Multidomain-sähköpostipalvelin

Teppo Vanhatalo

Opinnäytetyö

Ammattikorkeakoulututkinto

Savonia
ammattikorkeakoulu

SAVONIA-AMMATTIKORKEAKOULU **OPINNÄYTETYÖ**
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Teppo Vanhatalo	
Työn nimi Multidomain-sähköpostipalvelin	
Päiväys 11.12.2011	Sivumäärä/Liitteet 44
Ohjaaja(t) Kalevi Kolehmainen, lehtori	
Toimeksiantaja/Yhteistyökumppani(t) ITC-Solution Group Oy	

Tiivistelmä

Tämän insinöörityön aiheena oli toteuttaa multidomain-sähköpostipalvelin tehokkaalla roskaposti- ja haittaohjelmasuodatuksella hosting-palveluja tarjoavan yrityksen käyttöön.

Työn teoriaosuudessa on käsitelty eri ohjelmistovaihtoehtoja sekä käyttöön valittujen ohjelmistojen valintakriteerejä. Tietoa ohjelmistoista haettiin Internet-sivustoilta sekä testaamalla joitakin ohjelmistoja itse. Työssä käytettiin vain avoimen lähdekoodin ohjelmistoja, jotta tarvittaessa muutoksien tekeminen olisi mahdollista. Myös käyttöjärjestelmäksi valittiin avoimen lähdekoodin Linux-jakelu.

Työn käytännön osuudessa toteutettiin palvelinasennus kaikkine tarvittavine ohjelmistoineen, sekä toteutettiin usean asiakkaan käyttäjätilien siirto toisen palveluntarjoajan palvelimelta uudelle juuri asennetulle palvelimelle. Asennus pyrittiin tekemään tiukalla aikataululla, jotta palvelimen toiminnan testaamiselle jäisi tarpeeksi aikaa. Asiakkaalle tämä muutos uudelle palvelimelle näkyi tehostuneena roskapostien suodatuksena sekä parempina käyttöliittyminä palveluiden asiakasrajapinnoissa.

Avainsanat
multidomain, sähköpostipalvelin, Dovecot, Postfix, Amavisd-new, roskaposti, suodatus

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Teppo Vanhatalo			
Title of Thesis Multidomain Email Server			
Date	11 December 2011	Pages/Appendices	44
Supervisor(s) Mr. Kalevi Kolehmainen, Lecturer			
Project/Partners ITC-Solution Group Oy			

Abstract

The aim of this thesis was to design and install a multidomain capable email server with highly efficient spam and malware filtering for a company which offers hosting services to its customers.

First, the software used in this thesis project was examined on the Internet. Then some software was also tested on the server with other software to evaluate how they would work together. Only open-source software was used, mainly for economic reasons, but also to allow later modification, if needed. The selected operating system was also an open-source based Linux system.

The installation of the server hardware and software was carried out in quite a tight schedule to allow more time on testing and hardening the system. Plenty of existing customers' user accounts were transferred to the new server. The outcome to the customers was better spam and malware filtering and also better user interface on various services visible to the customer.

Keywords
Multidomain, email server, Dovecot, Postfix, Amavisd-new, Spam filtering

SISÄLTÖ

TERMIT JA LYHENTEET

AJAX	Asymmetric JavaScript And XML, tapa jolla web-sovelluksien käyttöliittymistä saadaan tehtyä vuorovaikutteisempia
Blacklist	Estolista
FQDN	Fully Qualified Domain Name, isäntänimi joka sisältää sekä nimen että jonkun TLD päätteen.
Greylisting	Roskapostin estotapa, jossa palvelin ei ota viestiä vastaan tuntemattomalta palvelimelta ja käskee lähettävää palvelinta odottamaan ennen viestin uudelleenlähetystä.
HELO/EHLO	Komento, jolla lähettävä palvelin aloittaa SMTP yhteyden. Tämä on yleensä FQDN isäntänimi.
IMAP	Internet Message Access Protocol, sähköpostien lukemiseen tarkoitettu protokolla
ISP	Internet Service Provider, palveluntarjoaja
Live-snapshot	Virtuaalikoneesta sen käynnissä ollessa otettava tilatiedosto, joka sisältää virtuaalikoneen sen hetkisen tilan
Milter	Mail Filter, Sendmailin sekä Postfixin tukema tapa sähköpostiviestien suodattamiseen
MTA	Mail Transfer Agent, ohjelmisto joka välittää sähköpostiviestejä
POP3	Post Office Protocol 3, yksinkertainen sähköpostien hakemiseen tarkoitettu protokolla
Relaydomain	Ei-paikallinen domain, jonka sähköpostiviestit välitetään eteenpäin.
SAS	Serial Attached SCSI, massamuistien liittämiseen käytetty nopeaan tiedonsiirtoon pystyvä väylästandardi
SMTP	Simple Mail Transfer Protocol, protokolla jota käytetään sähköpostiviestien välitykseen sähköpostipalvelimille
TLD	Top Level Domain
Webmail	Selaimen kautta käytettävä sähköposti
Whitelist	Sallittujen kohteiden lista

1 JOHDANTO

ITC-Solution Group Oy tarjoaa asiakkailleen tukipalveluiden lisäksi myös kaikenlaisia domainpalveluita. Aiemmin nämä palvelut oli hankittu yhteistyökumppaneiden kautta ja jälleenmyyty asiakkaille. Tämä malli ei kuitenkaan ollut paras mahdollinen. Muutoksien, lisäominaisuuksien tai asiakaskohtaisten räätälöityjen ratkaisujen hankkiminen näin oli vaivalloista, hidasta sekä kallista. Virhetilanteiden sattuessa ei aina ollut tietoa, oliko vika yhteistyökumppanin tietojärjestelmissä vai tietoliikenneyhteyksissä ja mikä olisi vian arvioitu kesto.

Tähän ongelmaan ITC-Solution Group Oy halusi kustannustehokkaan, turvallisen, varmatoimisen sekä helposti hallinnoitavan ratkaisun. Koska yrityksen tietoliikenneyhteyksissä oli reilusti ylimääräistä kapasiteettia ja koska kapasiteetti oli helposti laajennettavissa tarpeen vaatiessa, todettiin parhaaksi ratkaisuksi uuden, tähän tarkoitukseen omistetun palvelinlaitteiston hankkiminen. Koska ratkaisun piti olla helposti muokattavissa ja samalla kustannustehokas, päätettiin alustaksi ottaa sopiva Linux-jakelu sekä hyväksitodetut open-source-palvelinohjelmistot. Näille ohjelmistoille piti myös löytää, tai tarvittaessa itse kehittää, sopivat hallintatyökalut.

Opinnäytetyön kirjallisessa osassa käsitellään valittujen ohjelmistojen ominaisuuksia, valintaperusteita, vaihtoehtoja sekä valittujen ohjelmistojen asennusta kohdeympäristöön. Myös hallintasovellusten muokkausta sekä uusien sovellusten luontia käsitellään tässä osassa.

2 LAITTEISTON VALINTA

Itse sähköpostijärjestelmä ei tässä tapauksessa vaadi laitteistolta kovinkaan suurta suorituskykyä. Periaatteessa mikä tahansa nykyaikainen palvelinlaitteisto omaa tarvittavan suorituskyvyn palveluiden suorittamiseen.

Koska tilaajapuolelta tuli toivomus, että järjestelmä ajettaisiin virtuaalialustalla siirrettävyyden ja koko järjestelmän varmuuskopioinnin yksinkertaistamisen vuoksi, laitteiston tehontarve oli hieman suurempi, joskaan ei merkittävissä määrin. Myös laajennusvara tuli ottaa huomioon. Vaikka sähköpostijärjestelmä on tällä hetkellä ainoa järjestelmä, jota palvelinlaitteistossa ajetaan, hankittiin heti sellainen laitteisto, jonka kapasiteetti mahdollistaisi muidenkin virtuaalijärjestelmien ajamisen ilman erillistä laajennusta.

Laitteistoksi valittiin Fujitsu-Siemensin TX-sarjan palvelinlaitteisto, jossa on moniprosessorituki, nopeat SAS-levyt sekä riittävä määrä käyttömuistia. Varmuuskopiointia varten hankittiin ulkoisia kiintolevyjä, jotta varmuuskopiot saadaan helposti siirrettyä fyysisesti eri tilaan kuin palvelinlaitteisto on. Myös nauha-asemaa harkittiin, mutta varmistusnauhat, joiden kapasiteetti riittäisi tähän tarkoitukseen, olisivat kustannuksiltaan olleet huomattavasti kalliimmat. Lisäksi ulkoisten kiintolevyjen käyttöä puolsi niiden monikäyttöisyys ja yhteensopivuus. Tarvittaessa ne voidaan kytkeä käytännössä mihin tahansa PC-koneeseen, jolloin varmuuskopioiden tarkastelu ja käyttö onnistuu, vaikka alkuperäinen laitteisto olisikin rikkoontunut.

3 OHJELMISTOJEN VALINTA

Pääkriteerinä ohjelmistojen valinnassa oli kustannustehokkuus, toisin sanoen pyrittiin käyttämään täysin ilmaisia ohjelmistoja. Tuen saamista mahdollisissa ongelmatilanteissa myös tulevaisuudessa pidettiin tärkeänä. Siksi ohjelmistoiksi pyrittiin valitsemaan sellaisia ohjelmistoja, joilla on vakiintunut käyttäjäkunta. Näin voidaan olla varmempia tuen jatkuvuudesta sekä ohjelmistoista saatavilla olevan informaation laajuudesta.

3.1 Käyttöjärjestelmän sekä virtuaaliympäristön valinta

Koska kustannustehokkuus oli etusijalla, järkevimmäksi käyttöjärjestelmävalinnaksi osoittautui Linux. Linuxin moninaisesta jakeluvalikoimasta valittiin OpenSUSE-jakelu. Valinta perustui omiin käyttökokemuksiin ja etenkin siihen, että sitä kehitetään aktiivisesti ja sillä on iso käyttäjäkunta. Tällöin avun saaminen mahdollisissa ongelmatilanteissa helpottuu.

Virtuaaliympäristön valinnassa valinnanvaraa ei ollut kovinkaan paljon, koska ohjelmiston tuli olla ilmainen ja sen piti tukea ns. live-snapshotteja järjestelmästä. Tämä ominaisuus mahdollistaa koko järjestelmän varmuuskopioimisen sen ollessa käynnissä. Virtuaaliympäristöksi valittiin VMWaren ilmainen VMWare-server-ohjelmisto, joka sisältää halutut ominaisuudet. Haittapuolena on se, että kyseisen virtuaaliympäristön kehitys on lopetettu. Muita vaihtoehtoja olivat KVM, XEN sekä VMWare ESXi, mutta näiden tarjoamat ominaisuudet eivät olleet valintahetkellä sellaiset, että valinta olisi kohdistunut johonkin näistä.

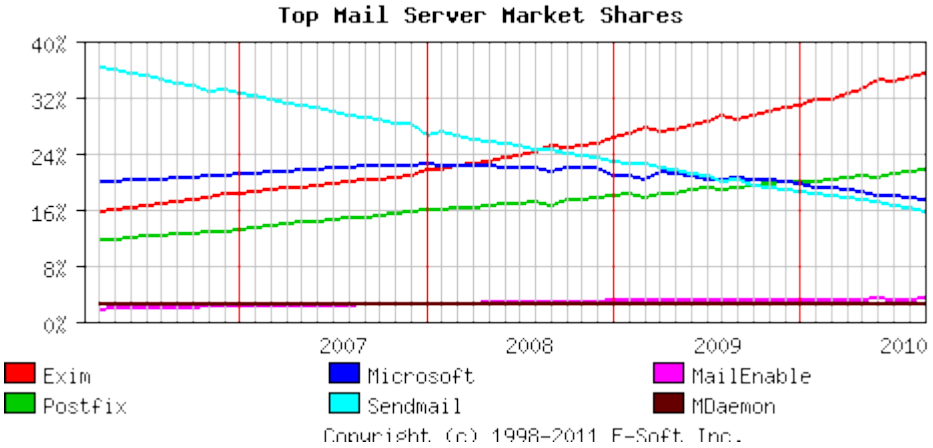
VMWare-server-ohjelmiston valintaa puolsi myös se, että pahan laiterikon yhteydessä voisi hätätilanteessa siirtää koko virtuaalikoneen normaaliin PC-koneeseen, koska VMWare-serverin virtuaalikoneet ovat yhteensopivia myös VMWaren muiden ohjelmistojen, esimerkiksi ilmaisen VMWare-playerin, kanssa. VMWare-serverillä luodut virtuaalikoneet ovat myös tarvittaessa tuotavissa VMWaren ESX-järjestelmiin, kunhan virtuaalikoneet on luotu sopivia yhteensopivuusasetuksia käyttäen (VMWare 2011).

3.2 Muiden ohjelmistojen valinta

Muut käytetyt ohjelmistot voidaan jaotella seuraavasti: MTA, sisällöntarkistus, IMAP- ja POP3-palvelinohjelmistot, webmail, hallintatyökalut sekä roskapostisuodattimen asiakasrajapinta, jossa voi tarkastella ja joko vapauttaa tai tuhota suodattimeen jääneitä viestejä. Myös lähettäjien white- ja blacklisting onnistuu tätä kautta.

3.3 MTA valinta

Ohjelmistojen valinta aloitettiin MTA:n (Mail Transfer Agent) valinnalla. Valinnanvaraa oli jonkin verran, mutta päätös oli kuitenkin helppo. Valinta tehtiin kolmen suosituimman ilmaisen MTA-ohjelmiston välillä (E-Soft Inc. 2010). Suosituin näistä oli Exim, sitten Postfix ja kolmanneksi suosituin oli Sendmail (KUVA 1. MTA-vertailu). Microsoft Exchangen osuus oli Sendmailia korkeampi, mutta koska se ei ole ilmainen eikä toimi Linux-alustalla, sen osuutta ei otettu huomioon MTA:ta valittaessa.



KUVA 1. MTA-vertailu

3.3.1 Exim

Exim on tehokas ja erittäin monipuolisesti konfiguroitavissa oleva MTA-ohjelmisto. Sitä on kehitetty jo vuodesta 1995 ja sillä on laaja käyttäjäkunta. Exim on suosittu kaikenlaisissa ympäristöissä muutaman käyttäjän testiservereistä tuhansien käyttäjien ISP-tason toteutuksiin.

Juuri erittäin monipuoliset konfiguraatiomahdollisuudet ovat yksi Eximin suosion peruspilareista. Sillä on mahdollista ohjata posteja lähes rajattomasti eri sääntöjen mu-

kaan. Esimerkiksi voit ohjata käyttäjälle B maanantai-iltapäivisin käyttäjälle A tulevat viestit, joiden otsikossa on sana ”kirsikka”.

Vaikka Eximillä on maine ollut huonohko tietoturvan osalta lähinnä Exim3:n takia, nykyisestä versiosta ei enää ole löydetty sellaisia ongelmia. Toisaalta lähes loputtomien konfiguraatiomahdollisuuksien takia voi tehdä helpommin virheitä, jotka johtavat jonkinasteisiin tietoturvaongelmiin. (Exim 2011)

3.3.2 Sendmail

Sendmail lienee vanhin vielä aktiivisessa kehityksessä oleva MTA-ohjelmisto. Sen kehitys aloitettiin jo vuonna 1982 ja se olikin pitkään suosituin MTA-ohjelmisto. Sen suosio on kuitenkin hiipunut nopeasti. Muun muassa E-Soft Inc:in tekemän tutkimuksen mukaan vuoden 2001 noin 40 % osuudesta oli tiputtu vuonna 2007 reiluun 29 % osuuteen ja vuoden 2010 tutkimuksessa osuus oli enää reilu 17 % (Bernstein 2001, E-Soft Inc. 2007, 2010).

Osaltaan suosion hiipumiseen on luultavasti vaikuttanut Sendmailin huono maine, sen vakavat tietoturvaongelmat sekä tietenkin kilpailijoiden kehittyminen. Sendmail toimii jollain tavalla perusasetuksillakin, mutta sen konfiguroiminen kunnolla on vaikeaa. Sitä pidetäänkin erittäin vaikeana konfiguroitavana eikä sitä ole todellakaan suunnattu aloittelijoille. Sitä ei myöskään pidetä yhtä tehokkaana kuin nykyisiä kilpailijoita (Howard 2004).

Sen dokumentaatio on erittäin hyvä, mutta kuten jo mainittiin, sen konfiguraatiotiedosto on erittäin iso, vaikeaselkoinen ja sen syntaksi tottumattomalle hankalaa. Tuntuukin siltä, että se alkaa pikkuhiljaa väistyä markkinoilta eikä sitä oteta enää juurikaan laajalti käyttöön uusissa järjestelmissä.

Vaikka ohjelmassa onkin hyvä laajennettavuus erilaisten milter-nimisten lisäosien avulla, on sen käyttöönotto ja asetusten tarvittava säätäminen aivan liian hankalaa jotta se olisi ollut järkevä valinta tämän projektin MTA-ohjelmistoksi. (Sendmail Inc. 2011)

3.3.3 Postfix

Postfix on tehty vuonna 1997 ja sen kehittämisen lähtökohtana oli luoda turvallinen sekä silti suorituskykyinen MTA-ohjelmisto. Oikein konfiguroituna se lieneekin turvallisin MTA-ohjelmisto tällä hetkellä. Toisin kuin muissa ohjelmistoissa, joiden kehityksestä on vastannut yhteisö tai muu isompi kehitystiimi, on Postfixin kirjoittanut lähes yksin Wietse Venema, joka johtaa kehitystä edelleen. Hän kehitti Postfixin vaihtoehdoksi turvattomammalle Sendmailille ja ehkä juuri sen takia siihen sisällytettiin tuki Sendmailin käyttämille milter-lisäosille, jotta Sendmailin käyttäjien olisi helpompi siirtyä käyttämään Postfixiä.

Turvallisuuden ei tarvitse kuitenkaan rajoittaa toiminnallisuutta tai tehdä hallinnasta ylitsepääsemättömän hankalaa. Postfixiä on helppo konfiguroida ja sen laajennettavuus on hyvä, joskaan ei niin erinomainen kuin Eximillä. Se on myös erittäin suorituskykyinen, joten edes nopeudesta ei ole jouduttu tinkimään turvallisuuden takia.

Postfix on myös monen Linux-jakelun vakio MTA-ohjelmisto ja ehkä juuri siksi sen konfiguroimisesta löytyy paljon ohjeita niitä tarvitsevalle. Myös Postfixin asetustiedostot ovat hyvin kommentoituja, joten erityisempiä ohjeita ei välttämättä sen käyttöönotossa tarvitse, kunhan vain jaksaa lukea asetustiedoston kommentit tarkasti. Sen dokumentointi on todella kattava ja aktiiviselta yhteisöltä saa kysyttäessä neuvoja varsin nopeasti.

Ohjelmiston turvallisuus sekä aikaisemmat kokemukseni Postfixistä ja sen hallinnoinnista vaikuttivat valintaan suuresti. Myös tiedossaolevan helppokäyttöisen www-pohjaisen hallintaohjelmiston olemassaolo vaikutti valintaan. Suosituksieni pohjalta MTA-ohjelmistoksi päätettiin valita Postfix. (Postfix, 2011)

3.4 Sisällöntarkistus

Vaikka suurin osa roskapostista saadaan torjuttua jo erilaisin lähettäjän ip-osoitteen tarkistamiseen perustuvin estolistoin, greylisting-periaatteella sekä muiden jo yhteyttä muodostettaessa käytettävien tarkistuskeinojen avulla, on sisällöntarkistus tärkeä osa sähköpostijärjestelmää. Tarkistuksella voidaan tehokkaasti estää roskapostin sekä virusten leviäminen.

3.4.1 Amavisd-new

Sisällöntarkistuksen perustana on Amavisd-new niminen ohjelmisto, joka toimii rajapintana MTA-ohjelmiston sekä sisällöntarkistusohjelmistojen välillä. Nimi Amavisd tulee sanoista A Mail Virus Scanner Daemon. Se on hyvin yhteensopiva erilaisten ohjelmistojen kanssa, koska se osaa kommunikoida MTA-ohjelmistojen kanssa SMTP-protokollaa käyttäen.

Amavisd-new ottaa viestit vastaan SMTP-protokollaa käyttäen, tekee tarkastuksen ja jos viesti läpäisi tarkastuksen, niin viesti välitetään takaisin MTA-ohjelmalle. Jos viesti ei läpäise tarkistusta, lähettää Amavisd-new MTA-ohjelmistolle virhekoodin sekä syyn miksi viestiä ei toimitettu perille. Tämän jälkeen Amavisd-new joko hylkää viestin tai laittaa viestin karanteeniin riippuen vastaanottajan konfiguraatioasetuksista. Jos näitä ei ole asetettu, niin käytetään globaalisti konfiguroituja arvoja.

Amavisd-new toimii monissa eri ympäristöissä sen takia, että se on kirjoitettu perl-ohjelmointikielellä, josta taas on versionsa hyvinkin monelle eri käyttöjärjestelmälle. Ainoat vaatimukset ovat perl-tuki sekä yhteydet sähköpostipalvelimeen, koska Amavisd-new voi sijaita fyysisesti eri palvelimella kuin itse MTA-ohjelmisto. Asennetussa järjestelmässä Amavisd-new välittää sähköpostiviestin kahdelle eri ohjelmalle, jotka tekevät roskaposti- ja virustarkistukset.

3.4.2 Roskapostin tarkistus

Roskapostin suodatukseen valittu SpamAssassin on ohjelma, joka tutkii viestin sisältöä erilaisin menetelmin ja yrittää tunnistaa roskapostit Bayesilaisen suodatuksen menetelmällä. Siinä lasketaan todennäköisyys roskapostille viestin otsaketiedoista sekä sen sisällöstä Bayesin teoreemasta johdetun kaavan avulla (Process Software 2010). Sitten SpamAssassin palauttaa Amavisd-new:lle tiedon viestin saamasta pistemäärästä. Pistemäärää verrataan konfiguroituihin raja-arvoihin, joiden mukaan päätetään mitä viestille tehdään. Tätä käsitellään lisää kappaleessa 5.2.

3.4.3 Virustarkistus

Viesti välitetään myös virustutkalle, joksi tässä tapauksessa valittiin ClamAV. ClamAV on yksi harvoista Linuxille tehdyistä ilmaisista virustutkista, joka toimii myös hyvin

sähköpostipalvelimen virustutkana. Sen konfigurointi on erittäin yksinkertaista ja se sisältää myös päivitystyökalun, joka päivittää virustunnisteita halutuin aikavälein. ClamAV:lla onkin aktiivinen kehittäjätiimi, joka päivittää virustunnisteita monta kertaa päivässä. Se on huomattava saavutus ilmaisohjelmalle. Tietenkään virustunnisteet eivät ole aivan yhtä korkealuokkaisia kuin kaupallisilla ohjelmilla, mikä onkin ymmärrettävää käytössä olevien resurssien vuoksi. Tunnistus on kuitenkin kohtuullisella tasolla ja ClamAV tunnistaa myös osan huijausviesteistä. Tarkastettuaan viestin ClamAV palauttaa tiedon tarkastuksesta Amavisd-new:lle, joka sitten tarkastuksen tuloksesta sekä vastaanottavan käyttäjän asetuksista riippuen joko välittää viestin eteenpäin, tuhoaa sen, tai laittaa viestin karanteeniin.

3.5 IMAP- ja POP3-ohjelmiston valinta

Jotta postia voisi hakea palvelimelta, pitää siihen tarjota sopiva rajapinta. Näistä selvästi yleisimmät ovat standardinmukaiset POP3 ja IMAP protokollat. Vaihtoehtoja oli useita, mutta vertailtavaksi valittiin kolme suosittua ohjelmistoa.

3.5.1 Cyrus

Cyrus on erittäin monipuolinen ja tehokas IMAP- ja POP3-palvelinohjelmisto. Se on suosittu erittäin isoissa ympäristöissä suorituskykynsä vuoksi. Se ei kuitenkaan ole täysin IMAP-protokollaa noudattava (Sirainen 2011) ja se on vaikeampi konfiguroida kuin monet muut kilpailijansa.

Cyrus käyttää sähköpostien säilyttämiseen omaa paranneltua versiotaan maildir-formaatista, joten siitä ei ole niin helppoa vaihtaa toiseen ohjelmistoon kuin muista perinteistä maildir-formaattia noudattavista ohjelmistoista. Cyruksen oma versio on kuitenkin nopeampi kuin perinteinen maildir, koska Cyrus käyttää apunaan indeksointia.

Cyrus tukee erilaisia kehittyneitä ominaisuuksia kuten quotaa ja pääsylistoja. Quotalla voidaan rajata käyttäjän varaamaa levytilaa ja pääsylistoilla voidaan antaa eri käyttäjille erilaisia oikeuksia sähköpostilaatikkokohtaisesti.

3.5.2 Courier

Courier Mail Server ei ole pelkkä IMAP- ja POP3-palvelinohjelmisto, vaikka sitä voi sellaisenakin käyttää. Siinä on itsessään mukana myös muun muassa MTA ja Web-mail-toteutukset. Viestien säilömiseen se käyttää pääasiassa maildir-formaattia, mutta se tukee myös vanhaa, yleisesti POP3-ympäristöissä käytettyä, mbox-formaattia. Kuten muutkin vertailun IMAP- ja POP3-ohjelmistot, se voi käyttää tietokantaa käyttäjätietojen säilyttämiseen ja käyttäjien autentikointiin.

Courier-IMAP ja Courier-POP ovat suosittuja komponentteja hosting-palvelujen jälleenmyyjien keskuudessa, johtuen luultavasti siitä että kaksi käytetyintä hallintapaneeliohjelmistopakettia, Plesk ja CPanel, käyttävät Courier-IMAP ja Courier-POP ohjelmistoja sähköpostiohjelmistoinaan. Myös alhainen muistinkäyttö ja prosessoritehon tarve edesauttaa ohjelmiston valintaa jaettujen resurssien ympäristöihin.

Courieria on moitittu hitaudesta verrattuna muihin ohjelmistoihin. Hitauteen lienee syynä se, ettei Courier käytä minkäänlaista indeksointia tai välimuistia postilaatikoissa, jolloin laatikon käsittely voi olla huomattavasti hitaampaa kuin kyseisiä tekniikoita käyttävillä kilpailijoillaan. Tämä nopeusero aiheuttanee ongelmia vasta suuremmilla sähköpostilaatikoilla, joissa voi olla satoja ellei jopa tuhansia viestejä.

3.5.3 Dovecot

Dovecot on suomalaisen Timo Siraisen kehittämä ja ylläpitämä IMAP- ja POP3-palvelinohjelmisto. Sen kehityksessä turvallisuus on pidetty etusijalla, mutta siitä huolimatta se on yksi suorituskykyisimmistä ja monipuolisimmista IMAP-palvelinohjelmistoista. Se on myös yksi harvoista IMAP-standardin täysin täyttävistä palvelinohjelmistoista (Sirainen 2011).

Dovecot käyttää maildir-formaattia sähköpostin varastointiin ja osaa käyttää myös vanhaa mbox-formaattia. Sillä on oma indeksointimenetelmänsä, jonka ansiosta se on huomattavasti nopeampi käsittelemään sähköpostilaatikoita kuin ilman indeksointia tapahtuvaa käsittelyä käyttävät ohjelmistot.

Dovecot on myös erittäin helppo konfiguroitava. Sen konfiguraatiotiedosto on hyvin kommentoitu ja selkeä. Siinä on helppoa ottaa käyttöön käyttäjien todentaminen tietokantaa hyväksikäyttäen, mikä taas helpottaa sen käyttöönottamista multidomain-

järjestelmissä, joissa kaikki käyttäjäinformaatio on säilötty tietokantoihin. Tämä myös helpottaa omien, varsinkin selainkäyttöliittymällä toteutettujen, hallintatyökalujen kehittämistä.

3.6 Webmail-vertailu

Webmail-toteutusta varten tutkittiin kolmea eri vaihtoehtoa, jotka olivat Horde, Squirrelmail ja Roundcube. Jokaisessa oli hyvät puolensa, mutta lopulta ratkaisu oli helppo. Seuraavissa luvuissa on lyhyt kuvaus jokaisesta ehdokkaasta.

3.6.1 Horde framework

Horde sisältää paljon muuta kuin pelkän webmail-osan. Horden ominaisuuksiin kuuluu muun muassa kalenteri, muistio sekä osoitekirja. Siihen on saatavilla myös lukuisia eri lisäosia. Ehkä juuri laajuutensa vuoksi Hordella on ollut jonkin verran pahoja tietoturvaongelmia, tosin uudemmista versioista niitä ei ole enää löytynyt.

Vaikka itselläni olikin aikaisempaa kokemusta vain Hordesta, ei sitä valittu webmail-toteutukseksi. Tarkoituksena oli asentaa mahdollisimman kevyt ohjelmisto, jolla on hyvä käyttöliittymä. Mainitut ominaisuudet eivät ole Horden vahvuuksia. Myös aikaisemmat tietoturvaongelmat arveluttivat. (Horde LLC 2011)

3.6.2 Squirrelmail

Squirrelmail on verrattain vanha webmail-ohjelmisto. Sen kehitys aloitettiin jo 1999, ja sen käyttöliittymä muistuttaakin kovasti tuon ajan tyypillistä web-sivuston käyttöliittymää. Jotain hyvääkin tästä tosin on, sillä Squirrelmail on erittäin yhteensopiva eri selainten ja alustojen kanssa. Käyttöliittymä on toteutettu standardinmukaisella html-kielellä eikä se vaadi edes JavaScript-tukea selaimelta. Ominaisuudet ovat hieman rajalliset, tosin ohjelmistolla on oma kannattajajoukkonsa. Myös plugineja eli eräänlaisia lisäosia on tarjolla kohtuullisen hyvin.

Ohjelmiston valintaa puolsi se, että se oli nykyisessä järjestelmässä käytössä. Sitä ei kuitenkaan valittu sen erittäin vanhahtavan käyttöliittymän vuoksi. (The SquirrelMail Project Team 2011)

3.6.3 Roundcube

Vaikka Roundcube oli valintaa tehtäessä vasta versiossa 0.4, sen toimivuudessa ei ollut havaittavissa puutteita. Myöskään haavoittuvuuksia ei ole tuoreemmista versioista löydetty. Roundcube tukee vain IMAP-protokollaa, mutta tämä ei ole ongelma, koska muu palvelinohjelmisto tukee sekä IMAP- että POP3-protokollia.

Roundcubea kehitetään myös aktiivisesti; tällä hetkellä uusin versio on 0.6. Vaikka versionumerot antavatkin ymmärtää, että kyseessä olisi vielä beeta-vaiheessa oleva ohjelmisto, on se otettu monessa paikassa tuotantokäyttöön.

Yksi suurimmista valintaperusteista oli se, että ohjelman käyttöliittymä on erittäin kehittynyt. Vaikka ohjelma on selainpohjainen, siihen on saatu työpöytäohjelmiston tuntua erilaisin keinoin. Se tukee muun muassa vedä ja pudota toimintoa, jolla voi siirtää viestejä eri kansioihin aivan kuin normaaleissa työpöytäohjelmistoissakin. Käyttöliittymän toimivuus ja helppokäyttöisyys vaikuttivat niin paljon, että tämä ohjelmisto päätettiin ottaa käyttöön muiden sijasta. (Roundcube 2011)

3.7 Roskapostiasetusten sekä karanteenin käyttäjärajapinta

Roskapostisuodatus on yleistynyt roskapostin määrän kasvaessa valtavasti. Usein voikin käydä niin, että käyttäjä ei saa koskaan tietää, mitä on estetty, miksi on estetty ja milloin on estetty. Yleensäkin suodatuspalveluita tarjoavilta toimijoilta saattaa saada vain suppeahkon myyntimielessä tehdyn listan suodatetuista määristä. Asiakkaan on myös vaikeaa saada haluamiaan asetuksia suodatukseen. Pahimmassa tapauksessa on mahdollista valita asennusvaiheessa vain parista eri vaihtoehdosta ja myöhempi säätäminen täytyy tehdä maksullisen mikrotuen kautta, koska minkäänlaista asiakasrajapintaa ei ole toteutettu. Myös ns. false-positive-tapausten eli väärien tunnistusten huomaaminen ja käsittely on hankalaa.

Jotta roskapostiasetusten säätämisestä saataisiin helppokäyttöisempi, on pyritty kehittämään työkaluja tätä varten. Vaikka aihe tuntuu kiinnostavan monia, yllättävän harva taho on julkaissut mitään ohjelmaa tähän tarkoitukseen. Projektin edetessä löydettiin vain kaksi vaihtoehtoa, joista toisen kehitys oli loppunut ja toisenkin kehitys

oli erittäin hidasta. Näiden kummankaan ominaisuudet eivät olleet tarpeisiin täysin sopivia, joten ainoaksi vaihtoehdoksi jäi kehittää itse sopiva ratkaisu.

3.7.1 Maia-mailguard

Valmiimpi ratkaisu kahdesta löydetystä vaihtoehdosta roskapostin käyttäjärajapinnaksi oli Maia-mailguard. Siinä on melko monipuolisesti ominaisuuksia, muun muassa käyttäjäkohtaiset asetukset roskapostin raja-arvoille, kohtuulliset tilastointiominaisuudet sekä käyttäjien mahdollisuus tutkia viestien sisältöä ennen niiden vapauttamista tai tuhoamista. Myös käyttäjäkohtaiset white- ja blacklistat ovat mahdollisia.

Maia-mailguardissa on kuitenkin joitain puutteita. Ensinnäkin se käyttää erittäin vanhaa ja kustomoitua versiota Amavisd-new-ohjelmasta. Vaikka Maia-mailguardin kehittäjät väittävät, ettei se ole mikään ongelma, niin yleisesti vanhojen ohjelmistoversioiden käyttöä pidetään tietoturvariskinä. Myös Maia-mailguardin käyttöliittymä on vanhahtava ja ohjelman päivitystahti erittäin hidas. (LeBlanc & Morton 2011)

3.7.2 mailzu-ng

Toinen vaihtoehto roskapostihallinnan käyttäjärajapinnaksi oli mailzu-ng. Se on kuitenkin erittäin keskeneräinen ja tuntuu siltä, että sen kehitys on lopetettu. Sen käyttöliittymä on paljon siistimpi kuin Maia-mailguardin mutta ominaisuuksia on huomattavasti vähemmän.

Mailzu-ng:n ominaisuuksiin kuuluu karanteenissa olevien viestien esikatselu, white- ja blacklist-ominaisuudet, domain- ja palvelinkohtaiset ylläpitotunnukset sekä domain- ja palvelinkohtaiset raportit. Siitä puuttuu käyttäjien sähköpostimuistutukset ja roskapostin raja-arvojen asettaminen. Sen lähdekoodista löytyi myös paljon turhaa koodia ja jäänteitä muiden ohjelmien lähdekoodista, joten vaikutelma ohjelmiston laadusta ei ollut kovinkaan myönteinen. (Husari 2011)

3.7.3 Oma toteutus

Koska valmiit vaihtoehdot eivät olleet sopivia, piti tarvittava ohjelmisto kehittää itse. Ohjelmiston ominaisuuksiin kuuluu mahdollisuus valita käyttäjäkohtaiset roskapos-

tiasetukset valmiista vaihtoehdoista, mitä ylläpitäjä voi vapaasti muokata ja lisätä. Myös käyttäjäkohtaiset white- ja blacklistit ovat tuettuja. Kielletyistä tiedostoliitteistä lähetetään huomautus vastaanottajalle, jolloin hän voi tarvittaessa käydä vapauttamassa kyseisen viestin karanteenista. Ominaisuuksiin kuuluu myös domain- ja palvelinkohtaiset ylläpitäjätilit sekä määräajoin lähetettävät karanteenin yhteenvetoviestit domainien ylläpitäjille. Domainin ylläpitäjä voi tarkastella oman domaininsa karanteenia ja vapauttaa viestejä muille saman domainin käyttäjille. Koko palvelimen ylläpitotunnuksella näin voi tehdä koko palvelimen viesteille.

Ohjelmassa olisi silti vielä paljon kehitettävää. Siinä on tällä hetkellä eri versiot paikallisille domaineille ja relay-domaineille. Siihen voisi lisätä yleisen sähköpostitilien hallinnan, jotta ei tarvitsisi käyttää useaa eri hallintaliittymää, vaan kaiken ylläpitotyön voisi hoitaa yhden hallintaliittymän alta. Se pitäisi myös kirjoittaa kokonaan uudelleen, koska siihen on lisätty ominaisuuksia ilman kunnon suunnittelua. Näin lopputulos on koodiltaan varsin rikkonainen ja osin kömpelö käyttää. Se on kuitenkin varsin hyvin toimiva ratkaisu ja tällä hetkellä tarpeita vastaava.

3.8 Hallintatyökalut

Jotta ylläpito olisi helpompaa ja nopeampaa, tarvitaan erityisiä hallintatyökaluja. Tähän löytyy joitain kaupallisia sovelluksia, joista suosituimpia lienevät CPanel ja Plesk. Niiden mahdollisuutta harkittiin, mutta hinta oli liian korkea, jotta niiden käyttö olisi tässä vaiheessa ollut kannattavaa. Lisäksi ne ovat ohjelmistosidonnaisia, joten ne eivät soveltuisi valittujen ohjelmistojen ylläpitoon. Tosin tämä ei olisi suuri ongelma, koska kaikki hallinta tapahtuisi näiden hallintaohjelmistojen kautta, jolloin itse ohjelmistovalinnalla ei ole niin suurta merkitystä.

Koska avoimen lähdekoodin ohjelmistoista ei löytynyt sopivaa hallintaohjelmistoa, jolla olisi voitu hallita kaikkia tarvittavia palveluja yhden käyttöliittymän alta, piti valita omat ohjelmistonsa eri hallintakohteita varten. Avoimen lähdekoodin hallintaohjelmistoista päätettiin valita käyttöön PostfixAdmin sähköpostitilien hallintaan sekä Webmin DNS-, käyttäjätili- sekä www-palveluiden hallintaan. Lisäksi valittiin jo edellä mainittu oma toteutus roskapostisuodattimen hallintaan. Hallintaohjelmien hajanaisuus onkin pieni ongelma, joten tarkoitus olisi jatkossa kehittää oma hallintatyökalu, jolla voisi helposti hallita kaikkia tarvittavia kohteita.

4 TIETOKANTAKUVAUS

Jotta käyttäjien ja domainien lisääminen olisi mahdollisimman helppoa ja palvelimen hallintaan käytettävien työkalujen saumaton yhteistyö mahdollista, on tietokantojen käyttö käyttäjä- ja domaintietojen säilytykseen järkevin vaihtoehto. Koska kaikki tarvittavat tiedot ovat tietokannassa, on selainpohjaisen hallintaliittymän luominen melko triviaali tehtävä. Selainpohjaista hallintaa tukee myös se, että selaimen kautta tapahtuva käyttäjien hallinnointi on paljon nopeampaa ja helpompaa kuin komentorivityökalujen käyttö. Tällöin perusylläpito ei vaadi syvempää tietämystä ohjelmistoista, vaan kaiken tarvittavan pystyy tekemään helpon käyttöliittymän avulla normaalilla www-selaimella. Seuraavaksi kerrotaan tietokantojen rakenteesta ja sisällöstä, jotta kokonaisuuden hahmottaminen olisi helpompaa. Tietoturvasyistä tietokannan taulujen nimet ovat tässä vain viitteelliset eivätkä täysin vastaa toteutusta.

4.1 Domain

Domain-taulussa on listattuna domainit, joiden postia palvelin ottaa vastaan. Listattuja tietoja ovat domainin nimi, informatiivisempi selite, luonti- ja muutosajat, domainkohtaiset quotat, postilaatikkojen ja aliaksien määrärajat sekä tieto, onko domain aktiivinen.

4.2 Relay

Relay-taulussa on listattu relay-domainit, eli domainit joiden postia välitetään eteenpäin toiselle palvelimelle sen sijaan että viestit talletettaisiin paikallisesti. Relay-domaineja käytetään tässä siksi, että voitaisiin tarjota roskapostisuodatuspalveluja esimerkiksi Exchange-käyttäjille, joiden postit sijaitsevat eri palvelimella kuin itse suodatusohjelmat. Tietokannassa on listattuna relay-domainin nimi, informatiivisempi tekstiselite sekä palvelin, jolle viesti välitetään eteenpäin.

4.3 Admin

Admin-taulussa on listattu ylläpitotilien tiedot. Näihin kuuluvat tunnus, salasanan MD5-tiiviste, luonti- ja muokkausajat, domainin tunnus, jota tällä tilillä voi hallita sekä tieto siitä, onko tili aktiivinen.

4.4 Mailbox

Mailbox-taulussa on listattu sähköpostitilien tiedot, kuten kirjautumistunnus, salasanan MD5-tiiviste, käyttäjän nimi, postilaatikon suhteellinen sijainti levyjärjestelmässä, quota, tilin luonti- ja muokkauspäivämäärät sekä tieto siitä, onko tili aktiivinen.

4.5 Alias

Alias-taulussa on listattuna kaikkien sähköpostitunnuksien aliakset. Jos vaikka kirjautumistunnus olisi ’kayttaja1@domain.fi’ voitaisiin tälle lisätä alias muotoa ’etunimi.sukunimi@domain.fi’. Yhdellä tunnuksella voi olla useita eri aliaksia.

4.6 Lomavastaaja

Lomavastaaja-taulussa on listattuna lomavastaajaviestit ja niihin kuuluvat tiedot. Näitä tietoja ovat sähköpostitilin tunnus, ilmoitusviestin otsikko, viestin sisältö, milloin vastaajaviesti on luotu sekä tieto, onko käyttäjän lomavastaaja aktiivinen.

4.7 Karanteeni

Karanteeni-taulussa on tiedot karanteeniin jääneistä viesteistä. Näihin tietoihin kuuluvat viestin lähettäjän sekä vastaanottajan sähköpostiosoite, viestin otsikko, karanteenin syy (roskaposti, rikkinäiset otsaketiedot vai kielletty tiedostoliite) sekä viestin sisältö. Tiedostoliitteitä ei talleteta tietokantaan vaan suoraan levyjärjestelmään, jolloin tietokantaan talletetaan vain viittaus kyseisen tiedoston sijaintiin.

4.8 Käyttäjien roskapostiasetukset

Tässä taulussa on käyttäjien roskapostiasetukset. Näitä asetuksia ovat karanteeniin päätyvien viestien pisterajat, sallitaanko kaikki tiedostoliitteet, sallitaanko rikkinäiset otsaketiedot ja sallitaanko virukset.

4.9 White- ja Blacklist

Tässä taulussa on lähettäjä-vastaanottaja osoiteparit sekä tieto onko osoitepari sallittujen vai estettyjen listalla. Parit on mahdollista tehdä myös domain-pohjaisesti, esimerkiksi voidaan sallia viestit domainista domain.fi osoitteeseen osoite@domain2.com.

4.10 Ulkoiset käyttäjät

Koska roskapostiasetusten hallintaan kirjaudutaan normaalisti sähköpostitilin tunnuksilla, pitää relay-domainien käyttäjille olla oma taulu, koska käyttäjän todentaminen olisi muuten erittäin vaikeaa, ellei jopa mahdotonta. Tietenkin myös relay-domainien hallintaliittymän pitää olla konfiguroitu käyttämään erillistä taulua käyttäjien tunnistukseen, eikä sähköpostitunnuksilla tapahtuvaa autentikointia, kuten normaalisti käytettäisiin. Tässä taulussa on käyttäjän tunnus sekä salasanan MD5-tiiviste.

5 OHJELMIEN KONFIGUROINTI

Tässä luvussa esitellään joitain tärkeimpiä konfiguraatiokohtia niistä ohjelmistoista, joiden asetuksia jouduttiin suuremmissa määrin muokkaamaan. Tietoturvasyistä joistain kohdista on vain konfiguroidun arvon selite, eikä oikeasti konfiguroitua arvoa.

5.1 Postfix

Jotta multidomainympäristön konfigurointi sujuisi mahdollisimman helposti, kannattaa osa konfiguraatiotiedoista siirtää tietokantaan. Postfix tukee mm. MySQL-tietokantoja ja MySQL onkin valittu tietokannaksi tässä toteutuksessa.

Jotta Postfix saatiin tukemaan paremmin quota-ominaisuuksia, siihen asennettiin Postfix VDA -niminen päivitys. Se antaa paremmat säätömahdollisuudet käyttäjäkohtaisille quota-asetuksille. Tämän takia osa taulukon (TAULUKKO 4 Tietokantoihin ja kokorajoituksiin liittyviä parametrejä) konfiguraatioparametreistä ei toimi ilman tätä päivitystä.

5.1.1 Perustiedot

Perustietoihin voi lukea isäntänimen (hostname), luotetut verkot (mynetworks), verkkoliitännät (inet_interfaces) sekä rele, jota kautta postit lähetetään toisiin kohteisiin (relayhost) sekä näihin liittyvät määritteet. Seuraavassa taulukossa (TAULUKKO 1 Perustiedot) esitellään joitain perustietoja sekä niiden oletus- ja konfiguroituja arvoja.

TAULUKKO 1 Perustiedot

Konfiguraatio-parametri	Parametrin selite	Konfiguroitu arvo	Oletusarvo
inet_interfaces	Missä osoitteessa palvelu toimii	localhost, mail.itc-hosting.fi	all
inet_protocols	Mitä protokollaa käytetään. Vaihtoehdot ipv4,ipv6,all	all	ipv4
mydomain	Palvelimen domainnimi	itc-hosting.fi	Palvelimen isäntänimi, josta on poistettu ensimmäinen komponentti

myhostname	Palvelimen isäntänimi	mail.itc-hosting.fi	Palvelimen isäntänimi
mynetworks	Osoitteet joista postia välitetään eteenpäin ulkoisen releen kautta	127.0.0.1/8 194.100.150.48/28	Generoidaan palvelimen ip-osoitteesta mynetworks_style arvon mukaisesti
mynetworks_style	Tapa jolla mynetworks arvo generoidaan automaattisesti jos sitä ei ole asetettu. Vaihtoehdot host, subnet, class	subnet	subnet
relayhost	Palvelin jolle muualle tarkoitetut viestit ohjataan	smtp.tdc.fi	tyhjä
content_filter	Ohjaus sisällöntarkistukseen ulkoiselle ohjelmalle	smtp-amavis:[127.0.0.1]:10024	tyhjä

5.1.2 Lähettäjien rajoitukset sekä käyttäjien todennus

Jotta palvelin ei toimisi avoimena releenä roskapostittajille (ja luultavasti täten joutuisi nopeastikin estolistoille), pitää lähettäjät todentaa eikä postia saa ottaa todentamattomalta käyttäjältä vastaan kuin pelkästään niihin domaineihin, joita kyseinen palvelin isännöi. Seuraavassa taulukossa (TAULUKKO 2 Lähettäjien rajoitukset sekä käyttäjien todennus) on esitelty lähettäjien rajoituksiin sekä käyttäjien todennukseen liittyviä konfiguraatioparametrejä.

TAULUKKO 2 Lähettäjien rajoitukset sekä käyttäjien todennus

Konfiguraatioparametri	Parametrin selite	Konfiguroitu arvo
relay_domains	Mihin domaineihin otetaan postia vastaan	
smtpd_recipient_restrictions	Katso kappale 5.1.3	Katso kappale 5.1.3
smtpd_sasl_auth_enable	Määrittelee onko SASL-autentikointimahdollisuus aktivoitu	yes
smtpd_sasl_path	Määrittelee mitä ohjelmaa tai sokettia käytetään SASL-autentikointiin	private/auth
smtpd_sasl_security_options	SASL-autentikoinnin turvakeinot	noanonymous
smtpd_sasl_type	SASL-autentikoinnin ulkoisen ohjelman tyyppi. Yleisimmät tuetut vaihtoehdot ovat dovecot ja cyrus.	dovecot
smtpd_tls_CAfile	SSL-sertifikaatin myöntäjän tunnistustiedot .pem formaatissa	polku ssl-sertifikaatin todentajan tunnistustiedostoon

smtpd_tls_cert_file	SSL-sertifikaattitiedosto. Mahdollista käyttää myös .pem –tiedostomuotoa jolloin avain on samassa tiedostossa kuin sertifikaatti.	polku ssl-sertifikaattitiedostoon
smtpd_tls_key_file	SSL-sertifikaatin avaintiedostoon, jos tahdotaan käyttää erillistä avaintiedostoa eikä yhdistetty .pem tiedostoa. Avain ei saa olla suojattu salasanalla.	polku ssl-sertifikaatin avaintiedostoon
smtpd_use_tls	Mahdollistaa TLS-salauksen, mutta ei pakota sitä. Käytännössä asiakkaan (joko käyttäjän tai palvelimen) kytkeytyessä smtp-palvelimeen antaa STARTTLS-komennon jonka asiakas voi jättää huomiotta jolloin jatketaan salaamattoman yhteyden muodostusta	yes

5.1.3 smtpd_recipient_restrictions

Smtpd_recipient_restrictions-parametrillä määritetään rajoitteet palvelimen käyttäjille. Parametrissä on kaikki rajoitukset listan muodossa, jonka järjestyksellä on merkitys. Kun listan alkioita aletaan käydä läpi alusta alkaen, pysähdytään ensimmäiseen kohtaan, jonka ehto täyttyy. Täten olisi typerää laittaa kaiken salliva ehto ensimmäiseksi, jolloin myöhempiä ehtoja ei tarkistettaisi. Kaiken salliva ehto on tärkeää muistaa laittaa listan viimeiseksi, varsinkin jos listassa on paljon kieltäviä ehtoja. Muuten käy helposti niin, että vaikka saapuva viesti ei osuisi yhteenkään kieltävään ehtoon, jäisi se toimittamatta sallivan ehdon puuttuessa. Taulukossa (TAULUKKO 3 smtpd_recipient_restrictions) on kuvattu tässä työssä käytetyt ehdot esiintymisjärjestyksessään. Kuten taulukosta voidaan nähdä, ennen kuin viesti otetaan vastaan välitettäväksi eteenpäin, tehdään useita tarkistuksia, jotta vältyttäisiin roskapostilta tai viruksilta. Useat saastuneet tietokoneet ympäri maailman lähettävät yhä sähköpostia niin, etteivät niiden HELO/EHLO-käskyt ole RFC-standardin mukaisia, jolloin suuri osa näistä viesteistä jää pois jo tässä vaiheessa ennen kuin viestiä edes on otettu vastaan. Toivoa sopii, että haittaohjelmien kirjoittajat eivät korjaa virheitään tuossa asiassa.

TAULUKKO 3 smtpd_recipient_restrictions

Ehto	Vaikutus
permit_sasl_authenticated	Sallitaan SASL-autentikoidut käyttäjät

permit_mynetworks	Sallitaan kaikki omista verkoista
check_policy_service unix:postgrey/socket	Välitetään pyyntö Postgrey-ohjelmalle joka viivyttää tuntematonta asiakasta kieltäytyen ottamasta postia vastaan ensimmäisellä yhteyskerralla. Tehokas tapa roskapostittajia vastaan.
reject_non_fqdn_hostname	Ei oteta vastaan postia jos HELO/EHLO käskyssä annettu domainnimi ei ole RFC mukainen FQDN-isäntänimi.
reject_unauth_destination	Ei oteta vastaan viestiä sellaiselle domainille, joka ei ole joko relay-listassa tai listattuna omissa domaineissa joko mydomain tai virtual_mailbox_domains määrittelyissä.
reject_invalid_hostname	Ei oteta vastaan postia jos HELO/EHLO käskyssä välitetään epäkelpo isäntänimi.
reject_non_fqdn_sender	Ei oteta vastaan postia jos lähettäjän sähköpostiosoite ei ole RFC mukainen ja sisällä FQDN-isäntänimeä.
reject_non_fqdn_recipient	Ei oteta vastaan postia jos vastaanottajan sähköpostiosoite ei ole RFC mukainen ja sisällä FQDN-isäntänimeä.
reject_unknown_sender_domain	Ei oteta vastaan postia jos lähettäjä ei ole jostain palvelimen domainista ja jos lähettäjän domainnimellä ei ole A- tai MX-tietuetta saatavilla.
reject_unknown_recipient_domain	Ei oteta vastaan postia jos vastaanottaja ei ole jostain palvelimen domainista ja jos vastaanottajan domainnimellä ei ole A- tai MX-tietuetta saatavilla.
reject_rbl_client sbl-xbl.spamhaus.org	Tarkastetaan lähettäjän IP-osoite blacklististä. Jos palvelin palauttaa arvon, joka osoittaa että IP-osoite on listattu, ei postia oteta vastaan.
reject_rbl_client bl.spamcop.net	Tarkastetaan lähettäjän IP-osoite blacklististä. Jos palvelin palauttaa arvon, joka osoittaa että IP-osoite on listattu, ei postia oteta vastaan.
reject_rbl_client cbl.abuseat.org	Tarkastetaan lähettäjän IP-osoite blacklististä. Jos palvelin palauttaa arvon, joka osoittaa että IP-osoite on listattu, ei postia oteta vastaan.
reject_rbl_client zen.spamhaus.org	Tarkastetaan lähettäjän IP-osoite blacklististä. Jos palvelin palauttaa arvon, joka osoittaa että IP-osoite on listattu, ei postia oteta vastaan.
reject_rbl_client multi.surbl.org	Tarkastetaan lähettäjän IP-osoite blacklististä. Jos palvelin palauttaa arvon, joka osoittaa että IP-osoite on listattu, ei postia oteta vastaan.

reject_rbl_client combined.rbl.msrbl.net	Tarkastetaan lähettäjän IP-osoite blacklististä. Jos palvelin palauttaa arvon, joka osoittaa että IP-osoite on listattu, ei postia oteta vastaan.
permit	Otetaan viesti vastaan.

5.1.4 Postilaatikkojen asetukset sekä tietokantojen hyödyntäminen

Seuraavaksi esitellään joitain konfiguraatioparametrejä, jotka liittyvät tietokantojen käyttöön sekä viestien ja sähköpostilaatikoiden kokorajoituksiin.

Koska monia konfiguraatioparametrejä voidaan määrittää tietokantoja hyväksikäyttäen, kannattaakin usein muuttuvat arvot tallettaa tietokantaan. Näin niiden ylläpitäminen helpottuu ja selainpohjaisten hallintaliittymien luominen on myös huomattavasti helpompaa. Raskaammin kuormitetuissa ympäristöissä on kannattavaa käyttää usein käytettyihin tauluihin proxy-määrettä, jolloin peräkkäiset samansisältöiset haut eivät aiheuta useaa tietokantakyselyä vaan vain yhden. Tämä helpottaa palvelimen kuormaa silloin, kun samaan osoitteeseen tai domainiin tulee nopeassa tahdissa useita viestejä. Ilman näitä määreitä voi myös törmätä ongelmaan, jolloin mysql-palvelin on liian kuormitettu vastatakseen pyyntöihin aiheuttaen näin virheen viestin vastaanotossa.

Kuten taulukosta (TAULUKKO 4 Tietokantoihin ja kokorajoituksiin liittyviä parametrejä) voidaan todeta, on virtual_mailbox_limit ensin alustettu arvoon 0 ja sen jälkeen on haettu kuitenkin tietokannasta arvo tämän tilalle. Tähän on kaksikin syytä. Ensiksi jos tätä arvoa ei ole asetettu, aiheuttaa message_size_limit parametrin asettaminen virheilmoituksen, jossa ilmoitetaan suurimman sallitun viestikoon olevan suurempi kuin suurin sallittu postilaatikon koko. Myöskään postilaatikon koon asettaminen tiettyyn arvoon tässä ilman erillistä uudelleenmäärittelyä ei ole järkevää, koska käyttäjillä voi olla erikokoiset postilaatikot. Tietokannoista haetuilla arvoilla postilaatikoiden koot on helppo asettaa käyttäjäkohtaisesti.

Erillisten MySQL-määritystiedostojen teko on helppoa. Niissä määritellään käyttäjänimi, salasana, palvelin, tietokannan nimi sekä suoritettava sql-lause. Esimerkiksi seuraavanlaisella tiedostosisällöllä saadaan tarkistettua onko vastaanottajaksi merkittyä sähköpostiosoitetta olemassa.

user = käyttäjätunnus

password = salasana
hosts = localhost
dbname = tietokanta
query = SELECT goto FROM alias WHERE address = '%s'

TAULUKKO 4 Tietokantoihin ja kokorajoituksiin liittyviä parametrejä

Konfiguraatioparametri	Parametrin selite	Konfiguroitu arvo
message_size_limit	Viestin kokorajoitus tavuina. 0 tarkoittaa rajoittamatonta.	0
virtual_mailbox_limit	Postilaatikon kokorajoitus tavuina. 0 tarkoittaa rajoittamatonta.	0
virtual_mailbox_limit_inbox	Rajoitetaanko vain INBOX kansion sisältöä vai koko Maildir-muotoista postilaatikkoa	yes
virtual_mailbox_base	Kertoo missä postilaatikot sijaitsevat levyjärjestelmässä	polku postilaatikoiden juurihakemistoon
transport_maps	Ylimääräiset hakutaulut viestien välitystä varten. Näissä on määritelty relay-domainit sekä lomavastaaja.	hash:transport_maps, proxy:mysql:sql_transport_maps.cf
virtual_alias_maps	Kertoo, mistä löytyy domainien aliastiedot.	proxy:mysql:sql_virtual_alias_maps.cf
virtual_mailbox_domains	Kertoo, mistä löytyy domainien tiedot	proxy:mysql:sql_virtual_domains_maps.cf
virtual_mailbox_limit_maps	Kertoo, mistä löytyy sähköpostilaatikoiden kokorajoitukset	mysql:sql_virtual_mailbox_limit_maps.cf
virtual_mailbox_limit_override	Mahdollistaa pienemmän kokorajoituksen sähköpostilaatikolle kuin suurimman viestin kokorajoitus	yes
virtual_mailbox_lock	Kertoo mitä sähköpostilaatikon lukitustapaa käytetään kun sinne kirjoitetaan. Tällä asetuksella ei ole väliä maildir-formaatissa koska sähköpostilaatikon viestit ovat jokainen omassa tiedostossaan	fcntl,dotlock
virtual_mailbox_maps	Kertoo, mistä löytyy sähköpostilaatikoiden tiedot	proxy:mysql:sql_virtual_mailbox_maps.cf
virtual_maildir_limit_message	Viesti, joka lähetetään viestin lähettäjälle jos vastaanottajan postilaatikko on täynnä	Ilmoitusviesti postilaatikon täyttymisestä sekä englanniksi että suomeksi.
virtual_overquota_bounce	Hylätäänkö viesti 5xx sarjan virheilmoituksella vai 4xx sarjan virheilmoituksella. Arvolla ”yes” ilmoitetaan 5xx sarjan virheilmoitus jolloin lähettäjälle tulee tieto että käyttäjän postilaatikko on täynnä. Arvolla ”no” ilmoitetaan 4xx sarjan virheilmoitus, jolloin lähettävä palvelin yrittää tietyn ajan päästä uudelleenlähetystä.	yes

5.2 Amavisd-new

Vaikka itse Amavisd-new onkin koko sisällöntarkistuksen ydin, sen käyttöönottaminen perusasetuksin on varsin suoraviivaista. Tässä tapauksessa kuitenkin säädettävää riittää, koska käyttöön otetaan tietokantayhteydet ja karanteeniin joutuneiden viestien vapautusrajapinta. Konfiguraatiotiedosto noudattaa perl-syntaksia, joten se ei ole aivan niin helppolukuinen kokemattomammalle käyttäjälle kuin esimerkiksi Postfixin konfiguraatiotiedosto. Taulukossa (TAULUKKO 5 Amavisd-new konfiguraatioparametrejä) on listattuna joitain tärkeimpiä konfiguraatioparametrejä selityksineen.

TAULUKKO 5 Amavisd-new konfiguraatioparametrejä

Parametri	$mydomain
Selite	Oma FQDN isäntänimi. Tätä parametriä käytetään myös muissa konfiguraatioparametreissä joten arvon on tärkeää olla oikein asetettu.
Konfiguroitu arvo	Palvelimen FQDN isäntänimi
Parametri	$inet_socket_port
Selite	Missä paikallisissa tcp-porteissa kuunnellaan yhteyksiä varten.
Konfiguroitu arvo	TCP-portit joissa otetaan yhteyksiä vastaan
Parametri	$interface_policy{'tcp porttinumero'}
Selite	Sidotaan tietty tcp portti tiettyyn policy-bankin policyyn.
Konfiguroitu arvo	Policyn nimi
Parametri	$policy_bank{'AM.PDP'}
Selite	Roskapostin vapautusjärjestelmän policy-määre. Arvo annetaan taulukkona.
Konfiguroitu arvo	protocol => 'AM.PDP', inet_acl => [qw(127.0.0.1 194.100.150.49/28)],
Parametri	@lookup_sql_dsn
Selite	Tietokantayhteyden määrittely käyttäjäkohtaisten asetusten hakuun
Konfiguroitu arvo	['DBI:mysql:database=tietokannan nimi;host=127.0.0.1;port=3306', 'käyttäjätunnus', 'salasana']
Parametri	@storage_sql_dsn
Selite	Tietokantayhteyden määrittely viestien varastointia varten. Voidaan määritellä myös osoittamaan toiseen muuttujaan, kuten tässä esimerkissä on tehty.
Konfiguroitu arvo	@lookup_sql_dsn
Parametri	$sql_select_policy
Selite	SQL-lause jolla haetaan käyttäjäkohtaiset policymääreet tietokannasta. Muuttuja %k pitää sisällään pilkuilla erotetun listan vastaanottajien osoitteista joille tietoja haetaan.
Konfiguroitu arvo	'SELECT *,users.id FROM users, policy'. ' WHERE (users.policy_id=policy.id) AND (users.email IN (%k))';
Parametri	$sql_select_white_black_list

Selite	SQL-lause, jolla tarkistetaan onko lähettäjän osoite käyttäjäkohtaisissa black- tai whitelistoissa. SQL-lauseessa ”?”-merkki korvataan aikaisemmassa SQL-kyselyssä haetulla user-id:llä ka %k on lähettäjän osoite.
Konfiguroitu arvo	'SELECT wb FROM wblist,mailaddr'. ' WHERE (wblist.rid=?) AND (wblist.sid=mailaddr.id)'. ' AND (mailaddr.email IN (%k))';
Parametri	$warnbannedrecip
Selite	Ilmoitetaanko viestin vastaanottajalle, jolle estetyn liitetiedoston sisältämäviesti oli tarkoitettu
Konfiguroitu arvo	1
Parametri	$warnbannedsender
Selite	Ilmoitetaanko viestin lähettäjälle, joka on lähettänyt estetyn liitetiedoston sisältämän viestin
Konfiguroitu arvo	0
Parametri	$bad_header_quarantine_method
Selite	Tapa jolla rikkinäiset otsikkotiedot omaavat viestit varastoidaan. Tämä voi osoittaa myös johonkin tiedostojärjestelmän kohteeseen.
Konfiguroitu arvo	‘sql:’
Parametri	$banned_files_quarantine_method
Selite	Tapa jolla kielletyn liitetiedoston sisältävät viestit varastoidaan. Tämä voi osoittaa myös johonkin tiedostojärjestelmän kohteeseen.
Konfiguroitu arvo	‘sql:’
Parametri	$spam_quarantine_method
Selite	Tapa jolla roskapostiksi luokitellut viestit varastoidaan. Tämä voi osoittaa myös johonkin tiedostojärjestelmän kohteeseen.
Konfiguroitu arvo	‘sql:’
Parametri	$notify_virus_recips_templ
Selite	Viestipohja, jota käytetään kun lähetetään ilmoitus kielletyn liitetiedoston sisältävän viestin tarkoitetulle vastaanottajalle. Vaikkakin parametrin nimestä voisi niin päätellä, ei viestiä lähetetä viruksen sisältävistä viesteistä.
Konfiguroitu arvo	read_text("/polku/banned-file-template");
Parametri	$banned_filename_re
Selite	
Konfiguroitu arvo	new_RE(qr'^\.(exe-ms|dll)$', qr'.\.(pif\|scr)$'i, qr'^application/x-msdownload$'i, qr'^application/x-msdos-program$'i, qr'^application/hta$'i, qr'\.[^./]*[A-Za-z][^./]*\.\s*(exe\|vbs\|pif\|scr\|bat\|cmd\|com\|cpl\|dll)[.\s]*$'i, qr'.\.(exe|vbs|pif|scr|cpl)$'i,);
Parametri	@av_scanners
Selite	Ensisijaiset virustutkat. Arvo annetaan taulukkona joten tässä voi olla useita vaihtoehtoja, jolloin viesti ajetaan jokaisen tutkan läpi
Konfiguroitu arvo	['ClamAV-clamd', \&ask_daemon, ["CONTSCAN {}\n", "/polku/clamd-socket"], qr/\bOK$/, qr/\bFOUND$/, qr/^.*?: (?!Infected Archive)(.*) FOUND$/m]

Parametri	@av_scanners_backup
Selite	Toissijaiset virustutkat. Näitä käytetään jos ensisijaisiin ei saada yhteyttä. Tämäkin parametri annetaan taulukkona jolloin viesti ajetaan jokaisen määritellyn tutkan läpi. Jos toissijaisetkaan virustutkat eivät toimi, jää viesti jonoon palvelimelle kunnes virustarkistus on voitu suorittaa.
Konfiguroitu arvo	['ClamAV-clamscan', 'clamscan', "--stdout --no-summary -r --tempdir=$TEMPBASE {}", [0], qr/:.*\sFOUND$/, qr/^.*?: (?!Infected Archive)(.*) FOUND$/m]

Suomalaisista operaattoreista ainakin DNA käyttää Amavisd-new-pohjaista suodatusta. DNA on nimennyt Amavisd-new:n päällä olevan suodatuksensa nimellä DNA Postiturva (näkyy X-Virus-Scanned headerissa). Muutos alkuperäiseen lienee vain kosmeettinen, koska muut header-kentät paljastavat Amavisd-new:n käytön. Tätä muutosta ei voi tehdä suoraan konfiguraatiotiedostosta, vaan tässä tapauksessa on täytynyt muokata alkuperäistä ohjelmatiedostoa, joka tosin on myös perl-skripti, jolloin sen muokkaus tällaisessa tapauksessa on varsin triviaalia.

5.3 Dovecot

Vaikka Dovecot onkin POP3- ja IMAP-ohjelmisto, se tarjoaa myös SMTP-autentikointirajapinnan. Tämä mahdollistaa SMTP-palvelimen käyttämisen kaikkialta käyttäjän omilla sähköpostitunnuksilla. Tämä ominaisuus on erittäin hyödyllinen, koska silloin ei tarvita useampia tunnuksia postin vastaanottamiseen ja lähetykseen. Tämä mahdollistaa myös lähettäjän jäljittämisen mahdollisissa ongelmatilanteissa. Esimerkiksi jos vaikka jonkun käyttäjän kone on saastunut ja se yrittää lähettää roskapostia, ei tarvita IP-pohjaisia estoja, vaan tunnuksen väliaikainen sulkeminen riittää.

Myös Dovecotin asentaminen sekä konfigurointi oli varsin vaivatonta. Sen konfiguraatiotiedosto on hyvin kommentoitu, jolloin sen muokkaaminen on helppoa. Dokumentaatiosta tarvitsi tarkistaa vain parin asetuksen syntaksi tarkemmin; kaikki muu oli selitetty hyvin konfiguraatiotiedostossa. Muutoksia tarvittiin lähinnä siihen, missä postilaatikot sijaitsevat levyjärjestelmässä sekä tietenkin tietokantayhteyksien asetuksiin. Seuraavassa taulukossa (TAULUKKO 6 Dovecot konfiguraatioparametrejä) on selitetty joitain Dovecot-ohjelman tärkeimpiä konfiguraatioparametrejä.

TAULUKKO 6 Dovecot konfiguraatioparametrejä

Konfiguraatio-parametri	Parametrin selite	Konfiguroitu arvo
protocols	Mitä protokollia tuetaan. Voidaan käyttää myös arvoa none jolloin pelkästään dovecot-auth on käytössä.. Vakiona pelkästään imap on käytössä.	imap imaps pop3 pop3s
ssl	Onko SSL/TLS-salaus käytettävissä. Vakiona pois päältä koska vakiona ei ole myöskään SSL-sertifikaatteja asennettuna.	yes
ssl_ca_file	Polku sertifikaatin myöntäjän varmenteeseen	Polku sertifikaatin myöntäjän varmenteeseen
ssl_cert_file	Polku sertifikaattitiedostoon	Polku sertifikaattitiedostoon
ssl_key_file	Polku sertifikaattitiedoston avaintiedostoon	Polku sertifikaattitiedoston avaintiedostoon
ssl_key_password	Jos avaintiedosto on suojattu salasanalla, sen voi laittaa tähän, jolloin aina ohjelmaa käynnistettäessä ei tarvitse syöttää salasanaa	avaintiedoston salasana
disable_plaintext_auth	Estetäänkö selväkielinen kirjautuminen ilman salausta. Vakioasetuksilla SSL ei ole käytössä ja selväkielinen autentikointi on pois käytöstä, jolloin minkäänlainen kirjautuminen ei onnistu.	no
mail_location	Missä postit sijaitsevat levyjärjestelmässä. Tällä kerrotaan myös postilaatikon tyyppi joka voi olla joko mbox tai maildir. Hakemistopolussa voi käyttää myös erilaisia muuttujia, esimerkiksi domain, käyttäjä, kirjautumistunnus ja kotihakemisto. Täysi lista löytyy Dovecotin dokumentaatiosta.	maildir:/polku/laatikoihin/domain/käyttäjä
imap_client_workarounds(imap)	Yhteensopivuusparametrit erilaisten imap-asiakasohjelmistojen kanssa.	delay-newmail netscape-eoh tb-extra-mailbox-sep
pop3_client_workarounds(pop3)	Yhteensopivuusparametrit erilaisten pop3 asiakasohjelmistojen kanssa.	outlook-no-nuls oe-ns-eoh
passdb authdb	Salasana ja autentikointiasetukset	driver: sql args: /polku/sql-määrityksiin
SQL määritykset		
Konfiguraatio-parametri	Parametrin selite	Konfiguroitu arvo
driver	Määrittelee käytettävän tietokannan ajurin	mysql
connect	Tietokannan yhteydenmuodostamisparametrit	host=127.0.0.1 port=3306 dbna-

		me=tietokanta user=käyttäjä password=salasana
default_pass_scheme	Missä muodossa salasana tallennetaan tietokantaan. Vaihtoehdot ovat PLAIN,CRYPT,MD5(-CRYPT),PLAIN-MD5	MD5
password_query	SQL-kysely salasanan tarkistusta varten	SELECT salasana FROM mailbox WHERE käyttäjä = '%u'
user_query	SQL.kysely käyttäjän postilaatikon sijainnin saamiseksi	SELECT maildir, FROM mailbox WHERE käyttäjä = '%u'

5.4 Muut ohjelmistot

Muiden ohjelmistojen konfiguraatiot eivät tarvinneet paljoakaan muokkausta. Lähinnä vain lokitiedostojen nimet ja sijainnit sekä joitain kosmeettisia asetuksia piti muuttaa.

SpamAssassinin osalta tarkistettiin, mitkä testit ovat käytössä. Tässä tapauksessa perusasetukset todettiin riittäviksi. Clamd:n asetuksista muutettiin vain viruskuvaustietokantojen päivitysväli hieman tiheämmäksi. Greylisting-ominaisuudesta vastaavan Postgreyn asetuksista säädettiin odotusaika kahteen minuuttiin, lisättiin tunnettujen palvelimien listalle suomalaisten operaattoreiden palvelimia sekä konfiguroitiin näytettävä viesti. Roundcube-webmailista muutettiin tietokanta- sekä sähköpostipalvelinasetukset.

6 TOIMINTAKUVAUS

Suurimmalla osalla sähköpostin käyttäjistä ei ole tietoa, kuinka se oikeasti toimii. Monella on sellainen käsitys, että kun käyttäjä on painanut lähetä-nappia, niin viesti ilmestyy pian vastaanottajan sähköpostilaatikkoon. Toki näin useimmiten käykin, mutta itse viestinvälitysprosessi ei ole aivan näin yksinkertainen. Varsinkin roskapostisuodatus ja sen eri aliprosessit tuovat monta uutta elementtiä viestin välitysprosessiin.

6.1 Yhteyden muodostus

Kuten kuviosta (KUVIO 1 Viestin vastaanottoprosessi) voidaan havaita, ensimmäinen askel yhteyden muodostamisessa on tarkistus, onko lähettäjä autentikoitunut palvelimelle. Autentikoidut käyttäjät ohittavat muut testit ja heidän lähettämänsä viestit menevät suoraan sisällöntarkistukseen.

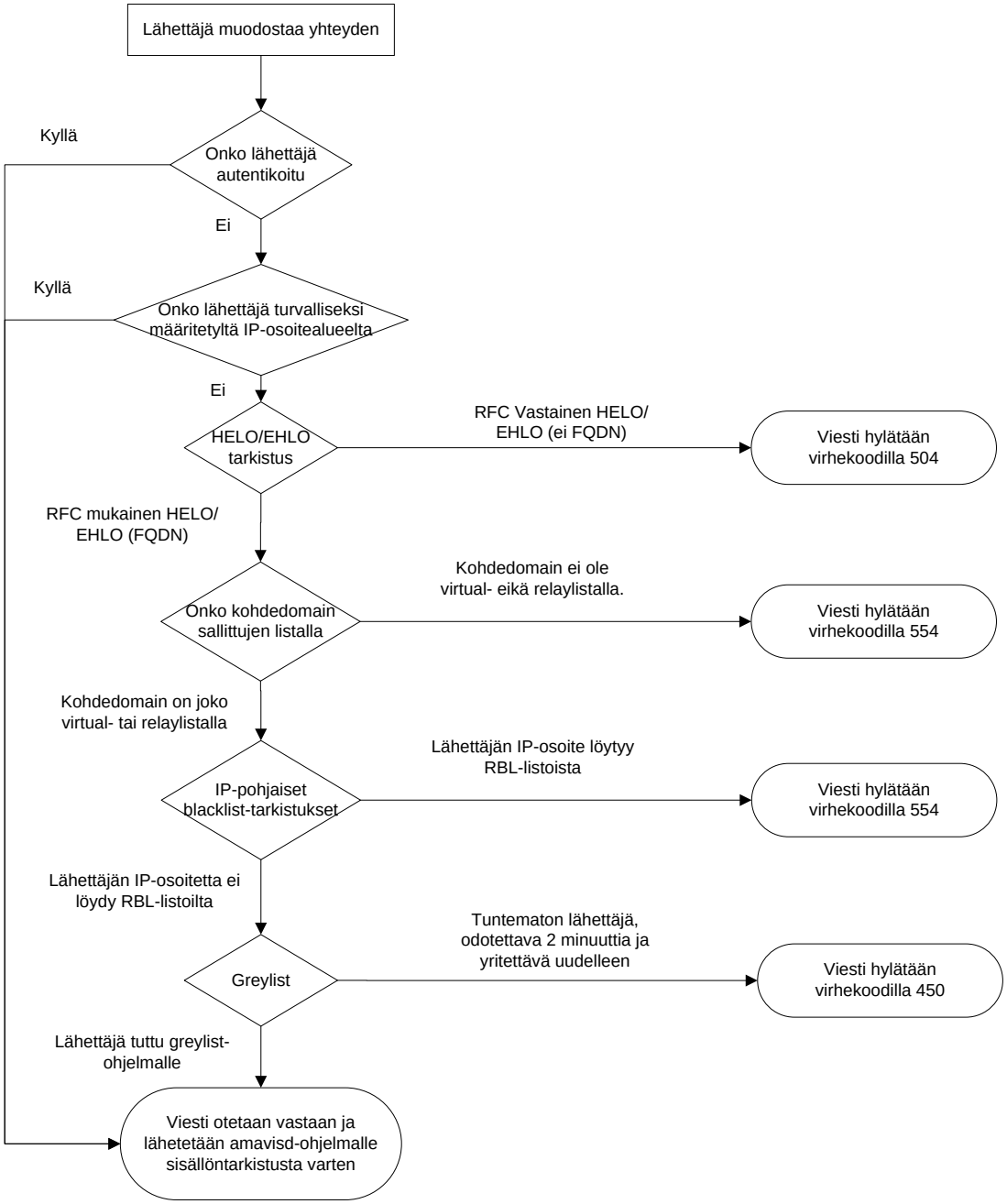
Jos lähettäjä ei ole autentikoitu, tarkastetaan onko lähettäjän IP-osoite turvalliseksi todetulla alueella. Palveluntarjoajien osalla tämä kattaa yleensä kaikki palveluntarjoajan asiakkailleen varaamat IP-alueet. Tässä tapauksessa turvallisiksi alueiksi on merkitty oma IP-blokki sekä palvelimen paikallinen localhost-osoite. Jos osoite löytyy listalta, ohitetaan kaikki loput tarkistukset ja siirrytään sisällöntarkistukseen.

Jos osoite ei ole turvallisten osoitteiden listalla, tarkastetaan yhteyden muodostuksessa käytettävä HELO/EHLO tunnus. Yleensä tämä on lähettäjäkoneen FQDN-isäntänimi, tosin yhä usea palvelin on konfiguroitu väärin, jolloin se käyttää RFC2821 vastaista HELO/EHLO formaattia. Myös useat haittaohjelmat eivät osaa tunnistautua oikein, vaan ne paljastuvat jo tässä vaiheessa. Jos HELO/EHLO tarkistus ei onnistu, palautetaan virhekoodi 504 ja lopetetaan yhteys.

Jos tarkistus onnistuu, tarkastetaan onko kohdedomain koneen relay- tai virtualdomain-listalla. Jos tätä tarkistusta ei olisi, kone toimisi avoimena releenä ja joutuisi hyvinkin pian monien palvelimien estolistoille, koska se suostuisi välittämään sille kuulumatonta liikennettä ja joutuisi näin varmasti pikaisesti roskapostittajien hyväksikäyttämäksi. Jos kohdedomain ei ole koneen sallittujen domainien listoilla, palautetaan virhekoodi 554 ja katkaistaan yhteys.

Jos kohdedomain kuuluu palvelimen sallimiin domaineihin, jatketaan seuraavaan tarkistukseen, joka on lähettäjäkoneen IP-osoitteen tarkistus erilaisia RBL (Real-time Block List) listoja kohtaan. Tämä tarkistus tehdään vasta tässä vaiheessa, koska HELO/EHLO ja kohdedomain-tarkistukset vievät vain vähän kapasiteettia ja näin saadaan vähennettyä palvelimen kuormaa. Myöskään RBL listojen ylläpitäjät eivät salli suuria yhteysmääriä ilman maksua, joten sekin on hyvä syy vähentää turhia tarkistuksia näitä listoja kohtaan. Jos lähettäjän IP-osoite löytyy näiltä listoilta, palautetaan virhekoodi 554 ja katkaistaan yhteys. Muussa tapauksessa jatketaan viimeiseen tarkistukseen ennen viestin välittämistä sisällöntarkistusta varten.

Viimeinen tarkistus on niin sanottu Greylist-tarkistus. Tällä menetelmällä pyritään vähentämään roskapostia siten, että jokainen uusi lähettäjäkone laitetaan odottamaan 2 minuuttia ennen kuin siltä suostutaan ottamaan viestiä vastaan. Normaalisti konfiguroitu palvelin osaa noudattaa Greylist-ohjelman antamaa koodia 450 ja yrittää myöhemmin uudestaan. Sen sijaan useat roskapostittajat yrittävät lähettää kerralla paljon viestejä ja kun lähettäjäkone mitä todennäköisimmin tällöin joutuu estolistoille, vaihtavat he lähettäjäkonetta. Tällöin Greylist-ohjelma ei tule saamaan viestiä määräajan puitteissa alkuperäiseltä lähettäjältä uudestaan, vaan kohtelee tämän lähettäjän yhteyksiä tulevaisuudessakin, kuten tämä olisi uusi lähettäjä. Jos taasen lähettäjä yrittää viestin lähetystä uudestaan määräajan kuluessa, todetaan lähettäjä tutuksi ja tämän lähettäjän viestit eivät joudu tulevaisuudessa enää odottamaan. Ohjelma voidaan konfiguroida myös niin, että se ”unohtaa” tietyn määräajan kuluttua IP-osoitteet, jotka eivät ole enää lähettäneet viestejä.



KUVIO 1 Viestin vastaanottoprosessi

6.2 Sisällöntarkistus

Kuviossa (KUVIO 2 Sisällöntarkistus) on kuvattuna sisällöntarkistusprosessi. Se alkaa lukemalla tietokannasta käyttäjän henkilökohtaiset asetukset suodatukselle. Jos näitä ei ole asetettu, käytetään vakioarvoja.

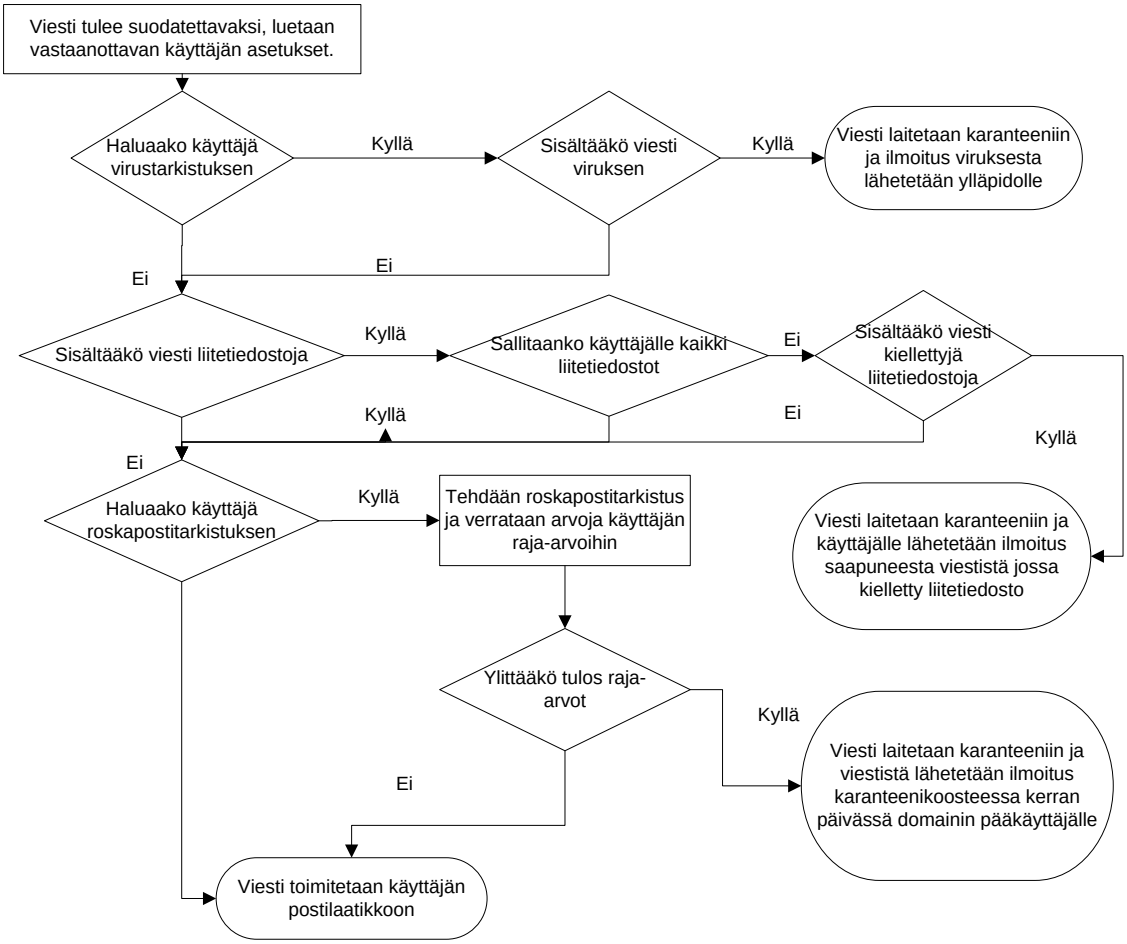
Ensimmäiseksi tarkistetaan, haluaako käyttäjä virustarkistuksen viestille ja sen liitetiedostoille. Jos käyttäjä haluaa tarkistuksen ja viestistä löytyy virus, lähetetään ilmoitus ylläpitäjälle ja viesti laitetaan karanteeniin. Viruskaranteeni eroaa roskapostika-

ranteenista siten, että virusten säilytyspaikka on pakattuna levyjärjestelmässä, kun taas roskapostiviestit säilytetään tietokannassa tutkiskelua ja vapauttamista varten. Jos käyttäjä ei halunnut virustarkistusta tai virusta ei löytynyt, siirrytään liitetiedosto-tarkistukseen.

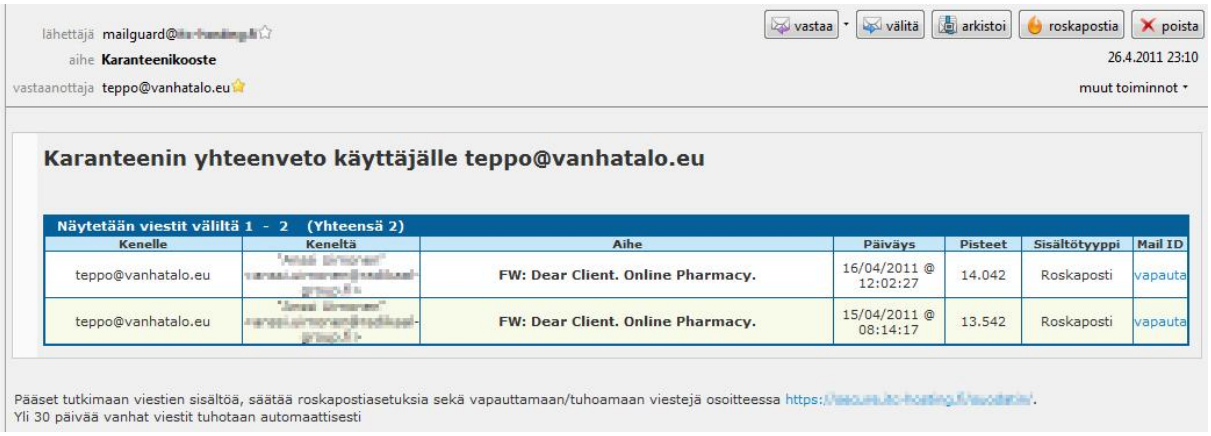
Liitetiedostotarkistuksessa ensimmäinen tarkistus on se, että sallitaanko käyttäjälle kaikki liitetiedostot. Koska virukset ja haittaohjelmat yhä saattavat levitä sähköpostin välityksellä, auttaa tämä tarkistus ennalta tuntemattomia viruksia vastaan. Kiellettyjen tiedostoliitteiden listalla ovat erilaiset ajettavat tiedostot, kuten .exe ja .scr -päätteiset tiedostot. Mikäli käyttäjän asetuksissa ei ole sallittu näitä kiellettyjä tiedostoliitteitä ja tällainen liite löytyy, laitetaan viesti karanteeniin ja lähetetään vastaanottajalle ilmoitus että viestistä löytyi kielletty tiedostoliite. Tällöin käyttäjä voi käydä vapauttamassa viestin, jos hän katsoo tämän olevan tarpeellista. Ilmoitusviestissä pyritään varoittamaan siitä, että tiedostoliitteet voivat sisältää viruksia tai haittaohjelmia, joskin nykypäivän käyttäjät eivät kuitenkaan ole kovinkaan valveutuneita, vaan lähes järjestelmällisesti avaavat jokaisen mahdollisen tiedostoliitteen ja painavat ”OK” jokaiseen kysymykseen sen suurempia miettimättä mahdollisia seurauksia. Mikäli kiellettyjä tiedostoliitteitä ei löydy tai käyttäjälle on sallittu kaikki liitetiedostot, siirrytään seuraavaan vaiheeseen, joka on roskapostitarkistus.

Roskapostitarkistuksen ensimmäinen askel on tarkistus siitä, että haluaako käyttäjä sitä suoritettavan. Jos tarkistus ohitetaan, toimitetaan viesti käyttäjän sähköpostilaatikkoon. Muussa tapauksessa luetaan käyttäjälle määritetyt roskapostin raja-arvot ja verrataan niitä viestille tarkistuksessa saatuihin arvoihin. Jos raja-arvot ylittyvät, toimitetaan viesti karanteeniin. Jos raja-arvot eivät ylity, viesti toimitetaan vastaanottajan sähköpostilaatikkoon.

Karanteeniin päätyneistä viesteistä lähetetään kooste kerran päivässä domainin ylläpitäjän sähköpostiosoitteeseen. Tässä viestissä on linkki karanteenisivustolle, jossa viestejä voi tutkia tarkemmin. Viestissä on myös suorat vapautuslinkit viesteille, jos käyttäjä pystyy jo lähettäjän osoitteesta sekä viestin otsikosta päättelemään, ettei viesti ole roskapostia. Kuvassa (KUVA 2. Esimerkki karanteenikoosteviestistä) on esimerkki käyttäjälle lähetettävästä karanteenikoosteviestistä. Karanteeniin päätyneet viestit poistetaan automaattisesti 30 päivän päästä siitä, kun viesti on joutunut karanteeniin.



KUVIO 2 Sisällöntarkistus



KUVA 2. Esimerkki karanteenikoosteviestistä

7 VARMUUSKOPIOINTI JA VIRHEISTÄ PALAUTUMINEN

Kuten muidenkin palvelimien, myös sähköpostipalvelimen varmuuskopioinnin tulee olla kunnossa. Lyhyetkin katkot viestinvälityksissä voivat olla kalliita loppukäyttäjille, varsinkin yritysmaailmassa. Siksi varmuuskopioinnin ja erilaisista virheistä palautumisen pitääkin olla kunnossa. Käyttäjämäärien ollessa vielä suhteellisen pieniä ei tarvetta ulkopuoliselle levyjärjestelmälle ole, vaan voidaan pitäytyä palvelimeen fyysisesti asennetuissa levyjärjestelmissä. Tässä palvelimessa käytettiin peilaavaa RAID-1 tason toteutusta, joka nimensä mukaisesti peilaa yhden kiintolevyn sisällön reaaliaikaisesti toiselle. Tällöin toisen levyn vioittuessa voidaan jatkaa toimintaa normaalisti ja vain vaihtaa vioittunut levy uuteen ehjään vastaavaan. Myös palvelimen virransyöttö on kahdennettu lisäämällä toinenkin virtalähde kokoonpanoon ja virta syötetään riittävän tehokkaista UPS-varavirtalaitteista.

Varmuuskopioiden ottoa on pyritty porrastamaan levyjärjestelmän kuorman tasaamiseksi. Käyttäjien sähköposteista, kotihakemistoista sekä tietokannoista otetaan kustakin varmuuskopio kerran päivässä. Tämä varmuuskopio siirretään ssh-tunnelin läpi toiselle palvelimelle, josta tiedot kopioidaan vielä ulkoiselle medialle lisävarmistuksen saamiseksi esimerkiksi tulipalon sattuessa. Koska palvelinohjelmistot sijaitsevat virtuaalipalvelimella, otetaan myös koko virtuaalipalvelimelta niin kutsuttu live-snapshot öisin. Tällöin laitteiston vikaantuessa voidaan virtuaalikone helposti siirtää toiselle palvelinlaitteistolle ja ottaa saman tien käyttöön ilman suurempia viiveitä.

Eri palveluiden jumiutumisen varalta palvelut käynnistetään uudelleen määräajoin. Tulevaisuudessa olisi tarkoitus ottaa käyttöön NAGIOS-ohjelmisto, jolla valvottaisiin eri palveluiden tilaa.

8 PÄÄTELMÄT

Aikaisempi kokemukseni Linux-ympäristöistä sekä suurimmasta osasta käytettäviä ohjelmistoja antoi minulle erinomaiset valmiudet toteuttaa työ sekä keskittää aikani uusien ominaisuuksien kehittämiseen ja kokonaisuuden toimintavarmuuden takaamiseen taaten näin tilaajayritystä varmasti tyydyttävän lopputuloksen.

Kokonaisuudessaan työ onnistui erittäin hyvin ja järjestelmä on toiminut lähes moitteetta alusta asti. Tilaajapuoli oli erittäin tyytyväinen asennettuun järjestelmään, joka on jatkuvassa ja alati lisääntyvässä käytössä. Alkuperäisiin asetuksiin jouduttiin toki tekemään joitain muutoksia käyttöasteen kasvaessa, joista toiminnan kannalta merkittävämpänä oli cache-määreen lisääminen Postfixin mysql-kyselyihin.

Tulevaisuudessa olisi tarkoitus tehdä hallintapaneelit täysin uusiksi, jotta kaikki tarvittavat toiminnot saataisiin yhden ja saman käyttöliittymän alle. Myös varmuuskopiointiin on kaavailtu muutosta. Uuden suunnitelman mukaan lisätään tiedostojen reaaliaikainen peilaus ja vasta peilattu data pakataan ja ajetaan ulkoiselle medialle. Tämä toimintatapa vähentäisi luultavasti niin verkon kuin I/O-järjestelmän kuormaa. Tällä hetkellä myös autentikoitujen käyttäjien lähettämät sähköpostiviestit ajetaan roskapostisuodattimen läpi. Tässä on se ongelma, että välillä liitetiedostoja jää roskapostisuodattimeen, koska vastaanottajan asetuksia ei ole saatavissa ja ajettavat liitetiedostot estetään vakiona. Tähän ongelmaan löytyi ratkaisu tätä opinnäytetyötä kirjoitettaessa ja toteutus olikin varsin yksinkertainen ottaa käyttöön.

LÄHTEET

Bernstein D.J., *Internet host SMTP Server Survey.* [verkkodokumentti] 2001 [viitattu 11.3.2011]. Luettavissa : http://cr.yp.to/surveys/smtpsoftware6.txt

E-Soft Inc., *Mail (MX) Server Survey.* [verkkodokumentti] 2010 [viitattu 11.3.2011]. Luettavissa: http://www.securityspace.com/s_survey/data/man.201003/mxsurvey.html

E-Soft Inc., *Mail (MX) Server Survey.* [verkkodokumentti] 2007 [viitattu 11.3.2011]. Luettavissa: http://www.securityspace.com/s_survey/data/man.200707/mxsurvey.html

Exim, *Exim Internet Mailer.* [verkkodokumentti] 2011 [viitattu 11.3.2011]. Luettavissa: http://www.exim.org

Horde Inc., *The Horde Project.* [verkkodokumentti] 2011 [viitattu 22.3.2011]. Luettavissa: http://www.horde.org/

Howard J., *SMTP Performance Benchmarking.* [verkkodokumentti] 2004 [viitattu 11.3.2011]. Luettavissa: http://www.jrh.org/smtp/index.html

Husari M., Mailzu-NG. [verkkodokumentti] 2011 [viitattu 24.3.2011]. Luettavissa: http://trac.husku.net/mailzu-ng/

LeBlanc R. & Morton D., *Maia Mailguard – A Spam and Virus Management System.* [verkkodokumentti] 2011 [viitattu 24.3.2011]. Luettavissa: http://www.maiamailguard.com/maia/wiki

Postfix, *The Postfix Homepage.* [verkkodokumentti] 2011 [viitattu 11.3.2011]. Luettavissa: http://www.postfix.org/start.html

Process Software, *Introduction to Bayesian Filtering.* [verkkodokumentti] 2010 [viitattu 14.3.2011]. Luettavissa: http://www.process.com/precisemail/bayesian_filtering.htm

Roundcube, *Roundcube - Free webmail for the masses.* [verkkodokumentti] 2011 [viitattu 22.3.2011]. Luettavissa: http://www.roundcube.net

Sendmail Inc., *Sendmail Community.* [verkkodokumentti] 2011 [viitattu 11.3.2011]. Luettavissa: http://www.sendmail.com/sm/open_source/

Sirainen T., *ImapTest/ServerStatus - Unofficial IMAP Protocol Wiki.* [verkkodokumentti] 2011 [viitattu 20.3.2011]. Luettavissa: http://www.imapwiki.org/ImapTest/ServerStatus

The SquirrelMail Project Team, *SquirrelMail - Webmail for Nuts!*. [verkkodokumentti] 2011 [viitattu 22.3.2011]. Luettavissa: http://www.squirrelmail.org

VMWare Inc., *VMware Server FAQs, Free Virtualization Server Consolidation.* [verkkodokumentti] 2011 [viitattu 10.3.2011]. Luettavissa: http://www.vmware.com/products/server/faqs.html