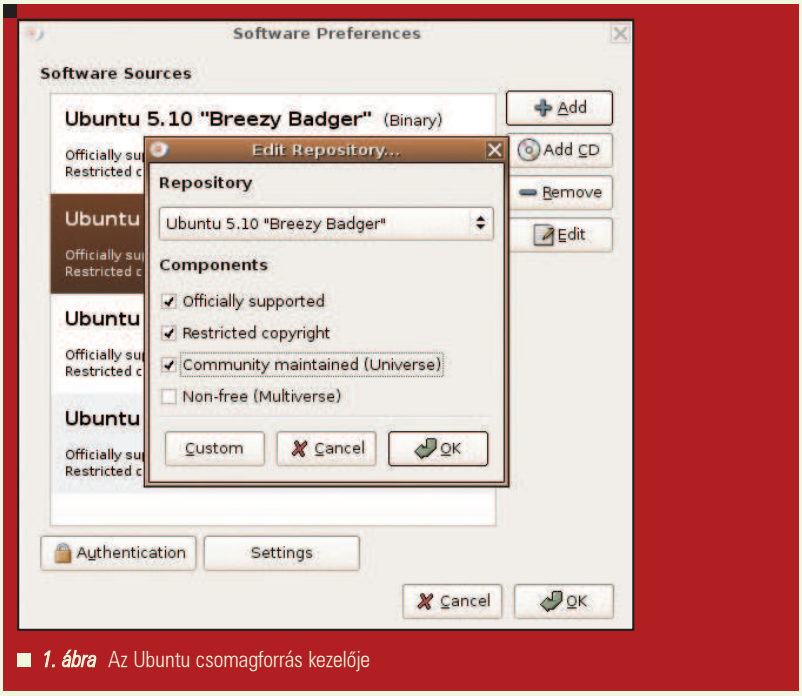
Segédeszközök tűzfal-szabályok beállításához

Internetezés közben Linux alatt sem vagyunk biztonságban, ezért érdemes valamilyen tűzfal alkalmazást használni, mely rendszerünk elsődleges védelmi vonala lesz. A számos elérhető konzolos és grafikus alkalmazás közül ebben a cikkben a Firestartert mutatom be.

A *Firestarter* a 2.4-es kerneltől meglévő *Netfilter* állapottartó csomagszűrő rendszerhez készült grafikus segédprogram. Segítségével könnyen és egyszerűen adhatunk meg tűzfal szabályokat, valós időben monitorozhatjuk a különböző hálózati eseményeket, nyithatunk vagy elrejthetünk portokat, megállíthatjuk *DoS* támadásokat.

A program több fajta csomagformátumban elérhető. Én *Ubuntu Linuxra* telepítettem, ahol először a hivatalos mellé fel kellett venni a közösség által karbantartott (*universe*) csomagforrást. Ez legegyszerűbben az *alkalmazások hozzáadása/beállítások/repository* alatt tehető meg. Ezután már csak ki kell adni az `apt-get install firestarter` parancsot. Ha *rpm* alapú csomagkezelővel rendelkező disztribúciónk van(több között *Red Hat, SuSE* vagy *Mandrake Linux*), akkor előbb a ➲ *www.fs-security.com/download.php* címről töltsük le a megfelelő csomagot. Majd rendszergazdaként adjuk ki az



1. ábra Az Ubuntu csomagforrás kezelője

```
rpm -Uvh firestarter*rpm
```

parancsot.

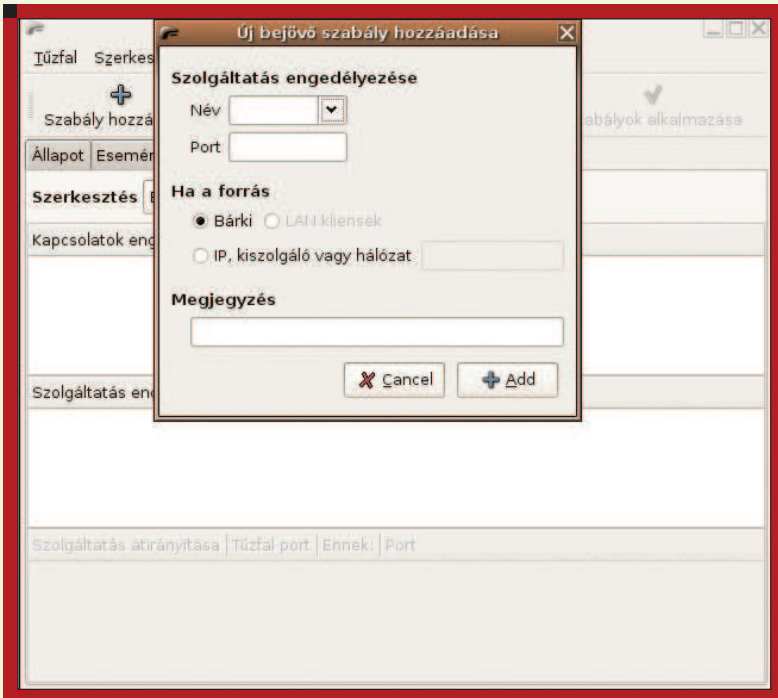
A programhoz csak rendszergazdai jogosultságokkal férhetünk hozzá. (Ha nem találjuk akkor az

Alt-F2 lenyomása után írjuk be, hogy `firestarter`) Első elindításakor egy varázsló segíti a tűzfalunk beállítását (ezeket megváltoztatni később sok más mellett a beállítások menüpont alatt lehet). Az üdvözlő képernyő után ki kell választanunk a használni kívánt hálózati eszközt. Ha modemet használunk vagy kábeles, *DSL* szolgáltatónk *PPPoE* protokollt használja akkor a *pppX*-t, egyébként *ethX*-t érdemes választani. (X=0,1...) Ezen kívül, ha betárcsázós *Internet* elérésünk van akkor választhatjuk, hogy a tűzfal csak a csatlakozás után induljon el. Ezt azonban nem javasolom mivel nem mindegyik tárcsázóval tud együtt működni a program. A következő képernyőn megadhatjuk, hogy ezen gépen keresztül más gép is el fogja érni a hálózatot, hanem akkor ne jelöljük be ezt az opciót. Utolsó lépésként mér csak a mentés gombra kell kattintani, ekkor alapértelmezett szabályokkal elindul a tűzfalunk. Ez azt jelenti,hogy korlátozni fogja a bejövő forgalmat, a kimenőt pedig engedélyezni. Tehát védve vagyunk a külső támadások elől, de korlátozás nélkül használhatjuk többek között a böngészőnket, levelező programunkat.
A megjelenő ablakon három fül található: állapot, események, és a szabályok. Az elsőn információkat kaphatunk a program aktuális állapotáról: le van e tiltva tűzfal, milyen volt a hálózati forgalom aktivitása(elküldött, fogadott *MB*-tok értéke), valamint, hogy mennyi a meggátolt behatolási kísérletek és nem engedélyezett kifelé irányuló próbálkozások száma. Ezekről részletes információt az események fül alatt kaphatunk pl.: mikor történt, iránya (belső hálózatról vagy az Internet felől), mi a forrás *IP* címe, mely szolgáltatást akarták használni, blokkolt csomag nagysága. Ezek nem mindegyike jelenik meg alapból, a hiányzóakat az ***események/oszlop mutatása*** menüpont alatt adhatjuk a többihez. A különböző támadásfajták színekkel is meg vannak különböztetve:

- fekete: Általános csatlakozási kísérlet egy találomra választott *port*-on. Ide kerülnek a lefülelt *port* szkennelési támadások.

- piros: Csatlakozási kísérlet egy nem publikus szolgáltatáshoz. (például: *FTP*-hez).

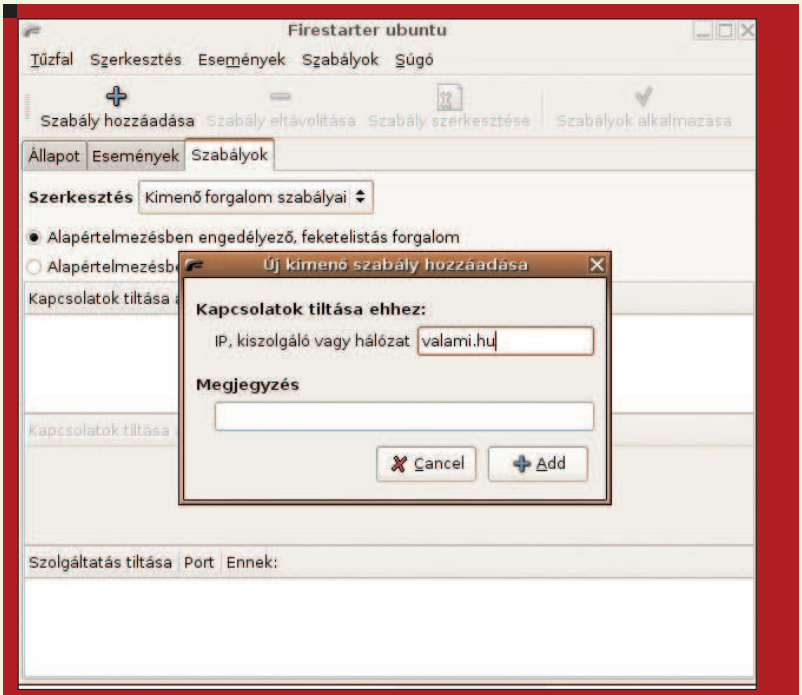
2. ábra A képen a tűzfal le van tiltva rossz hálózati eszköz választás miatt



3. ábra A szolgáltatás elérésnek engedélyezése

- szürke: Ártalmatlan kísérlet. Ebbe a csoportba elsősorban az üzenetszórási forgalom található meg.

Ha a jobb egérgombbal egy sorra kattintunk beállíthatjuk, hogy mit csináljon a program hasonló esemény esetén, tehát már itt megváltoztathatjuk



■ *4. ábra* A valami.hu felkerül a fekete listára

az alapértelmezett tűzfalszabályokat. Az esemény irányától függően a következőeket adhatjuk meg:

1. Ha befelé irányuló (csatlakozási kísérlet az Internet vagy helyi hálózat felől a tűzfalt futtató ***host***-hoz.)
   - A forrás ***IP***-nél megjelenő cím számára mindenfajta csatlakozás engedélyezése.
   - Használni kívánt szolgáltatás engedélyezése mindenkinek illetve csak a forrás címnek. Utóbbi esetben a szolgáltatás rejtve van más ***host***-ok esetében
2. Kifelé irányuló próbálkozás esetén:
   - Csatlakozás engedélyezése a célhoz
   - Adott külső szolgáltatáshoz való csatlakozás engedélyezése a helyi hálózaton adott/mindegyik kliens számára

Az utolsó fülön bejövő és kimenő hálózati forgalomra adhatunk meg szabályokat.
A bejövő forgalom alapértelmezetten tiltva van, s itt adhatunk meg ezt felülbíráló szabályokat, vagyis a legitim forgalom számára lyukat tehetünk a tűzfalba. Három fajta szabálycsoport megadására van lehetőség:

- Megadhatjuk, hogy mely távoli ***host***-ok felől érkező forgalom haladhat át legálisan a tűzfalon. Ezt megtehetjük ***IP*** cím vagy ***host*** nevének megadásával.
- Engedélyezhetünk különböző szolgáltatások elérését. Meg kell adni a szolgáltatás nevét (egy legördülő listából választható ki) vagy az általa használt ***port***ot. és, hogy kiknek legyen engedélyezve (Bárkinek, ***LAN*** vagy adott ***IP***-vel rendelkező kliensnek)

Lehetőség van, hogy a program szolgáltatást kérést közvetítsen a helyi hálózat felé. Ha több gép is osztozik egy adott ***Internet*** elérésen, akkor ezek csak egy gépnek látszódnak az ***Internet*** felől, és beállítható, hogy melyik helyi gép, melyik ***port***-jára küldje tovább a ***Firestarter*** az adott szolgáltatási kérést.
Kimenő forgalomra vonatkozó szabályok kezelésére a program kétfajta megközelítést kínál:

- ***Megengedő mód***: Alapértelmezetten így indul a program, a kifelé irányuló forgalom engedélyezve van Szabályozás eszköze: a fekete lista. Az erre felkerülő ***IP*** címhez, kiszolgálóhoz vagy hálózathoz, nem csatlakozhatnak a sem helyi hálózatról sem a ***Firestartert*** futtató gépről. Ezenkívül ezen fülön megadhatjuk, hogy lokális gépek közül melyik nem érheti el az ***Internetet***, illetve letilthatjuk a különböző szolgáltatások elérését.
- ***Korlátozó mód***: Minden olyan kifelé irányuló forgalom tiltva van, mely nincs engedélyezve az un. fehér listán. Maximális védelmet biztosít, de minden hálózati alkalmazásra külön szabályt kell alkotni. Először is megadhatjuk, hogy melyik ***IP*** cím, kiszolgáló vagy hálózat érhető el. Ez például jól jöhet, ha gyerekeink számára le akarjuk korlátozni a meglátogatható honlapokat. Megadhatjuk, hogy a helyi hálózat melyik gépe csatlakozhat az Internethez, és milyen szolgáltatás érhet el.

Mindkét módban az új szabályok csak a ***szabály alkalmazása*** gomb megnyomása után lépnek életbe.
A működő tűzfalunk további finomhangolásra a beállítások menüpont alatt van lehetőség. Az itt megjelenő opciók közül zárásként mindössze egyet emelnék ki. Az ***ICMP*** protokoll lehetővé teszi különböző hibaüzenetek, teszt csomagok küldését egy adott ***host***-nak. Sok ilyen küldésével egy adott gép elérést meghiúsítják, ez az úgynevezett ***DoS*** támadás. Megadhatjuk, hogy a tűzfal korlátozza az ***ICMP*** üzenetek létrehozását és fogadását, illetve, hogy közülük melyikre ne vonatkozzon ez.

Fekete Imre
(imre.fekete@gmail.com)

Programtervező-matematikusként végeztem a Debreceni Egyetemen. A Linuxtól kezdetben idegenkedtem, de ma már csak azt tudom mondani róla, hogy remek rendszer.