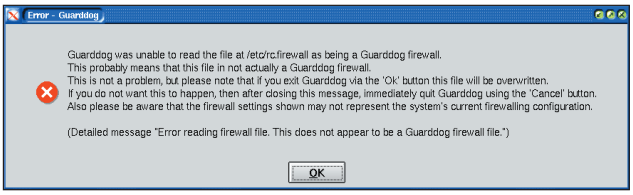
Személyes tűzfalak Linuxon

A mókásan csak aszbesztkabátnak hívott programok GNU/Linux alatt is elérhetőek.

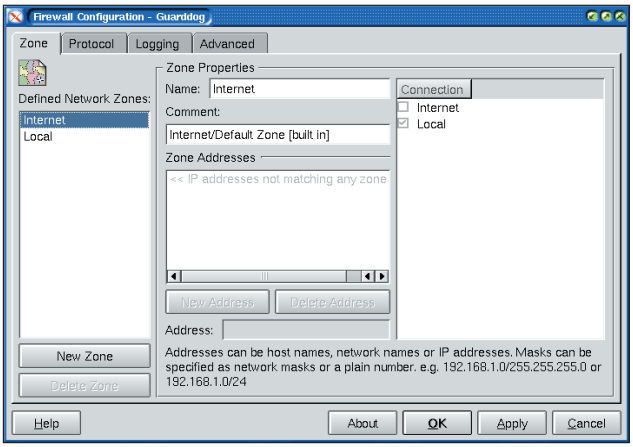
Gyakran, ha a biztonságról esik szó, hiába bizonygatja az ember az átlagosnál többet tudó felhasználóknak, hogy a Linux biztonságosabb, jobb és szebb, mint a jégbe fagyott ablak. Azonnal azt kérdezik: hol van a ***ZoneAlarm*** Linuxra? Sokak számára ugyanis ez a program jelenti a sérthetetlenséget. A kutatások eredményeképpen megismerhettük a placebohatást: pszichikai eredetű betegségekben szenvedőkkel elhitetik, hogy orvosságot kapnak, és ennek következtében hirtelen „meggyógyulnak", ha viszont azt mondják nekik, hogy nem tudnak segíteni, az állapotuk rosszabbodik – csakhogy a bitek világában sajnos nem ér semmit, ha egyre azt mondogatjuk magunkban: nem történt semmi, nem törték fel a gépemet. Akkor is feltörhették, ha azt sulykoljuk, hogy nem történt semmi baj. Szóval nehéz elmagyarázni, hogy a biztonság nem pusztán abból áll, hogy felteszek valamit, ami a kívülről jövő kapcsolatokat engedélyezi vagy éppen letiltja. A ZoneAlarm program viszont nagyon látványos, elindulásakor kis tülkölés hangzik fel, szép kis kijelzőt láthatunk a hálózati forgalomról, mint amilyen például az IceWM tálcáján is található. Egy szó, mint száz, valami hasonlót kell adni felhasználóknak, máskülönben nem békélnek meg a gondolattal, hogy „csak" egy proxy (például Squid) és állapottartó csomagszűrő védi őket a hálózati átjárón az Internet felé. Csupán azon magyarázatunkra csillan fel a szemük, hogy a ZoneAlarm sem több, mint egy csomagszűrő – ezt csak a letölthető változatról állíthatom, ugyanis ezt ismerem –, és ezt akármelyik terjesztés nyújtani képes. Ekkor felvillan a lehetősége, hogy többek között a „gonosz" munkatársak és a rendszergazda ellen beállíthatják maguknak a védelmet, viszont amikor meglátják, hogy mindent kézzel kell megtenni, a Linuxot újra a kőkorszakba sorolják. Erre kellene egy jó megoldás, és ezt a Guarddog program jelentheti. Ebben minden megvan, ami szükséges. Hangzatos név, grafikus beállítófelület a leggyakoribb alkalmazásokhoz. A program a ➲ http://www.simonzone.com/software/guarddog/ címen érhető el.

Telepítés után a programot a `guarddog` paranccsal indíthatjuk a KDE alatti ***K*** menüből, vagy ha más ablakkezelőt használunk, akkor egy grafikus felület alatti konzol alól, mint amilyen az Xterm vagy Eterm programok. Figyelem! Ha nem rendszergazdaként indítjuk, a program tájékoztat minket, hogy beállíthatjuk, milyen védelmet szeretnénk, de nem fog életbe lépni, mert nincs rendszergazdai jogosultságunk. Ezt szemlélteti az *1. kép*. Erre kínál megoldást, ha például az Xterm alatt `su -m` parancscsal (a `-m` kapcsoló hatására grafikus felületet használó programokat is megfelelően tudjuk használni), hogy ekkor mi

1. kép Lényegre törő figyelmeztetés



2. kép Az első indítás öröme



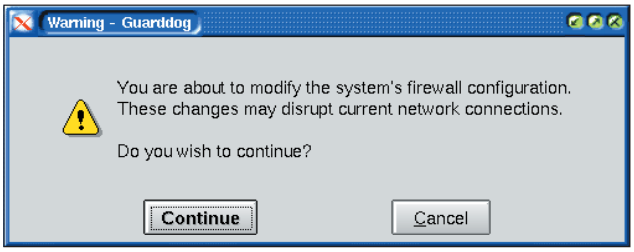
3. kép Kezdődhet a beállítás

történik, a *2. képen* láthatjuk. A képen már rendszergazdai jogosultságokkal rendelkezünk, de mint kitűnik, előtte meg kell adni a rendszergazda (root) jelszavát.

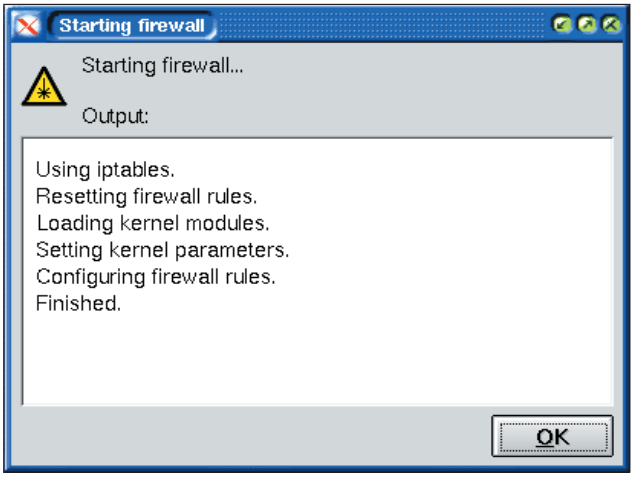
Ha `guarddog`-ot innen indítjuk el, az első alkalommal tájékoztat minket, hogy csomagszűrő tűzfalunk nincs beállítva. Ez természetes is, hiszen most indítjuk először a programot. Nyugodtan haladjunk tovább az ***OK*** gombbal. A *3. képen* látható képernyő fogad minket.

Nézzük végig a füleket!

- ***Zone***
  Zónákat vehetünk fel, illetve törölhetünk, kivéve a két beépítettet: az Internet és a Local nevűt.
  Új zóna felvételénél adjuk meg a nevét (***Name***), valamint a címtartományt, amelyre vonatkozik (***Zone Addresses***). Egész címtartományokat is megadhatunk (`192.168.0.0/24`), de akár egyedi címeket vagy csak egy címet is megadhatunk.
- ***Protocol***
  Ezen a fülön állíthatjuk be a szabályozást. A lenyíló listából válasszuk ki az ***Internet*** zónát. Ezután, mint a 3. képen is láthatjuk, elég egy grafikus menüben kijelölni a használni kívánt alkalmazásokat – valójában a protokollokat, hiszen például az ICQ-protokollt is több program ismeri. Ha egy alkalmazás neve mellett a jelölőnégyzet üres vagy egy x jelet látunk, akkor az le van tiltva, pipa estén engedélyezett. Válasszuk ki, mit szeretnénk használni és engedélyezzük.
  A beállítást azonnal érvénybe léptethetjük, ha az ***Apply*** gombot lenyomjuk. Ekkor a rendszer figyelmeztet, hogy



4. kép Reméljük, nem felejtettünk ki semmit!



5. kép Most már védve vagyunk

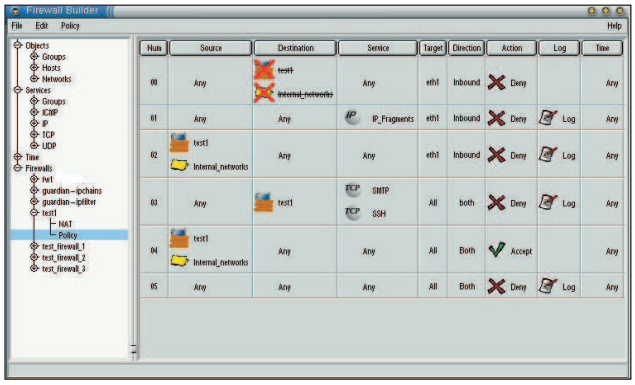
a szabályok életbe léptetésével bizonyos internetkapcsolataink megszakadhatnak. Ez csak akkor fordulhat elő, ha pillanatnyilag olyan alkalmazást is használunk, amelyet az új beállításban letiltunk. Például már nem akarunk többet ICQ-ra csatlakozni, de a program még fut, ekkor a szabályok érvényesítése után kapcsolata megszakad. A figyelmeztetést a következő, *4. képen* láthatjuk.

Az érvényesítés eredményét az *5. képen* látható ablakban tekinthetjük meg. Az ablakban az ***OK*** gombra kattintsunk.

Ekkor a beállításokat a rendszer a kapcsolat típusától függően

- ADSL-vonal estén a ***/etc/ppp/ip-up.local*** fájlba menti, és beszúr egy bejegyzést a parancsfájlba, ami a külső hálózatra csatlakozáskor hívódik meg;
- Más típusú kapcsolat esetén a ***/etc/ppp/ip-up*** fájlba menti, így az előbbi fájlt hívja meg, és a védelem kiépül. Mivel ezek a fájlok minden Internetre történő kapcsolódáskor végrehajtódnak, soha nem fogjuk elfelejteni bekapcsolni, és nem maradunk védtelenek. Érdemes lehet a már elkészített konfigurációt egy fájlba exportálni és későbbi használatra menteni.

- ***Logging***
  Ezen az oldalon a csomagszűrő naplózását állíthatjuk be, valamint a 2.4-es rendszemag lehetőségeit kihasználva korlátozhatjuk, hány csomagot szeretnénk fogadni.
- ***Advanced***
  Itt többek között az ***Export*** gomb segítségével a beállításokat szövegfájlba tudjuk menteni, amelynek mi adhatunk nevet, illetve az ezzel mentett beállítást az ***Import*** gombbal vissza is tudjuk olvasni. Ez a lehetőség akkor hasznos, ha a beállításokat menteni szeretnénk. Ezenkívül lehetőségünk nyílik rá, hogy a tűzfalat letiltsuk (***Disable firewall***), és az eredeti beállításokat visszaállítsuk (***Restore factory defaults***). Fontos még, hogy ha a címet DHCP-n keresztül önműködően kapjuk, be kell kapcsolnunk az ***Enable DHCP on interface*** négyzetet, ahol meg kell adnunk, hogy melyik az a hálózati csatoló, amelyiken a címet kapjuk. Ha a címkiosztást mi szeretnénk elérhetővé tenni az ügyfelek számára, a ***Enable DHCP server on interface*** négyzetet kell bejelölnünk, és hasonló módon megadnunk a csatolófelület nevét.



6. kép Rendezett, szép megjelenítés

Mint a fentiekből is látszik, ha tanult felhasználóinkat el akarjuk kápráztatni, kitűnő eszköz a Guarddog. Hasonló programokból nincs hiány, de ez a program tűnik a legalkalmasabb eszköznek, mert a felhasználók könnyen beállíthatják, és mi is könnyedén ellenőrizhetjük a beállításokat, ha a felhasználó elakad.

A versenytárs „termékek"

Nem a Guarddog azonban az egyetlen grafikus beállító csoda a szabad programok „piacán". Létezik még használható program erre a célra. Nézzük át, hogy melyek is ezek, és milyen előnyökkel, illetve hátrányokkal bírnak!

Firewall Builder

Második számú kedvencem, ha a felhasználókat arról kell meggyőznöm, hogy itt is van személyes tűzfal. Nagy előnye, hogy nemcsak a Linux csomagszűrőjét támogatja, hanem az `ipfilter`-t és az OpenBSD `pf`-jét is ismeri. A kezelőfelület GTK-ban lett megírva, ennek köszönhetően minden további nélkül fut Gnome és KDE alatt is. Felhasználási szerződése természetesen GPL. Másik nagy előnye, hogy a Debian-, illetve a Mandrake-terjesztés ezt a programot alapból tartalmazza. A beállításokat a formátumfüggetlenség jegyében XML-ben tárolja, a grafikus felület pedig a húzd és dobd szemlélet jegyében működik. A beállított szabályokat gyönyörű kivitelezésben láthatjuk.
➲ http://www.fwbuilder.org

gShieldConf

Ha nem a 2.4-es rendszermagot akarjuk használni, vagy azt használjuk, de valamilyen oknál fogva ragaszkodunk az IP Chainshez (a 2.2-es rendszermag csomagszűrője), akkor is létezik megoldás. Ez a gShield, illetve a gShiledConf, mely szintén moduláris felépítést alkalmaz – külön, saját láncok a szűréshez, feladattól vagy meghatározástól függő elnevezésekkel.
➲ http://members.shaw.ca/vhodges/gshieldconf.html

Deim Ágoston (ago@lsc.hu)
Kedveli a sört, szereti a futást és imádja Szabó Lőrinc verseit. Nem hisz vakon egyik rendszerben sem. Vonzódik a BSD-hez is. Tagja az LME-nek és a MBE-nek. Mottója: a gép nem lehet fontosabb az embernél.