IPCop
a hálózsaru

Szolgál és véd, ráadásul megoszt és felügyel is. Könnyen és gyorsan telepíthető – jó, jó, tudom, most majdnem mindegyik disztribúció ezt hangoztatja.. – speciális Linux változat az IPCop, s legfőbb célja tűzfalként védeni az internet felé és felől irányuló forgalmat, valamint igény esetén útválasztóként is tud üzemelni. Bővíthetősége kiváló, s csekély hardverigényéhez viszonyított rugalmas paraméterezhetősége miatt jó alternatívája lehet egy hardveres tűzfal/router eszköznek.

A tűzfalépítés alapanyagai

Hozzávalók: 1 db számítógép 2 db hálókártyával, 1 db *IPCop Linux*, 1 db eszköz az internet hozzáféréshez (például modem), 1 db switch és egyenes patchkábelek ha több gépet akarunk csatlakoztatni (ha csak egyet, akkor elég egy crosslink kábel, és a switch sem szükséges).
Végy egy számítógépet, de még jobb, ha leporolod a sarokban porosodó, elavultnak hitt konfigurációdat. Már egy *Pentium 1* kategóriájú (türelmesebbeknek akár 486-os is) is megteszi, de az se keseredjen el, akinek „csak” egy alfaprocesszoros gépe pihen használaton kívül, ezen is fut a szerzők szerint.
Ha kicsit többre vágyunk, például betörésdetektáló szolgáltatásra, akkor az ajánlott minimum körülbelül egy *Pentium II* tudású gép, legalább 64 MB RAM-mal, és körülbelül 1 GB merevlemezzel. Internetkapcsolatunktól függ, de általában két hálózati kártya elegendő ahhoz, hogy a belső hálózat felé meg tudjunk osztani például egy *ADSL* vagy kábeles kapcsolatot. Ez a roppant olcsó konfiguráció az árához képest sok segítséget tud nyújtani nekünk, néhány ezek közül:

- Tűzfal
- Útválasztó (router)
- Betörésdetektálás
- *DHCP* szerver (és kliens)
- Proxyszerver
- *DNS* gyorsítótár
- *VPN*
- forgalomtervezés, illetve *QoS*

Ne ijedjünk meg, ha nem mindegyik fogalommal vagyunk tisztában, ezek egy részét utólag lehet hozzáadni rendszerünkhöz, s kezdetben célunk pusztán egy internetmegosztásra is képes, védett kapcsolatot biztosító *Linux* üzembe helyezése.

Még két dolog szükséges a kapcsolathoz: az internetszolgáltatás eléréséhez tartozó hardvereszköz (például *ISDN*-kártya, kábelmodem stb.), valamint maga az *IPCop*. Utóbbit a ➲ *http://www.ipcop.org/* címről kiindulva tölthetjük le, körülbelül 40 megabájt lemezre mentésével. Ügyeljünk arra, hogy éles használatra ne bétaverziót szerezzünk be, hanem valamely újabb stabil változatot, például az 1.4.10-et.

Alapelvek

Az *IPCop* négy elkülönülő részre osztja a hálózati kapcsolatokat, tipikusan:

- *GREEN* interfész: általában a védendő saját belső hálózatunkat (ami lehet akár egy darab számítógép is) jelenti
- *RED* interfész: általában ő az internetkapcsolat, azaz a biztonsági szempontból legmegbízhatatlanabb kapcsolat

- *BLUE* interfész: az egyre népszerűbb vezeték nélküli (*WI-FI*) kapcsolatokat lehet bevonni a felügyelt rendszerbe
- *ORANGE* interfész: az ún. demilitarizált zóna (*DMZ*) eszközeit tartalmazza, azaz olyan szervereket és szolgáltatásokat, melyek internet felől is láthatók részben (például a honlapunkat üzemeltető saját webszerver, vagy a levelezőszerver), de védelmet igényelnek

Ezek közül minimálisan a *RED* és a *GREEN* konfigurálása szükséges ahhoz, hogy a védendő belső hálózat gépei kijussanak az internetre. Egy tipikus, kisebb irodai hálózat igényeit kielégíteni képes *DSL* vagy kábeles elérés esetén két hálózati kártya kell a gépbe: az egyik a *GREEN* interfész lesz, és a belső hálózat felé biztosítja az internetet, míg a másik a *RED* interfész, mely közvetlenül a szolgáltató által biztosított hardvereszközhöz csatlakozik (kábelmodem vagy *ADSL*-modem).
Ahhoz, hogy a tűzfal valóban védjen is, külön „alhálózatokat" (lásd később) kell képeznünk a különböző interfészekhez, és az internettel közvetlen kapcsolatban álló *RED* eszköz lesz az átjáró a belső hálózat gépei és az internetet biztosító szolgáltató fogadógépe között.

Praktikák

A tűzfalgép valójában egy 24 órás működésre tervezett szerverként kell funkcionáljon, ezért érdemes úgy beállítani, hogy a leginkább hibatűrő módon tudja feladatát ellátni. Ha lehetőség van rá, kapcsoljuk ki az energiatakarékos funkciókat a *BIOS*-ban. Állítsuk be, hogy automatikusan újrainduljon a gép – így például egy áramszünet után jó eséllyel magához tér külső beavatkozás nélkül is. Ha csak távolról szeretnénk adminisztrálni, akkor a billentyűzet, egér és monitor is eltávolítható, de ezeket is be kell állítani a *BIOS*-ban, nehogy hiánya miatt hibaüzenettel megálljon indításkor maga a számítógép. Telepítés után mindenképp javasolt a floppyról indítás lehetőségét megszüntetni, ugyanis biztonsági mentéseket írhatunk floppylemezre, s elég kellemetlen, ha egy bent felejtett lemez miatt nem indul el legközelebb a számítógép.
Azokat az eszközöket is nyugodtan letilthatjuk, melyekre nincs szükség – például hangkártya, *USB* portok – általában ezek nélkül vígan elvan a rendszer. Ugyanez igaz szoftveresen is, bár az *IPCop* disztribúciók többnyire eleve nélkülözik a szükségtelen és biztonsági szempontból kifogásolható csomagokat, viszont utólag különböző kiegészítők hozzáadásával saját magunk sokat ronthatunk az egyébként jól kialakított rendszer megbízhatóságán.
Elszántabbak akár teljesen csendes verzióját is használhatják, hiszen a dokumentációban olvasható egy leírás a merevlemez helyett *CF* memóriakártyáról futni képes *IPCopról*. Azonban ebben az esetben ne akarjuk az eredeti felépítésben szereplő verziót futtatni, hiszen a naplófájlok, a */var*, */tmp* stb. könyvtárak sűrű írási műveleteket igényelnek, ez pedig hamar tönkreteheti a flashmemóriát. Nézzük meg inkább a leírásban említett héjprogramot, és olvassuk el a szükséges segítséget a használathoz, hogy a fizikai memória közbeiktatásával elkerülhetőek legyenek ezek a problémák.

(Tűz)falazás előtti tudnivalók

Egy alapfunkciókkal már jól működő *IPCop* feltelepítése fájdalommentes és gyors az esetek többségében, még akkor is, ha nincs nagy tapasztalatunk *Linuxszal*. Ehhez mindössze a következő információkat kell előre megtudnunk:

- Állandó *IP* címet kaptunk-e az internetszolgáltatónktól, és ha igen, mi ez a cím, illetve mi a *DNS*-szerver(ek) *IP* címe. Általában ha ezt nem igényeltük külön, akkor változó címet kapunk, ekkor viszont a szolgáltató dinamikus *IP*-címeket kiosztó szerverének (*DHCP*) címére lesz majd szükségünk a beállításokhoz.
- Milyen típusú elérésünk van? Az *IPCop* szempontjából a következő négy protokoll és technikai megoldás közül kell választanunk majd: *PPoE*, *PPTP*, *DHCP*-vel kiosztott cím, vagy statikus *IP* cím.
- A hálózati kártyák típusa, ami elsődlegesen a rajtuk lévő chip fajtáját (például *Realtek RTL8169*), s nem a kártya gyártói fantázianevét (például *Ovislink GE-2032R*) jelenti.

Ha működő gépről kell megszerezni ezeket az adatokat, akkor a következő módon juthatunk egyszerűen ezekhez az információkhoz:
Linux használatakor a következő parancsot írjuk be:

```
dmesg | grep ^eth[0123]\:
```

És az `eth0: registered` as kezdetű sorokban szereplő információra figyeljünk, az `eth0`, `eth1` stb. jelentheti az egyes hálózati kártyákat.
Windows esetében pedig parancssorban adjuk ki a következő utasítást:

```
ipconfig /all > c:\halochip.txt
```

s a C meghajtó gyökerében keletkező `halochip.txt` fájlt megnyitva a „Leírás:…" mellett szereplő információkat írjuk fel magunknak.

15 perc a falazási szintidő – ráadásul még kőműves sem kell hozzá

A telepítés legegyszerűbb módja, ha a letöltött *CD*-képet felírjuk (természetesen a *CD*-kép lemezre írása opciót kiválasztva az adott íróprogramban), majd *BIOS*-ban beállítjuk, hogy a rendszerindítás *CD-ROM*-ról történjen, és behelyezzük a lemezt. Ha minden jól megy, hamarosan egy rövid karakteres üdvözlőképernyőt látunk, ahol a boot: melletti sorba írhatunk indítási opciókat. Ezek a következők lehetnek:

- *nousb* – *USB* eszközöktől mentes használathoz
- *nopcmcia* – ha nincs *PCMCIA* eszközünk, és általában asztali gépeken ez a helyzet;
- *dma* – elsősorban a *SIS* chipeket tartalmazó alaplapokhoz készült, a merevlemezkezeléshez lehet rá szükség

A következő képernyőn már a telepítés nyelvét tudakolja tőlünk a rendszer: válasszuk ki bátran a *Magyart*. Nemsokára megkérdezi, hogy *CD-ROM*-ról, avagy hálózatról

(*HTTP/FTP*) szeretnénk-e folytatni a telepítést. Utóbbi a gyakorlatban azt jelenti, hogy előre felmásoljuk a fájlokat például saját webszerverünkre, s az elérési útját megadva folytatjuk majd az installálást. Mi a könnyebbség okán maradjunk az előbbinél.
Ezek után sem törekszik a rendszer a kelleténél nagyobb interaktivitásra: közli, hogy elvégzi a particionálást, és létrehozza a szükséges fájlrendszereket. Nyugodtan hagyjuk rá, de legyünk tudatában annak, hogy ezzel a merevlemez korábbi tartalma eltűnik, átadva helyét a tűzfalszerver fájljainak. Ha valaki kíváncsiskodni szeretne, az *ALT* és az *F2* billentyűk együttes lenyomásával megtekintheti a részletes történéseket, az *ALT* és az *F12* együttes leütésével pedig leginkább a rendszerindításkor hibásnak jelzett modulokkal kapcsolatban láthat információt; visszaváltani a telepítő képernyőre az *ALT* és az *F1* nyomva tartásával lehet.
A telepítés következő fázisában visszatölthetnénk egy már korábban elmentett *IPCop* konfigurációt, azaz ha valamiért újratelepítjük a rendszert, esetleg ilyen módon frissítjük korábbi verzióról, akkor lehetőségünk van a már bevált beállításokkal használni a frissen életre keltett rendszert. Ezt mi most kihagyjuk, viszont a következő, Hálózat beállítása című párbeszédablak már fontos állomás a telepítésben. Ha a gépre próbáljuk bízni a *GREEN* interfészhez tartozó hálózati kártya felismerését, akkor válasszuk a Próba feliratú gombot, s ő jó eséllyel megtalálja az első hálózati kártyát (linuxosan szólva az *eth0* –t). Ha ez nem sikerülne, nekünk kell a Kiválaszt gombot megnyomni, s megtalálni a kártyát

1. ábra A RED interfész telepítése sem ördöngősség

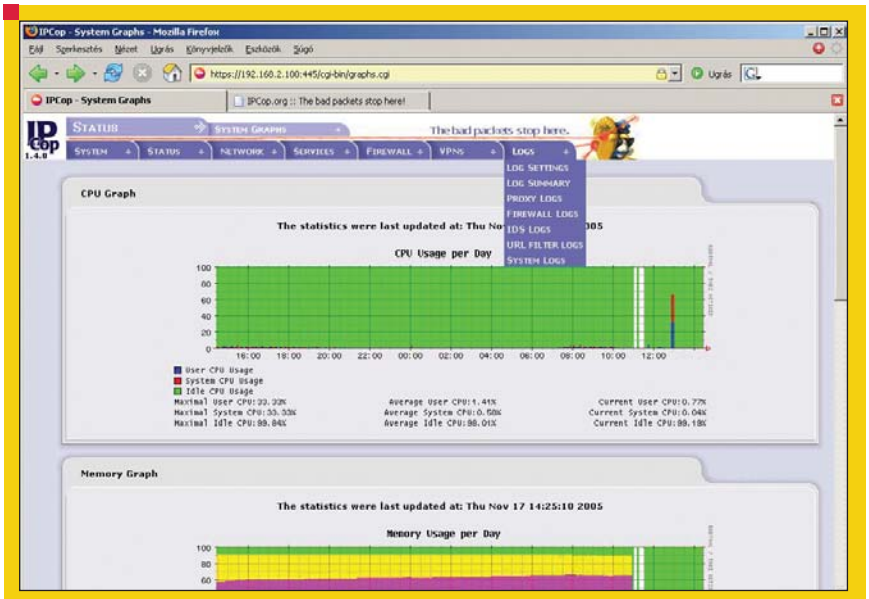
a listában, legrosszabb esetben a pontos paraméterezések ismeretében manuálisan beállítani.
Ha sikerült felismertetni a *GREEN* interfészt, akkor egy hozzá tartozó *IP* címet kér a gép. Mivel ez a hálózati kártya átjáróként fog működni két hálózati szegmens (a mi belső hálózatunk az egyik, és az internetet biztosító szolgáltatói szerver és vele kapcsolatban álló *RED* interfészünk a másik) között, ezért konvencionálisan `xxx.xxx.xxx.001` utótagú címet szokás adni neki. Gyakorlatilag rajtunk múlik, hogy az ún. privát címek közül melyiket adományozzuk ennek a kártyának, de érdemes a későbbi fejlesztések miatt következetesen használni őket.
Használható privát címtartományok az *RFC-1918* szabályzat értelmében:

10.0.0.1 – 10.255.255.254 vagy
172.16.0.1 – 172.31.255.254 vagy
192.168.0.1 – 192.168.255.254

Így például ha a a saját belső hálózatunk az ***192.168.1.2***, ***192.168.1.3***, ***192.168.1.4 IP*** című gépekből áll, akkor az *IPCop GREEN* interfészét ***192.168.1.1***-re állíthatjuk, míg például a vezeték nélküli hálózatot használó gépeink ***192.168.0.2*** , ***192.168.0.3*** stb. címűek, akkor az őket összekötő *BLUE*-t ***192.168.0.1***-re (leegyszerűsítve a szétválasztás azt jelenti, hogy jobbról nézve legalább az utolsó előtti számnak eltérőnek kell lennie a különböző interfészek ill. hozzájuk csatlakozó hálózatok esetén).
A rendszer ezután telepíti a betöltéshez szükséges alkalmazást, majd egy információs képernyőn tájékoztat minket arról, hogy böngészőből hogyan lehet elérni az adminisztrációs felületet. Billentyűzetkiosztást (***hu***, vagy ***hu101***), majd időzónát (***Europe/Budapest***) választhatunk a következőkben, végül az *IPCopot* futtató számítógépet keresztelhetjük más névre (alapértelmezettként ***ipcop*** lesz), és amennyiben szükségét érezzük, megváltoztathatjuk a tartománynevet (***localdomain***) is.
Ha nincs *ISDN*-kártya a gépben, ill. nem szeretnénk azt használni, válasszuk az *ISDN* tiltva nyomógombot a következő képernyőn, ellenkező esetben a protokollt és a kártya típusát, valamint a telefonszámot is meg kellene adnunk ahhoz, hogy *ISDN* vonalon keresztül érjük el az internetet.
Ismét egy Hálózati beállítás ablak köszönt ránk, melyben első lépésként a ***Hálózati konfiguráció*** típust kell megváltoztatni *GREEN + RED* formátumúra (jelen esetben nem jó nekünk az alapértelmezett *RED* is ***modem/ISDN***, hiszen kábel vagy *DSL* típusú elérést szeretnénk beállítani). Ha ezzel megvagyunk, a ***Driver*** hozzárendelése kártyákhoz menüpontot aktiválva kiválasztjuk a még szabad másik hálózati kártyát, s ő lesz a *RED* interfész.
Következhetnek a ***Cím beállítások***, s azon belül is a *RED* interfész, mivel ő még nem kapott *IP* címet.
A beállítási lehetőségek ebben az ablakban (a szóközbillentyűvel aktiválhatók az egyes lehetőségek, s csak egy választható ki):

- ***Statikus***: a szolgáltató úgynevezett fix *IP* címet biztosít számunkra, azaz az internet felől nézve mindig ugyanazzal a címmel rendelkezünk. Egyszerű a feladat: ezt a kapott címet kell beírni, a ***Hálózati mask (netmask)*** minden bizonnyal jól van kitöltve.
- *DHCP*: ebben az esetben dinamikusan osztja ki egy szerver számunkra a címet, s ennek változtatásáért és karbantartásáért is ő felel, ezért csak a szolgáltató által megadott számítógép nevét kell a *DHCP* gépnév mellé beírni.
- *PPOE*: tipikusan *DSL* típusú kapcsolatoknál találkozunk vele, s mivel a telefonvonal egyértelműen azonosít, nincs is semmi teendőnk (arra azért ügyeljünk, hogy esetleg a szolgáltató igényli bizonyos beállítások, például speciális gépnév vagy tartománynév használatát, s akkor ezeket a korábban írt lépések során figyelembe kell venni).
- *PPTP*: kábelmodem esetén (is) előforduló típus, itt is csak a szolgáltatótól kapott *IP* címet kell beírni.

A ***DNS és Átjáró*** beállítások menüpontban beállíthatjuk a *DNS* szolgáltatásokért felelős szerverek elérhetőségét, ill. az átjárót is, amennyiben nem *DHCP*-vel kapjuk meg ezeket az címeket. Ezek beállításában is hagyatkozzunk az internetszolgáltatótól kapott információra.



1. ábra Grafikus felületen könnyű dolgunk van

Ha a Rendben gomb megnyomásával túljutottunk ezen a szakaszon, csatasorba állíthatjuk az *IPCop DHCP*-szerver szolgáltatását az Engedélyezve kipipálásával. Ennek segítségével ő osztja ki dinamikusan a belső hálózat gépei számára az *IP*-címeket. Mi egyelőre hagyjuk ki ezt a lehetőséget.
Végül a rendszerünkben mindenható *root* rendszergazdának, s a működtetésért felelős adminisztrátori *admin* felhasználónak adhatunk belépési jelszót. Válasszunk kellemetlenül bonyolult, számok és betűk (kerüljük az ékezeteket ha lehet, mert a billentyűzetkiosztások csúnyán megtréfálhatnak bennünket) kombinációjából összeállított, lehetőleg hosszú és nem szokványos megoldásokat keressünk – mint amilyen például a *130r0tvaha13t0rta*.
Ezzel gyakorlatilag készen is vagyunk, az *OK* megnyomása után hátradőlhetünk: szinte tovább tart végigolvasni ezt a leírást, mint végigcsinálni a folyamatot. Azért teljesen ne bízzuk el magunkat, ha ugyanis az újraindításkor a *CD*-olvasóban felejtettük a telepítőlemezt, „negyedórával korábban mintha ezt már láttam volna” érzés keríthet hatalmába, ezért egyszerűbb a *BIOS*-ban átállítani a betöltési sorrendet a merevlemezzel kezdődőre.

Áll a fal, de hogyan tovább?

A klienseken be kell állítani az *IPCop GREEN* interfészhez tartozó *IP* címét átjárónak, később a szolgáltatások elindítása és a beállítások finomhangolása után érdemes *DNS*-szervernek is megadni, s elméletileg tűzfalunk indulása után már elérhető az internet.
Az induló rendszer négyféle kernelváltozat közül enged választani, nekünk most jó lesz az alapértelmezett első. Betöltés után konzolos ablak fogad, látszólag nem kényezteti el a felhasználót. Hol itt akkor az egyszerűség, könnyű használat, felhasználóbarátság?
Az *IPCop* elsődlegesen böngészőből adminisztrálható, átlátható és jól beállítható felülete miatt népszerű azok körében is, akik nem szívesen irkálnak át mindenféle konfigurációs fájlokat kézzel. Ennek elérését legegyszerűbben így tehetjük meg:
Indítunk egy internetböngésző programot, és a címsorba beírjuk

```
https://192.168.1.1:445/
```

A *https* a biztonságos, titkosított *SSL* kapcsolatot jelzi, s fontos a 445-ös portszám beírása is a kettőspont után. Az idézett *IP* cím (*192.168.1.1*) helyett jó esetben a telepítés során megadott gépnév (például *ipcop*) is használható, de mindenképp azt a címet vagy nevet kell beírni, ami a *GREEN* interfészhez tartozik, tehát a belső hálózat gépeivel azonos hálózati szegmensen található.
A *Connect*-re kattintva beírhatjuk az *admin* felhasználónevet, és a hozzá tartozó jelszót, s máris beléptünk a tűzfalszerverbe.

A nyelvet magyarra is állíthatjuk a *System* menüpont *GUI Settings* pontját választva, de ha a későbbiekben szeretnénk egyéb funkciókat is ellátó csomagokat telepíteni, akkor fontoljuk meg – legalább ideiglenesen – az eredeti angol nyelvű szövegek visszaállítását, mert jócskán megkönnyíti dolgunkat a dokumentációk olvasása során.
Amennyiben valamiért szükségünk lenne átírni az eredeti konfigurációt, például megváltoztatni a hálózati beállításokat, akkor az *IPCop* konzolos felületére belépve a *setup* parancs beírásával a telepítéskor feljövő ablakok szűkebb változatának segítségével megtehetjük azt.
Ha tartunk attól, hogy nagy étvágyú és rosszindulatú egyének megeszik pingvinünket vacsorára, töltsük le az aktuális programfrissítéseket. Ezt a *Rendszer* menü *Frissítések* pontja alatt mazsolázva tehetjük meg, ahol tételesen felsorolva látjuk a megjelent és említésre méltó változásokat, s jobboldali oszlop Információ feliratú linkjére kattintva le is tölthetjük azokat. A lementett fájlt ugyanezen lapon alul a *Tallózást* választva tölthetjük fel, majd az *IPCop* megvizsgálja szavahihetőségét, s telepíti azt.
Munkánkat grafikonok is segítik, valamint szűrhető tűzfal- és egyéb naplózás is a rendelkezésünkre áll. Barátkozzunk a rendszerrel, s olvassunk a témába vágó elméleti és gyakorlati aspektusokkal egyaránt foglalkozó szakirodalmat, hiszen egy igazán jó védelmi rendszernek és üzemeltetőjének illik naprakésznek lennie.
Ráadásul a java még csak most következik, hiszen a feltelepített konfigurációt hamar testre akarjuk majd szabni, s elvárásainkkal összhangban szorgalmunknak is növekednie kell.

Tóth Virgil Zoltán
(m_v@c2.hu)
Szoftverfejlesztő informatikus és rendszergazda, kedvence a Debian disztribúció. Szabadidejét legszívesebben felesége és szépirodalmi regények társaságában tölti. Lenyűgözőnek tartja a Linux rugalmasságát, és a vele dolgozók aktivitását.