# A legjobb biztonsági rendszer... ugat!

Hála az égnek, a Guarddog nagyobbat harap, mint amilyen hangosan ugat.

Nem, ***François***, nem tűnt fel, hogy valami baj lenne az internet-kapcsolattal. Ja, értem, szóval új tűzfalat telepítettél, ami most nem enged ki. Hm, lássuk csak a beállításokat. Azt hiszem, tudom, mi a gond, ***mon ami***. A beállítások rendkívül szigorúak, viszont kiváló biztonságot nyújtanak. Semmi nem juthat be, de semmi sem jut ki. Tökéletesen biztonságos.

Igen, ***François***, csak vicceltem.

Ha a biztonságról van szó, mindenki túlzó hasonlatokat használ. Egyszer azt hallottam, hogy egy kiszolgálót úgy lehet a legbiztonságosabbá tenni, ha kihúzzuk, és a szekrénybe zárjuk. Ha már viccelődünk, miért ne menjünk tovább? Öntsük betonba a kiszolgálót, és temessük egy 15 méter mélyen fekvő, ólommal bélelt pincébe. A tréfát félretéve, ***mon ami***, meg kell találni a helyes egyensúlyt az elfogadható biztonság és a teljességgel használhatatlan rendszer között. Ez szerepel a mai étlapon, és amikor a vendégeink végre megérkeznek, felszolgálunk néhány tetszetős tűzfal-alkalmazást.

De már itt is vannak, ***François***. Mindenkit üdvözlünk ***Marcelnál***, ahol a remek ***Linux*** fogások és a kitűnő borok tökéletes harmóniát alkotnak. Hűséges pincérem az asztalhoz kíséri önöket, utána pedig behozza a bort. A 2002-es ***Sonoma Belle Glos Pinot Noir*** remekül hangzik – azt hiszem, ***François***, az északi szárnyban találod meg, ***Henri*** éppen ott tölti fel a készletet.

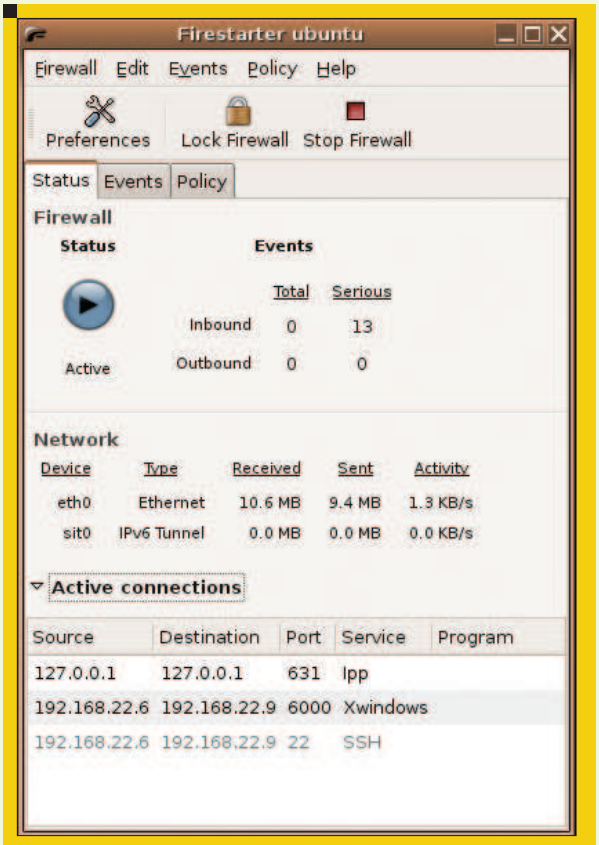
A ***Linuxot*** forgalmazó csoportok általában biztosítanak valamilyen tűzfalat a terjesztéshez, de nem mindegyik. Ezeket rendes estben a gyártó által rendelkezésre bocsátott rendszervezérlő eszközön keresztül érhetjük el. Időnként a tűzfal eszközök lényegében a parancssori ***iptables*** programok. Semmi gond nincs azzal, ha kizárólag a parancssor alkalmazásával húzunk fel tűzfalat, de sokan vannak, akik nagyon szívesen fogadnak egy kis irányított, egyszerűsített, grafikus segítséget. A ma tárgyalt tűzfalépítők az egyszerű használhatóság és beállíthatóság mellett rendelkeznek még egy előnnyel: mindkettő lehetővé teszi a tűzfal valósidejű módosítását. Mindegyik nagyon szigorú beállításokat alkalmaz a bejövő forgalomra (minden adatcsere tiltott, hacsak nem engedélyezik kifejezetten), továbbá nem terjesztésfüggők.

Ha úgy döntünk, hogy terjesztést váltunk, használhatjuk ugyanazokat az eszközöket.

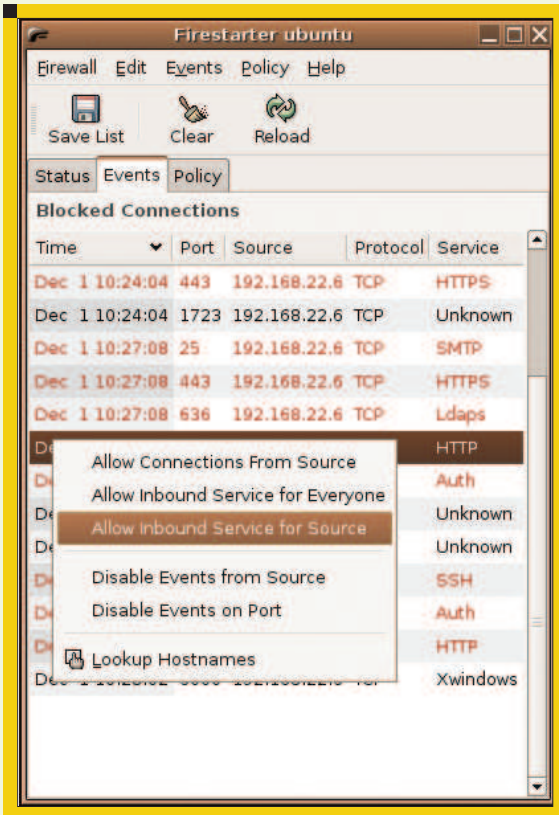
***François***, jó, hogy visszatértél. Kérlek, tölts a vendégeinknek!

A mai első fogás ***Thomas Junnon*** kitűnő ***Firestarter*** alkalmazása, egy könnyen használható, grafikus tűzfalprogram, amely lehetővé teszi a biztonsági szabályok valósidejű válaszát és beállítását. A ***Firestarter*** futtatásakor (parancsnév, ***firestarter***), meg kell adnunk a fő jelszót. Az első futtatáskor a program elindít egy tűzfalvarázslót (***Firewall Wizard***), amely segít a kezdeteknél. Mivel az első képernyő gyakorlatilag csak egy üdvözlés, olvassuk el az üzenetet, majd a ***Forward (Tovább)*** gombra kattintva lépjünk tovább.

Ezután az internet-kapcsolat megosztását kezelő képernyőre jutunk. Az egyfelhasználós gépeknél nem kell emiatt aggódnunk, egyszerűen továbbléphetünk a következő képernyőre. Ha azonban az otthoni vagy az irodai ***PC*** más ***PC***-k ***NAT*** (címfordító) átjárójaként szolgál, kattintsunk az ***Enable Internet connection sharing (Internet-kapcsolat megosztásának engedélyezése)*** jelölőnégyzetre. Ismét megadhatjuk, hogy alapértelmezésben milyen ***Ethernet*** kártyát (vagy telefonos kapcsolatot) használunk az internethez való csatlakozáskor. Közvetlenül ezalatt ***DHCP*** kiszolgálón keresztül adhatunk meg címeket. Ha a rendszeren nem telepítettünk ***DHCP*** kiszolgálócsomagot, ez a lehetőség szürkén jelenik meg.




*1. ábra* A Firestarter felülete világos és könnyen kezelhető




*2. ábra* A Firestarter Events lapján folyamatosan lehet létrehozni a forgalmat engedélyező szabályokat

A beállítások elvégzése után kattintsunk a ***Forward*** gombra, és tulajdonképpen végeztünk is a varázslóval. Mielőtt a ***Save (Mentés)*** és a ***Quit (Kilépés)*** gombra kattintanánk, nézzük meg figyelmesen a képernyőt. Észrevehetjük a ***Start firewall now (Tűzfal azonnali indítása)*** gombot, amely eleve ki van pipálva. A varázsló által létrehozott alapértelmezés szerint a ***Firestarter*** szabályai meglehetősen korlátozzák a bejövő forgalmat (ahogy ezt elvárnánk), és ez általában nem jelent problémát. Ahogy azonban a képernyőn megjelenő tipp is tájékoztat, ha távolról végezzük a telepítést, ez gondot okozhat.

Ha nem a szóban forgó munkaállomásnál ülünk, kapcsoljuk ki az azonnali indítás lehetőségét. Készen is vagyunk. Kattintsunk a ***Save*** gombra, és a ***Firestarter*** élesíti az új tűzfalat, valamint megjeleníti az állapotablakot (*1. ábra*).

A kezelőfelület egyszerű, három lapból áll. A lapok címkéje ***Status (Állapot)***, ***Events (Események)*** és ***Policy (Szabályok)***. Az állapotnézet az, amelyik nagy valószínűséggel rendszeresen érdekelhet bennünket. A kijelző megjeleníti a tűzfal futásának állapotát (***Active – Aktív vagy Disabled – Kikapcsolt***), a bejövő és kimenő kapcsolatokat, valamint a különböző felületeken keresztül zajló forgalmat. Az ablak alján található ***Active connections (Élő kapcsolatok)*** rész alaphelyzetben be van zárva. A címke melletti nyílra kattintva megtekinthetjük ezeket a kapcsolatokat.

Ki kell emelni, hogy a ***Firestarter*** először minden elképzelhető bejövő szolgáltatást kizár. Ennek következményeként, ha nem az asztali számítógépen, hanem a kiszolgálón futtatjuk, azt tapasztaljuk, hogy senki semmit nem tud majd futtatni, még a ***biztonságosnak*** gondolt szolgáltatásokat sem, például a webkiszolgálót. Ennek ellenére minden kimenő forgalom megengedett, tehát ez nem érinti a hagyományos asztali szolgáltatásokat, vagyis az e-mail olvasást, a webes böngészést és az ***IM*** (azonnali üzenetküldő) ügyfelekkel történő csevegést. A fent említett ***Active connections*** ablak azonnal megjeleníti a kapcsolódási kísérleteket, de ezek pár másodperc múlva elhalványodnak és eltűnnek.

Az ***Events*** lapra kattintva megtudhatjuk, milyen kapcsolódási események történtek, így eldönthetjük, hogy melyiket engedjük be. Itt megtaláljuk a számítógép teljes forgalmának naplóját (*2. ábra*).

Ha a jobb gombbal valamelyik bejegyzésre kattintunk, megjelenik egy felugró menü a kapcsolatokra vonatkozó lehetőségekkel. Amennyiben például a 80-as kapu (***HTTP*** szolgáltatás) egy eseményéről van szó, érdemes bejelölni az ***Allow inbound Service for Everyone (Belső szolgáltatás engedélyezése mindenki számára)*** lehetőséget. Más a helyzet viszont a 22-es kapun érkező biztonságos héjszolgáltatás (***secure shell***) kapcsolattal, amelynél csak az ***Allow inbound Service for Source (Beérkező szolgáltatás engedélyezése a forrás számára)*** jelölőnégyzetet pipáljuk ki. Egy adott ***IP*** cím (például egy belső hálózaton található

PC) engedélyezéséhez válasszuk az ***Allow Connections From Source (Forrástól érkező kapcsolatok engedélyezése)*** lehetőséget. Azt is megtehetjük, hogy egy adott gazdagép, kapuszám vagy szolgáltatás kapcsolatait nem naplózzuk.

Én személy szerint nem hiszem, hogy a rendszergazdák először megnézik, ki kopog, és csak azután engednek bizonyos szolgáltatásokat a rendszerb. Aki webkiszolgálót üzemeltet, annak valószínűleg előnyösebb, ha engedélyezi a 80-as kaput. Ugyanez az elv érvényes akkor, ha egy ***Samba*** kiszolgálón engedélyeznünk kell, hogy az irodában dolgozók hozzáférjenek a kiszolgálón tárolt megosztásokhoz. A ***Policy*** lapra kattintva elkerülhetjük, hogy a bekövetkezésük pillanatában kelljen kezelni az eseményeket. Ez az ablak két vízszintes részre vagy táblára van osztva.

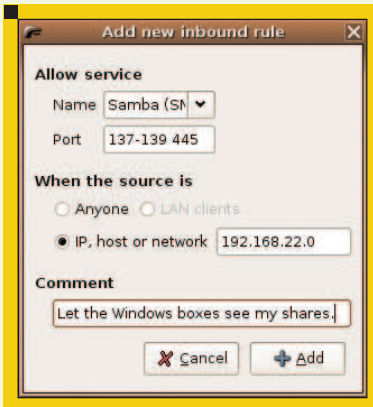
A felső egy adott gazdagép vagy gazdagép-csoport általános kapcsolatait kezeli, az alsó tábla pedig az egyes szolgáltatásokkal illetve azokkal a kapukkal foglalkozik, amelyeken ezek a szolgáltatások futnak. Az ***Events*** lapon hozzáadott szolgáltatások itt jelennek meg. Ha úgy akarunk további szabályokat hozzáadni, hogy ne kelljen végiglépkedni az ***Events*** párbeszédablakon, kattintsunk a jobb gombbal a felső vagy az alsó táblára, majd a felugró menüben válasszuk az ***Add rule (Szabály hozzáadása)*** lehetőséget. Megjelenik egy kis barátságos párbeszédablak, amely megkönnyíti a folyamatot (*3. ábra*).

Adjunk hozzá egy olyan szabályt, ami engedélyezi a helyi hálózatra csatlakozó ***PC*** számára, hogy elérje a ***Samba*** szolgáltatást. A párbeszédablak tetején szerepel egy lenyíló lista, amely a lehetséges szolgáltatásokat tartalmazza (például ***DHCP***, ***BitTorrent***, ***IMAP*** és a többi). Én a ***Sambát (SMB)*** választom a listából. Észrevehetjük, hogy az ismert szolgáltatásoknál a kapu (vagy kapuk) mezője automatikusan kitöltődik. Ezután a ***When the source is (Amikor a forrás...)*** címke alatti választógombbal engedélyezhetjük az összes kapcsolatot, illetve egy meghatározott gazdagépet vagy hálózatot. Ebben az esetben a saját ***C*** osztályú hálózatomat állítom be. Végül, a lent szereplő mezőben valamilyen megjegyzést is hozzáadhatunk. Kattintsunk az ***Add (Hozzáadás)*** gombra, és készen is vagyunk. Az új szabály megjelenik a ***Policy*** ablakban. Kattintsunk a ***Firestarter*** fő ablakának tetején található ***Apply Policy (Szabály alkalmazása)*** gombra az új szabály érvényesítéséhez.

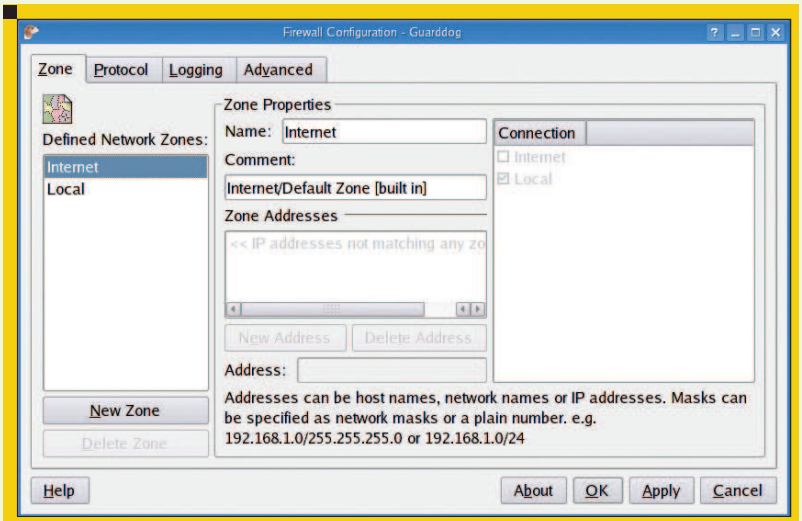
A most létrehozott szabályokhoz mellesleg a ***Firestarternek*** nem feltétlenül kell futnia. A program az */etc/rc.firewall* fájlban tárolja a tűzfal adatait. Mivel ez egy indítás szintű parancsfájl, valahányszor újraindítjuk a rendszert, a tűzfal már futni fog.

Itt a kiváló alkalom, hogy kis szünetet tartsunk és lazítsunk, amíg ***François*** mindenki poharát újratölti. Ezalatt hadd meséljek el még egy bölcseletet a biztonsággal kapcsolatban. Sok évvel ezelőtt valaki azt mondta, hogy a lehető legjobb biztonsági riasztórendszer, amit egy házhoz beszerezhetünk, az a kutya. Azt mondták, felejtsem el a csillogó elektronikus ketyeréket, és vegyek magamnak egy nagy német juhászt. Valószínűleg ez a gondolat sugallta a mai étrend második fogását. ***Simon Edwards Guarddog (Őrkutya)*** programja egy grafikus tűzfalbeállító eszköz, amely kutya biztonságossá teszi a ***Linux*** rendszert. A ***Guarddog*** az asztali számítógépeken nagyszerű, viszont még a bonyolult kiszolgáló összeállításokon is ideális eszköz.

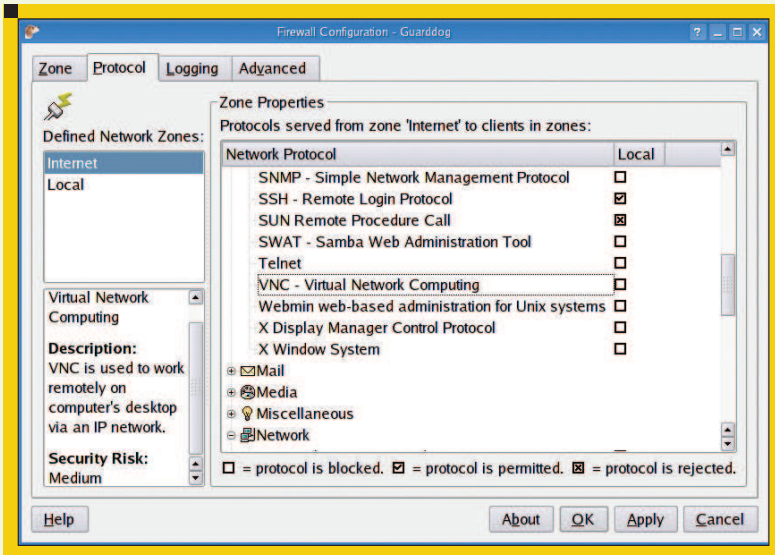
Mielőtt bemutatnám a ***Guarddogot***, ki kell emelni, hogy nem rendszergazdaként is futtatható, viszont a végrehajtott változtatásokat nem lehet menteni. Ez azért van, mert a tűzfal szabályainak megváltoztatásához rendszergazda hozzáférés szükséges. Egyértelműen jobb, ha rendszergazdaként futtatjuk az alkalmazást, kivéve, természetesen, ha előbb el szeretnénk sajátítani a működését. Ez hasznos lehet; nemsokára elmondom, miért. Még valamire fel szeretném hívni a figyelmet. A ***Guarddog*** a */etc/rc.firewall*-ban tárolja a tűzfalszabályokat, és így lehetséges (bár nem valószínű), hogy ezen a helyen már létezik egy fájl. Ebben az a furcsa (és talán egy kicsit mulatságos), hogy a ***Guarddog*** egy ilyen nevű fájlt telepít, és lehet, hogy induláskor beleütközik. Ez nem túl nagy gond, de ha erre utaló üzenetet látunk, jó, ha tudjuk, hogy valószínűleg minden




***3. ábra*** Bejövő forgalomra vonatkozó szabály hozzáadása a Firestarterrel




***4. ábra*** A Guarddog tűzfal program fő ablaka




**5. ábra** A Guarddog protokollokat egyetlen egérkattintással tilthatjuk, engedélyezhetjük vagy visszautasíthatjuk

rendben van. Adjuk meg a rendszergazda jelszót, és indítsuk a programot úgy, hogy teljes hozzáféréssel rendelkezik a tűzfalhoz.

A ***Guarddog*** fő kezelőfelülete négy lapból áll, amelyek ***Zone (Tartomány)***, ***Protocol (Protokoll)***, ***Logging (Naplózás)*** és ***Advanced (További beállítások)*** címkével rendelkeznek (*4. ábra*).

A ***Zone*** lapon két előre meghatározott tartomány szerepel. A ***Local (Helyi)*** a helyi címhez érkező forgalmat jelöli, az internet pedig a rendszert elhagyó, az internetre irányuló forgalmat. Ez nagyon fontos. A ***Guarddog*** a semleges terület (***Demilitarized Zone – DMZ***) beállítások, különböző kártyák és ehhez hasonlók alkalmazásával viszonylag könnyűvé teszi a bonyolult tűzfalak létrehozását. Egyelőre összpontosítsunk az alapvető asztali tűzfalbeállításra, ami egy internetre kapcsolódó gép.

Ahogy elindítjuk a ***Guarddogot*** (parancsnév guarddog) és az ***Apply (Alkalmazás)*** gombra kattintunk, azonnal működésbe lép a tűzfal, és minden bejövő illetve kimenő forgalmat visszatart. Ez egy erősen korlátozó beállítás, ezért nagy biztonságban vagyunk. Talán egy túlságosan is: semmi sem jut ki vagy be – ez az egyik nyomós érv, amiért érdemes először nem rendszergazdaként kísérletezni. Ez nem olyan furcsa, mint amilyennek először tűnik. A ***DMZ***-ben található rendszerek összetettebb tűzfalait, rendszerint kizárják a belső hálózatról, és csak néhány külső szolgáltatást kapcsolnak be. Ha túlságosan védett területre kerülnénk, kattintsunk az ***Advanced*** lapra, majd pipáljuk ki a bal felső sarokban szereplő ***Disable firewall (Tűzfal kikapcsolása)*** jelölőnégyzetet, ezután pedig kattintsunk a jobb alsó sarokban található ***Apply*** gombra. Szintén az ***Advanced*** lapon található az a gomb, amellyel visszatérhetünk a ***Guarddog*** alapértelmezett, mindent tiltó gyári beállításaihoz.

Így vagy úgy, engedélyeznünk kell bizonyos forgalmat. Kattintsunk a ***Protocol*** lapra, és megjelenik a különböző forgalomtípusokat képviselő kategóriák listája: ***Chat (Csevegés)***, ***Data Serve (Adatszolgáltatás)***, ***File Transfer (Fájltovábbítás)***, ***Game (Játék)***, ***Interactive Session (Interaktív munkamenet)***, ***Mail (Levelezés)***, ***Media (Média)***, ***Miscellaneous (Vegyes)***, ***Network (Hálózat)*** és ***User Defined (Felhasználói beállítás)***.

Minden kategória mellett látható egy plusz jel, az önálló protokollok pedig almenükben jelennek meg. Kattintsunk az egyes protokollokra, és a bal alsó táblában megjelenik a rövid leírásuk, valamint az általuk képviselt biztonsági kockázat becsült mértéke.

A protokollok neve mellett egy-egy jelölőnégyzet látható, amelyekre kattintva letilthatjuk, engedélyezhetjük vagy visszautasíthatjuk az adott protokollt (*5. ábra*). Ahogy korábban említettem, a kapu alaphelyzetben tiltott. Egyszer kattintva engedélyezzük a protokollt, ha pedig újból kattintunk, visszautasítjuk a csomagot.

A tűzfal korlátozó jellegét tekintve először végignéztem az internet tartomány protokolljait, és engedélyeztem mindent, ami szükséges (például azonnali üzenetküldés, e-mail, webböngészés és így tovább). Ezekre van szükség egy olyan asztali munkaállomáson, ahol lényegében minden kimenő forgalom engedélyezett.

A változtatások elvégzése után kattintsunk a fő ablak alján található ***Apply*** gombra az új tűzfalbeállítás érvényesítéséhez. Egy kis felugró ablak figyelmeztet, hogy a működő tűzfalon végrehajtott módosítások hatással lehetnek a meglévő kapcsolatokra. Kattintsunk a ***Continue (Folytatás)*** gombra a tűzfal újbóli élesítéséhez.

Ha valamilyen kiszolgálót működtetünk (például ***Samba*** fájlmegosztást), szinte hallhatjuk a kedves kiskutya morgását, ugye? Esetleg biztonságos héjszolgáltatás (***SSH***) is fut annak érdekében, hogy ezt a gépet egy másik, otthoni vagy irodai számítógépről elérhessük. Kattintsunk a ***Local*** tartományra, és válasszuk ki azokat a protokollokat, amelyekkel forgalmat bonyolítunk. Ne feledjük, hogy ez most bejövő forgalom, tehát nem szabad túl nagylelkűnek lenni.

Ha már erről van szó, attól tartok, nemsokára záróra. Azért nem kell sietni. Hűséges pincérem, ***François*** szívesen újratölti a poharukat még utoljára, mielőtt elbúcsúznánk. Kérem, emeljék magasra a poharat, ***mes amis***, és igyunk egymás egészségére.

A ***votré Santé! Bon appétit!***

*Linux Journal 2006., 143. szám*

***Marcel Gagné***
(mggagne@salmar.com)
Mississaguában, Ontario államban él.
Ő a szerzője a Kiskapu kiadásában tavaly szeptemberben megjelent Linux-rendszerfelügyelet (ISBN 96-9301-40) című könyvnek.

## A CIKK FORRÁSAI

➲ www.linuxjournal.com/article/8745