Opinnäytetyö (AMK)

Tietojenkäsittelyn koulutusohjelma

Tietoliikenne

2012

Tero Mäkelä

KANSALAISEN MIKROTUEN PALOMUURIJÄRJESTELMÄ

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

Turun ammattikorkeakoulu

Tietojenkäsittelyn koulutusohjelma | Tietoliikenne

Marraskuu 2012 | 59 sivua

Esko Vainikka

Tero Mäkelä

KANSALAISEN MIKROTUEN PALOMUURIJÄRJESTELMÄ

Opinnäytetyön tavoitteena on luoda Kansalaisen mikrotuelle palomuurijärjestelmä, jolla saadaan jaettua asiakas- ja työntekijälaitteet omiin verkkoihin. Rajatussa asiakasverkossa laitteet voidaan huoltaa turvallisesti vaikuttamatta muiden laitteiden tietoturvallisuuteen haitallisesti. Lisäksi luodaan palomuurijärjestelmän käyttöohjeet.

Palomuurijärjestelmän luomisprosessia tarkastellaan järjestelmäkehityksen elinkaarimallin avulla. Palomuurin ja RAID-tekniikoiden toiminta pyritään selvittämään perusominaisuuksien ja toimintaperiaatteiden osalta.

Järjestelmän alkuunpanossa selvitetään palomuurin vaatimusmäärittelyt, jonka jälkeen hankitaan tarvittavat laitekomponentit ja selvitetään Kansalaisen mikrotuen verkon rakenne. Tämän jälkeen suoritetaan palomuurijärjestelmien vertailu, jonka perusteella valitaan käyttöön tuleva palomuurijärjestelmä. Lopuksi järjestelmä asennetaan ja asetetaan asetukset vaatimusmäärittelyn mukaisesti.

Järjestelmä saatiin otettua käyttöön useista järjestelmän asennuksen aikana syntyneistä vastoinkäymisistä huolimatta. Järjestelmä saatiin vastaamaan vaatimusmäärittelyjä muuten, paitsi välityspalvelimen osalta.

ASIASANAT:

Palomuurit, RAID, Kansalaisen mikrotuki, pfSense

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communication

November 2012| 59 pages

Esko Vainikka

Tero Mäkelä

CITIZEN'S HELPDESK FIREWALL SYSTEM

The aim of this thesis is to create a computer firewall system for Citizen's helpdesk. The firewall divides the customer and the employee equipment to different own networks. In a limited customer network, the devices can be serviced safely without affecting the information security of other devices adversely. In addition a user guide for the firewall system is created.

The process of creating a firewall system is examined with the life cycle model of the system development. The firewall and the RAID technologies' basic features and principles of operation are explained.

Firewall requirement specifications are explained in the system initiation and after that all the necessary device components are acquired and the structure of the Citizen's helpdesk network is explained. After this the comparison of the firewall systems is performed and a suitable firewall system is selected for usage. Finally, the system is installed and the settings are set in accordance with the requirement specification.

In the end, the system was operational despite all the trouble during the installation of the firewall system. The system meets all the requirements of the specifications except for the proxy server.

KEYWORDS:

Firewalls, RAID, Citizen's Helpdesk, pfSense

SISÄLTÖ

LIITTEET

KUVAT

1 JOHDANTO

Opinnäytetyön tavoitteena on luoda Kansalaisen mikrotuelle (myöhemmin KMT) konstruktiivisen tutkimusotteen mukaisesti toimiva palomuurijärjestelmä ja oppia samalla, kuinka se tapahtuu. Tavoitteena on luoda palomuurijärjestelmä, jolla saadaan jaetuksi asiakas- ja työntekijälaitteet omiin verkkoihinsa. Rajatussa asiakasverkossa laitteet voidaan huoltaa turvallisesti vaikuttamatta muiden laitteiden tietoturvallisuuteen haitallisesti. Vaadittavat toimenpiteet järjestelmän luomiseen toteutetaan järjestelmäkehityksen elinkaarimallin (SDLC, system development life cycle) vaiheiden mukaisesti.

Palomuurijärjestelmän laadinta alkaa toimeksiantajan vaatimusmäärittelyllä ja jatkuu valmistelevilla suunnittelutoimenpiteillä järjestelmän työstämiseksi. Alkutoimenpiteinä tehtyjen päätösten perusteella järjestelmä toteutetaan ja testataan, kunnes se täyttää vaatimukset ja järjestelmä on sen jälkeen valmis otettavaksi käyttöön. Toimivan järjestelmän ylläpito ja jatkotoimenpiteet jäävät KMT:n projektipäällikön tehtäväksi. Valmiin palomuurijärjestelmän lisäksi laaditaan asennus- ja käyttöohjeet, joiden avulla palomuurijärjestelmän pystyy asentamaan perehtymättä siihen syvällisemmin ja käyttämään sitä vastaavanlaisessa ympäristössä kuin mihin se nyt rakennetaan.

Opinnäytetyössä käsitellään ja selostetaan työn eri vaiheita: mitä siinä on tehty, miksi tiettyihin ratkaisuihin on päädytty ja kuinka jokainen vaihe onnistui työskentelyn edetessä. Opinnäytetyön tiedonhankintamenetelminä käytetään pääasiassa omaa tietotaitoa ja yritys-erehdys -kokeiluja, mutta kirjallisuutta, haastatteluja ja sähköpostikysymysten esittämisiä hyödynnetään niiltä osin, kun omaa tietotaitoa ei ole.

2 JÄRJESTELMÄKEHITYKSEN ELINKAARIMALLI

Opinnäytetyötä tehdään järjestelmäkehitysen elinkaarimallin (SDLC - System Development Life Cycle) mukaisesti (kuva 1). Tietoturvaan ja standardeihin perehtyneen yhdysvaltalaisen kauppaministeriön alaisen viraston National Institute of Standards and Technologyn (NIST) mukaan SDLC on jaoteltu alkuunpanoon, kehittämiseen ja hankkimiseen, täytäntöönpanoon ja arviointiin, toimintaan ja ylläpitoon ja käytöstä poistoon (Radack 2009, 2-3). Jokaisessa vaiheessa on syytä tarkastella järjestelmän kehitystä tietoturvan näkökulmasta. Tarkoitus on selvittää, mitä jokainen vaihe sisältää ja miten niitä voidaan hyödyntää palomuurijärjestelmän laadinnassa.

Kuva 1. Järjestelmäkehityksen elinkaarimallin kiertokulku (Kissel ym. 2008, 11).

Alkuunpano

Organisaatio selvittää järjestelmälle ilmaistut tarpeet ja sen, mihin tarkoitukseen järjestelmää aiotaan käyttää. Näiden tietojen perusteella järjestelmän vaatimukset dokumentoidaan. On hyvin tärkeää, että vaatimusmäärittely on

mietitty riittävän tarkkaan tietoturvan osalta, jotta myöhemmissä vaiheissa osataan ottaa ne huomioon. (Radack 2009, 3-4.)

Kehittäminen ja hankkiminen

Järjestelmä on suunniteltu, ostettu, ohjelmoitu, kehitetty tai muuten rakennettu valmiiksi. Vaihe sisältää usein muita määriteltyjä kiertoja, kuten järjestelmänhankinnan kehityskierron. Kehittämisen ja hankinnan tietoturvasta tehdään riskiarviointeja ja analysoidaan turvavaatimukset. (Radack 2009, 4.)

Täytäntöönpano ja arviointi

Järjestelmä asennetaan, minkä jälkeen suoritetaan erilaisia kokeiluja ja testejä, jotta saadaan selvitetyksi järjestelmän toiminta käyttötarkoitukseen kuuluvalla tavalla. Järjestelmän tietoturvallisuus myös testataan erilaisilla testeillä, jotta saadaan varmistettua, että järjestelmä täyttää kaikki vaaditut tietoturvaominaisuudet. (Radack 2009, 4-5.)

Toiminta ja ylläpito

Testausvaiheen jälkeen järjestelmä on otettu toimintaan ja sen käyttöä seurataan. Tarkoituksena on, että järjestelmä suoriutuu työstä, johon se on suunniteltu. Seurannan aikana saatetaan kuitenkin tehdä mahdollisia parannuksia tai muutoksia järjestelmään muun muassa tietoturvan osalta. (Radack 2009, 5.)

Käytöstä poisto

Laaditaan suunnitelmat käytöstä poistettavan järjestelmän alasajosta ja vanhan järjestelmän korvaamisesta uudella järjestelmällä. Järjestelmä poistetaan käytöstä vasta sen jälkeen, kun siirtyminen uuteen järjestelmään on valmistunut ja on toiminnassa. Vanhan tiedon tietoturva täytyy pitää kunnossa, kun tieto siirretään korvaavaan järjestelmään, säilytetään tai tuhotaan. (Radack 2009, 5.)

3 JÄRJESTELMÄN ALKUUNPANO

Opinnäytetyön aihe sai alkunsa tarpeesta saada KMT:lle palomuuri, jolla saataisiin eriytettyä asiakaslaitteet rajoitettuun ympäristöön. Silloin asiakaslaitteilla olisi pääsy vain rajoitettuihin palveluihin. KMT:n projektipäällikkö Ari Mäkeläinen ilmoitti palomuurijärjestelmän tarpeesta. Aihe tuntui kiinnostavalta ja projektipäälliköltä selvitettiin tarvetta ja vaatimuksia pääpiirteissään ennen opinnäytetyön valinnantekoa.

Vaatimuksina olivat liikenteen lokitus, estetyn liikenteen lokitietojen lyhyt, noin viikon säilytysaika, myöhemmin määriteltävä sallitun liikenteen säilytysaika, yhteyksien musta ja valkoinen listaus, hallinnan ja käyttöliittymän yksinkertainen ja selkeä ulkoasu, josta on mahdollisuus seurata lokeja, proxy-ohjelmiston asennus, maksuton Unix, BSD tai vastaava käyttöjärjestelmä ja kahden verkkokortin laite. Lisäksi järjestelmässä ei saa olla minkäänlaista etähallintaa. Järjestelmässä voidaan käyttää päivityksiä, mutta ne eivät saa rikkoa järjestelmän toimintoja. (Mäkeläinen 2.5.2011.)

Tärkeintä mustassa ja valkoisessa listauksessa on, että laitteet eivät näe toisiaan. Oletuksena kaikki liikenne on estetty poislukien määritellyt palvelut ja niiden päivittäminen, kuten Windows Update, SUPERAntiSpyware, Malwarebytes ja Avast. Valkoiselle listalle pääsee käsiksi vain paikallisesti ja siirto listalle on tehtävä manuaalisesti. Lisäksi tulevat merkinnät vanhenevat automaattisesti viikossa. Palomuurin ei tule suorittaa osoitteenmuunnosta, koska ip-osoitteet jaetaan NAT-laitteelta. (Mäkeläinen 2.5.2011.)

Työnkuvaus tuntui tekijän taitoihin nähden sopivalta, joten hyväksymisprosessia lähdettiin viemään eteenpäin. Aihe hyväksyttiin ja päätettiin, että pidetään tapaaminen, jossa keskustellaan opinnäytetyön tekijän, KMT:n projektipäällikön ja tietojenkäsittelyn opettajien kanssa palomuurijärjestelmän rakentamisen aloittamisesta.

Tapaaminen

Ennen tapaamista selvitettiin, minkälaisia vaihtoehtoja palomuurijärjestelmän käyttöjärjestelmälle löytyy ja minkälainen laitteisto järjestelmän käyttämiseen vaaditaan. Hakukoneella etsittiin hakusanalla ”open firewall distro” palomuurijärjestelmiä ja löydettiin LinuxQuestions.org-sivulta hyvä listaus järjestelmistä (Firewall distributions 2010). Vertailtavaksi otettiin vain järjestelmät, jotka sopivat vaatimusmäärittelyn kriteereihin. Vertailun ulkopuolelle jätettiin kaupalliset, ei-aktiiviset, täysin komentorivipohjaiset, disketti- ja CD-pohjaiset järjestelmät. Tarkoituksena on valita ilmainen, tuettu, helppokäyttöinen ja muokattava järjestelmä, jossa onnistuu kiintolevyasennus.

Tutkittavaksi palomuurijärjestelmiksi valittiin Endian, m0n0wall, pfSense, Smoothwall Express ja Zeroshell. Tutkittavaksi valittujen järjestelmien verkkosivuilta selviää, että ne eivät vaadi laitteistolta suurta suorituskykyä, mutta toimivat uudemmillakin laitteistoilla. Palomuurijärjestelmästä riippuen laitteiston vähimmäisvaatimukset vaihtelevat Pentium-tasoisesta prosessorista 500 MHz:n prosessoriin, 16 megatavusta 256 megatavuun keskusmuistia ja levytila 256 megatavusta 4 gigatavuun. (Endian 2011b; M0n0wall 2011; PfSense 2011d; Smoothwall 2011a; Zeroshell 2011.)

PfSensen sivuillta löytyy hyvä laitteiston skaalaukseen liittyvä ohjeistus. Ohjeistuksen mukaan, jos haluaa hyödyntää KMT:n tiloihin tulevan 100 megabitin yhteysnopeuden kokonaan, vaaditaan vähintään 1 GHz nopeuksinen prosessori, jotta yhteys ei hidastelisi ja prosessori jäisi pullonkaulaksi. Mikäli laitteeseen asennetaan tunkeilijan havaitsemisjärjestelmä Snort tai verkkoliikenteen analysointiväline Ntop, on muistikapasiteetin oltava vähintään 512 megatavua. (Pfsense 2011a.)

Tapaamisessa keskusteltiin, miksi palomuuria tarvitaan ja minkälaisia vaatimuksia palomuurijärjestelmälle on. Keskusteluissa ilmeni, että palomuuria tarvitaan erottamaan asiakaslaitteet rajattuun verkkoon, jossa KMT:n henkilökunnan on helppo huoltaa asiakaslaitteet turvallisessa ympäristössä

vaarantamatta jo huollettuja laitteita, henkilökunnan laitteita ja vähentämällä turhaa ylimääräistä liikennettä ulkoverkkoon.

Tarkoitus on pitää kaikki laitteet ensin mustalla listalla, joka rajoittaisi pääsyn kaikkialle paitsi käyttöjärjestelmän, virustorjuntaohjelmien ja huolto-ohjelmien päivityspalvelimille. Kun huolto-operaatiot on saatu valmiiksi, projektipäällikkö siirtää laitteen valkoiselle listalle. Valkoisella listalla sallittaisiin liikenne internetiin, mutta ei sisäverkon laitteisiin.

Tapaamisessa selvitettiin mahdollisuutta varmuuskopioida lokitiedot lokipalvelimelle. Sellaista laitetta ei ole kuitenkaan hankinnassa, joten lokitiedot säilytetään pelkästään palomuurissa. Lisäksi selvitettiin, miksi tavallista Windows-työkonetta ei kannata käyttää palomuurina. Windows-laitteilla on suurempi riski joutua hyökkäyksen kohteeksi. Järjestelmä on päivitettävä säännöllisesti, jotta tietoturva-aukot saadaan korjattua. Lisäksi ylläpito vie enemmän resursseja ja aikaa ja suorituskyky on heikompi. Työasemien palomuurit on suunniteltu suojaamaan vain yksittäistä tietokonetta eikä koko verkkoa. Verkon suojaamiseen on järkevintä käyttää siihen dedikoitua erillistä palomuurilaitetta. (Microsoft 2011.)

Vaatimuksiksi määriteltiin käytettäväksi KMT:n projektipäällikön suunnitelman mukaan laadittua vaatimusmäärittelyä pienin lisäyksin. Järjestelmältä halutaan vikasietoisuutta ja mahdollisuutta eriyttää palomuurin hallinta omalle verkkokortille. Vikasietoisuuden lisäämiseksi ehdotettiin vaihtoehdoksi SSD-levyä tai kiintolevyistä tehtävää RAID-järjestelmää. Vaihtoehdoista todettiin, että tulee edullisemmaksi rakentaa kiintolevyistä ohjelmistopohjainen RAID5-järjestelmä, koska käytettävissä on AMK:n poistettujen tietokoneiden kiintolevyjä. Lisäksi järjestelmässä on oltava liitännät kolmelle verkkokortille, jotta sisä-, asiakasverkko ja palomuurin hallintaverkko ovat mahdollisimman turvatut.

4 PALOMUURIN TOIMINTA

Palomuuri on tietoturvajärjestelmä, joka suodattaa läpikulkevaa liikennettä. Palomuurijärjestelmä suodattaa suojattavan verkon ja vaarallisemman verkon välisiä yhteyksiä. Useimmiten palomuuria tarvitaan avoimesta Internet-yhteydestä tulevilta hyökkäyksiltä suojautumista varten, mutta myös ulkomaailmaan lähtevää liikennettä suodatetaan, esimerkiksi haittaliikennettä. Palomuurilaitteilla on sääntöjä, joilla sisään tulevista yhteyksistä suodatetaan pois kaikki muu paitsi välttämättömät yhteydet. (Palomuuri 2012.)

Palomuurit käytännössä

Useimmiten palomuureja on isoissa yritysverkoissa useampia. Palomuurien perusongelma on, että niiden läpi hyökännyttä murtautujaa ei voida enää estää tekemästä tuhoa. Tämän takia yrityksillä on eteisverkko eli demilitarisoitu alue (demilitarized zone, DMZ), joka sijaitsee luotetun sisäverkon ja Internetin välissä. Palomuurit sijoitetaan Internetin ja eteisverkon sekä eteisverkon ja sisäverkon väliin. Julkiset palvelimet sijoitetaan eteisverkkoon. Tästä on se hyöty, että vaikka tunkeutuja pääsisi murtautumaan kyseisille palvelimille, olisi hänellä vielä toinen palomuuri edessään ennen sisäverkkoa. (Palomuuri 2012.)

Palomuurilaitteet osaavat toteuttaa tarvittaessa useita erilaisia eteisverkkoja sisältävän konfiguraation yhdellä laitteella. Palomuurilaitteeseen vain lisätään verkkoliitäntöjä ja sille määritetään, onko liitäntöjen takana luotettu verkko, täysin turvaton verkko vai jotain siltä väliltä. (Palomuuri 2012.)

Palomuuritekniikat

Yksinkertaisin palomuuri on kuljetuskerroksella toimiva pakettisuodatin ja yhdyskäytävä. Pakettivirrasta seulotaan paketit lähde- ja kohdeosoitteen sekä porttien perusteella. Näitä on kahdentyyppisiä: tilattomia (stateless) ja tilallisia (stateful). Tilaton palomuuri vertaa jokaista pakettia palomuurisääntöihin siten, että ei-sallittuja paketteja ei välitetä eteenpäin ja sallitut välitetään. (Palomuuri 2012.)

Tilallinen palomuuri mahdollistaa liikenteen tarkemman valvonnan. Tilallinen palomuuri pitää kirjaa muodostetuista TCP-yhteyksistä ja virallisista UDP-yhteyksistä ja sallii vain yhteyteen kuuluvat paketit. TCP-yhteyksillä tutkitaan myös tilasiirtymien laillisuus, jolloin tilallinen palomuuri pitää yllä samoja tietoja kuin TCP/IP-paketti. (Palomuuri 2012.)

Tilattoman palomuurin ongelma on se, että paluupakettien portteja ei voida kaikissa protokollissa tietää tarkasti, jolloin joidenkin ohjelmien toimivuuden vuoksi porttinumeron 1024 jälkeiset portit on avattava paluuyhteydelle. Tämän jälkeen porttialueella olevaan palveluun voidaan ottaa yhteys ilman palomuurin väliintuloa. (Palomuuri 2012.)

Tilallinen palomuuri tarkistaa jokaisen paketin kohdalla, kuuluuko se johonkin olemassa olevaan yhteyteen ja olemassa oleviin yhteyksiin liittyvät paketit päästetään läpi. TCP-yhteyden avaamisen jälkeen tutkitaan ensin, onko yhteys sallittu palomuurin sääntöjen perusteella. Hyväksytyn yhteyden tiedot lisätään palomuurin yhteyslistaan ja kaikki kyseiseen yhteyteen liittyvät paketit päästetään jatkossa läpi. Usein myös sallitaan yhteyteen liittyvät ICMP-sanomat. (Palomuuri 2012.)

Yhteyden sulkeuduttua tai tietyn käyttämättömän ajan jälkeen yhteyden tiedot poistetaan yhteyslistalta eikä kyseiseen yhteyteen kuuluvia paketteja enää päästetä läpi. Tilallisessa palomuurissa on sama ongelma tuntemattomien protokollien kanssa kuin tilattomassakin, mutta siihen voidaan tarvittaessa lisätä sääntöjä tunnettuja protokollia varten. (Palomuuri 2012.)

Sovelluskerroksella toimivassa sovelluspalomuurissa paketin sisältämää dataa tarkkaillaan esimerkiksi laittomista komennoista. Muille palomuurityypeille ongelmallinen aktiivinen FTP toimii tämäntyyppisessä palomuurissa, koska palomuuri lukee avattavan datakanavan portin numeron FTP-komentokanavan sanomasta ja sallii yhteyden siihen. Palomuuri voi myös suodattaa liikennettä sisällön perusteella esimerkiksi estämällä HTTP-paketeista tunnettuja turvallisuusaukkoja hyödyntävät murtoyritykset. (Palomuuri 2012.)

Useimmat nykyaikaiset työasemakohtaiset palomuurit ovat sovellus- ja tilallisen palomuurin yhdistelmiä. Niissä myös sovellus voi vaikuttaa siihen, sallitaanko jokin yhteys. Erona perinteisiin palomuureihin on se, että ennalta tiedetään tarkkaan, mitkä palvelut ovat sallittuja ja samoin, mikä liikenne kohdistuu työasemaan. Perinteiset palomuurit joutuvat toimimaan vähempien tietojen perusteella. (Palomuuri 2012.)

Palomuurien heikkouksia

Palomuuri suodattaa vain lävitseen kulkevia yhteyksiä. Niinpä verkkoon voi päästä vaihtoehtoisia reittejä, kuten langattoman lähiverkon tukiasemien kautta tai fyysisesti pääsemällä yrityksen toimitiloihin. Palomuuri ei myöskään kykene suodattamaan esimerkiksi IPSec-salattua liikennettä, josta ei näy kohdeporttia tai välttämättä edes kohdekonetta. Tämän takia salattu VPN-liikenne pyritään viemään erilliselle eteisverkolle, josta se voidaan viedä vielä salaamattomanakin palomuurin läpi uudelleen. (Palomuuri 2012.)

5 LAITTEISTOHANKINNAT JA TILANNEKARTOITUS

Palomuurin rakentaminen aloitetaan kartoittamalla saatavilla olevat komponentit palomuuria varten. Tulevaisuutta varten on hyvä valita riittävän moderni ja tehokas kokoonpano, jotta tarvittavia ohjelmisto- ja komponenttilaajennuksia pystytään myöhemmin tekemään. AMK:n puolesta olisi ollut mahdollista saada poistettuja Fujitsu Siemens Esprimo P5915 -pöytäkoneita palomuurikäyttöön, mutta koneissa on todettu useita tyyppivikoja, toimintavarmuuteen liittyviä ongelmia sekä kotelon soveltumattomuutta RAID-järjestelmän levypakalle. Koneet päätettiin purkaa ja ottaa projektia varten kaikki keskusmuistit ja kiintolevyt ja käyttää yli jääneet komponentit varaosina.

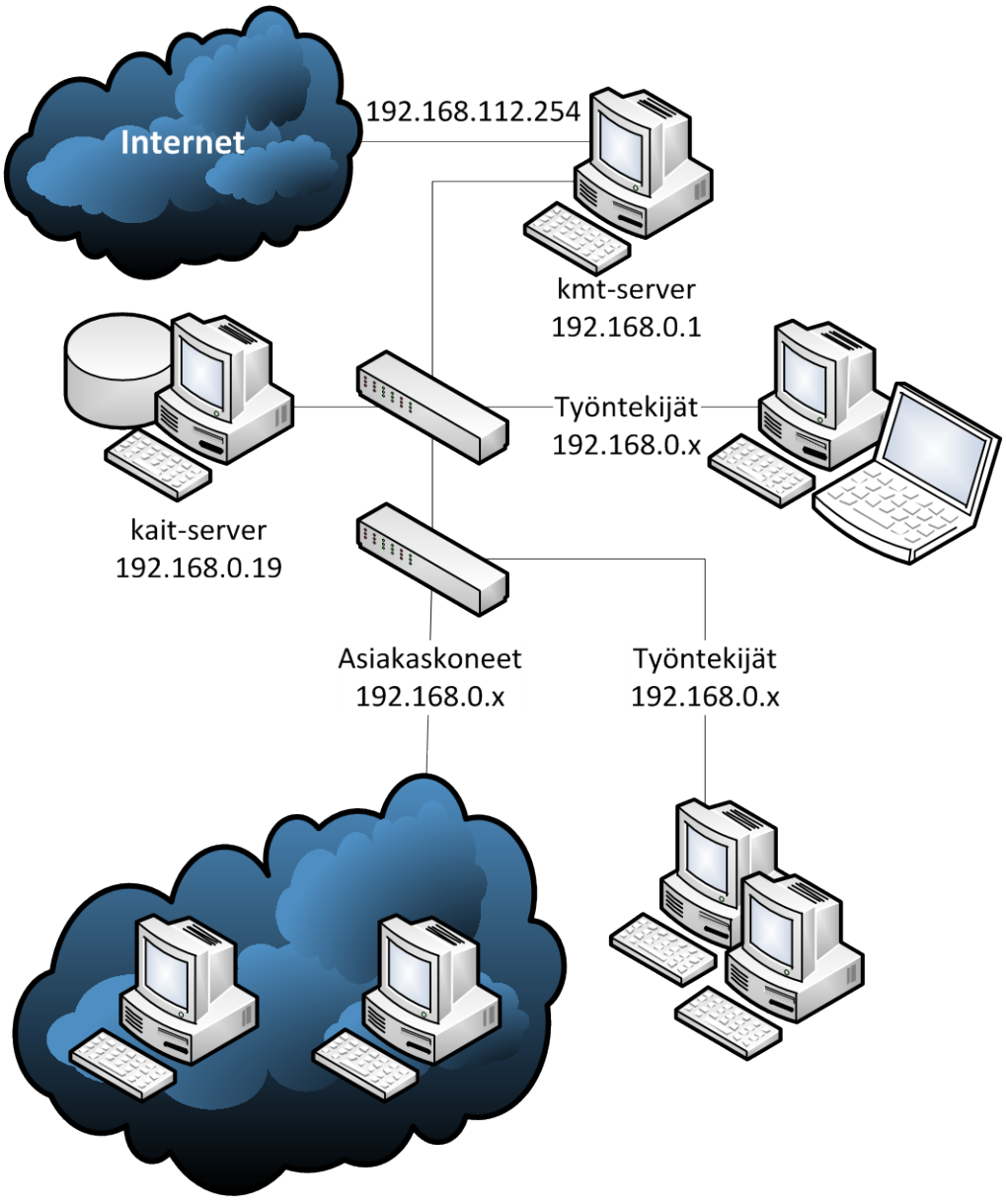
AMK:n varastossa oli erilaisia tietokonekoteloita ja niistä löytyi yksi kriteerien täyttävä avara tornimallinen ATX-kotelo projektia varten. Varastosta löytyi lisäksi kolme 3Comin 100 megabitin verkkokorttia, jotka sopivat hyvin projektia varten. Valitettavasti AMK:lla ei ollut tarjota muita komponentteja, joten opinnäytetyön tekijä toimitti omasta varastostaan emolevyn, prosessorin, virtalähteen ja näytönohjaimen.

Palomuurin laitteisto-osuuden rakentaminen aloitettiin, kun tarvittavat komponentit oli kerätty. Komponentit asennettiin niille tarkoitetuille paikoille. Emolevyyn asennettiin vain välttämättömät laitteet ja kaapelit. Kun kiintolevyt oli asennettu, ne numeroitiin emolevyn porttinumeroiden perusteella, jotta rikkoutunut levy on helpompi löytää. Kotelon takaosaan asennettiin tuuletin ja sijoitettiin kaapelit siten, että ne olisivat mahdollisimman vähän ilmavirran tiellä, jotta komponentit eivät altistuisi ylimääräiselle lämmölle, joka lyhentäisi niiden käyttöikää.

Laite käynnistettiin onnistuneesti heti ensimmäisellä käyttökerralla ja tämän jälkeen aloitettiin BIOS-asetusten asettaminen. BIOS-asetuksista poistettiin käytöstä kaikki muut liitännät ja ohjaimet paitsi USB-liittimet ja SATA-kiintolevyohjain, koska jokainen ylimääräinen liitäntä ja ominaisuus on tietoturvariski. Parametrien asettamisen jälkeen tarkistettiin, että emolevylle on asennettu viimeisin BIOS-päivitys. BIOS:n valmistelun jälkeen aloitettiin

keskusmuistin ja prosessorin rasitustesti. Kone toimi virheittä ja vakaasti sallitun lämpötilarajan rajoissa täydessä rasituksessa yli vuorokauden ajan.

Laitteiston suunnittelun ja toteutuksen lisäksi on syytä tutustua KMT:n lähiverkkoon ja tehdä siitä looginen verkkokuva, jotta saisi paremman käsityksen lähtötilanteesta (kuva 2). Verkkokuvan perusteella pystyy aloittamaan vaadittujen parannustoimenpiteiden suunnittelun ja toteuttamisen.



Kuva 2. KMT:n nykyinen looginen verkkokuva.

KMT:n verkkoa tutkittiin ja saatiin selvitetyksi palvelinten ja verkkolaitteiden kytkennät ja toiminta. Kmt-server toimii KMT:n ulko- ja sisäverkon välisenä palvelimena. Tästä palvelimesta yhteys jatkuu kytkimeen, josta yhteys jakautuu kait-serverille, muutamalle työntekijäkoneelle ja toiselle kytkimelle. Toiseen kytkimeen ovat yhteydessä kaikki asiakaskoneet ja muutama työntekijäkone. KMT:n projektipäällikkö ylläpitää palvelimia ja työntekijäkoneita. Kummallekin palvelimelle on määritelty omat salasanat ja työntekijäkoneille yhteinen salasana.

Kmt-server suorittaa verkko-osoitemuunnoksen, jakaa sisäverkon osoitteet ja suodattaa palomuurisääntöjen mukaan verkkoliikennettä. Laitteelle on asetettu kiinteä ip-osoite 192.168.0.1 ja se esiintyy ulkoverkkoon ip-osoitteella 192.168.112.254. Kaikille muille laitteille jaetaan ip-osoitteet koko 192.168.0.0-osoiteavaruuden sisältä alkaen 2:sta päättyen 254:ään. Kait-server toimii KMT:n asiakastietokantana, jonne uudet huoltotyöt kirjataan ja tietoja käsitellään työntekijäkoneilta. Oletettavasti laitteen ip-osoite on kiinteä 192.168.0.19, koska asiakaslaitteiden kirjaukset tehdän kyseiseen osoitteeseen. Asiaa ei pystynyt tarkistamaan, koska laitteelle ei onnistuttu kirjautumaan millään tiedossa olevista salasanoista.

Vaatimusten mukaan asiakaslaitteet pitää saada suojatuksi palomuurilla. Tällöin KMT:n verkkoa on muutettava siten, että asiakaslaitteiden käyttöön tarkoitettua kytkintä ennen asennetaan palomuuri. Toiseen kytkimeen kytketään kaikki työntekijälaitteet, palvelimet ja asennetaan asiakaslaitteita suojaava palomuuri.

Palomuuriin kytketään lisäksi hallinnointipääte, joka toimii samalla myös projektipäällikön työkoneena. Tällöin projektipäällikön työkoneessa on oltava kaksi verkkokorttia: toinen palomuurin hallinnointiin, toinen työntekijäverkossa muuhun käyttöön. Palomuurille ei sallita hallinnointia muualta kuin projektipäällikön tietokoneelta, joten yhteys hyväksytään vain hallinnointiverkosta ja määritetystä verkkolaitteesta.

6 PALOMUURIJÄRJESTELMIEN VERTAILU

Vertailtavat palomuurit rajattiin jo aiemmin esiselvitettyihin Endian, Smoothwall Express, m0n0wall, pfSense, Zeroshell -palomuurijärjestelmiin. Tarkoituksena on valita KMT:lle sopivin palomuurijärjestelmäratkaisu ja ottaa tutkittavaksi vain rajattu määrä eri palomuurijärjestelmiä, jotta palomuuri saadaan mahdollisimman nopeasti rakennetuksi.

Eri järjestelmiä voi asentaa ja käyttää erilaisin tavoin. Järjestelmää voi käyttää CD-levyltä tai muistikortilta tai asentaa se täydellisenä asennuksena tietokoneen kiintolevylle. CD-levyltä käytettäessä järjestelmää voi käyttää asentamatta sitä kiintolevylle tai muistikortille ja asetukset voidaan tallentaa disketille tai USB-muistitikulle. CD:n tiedostoja ei käytetä usein käynnistyksen jälkeen, koska järjestelmä toimii silloin pääasiassa keskusmuistilta. Levyä ei kuitenkaan saa poistaa käynnissä olevasta järjestelmästä. Yleisesti CD-version käyttötarkoituksena on arvioida ohjelmistoa tietyllä laitteistolla, jonka jälkeen järjestelmä asennetaan muistikortille tai kiintolevylle. PfSensen tapauksessa käyttäjät eivät voi käyttää paketteja ja suorituskyvyn historiagraafit häviävät uudelleenkäynnistyksessä. (Buechler & Pingle 2009, 7.)

Sulautettu versio on räätälöity käytettäväksi Compact Flash -muistikortilla samalla tavalla kuin kiintolevyltä. Koska muistikorteille voidaan kirjoittaa rajattuja kirjoituskertoja, käytetään muistikorttia vain luku -tilassa ja keskusmuistissa tiedostojärjestelmää, johon voi kirjoittaa ja jota voi lukea lukemattomia kertoja. Sulautettuja järjestelmiä tuetaan laajasti monilla laitteistoilla ja muuntimilla. Muistikorteilla käytetään muistipiirejä, jolloin ei ole mahdollista riskiä rikkoutuvasta kiintolevyn pyörivästä kiekosta. Koska niissä ei ole liikkuvia osia, ne kuluttavat vähemmän virtaa, tuottavat vähemmän lämpöä, ovat hiljaisia ja toimivat riittävän nopeasti useissa verkoissa. Kuten CD-versiossa, myös sulautetussa versiossa on riski menettää historiagraafit, mutta vain äkillisissä virtakatkoksissa. (Buechler & Pingle 2009, 7-8.)

Täysasennuksella järjestelmä asennetaan hyödyntäen koko kiintolevyn kapasiteetti. Se on yleisin ja suositelluin tapa useimmissa käyttöönotoissa.

(Buechler & Pingle 2009, 7). Järjestelmä asennetaan käyttämällä täysasennusta, koska käytössä on useita kiintolevyjä ja kiintolevyt on asennettu RAIDiin, jolloin vikatilanteessa rikkinäisen kiintolevyn pystyy korvaamaan toisella. Palomuurissa ei kuitenkaan aiota pitää optista asemaa tietoturvasyistä ja graafien menettäminen uudelleenkäynnistyksessä tai sähkökatkon takia on tapahtumahistorian seuraamisen kannalta ongelmallinen. Tällöin täysasennus on ainut KMT:n ympäristössä toimiva ratkaisu.

Palomuurijärjestelmien tarkastelu

Endian ja Smoothwall tarjoavat sekä ilmaisen että maksullisen linux-pohjaisen ratkaisun. Ilmaisessa versiossa on ohjelmisto- ja laitteistorajoituksia, jotka saa käyttöön maksullisessa versiossa. Vaikka Endian ja Smoothwall tarjoavat yhteisö- ja kaupallisen version, saattaa yhteisöversiosta puuttua jokin tärkeä tai oleellinen osa, joka on osana kaupallista versiota.

Endianin yhteisöversio on kohdistettu kehittäjille ja testikäyttöön ei-kriittiseen ympäristöön tai yksityiseen käyttöön. Oleellisina puutteina tai rajoitteina voisi pitää sitä, että järjestelmä on tarkoitettu pieneen ja voittoa tavoittelemattomaan käyttöön. Tukea ei ole kaupallisille virustorjunta- ja roskapostiohjelmille ja virtualisointia varten. Käyttöjärjestelmä ja tietoturvapäivitykset eivät tule reaaliajassa eikä myöskään ole pääsyä uusiin ominaisuuksiin. Järjestelmää ei voida valita, mikäli toiminta muuttuu joskus tulevaisuudessa kaupalliseksi. Tähän asiaan ei ole yksiselitteistä vastausta, joten kyseinen järjestelmä jätetään valitsematta tästä syystä. (Endian 2011a.)

Smoothwall Express 3 yhteisöversiossa oleellisina puutteina ovat rajoitettu ulospäin menevän liikenteen hallinta, objektikohtaisten porttisääntöjen puuttuminen ja lähde- ja kohdeosoitteiden liikenteen eston pudotus ja hylkäys. Järjestelmän hallinnoinnista on poistettu hyödyllisiä toimintoja ja tilanäkymiä. Suurin ongelma tulee kuitenkin siitä, kun käytössä ei voi olla useaa aliverkkoa ja kahta paikallista sisäverkon aluetta, joista toisessa olisivat asiakaslaitteet ja toisessa hallintapääte. Ongelmia tuottaa myös se, että järjestelmässä ei voi käyttää varmuuskopiointia ja palautusta. Järjestelmään ei kannata tutustua sen

tarkemmin, koska se ei vastaa vaatimusmäärittelyä ja tämän takia sitä ei myöskään voida valita. (Smoothwall 2011b.)

M0n0wall ja pfSense ovat BSD-pohjaisia järjestelmiä. Järjestelmät ovat muuten samanlaisia, mutta pfSense-järjestelmää on lähdetty kehittämään alun perin täydelliseksi PC-asennukseksi ja parantamaan m0n0wallin ominaisuuksia. Toisin kuin pfSense, m0n0wall on tarkoitettu pelkästään sulautettuihin järjestelmiin. Tämä onnistuu myös nykyään pfSenselläkin. PfSenseen on lisäksi mahdollista asentaa käyttötarpeen mukaan hyödyllisiä paketteja, jotka toimivat graafisessa web-liittymässä ja lisäävät verkon tietoturvaa, ylläpitotoimintoja ja palveluita. (PfSense 2011b, 2011c.) Koska käytössämme ei ole sulautettu järjestelmä, m0n0wall karsiutuu valittavista järjestelmistä.

PfSensen kehittäjät valitsivat FreeBSD:n järjestelmän pohjaksi OpenBSD:n sijaan, koska järjestelmän ajurituki ja verkon suorituskyky ovat parempia. FreeBSD sisälsi aikanaan monipuolisempia ominaisuuksia ja tietoturvallisempia ratkaisuja kuin OpenBSD. Vaikkakin ajan kuluessa kummatkin järjestelmät ovat kehittyneet, on FreeBSD pysynyt suorituskykyisempänä järjestelmänä. (Buechler & Pingle 2009, 2.)

Zeroshell tarjoaa myös linux-pohjaisen ratkaisun, mutta sen web-liittymän ulkoasu on vanhanaikainen ja vaikeantuntuinen. Järjestelmää ei ole tarkoitettu kiintolevylle asennettavaksi, vaan käytettäväksi CD-levyltä tai sulautettuna järjestelmänä (Zeroshell 2012). Zeroshellin perusominaisuuksista puuttuu mm. MAC-kohdeosoitteen suodatus ja edistyneemmistä ominaisuuksista tarpit, joka hidastaa tulevia yhteyksiä ja transparent to traceroute, joka piilottaa laitteen traceroute-komennolta. (Comparison of firewalls 2012; Tarpit (networking) 2012; InetDaemon 2012.)

Palomuurijärjestelmäksi valittiin pfSense, koska muut järjestelmät ovat epäsopivia suunniteltuun käyttötarkoitukseen. PfSense on hyvä valinta, koska se on täysin ilmainen ja avoimen lähdekoodin projekti, siinä on hyvät ominaisuudet, sitä päivitetään säännöllisesti, se sisältää selkeän ja helppokäyttöisen graafisen käyttöliittymän, se on turvallinen, se on

laajennettavissa lisäpaketeilla ja siihen on mahdollista hankkia maksullista tukea. Lisäksi sen voi asentaa kiintolevylle ja siitä ei ole poistettu tai rajoitettu ominaisuuksia kuten muiden järjestelmien yhteisöversioista. pfSenseltä löytyy yhteisö, jolta voi kysyä tarvittaessa neuvoa ongelmatilanteissa.

7 PALOMUURIJÄRJESTELMÄN ASENNUS

RAID-tekniikoiden vertailu

Palomuurilaitteiston toimivuuden testaamisen jälkeen on selvitettävä, miten järjestelmä asennetaan vikasietoista levyjärjestelmää eli RAID-järjestelmää hyödyntäen ja mitä RAID-järjestelmää kannattaa käyttää. Vaihtoehtoina ovat laitteisto- tai ohjelmistopohjainen RAID-järjestelmä. Ohjelmistopohjaisella RAID-järjestelmällä levyjärjestelmää hallitsee käyttöjärjestelmä, kun taas rautapohjaisella RAID-järjestelmällä emolevyllä oleva tai erilliskortilla oleva RAID-ohjain. (Vinum volume manager 2012.)

Aikaisemmin suurin pullonkaula ohjelmistopohjaiseen RAID:n pariteettilaskentaan muodostui prosessorin hitaudesta. Nykyaikaiset prosessorit pystyvät laskemaan nykyisten levyjärjestelmien pariteetin huomattavasti pienemmällä suorituskyvyn alenemisella. Ohjelmistopohjaiset RAID-järjestelmät voivat käyttää kehittyneempiä algoritmeja kuin laitteistopohjaiset RAID-järjestelmät saavuttaen siten paremman suorituskyvyn. (Redundant array of independent disks 2012.)

Laitteistopohjainen RAID-ohjain ei vaadi prosessorilta resursseja. Useissa laitteistopohjaisissa RAID-ohjaimissa on luku- ja kirjoitusvälimuisti, joka parantaa suorituskykyä riippuen tiedonsiirron määrästä. Emolevyllä olevaa levyohjainta ei tule sekoittaa RAID-ohjaimeen, joka suorittaa laskennan. Näitä emolevyllä olevia ”vale-RAID”-levyohjaimia valmistajat kutsuvat harhaanjohtavasti RAID-ohjaimiksi, jotka kuluttavat laskentaan prosessoritehoa kuten ohjelmistopohjainenkin RAID-järjestelmä. Emolevyn tarjoama levyohjaimen käyttö on hieman helpompi kuin ohjelmistopohjaisen RAID:n, mutta siinä on kummankin tekniikan huonot puolet. (Redundant array of independent disks 2012.)

Laitteistopohjaisessa RAID-järjestelmässä on se etu, että se voidaan patterivarmentaa. Tällöin levyjärjestelmään kirjoitettava data säilyy ohjainkortin välimuistissa, vaikka sattuisikin sähkökatkos. Tämä on tärkeää, ettei kriittinen data katoa tai muutu lukukelvottomaksi. Tosin ohjelmistopohjaisella ratkaisulla

suojauksen voi tehdä siten, että jokainen levyjärjestelmän kiintolevy voidaan patterivarmentaa ja UPS:n avulla järjestelmän voi pitää päällä lyhyen sähkökatkoksen ajan tai ajaa turvallisesti alas. (Redundant array of independent disks 2012.) Järkevää olisi siis hankkia vähintään UPS-suojaus palvelimille ja palomuurille sähkökatkoksia varten.

Ohjelmistopohjainen RAID-järjestelmä voidaan helposti siirtää koneelta toiselle, kunhan käyttöjärjestelmä pysyy samana. Siirtäminen ei ole laitteistopohjaisella RAID-järjestelmällä yhtä helppoa, koska tällöin on käytettävä yhteensopivaa laitteistopohjaista ohjainta. Jos RAID-ohjain hajoaa, dataa ei pysty välttämättä palauttamaan, jollei käytetä yleensä saman valmistajan samantyyppistä laitteistopohjaista ohjainta. (Redundant array of independent disks 2012.)

Jokaisella tekniikalla on hyvät ja huonot puolet. Lähtökohtana on se, että käyttöön saadaan turvallinen levyjärjestelmä, jonka kustannukset ovat mahdollisimman alhaiset. Koska käytössä on useita kiintolevyjä ja riittävän suorituskykyinen prosessori, kannattaa tällöin käyttää RAID 5 -tekniikkaa, jolloin saadaan vikasietoisuutta ja suurempaa luku- ja kirjoitusnopeutta. (Redundant array of independent disks 2012.)

Toteutukseen ei voida käyttää emolevyllä olevaa RAID-piiriä, koska piiri ei ole kovin yleinen eikä yhtään parempi kuin ohjelmistopohjainenkaan RAID-ratkaisu. Erillisten RAID-korttien yhteensopivuus palomuurin kanssa on epäselvä ja hinta on varmasti suurempi kuin ohjelmistopohjaisella RAID-järjestelmällä. Tästä syystä ainoaksi vaihtoehdoksi jää ohjelmistopohjainen RAID-järjestelmän laadinta. Huomioitavaa on myös se, että palomuuri ja muut kriittiset laitteet suojataan UPS:lla.

Ohjelmistopohjaisen RAID-järjestelmän asennus

Ohjelmistopohjaisen RAID-järjestelmän asennuksen apuna käytetään Mario Theodoridisin laatimaa ohjeistusta siitä, kuinka ohjelmistopohjainen RAID tehdään FreeBSD:lle. Ohjeistus pohjautuu loogiseen taltiohallintajärjestelmä Vinumiin, jota kutsutaan tutummin ohjelmistopohjaiseksi RAID-tekniikaksi. Vinum mahdollistaa kiintolevyjen ja niiden osioinnin erottamisen toisistaan

loogisesti. Tällöin voidaan yhdistää esimerkiksi kahden tai neljän kiintolevyn käytössä oleva kapasiteetti yhdeksi osioksi. (Looginen taltiohallinta 2012.)

Vinum ei pysty käynnistämään järjestelmää lomitetulla RAID 0 -tekniikalla, peräänkytketyiltä kiintolevyiltä tai RAID 5 -tekniikalla, mutta peilatulla RAID 1 -tekniikalla sen pitäisi onnistua (Theodoridis 27.5.2011). Epävakautta saattaa ilmetä, jos tekee muutoksia järjestelmän osioihin jälkikäteen, mutta muuten järjestelmän pitäisi olla varsin vakaa. Aluksi pitää selvittää, pystyykö järjestelmän asentamaan ohjeiden mukaisesti määrittelemällä järjestelmän käynnistys- ja järjestelmäosiot omiksi RAID 1 -osioiksi, swap RAID 0 -osioksi ja data RAID 5 -osioksi. (Schmut 2011.)

Seuraavaksi asennuslevykuva tallennetaan muistitikulle raakakopiona käyttämällä dd-komentoa. Järjestelmä käynnistyy muistitikulta normaalisti, mutta asennusohjelmassa kiintolevyjen laitetunnukset ad4, ad6, ad8 ja ad10 poikkeavat ohjeistuksen da0-da3:sta. Tämä johtuu siitä, että ”ad” tarkoittaa IDE-levyä ja ”da” SCSI- tai SATA-levyä. Asennusohjelmassa ei ole kuitenkaan valintaa RAID-levyjärjestelmän luomiseen, mutta osiointityökalulla saa luotua järjestelmäosioita, joita FreeBSD-järjestelmässä kutsutaan nimellä slice. (Schmut 2011; FreeBSD 2011.)

Ohjeen mukaan pitäisi käyttää fdisk -osiointieditoria ja bsdlabel -levynnimeämiseditoria, mutta asennusohjelmasta ei pääse suorittamaan komentorivikomentoja. Koska komentoriville ei päässyt siirtymään, pitää selvittää, pystyykö järjestelmän luomaan toisella FreeBSD-jakelulla. Ensin kokeiltiin FreeSBIE-järjestelmää, mutta se ei käynnistynyt CD-levyltä tai USB-muistilta. Seuraavaksi kokeiltiin Frenzy-järjestelmää, joka ei suostunut käynnistymään USB-muistilta, mutta CD-levyltä järjestelmä käynnistyi. (Schmut 2011.)

Fdiskin ja bsdlabelin manuaaleista tutkittiin, mitä ohjeessa mainitut komennot ja niiden valinnat tekevät. Valinnat vaikuttivat manuaalin mukaan olevan järkeviä, mutta ensimmäisen komentosarjan jälkeen tulokseksi ilmestyi kuitenkin fdiskin ilmoitus ”luokkaa ei löydy”. Internetistä ei löytynyt minkäänlaista ratkaisua

ongelmaan eivätkä ohjeiden muutkaan kohdat näin ollen voi toimia. (Schmut 2011.)

RAID-kortin hankinta

Koska ohjelmistopohjaisen RAID-järjestelmän laadinnan todettiin olevan hankalaa ja ratkaisua eteen tuleviin ongelmiin ei löytynyt, täytynee hankkia laitteistopohjainen RAID 5 -ohjainkortti. Ennen laitteen hankintaa on selvitettävä, mitkä ohjainpiirit ovat yhteensopivia FreeBSD:n kanssa ja sen jälkeen ohjainkortit, joissa on tuettu ohjainpiiri. Tutkittiin, että HighPoint RocketRaid 2640x4 -ohjainkortti toimii PfSensellä ja ohjaimen hankintahinta pysyi alle 150 € budjetin, jonka jälkeen se tilattiin Turun PC-huollosta.

PfSensen testaus

Sillä aikaa, kun ohjainkorttia joutui odottelemaan, testattiin järjestelmän asennus ja laitteiston toiminta ilman RAID-levyjärjestelmää. Järjestelmä asennettiin muistitikulta ja valittiin asennusvaihtoehdoista pika-asennus moniydinprosessorituella. Verkkokortteja määriteltäessä on jokainen liitäntä nimettävä verkkokortin ajurin nimellä ja juoksevalla numerolla sekä määriteltävä jokaiselle liitännälle IP-osoite ja aliverkon peite. Tarvittaessa jokaiselle verkkokortille voidaan määritellä oma virtuaalinen verkko eli VLAN.

Koska järjestelmän asennus ja web-ympäristöön pikainen tutustuminen ehdittiin käydä läpi ennen kuin ohjainkortti saapui, päätettiin päivittää tietokoneen prosessoria uudemmalla ja nopeammalla mallilla. Valitettavasti uudella prosessorilla kone ei kuitenkaan käynnistynyt odotetulla tavalla, vaan jäi jumiin. Ongelma pysyi, vaikka otti kaikki ylimääräiset komponentit irti. Koska vika ilmeni prosessorin asennuksen jälkeen, pitäisi järjestelmän toimia alkuperäisellä prosessorilla. Näin ei kuitenkaan ollut, vaan kone jumitti samassa kohdassa samalla tavalla, vaikka nollasi BIOS:n. Todettiin, että emolevy rikkoutui ja tästä syystä vaihdettiin toimivat uudemmat komponentit tilalle.

Kone saatiin toimaan uusilla komponenteilla ja karsituilla BIOS-asetuksilla moitteetta, joten seuraavaksi voitiin asentaa RAID-ohjainkortti. Ohjainkortin

asentaminen tapahtui samalla tavalla kuin verkkokorttienkin ja samoja datakaapeleita voitiin hyödyntää kuin testausvaiheessa, koska ohjainkortissa on käytössä tavalliset SATA-liittimet. Lopuksi kone asetettiin käynnistymään RAID-ohjainkortilta.

Laitteistopohjaisen RAID-järjestelmän asennus

Jotta PfSensen voi asentaa, pitää ensiksi alustaa ja luoda RAID-ohjainkortin hallintaohjelmistolla RAID 5 -levyjärjestelmä. Välimuistipolitiikaksi valittiin datan kirjoittaminen kiintolevyille samanaikaisesti, kun se kirjoitetaan välimuistiin. Tällöin saavutetaan paras vikasietoisuus verrattuna siihen, että odotetaan välimuistin täyttymistä, jonka jälkeen kirjoitetaan kiintolevylle. Lisäksi kiintolevyt asetetaan käynnistymään porrastetusti. Tällöin saadaan korkeampi luotettavuus, mutta samalla saadaan estettyä huomattava virtapiikki, jos kaikki kiintolevyt käynnistyvät samanaikaisesti koneen käynnistyessä. Lisäksi virrankulutus saadaan tasaisemmaksi ja virtalähteen äkillistä ylirasitusta pystytään laskemaan. (Spin-up 2012.)

RAID-ohjainkortin mukana tuli ajurilevy, mutta sitä ei kuitenkaan otettu käyttöön, koska ajuri on tarkoitettu vanhemmalle järjestelmäversiolle. Valmistajan sivuilta ladattiin PfSensen kanssa yhteensopiva viimeisin ajuri, käyttöohje ja komentorivi- ja verkkopohjainen käyttöliittymän hallintaohjelma. Näin RAID-levyjärjestelmän kiintolevyjen tilaa pystytään seuraamaan vika- tai häiriötilanteissa. Samalla tarkistettiin RAID-ohjaimen ohjelmiston päivitystarve, mutta todettiin, että uusimmassa versiossa ei ole uusia ominaisuuksia tai korjauksia, joita pystytään hyödyntämään palomuurijärjestelmässä.

Jotta levyjärjestelmän pystyy käynnistämään, on sisällytettävä vaadittavat ajurit asennusmedialle eli tässä tapauksessa muistitikulle. Tarkoituksena on lisätä ajurit pfSensen-levykuvaan, jonka jälkeen se kopioidaan muistitikulle. PfSensen levykuva muistitikuille on ufs-tiedostojärjestelmämuodossa. Levykuvaa ei pysty oletuksena muokkaamaan Ubuntu-Linuxilla, mutta sen pystyy liittämään ja tiedostojärjestelmän tiedostoja pystyy lukemaan vain luku -tilassa. Jotta

Ubuntulla pystyisi muokkaamaan levykuvaa, täytyy järjestelmän kernel kääntää uudelleen ja lisätä siihen ufs-kirjoitusominaisuus. (Ghantoos 2009.)

Ensin ladataan, asennetaan ja puretaan uusin linux-lähdekoodi ja kopioidaan nykyisen järjestelmän asetustiedosto purettuun hakemistoon. Tämän jälkeen lisätään ufs-kirjoitustuki manuaalisesti ja käännetään hakemisto uudelleen paketiksi, joka asennetaan. Asetusvalikkoa ei tarvitse käyttää, mikäli muokkaa asetustiedostoa manuaalisesti. Tämän jälkeen järjestelmän voi käynnistää uudelleen uudella kernelillä ja tarkistaa kernelin version ”uname -r” komennolla. (Quiet Earth 2006.)

BSD-pohjaisessa järjestelmässä levykuva liitetään käyttämällä mdconfig-komentoa. Kyseistä komentoa ei ole Linuxissa, joten on käytettävä mount-komentoa levykuvan liittämiseen. Mount-komento antaa kuitenkin virheilmoituksia lohkolaitteesta, tiedostojärjestelmän väärästä tyypistä, valitsimen virheellisyydestä, viallisesta laitteen superlohkosta, puuttuvasta koodisivusta tai apuohjelmasta yritettäessä liittää levykuvaa. (LinuxQuestions.org 2007.)

Tutkittaessa tarkemmin kernelin viestipuskurissa olevia ajuriviestejä selvisi, että ufs-järjestelmätyyppiä ei ollut yksilöity (Dmesg 2012). Vaikka järjestelmän tyypiksi laittoi minkä vain eri vaihtoehdoista, antoi järjestelmä virheilmoituksen ”ufs_reader_super: bad magic number”. Ongelmaan ei löytynyt minkäänlaista ratkaisua manuaalista tai verkkohaulla, joten muistitikkulevykuvan muokkaaminen täytyi jättää sikseen ja saada muokatuksi CD-levykuvaversiota.

CD-levykuvan liittäminen tiedostojärjestelmän liitoskohtaan onnistui ja levykuvan sisältö kopioitiin paikallisen levyn hakemistoon. Samalla muutettiin kopioitujen tiedostojen ja hakemistojen käyttöoikeudet kaikille käytettäväksi. Tämän jälkeen kopioitiin RAID-ohjainkortin ajuritiedosto, komentorivihallintaliittymän asennustiedosto ja jälkiasennusskripti kopioidun levykuvahakemiston oikeisiin hakemistopolkuihin ja muokattiin järjestelmän käynnistysasetukset siten, että järjestelmän käynnistyessä ladataan RAID-ohjainkortin ajuri.

Hakemistosta pystyisi luomaan levykuvan, mutta mahdollisten ongelmien välttämiseksi muokatut tiedostot lisättiin levykuvaan suoraan, jotta ongelmia tulisi mahdollisimman vähän käynnistys- ja asennusvaiheessa. Levykuvan muokkaamiseen käytettiin ISO Master -optisten levyjen kirjoitusohjelmaa, jolla lisättiin asennustiedostot ja muokattiin käynnistystiedostot. Ensimmäisellä levyllä poltto ja asennusohjelma eivät toimineet, koska levy oli viallinen, mutta toisella levyllä pääsi valitsemaan käynnistysvalintoja.

Jostain syystä oletuskäynnistysvalinnalla järjestelmä jää jumiin, mutta komentokehoitevalinnalla pystyy tarkistamaan, että RAID-ajuri ei käynnistynyt. Ajurin kuitenkin pystyy lataamaan komentokehoitteessa ja käynnistämään järjestelmän sen jälkeen ilman virheilmoituksia. Järjestelmän käynnistyttyä pystyy käynnistämään asennusohjelman.

Käynnistymisen jälkeen järjestelmä asennetaan mukautettuna asennuksena. Kiintolevy osioidaan hyödyntäen sen koko kapasiteetti ja muuten käytetään oletusasetuksia. Swap-aliosiolle osoitetaan tuplasti käytössä olevan keskusmuistin verran. Tällöin järjestelmä ei mene jumiin, jos muisti loppuu kesken. Lopuksi valitaan tuki moniydinprosessoreille, jotta pystytään hyödyntämään laitteistoa täydellisesti. Asetusten mukauttamisen jälkeen järjestelmä asentuu ongelmitta ja ennen uudelleenkäynnistystä ilmoittaa web-käyttöliittymän kirjautumistiedot.

Järjestelmä ei kuitenkaan käynnisty, joten täytyy tehdä muokkauksia komentokehotteessa. Järjestelmäosio liitetään ja lisätään käynnistyksen asetustiedostoon ja moduuleihin RAID-ajurin käynnistystiedot. Ne eivät kuitenkaan korjaa virhettä käynnistyksessä. Järjestelmän käynnistyminen saatiin ratkaistua osittain sillä, että komentokehotteessa ladattiin RAID-ajuri, jonka jälkeen järjestelmä latautui, kuten pitääkin. Järjestelmää sammutettaessa kuitenkin ilmeni virheilmoitus, joka esti koneen sammumisen. Se ei ole toiminnan kannalta yhtä oleellinen ongelma kuin se, että järjestelmä ei käynnisty.

Seuraavaksi pitää selvittää, mikä aiheuttaa vian, joka estää koneen käynnistymisen normaalisti. Tällöin ei tarvitse jokaisella käynnistyskerralla erikseen ladata manuaalisesti RAID-ajuria. Sammumisen aikana tuleva virheilmoitus on myös saatava korjatuksi. Vikaa yritettiin selvittää kysymällä ongelmasta pfSensen foorumilta.

Foorumilla kerrottiin, että käynnistyskomennon kuuluu olla paikallisessa käynnistyksen asetustiedostossa eikä käynnistyksen oletusasetustiedostossa. Komennon lisääminen eri hakemistopolkuun ei kuitenkaan korjannut ongelmaa, koska järjestelmän käynnistyminen epäonnistui silti. Ongelmana voi olla myös se, että järjestelmä on esijulkaisuversio ja joitain vikoja siinä saattaa vielä esiintyä, joten järjestelmään kokeillaan asentaa uudempi laiteohjelmisto.

Uudempi laiteohjelmisto ei kuitenkaan korjannut käynnistyksen aikana tapahtuvaa virhettä, mutta sammutuksen estävän virheilmoituksen se poisti. Päivitys päivitti järjestelmäytimen hakemistossa olevat tiedostot, jotka nollaantuivat päivityksessä. Tämän vuoksi käynnistyksen asetustiedostoon täytyy lisätä RAID-ajurin käynnistämiskomento uudelleen, mutta sekään ei korjaa käynnistymisongelmaa. Ongelma voi olla myös siinä, että RAID-ajuri on väärässä hakemistopolussa. Loogisesti päättelemällä oikea hakemistopolku sille on käynnistysmoduuli-hakemisto, mutta järjestelmä ei lataa ajuria siltäkään.

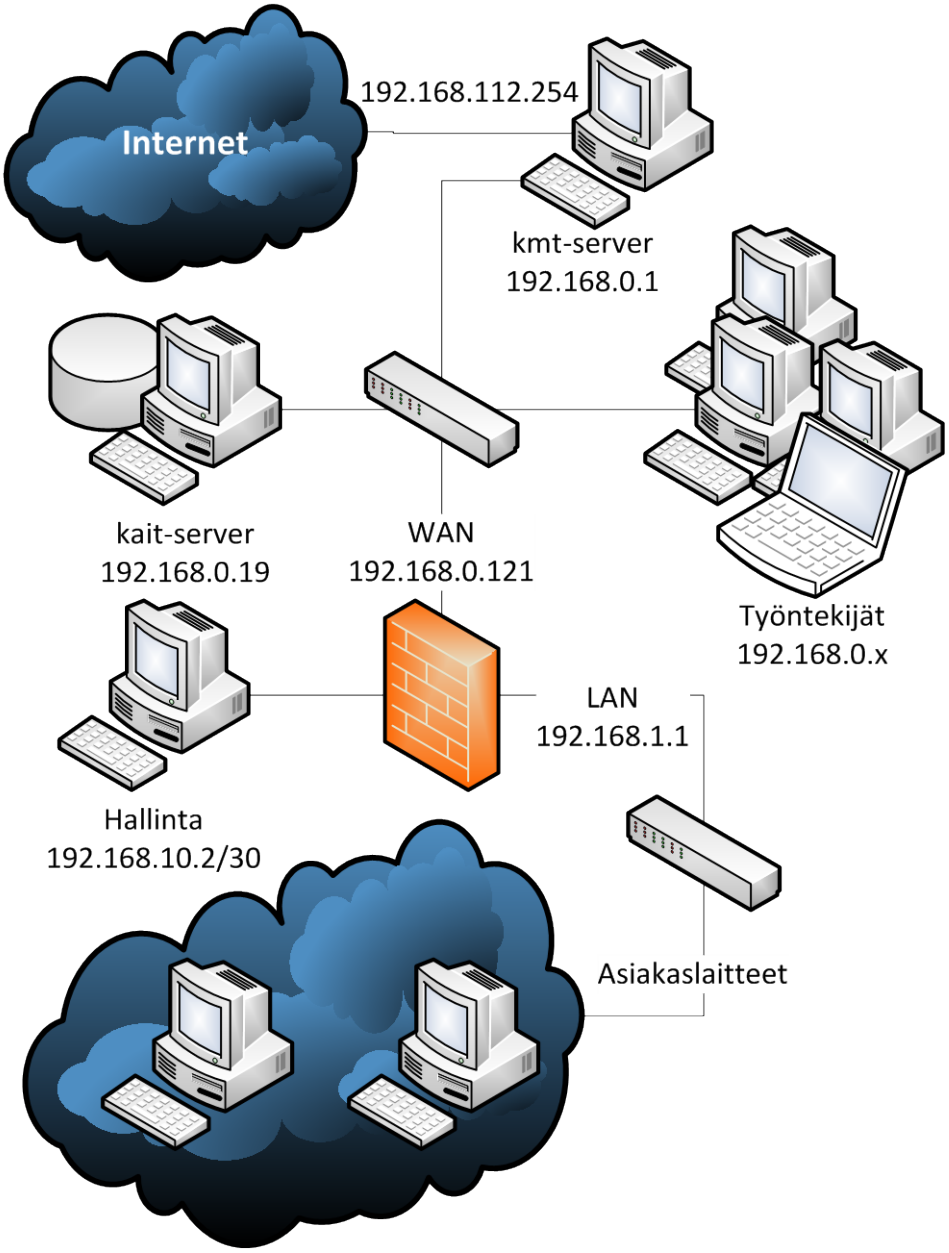
Järjestelmän asetustiedostoissa voi olla jokin merkintä, joka on voinut jäädä huomioimatta, joten kaikki asetustiedostot etsittiin ja luettiin läpi. Paikalliseen järjestelmän taustapalvelun konfiguraatiotietokantaan kokeiltiin lisätä RAID-ajurin latauskomento, mutta sekään ei auttanut. Koska ongelmaan ei löytynyt ratkaisua, päätettiin lukea valmistajan antamat ohjeet kertaalleen läpi kohta kohdalta. Ohjekirjasta ei löytynyt kohtaa, joka olisi jätetty väliin, mutta luettaessa jälkiasennusskriptin sisältöä huomio kiinnittyi kohtaan, jossa RAID-ajuri kopioitiin järjestelmän hakemistoon ilman versionumeroa. Järjestelmä käynnistyi normaalisti, kun ajurin nimestä poisti versionumeron.

Jotta RAID-ajuri ei poistuisi ja asetukset eivät palautuisi oletusarvoisiksi päivityksen yhteydessä, RAID-ajuri kopioitiin järjestelmäytimen ja moduuleiden

käynnistyshakemistoihin ja asetukset käynnistyksen latausasetuksiin ja paikallisiin latausasetuksiin. Järjestelmä käynnistyi uuden laiteohjelmistopäivityksen jälkeen normaalisti, joten järjestelmää voi pitää ajan tasalla ilman ylimääräistä säätöä.

Nyt kun järjestelmä saatiin asennetuksi, voidaan suunnitella jatkotoimenpiteitä. Palomuurin verkotus pitää saada järkevästi luoduksi ja tutustua palomuurin sallintamäärityksiin, jotta erilaiset virustentorjuntaohjelmat ja haittaohjelmien poistotyökalut pääsevät asiakaskoneilta päivittämään tietokantansa. Kiintolevyjärjestelmän tarkkailuohjelmisto on myös asennettava, jotta kiintolevyjen tilaa voidaan seurata mahdollisten levyrikkojen varalta.

8 PALOMUURIN ASETUSTEN ASETTAMINEN



Kuva 3. KMT:n looginen verkkokuva palomuurijärjestelmällä.

KMT:n verkosta rakennetaan kuvan 3 kaltainen ratkaisu, jossa palomuuriin tulevat verkot pitää määritellä siten, että työntekijöiden koneet ja palvelinkoneet ulkoverkosta eivät pääse kirjautumaan palomuuriin tai liikennöimään sen kautta. Hallintaverkossa on ainoastaan yksi kone, jolla pääsee hallintaliittymään käsiksi ja asiakaslaitteiden verkko on suodatettu siten, että yksikään asiakaslaite ei näe

toista ja laitteet pääsevät päivittämään huollossa tarvittavat ohjelmat ja asentamaan päivitykset.

Palomuuriin kytketyt verkot asennetaan eri aliverkkoihin, jolloin eri verkot eivät näe toisiaan. Asiakaskoneet täytyy kytkeä kytkimeen, jotta monta laitetta pystytään huoltamaan samanaikaisesti. Tämä saattaa aiheuttaa sen, että koneet näkevät toisensa samassa aliverkossa. Ongelma voidaan ratkaista siten, että muokataan palomuurisäännöistä jokainen kytkimen portti omaksi aliverkoksi jakamalla niihin DHCP:llä vain yksi osoite. Vaihtoehtoisesti verkot voidaan erottaa toisistaan virtuaaliverkoilla.

Palomuurin säätämistä aloitettiin testaamalla eri vaihtoehtoja. Palomuurin ulko- ja sisäverkkoon annettiin ensin IP-osoitteet, jotta web-liittymään pääsee käsiksi muokkaamaan asetuksia ja testaamaan palomuurisääntöjä. Jostakin syystä palomuuriin ei saa yhteyttä, joten jätetään ainoastaan ulkoverkon liitäntä toimimaan. Näin pystytään selvittämään estävätkö muut liitännät laitteen toiminnan. Tämän jälkeen palomuurin web-liittymään pääsee kirjautumaan ja tutustumaan tarkemmin erilaisiin valikkoihin ja valintoihin. Jostakin syystä web-liittymä vastaa ainoastaan ulkoverkosta, vaikka muutkin verkot kytketään toimintaan.

Asetuksista säädetään palomuuri oikeaan aikavyöhykkeeseen, asetetaan ulkoverkon osoitteeksi sama osoite kuin palvelimelta saatu osoite ja poistetaan palomuurin DHCP käytöstä. Asiakasverkko ja ulkoverkkoverkko ovat samassa aliverkossa, jolloin NAT-kone jakaa asiakasverkolle osoitteet. Lisäksi on selvitettävä, miten palvelimelle asetetaan kiinteä IP-osoite, miten ulkoverkon IP-osoitteen saa vaihdetuksi ja toimimaan jollakin muulla arvolla, jonka osoitealueen palvelin jakaa. Asiakasverkkoon asetettiin oletusyhdyskäytäväksi palomuurin asiakasverkon osoite ja nimipalvelimiksi AMK:n nimipalvelimet, mutta yhteys asiakasverkosta internetiin ei siltikään toiminut.

Verkkojen asetuksia yritettiin säätää, jotta asiakasverkosta pääsisi ulkoverkkoon, mutta web-liittymään ei päässyt asetusten muokkaamisen jälkeen. Nollattiin asetukset poistamalla kaikki verkot ja lisäämällä ne uudelleen.

Perusasetusesimerkkien dokumentista ja asennusohjeesta etsittiin neuvoja, kuinka järjestelmän saa toimintaan. Koska käytössä on jo natattu yksityisverkko, kokeillaan NAT-asetusten ottamista kokonaan pois käytöstä. Asetuksen muutos ei vaikuttanut mihinkään, joten muutetaan se takaisin oletusarvoonsa.

Koska järjestelmän hallintaan tarvitaan hallintaliittymä, käyttöön otettiin kolmas verkkokortti. Liitännän asetuksia muokattiin siten, että hallintaverkkoon tulee yksi aliverkko, johon ei ole mahdollista liittää mitään muuta kuin palomuuri ja hallintapääte. Lisäksi testattiin hallintapäätteeltä, että palomuuriin saa yhteyden. Asetuksia päätettiin muokata, kun asiakasverkko saadaan toimintaan.

Tutkitaan, mitä palomuurin eri verkkoliitännät ilmoittavat tilakseen. Asiakasverkon puoli ilmoittaa, että oma liitäntä ja ulkoverkon liitännät toimivat oikein, mutta ulkoverkko ilmoittaa, että asiakasverkon kaapelia ei ole kytketty. Tarkistettiin, että kaapelit ovat ehjiä ja ne on kytketty kunnolla verkkokortteihin. Lisäksi vaihdettiin toinen verkkokortti rikkinäiseksi epäillyn tilalle, mutta sama virheilmoitus toistui silti. Koska laitteistossa ei löytynyt vikaa, täytyy vian olla verkkokorttien välisen linkin reitityksessä. Kokeiltiin reititysten lisäämistä asiakasverkon ja ulkoverkon välille, mutta kyseisiä asetuksia ei tarvinnut muokata.

Verkko alkoi toimia, kun palautti NAT-asetukset oletuksiksi ja jätti vain ulkoverkon verkkoliitäntään oletusyhdyskäytävän määrityksen ja poisti muista verkkoliitännöistä oletusyhdyskäytävän merkinnän (Multi-LAN Setup 2010). Internet-yhteys toimi niin kauan, kunnes palomuurisäännöistä poistettiin asiakasverkosta ja asiakasverkkoon sallittu kaikki liikenne, joka on hyvä asia, koska tällöin palomuurisäännöt toimivat. Asiakasverkosta poistetaan DHCP:n osoitteiden jakaminen, jolloin jokaiseen asiakaskoneeseen täytyy käsin asettaa verkkoasetukset ja saadaan testattua, miten se toimii käytännössä.

PfSensen perusasetusten esimerkkidokumentista tutkitaan esimerkkejä peruspalomuurisäännöistä. Ohje on aika suppea, mutta perusperiaate käy siitä selville. Palomuurisäännöt koskevat aina verkkokortille tulevaa liikennettä. Säännöistä tarvitaan ainoastaan tavallisen ja salatun verkkoliikenteen sallinta

sekä nimipalvelimille olevan liikenteen sallinta. (Example basic configuration 2007.)

Asetetaan asiakasverkolle ja hallintaverkolle yksityis- ja ei-hyväksyttyjen IP-osoitteiden eli bogon-verkkojen esto, jotta turha liikenne saadaan pois. Samalla kuitenkin huomataan, että verkko ei toimi. Tämä johtuu siitä, että ulko- ja sisäverkko ovat kummatkin yksityisverkossa, joten sallitaan yksityisverkkojen liikenne ja verkko toimii jälleen.

Asiakasverkosta poistetaan kaiken liikenteen sallinta, jotta voidaan tarkistaa järjestelmän lokitiedoista palomuurin tilatiedoista sallittava liikenne. Asetuksella ei tuntunut olevan minkäänlaista vaikutusta liikenteen suodatukseen, joten poistetaan kaikki mahdolliset sallinnat ulko- ja sisäverkosta, mutta sallitaan ainoastaan TCP-liikenne. Palomuuriasetuksen hyväksymisen jälkeen web-liittymään ei päässyt mitenkään. Tämän seurauksena palomuurin konsolin avulla piti löytää keino saada palomuurisäännöt nollattua.

PfSensen dokumenteista löytyi ohje, jolla saa tilapäisesti vaihdettua palomuurisääntöjä. Kytkemällä palomuurin pois päältä verkko toimii, mutta hetken päästä säännöt palautuvat takaisin. Muokkaamalla asiakasverkon säännöt sallituksi pystyy kirjautumaan web-liittymään ja korjaamaan palomuurisäännöt siten, että palomuurin asetuksiin pääsee käsiksi. (I locked myself out of the WebGUI, help! 2011.)

Projektipäällikön kanssa keskusteltiin, mitä asioita pitäisi seuraavaksi selvittää. Pitäisi selvittää, onko mahdollista käyttää VLAN:eja, luoda palomuurille sallittujen osoitteiden valkoisen ja kiellettyjen osoitteiden mustan listan ja pystyykö sen tekemään manuaalisesti suodatusasetusten tekstitiedostoon. VLAN:it pystytään asettamaan palomuurin portteihin, mikäli sille on tarvetta.

Tutkittiin, voiko pfSensen säännöt luoda tekstitiedostoon vai onko käytettävä web-liittymää. Säännöt on tarkoitettu tehtäväksi web-liittymän kautta eikä tekstitiedostoon. Säännöt on mahdollista kirjoittaa tekstitiedostoon, mutta tälle ei pitäisi olla tarvetta, koska vastaavat toimenpiteet on mahdollista tehdä graafisessa käyttöliittymässäkin. (How can I edit the PF ruleset 2009.)

Järjestelmästä ei kannata tehdä turhan monimutkaista. Verkko asetetaan toimimaan siten, että ulkoverkosta ei pääse palomuurin web-liittymään, mutta muu liikenne on sallittu. Asiakasverkosta pääsee vain päivittämään tietokoneiden järjestelmät ja huolto-ohjelmat ja muu liikenne voidaan sallia vain tarvittaessa koneen IP-osoitteen perusteella. Hallintaverkosta tulee päästä ainoastaan palomuurin web-liittymään, jonka hallinnointi on täysin KMT:n projektipäällikön vastuulla.

Palomuurisääntöjen asetus

DHCP-palvelu otettiin käyttöön asiakasverkossa, koska laitteet ovat eri aliverkossa eivätkä saa enää IP-osoitetta NAT-koneelta. Sitten tarkistettiin, että tietokoneet saavat IP-osoitteen. Tämän jälkeen testattiin palomuurisääntöjä sallien ensin kaikki liikenne ja sitten TCP-liikenne, UDP-liikenne ja TCP- ja UDP-liikenne. Tämän jälkeen testattiin liikenne tiettyyn verkko-osoitteeseen ja tietystä verkko-osoitteesta palomuuriin.

Asiakasverkolta sallitaan yhteys DNS-palvelimille ja kaikilla protokollilla kaikista osoitteista kaikkiin osoitteisiin, jolloin verkkoliikenne toimii rajoittamattomana, kuten pitääkin. Tämän jälkeen muokataan sääntöä siten, että sallitaan ainoastaan TCP- ja UDP-liikenne ja verkkoliikenne toimii yhä. Lopuksi, kun testaus suoritetaan erikseen TCP- ja UDP-liikenteen sallinnoilla, testatut Googlen ja uutissivustojen verkkosivustot eivät aukea.

Testausta jatketaan hyväksymällä kaikki TCP- ja UDP liikenne, mutta vain tiettyyn osoitteeseen. Testiosoitteeksi valittiin Hewlett-Packardin (HP) verkko-osoite www.hp.fi, koska kyseiseltä sivustolta voi myös ladata ohjelmistopäivityksiä. Selvitetään HP:n verkko-osoitteen IP-osoite pingaamalla HP:n kotisivulle, jonka jälkeen testataan palomuurisääntöjen toimivuus saatuun IP-osoitteeseen.

Jostain syystä sivu ei lataudu, joten palomuurin käyttäytymistä testataan siten, että sallitaan kaikki verkko-osoitteet, joiden kautta liikenne kulkee kohdeosoitteeseen. Kaikkien verkkolaitteiden IP-osoitteet, jotka ovat lähde- ja kohdeosoitteiden välillä, saadaan käyttämällä komentoa traceroute. Kun kaikki

IP-osoitteet on saatu, ne lisätään palomuurisääntöihin lähtöosoitteesta alkaen. Palomuuri lukee säännöt järjestyksessä rivi riviltä, jolloin väärässä järjestyksessä olevat säännöt saattavat katkaista liikenteen etenemisen ensimmäisen verkkolaitteen jälkeen.

Vaikka kaikki tracerouten osoitteet lisättiin sallituiksi, ei HP:n sivuille kuitenkaan päässyt. Kun kohdeosoitetta tarkasteltiin tarkemmin, se oli erilainen kuin aiemmin saatu IP-osoite ping-komennolla. Tästä voimme vetää johtopäätöksen, että HP:lla on käytössään useampi palvelin. Silloin kaikkien HP:n palvelimien osoitteet on lisättävä sallituiksi, jotta sivut aukeaisivat. Tästä syystä testisivuksi vaihdettiin Turun ammattikorkeakoulun kotisivu. Kun HP:n IP-osoitteen muutti Turun ammattikorkeakoulun IP-osoitteeksi, uudet sivut aukesivat ongelmitta.

Kun yhteys alkoi toimia, voitiin selvittää, tarvitseeko lähde- ja kohdeosoitteiden välisiä verkko-osoitteita sallia. Vähentämällä sallittuja osoitteita yksitellen nähdään, onko niille tarvetta. Sääntöjen poistaminen aloitettiin loppupäästä ja yhteys kohdeosoitteeseen testattiin jokaisen poiston jälkeen. Käytöstä voitiin poistaa kaikki säännöt, jotka koskivat lähde- ja kohdeosoitteen välillä olevia IP-osoitteita ja yhteys toimi silti. Tästä voidaan tehdä johtopäätös, että verkkosivu saadaan latautumaan, kunhan pelkkä kohdeosoite on määritelty asiakasverkosta TCP- ja UDP-protokollilla. Näin asian pitääkin olla.

Kun palomuurin toiminta saatiin selvitetyksi, voitiin aloittaa päivityspalvelimien IP-osoitteiden selvittäminen. Selvittäminen aloitettiin Windowsin päivityspalvelimista. PfSensen foorumeilta löytyi samasta aiheesta oleva kysymys, jossa käsiteltiin päivitysosoitteiden lisäämistä omaksi alias-nimeksi (PfSense 2012). Alias-nimen käyttöä kokeiltiin luomalla Windows-päivityksille oma alias. Ongelmaksi muodostui se, minkä tyyppinen alias tulisi valita. Host vaatii IP-osoitteen, network vaatii verkkoalueen ja -peitteen. Loogisesti ajateltuna pitäisi käyttää URL- tai URL table -valintaa, koska Microsoft ei anna palveluiden IP-osoitteita, vaan ainoastaan URL-verkko-osoitteet (Microsoft 2012). URL-valinnalla järjestelmä ilmoittaa verkko-osoitteen virheelliseksi sekä http-protokollan kanssa että ilman sitä. URL table -valinnalla alias saatiin

luoduksi, mutta palomuuri varoitti puuttuvasta sääntötiedostosta ja varoituksen takia kaikki palomuurisäännöt olivat pois käytöstä.

Palomuuri päätettiin käynnistää uudelleen, koska muokkaus saattoi vaatia uudelleenkäynnistystä. Kun kone käynnistyi uudelleen, se jäi jumiin kesken käynnistyksen ja sammui jonkin ajan kuluttua itsestään. Sama ongelma toistui, valitsi minkä tahansa käynnistysvaihtoehdon. Järjestelmän käynnistys jäi aina jumiin PCI-laitteiden alustuksen jälkeen. Vian voitiin päätellä liittyvän jollakin tavalla PCI-laitteisiin. Kokeiltiin ensin verkkokorttien verkkokaapelien irroittamista ja järjestelmän käynnistämistä uudelleen. Kaikeksi onneksi palomuuri käynnistyi normaalisti. Tämän jälkeen kokeiltiin verkkokaapelien uudelleen liittämistä ja järjestelmän käynnistämistä uudelleen. Jumiutumista ei kuitenkaan saatu toistetuksi.

Kun palomuuri toimi taas normaalisti, alias-asetukset avattiin. Palomuuri oli poistanut aiemmin luodun URL-taulun, joten tutkittiin tarkemmin PfSensen sivuilta, miten verkko-osoitteista luodaan oma alias. Dokumentissa ei mainita tarkkaan, millä tavalla verkko-osoitteen suodatussääntö kuuluu luoda. Palomuurisääntölistan saa kuitenkin siistimmäksi, kun käyttää alias-ryhmiä. (Aliases 2009.)

Foorumikirjoituksen perusteella selvisi, että URL- ja URL Table -kenttiin määritellään verkko-osoite tai hakemistopolussa oleva tiedosto, josta löytyvät kaikki käsiteltävät IP-osoitteet. Jotta tiettyjä verkko-osoitteita voidaan käsitellä ilman erillistä tiedostolistausta, käsittelyyn käytetään alias-ryhmän host tai network valintaa kirjoittamalla verkko-osoite tai verkkoalue kenttään, jossa pyydetään IP-osoitetta. (PfSense 2010.)

Alias Host-valintaa kokeillaan Turun ammattikorkeakoulun verkkosivulla ja sallitaan liikenne vain alias-ryhmän osoitteeseen. Palomuuri päästi odotetusti liikenteen läpi ammattikorkeakoulun sivuille. Tämän jälkeen on mahdollista helposti lisätä tarvittavia verkko-osoitteita alias-ryhmiin, jolloin palomuurisääntöihin ei tarvitse tehdä muutoksia. Seuraavaksi pitää selvittää jäljellä olevien ohjelmien päivityspalveluiden osoitteet.

F-Securen virustunnistetietokantojen päivityspalvelinten osoitteet löytyivät helposti Google-hakujen kautta (F-Secure 2012). Microsoftin päivitysosoitteista suositeltiin jättämään asteriskilla eli tähtimerkillä määritelty verkko-osoitteen osa pois. (PfSense 2012). Nortonin ja Panda Cloudin päivityspalvelimien verkko-osoitteita ei löytynyt tuotetukisivuilta tai verkkohakujen avulla, joten niitä kysyttiin suoraan Nortonin ja Panda Securityn asiakastuesta. Symantecin Norton-tuotteilla on ainoastaan yksi osoite ja Pandalla useita osoitteita, joista voidaan ladata päivitykset (Symantec 28.9.2012; Panda 8.10.2012.). Avastin osoitteet voidaan lisätä käyttämällä aiemmin kokeiltua URL aliasta, koska Avastin käyttämät palvelinosoitteet on listattu ohjelman asennushakemiston tiedostoon (Avast 2009). Ubuntun päivityspalvelimet löytyvät järjestelmän asetustiedostosta (Sources.list 2012). SUPERAntiSpywaren päivitysosoite kerrottiin tuotteen tukisivuilta ja Malwarebytesin päivitysosoitteet löytyivät sivuston foorumilta (SUPERAntiSpyware 2012; Malwarebytes 2011).

Osoitteiden toimivuutta kokeiltiin lisäämällä ne palomuurin Alias-ryhmään. Tarkat verkko-osoitteet ja verkkoalueet toimivat ongelmitta. SUPERAntiSpywaren kanssa ilmeni ongelmana se, että KMT:n käytössä oleva versio on ilmaisversio, jota ei voi päivittää. Ohjelman päivittämistä ei pystynyt siten testaamaan. Malwarebytesin verkko-osoitteet eivät toimineet, joten selvitettiin ohjelman päivityspalvelimen osoite käynnistämällä ohjelman päivitystoiminto ja katsomalla palomuurin lokista estetty päivityspalvelimen verkko-osoite.

Kaikkein suurin ongelma muodostui Windowsin ja Microsoftin tuotteiden päivittämisestä. Testattavana ollutta Windows XP -konetta ei saanut päivitetyksi muokatuilla Microsoftin verkko-osoitteilla. Koska asteriskia ei voinut käyttää ja ilman sitä päivittäminen ei onnistu, Microsoftin päivitysosoitteet pitää tietoturvasyistä lisätä yksitellen sallituiksi osoitteiksi. IP-osoitteiden kohdentamisesta oikeaan palveluun on ongelmana se, että Microsoftin IP-osoitteet eivät vastaa ping-, traceroute- tai nslookup-kyselyihin.

Selvitystä ei myöskään helpota se, että Microsoftin päivityspalvelimen IP-osoite voi vaihtua samana päivänä muutaman kerran aivan toiseen verkko-

osoitteeseen ja vaihtoehtoisia verkko-osoitteita on useita tuhansia. Lisäksi Windows Update ei ole käytössä vikasietotilassa, jolloin muut palvelut saataisiin pois häiritsemästä verkkoliikennettä.

Palomuuri on näiden toimenpiteiden jälkeen käyttövalmis. Ainoaksi ongelmaksi jäi se, että Microsoftin tuotteiden päivittämiseen ei löytynyt helppokäyttöistä ja kätevää ratkaisua. Jatkoprojektina voisi ajatella mahdollisuutta lisätä palomuuriin Windows-päivitysten tallennustoiminto palomuurin kiintolevylle välimuistiin. Sellainen pitäisi olla mahdollista squid-ohjelmalla, joka tallentaa verkkosivustoja tai tässä tapauksessa Microsoftin päivitystiedostot paikallisen koneen välimuistiin, josta ne saadaan nopeasti asiakaskoneiden käyttöön. (Squid (software) 2012.)

9 YHTEENVETO

Opinnäytetyön tavoitteena oli rakentaa palomuurijärjestelmä, joka suojaa huollettavia asiakaslaitteita ja estää mahdollisesti saastuneiden asiakaslaitteiden aiheuttaman KMT:n verkon kuormituksen haittaliikenteeltä. Lisäksi se suojaa verkkoon kytkettyjä laitteita haitallisilta ohjelmilta. Tavoitteena oli rakentaa palomuuri järjestelmäkehityksen elinkaarimallin mukaisesti noudattaen annettuja vaatimusmäärittelyjä. Lisäksi luotiin palomuurijärjestelmän asennus- ja käyttöohjeistus.

Vaatimusmäärittelyn mukaan estetyn verkkoliikenteen lokitiedot tulee säilyttää noin viikon ajan, mutta sallittu liikenne määritellään myöhemmin. Verkkoyhteydet tulee pystyä määrittelemään mustalle ja valkoiselle listalle. Järjestelmällä pitää olla selkeä ulkoasu, yksinkertainen hallinta ja käyttöliittymä, josta on mahdollisuus lokien seuraamiseen. Lisäksi haluttiin, että järjestelmään asennetaan proxy-ohjelmisto, järjestelmä pohjautuu maksuttomaan Unixiin, BSD:hen tai vastaavaan käyttöjärjestelmään, laitteessa on kaksi verkkokorttia ja estetty etähallinta. Toiminnallisuuden on säilyttävä, vaikka järjestelmän päivittää.

Mustan ja valkoisen listan tarkoituksena on estää laitteita näkemästä toisiaan. Ainoastaan päivittämispalveluiden liikenne sallitaan, mutta muu liikenne estetään. Laitteet voidaan siirtää valkoiselle listalle vain käsin ja merkinnät vanhenevat automaattisesti viikon välein. Osoitteenmuunnosta ei aseteta, koska ip-osoitteet jaetaan NAT-laitteelta.

Vaatimusmäärittelyiden jälkeen pyrittiin selvittämään palomuurin toimintaperiaatteet, miten ja minkälaisissa käyttöympäristöissä sitä käytännössä pääasiassa käytetään. Lisäksi käytiin läpi palomuurin erilaisia tekniikoita ja heikkouksia mm. salauksen osalta.

Palomuurijärjestelmän laitekomponentit hankittiin vaatimusmäärittelyjen mukaisesti ja testattiin, että kone käynnistyy ja toimii ja komponentit kestävät pitkän rasitustestin. Lisäksi selvitettiin KMT:n verkon lähtötilanne, jotta saataisiin

parempi käsitys siitä, miten ympäristö toimii ja kuinka palomuurijärjestelmä kannattaisi siihen asentaa.

Ympäristöön tutustumisen jälkeen vertailtiin palomuurijärjestelmiä. Vertailtavaksi otettiin vain järjestelmät, jotka sopivat vaatimusmäärittelyn kriteereihin. Vertailun ulkopuolelle jätettiin kaupalliset, ei-aktiiviset, täysin komentorivipohjaiset, disketti- ja CD-pohjaiset järjestelmät. Tarkoituksena oli valita ilmainen, tuettu, helppokäyttöinen ja muokattava järjestelmä, jossa onnistuu kiintolevyasennus. Valinta kohdistui pfSense-palomuurijärjestelmään, koska se oli ainut järjestelmä, joka vastasi vaatimusmäärittelyn kriteereihin.

Palomuurijärjestelmän asennus aloitettiin selvittämällä aluksi eri RAID-järjestelmien toiminta ja sitten vertailtiin niitä keskenään. RAID-järjestelmää lähdettiin luomaan ensin ohjelmistopohjaisella RAID-järjestelmällä, mutta sen huomattiin olevan usean epäonnistumisen jälkeen liian vaikeaa. RAID-järjestelmä vaihdettiin laitteistopohjaiseksi ostamalla koneeseen RAID-ohjainkortti. Järjestelmä saatiin asennetuksi, mutta RAID-ohjainkortin ajurin latautumisen kanssa ilmeni ongelma. Ongelma saatiin kuitenkin ratkaistuksi, kun perehdyttiin asennusskriptiin tarkemmin.

Palomuurijärjestelmän asentamisen jälkeen suunniteltiin KMT:n verkkokuva, johon on asennettu palomuuri ja jonka mukaan verkko lopulta rakennettiin. Palomuurin verkkoasetukset määriteltiin vaatimusmäärittelyn ja verkkokuvan mukaisiksi. Erilaisia vaihtoehtoja kokeiltiin, kunnes toimivat asetukset löytyivät. Tämän jälkeen selvitettiin palomuurisääntöjen ja alias-ryhmien toiminta, jonka jälkeen voitiin tehdä päivitysosoitteisiin kohdistuvat palomuurisallinnat. Palomuuri saatiin toimimaan toivotulla tavalla, paitsi Microsoftin päivitysosoitteiden kanssa, koska päivityspalvelinten verkko-osoitteet eivät toimineet ohjeiden mukaisesti.

Vaatimusmäärittelyä jouduttiin muokkaamaan työn edetessä, kun selvisi tarkemmin, miten palomuurijärjestelmä toimi. Liikenteen jakaminen eri listoihin saatiin toteutetuksi, mutta eri tavalla kuin oli ajateltu. Proxy-ohjelmiston asennus karsittiin vaatimusmäärittelyistä, koska siitä olisi tullut liian laaja. Ohjelmiston

saa kuitenkin asennetuksi käyttämällä squid-ohjelmaa, joka tallentaa verkkosivustoja tai tiedostoja palomuurin välimuistiin. Sieltä ne saadaan nopeasti asiakaskoneiden käyttöön.

Palomuurijärjestelmän rakentaminen sinänsä ei ollut kovin monimutkainen, mutta vaatimusmäärittely RAID-ohjelmiston osalta hankaloitti työn etenemistä huomattavasti. Järjestelmä saatiin kuitenkin käyttökuntoon useista järjestelmän asennuksen aikana ilmenneistä vastoinkäymisistä huolimatta.

LÄHTEET

Aliases 2009. PfSense. Viitattu 11.9.2012 http://doc.pfsense.org/index.php/Aliases.

Avast 2009. Defining update addresses in the firewall settings. Viitattu 9.10.2012 https://support.avast.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=316.

Buechler, C. & Pingle, J. 2009. PfSense: The Definitive Guide. Reed Media Services.

Comparison of firewalls 2012. Wikipedia. Viitattu 28.2.2012 http://en.wikipedia.org/wiki/Comparison_of_firewalls.

Dmesg 2012. Wikipedia. Viitattu 7.3.2012 http://en.wikipedia.org/wiki/Dmesg.

Endian 2011a. Download - Which Edition is Right for You?. Viitattu 17.5.2011 http://www.endian.com/us/community/download/.

Endian 2011b. Software Appliances. Viitattu 3.5.2011 http://www.endian.com/us/products/security-gateways-utm/software-appliances/.

Example basic configuration 2007. PfSense. Viitattu 4.10.2011 http://doc.pfsense.org/index.php/Example_basic_configuration.

Firewall distributions 2010. LinuxQuestions.org. Viitattu 3.5.2011 http://wiki.linuxquestions.org/wiki/Firewall_distributions.

FreeBSD 2011. FreeBSD Handbook Chapter 4 UNIX Basics - Disk Organization. Viitattu 24.5.2011 http://www.freebsd.org/doc/handbook/disk-organization.html.

F-Secure 2012. F-Secure virus definition database update server addresses. Viitattu 23.9.2012 http://www.f-secure.com/fi/web/business_fi/support/article/kba/2712

Ghantoos 2009. Mounting UFS in read/write under Linux (debian). Viitattu 25.5.2011 http://ghantoos.org/2009/04/04/mounting-ufs-in-readwrite-under-linux.

How can I edit the PF ruleset 2009. PfSense. Viitattu 26.10.2011 http://doc.pfsense.org/index.php/How_can_I_edit_the_PF_ruleset.

I locked myself out of the WebGUI, help! 2011. PfSense. Viitattu 5.10.2011 http://doc.pfsense.org/index.php/I_locked_myself_out_of_the_WebGUI,_help!

InetDaemon 2012. Using Traceroute. Viitattu 28.2.2012 http://www.inetdaemon.com/tutorials/troubleshooting/tools/traceroute/using_traceroute.shtml.

Kissel, R; Stine, K; Scholl, M; Rossman, H; Fahlsing, J & Gulick, J. 2008. Security Considerations in the System Development Life Cycle. Viitattu 16.10.2011 http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf.

LinuxQuestions.org 2007. How to mount a FreeBSD image in Linux. Viitattu 27.5.2011 http://www.linuxquestions.org/questions/programming-9/how-to-mount-a-freebsd-image-in-linux-516058/.

Looginen taltiohallinta 2012. Wikipedia. Viitattu 5.3.2012 http://fi.wikipedia.org/wiki/Looginen_taltiohallinta.

M0n0wall 2011. Hardware. Viitattu 3.5.2011 http://m0n0.ch/wall/hardware.php.

Malwarebytes 2011. Allowing Updates from Malwarebytes Servers. Viitattu 11.10.2012 http://forums.malwarebytes.org/index.php?showtopic=91439.

Microsoft 2011. Security TechCenter - Firewalls. Viitattu 8.5.2011 http://technet.microsoft.com/en-us/library/cc700820.aspx.

Microsoft 2012. Windows update IP addresses range and subnet mask for Windows Server 2008. Viitattu 10.9.2012 http://social.technet.microsoft.com/Forums/eu/winserversecurity/thread/b596aa81-2775-496c-b159-dcfc5c5bf22d.

Multi-LAN Setup 2010. PfSense. Viitattu 3.9.2011 doc.pfsense.org/index.php/Multi-LAN_Setup.

Palomuuri 2012. Wikipedia. Viitattu 29.10.2012 http://fi.wikipedia.org/wiki/Palomuuri.

PfSense 2010. Alias. Viitattu 21.9.2012 http://forum.pfsense.org/index.php?topic=29091.0.

PfSense 2011a. Hardware Sizing Guidance. Viitattu 3.5.2011 http://www.pfsense.org/index.php?option=com_content&task=view&id=52&Itemid=49.

PfSense 2011b. History. Viitattu 19.5.2011 http://www.pfsense.org/index.php?option=com_content&task=view&id=68&Itemid=76.

Pfsense 2011c. Home. Viitattu 19.5.2011 http://www.pfsense.org/index.php.

PfSense 2011d. Minimum Hardware Requirements. Viitattu 3.5.2011 http://www.pfsense.org/index.php?option=com_content&task=view&id=45&Itemid=48.

PfSense 2012. DMZ rule/out, allow windows update servers only. Viitattu 9.9.2012 http://forum.pfsense.org/index.php?topic=40691.0.

Quiet Earth 2006. Ubuntu: Compiling a custom kernel. Viitattu 26.5.2011 http://www.quietearth.us/articles/2006/09/15/Ubuntu-Compiling-a-custom-kernel.

Radack 2009. The System Development Life Cycle (SDLC). Viitattu 16.10.2011 http://csrc.nist.gov/publications/nistbul/april2009_system-development-life-cycle.pdf.

Redundant array of independent disks 2012. Wikipedia. Viitattu 4.3.2012 http://en.wikipedia.org/wiki/Redundant_array_of_independent_disks

Schmut 2011. FreeBSD Software RAID Howto. Viitattu 23.5.2011 http://www.schmut.com/howto/freebsd-software-raid-howto

Smoothwall 2011a. Express Feature List. Viitattu 3.5.2011 http://www.smoothwall.org/about/express-feature-list/.

Smoothwall 2011b. Feature Comparison Chart. Viitattu 18.5.2011 http://www.smoothwall.org/about/feature-comparison-chart/.

Sources.list 2012. Linux.fi. Viitattu 10.10.2012 http://linux.fi/wiki/Sources.list

Spin-up 2012. Wikipedia. Viitattu 6.3.2012 http://en.wikipedia.org/wiki/Spin-up.

Squid (software). Wikipedia. Viitattu 2.11.2012 http://en.wikipedia.org/wiki/Squid_(software).

SUPERAntiSpyware 2012. Frequently Asked Questions - How do I configure my proxy to allow SUPERAntiSpyware to connect to the Internet?. Viitattu 11.10.2012 http://www.superantispyware.com/supportfaqdisplay.html?faq=53.

Tarpit (networking). Wikipedia. Viitattu 28.2.2012 http://en.wikipedia.org/wiki/Tarpit_(networking).

Vinum volume manager 2012. Wikipedia. Viitattu 29.2.2012 http://en.wikipedia.org/wiki/Vinum_volume_manager.

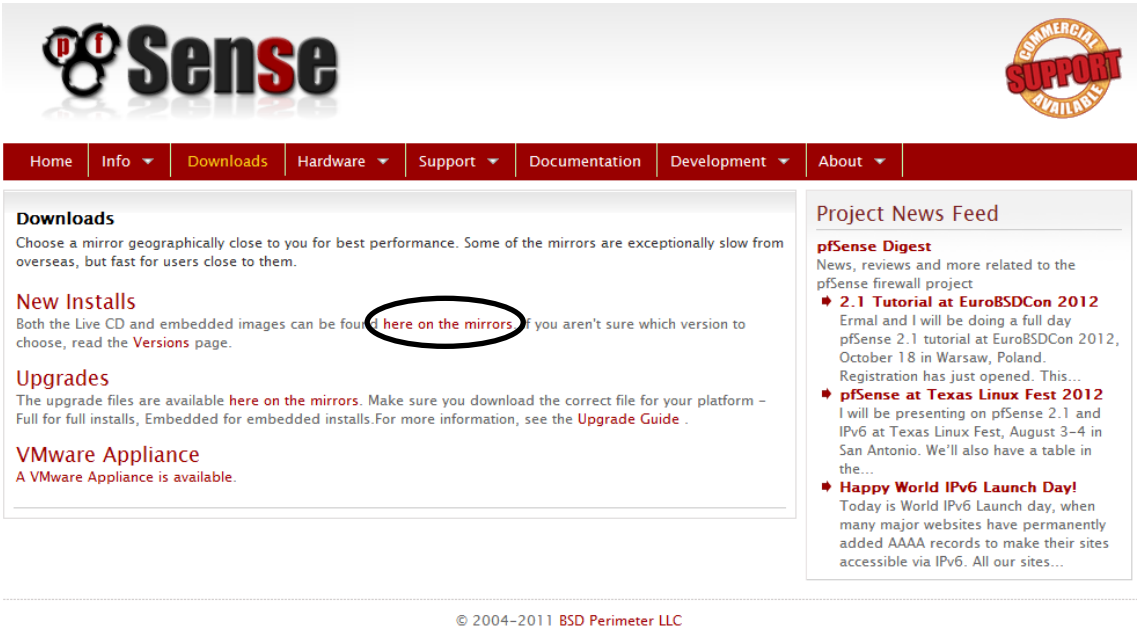
Zeroshell 2011. Hardware compatibility. Viitattu 3.5.2011 http://zeroshell.org/hw/.

Zeroshell 2012. Router/Bridge Linux Firewall. Viitattu 28.2.2012 http://zeroshell.org/.

KMT:n palomuurin asennus- ja käyttöohje

Asennus

Siirry osoitteeseen http://www.pfsense.org/ ja valitse sieltä Downloads ja New Installs -otsikon alta linkki ”here on the mirrors”.



Valitse listalta jokin pfSenseä tarjoava palvelin. Esimerkiksi jostakin Euroopan maasta, mutta kuitenkin maantieteellisesti mahdollisimman läheltä.

Valitse listasta käyttötarpeeseen sopiva levykuva. Esimerkiksi CD-levylle poltettava iso-levykuva 32-bittiseen järjestelmään. Tarvittaessa voit ladata md5-tarkistussumman, jolla voit tarkistaa tiedoston eheyden ennen CD:n polttoa. Tarkistuksen voi tehdä Windowsissa esimerkiksi Microsoft File Checksum Integrity Verifier -ohjelmalla tai muissa järjestelmissä komennolla md5. Sulautetuille järjestelmille on ladattavissa erikokoisille muistikorteille sopivia nanobsd-tiedostoa, mutta tähän asiaan ohjeessa ei paneuduta sen tarkemmin.

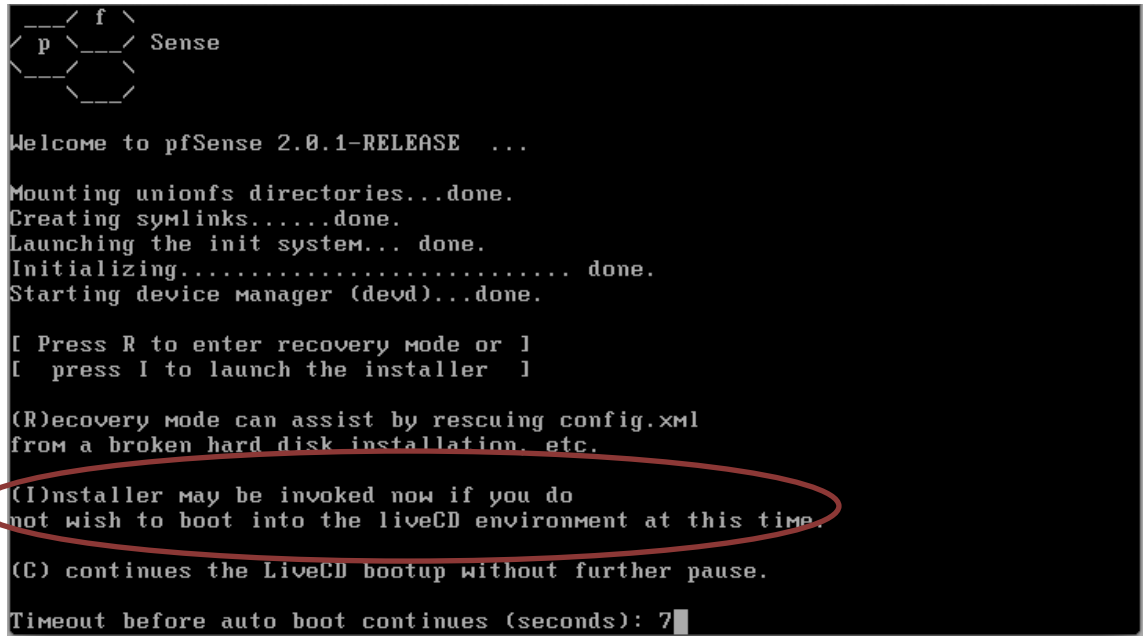
Index of /mirror/pfsense/downloads

Name	Last modified	Size	Description
Parent Directory		-	
pfSense-memstick-2.0.1-RELEASE-i386.img.gz.sha256	20-Dec-2011 21:26	119	
pfSense-memstick-2.0.1-RELEASE-i386.img.gz.md5	20-Dec-2011 21:26	84	
pfSense-memstick-2.0.1-RELEASE-i386.img.gz	13-Dec-2011 21:11	98M	
pfSense-memstick-2.0.1-RELEASE-amd64.img.gz.sha256	20-Dec-2011 21:26	120	
pfSense-memstick-2.0.1-RELEASE-amd64.img.gz.md5	20-Dec-2011 21:26	85	
pfSense-memstick-2.0.1-RELEASE-amd64.img.gz	13-Dec-2011 21:11	110M	
pfSense-2.0.1-RELEASE-i386.iso.gz.sha256	20-Dec-2011 21:26	110	
pfSense-2.0.1-RELEASE-i386.iso.gz.md5	20-Dec-2011 21:26	75	
pfSense-2.0.1-RELEASE-i386.iso.gz	13-Dec-2011 21:10	98M	
pfSense-2.0.1-RELEASE-amd64.iso.gz.sha256	20-Dec-2011 21:26	111	
pfSense-2.0.1-RELEASE-amd64.iso.gz.md5	20-Dec-2011 21:26	76	
pfSense-2.0.1-RELEASE-amd64.iso.gz	13-Dec-2011 21:09	110M	

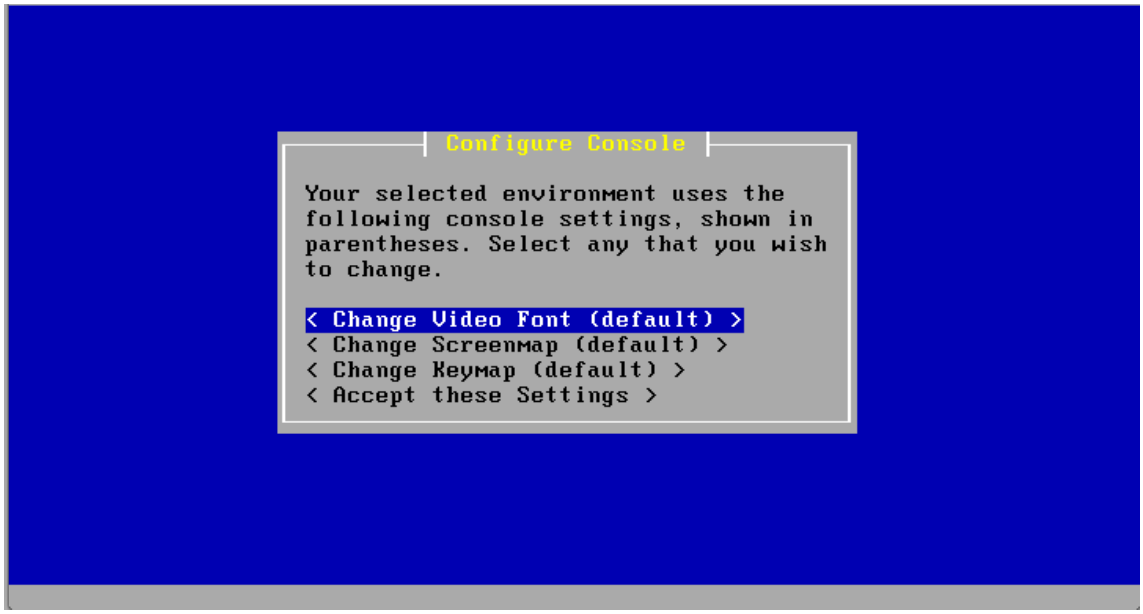
Levykuva tulee polttaa CD:lle levykuvana eikä data-CD:nä, joka sisältää yhden iso-tiedoston. Windowsissa voi käyttää esimerkiksi ohjelmaa ImgBurn tai Nero ja Linuxissa K3B tai Brasero.

Kun levykuva on poltettu levylle, palomuurijärjestelmän voi käynnistää ja asentaa siltä. Jos tietokone ei käynnistä CD-levyltä, kannattaa tarkistaa BIOS-asetuksista käynnistysjärjestys tai painaa Esc tai F12 -näppäintä, jolloin saa näkyviin tietokoneen käynnistysvalikon (Boot menu).

Kun järjestelmä on latautunut CD-levyltä ja kysyy jatkotoimenpiteitä, voi painaa I-näppäintä, jolloin pfSensen asennusohjelma käynnistyy.

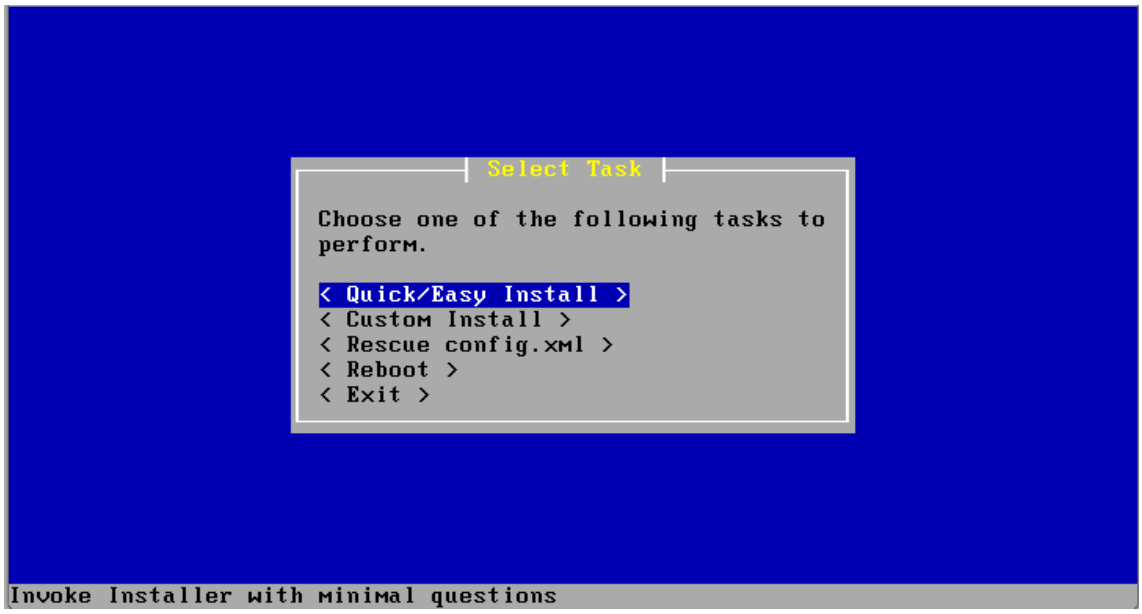


Ensimmäisessä ruudussa voi muokata konsolin ja näppäinasettelun asetuksia. Näitä ei tarvitse muokata, vaan voi siirtyä seuraavaan vaiheeseen.

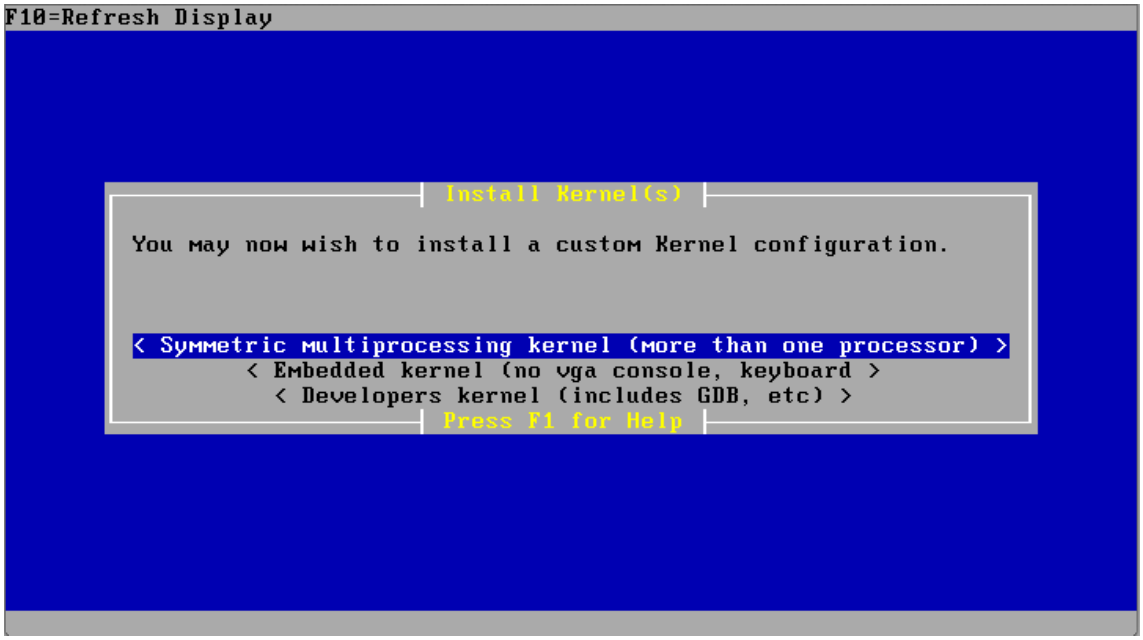


Toisessa ruudussa voi valita, haluaako asentaa järjestelmän pika-asennuksena tai mukautettuna asennuksena. Jos käytössä on vain yksi kiintolevy ja

asennusta ei tarvitse mukauttaa, voi valita nopean ja helpon asennuksen, jolloin asennusohjelma valitsee oletusarvot.

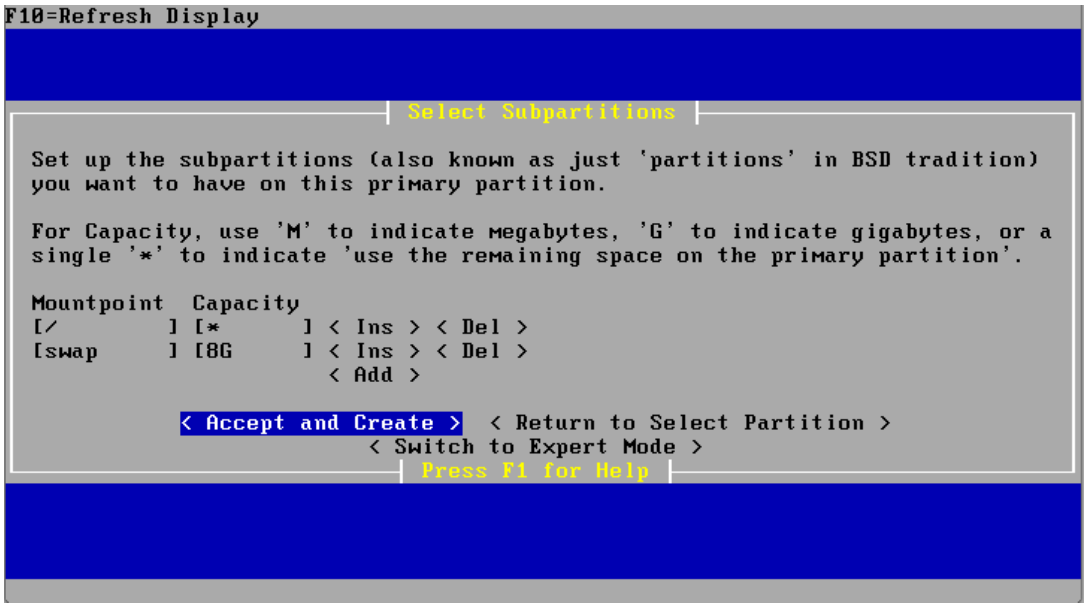


Pika-asennusvalinnan jälkeen järjestelmä asentuu ja tiedostojen kopioinnin jälkeen järjestelmä kysyy, minkä järjestelmäytimen (kernelin) haluaa asentaa. Näistä kannattaa valita oletusarvo.



Mukautettu asennus poikkeaa pika-asennuksesta siten, että asennuksessa voi valita, mille kiintolevylle järjestelmä asennetaan, suorittaa kiintolevyn

alustuksen, muokata kiintolevyn geometriaa, luoda osioita kiintolevylle, lisätä ja poistaa käynnistyslohkoja eri kiintolevyille ja muokata aliosioita. Muuten asennus etenee vastaavanlaisesti kuin pika-asennuskin. Aliosioiden muokkaaminen on todennäköisesti ainut vaihe, jota voi tarpeen mukaan muokata. Siinäkin vaiheesta ainoastaan heittovaihto-osion (swap) muokkaaminen suuremmaksi tai pienemmäksi voi olla käyttötapauksesta riippuen tärkeää.



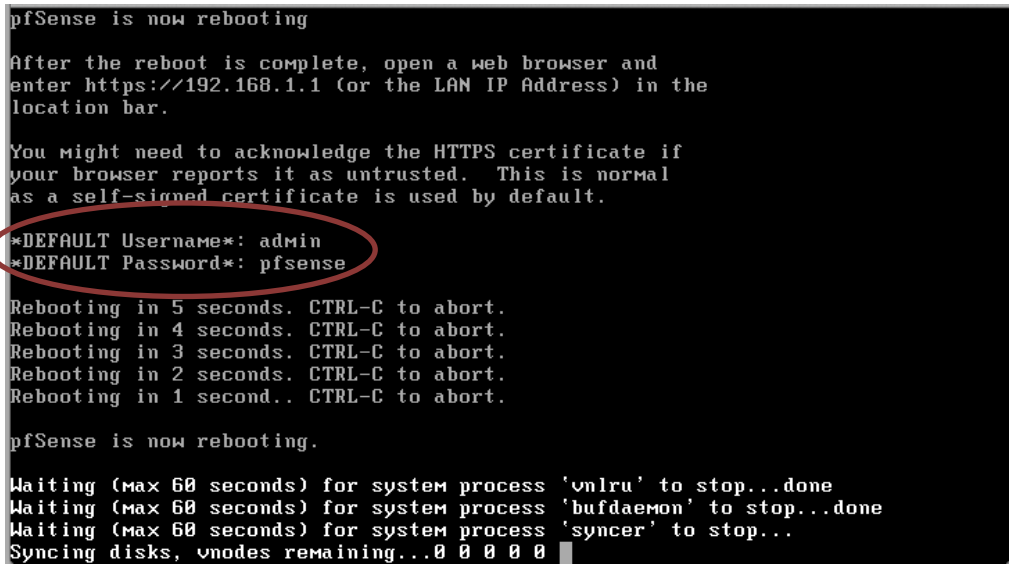
Tämän jälkeen järjestelmä on asennettu kiintolevylle ja tietokone voidaan käynnistää uudelleen.

Uudelleenkäynnistysvaiheessa järjestelmä ilmoittaa web-liittymän kirjautumisosoitteen ja oletusarvot käyttäjänimelle ja salasanalle, jotka ovat seuraavanlaiset:

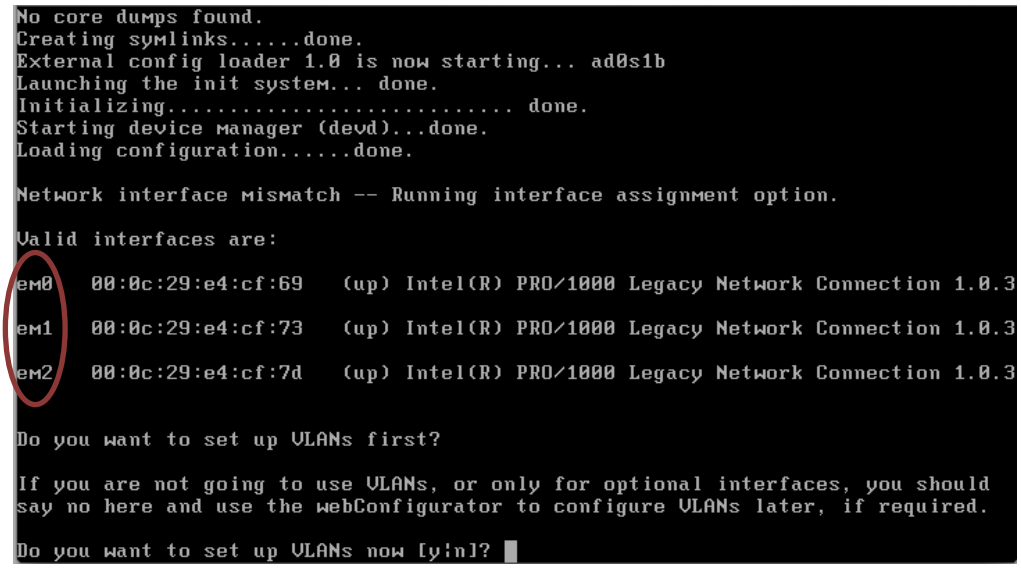
Käyttäjätunnus: admin

Salasana: pfsense

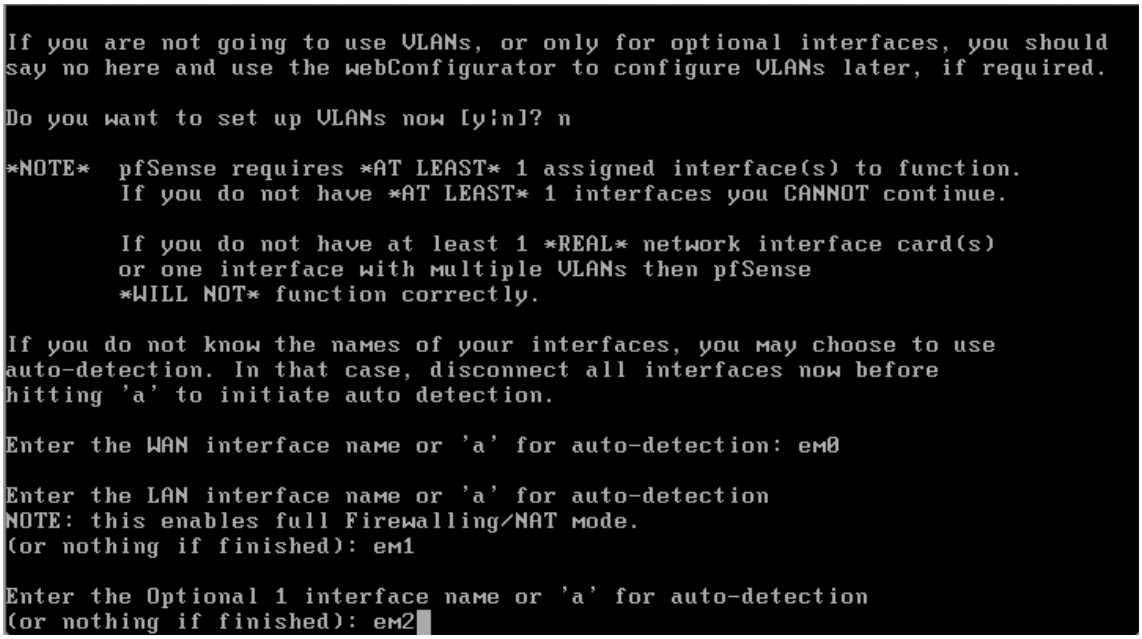
Tunnukset on mahdollista vaihtaa myöhemmin.



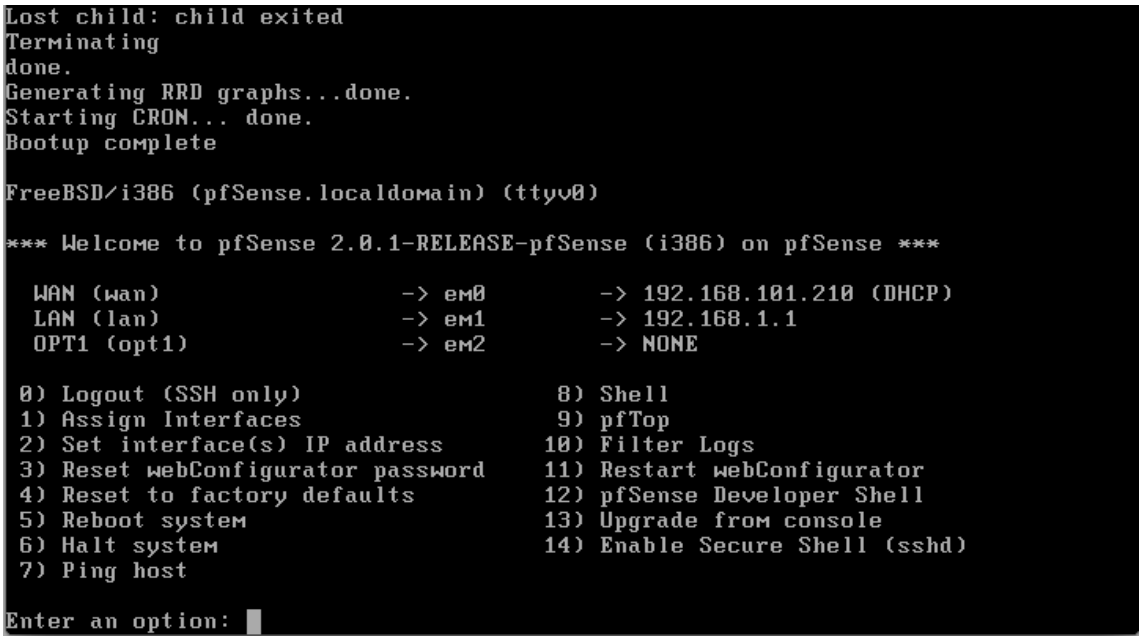
Käynnistyksen jälkeen komentorivillä asetetaan palomuurin verkkokortin asetukset. Aluksi järjestelmä näyttää käytettävissä olevat verkkoliitännät. Kuvassa verkkoliitännät em0, em1, em2.



Kuvan mukaisesti asetetaan aiemmin ilmoitetut käytettävissä olevat verkkoliitännät WAN- ja LAN-verkkoliitännöiksi. Kun vähintään WAN-verkkoliitäntä on konfiguroitu, pääsee palomuurin perusnäkymään.



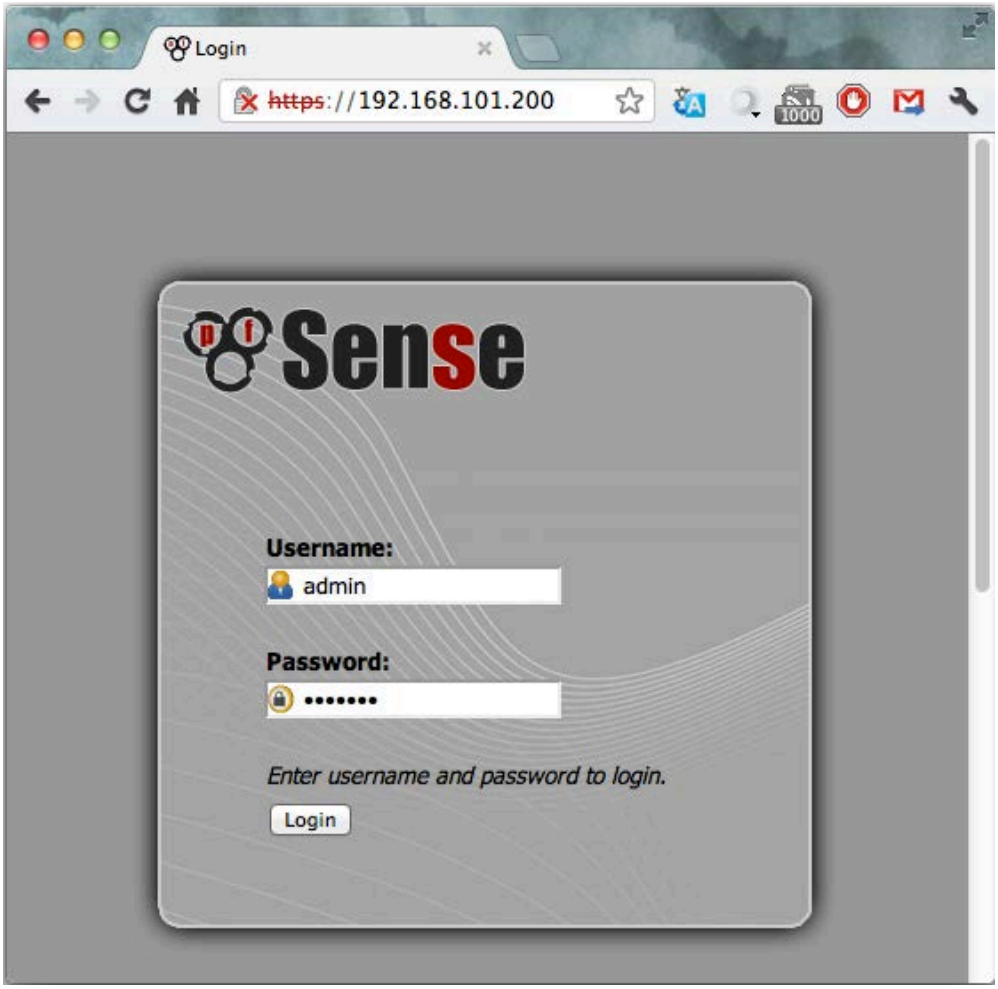
Palomuurin perusnäkymässä on mahdollista mm. muokata verkkoyhteyksien asetuksia, nollata verkkoliittymän salasana, käynnistää palomuuri uudelleen, pingata verkko-osoitteisiin, kirjautua komentoriville ja katsoa järjestelmän tietoja.



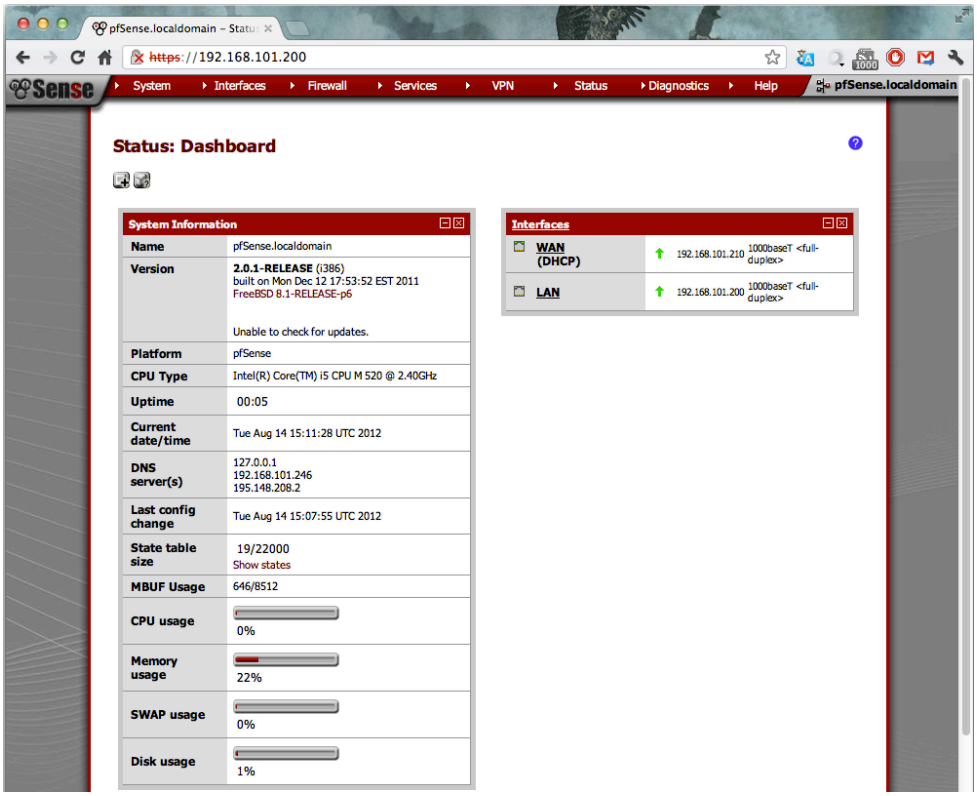
Tarvittaessa verkkoasetuksia voi muokata haluamakseen perusnäkymän kautta. Kuvassa muokataan LAN-verkkoliitännän verkkoasetuksia.

```
 6) Halt system                      14) Enable Secure Shell (sshd)
 7) Ping host

Enter an option: 2

Available interfaces:

1 - WAN
2 - LAN
3 - OPT1

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.101.200

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count:
> 24

Do you want to enable the DHCP server on LAN? [y:n]  n
```

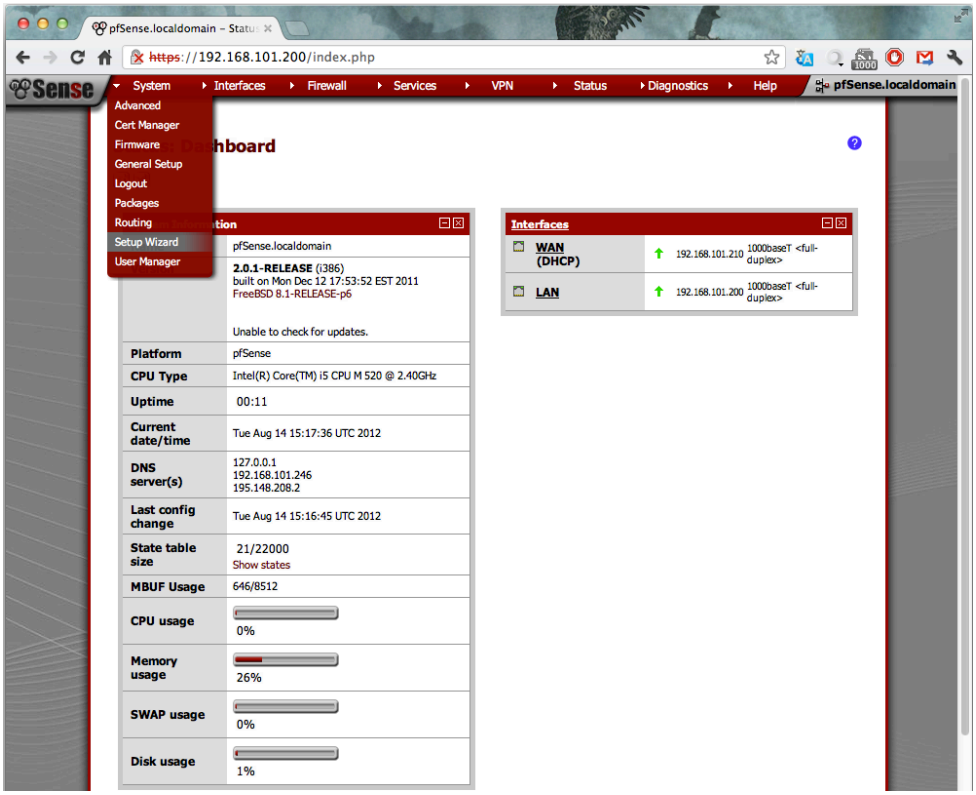
Mahdollisten muutosten jälkeen voidaan kirjautua palomuurin web-liittymään käyttämällä asennusvaiheessa annettua käyttäjätunnusta ja salasanaa.



Kirjautumisen jälkeen aukeaa palomuurin hallintanäkymä, josta näkee ohjelmiston, laitteen ja verkkojen perustiedot.

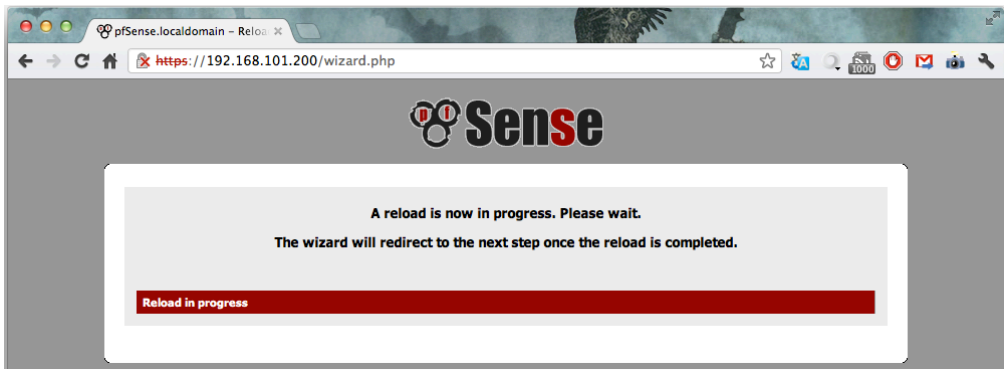


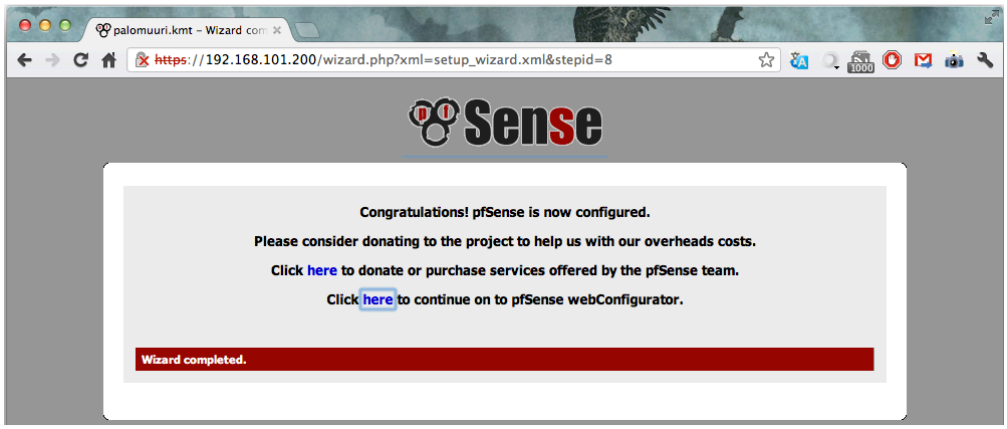
Kirjautumisen jälkeen kannattaa käyttää asennusvelhoa. System\Setup Wizard.



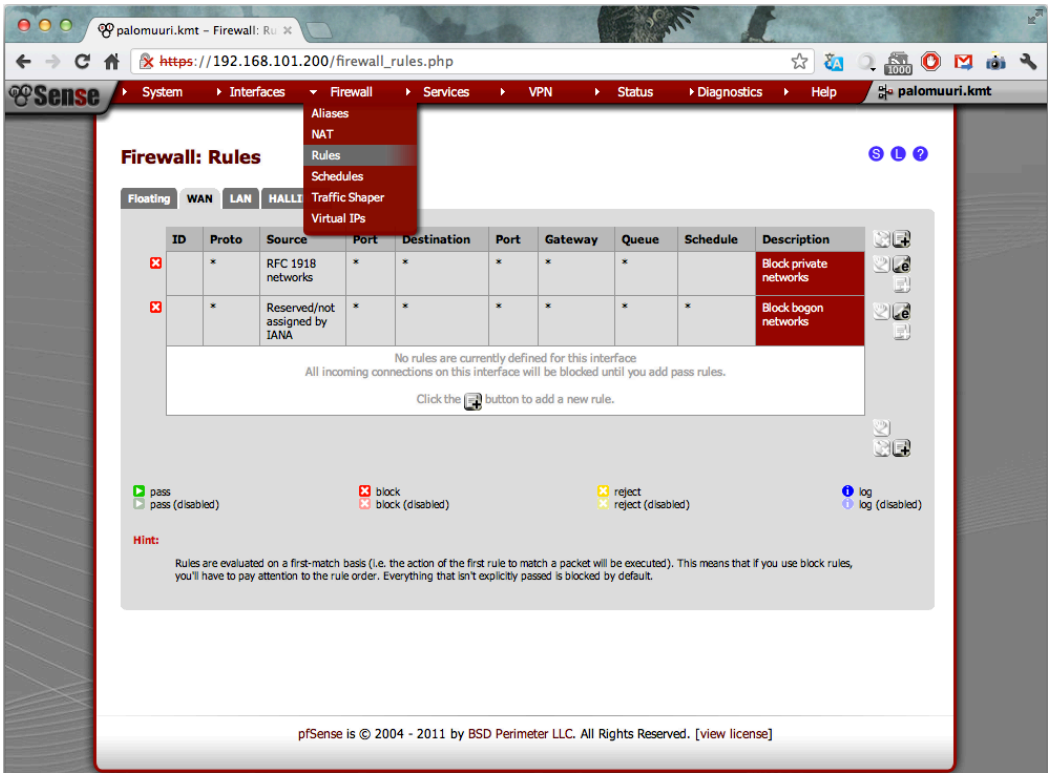
Asennusvelhon avulla saa tehtyä helposti ja nopeasti pfSensen alkuasetukset: esimerkiksi koneen nimen, toimialueen ja DNS-palvelimien osoitteet, määriteltyä aikapalvelimen ja verkkoliitäntöjen asetukset. Kuvassa WAN-verkon asetukset määritelty staattiseksi, muutettu IP-osoite ja lisätty välityspalvelimen osoite.

Tämän jälkeen alkuasetukset on määritelty.

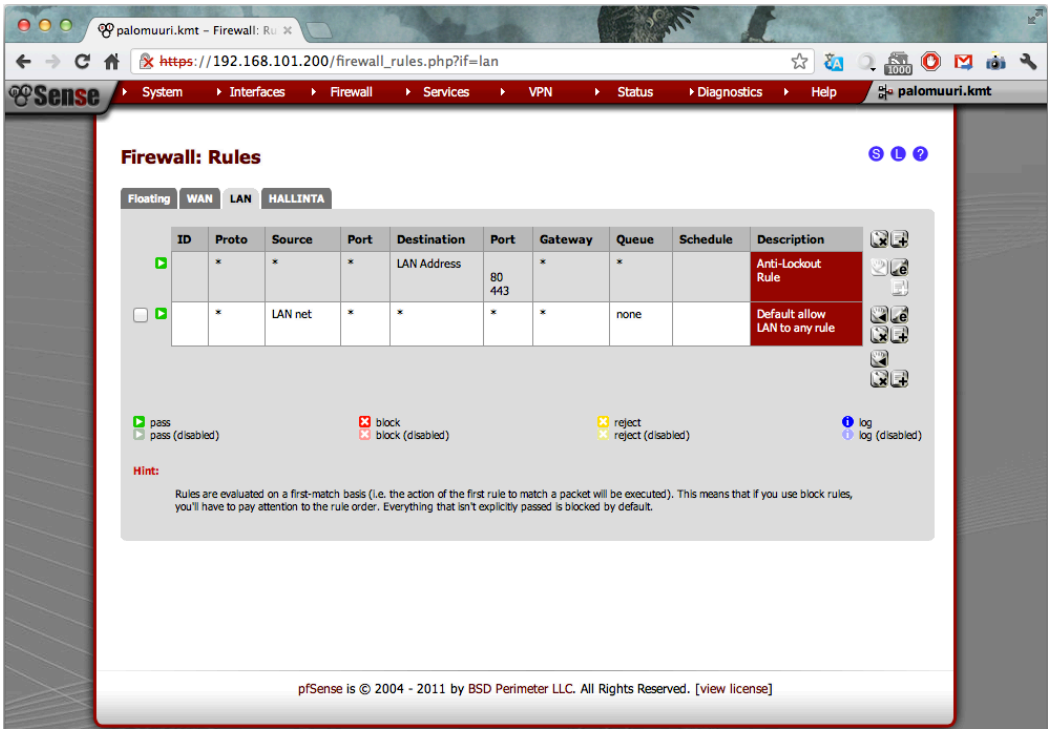




Alkuasetusten jälkeen voidaan muokata palomuurin suodatusasetuksia. Firewall\Rules. Kuvassa WAN-liitännän säännöissä on kielletty ulkoverkon varattujen osoitteiden ja yksityisverkon osoitteiden pääsy palomuurin läpi.

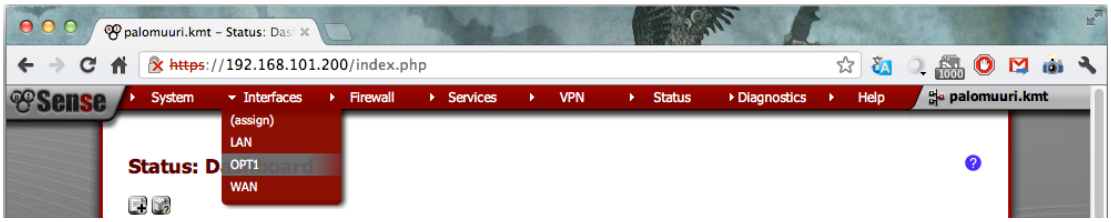


LAN-liitännän asetuksissa on määritelty valmiiksi hallintayhteyden lukituksen esto ja LAN-verkon osoitteista sallinta kaikkiin mahdollisiin osoitteisiin.

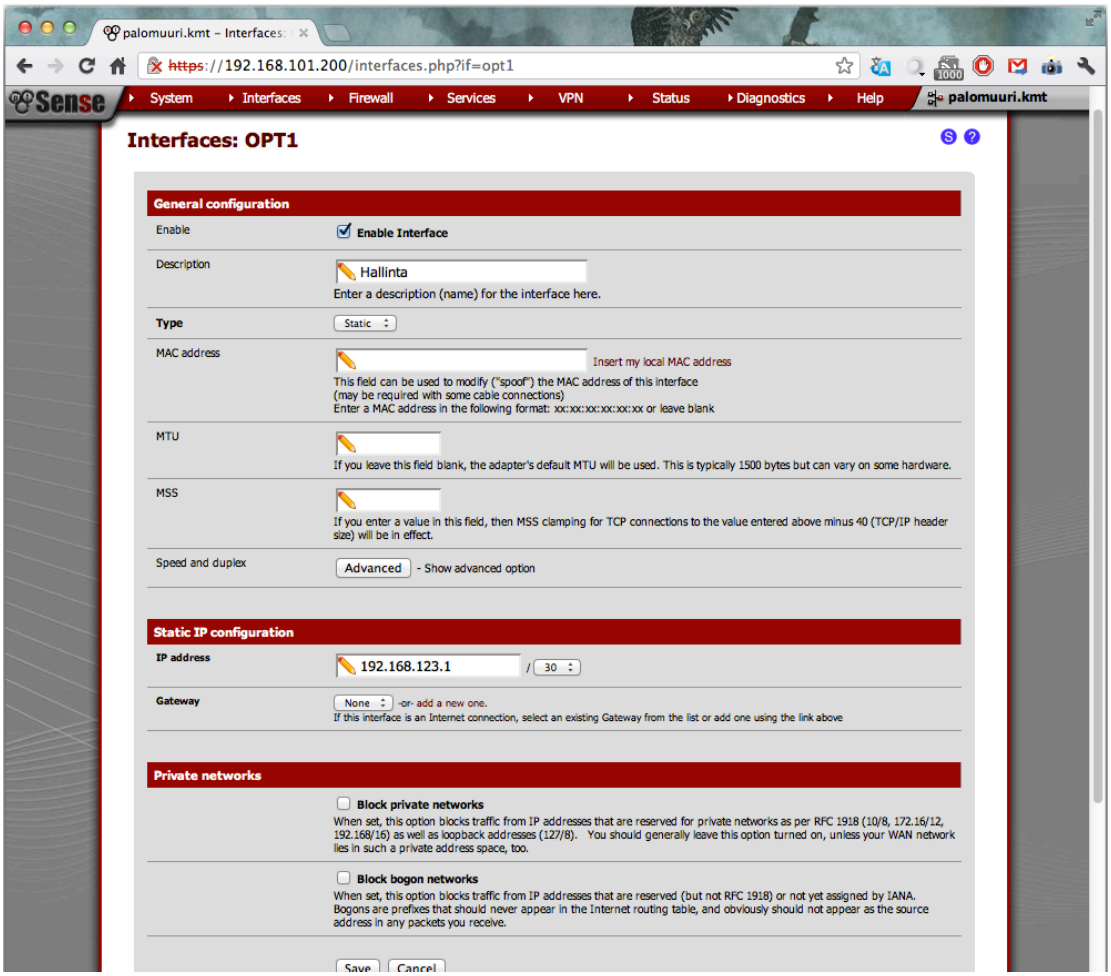


Hallintayhteys kannattaa asettaa omaan virtuaaliverkkoon tai kokonaan toiseen verkkoliitäntään. Jos kuitenkin halutaan hallita palomuuria kaikilta LAN-verkkoon kytketyiltä laitteilla, kannattaa määrittää käyttäjähallinta kuntoon.

Jos käytössä on kolmas verkkokortti, voidaan käyttää verkkoliitäntää Interfaces\OPT1.



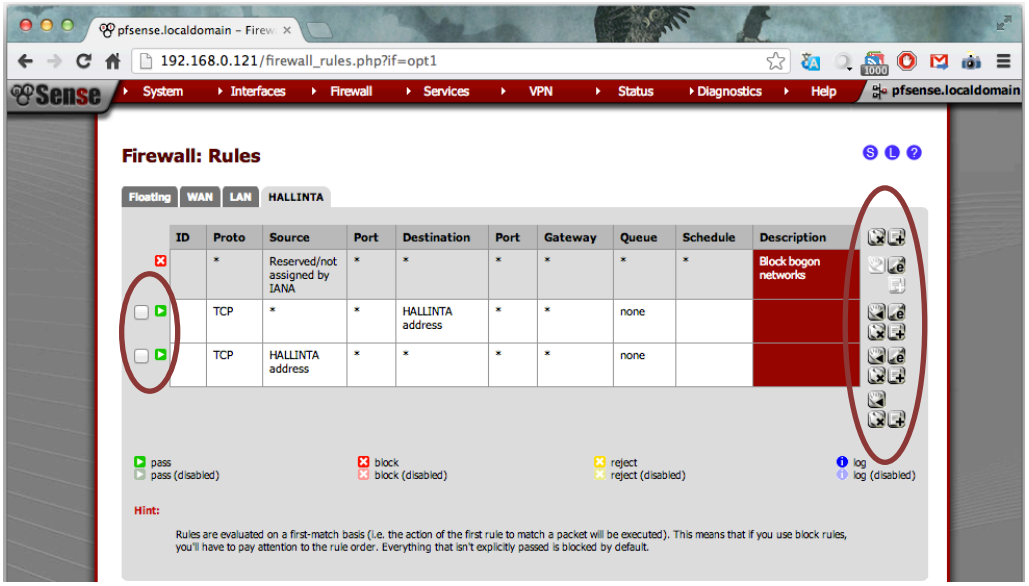
Liitännän asetukset voidaan määritellä halutulla tavalla. Hallintayhteys kannattaa rajata riittävän kattavalla verkon peitteellä. Esim. määrittelemällä IP-osoite ja verkon peite x.x.x.x/30 mahtuu aliverkkoon ainoastaan kaksi verkkolaitetta, joista toinen on palomuuri.



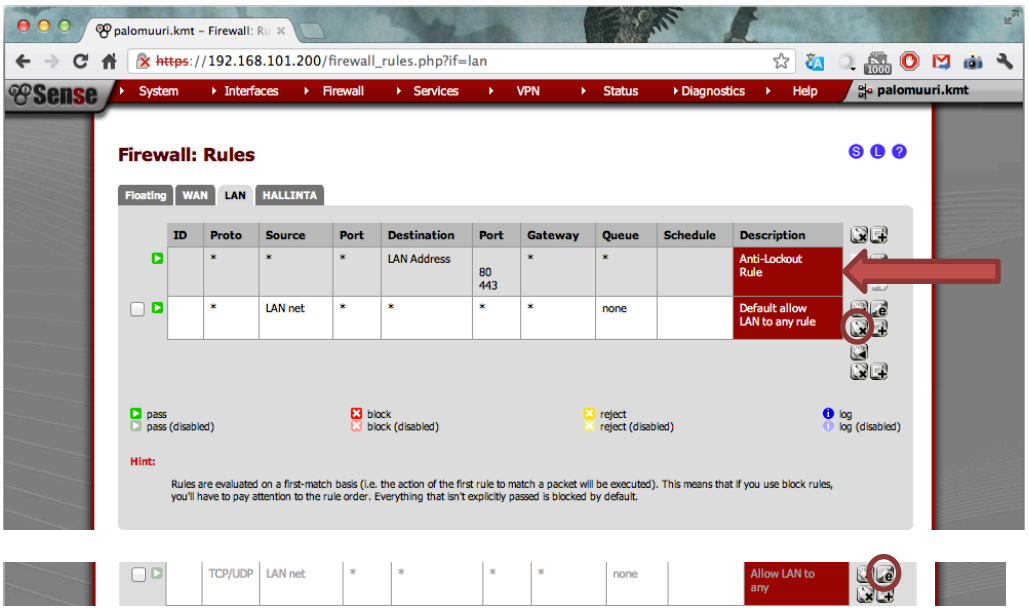
Hallintaverkossa kannattaa sallia hallintayhteys palomuuriin aliverkon osoitteesta.

Käyttöohje

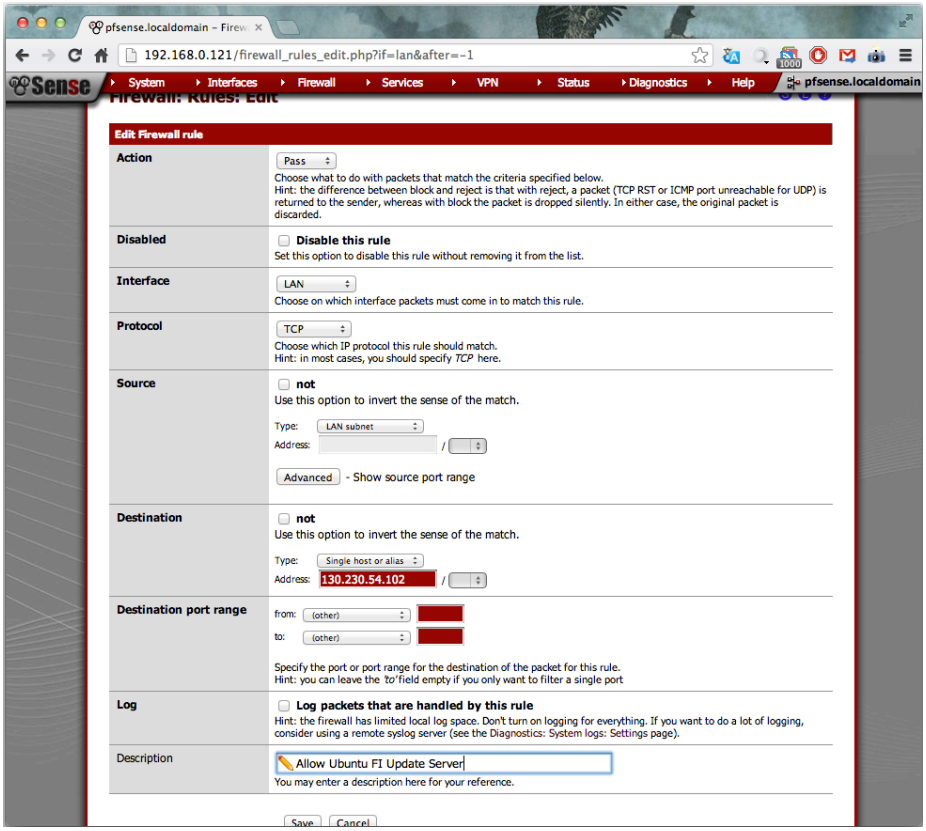
Palomuurisäännöt lisätään Firewall\Rules-näkymässä. Välilehdeltä voidaan valita konfiguroitava verkko ja nähdä sen hetkiset palomuurisäännöt. Näkymän oikeassa reunassa on nappeja, joilla voidaan tiettyyn kohtaan lisätä ja poistaa sääntöjä sekä järjestää säännöt eri järjestykseen.



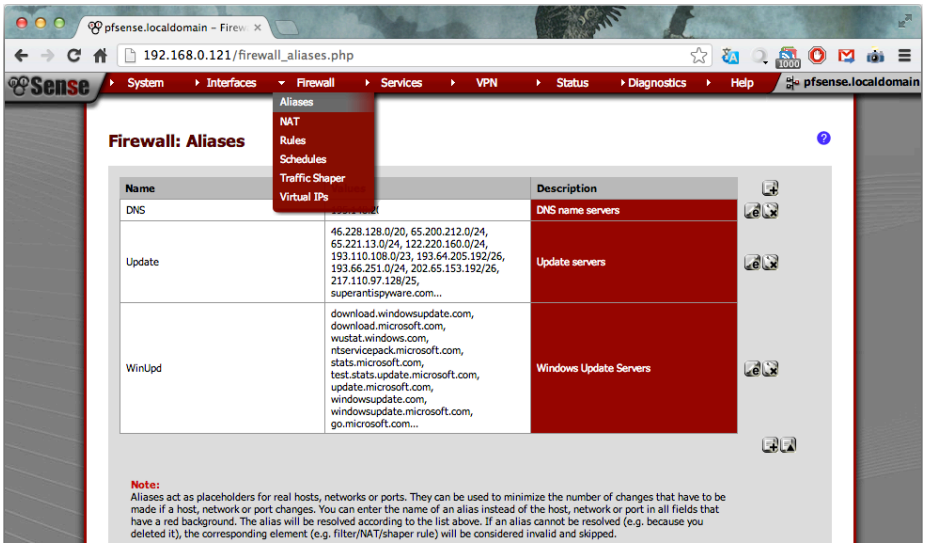
Kun halutaan tehdä verkosta turvallinen, kannattaa kieltää tai poistaa käytöstä kaikki ulkoverkkoon menevän liikenteen sallinnat. Tämän jälkeen on helppo lisätä sallinnat vain tiettyihin verkko-osoitteisiin, kuten päivityspalvelimiin. Sallintoja poistettaessa kannattaa olla tarkkana. Jos hallintayhteys palomuuriin estetään (nuoli), täytyy kaikki palomuurisäännöt ottaa tilapäisesti pois käytöstä palomuurin komentorivillä. Alhaalla kuvissa napit: poisto (x) ja muokkaus (e).



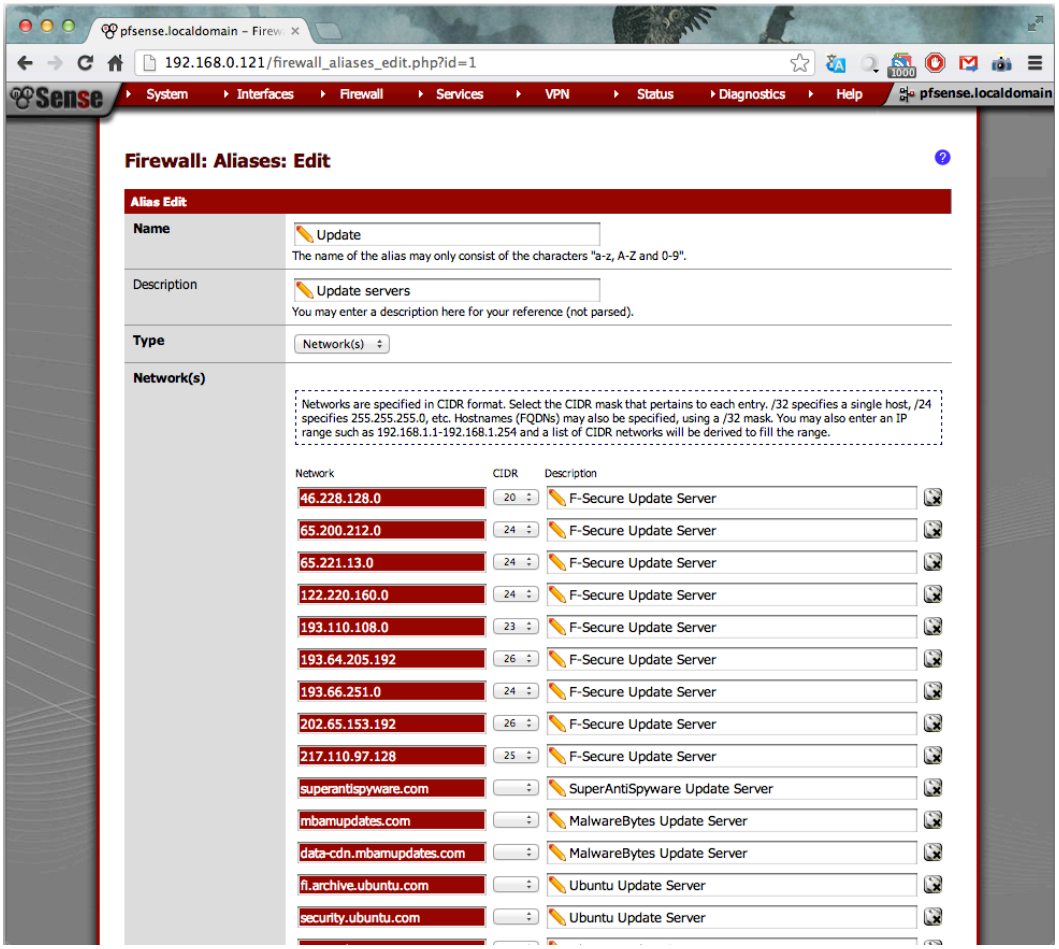
Palomuurisääntöjen lisääminen tapahtuu siten, että ensin määritellään sallinta tai kielto, jonka jälkeen määritellään liitäntä, josta paketit tulevat palomuuriin. Sitten valitaan protokolla, lähdeosoite ja kohdeosoite tai -osoitteet tai alias-ryhmä. Tarvittaessa voidaan määritellä porttialueet lähde- ja kohdeosoitteista. Lopuksi on järkevää nimetä sääntö, jotta ei tarvitse tulkita sääntölistalla, mitä mikin palomuurisääntö tekee.



Jos yksittäisiä sääntöjä on useita, kannattaa hyödyntää alias-ryhmiä Firewall\Aliases.



Alias-ryhmät voidaan luoda käyttämällä erilaisia tiloja. Tiettyyn tilanteeseen kannattaa käyttää tiettyä tilaa. Näistä Host ja Network ovat yleisesti käytetyimmät tilat.



Kun Alias-ryhmä(t) on luotu, on helppoa vain lisätä uudet verkko- ja IP-osoitteet suojausasetusten mukaiselle sopivalle listalle. Palomuurin sääntöjä on helpompi lukea, kun suuri määrä osoitteita on sisällytetty alias-ryhmän yhteen riviin.