A DansGuardian tartalomszűrő és a pehelysúlyú Tinyproxy összehangolása és beállítása

Amikor a *Microsoft* felhasználók kezdenek *Linux* operációs rendszert használni, különböző elvárásokkal érkeznek; például olyan tartalomszűrőt keresnek, mint amilyet *Microsoft Windows XP* alatt is használtak. A *Linuxra* áttérők gyakran az otthoni, különálló számítógépükkel kísérleteznek. Mivel a legtöbb ember arra használja számítógépét, hogy megfelelő információkat, képeket töltsön le az internetről, a tartalomszűrő rendszer használata kulcsfontosságú – különösen akkor, ha a szülők és a gyermekek közös számítógépet használnak, és a felnőtt felügyelet nem mindig megoldott. A *DansGuardian* és a *Tinyproxy* használatával a szülők távollétükben is felügyelhetik az internetes tartalmakat. A *DansGuardian* sokoldalú tartalomszűrő; nyílt forrású szoftver, amelyet alapértelmezett beállításaival nem kereskedelmi használatra szántak. A kereskedelmi változathoz szánt konfigurációhoz hozzájuthatunk a megfelelő licenc (vagy a *„SmoothGuardian”*) megvásárlásával. A *Tinyproxy* együttműködik a *DansGuardiannal* – ez egy kicsiny, nyílt forrású program, amely képes értelmezni és kiértékelni a számítógépen áthaladó információkat. E két eszköz együtt olyan adminisztratív felügyeleti lehetőséget biztosít, mellyel hatékonyan gátat lehet vetni a célba vett internetes tartalmaknak.

Tartalomszűrés 5000 láb magasból

A *DansGuardian* nem más, mint megadott szavak, mondatok és képek által megfogalmazott áthaladásgátlók együttese, melyek révén egyes weboldalak letilthatóak. A *DansGuardian* szűrői az internet és a böngészőprogram (például *Firefox*) közé illesztett programként működnek. A *Firefox* a weboldalak lekérését a *DansGuardianhoz* intézi, ami ezt a *Tinyproxynak* továbbítja – ez tartja a közvetlen kapcsolatot az internettel. Az internetről érkező adatcsomagok a *Tinyproxyn* és a *DansGuardianon* haladnak keresztül, mielőtt elérkeznének a böngészőklienshez. Természetesen csak a jóváhagyott információk jutnak át a szűrőkön és jelennek meg a böngészőablakban; tiltott weboldalak esetén a *DansGuardian* egy *„access denied” („hozzáférés megtagadva”)* képernyőt jelenít meg.
Mindez természetesen a szűrési folyamatnak csak egy meglehetősen vázlatos leírása. Valójában ennél sokkal összetettebb és érdekesebb a *DansGuardian* és a *Tinyproxy* együttműködése. Aki erre kíváncsi, látogasson el a *DansGuardian „folyamatábra”* oldalára (*„Flow of Events”*, lásd a cikkhez tartozó forrásokat). Itt egy mélyrehatóbb tanulmányt olvashatunk arról, hogy hogyan működnek ezek a szűrők, és hogy miként továbbítódnak az adatok a két program és az internet között.

Amit viszont fontos tudnunk: a *DansGuardiannak* megadható soksok tilalom alá eső szó, kifejezés, *URL*. A weboldalakon található szövegek vizsgálatán túl a *DansGuardian* még képek alapján is tud szűrni, és meg tudja gátolni bizonyos fájlok letöltését. Ez a szűrőmódszer kombináció sokkal hatékonyabb, mint az olyanok, amelyek csak a tilalomlistán levő *URL*-ek alapján korlátozzák a böngészést. Kezdő *Linux*-felhasználók számára először bonyolultnak tűnhet a *DansGuardian* húszegynéhány konfigurációs fájlja – azonban világos útmutatást kapunk, hogy miként kell őket igényeinkhez mérten megszerkeszteni. Próbálkozásaim során alig kellett változtatnom ezeken, mert az alapértelmezett szűrési beállítások szinte tökéletesen megfelelnek családi használatra.

A telepítés

Először a *DansGuardiant* és a *Tinyproxyt* kell telepíteni és beállítani. Ezt követően igen fontos lépés, hogy úgy állítsuk be az asztali környezetünket, hogy a normál felhasználók ne tudják egyszerűen kikapcsolni a tartalomszűrést.
Telepítés előtt érdemes megvizsgálni, hogy disztribúciónk tartalmazza-e a *DansGuardian* és *Tinyproxy* csomagokat. Néhány esetben a legegysze-

rűbb ezeket egy grafikus felületű csomagkezelővel, például a *Novell SUSE YaST* programjával vagy a *Synaptic*-kal feltelepíteni. Debian Linuxban elendő a a *root* felhasználó által kiadott

```
apt-get install dansguardian
➥tinyproxy
```

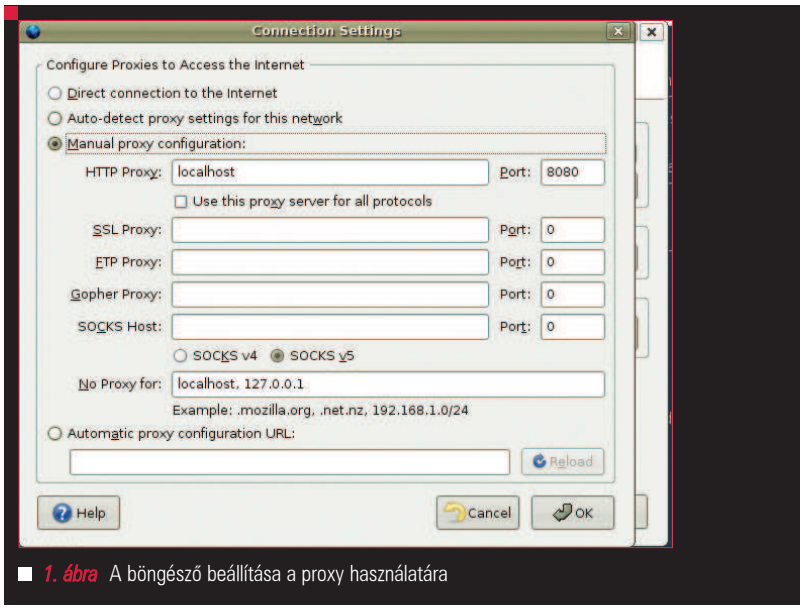
parancs.
Ha ezen programok bináris változatai netán mégsem lennének megtalálhatóak az adott disztribúcióban, le is lehet tölteni őket a megfelelő webhelyekről (lásd a cikkhez tartozó forrásokat). Letöltés után az *INSTALL* fájlban olvasható a telepítéshez szükséges eligazítás.

A DansGuardian és a Tinyproxy beállítása

Következő teendőnk a *DansGuardian* és a *Tinyproxy* konfigurációs fájljainak testre szabása. Tesztelési célokra *Ubuntu Dapper Drake*-et használok, így a könyvtárak és fájlnevek ezt a világot tükrözik. Nyilván más disztribúciók is többé-kevésbé hasonlóan szervezik fájljaikat; előfordulhat, hogy kicsit körül kell nézni, hogy hol is található a telepítési könyvtár. A jellemzők átszerkesztéséhez egy közönséges editor is elég, mint például a *GNOME gedit* programja.
Saját szerkesztőnkkel – root felhasználóként – nyissuk meg a */etc/dansguardian/dansguardian.conf* fájlt. Módosítsuk a *filterport*, a *proxyip* és a *proxyport* értékét az alábbiaknak megfelelően. Disztribúciónktól függően szükség lehet néhány `UNCONFIGURED` szóval kezdődő sor megjegyzéssé alakítására („kikommentezésére") a **#** jel segítségével.

```
# the port that DansGuardian
➥listens to.
filterport = 8080
# the ip of the proxy–default
➥is the loopback (this server)
proxyip = 127.0.0.1
# the port DansGuardian
➥connects to proxy on
proxyport = 3128
```

A *DansGuardian* általában a 3128-as portra kapcsolódik alapértelmezetten, mert ugyanezt a portot használja a méltán oly népszerű *Squid* proxy is.



1. ábra A böngésző beállítása a proxy használatára

Két utat választhatunk: vagy ezt az értéket állítsuk át a *Tinyproxy* által használt alapértelmezett portszámra (8888), vagy a *Tinyproxy* port értékét változtassuk meg a *DansGuardian* (azaz a *Squid* alapértelmezett port) értékére. Én ez utóbbit követtem.
A *Tinyproxy* testreszabásához – root felhasználóként – nyissuk meg szerkesztésre a */etc/tinyproxy/tinyproxy.conf* fájlt. Olvassuk végig, és győződjünk meg arról, hogy a *User, Group, Port* és *ViaProxyName* (*felhasználó, csoport, port, proxynkeresztül*) értékét szükséges-e megváltoztatnunk. Ha ezt az utat választjuk, akkor fontos, hogy a *Tinyproxy* port értékét módosítsuk úgy, hogy a *DansGuardian* által várt 3128-as portot használja:

```
# Port to listen on.
#
Port 3128
```

Ezek után egy terminálablakból adjunk ki egy

```
tinyproxy
```

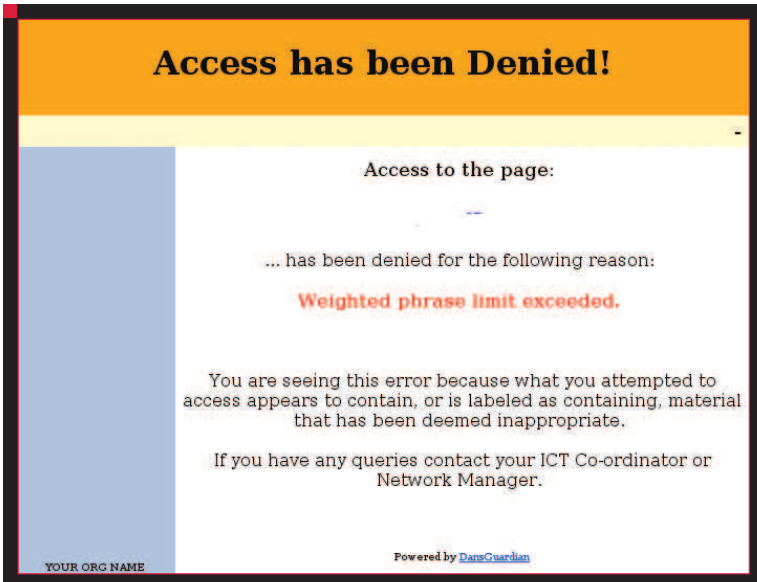
parancsot, vagy – *Debian* és *Ubuntu* alapú disztribúciók esetén – egy

```
sudo /etc/init.d/tinyproxy
➥start
```

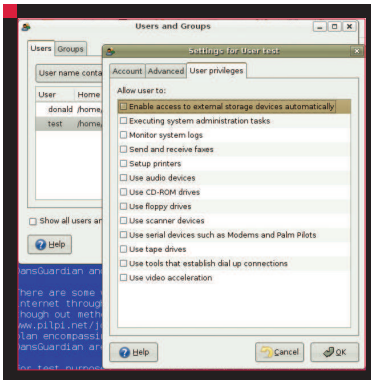
parancsot. Ez elindítja a proxyt, és innentől már csak a böngészőben kell beállítani egy-két dolgot a telepítés befejezéséhez. A fenti folyamat további tanulmányozásához érdemes átolvasni a *DansGuardian* dokumentációjának hivatkozásait (lásd a források közt).

A böngésző beállítása

Az *Ubuntu Linux* (és még néhány más disztribúció) a *Firefox* böngészőt ajánlja alapértelmezettnek, így az alább vázolt lépések is erre vonatkoznak. Nyilván a többi (összemérhető szintű) böngészőben is megvannak az ezzel analóg lehetőségek, amiket megtalálhatunk a megfelelő dokumentációban vagy a weben.
A telepítés ezen utolsó lépcsőfoka ráállítja a böngészőt a 8080-as port használatára, így ez csak a *DansGuardianon* és *Tinyproxyn* keresztül fog tudni adatokat küldeni. *Firefoxban* válasszuk a *Szerkesztés* menü | *Beállítások* almenü | *„Általános"* fül | *„Kapcsolat beállításai"* gombot. Az *1. ábrán* látható az ennek hatására kapott dialógusablak, valamint az is, hogy a „kézi proxybeállítás"-t miként lehet beállítani „localhost" *HTTP-proxy* és „8080"-as *port* értékre. Ez azt feltételezi, hogy a *DansGuardiant* és *Tinyproxyt* minden munkaállomáson használni fogjuk. Ha egy külön szerveren állítjuk be a *DansGuardiant* és *Tinyproxyt*, akkor a *HTTP-proxy* értékét értelemszerűen nem `localhost`-ra, hanem a *DansGuardiant* és *Tinyproxyt* futtató gép nevére vagy *IP*-címére kell állítani.



2. ábra Tipikus DansGuardian „hozzáférés megtagadva” oldal



3. ábra Ubuntu Dapper Drake felhasználói jogosultság-beállító

A böngésző újraindítása után ellenőrizhető, milyen jól működnek a szűrők. Egy-egy új szűrő kipróbálásakor a *2. ábrán* láthatóhoz hasonló, hozzáférést megtagadó képernyőt kell látnunk. Mielőtt továbblépnénk, érdemes körbejárni, milyen gondok adódhatnak az alapértelmezett beállítások miatt. Én pl. gyakran töltök le ***.tar*** és egyéb hasonló „végrehajtható” fájlokat. Az eredeti konfiguráció leállítja ezen fájlok letöltését. Ennek orvoslásához a ***bannedextensionlist.txt*** fájlt kell szerkeszteni; a sor elejére írt # jel által megjegyzésbe lehet tenni azon kiterjesztéseket, amiket át szeretnénk engedni a szűrőnkön.
Az érdeklődőbb olvasóknak azt javaslom, hogy rágják át magukat valamennyi ***DansGuardian*** konfigurációs ***.txt*** fájlon, hogy felelősségteljesen legyen testreszabva a szűrők működése. Nyilván nem lehet elképzelni az összes szituációt, amibe valaha is belefutunk, mégis, ez egy jó alkalom arra, hogy némileg belelássunk eme alkalmazás fantasztikus lehetőségeibe.

Sebezhetőségek

Nincs tökéletes rendszer. Van néhány nyilvánvaló megoldás, amellyel ki lehet játszani a ***DansGuardiant*** és a ***Tinyproxyt***; főleg, ha a felhasználók könnyedén ki tudják kapcsolni a proxyt és a szűrőket. Ha ezt nem akadályozzuk meg, akkor vissza lehet állítani a ***Firefox*** beállítási menüjében a közvetlen internetkapcsolatot, ami elkerüli a ***DansGuardian*** és ***Tinyproxy*** használatát. Innentől kezdve pedig korlátlan internetelérés áll a felhasználók rendelkezésére.
Van néhány módszer arra, hogy biztonságosabbá tegyük a ***DansGuardian*** szűrőit azáltal, hogy minden internetes adatáramlást a 8080-as porton kényszerítünk át. A ***DansGuardian*** webes dokumentációjában található egy hivatkozás, ami elmagyaráz egy remekül kigondolt módszert, amely a ***FireHol*** segítségével ezt a kényszerfeltételt minden internetes adatkapcsolatra érvényesíti (lásd a forrásokat).
A kezdő felhasználók készíthetnek egy egyszerűbb szűrési tervet is. Ez azon alapul, hogy vannak korlátozott jogosultságú felhasználók, akik számára rögzítünk bizonyos böngészőbeállításokat, valamint beállítjuk, hogy a számítógép bekapcsolásakor mindig elinduljanak a proxyszűrők.
Tesztelési célra készítettem egy új felhasználói azonosítót ***Ubuntu Dapper Drake***-et futtató számítógépemen (*3. ábra*). Bizonyos jellemzők megadásával szigorúan leszabályoztam eme felhasználó képességeit, oly módon, hogy ezek a jogosultságok azért bőven használhatóak legyenek bárki számára, aki nem különösebben járatos a számítógépes világban, vagy egyszerűen csak nem kellően megbízható. Az ***update-rc.d*** vagy ***fcconf*** segítségével meg lehet határozni, hogy mely programok induljanak el rendszerbetöltéskor. A magam részéről a ***BUM*** nevű programbetöltés-szervezőt használom a ***DansGuardian*** és a ***Tinyproxy*** elindítására.
Végül le kellett zárnom a ***Firefox*** beállításait. Ez nem olyan nagy feladat, mint amekkorának első hallásra tűnik. Olvastam egy részletes, régi (szerzői jogokkal védett) cikket ***Warren Togamitól*** (lásd a forrásokat) ***„Mozilla beállításlezárási HOGYAN LTSP Linux számára”***, (***„HOWTO Lock Down Mozilla Preferences for LTSP”***) címmel. Én azonban nem szeretnék mélyreható bitbuherálással zűrzavart teremteni, mikor ennek egyszerűbb módja is van. Miután beleástam magam a ➲ ***Mozilla.org*** weboldalának átolvasásába, arra jutottam, hogy elegendő egy ***lockPref*** utasítást beírni a ***Firefox*** konfigurációs fájljába ahhoz, hogy a felhasználók ne tudják megváltoztatni a kapcsolati beállításokat. Szerkeszteni kezdtem tehát a ***/usr/lib/firefox/firefox.cfg*** fájlt, ahogy az az *5. ábrán* is látszik. Az utolsó három sor kényszeríti ki a ***localhost*** kézi proxybeállítását a 8080-as portra.
E fájl elmentése és a ***Firefox*** újraindítása után már nem lehetséges a kapcsolati beállítások alapértelmezettre állítása. Természetesen megfelelő adminisztrátori jogosultság nélkül a felhasználók nem tudják ezeket a beállításokat átírva megkerülni a szűrőket.

Karbantartás

Miután ízlésünknek megfelelően testreszabtuk a szűrőket, fontos tudni, hogy bizonyos beállítások

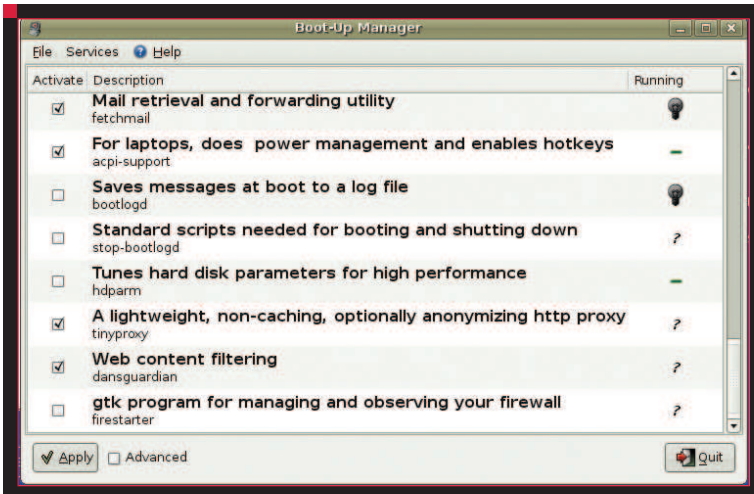
elévülhetnek. Egyes tiltott webhelyek és kifejezések hamarabb, mások később mennek ki a „divatból”. Gyakran új weboldalak jelennek meg, és bizonyos szókapcsolatok a régiek helyébe lépnek. A *DansGuardian* webhelyén van egy *„Extras” („Egyebek”)* hivatkozás, ahol a feketelistára tett oldalakról további információk olvashatók. Ráadásul találhatunk olyan szkripteket is, melyeket áldozatkész felhasználók azért publikáltak, hogy automatizálni lehessen velük a feketelisták készítését és naprakészen tartását.

Egy másik alternatíva az ➲ *URLblacklist.com* használata, mely az új felhasználók számára az első letöltést ingyenesen lehetővé teszi. Ha ez megtetszik, elő lehet fizetni a további remek frissítésekre. Ezeknek az adatoknak a *DansGuardian* számára való átalakítása megtalálható a weben. Érdemes figyelni, hogy a proxy és a szűrők mennyire lassítják a szörfözést, az oldalak betöltődését. Lehetnek helyzetek, amikor a felhasználóknak el kell viselniük bizonyos mértékű teljesítményromlást a *Tinyproxy* használatakor. Saját kísérletezéseim során észleltem némi késést, valamint néhány új tételt a böngésző gyorstárában. A *Firefox* gyorstárának *Ctrl-Shift-Del* gombkombinációval való törlése azonban rögtön orvosolta ezt a problémát. Előfordulhat, hogy szükséges lehet a *Tinyproxy* újraindítása az internetelérés sebességének növeléséhez. Ezek kissé zavaróak, mégis elfogadható kompromisszumot jelenthetnek a hétköznapi munka során.

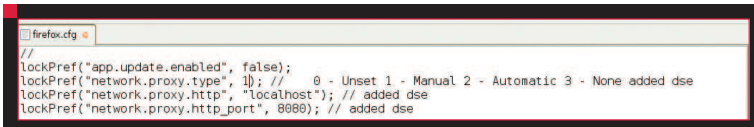
A naplófájlok áttekintése

Mind a *DansGuardian*, mind a *Tinyproxy* készít naplófájlokat, melyeket az adminisztrátornak célszerű időnként átnéznie. A */var/log*-on belül készül egy-egy könyvtár a *DansGuardian* és a *Tinyproxy* számára. Egy egyszerű editorral megnyitva a megfelelő fájlokat érdemes átpásztázni az adatokat, hogy tudjuk, mi történt a számítógépen. Az egymás utáni sorokban tárolt információk és világos megjegyzések teszik egyszerűbbé az események megértését.

A *DansGuardianhoz* készített valaki egy olyan szkriptet is, amivel a keresés és az adatok kijelzése sokkal inkább felhasználóbarát formátumban valósítható meg.



4. ábra A DansGuardian és a Tinyproxy beállítása – bootoláskor induljanak el



5. ábra A Firefox beállításainak lelakatolása – adminisztrátori jogosultság nélkül ezek nem változtathatóak meg

Sajnos a *DansGuardianból* hiányzik az a lehetőség, hogy e-mailben is elküldje a naplófájlokat (*ám ez könnyedén megoldható például a* cron *segítségével – a ford.*). Erős motiváció lehet bizonyos felhasználók viselkedésének kordában tartására az a tudat, hogy egy felelős ember időnként átvizsgálja az internetes tevékenységüket.

Záró gondolatok

Mielőtt döntést hozunk a tartalomszűrés fent vázolt technikai megvalósításáról, fontoljuk meg, milyen igényeket szeretnénk megvalósítani az elkövetkező hónapokban. Ha csak egyetlen számítógépről van szó, és szívesen bütyköl valaki konfigurációs fájlokat, akkor a *DansGuardian* valószínűleg jó választás. Azonban a *SmoothGuardian* is jó vásárnak tűnik a maga 90 dolláros árával. A szoftver felhasználóbarát webes kezelőfelületet és egy egyszerűsített telepítőt is tartalmaz. Mindamellett a *DansGuardian* és *Tinyproxy* beállítása egyáltalán nem mutat túl még a kezdő *Linux*-felhasználók képességein sem, és az ingyenes hozzájutás a legtöbb költségvetésben jól fest. Eme cikk és a megadott hivatkozások segítségével valószínűleg nem lesz probléma a telepítéssel és futtatással. Ha valami akadály fel is bukkanna, a *Google*-n bizonyára könnyen megtaláljuk a megoldást.

A *DansGuardian* honlapján (lásd a forrásokat) hivatkozás látható egy webes tartalomszűrési portálra, valamint egy témába vágó *IRC* csevegőhelyre is. Általánosságban elmondható, hogy a *DansGuardian* és a *Tinyproxy* a szabad szoftveres világ élharcosai – segítik az átállást a *Microsoft Windows* környezetből. Megítélésem szerint a rugalmas szűrőfeltételek megadásának lehetősége és a pehelysúlyú proxyterhelés jó választássá teszi e két program kombinációját kisebb hálózatokon.

Linux Journal 2006., 151. szám

Donald Emmack vezetőségi tag a The IntelliGents & Co. cégnél. Kiterjedt munkát végez íróként és üzleti tanácsadóként Észak-Amerikában. Elérhető a donald@theintelligents.com e-mail címen vagy a 2 méteres amatőr rádiócsatornákon.

A cikk forrásai

➲ www.linuxjournal.com/article/9291