Lopakodó e-mail kiszolgáló

Lopakodó e-mail kiszolgáló dinamikus DNS-sel és Treo 650 okostelefonnal.

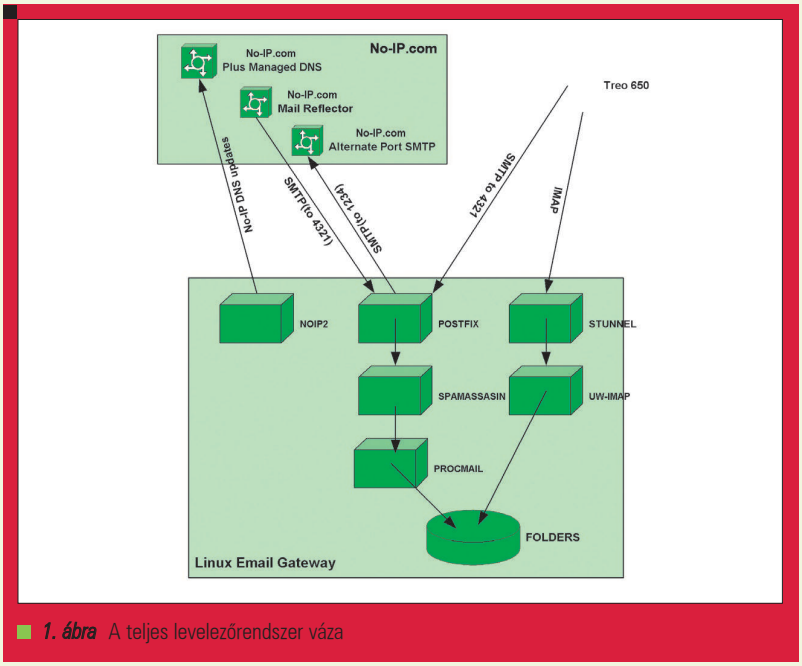
Szinte az e-mail megjelenésétől kezdve saját levelezőkiszolgálót tartok fenn, biztosítva ezzel, hogy mindig naprakész legyek az internetes kommunikáció területén. A technológia, ami egy ilyen projekt felépítéséhez szükséges, más területeken remekül újrahasznosítható, ám folyamatos tájékozódást igényel.
Eleinte igen egyszerű volt a feladat. Csatlakoztattuk a modemet, kerestünk egy közösségi ***UUCP*** kiszolgálót, beállítottuk a betárcsázós kapcsolatot, a ***uucico***-t és a ***Sendmailt***. Ez volt az e-mail T- modellje. Többnyire nem maradt el egy ***C-News Usenet*** hírcsoport beállítása sem, amin keresztül hozzáférhetővé vált az akkor még viszonylag kis méretű Internet összes számítógépének ***UUCP*** címe.
Az internet nagykorúvá válásával azonban jelentősen bonyolultabb lett a helyzet. A kiszolgálóink az internetes betörők célpontjaivá váltak, a hálózaton közlekedő e-mail csomagjainkat lehallgathatják, postafiókjainkat pedig kéretlen levelek ezrei árasztathatják el. És ha ez még nem lenne elég, sok munkahely annyira biztonságos lett, hogy a munkahelyi hálózatból napközben el sem érhetjük saját levelező szerverünket.
A korábbi linuxos kiszolgálóm statikus ***IP*** címmel ***DSL*** vonalon keresztül kapcsolódott az internetre. Ez a gép többek közt ***DNS*** szolgáltatást nyújtott és tűzfalként (***netfilter***) működött.
A levelek küldését és fogadását a ***Postfix*** végezte, a levélszemét szűrését pedig a ***SpamAssassin***. A leveleimet a laptopommal ***IMAP***-on keresztül, ***Netscape Communicatorral*** értem el, és ugyanez a program intézte a levelek szétválogatását is különböző ***IMAP*** mappákba.

Ez az egyszerű rendszer már a múlté, mióta a ***San Francisco*** öbölben található otthonomból ***Coloradóba***, ***Denverbe*** költöztem. A statikus ***IP*** címet biztosító ***DSL*** kapcsolat lehetősége megszűnt, helyette van egy monopol helyzetű fasisztoid internetszolgáltató. Statikus ***IP*** nincs (legalábbis nekem), ráadásul a szolgáltató szűri a leggyakrabban használt ***IP*** portokat. Az új munkahelyem annyira biztonságos, hogy a laptopomat már nem is érdemes magammal hordanom és a munkahelyi hálózatból sem érem el a levelezőkiszolgálómat. Mindez persze érthető. A szolgáltató védekezni akar a levélszemét ellen, és az alkalmazottak miatt is indokolt a nagyfokú biztonság. A leveleimet viszont akkor is el akarom olvasni napközben is.
Az említett akadályok leküzdése személyes kihívássá vált. E-mail olvasó gyanánt egy ***Treo 650*** mellett döntöttem, hogy áthidaljam a munkahelyi biztonság problémáját. Az otthoni levelezőkiszolgálómat beállítottam, hogy egy új lopakodó beállítást lehetővé tevő szolgáltatást használjon, amely biztosít dinamikus ***DNS*** szolgáltatást és levéltovábbítást tetszőleges kapura. Íme a lényegesebb beállítások, amelyeket később majd lépésről lépésre bemutatok:

- A levelezőkiszolgáló ***Gentoo Linuxot*** futtat és ***DHCP***-vel kiosztott ***IP*** címmel ***VDSL*** (a ***Qwest*** nevű szolgáltató által biztosított nagyon nagy sebességű ***DSL***) vonalon keresztül kapcsolódik az internetre. A ***DNS*** regisztrátor a ***No-IP.com***, amely figyeli az ügyfél ***IP*** címének változásait. Ehhez a kiszolgálónkon a noip2 nevű ügyfélprogramot kell futtatnunk, ami a ***No-IP.com DNS*** kiszolgálójához kapcsolódva percenként frissíti a ***DNS*** bejegyzésünket. A szolgáltatás neve ***Plus Managed DNS***.
- A ***No-IP.com Mail Reflector*** szolgáltatását is igénybe veszem, amely a tartományom számára biztosít egy ***MX*** bejegyzést a saját kiszolgálójukon, a leveleket pedig továbbítja a kiszolgálóm egy szabadon választott portjára. Így áthidaltam azt a problémát, hogy az internetszolgáltatóm blokkolja a bejövő 25-ös kaput.
- A szolgáltatóm internetes levélszemétküldő feketelistákon szerepelteti a ***DHCP*** címemet, így minden próbálkozás, hogy leveleket közvetlenül a saját kiszolgálómról kézbesítsek, eleve kudarcra van ítélve. Erre a ***No-IP.com Alternate-Port SMTP*** szolgáltatása kínál megoldást, amely a kimenő levelek továbbítását biztosítja. Minden levelemet a ***No-IP.com SSL*** azonosítást használó kiszolgálójának egy nem szabványos portjára irányítom, így nem számít, hogy az internetszolgáltatóm blokkolja a kimenő ***SMTP*** forgalmat.
- ***MTA***-nak, azaz levéltovábbító ügynöknek (***Mail Transfer Agent***) ***Postfixet*** használok, amely könnyedén beállítható lopakodáshoz nem szabványos kimenő és bejövő kapukkal.
- A levélszemét szűréséhez ***SpamAssassint*** használok. A beállítása egyszerű és remekül működik. Feladata dióhéjban annyi, hogy megvizsgálja a leveleket, a spam-gyanúsakat pedig egy ***X-Spam-Level*** fejléc mezővel látja el. Minél több csillag karaktert tartalmaz ez a mező, vagyis minél

magasabb a pontszám, annál biztosabb, hogy levélszeméttel van dolgunk. Már egyetlen csillag esetén is megalapozott a gyanú.

- Nem tárolhatom az összes levelemet az okostelefonon és a levélszűrést sem végeztethetem azzal, mivel ennyi levél el sem fér rajta. A szűrés feladata (vagyis az e-mail üzenetek szétválogatása külön *IMAP* mappákba), melyet eddig a *Netscape Communicator* ügyféloldalon látott el, most átkerül a *Procmailhez*. Létrehoztam egy *.procmailrc* fájlt, benne mindazokkal a szabályokkal, amelyek alapján a levélszemét és levelezőlistákra érkezett üzenetek elhelyezése történik a kiszolgáló könyvtárszerkezetében. Ez azért is hasznos, mert így bárhonnan hozzáférhetek az archivált üzeneteimhez is.
- Az egyik legkomolyabb problémát az *IMAP* kiszolgáló kiválasztása jelentette. Jobban szeretem ugyanis a hagyományos *mailbox* formátumú postafiókokat, ahol az egy mappába tartozó üzenetek egyetlen fájlban tárolódnak. A legtöbb modern *IMAP* kiszolgáló, mint a *Courier*, vagy a *Cyrus* a leveleket az újabb *maildir*, vagy *MH* formátumban tárolják, ahol minden levél egyetlen fájlnak felel meg, elképesztő mennyiségű *inode*-ot felemésztve. Sajnos csak egyetlen nyílt forrású *IMAP* kiszolgálót találtam, amely a hagyományos *mailbox* mappákkal működik. Ez a *uw-imap* (ne számoljuk ide a *CommuniGate Pro*-t, amely szintén támogatja ezt a formátumot, viszont kereskedelmi termék), amelynek viszont számos gyengéje akad, főleg az *SSL*-protokoll területén. A tesztelés során az uw-imap és a választott *SSL IMAP* ügyfélprogram, a *PalmOS*-on futó *VersaMail* közötti kapcsolódási hibák miatt más megoldás után kellett néznem. A cél elérése érdekében – ami pedig az egyetlen fájlból álló mappák és működő *SSL* kapcsolat – az *IMAP* szolgáltatást és az *SSL* titkosítást két külön kiszolgálóval kellett megvalósítanom: *stunnellel* és *uw-imappal*. A *stunnel* igen hatékonynak bizonyult az *SSL* beállítások, a naplózás és hibakeresés területén.



1. ábra A teljes levelezőrendszer váza

- A levelezőrendszerem ügyféloldali részét eredetileg a *Treo 650*-hez kapott gyári *PalmOS*-on futó *VersaMail* program és a *Sprint* nevű szolgáltatónál kötött előfizetés képezte. A döntés fő oka a havi mindössze 15 dollárért kínált korlátlan internet elérés volt. A *VersaMail IMAP* támogatása is elég jó, a *Blazer Web* böngészővel való integráció miatt pedig különösen jó vételnek tűnt. Sajnos azonban problémák merültek fel a *VersaMail* intenzív használata során. A rendszer sarkalatos pontja a megbízható levelezőkiszolgáló, illetve azon az új üzenetek lekérdezése. A *VersaMailnek* viszont van egy, a lekérdezés ütemezését érintő hibája, ami nagymértékben csökkenti a hatékonyságát. Így végül a *SnapperMail*-re (érdekes példája annak, hogyan képes kilenc új-zélandi fickó megelőzni egy olyan nagy céget, mint a *Palm Software*) esett választásom, ami az egyik legjobb *PalmOS* alkalmazásnak bizonyult, amivel valaha találkoztam.

Egyszóval van itt néhány mozgó alkatrész, így jól fog jönni egy diagram (*1. ábra*).
Az *1. ábrán* látható, hogy a beállításokat három területen kell elvégeznünk: ezek a *Linux* kiszolgáló, a *No-IP.com* és a *Treo 650* levelező ügyfél.

A Linux kiszolgáló beállítása

A *Gentoo Linuxra* az igen kényelmes *Portage* csomagkezelő rendszer miatt esett a választásom. *Portage*-et használva nem kell egyenként megkeresnünk a szükséges csomagokat. Működését tekintve a *Perl CPAN*-hoz, vagy a *Debian apt-get*-jéhez hasonlít. A *Gentoo* telepítéséhez lásd a *gentoo.org* webhelyen található dokumentációt. Az operációs rendszer telepítése többnyire kézileg vezérelt és akár nagyon hosszadalmas is lehet (némely telepítés akár napokig eltarthat, mivel mindent magunknak kell lefordítanunk), ám a befektetés megtérül a karbantartás és az alkalmazások beállítása során.
Szükség lesz még a *No-IP.com* fent említett *DNS* és *SMTP* szolgáltatásaira. Ezek dokumentációja megtalálható a *No-IP.com* webhelyén.
A következő utasítások *Gentoohoz* íródtak, de könnyen alakíthatók más terjesztésekhez is. A lényeg, hogy a telepített programok rendelkezzenek a szükséges képességekkel (mint például az *SASL* támogatás).

Postfix MTA

Telepítsük elsőként a rendszer alapját képező *Postfixet*. A *Gentoo* alaptelepítése tartalmaz egy egyszerű levéltovábbító ügynököt, az *ssmtp*-t – ezt el kell távolítanunk a *Postfix* telepítése előtt. A *Postfixet SASL*

támogatással kell telepítenünk, azaz lefordítanunk. Ez a ***No-IP.com Alternate-Port SMTP*** szolgáltatásánál a hitelesített levél továbbításhoz szükséges.
Az ***SASL*** támogatás engedélyezéséhez az ***/etc/make.conf*** fájlban adjuk hozzá az ***sasl*** kulcsszót a ***Gentoo USE*** változójához:

```
/etc/make.conf:
USE="sasl"
```

Telepítsük az ***SASL*** könyvtárakat:

```
# emerge dev-libs/cyrus-sasl
```

Töröljük az ***ssmtp***-t, telepítsük a ***Postfixet***:

```
# emerge -C ssmtp
# emerge postfix
```

A rendszer indításakor indítsuk el a ***Postfixet***:

```
# rc-update add postfix default
```

A ***Postfix*** beállítása kifejezetten egyszerű, mindössze két beállításfájllal kell foglalkoznunk: az ***/etc/postfix*** könyvtárban található ***main.cf***-fel és ***master.cf***-fel.
Adjuk meg a ***main.cf*** fájlban az átjárónk tulajdonságait. Itt most az átjáró gépneve `mygateway`, a tartománynév pedig `foobar.net`. A ***relay host***, amelyen keresztül leveleinket küldjük a `relayhost.no-ip.com`, amely a 1234-es kapun fogad ***SMTP*** kapcsolatokat. Ezt a ***No-IP.com*** biztosítja az ***Alternate-Port SMTP*** szolgáltatás részeként.

```
myhostname = mygateway
mydomain = foobar.net
myorigin = $mydomain
mydestination = $myhostname,
➥localhost.$mydomain $mydomain
#home_mailbox = .maildir/
relayhost = relayhost.no-
➥ip.com:1234
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:
➥/etc/postfix/saslpass
smtp_sasl_security_options =
```

Adjunk meg még egy kaput, a 4321-est, a 25-ösön kívül a ***Postfix master.cf*** fájljában. Ezen fogunk ***SMTP*** kapcsolatokat fogadni a ***Mail Reflector No-IP.com*** szolgáltatás keretében és a ***Treo 650***-ről is.

```
4321    inet  n       -       n       -
➥-         smtpd
```

Hozzunk létre egy ***SASL*** jelszófájlt ***/etc/postfix/saslpass*** néven. Ez fogja tartalmazni a `foobar.net@noip-smtp` felhasználó jelszavát (????) a ***relayhost.no-ip.com*** gazdagéphez. Ezek is a ***No-IP.com*** szolgáltatásának beállításai.

```
/etc/postfix/saslpass:
relayhost.no-ip.com
➥foobar.net@noip-smtp:????
```

Hozzunk létre egy ***dbm*** táblát:

```
# cd /etc/postfix
# postmap saslpass
```

Utolsó simításként engedélyezzük a levéltovábbítást a ***Treo 650***-ről. Itt a ***Sprint*** szolgáltatását használjuk, tehát meg kell tudnunk, hogy milyen ***IP*** cím tartományból fogunk csatlakozni a kiszolgálónkhoz. A ***Postfix main.cf*** fájljának ***mynetworks*** paraméterének tartalmaznia kell a switch címét. Most az otthoni hálózat és a helyi visszacsatoló hálózat mellett a ***70.0.0.0/8***-at adjuk meg, biztonsági okokból azonban érdemes lehet szűkíteni ezt a címtartományt.

```
mynetworks = 192.168.1.0/24
➥127.0.0.0/8 70.0.0.0/8
```

Spam szűrő

További két csomagra lesz szükség, ezek a ***spamassassin*** és a ***procmail***.
A telepítés lépései (***Gentoon***) a következők.
Telepítsük a ***Procmailt***:

```
# emerge procmail
```

Telepítsük a ***SpamAssassint***:

```
# emerge spamassassin
```

A ***SpamAssassin*** automatikus indításához frissítsük az rc indítószkripteket (más csomagkezelők használata esetén ez már meg is történt):

```
# rc-update add spamd default
```

Módosítsuk a ***Postfix*** beállításait, hogy az a ***Procmaillel*** kézbesítse a leveleket. Adjuk az alábbi sort az ***/etc/postfix/main.cf*** fájlhoz:

```
mailbox_command =
➥/usr/bin/procmail
```

Hozzuk létre a ***Procmail*** beállításfájlját ***/etc/procmailrc*** néven és adjuk hozzá az alábbi szabályt, hogy a levelek keresztülmenjenek a ***SpamAssassinon***:

```
DEFAULT=/var/spool/mail/$LOGNAME
:0fw: spamassassin.lock
* < 256000
| /usr/bin/spamc
```

Indítsuk el a ***spamd*** kiszolgálót:

```
# /etc/init.d/spamd start
```

Kézbesítés

Hozzunk létre egy ***IMAP*** könyvtárszerkezetet, majd állítsuk be a ***Procmailt***, hogy ezekbe kézbesítse a leveleket. Ha több felhasználónk van, ezt mindegyiknél végre kell hajtanunk. Az alábbi beállítások a ***~/.m*** könyvtárat jelölik ki gyökérkönyvtárnak. A felhasználók ***Procmail*** beállításai a ***~/.procmail*** fájlba kerülnek. Kiindulópontként használhatjuk az alábbi példát, amely különválogatja a levélszemetet és a levelezőlistákra érkezett leveleket. További részletekért lásd a ***procmailrc(5)*** kézikönyvoldalt.

```
PATH=/bin:/usr/bin:/usr/sbin
MAILDIR=$HOME/.m
DEFAULT=$MAILDIR/Mbox
LOGFILE=$HOME/.procmail.log
VERBOSE=yes

# File gentoo-user mailing list
➥into ~/.m/lst/gentoo
:0:
* (^To.*|^Cc.*)gentoo-
➥user@lists.gentoo.org
lst/gentoo

# File jobserve mail into ~/.m/
➥lst/jobserve
:0:
* ^From.*jobserve.com
lst/jobserve

# File SPAM into ~/.m/Spam with
➥some exceptions:
:0:
```

```
* ^X-Spam-Level:.*\*
 * !^From.*netflix
 * !^From.*vail
 * !^From.*ebay member
 * !^From.*cnet
Spam

# File SPAM that escaped
➥spamassassin:
:0
* ^From.*eversave.com
Spam
:0:
* ^From.*sears.com
Spam
```

Most, hogy a levélfeldogozó rendszer darabjai a helyükre kerültek, elindíthatjuk a ***Postfixet*** és várhatjuk a leveleket. Lefogadom, hogy az első üzenetek a *~/.m/Spam* mappában fognak megjelenni:

```
# /etc/init.d/postfix start
```

Az IMAP kiszolgáló

Az ***IMAP*** szolgáltatásunk a ***stunnelből*** és az ***uw-imapból*** áll össze. Az ***uw-imap*** telepítése némiképp eltér a szokványostól, mivel a Gentoo alapbeállításai nem teszik lehetővé a lefordítását ***clear-text***, azaz titkosítatlan jelszavas azonosítással titkosítatlan csatornán. Nekünk mégis ez kell, hiszen a kiszolgálónk ***stunnel*** mögött lesz. A megoldás egy speciális ***USE*** beállítás, amely kikapcsolja az ***SSL*** támogatást és engedélyezi a titkosítatlan jelszavakat. ***Gentoo Linuxon*** a telepítés a következő paranccsal történik:

```
# USE="-ssl clearpasswd" emerge
➥uw-imap
```

A ***stunnel*** beállításfájlba fel kell vennünk egy ***IMAP*** részt az alábbi módon:

```
pid = /var/run/stunnel/
➥stunnel.pid
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
cert = /etc/ssl/certs/
➥foobar.net.pem
[imaps]
accept  = 993
exec = /usr/sbin/imapd
execargs = imapd
```

Hozzunk létre ***self-signed***, vagyis saját aláírású ***SSL*** tanúsítványt *foobar.net.pem* fájlnévvel:

```
# cd /etc/ssl/certs
# openssl req -new -x509 -nodes
➥-out cacert.pem -keyout
➥cakey.pem -days 5000
        Country Name (2 letter
➥code) [AU]:US
        State or Province Name
➥(full name) [Some-State]:CO
        Locality Name (eg,
➥city) []:Highlands Ranch
        Organization Name (eg,
➥company) [Internet Widgits
➥Pty Ltd]:
        Organizational Unit
➥Name (eg, section) []:home
        Common Name (eg, YOUR
➥name) []:foobar.net
        Email Address
➥[]:me@foobar.net
# cat cakey.pem cacert.pem >
➥foobar.net.pem
```

Gentoon a ***stunnel*** automatikus indításához frissítenünk kell az indítószkripteket is:

```
# rc-update add stunnel default
```

A Treo 650 beállítása

PalmOS operációs rendszerhez két jó ***IMAP*** ügyfélprogram található. Az egyik a ***Treora*** gyárilag telepített ***VersaMail***, a másik pedig egy kereskedelmi alkalmazás, a ***SnapperMail***. Én az utóbbit választottam, még a meglehetősen borsos ára ellenére is (körülbelül 60 dollárba kerül). Mindkét programmal feliratkozhatunk ***IMAP*** mappákra a kiszolgálón és kezelhetünk csatolt fájlokat. A ***SnapperMailt*** viszont alaposabban tesztelték és a további szolgáltatásai miatt megéri az árát. ***PalmOS*** programok telepítéséhez és általában a ***Treo 650*** kezeléséhez ***Linuxon*** a ***pilot-link*** programcsomagot használom. ***Gentoon*** így telepíthetjük:

```
# emerge pilot-link
```

A ***pilot-linkkel*** készíthetünk biztonsági mentést a ***Treoról***, amit aztán a ***Linux*** valamely könyvtárában tárolhatunk és programokat is, mint a ***SnapperMailt*** is ezzel telepíthetünk. A ***Treot Bluetooth***-szal és ***PPP***-vel csatlakoztatom a ***Linux*** notebookomhoz, de használhatnék akár ***USB***-t is. A ***pilot-link*** programcsomag által használt kapcsolat típusát a `PILOTROOT` környezeti változóval adhatjuk meg, ***USB*** kábel esetén így:

```
# export PILOTPORT=/dev/
➥tts/USB1
```

Bluetooth esetén pedig így:

```
# export PILOTPORT=net:any
```

Létrehoztam egy ***treo*** nevű könyvtárat a saját könyvtáramban, amelybe programok telepítése előtt a következő paranccsal készítek biztonsági mentést a ***Treoról***:

```
# pilot-xfer -b treo
```

Így pedig növekményesen menthetjük, azaz szinkronizálhatjuk az okostelefon tartalmát ugyanebbe a könyvtárba:

```
# pilot-xfer -s treo
```

A biztonsági mentés visszaállítására a következő parancs szolgál:

```
# pilot-xfer -r treo
```

A ***SnapperMail*** telepítéséhez töltsük le az *SME231.zip* nevű fájlt a ***www.snappermail.com*** webhelyről, csomagoljuk ki, majd futtassuk az alábbi parancsot:

```
# pilot-xfer -i SnapperMail-
➥ent.prc
```

A ***Treo 650*** legkönnyebben a szolgáltatótól megrendelhető ***Sprint PCS Vision Professional Pack*** csomag segítségével állíthatjuk be a ***Sprint*** hálózatához. A ***SnapperMailhez*** jár egy 60 oldalas ***PDF*** formátumú felhasználói kézikönyv, de a beállítása is magától értetődő.

Linux Journal 2006., 143. szám

Peter Ziobrzynski Kanadában, Torontóban dolgozik független tanácsadóként. UNIX és Linux tanácsadói szolgáltatást nyújt San Franciscó-i (California), és újabban denveri (Colorado) ügyfeleknek.