TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikka
Tietoliikennetekniikka

Tutkintotyö

Juho Kulmala

Linux SME ja Smoothwall pk-yritysten palvelin- ja palomuuriratkaisuna Windows-ympäristössä

Työn ohjaaja Ilkka Tervaoja
Työn teettäjä Hippinet, valvojana Kimmo Hippi
Tampere 2008

TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikka
Tietoliikennetekniikka
Kulmala, Juho Linux SME ja Smoothwall pk-yritysten palvelin- ja palomuuriratkaisuna Windows-ympäristössä

Tutkintotyö 54 sivua + 16 liitesivua
Työn ohjaaja Ilkka Tervaoja
Työn teettäjä Hippinet, Kimmo Hippi
Kesäkuu 2008
Hakusanat Linux, Linux SME, Smoothwall, Samba, palomuuri, qmail

TIIVISTELMÄ

Pk-yritysten tietoliikenneverkon suunnitteleminen ja toteuttaminen saattaa usein kasvaa kokonaiskustannuksiltaan todella mittavaksi. Tämä pystytään todentamaan, jos it-kuluja verrataan yrityksen vuosittaiseen liikevaihtoon tai katteeseen. Osasyy isoille kuluille löytyy ohjelmistolisensseistä ja hintavista laitteistoista. Laitteistot vanhentuvat nopeasti ja tietoliikennejärjestelmä vaatii jatkuvaa ylläpitoa. Näiden asioiden johdosta vapaaseen lähdekoodiin perustuvat ohjelmat ovat alkaneet kiinnostaa monia yrityksiä. Silti monilla on vielä erittäin varautuneita käsityksiä ilmaisia ohjelmia kohtaan, eikä niiden käyttöön uskalleta siirtyä. Tosiasiassa esim. Windows-palvelimen vaihto Linux-palvelimeen ei ole mikään ongelma ja kokonaiskustannuksia pystytään karsimaan tuntuvasti. Linux-palvelimia käytettäessä ylläpitopalvelut siirtyvät yleensä täysin palvelimen toimittajalle, eli erillistä ohjelmistotukea ei ole saatavilla samalla tavalla kuin Windows-palvelimelle. Huomattavaa on, että kummankin palvelinratkaisun kohdalla vaaditaan kuitenkin aina it-asiantuntijan apua, kun ongelmatilanne palvelinjärjestelmässä syntyy.

Tämän työn tarkoituksena on luoda toimiva ja joustava tietoliikennejärjestelmä pk-yritysten käyttöön. Tietoliikennejärjestelmän suunnittelemisessa ja toteuttamisessa vaaditaan lähes aina verkkolaitteiden lisäksi palvelinratkaisu sekä palomuuri. Molemmat voidaan toteuttaa erittäin kustannustehokkaasti käyttämällä vapaan lähdekoodin ohjelmia.

Linux SME -palvelin on hyvä ja keskitetty ratkaisu niin tiedosto-, sähköposti- kuin web-palvelimeksikin. Sen asennus ja konfigurointi ei ole liian monimutkaista. Oleellisimmat käskyt ja komennot on nopeasti opittavissa eikä järjestelmä vaadi palvelinohjelmiston osalta jatkuvaa ylläpitoa. Ylläpito ja ohjelmistoasennukset ovat myös helposti suoritettavissa ulkoverkosta käsin etäyhteyden kautta.

Smoothwall-palomuuri taas tuo palomuuritoimintojen lisäksi myös paljon muita hyödyllisiä ominaisuuksia. Smoothwall sisältää tehokkaan sisältösuotimen sekä roskapostisuotimen. Palomuurin perustehtävä on estää ulkoverkosta tuleva haitallinen verkkoliikenne. Smoothwall pystyy estämään myös haitalliset virukset, roskapostit sekä erilaiset mainosohjelmat, ennen kuin ne edes pääsevät yrityksen sisäverkkoon. Tämän lisäksi Smoothwall ei vaadi kovin tehokasta laitteistokokoonpanoa.

TAMPERE UNIVERSITY OF APPLIED SCIENCES
Computer science
Telecommunications Engineering
Kulmala, Juho

	Linux SME and Smoothwall as the server / firewall solution in Small and Medium-Sized Enterprises in Windows environment
Thesis	54 pages + 16 appendices
Thesis Supervisor	Ilkka Tervaoja
Commission Company	Hippinet, Kimmo Hippi
June 2008	
Keywords	Linux, Linux SME, Server, Firewall, Samba, Smoothwall

ABSTRACT

The total costs of designing a data communications network for a Small or Medium-sized Enterprise may often prove to be very steep. This can be verified by comparing the amount of IT costs to the annual turnover or contribution margin. Reasons for the high total costs can be found e.g. in the prices of software licences as well as hardware costs. It does not take too long for hardware to get out-dated and in addition, the data communications system requires constant maintenance. Consequently, it is not surprising that various open source software alternatives have become more popular. That said, many enterprises are still suspicious of freely distributed software as an alternative to commercial software. Objectively, replacing a Windows server with an open source Linux based alternative is not such great an effort and is likely to reduce total costs considerably. One of the weaknesses of Linux based systems is the lack of official support services. This obstacle can be mitigated by acquiring the services of third-party professionals that are usually needed with Windows servers also, when problems arise.

The purpose of this report is to create a functional and flexible data communications system to be used in Small and Medium-sized Enterprises. Designing and implementing such a system requires various pieces of network hardware and most importantly, a server solution that includes a firewall. This task can be carried out very cost-efficiently by using open source software.

The Linux SME server software is a good, centralized solution that can be used e.g. as a file server, mail server and as a web server. Installing and configuring Linux SME is quite straightforward and basic commands are easy to use. In addition, the server software does not require constant maintenance. The ability to perform maintenance duties and software installations through remote access adds ease of use.

Smoothwall is an open source firewall solution, which in addition to conventional firewall capabilities, also contains many other useful features. The most basic task of a firewall is to prevent harmful incoming connections. In addiotion, Smoothwall contains effective and efficient content and spam filtering capabilities that prevent viruses, spam and other harmful content from reaching the private network. Smoothwall is also fairly flexible concerning hardware requirements.

SISÄLLYSLUETTELO

LIITTEET

LYHENTEET JA MERKIT

SMTP	Simple Mail Transfer Protocol, TCP-pohjainen protokolla, jota käytetään sähköpostiviestien välittämiseen lähettäjän postiohjelmasta postipalvelimen kautta vastaanottajan postipalvelimelle.
SSH	Secure Shell, tarkoitettu turvalliseen tiedonsiirtoon.
HTTP	Hypertext Transfer Protocol, protokolla, jota selaimet ja webpalvelimet käyttävät tiedonsiirtoon.
HTTPs	Hypertext Transfer Protocol secure, HTTP:n turvallisempi versio.
IMAP	Internet Message Access Protocol, sähköpostien lukemiseen tarkoitettu protokolla.
IMAPs	Internet Message Access Protocol secure, IMAP:n turvallisempi versio.
POP3	Post Office Protocol version 3, sähköpostin hakemiseen tarkoitettu protokolla.
POP3s	Post Office Protocol version 3 secure, POP3:n turvallisempi versio.
PPTP	Point-to-Point Tunneling Protocol, VPN-tunnelointiprotokolla.
FTP	File Transfer Protocol, TCP-protokollaa käyttävä tiedostonsiirtomenetelmä.
RAID	Redundant Array of Independent Disks eli tekniikka, jolla tietokoneiden vikasietoisuutta ja nopeutta kasvatetaan käyttämällä useita erillisiä kiintolevyjä.
NAT	Network Address Transformation, osoitteenmuunnostekniikka.
PAT	Port Address Transformation, porttimuunnostekniikka.
TCP	Transmission Control Protocol, kuljetuskerroksen protokolla, jolla luodaan yhteyksiä tietokoneiden välille ja luodaan tiedonsiirrosta luotettavaa.
UDP	User Datagram Protocol, kuljetuskerroksen protokolla, jolla luodaan myös yhteyksiä tietokoneiden välille, mutta paketin perille menoa ei varmisteta päästä päähän.

1 Johdanto

Nykyään yhä useampi pieni ja keskisuuri yritys on siirtymässä keskitettyihin palvelinratkaisuihin. Kun yritys alkaa laajentua, on hyvä olla jo valmiiksi sellainen tietoliikennejärjestelmä, joka on tarpeeksi joustava ja joka pysyy tarpeiden mukaisella tasolla. Varsinkin yrityksen alkuvaiheilla ovat kustannustekijät todella ratkaisevat, sillä Windows-palvelimen lisenssi maksaa töineen ison summan. Myös hallittavat kytkimet ja reitittimet virtuaali-lan-ratkaisuineen maksavat paljon. Nämä tekijät pienentävät tuntuvasti yritysten kynnystä siirtyä vapaan lähdekoodin ohjelmistoihin. Linux-pohjaisissa palvelinratkaisuissa, kuten esimerkiksi SME:ssä on todella hyvät ominaisuudet sekä keskitetyt palvelut, jolloin Windows-palvelimelle ei välttämättä ole mitään tarvetta. On silti todettava, että jotkin ominaisuudet, kuten esimerkiksi Windowsin active director ja siihen liittyvät käyttäjäkohtaiset hallinnointimenetelmät pitävät Windows-palvelimen edelleen suosittuna palvelinratkaisuna. Linux-palvelimien puolesta puhuu taas niiden tehokkuus, vaatimaton laitteiston suorituskyvyn tarve sekä huomioitavan hyvä luotettavuus. Myös tietoturvaa voi pitää Linux-järjestelmissä hyvänä, koska esimerkiksi suurin osa viruksista tehdään Windows-ohjelmistoille.

Tulen esittämään tässä työssäni, miten ja millä tavalla yritys pystyy hyödyntämään SME-palvelinta ja Smoothwall-palomuuria omassa tietoliikennejärjestelmässään. Tuon myös esille asioita yrityksen sekä ylläpitäjän näkökulmasta ja pyrin luomaan sellaisen palvelin- ja palomuuriratkaisun, joka on integroitavissa niin pieniin kuin keskisuuriinkin yrityksiin. Otan esille myös vaihtoehtoisia ratkaisumalleja, koska moni asia ja tapa eivät sovellu jokaiseen ympäristöön samalla tavala. Työn alussa tuon esille myös itse toteutusta tukevaa teoriaa, jotta tietyt seikat toteutuksesta olisi helppo ymmärtää. Toteutus osion viimeisessä kappaleessa on esitetty yksi esimerkkiratkaisu koko tietoliikennejärjestelmän kustannuslaskelmasta. Samassa kappaleessa on myös eriteltynä koko projektiin kuluva aika.

2 Linux-järjestelmät

Ennen kuin siirrytään käyttämään Linux-pohjaista palvelin -ja palomuuriratkaisua, on hyvä selvittää itselle muutamia perusasioita, jotka liittyvät yleisesti kaikkiin Linux-järjestelmiin. Kaikissa Linux-järjestelmissä tietyt asiat ovat hyvin samankaltaisia, esimerkiksi laitenimet, hakemistorakenne ja tiedostojärjestelmä. Moni asia on toteutettu hyvin eri tavalla verrattuna perinteisiin Windows-pohjaisiin järjestelmiin, joten näihin asioihin on hyvä perehtyä etukäteen.

2.1 Linux-järjestelmien laitenimet

Linuxissa eri laitteita kutsutaan laitenimillä. IDE-kiintolevyt nimetään Linuxissa siten, että ensimmäinen levy on /dev/hda, toinen levy /dev/hdb, kolmas levy /dev/hdc jne. Nimeäminen ja kovalevyjen järjestys menee siis aakkosten mukaan. Eli jos tehdään Linuxin asennus ensimmäiseen IDE-kiintolevyyn, niin sen laitenimi on tällöin /dev/hda. Tyypillinen piirre kaikissa Linux-järjestelmissä on se, että laitteet täytyy ensin liittää järjestelmään, ennen kuin ne ovat käytettävissä. Linuxissa kaikki laitetiedostot ovat /dev-hakemistossa. Esimerkiksi haluttaessa liittää ja irrottaa levykeasema tapahtuu se seuraavasti: /1/

```
mount /dev/fd0          ; Levykeaseman liitos
umount /dev/fd0         ; Levykeaseman irrotus
```

Laitteet on myös mahdollista saada käyttövalmiuteen jo käynnistyksen yhteydessä, jolloin erillistä mount-komentoa ei tarvita. Käynnistyksen yhteydessä liitettävät laitteet ovat /etc/fstap-tiedostossa, ja ne laitteet, joissa on defaults eli oletus päällä, liitetään automaattisesti./1/

Windowsissa eri kovalevyosioiden nimeäminen tapahtuu niin, että ensimmäinen asema on c, toinen d ja kolmas e jne. Linuxissa taas kovalevyn eri osioiden nimeäminen tapahtuu numeroidusti tyyliin hda1, hda2, hda3 jne. Nimeämiskäytäntö Linuxissa on joka tapauksessa selkeämpi kuin Windowsissa, koska esimerkiksi ensimmäisen kiintolevyn osi-

on lisääminen tai poistaminen ei vaikuta muiden levyjen asematunnuksiin. Toinen Linux-järjestelmien huomattava etu on niiden joustava hakemistorakenne. Käyttöjärjestelmä voidaan hajauttaa usealle eri osiolle tai jopa kokonaan eri levyille. Tämä asia tulee ilmi Linux SME-palvelimen asennuksen yhteydessä myöhemmin. /1/

IDE-väyläiset CD-asemat näkyvät Linuxissa samoin kuin kiintolevytkin. Yleensä CD-asema on toisessa IDE-väylässä kiinni Master-moodissa (ensisijaisena), jolloin sen laitenimi Linuxissa on /dev/hdc. Samassa kaapelissa oleva toinen asema on tällöin Slave-moodissa (toissijaisena), ja sen laitenimi on hdd. Huomioitavaa on kuitenkin se, että polttava CD-asema näkyy Linuxissa SCSI-laitteena, esim. /dev/scd0. Käytännössä lähes kaikki CD-ja DVD-asemat näkyvät Linuxissa nykyään SCSI-laitteina, koska niissä on poltto-ominaisuus jo integroituna. Aseman vaihto SCSI-laitteeksi tapahtuu käynnistyslataajan parametreilla, esimerkiksi ’hdc=ide-scsi’. Nykyisissä uusissa Linuxin 2.6-sarjan ja siitä ylöspäin olevissa ytimissä tätä vaihtoa ei enää tarvitse suorittaa, ja SCSI-laitteet nimetään vastaavasti /dev/sda, /dev/sdb, /dev/sdc jne. /1/

SCSI-laitteiden kanssa joutuu olemaan todella tarkkana, koska esimerkiksi uudet Serial-Ata-kovalevyt luokitellaan myös tähän ryhmään /3/. Linuxin kernelissä on myös ohjelmistopohjainen RAID-toteutus eli md (multidisk). RAID, eli Redundant Array of Inexpensive Disks, on tekniikka, joka mahdollistaan sen, että useita kiintolevyjä voidaan järjestää näkymään käyttöjärjestelmälle yhtenä levynä. Tällöin tämä ”yksi” levy on isompi, nopeampi ja myös huomattavasti luotettavampi kuin sen muodostavat osat /5/. Linux ja varsinkin Linux-palvelimet tukevat useita erilaisia RAID-laitteita /5/. RAID-toteutus on mahdollista tehdä ohjelmistopohjaisesti tai laitteistopohjaisesti. Tästä kerrotaan tarkemmin Linuxin SME-palvelimen asennuksen yhteydessä. RAID-paikkoja ohjelmistopohjaisessa asennuksessa vastaavat /dev/mdx-laitteet, jotka käyttäytyvät kuten normaalitkin levyasemat /4/.

Pakolliset kovalevyosiot Linuxissa ovat /- eli ns. juuriosio (root) ja swap-osio. Erillistä boot-osiota ei tarvita, jos asennetaan erillinen käynnistyslataaja (Lilo tai Grup) MBR:ään. MBR on lyhenne sanoista Master Boot Record, joka tarkoittaa pääkäynnistyslohkoa. Swap-osio on varattu ns. lisämuistia varten, eli jos tietokoneen fyysinen Ram-muisti ei riitä, käyttää Linux tätä kovalevystä varaamaansa tilaa hyödyksi. Swap-osiota voisi ver-

rata Windowsin käyttämään näennäismuistiin. Swap-osion koko määräytyy RAM-muistin määrän mukaan, ja yleensä sen koko on 2 kertaa RAM-muistin määrä, mutta esimerkiksi Linux-pohjaisessa Smoothwall-palomuurissa swap-osion koko vastaa oletusarvoisesti RAM-muistin määrää. /1/

2.2 Linuxin hakemistorakenne

Linuxin hakemistorakenteen perustana on Filesystem Hierarchy Standard (FHS). Taulukossa 1 on esitelty kaikki hakemistot ja symboliset linkit eri hakemistoihin, joiden täytyy FHS-standardin mukaan sijaita juurihakemistossa. Standardi koskee kaikkia Linux-käyttöjärjestelmiä. /2/

Taulukko 1 Linuxin FSH-standardin mukaiset hakemistot. /2/

Hakemisto	Kuvaus
bin	Välttämättömät komentobinäärit kaikille käyttäjille
boot	Käynnistyslataimen pysyvät tiedostot
dev	Laitetiedostot
etc	Systeemin konfigurointitiedostot
lib	Välttämättömät jaetut kirjastot ja kernelin moduulit
media	Liitospiste siirrettävälle medialle
mnt	Liitospiste tiedostojärjestelmän väliaikaiseen liittämiseen
opt	Lisäsovellusten ohjelmapaketit
sbin	Välttämättömät järjestelmäbinäärit root-käyttäjälle
srv	Järjestelmän palvelujen tuottama data
tmp	Väliaikaistiedostot
usr	Toiseksi tärkein hakemistopuu juurihakemiston jälkeen
var	Muuttuva data

2.3 Linuxin tiedostojärjestelmä

Linuxin tiedostojärjestelmä poikkeaa oleellisesti Windowsin tiedostojärjestelmästä. Ensinnäkin Linuxissa on tiedostojärjestelmälle enemmän vaihtoehtoja. Yhtenevää Linuxin

tiedostojärjestelmissä on kuitenkin se, että koko tiedostojärjestelmä koostuu liitettävistä laitteista. Laitteina voivat olla eri laitetiedostot, hakemistot tai tiedostot sekä myös kokonaiset osiot. Linuxin ydin eli kernel näkee kaiken tiedostoina. Esimerkiksi DVD-asema on vain laitetiedosto, joka otetaan käyttöön ajurin avulla. Linuxin ytimen kannalta voidaan puhua pelkästään eri suhteessa toisiinsa olevista tiedostoista tai hierarkkisesta tiedostojärjestelmästä. Joka tapauksessa jokainen lohkolaite, esimerkiksi kiintolevy, vaatii erikseen tiedostojärjestelmän luonnin, ennen kuin sitä on mahdollista käyttää. Käytännössä tiedostojärjestelmän luonti tarkoittaa sitä, että levy täytyy ensin alustaa ja tehdä sille kirjanpito sekä kirjoittaa datan rakenne levyn omaan MBR:ään.

Windowsissa tiedostojärjestelmänä käytetään NTFS:ää tai vanhempaa FAT32:sta. Nykyään Linuxissa tiedostojärjestelmänä on käytössä joku seuraavista: ext3, JFS, XFS tai ReiserFS. Nämä järjestelmät ovat korvanneet vanhan ext2-tiedostojärjestelmän. Yleensä on järkevää ottaa se tiedostojärjestelmä käyttöön, joka on asennuksen yhteydessä suosituksena. Usein Linuxin asennuksen yhteydessä tiedostojärjestelmä luodaan automaattisesti, mutta toisin kuin Windowsissa, se on myöhemmin mahdollista muuttaa toiseen ilman kovalevyn osion formatoimista. /1/

3 Palvelinympäristö

Palvelinta asennettaessa yrityksen palvelinympäristöön on myös ymmärrettävä asioita, jotka eivät ole täysin riippuvaisia palvelimesta itsestään. Reitittävät laitteet, Internet-yhteyden tarjoaja ISP ja käytettävät verkkoprotokolat luovat kaikki edellytykset palvelimen toiminnalle. Samalla kun nämä asiat luovat edellytykset, niin joissain tapauksissa ne luovat myös tiettyjen palvelujen rajat. Esimerkiksi käytettävän Internet-yhteyden kaista ulkoverkkoon luo rajat niille palveluille, joita palvelin ohjaa ulkoverkkoon. Sisäverkossa rajoja taas luovat sisäverkon suunniteltu maksiminopeus sekä verkon muuttuva kuorma. Reitittävissä laitteissa on myös oltava oikeanlaiset asetukset mm. eri porttiohjauksille ja eri protokolille, jotta palveluiden välittäminen eri tahoille onnituisi. Seuraavissa kappaleissa esitetään yksityiskohtaisemmin kaikki oleellisimmat asiat, jotka pääsääntöisesti liittyvät palvelimen ulkopuolisiin seikkoihin. Tässä vaiheessa on hyvä ottaa myös esille se, että otan kantaa ainoastaan ethernet-tekniikalla toteutettuihin verkkoihin.

3.1 NAT ja PAT

NAT eli Network Address Translation on 1996/97 kehitetty tekniikka, jonka tarkoituksena oli vähentää IPv4-osoitteiden kulutusta. Ennen sen kehittämistä jokaisella Internetiin kytketyllä koneella oli oltava oma julkinen IP-osoite. /9/

NAT:n avulla reititin, palomuuri tai esimerkiksi reitittävä ADSL-modeemi voi saada kaikki sen takaa sisäverkosta ulospäin Internetiin otetut yhteydet näkymään reitittimen omalla IP-osoitteella. Tämä reitittimen oma IP-osoite on siis se julkinen IP-osoite, jonka reititin saa suoraan palveluntarjoalta ja jolla ollaan yhteydessä ulkoverkkoon. Useimmissa tapauksissa julkisia IP-osoitteita on vain yksi. NAT:n avulla kaikki sisäverkon liikenne ulkoverkkoon ohjataan tämän yhden osoitteen kautta ulkoverkkoon. Tällöin sisäverkon koneilla voi olla mikä tahansa lähiverkon IP-osoite käytössä, kunhan se kuuluu harmaan sarjan osoiteavaruuteen. Lähiverkon IP-osoite ei vaikuta millään lailla Internet-liikenteeseen. /9/

Käytännössä, kun paketti tulee NAT-tekniikkaa käyttävän verkon sisäpuolelta Internetiin päin olevaan reitittimeen, vaihtaa reititin siihen oman julkisen IP-osoitteensa sisäverkon koneen IP-osoitteen tilalle. Vastaavasti reititin vaihtaa verkkonsa sisäpuolelle tulevien pakettien osoitteet julkisesta koneiden yksityisiin. Näin sisäverkon ulkopuolella olevat koneet eivät voi tietää pakettien tulevan useammalta kuin yhdeltä koneelta.

Kuten edellä tuli mainittua, niin NAT-tekniikkaa käyttävän sisäverkon koneiden IP-osoitteiksi ei voi valita aivan mitä tahansa. Jos esimerkiksi yhden koneen osoitteeksi asetettaisiin julkinen IP-osoite 207.46.19.190, mikä on www.microsoft.com:n IP-osoite, niin sisäverkosta ei enää Microsoftin sivuille pääsisi, koska kaikki pyynnöt ohjautuisivat sille sisäverkon koneelle, jolle tämä osoite on asetettu. Tästä syystä IANA on kehittänyt RFC 1918 -standardin, jossa määritellään sisäverkoissa sallitut IP-osoiteavaruudet. Nämä osoitteet eivät voi olla käytössä Internetin puolella, ja niitä kutsutaan harmaan sarjan IP-osoitteiksi. Harmaan sarjan osoitteiksi luokitellaan seuraavat osoittealueet: /9/

10.0.0.0	-	10.255.255.255	(luokka A)	/9/
172.16.0.0	-	172.31.255.255	(luokka B)	/9/
192.168.0.0	-	192.168.255.255	(luokka C)	/9/

Osoitteen muunnos voidaan suorittaa neljällä eri tavalla. Ensinnäkin voidaan tehdä staattinen osoitteen muunnos, jolloin reitittimelle on konfiguroitu tietty määrä IP-osoitteita, jotka vastaavat tiettyä määrää sisäverkossa käytettyjä osoitteita. Tällöin sisäverkon ja ulkoverkon osoitteilla voisi olla taulukon 2 kaltainen yhteys. /10/

Taulukko 2. Esimerkki staattisesta osoitemuunnoksesta. /10/

Sisäverkon osoite	Ulkoverkon osoite
192.168.1.1	193.65.76.1
192.168.1.2	193.65.76.2
…	
192.168.2.1	193.76.77.1

Dynaamisessa osoitteen muunnoksessa sisäverkosta voi tulla ulkoverkkoon kerralla yhteyksiä myös tietty rajattu määrä, mutta sisäverkon osoitteiden määrä voi olla suurempikin. /10/

PAT-tekniikassa eli porttimuunnoksessa on reitittimelle konfiguroitu myös tietty rajattu määrä IP-osoitteita. Näihin IP-osoitteisiin on liitettynä tiettyjä portteja, joita käytetään yksittäisille yhteyksille sitä mukaa, kun tarvetta syntyy. Jokaisella IP-osoitteella on 65 535 tähän tarkoitukseen käytettävää porttia, joten on mahdollista, että jokaista julkista IP-osoitetta kohti voi olla auki lähes yhtä monta yhteyttä. Ainoastaan yhden julkisen IP-osoitteen takaa voidaan liikennöidä tuhansia koneita. Käytännössä porttimuunnos voisi näyttää taulukon 3 kaltaiselta. /10/

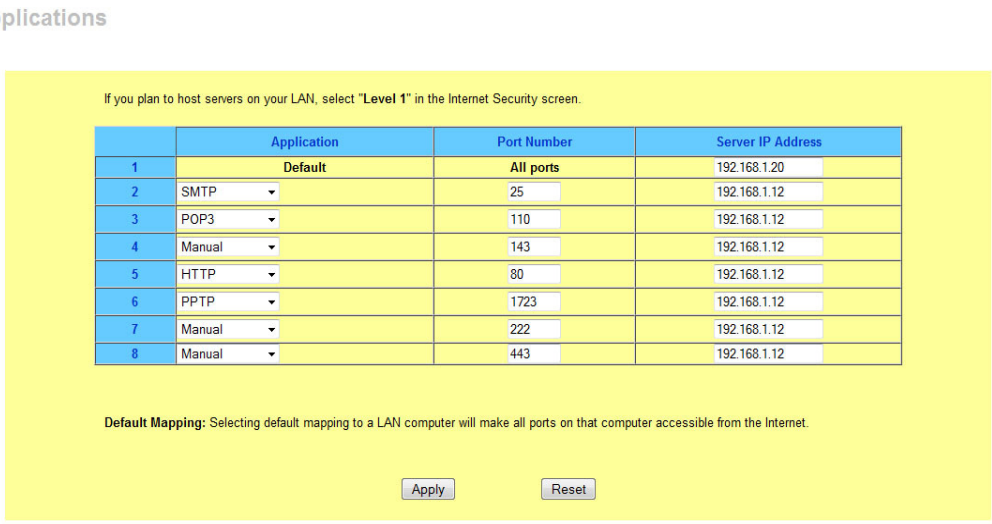
Taulukko 3. Esimerkki porttimuunnoksesta /10/

Sisäverkon osoite	sisäverkon portti	ulkoverkon osoite	ulkoverkon portti
192.168.1.1	1111	193.65.76.1	1025
192.168.1.1	1112	193.65.76.1	1026
192.168.1.2	2001	193.65.76.1	1027
192.168.1.1	1113	193.65.76.1	1028

Lisäksi voidaan käyttää käänteistä osoitteenmuunnosta. Tällöin osoitteen muunnosta ei tehdä ulospäin lähtevien yhteyksien lähdeosoitteille, vaan päinvastoin sisäänpäin tulevien yhteyksien kohdeosoitteille. Käänteistä osoitteenmuunnosta käytetään useimmiten kuormanjaon tekemiseen, eli yhdelle IP-osoitteelle sisään tulevien yhteyksien jakamiseen vaikkapa neljän sisäverkon palvelimen kesken /10/.

3.2 Palvelimen tarvitsemat porttiohjaukset

Palvelin tarvitsee tietyt porttiohjaukset monille palveluille ja toiminnoille, joita se ohjaa suoraan ulkoverkkoon sekä vastaanottaa suoraan ulkoverkosta. On olemassa lukuisia eri palveluja ja ohjelmia, jotka toimiakseen vaativat lukuisien porttien olevan auki. Kuvassa 1 on esitettynä yksi esimerkkiratkaisu tarvittavista porttiohjauksista.



Kuva 1. Esimerkkiratkaisu palvelimen porttiohjauksista

Kuva 1 on otettu Zyxelin Prestige-sarjan laajakaistamodeemista. Kuvassa kaikki tarvittavat portit on ohjattu suoraan palvelimen IP-osoitteeseen 192.168.1.12 ja muut portit on ohjattu suoraan sisäverkon IP-osoitteeseen 192.168.1.20, jota ei käytännössä ole edes olemassa. Se, että kaikki muut sisään tulevat portit on ohjattuina IP-osoitteeseen, jota ei ole olemassa, lisää tietoturvaa tai ainakin vaikeuttaa hakkerien yrityksiä murtautua yrityksen tietojärjestelmään. Tämä tapa ei sinänsä korvaa palomuuria, mutta toimii ainakin hyvänä lisäsuojana tietomurtojen estämiseksi.

Kuvan 1 porttiohjauksilla saadaan esimerkiksi Linux SME -palvelin toimimaan web- ja -sähköpostipalvelimena. Jotta web-palvelimessa sijaitsevat Internet-sivut ja palvelut näkyisivät ulkoverkkoon, täytyy porttien 80 (HTTP) ja 443 (HTTPS) olla ohjattuna palvelimen sisäverkon IP-osoitteeseen. Kun palvelin toimii lisäksi myös sähköpostipalvelimena, täytyy porttien 25 (SMTP), 110 (POP3) ja 143 (IMAP) olla avoinna ja ohjattuna myös samaan sisäverkon IP-osoitteeseen.

Kuvassa 1 portti 1723 (PPTP) on käytössä Virtual Private Network (VPN) -yhteydelle. VPN-yhteydellä voidaan ulkoverkosta ottaa yhteys esimerkiksi työpaikalle, jolloin työntekijällä voi olla käytössään samat palvelut ja oikeudet kuin normaalisti työpaikan sisäverkossa olisi. VPN-yhteyden luominen Windows Xp Pro -työasemalta palvelimelle on esitettynä liitteessä 3.

Palvelimen ylläpitäjä tarvitsee myös oman portin palvelimen etähallintaa varten. Tällöin käytetään lähes aina Secure Shell -protokollaa hyväksi. Secure Shell eli SSH käyttää oletuksena porttia 22, mutta se voidaan turvallisuuden lisäämiseksi muuttaa palvelimelle esimerkiksi portiksi 222, kuten kuvassa 1 on tehty.

Lähes kaikissa porttiohjauksissa riittää se, että ohjaus on tehty ainoastaa tcp-protokolalle. Tcp on kuljetuskerroksen protokola, jonka tehtäviin kuuluu tiedonsiirron luotettavuus ja virheettömyys. Udb:tä käytetään silloin, kun halutaan tiedonsiirto maksimaalisen tehokkaaksi. Tällöin tiedonsiirron luotettavuus ei vastaa Tcp:n tasoa. Esimerkiksi videon ja musiikin välitys tapahtuu udb:llä, joten www-selaukseen käytettävä portti 80 tulisi ohjata palvelimelle niin, että molemmat protokollat ovat käytössä.

4 Linux SME -palvelin

Linux SME -palvelin on Linux-pohjainen, eli vapaaseen lähdekoodiin perustuva palvelinohjelmisto. SME tulee englannin kielen sanoista Small and Medium Enterprises tai Small- and Medium-sized Enterprises /8/. SME on siis tarkoitettu pienille ja keskisuurille yrityksille, mutta sitä on toki mahdollista käyttää suuremmissakin yrityksissä, esimerkiksi vain tiettyjen palvelujen suorittamiseen. Tässä palvelinratkaisussa on integroituna erittäin monipuoliset ja yritysten tarpeita vastaavat palvelut. Tämän työn toteutuksessa SME-palvelimen asennus suoritettiin versiolla 7.3, joka oli kyseisellä hetkellä uusin versio. SME on 32-bittinen palvelinjärjestelmä ja siinä ei ole graafista käyttöliittymää. Kaikki asiat eivät kuitenkaan tapahdu komentorivin kautta, vaan asetuksia tehtäessä käytetään server-manager-ja server-console -valikkoja. Näistä valikoista kerrotaan tarkemmin pk-yrityksen tietoliikennejärjestelmän toteutuksen yhteydessä.

4.1 SME-palvelimen ominaisuudet

SME sisältää lukuisia palveluita ja ominaisuuksia. Suurin osa SME:n palveluista on heti asennuksen jälkeen oletuksena käytössä, kun taas osa palveluista joudutaan aktivoimaan erikseen komentorivin tai server-manager valikon kautta. Palvelujen määrään vaikuttaa sekin, minkälaiseen tehtävään palvelin on omaan verkkotopologiaan asetettu. SME:n roolista kerrotaan tarkemmin myöhemmin tämän osion viimeisessä kappaleessa.

Seuraavassa listauksessa on esitettynä SME-palvelimen tärkeimmät palvelut:

- Sähköpostipalvelin, Horden webmail
- Korkean tason tietoturvaominaisuudet, jotka vähentävät tietomurtoihin liittyviä riskejä
- Keskitetty tiedostopalvelin, joka mahdollistaa informaation vaihdon Windowsin, Macintoshin ja Unix-laitteiden kesken.
- Web-palvelimen, mukana PHP- ja MySQL-tuki
- Selainpohjaisen palvelimen hallintaohjelman, server-manager
- Jaetut sähköpostikirjastot, joita ylläpidetään automaattisesti

- Roskapostisuodin sähköpostiliikennettä varten
- Viruksentorjuntaohjelmana clamAv

Näiden ominaisuuksien lisäksi SME-palvelimeen on mahdollistaa asentaa lukuisia lisäsovelluksia. Esimerkiksi Moodle-ohjelmisto on mahdollista asentaa suoraan komentorivin kautta yhdellä ainoalla käskyllä:

‘yum --enablerepo=smecontribs install moodle smeserver-moodle’ /19/

4.2 Laitteistovaatimukset

Linux SME -palvelin on mahdollista saada toimimaan myös hieman vaatimattomalla laitteistokokoonpanolla (ks. taulukko 4.). On kuitenkin hyvä muistaa, että laitteistovaatimukset riippuvat paljolti siitä, mihin käyttötarkoitukseen palvelin halutaan ja myös siitä, millaiseen käyttöympäristöön palvelin tulee.

Taulukko 4. Minimivaatimukset. /6/

Kategoria	Tarkennukset
Arkkitehtuuri	PCI-pohjainen i586 tai i686-yhteensopiva prosessori
Prosessorin nopeus	400 MHz
RAM	256 MB
Kovalevy	IDE tai SCSI – koko vähintään 4 GB
SCSI adapteri	SCSI-adapterin tulee olla näkyvillä tuettujen adapterien listauksessa (Vain tarpeellista SCSI-kokoonpanoissa)
Verkkokortit	Verkkokorttien tulee olla tuettujen laitteiden listauksessa
Modeemi	Voidaan käyttää ainoastaan modeemeja, jotka ovat yhteensopivia linuxien kanssa.
CD-asema	ATAPI tai SCSI
Näyttölaite	Mikä tahansa
Näytönohjain	Mikä tahansa

Myös taulukon 5 suositusvaatimukset saattavat tuntua hieman vaatimattomilta, mutta SME pystyy toki käyttämään tehokkaasti hyväksi tehokkaampiakin laitteistokokoonpanoja. Tärkeintä on kuitenkin valita sellainen laitteistokokoonpano, jolla on hyvät edellytykset pysyä pystyssä useitakin vuosia ja joka vastaa yrityksen tarpeita.

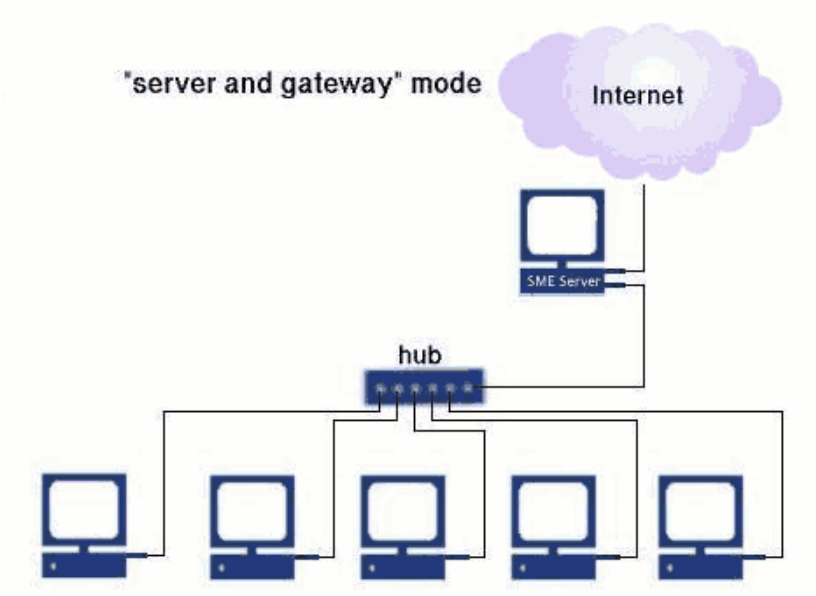
Taulukko 5. Suositusvaatimukset. /6/

Kategoria	Tarkennukset
Arkkitehtuuri	PCI-pohjainen i686-yhteensopiva prosessori
Prosessorin nopeus	1.5 GHz
RAM	512 MB
Kovalevy	yksi tai useampi IDE -tai SCSI-kovalevy – vähintään 40 GB
SCSI adapteri	SCSI-adapterin tulee olla näkyvillä tuettujen adapterien listauksessa (Vain tarpeellista SCSI-kokoonpanoissa)
Verkkokortit	Verkkokorttien tulee olla tuettujen laitteiden listauksessa
Modeemi	Voidaan käyttää ainoastaan modeemeja, jotka ovat yhteensopivia linuxien kanssa.
CD-asema	ATAPI tai SCSI
Näyttölaite	Mikä tahansa
Näytönohjain	Mikä tahansa

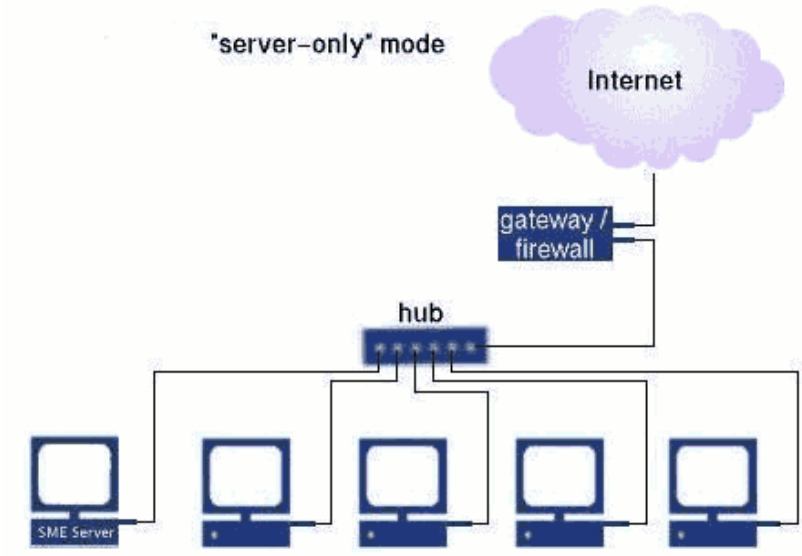
4.3 SME-palvelimen tehtävä ja sijoitus yrityksen verkkotopologiassa

SME-palvelin ja monet muutkin palvelimet voidaan sijoittaa verkkoon joko kuvan 2 tai kuvan 3 mukaisella tavalla. Normaalisti, jos yrityksessä on käytössä erillinen palomuuriratkaisu, on kuvan 2 tapa tyypillisin ja varmin. Kuvan 2 tapaisessa palvelimen sijoituksessa palvelin on asetettu palvelin ja yhdyskäytävä -tilaan. Tällöin palvelin tarjoaa normaalien palveluidensa lisäksi myös datan reititykseen liittyvät tehtävät. Käytännössä niin lähtevä kuin saapuvakin data kulkee palvelimen kautta. Palvelimessa on tällöin käytössä oma palomuuriratkaisu. Kuvan 2 tapa on kuitenkin käytännössä melko harvinainen ja ei-suositeltu tapa, koska tällöin palvelin joutuu liian kovalle rasitukselle. On suositeltavaa aina hajauttaa tietyt palvelut useille eri laitteille. Tämän takia kuvan 3 tapa, jossa palvelin

on kytkettynä työasemien tapaisesti suoraan kytkimeen, on loogisesti ideaalisin ja varmin.



Kuva 2. SME-palvelin sekä palvelimena että liikenteen jakajana. /6/

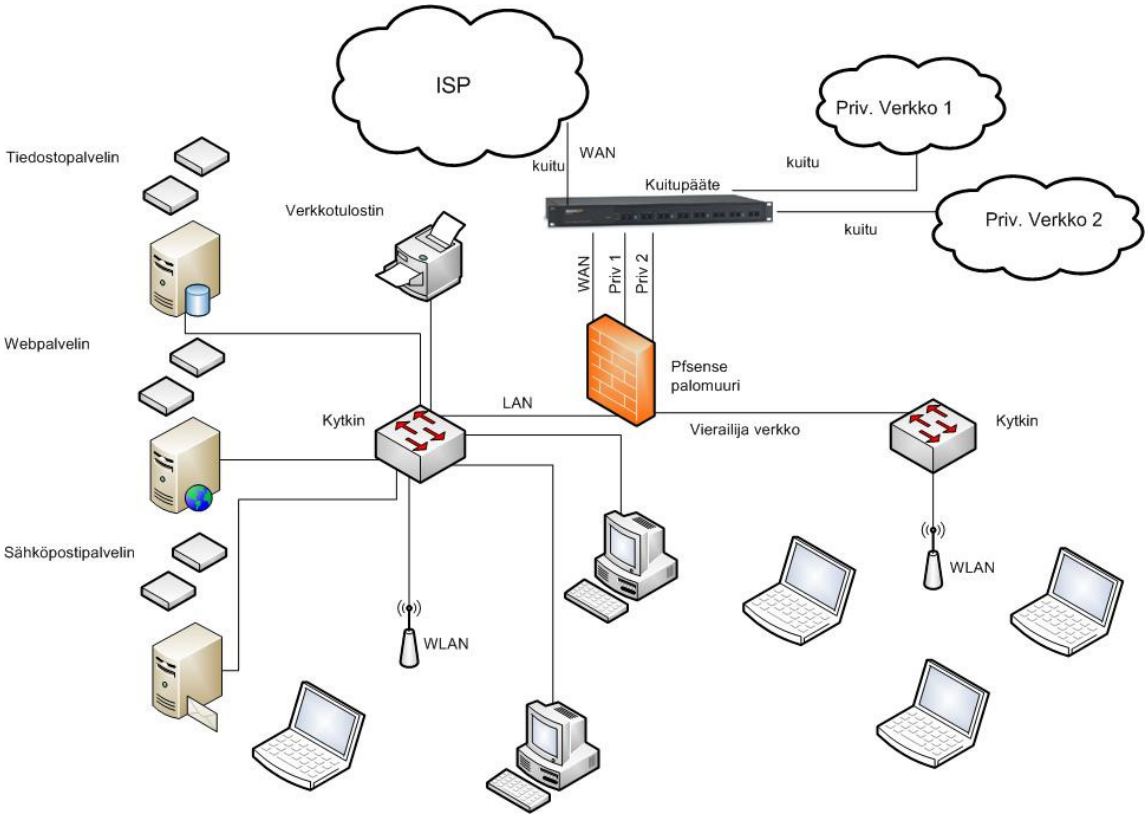


Kuva 3. SME-palvelin ”vain palvelin”-tilassa. /6/

Monet pk-yritykset, jotka siirtyvät käyttämään omaa palvelinratkaisua valitsevat keskitetyn palvelinratkaisun. Tällöin yrityksen lähiverkossa toimii vain yksi palvelin, jonka päätehtävänä on toimia tiedostopalvelimena. SME on suunniteltu juuri näitä yrityksiä varten, koska se toimii todella hyvin yhteen Windows-työasemien kanssa. Tämän lisäksi on mahdollista keskittää koko yrityksen sähköpostiliikenne sekä yrityksen omat Internet-sivut samalle palvelimelle.

Pelkkä SME toimii todella hyvin tiettyyn pisteeseen asti, mutta kun yrityksen resurssit ja verkkoliikenne kasvavat todella mittaviksi, on aika hajauttaa palveluita useille palvelimille. Käytännössä pelkkä SME on erinomainen vaihtoehto yrityksille, jotka ovat juuri aloittaneet liiketoiminnan sekä myös niille yrityksille, joilla on n. 5 - 10 työasemaa yhtäaikaa yrityksen verkossa käytössä.

Ongelma täysin keskitetyssä palvelinratkaisussa on se, että palvelinrikon tapahtuessa koko yrityksen toiminta saattaa seisahtua kokonaan. Yrityksen on tällöin itse tiedostettava se, onko sillä varaa siihen, että sen toiminta on täysin yhden palvelimen varassa. Kuvassa 4 on esitettynä verkkotopologiamalli, jossa palvelimet ovat hajautettuna kolmeen osaan. Palvelinrikon tapahtuessa kaikki palvelut eivät seisahdu ja yritys pystyy silti jatkamaan toimintaansa, vaikkakin puutteellisesti. Kustannustekijät tulevat ratkaisemaan sen, kumpi näistä vaihtoehdoista sopii yritykselle paremmin. Hajautetetun palvelinratkaisun toteutus tulee luonnollisesti maksamaan yritykselle enemmän, mutta kuinka paljon yritykselle tulee maksamaan se, että sen toiminta on palvelinrikon aikana kokonaan katki. Kustannusarvioista ja yrityksen tarpeista on tehtävä tarkat analysoinnit, ennen palvelinympäristön toteuttamista.



Kuva 4. Esimerkkiverkkotopologia hajautetusta palvelinympäristöstä.

5 Pk-yrityksen tietoliikenneverkon suunnittelu ja toteutus

Tässä kappaleessa toteutetaan toimiva ja kokonaisvaltainen tietoliikennejärjestelmä, joka on helposti integroitavissa yritykseen kuin yritykseen. Verkkotopologia ja tarvittavat laitteet sekä palvelut ovat tietysti aina kiinni yrityksen tarpeista. Kuitenkin tietyt asiat, kuten palomuuri- ja palvelinratkaisut ovat todella yhteneviä kaikissa yrityksissä. Jossain tapauksissa on parempi, että esimerkiksi palvelimet hajautetaan moneen osaan. Tällöin sähköpostipalvelin toimii omana palvelinkokonaisuutena, kuten myös tiedostopalvelin ja web-palvelin. Tällä tavalla saavutetaan se hyöty, että käytettävät resurssit voidaan jakaa monelle laitteelle. Tämän ansiosta yksi palvelin ei vaadi niin suurta kapasiteettia ja tehokkuutta. Linux SME kuitenkin mahdollistaa sen, että kaikki palvelinratkaisut voidaan toteuttaa yhdellä palvelimella. SME:ssä on integroituna kaikki yritykselle tärkeät ominaisuudet, mutta silti se ei vaadi kovin tehokasta laitekokoonpanoa, koska siinä ei ole erillistä graafista käyttöliittymää, joka vaatisi prosessoritehoja ja muistia. Silti on muistettava se, että keskitetty palvelinratkaisu ei sovi kaikille yrityksille. Tarkemmin tätä asiaa on pohdittu edellisessä kappaleessa.

Pk-yrityksen palomuuriratkaisu voidaan toteuttaa monella eri tavalla. Voidaan tehdä ratkaisu, jossa on ainoastaan pelkkä palomuuritoiminto, jolloin puhutaan usein rautapalomuurista. Toinen vaihtoehto on palomuuriohjelma, joka sisältää palomuuritoimintojen lisäksi myös sisältösuotimen www-sivujen selausta varten ja tehokkaan roskapostisuotimen sähköpostille. Tämän lisäksi palomuurissa on myös oma proxy-palvelin, joka nopeuttaa www-sivujen selaamista. Tällaisia palomuuriratkaisuja on monia, jotka toimivat Linux-pohjaisella ohjelmistolla, esimerkiksi Smoothwall, Securepoint, Evian ja Pfsense.

Monella yrityksellä on jäänyt varastoihin vanhoja tietokoneita, jotka voidaan nykyaikana luokitella ongelmajätteeksi. Näitä vanhoja tietokoneita on kuitenkin mahdollista uusiokäyttää, kun niihin asennetaan palomuuriohjelmisto. Palomuuritoiminnot eivät vaadi kovin tehokasta laitteistoa toimiakseen, koska graafista käyttöliittymää ei tarvita. Silti fyysisen RAM-muistin tarve nousee usein koko palomuurijärjestelmän kulmakiveksi. Vanhojen laitteiden käytön riskit ovat luotettavuudessa. Kestävätkö ne jatkuvaa käyttöä ja kuormitusta, ja kuinka helposti saadaan korvaava tilalle, kun vanha

hajoaa. Näitä kysymyksiä miettiessä on silti muistettava se, ettei mikään tietotekninen laite ole ikuinen. Silti on aina minimoitava nämä riskitekijät käyttämällä sellaisia laitekokoonpanoja, jotka ovat kokemuksen ja testauksen kautta osoittautuneet luotettaviksi.

Kuten edellä tuli jo mainittua on Linux-pohjaisia palomuuriratkaisuja useita. Jos yrityksellä on esimerkiksi käytössään kuituyhteys, joka halutaan jakaa ja erottaa usealle eri yhteydelle käyttämällä virtuaalilähiverkkoja, on Pfsense hyvä valinta. Linux-pohjainen Smoothwall on hyvä vaihtoehto, kun yrityksellä on käytössä perinteinen ADSL-yhteys, eikä verkkoa tarvitse jakaa useisiin virtuaaliverkkoihin. Smoothwall tulee esittämään oman totetusesimerkkini palomuuriratkaisua.

Tulen esittämään tässä työssä SME-palvelimen ja Smoothwall-palomuurin asennuksen ja konfiguroinnin eri vaiheet sekä myös muutamia vaihtoehtoisia ratkaisuja. Tuon myös esille yksityiskohtia, jotka liittyvät yrityksen verkkotopologiaratkaisuihin sekä pyrin luomaan mahdollisimman tehokkaan, kustannuksiltaan siedettävän ja työmäärältään järkevän tietoliikennejärjestelmän toteutuksen. Kokonaiskustannuslaskelma yhdelle esimerkkiyritykselle on esitettynä tämän osion viimeisessä kappaleessa.

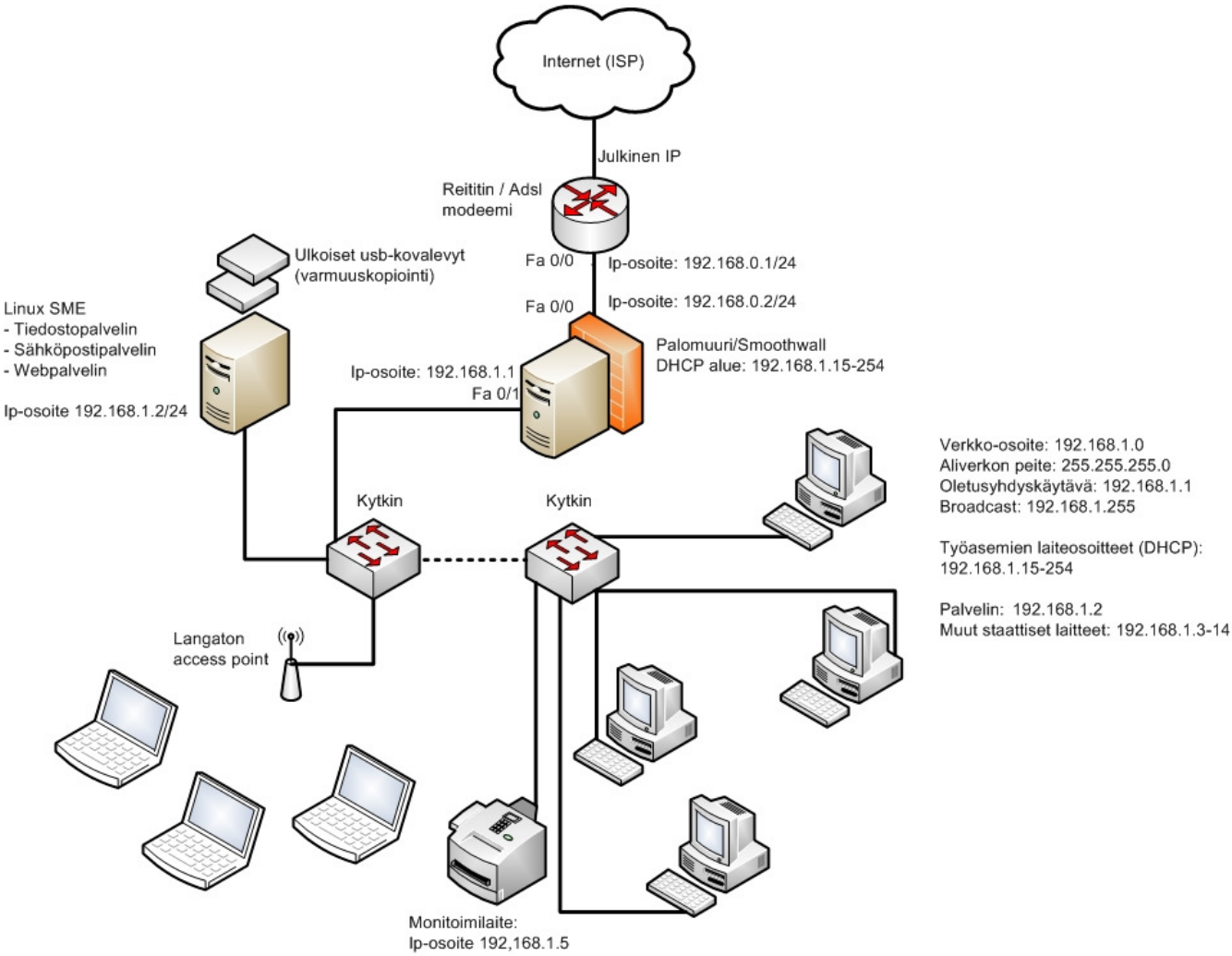
5.1 Looginen verkkotopologia

Kuvassa 3 on esitettynä looginen verkkotopologiamalli, joka toimii hyvin tämän työn toteutuksen pohjana. Palomuurina toimii siis Smoothwall ja palvelimena Linux SME. Kuvan 5 loogisessa verkkotopologiassa, kuten myös omassa toteutuksessani on Smoothwall-palomuurissa käytössä vain red- ja green-rajapinta. Red tarkoittaa ulkoverkkoon menevää turvatonta verkkoa ja green taas suojattua sisäverkkoa. Palomuuri toimii normaalin PC:n päällä, jolloin sen rajapintoina toimivat verkkokortit. Verkkokortit ovat useimmiten PCI-väyläisiä ja nopeudeltaan 10/100 MB/s. Nykyään myös gigabitin suuruiset kortit ovat erittäin yleisiä sekä suhteellisen edullisia. Uuden verkon lisäys palomuuriin onnistuu helposti: tarvitaan ainoastaan uusi verkkokortti. Verkkokortin lisäyksen jälkeen se täytyy vain asettaa eri verkkoalueelle. Kolmatta verkkoa kutsutaan Smoothwallissa purple-rajapinnaksi, joka on mahdollista ottaa käyttöön esimerkiksi vierailijaverkolle. Tällöin tästä verkosta ei ole pääsyä yrityksen omaan sisäverkkoon.

Huomioitavaa on se, että kun virtuaalilähiverkkoratkaisut tehdään palomuurin kautta, ei hallittavia kytkimiä tarvita. Tämä tuo ison säästön tietoliikenneverkon kokonaiskustannuksiin, koska normaalit peruskytkimet ovat huomattavasti halvempia.

Linux SME toimii tässä verkkotopologiassa ainoana palvelimena. Se toimii tiedosto-, sähköposti- ja web-palvelimena. Mikäli yrityksen verkkoliikenne on todella nopeaa ja kuormittavaa, on palveluiden hajauttaminen suotavaa. Tällöin SME:n jakamat palvelut voitaisiin jakaa kolmelle eri palvelimelle. Silti on todettava, että pk-yrityksissä on harvemmin tilanteita, jolloin hajauttaminen olisi tarpeellista, koska verkkolaitteiden määrä on alhainen. Silti erillinen varmuuskopiopalvelin olisi aina hyvä lisä verkkoon kuin verkkoon, koska kaikkein arvokkain tieto on menetetetty tieto.

Kuvan 3 kaltaisessa tietoliikenneverkossa on yleensä vain yksi julkinen IP-osoite käytössä. Tämän osoitteen kautta kaikki työasemat ja laitteet muodostavat yhteyden ulkoverkkoon. Tällöin reititin tai laajakaistamodeemi toimii Internet-yhteyden välittäjänä palomuurille. Reititin tai laajakaistamodeemi tulee konfiguroida siten, että se ohjaa kaikki tarvittavat portit palomuurille. Palomuuri asetetaan taas ohjaamaan palvelimen tarvitsemat portit suoraan sen sisäverkon IP-osoitteeseen. Palomuurilla on oltava saman verkkoalueen IP-osoite reitittimen kanssa, ja lisäksi sen täytyy tarjota eri verkkoalue sisäverkolle. Työasemille tarjotaan IP-osoitteet, aliverkon peite, oletusyhdyskäytävä ja nimipalvelimen (DNS) IP-osoite DHCP-palvelun kautta automaattisesti. Kuvan 5 topologiassa on jätetty 15 laiteosoitteen alue staattisille laitteille. Työasemat, jotka käyttävät DHCP-palvelua eivät voi vahingossakaan saada näitä osoitteita käyttöönsä. Esimerkiksi palvelimella on aina oltava staattinen IP-osoite. Tässä tapauksessa palomuuri toimii siis DHCP-palvelimena mutta se voisi olla palvelinkin.



Kuva 5. Looginen verkkotopologia

5.2 Linux SME -palvelin

Tässä osiossa esitetään kaikki oleelliset tiedot, jotka liittyvät SME-palvelimen asennukseen ja konfigurointiin. SME:stä luodaan tiedostopalvelin, sähköpostipalvelin sekä web-palvelin. Lisäksi asetukset luodaan siten, että palvelinta on mahdollista etähallita ulkoverkon kautta sekä SSH:n avulla että myös VPN-yhteyden kautta. Lopuksi esitetään myös yksi ratkaisu, jolla voidaan toteuttaa koko palvelinjärjestelmän varmuuskopiointi.

5.2.1 SME-palvelimen asennus

Linux SME -palvelimen asennus ei vaadi asentajalta mitään erityisosaamista, koska moni asia asennuksen yhteydessä tapahtuu automaattisesti. Tämän vuoksi täytyy kuitenkin tehdä hieman taustatutkimusta ja ottaa selville muutamia seikkoja, jotka liittyvät asennukseen.

SME:ssä on oletuksena käytössä ohjelmallinen kovalevyjen peilaus. Peilauksella tarkoitetaan sitä, että jos laitteistoon on esimerkiksi asennettu 2 kovalevyä ja toinen kovalevyistä menee myöhemmin rikki, pystyy SME käyttämään toista kovalevyä suoraan ns. lennosta, eivätkä käyttäjät edes ehdi huomata kovalevyrikkoa. Silti ylläpitäjä saa heti tiedon kovalevyn rikkoutumisesta sähköpostitse ja voi käydä vaihtamassa sen.

Riippuen kovalevyjen määrästä asentaa SME ne automaattisesti ja kysymättä seuraavalla tavalla:

- 1 kovalevy - ohjelma RAID 1 (valmis vastaanottamaan toisen kovalevyn)
- 2 kovalevyä - ohjelma RAID 1
- 3 kovalevyä - ohjelma RAID 1 + 1 spare-kovalevy
- 4-6 kovalevyä - ohjelma RAID 5 + 1 spare-kovalevy
- 7 ja enemmän - ohjelma RAID 6 + 1 spare-kovalevy

RAID tarkoittaa tässä datan tallennustapaa, jossa data on tallennettuna useammalle kovalevylle. Jos silloin yksi kovalevy menee rikki, niin järjestelmä pysyy silti aktiivisena ja toimivana. Spare-levyt tarkoittavat ns. varalevyjä, jotka eivät sisälly jo toimivaan järjestelmään, vaan niihin tehdään järjestelmän varmuuskopioinnit. Varmuuskopioinnit voidaan ajoittaa siten, että ne tapahtuvat esimerkiksi 3 kertaa viikossa ja sellaiseen aikaan, ettei yrityksen toiminnalle aiheudu haittaa. Kovalevyjen tulisi myös aina olla samankokoisia tai suurempia kuin järjestelmän ensijainen kovalevy. Suositeltavaa on, että kaikki järjestelmän kovalevyt ovat samankokoisia.

Varmuuskopiointi ulkoiseen spare-levyyn tapahtuu siten, että levylle tehdään täysin toimiva klooni järjestelmästä. Käytännössä tämä tarkoittaa sitä, että jos kaikki järjestelmän kovalevyt rikkoutuvat, voidaan spare-levy vain asettaa kiinni, ja se on heti toimintaval-

mis. Tämän jälkeen voidaan asettaa taas uusi samankokoinen tyhjä kovalevy rinnalle, jolloin SME voidaan asettaa synkronoimaan ohjelmallista RAID 1:stä. Tällä tavalla järjestelmä on taas nopeasti samassa tilassa kuin ennen kovalevyrikkojen tapahtumista. Koska kovalevyt eivät ole nykypäivänä enää kovin kalliita, on tämä tapa myös tehokkuuden lisäksi erittäin edullinen ratkaisu.

Jos tiedetään, että myöhemmin spare-levyinä halutaan käyttää USB-kovalevyjä, pitää asennuksen alussa antaa käsky 'sme nolvm'. Tällöin järjestelmä näkee USB-kovalevyt normaalisti spare-levyinä, eikä ala heti automaattisesti synkronoida niitä RAID-järjestelmään mukaan.

Itse toteutin asennuksen kahdella 160 Gt:n PATA-kovalevyllä, jolloin kyseessä on ohjelma RAID 1. Laitoin molemmat kovalevyt samaan IDE-väylään kiinni siten, että molemmissa on jumpperit Cable Select -moodissa. Parempi vaihtoehto olisi ollut se, että kovalevyt olisivat eri IDE-väylissä kiinni, mikä hieman nopeuttaisi järjestelmän datansiirtokykyä.

Varmuuskopioinnin toteutus on selitetty tarkemmin kappaleessa 5.2.5. Tässä kappaleessa otetaan myös esille eri mahdollisuuksia tehdä varmuuskopioinnista tulevaisuudessa vielä entistä varmempaa affa-ohjelman avulla. Itse SME-palvelimen asennus on hyvin yksinkertainen prosessi, joka on esitettynä liitteessä 1, samassa liitteessä selvitellään myös asennuksen jälkeinen konfigurointi. Konfiguroinnin yhteydessä asetetaan palvelimelle muun muassa salasana, domain ja sisäverkon IP-osoite. Näitä asetuksia on mahdollista toki muuttaa myöhemmin SME-palvelimen server-console-valikon kautta.

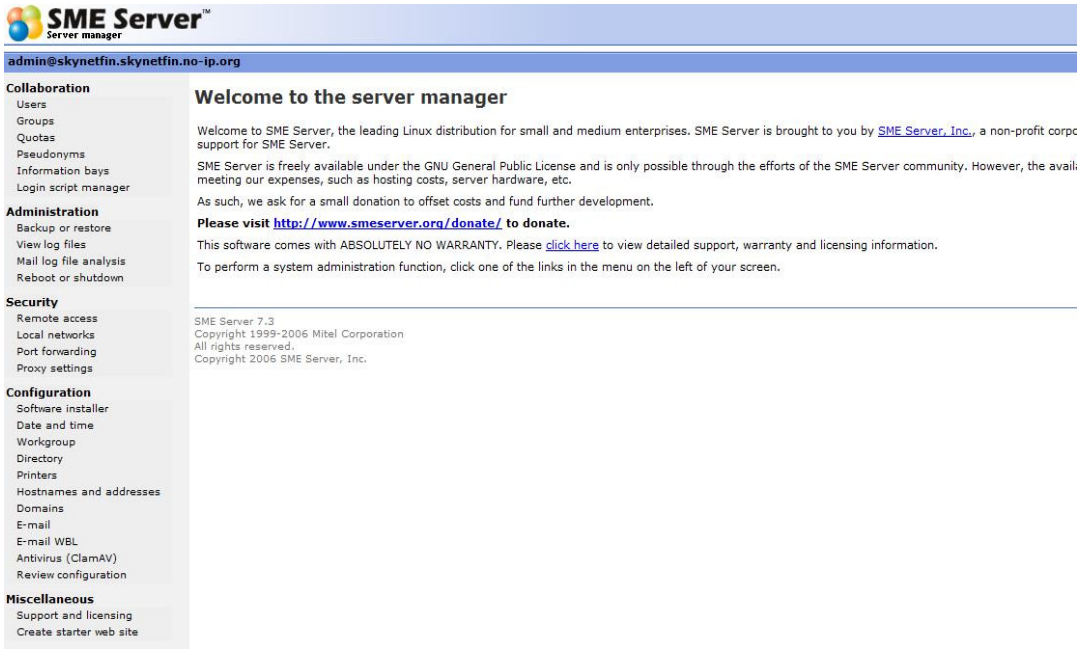
5.2.2 Tiedostopalvelimen konfigurointi

SME-palvelin on heti asennuksen jälkeen toimintavalmis, eli lähes kaikki palvelut ovat heti käytettävissä. Tiedostopalvelinkin on heti käytössä, mutta se vaatii silti hieman konfigurointia, jotta se saadaan yrityksen haluamaan tilaan.

SME:n tiedostopalvelimen perustana toimii Samba-niminen ohjelma. Samba on yleisesti käytössä lähes kaikissa Linux-järjestelmissä. Sen avulla voidaan toteuttaa Microsoftin

verkkojärjestelmä muussa kuin Windows-ympäristössä. Samba tarjoaa Windows-verkkojen palvelut ja yhteensopivuuden Unix -ja Linux-järjestelmille. /21/

Aluksi on lisättävä kaikki käyttäjät, käyttäjille omat ryhmät ja ryhmille omat verkkoasemat. Kaikki nämä asiat luodaan server-managerin kautta. Server-manageriin päästään suoraan sisäverkosta selaimen kautta tai suoraan SME-palvelimen kautta kirjautumalla järjestelmänvalvojan tunnuksilla. Selaimen kautta server-manageriin päästään, kun annetaan sisäverkon IP-osoite ja perään server-manager, eli esimerkiksi https://10.0.0.4/server-manager. SME:n server-manager käyttää suojattua HTTPS-yhteyttä. Itse server-manager näyttää kuvan 6 kaltaiselta.



Kuva 6. SME:n server-manager

Server-managerin kautta luodaan ensin käyttäjätilit. Tilien luominen tapahtuu users-valikon kautta. Ensin lisätään käyttäjä ja kirjataan käyttäjälle kaikki tarpeelliset tiedot. Tämän jälkeen tili aktivoidaan asettamalla käyttäjälle salasana. SME:ssä on oletuksena erittäin kovat salasanamääritykset. Salasanassa tulee olla vähintään 7 merkkiä, vähintään yksi erikoismerkki ja numero sekä yksi iso kirjain. Tämän lisäksi sanan ei saa muistuttaa mitään oikeaa sanaa. Joissain tilanteissa voi olla parempi, etteivät salasanojen kriteerit olisi näin kovat. /11/

Kriteerejä voidaan muuttaa komentorivin kautta seuraavanlaisilla käskyillä:

‘config setprop passwordstrength Admin strengthvalue’ /11/
‘config setprop passwordstrength Users strengthvalue’ /11/
‘config setprop passwordstrength Ibays strengthvalue’ /11/

Tällöin srentgthvalue-kohtaan voidaan asettaa ’strong’, ’normal’ tai ’none’. Asetettaessa ’strong’ vaatimukset eivät muutu, koska se on oletuksena päällä. Normal-asetuksessa vaaditaan myös iso kirjain, pieni kirjain, numero ja vähintään 7 merkkiä. None-asetuksessa taas vaaditaan vain salasana, jossa on 7 merkkiä. /11/

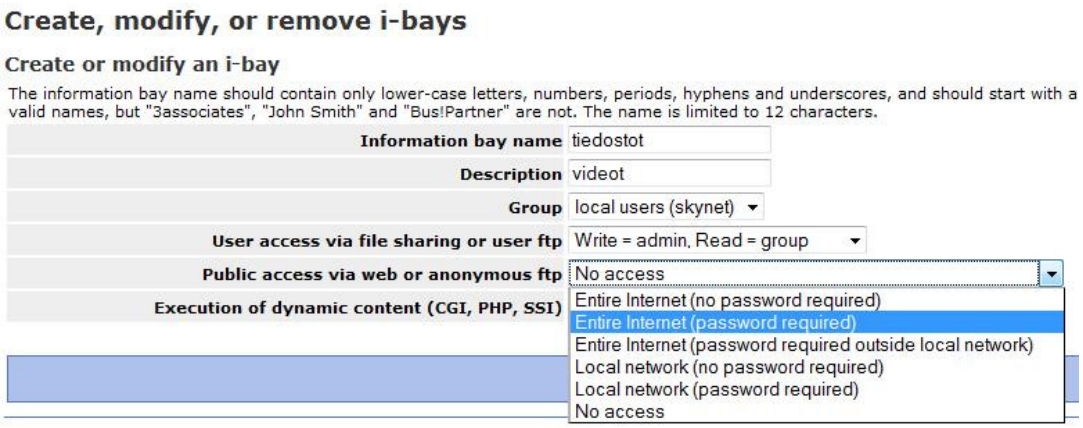
Kun asetukset on muutettu, annetaan käsky ’signal-event post-upgrade; signal-event reboot’, jotta asetukset tulevat voimaan. /11/

Kun kaikki käyttäjät on lisätty, voidaan luoda käyttäjille omat ryhmät, joihin he kuuluvat; esimerkiksi erikseen ryhmät myynnille, hallinnolle ja suunnittelulle. Kun ryhmä luodaan groups-valikon kautta, voidaan samalla lisätä ryhmään kaikki ne käyttäjät, jotka siihen kuuluvat.

Oletuksena SME tekee automaattisesti jokaiselle käyttäjälle oman kotikansion. Kotikansio lisätään Windowsiin verkkoasemaksi automaattisesti, kun henkilö kirjautuu domainiin. Kirjautumisen yhteydessä on kuitenkin mahdollista luoda useita eri verkkoasemia käyttäjien käytettäväksi. On mahdollista, että vain tietyt verkkoasemat tulevat vain tietyille käyttäjille ja ryhmille käyttöön kirjautumisen yhteydessä.

Verkkokansiot voidaan luoda suoraan server-managerin i-bays-valikon kautta (information bays). Kuvasta 7 nähdään, miten hakemistopolku luodaan, ja mitä oikeuksia niihin voidaan määrittää. Ensin luodaan hakemistolle nimi ja sen tarkoitusta ilmaiseva kuvaus. Tämän jälkeen määritetään, millä käyttäjäryhmällä on tähän kansioon oikeus. Sitten määritetään luku- ja kirjoitusoikeudet sekä FTP-yhteydelle että lähiverkolle. Myös julkiselle yhteydelle, joka suoritetaan joko Internetin tai FTP-ohjelman avulla, voidaan määrittää oikeudet. Tässä vaiheessa tulisi tietää se, halutaanko tämä kansio näkyviin vain omassa lähiverkossa, vai halutaanko siihen päästä käsiksi myös ulkoverkosta. Kuten

kuvasta 7 nähdään, voidaan oikeudet määrittää viidellä eri tavalla. Jos hakemistoon halutaan päästä käsiksi julkisesta verkosta, on salasanan käytön vaatimus aina suositeltavaa. SME tekee erikseen jokaiselle kansiolle oman web-hakemiston. Samalla voidaan määrittää, halutaanko web-hakemistoon myös PHP-, CGI- ja SSI-tuki päälle. /12/



Kuva 7. Server-managerin information ibays-valikko.

Kun lähiverkossa oleva työasema nostetaan domainiin ja käyttäjä kirjautuu koneelle omilla tunnuksillaan, on kirjautumisen yhteyteen mahdollista ajoittaa monia asioita. Nämä asiat tapahtuvat suoraan palvelimen kautta, ja ne toimivat automaattisesti. Näitä asioita voivat olla esimerkiksi kellonaika, verkkoasemien ja verkkotulostimien liittäminen, ajoitettu virusten tarkistus ja erilaisten ohjelmien päivitys.

SME:ssä on oletuksena päällä vain sellainen kirjautumiskomentojono, joka hakee käyttäjän oman kotihakemiston sekä päivittää työaseman kellonajan. Tämä komentojono sijaitsee netlogon.bat nimisessä tiedostossa, eikä sitä voida oletuksena suoraan hallinnoida server-managerin kautta. Tähän on kuitenkin saatavilla käyttökelpoinen lisäosa, joka asennetaan erikseen seuraavalla tavalla:
‘rpm -Uvh
http://distro.ibiblio.org/pub/linux/distributions/smeserver/contribs/jbennett/sme7/loginscript/RPM/smeserver-loginscript-0.2-8.noarch.rpm’ /7/.

Asennuksen jälkeen se aktivoidaan seuraavasti:
‘/etc/e-smith/events/actions/navigation-conf’ /7/.

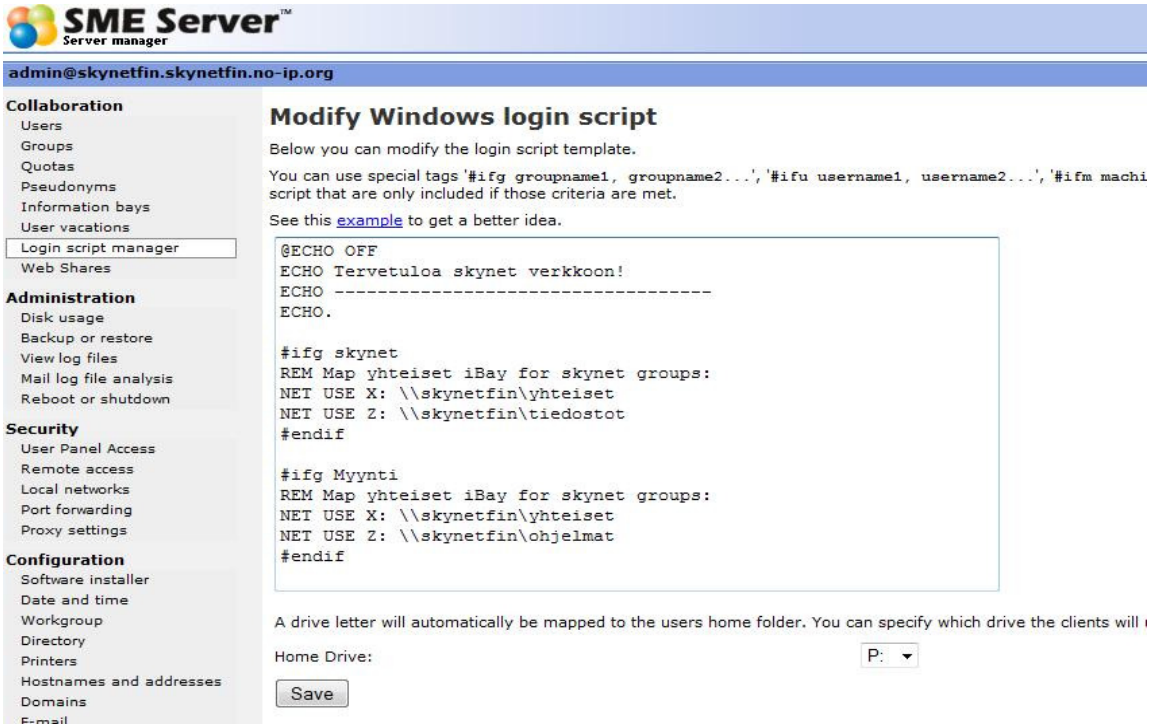
Asennus suoritetaan suoraan komentorivin kautta, jolloin palvelimelle kirjaudutaan rootin tunnuksilla. Kuvasta 8 nähdään, miltä asennettu lisäosa näyttää server-managerissa. Mukana tulee myös esimerkkikoodi, jolla pääsee hyvin alkuun, kun komentojonoa aletaan muokata. Yksinkertainen esimerkkikomentojono voisi olla seuraavanlainen:

```
@ECHO OFF
ECHO Tervetuloa skynet verkkoon!
ECHO ----------------------------------
ECHO.

#ifg skynet
REM Map yhteiset iBay for skynet groups:
NET USE X: \\skynetfin\yhteiset
NET USE Z: \\skynetfin\tiedostot
#endif

#ifg Myynti
REM Map yhteiset iBay for skynet groups:
NET USE X: \\skynetfin\yhteiset
NET USE Z: \\skynetfin\ohjelmat
#endif
```

Komentojonossa kahdelle eri ryhmälle asetaan niille kuuluvat verkkoasemat, jotka on aiemmin luotu i-bays:llä. Yhteiset-asema on molempien ryhmien käytössä. Jokaiselle käyttäjälle tulee myös oma henkilökohtainen verkkoasema automaattisesti. Tämän verkkoaseman tunnusta ei määritetä komentojonossa, vaan kuvan 8 oikeasta alareunasta.



Kuva 8. Server-manageriin asennettu loginscript-lisäosa.

Tässä vaiheessa voidaan kaikki Windows Xp Pro työasemat ”nostaa” domainiin liitteen 2 mukaisesti ja kirjautumisen yhteydessä kaikki ajoitetut tehtävät tapahtuvat automaattisesti. Tiedostopalvelin on tältä osin konfiguroitu.

5.2.3 Sähköpostipalvelimen konfigurointi

Sähköpostipalvelin on SME:ssä jo valmiiksi toimintavalmis. Silti tietyt palvelut ja toiminnot on asetettava manuaalisesti päälle. Sähköpostipalvelin, kuten myös webpalvelin, vaatii erikseen rekisteröidyn domainin käyttöönsä, jotta yritys pystyy käyttämään sitä hyväkseen myös julkisessa verkossa Internetin kautta. Domainin rekisteröintipalveluita löytyy Internetistä useita. Hintaluokka ja palvelujen tarjonta vaihtelee näissä todella paljon, joten on hyvä katsoa useita vaihtoehtoja ensin läpi ja tehdä hieman suuntaa antavaa hintavertailua.

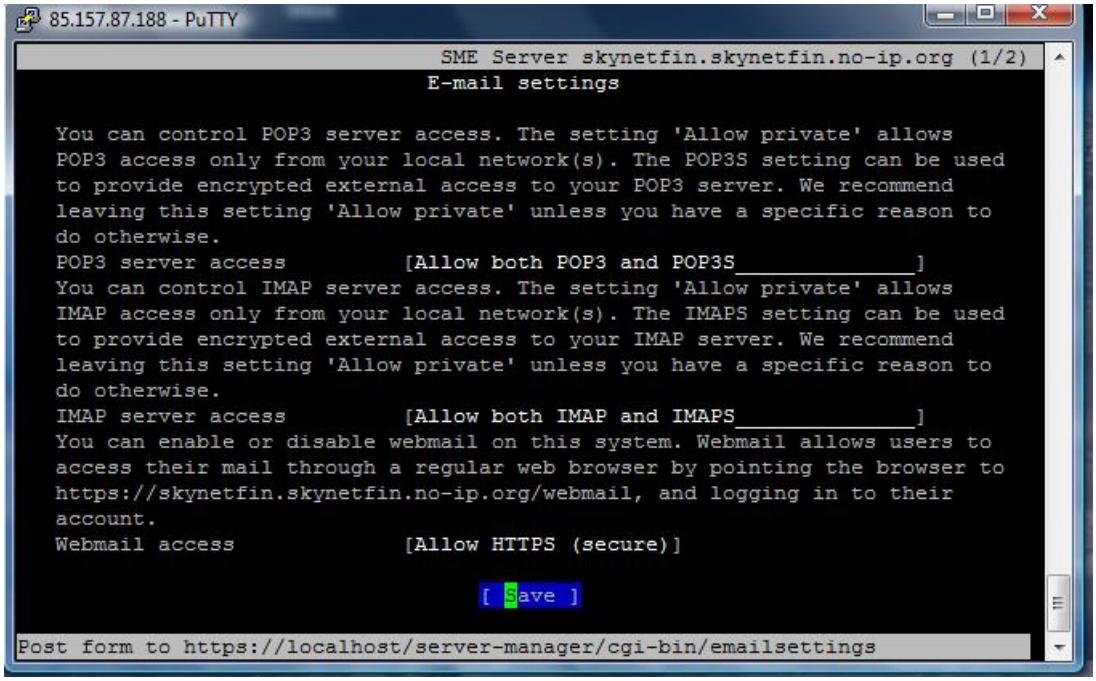
Testimielessä on kuitenkin mahdollista rekisteröidä täysin ilmainenkin domain. Ilmaisia domainin rekisteröintipalveluita on myös useita. Itse valitsin omaan testiympäristööni domainin no-ip.com:n kautta. Tähän palveluun sisältyy dynaaminen palvelu, eli jos jul-

kinen IP-osoite vaihtuu esimerkiksi palvelimen käynnistyksen yhteydessä, pystyy kyseinen palvelu integroimaan uuden julkisen IP-osoitteen jo rekisteröityyn domainiin. Ilmaiseen palveluun on mahdollista rekisteröidä 5 osoitetta, ja jokaiselle osoitteelle voidaan määrittää erikseen oma erillinen osoite sähköpostipalvelimelle. /13/

SME:ssä sähköpostipalvelimen toiminnan perustana toimii Qmail-niminen sähköpostiagentti. Qmail on kehitetty korkean tietoturvan omaavaksi sekä myös resursseiltaan tehokkaaksi ja nopeaksi ohjelmaksi. Esimerkiksi Sendmail on paljon alttiimpi kohde erilaisille hyökkäyksille. /15/

Sähköpostissa käytetään pääasiassa POP3(S) ja IMAP(S) protokollia. Nämä protokollat täytyy asettaa päälle erikseen server-managerista, niin että ne ovat toiminnassa sekä sisäettä ulkoverkon kautta. SME:ssä on myös integroituna Horden sähköpostiohjelma, joka toimii selaimen kautta niin ulko- kuin sisäverkossa. Tähän ohjelmaan päästään käsiksi ulkoverkosta, kun oman domainin perään kirjoitetaan webmail. Horden selainpohjainen sähköpostiohjelma on todella yleinen, ja se on käytössä monella palveluntarjoajalla Suomessa. Kuvassa 9 on esitettynä, miltä asetusten tulisi näyttää palvelimella, jotta sähköpostin toiminta on mahdollista. Kuvan 9 Webmail access -kohtaan tulee asetus, jossa sallitaan HTTPS:n yhteys. Esimerkiksi horden selainpohjainen sähköpostiohjelma ei toimi ilman https –yhteyden sallimista.
POP3 ja IMAP voidaan asettaa myös päälle palvelimen komentorivin kautta seuraavasti:

‘config setprop pop3 access public’ /14/
‘config setprop imap access public’ /14/
’signal-event email-update’ /14/

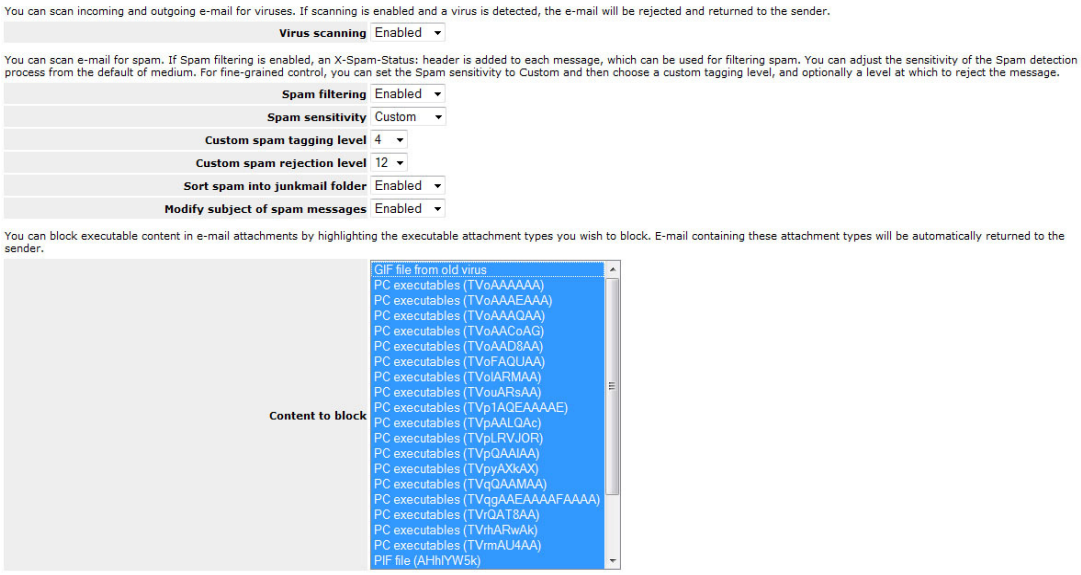


Kuva 9. Sähköpostiasetuksien asetus server-managerista (kuva otettu etäyhteyden kautta ulkoverkosta).

Nykyään roskapostisuotimet ovat erittäin tärkeissä rooleissa jokaisessa yrityksessä. SME:ssä on integroituna spamassansis-niminen palvelu roskapostin suodatukseen. Roskapostin suodatusasetuksiin päästään server-managerin email-linkin kautta. Näihin asetuksiin kuuluu virusten tarkistus, roskapostin esto sekä erilaisten liitetiedostojen esto (ks. kuva 10).

Kuva 10. SME:n sähköpostipalvelimeen liittyvät suodinpalvelut

Kuvan 10 eri palvelujen tarkemmat asetukset löytyvät kuvasta 11. On täysin kiinni ylläpitäjästä, millaiset ja kuinka tiukat asetukset hän haluaa roskapostin suodatukseen ottaa. Kuvassa 11 on yksi esimerkkiratkaisu, miltä asetukset voisivat näyttää.



Kuva 11. Roskapostisuotimen asetukset

Tiettyjä asetuksia ei ole mahdollista muuttaa suoraan server-managerin kautta, vaan ne muutetaan erikseen komentorivin kautta. Esimerkiksi, jos halutaan roskapostien poistuvan automaattisesti 2 kuukauden välein, suoritetaan seuraava käsky:

‘db configuration setprop spamassassin MessageRetentionTime 60’ /14/
‘signal-event email-update’ /14/

Monet roskapostien lähettäjät ovat jo joutuneet niin sanotulle mustalle listalle. Tätä listaa pidetään yllä Internetissä jatkuvasti, ja se on mahdollista integroida palvelimen käyttöön. Tällöin jokainen sähköpostiviesti, joka saapuu palvelimelle, käy läpi tarkistuksen tämän listan kautta ja mikäli viestin lähettäjä kuuluu tähän mustaan listaan, siirtyy viesti automaattisesti roskapostikansioon. RBL, eli Real-Time Blackhole List aktivoidaan SME:ssä seuraavalla tavalla:

‘config setprop qpsmtpd DNSBL enabled RHSBL enabled’
‘signal-event email-update’ /14/

Asetuksia ja listoja on mahdollista muokata manuaalisesti itse haluamalla tavalla. Tässä kuitenkin yhden lähteen antama esimerkkiratkaisu:

’config setprop qpsmtpd RBLList zen.spamhaus.org:whois.rfc-ignorant.org:dnsbl.njabl.org’
’signal-event email-update’ /14/

Vaihtoehtoisesti voidaan lisäksi määrittää tarkasti muita roskapostiviesteihin liittyviä asetuksia. Seuraavan esimerkin konfiguroinnissa asetetaan roskapostiohjelma spamassansis päälle ja annetaan sille käsky tuhota kaikki alle 12 tason roskapostit. Tason 4-12 roskapostien otsikko-kenttään asetetaan spam-sana, jotta käyttäjäkin tietää minkälaisesta viestistä on kyse. Heti aluksi asetetaan päälle bayesian-suodatin, jonka tarkoituksena on oppia erottamaan oikeat ja väärät roskapostit. Tämä pienentää mahdollisuutta, että myös oikeat viestit tunnistuisivat roskaposteiksi. Sekä DNSBL:ään (DNS Blacklist) että RHSBL:ään (Right Hand Side Blacklist) asetetaan oletusasetukset päälle.

‘config setprop spamassassin UseBayes 1’
‘config setprop spamassassin BayesAutoLearnThresholdSpam 4.00’
‘config setprop spamassassin BayesAutoLearnThresholdNonspam 0.10’
‘expand-template /etc/mail/spamassassin/local.cf’
‘sa-learn --sync --dbpath /var/spool/spamd/.spamassassin -u spamd’
‘chown spamd.spamd /var/spool/spamd/.spamassassin/bayes_*’
‘chown spamd.spamd /var/spool/spamd/.spamassassin/bayes.mutex’
‘chmod 640 /var/spool/spamd/.spamassassin/bayes_*’
‘config setprop qpsmtpd DNSBL enabled’
‘config setprop qpsmtpd RHSBL enabled’
‘config setprop spamassassin status enabled’
‘config setprop spamassassin RejectLevel 12’
‘config setprop spamassassin TagLevel 4’
‘config setprop spamassassin Sensitivity custom’
’signal-event email-update’ /14/

Roskapostisuotimen konfigurointi ei ole täysin ongelmatonta, vaan usein vasta kokemus ja tulokset saavat aikaan kaikkein parhaimmat asetukset. Asetuksia siis tulee muuttaa sitä mukaa, kun roskapostiliikennettä alkaa ilmaantua. Aina ajoittain on hyvä tarkistaa, ovatko esimerkiksi jotkut tietyt roskapostiviestit päässeet läpi tai onko oikeita viestejä mer-

kattu roskaposteiksi. Tätä kautta roskapostisuodinta on mahdollista opettaa edelleen tehokkaammaksi ja luotettavammaksi.

5.2.4 Web-palvelimen konfigurointi

Web-palvelin, kuten myös lähes kaikki muutkin SME:n integroidut palvelut, ovat heti asennuksen jälkeen täydessä toiminnassa. Oletuksena SME:ssä on PHP-, CGI- ja SSI-tuki päällä. Myös komentorivipohjainen MySQL-tietokantapalvelin on heti toimintavalmis. Ensisijainen web-hakemisto löytyy hakemistopolun /home/e-smith/files/ibays/Primary alta. Tämän hakemiston Internet-sivut aukeavat, kun rekisteröity domain kirjoitetaan selaimeen. Toissijaiset sivut luodaan i-bays:n kautta server-managerista. Näiden sivujen hakemistot löytyvät aina hakemiston /home/e-smith/files/ibays alta. Tarkemmin i-bays:n toiminnasta on kerrottu tiedostopalvelimen konfiguroimisen yhteydessä. Reitittimeltä tulee ohjata ainakin 80 (HTTP) ja 443 (HTTPS) portit suoraan palvelimen sisäverkon IP-osoitteeseen, jollei palvelimella ole käytössä omaa julkista IP-osoitetta.

Tämän hetkinen MySQL-palvelimen versio SME:ssä on 4.1.20. Esimerkiksi SME:n integroitu Horden selainpohjainen sähköpostiohjelma käyttää hyväkseen MySQL-tietokantaa. MySQL ei toimi SME:ssä porttien vaan suoraan kannan kautta. Tämä tapa parantaa oleellisesti tietoturvaa, koska ainoastaan palvelimella itsellään on pääsy MySQL-tietokantaan. Ylläpitäjällä on kuitenkin mahdollisuus muuttaa MySQL:n asetuksia niin, että myös lähiverkon koneilta päästään siihen käsiksi. MySQL:ssä on rootille oletuksena 72-merkkinen täysin satunnaisesti generoitu salasana. Salasana luodaan SME:n asennuksen yhteydessä. Tätä salasanaa ei saa koskaan muuttaa, koska muuttaminen sekoittaa monien ohjelmien toiminnallisuuden. Vaikka MySQL:ssä onkin tämä kyseinen salasana voimassa, on rootin tunnuksilla mahdollista päästä MySQL:n asetuksiin sisälle, vaikka salasanaa ei ole mahdollista saada mistään selville. Tietyn palvelimen sisäisen mekanismin avulla ja rootin tunnuksien kautta ei salasanaa edes kysytä. Pelkkä komento ’mysql’ riittää komentorivillä, jonka jälkeen asetuksiin päästään sisälle. /16/

5.2.5 Varmuuskopiointi

Palvelimen varmuuskopiointitapoja on useita. Tulen esittämään tässä yhden vaihtoehtoisen tavan, jota käytin omassa toteutuksessani.

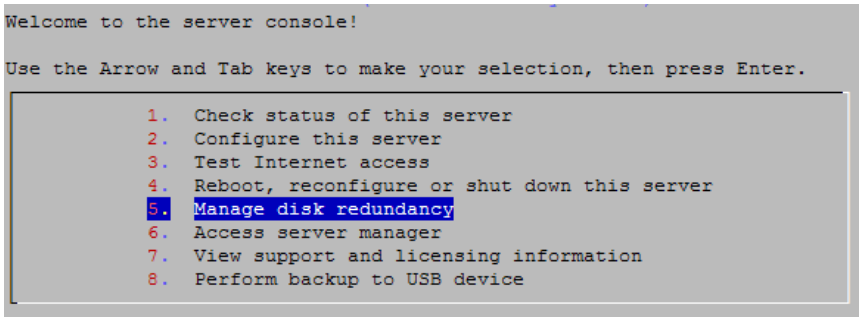
Omassa toteutuksessa otin käyttöön RAID 1 -ohjelman, jolloin palvelimessa on kaksi 160 Gt:n PATA-kovalevyä samassa väylässä. Tällöin kovalevyt ovat identtisiä toisiinsa nähden, eli jos toinen kovalevy hajoaa, niin toisessa on edelleen samat tiedot eikä toiminnallisuus katoa. Kun kovalevy hajoaa, tulee siitä heti tieto admin-tilin sähköpostiin, joka SME:ssä vastaa samalla rootin sähköpostiosoitetta.

RAID 1 -ohjelman lisäksi tein ajastetun varmuuskopioinnin ulkoiseen usb-levyyn. Tätä ulkoista kovalevyä kutsutaan spare-levyksi. Spare-levyn käyttöön ottamisen suoritin siten, että tein ensin USB-levylle täydellisen varmuuskopioinnin. Täydellinen varmuuskopiointi voidaan tehdä suoraan SME:n komentorivin kautta seuraavalla käskyllä:

‘dd if=/dev/hda of=/dev/sda bs=512’

Käsky toimii silloin, kun oletetaan, että ensisijainen PATA-levy on kiinni ensimmäisessä IDE-väylässä (hda) ja USB-levy tunnistetaan ensimmäiseksi sd-laitteeksi (sda). Käskyssä ’bs’ tarkoittaa mtu-arvoa, eli kun siirretään useita pieniä tiedostoja, on bs-arvon oltava mahdollisimman pieni maksimaalisen nopeuden takaamiseksi. Taas jos tiedostot ovat pääsääntöisesti suuria, tulisi bs-arvon vastaavasti oltava mahdollisimman suuri.

Itse toteutin täydellisen varmuuskopioinnin siten, että otin toisen RAID-levyistä pois ja laitoin USB-levyn kiinni IDE-väylään toisen ensisijaisen RAID-levyn rinnalle. Tämän jälkeen käynnistin palvelimen uudelleen ja menin järjestelmänvalvojan tunnuksilla server-consol ohjelmaan. Server-consolesta valitsin vaihtoehdon manage disk redundancy (ks. kuva 12). Tämän jälkeen ohjelma havaitsi heti uuden käyttämättömän kovalevyn, jonka jälkeen valitsemalla Ok, järjestelmä aloitti uuden kovalevyn täydellisen synkronoimisen. Tällöin kopiointi suoritetaan rsync-käskyn avulla, joten se tapahtuu huomattavasti nopeammin kuin edellä mainittua dd-käsky käytettäessä, koska rsync-käskyä käytettäessä ei kopiointiin sisällytetä kovalevyn vapaata tilaa.



Kuva 12. SME – server console.

Kun täydellinen varmuuskopiointi levylle on suoritettu, levylle on suoritettava ajastettu varmuuskopiointi, jotta varmuuskopio pysyisi ajan tasalla. Ajastettu varmuuskopio suoritetaan myös rsync-käskyn avulla siten, että varmuuskopioon sisällytetään ainoastaan järjestelmän uudet muutokset. Yksi hyvä tapa ajastukselle on esimerkiksi 3 kertaa viikossa, sunnuntaina, tiistaina ja perjantaina. Ajankohdan tulisi aina sijoittua yölle, jolloin verkkoliikenne on hiljaisimmillaan, eikä palvelimen kuormituksesta aiheutuva verkkoliikenteen hidastuminen vaikuta työaikana ja aiheuta negatiivisia seurauksia.

Omassa toteutuksessani ulkoisena USB-levynä toimii tavallinen PATA-kovalevy, joka integroidaan ulkoiseen koteloon. Koteloon tulee erillinen verkkovirta suoraan, ja siinä on oma USB-lähtö. Kun USB-levy on kytketty, niin se liitetään järjestelmään seuraavalla tavalla:

‘mount /dev/sda1 /media/boot’
‘mount /dev/sda3 /media/backup’

Ennen näitä käskyjä media-kansion alle luodaan kansiot backup ja boot. Sda2:ssa on järjestelmän swap-osio, joten sitä ei voi liittää mukaan. Tämän jälkeen on hyvä käydä katsomassa ja tarkistamassa, että liitetyissä kansioissa on kaikki tiedot olemassa. Tarkistuksen jälkeen voidaan liitokset poistaa käytöstä käänteisillä käskyillä:

‘umount /dev/sda1’
‘umount /dev/sda3’

Liittessä 5 on esitettynä ohjelman koodi, jolla varmuuskopiointi voidaan ajaa. Ohjelma usb_backup.sh kopioidaan juurihakemistoon. Ohjelma tekee varmuuskopioinnin ja ilmoittaa varmuuskopioinnin onnistumisesta tai epäonnistumisesta suoraan sähköpostiin. Sähköpostiosoitetta sekä ilmoituksiin liittyviä tekstejä on mahdollista muuttaa muokkaamalla liitteen 5 ohjelmakoodia.

Ajastuksen voi tehdä manuaalisesti muokkaamalla etc-kansion alla olevaa crontab-tiedostoa. Crontab-tiedoston sisältö muokkauksineen on esitettynä liitteessä 6. Itse toteutin ajastuksen siten, että se tehdään tiistaisin, torstaisin ja lauantaisin kello 1:30 aamuyöstä. Tämä malli toimii hyvin sellaisissa yrityksissä, joissa liike on kiinni viikonloppuisin.

SME:stä on mahdollista tehdä myös varmuuskopiointipalvelin. Tällöin siihen asennetaan affa-niminen ohjelma, jonka avulla voidaan ottaa varmuuskopioinnit esimerkiksi Windows-työasemista. Affa toimii hyvin yhteen kaikkien Windows-käyttöjärjestelmien kanssa. Windows-työasemiin on kuitenkin ensin asennettava Cygwin-niminen ohjelma, joka mahdollistaa sen, että työasema ja SME pystyvät kommunikoimaan keskenään. Kaikki varmuuskopioinnit tapahtuvat aina verkon kautta ja tunnistautumisessa käytetään SSH:ta. Käytettävän SSH-portin voi määritellä itse manuaalisesti. Muuten affa on täysin komentorivipohjainen ohjelma, joten sen käyttäminen vaatii hieman harjoittelua. Varmuuskopioinnissa käytetään rsync-käskyä kopioinnin nopeuttamiseksi. Kun SME:stä tehdään varmuuskopiointipalvelin, olisi hyvä, ettei se silloin tarjoa muita palveluja yrityksen sisällä. Varmuuskopiointi vaatii aina runsaasti kovalevytilaa varsinkin, jos yrityksen sisällä on useita työasemia, joista varmuuskopiointi otetaan. Affa toimii hyvin myös silloin, kun halutaan ottaa varmuuskopiointeja toisista SME-palvelimista tai vaihtoehtoisesti myös niissä tapauksissa, kun halutaan siirtää SME kokonaan toiseen laitteistoon. /18/

5.3 Työasemien konfigurointi

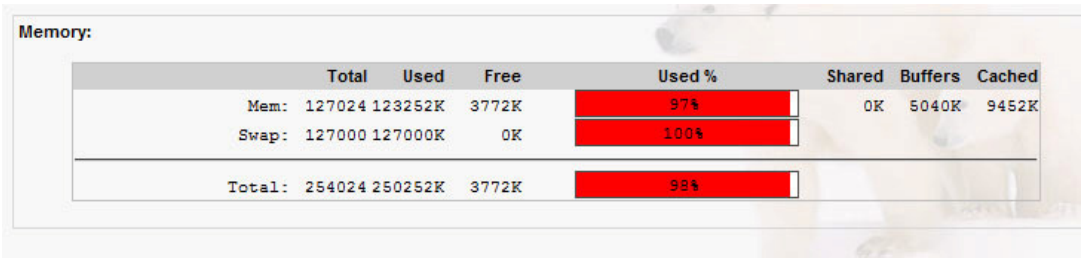
Linux SME toimii erittäin hyvin yhteen Windows-ympäristössä. Liitteen 3 ohjeistuksessa on domainiin liittäminen suoritettu Windows Xp Pro -työasemalla. Melkein samalla tavalla voidaan liittää muutkin Windows-versiot. Tässä vaiheessa on hyvä kuitenkin muistaa se, että Windowsin Home-versioita ei ole mahdollista yhdistää domainiin. Home-versioillakin päästään kyllä käsiksi tiedostopalvelimen tarjoamiin verkkoasemiin ja oh-

jelmiin siten, että asetetaan työryhmä samaksi palvelimen domainin työryhmän kanssa ja asetetaan paikalliselle koneelle sama käyttäjänimi ja salasana kuin palvelimella. Silti käyttäjän omat verkkoasemat eivät yhdisty automaattisesti kirjautumisen yhteydessä, vaan ne pitää hakea koneelle manuaalisesti. Tällöin voidaan toki kopioida palvelimella oleva netlogon.bat niminen tiedosto suoraan paikallisen koneen käynnistysvalikkoon, jolloin se ajetaan aina käynnistyksen yhteydessä automaattisesti. Silti on aina suotavaa käyttää Windowsin Professional-versioita yrityksissä.

VPN-yhteyden luominen Windowsissa on myös hyvin yksinkertainen prosessi, joka on esitettynä liitteessä 4. Yhteyden luomisen jälkeen verkkoasemien yhdistäminen täytyy tehdä manuaalisesti uudestaan, vaikka kyseessä olisikin Windowsin Pro-versio.

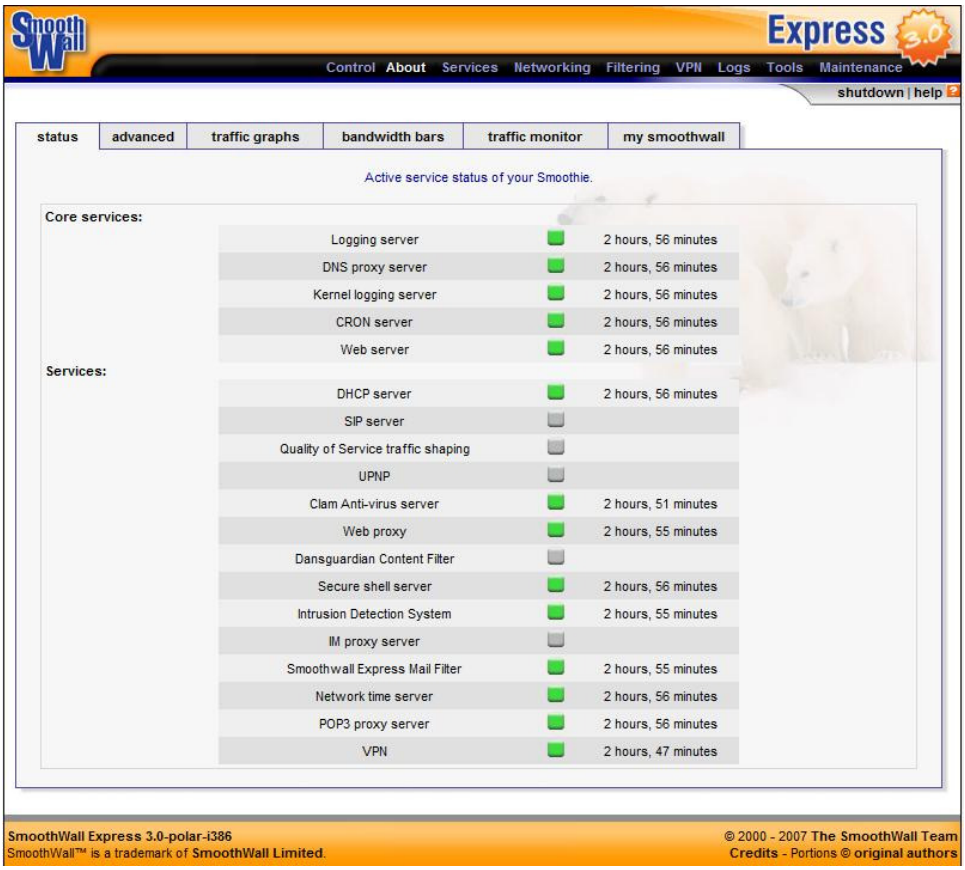
5.4 Smoothwall -palomuuri

Omassa palomuuriohjelman valinnassani päädyin Linux-pohjaiseen Smoothwall-palomuuriin, koska se tarjoaa palomuuritoimintojen lisäksi myös paljon muita hyviä palveluita. Smoothwall on Linux-ohjelmien tapaisesti täysin ilmainen. Suoritin asennuksen vanhan Pentium II -laitteiston päälle, jossa RAM-muistia 128 Mt:a. Myöhemmin kävi selväksi se, että 128 Mt ei silloin riitä jos halutaan pitää maksimaalinen määrä palomuuritoimintoja päällä, vaikka 128 Mt:a onkin ohjelmistolle asetettu suositusvaatimus. Esimerkiksi välityspalvelimen välimuistin määrää on tuntuvastti alennettava jos muistia ei ole tarpeeksi. Muistin tarpeen merkitys voidaan helposti todeta kuvasta 13, jossa jopa swap on jo kokonaan käytössä.



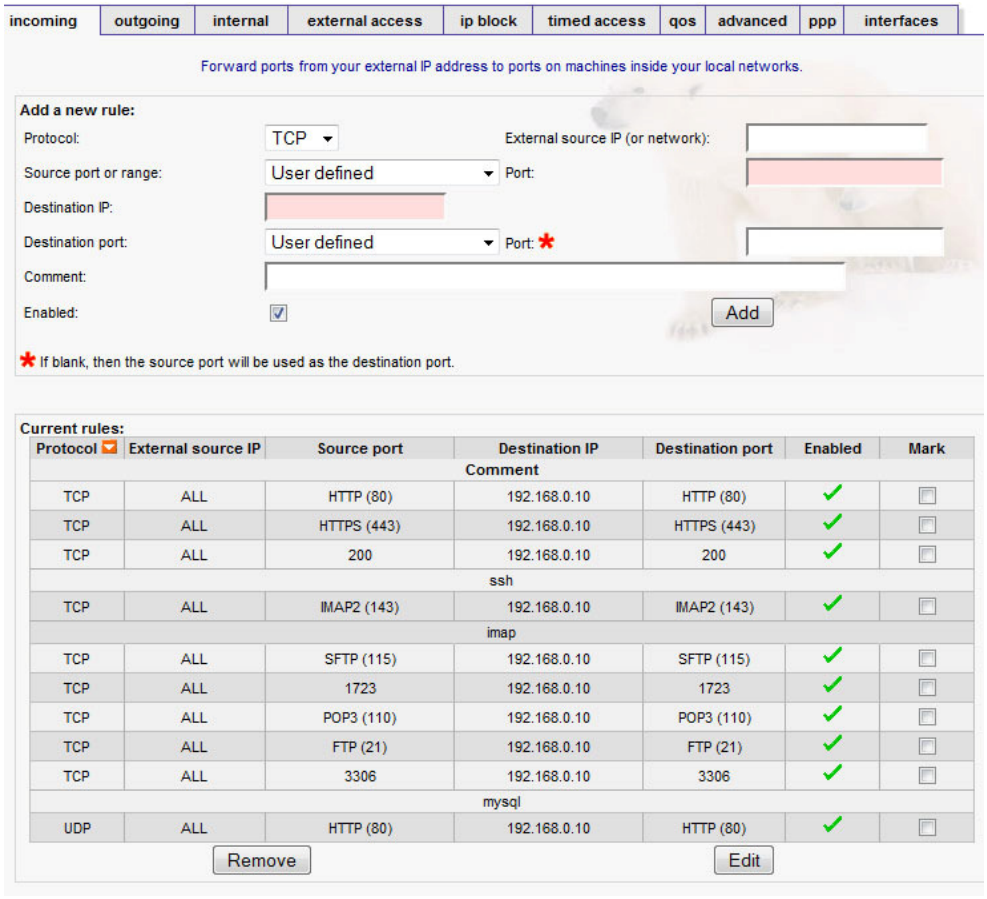
Kuva 13. Smoothwall-palomuurin muistin käyttö.

Kuvasta 14 nähdään Smoothwallin tila, eli kuvasta on mahdollista nähdä kaikki palvelut, jotka ovat käynnissä tai suljettuina. Samalla nähdään myös se, kuinka kauan tietty palvelu on ollut käynnissä. Palvelut ovat jaettu ydinpalveluihin ja ns. peruspalveluihin.

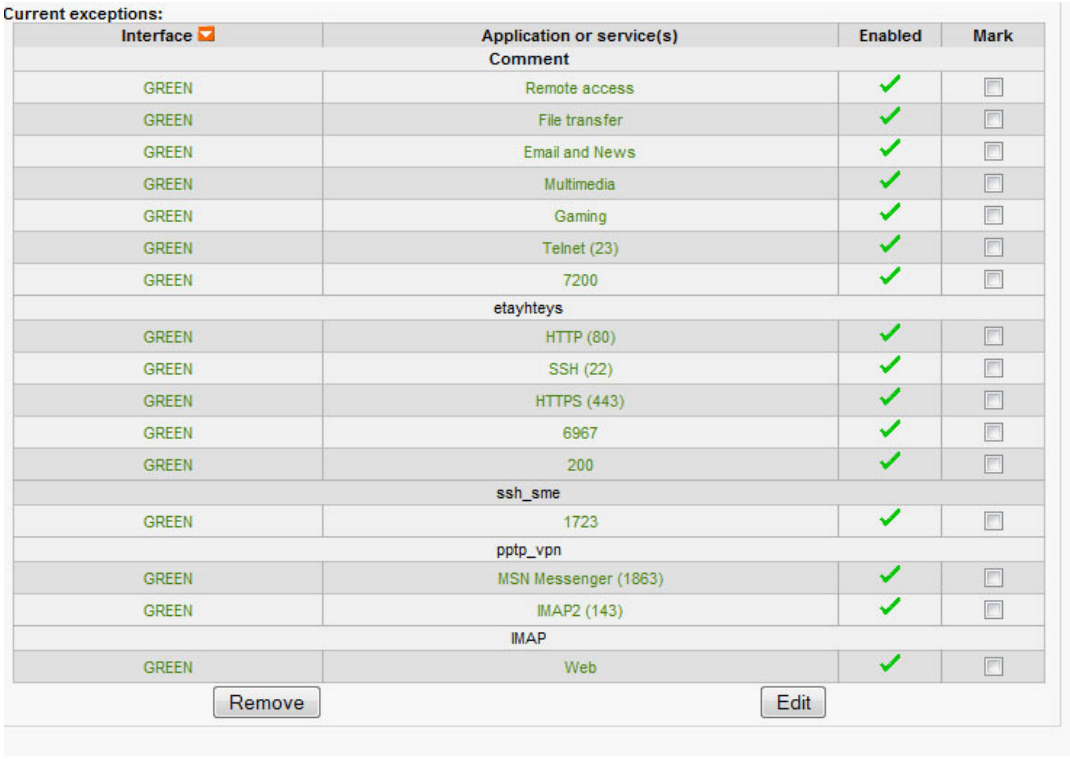


Kuva 14. Smoothwall-palomuurin tila.

Oikein konfiguroituna Smoothwall on täysin yhteensopiva palomuuri erilaisten palvelinten kanssa, jotka tarvitsevat oikeanlaiset porttiohjaukset omille palveluilleen. Kuvassa 15 on esitettynä sisääntulevan liikenteen porttiohjaukset ja kuvassa 16 taas esitettynä sallittujen palvelujen luettelo. Kuvan 16 palvelut ovat kohdistettuna palvelimen sisäverkon IP-osoitteeseen. Porttiohjauksissa käytettävistä palveluista ja protokollista on kerrottu tarkemmin kappaleissa 3.1 ja 3.2.

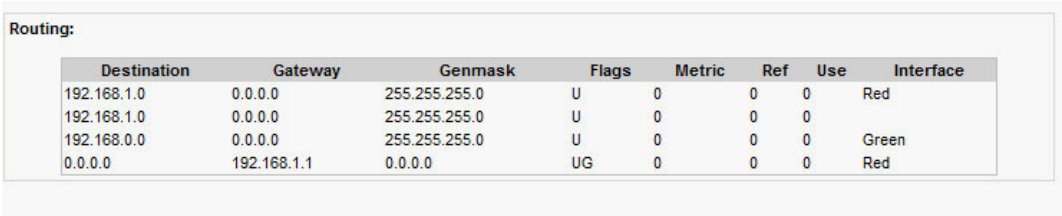


Kuva 15. Sisääntulevan liikenteen ohjaus palvelimen eri portteihin.



Kuva 16. Sallittujen palveluiden luettelo lähtevälle liikenteelle.

Kuvasta 17 nähdään Smoothwall-palomuurin reititystaulu. Reitystaulukosta nähdään sisäverkon eli greenin verkkoalue sekä ulkoverkon eli redin verkkoalue. Viimeisellä rivillä on palomuurin oletusreitti ulkoverkkoon.


Routing:

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	Red
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	Green
0.0.0.0	192.168.1.1	0.0.0.0	UG	0	0	0	Red

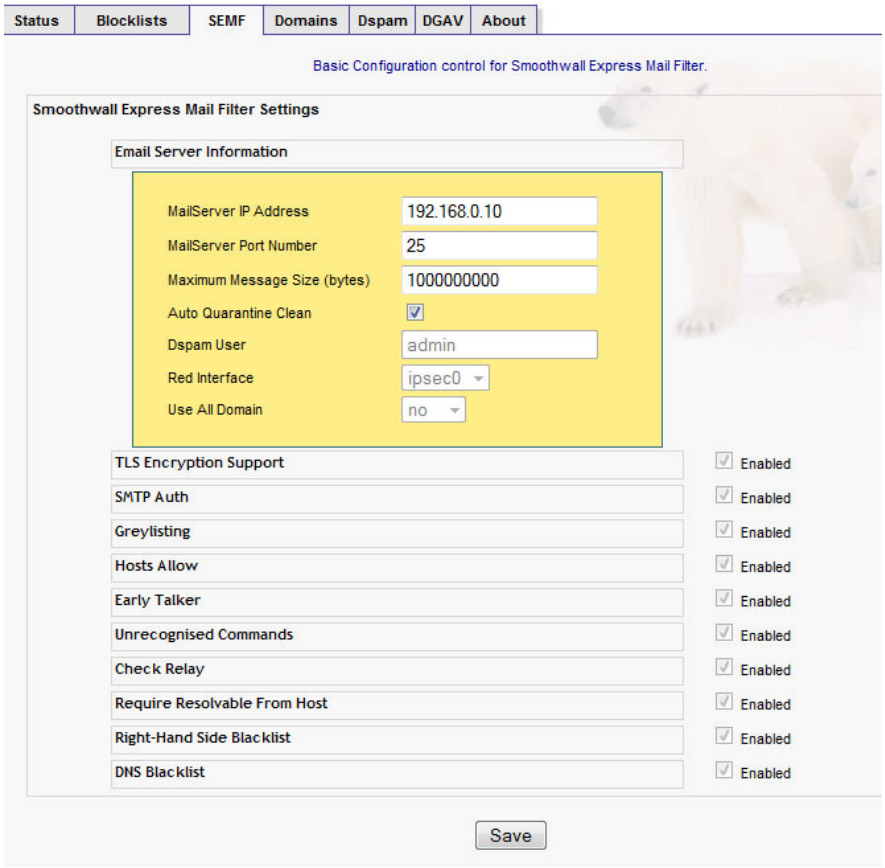
Kuva 17. Smoothwall-palomuurin reititystaulu.

Smoothwall-palomuuriin on myös mahdollista saada tehokas sisältösuodin. Sisältösuodin estää työntekijöiltä pääsyn niille Internet-sivustoille, joilla on raportoitu olevan haitallisia viruksia tai jotain muuta sellaista sisältöä, joka ei ole yrityksen politiikan mukaista. Sisältösuodin kantaa nimeä dansguardian, ja se on Smoothwallin ohella myös täysin ilmainen ohjelma. /17/

Sisältösuotimen ohella Smoothwall-palomuuriin voidaan asentaa lisäosana roskapostisuodin, joka kantaa nimeä SmoothWall Express Mail Filter, lyhyemmin SEMF. SEMF:n asennus kannattaa suorittaa, jos omassa yrityksen verkossa toimii oma sähköpostipalvelin. Kaikki sähköpostiliikenne, joka menee palomuurin kautta sähköpostipalvelimelle, käy ensin läpi tarkistuksen virusten ja roskapostien varalta, ennen kuin se välitetään palvelimelle. SEMF käyttää dspam-nimistä open source -ohjelmaa roskapostin suodatukseen. Virustentorjuntaohjelmana toimii Clam Antivirus ja se on integroituna palveluna sekä SEMFille että dansguardianille. Kun palomuuriin asennetaan roskapostifiltteri, ei SME-palvelimen tarvitse käyttää omaa roskapostiohjelmaansa. SEMFin konfiguroinnin vaiheet on esitettynä seuraavassa kappaleessa.

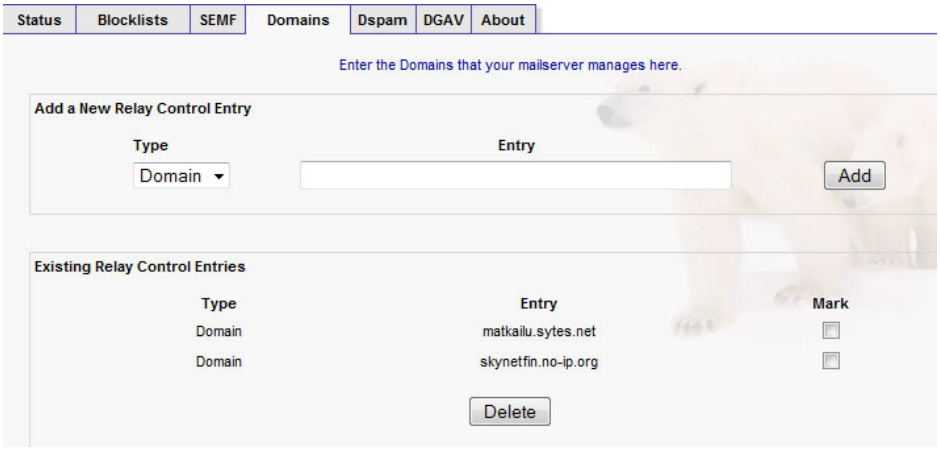
5.4.1 SmoothWall Express Mail Filterin konfiguroiminen

SEMF voidaan konfiguroida seuraavasti. Ensin asetetaan käytössä olevan sähköpostipalvelimen tiedot kuvan 18 kaltaisesti. Tietoihin liittyvät käytössä oleva SMTP-portti sekä palvelimen sisäverkon IP-osoite. Samalla asetetaan viesteille maksimikoko bitteinä. /20/



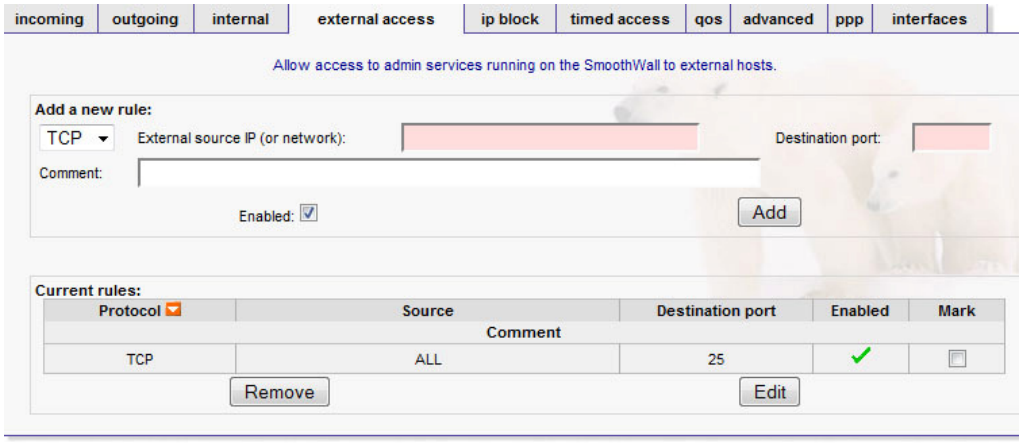
Kuva 18. Sähköpostipalvelimen tietojen asettaminen SEMFiin.

Kuvassa 19 asetetetaan kaikki sähköpostipalvelimella käytössä olevat domainit, tähän liitetään siis ensisijainen, virtuaaliset sekä kaikki alidomainit.



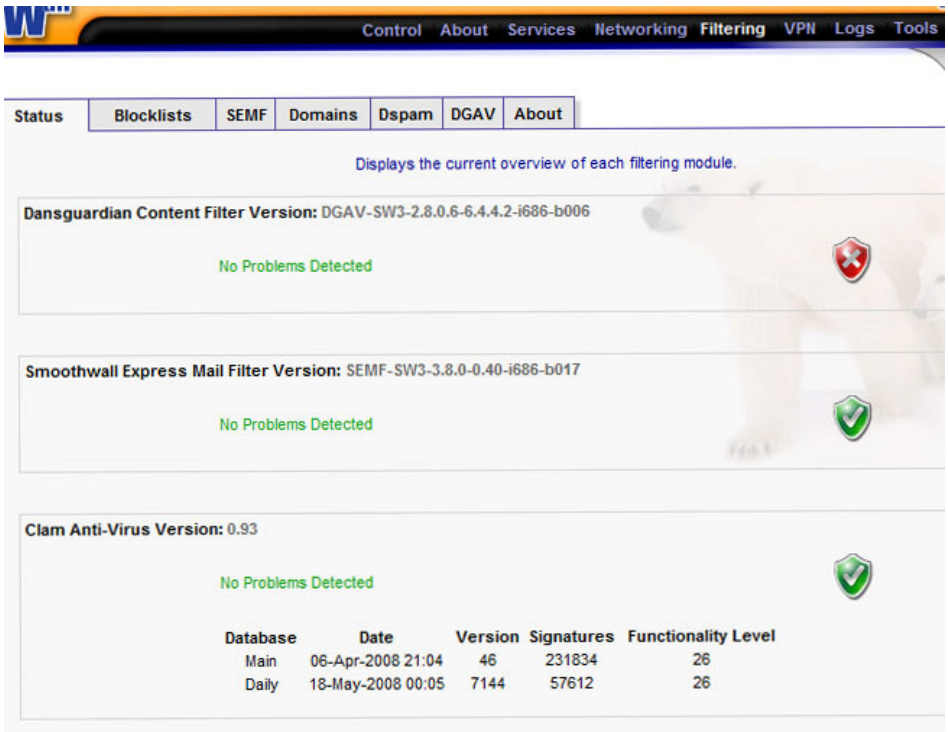
Kuva 19. Asetetaan sähköpostipalvelimella käytössä olevat domainit.

SEMF vaatii toimiakseen SMTP portin 25 auki ns. ulkopuolisesta verkosta, kuvan 20 tavalla. /20/



Kuva 20. Asetetaan SMTP-portti 25 päälle kohtaan external-access.

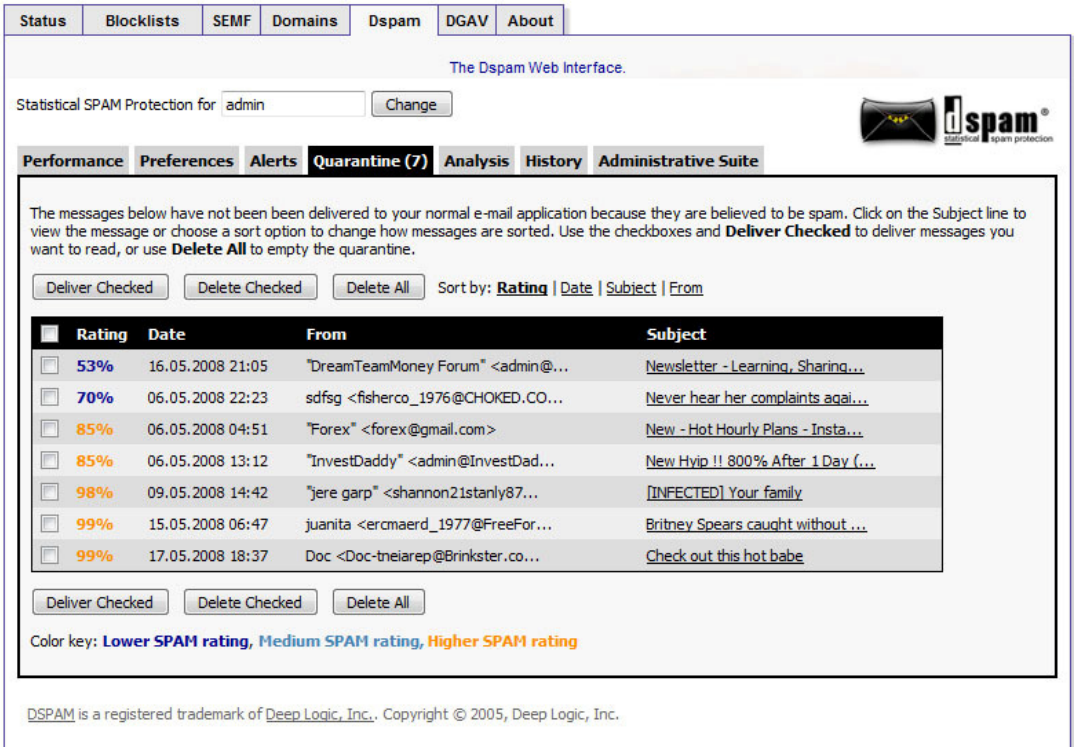
Lopuksi tarkistetaan SEMFin tila, eli onko se käynnissä, kuten kuvassa 21, jos ei, niin painetaan hiirellä kuvassa oikealla näkyvää ikonia



Kuva 21. SEMFin tila.

Nyt kaikki sähköpostipalvelimen kautta kulkevat viestit menevät SEMFin kautta. SEMF vaatii vähintään 200 viestiä ennen kuin sen todellinen toiminta alkaa. Hyvänä puolena on

sanottava se, että se ei kovin herkästi aseta oikeita sähköpostiviestejä roskapostiksi. Kaikki sähköpostit joissa on havaittu virus tai jotka ovat tunnistettu roskapostiksi, menevät karanteeni kansioon esimerkkikuvan 22 kaltaisesti. Oletusasetuksena nämä viestit eivät koskaan saavu käyttäjälle, ei edes erilliseen spam-kansioon, tämä auttaa myös omalta osaltaan Windows-työasemien tietoturvaa. Kuvasta 21 nähdään myös se, että SEMF asettaa tunnistetuille roskaposteille ja virusten sisältämille sähköposteille prosentuaaliset arvot vakavuusluokan mukaan. Jos jostain syystä jokin oikea viesti on mennyt karanteenikategoriaan, on se mahdollista palauttaa sieltä pois. Toistaiseksi näin ei ole käynyt kertaakaan viimeisen 3 kuukauden aikana.



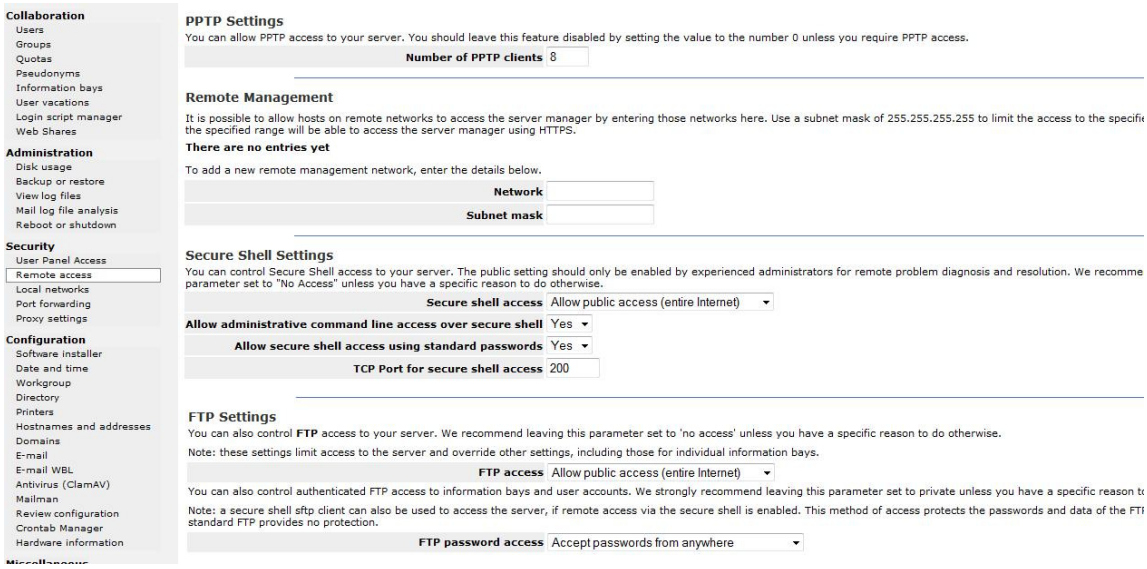
Kuva 22. SEMFin karanteeni-kansion roskapostilistaus.

5.5 Etäyhteyksien luonti

Etäyhteyksien luonti palvelimelle suoritetaan SSH-yhteyden kautta. Toki FTP-palvelunkin saa SME:ssä päälle, mutta SSH on huomattavasti turvallisempi vaihtoehto. Käytettävän SSH-portin voi itse määrätä niin, ettei sen tarvitse olla oletusportti 22. Yhteys palvelimen komentoriville voidaan suorittaan esimerkiksi Putty-nimisellä ohjelmalla ja tiedostojen kopioimisessa voidaan käyttää esimerkiksi Winscp-ohjelmaa. Palomuuriin

ei päästä käsiksi ulkoverkosta ssh-yhteyden kautta, ainoastaan sisäverkosta. Sekin on kyllä mahdollista, jos erikseen tehdään ns. tunnelointi palvelimen kautta tai vaihtoehtohtoisesti käytetään olemassa olevaa VPN-yhteyttä.

Kuvassa 23 on esitettynä server-managerin etähallintavalikko.Tämän valikon kautta luodaan VPN-yhteyksille maksimikäyttäjämäärä, joka on kuvassa 8 (PPTP asetukset). SSH-portiksi on asetettu 200 sekä FTP-portti 21 on myös aktivoitu niin, että sen kautta on pääsy palvelimelle. FTP-porttia ei voi muuttaa server-managerin kautta.



Kuva 23. Server-managerin etäyhteyksien hallinta.

5.6 Kokonaiskustannuksien arviointi

Kustannuslaskelman pohjana toimii kuvitteellinen tilitoimisto, joka on juuri aloittanut toimintansa. Tilitoimisto tarvitsee toimivan tietoliikennejärjestelmän. Järjestelmään kuuluu yksi palvelin (Linux SME), joka toimii sähköposti, web -ja tiedostopalvelimena. Internetnet-yhteyden muodostamiseen tarvitaan adsl-modeemi sekä erillinen palomuurilaitteisto (Smoothwall). Yrityksen verkkotopologiamalli tulee olemaan kappaleessa 5.1 esitetyn kuvan 5 kaltainen. Verkkoon liitetään kaksi 16-porttista kytkintä ja yksi langaton tukiasema. Tämän lisäksi tarvitaan 10 erillistä työasemaa sekä kaksi verkkotulostinta.

Laitteistoista aiheutuvat kustannukset on esitettynä taulukossa 6. Kustannuksiin on eritelty arvonlisäveron osuus, kappalemääräiset hinnat sekä kokonaiskustannukset. Pohja laitteistokuluille on otettu tietotekniikan tukkutoimittajan Techdatan sivuilta. Työn osuuden yksityiskohtainen erittely tuntimäärien ja kulujen mukaan on esitetty taulukossa 7. Taulukkoon 8 on eriteltynä lopulliset kokonaiskustannukset. Kustannuksiin on lisätty myös kustannusylitysvaraus, joka on 20 %. Työtuntimäärien arviointi saattaa usein olla hieman ongelmallista, koska asennusten yhteydessä tapahtuu aina jotain ennalta arvaamatonta. Siksi aikaa on hyvä varata hieman odotettua enemmän. Kokonaiskustannuksissa ei ole huomioitu kaapelointia, domainin rekisteröintiä ja Internet-yhteyden avausta. Nämä seikat on jätetty palveluntarjoajan suoritettaviksi.

Koska palvelintoteutus suoritetaan Linux SME:llä, vähenevät kokonaiskustannukset oleellisesti. Windows-palvelimen lisenssit tulevat maksamaan lähes yhtä paljon kuin varmuuskopiopalvelin kokonaisuudessaan, joten käyttämällä Linux-palvelinta saa yritys periaatteessa ilmaisen varmuuskopiopalvelimen. Vaihtoehtoisesti varmuuskopiopalvelimen voi jättää tulevaisuuden hankintasuunnitelmiin. Kustannuslaskelmissa sen osuus on esitetty mahdollisena optiona.

Taulukko 6. Laitteistoista aiheutuvat kustannukset.

	Tuotekuvaus	Kpl	Veroton kpl hinta	ALV 22%	verollinen kpl hinta	verollinen hinta yhteensä
Palvelinlaitteisto:						
Emolevy	Asus - ASUS M2N-X Plus - Kanta AM2 ja malli ATX - sis. Näytönohjaimen ja verkkokortin	1	43,2 €	12,2 €	55 €	55,4 €
Prosessori	AMD Athlon 64 X2 5000+ / 2.6GHz - 1MB (65W) socket AM2 kanta	1	71,6 €	20,2 €	92 €	91,8 €
RAM	Kingston - 1GB 667MHz - DDR2 Non-ECC CL5 DIMM	2	17,9 €	5,0 €	23 €	45,9 €
Kovalevyt (RAID 1) + Spare X 2	Western Digital - Caviar - SE/500GB SATA300 7200rpm 16MB	4	64,2 €	18,1 €	82 €	329,4 €
ATX - kotelo ja virtalähde	Antec New Solution NSK4480-EC - Minitorni, ATX - virtalähde 380 watt	1	63,2 €	17,8 €	81 €	81,0 €
USB-kotelo kovalevylle	SPIRE MegaPod III SATA	2	32,6 €	9,2 €	42 €	83,7 €
Palomuurilaitteisto:						
Emolevy	Pentium III -kantainen - sis. integroidun näytönohjaimen	1	15,8 €	4,5 €	20 €	20,3 €
Prosessori	Pentium III, 350Mhz	1	10,5 €	3,0 €	14 €	13,5 €
RAM	64Mt, SDRAM, yhteensä 256Mt	4	3,2 €	0,9 €	4 €	16,2 €
Kovalevy	10Gt, Ata-100	1	10,5 €	3,0 €	14 €	13,5 €
ATX - kotelo + virtalähde	ATX-kotelo (ei hienouksia), virtalähde 200	1	15,8 €	4,5 €	20 €	20,3 €
Verkkokortit	A-LINK NA110HR - PCI - EN, Fast EN - 10Base-T, 100Base-TX	2	5,6 €	1,6 €	7 €	14,3 €
Työasemat	Lenovo ThinkCentre A55 9265, työasema - Käyttöjärjestelmä Windows Xp Pro	10	358,0 €	101,0 €	459 €	4 590,0 €
Näytöt	Viewsonic - ViewSonic VA926 - Litteä paneelinäyttö - TFT - 19"	10	170,2 €	48,0 €	218 €	2 181,6 €
Verkkotulostimet	Canon - Canon i-SENSYS LBP3360 - Laser-Tulostin - mustavalkoinen - USB, 10/100Base-TX	1	296,9 €	83,8 €	381 €	380,7 €
	Canon - Canon i-SENSYS LBP5300 - Laser-Tulostin - väri - USB, 10/100Base-TX	1	863,5 €	243,5 €	1 107 €	1 107,0 €
Adsl-modeemi	ZyXEL Prestige 870M-I1 v2 - DSL modeemi,ulkoinen - Fast Ethernet, ethernet over VDSL	1	61,1 €	17,2 €	78 €	78,3 €
Kytkin	D-Link DES 1016D - Kytkin 16 porttia - Fast EN - 10Base-T, 100Base-TX	2	68,4 €	19,3 €	88 €	175,5 €
Langaton access-point	ZyXEL ZyAIR G-570S v2, Langaton liityntäpiste -802.11b, 802.11g, 802.11 Super G	1	78,4 €	22,1 €	101 €	100,6 €
OPTIOT:						
Varmuuskopiopalvelin:						
Emolevy	Asus - ASUS M2N-X Plus - Kanta AM2 ja malli ATX - sis. Näytönohjaimen ja verkkokortin	1	43,2 €	12,2 €	55 €	55,4 €
Prosessori	AMD - Athlon 64 X2 5000+ / 2.6GHz 1MB (65W) socket AM2 kanta	1	71,6 €	20,2 €	92 €	91,8 €
RAM	Kingston - 1GB 667MHz DDR2 Non-ECC CL5 DIMM	2	17,9 €	5,0 €	23 €	45,9 €
Kovalevyt (RAID 1)	Western Digital - Caviar -GP/1TB SATA300 7200rpm 16MB	2	155,8 €	44,0 €	200 €	399,6 €
ATX - kotelo ja virtalähde	Antec New Solution NSK4480-EC - Minitorni,ATX - virtalähde 380 watt	1	63,2 €	17,8 €	81 €	81,0 €
				ALV:n osuus 22%	Veroton kokonaishinta	Verollinen kokonaishinta
KAIKKI YHTEENSÄ ILMAN OPTIOITA				2 067,7 €	7 331,1 €	9 398,8 €
KAIKKI YHTEENSÄ OPTIOIDEN KANSSA				2 215,9 €	7 856,5 €	10 072,5 €

Taulukko 7. Laskennallinen kustannusarvio työn osuudelle.

Työn osuus:	Arvioitu tuntimäärä	Veroton hinta / h	ALV 22%	Verollinen hinta / h	Yhteensä
Palvelimen kokoaminen ja asennus sekä Varmuuskopiointijärjestelmän luominen	2	39 €	11 €	50 €	100 €
Palomuurin kokoaminen ja asennus	1	39 €	11 €	50 €	50 €
Palomuurin konfigurointi sekä tarvittavien porttiohjausten muodostaminen reitittimelle ja palomuurille	2	39 €	11 €	50 €	100 €
Palvelimen konfigurointi:					
Käyttäjien ja ryhmien lisäys palvelimelle	2	39 €	11 €	50 €	100 €
Sähköpostipalvelin	1	39 €	11 €	50 €	50 €
Roskapostisuodin	2	39 €	11 €	50 €	100 €
Internetsivujen siirto webpalvelimelle	1	39 €	11 €	50 €	50 €
Tiedostopalvelimen kirjautumisajoitukset	1	39 €	11 €	50 €	50 €
Keskitettyjen verkko-ohjelmien asennus Esim. Passeli pro, openoffice, verkkotulostin jne.	8	39 €	11 €	50 €	400 €
Työasemakohtaiset asennukset:					
Käyttöjärjestelmien asennukset	10	39 €	11 €	50 €	500 €
Työasemien yhdistäminen toimialueeseen ja domain-oikeuksien asettaminen paikalliselle koneelle	5	39 €	11 €	50 €	250 €
Ohjelmisto, laite -ja ajuriasennukset	5	39 €	11 €	50 €	250 €
Mahdolliset optiot:	Arvioitu tuntimäärä	Veroton hinta / h	ALV 22%	Verollinen hinta / h	Yhteensä
Varmuuskopiointipalvelin:					
Asennus ja kokoaminen	2	39 €	11 €	50 €	100 €
Konfigurointi	8	39 €	11 €	50 €	400 €
	Tuntimäärä yht.		ALV:n osuus	Veroton kokonaishinta	Verollinen kokonaishinta
Työ yhteensä ilman optioita:	40		440 €	1 560 €	2 000 €
Työ yhteensä optioiden kanssa	50		550 €	1 950 €	2 500 €

Taulukko 8. Kokonaiskustannusten yhteenveto.

	Veroton hinta	ALV:n osuus	Verollinen hinta
Palvelinlaitteisto	536 €	151 €	687 €
Palomuurilaitteisto	76 €	22 €	98 €
Muut laitteistot ja ohjelmat	6 719 €	1 895 €	8 614 €
Työn osuus	1 560 €	440 €	2 000 €
Kaikki yhteensä	**8 891 €**	**2 508 €**	**11 399 €**
Kustannusylitysvaraus 20%	10 669 €	3 009 €	13 679 €
Optioiden kanssa	**9 807 €**	**2 766 €**	**12 572 €**
Kustannusylitysvaraus 20%	11 768 €	3 319 €	15 087 €

6 Päätelmät

Linux SME-palvelimen asentaminen, konfiguroiminen ja käyttö osoittautui huomattavasti helpommaksi, kuin olin alun perin ajatellut. Toisaalta SME antaa Linux-palvelimista hieman väärän kuvan, koska se on suunniteltu täysin valmiiksi paketiksi. Moni palvelu on heti asennuksen jälkeen automaattisesti käytössä, kuten esimerkiksi ohjelmallinen RAID. Eri palvelujen konfiguroiminen on myös erittäin vaivatonta, suuri kiiitos tästä kuuluu SME-palvelimen omalle tukisivustolle wiki.contribs.org, jossa suurin osa asioista on selitettynä. Lisäksi myös SME:n oman tukisivuston forumin kautta on mahdollista saada apua ongelmatilanteissa. Erilaisten lisäohjelmien asennus ei aina ole täysin suotavaa. Tämä johtuu siitä että useat lisäosat ovat täysin irrallisia ohjelmia, jotka eivät liity ns. virallisena standardina alkuperäiseen järjestelmään. Vaikka jokin lisäohjelma toimisikin hyvin, ei ole mitään takeita siitä mitä tapahtuu seuraavien palvelinpäivitysten jälkeen. Ainoastaan virallisten ohjelmistolaajennusten asennus on suotavaa. Heikkoutena SME:ssä on web-palvelin. Uusien Internet-sivujen liittäminen SME:n on todella vaivatonta mutta suurimmat hankaluudet tulee vastaan mysql-tietokantapalvelimen kanssa. Tietokantaan ei ole olemassa erillistä hallintapaneelia, vaan kaikki kantojen lisäykset sekä käyttäjäkohtaiset oikeudet on tehtävä komentorivin kautta. Silti kokonaisuutena SME on erinomainen palvelinjärjestelmä.

Smoothwall osoittautui todella hyväksi palomuurijärjestelmäksi. Sen ominaisuudet vastaavat hyvin pk-yritysten tarvetta. Konfigurointikin on suhteellisen helppoa jos ymmärtää kaikki perusasiat liittyen verkkoliikenteeseen, edes yleisellä tasolla. Laitteiston osalta suuria vaatimuksia ei ole, ainoastaan RAM-muistin määrä osoittautui kaikkein merkittävimmäksi tekijäksi.

Kaiken kaikkiaan tietoliikennejärjestelmän toteuttaminen on hyvin moniosainen prosessi. Siihen liittyy palvelimen ja palomuurin lisäksi paljon muitakin asioita. Pääpaino toteutuksessa liittyi lähinnä palvelinympäristön puolelle sekä Linux-järjelmien konfigurointiin. Otin työssä myös esille erilaisia vaihtoehtoisia ratkaisumalleja, koska yksi malli ei aina sovellu kaikkiin tilanteisiin. Kustannuslaskelman osalta on esimerkkiyrityksen avulla otettu kantaa siihen, mitä kaikkia asioita liittyy koko järjestelmän toteutukseen. Koko projektin kokonaisaika ja kustannukset ovat aina paljolti kiinni siitä, mitä eri asioita yri-

tys omaan tietoliikenneympäristöön haluaa. Kokemuksen kautta syntyy kuitenkin melko tarkka kuva siitä, kauanko koko projekti tulee kestämään ja kuinka paljon se tulee lopulta yritykselle maksamaan.

Omalta osaltani olen erittäin tyytyväinen lopputulokseen. Työ toi mukanaan paljon Linux-järjestelmiin liittyvää järjestelmäasiantuntemusta sekä äärettömän hyödyllistä tietotaitoa. Toteutus palvelimen ja palomuurin osalta onnistui lähes täydellisesti. Suuria ongelmia ei tullut missään vaiheessa vastaan. Päättötyön toteustuspuolta edesauttoi se, että sain harjoittelupaikkani kautta myös todellista kokemusta, toteuttamalla Linux-järjestelmiä oikeisiin yrityksiin.

LÄHTEET

Sähköiset lähteet

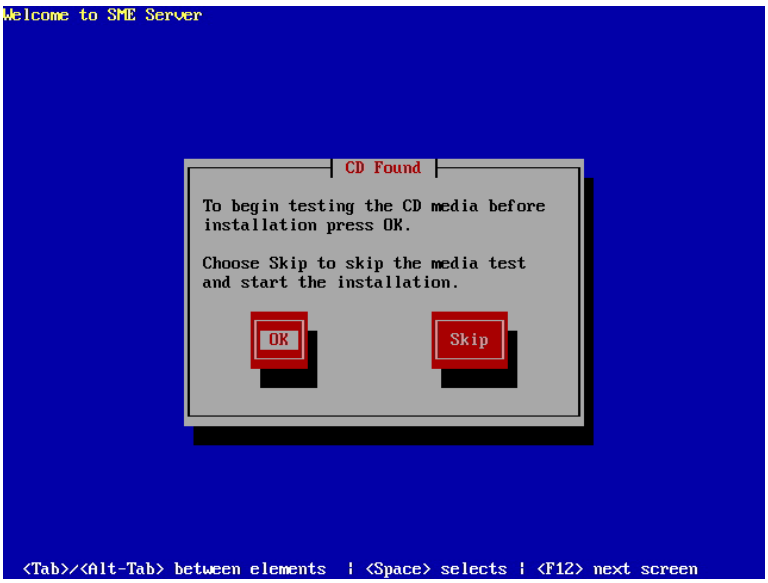
1 Tapani Räikkönen [www-sivu]. [viitattu 1.3.2008]
Saatavissa: http://linux.ilmainen.net
2 Filesystem Hierarchy Standard [www-sivu]. [viitattu 1.3.2008]
Saatavissa: http://www.pathname.com/fhs/pub/fhs-2.3.html#INTRODUCTION
3 linuxmafia [www-sivu]. [viitattu 10.3.2008]
Saatavissa: http://linuxmafia.com/faq/Hardware/sata.html
4 Linux.fi [www-sivu]. [viitattu 27.3.2008]
Saatavissa: http://linux.fi/index.php/Ohjelmistopohjainen_RAID
5 Linux.fi [www-sivu]. [viitattu 28.3.2008]
Saatavissa: http://linux.fi/index.php/RAID
6 SME Server inc. [www-sivu]. [viitattu 1.4.2008]
Saatavissa: http://wiki.contribs.org/Main_Page
7 Greeknet.us [www-sivu]. [viitattu 4.4.2008]
Saatavissa: http://greeknet.us/index.php?option=com_content&task=view&id=14&Itemid=32
8 Wikipedia[www-sivu]. [viitattu 10.4.2008]
Saatavissa: http://en.wikipedia.org/wiki/Small_and_medium_enterprise
9 Linux.fi [www-sivu]. [viitattu 16.4.2008]
Saatavissa: http://linux.fi/index.php/NAT
10 Wikipedia [www-sivu]. [viitattu 20.4.2008]
Saatavissa: http://fi.wikipedia.org/wiki/Osoitteenmuunnos
11 SME Server inc [www-sivu]. [viitattu 20.4.2008]
Saatavissa: http://wiki.contribs.org/SME_Server:Documentation :FAQ#Password_Strength_Checking
12 SME Server inc [www-sivu]. [viitattu 22.4.2008]
Saatavissa: Http://wiki.contribs.org/SME_Server:Documentation:Administration_Manual:Chapter14
13 No-ip.com [www-sivu]. [viitattu 23.4.2008]
Saatavissa: http://www.no-Ip.com/services/managed_dns/free_dynamic_dns.html
14 SME Server inc [www-sivu]. [viitattu 26.4.2008]
Saatavissa: http://wiki.contribs.org/Email
15 Wikipedia [www-sivu]. [viitattu 1.5.2008]
Saatavissa: http://en.wikipedia.org/wiki/Qmail
16 SME Server inc [www-sivu]. [viitattu 4.5.2008]
Saatavissa: http://wiki.contribs.org/MySQL
17 Dansguardian [www-sivu]. [viitattu 10.5.2008]
Saatavissa: http://dansguardian.org/?page=whatisdg
18 SME Server inc [www-sivu]. [viitattu 12.5.2008]
Saatavissa: http://wiki.contribs.org/Affa
19 SME Server inc [www-sivu]. [viitattu 15.5.2008]
Saatavissa: http://wiki.contribs.org/Moodle
20 Smoothwall community [www-sivu]. [viitattu 18.5.2008]
Saatavissa: http://community.smoothwall.org/forum/viewtopic.php?f=50&t=28227
21 Wikipedia [www-sivu]. [viitattu 30.5.2008]
Saatavissa: http://fi.wikipedia.org/wiki/Samba_(ohjelmisto)

LIITE 1

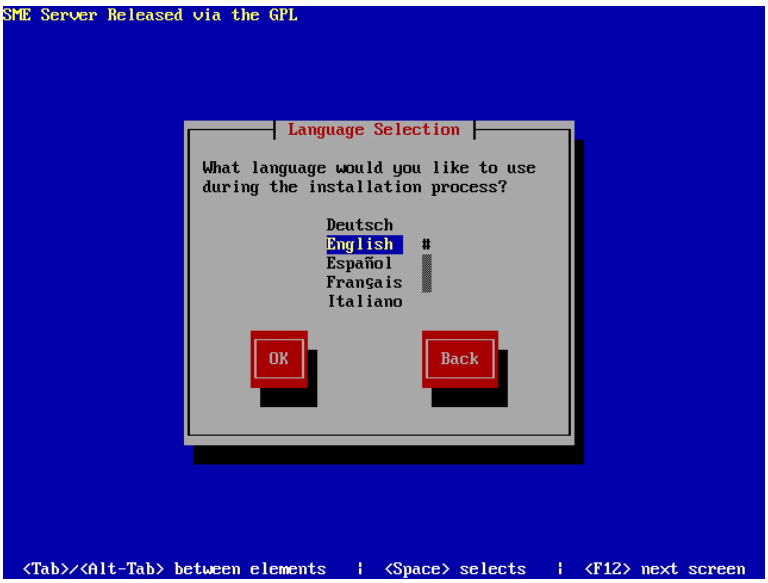
Sme-palvelimen asennus vaihe vaiheelta

Vaihe 1: Laitetaan SME:n asennuslevy cd-asemaan ja käynnistetään kone cd:tä

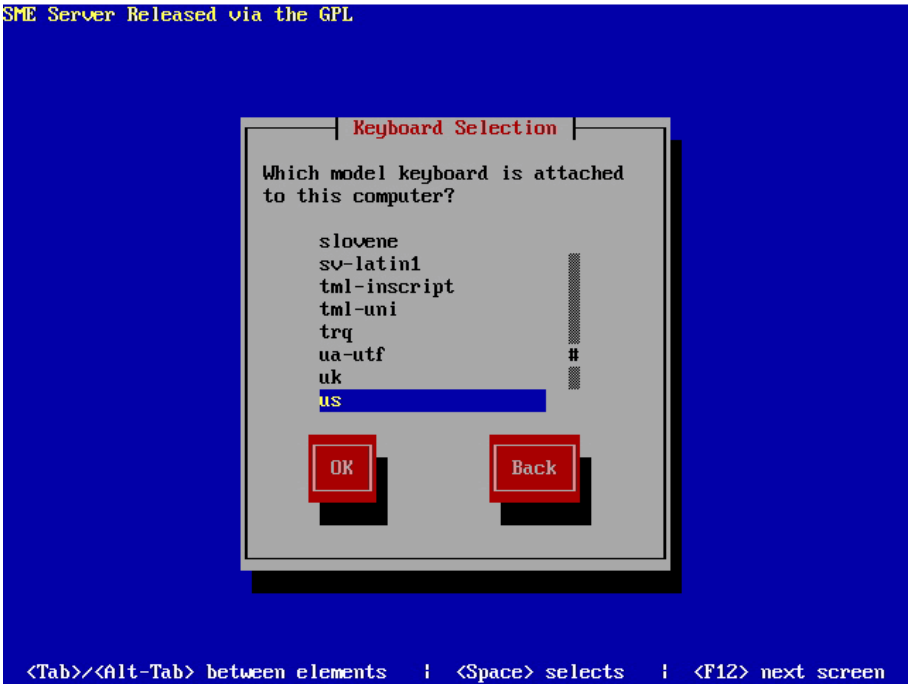
Vaihe 2: Voidaan seuraavan kuvan mukaisesti ensin testata CD:llä olevat mediat ennen varsinaista asennusta. Tämä vaihe on mahdollista myös ohittaa.



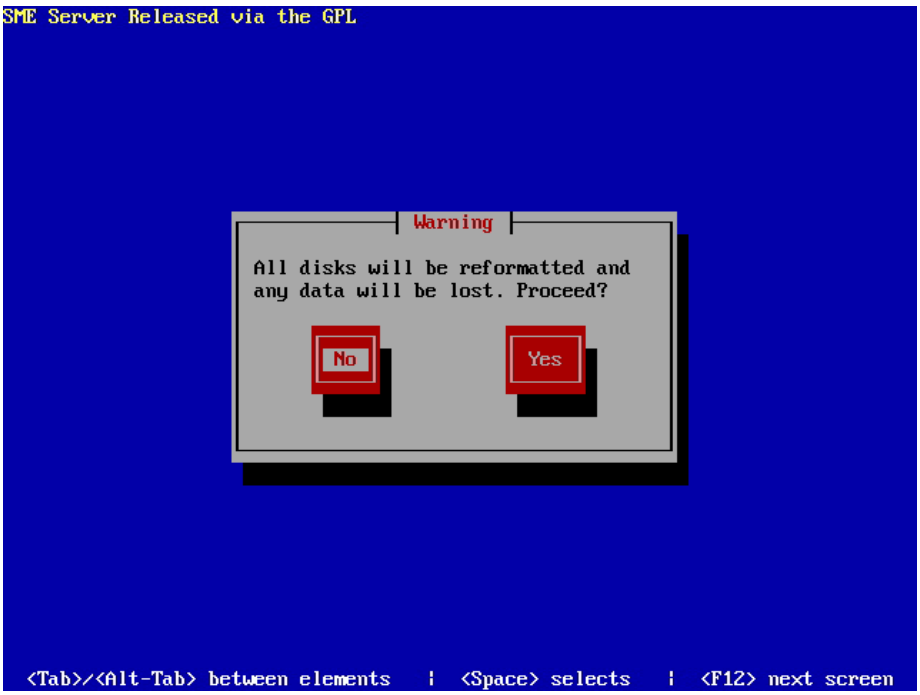
Vaihe 3: Valitaan asennuksen yhteydessä käytettävä kieli.



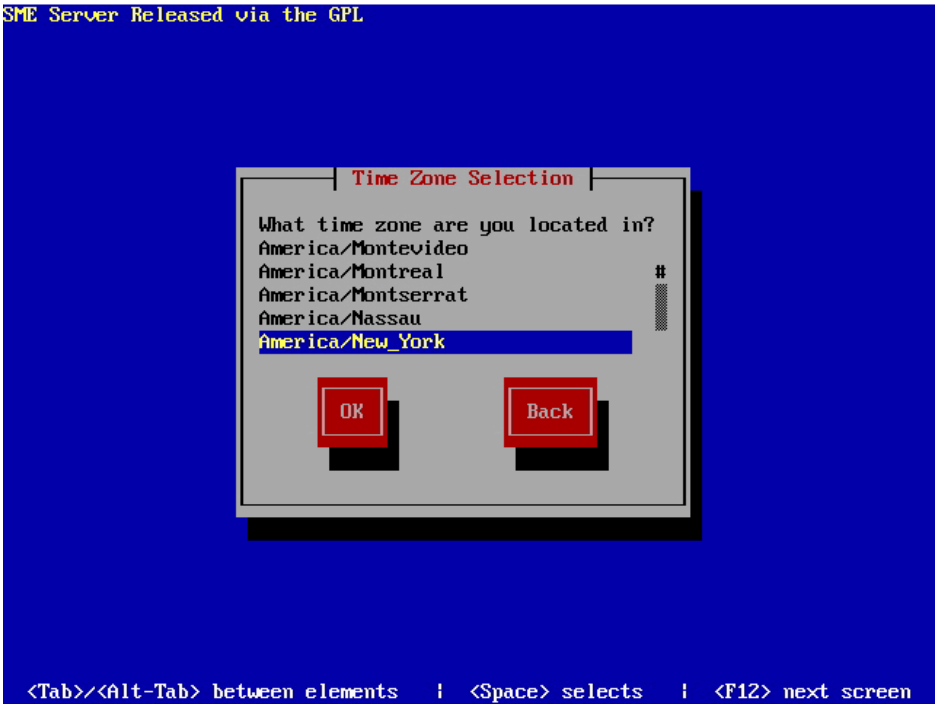
Vaihe 4: Valitaan näppäimistölle käytettävä kieli (fi).



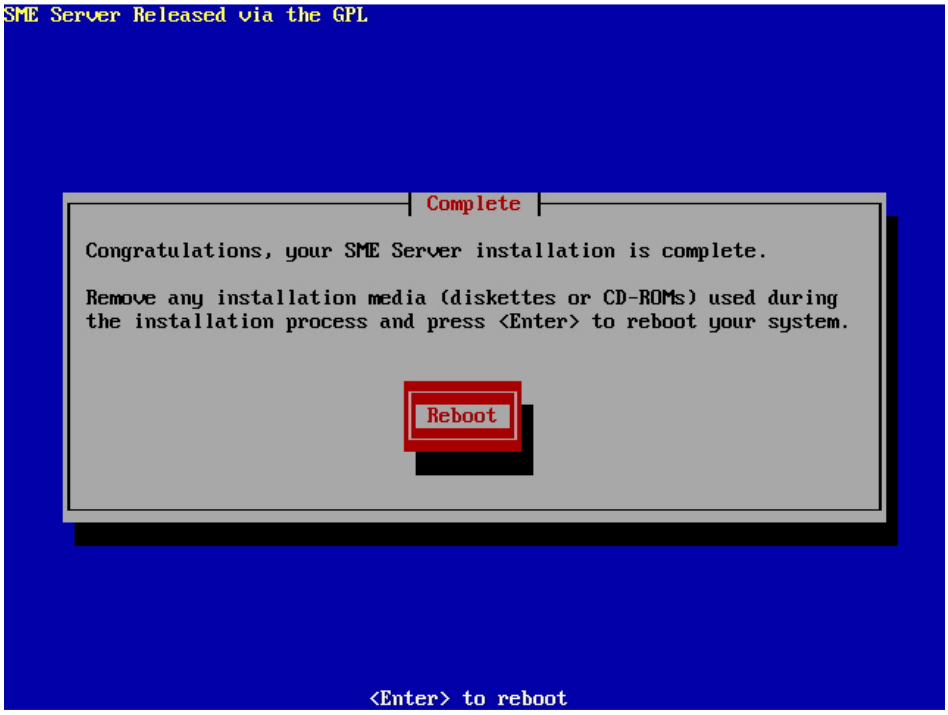
Vaihe 5: Tässä vaiheessa varmistetaan, että käyttäjä varmasti haluaa formatoida ja poistaa kaikki olemassa olevat tiedot kovalevyiltä.



Vaihe 6: Valitaan aikavyöhyke, joka on suomessa GMT+2.



Vaihe 7: Lopuksi tulee ilmoitus asennuksen onnistuneesta lopputuloksesta, minkä jälkeen järjestelmä käynnistetään uudelleen.

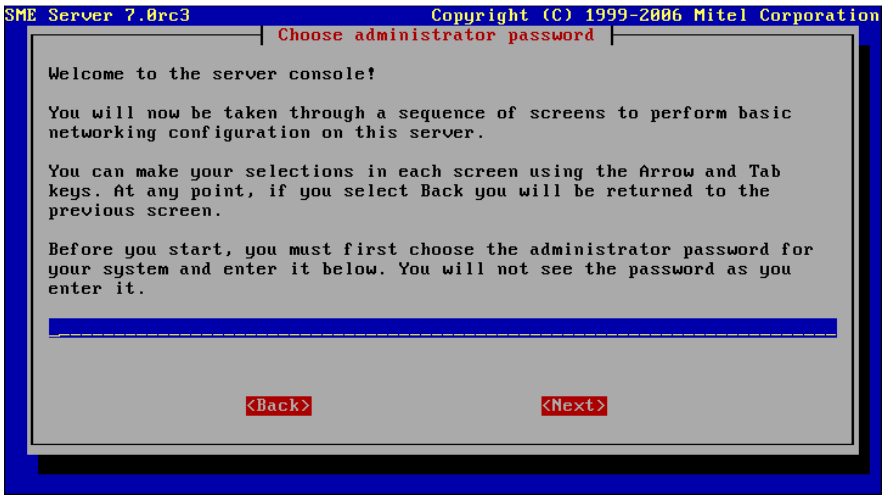


SME-palvelimen asennuksen jälkeinen konfigurointi

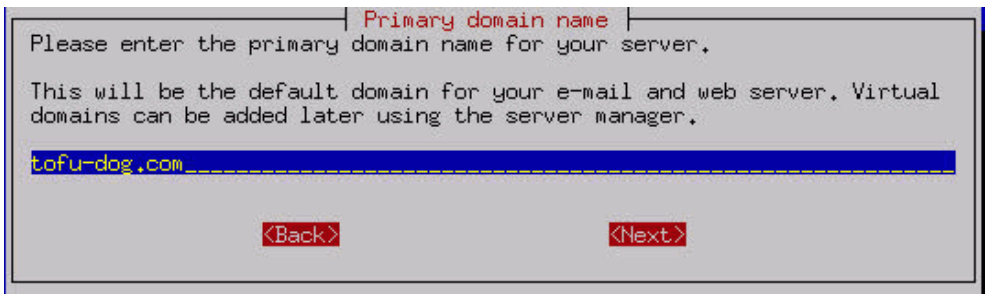
Kun asennus on suoritettu ja järjestelmä uudelleen käynnistetty, tehdään palvelimeen perusasetukset kuntoon.

Seuraavassa on esitetty perusasetusten konfigurointi vaihe vaiheelta.

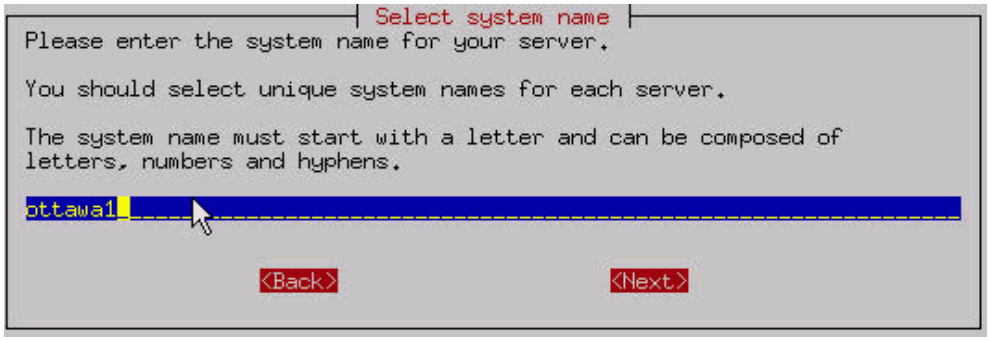
Vaiheessa 1 asetetaan järjestelmänvalvojan salasana (ks. kuva 5). Sama salasana tulee automaattisesti käyttöön myös rootille.



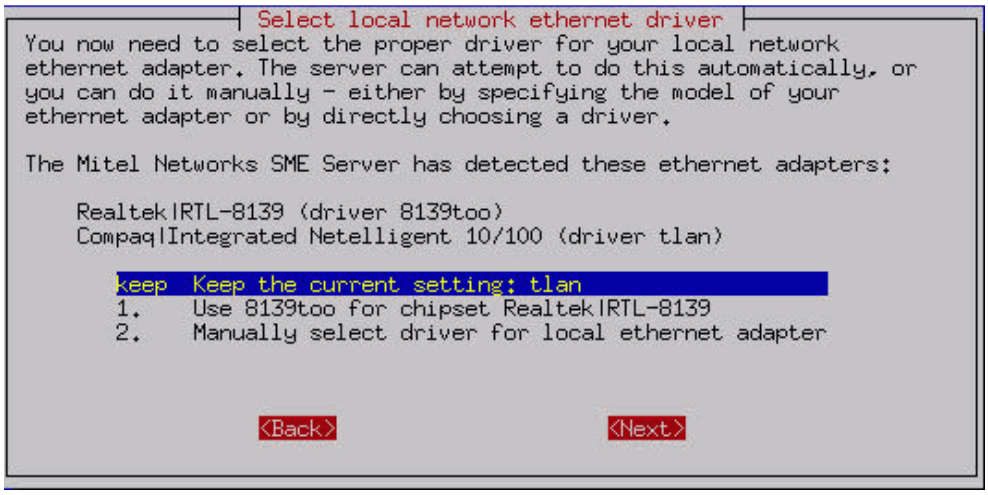
Toisessa vaiheessa asetetaan haluttu domain (ks. kuva 6). Tämä domain täytyy myöhemmin rekisteröidä, jos sitä halutaan käyttää julkisessa verkossa. Tämän takia, täytyy ensin varmistaa se, ettei kyseinen domain ole jo käytössä. Myöhemmin voidaan server-managerin kautta lisätä useita virtuaali-domaineja, jotka kaikki kohdistuvat tähän pää-domainiin.



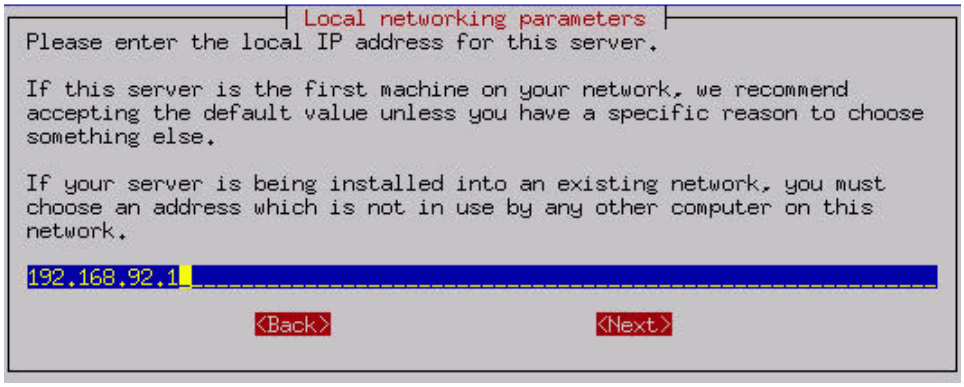
Vaiheessa 3 annetaan haluttu nimi järjestelmälle (ks. kuva 7). Tämä nimi näkyy vain yrityksen omassa verkossa.



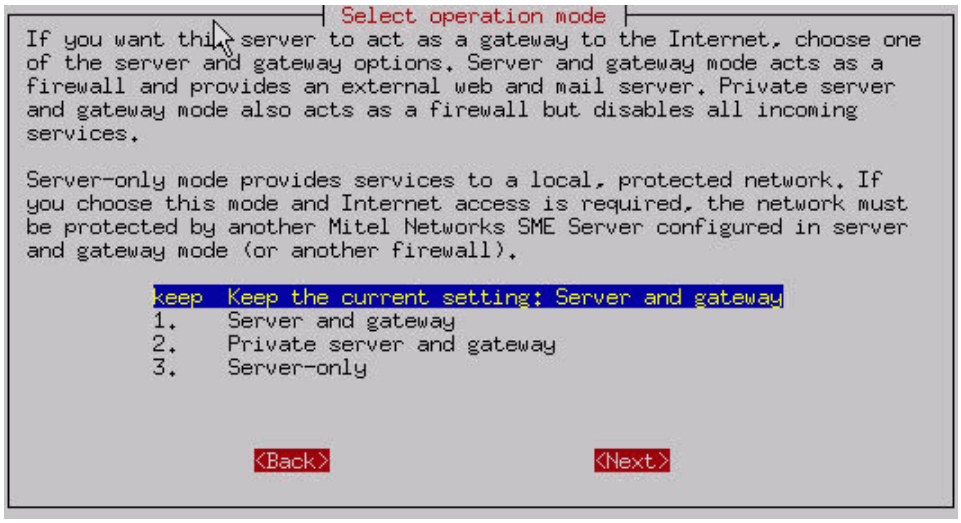
Tässä vaiheessa valitaan käytettävissä olevan verkkokortin ajurit (ks. kuva 8). Ajurit voidaan hakea automaattisesti tai manuaalisesti. Manuaalista vaihtoehtoa kannattaa käyttää silloin, jos automaattinen toiminto ei osaa hakea oikeita ajureita.



Vaiheessa 5 annetaan palvelimelle staattinen sisäverkon IP-osoite (ks. kuva 9). IP-osoite on tässä tapauksessa yleensä harmaan sarjan osoite, jonka reititin tai laajakaistamodeemi jakaa DHCP:ltä suoraan työasemille. Tällöin täytyy olla varma siitä, ettei sama IP-osoite ole yhdelläkään työasemalla jo käytössä. Palvelimen käyttämä IP-osoite tulisi myös asettaa reitittimelle tai laajakaistamodeemille staattiseksi, ettei jokin muu laite tai työasema saa sitä käyttöönsä koskaan.



Tässä vaiheessa valitaan servelille oma rooli.

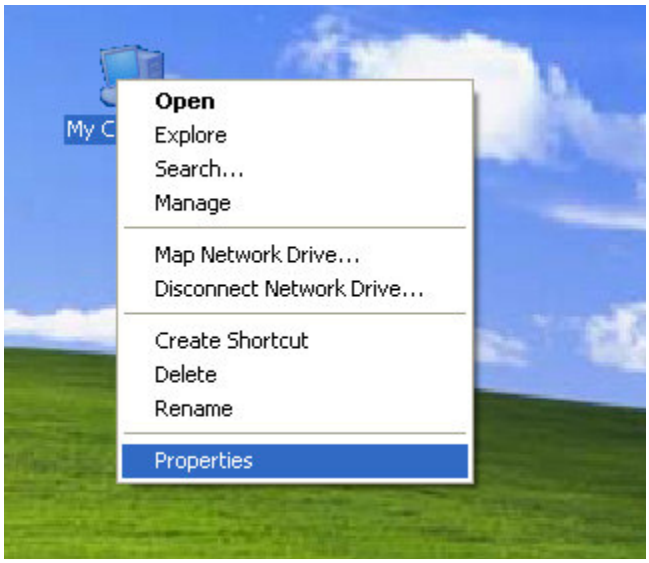


Kun valittuna tässä tapauksessa on server-only mode, voidaan DNS-asetus jättää tyhjäksi, koska palvelin saa DNS-palvelimen asetutukset automaattisesti reitittimen tai laajakaistamodeemin kautta. Lopuksi palvelin vaatiin ns. reconfigure-käynnistyksen, jotta tehdyt asetukset astuvat voimaan. Kun uudelleen käynnistys on suoritettu, voidaan Internet-yhteyttä testata server-console-valikon kautta.

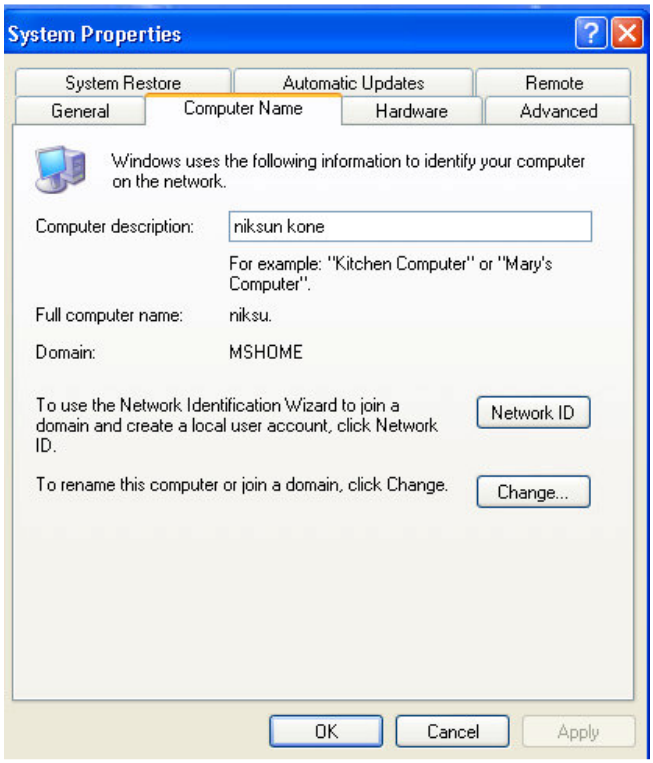
LIITE 2

Tietokoneen yhdistäminen domainiin
Käyttöjärjestelmänä Windows Xp Professional (eng ja fin)

Vaihe1: Valitaan hiiren oikealla painikkeella oma tietokone → ominaisuudet.

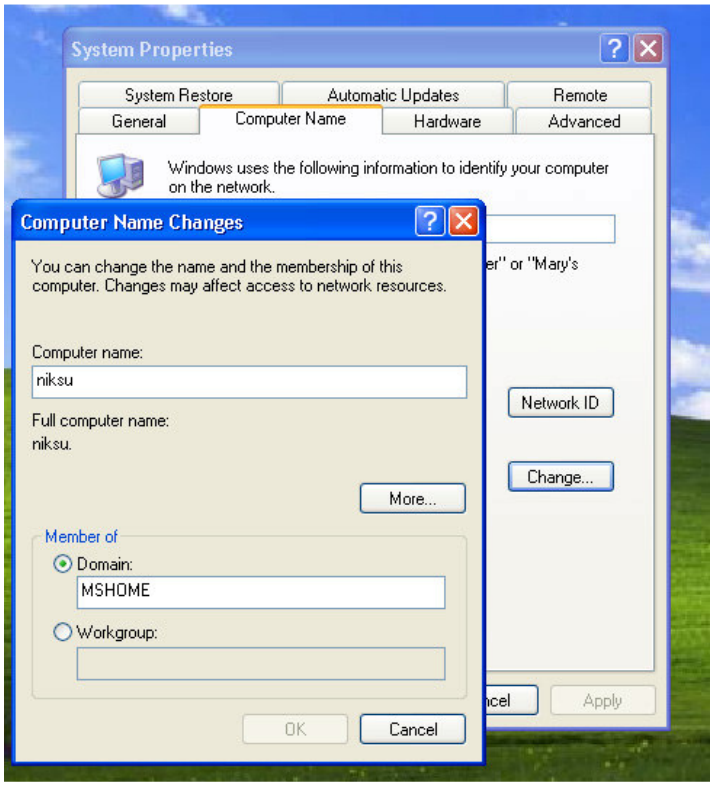


Vaihe 2: Valitaan välilehti ”tietokoneen nimi” aktiiviseksi.

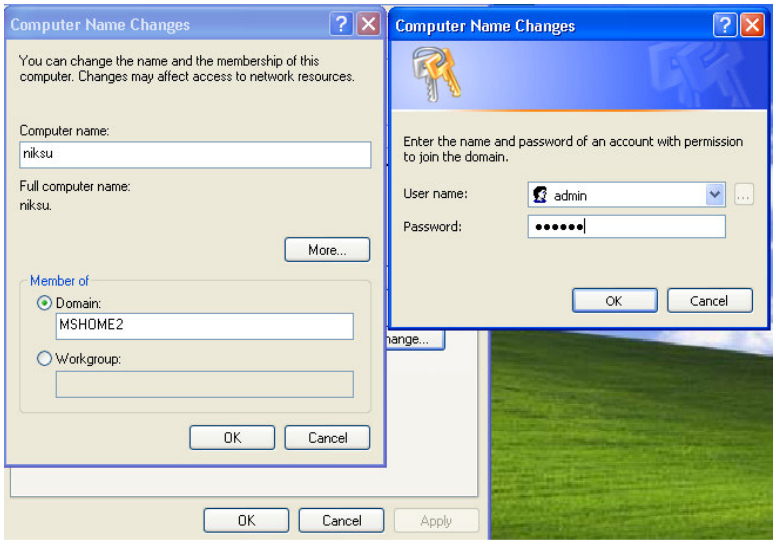


Vaihe 3: Tietokoneen nimi välilehdeltä valitaan kohta vaihda.

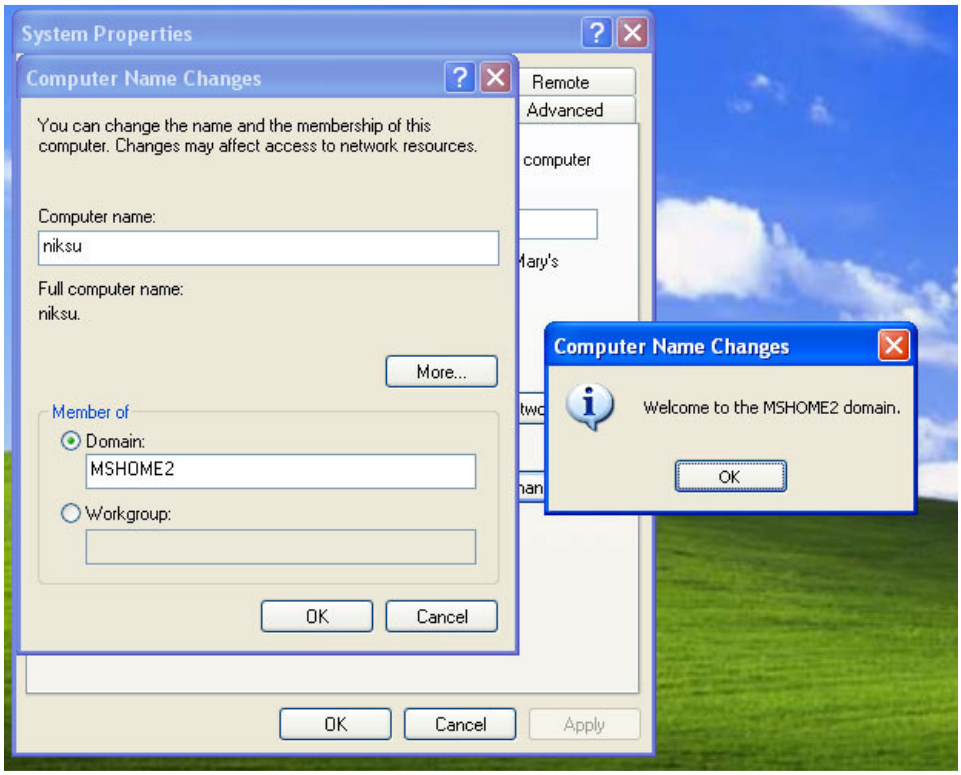
Tässä vaiheessa domain kohtaan kirjoitetaan palvelimelle asetettu työryhmä.



Vaihe 4: Tässä vaiheessa asetetaan järjestelmänvalvojan tunnukset palvelimelle.



Vaihe 5: Kun domainiin kirjautuminen onnistuu, seuraavanlainen kuvake ilmestyy.



.

Tässä vaiheessa tietokone on käynnistettävä uudelleen, jotta asetukset tulevat voimaan. Uudelleen käynnistämisen jälkeen on kuitenkin ensin kirjauduttava paikallisena käyttäjänä ja järjestelmänvalvojan oikeuksilla, jos halutaan vaihtaa domain-käyttäjien oikeuksia paikalliselle tietokoneelle.

Palomuuriohjelmat saattavat estää domainiin kirjautumisen, joten jos kirjautuminen epäonnistuu, niin kannattaa palomuuriohjelma ottaa hetkeksi pois päältä. Vaihtoehtoisesti palomuuriohjelmaan voidaan luoda sääntö, joka sallii kirjautumisen.

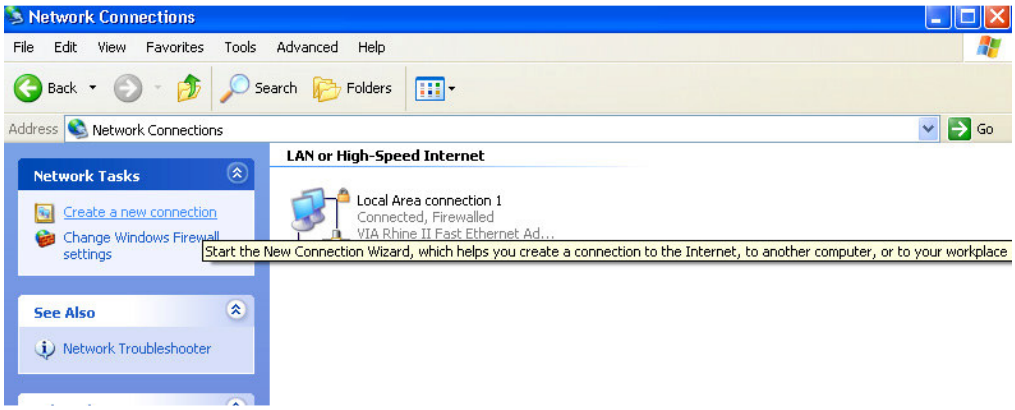
LIITE 3

VPN yhteyden muodostaminen palvelimelle

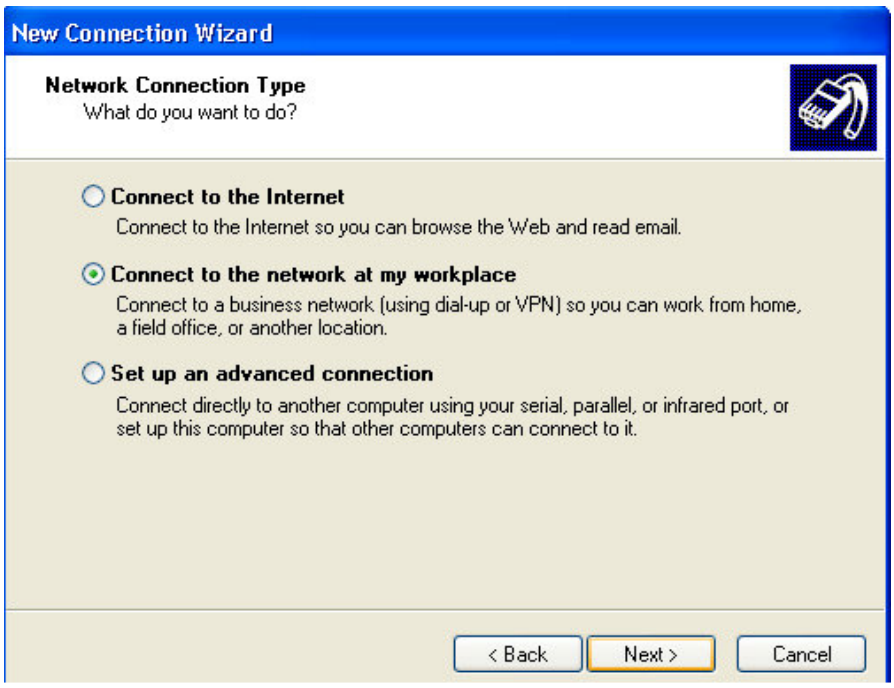
Käyttäjärjestelmänä Windows Xp Pro

VPN-yhteyden luominen ulkoverkosta palvelimelle.

Vaihe 1: Ohjauspaneeli → verkkoyhteydet → lisää uusi verkkoyhteys.

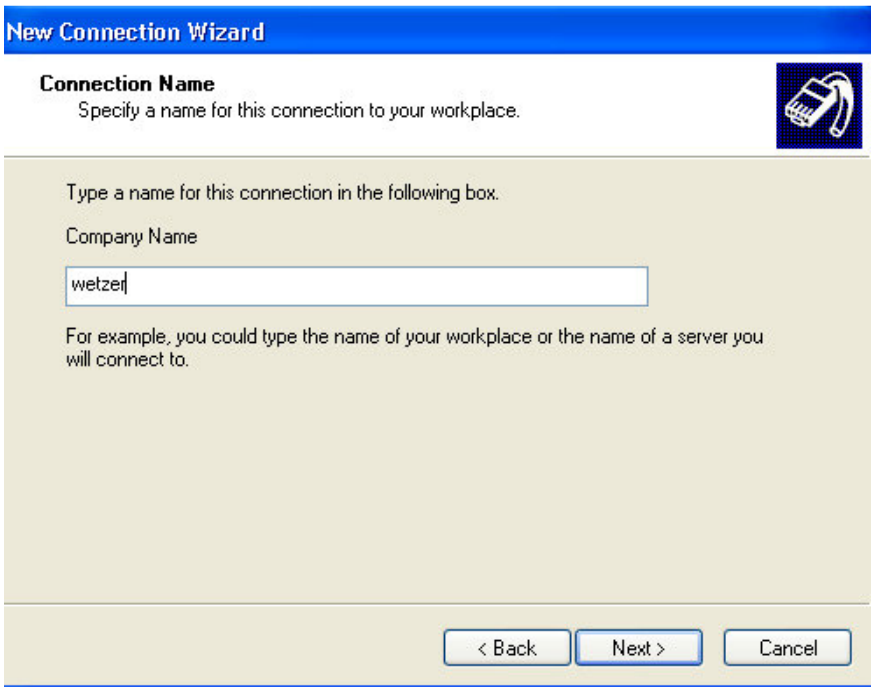


Vaihe 2: Yhdistä työaseman verkkoon.



Vaihe 3: Valitaan VPN-yhteys.

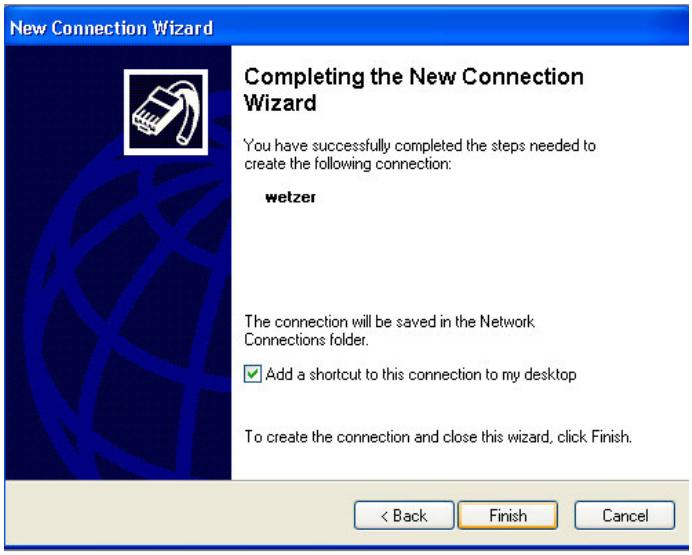
Vaihe 4: Annetaan yrityksen nimi (voidaan kirjoittaa mitä vain).



Vaihe 5: Annetaan palvelimen julkinen IP-osoite tai domain.

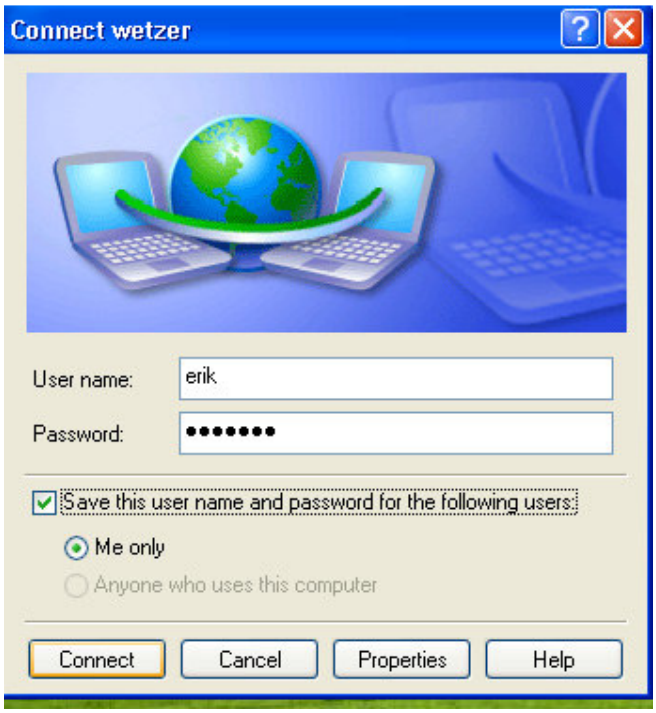
Vaihe 6: Valitaan yhteys vain omaan käyttöön.

Vaihe 7: Ruksi kohtaan lisää työpöydälle pikakuvake.



Vaihe 8: Annetaan käyttäjänimi ja salasana.

Haluttaessa ne voidaan tallentaa oman profiilin muistiin.



Mikäli portti 1723 on ohjattuna laajakaistamodeemin tai palomuurin kautta palvelimen
sisäverkon ip-osoitteeseen, saadaan yhteys onnistuneesti suoritettua.

LIITE 4

Varmuuskopio-ohjelman usb_backup.sh koodi

```
#!/bin/bash
###
### chmod +x usb_backup.sh antaa tälle scriptille suoritusoikeuden
###
### varmuuskopioidaan koko levy rsynciä käyttäen ulkoiselle usb kiintolevylle
### Ennen kuin tästä on apua pitää ottaa kopio dd:llä master levystä usb
### levylle, muuten varalevy ei buuttaa
### esim. komennolla dd if=/dev/master of=/dev/varalevy
### master ja varalevy tekstien kohdalle pitää laittaa oikeat laitetiedostot
### ja mieluusti tehdä kopio siten että molemmat levyt ovat kiinni ide/sata
### väylässä

### Scripti on tarkoitettu ajettavaksi rootin oikeuksin jotta oikeuksien
### puute ei aiheuta ongelmia

### Muuttujat, muokkaa sellaisiksi kun haluat, muuta ei luultavasti
### tarvitse muokata

email=yllapitaja@domain.com
source_dir=/ # juuriosio koska otetaan koko levystä kopio
dest_dir=/media/backup # kohdehakemisto jonne ulkoinen asema mountataan

### muuttujat /boot osion backuppia varten
boot_src=/boot
boot_dest=/media

# Mountataan ulkoinen usb levy ensin kunhan on siirrytty juurihakemistoon
# ensin,muista tarkastaa mikä on laitetunnus kyseiselle ulkoiselle levylle.
# Mounttaushakemisto on /media, nykyään melkein kaikki Linux jakelut käyttävät
# /media hakemistoa

cd /

# FIX THIS BEFORE USING SCRIPT
mount /dev/sda2 /media/backup

#############################################################################
# HUOM!!!!! Jotta seuraava tarkastus toimisi taytyy varalevylle tehda¤ juuri- #
# hakemistoon .backup.txt tiedosto etukateen.                                 #
# HUOM!!!!!¤Talla tavoin tarkistetaan etta ulkoisen usb levyn mounttaus on   #
# onnistunut ja jos ei onnistunut niin ei tehda mitaan                        #
#############################################################################


if [ ! -e /media/backup/.backup.txt ]; then

                date '+%d-%B-%Y-%k:%M:%S' | mutt -s "Nightly backup to\
 external disk has _F A I L E D_, make sure that external usb disk really is\
 connected to the computer " $email

else
```

```
# Ennen kuin aloitetaan backup niin otetaan talteen päiväys ja kellonaika

 echo Backup_starts-`date '+%d-%B-%Y-%k:%M:%S'` >> /.backup.txt

# Ennen varsinaista käyttÃ¶nottoa pitää varmistaa että tarvitaanko --exclude
# /backup optiota vai riittääkÃ¶ tuo -x estämään sen ettei /backup hakemistoa
# varmisteta tuplaten
# Koska /boot hakemistosta otetaan myÃ¶myohemmin erikseen backup niin jatetaan
# se myos pois tassa vaiheessa

 rsync -aupx --delete --force --exclude /proc --exclude /boot $source_dir $dest_dir

# Kun varmuuskopio on tehty niin merkitään muistiin myÃ¶s tästä
# tapahtumasta päiväys ja kellonaika.
# Jälkikäteen on helppo tarkastaa backup.txt tiedostosta kauanko kunkin
# varmuuskopion ottaminen on kestänyt ja se kertoo mahdollisista ongelmista
# jos yhtäkkiä backupin otto kestääkin huomattavan paljon kauemmin kuin aiemmin.
# Varmuuskopio täytyy olla valmis ennen tÃ¶iden alkua aamulla.

 echo Backup_completed-`date '+%d-%B-%Y-%k:%M:%S'` >> /.backup.txt
 echo " " >> /.backup.txt

# sama tieto halutaan myÃ¶s tehdylle kopiolle joten kopioidaan tiedosto
# varmuuskopio.txt /media/backup -hakemistoon

 cp /.backup.txt /media/backup/.backup.txt

# kun varmuuskopiointi on valmis niin unmountataan levy

 umount /media/backup

# Otetaan myÃ¶s /boot hakemistosta backup. Mahdolliset kernelpaivitykset
# saadaan talteen talla tavoin. Tarkista laitetiedosto ja kohdehakemisto.

 mount /dev/sda1 /media/boot

# Otetaan varsinainen backup

 rsync -aupx --delete --force $boot_src $boot_dest

# Unmountataan /media/boot

 umount /media/boot

# Lähetetään postia tapahtuneesta

 tail -9 /.backup.txt | mutt -s "Nightly backup to external disk\
  S U C C E S F U L L Y completed" $email

fi

# Asetetaan levyn spindown aika 1 minuuttiin, X == ulkoisen levyn laitetunnus
# Pitää tarkastaa tarvitaanko tätä tässä scriptissä, ehkä sen voi
# fiksusti asettaa muuallakin. Esim. ehkä /etc/sysconfig/ hakemistossa on jokin
# tiedosto johon tämän voi asettaa levykohtaisesti.

# hdparm -S 12 /dev/sdX # arvo 1 on n. 5 sekuntia, arvo 2 on n. 10 sekuntia jne..
```

LIITE 5

Varmuuskopioinnin ajastus etc/crontab-tiedostoon

```
#-------------------------------------------------------------
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# run-parts

01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly

# logrotate
12 1 */7 * * root       /sbin/e-smith/signal-event logrotate

# Ajoittaa varmuuskopioinnin ulkoiselle kovalevylle kolmena päivänä viikossa
30 1 * * 2 root /root/usb_backup.sh
30 1 * * 4 root /root/usb_backup.sh
30 1 * * 6 root /root/usb_backup.sh

# malli muistutukseksi
#*     *   *   *    *  command to be executed
#-     -    -    -    -
#|     |     |     |     |
#|     |     |     |     +------ päivä viikosta (0 - 6) (Sunday=0)
#|     |     |     +------- kuukausi (1 - 12)
#|     |     +--------- päivä kuukaudesta (1 - 31)
#|     +----------- tunnit (0 - 23)
#+------------- minuutit (0 - 59)


# Backup task is disabled
# Workstation Backup task is disabled

02 4 * * * root /sbin/e-smith/check4updates -m


# smeserver-clamscan filesystem scan
12          0          *          *          *          root
/sbin/e-smith/smeserver-clamscan



50 4 * * * root squid -k rotate

51 21 * * 2 root  sleep $[ $RANDOM \% 60 ]; /sbin/e-smith/statusreport
```