36

Sähköpostipalvelu

Sähköposti on Internetin tärkeimpiä palveluita heti WWW:n jälkeen. Vaikka sähköposti on näennäisesti yksinkertainen palvelu, on sen konfiguroinnissa ja ylläpidossa paljon tehtävää. Palvelinohjelmia on useita ja palvelun laatua voi parantaa roskapostin ja virusten estolla.

36.1 Sendmail

Sendmail on eniten käytetty ja perinteisin sähköpostipalvelin. Sen pitkä ikä näkyy sen konfiguroinnin monimutkaisuudessa, vaikka se onkin helpottunut. Toisaalta siitä löytyy paljon tietoa ja osaamista ja sitä pidetään edelleen standardina. Linuxille löytyy kuitenkin muitakin postipalvelimia ja esimerkiksi postfix voi olla järkevämpi valinta jos jo ei ole sendmailia tottunut käyttämään.

Postipalvelin kuuluu Linuxin perusasennukseen. Sitä tarvitaan jo pääkäyttäjän postin käsittelyyn, jota syntyy esimerkiksi cronin käytöstä eli ilman postipalvelinta on hyvin vaikea olla. Oletuksena sendmail välittääkin vain paikallista postia ja jotta sen saisi toimimaan kuten “oikea postipalvelin”, pitää asetuksiin tehdä muutoksia.

36.1.1 Sendmailin konfigurointi

Jotta voisit käyttää täysimittaista postipalvelinta, sinulla pitää olla Internet-liittymä, jossa on kiinteä IP-osoite. Yleensä se on vain yrityksille tarkoitetuissa liittymissä, mutta se ei tarkoita välttämättä, että hinta olisi erityisen korkea. Kiinteää IP-osoitetta tarvitaan, koska viestintävirasto on määrännyt (13 A/2008 M), että “Internet-liittymiä tarjoavan teleyrityksen on estettävä kuluttajaliittymään suuntautuva SMTP-liikenne (Simple Mail Transfer Protocol) muualta kuin sovittujen SMTP-liikenteelle tarkoitettujen palvelimien kautta.” ja “Internet-liittymiä tarjoavan teleyrityksen on estettävä kuluttajaliittymistä lähtevä rajoittamaton SMTP-liikenne muuten kuin sovittujen lähtevälle SMTP-liikenteelle tarkoitettujen palvelimien kautta.” Molemmissa tapauksissa esto voidaan pyynnöstä poistaa, mutta dynaamisen IP-osoitteen kanssa se olisi teknisesti niin hankalaa, että palveluntarjoajat eivät sitä tee.

Ennen kuin lähdet konfiguroimaan sendmailia, on järkevää asentaa dokumentointi ja välttämätöntä asentaa konfigurointipaketti:

```
yum install sendmail-doc sendmail-cf
```

Sendmailin konfigurointitiedostot ovat hakemistossa `/etc/mail`. Sen lisäksi `/etc/sysconfig/sendmail`, `/etc/aliases` ja hakemiston `/etc/smrsh` sisältö vaikuttavat sendmailin toimintaan. Hakemistossa `/etc/mail` on seuraavia tiedostoja:

- **access** luettelo koneista ja verkkoalueista joista pääsy on estetty tai sallittu. Lisää rivi “Connect:192.168.0 RELAY”, jos paikallisverkkosi on tyypillisin C-luokan yksityisverkko ja haluat välittää muista koneista lähtevän postin tämän koneen kautta. Estolistaa tähän tiedostoon ei kannata kerätä, vaikka se olisikin mahdollista.
- **domaintable** toimialueiden linkitys. Käyttökelpoinen, jos esimerkiksi yrityksesi nimi muuttuu.
- **local-host-names** lista kone- ja toimialuenimistä, joille muut voivat lähettää tähän koneeseen postia. Tärkeämpiä kuitenkin ovat nimipalvelun MX-tietueet, jotka määrittelevät toimialueen postipalvelimet (joita pitäisi olla vähintään kaksi).
- **sendmail.cf** älä muokkaa tätä tiedostoa suoraan, tämä generoidaan `sendmail.mc`-tiedostosta.
- **sendmail.mc** tärkein sendmailin konfigurointitiedosto.

Välittävän postipalvelimen konfigurointi

Välittävä postipalvelin käyttää Internet-palveluntarjoajan postipalvelinta apunaan ja se soveltuu vaikka koneella ei ole kiinteää IP-osoitetta. Yksityisen paikallisverkkosi koneiden kannalta välittävä postipalvelin on aivan kuin täysimittainen postipalvelin.

Edut tästä järjestelystä riippuvat Internet-palveluntarjoajastasi, joten muuta ei voi yksiselitteisesti sanoa kuin, että omassa postipavelimessasi asetat itse rajat ja palvelun laadun. Haittana on konfigurointi, joka on melko helppoa ja nopeaa sekä ylläpito, josta pitäisi selvitä melko pienellä vaivalla.

Sendmailin osalta ainoa konfiguroitava asia on ns. smarthost-asetus. Sendmailin `sendmail.mc`:ssä on valmiina kommentoitu rivi:

```
dnl define('SMART_HOST', 'smtp.your.provider')dnl
```

Poista rivin alusta "dnl" ja korvaa smtp.your.provider palveluntarjoajasi postipalvelimen nimellä. Anna muokkauksen jälkeen komento "make -C /etc/mail". Toinen tapa saada uudet asetukset käyttöön on käynnistää sendmail uudelleen.

Soneran postipalvelin on konfiguroitu väärin (ainakin syksyllä 2009) ja sen takia edelliset ohjeet eivät aivan sellaisinaan päde. Ongelmana on, että posti pitäisi kulkea palvelimen mail.inet.fi kautta, mutta nimipalvelun mx-tietueen mukaan mail.inet.fi koneen ensisijainen postipalvelin on mta.inet.fi, jossa taas palomuuri estää postin vastaanoton. Tarkistetaan ensin mx-tietue:

```
# host mail.inet.fi
mail.inet.fi has address 195.156.147.15
mail.inet.fi mail is handled by 10 mta.inet.fi.
# dig mx mail.inet.fi
...
;; ANSWER SECTION:
mail.inet.fi.           1614    IN      MX      10 mta.inet.fi.
....
```

Sitten koneen mta.inet.fi IP-osoite ja sen avoimet palvelut:

```
# host mta.inet.fi
mta.inet.fi has address 195.156.147.12
mta.inet.fi mail is handled by 10 mta.inet.fi.
# nmap 195.156.147.12

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2009-10-27 21:15 EET
Interesting ports on mta.inet.fi (195.156.147.12):
Not shown: 1678 closed ports
PORT    STATE    SERVICE
25/tcp  filtered smtp
443/tcp open     https

Nmap finished: 1 IP address (1 host up) scanned in 9.725 seconds
```

Tämän ongelman voi kiertää pakottamalla sendmailin käyttämään palvelinta mail.inet.fi laittamalla sen hakasulkeisiin, jolloin sendmail ei tarkista nimipalvelusta mx-tietuetta:

```
define('SMART_HOST', '[mail.inet.fi]')dnl
```

Toinen konfiguroitava asia on postin haku, mutta siihen tarvitaan esimerkiksi `fetchmail`:

```
yum install fetchmail
```

Fetchmail vaatii yhden konfigurointitiedoston, `/.fetchmailrc`, joka kuitenkin on melko yksinkertainen.

```
set logfile fetchlog
set daemon 43200  # Hae 12 tunnin välein.
poll smtp.isp.fi proto IMAP:
      etakayttaja kayttajatunnus there pass salasana is paik_kayttaja here smtphost localhost;
```

Lokitiedostoa ei voida kirjoittaa hakemistoon `/var/log`, jos `fetchmail` käynnistetään tavallisena käyttäjänä, jolla ei ole kirjoitusoikeutta ko. hakemistoon. Fetchmail käynnistyy näillä asetuksilla taustalle, mutta jos halutaan varmistaa, että se käynnistyy automaattisesti, sen käynnistyskomento voidaan lisätä `/etc/rc.d/rc.local`-tiedostooon:

```
su kayttajatunnus /usr/bin/fetchmail --fetchmailrc /home/kayttajatunnus/.fetchmailrc
```

Tai vaihtoehtoisesti, jos halutaan varmistaa, että se käynnistyy uudelleen mikäli se jostain syystä kuolisi, lisätään `/etc/crontab`-tiedostoon rivi:

```
# fetchmail starts as a daemon, but to ensure it runs, it can be
# awakened daily.
59 2 * * * kayttajatunnus /usr/bin/fetchmail --fetchmailrc /home/kayttajatunnus/.fetchmailrc
```

Itsenäisen postipalvelimen konfigurointi

Kuten edellä jo kerrottiin, tarvitset kiinteän IP-osoitteen sekä palomuurissa tarvittavat portit avoimiksi. Postipalvelin ottaa postia vastaan portissa 25. Lisäksi jatkossa on oletettu, että sinulla on oma domain-nimi ja nimipalvelutiedoissa MX-tietue osoittaa sähköpostipalvelimeesi.

Voit tarkistaa verkkoalueen (domainin) MX-tietueet `dig`-ohjelmalla:

```
dig  lineox.net mx

; <<>> DiG 9.3.4-P1 <<>> lineox.net mx
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2293
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 8
```

```
;; QUESTION SECTION:
;lineox.net.                    IN      MX

;; ANSWER SECTION:
lineox.net.             10800   IN      MX      100 smtp2.easydns.com.
lineox.net.             10800   IN      MX      5 lineox.net.
lineox.net.             10800   IN      MX      9 rk2.lineox.net.
lineox.net.             10800   IN      MX      10 smtp.easydns.com.
....
```

Verkkoalueelle `lineox.net` on määritelty neljä postipalvelinta, joista ensisijainen on `lineox.net`, koska sen prioriteetti on alin eli 5 ja toissijainen on `rk2.lineox.net`, koska sen prioriteetti on toiseksi pienin eli 9.

sendmail.mc-tiedoston perusasetukset Jotta sendmail suostuisi ottamaan vastaan postia ulkomaailmasta, poista “dnl” ja “Addr=127.0.0.1,” ylemmältä riviltä, jolloin tuloksena on alempi rivi:

```
dnl DAEMON_OPTIONS('Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
DAEMON_OPTIONS('Port=smtp, Name=MTA')dnl
```

Jos haluat avata “submission”-portin, jolloin esimerkiksi kännyköillä voidaan lähettää sähköpostia palvelimesi kautta, jos ne autentikoituvat, poista “dnl” seuraavan rivin alusta:

```
DAEMON_OPTIONS('Port=submission, Name=MSA, M=Ea')dnl
```

Seuraavalle riville kannattaa vaihteeksi lisätä “dnl” rivin alkuun, jotta loppuosa muuttuu kommentiksi:

```
dnl FEATURE('accept_unresolvable_domains')dnl
```

Näillä asetuksilla pitäisi päästä alkuun, mutta `sendmail.mc`-tietostoon kannattaa vielä lisätä virus- ja roskapostintorjunta, mutta niistä myöhemmin.

local-host-names Tähän tiedostoon pitää lisätä kaikki koneesi konenimet. Huomaa, että domainissa kannattaa määritellä yksi “pääkone”, jolla konenimi on pelkkä domainnimi ja jos tämä sähköpostipalvelin on myös “pääkone”, tulee tähän tiedostoon myös se nimi. Tiedoston sisältö voi siis olla esimerkiksi:

```
# local-host-names - include all aliases for your machine here.
www.raimokoski.com
raimokoski.com
lineox.net
www.lineox.net
```

Uudelleenkäynnistys ja testaus Edellä esiteltiin postipalvelimen perusasetukset. Sendmail on hyvä käynnistää uudelleen niiden konfiguroinnin jälkeen ja tarkistaa, että postin lähetys ja vastaanotto toimii. Lokitiedostoa `/var/log/maillog` kannattaa lukea ja käyttää jossain muualla olevaa sähköpostitiliä (gmail, hotmail, jne.) testiviestien lähetykseen ja vastaanottoon.

Lähes itsenäisen postipalvelimen konfigurointi

Vaikka sinulla ei olisikaan kiinteätä IP-osoitetta, voi silti olla mahdollista, että pystyt konfiguroimaan lähes itsenäisen postipalvelimen. Postin lähetys voidaan hoitaa, kuten edellä kuvattiin luvussa "Välittävän postipalvelimen konfigurointi" ja vastaanotto, kuten edellisessä luvussa "Itsenäisen postipalvelimen konfigurointi". Vastaanotto vaatii tietysti, että palveluntarjoajasi ei ole sulkenut sisääntulevan postin porttia. Koska tiettävästi viestintäviraston määräyksen mukaan kaikista kuluttajaliittymistä eli ei-kiinteällä IP-osoitteella varustetuista Internet-liittymistä postin suora lähetys on estetty, pitää vastaanotto testata kiinteällä IP-osoitteella varustetusta koneesta. Yleensä tämä onnistuu esimerkiksi työpaikalta käsin.

Koska tämä konfiguraatio on edellä esitettyjen yhdistelmä, tapahtuu konfigurointi soveltaen yhdistelemällä niitä.

Virustorjunta

Sähköposti on eräs tavoista, joilla virukset leviävät. Niiden esiintymistiheys vaihtelee, mutta tyypillisesti viesteistä korkeintaan muutama promille sisältää viruksia. Lisäksi ne tarttuvat vain rajoitetusti, joten ongelma on määrällisesti pieni, mutta osuessaan vakava.

ClamAV on yleisesti käytetty virusten "skannausohjelma" ja sen integrointi postipalvelimeen helppoa. CentOS Linux 5.4:ssa sitä ei ole mukana, mutta Fedora Linux:ssa se on, joten vain CentOS Linuxissa tarvitaan seuraava valmisteleva toimenpide:

```
#Valitse koneesi arkkitehtuurille sopiva
#rpm -iv http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.i386.rpm
#rpm -iv http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.x86_64.rpm
```

Lisäksi tiedostossa `/etc/yum.repos.d/rpmforge.repo` pitää muuttaa rivillä "enabled = 0" 0 asetukseksi 1.

ClamAV on jaettu useaan pakettiin. Postipalvelimella tarvitaan seuraavat:

- **clamav-db** – virustietokanta
- **clamav** – virusten skannausohjelma
- **clamd** – virustietokantaa päivittävä demoni

- **clamav-milter** – postipalvelimen integrointi

Nämä kaikki asentuvat riippuvuuksien kautta yksinkertaisesti:

```
# CentOS 5.x
yum install clamav-milter
# Fedora 10
yum install clamav-milter-sendmail
```

Tämän jälkeen on jälleen muokattava `/etc/mail/sendmail.mc`-tiedostoa ja lisättävä seuraava rivi ennen MAILER-rivejä:

```
INPUT_MAIL_FILTER('clamav', 'S=local:/var/run/clamav/clmilter.sock, F=, T=S:4m;R:4m;C:30s;E:10m')dnl
define('confINPUT_MAIL_FILTERS', 'clamav')
```

Fedora Linux 12:ssä riittää yksi rivi:

```
INPUT_MAIL_FILTER('clamav', 'S=local:/var/run/clamav-milter/clamav.sock, F=, T=S:4m;R:4m')dnl
```

Imap- ja pop3-palvelimen konfigurointi

Imap ja pop3 ovat protokollia, joiden avulla käyttäjien sähköpostiohjelmat hakevat postin palvelimelta. Imap on uudempi ja monipuolisempi, mutta niitä voi käyttää rinnakkain ja käsittelemme molempien konfiguroinnin.

Ensiksi pitää tarkistaa, onko imap-palvelinohjelma jo asennettu käskyllä:

```
# rpm -qa \*imap\*
cyrus-imapd-utils-2.3.7-2.el5_3.2
cyrus-imapd-2.3.7-2.el5_3.2
cyrus-imapd-perl-2.3.7-2.el5_3.2
```

Tässä tapauksessa asennettuna oli `cyrus-imapd`, joka on huomattavasti hankalampi konfiguroida. `cyrus-imapd` voidaan asentaa siten, että se on useammassa koneessa ja kuormitus jakautuu niiden kesken. Jos halutaan käyttää `cyrus-imapd`:tä ja se on jo asennettu, sen dokumentointia voi lukea esimerkiksi selaimella syöttämällä osoitekenttään:
`file:///usr/share/doc/cyrus-imapd-2.3.7/install-configure.html`
(tarkista versionumero!).

Fedorassa on tarjolla myös `uw-imap`, joka soveltuu tavanomaiselle kuormalle. CentOSiin se löytyy EPEL-repositorysta ja mikäli repositoryn määrittely on kunnossa, asentuu `uw-imap` `cyrus-imapd`:n tilalle seuraavasti:

```
yum erase cyrus-imapd-utils cyrus-imapd cyrus-imapd-perl
yum --enablerepo=epel install uw-imap-utils uw-imap
```

`uw-imap`:n konfigurointi on hyvin helppoa. Oletuksena mikään protokollista ei ole käytössä ja konfiguointi pitäisikin koostua vain haluttujen sallimisesta. `uw-imap`:n palvelinohjelmat eivät käynnisty suoraan vaan xinetd:n kautta. Palvelinohjelmia on kullekin protokollalle omansa ja niille konfigurointitiedostot:

- **/etc/xinetd.d/imap** - imap-palvelin.
- **/etc/xinetd.d/imaps** - imap-palvelin salauksella
- **/etc/xinetd.d/ipop2** - pop2-palvelin (ei juuri enää käytössä)
- **/etc/xinetd.d/ipop3** - pop3-palvelin
- **/etc/xinetd.d/pop3s** - pop3-palvelin salauksella

Valitse haluamasi protokollat ja muuta niiden konfigurointitiedostoissa rivi “disable” arvoon “no”.

Sähköpostin uudelleenohjaus, aliakset, automatisointi

Sähköpostin uudelleenohjaus avaa useita mahdollisuuksia eli se on hyvin monipuolinen ja tehokas ominaisuus.

Sendmail tarjoaa kaksi tapaa postin uudelleenohjaukseen. Keskitetysti se voidaan määritellä tiedostossa `/etc/aliases`. Tiedoston alussa on ohje sen käyttöön:

```
#       >>>>>>>>>>      The program "newaliases" must be run after
#       >> NOTE >>      this file is updated for any changes to
#       >>>>>>>>>>      show through to sendmail.
```

Eli tee muutokset, talleta ja aja ohjelma `newaliases`, jolloin sendmailin käyttämä tietokanta luodaan uudelleen.

Tavanomaisimpia muutoksia tai lisäyksiä on pääkäyttäjän postin uudelleenohjaus ja pitkien nimien ohjaaminen lyhemmiksi:

```
root:           rk

raimo.koski:    rk
```

Huomaa, että piste käyttäjätunnuksessa voi aiheuttaa ongelmia. Kaikki versiot käyttäjien käsittelykomennoista (shadow-utils-paketti) eivät hyväksy pistettä. Sähköpostiosoitteissa piste on kuitenkin lähes sääntö. Aliaksia käyttämällä ongelma poistuu.

Toinen tavanomainen lisäys on ryhmät ja toimintaan tai tehtävään liittyvät aliakset. Esimerkiksi yrityksessä tilaukset voivat mennä usealle henkilölle, mutta koska henkilöt vaihtuvat, on parempi käyttää aliasta. Alla esimerkki:

```
subscriptions:  tilaukset
lineox.service: tomi, rk
```

Lisäksi jotkut ohjelmat, jotka käyttävät sähköpostia apunaan, vaativat lisäyksiä alias-tietokantaan. Tyypillinen on postituslistaohjelma `mailman`, joka neuvoo lisäämään rivejä, kun luodaan uusia postituslistoja. Alla esimerkki:

```
# mailman mailing list
mailman:              "|/var/mailman/mail/mailman post mailman"
mailman-admin:        "|/var/mailman/mail/mailman admin mailman"
mailman-bounces:      "|/var/mailman/mail/mailman bounces mailman"
mailman-confirm:      "|/var/mailman/mail/mailman confirm mailman"
mailman-join:         "|/var/mailman/mail/mailman join mailman"
mailman-leave:        "|/var/mailman/mail/mailman leave mailman"
mailman-owner:        "|/var/mailman/mail/mailman owner mailman"
mailman-request:      "|/var/mailman/mail/mailman request mailman"
mailman-subscribe:    "|/var/mailman/mail/mailman subscribe mailman"
mailman-unsubscribe:  "|/var/mailman/mail/mailman unsubscribe mailman"
```

Toinen tapa uudelleenohjauksen määrittelyyn on käyttäjäkohtaiset `.forward`-tiedostot. Molemmilla tavoilla saavutetaan lähes sama toiminnallisuus, mutta `/etc/alias`-tiedostoa voi muokata vain pääkäyttäjänä ja sinne voidaan lisätä tavallaan virtuaaleja postilaatikoita, joita vastaavia käyttäjätunnuksia ei ole olemassa.

`.forward`-tiedoston formaatti on varsin yksinkertainen. Kullakin rivillä on joko käyttäjätunnus tai sähköpostiosoite, jonne posti ohjataan. Jos postista halutaan kopio, lisätään myös ko. käyttäjän oma käyttäjätunnus. Sen tilalla on voinut käyttää myös pelkkää pistettä, mutta tämä lyhyempi muoto ei välttämättä toimi. Postin voi myös putkittaa ohjelmalle aivan samoin kuin yllä `mailman`in tapauksessa. Aivan suoraan tämä ei kuitenkaan toimi. Kaikki postia käsittelevät ohjelmat pitää löytyä hakemistosta `/etc/smrsh/`. Tyypillisesti ne ovat linkkejä:

```
# ls /etc/smrsh/ -l
total 0
lrwxrwxrwx    1 root     root           28 maalis 16  2005 autoresponder -> /usr/local/bin/autoresponder
lrwxrwxrwx    1 root     root            8 maalis 16  2005 awk -> /bin/awk
lrwxrwxrwx    1 root     mailman        30 touko   6  2005 mailman -> ../../var/mailman/mail/mailman
```

Lisäksi `smrsh` pitää olla sallittu `/etc/mail/sendmail.mc`-tiedostossa rivillä:

```
FEATURE('smrsh','/usr/sbin/smrsh')dnl
```

Sähköpostin avulla voi automatisoida uskomattoman paljon. Osittain sen varaan voi rakentaa esimerkiksi kaupan. Esimerkiksi sähköisiä maksuja käsittelevä PayPal voidaan konfiguroida siten, että maksutapahtuman jälkeen tulee tietyn muotoinen sähköposti, joka pitää tunnistaa ja sen jälkeen "filtteri" suorittaa halutut toimenpiteet, esimerkiksi luo käyttäjätunnuksen ja sille salasanan www-palvelimen jonkin hakemiston `.htaccess`-tiedostoon, jolloin käyttäjä pääsee kyseiseen hakemistoon lataamaan ostamansa ohjelman, tiedoston tms. Filtteri voi myös lähettää vastausviestin, jossa tuo uusi käyttäjätunnus ja salasana on.

Sähköposti ei kuitenkaan ole ainoa tapa käsitellä maksutapahtumia. Esimerkiksi PayPal voidaan konfiguroida lähettämään myös IPN-viesti ja valmiita kauppasovelluksia on saatavana jopa ilmaiseksi, joten sähköpostifiltterien teko itse ei enää ole välttämättä järkevin tapa. Pienimuotoiseen ja erikoisiin tarpeisiin se kuitenkin on näppärä. Sähköposti on kuitenkin niin yleisesti käytetty ja hyvin tuettu, että sen varaan on rakennettu ja varmasti tullaan rakentamaankin monenlaisia automatisoituja ratkaisuja.

Lineox Oy myi pääsyoikeuksia tiedostolataukselle www- ja rsync-palvelimilta. Maksut kulkivat PayPalin kautta ja niistä tuli viesti osoitteeseen lineox@lineox.net. Käyttäjän lineox kotihakemistossa oli `.forward`-tiedosto, jossa rivi:

```
''|awk -f /home/lineox/acquota.awk''
```

käynnisti filtterin, joka tunnisti myydyn tuotteen, loi tarvittaessa tunnuksen salasanoineen, määritteli sen www- tai rsync-palvelimelle ja lähetti vastausviestissä lataamisessa tarvittavat tiedot. Kaikki tapahtui automaattisesti ja asiakas sai vastausviestinsä yleensä vain sekuntien viiveellä.

Roskapostin torjunta

Roskaposti on ongelma, josta on käytännössä mahdoton päästä eroon, mutta sitä voi kuitenkin vähentää. Tässä luvussa esitellään menetelmät, joilla pystytään estämään tyypillisesti noin 90 prosenttia roskapostista. Lopussa esitellään skripti, joka näyttää tilastotietoja onnistumisesta. Alla sen tuloste:

```
# spamstats
Total accepted:     298
Blocked due to a virus:   0
csma.biz blacklist:       0
spamhaus.org blacklist:   3049
dsbl.org blacklist:       0
spamcop.net blacklist:    3
```

```
njabl.org blacklist:      19
ahbl.org blacklist:       0
sorbs.net blacklist:      4
ordb.org blacklist:       0
Blacklist total blocked:  3075
DNS blocked:              2
Delay blocked:            631
Total received:     4006
Total blocked:      3708
Percentage blocked: 92.5612
```

Virusten torjunta esiteltiinkin jo aiemmin eikä viruspostit puhtaasti ottaen ole roskapostia, ainakaan aina.

Suurin torjuntaprosentti saavutetaan mustilla listoilla. Ne ovat teknisesti toteutettu siten, että mustan listan ylläpitäjä päivittää tietoja tunnetuista roskapostittajista nimipalvelimeen. Sendmail kysyy saapuvan postin lähetysosoitetta ko. nimipalvelimelta ja vastauksen perusteella joko hylkää tai päästää viestin seuraaviin tarkastuksiin.

Rivillä “Delay blocked” on myös suuri määrä hylättyjä viestejä. Tämä roskapostin esto perustuu siihen, että roskapostittajien käyttämät ohjelmat on viritetty niin nopeiksi, että ne eivät viitsi odottaa standardin edellyttämään aikaa postipalvelimen kättelykuittauksille. Tätä roskapostin estoa käyttävä postipalvelin vaikuttaa siis hitaalta, mutta vain yksittäisille lähettäjille. Se pystyy kuitenkin käsittelemään rinnakkain useita viestien lähettäjiä, joten käytännössä viive ei hidasta.

Rivillä “DNS blocked” on niiden viestien lukumäärä, joiden lähettäjää nimipalvelimet eivät tunne. Tämä esto on helppo ottaa käyttöön, mutta tehokas se ei ole.

Alla ovat `/etc/mail/sendmail.mc`-tiedoston rivit, jotka liittyvät mustiin listoihin:

```
FEATURE(‘blacklist_recipients’)dnl
dnl FEATURE(‘dnsbl’, ‘bl.csma.biz’,  ‘ ••• SPAM Blocked from $&{client_addr} - See http://bl.csma.biz/ .’)dnl
FEATURE(‘dnsbl’, ‘zen.spamhaus.org’, ‘550 Mail from  $&{client_addr}  refused - see http://www.spamhaus.org/zen/’)dnl
dnl FEATURE(‘dnsbl’, ‘list.dsbl.org’, ‘550 Mail from  $&{client_addr}  refused - see http://dsbl.org/’)dnl
FEATURE(‘dnsbl’, ‘bl.spamcop.net’, ‘450 Mail from  $&{client_addr}  refused - see http://spamcop.net/bl.shtml’)dnl
FEATURE(‘dnsbl’, ‘combined.njabl.org’, ‘450 Mail from  $&{client_addr} refused - see http://njabl.org/lookup?$&{client_addr}’)dnl
dnl FEATURE(‘dnsbl’, ‘dnsbl.ahbl.org’, ‘550 Mail from  $&{client_addr} refused - see http://www.ahbl.org/tools/lookup.php?ip=’’$&{client_addr}’’’)dnl
FEATURE(‘dnsbl’, ‘dnsbl.sorbs.net’, ‘554 Rejected  $&{client_addr} found in dnsbl.sorbs.net’)dnl
```

Osa mustista listoista on ajan myötä lopettanut toimintansa ja sen takia joillakin riveillä on alussa “dnl” eli ne on kommentoitu pois käytöstä.

Viive määritellään rivillä:

```
FEATURE(‘greet_pause’, ‘1500’)dnl
```

Tuntemattomat lähettäjät estetään kommentoimalla rivi, joka on alla alimmaisena:

```
dnl We strongly recommend to comment this one out if you want to protect
```

```
dnl yourself from spam. However, the laptop and users on computers that do
dnl not have 24x7 DNS do need this.
dnl FEATURE(‘accept_unresolvable_domains’)dnl
```

Lopuksi vielä skripti `/usr/local/bin/spamstats`

```
#!/bin/bash
if [ $1x = "x" ]
then
  LOGS=/var/log/maillog
else
  LOGS=$@
fi
totacc=‘grep " to=" $LOGS | wc -l‘
virusblock=‘grep "Milter: data, discard" $LOGS | wc -l‘
CSMA=‘grep "bl.csma.biz" $LOGS | wc -l‘
spamhaus=‘grep www.spamhaus.org $LOGS | wc -l‘
dsbl=‘grep dsbl.org $LOGS | wc -l‘
cop=‘grep spamcop.net $LOGS | wc -l‘
njabl=‘grep njabl.org $LOGS | wc -l‘
ahbl=‘grep dnsbl.ahbl.org $LOGS | wc -l‘
sorbs=‘grep dnsbl.sorbs.net $LOGS | wc -l‘
ordb=‘grep "see http://www.ordb.org/faq/" $LOGS | wc -l‘
bls=‘echo $CSMA  $spamhaus  $dsbl  $cop $njabl $ahbl $sorbs $ordb | awk ’{print $1+$2+$3+$4+$5+$6+$7+$8}’‘
dns=‘grep "Domain of sender address" $LOGS | wc -l‘
delb=‘grep "due to pre-greeting traffic" $LOGS | wc -l‘
totb=‘echo $virusblock $bls $dns $delb | awk ’{print $1+$2+$3+$4}’‘
totrec=‘echo $virusblock $totacc $bls $dns $delb | awk ’{print $1+$2+$3+$4+$5}’‘
perblock=‘echo $totb $totrec | awk ’{print  $1*100/$2}’‘
echo  "Total accepted:    " $totacc
echo  "Blocked due to a virus:  " $virusblock
echo  "csma.biz blacklist:      " $CSMA
echo  "spamhaus.org blacklist:  " $spamhaus
echo  "dsbl.org blacklist:      " $dsbl
echo  "spamcop.net blacklist:   " $cop
echo  "njabl.org blacklist:     " $njabl
echo  "ahbl.org blacklist:      " $ahbl
echo  "sorbs.net blacklist:     " $sorbs
echo  "ordb.org blacklist:      " $ordb
echo  "Blacklist total blocked: " $bls
echo  "DNS blocked:             " $dns
echo  "Delay blocked:           " $delb
echo  "Total received:    " $totrec
echo  "Total blocked:     " $totb
echo  "Percentage blocked:" $perblock
```

Skripti ei tarvitse parametriä, mutta oletuksena olevan viimeisen lokitiedoston sijaan voi antaa vanhemman lokitiedoston nimen.