Kimmo Virtanen (AMK)

Tietojenkäsittely

Tietoliikenne

2014

Kimmo Virtanen

VERKON RAKENTEEN UUSIMINEN KANSALAISEN MIKROTUESSA TIETOTURVAN PARANTAMISEKSI

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Huhtikuu 2014 | 36 sivua

Esko Vainikka

Kimmo Virtanen

VERKON RAKENTEEN UUSIMINEN KANSALAISEN MIKROTUESSA TIETOTURVAN PARANTAMISEKSI

Opinnäytetyön aiheena on uudistaa ja parantaa Turun ammattikorkeakoulussa sijaitsevan Kansalaisen mikrotuen tietoliikenneverkkoa. Tarkoituksena on parantaa tietoturvaa jakamalla verkko osiin palomuurin taakse. Näin potentiaalisesti saastuneet asiakaskoneiden haittaohjelmat eivät pääse leviämään Kansalaisen mikrotuen henkilökunnan verkkoon tai koulun verkkoon. Lisäksi opinnäytetyössä tutkitaan mahdollisuuksia, kuinka verkosta ja Kansalaisen mikrotuen tiloista voitaisiin tehdä entistä turvallisempia.

Työtä ryhdytään tutkimaan konstruktiivisella tutkimusotteella ja tutustumalla aikaisempiin opinnäytetöihin Kansalaisen mikrotuesta. Alkutilanteessa selvitetään asiakas- ja henkilökuntaverkon vaatimukset sekä suunnitellaan tilan kaapelointi.

Kansalaisen mikrotuen verkko saatiin toimimaan pienien ongelmien jälkeen halutulla tavalla. Tietoturvaa tutkittaessa ei löytynyt kuin pieniä mahdollisia korjattavia asioita, sillä Kansalaisen mikrotuen tietoturva toimii.

ASIASANAT:

Kansalaisen mikrotuki, tietoturva, lähiverkko

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communications

April 2014 | 36 pages

Esko Vainikka

Kimmo Virtanen

RENEWING THE NETWORK IN THE CITIZEN'S HELPDESK TO ENHANCE THE INFORMATION SECURITY

The objective of the present bachelor's thesis is to renew and enhance the Citizen's helpdesk network. Citizen's helpdesk is located in the premises of Turku University of Applied Sciences. The aim of the study is to divide the network into separate networks that are protected by a firewall. In this way, it is possible to prevent potentially infected customer computers from infecting further Citizen's helpdesk computers or even the school network. In addition, the present thesis explores the possibilities to take the information security even further in Citizen's helpdesk and its network.

The study applies a constructive research method and explores the previous theses about Citizen's Helpdesk. At the beginning, the requirements for the customer and employee network are discussed and the plans for the cabling in the room are also explained.

Finally, after some minor problems were solved, the Citizen's Helpdesk network is fully operational and the investigation of the information security revealed only some minor improvement possibilities because the information security at Citizen's Helpdesk works.

KEYWORDS:

Citizen's Helpdesk, information security, LAN

SISÄLTÖ

1 JOHDANTO **5**

2 LÄHTÖTILANNE **7**

2.1 Lähtökohdat 7

2.2 Verkon topologia 10

3 VERKON TOTEUTUS JA ONGELMIEN RATKAISU **12**

3.1 Palomuuri 12

3.2 Windows Update 13

3.3 Muut sivustot 14

4 TILAN UUDELLEENJÄRJESTÄMINEN **15**

5 TIETOTURVAN PARANNUSEHDOTUKSET **17**

6 JATKOTOIMENPITEET **20**

7 YHTEENVETO **23**

LÄHTEET **25**

LIITTEET (SALAINEN)

1 JOHDANTO

Kansalaisen mikrotuki (KMT) on Turun ammattikorkeakoulussa toimiva palvelu, johon asiakkaat voivat tulla ATK-ongelmiensa kanssa. Kuten kaikkien palveluiden, myös KMT:n on kehityttävä ajan mukana.(Saarinen 2010)

Kansalaisen mikrotuessa käy kuukaudessa jopa satoja asiakkaita, joiden tietokoneiden ongelmat vaihtelevat hyvin paljon. Kuitenkin monet koneet ovat hyvin pahasti saastuneita haittaohjelmista, jotka täytyy saada poistettua. Puhdistusprosessin jälkeen kuitenkin koneet pitäisi kytkeä Internetiin esimerkiksi lataamaan päivityksiä tai hakemaan hyötyohjelmia. Haittaohjelmat ja virukset voivat kuitenkin olla todella sitkeitä ja jopa läpikotainen puhdistus ei aina riitä. Verkkoon kytkettynä ilman mitään rajoituksia nämä saastuneet koneet ovat riski niin Kansalaisen mikrotuen omalle verkolle kuin koulun verkolle.

Tavoitteena on jakaa asiakaskoneet ja henkilökunnan oma verkko erilleen. Asiakaskoneiden verkkoliikennettä säädellään tiukasti palomuurisäännöillä ja henkilökunnan tietokoneet pääsevät yhdistymään melko vapaasti Internetiin. Molemmat verkot ovat palomuurin takana, mutta asiakaskoneista pääsee vain ja ainoastaan tiettyihin ennalta määritettyihin osoitteisiin.

Asiakkaiden koneet ovat nykyään jo lähestulkoon kaikki kannettavia tietokoneita, joiden kytkeminen langattomaan yhteyteen olisi työtä helpottavaa. Langattoman yhteyden tuominen ympäristöön kuitenkin lisää tietoturvariskejä ja voi aiheuttaa ongelmia olemassa olevien langattomien Sparknet- ja Eduroam-yhteyksien kanssa.

Työn pohjana toimii Tero Mäkelän (2012) opinnäytetyö palomuurikoneesta Kansalaisen mikrotuelle, mutta työ alkoi tutustumalla myös muihin aikaisempiin opinnäytetöihin Kansalaisen mikrotuesta. Mahdollisten ongelmien esiintymisiin ei juuri voitu varautua, joten vaihtoehtona oli lähteä yrittämään ja erehtymään sekä samalla etsiä Internetistä apua. Yritys- ja erehdysmenetelmä on heuristinen ongelman ratkaisumalli, korjaus tai tapa hankkia tietoa. Tietojenkäsittelyssä

tapaa kutsutaan myös ”generate and test” eli tuota ja testaa. (Trial and error 2014.)

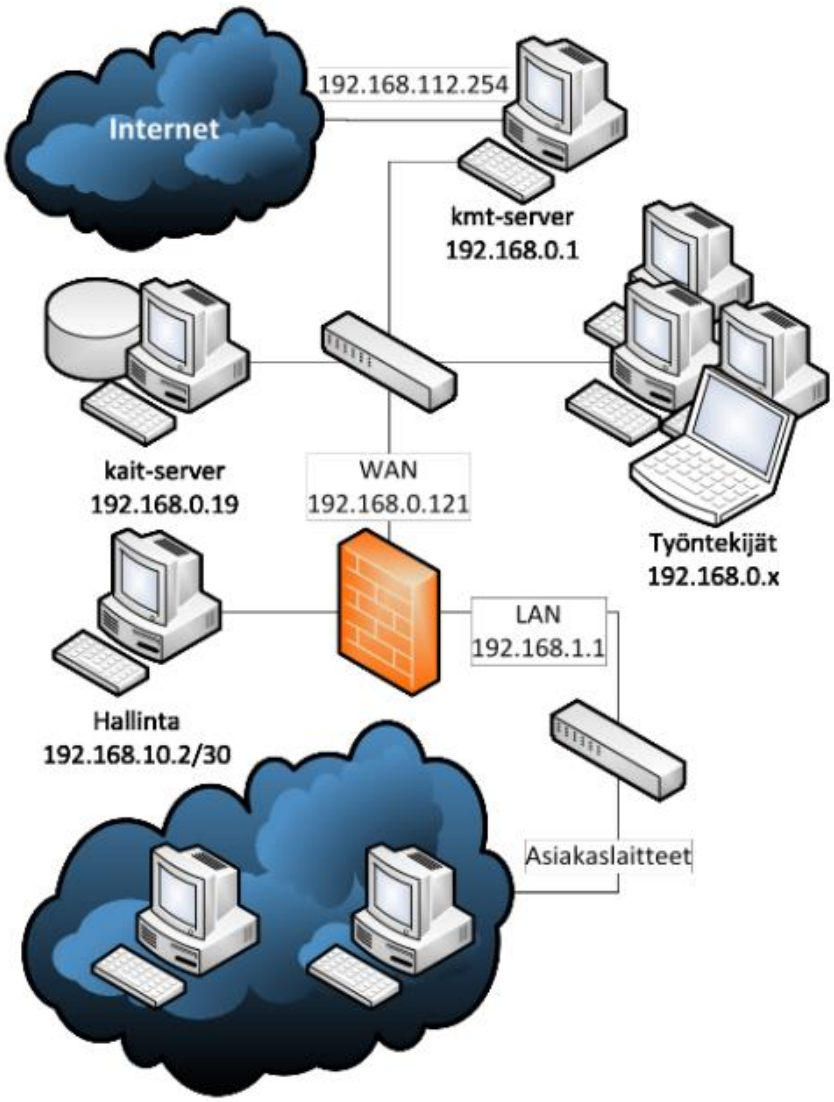
Konstruktiivinen tutkimusote on kekseliäitä ratkaisuja tuottava metodologia, jolla pyritään ratkaisemaan aitoja ongelmia ja tätä kautta tuottamaan tuloksia sille tieteenalalle, jossa sitä sovelletaan. Tiivis vuorovaikutus käytännön ja teorian välillä ovat tutkimusmetodina konstruktiiviselle tutkimusotteelle luonteenomaisia piirteitä. Konstruktiivinen tutkimusote on yksi case-tutkimuksen muoto (Metodix 2014). Case- eli tapaustutkimus on käytännön tutkimus, joka käyttää monipuolista eri tavoilla hankittua tietoa tutkimaan tiettyä tapahtumaa tai toimintaa tietyssä rajatussa ympäristössä (Case-tutkimus 2014).

Yritys- ja erehdysmenetelmä on mainio keino selvittää tämän työn kaltaisia ongelmia, joissa täytyy kokeilla useita eri verkko-osoitteita tai erilaisia asetuksia. Tämä metodi on lisäksi hyvä keino saada lisätietoa, koska epäonnistunut kokeilu karsii aina yhden mahdollisuuden pois. (Exforsys 2014.)

2 LÄHTÖTILANNE

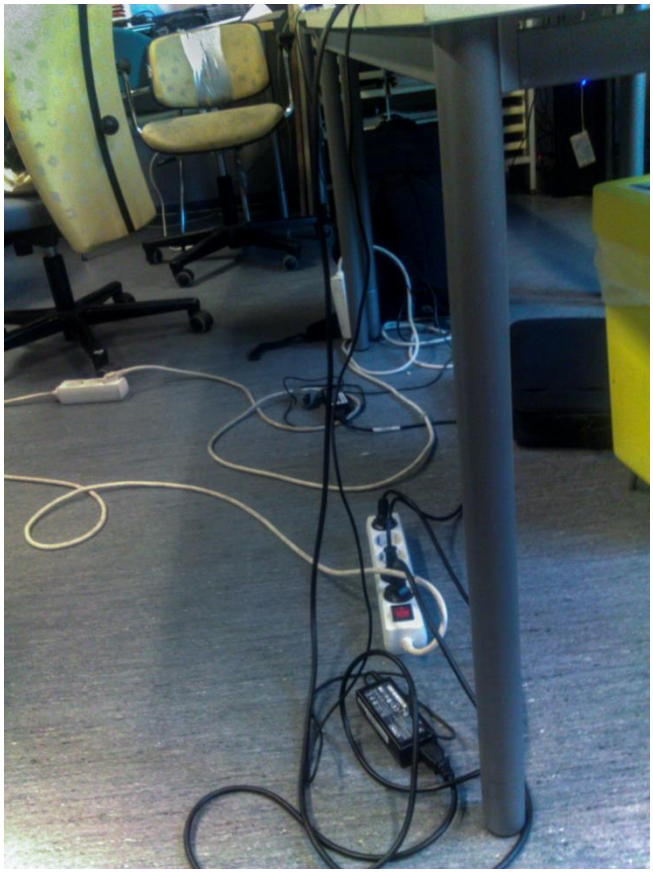
2.1 Lähtökohdat

Alkutilanne on sama kuin Mäkelän (2012, 15) kuvassa. Pieni muutos tosin on se, että palomuurikoneen tilalla on vanha NAT-kone, joka tulee vaihtaa uuteen koneeseen. Koneet on yhdistetty verkkoon kuvan 1 mukaisesti. Työtekijöiden koneet on kytketty kytkimeen, jonka avulla kaikki työntekijöiden koneet saadaan kytkettyä verkkoon langallisesti.



Kuva 1. Verkon topologia (Mäkelä 2012, 15).

Kaapeloinnit tullaan yksinkertaistamaan ja asettamaan pois tieltä, koska kuten kuvista 2 ja 3 näkyy, verkko- ja sähkökaapelit ovat vaarallisesti jaloissa ja näkyvillä. Johdotus tehdään seinien kautta ja kytkimiä hyödyntäen.



Kuva 2. Kansalaisen mikrotuen työnskentelytilan lattia.

Kuvassa 2 näkyvä tilanne ei ole kovin turvallinen monesta syystä. Tilanne voi aiheuttaa kompastumisen ja henkilövahinkoja sekä vahinkoja laitteisiin. Sähköjohdot saattavat irrota ja pahimmassa tapauksessa hajota kokonaan repeytyessään irti äkillisesti. Tämä saattaisi aiheuttaa hengenvaarallisen tilanteen. ”Työnantaja on tarpeellisilla toimenpiteillä velvollinen huolehtimaan työntekijöiden turvallisuudesta ja terveydestä työssä” (Työturvallisuuslaki 23.8.2002/738).

Monet ohjelmat, kuten Windows Update ja muut päivitystoimenpiteet, eivät reagoi hyvin, jos tietokone sammuu kesken kaiken virran katketessa. Tiedostojen korruptoituminen on myös hyvin mahdollista, jos esimerkiksi varmuuskopioimisen aikana virrat katkeavat laitteista.

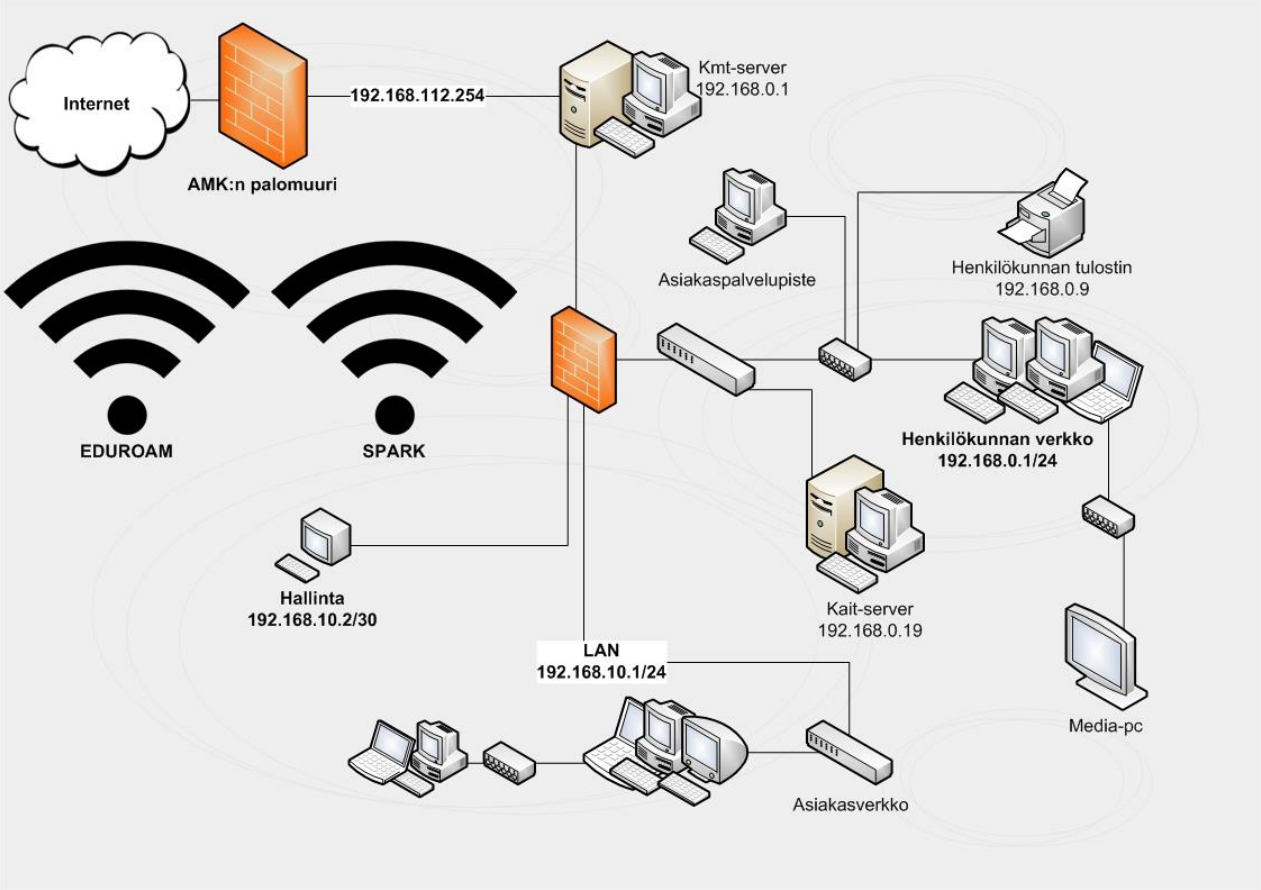
Kuvan 3 järjestely ei varsinaisesti ole uhka turvallisuudelle, mutta se ei anna kovin ammattimaista kuvaa asiakkaille, koska asiakaspalvelutiskiltä on suora näköyhteys tähän järjestelyyn. Ajan kuluessa nämä teippien alla olevat verkkokaapelit saattavat myös katketa, koska ne ovat keskellä kulkutietä.

Kuva 3. Kansalaisen mikrotuen asiakaspalvelupuolen lattia.

Tarkoituksena on löytää pitkäaikainen ratkaisu, jottei samanlaisiin tilanteisiin jouduta. Henkilökunta kuitenkin vaihtuu noin puolen vuoden välein ja uusi projektipäällikkö saattaa haluta muuttaa huoneen järjestystä.

2.2 Verkon topologia

Verkkokaavio ei eroa merkittävästi Mäkelän kuviosta, mutta sen tarkoitus on olla yksityiskohtaisempi versio, josta näkyvät kaikki laitteet verkon laitteet.



Kuva 4. Kansalaisen mikrotuen verkko.

Kuvassa 4 näkyvät kytkimet ovat niin sanotusti ”tyhmiä kytkimiä”, joiden tarkoitus on mahdollistaa kaikkien työntekijöiden koneiden kytkeminen verkkoon. ”Tyhmällä kytkimellä” tarkoitetaan tässä yhteydessä kytkintä, joka on asetettu vain välittämään liikennettä.

KMT:n ulko- ja sisäverkon välisenä palvelimena toimii Kmt-server. Palvelimesta yhteys etenee kytkimeen, jonka kautta yhteys jakautuu Kait-serverille, toiselle kytkimelle ja työntekijäkoneille. Molemmille palvelimelle on määritelty salasanat, ja KMT:n projektipäällikkö pitää huolta palvelimista sekä työntekijäkoneista.

Kait-server toimii asiakastietokantana, johon tallennetaan huoltotyöt. (Mäkelä 2012, 16).

Media-pc on työntekijöiden viihdekäyttöön tarkoitettu tietokone, josta voi katsoa videoita tai kuunnella musiikkia. Tietokone ei eroa kuitenkaan muuten muista koneista ja se toimii normaalisti osana henkilökunnan verkkoa.

3 VERKON TOTEUTUS JA ONGELMIEN RATKAISU

3.1 Palomuuri

Pfsense on ilmainen vapaan lähdekoodin palomuuriohjelmisto, joka perustuu FreeBSD-kerneliin. FreeBSD on kehittynyt ja vapaa Unix-käyttöjärjestelmä (Freebsd 2014). Pfsense on käytännöllinen, koska sitä voi ajaa pelkästään muistitikulta tai CD-levyltä. Lisäksi se on äärimmäisen kevyt, mikä tarkoittaa, että vanhastakin tietokoneesta voidaan saada kätevä palomuurikone. Palomuuriohjelmistosta saa vielä paljon enemmän irti erilaisilla lisäpaketeilla, jotka voidaan asentaa helposti Web-näkymän kautta. (TechRepublic 2014.)

Palomuurikoneessa ajetaan Pfsenseä, koska siinä on kätevät ominaisuudet, se sisältää helppokäyttöisen graafisen käyttöliittymän ja sille löytyy valmiiksi yhteisö, jolta voi hankkia apua tarvittaessa (Mäkelä 2012, 19–20).

Palomuurin asetukset

Koneiden paikkojen vaihdossa ei ilmennyt ongelmia, mutta palomuurikone ei aluksi suostunut pysymään käynnissä muutamaa minuuttia enempää. Tämä ongelma kuitenkin korjautui itsestään ja syyksi epäiltiin koneen väärin tapahtunutta sulkemista. Koneen asetuksia muuttamaan päästäessä asetuksista muutettiin hallintaportin rajoitteet pois ja vaihdettiin porttien nimet. LAN vaihdettiin Asiakas-portiksi, Hallinta henkilöstöksi, mutta WAN-portti pidettiin samannimisenä. NAT-koneen osoite 192.168.192.254 muutettiin WAN-osoitteeksi palomuurille. DHCP-asetuksissa konfiguroitiin asiakasverkolle osoite-alue 192.168.1.2 – 192.168.1.254 ja henkilöstöverkolle 192.168.10.2 – 192.168.10.254. Jokainen portti vastasi kutsuun, mutta verkko ei kuitenkaan toiminut, koska WANin oletusyhdyskäytävä oli konfiguroitu väärin. Tämän korjaaminen ei vaikuttanut verkon toimimattomuuteen. Asetukset palomuurissa olivat oikein, mutta jostain syystä verkosta ei päässyt reitititintä pidemmälle. Lukuisten yritysten jälkeen päätettiin, että palomuurin käyttöjärjestelmässä saattaa olla vikaa ja päätettiin asentaa Pfsense kokonaan uudestaan.

Tämän toimenpiteen jälkeen henkilökuntaverkosta päästiin ilman hankaluuksia toimimaan normaalisti verkossa sekä Internetissä, mutta asiakasverkko ei toiminut ollenkaan. Ongelmaksi havaittiin ensimmäiseksi se, että palomuuriohjelmistosta olivat säännöt pois päältä, mikä esti kaiken liikenteen. Ongelma ei ratkennut, mutta palomuurikoneesta paljastui, että asiakasverkon ja henkilökuntaverkon kaapelit oli kytketty vääriin portteihin. Tämän toimenpiteen jälkeen havaittiin palomuurikoneen jakavan suoraan kaapeliin kytkettynä osoitteen normaalisti tietokoneille, mutta kytkimeen kytkettynä DHCP-palvelin ei jakanut mitään osoitteita.

Kytkimen todettiin olevan todennäköisesti viallinen, joten se vaihdettiin uuteen. Kun kytkin vaihdettiin, DHCP-palvelin pystyi jakamaan koneille osoitteet, mutta palomuuriin asetetut säännöt eivät silti toimineet oikein eivätkä koneet pystyneet yhdistämään Windows update –palveluun tai käyttämään sääntöjen mahdollistamia sivuja.

Ongelmaksi osoittautui palomuurikoneelle asetettu DNS-forwarder, joka antoi väärän DNS-palvelimen. Tämän asetuksen pois käytöstä ottaminen ja DNS-palvelimen vaihtaminen Turun ammattikorkeakoulun DNS-palvelimen osoitteisiin korjasi ongelman sekä näin mahdollisti yhdistämisen esimerkiksi www.java.com-osoitteeseen.

3.2 Windows Update

Windows Update –palvelu ei kuitenkaan toiminut, koska Windows Update vaihtaa joka yhdistämiskerralla osoitetta tietoturvasyistä ja palomuuriin asetetut säännöt eivät toimi näin ollen. Ratkaisu löytyi tarkastelemalla palomuurin lokitiedostoista, mihin testikone yrittää saada yhteyttä. Palomuurisääntöihin lisättiin pääsy Microsoftin IP-alueelle, joka on 65.52.0.0 – 65.55.255.255. Windows Update pystyi hakemaan ja löytämään päivityksiä asiakasverkosta, mutta niiden lataaminen ei onnistunut vielä. Palomuurin liikennettä asiakasverkossa seuraamalla löytyi osoite, josta Windows Update yrittää ladata päivityksiä. RIPE.comia selailemalla selvisi Akamai Technologiesin Internet-osoite, joka on

82.96.58.0/24 (Comodo forums 2011). Asiakasverkosta pystyi nyt etsimään ja lataamaan Windowsin päivityksiä normaalisti. Osoitealue on kuitenkin rajallinen eikä asiakaskone välttämättä pysty hakemaan päivityksiä aina, mutta tämä korjaantuu käynnistämällä Windows Update uudestaan niin usein kuin on tarve. Tämän katsottiin olevan niin pieni ongelma, että sen kanssa pystyttiin työskentelemään.

Olisi mahdollista myös käyttää squid-lisäosaa tallentamaan Microsoftin päivitystiedostoja paikallisen koneen välimuistiin, josta ne saisi asiakaskoneiden käyttöön (Mäkelä 2012).

3.3 Muut sivustot

Kansalaisen mikrotuessa voidaan asentaa asiakkaan luvalla erilaisia hyödyllisiä ohjelmia, joita asiakas todennäköisesti tulee tarvitsemaan. Tämän vuoksi olisi hyödyllistä, että asiakasverkosta pystyisi lataamaan esimerkiksi Javan, Flashin tai virustorjuntaohjelman päivitykset. Projektipäällikön kanssa suunniteltiin ja pohdittiin eräänlainen lista tarpeellisista ohjelmista ja sivustoista. Asiakasverkosta tulisi pystyä yhdistämään näihin sivustoihin sekä lataamaan niiden sisältöä.

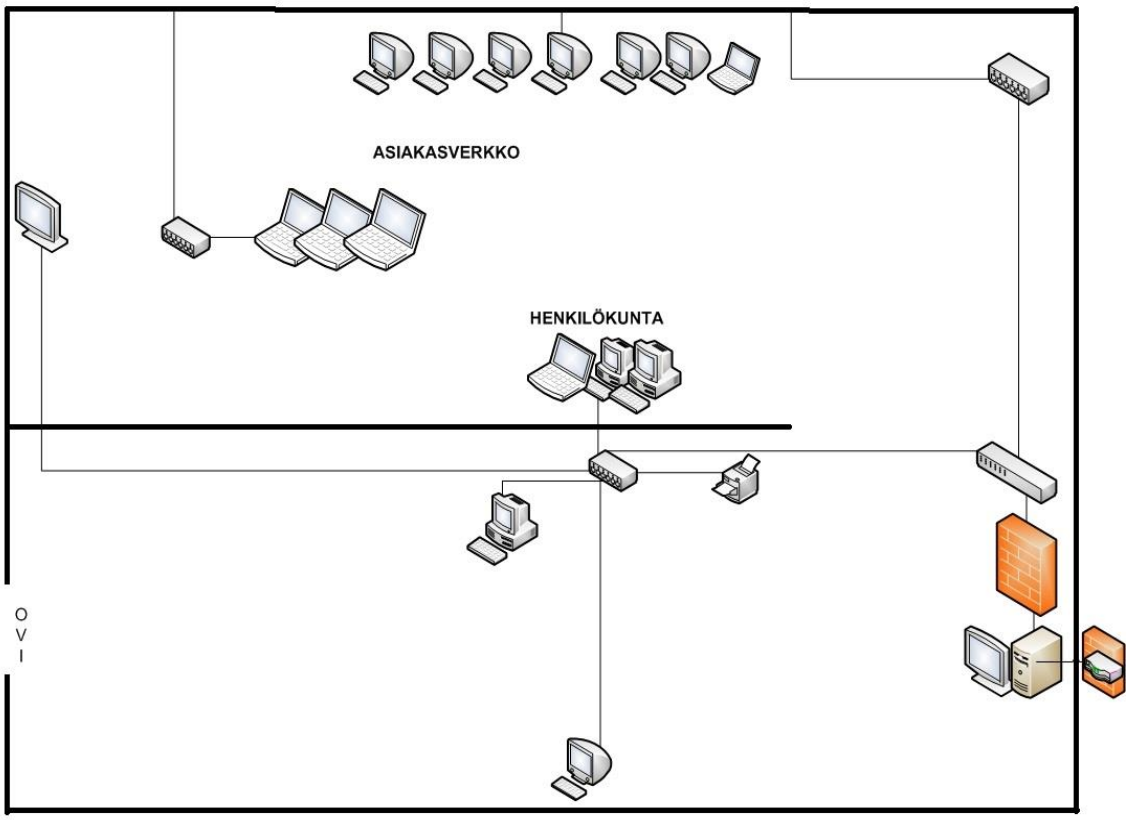
Palomuurin verkkoliikenne-näkymästä pystyy erottamaan samalla tavalla halutun liikenteen kuin Windows Updaten tapauksessa. Päädyttiin käyttämään sivustoa ja ohjelmaa nimeltä Ninite, joka oli projektipäällikön henkilökohtaisesta käytöstä jo tuttu.

Ninite on ilmaisohjelma, jonka käyttö on yksinkertaista. Selaimella siirrytään Niniten kotisivuille, josta valitaan ensin halutut asennusohjelmat ja tämän jälkeen ladataan asennusohjelma, joka hoitaa kaiken loppuun. Asennusohjelma ei asenna mitään ylimääräisiä työkalupalkkeja tai muita turhia asioita. (Tamminen 2010.)

4 TILAN UUDELLEENJÄRJESTÄMINEN

Aikaisemmin asennettu sähkökouru helpottaa huomattavasti, koska koko asiakasverkon saa pidettyä takaseinällä. Ongelmaksi muodostuivat aikaisemmissa kuvissa 2 ja 3 näkyvät kohdat, sillä muita reittejä ei oikein ollut. Asiakaspalvelutiskille menevät verkkokaapelit päätettiin jättää kulkemaan lattian kautta teipattuna vahvasti, koska tarpeeksi pitkiä kaapeleita ei ollut saatavilla. Ongelma oli kuitenkin lähinnä esteettinen, mikä ei haittaa työntekijöitä eikä aiheuta vaaratilanteita.

Kuvassa 5 on esitetty pohjapiirros Kansalaisen mikrotuen tiloista.



Kuva 5. Tietokoneiden asettelu Kansalaisen mikrotuen tiloissa.

Takaseinällä on sähkökouru, jossa on myös paikat verkkokaapeleille. Asiakasverkon koneet saadaan helposti näin kiinni verkkoon. Kuitenkaan tila ei riitä kai-

kille asiakkaiden koneille, joten keskeltä huonetta on lisäpöytä, jota voidaan käyttää kannettavien tietokoneiden huoltamiseen.

Kannettavia ei tosin ole pakko kytkeä verkkoon, koska puhdistustoimenpiteiden jälkeen koneet voidaan kytkeä langattomaan verkkoon, jolloin vältytään käyttämästä ylimääräisiä verkkokaapeleita.

5 TIETOTURVAN PARANNUSEHDOTUKSET

Tässä luvussa on tutkittu erilaisia mahdollisia tietoturvan parannusmahdollisuuksia niin verkon, tietokoneiden kuin tilan puolesta.

Turvallisuus

Kansalaisen mikrotuki sijaitsee vanhassa opetustilassa, jossa on omat hyvät puolensa, mutta myös puutteita. Huoneen verhot ovat pimentävät ja estävät näköyhteyden ulkoa, mutta keräävät myös paljon pölyä, jonka vuoksi paloturvallisuus tulee ottaa huomioon. Ratkaisu ongelmaan olisi esimerkiksi verhojen vaihto sälekaihtimiin. Monet koneet saattavat vaatia paljon aikaa puhdistuksessa, mutta koneiden yöksi päälle jättäminen ilman valvontaa on riski kaikille asiakas- ja henkilökunnan tietokoneille. Koneiden määrän vuoksi myös jatkojohtoja ja verkkokaapeleita on lattialla, mutta verkkokaapelit ovat selvästi marginaalinen ongelma uuden asennetun sähkökourun vuoksi.

Nykyinen tilajärjestys estää työntekijöiden näköyhteyden tiskille, jossa saatetaan huoltaa jotain nopeita ja helppoja asiakastapauksia. Työntekijät eivät näe myöskään asiakkaiden tuloa, ja asiakkaat eivät aina huomaa tai ymmärrä painaa asiakaskelloa. Mahdollinen ratkaisu olisi määrittää vaihtuva päivystäjä tiskille. Hieman erilaisempi tapa olisi ratkaista ongelma vaikka kameravalvonnalla huoneessa. Esimerkiksi web-kameran voisi sijoittaa kuvaamaan pääovea, jolloin työntekijät voisivat nähdä näytöltä tiskin koko ajan ja myös potentiaaliset kutsumattomat yövieraat tallentuisivat kameralle. Näin raskaalle järjestelmälle tuskin kuitenkaan on mitään tarvetta oikeasti, koska suoratoisto itsessään jo riittäisi. (Mäkelä & Virtanen 2014, 89-94.)

Tietoaineistoturvallisuus

Tiloissa säilytetään asiakastietolomakkeita, jotka sisältävät tietokantaan tallennettavat asiakastiedot. Nämä paperit pitäisi säilyttää lukitussa kaapissa poissa näkyvistä, ja niille tulisi määrittää jonkinlainen säilytysaika.

Henkilöstöturvallisuus

Koska kansalaisen mikrotuessa vaihtuvat työntekijät noin puolen vuoden välein, on tärkeää säilyttää ja jatkaa tietotaitoa uusille projektipäälliköille sekä varaprojektipäälliköille. Uuden projektipäällikön perehdytys voi olla hyvin intensiivistä ajan puutteen takia, eikä kaikkea voi edes muistaa. Tätä varten olisi hyvä olla erityinen ohjeistus projektipäällikölle, mikä sisältäisi kaikki pääasiat KMT:n toiminnasta. Ohjenuoraa voisi aina päivittää projektipäälliköiden toimesta, jos siihen lisättävää asiaa tulisi mieleen esimerkiksi kauden lopussa.

KMT:n tietoturvaohjeita ovat esimerkiksi seuraavat säännöt:

• Käsittele vain niitä tiedostoja, jotka ovat työtehtävän kannalta olennaisia.

• Asiakkaat eivät saa mennä henkilökunnan työskentelytilaan.

• Valvo ja ohjaa asiakasta, jos päästät hänet KMT:n asiakaskoneelle.

• Työtila ei saa jäädä valvomatta työpäivän aikana.

• Vastuuhenkilön on oltava aina paikalla.

• Lukitse ovet ja sulje laitteet tilan jäädessä tyhjäksi.

• Neuvo asiakasta käyttämään monimutkaisia ja erilaisia salasanoja. (Mäkelä & Virtanen 2014, 91.)

Ohjelmistoturvallisuus

Työntekijöiden tietokoneissa ei välttämättä ole virustorjuntaohjelmaa, koska eri ohjelmien lisensioinnista on ollut epäselvyyttä. Koululla on kuitenkin lisenssit F-Secure -ohjelmaan, joka on kyllä raskas, mutta hoitaa asiansa ja lisää tietoturvaa. Ohjelmat tarvitsevat hyvin usein päivityksiä, joten tätä varten tulisi valita päivityksiä hoitava henkilö. Esimerkiksi joka maanantai voisi olla hyvä tarkistaa yleisimpien ohjelmien päivitykset.

Asiakaskoneiden selaimiin asennetaan mainossuodatus, koska haittaohjelmia tulee hyvin usein verkkomainosten välityksellä. Vaikka Java-ohjelmaa käytetään paljon kaikkialla, tietoturvallisuus ei ole aina ajan tasalla ja sitä käytetään yhä vähemmän asiakkaiden käyttötarpeissa. Tällöin kyseessä oleva ohjelma voidaan poistaa ja tarvittaessa asentaa takaisin uudelleen, jos näin halutaan.

Muut

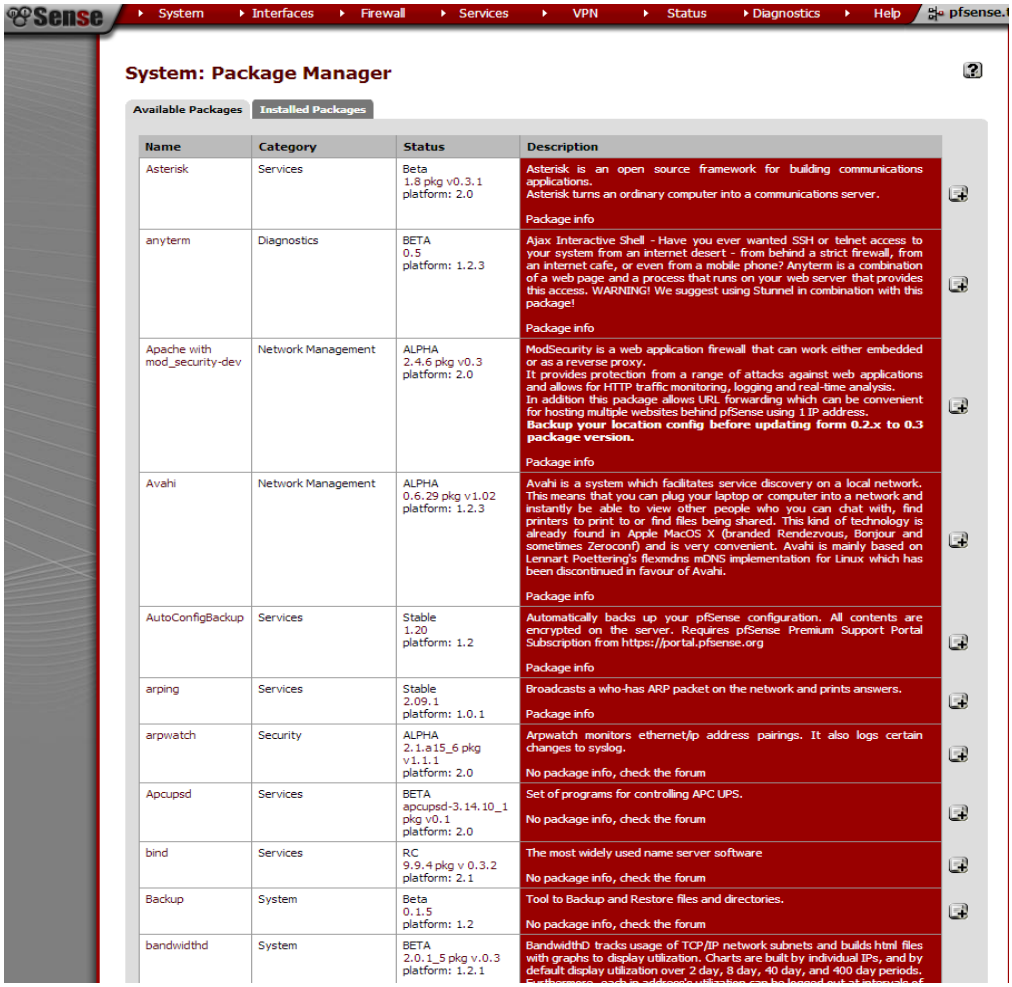
Kansalaisen mikrotuessa on käytössä ulkoisia kiintolevyjä, joihin voi tarvittaessa tallentaa asiakkaiden tärkeitä tiedostoja talteen esimerkiksi tietokoneen vaihdon yhteydessä tai tiedostojen palauttamista varten. Tiedostoja pyritään säilyttämään vain sen ajan, kun asiakkaan kone on huollettavana. Tiedostot hävitetään harjoittelujakson lopussa KMT:n tallenteista. Mikäli tila loppuu ulkoiselta medialta, poistetaan tiedostot vanhimmasta luovutetuista koneista.

> “KMT:n uuteen järjestelmään alunperin suunnittelimme lisäävämme etäseurantamahdollisuuden, jonka avulla asiakkaat pääsisivät katsomaan huollossa olevan koneen tilaa. Tällaista ominaisuutta oltaisiin tarvittu, sillä asiakkaat soittavat jatkuvasti KMT:lle huollossa olevien koneiden perässä. Olisi hyvä, jos olisi vaihtoehtoinen tapa selvittää koneen tila, sillä vaikka kaikilla asiakkailla ei olekaan toista konetta, vähentäisi se silti soittojen määrää. Tätä mahdollisuutta ei kuitenkaan lisätty, sillä KMT:n verkkoon ei pääse ulkoverkosta mitenkään.” (Hiltunen & Nummela 2011, 38.)

6 JATKOTOIMENPITEET

Pfsense on todella modulaarinen palomuurijärjestelmä, koska siihen pystyy asentamaan paketteja. Paketit ovat Pfsensen lisäosia, joilla voidaan lisätä monenlaisia ominaisuuksia jo valmiiksi hyvään palomuurijärjestelmään.

Kaikkia mahdollisia ominaisuuksia ei tulla käsittelemään vaan ainoastaan hyödylliseksi tai tarpeelliseksi katsotut paketit Kansalaisen mikrotuen kannalta. Yksi näistä paketeista on Mäkelän mainitsema Squid-ohjelma, joka voisi olla yksi lähestymistapa Windows Updaten osalta. (Mäkelä 2012, 38.)



Kuva 6. Pfsensen paketinhallintanäkymä.

Pakettien asentaminen on helppoa. Pfsenseen on rakennettu kuvassa 6 näkyvä hallintaohjelma, jonka avulla voidaan asentaa tai poistaa halutut paketit helposti. Hallintanäkymässä on myös lyhyt kuvaus siitä, mitä paketin ohjelma tekee ja sisältää.

Squid

Squid on välimuistipalvelin, joka tukee HTTP-, HTTPS- ja esimerkiksi FTP-protokollia. Sen tarkoitus on vähentää palvelimen rasitusta ja nopeuttaa useasti vierailtujen sivujen latautumista. Squidia voi myös käyttää vain käytetyn sisällön kopioimiseen ympäri maailmaa tehokkaasti. (Squid-cache 2014.)

Squid-ohjelmaa käyttämällä olisi mahdollista tallentaa Windows Update-päivitykset suoraan välimuistiin. Windows Update käyttää yleisesti http-alue-osoitetta ladatakseen osia Microsoftin päivitysarkistosta. Ongelmaksi voi kuitenkin muodostua hitaus, koska jotkut Microsoftin palvelimet eivät halua Squidin tallentavan arkiston tiedostoa. Tämä tarkoittaa sitä, että Squid joutuu lataamaan koko arkiston joka kerta, kun se tarvitsee pientä osaa siitä. (Squid-cache Wikipedia 2014.)

Useiden asiakkaiden koneet tarvitsevat käyttöjärjestelmän uudelleenasennusta, mikä tarkoittaa, että suuret service pack -päivitykset täytyy ladata sekä asentaa koneille. Squid saattaa myös hidastella näiden päivitysten kanssa suuren koon vuoksi. (Squid-cache wiki 2014.)

Darkstat

Darkstat on tarkoitettu ajettavaksi taustalla ja kaappaamaan verkkoliikennettä, josta voidaan luoda oman verkon tilasto. Darkstatin keräämää informaatiota pääsee näkemään käyttämällä selainkäyttöliittymää. Näin pystyy helposti tunnistamaan verkkoliikenteen tai estämään tietyn verkkoliikenteen. (Skear.Hubpages 2014.)

Tällä ohjelmalla pystyisi optimoimaan ja seuraamaan Kansalaisen mikrotuen verkkoliikennettä mahdollisten tietoturva-aukkojen varalta. Pfsensen oman

”nuuskijan” sijaan Darkstat on paljon selkeämpi ja sen kanssa on helpompi ylläpitää palomuurilokeja.

Squidguard

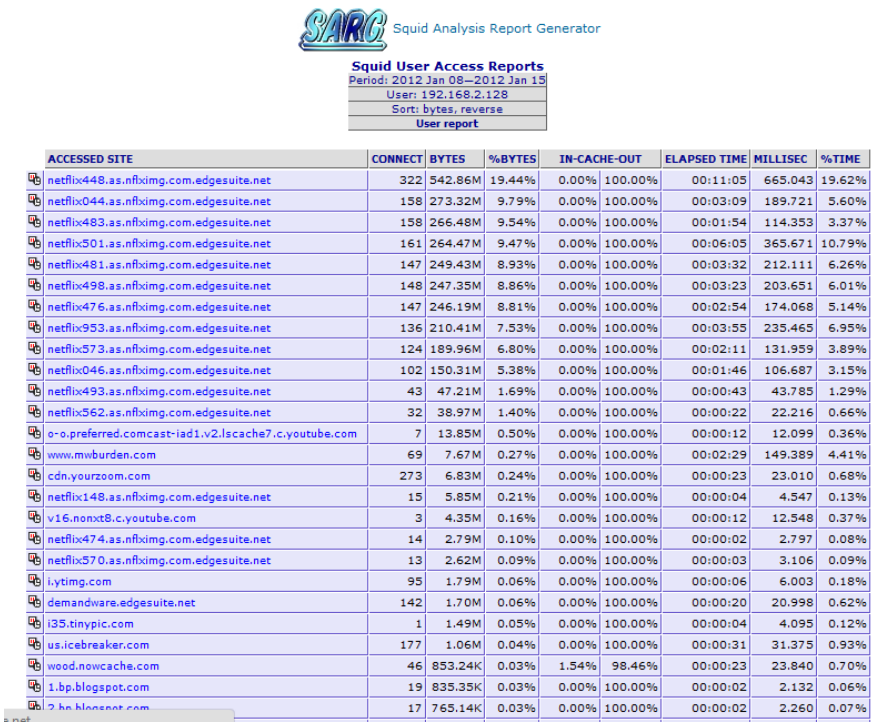
Squidguard on pääsynohjaaja, uudelleenohjaaja ja filtteri-liitännäinen Squidille. Tätä voidaan käyttää rajoittamaan käyttäjien Internetiin pääsyä, luoda mustia listoja ja asettaa erilaisia säännöksiä eri ryhmille. (Squidguard 2014.)

Kansalaisen mikrotuessa tätä voisi käyttää vahvistamaan asiakasverkon jakamista, koska vaikka Pfsensen vakio pääsynhallinta on toimiva, saisi Squidguardilla toteutettua lisää toiminnallisuutta.

SARG

SARG tulee sanoista Squid Analysis Report Generator. Se on työkalu, jonka avulla pystytään seuraamaan verkon käyttäjien verkkoliikennettä.

SARG luo kuvan 7. mukaisia HTML-raportteja, joissa on tiedot käyttäjästä, IP-osoitteet ja vieraillut sivut sekä kellonaika (Sarg.sourceForge 2014).



Squid Analysis Report Generator

Squid User Access Reports

Period: 2012 Jan 08—2012 Jan 15
User: 192.168.2.128
Sort: bytes, reverse
User report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
netflix448.as.nflximg.com.edgesuite.net	322	542.86M	19.44%	0.00%	100.00%	00:11:05	665.043	19.62%
netflix044.as.nflximg.com.edgesuite.net	158	273.32M	9.79%	0.00%	100.00%	00:03:09	189.721	5.60%
netflix483.as.nflximg.com.edgesuite.net	158	266.48M	9.54%	0.00%	100.00%	00:01:54	114.353	3.37%
netflix501.as.nflximg.com.edgesuite.net	161	264.47M	9.47%	0.00%	100.00%	00:06:05	365.671	10.79%
netflix481.as.nflximg.com.edgesuite.net	147	249.43M	8.93%	0.00%	100.00%	00:03:32	212.111	6.26%
netflix498.as.nflximg.com.edgesuite.net	148	247.35M	8.86%	0.00%	100.00%	00:03:23	203.651	6.01%
netflix476.as.nflximg.com.edgesuite.net	147	246.19M	8.81%	0.00%	100.00%	00:02:54	174.068	5.14%
netflix953.as.nflximg.com.edgesuite.net	136	210.41M	7.53%	0.00%	100.00%	00:03:55	235.465	6.95%
netflix573.as.nflximg.com.edgesuite.net	124	189.96M	6.80%	0.00%	100.00%	00:02:11	131.959	3.89%
netflix046.as.nflximg.com.edgesuite.net	102	150.31M	5.38%	0.00%	100.00%	00:01:46	106.687	3.15%
netflix493.as.nflximg.com.edgesuite.net	43	47.21M	1.69%	0.00%	100.00%	00:00:43	43.785	1.29%
netflix562.as.nflximg.com.edgesuite.net	32	38.97M	1.40%	0.00%	100.00%	00:00:22	22.216	0.66%
o-o.preferred.comcast-iad1.v2.lscache7.c.youtube.com	7	13.85M	0.50%	0.00%	100.00%	00:00:12	12.099	0.36%
www.mwburden.com	69	7.67M	0.27%	0.00%	100.00%	00:02:29	149.389	4.41%
cdn.yourzoom.com	273	6.83M	0.24%	0.00%	100.00%	00:00:23	23.010	0.68%
netflix148.as.nflximg.com.edgesuite.net	15	5.85M	0.21%	0.00%	100.00%	00:00:04	4.547	0.13%
v16.nonxt8.c.youtube.com	3	4.35M	0.16%	0.00%	100.00%	00:00:12	12.548	0.37%
netflix474.as.nflximg.com.edgesuite.net	14	2.79M	0.10%	0.00%	100.00%	00:00:02	2.797	0.08%
netflix570.as.nflximg.com.edgesuite.net	13	2.62M	0.09%	0.00%	100.00%	00:00:03	3.106	0.09%
i.ytimg.com	95	1.79M	0.06%	0.00%	100.00%	00:00:06	6.003	0.18%
demandware.edgesuite.net	142	1.70M	0.06%	0.00%	100.00%	00:00:20	20.998	0.62%
i35.tinypic.com	1	1.49M	0.05%	0.00%	100.00%	00:00:04	4.095	0.12%
us.icebreaker.com	177	1.06M	0.04%	0.00%	100.00%	00:00:31	31.375	0.93%
wood.nowcache.com	46	853.24K	0.03%	1.54%	98.46%	00:00:23	23.840	0.70%
1.bp.blogspot.com	19	835.35K	0.03%	0.00%	100.00%	00:00:02	2.132	0.06%
2.bp.blogspot.com	17	765.14K	0.03%	0.00%	100.00%	00:00:02	2.260	0.07%

Kuva 7. SARGin HTML-raportti (Jimiz.net 2014).

7 YHTEENVETO

Tavoitteena opinnäytetyössä oli saada palomuurijärjestelmä toimimaan Kansalaisen mikrotuessa. Palomuuri jakaisi verkon asiakaslaitteisiin ja henkilökunnan tietokoneisiin. Tehtävänä oli myös tutkia erilaisia mahdollisia tietoturvan parannuskeinoja sekä järjestellä yleisesti tiloja järkevämmiksi ja turvallisemmiksi. Lisäksi määriteltiin asiakasverkon sallittu liikenne vaaditulla tavalla eli että asiakasverkosta ei pääse kuin tärkeiksi valittuihin paikkoihin. Näin estetään mahdollisten saastuneiden asiakaskoneiden haittaohjelmien leviäminen Kansalaisen mikrotuen verkkoon ja sitä kautta koulun verkkoon. Asiakaskoneet kuitenkin puhdistetaan ensin melko perusteellisesti ennen verkkoon liittämistä, joten asiakasverkon liikenteen esto on kuin takuu haittaohjelmien leviämisen estämiseksi.

Tilat olivat jo entuudestaan tuttuja työharjoittelusta, joten pääkohdat olivat tiedossa. Työ alkoi keskittymällä palomuurikoneen toimintakuntoon saattamiseen, mikä hoitui tutustumalla aikaisempaan opinnäytetyöhön. Pfsense-järjestelmän uudelleenasentamisen jälkeen esiintyi ongelmia, mutta niihin keksittiin ratkaisu nopeasti. Laitteisto-ongelmat korvattiin vaihtamalla vioittuneet kytkimet toimiviin, jotka hankittiin Kansalaisen mikrotuesta tai Turun AMK:n varastosta. Kun verkko toimi halutulla tavalla, ryhdyttiin selvittämään asiakasverkon liikennettä. Sallittu liikenne määriteltiin sen hetkisen projektipäällikön kanssa seuraamalla lokitietoja ja valitsemalla oikeat osoitteet. Vain hyötysivustot ja ohjelmat sallittiin valkoiselle listalle, mutta muu liikenne estettiin kokonaan. Seuraava askel olisi hankkia kytkin, jonka avulla asiakaskoneet saataisiin omiin virtuaalisiin lähiverkkoihinsa, jolloin ne eivät pystyisi edes näkemään toisiaan. Toimenpide jätettiin pois, koska varastosta ei löytynyt ylimääräisiä kytkimiä ja sellaisen hankkimiseen ei saatu rahoitusta.

Palomuurikoneen ja verkon toimiessa vaaditulla tavalla ryhdyttiin tekemään suunnitelmia fyysisille toimenpiteille.

Suurimmat ongelmat koettiin palomuurikoneen kanssa, koska Pfsense piti periaatteessa asentaa kokonaan uudelleen, mikä poisti kaikki vanhat toimivat asetukset

Tilan järjestely ei vienyt kovinkaan kauaa ja mielenkiintoisinta oli osallistua Turun AMK:n julkaisun Näkökulmia Tietoturvaan 2 tekemiseen, missä tutkittiin Kansalaisen mikrotuen tietoturvaa sekä mietittiin tietoturvan parannuskeinoja.

LÄHTEET

Case-tutkimus 2014. Virtuaali ammattikorkeakoulu. Viitattu 3.3.2014. http://www2.amk.fi/digma.fi/www.amk.fi/opintojaksot/0709019/1193463890749/1193464144782/1194348546586/1194356433452.html.

Comodo forums. 2011. How to define a Network Zone for Windows Update servers? Viitattu 6.1.2014. https://forums.comodo.com/firewall-help-cis-b135.0/-t68776.0.html.

Exforsys, The use of trial and error to solve problems 2014. Viitattu 29.1.2014. http://www.exforsys.com/career-center/problem-solving/the-use-of-trial-and-error-to-solve-problems.html.

Freebsd 2014. The FreeBSD Project. Viitattu 28.2.2014. http://www.freebsd.org/.

Hiltunen, T. & Nummela, A. 2011. Mikrotukipalvelun huoltotietokanta. Opinnäytetyö. Tietojenkäsittely koulutusohjelma. Turku: Turun ammattikorkeakoulu.

Intergrated Technology.com 2014a. Internet cloud icon visiocloud image vector clip art online royalty free public domain. Viitattu 13.3.2014. http://intergratedtechnology.com/wp-content/uploads/2013/11/internet-cloud-icon-visiocloud-image---vector-clip-art-online-royalty-free-public-domain-mvn105bf.png.

Intergrated Technology.com 2014b. Wifi icon transparent black wifi icon clip art vector clip art online royalty free. Viitattu 13.3.2014. http://intergratedtechnology.com/wp-content/uploads/2013/10/wifi-icon-transparentblack-wifi-icon-clip-art---vector-clip-art-online-royalty-free-extietww.png.

Jimiz.net 2014. Pfsense – SARG (squid reports) setup. Viitattu 17.2.2014. http://jimiz.net/2012/01/pfsense-sarg-squid-reports-setup/#axzz2tZZCBVXP.

Metodix 2014. Konstruktiivinen tutkimusote. Viitattu 28.2.2014. http://www.metodix.com/fi/sisallys/04_virtuaalikirjasto/dokumentit/aineistot/konstruktiivinentutkimusote.

Mäkelä, T. 2013. Kansalaisen Mikrotuen palomuurijärjestelmä. Opinnäytetyö. Tietojenkäsittely koulutusohjelma. Turku: Turun ammattikorkeakoulu.

Mäkelä, T. & Virtanen, K. 2014. Tietoturva Kansalaisen mikrotuen oppimisympäristössä. Teoksessa Paavola, J. (toim.) Näkökulmia tietoturvaan 2. Turku: Turun ammattikorkeakoulu. Viitattu 13.3.2014. http://julkaisut.turkuamk.fi/isbn9789522164445.pdf. 89-94.

Saarinen, A. 2010. Kansalaisen Mikrotuki: nykytila ja tulevaisuus. Opinnäytetyö. Tietojenkäsittely koulutusohjelma. Turku: Turun ammattikorkeakoulu.

Sarg.SourceForge.net 2014. Project information. Viitattu 17.2.2014. http://sarg.sourceforge.net/.

Skear.HubPages.com 2014. The Best pfSense Packages. Viitattu 8.1.2014. http://skear.hubpages.com/hub/The-Best-pfSense-Packages.

Squid-cache.org 2014. Squid: Optimising Web Deliver. Viitattu 8.1.2014. http://www.squid-cache.org/.

Squid-cache wiki 2014. How do I make Windows Updates cache? Viitattu 8.1.2014. http://wiki.squid-cache.org/SquidFaq/WindowsUpdate.

Squidguard.org 2014. About squidGuard. Viitattu 15.1.2014. http://squidguard.org/about.html.

TechRepublic 2014. DIY pfSense firewall system beats others for features, reliability, and security. Viitattu 28.2.2014. http://www.techrepublic.com/blog/linux-and-open-source/diy-pfsense-firewall-system-beats-others-for-features-reliability-and-security/1110/.

Tamminen, T. 2010. Ninite Easy Pc Setup. Viitattu 6.1.2014. http://www.mbnet.fi/artikkeli/ajankohtaiset/viikon_ohjelmat/ninite_easy_pc_setup.

Trial and error. Wikipedia 2014. Viitattu 3.2.2014. http://en.wikipedia.org/wiki/Trial_and_error.

Työturvallisuuslaki 23.9.2002/738.