TEKNIIKKA JA LIIKENNE

Tietotekniikka

Tietoverkot

INSINÖÖRITYÖ

SMTP-RELEOINTIPALVELUN VALVONTA JA RAPORTOINTI

Työn tekijä: Visa Hänninen
Työn ohjaajat: Tarmo Tuomi

Työ hyväksytty: ___. ___. 2010

Marko Uusitalo
lehtori

Metropolia

ALKULAUSE

Tässä työssä tutkittiin SMTP-releointipalvelun raportointi- ja valvontamahdollisuuksia sekä toteutettiin ne. Kiitän kaikkia minua eri tavoin auttaneita ihmisiä.

Helsingissä 25.10.2010

Visa Hänninen

TIIVISTELMÄ

Työn tekijä: Visa Hänninen

Työn nimi: SMTP-releointipalvelun valvonta ja raportointi

Päivämäärä: 25.10.2010 **Sivumäärä:** 55 s.

Koulutusohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoverkot

Työn ohjaaja: lehtori Marko Uusitalo

Työn ohjaaja: DI Tarmo Tuomi

Tässä työssä tutkittiin SMTP-releointipalvelun valvontaa ja raportointia. Tarkoitus oli selvittää, kuinka raportointi ja valvonta voidaan toteuttaa sähköpostin välitykseen käytettävässä järjestelmässä.

Työn alussa käsitellään ensin tiedonsiirtoa lyhyesti, jonka jälkeen esitellään SMTP- sekä SNMP-prokollan toimintaa ja ominaisuuksia. Seuraavaksi kuvataan releointi-palvelun toimintaa ja sitä, mihin tarkoituksiin se soveltuu. Tämän jälkeen käydään läpi releointipalvelussa käytettävät komponentit. Lisäksi esitellään sähköpostin turvallisuuteen sekä reititykseen liittyviä asioita.

Reitityksen ja turvallisuuden jälkeen käydään läpi asioita sähköpostin suodatuksesta. Työssä käsitellään yleisellä tasolla niin viruksia, matoja ja roskapostin suodattamista. Lisäksi esitellään, mitä muita uhkia sähköpostille saattaa saapua Internetistä.

Tämän jälkeen esitellään työn tavoitteet. Aluksi esitellään nykyinen tilanne, jonka jälkeen määritellään tavoitteet, joihin työssä pitäisi päästä. Painopiste on valvonnan ja raportoinnin käyttöönotossa.

Seuraavana käsitellään raportoinnin toteutus. Tässä osiossa esitellään raportoitavat asiat, raportin muoto sekä ongelmat ja vaikutukset. Valvonnan toteutus esitellään seuraavana. Valvonnasta käydään läpi valvonnan toteutus sekä suodatin, että ohjauskoneille. Tässä kohtaa esitellään sekä telnet- että SNMP-valvonta.

Viimeisenä vuorossa ovat loppupäätelmät. Tässä osiossa tehdään yhteenveto tehdystä työstä. Osiossa käydään läpi tavoitteisiin pääseminen, työssä kohdatut ongelmat sekä työn kannalta merkitykselliset jatkotoimenpiteet. Jatkotoimenpiteissä kerrotaan asioista, joilla järjestelmää voitaisiin kehittää eteenpäin.

Avainsanat: SMTP, Sähköposti, releointi, SNMP, Symantec Brightmail, sähköpostin suodatus

Metropolia

ABSTRACT

Name: Visa Hänninen

Title: Reporting and monitoring of SMTP relay service

Date: 25.10.2010 **Number of pages:** 55

Department: Information Technology **Study Programme:** Data networks

Instructor: Marko Uusitalo, Senior Lecturer

Supervisor: Tarmo Tuomi, M.Sc. Tech

This final project studies the reporting and monitoring of SMTP-relay services. The purpose was to find out how reporting and monitoring can be arranged in an e-mail relaying system.

The theory part begins with a brief look at data transmission. It continues with a section that discusses the SMTP-protocol. After that there is a brief introduction to SNMP and an example how it works. Next is the description of the relay service, followed by the introduction of the components used in the relay service.

The next section discusses the goals of the final project. First the current situation is presented and then the situation which should be accomplished. The focus is on the reporting and monitoring of the relay service. There is also a brief look at the security and routing of e-mail.

The following chapter discusses the filtering of e-mail. In this chapter the filtering of viruses, worms and commercial bulk e-mail, also known as spam is covered. The next chapter talks about other threats to e-mail that originate from the Internet.

The goals of this project are set in the next chapter. The chapter talks about the goals in reporting and also in the monitoring. Also the form, problems and effects of the reporting are covered. The monitoring part covers the monitoring on both scanner and control center in Symantec Bightmail environment using telnet and SNMP.

Finally there is a summarizing chapter about achieved goals and also remained things to be developed in the future. Also the problems that were encountered are explained.

Keywords: SMTP, e-mail, relay, SNMP**,** Symantec Brightmail, e-mail filtering

1 JOHDANTO

Tässä insinöörityössä tutkittiin SMTP-releointipalvelun valvontaa sekä raportointia. Työssä toteutettiin valvonta sähköpostia välittäville palvelimille käyttäen hyväksi SNMP-rajapintaa, joka palvelimista löytyi. Lisäksi valvontaa suoritettiin yhteyskokeiluilla. Raportointiosiossa tutkittiin erilaisia mahdollisuuksia raportoinnin toteuttamiseen. Raportoinnissa käytettiin myös palvelinten omia työkaluja. Työssä on käytetty BMC Patrol -valvontaohjelmistoa ja siihen erikseen tehtyä laajennusta, joka tukee Symantec Brightmail Gateway -tuotetta. Työ tehtiin yhteistyössä suuren tietotekniikka-alan yrityksen kanssa. Työssä on käytetty komponentteja, jotka eivät ole kaikkien vapaasti käytettävissä, vaan ovat yrityksen omia laajennuksia.

Työn alussa käsitellään lyhyesti tiedonsiirtoa verkossa. Työ jakautuu useampaan eri osaan, joista ensimmäinen käsittelee SMTP-protokollaa. Protokollasta käydään läpi yleisesti sen tälle työlle merkitykselliset asiat. Seuraavassa osassa käsitellään valvonnassa käytettävää SNMP-rajapintaa ja sen tässä työssä käytettyjä ominaisuuksia. Tämän jälkeen vuorossa on releointipalvelun kuvaus, jossa kerrotaan, millaisia käyttökohteita palvelulla on. Seuraavana esitellään palvelun tuottamiseen vaadittavat komponentit. Lisäksi tässä luvussa käsitellään sähköpostin turvallisuutta ja reititystä sekä kerrotaan lokien merkityksestä.

Työssä käsitellään myös sähköpostin suodatukseen liittyviä asioita yleisellä tasolla. Näihin liittyen käydään läpi erilaisiin listoihin perustuva suodatus sekä muita tapoja, joilla sähköpostin sisältöä voidaan suodattaa. Työssä esitellään virustarkistus sekä roskapostisuodatus käyttäen hyväksi Windows Server 2003 -palvelinta sekä Symantec Brightmail Gatewayta. Brightmailista on käytössä versio 9.0.

Seuraavaksi käsitellään muita sähköpostille merkityksellisiä uhkia, joita Internetissä esiintyy. Tämän jälkeen määritellään työn tavoitteet. Aluksi kuvaillaan nykyinen tilanne, jonka jälkeen määritellään tavoite, johon työssä tulisi päästä.

Seuraavana vuorossa on raportoinnin toteutus. Raportoinnista käydään läpi raportoitavat asiat, raportin muoto, mahdolliset ongelmat sekä vaikutukset.

Näiden jälkeen on vuorossa valvonta. Valvonnan osuus koostuu valvonnan suunnittelusta, valvontaohjelmiston esittelystä sekä erillisistä osioista suodatin- ja ohjauskoneille.

Työn lopussa esitellään yhteenveto työssä käsitellyistä asioista sekä tutkitaan, päästiinkö ennalta asetettuihin tavoitteisiin. Lisäksi pohditaan mahdollisia jatkotoimenpiteitä. Näiden lisäksi käydään läpi työssä kohdatut ongelmat ja työn kirjoittajan omat mietteet.

1.1 Tiedonsiirto

Siirrettäessä tietoa kahden tai useamman eri pisteen välillä on käytössä aina siirtoprotokolla. Kun tietoa siirretään esimerkiksi kahden työaseman välillä, on käytössä ensiksi itse sovellus, joka tietoa siirtää. Tämän jälkeen tulee kuljetuskerroksen protokolla, joka on esimerkiksi TCP tai UDP riippuen siitä, minkä tyyppistä siirrettävä liikenne on. Kuljetuskerroksen jälkeen tulee verkkokerroksen protokolla, joka on yleisesti IP eli Internet Protocol. Tätä seuraa Datalink Layer eli siirtokerros, jossa protokollana on Ethernet. Vasta siirtokerroksen jälkeen tulee itse fyysinen siirtomedia, joka voi olla esimerkiksi kategoria viiden mukainen kuparikaapeli tai suorituskykyisempi valokuitu. [1.]

Tiedonsiirtoa kuvataan usein seitsemänkerroksisen Open Systems Interconnectin eli OSI-mallin avulla.

7. Sovelluskerros
6. Esitystapakerros
5. Istuntokerros
4. Kuljetuskerros
3. Verkkokerros
2. Siirtokerros
1. Fyysinen kerros

Kuva 1 OSI-malli

Kaikkea tiedonsiirtoa ei voida suoraan pilkkoa seitsemään eri kerrokseen. Kerrosmalli kuitenkin auttaa hahmottamaan, mistä kaikesta tiedonsiirto kahden järjestelmän välillä koostuu. Myös muunlaisia kerrosmalleja tiedon siirron kuvaukseen on olemassa, mutta OSI-malli on varmasti tunnetuin.

1.2 TCP

Tässä työssä ei keskitytä niinkään siirtokerroksen protokolliin, vaan ne esitellään vain lyhyesti. Olennaista onkin ymmärtää TCP:n ja UDP:n suurimmat erot ja niiden perusteella käyttö eri sovelluksissa.

TCP eli Tranmission Control Protocol on luotettavaan tiedonsiirtoon kehitetty protokolla. Luotettavalla tiedonsiirrolla tarkoitetaan sitä, että jos siirron aikana tapahtuu häviöitä tai siirretty bitti vastaanotetaan virheellisenä, voidaan kyseinen vioittunut osa siirtää uudelleen. TCP pitää sisällään menetelmän valvoa siirrettyä tietoa. Tämä on toteutettu sekvenssinumeroin, eli jokainen 8-bitin oktetti on numeroitu. Muuttumattomuus varmistetaan tarkistussummien avulla, joita TCP laskee lähetetylle tiedolle. Mikäli vastaanottaja päässä tehdyssä tarkastuksessa huomataan, että tarkistussumma ei vastaa siirrossa vastaanotettua tietoa, voidaan lähettäjää pyytää lähettämään tieto uudelleen.

Tiedonsiirto TCP:n avulla alkaa aina kolmevaiheisella kättelyllä. Ensin lähettävä osapuoli ottaa yhteyden vastaanottavaan osapuoleen lähettämällä viestin SYN. Tämän jälkeen vastaanottava osapuoli vastaa lähettäjälle SYN ACK –viestin, jonka lähettävä osapuoli kuittaa vielä ACK-viestillä. Näin kolmivaiheinen kättely on suoritettu ja TCP-yhteys muodostettu. Kun tieto on lähettäjän ja vastaanottajan välillä siirretty, voidaan TCP-yhteys purkaa. Purku tapahtuu käyttämällä FIN-viestiä, jolla lähettäjä ilmoittaa, ettei sillä ole enempää tietoa siirrettäväksi. Yhteyden purkamisen jälkeen ei vanhaan yhteyteen enää palata, vaan muodostetaan uusi yhteys SYN-viestiä käyttämällä. [2, s.30.]

TCP pitää sisällään myös joukon muita mekanismeja, kuten linkin ruuhkautumisen eston sekä vastaanotetun datan kuittaukset. Tämän työn kannalta on kuitenkin oleellista ymmärtää vain, että TCP on luotettava tiedonsiirtoprotokolla.

TCP on oikea valinta siirtoprotokollaksi, kun kyseessä on sovellus, joka vaatii, että tieto siirretään virheettömästi ja oikeassa järjestyksessä. Tämä tekeekin TCP:stä hyvän valinnan Hyper Text Transport Protocol:n HTTP:n käyttöön. Reaaliaikaisen videon ja äänen siirtoon TCP ei ominaisuuksiensa vuoksi sovellu. TCP vaatii kuittauksen jokaisesta vastaanotetusta paketista, joka aiheuttaa ylimääräistä kuormaa ja hitautta.

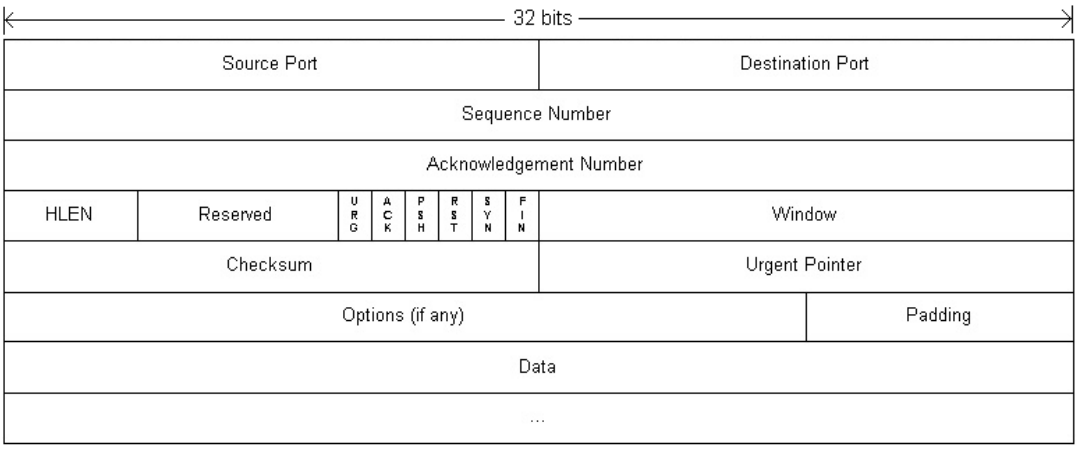
1.3 UDP

UDP eli User Datagram Protocol on toinen tiedonsiirtoon käytettävä protokolla. Toisin kuin TCP, UDP ei ole luotettava protokolla. TCP muodostaa aina ensin päästä päähän yhteyden lähettäjän ja vastaanottajan välillä, jonka jälkeen varsinainen tiedonsiirto alkaa. UDP ei muodosta minkäänlaista yhteyttä, vaan tieto ikään kuin ”valuu” koko ajan lähettävästä päästä. Tästä seikasta johtuen UDP:tä ei voi käyttää samanlaisissa sovelluksissa kuin TCP:tä. Mikäli UDP:tä kuitenkin halutaan käyttää sovelluksissa, jotka vaativat luotettavaa tiedonsiirtoa, on virheiden tarkistus tehtävä ylemmillä kerroksilla. Toisaalta taas keveyden ja yksinkertaisuutensa takia UDP sopii aikakriittisiin sovelluksiin paremmin kuin TCP. [3, s. 1.]

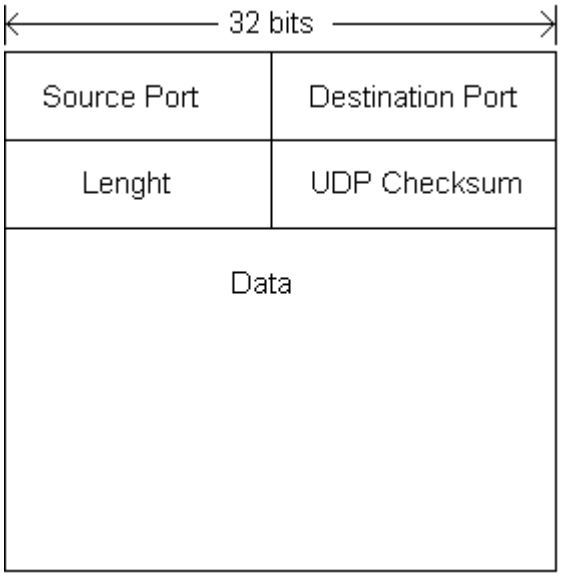
Luotettavaa tiedonsiirtoa tarvitaan useissa jokapäiväisissä sovelluksissa, kuten sähköpostin lähetyksessä tai web-surffauksessa. Sekä SMTP että HTTP käyttävät hyväkseen TCP:tä. Monet sovellukset eivät kuitenkaan hyödy hukkuneen tiedon uudelleenlähetyksestä aikakriittisyytensä vuoksi, mutta sietävät sen sijaan pientä pakettihävikkiä. Tällaisia sovelluksia ovat esimerkiksi Voice over Internet Protocol (VoIP), eli Internet-puhelut, sekä erilaiset Internetin videopalvelut, kuten videokeskustelut. Nämä palvelut ovat kriittisiä ajan suhteen. Siksi TCP ei sovellu hyvin niiden käyttöön vaan käytössä on UDP. UDP vaatii huomattavasti vähemmän kaistaa kuin TCP ja sen aiheuttama prosessointikuorma on myös pienempi. UDP on myös järkevämpi vaihtoehto esimerkiksi puheensiirtoon, sillä vaikka TCP tarjoaa mahdollisuuden pyytää hukkunut paketti uudelleen, ei siitä ole iloa esimerkiksi puhelinkeskustelussa.

Tässä työssä käsitellään tarkemmin SMTP- sekä SNMP-protokollia. Näistä SMTP käyttää hyväkseen TCP:tä ja SNMP UDP:tä. SMTP on kriittinen siirrettävän tiedon oikeellisuuden suhteen. SNMP puolestaan on käytössä useimmiten sellaisissa ympäristöissä, joissa muuta liikennettä voi olla koh-

tuullisen paljon, eikä verkkoa haluta kuormittaa enempää. SNMP hoitaa itse pakettien pyytämisen uudelleen, mikäli niitä siirrossa hukkuu, lukuun ottamatta Trap-viestejä.



Kuva 2 TCP-segmentin rakenne



Kuva 3 UDP-segmentin rakenne

2 SMTP

2.1 Historia

Simple Mail Transfer Procol, eli SMTP, on alun perin Etelä-Kalifornian yliopistossa vuonna 1982 sähköpostin siirtoon kehitetty protokolla. Aikaisemmin sähköpostin välitykseen oli käytetty useita erilaisia protokollia suurien pääkoneiden välillä. Kun yhä useammat yritykset sekä Yhdysvaltain hallitus

toivat verkkoon lisää tietokoneita, tarvittiin yhtenäinen protokolla sähköpostin kuljettamiseen. Nykyisin SMTP dominoi sähköpostiviestien välitystä Internetissä eikä muita protokollia enää käytetä. [4, s. 1 – 3.]

SMTP on peräisin aikakaudelta, jolloin luotettavalla tiedonsiirrolla oli suurempi painoarvo kuin turvallisuudella. Tuohon aikaan verkon käyttäjiä oli niin vähän, että kaikki lähestulkoon tunsivat toisensa. Suurin osa käyttäjistä koostui yliopistojen tutkijoista sekä Yhdysvaltain asevoimien henkilökunnasta. Tuolloin ei myöskään ymmärretty, että yksinkertainen ja helposti omaksuttava protokolla, jossa ei ole vahvaa tunnistusta, tarjoaisi tulevaisuudessa lähes täydellisen tavan levittää matoja, viruksia sekä roskapostia. SMTP:tä onkin kritisoitu moneen otteeseen juuri sen yksinkertaisuudesta. Löyhät määrittelyt ja tunnistuksen puute mahdollistavat helpon väärinkäytön.

2.2 Viestit

SMTP nojaa ASCII-merkistöön, eli kaikki sen lähettämät viestit ovat selkokielisiä ja ne ovat helposti ymmärrettävissä. SMTP ei ota kantaa siihen ovatko viesteissä käytetyt merkit isoja tai pieniä. SMTP:n lähettämät viestit on jaettu neljään eri kategoriaan sen mukaan, minkälaisesta informaatiosta on kyse. Eri kategoriat ovat 2xx, 3xx, 4xx ja 5xx, ja ne jakautuvat seuraavalla tavalla:

- 2xx pitää sisällään yleisiä ilmoituksia.
- 3xx pitää sisällään viestien kirjoituksen aloituskomennon.
- 4xx pitää sisällään joukon virheilmoituksia liittyen palvelun saatavuuteen.
- 5xx pitää sisällään joukon virheilmoituksia liittyen komentosyntaksiin ja palvelun saatavuuteen.

Vaatimuksena on, että jokaisesta lähetetystä viestistä on saatava yksirivinen vastaus takaisin. Lisäksi vastausviestit on numeroitu niin, ettei ohjelmistojen ole tarpeellista analysoida viestissä olevaa tekstiä. Virhekoodit on suunniteltu siten, että palvelin saa kaiken tarvitsemansa informaation kolminumeroisesta numerosarjasta. Ainoat viestit, joista odotetaan tulevan vastaukseksi useampi rivi tekstiä, ovat EXPN ja HELP. Useampia rivejä sisältäviä vastauksia ei kuitenkaan ole estetty muiltakaan komennoilta. [4, s. 33 – 38.]

SMTP ei ole riippuvainen alla olevasta siirtojärjestelmästä, vaan vaatii ainoastaan luotettavan ja järjestetyn tietovirran. [4, s. 1.] Tästä johtuen käytössä on TCP-protokolla. Yhteys, joka muodostetaan kahden SMTP-palvelimen välille, on aina kaksisuuntainen. Lähettävä osapuoli ei aloita lähettämään tietoa vastaanottavalle osapuolelle ennen kuin tämän kanssa on muodostettu yhteys. Yhteyden muodostus tapahtuu HELO- tai EHLO-komennolla. HELO on SMTP:n alkuperäinen vastaanottavan palvelimen tervehtimiseen tarkoitettu komento ja EHLO uudempi ESMTP:n mukana tullut komento.

Yleisesti ottaen SMTP on käytössä, kun normaali käyttäjä lähettää sähköpostiviestin sähköpostiohjelmastaan. Kun viestiä haetaan sähköpostipalvelimelta luettavaksi, on käytössä yleensä muita protokollia kuten Post Office Procol (POP) tai Internet Message Access Procol (IMAP). Useilla yrityksillä käytössä olevat Microsoft Outlook- ja Lotus Notes –sähköpostiohjelmat käyttävät omia yksityisiä protokollia viestin lähetykseen ja noutamiseen palvelimelta.

2.3 SMTP-yhteys esimerkki

SMTP on hyvin yksinkertainen protokolla, ja perusmuotoa oleva kättely on erittäin helposti ymmärrettävä. Seuraavassa esimerkki siitä, miltä yhteyden muodostaminen ja viestin lähettäminen toisen SMTP-palvelimeen kautta näyttää.

220 email.vaastaanottaja.com SMTP Spamlet Thu Jun 03 13:09:06 EEST 2010
HELO lahettava.palvelin.com
250 email.vaastaanottaja.com Helo lahettava.palvelin.com, nice to interact with you
MAIL FROM: <joku123@ lahettava.palvelin.com>
250 sender <joku123@ lahettava.palvelin > OK
RCPT TO: <kuka123@postipalvelin.com>
250 recipient <kuka123@ postipalvelin.com > OK
DATA
250 OK; enter text, end with .
Tämä on viestin sisältö.
.
250 postipalvelin.com OK; message accepted for delivery
QUIT

Edellä olevan esimerkin ensimmäisellä rivillä avataan yhteys email.vastaanottaja.com -nimiseen SMTP-palvelimeen. Toisella rivillä yhteyttä ottava palvelin, tässä tapauksessa lahettava.palvelin.com, lähettää ”HELO” -sanoman, jolloin vastaanottava palvelin vastaa ”250 nice to interact

with you”. Näin yhteys SMTP-palvelimesta toiseen on muodostettu. Rivillä neljä ”MAIL FROM” -kohdassa on kerrottu lähettäjän sähköpostiosoite, johon vastaanottava palvelin kuittaa ”250 sender <> OK”. Rivillä viisi kerrotaan vastaanottajan osoite ”RCPT TO <>” komennolla, johon vastaanottava palvelin kuittaa ”250 recipient OK”. Seuraavaksi komennolla ”DATA” käynnistetään varsinainen viestin kirjoitus. Tähän vastaanottava palvelin kuittaa ”250 OK; enter text, end with .” eli viesti lopetetaan pisteellä. Tämä ei tarkoita sitä, että viesti ei voisi sisältää kuin yhden lauseen, vaan piste on oltava tyhjän rivin alussa. Kun viesti on kirjoitettu, vaihdetaan riviä ja syötetään piste ja painetaan ”enter”. Tällöin vastaanottava palvelin tietää, että viestin kirjoitus on loppunut ja palvelin kuittaa vastaukseksi ”250 postipalvelin.com OK; message accepted for delivery”. Tämän jälkeen yhteys voidaan purkaa ”QUIT” -komennolla. [5, s. 1.]

2.4 SMTP-otsake

Otsake eli header on viestin osa, johon on kirjattu polku, jota pitkin viesti on matkannut. Suurin osa sähköpostin lukemiseen ja kirjoittamiseen käytetyistä ohjelmista näyttää vain osan otsake-tiedoista. Yleisesti käyttäjälle näkyvät vain lähettäjä-, vastaanottaja-, otsikko- ja kopio-kentät. Muut otsakkeen sisältämät kentät on yleensä piilotettu. Käyttäjä saa ne kuitenkin näkyviin, joskin jokaisessa ohjelmassa eri tavalla. Otsake toimii sähköpostissa samalla tavoin kuin postileima normaalissa kirjepostissa. Kirjeen vastaanottaja voi päätellä postileimoista, mistä kirje on alun perin lähetetty ja missä kaikissa postikonttoreissa se on käynyt. Samalla tavoin sähköpostin otsake-tietoihin jää merkintä kaikista sähköpostipalvelimista, joiden kautta viesti on kulkenut. Nämä tiedot löytyvät ”received”, eli vastaanotettu-kentästä, johon tallentuu palvelimen nimi sekä IP-osoite. Näin viestin vastaanottaja voi halutessaan selvittää, mitä kautta viesti on kulkenut ja mistä se on alun perin lähetetty. [6, s. 1 - 3.]

Otsake-tiedot ovat normaalisti huonosti luettavassa muodossa. Tähän kuitenkin löytyy apu Internetistä. Monet sivut tarjoavat ”laatikon”, johon tutkittavan viestin sisältö on mahdollista liittää. Tämän jälkeen sivusto järjestelee otsake-tiedot selkeämpään muotoon. Tällaisia lajittelupalveluja tarjoaa esimerkiksi www.mxtoolbox.com. Yksityisyyttään varjelevien on syytä pitää mielessä, että mikäli ei halua kenenkään muun saavan tietoa omien viestien liikkeistä, on järkevintä analysoida otsakkeet itse. Seuraava esimerkki otsak-

keista on kopioitu Gmailista normaalissa muodossa. Alempana on kuva mxtoolboxin avulla järjestellyistä otsakkeista.

Delivered-To: visa.hanninen@gmail.com
Received: by 10.213.7.7 with SMTP id b7cs15933ebb;
Fri, 2 Jul 2010 00:21:11 -0700 (PDT)
Received: by 10.100.201.16 with SMTP id y16mr295862anf.241.1278055270216;
Fri, 02 Jul 2010 00:21:10 -0700 (PDT)
Return-Path: <Order_Shipped@hobbyking.com>
Received: from www.hobbyking.com (www.hobbyking.com [174.143.95.154])
by mx.google.com with ESMTP id j5si1047848ybe.96.2010.07.02.00.21.09;
Fri, 02 Jul 2010 00:21:10 -0700 (PDT)
Received-SPF: pass (google.com: domain of Order_Shipped@hobbyking.com designates 174.143.95.154 as permitted sender) client-ip=174.143.95.154;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of Order_Shipped@hobbyking.com designates 174.143.95.154 as permitted sender) smtp.mail=Order_Shipped@hobbyking.com
Received: from mail pickup service by www.hobbyking.com with Microsoft SMTPSVC;
Fri, 2 Jul 2010 15:21:09 +0800
thread-index: AcsZtySqOSYyAztuQkSD9v85bZ+xLw==
Thread-Topic: Your parcel has been sent from the HobbyKing.com warehouse!
From: <Order_Shipped@HobbyKing.com>
To: <visa.hanninen@gmail.com>
Subject: Your parcel has been sent from the HobbyKing.com warehouse!
Date: Fri, 2 Jul 2010 15:21:09 +0800
Message-ID: <9A100C8E4AAE4917A909008830CDCD3E@228006web1>

Email Header Analyzer

Paste Header:

```
Delivered-To: visa.hanninen@gmail.com
Received: by 10.213.7.7 with SMTP id
b7cs15933ebb;
        Fri, 2 Jul 2010 00:21:11 -0700
(PDT)
Received: by 10.100.201.16 with SMTP id
y16mr295862anf.241.1278055270216;
```

Analyze Header

Hop	Delay	from	by	with	time (UTC)
1	*	mail	www.hobbyking.com	Microsoft SMTPSVC	7/2/2010 7:21:09 AM
2	1 second	www.hobbyking.com 174.143.95.154	mx.google.com	ESMTP	7/2/2010 7:21:10 AM
3	0 seconds		10.100.201.16 10.100.201.16	SMTP	7/2/2010 7:21:10 AM
4	1 second		10.213.7.7 10.213.7.7	SMTP	7/2/2010 7:21:11 AM

HeaderName	HeaderValue
Delivered-To	visa.hanninen@gmail.com
Return-Path	<Order_Shipped@hobbyking.com>
Received-SPF	pass (google.com: domain of Order_Shipped@hobbyking.com designates 174.143.95.154 as permitted sender) client-ip=174.143.95.154;
Authentication-Results	mx.google.com; spf=pass (google.com: domain of Order_Shipped@hobbyking.com designates 174.143.95.154 as permitted sender) smtp.mail=Order_Shipped@hobbyking.com
thread-index	AcsZtySqOSYyAztuQkSD9v85bZ+xLw==
Thread-Topic	Your parcel has been sent from the HobbyKing.com warehouse!
From	<Order_Shipped@HobbyKing.com>
To	<visa.hanninen@gmail.com>
Subject	Your parcel has been sent from the HobbyKing.com warehouse!
Date	Fri, 2 Jul 2010 15:21:09 +0800
Message-ID	<9A100C8E4AAE4917A909008830CDCD3E@228006web1>

Kuva 4 Viestin otsaketiedot järjesteltynä helpommin luettavaan muotoon

Otsakkeiden avulla on myös mahdollista onkia esiin muita viestiin liittyviä tietoja. Niistä selviää muun muassa, tukevatko matkan varrella olleet palvelimet ESMTP:tä vai vanhempaa SMTP:tä. Lisäksi otsakkeiden analysoinnilla selviää viestin lähettämisestä saapumiseen kulunut aika.

Otsake-tietoja käytetään myös roskapostin torjuntaan. Roskapostia voi yrittää torjua esimerkiksi www.spamcop.net-sivuston avulla. Tällöin saadusta roskapostista on ensin kaivettava esiin otsake-tiedot. Sen jälkeen niitä on tutkittava joko jonkin avustavan palvelun kautta tai ilman. Otsakkeiden analysoinnissa on syytä olla tarkkana, sillä yksi roskapostittajien käyttämä taktiikka on ujuttaa vastaanotettu-kenttään vääriä palvelinten nimiä ja IP-osoitteita jäljityksen hankaloittamiseksi. Kun otsakkeista on saatu esiin sähköpostipalvelin, joka viestin on alun perin lähettänyt, voidaan se ilmoittaa Spamcopille. Spamcop osaa selvittää, kenen Internet-operaattorin verkossa kyseinen palvelin on. Tämän jälkeen se lähettää viestin kyseiselle operaattorille, joka puolestaan voi lähettää huomautuksen asiakkaalleen tai jopa sul-

kea liittymän. Spamcopin tarjoama raportointipalvelu on maksuton vaihtoehto, jolla roskapostia voidaan vähentää.

Toinen tekniikka on Reverse MX, eli RMX-tietue, jonka idea on tarkistaa FROM-kentässä näkyvän lähettäjän toimialue ja IP-osoite, ennen kuin viestiä suostutaan ottamaan vastaan. Näitä tietoja verrataan Domain Name Systemistä (DNS) löytyvään IP-osoitteeseen ja toimialueen nimeen. Mikäli osoitteet eivät vastaa toisiaan, on todennäköistä, että viestin lähettäjä-osoite on väärennetty ja viesti on todennäköisesti roskapostia. Suodatukseen on myös olemassa huomattavasti tarkempia, viestin sisältöä analysoivia ohjelmia joista lisää edempänä. RMX-tietueen käyttö jäi vähäiseksi, eikä se ole käytössä nykyään laajalti siihen liittyneiden ongelmien takia. Periaatteessa RMX suodattaisi viestejä yhteystasolla, eli ylimääräistä kuormaa verkon muille laitteilla ei roskapostista syntyisi. [7.]

RMX-tietuetta paljolti muistuttava Sender Policy Framework (SPF) on sen sijaan menestynyt paremmin. SPF tarjoaa keinon lähettäjä-kentän osoitteen väärennystä vastaan. SPF:n käyttö edellyttää, että toimialueen omistaja määrittelee DNS-tietoihin, mitkä palvelimet ovat toimialueen lähettäviä postipalvelimia. Kun vastaanottava palvelin sitten vastaanottaa viestiä, voi se tarkistaa, vastaako lähettäjä-kentässä oleva osoite DNS:stä löytyvää osoitetta. Mikäli osoitetta ei löydy, voidaan todeta, että lähettäjä-kentän osoite on väärennetty. SPF:n todellinen hyöty saadaan käyttöön siinä vaiheessa, kun jokainen lähettävä sähköpostipalvelin on listattu DNS-palvelinten tietoihin ja jokainen sähköpostia vastaanottava palvelin on määritelty varmistamaan lähettäjä-osoite DNS-palvelimelta.

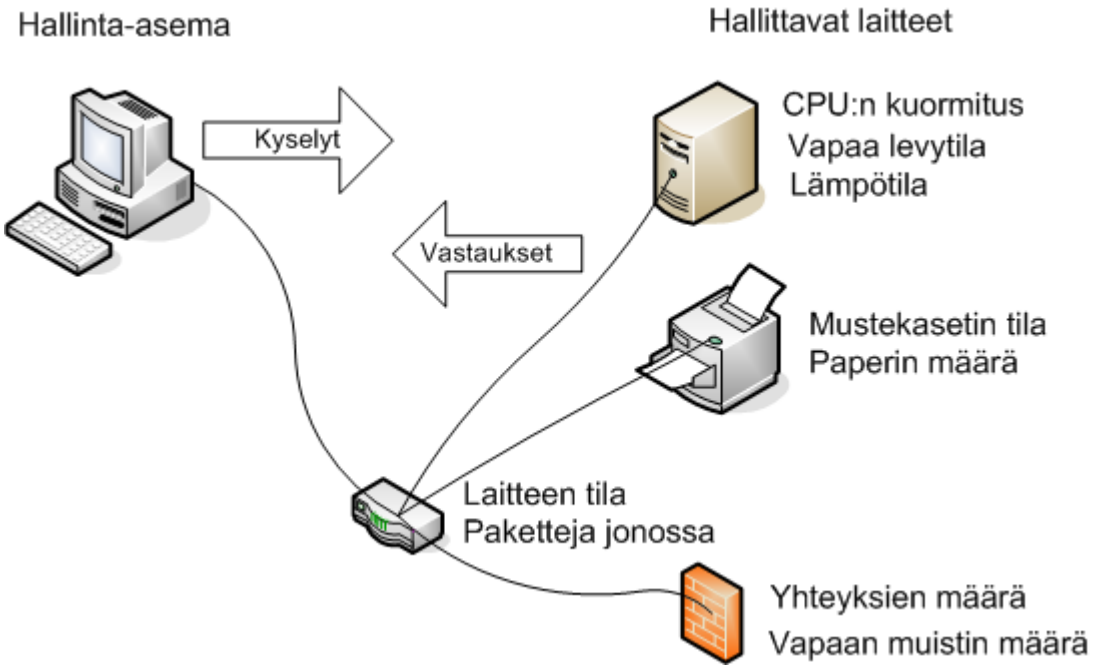
3 SNMP

Simple Network Management Protocol (SNMP) on verkkolaitteiden valvontaan ja hallintaan kehitetty protokolla. Aikaisemmin verkkolaitteita valvovat henkilöt joutuivat ottamaan yhteyden suoraan kulloinkin valvottavaan laitteeseen esim. Telnetin tai Secure Shellin (SSH) kautta. SNMP mahdollistaa verkkolaitteiden monitoroinnin erillisellä SNMP-pohjaisella verkonvalvontaohjelmalla, johon voidaan koota useiden eri laitteiden tiedot samanaikaisesti. Tämä nopeuttaa ja helpottaa laitteiden valvontaa, koska erillisiä terminaaliyhteyksiä ei tarvitse avata jokaiselle laitteelle, vaan kaikkien laitteiden tiedot saadaan kerättyä keskitetysti. Tällöin valvoja saa halutessaan tiedot kaikista

verkossa olevista laitteista yhteen näkymään, josta näkee nopeasti, jos jokin laite on vikaantunut. Verkossa olevat laitteet voidaan myös konfiguroida lähettämään tietoa automaattisesti jollekin valvontakoneelle, jolloin käyttäjän ei tarvitse käyttää aikaa tiedon keräämiseen. Mikäli valvontakoneella käytettävä ohjelmisto on tarpeeksi monipuolinen, voi se lähettää tiedon tapahtumista esimerkiksi sähköpostilla tai tekstiviestillä. Tämä mahdollistaa sen, ettei valvontakoneen tarvitse olla miehitettynä kellon ympäri. [8.]

SNMP koostuu SNMP-osapuolesta, jota kutsutaan yleensä agentiksi, hallinta-asemasta sekä hallintaprotokollasta. Hallintaprotokollaa käytetään tiedonsiirtoon agentin ja hallinta-aseman välillä. SNMP vaatii toimiakseen valvottavan laitteen, jossa agentilla on pääsy järjestelmän tietoihin, sekä verkonhallintaohjelmiston hallinta-asemalla. Luonnollisesti vaaditaan myös verkko, jotta edellä mainitut laitteet pystyvät kommunikoimaan keskenään. Lisäksi SNMP tulee olla verkossa sallittujen palveluiden listalla. SNMP:stä on olemassa kolme eri versiota, mutta käytännössä riittää, jos ymmärtää, kuinka versio 1 toimii. [9, s. 1 - 4.]

Nykypäivän verkoissa tietoturvaan on syytä kiinnittää huomiota ja sen takia myös SNMP-protokollaan on kehitetty salaus. Salaus on tosin mukana vasta SNMP:n kolmannessa versiossa. Salauksen etuna on se, että SNMP:tä voidaan käyttää myös sellaisissa verkoissa, jotka eivät ole omassa omistuksessa. Näin ollen niiden turvallisuutta on vaikea taata. Kolmannessa versiossa on mukana myös aikaisempia versioita vahvempi autentikointi, joka perustuu joko Message Digest 5 (MD5) tai Secure Hash Algorithm (SHA). Näiden ansiosta käyttäjänimet ja salasanat eivät kulje verkossa selkokielisinä, vaan tiivisteinä. [10, s. 271.] Kuvasta viisi selviää SNMP:n toiminta yksinkertaistettuna. Erilaisilta laitteilta voidaan valvoa erilaisia arvoja, kuten paperin määrä, vapaan muistin määrä ja niin edelleen.



Kuva 5 SNMP:n toiminta yksinkertaistettuna

3.1 MIB

Nimensä mukaisesti SNMP on melko yksinkertainen protokolla. SNMP-protokolla ei itse määrittele, minkälaista tietoa laitteesta voidaan lukea, vaan toiminta perustuu Management Information Baseihin, eli MIB:eihin. Jokaisella laitteella on omanlaisensa MIB, johon on määritelty muuttujia, joita kyseisestä laitteesta voidaan valvoa. Näitä voivat esimerkiksi olla suorittimen kuormitusaste, vapaana olevan muistin määrä tai tuulettimen kierrosnopeus. Kun valvontakoneella oleva SNMP-ohjelma ottaa yhteyttä valvottavaan verkkolaitteeseen, pyytää se muuttujien arvoja, jotka MIB:ssä on määritelty. Valvottavalla laitteella oleva agentti koostaa tiedon MIB:ssä määritellyistä asioista ja muuntaa ne SNMP:n käyttämään muotoon. Tämän jälkeen tieto siirtyy valvontakoneelle, jossa sitä voidaan analysoida.

Kaikkia MIB:ssä määriteltyjä muuttujia ei suinkaan tarvitse valvoa. Mikäli kyseessä on esimerkiksi virtualisoitu palvelin, on turhaa valvoa tuulettimien kierrosnopeutta, sillä niiden arvo on nolla. Tällöin hallinta-asemalla voidaan valita vain kiinnostavat muuttujat, joita valvotaan. Näin kysely on nopeampi, ja kapasiteettia säästyy. Lisäksi säästyy levytilaa, mikäli muuttujien arvoista kerätään statistiikkaa. Muutoksia ei kuitenkaan kannata tehdä varsinaisen valvottavan laitteen MIB:iin vaan tehdä ne pelkästään hallinta-asemalle. [9, s. 3 – 4.]

3.2 OID

Tärkeä osa SNMP-protokollaa on myös Object Identifier (OID). OID:t ovat yksittäisiä muuttujia MIB:ssä. Esimerkkinä OID:stä voisi olla vaikkapa tuulettimen kierrosnopeus työasemassa. Sillä on jokin numerosarjaa muistuttava tunnus, esimerkiksi 1.2.3.4.5.6.7.8.9, jolla se pystytään tunnistamaan tuulettimen kierrosnopeudeksi. Tällä tunnuksella sitä voidaan lukea käyttämällä valvontakoneella olevaa SNMP-pohjaista hallintaohjelmaa. Kaikki laitteesta löytyvät muuttujat on siis kuvattu numeerisin arvoin ja kerätty laitteen MIB:iin. [11.]

Tietoa voidaan siirtää myös toiseen suuntaan. Osa verkkolaitteista antaa mahdollisuuden asetusten muuttamiseen SNMP:tä käyttämällä. Tällöin valvontakone lähettää muutettavan arvon kohti valvottavassa verkkolaitteessa olevaa agenttia, joka tekee muutokset laitteen konfiguraatioon. Arvot, joita voidaan tällä tavoin muutella vaihtelevat laitteesta riippuen. Jostain laitteesta voi vaihtaa nimen tai portille määrätyn IP-osoitteen, kun jostain toisesta laitteesta ei voi vaihtaa mitään. Jos käytössä on laite, joka tukee asetusten muuttamista SNMP:n avulla, on syytä pitää mielessä, että SNMP-versio 1 lähettää tiedon selkokielisenä tekstinä, eli kuka tahansa voi kaapata tiedon siirron aikana. Lisäksi tunnistaminen perustuu selväkielisinä lähetettäviin Community Stringeihin, joita kuka tahansa pystyy kaapatessaan lukemaan.

3.3 Komennot

SNMP-protokollan ensimmäisessä versiossa on määritelty seuraavat viisi komentoa tiedonkeruuta ja muuttamista varten:

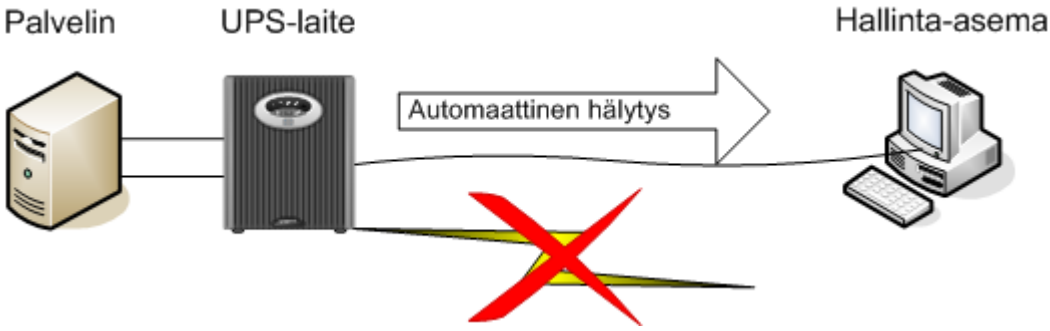
- GetRequest
- GetNextRequest
- SetRequest
- GetResponse
- Trap.

Yksinkertaisimmillaan tiedonkeruu tapahtuu käyttämällä GetRequest-komentoa, jolloin valvontatyöasema tai -järjestelmä hakee yhden tai useamman arvon valvottavan laitteen agentilta. GetNextRequest hakee vastaa-

vasti seuraavan kentän arvon. Tietoa voidaan muuttaa laitteella käyttämällä SetRequest-komentoa. GetResponse on valvottavalla laitteella olevan agentin lähettämä vastaus valvontakoneelle. Tiedonkeruuseen valvottavalta laitteelta voidaan käyttää myös SNMPWALKia, jolloin ennalta määritellyt tiedot haetaan yhdellä komennolla ilman, että joudutaan käsin lähettämään erikseen jokaista GetRequest-komentoa. [12.] SNMPWALK ikään kuin ”kävelee” MIB:ssä määritellyt tietokentät läpi ja hakee niistä haluttuja tietoja.

3.4 Trap

Tietoa valvottavista laitteista voidaan kerätä myös ”trapeillä”. Träppi on jokin ehto tai ehtojen kokonaisuus, joiden täyttyessä valvottava laite lähettää itse omista tiedoistaan generoiman raportin. [8.] Tällaisen raportin voi esimerkiksi generoida Uninterruptible Power Supply eli UPS-laite. Raportti generoidaan esimerkiksi sähkökatkon sattuessa tai akun varauskapasiteetin laskiessa. Tällä tavoin esimerkiksi tieto sähkökatkoksesta lähtee heti kohti valvontakonetta, joka voi esimerkiksi hälyttää teknikon paikalle tekstiviestillä. Jos träppejä ei käytettäisi, pitäisi valvontakoneen ”pollata” eli lähettää kyselyä jatkuvasti UPS-laitteelle, joka puolestaan lisäisi kuormaa verkossa.



Kuva 6 SNMP-trapin toiminta sähkökatkon sattuessa

4 SMTP-RELEOINTIPALVELU

SMTP-releointipalvelu ei ole mikään uusi keksintö. Releointia on käytetty niin kauan kuin sähköpostia on välitetty SMTP:n avulla. Itse sana releointi tarkoittaa vain jonkin asian välittämistä eteenpäin. Lähetettäessä sähköpostia yrityksen sisällä samassa toimipisteessä olevien henkilöiden välillä, ei sähköposti välttämättä kulje releointi-palvelimen kautta. Tällöin lähetetty viesti toimitetaan samalla palvelimella olevan käyttäjän postilaatikkoon ilman, että se kulkee ulos muille palvelimille. Näissä tapauksissa viestinvälitys on yleensä nopeaa, ja virheitä syntyy vähän.

4.1 Palvelun kuvaus

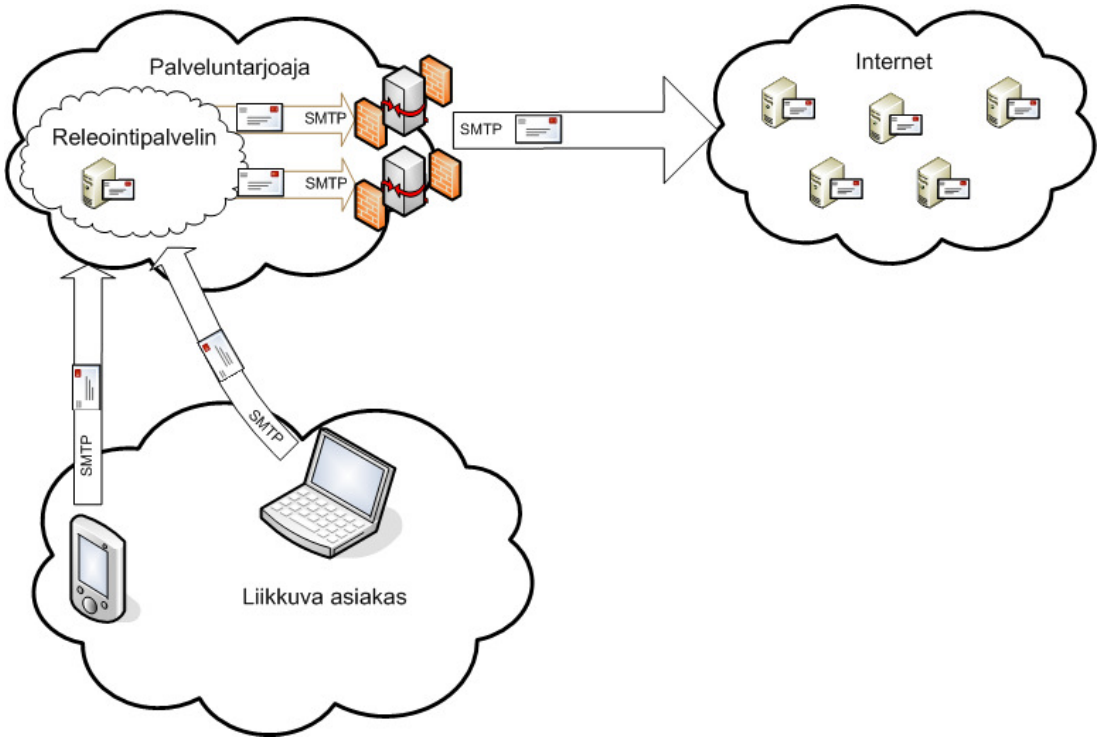
Kun sähköpostia lähetetään yrityksestä toiseen tai kotikäyttäjältä toiselle, kiertää viesti yleensä muutaman palvelimen kautta. Tällöin lähettäjä-palvelimen ja vastaanottaja-palvelimen välissä olevia palvelimia kutsutaan releointi-palvelimiksi, sillä ne ottavat viestin vastaan ja lähettävät sen eteenpäin. Posti voi kiertää, kuinka monen palvelimen kautta tahansa ja mahdollinen vastaus viesti saattaa kiertää eri reittiä pitkin. Jos esimerkiksi käyttäjä, jolla on oma Internet-yhteys kotonaan, lähettää viestin käyttämällä esimerkiksi Outlook Express- tai Mozilla Thunderbird –sähköpostiohjelmistoa, lähtee viesti häneltä kohti palveluntarjoajaa SMTP-protokollan välityksellä. Jos käyttäjä päättää käyttää webmail-sovellusta, eli web-selaimella käytettävää sähköpostia, ei viesti lähde hänen työasemaltaan SMTP-muotoisena vaan se kulkee HTTP:n ylitse palveluntarjoajan sähköpostipalvelimelle, josta se lähtee eteenpäin SMTP-muodossa.

Käyttäjän painaessa lähetä-nappia sähköpostiohjelmistossaan, lähtee viesti kohti palveluntarjoajan SMTP-palvelinta. [5, s. 1.] Tällöin käyttäjän sähköpostiohjelma muodostaa SMTP-yhteyden palveluntarjoajan sähköpostipalvelimeen. Yleisesti ottaen palveluntarjoajat eivät anna muiden palveluntarjoajien asiakkaiden käyttää omia SMTP-palvelimiaan releointiin. Suodatus perustuu usein IP-osoiteavaruuksiin, sillä palveluntarjoajilla on tieto niistä IP-osoitteista, jotka sijaitsevat heidän omissa verkoissa. Kun käyttäjä on tunnistettu omaksi, voidaan hänen antaa muodostaa SMTP-protokollan mukainen yhteys palvelimen kanssa. Jotkin palveluntarjoajat saattavat lisäksi edellyttää muunlaista varmentamista, kuten käyttäjätunnusta ja salasanaa, viestien välitykseen.

Kuten aiemmin on mainittu, palveluntarjoajat eivät mielellään anna käyttää sähköpostipalvelimiaan muiden kuin omien asiakkaidensa viestien välitykseen. Tästä saattaa muodostua ongelmia varsinkin matkustaville käyttäjille. Jos käyttäjä on tehnyt kannettavan tietokoneensa sähköpostiohjelmaan määritykset, mitä sähköpostipalvelinta käytetään viestin lähetykseen kotona ollessa, eivät samat määritykset välttämättä toimi, jos viestejä yritetään lähettää esimerkiksi lentokentältä tai nettikahvilasta langatonta verkkoa pitkin. Tämä johtuu siitä, että tällöin käyttäjä voi olla eri palveluntarjoajan verkossa. Käyttäjän pitäisi tällöin vaihtaa omat sähköpostipalvelin määritykset oikeiksi. Tätä varten pitäisi kuitenkin tietää käytettävissä olevan palveluntarjoajan

sähköpostipalvelimen osoite ja mahdolliset tunnukset sen käyttöä varten. Näitä tietoja ei tosin aina ole saatavilla.

Ongelmaan on olemassa melko yksinkertainen ratkaisu. Käyttäjä, joka matkustaa usein ja haluaa käyttää sähköpostia eri paikoissa, voi käyttää webmail-sovellusta, joka on immuuni tällaisille ongelmille. Toinen vaihtoehto on käyttää jotain releointi-palvelua, joka vastaanottaa käyttäjän sähköpostiohjelmistolla luodut viestit ja lähettää ne eteenpäin. Tällaisia releointi-palveluita on tarjolla useita, niin koti- kuin ulkomaisiakin. Palvelua tarjoavat myös jotkin teleoperaattorit. Käytettäessä jotain releointi-palvelua käyttäjän tarvitsee yleensä määritellä sähköpostin lähetykseen liittyvät asetukset vain kerran. Vaikka käyttäjä veisi kannettavansa johonkin toiseen verkkoon, pystyy sähköpostiohjelmisto muodostamaan yhteyden aiemmin määriteltyyn releointipalvelimeen ja lähettämään viestit. Tällöin on kuitenkin suositeltavaa suojata yhteys käyttämällä esimerkiksi Transport Layer Security:ä (TLS), etteivät viestit joudu vääriin käsiin.



Kuva 7 Sähköpostin lähetys releointi palvelinta käyttäen

Periaatteessa on mahdollista pystyttää oma sähköpostin releointiin käytettävä palvelin kotiin. Ongelmaksi saattaa kuitenkin muodostua palveluntarjo-

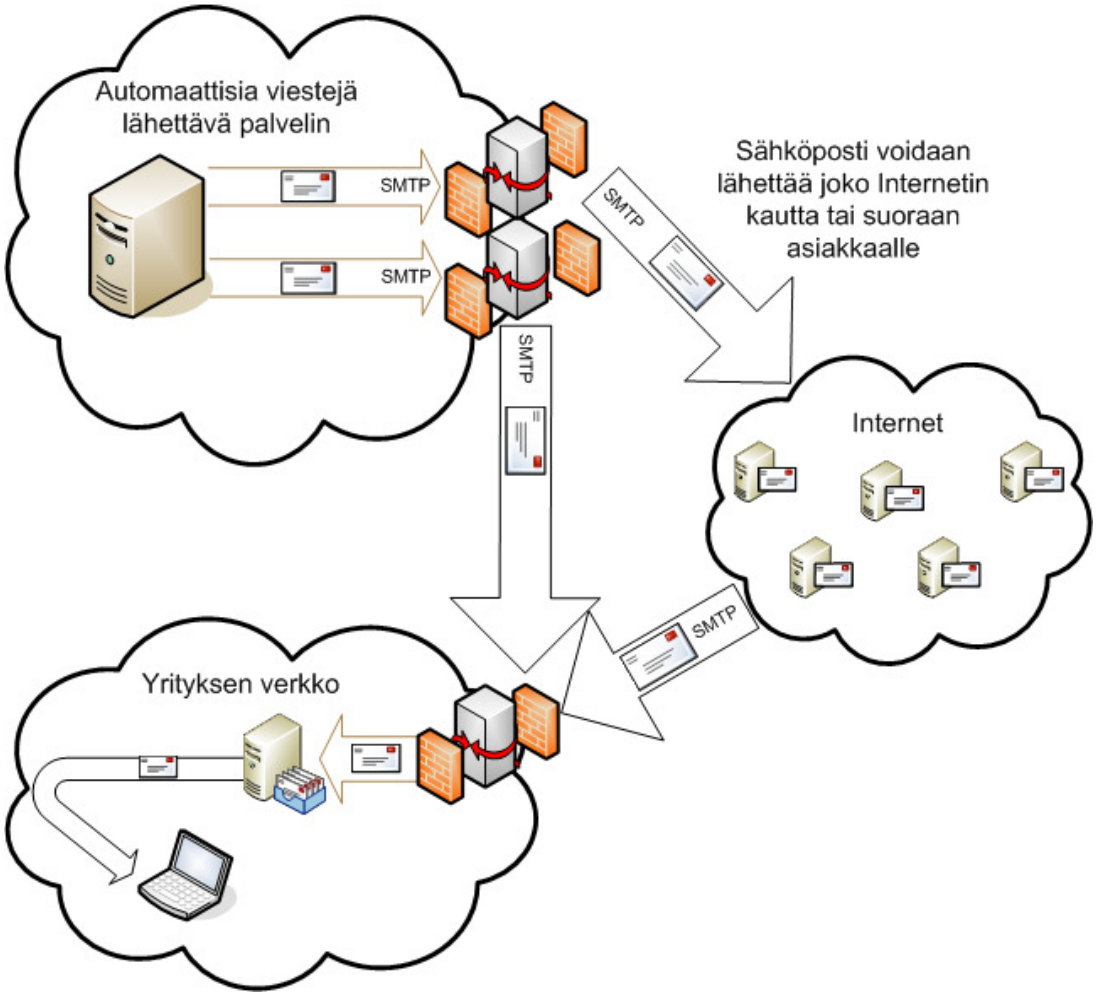
ajan politiikka omien palvelinten pitoa kohtaan. Osa operaattoreista on myös kieltänyt liikenteen porttiin 25, joka on yleisesti SMTP-liikenteen käyttämä portti. Lisäksi on huomioitava oman palvelimen maineen puhtaana pysyminen. Jos omaa palvelinta käyttää ainoastaan yksi käyttäjä, ongelmia tuskin syntyy. Mikäli useampi käyttäjä käyttää samaa lähtevän postin palvelinta, on olemassa vaara, että palvelimen kautta välitetään roskapostiksi, eli spämmiksi, luokiteltavia viestejä. Roskaposti on sähköpostin kannalta kiusallinen ilmiö, sillä käyttäjillä, joilla ei ole aktiivista roskapostin suodatinta, kuluu valtavasti aikaa oikeiden viestien erottelemiseen roskan seasta. Tämän takia roskapostiin ja sitä lähettäviin palvelimiin suhtaudutaan kielteisesti. Mikäli omassa käytössä olevalta palvelimelta lähetetään roskapostiksi luokiteltavia viestejä, on vaarana palvelimen joutuminen niin sanotulle mustalle listalle. Tällöin eteenpäin lähetetyt oikeat viestit eivät pääse enää perille, koska osa roskapostisuodattimista suodattaa kaiken tietyistä IP-osoitteista tulevan liikenteen, oli se roskapostia tai ei. Palveluntarjoaja voi myös sulkea liittymän, josta roskapostia lähetetään.

Osa releointi-palvelua tarjoavista yrityksistä on ratkaissut palvelimen maineen säilymiseen liittyvän ongelman suodattamalla myös kaiken ulos lähtevän liikenteen. Yleensä puhuttaessa sähköpostiliikenteen suodatuksesta, tarkoitetaan nimenomaan sisään tulevaa liikennettä. Lähtevän postin suodatus on kuitenkin tärkeää, sillä siten voidaan estää palvelimen joutuminen mustalle listalle ja sen avulla varmistamaan postin kulkeminen oikealla tavalla. Lisäksi on hyvien tapojen mukaista lähettää vain oikeaa ja tarkistettua postia. Roskapostia ja viruksia lähettävää yritystä ei katsota hyvällä ja ennemmin tai myöhemmin tällainen toiminta kostautuu yritykselle.

Yksi käyttökohde releointi-palvelulle on tilanne, jossa jokin järjestelmä lähettää esimerkiksi automaattisesti generoituja raportteja suoraan käyttäjille. Tällainen palvelu voi lähettää esimerkiksi tietoja palvelimen levytilasta tai muuta valvontatietoa. Jos viestien katsotaan sisältävän tietoa, jonka ei haluta joutuvan vääriin käsiin, voidaan releointi-palvelimella tehdä asetus, joka pakottaa käyttämään TLS-salausta. Näin SMTP-yhteyttä muodostaessaan palvelin neuvottelee ensin salatun ”käytävän”. Vasta kun käytävä on neuvoteltu, muodostaa palvelin SMTP-yhteyden.

Tällaisia automaattisia järjestelmiä on käytössä asiakkailla, jotka ottavat esimerkiksi palautetta vastaan jonkin web-lomakkeen avulla. Kun henkilö on

täyttänyt lomakkeen ja painaa lähetä-nappia, muuntaa palvelin raportin sähköpostimuotoon. Tämän jälkeen palvelin lähettää palauteviestin palautetta keräävälle yritykselle ja mahdollisen kiitoksen palautteen antajalle. Sähköposti on käytössä useissa automaattisissa raportointijärjestelmissä, joiden tehtävä on lähettää tietoa esimerkiksi jonkin palvelimen tai palvelun tilasta. Sähköposti on luonteva ratkaisu tähän, sillä sitä voi vastaanottaa helposti ja se on yksinkertainen toteuttaa.



Kuva 8 Sähköpostin releointi palveluntarjoajan verkosta asiakkaan verkkoon

4.2 Palvelun komponentit

Releointipalvelun komponentteina toimivat asiakas, jolla on kyseiselle palvelulle tarvetta, itse releointi-palvelin sekä pohjalla olevat tietoliikenneyhteydet. Palvelimella on oltava asennettuna jokin releoinnin mahdollistava ohjelmisto, esimerkiksi Windows Server ja IIS tai vaihtoehtoisesti avoimen lähdekoodin ohjelma. Windows-ympäristöön löytyy myös muita ilmaisia vaihtoehtoja, kuten Synametrics SMTP Gateway, jonka käyttö on maksutonta, mutta tuki

maksullista. Lisäksi releointi-palvelimella voi olla jokin viestejä suodattava ohjelmisto, kuten Symantec Brightmail tai Microsoft Antigen. Myös avoimen lähdekoodin vaihtoehtoja on saatavilla. Linuxille löytyy jo hieman iäkkäämpi Sendmail tai Postfix. Näihin on myös mahdollista liittää esimerkiksi Clam AV ja SpamAssassin. Tämän kaltaisilla tuotteilla voidaan suodattaa viruksia, matoja ja roskapostia, ja auttaa näin palvelinta pysymään poissa mustilta listoilta. Olemassa olevan tietoliikenneinfrastruktuurin on tietysti tuettava sähköpostin siirtoa, eli ainakin TCP-portti 25 on oltava sallittuna. Lisäksi on huomioitava sähköpostiliikenteen verkolle aiheuttama kuorma.

Jotkin valmistajat ovat myös alkaneet tuoda pelkästään releointi- ja yhdyskäytäväpalveluihin suunniteltuja tuotteita. Näitä ovat esimerkiksi Symantecin Brightmail Gateway sekä vuonna 2007 Ciscon omistukseen siirtynyt IronPort. Molemmissa tuotteissa on pohjalla räätälöity Linux, jonka päällä ajetaan valmistajan omaa sovellusta, jolla viestejä välitetään. IronPort edustaa omanlaistaan tuotetta, sillä se on erikseen myytävä ja asennettava fyysinen laite, joka kytketään verkkoon. IronPort asennetaan tavanomaisesti räkkiin. Brightmail Gateway on taasen saatavana sekä fyysisenä laitteena että virtualisoitavana sovelluksena, jota voidaan ajaa esimerkiksi yritykseltä ennestään löytyvällä virtualisoidulla VMware-alustalla. Tällä tavoin vältytään laiteinvestoinneilta ja säästetään tilaa sekä sähköä konesalissa. Toki tällöin tulee huomioida verkkokorttien riittävyys tai käyttää virtuaaliverkkoja. Liikennettä saattaa generoitua paljon, jolloin viivettä postien läpipääsyssä esiintyy, mikäli verkkoyhteys on riittämätön. Lisäksi palvelimella saattaa jo ennestään pyöriä virtualisoituja sovelluksia, jotka käyttävät verkkoa. Nykyiset järjestelmät kuitenkin mahdollistavat verkkokorttien lisäämisen järjestelmään ja antavat myös mahdollisuuden osoittaa tietyn verkkokortin kapasiteetti vain yhden virtuaalikoneen, tässä tapauksessa Brightmail Gatewayn käyttöön.

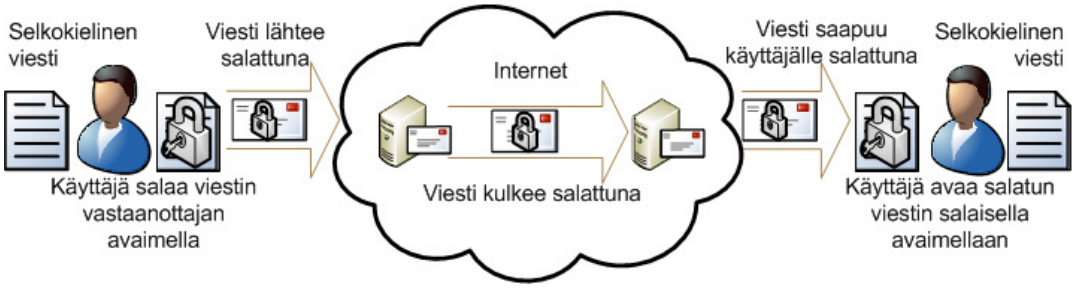
Joissain tapauksissa on myös ilmennyt ongelmia releointi-komponenttien välillä. Jotkin Mail Transfer Agentit (MTA) eivät tuota oikeanlaisia SMTP-viestejä, josta aiheutuu ongelmia muiden MTA:den kanssa. Osa agenteista on esimerkiksi muuttanut viestien otsake-kenttien järjestystä siten, ettei seuraava MTA ole enää saanut viestistä selvää. Myös liitetiedostojen korruptoituminen oli aiemmin tavallista. MTA saattoi muuttaa kohtaa, jossa liitetiedosto sijaitsi, jolloin seuraava MTA ymmärsi, että liitetiedosto oli olemassa, mut-

ta nimi ei ollut enää luettavissa. Liitteestä saattoi myös hävitä tiedostopääte, jolloin tiedosto ei ollut enää mitään tyyppiä, eikä sitä voinut avata.

4.3 Sähköpostin turvallisuus

4.3.1 PGP

SMTP on protokolla, joka lähettää viestit selkokielisinä. Tästä johtuen kaikki viestit on mahdollista lukea ja niitä on mahdollista peukaloida, mikäli joku osaava henkilö kytkeytyy linjalle. Urkinnalta ja peukaloinnilta voi suojautua käyttämällä esimerkiksi Pretty Good Privacya, eli PGP:tä. PGP muodostaa niin sanottuja luottamusverkkoja eli käyttäjä voi itse määritellä, ketkä salatun viestin pystyvät avaamaan. [13.] Toiminta perustuu siihen, että lähettäjä salaa viestin vastaanottaja julkisella avaimella, jolloin viestiä ei voi avata kuin vastaanottajan salaisella avaimella. Tähän tarkoitukseen löytyy ilmaisia ohjelmia kuten Enigmail, joka on Mozilla Thunderbirdin liitännäinen. Enigmail mahdollistaa salattujen sähköpostien lähetyksen ja vastaanoton sekä viestien allekirjoittamisen. Myös kahden sähköpostipalvelimen välinen liikenne on mahdollista salata.



Kuva 9 PGP-salatun viestin kulku

4.3.2 S/MIME

S/MIME, eli Secure Multipurpose Internet Mail Extension, on MIME-tiedon salausta varten kehitetty julkisen avaimen salausmenetelmä. S/MIME tarjoaa todennuksen, viestin koskemattomuuden ja lähettäjän väärennyksen eston käyttäen digitaalista allekirjoitusta. [14.] S/MIME:n etuna esimerkiksi PGP:hen on se, että se on osana useita moderneja sähköpostiasiakasohjelmia. S/MIME tuki löytyy esimerkiksi Microsoft Outlookista, joka on laajalti käytössä yritysmaailmassa. Toimiakseen tämä vaatii kuitenkin käyttäjätiliin liitetyn sertifikaatin, jonka avulla viestin salaaminen tapahtuu.

Tämän lisäksi sertifikaatti on toimitettava myös vastaanottavaan päähän. Muutoin vastaanottajan on tyydyttävä pelkkään kirjainsekamelskaan. Sertifikaattien lisääminen käyttäjätiliin sekä niiden jakelu muille kuuluu yleensä yrityksen teknisen tuen piiriin, jolloin loppukäyttäjän ei tarvitse huolehtia muusta kuin postin lähetyksestä.

4.3.3 TLS

Joillain palvelimilla saattaa olla käytössä muitakin tunnistamiseen käytettäviä metodeita kuin pelkkä IP-osoitesuodatus. Näitä voivat olla salasana tai sertifikaatti. Lisäksi osa palvelimista saattaa vaatia käytettäväksi Tranport Layer Securityä eli TLS:ää. Mikäli TLS on pakotettuna, ei postia voi lähettää, mikäli lähettäjän sähköpostiohjelma ei TLS:sää tue. Joissain tapauksissa TLS on valinnaisena, eli sitä voidaan käyttää, mutta se ei ole pakollista.

TLS tuki löytyy esimerkiksi Microsoft IIS -ohjelmistosta, ja se voidaan kytkeä käytettäväksi tietyille toimialueille yhdellä ruksilla. Tällöin toimialueen liikennöinti salataan käyttäen TLS-salausta.

TLS on sähköposti- ja VoIP-sovelluksissa käytettävä turvallisuutta lisäävä mekanismi. Normaalisti esimerkiksi sähköpostiviestit kulkevat selkokielisenä verkossa, jolloin kuka tahansa pystyy tutkimaan niiden sisältöä ja muokkaamaan sitä haluamakseen. TLS tarjoaa puitteet käyttäjien ja palvelimien varmentamiseen, tiedon salaukseen ja peukaloimisen estoon. TLS-suojatun yhteyden yli kulkevaa tietoa ei voida muuttaa eikä lukea siirtotiellä. TLS:n käyttö ei rajoitu pelkästään VoIP:n ja SMTP:n käyttöön, vaan sitä voidaan käyttää muillakin protokollilla.

Käytettäessä TLS:a suoritetaan ennen varsinaista SMTP-yhteyden muodostamista TLS-yhteyden avaus. TLS:n kanssa voidaan käyttää samaa TCP-porttia 25 kuin mitä SMTP käyttää ilman salausta. Kun TLS-yhteys vastaanottajaan on avattu, suoritetaan normaali SMTP-protokollan mukainen yhteyden muodostus ja siirretään posti. Kun posti on siirretty, suljetaan ensin SMTP-yhteys, jonka jälkeen myös TLS-yhteys voidaan purkaa.

Vaikka TLS tarjoaa suojaa salakuuntelijoilta ja urkkijoilta, on muutama asia syytä pitää mielessä. Ensinnäkin, TLS ei ota kantaa siihen, onko lähetyksessä oleva viesti saapunut TLS-suojattuna tai onko se ylipäätään kotoisin luotettavasta lähteestä. Toiseksi, TLS ei ota millään tavalla kantaa viestin sisäl-

töön ja sen mahdolliseen haitallisuuteen. TLS:n tehtävä on ainoastaan hoitaa sen hetkisen yhteyden suojaus. Alempaa löytyy esimerkki TLS-suojatun SMTP-yhteyden avaamisesta. [15.]

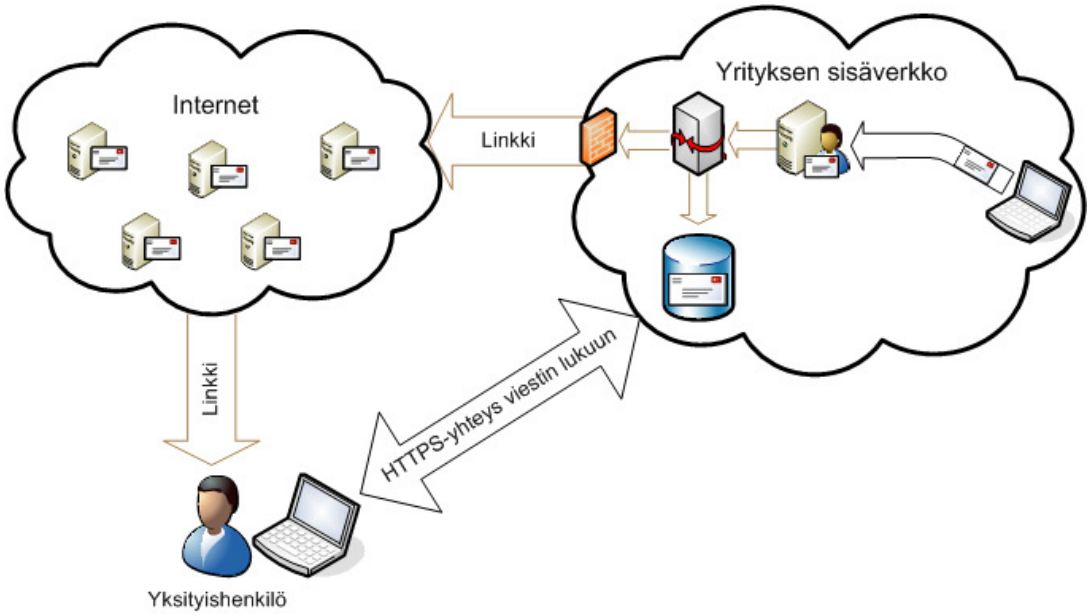
S: <Odottaa yhteydenottoa TCP porttiin 25>
C: <yhteyden avaus>
S: 220 mail.imc.org SMTP service ready
C: EHLO mail.example.com
S: 250-mail.imc.org offers a warm hug of welcome
S: 250-8BITMIME
S: 250-STARTTLS
S: 250 DSN
C: STARTTLS
S: 220 Go ahead
C: <aloittaa TLS neuvottelun>
C & S: <neuvotellaan TLS istunto>
C & S: <tarkastetaan neuvottelun tulokset>
C: EHLO mail.example.com
S: 250-mail.imc.org touches your hand gently for a moment
S: 250-8BITMIME
S: 250 DSN

4.3.4 Deltagon

Toisenlaista lähestymistapaa turvalliseen sähköpostiin tarjoaa suomalainen Deltagon. Deltagonin idea ei perustu viestin tai palvelinyhteyden salaamiseen. Turvallisuus luodaan täysin erilaisella tavalla. Deltagonin toiminta perustuu sähköpostin jättämiseen turvalliselle palvelimelle. Turvallinen palvelin puolestaan lähettää viestin sähköpostin vastaanottajalle, jossa on pelkkä linkki. Kun käyttäjä avaa viestin ja klikkaa linkkiä, avautuu Internet-selain. Selain muodostaa yhteyden turvalliselle palvelimelle käyttäen HTTPS-protokollaa, joka on siis HTTP-protokollan salattu versio. Kun yhteys on muodostettu palvelimelle, pääsee käyttäjä lukemaan hänelle lähetetyn sähköpostiviestin. Samalla käyttäjä voi halutessaan vastata viestiin käyttämällä samaa turvallista istuntoa selaimellaan.

Deltagonin tapainen ratkaisu sopii hyvin yrityksille, joiden pitää pystyä lähettämään sähköpostiviestejä turvallisesti yksityisille henkilöille. Suurella osalla ihmisistä on käytössään vain ilmaisia sähköposti-tilejä kuten Hotmail tai Gmail. Näiden turvallisuudesta ei ole välttämättä mitään takeita. Salattu HTTP-yhteys tarjoaa turvalliset puitteet viestien lähetykseen ja vastaanottoon, vaikka kyseessä olisikin ilmainen sähköposti-tili. Lisäksi turvallisuutta on vielä mahdollisuus parantaa lisäämällä linkin avaamiseen vaadittava salasana. Järjestelmä voi lähettää salasanan henkilön kännykkään, ja se voi

olla niin sanottu OTP, eli kertakäyttöinen salasana kuten pankkitunnuksissa. Deltagonin etuna on lisäksi se, ettei yksittäisten käyttäjien tarvitse itse asentaa mitään lisäohjelmia, vaan palvelu toimii suoraan selaimella.



Kuva 10 Postin kulku Deltagonia käytettäessä

4.4 Sähköpostin reititys

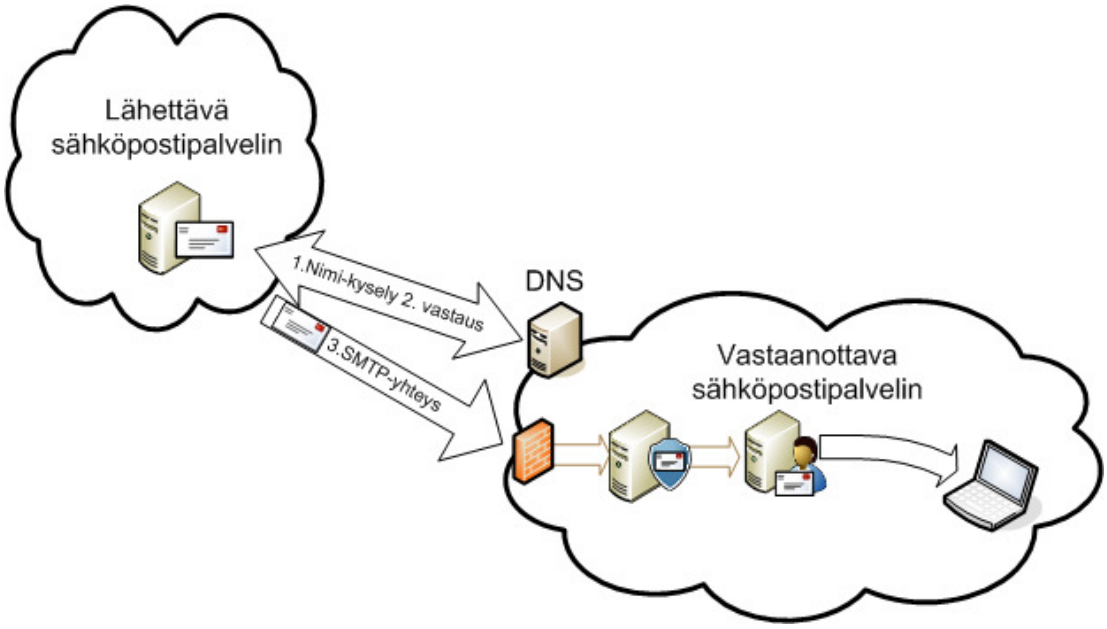
Sähköpostin reititys voidaan toteuttaa muutamalla eri tavalla. Yleensä reititettäessä postia eri palvelimelta toiselle käytetään hyväksi Domain Name Serviceä eli DNS:ää. DNS on nimipalvelu, joka kertoo esimerkiksi, mistä IP-osoitteesta löytyy toimialue metropolia.fi. DNS osaa myös kertoa, mille palvelimelle lähettää posti, joka on lähetetty osoitteella etunimi.sukunimi@metropolia.fi. Tällöin DNS katsoo, minne toimialueen metropolia.fi MX-tietue viittaa. Näin saadaan selville, minne posti pitää lähettää, jos vastaanottajalla on @metropolia.fi muotoa oleva sähköpostiosoite.

Mikäli releointi-palvelin ottaa myös ulkopuolelta tulevaa postia vastaan, on toimialueen MX-tietueen viitattava luonnollisesti tähän palvelimeen ja tarkemmin sanottuna sen IP-osoitteeseen. MX-tietueiden kääntö osoittamaan johonkin tiettyyn IP-osoitteeseen voi pahimmillaan olla todella hankala operaatio. Yleensä nimipalvelu on jonkin ison operaattorin hallussa, jolta pitää tilata kääntö toiseen suuntaan. DNS-tietojen omistajan voi selvittää nslookup-nimisen ohjelman avulla, kunhan vaihtaa tyypiksi ”SOA”. Esimerkiksi toimialueen metropolia.fi ensisijainen nimipalvelin on ns.metropolia.fi, joka on vastuussa kyseisen toimialueen nimipalvelutietojen välittämisestä.

Toinen tapa reitittää postia on staattinen reititys. DNS:ään perustuva reititys on dynaamista, eli kun palvelimen nimi tai IP-osoite vaihtuu, päivitetään se DNS-palvelimelle. Sen avulla posti voidaan reitittää oikein. Staattisessa reitityksessä ideana on määritellä käsin pakotetusti jokaisen vastaanottavan sähköpostipalvelimen osoite lähettävälle palvelimelle. Tällöin, kun palvelin haluaa reitittää postia esimerkiksi metropolia.fi toimialueelle, katsoo se itse omasta listasta osoitteen sen sijaan, että kysyisi osoitetta DNS-palvelimelta. Jos vastaanottavan palvelimen IP-osoite vaihtuu, täytyy se määritellä käsin uudelleen, jotta posti taas kulkee. Staattisista määrittelyistä saattaa aiheutua myös päänvaivaa suurissa verkkoympäristöissä. Dynaaminen reititys mukautuu itse muutoksiin, kun taas staattista reititystä käyttäville laitteille on manuaalisesti käytävä kertomassa muutokset.

Käytännössä suurin osa sähköpostipalvelimista käyttää hyväkseen DNS-palvelimien tarjoamia MX-tietueita. Tästä on myös se hyöty, että toimialueella voi olla useampia sisään tulevaa postia vastaanottavia palvelimia. Jos jokin näistä palvelimista vikaantuu ja lakkaa vastaamasta, voidaan siirtyä käyttämään seuraavaa palvelinta. MX-tietueet on määritelty tietyllä preferenssillä ja alimman preferenssin omaava palvelin on aina ensisijainen, johon postia aletaan reitittää. Myös MX-tietueiden selvitys onnistuu nslookupilla, kunhan tyypiksi vaihdetaan ”mx”. Internetistä löytyy lisäksi useita sivuja, joilla voi selvittää mihin, jonkin tietyn toimialueet MX-tietueet viittaavat. Toisin päin selvittäminen, eli minkä toimialueen MX-tietueet viittaavat jollekin yksittäiselle palvelimelle, onkin haastavampaa. Internetistä löytyy kuitenkin sivusto tähänkin tarkoitukseen, tosin sen tarjoamien tietojen oikeellisuudesta ei ole varmuutta. Palvelu vaikuttaa perustuvan ainoastaan listaan selvitetyistä MX-tietueista, eikä se siis tee varsinaista selvitystä itse.

Sähköpostin reitityksellä on myös suuri vaikutus postin oikeaan kulkuun. Pahimmillaan huonosti tehdystä reitityksestä on seurauksena viestien välitys henkilöille, joille ne eivät kuulu. Reititysongelmat saattavat näkyä myös postien katoamisena, eli ne eivät koskaan saavu vastaanottajalle. Ajan tasalla pysyminen on oikeanlaisen reitityksen kannalta tärkeää. Mikäli vanhoja tietoja jätetään DNS-palvelimelle tai sähköpostia välittäville palvelimille, saattaa seurauksena olla postin kulku väärälle palvelimelle.



Kuva 11 DNS:n toiminta sähköpostin lähetyksessä

Kuvassa 11 näkyy, kuinka lähettävä sähköpostipalvelin tekee ensin DNS-kyselyn ja saa siihen vastauksen nimipalvelimelta. Vasta tämän jälkeen palvelin tietää, mihin osoitteeseen sen tulee ottaa yhteyttä. Kun osoite on selvillä, voidaan SMTP-yhteys vastaanottavaan palvelimeen muodostaa ja lähettää posti.

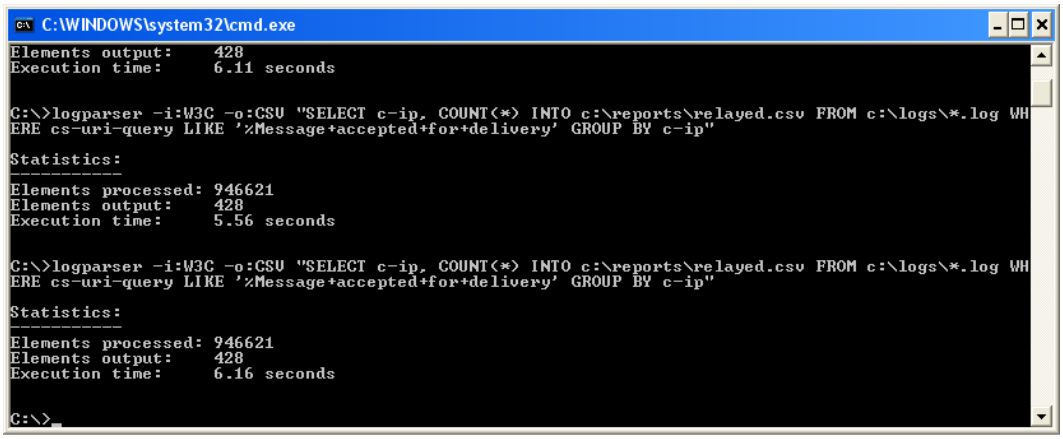
4.5 SMTP-lokit

Oli kyseessä sitten sähköpostipalvelin tai web-palvelin, tuottaa se aina jonkinlaista lokia. Lokit ovat erityisen hyödyllisiä selvitettäessä virheitä, sillä niihin tallentuu runsaasti tietoa tapahtumista. Joissain ohjelmistoissa on myös mahdollista nostaa lokin tarkkuutta ja valita lisää asioita, joista lokia kerätään.

Useat palveluntarjoajat myyvät releointi-palvelua johonkin kiinteästi määriteltyyn hintaan. Hinnoittelun perusteena ei käytetä releoitujen viestien määrää vaan asiakas maksaa kiinteän kuukausimaksun, lähetti hän sitten kaksi tai kaksituhatta sähköpostia palvelun kautta. Niissä tapauksissa, joissa käytössä on Windows Server –alustalla ajettava IIS, on välitettyjen viestien laskeminen kuitenkin suhteellisen yksikertaista.

Lokit eivät ole kovinkaan helposti luettavissa ilman järjestelyä. Järjestelyyn on olemassa useita eri ohjelmia, sekä ilmaisia että maksullisia. Microsoft tarjoaa ilmaisena ohjelmaa nimeltä Log Parser. Log Parser on oikeastaan

enemmän Structured Query Languagea, eli SQL:ää muistuttava moottori, johon voidaan luoda sopivia kyselyitä. Kun oikeanlainen kysely kohdistetaan IIS:n tuottamiin SMTP-lokitiedostoihin, saadaan analysoitua tarkasti, kuinka monta viestiä mistäkin IP-osoitteesta on lähetetty palvelimen kautta ja kuinka monta lähetystä on epäonnistunut. Log Parser mahdollistaa lokin analysoinnin erittäin tarkasti, kunhan käyttäjä jaksaa opetella ohjelman kryptisen syntaksin. Log Parser on komentoriviltä käytettävä työkalu, joka ei tarjoa minkäänlaista graafista käyttöliittymää, vaan sitä ohjaillaan pelkästään komentojen avulla. Tämä aiheuttaa alussa hankaluuksia, mutta jos syntaksin vaivautuu opettelemaan, tarjoaa Log Parser suorituskykyä ja mahdollisuuksia, jotka graafisista ilmaisohjelmista puuttuvat. Lisäksi Log Parserilla on mahdollista analysoida vaikka koko kuukauden lokit kerralla, joka ei onnistunut millään graafisella ilmaisohjelmalla. Lokien koot ovat niin suuria, että graafisella käyttöliittymällä varustetut ohjelmat kaatuivat tai eivät edes antaneet analysoida niin suurta määrää tietoa.



Kuva 12 Log Parserin käyttöliittymä ja esimerkkikysely

4.6 Avoin releointi

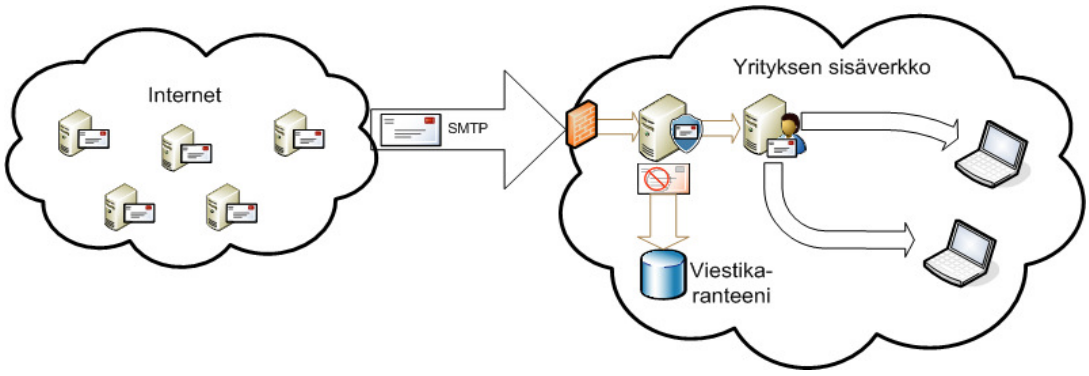
Aikaisemmin, kun Internet ei toiminut pelkästään TCP/IP:n päällä, oli olemassa joukko yleisiä avoimia postipalvelimia, joiden kautta postia saattoi kuka tahansa lähettää. Lähettävät postipalvelimet käyttivät näitä avoimia palvelimia viestien välitykseen verkosta toiseen. Tämä mahdollisti myös sen, että kuka tahansa saattoi ottaa yhteyden palvelimen porttiin 25 ja lähettää telnettiä käyttämällä sähköpostia kenelle tahansa. Tällöin viestien lähettäjäkenttään pystyi myös laittamaan minkä tahansa nimen ja toimialueen. Nykyi-

sin, kun Internet käyttää TCP/IP:tä kaikkialla, ja reititys on reitittimillä automatisoitua, ei tarvetta julkisille avoimille postipalvelimille ole.

Tällaiset julkiset avoimet postipalvelimet joutuisivat nykyään automaattisesti mustalle listalle. Tämä johtuu siitä, että roskapostin lähettäjät käyttäisivät näitä palvelimia armotta hyödyksi omien viestiensä välityksessä.

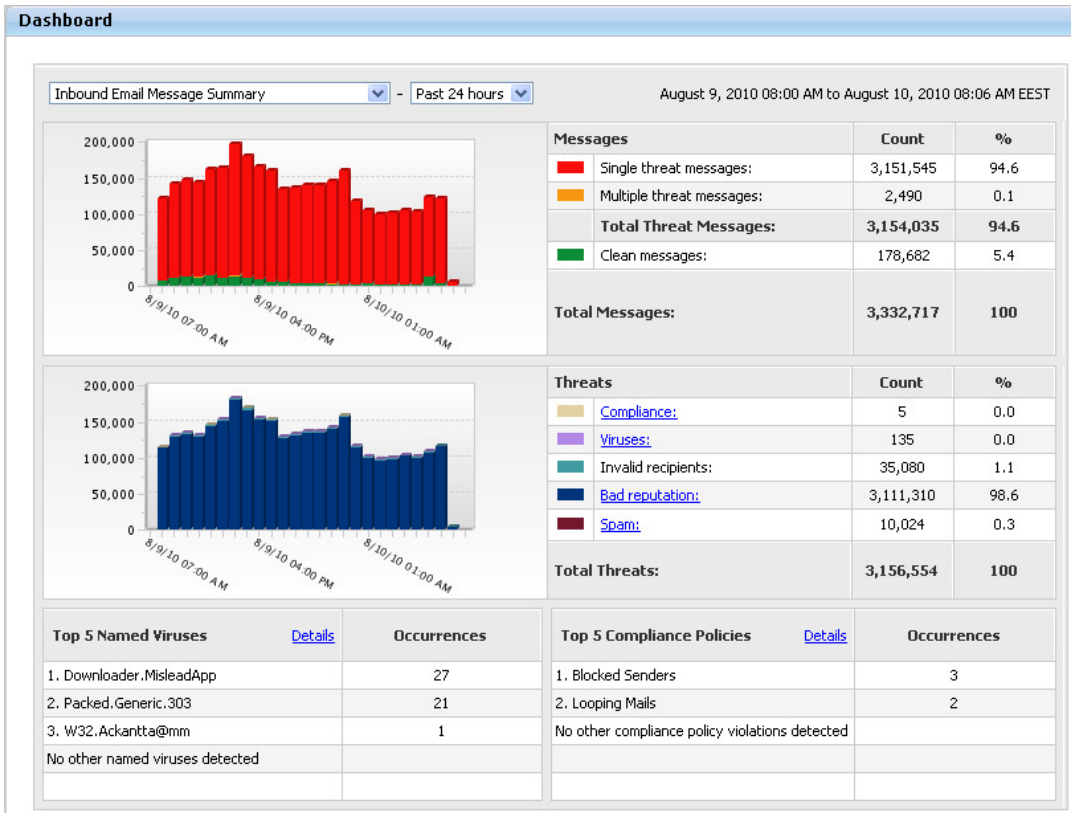
5 SÄHKÖPOSTIN SUODATUS

Viime vuosina sähköpostin käyttö haitallisten ohjelmien sekä massamainonnan levitykseen on lisääntynyt räjähdysmäisesti. Aikaisemmin sähköpostia käyttävän ihmisen ei tarvinnut huolehtia juurikaan siitä, oliko hänen osoitteensa julkisesti verkossa tai jollain julkisella jakelulistalla. Mikäli osoite löytyi julkiselta sivulta, saattoi joutua silloin tällöin jonkun opiskelijan piloillaan lähettämän sähköpostin kohteeksi. Yleensä tällaisen pilan pystyi tunnistamaan oudosta lähettäjä-kentästä, jossa saattoi esiintyä vaikkapa aku.ankka@ankkalinna.fi. Tällaisten väärennetyillä osoitteilla varustettujen viestien vastaanotto ei varsinaisesti muodostanut aikaisemmin sen suurempaa ongelmaa. Nykyisin tilanne on kuitenkin toinen ja huolimattomasti sähköpostiosoitettaan levittelevä käyttäjä saattaakin löytää postilaatikostaan viruksia, matoja sekä roskapostia. Nykypäivänä onkin tavallista, että ennen varsinaista sähköpostipalvelinta, kuten Microsoft Exchange tai IBM Lotus Domino, postin ottaa vastaan palvelin, joka suodattaa postia. Suodatuksessa löydetyt haitalliset viestit siirretään erilliseen karanteeniin, josta käyttäjä voi halutessaan viestin käydä lukemassa.



Kuva 13 Sisään tulevan postin suodatus

Pientä perspektiiviä haitallisten viestien valtaisaan määrään antaa kuva 14. Kuva on peräisin yrityksen omalta postia vastaanottavilta suodatinkoneilta tai oikeammin niiden ohjauskoneelta. Ylhäällä oikealla näkyy sellaisten viestien määrä, jotka sisältävät vain yhden uhan. Uhalla tarkoitetaan tässä tapauksessa viesteissä olevia matoja, viruksia tai mainoksia. Tällaisia viestejä kyseinen suodatinkone oli vastaanottanut vuorokauden aikana 3 156 545 kappaletta. Näiden viestien osuus kaikista vastaanotetuista viesteistä oli 94,6 %. Viestejä, joihin liittyi useampi uhka, oli vastaanotettu 2490 kappaletta. Näiden osuus kaikista viesteistä oli 0,1 %. Vaarattomia viestejä, eli jotka siis sisältävät mitä todennäköisimmin oikean viestin, oli vastaanotettu 178 682 kappaletta. Näiden osuus kaikista viesteistä oli 5,4 %.



Kuva 14 Saapuvan postin suodatus

Hieman alempana oikealla näkyy tietoa, mistä syistä viestejä on hylätty. Ylimpänä listassa näkyy sellaisten viestien määrä, jotka eivät jollain tavalla täytä viestiliikenteelle määritettyjä ehtoja. Seuraavana näkyy niiden viestien määrä, jotka sisälsivät tai joidenka epäiltiin sisältävän viruksen. Virheellisellä vastaanottajalla lähetetyt viestit näkyvät seuraavana. Seuraavana näkyy niiden viestien määrä, jotka on estetty, koska lähettävä sähköpostipalvelin on huonossa maineessa. Tämä tarkoittaa siis sitä, että joku on raportoinut ky-

seisen palvelinten lähettävän viestejä, joissa on haitallista sisältöä. Tämän jälkeen palvelin on lisätty Symantecin ylläpitämälle maailman laajuiselle listalle. Viimeisenä näkyy roskapostia sisältävien viestien määrä. Nämä ovat laitteen oman heuristiikan havaitsemia viestejä. Suurin osa aiemmin mainituista huonomaineisista osoitteista tulevista viesteistä sisältää myös viruksia tai roskapostia, mutta laitteen oman heuristiikan ei tarvitse tutkia niitä. Käyttäjällä ei ole mahdollisuutta vaikuttaa laitteen heuristiikan toimintaan, vaan siitä vastaa Symantec itse.

Lisäksi vasemmassa alakulmassa näkyvät suosituimmat virukset ja niiden esiintymismäärät. Nämä ovat suodatinkoneen itsensä viesteistä löytämiä viruksia. Näihin eivät lukeudu viestit, joissa epäillään olevan viruksia, vaan mukana ovat pelkästään todennetut virukset.

Kuvasta käy selkeästi ilmi, kuinka tärkeää sisään tulevan postin suodattaminen on. Jos kaikki viestit ohjattaisiin suoraan esimerkiksi Microsoft Exchange –sähköpostipalvelimelle, ruuhkautuisi se todennäköisesti erittäin pahasti. Tällöin postit, jotka eivät sisällä haitallista materiaalia, eivät myöskään pääsisi vastaanottajille.

5.1 Virus- ja matosuodatus

Sähköposti on maailmanlaajuisesti käytettävä viestintäväline, jota käytetään valitettavasti myös virusten ja matojen lähetykseen. Ero viruksella ja madolla on se, että mato ei tarvitse ihmisen apua levitäkseen järjestelmästä toiseen, vaan se liikkuu verkossa itsestään. Virus tarvitsee ihmisen apua levitäkseen eteenpäin. Molemmat ovat haitallisia ja saattavat aiheuttaa vakavaa tuhoa järjestelmissä, joissa säilytetään tärkeää tietoa. Jos sähköpostin mukana saapuu jokin kuvatiedostoksi nimetty tiedosto, vaikkapa ’funnypic.exe’, ei tiedostoa tulisi missään nimessä avata ja suorittaa. Muutenkin sähköpostien, joiden otsake-kentässä on jotain epäilyttävää, avaamista kannattaa välttää. Koneelle päästetty viruksen sisältävä sähköposti ei välttämättä tee mitään, ellei käyttäjä avaa usein liitteenä olevaa ohjelmaa ja suorita sitä. Jos käyttäjä ajaa ohjelman, saattaa aluksi näyttää siltä kuin mitään ei olisi tapahtunutkaan. Tämä on kuitenkin täysin suunniteltua ja seuraavalla kerralla kun käyttäjä vaikkapa kirjautuu tietokoneelleen, saattaa osa tiedostoista olla korruptoituneita. Tuolloin niitä ei voi enää avata, ja niiden luomiseen käytetty aika on mennyt hukkaan.

Kuten jo aikaisemmin todettu, sähköpostia voidaan suodattaa pelkästään lähettäjän IP-osoitetta ja lähettäjän toimialueen nimeä vertailemalla. Tämä ei kuitenkaan yksistään riitä, sillä vaikka toimialue olisi oikea ja vastaisi DNS:ssä määriteltyyn IP-osoitteeseen, voi sieltä silti tulla viruksia sisältäviä posteja. Vastaanottavassa päässä olevalla suodatin-palvelimella voidaankin tehdä monenlaista suodatusta. Osa postista voidaan karsia heti alussa pois ja lopuille voidaan tehdä erilainen seula. Matoja ja viruksia suodattavat ohjelmistot perustuvat siihen, että ne käyvät viestissä olevaa tietoa läpi ja etsivät sieltä tietynlaisia koodinpätkiä. Koodinpätkät toimivat ikään kuin sormenjälkinä, jotka suodattava ohjelma tunnistaa.

Suodattava ohjelma voi noutaa uudet virus- ja matotunnisteet esimerkiksi päivittäin tai tunneittain keskitetyltä palvelimelta, joka on ohjelmiston tuottajan ylläpitämä. Näin uudetkin madot ja virukset saadaan suodatettua pois postin joukosta. Suodatusohjelmistoissa saattaa olla integroituna useita eri suodattimia, jotka kukin tutkivat viestejä omalla tavallaan, jolloin saadaan tarkempi kuva siitä, onko viestissä mahdollisesti jotain haitallista.

Suodattavia ohjelmistoja on saatavilla niin ilmaisia kuin maksullisiakin. Microsoft tarjoaa Antigen- ja ForeFront-nimisiä ohjelmistoja, jotka ovat maksullisia. Nämä ovat itse asiassa sama tuote. ForeFront on vain uudempi nimi tuotteelle. Symantec tarjoaa Brightmail tuoteperhettään ja Cisco IronPorttia, jotka ovat molemmat maksullisia. Myös avoimen lähdekoodin sovelluksia löytyy Linuxin päällä ajettaviksi. Näistä tunnetuimpia lienee Clam AV, joka on kehitetty nimenomaan yhdyskäytävä-tyyppisiin sähköpostipalvelimiin. Clam Av on saatavilla kaikille tunnetuille Linux-jakeluille.

Vaikka käytössä olisikin jokin yllämainituista suodatusjärjestelmistä, on silti mahdollista, että mato tai virus pääsee seulasta läpi. Tämä voi johtua monesta eri seikasta kuten siitä, milloin suodattimen tunnisteet on viimeksi päivitetty. Lisäksi viime aikoina ovat lisääntyneet erilaiset asiakaskohtaisesti räätälöidyt haittaohjelmat. Näitä vastaan on hankala suojautua, sillä jokaista hyökättävää tahoa vastaan on omanlaisensa haittaohjelma, jolloin sen havainnointi sormenjälkiin perustuvien järjestelmien avulla on vaikeaa. Niin sanottuja ”False positive” -viestejä, eli viestejä, joiden ei olisi pitänyt päästä läpi, pääsee läpi aina silloin tällöin. Tähän vaivaan auttaa käyttäjien oikeanlainen ohjeistaminen siitä, kuinka sähköpostia tulisi käyttää ja keneen voi luottaa.

5.2 Roskapostisuodatus

Roskaposti on maailmanlaajuinen kiusallinen ilmiö, jonka uhreiksi joutuvat niin yksityiset ihmiset kuin suuret organisaatiotkin. Määrä on kokoajan vain kasvanut eikä kasvulle näy loppua. Joidenkin arvioiden mukaan jopa 90 prosenttia koko maailman sähköpostiliikenteestä on roskaa. [16.] Roskapostin tekee erityisen ilkeäksi se, että normaali käyttäjä, jolla ei ole mahdollisuutta suodattaa postiaan, saattaa saada jopa satoja roskapostiviestejä päivässä. Lisäksi nämä sekoittuvat oikeiden viestien joukkoon. Käyttäjältä kuluu huomattavia määriä aikaa postin suodatukseen, kun hän yrittää erotella, mitkä viestit ovat oikeita ja mitkä roskapostia. Lisäksi roskaposti saattaa pahimmillaan tukkia käyttäjän sähköpostilaatikon. Tällöin oikeat viestit eivät enää mahdu postilaatikkoon. Roskaposti on riesa myös tietoliikenteen kannalta, sillä se on täysin hyödytöntä ja turhaa liikennettä, joka kuitenkin varaa kaistaa itselleen.

Kuten matoja ja viruksia, myös roskapostia voidaan suodattaa monella eri tapaa. Monet sähköpostia vastaanottavat palvelimet kieltäytyvät vastaanottamasta sähköpostia IP-osoitteista, jotka ovat roskapostittajan maineessa. Tämä niin kutsuttu ”Reputation Based Filtering” eli maineeseen perustuva suodatus perustuu eri tahojen ylläpitämiin listoihin palvelimien IP-osoitteista, joista ovat vastaanottaneet roskapostia. Näillä listoilla olevat IP-osoitteet voidaan sitten kirjata ylös sähköpostia vastaanottavalle palvelimelle ja estää näin viestien saapuminen kyseiseltä palvelimelta. Tämä on hyvä keino, mutta valitettavasti se ei riitä kaiken roskapostin suodatukseen sillä osa postista tulee palvelimilta, joiden IP-osoite ei ole tällaisella listalla. Lisäksi roskapostittajat vaihtelevat palvelimiensa IP-osoitteita, mikä hankaloittaa listojen ajan tasalla pitämistä.

Myös roskapostille on olemassa suodatusohjelmistoja, joissa suodatin käy läpi viestin sisältöä ja yrittää löytää sieltä tiettyjä merkkijonoja tai niiden yhdistelmiä. Kun tiettymäärä tunnusmerkkejä täyttyy, voidaan viesti luokitella roskapostiksi, eli spämmiksi. Yleisesti puhutaan Spam Confidence Levelistä, eli SCL:stä. SCL:ssä on eri tasoja, joiden mukaan viesti voidaan luokitella. Tasot ylettyvät nollasta yhdeksään, nollan ollessa spämmitön viesti ja yhdeksän erittäin varmasti spämmiä. Kun viestille on määritelty tietty taso, voidaan se joko poistaa kokonaan tai laittaa karanteeniin. Karanteeniin joutuneista viesteistä voidaan tehdä ilmoitus, jolloin käyttäjä voi halutessaan lu-

kea viestin. Eri tasoille voidaan myös määritellä erilaisia tarkistussääntöjä. Jos viesti vaikuttaa olevan spämmiä, voidaan sille suorittaa lisää toimenpiteitä.

Nämäkään suodattimet eivät kuitenkaan ole erehtymättömiä ja myös roskapostin yhteydessä ilmaantuu välillä aiemmin mainittuja ”False Positive” viestejä. Tämä on kuitenkin normaalia ja loppukäyttäjän kannalta yksi roskapostiviesti kuukaudessa ei aiheuta hurjaa päänvaivaa. On kuitenkin suositeltavaa, että loppukäyttäjiä ohjeistetaan olemaan vastaamatta viesteihin, sillä se ei ainakaan paranna tilannetta, vaan pikemminkin päinvastoin.

Jotkin epärehelliset yritykset ovat löytäneet uuden tavan tehdä rahaa suodatukseen käytettävien mustien listojen avulla. Sähköpostipalvelimet käyttävät oman suodatusälynsä lisäksi erilaisia listoja, joissa on mainittu toimialue nimiä tai IP-osoitteita, joista roskapostia tulee. Osa näiden listojen ylläpitäjistä ei kuitenkaan ole luotettavia tahoja, vaan suoranaisia huijareita. Huijarit ansaitsevat suuria summia rahaa lisäämällä listalleen sattumanvaraisesti jonkin sähköpostia lähettävän palvelimen. Kun palvelin on lisätty listalle, ei sen lähettämiä viestejä enää oteta vastaan niillä palvelimilla, jotka käyttävät suodatukseen kyseistä listaa. Kun ongelmaa aletaan tutkia, huomataan, että yritykseltä vaaditaan suuri summa rahaa listalta pois pääsemiseksi. Epärehelliset listojen ylläpitäjät voivat tällä tavoin kiristää rahaa sähköpostipalvelimia hallinnoivilta yrityksiltä.

6 SÄHKÖPOSTIN UHAT INTERNETISTÄ

6.1 DHA

DHA eli Directory Harvest Attack on roskapostittajien keino hankkia oikeita sähköpostiosoitteita. DHA perustuu SMTP-protokollan mahdollistamaan tapaan erottaa väärät sähköpostiosoitteet oikeista osoitteista. Roskapostittaja hyödyntää tätä ominaisuutta saadakseen selville oikeita osoitteita, joihin roskapostia voi myöhemmin alkaa lähettämään. DHA toimii niin, että roskapostittaja lähettää ensin suuren määrän viestejä mahdollisiin sähköpostiosoitteisiin. Tässä vaiheessa iso osa osoitteista on vääriä. Kun SMTP-yhteys on muodostettu, lähettää roskapostittaja RECIPIENT TO viestin, jossa määritellään vastaanottajan osoite. Vastaanottava palvelin katsoo, tunnistaako se tällaista osoitetta. Mikäli osoitetta ei tunnisteta, lähettää vastaanottava palve-

lin viestin ”mailbox unavailable”, jolloin lähettävä palvelin siirtyy seuraavaan osoitteeseen. Mikäli seuraavan RECIPIENT TO -viestin kohdalla lähettävä palvelin saa kuittaukseksi ”250 recipient ok”, tietää se heti, että kyseessä on oikea osoite, joka todennäköisesti on jonkun käytössä ja johon voidaan lähettää roskapostia. [17.] Osoitteiden löytämisen tehostamiseksi viesteissä käytetään usein yleisiä nimiä ja niiden eri kirjoitusasuja, esimerkiksi visa.hanninen@yritys.com, vhanninen@yritys.com tai hanninen.v@yritys.com. Kun toimiva sähköpostiosoite on löydetty, voidaan helposti päätellä, millaista nimeämiskäytäntöä yrityksessä käytetään sähköpostiosoitteissa.

DHA on selitys siihen, miten uusi sähköpostilaatikko voi saada roskapostia, vaikka osoitetta ei olisi tiedossa edes käyttäjällä itsellään. DHA:lta voi suojautua määrittämällä sähköpostipalvelimelle rajan kuinka monta yhteyttä aikayksikössä sallitaan. Tämä ei poista ongelmaa kokonaan, mutta hidastaa ja hankaloittaa roskapostittajien työtä.

6.2 SMTP VRFY

SMTP-protokolla pitää sisällään VRFY-viestin. VRFY mahdollistaa sähköpostiosoitteen todentamisen SMTP-palvelimella. Kun normaali SMTP-yhteys on muodostettu kahden palvelimen välille, voi lähettävä palvelin kysyä vastaanottavalta palvelimelta, onko jokin tietty osoite olemassa. Tämä tapahtuu lähettämällä esimerkiksi viesti ”VRFY visa”, johon vastaanottava palvelin voi vastata esimerkiksi ”250 visa.hanninen@metropolia.fi”. Jos taas palvelimella ei ole tietoa tällaisesta käyttäjästä, voi se vastata ”553 User ambiguous”. Nykyisin tämä ominaisuus on katsottu turvallisuusriskiksi, joten useat sähköpostipalvelimet eivät tätä toimintoa tue. Aikaisemmin myös tämä on ollut yksi keino roskapostittajille etsiä toimivia sähköpostiosoitteita. [4, s. 7.]

6.3 SMTP EXPN

Aikaisemmin oli myös mahdollista hankkia sähköpostiosoitteita käyttämällä hyväksi SMTP-protokollan EXPN-viestiä. EXPN on komento, jolla jakelulistan pystyy avaamaan ja näkemään näin jakelulistalle kuuluvien henkilöiden sähköpostiosoitteet. Aluksi lähettävä palvelin muodostaa normaalin SMTP-yhteyden vastaanottavaan palvelimeen. Tämän jälkeen lähettäjä voi kysellä EXPN-viestillä, mitä sähköpostiosoitteita kuuluu jollekin tietylle postituslistalle. Tällä tavoin roskapostittajat saavat haltuunsa osoitteita, joihin lähettää

roskapostia. Nykyisin tämä ominaisuus on useista SMTP-palvelinohjelmistoista poistettu juuri väärinkäytön takia. [4, s. 7.]

6.4 Yhteyksien ylikuormitus

Yleinen uhka sähköpostipalvelimille ja varsinkin yhdyskäytäväkoneille ovat purskemaiset viestimassat. Tällaisissa tilanteissa sähköpostia vastaanottava palvelin joutuu valtaisan sähköpostiryöpyn kohteeksi. Näissä tilanteissa postin käsittely yleensä hidastuu tai pahimmassa tapauksessa jumiutuu kokonaan. Tällaisissa tilanteissa roskapostia alkaa ryöpytä jostain IP-osoitteesta todella nopealla tahdilla, jolloin vastaanottava palvelin ei vain pysty käsittelemään alati kasvavaa viestivirtaa.

Ylikuormitusta voidaan kuitenkin hillitä. Yhteysmääriä voidaan rajoittaa niin sanotuilla traffic shaper –laitteilla eli liikenteen muokkaajilla. Liikenteen muokkaaja toimii ikään kuin rajoittimena Internetin ja yrityksen sähköpostijärjestelmien välissä. Liikenteen rajoittimille voidaan määrittää erilaisia tapoja rajoittaa liikennettä. Yksi näistä on rajoittaa tietyistä IP-osoitteista tulevia yhteysmääriä perustuen johonkin listaan. Esimerkiksi Symantec tarjoaa liikenteen rajoittimia perustuen juuri tällaisiin listoihin.

Lisäksi liikenteen rajoittimia voi myös opettaa. Opettamista voidaan hyödyntää tilanteessa, jossa esimerkiksi palomuuri, reititin tai jokin muu verkkolaite havaitsee nopean yhteysmäärän kasvun jostain tietystä IP-osoitteesta. Tämä havaittu IP-osoite voidaan lisätä liikenteen muokkaajan mustalle listalle, jolloin kyseisestä osoitteesta ei hyväksytä yhteyspyyntöjä. Vaihtoehtoisesti osoite voidaan lisätä myös jollekin painotetulle listalle. Tällöin liikennettä kyseisestä osoitteesta ei kokonaan kielletä, vaan rajoitetaan tiettyyn määrään aikayksikössä. Näin liikenteen muokkaaja säästää verkkoresursseja ja auttaa alentamaan yhdyskäytävä-palvelimelle kertyvää kuormaa.

Symantecin Brightmail Traffic Shaper hoitaa liikenteen muokkauksen TCP-tasolla. Tämä tarkoittaa sitä, että jos jokin IP-osoite on joutunut joko Symantecin tai laitteen omalle mustalle listalle, kieltäytyy laite TCP-kättelyistä kyseisen osoitteen kanssa. Samalla tavoin toimitaan myös painotettujen listojen kanssa. Tällöin resursseja säästyy ja oikeaa sähköpostia lähettäville IP-osoitteille voidaan antaa enemmän kaistaa.

7 TYÖN TAVOITTEET

7.1 Raportointi

Yleisesti ottaen käytössä ollut Microsoft IIS tuottaa lokitiedostoissaan tietoa yllin kyllin, eikä kaikkea voida hyödyntää. Osa lokista on kuitenkin erittäin hyödyllistä varsinkin pienen suodatuksen jälkeen. Suodatuksen ansiosta lokia on myös helpompi lukea ja siitä pystyy poimimaan tiettyjä säännön mukaisuuksia. Kun tähän lisätään vielä lokin muuntaminen esimerkiksi Microsoft Excelin ymmärtämään CSV-muotoon, on raportti lähestulkoon valmis. Tätä ratkaisua ei voida pitää itsessään kovinkaan automaattisena. Kuka tahansa voi kuitenkin halutessaan ajastaa esimerkiksi Log Parserin ajamaan tiettyä kyselyä halutuille lokitiedostoille käyttäen käyttöjärjestelmän tarjoamia ajastusominaisuuksia. Tällöin raportti saadaan automaattisesti haluttuun muotoon.

Yritys, jonka kanssa työ tehtiin, on tarjonnut releointi-palvelua asiakkailleen jo useiden vuosien ajan. Palvelusta ei kuitenkaan ole kerätty minkäänlaista statistiikkaa, jota olisi voitu käyttää esimerkiksi laskutusperusteena. Nyt yritys halusi kuitenkin tutkia mahdollisuutta kerätä tietoa välitettyjen viestien määristä sekä Windows Server 2003 –alustalla että uudella Symantec Brightmail Gateway –alustalla. Työn tavoitteena oli siis selvittää, kuinka Microsoftin IIS-ohjelmiston kirjoittamasta lokista saadaan esille tietystä IP-osoitteesta tulevat viestit ja kuinka ne saadaan laskettua yhteen. Saman tuli tietysti onnistua myös uudella Brightmail Gatewayllä.

Työssä oltiin kiinnostuneita myös lähettämättä jääneistä viesteistä ja niiden määristä. Tämä ei kuitenkaan ollut varsinainen tavoite, vaan lähettämättömät viestit haluttiin vain pystyä jäljittämään, mikäli asiakas näin vaatisi. Viestien sisällöstä ei tässä kohtaa oltu kiinnostuneita. Raportoinnissa hyödynnettiin Microsoftin ilmaiseksi tarjoamaa Log Parseria sekä itse tehtyä SQL-tyyppistä kyselyä. Uudessa ympäristössä käytettiin hyväksi Brightmail Gatewayn sisäänrakennettua raportointityökalua. Tavoitteena oli saada aikaiseksi sellaista tietoa asiakkaiden viestimääristä, mitä voitaisiin käyttää myöhemmin mahdollisesti perusteena laskutukselle.

Yksi raportoinnissa esille tulleista asioista oli raportin formaatti. Käyttämällä Log Parseria on mahdollista saada aikaan raportti esimerkiksi graafisessa muodossa tai Microsoft Excelin ymmärtämässä CSV, eli Comma Separated

Value -muodossa. Tässä muodossa raportin eri solut ja niiden arvot on eritelty toisistaan pilkun avulla. Symantec Brightmail Gateway tarjoaa vain omat raporttinsa. Raportit tulevat Control Center eli valvontakoneelta ja valittavana on näyttää raportti joko suoraan ruudulla tai lähettää se sähköpostilla itselleen tai jollekin muulle. Myös Brightmail Gateway tarjoaa erilaisia formaatteja raportteja varten. Brightmail tarjoaa lisäksi mahdollisuuden ajastaa raporttien tuotto ja lähetys. Näin järjestelmästä vastaava henkilö saa halutessaan halutun muotoisen raportin esimerkiksi joka viikko.

7.2 Valvonta

Nykyisin palveluita kuten sähköpostin lähetystä tai laskun maksua verkossa pidetään itsestäänselvyytenä. Niiden myös oletetaan olevan toiminnassa ja käytettävissä ympäri vuorokauden jokaisena vuoden päivänä. Useisiin palveluihin on määritelty niin kutsuttuja palvelusopimuksia, joissa määritellään kuinka monta prosenttia ajasta tuotettu palvelu on oltava käytössä. Jos palvelusopimuksessa on määritelty käytettävyydeksi esimerkiksi 99.999 % tarkoittaa se sitä, että palvelu saa olla pois käytöstä 5 minuuttia ja 15 sekuntia vuodessa tai 25 sekuntia joka kuukausi. Näin korkeaan käytettävyyteen harvoin päästään ilman kokonaan kahdennettua ympäristöä. Jos esimerkiksi tarjotaan asiakkaalle sähköpostipalvelua, on mahdollista tuottaa palvelua useammalla palvelimella. Tällaista ratkaisua kutsutaan usein klusteriksi. Klusterissa voi olla useita samanlaisia palvelimia, jotka tuottavat samaa palvelua. Mikäli yksi palvelimista vikaantuu, voi asiakas jatkaa palvelun käyttöä muilla palvelimilla. Yleensä tällaisesta aiheutuu muutaman sekunnin mittainen katko, jota asiakas ei välttämättä edes huomaa. Klusteri on myös helpompi päivittää kuin yksittäinen palvelin. Yleensä päivityksien asentaminen varsinkin Windows-palvelimeen edellyttää palvelimen uudelleen käynnistystä. Klusterissa palvelimet voidaan päivittää yksi kerrallaan, jolloin palvelua tuotetaan muilta palvelimilta, jotka ovat käynnissä.

Valvonnalla voidaan paitsi havaita jo ilmennyt vika, ja ennakoida tulevia katkoksia ennen kuin ne tapahtuvat. Yleisesti ottaen ihmiset myös hyväksyvät helpommin ennakkoon tiedotetun ongelman kuin täytenä yllätyksenä tulevan. Valvonnalla voidaan ennakoida ongelmia, jotka liittyvät esimerkiksi levytilan käyttöön, suorittimen kuormitukseen tai verkkoon. Valvonnassa olevalta palvelimelta voidaan kerätä tietoa ja ne voidaan tallettaa omaan tietokantaansa. Tietokannassa olevasta tiedosta voidaan muodostaa käsitys siitä,

millainen on vaikkapa palvelimen muistinkäyttö normaaliolosuhteissa. Mikäli normaalista poiketaan toistuvasti, voidaan tehdä päätös hankkia lisää muistia kyseiselle palvelimelle. Näin ennakoimalla voidaan estää palveluiden katkoksia ja pitää asiakas tyytyväisenä.

Laitteiden automatisoidulla valvonnalla on nykyään suuri merkitys. Yritysten konesaleissa on käynnissä tuhansia palvelimia, joten niiden valvonta ilman jonkinlaista valvontaohjelmistoa on käytännössä mahdotonta. Niinpä nykyisin tuotteet kuten BMC Patrol tai muut vastaavat ovat yrityksissä laajassa käytössä. Niiden valvonnan piiriin on liitetty parhaimmillaan kaikki yrityksen palvelimet. Kun valvonta on toteutettu keskitetysti yhdellä järjestelmällä, pysyy sen hallinta tarpeeksi yksinkertaisena. Valvonta voidaan lisäksi integroida muihin järjestelmiin, kuten toiminnanohjausjärjestelmään. Yksinkertaisuudella tarkoitetaan sitä, ettei vastuussa olevien henkilöiden tarvitse käyttää useita eri työkaluja valvontaan, vaan kaikki hoituu yhdellä työkalulla. Lisäksi valvontaohjelmat tarjoavat useimmiten myös hälytyksen lähetys mahdollisuuden joko sähköpostitse tai tekstiviestillä. Jotkin tuotteet saattavat vaatia väliin jonkin toisen laitteen, jotta viestejä voidaan lähettää. Viestien lähetys on huomattava etu, sillä tällöin erillistä valvomoa ei tarvitse pitää miehitettynä, vaan viesti voidaan toimittaa järjestelmästä vastaavan henkilön puhelimeen, vaikka tämä olisi kotonaan.

Releointi-palvelussa käytetyt Windows Server 2003 -palvelimet eivät olleet aiemmin minkään järjestelmän valvonnassa. Näin ollen niihin ei tehty muutoksia. Vanhat palvelimet olivat muutenkin poistumassa uusien virtuaalisten Brightmail Gatewayden tieltä.

Työn alussa valvonta ei ollut käytössä uusilla releointi-palvelimilla. Valvonta haluttiin ulottaa palvelimiin, jotta mahdollisia palvelukatkoksia ei syntyisi ja asiakkaat pysyisivät näin tyytyväisenä. Brightmail Gatewayn tapauksessa valvontaan toi haastetta se seikka, ettei kyseisiin palvelimiin saa asentaa muuta kuin Symantecin itsensä tekemiä ohjelmia. Symantec on rakentanut ohjelmistonsa räätälöidyn Linux-käyttöjärjestelmän päälle, josta on karsittu pois kaikki ylimääräinen. Useat tunnetut komentorivikomennot eivät myöskään toimi rajoitetussa ympäristössä. Laitteet toimivat virtualisoidussa VMware-ympäristössä eli ne eivät ole omia fyysisiä laitteita. Ne tukevat kuitenkin SNMP-rajapintaa, kun sen vain ensiksi kytketään toimintaan. SNMP:n avulla on mahdollista saada paljon tietoa laitteen toiminnasta ja tehdä tarvit-

taessa hälytys. Tavoitteena oli saada laitteen valvonta sellaiselle tasolle, että laitteen vikaantuessa lähtisi siitä automaattisesti hälytys käyttäen BMC Patrol –valvontajärjestelmää. Vikaantumisen merkeiksi määriteltiin liikaa kasvanut viestijono, viestin välityksen loppuminen sekä yhteyden katkeaminen. Yrityksessä BMC Patrol on laajassa käytössä, joten se on järkevin vaihtoehto myös uusien laitteiden valvontaan.

8 RAPORTOINTI

8.1 Raportoitavat asiat

Raportoinnin katsottiin olevan tarpeellinen, mikäli palvelun laskutusta uudistettaisiin. Laskutus perustuu tällä hetkellä kiinteään hintaan. Laskutuksen muuttamista on puoltanut se, että osa palvelun käyttäjistä lähettää yhden tai kaksi viestiä kuukaudessa ja osa satoja, jopa tuhansia, viestejä päivässä. Releointi-palvelun laskutusta ei kuitenkaan muutettaisi kappalehintaiseksi vaan siihen mietittiin jonkin asteista porrastusta. Palvelun hinta voitaisiin siis esimerkiksi määritellä useamman eri portaan avulla. Hinnaston suunnittelu ei kuitenkaan ollut tämän työn aiheena.

Raportoitavia asioita on siis lähetettyjen viestien määrä. Tämä on helposti selvitettävissä vanhemmissa Windows-palvelimissa, sillä IIS tuottaa monipuolista lokia. Lokin voi järjestellä Log Parserilla sellaiseen muotoon, mistä näkee suoraan, kuinka monta viestiä mistäkin toimialueesta on tullut. Myös uudemmista Symantec Brightmail –palvelimista saa raportin, jossa näkyy kuinka monta viestiä mistäkin toimialueesta on lähetetty. Lisäksi Brightmail kertoo, kuinka monta viestiä sisälsi roskapostia tai viruksia. Brightmailin raportointimahdollisuudet ovat suppeammat kuin IIS:n tarjoamat, mutta etuna on helppous. Brightmailille voi kertoa millaista raporttia haluaa ja ajastaa sitten raportin tulemaan vaikka joka viikko tai joka kuun kolmas päivä. Brightmailissa raportointi on nidottu kiinni ohjauskoneen web-hallintaan, eikä varsinaisilta suodatinkoneilta saa minkäänlaista raporttia ulos. Tämä johtuu siitä, että kyseessä on Symantecin rajoittama versio Linuxista, jossa ei haluta ajaa mitään ylimääräistä ohjelmakoodia.

Toisena raportoitavana asiana olivat toimittamattomat viestit. Toimittamattomista viesteistä oli kiinnostuttu palvelun laadun takia. Suurin osa toimittamattomista viesteistä johtuu väärästä osoitteesta. Tätä ei voida pitää muuta

kuin asiakkaan virheenä. Osa sähköposteista jää toimittamatta myös sen takia, ettei kyseiselle toimialueelle löydy MX-tietuetta. Tämäkään ei ole palveluntoimittajasta johtuva asia. Joskus kuitenkin käy niin, että viesti ei syystä tai toisesta vain mene asiakkaalle perille. Näitä tapauksia varten raportointi toimittamattomista viesteistä on hyvä olla olemassa. Kuten lähetettyjen viestien tapauksessa, IIS tarjoaa tietoa myös toimittamattomista viesteistä. Lokia voi järjestää esimerkiksi Log Parserilla ja käyttää sopivaa kyselyä, joka sitten näyttää toimittamatta jääneet viestit. Myös Brightmail osaa generoida raportin toimittamattomista viesteistä ja sen voi myös ajastaa samalla tavoin kuin lähetettyjen viestien raportin.

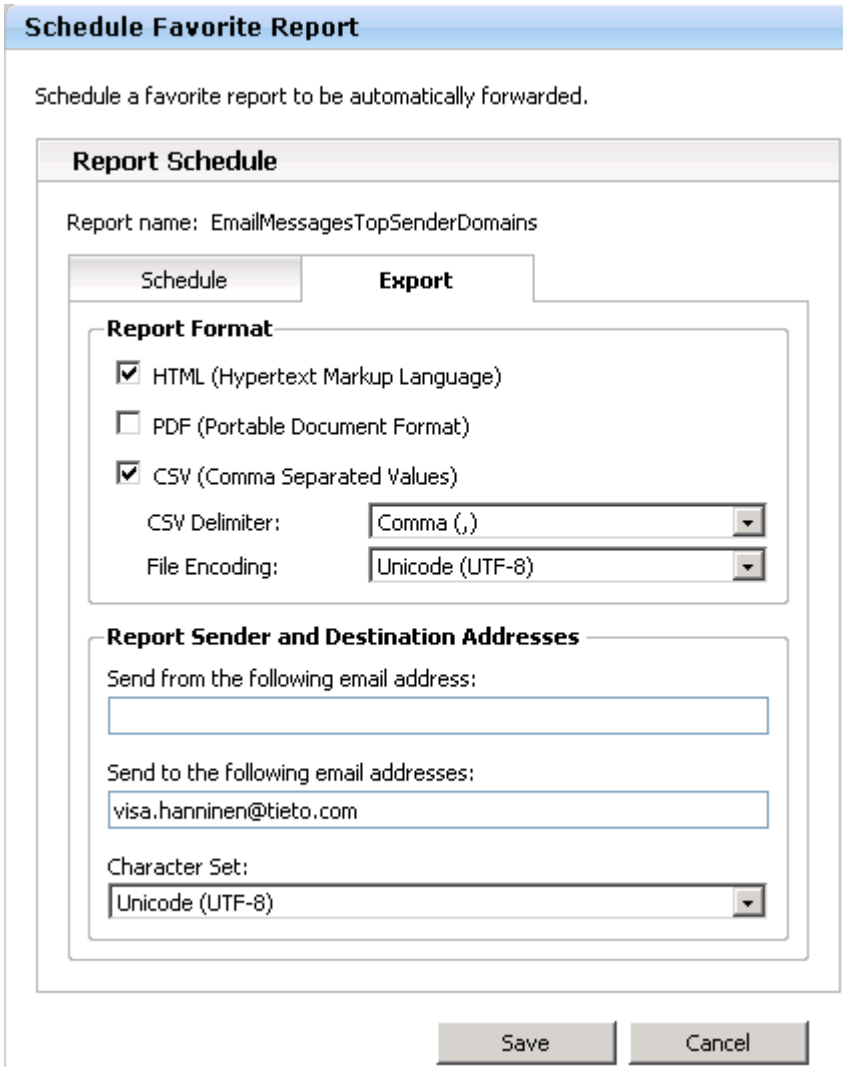
IIS:n tapauksessa raportin saa palvelinkohtaisesti riippuen siitä, minkä SMTP-lokin ottaa käsiteltäväkseen. Brightmailin kanssa asia on hieman erilainen. Käytössä olevat kaksi Brightmail-suodatinkonetta raportoivat yhdelle ohjauskoneelle, jossa on siis käyttöjärjestelmänä sama Symantec Brightmail. Raportteihin, joita ohjauskoneelta noudetaan, tulee kuitenkin automaattisesti mukaan kummankin suodatin koneen tiedot. Tätä ei pysty muuttamaan muuta kuin katkaisemalla yhteyden ohjauskoneen ja suodattimen välillä, mikä ei ole suositeltavaa.

8.2 Raportin muoto

Kuten on aiemmin todettu Microsoftin IIS-palvelimen loki suorastaan pursuaa tietoa. Kaikki tästä tiedosta ei kuitenkaan ole relevanttia raportoinnin kannalta. Käytössä olevilla releointi-palvelimilla oli lisäksi kytketty ”Extended W3C” -lokiformaatti käyttöön, eli loki oli vielä tavallista laajempaa. Myös IIS:n asetuksista oli otettu käyttöön kaikki mahdolliset valinnat. Normaalisti loki on normaalia tekstiä, jossa vilisee osoitteita, smtp-vastauskoodeja, aikaleimoja ynnä muuta. Lisäksi loki on log-tiedostomuodossa. Kun Log Parserilla oli saatu aikaan sopiva kysely, joka tulostaisi vain halutut tiedot, valittiin tulostusformaatiksi CSV. Tämän kaltainen tiedosto on mahdollista tuoda Exceliin ja saada laskettavaan muotoon.

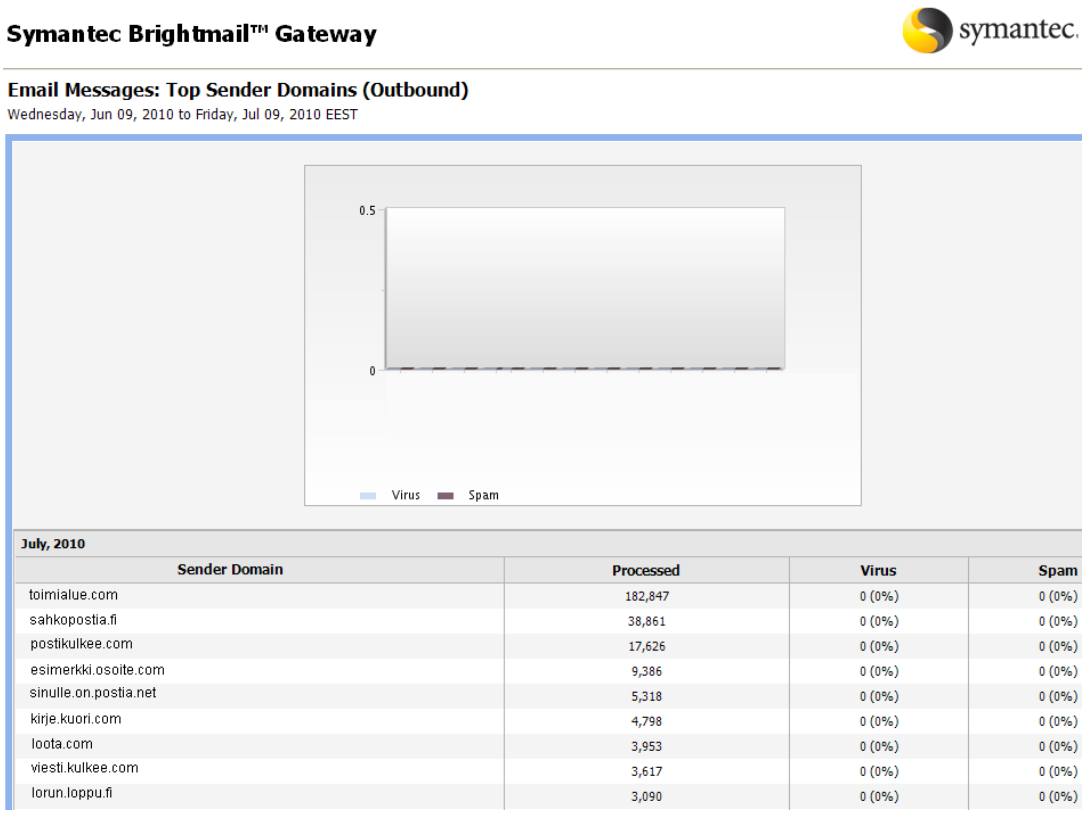
Brightmail tarjoaa myös eri tiedostomuotoja raporteille. Oletuksena se lähettää sähköpostissa raportin, joka sisältää sekä graafisen kuvaajan tilanteesta että html-muotoisen taulukon, jossa on numeerista tietoa. Tämä formaatti sopii osaan raporteista. Mikäli halutaan käyttää raportteja laskutuksen perustana, on helpompaa, jos raportti saadaan tuotua suoraan Exceliin. Onneksi

ajastettujen raporttien alta löytyy myös mahdollisuus käyttää CSV-tiedostoformaattia raportoinnissa. Mikäli laskutusta päädytään uusimaan, helpottaa laskutusta huomattavasti, jos tiedot viestien määristä on valmiiksi Excelin ymmärtämässä muodossa.



Kuva 15 Brightmailin raportin muodon valinta

Raportoinnin avulla voidaan toki kerätä tietoa muuhunkin kuin laskutuksen tarkoituksiin. Näissä tilanteissa on jokin muu kuin pilkulla erotettu muoto varmasti parempi vaihtoehto. Log Parser hallitsee jonkin laisten graafisten kuvaajien piirron. Samaan kykenee myös Brightmail. Graafinen esitystapa on usein epätarkempi mutta myös helpompi lukea kuin esimerkiksi pilkulla erotettu luettelo. Raportin muoto määräytyykin tilanteen mukaan. Kuvassa 16 näkyy raportti, johon on tosin muokattu tekaistut toimialueiden nimet. Normaalisti Sender Domain –kohdassa on mainittu lähettävän toimialueen nimi.



Symantec Brightmail™ Gateway symantec.

Email Messages: Top Sender Domains (Outbound)

Wednesday, Jun 09, 2010 to Friday, Jul 09, 2010 EEST

July, 2010

Sender Domain	Processed	Virus	Spam
toimialue.com	182,847	0 (0%)	0 (0%)
sahkopostia.fi	38,861	0 (0%)	0 (0%)
postikulkee.com	17,626	0 (0%)	0 (0%)
esimerkki.osoite.com	9,386	0 (0%)	0 (0%)
sinulle.on.postia.net	5,318	0 (0%)	0 (0%)
kirje.kuori.com	4,798	0 (0%)	0 (0%)
loota.com	3,953	0 (0%)	0 (0%)
viesti.kulkee.com	3,617	0 (0%)	0 (0%)
lorun.loppu.fi	3,090	0 (0%)	0 (0%)

Kuva 16 Brightmailin tuottama graafinen raportti

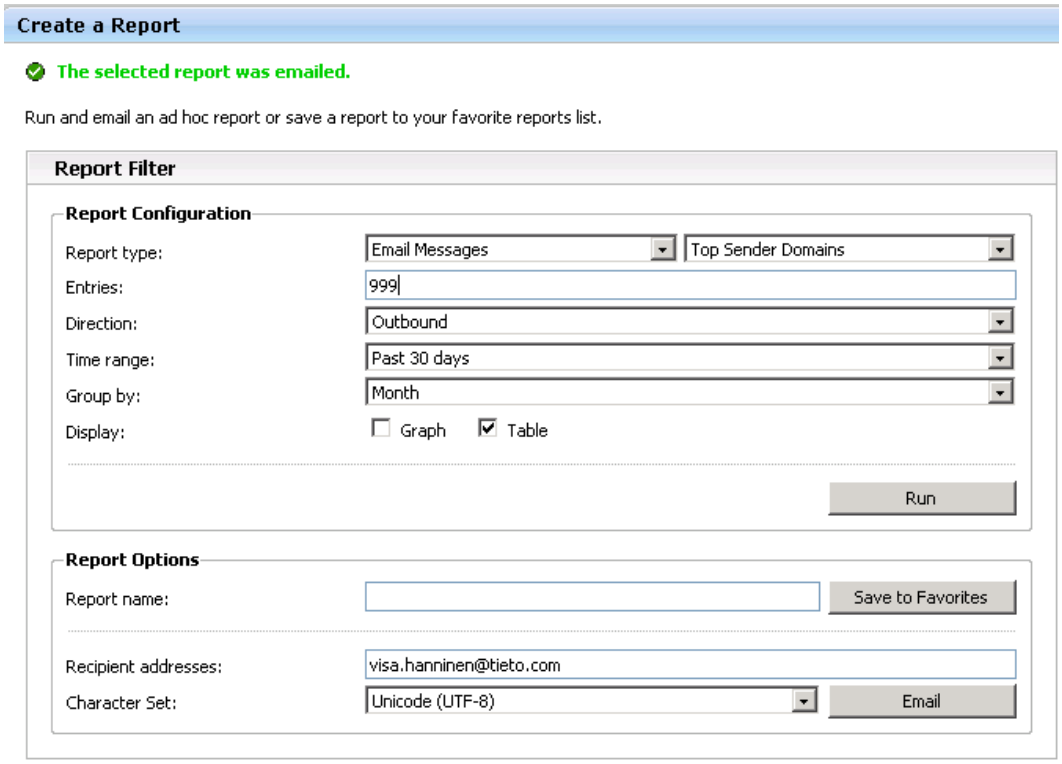
8.3 Raportoinnin ongelmat

Raportoinnissa törmättiin myös ongelmiin. Aluksi IIS:n tuottamista lokeista yritettiin kasata raportteja käyttämällä graafisen käyttöliittymän omaavia ohjelmia. Lokitiedostot ovat kuitenkin kooltaan niin suuria, että jokainen kokeiltu graafinen ilmaisohjelma jumiutui jossain kohtaa. Tällä tavoin raportteja ei siis voitu tuottaa. Myöskään raportoinnin automatisointi ei näillä tuotteilla onnistuisi.

Apu ongelmaan löytyi kuitenkin nopeasti. Microsoftin Log Parser on ilmainen ja tehokas, joskin hieman haastava ohjelma lokien analysointiin. Siinä missä eräs graafisen käyttöliittymän omaava ohjelma käsitteli lokia yli kymmenen minuuttia kaatuen lopulta, selvisi Log Parser alle minuutissa ilman kaatumista. Log Parser vaatii tosin perehtymistä ohjelman käyttämään syntaksiin ennen kuin sillä voi tehdä mitään. Log Parserin käyttäminen varsinaisella tuotannossa olevalla palvelimella ei myöskään ole suotavaa, sillä vaikka käytössä oli moderni kannettava tietokone, sai Log Parser sen polvilleen. Tällöin konetta ei voinut käyttää mihinkään muuhun. Erityisen hankalaksi tilanne meni kun Log Parserille syötettiin koko kuukauden loki. Tällöin edes hiiren

osoittimen liikuttaminen näytöllä ei onnistunut. Heti kun Log Parser oli suorittanut lokin analysoinnin, toimi kone kuitenkin normaalisti. Mikäli samoja tehtäviä olisi suoritettu tuotannossa olevalla palvelimella, jolla on jo ennestään kuormaa, olisi seurauksena saattanut olla sähköposti-liikenteen jumiutumien tai pahimmillaan palvelimen kaatuminen. Periaatteessa ongelmaan on olemassa ratkaisu. Windows Server 2008 tarjoaa ominaisuuden, jolla pitäisi pystyä määrittelemään, kuinka paljon suoritustehoa jollekin yksittäiselle prosessille annetaan. Tällä voitaisiin rajata Log Parserille annettavan suoritustehon määrä siten, että myös muille prosesseille jäisi vapaata suoritustehoa. Tätä ei ollut kuitenkaan mahdollista todentaa käytännössä, sillä releointipalvelimilla oli käytössä Windows Server 2003.

Myös Brightmail aiheutti omanlaisia ongelmia. Kyseessä on siis tuote, jota Symantec tarjoaa ja joka on tarkoitettu pelkästään sähköpostin ja pikaviestien turvallisuuden ylläpitämiseen. Ohjelmisto on tästä syystä koottu rankasti karsitun Linux-järjestelmän päälle. Alla pyörivästä Linuxista on karsittu pois kaikki ylimääräinen. Ongelmaksi muodostui paikka paikoin se, että raportteja voi luoda vain ohjauskoneen kautta. Tällöin raportti luodaan perustuen molempien suodatinkoneiden tietoihin. Lisäksi raporttien kokoa on rajoitettu. Työn tekovaiheessa ei vastaan tullut kuitenkaan tilannetta jossa raportin koko olisi ylittynyt. Maksimirivien määrä html-muotoisessa raportissa on 999 riviä.



Kuva 17 Brightmailin raportointivalikko

8.4 Raportoinnin vaikutukset

Kun raportointia aluksi mietittiin, tuli ensin mieleen pelkästään laskutuksen kehittäminen ja muuttaminen jollain tapaa volyymi-perustaiseksi. Työn edetessä mieleen tuli muitakin asioita, joita raportoinnin avulla voitaisiin kehittää. Yksi tällainen kehitettävä asia on tietoturva ja palomuurit. Jotta sähköposti pääsisi lähettävältä palvelimelta releointi-palvelimelle, täytyy välissä olevat palomuurit avata. Nykyisin kun uusia avauksia tehdään, ei vanhojen käyttämättömien yhteyksien purkamista tapahdu ollenkaan. Raportoinnin avulla olisi mahdollista seurata, mistä IP-osoitteista liikennettä oikeasti tulee. Ne IP-osoitteet, joista sähköpostiliikennettä ei tule, voitaisiin koota yhteen ja niitä varten avatut palomuurien aukot sulkea. Tämä olisi selkeä parannus tietoturvaan.

Lisäksi olisi tietysti hienoa, jos tämänlainen toiminta voitaisiin jollain tapaa automatisoida. Asioilla on tunnetusti paha tapa unohtua. Jos esimerkiksi tämän työn aikana tehtyjä palomuuriavauksia käytäisiin läpi muutaman vuoden kuluttua, olisin yllättynyt, mikäli ne olisivat edelleen käytössä. Toisaalta, avaukset palomuureissa säilyvät, mikäli tällaista automaatioita ei saada kehitettyä. Raportoinnin automatisointi käytettävien yhteyksien suhteen on kuiten-

kin täysin ulkona tämän työn aihealueesta. Toisaalta on mielekästä huomata, mitä kaikkea hyötyä kunnollisesta raportoinnista voidaan saada.

9 VALVONTA

9.1 Valvonnan suunnittelu

Kun valvontaa alettiin suunnitella uusille Symantec Brightmail Gateway –palvelimille, piti aluksi miettiä, mitä kaikkea palvelimista haluttiin valvoa. Kyseessä olevat palvelimet olivat siis virtuaalisia, eli niitä ajettiin virtuaalialustalla. Tästä johtuen palvelimelta ei ollut järkevää valvoa kaikkia MIB:n mahdollisia muuttujia. Brightmail Gatewayn oletuksena tarjoamassa MIB:ssä oli määriteltynä muuttujia, kuten levyohjaimen vikasietoisuus sekä tuulettimien pyörimisnopeus. Näiden muuttujien arvo on jatkuvasti nolla, sillä virtuaalikoneessa ei ole yleensä useita levyohjaimia saati tuulettimia. Tästä johtuen oli mietittävä, mitkä olisivat valvonnan kannalta olennaisia tietoja, joita kannattaisi valvoa.

Pohdinnan jälkeen päädyttiin siihen tilanteeseen, että järkevintä oli selvittää onko palvelimen MTA, joka siis sähköposteja välittää, ylipäätään toiminnassa. Toinen olennainen tieto oli viestien määrä jonossa, sillä sen katsottiin olevan suoraan yhteydessä palvelimen toimintaan. Kun valvottavat asiat oli saatu selville, oli edessä arvojen miettiminen. MTA:n toiminnan kannalta arvoja on oikeastaan vain kaksi. MTA joko toimii tai ei toimi. Tämän pystyy melko luotettavasti toteamaan ottamalla telnet-yhteyden palvelimen porttiin 25. Mikäli palvelin vastaa jotain, joka alkaa ”220 STMP”, on se mitä todennäköisimmin käynnissä, yhteydessä verkkoon ja pystyy toimimaan oikein. Tietoa telnet-yhteydestä kerätään Patrolin tietokantaan, josta oli helppo nähdä, jos palvelin oli jossain vaiheessa kieltäytynyt yhteydestä.

Jonon rajojen määrittely olikin sitten hieman hankalampaa. Oletuksena maksimi toimitusjonon koko oli 150 000 viestiä. [18, s. 101.] Tämä oli kuitenkin liikaa, sillä tässä vaiheessa palvelin todennäköisesti kaatuisi, eikä ongelmaan auttaisi kuin uudelleen käynnistys. Avuksi otettiin tilanne normaalilta ajanhetkeltä ja tilanne, jolloin sähköpostia oli tullut massalähetyksenä jostain osoitteesta. Normaalitilanteessa palvelimella oli jonossa hiukan alle 200 viestiä. Pahin lähiaikoina osunut huippu oli lähes 17 000 viestiä jonossa. Tätä huippua tarkemmin tutkittaessa huomattiin, että se kasvoi nopeasti huip-

puunsa ja ongelman korjaannuttua purkautui myös nopeasti. Kun huippua verrattiin normaalitilanteeseen ja tutkittiin muita päiviä, todettiin, että sopiva varoitusraja olisi 1000 viestiä jonossa. Lisäksi hälytysrajaksi asetettiin 2000 viestiä jonossa.

9.2 Valvontaohjelmisto

Valvonnassa käytettävä ohjelmisto on BMC Patrol Agentless Monitoring. Uusien palvelinten tapauksessa on käytettävä agentitonta valvontaa, joka hyödyntää SNMP:tä ja telnettiä. Normaalissa Windows-palvelinkäytössä palvelimen käyttöjärjestelmään asennettaisiin agentti, joka keräisi tietoa valvottavasta palvelimesta. Agentti lähettäisi sitten keräämänsä tiedot varsinaiselle valvontakoneelle. Brightmail Gatewayn tapauksessa käytössä on agentiton valvonta siitä syystä, että tuote on Symantecin räätälöity Linux-pohjainen käyttöjärjestelmä, johon ei ole lupaa asentaa ulkopuolista ohjelmistoa, kuten Patrol agenttia. Tämä kuitenkaan ei ole ongelma, sillä Symantec on jättänyt mahdollisuuden käyttää SNMP-rajapintaa valvonnan hoitamiseen.

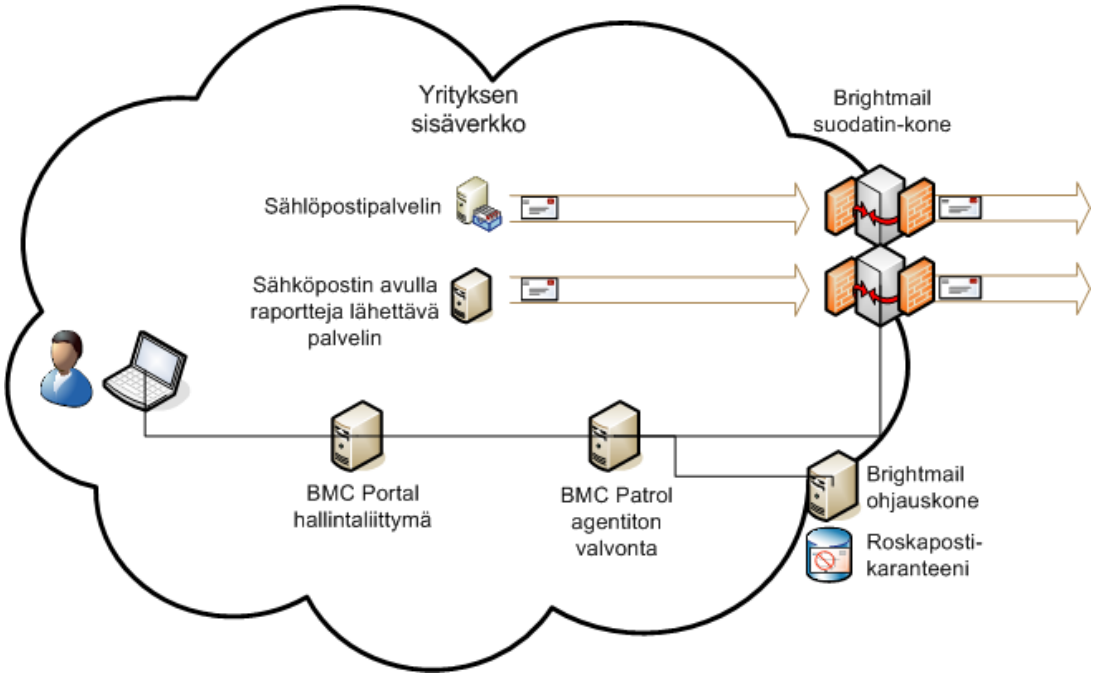
BMC Patrol tarjoaa loputtomalta tuntuvan määrän säätömahdollisuuksia valvonnan hienosäätöön. Esimerkiksi tutkittaessa sitä, vastaako valvottava palvelin telnet-yhteyteen, voidaan itse määrittää, mitä hyväksytään vastaukseksi. Brightmail Gatewayn tapauksessa vastaus telnet-yhteyden avauksessa on muotoa ”220 nimi.domain.com ESMTP Symantec Brightmail Gateway”. Patrol osaa esimerkiksi poimia tästä vastauksesta kirjainyhdistelmän ”SMTP” ja päätellä siitä, että valvottava palvelin vastaa halutulla tavalla. Mikäli valvottava palvelin ei vastaa halutulla tavalla, tulkitsee valvontajärjestelmä jonkin olevan pielessä. Jos valvontajärjestelmä ei lukisi vastausta valvottavalta palvelimelta, saattaisi käydä niin, että vaikka yhteys palvelimeen olisi kunnossa, ei palvelin silti olisi toimintakuntoinen. Tällöin valvontajärjestelmä ei epäilisi virhettä, eikä myöskään tekisi hälytystä. Tästä syystä onkin tärkeää, että valvontajärjestelmä todella lukee, mitä valvottava palvelin sille vastaa.

Lisäksi SNMP-rajapinnan kautta tapahtuvaa valvontaa on myös mahdollista virittää tahtonsa mukaan. Valvonta perustuu Brightmailin MIB:iin, josta on valittu joukko arvoja, joita laitteelta luetaan. Kaikkia arvoja ei kuitenkaan lueta, koska ne eivät tarjoa hyödyllistä tietoa. Patrol-valvontapalvelin tallentaa keräämänsä tiedot tietokantaan ja laskee niistä keskiarvoa, jota voi käyttää vertailukohtana arvoja tutkiessa. Tämänkin takia on järkevää lopettaa nolla-

tiedon kerääminen, sillä turha tieto kertyy tietokantaan ja kasvattaa kannan kokoa turhaa.

9.3 Suodatinkone

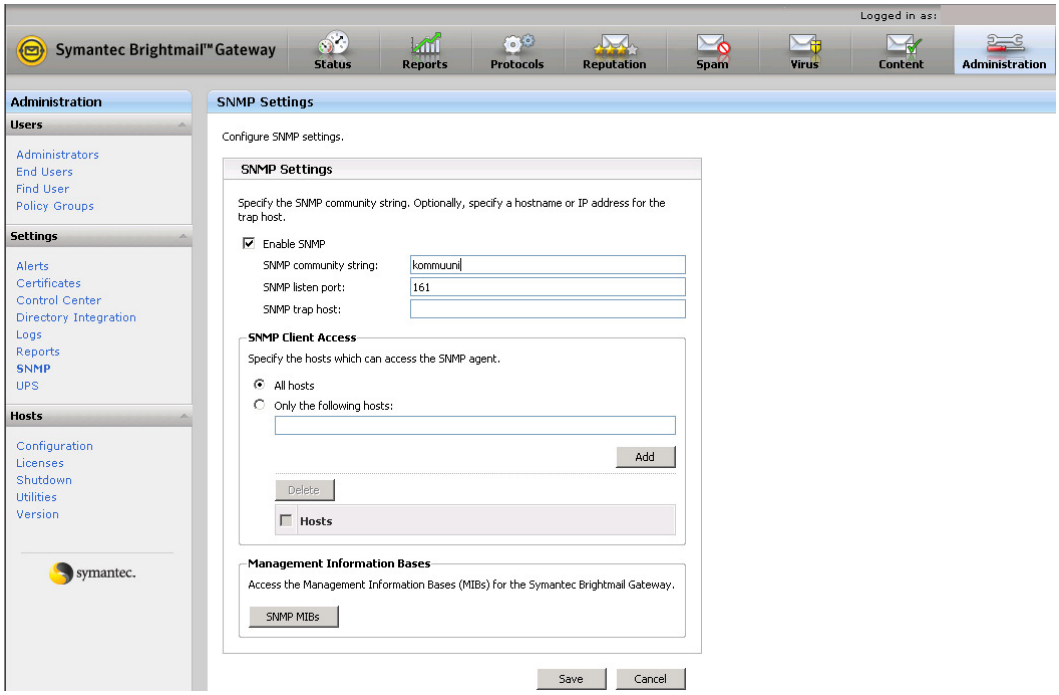
Valvonnan tavoitteena oli siis ulottaa yrityksessä laajassa käytössä oleva BMC Patrol -valvontaohjelmisto valvomaan myös uusia Brightmail-palvelimia. Valvonta toteutettiin käyttämällä SNMP-rajapintaa, joka on vaihtoehto Patrol-agentille. Valvontaa varten oli aluksi tehtävä palomuurien avauspyynnöt, jotta yhteys valvontakoneen ja valvottavien koneiden välillä olisi auki. Palomuureista pyydettiin avattavaksi portit TCP/25 sekä UDP/161. TCP-portin 25 kautta oli tarkoitus valvoa, vastaako Brightmail telnettiin, eli onko se kykenevä hyväksymään SMTP-yhteyksiä viestejä lähettäviltä sähköpostipalvelimilta. UDP-potin 161 kautta oli puolestaan tarkoitus valvoa jonon kokoa SNMP-protokollaa käyttämällä.



Kuva 18 BMC Patrol valvonnan rakenne

Palomuuriavausten jälkeen oli seuraavana vuorossa SNMP-protokollan aktivointi Brightmail-palvelimilta. Tämä tapahtuu ohjauskoneen web-hallinnasta Administration-valikosta. SNMP:tä varten pitää sopia SNMP Community String, jota käytetään ikään kuin salasanana hallinta-aseman ja hallittavan laitteen välillä. Lisäksi samasta valikosta on mahdollisuus rajoittaa SNMP-yhteyksiä sallituiksi vain tietyistä IP-osoitteista. Samasta valikosta pääsee lisäksi lataamaan laitteen MIB:in työasemalleen. Tämä on tärkeää, sillä

SNMP-valvontaohjelmisto tarvitsee MIB:in, jotta se osaa valvoa oikeita asioita valvottavasta laitteesta.

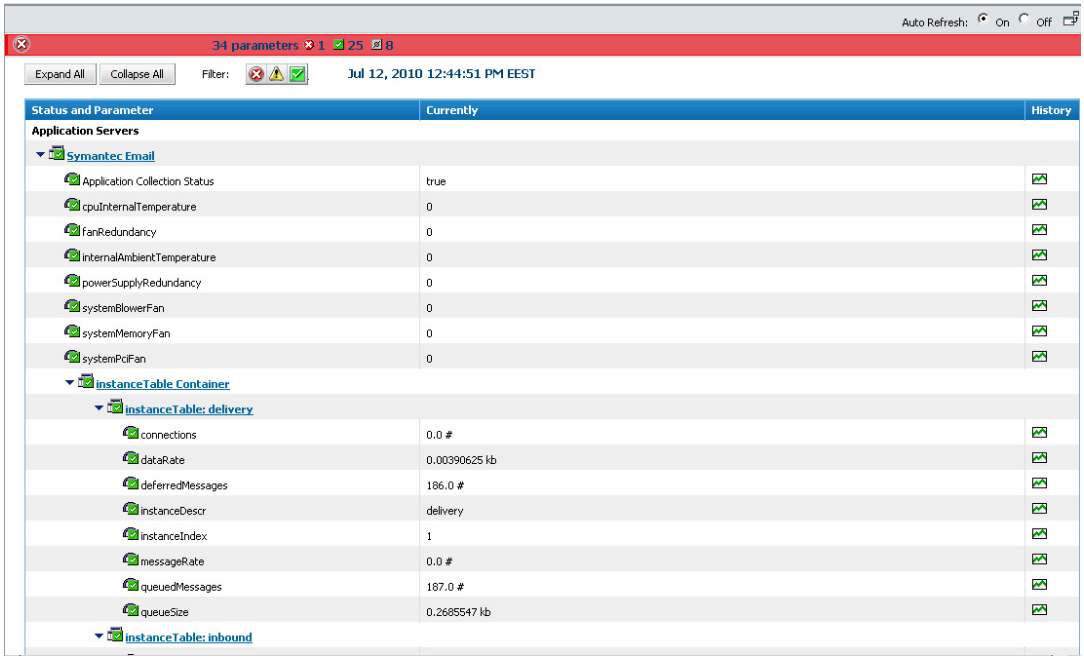


Kuva 19 Brightmailin SNMP-asetussivu

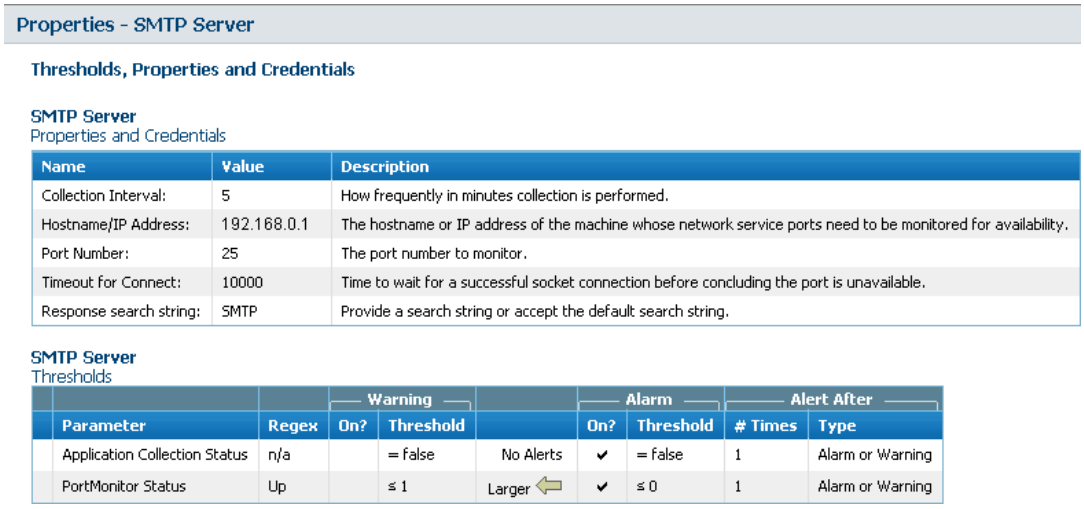
Kun Brightmail oli saatu kuntoon, oli aika siirtyä Patrolin kimppuun. Patrolista oli siis käytössä agentiton valvonta eli valvontaan käytetään palvelinta, josta on SNMP- sekä telnet-yhteys valvottavaan palvelimeen. Patrolin valvonta perustuu siihen, että valvontakoneelle on kerrottu, mihin osoitteisiin sen tulee yrittää telnet-yhteyttä. Lisäksi kerrotaan mihin osoitteisiin yritetään SNMP-yhteyttä. Yrityksessä on releointi käytössä kolme Symantec Brightmail Gateway –palvelinta. Kaksi näistä on varsinaisia suodattimia, joiden läpi sähköposti kulkee. Yksi kone on pelkästään kahden suodattimen ohjaukseen käytettävä kone. Ohjauskoneen tehtäviä on muun muassa huolehtia virustietojen päivityksestä, käyttöjärjestelmän versiopäivityksistä sekä roskaposti karanteenista. Molemmilta suodatinkoneilta käydään kysymässä viestijonon kokoa viiden minuutin välein, joka tallennetaan Patrolin tietokantaan. Lisäksi suodatinkoneille yritetään telnet-yhteyttä viiden minuutin välein. Kuvista 20 ja 21 on näkymä sekä erilaisista valvottavista muuttujista että porttien valvonnasta.

Suodatinkoneiden kanssa tuli kuitenkin ongelma telnet-kyselyiden kanssa. Vakio asetuksilla Brightmail ei nimittäin hyväksy tuntemattomista IP-osoitteista tulevia yhteyspyyntöjä porttiin 25. Telnet-yhteyteen saatiin vasta-

ukseksi vain ”554 <unknown[ip-osoite]>”. Tämä ongelma saatiin kuitenkin korjattua, kun agentittoman valvonnan palvelimien IP-osoitteet lisättiin sallittujen IP-osoitteiden listalle Brightmailin ohjauskoneessa. Lisäksi valittiin ”Apply above settings to all scanners”, jolloin tieto sallituista osoitteista levittyi automaattisesti molemmille suodatinkoneille.



Kuva 20 BMC Patrol valvottavat muuttujat



Kuva 21 Patrolin porttien valvontamääritykset

9.4 Ohjauskone

Koska ohjauskone ei välitä sähköpostia ollenkaan, ei siltä kannata myöskään kysellä jonon kokoa. Samasta syystä johtuen ei myöskään ole järkevää yrittää telnettiä ohjauskoneen porttiin 25. Ohjauskoneen valvonta hoidettiin

muulla tavoin. Brightmailin omat MIB:t keskittyvät hyvin pitkälle kuvailemaan arvoja, jotka löytyvät fyysisistä laitteista. Näistä ei kuitenkaan ole hyötyä, sillä ohjauskone pyörii myös virtuaalialustalla. Ohjauskoneelta piti siis saada esille jotain, joka kertoisi, onko se toiminnassa.

Ongelmaan löytyi ratkaisu Brightmailin karanteenin käyttämästä portista. Uusissa versioissa Brightmailin viestikaranteeni sijaitsee ohjauskoneella. Kun suodatinkone haluaa siirtää viestin karanteeniin, avaa se SMTP-yhteyden ohjauskoneeseen ja siirtää viestin sinne. Tätä toimintoa varten ohjauskone kuuntelee TCP-porttia 41025. Kun porttiin 41025 otettiin yhteys telnettiä käyttäen, huomattiin, että se vastaa ”220 SMTP receive ready”. Tämä vastaus määriteltiin BMC Portaliin hyväksytyksi vastaukseksi. Lisäksi Portal asetettiin ottamaan yhteyttä viiden minuutin välein. Näin myös ohjauskone saatiin liitettyä valvonnan piiriin. Tässä vaiheessa oli kuitenkin tehtävä uusi palomuurien avaus TCP-portille 41025, sillä alkuperäinen avaus koski vain TCP/25- ja UDP/161-portteja.

Toinen mahdollisuus ohjauskoneen, ja miksei myös suodatinkoneiden, valvontaan olisi ollut VMware-alustan kautta tapahtuva valvonta. VMware tarjoaa mahdollisuuden valvoa sen sisällä ajettavien virtuaali-käyttöjärjestelmien suorituskyky arvoja. Tämä tarkoittaa sitä, että esimerkiksi Brightmailin vapaana olevan keskusmuistin määrää voisi valvoa VMvaren kautta. Lisäksi valvonnan voisi kytkeä BMC Patrol–järjestelmään niin, että tietyn varatun muistimäärän ylityttyä aiheesta lähtisi hälytys. VMwaren tapauksessa käytössä oleva ESXi-versio olisi kuitenkin mahdollisesti jouduttu päivittämään johonkin toiseen versioon, sillä i-malli on maksuton, eikä sisällä kaikkia ominaisuuksia joita maksullisista versioista löytyy. Tästä syystä Patrolin agentiton valvonta tuntui järkevämmältä vaihtoehdolta valvontaan, koska siitä ei aiheutunut minkäänlaisia lisäkuluja.

10 LOPPUPÄÄTELMÄT

10.1 Tavoitteisiin pääseminen

Työn alussa asetettuihin tavoitteisiin päästiin sekä raportoinnin että valvonnan osalta. Tavoitteet katsottiin täyttyneiksi raportoinnin osalta, sillä uudesta releointi-käyttöön tarkoitetusta Symantec Brightmail Gateway –laitteesta saatiin ajastettuja raportteja viestien välitysmääristä. Lisäksi raportit saatiin

vielä helposti Excelillä käsiteltävään muotoon. Myös valvonta saatiin toteutettua, vaikka Symantec oli estänyt ohjelmiston asennuksen laitteeseen. Valvonta toimi kuitenkin hyvin SNMP-rajapinnan ylitse, ja hälytykset saatiin lähtemään, mikäli jono kasvoi viestejä välittävillä laitteilla liian suureksi tai telnet-yhteys ei onnistunut. Myös ohjauskone saatiin valvonnan piiriin, vaikka sen kanssa olikin aluksi vaikeuksia.

10.2 Työssä kohdatut ongelmat

Alusta asti oli selvää, että kaikki ei välttämättä toimisi suoraan, vaan osaan asioista menisi enemmän aikaa. Kaikki kuitenkin saatiin toimimaan, jopa yllättävän helposti. Osa ongelmista, kuten Brightmailin raportin suppeus, ovat sellaisia, joihin ei ollut mahdollista vaikuttaa millään tavoin. Näihin asioihin saattaa joskus tulla korjaus, mikäli Symantec katsoo sen tarpeelliseksi. Lisäksi valvontaa toteutettaessa oli jossain kohtaa tyydyttävä siihen, mitä oli saatavilla. Omista ideoista oli vain jossain kohtaa luovuttava ja hoidettava asiat käytössä olevilla työkaluilla niin hyvin kuin mahdollista. Tätä voi kuitenkin mielestäni pitää sekä hyvänä että huonona asiana. Mikäli käytössä olisi ollut rajattomat mahdollisuudet tehdä asioita, kuinka haluaa, olisi se toki ollut mukavaa ja tulokset olisivat saattaneet olla myös erilaiset. Kuitenkin tilanne, jossa käytettävissä on vain tietyt työkalut jonkin asian hoitamiseen, opettaa hyödyntämään näitä työkaluja eri tavoin. Tekijä on tyytyväinen, että pääsi työskentelemään näin suljettujen laitteiden kanssa, sillä niiden kanssa joutuu opettelemaan uusia tapoja tehdä asioita.

Työn edetessä vastaan tuli kuitenkin sellaisia ongelmia, joita alussa ei tullut miettineeksi ollenkaan. Ongelmat liittyivät suurelta osin tietoliikenteeseen, sekä työskentelyyn suuressa yrityksessä. Koulussa tehdyissä projekteissa oli tottunut siihen, että mitä enemmän itse tekee töitä, sitä nopeammin saa työn valmiiksi. Yritysmaailmassa joutui kuitenkin totuttelemaan siihen, että jos teet työtä ahkerasti, joudut jossain vaiheessa odottelemaan, sillä muut eivät välttämättä saa muilta osin asioita valmiiksi yhtä nopeasti. En tarkoita sitä, että muut olisivat hitaita, vaan sitä, että asiat etenevät portaittain eivätkä lineaarisesti. Jokainen porras vaatii oman aikansa, joten yhden ihmisen on hankala nopeuttaa muun kuin oman portaansa suoritusta. Suuressa yrityksessä on myös enemmän portaita kuin pienessä, eli tehtävät jakautuvat väkisinkin laajalle. Tämä puolestaan hidastuttaa työn valmistumista. Työ kuitenkin saatiin tehtyä aikataulun puitteissa, joka on jo jonkinlainen saavutus.

10.3 Jatkotoimenpiteet

Työn varsinainen idea oli tutkia releointi-palvelun raportointia ja valvontaa. Lisäksi oli tarkoitus saada uudet releointi-palvelimet automaattisen valvonnan piiriin. Työn loppuvaiheessa raportointi toimii automaattisesti ja valvonta on myös automatisoitu yrityksessä käytössä olevan BMC Patrol-järjestelmän kanssa. Kuitenkaan raportointi ei itsessään tuota vielä mitään hyötyä. Jonkun pitää ottaa asiakseen mahdollinen laskutuksen uusiminen ja käyttämättömien yhteyksien sulkeminen. Tämä työ on oikeastaan vain ensimmäinen askel pitkässä ketjussa.

Sen sijaan valvonnasta saadaan hyötyä heti. Vaikkakaan kyseessä ei ole mikään erityisen kriittinen järjestelmä, on silti hyödyllistä tietää kuinka paljon viestejä on jonossa ja toimiiko palvelu ylipäätänsä ollenkaan. Näistä asioista on suoraan hyötyä ilman sen suurempaa jalostamista. Valvonnassa on kuitenkin otettava huomioon ohjeistus. Hälytyksistä ja varoituksista ei ole valvojalle hyötyä, ellei hän tiedä kuinka toimia sellaiseen törmätessään. Oikeanlaisen ohjeistuksen avulla hän tietää mitä tehdä tällaisessa tilanteessa. Näin voidaan vaikuttaa palvelun alhaalla oloaikaan ja asiakkaiden tyytyväisyyteen.

Joitain asioita jää siis tehtäväksi vielä tämän työn jälkeenkin. Näitä asioita on kuitenkin hankalaa ulottaa tämän työn yhteyteen, sillä yrityksillä on kaikilla omat toimintatapansa näissä asioissa. Mikäli tällaisia toimintatapoja olisi alettu käsittelemään yksityiskohtaisesti, olisi se saattanut johtaa siihen, että osa työstä olisi jouduttu julistamaan salaiseksi. Näin ollen onkin järkevämpää vain tiedostaa asiat yleisellä tasolla, joka ei ole millään tavalla salaista tietoa.

10.4 Omat mielipiteet

Olen on tyytyväinen lopputulokseen ja siihen, millainen työstä tuli. Alusta asti oltiin sitä mieltä, että on hyvä asia, jos työtä tai osaa siitä ei tarvitse julistaa salaiseksi. Koulussa törmättiin muutamaan työhön, joista iso osa oli julistettu salaiseksi. Näistä töistä olisi todennäköisesti tuolloin saanut paljon hyvää materiaalia esitelmään sekä oppinut asioita, jotka olivat ennestään vieraita. Salaiseksi julistamisen takia näin ei kuitenkaan käynyt. Tämä työ palvelee

hyvin myös tulevia opiskelijoita. Se on yleinen kuvaus sähköpostin releointipalvelun toiminnasta ja siinä esitellään myös muita sähköpostin kannalta olennaisia asioita. Lisäksi raportointia on esitelty eri tavoilla, eikä vain yhdellä. Myös valvonta on toteutettu tavalla, joka on useissa tilanteissa mahdollinen. Työ tarjoaa hyvää materiaalia asiasta kiinnostuneelle. Työ oli myös erittäin opettavainen tekijän kannalta. Tällä hetkellä tekijän tietämys aiheesta on huomattavasti suurempi kuin työn alkuvaiheessa.

VIITELUETTELO

[1] Socolofsky, T - Kale, C, RFC1180 A TCP/IP tutorial [verkkodokumennti, viitattu 4.6.2010]. Saatavissa: http://www.faqs.org/rfcs/rfc1180.html.

[2] RFC793 Transmission Control Protocol [verkkodokumentti, viitattu 4.6.2010].Saatavissa: http://tools.ietf.org/html/rfc793.

[3] RFC768 User Datagram Protocol [verkkodokumentti, viitattu 5.6.2010]. Saatavissa: http://tools.ietf.org/html/rfc768.

[4] Postel, Jonathan B, RFC821 Simple Mail Transfer Protocol [verkkodokumentti, viitattu 5.6.2010]. Saatavissa: http://tools.ietf.org/html/rfc821.

[5] Tschabitscher, Heinz, SMTP Inside Out, About.com Guide [verkkodokumentti, viitattu 6.6.2010]. Saatavissa: http://email.about.com/cs/standards/a/smtp.htm.

[6] Tschabitscher, Heinz, What Email Headers Can Tell You About the Origin of Spam [verkkodokumentti, viitattu 6.6.2010]. Saatavissa: http://email.about.com/cs/spamgeneral/a/spam_headers.htm.

[7] Reverse MX [verkkodokumentti, viitattu 6.6.2010]. Saatavissa: http://en.citizendium.org/wiki/Reverse_MX.

[8] Haikonen, Jarno - Hlinovsky, Jan - Paju, Antti, Verkonhallinta SNMP [verkkodokumentti, viitattu 7.6.2010]. Saatavissa: http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/47/snmp.shtml.

[9] Rose, M – McCloghrie, K, RFC1155 Structure and Identification of Management Information for TCP/IP-based Internets [verkkodokumentti, viitattu 7.6.2010]. Saatavissa: http://tools.ietf.org/html/rfc1155.

[10] Froom, Richard - Sivasubramanian, Balaji - Frahim, Erum, Implementing Cisco Switched Networks (SWITCH), IN 46240, Indianapolis, Cisco Press 2010.

[11] SNMP, MIBs and OIDs - an Overview [verkkodokumentti, viitattu 7.6.2010]. Saatavissa: http://www.paessler.com/support/kb/questions/49.

[12] An introductory guide to SNMP, [verkkodokumentti, viitattu 7.6.2010]. Saatavissa: http://www.industrialnetworking.co.uk/mag/v9-6/f_snmp.html.

[13] Pretty Good Privacy [verkkodokumentti, viitattu 10.6.2010]. Saatavissa: http://en.wikipedia.org/wiki/Pretty_Good_Privacy.

[14] RFC2633 S/MIME Version 3 Message Specification [verkkodokumentti, viitattu 10.6.2010]. Saatavissa: http://tools.ietf.org/html/rfc2633.

[15] STARTTLS [verkkodokumentti, viitattu 11.6.2010]. Saatavissa: http://en.wikipedia.org/wiki/STARTTLS.

[16] Linja-aho, Vesa, Vaarallisen roskapostin määrä räjähti käsiin: 3 miljardia viestiä – päivässä [verkkodokumentti, viitattu 9.8.2010]. Saatavissa: http://www.mikropc.net/kaikki_uutiset/article375826.ece.

[17] Burdick, William, Directory Harvest Attack [verkkodokumentti, viitattu 20.7.2010].Saatavissa: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci970104,00.html.

[18] Symantec Corporation, Symantec Brightmail™ Gateway 9.0 Administration Guide, Mountain View, CA 94043.