HAAGA-HELIA
ammattikorkeakoulu

Palomuurin valitseminen kannettavaan tietokoneeseen

Teemu Kolari

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

2012

Tiivistelmä

HAAGA-HELIA ammattikorkeakoulu

Tietojenkäsittelyn koulutusohjelma

Tekijä Teemu Kolari	**Ryhmä tai aloitusvuosi** 2011
Opinnäytetyön nimi Palomuurin valitseminen kannettavaan tietokoneeseen	**Sivu- ja liitesivumäärä** 57
Ohjaaja tai ohjaajat Titta Ahlberg	

Tämä opinnäytetyö käsittelee kannettavan tietokoneen tietoturvaa. Työssä käsitellään tietoturvaa yleisesti sekä tietoturvaa kannettavan tietokoneen näkökulmasta. Tähän näkökulmaan kuuluu olennaisena osana tilallinen palomuuri, jonka tehtävä, toimintatapa, mekanismit, hallinta, lokit ja sovelluskontrolli esitellään työssä.

Tutkimusosuudessa vertaillaan kolmea eri tilallista palomuuria, jotka ovat: Windows 7 Enterprise käyttöjärjestelmän palomuuri, F-Secure Internet Security 2012 palomuuri sekä Comodo palomuuri.

Tutkimuskysymyksiä on kaksi:
1) Miten tutkimukseen valitut palomuurit eroavat tietoturvaa parantavilta lisäominaisuuksiltaan sekä palomuurisääntöjen oletusasetuksiltaan?
2) Miten palomuurien lokitiedostot eroavat ominaisuuksiltaan ja kuinka konfiguroitavissa ne ovat?

Tutkimuksessa pyritään löytämään näistä kolmesta palomuurista soveltuvin kannettavan tietokoneen käyttäjille, jonka tietoturva-asiat (tässä tapauksessa palomuuri) on hänen itsensä hoidettavanaan.

Tutkimus toteutettiin ja vastauksia tutkimuskysymyksiin etsittiin asentamalla kyseiset palomuuri yksi kerrallaan Windows 7 käyttöjärjestelmän kannettavaan tietokoneeseen ja tekemällä havaintoja palomuureista sekä niihin kuuluvista tietoturvaa parantavista lisäohjelmistoista. Lisäksi palomuureille tehtiin hakkeriliikennettä simuloiva Nmap – porttiskanneritesti, jonka tulokset esitellään työssä.

Tämän opinnäytetyön teko aloitettiin keväällä 2011 ja se valmistui syksyllä 2012.

Tutkimuksen tuloksena suositellaan näistä kolmesta palomuurista Windows 7 Enterprise palomuuria.

Asiasanat
Palomuurit – Tietoturva, Kannettava tietokone, Windows 7

Abstract

HAAGA-HELIA ammattikorkeakoulu

Degree programme in Business Information Technology

Authors Teemu Kolari	**Group or year of entry** 2011
The title of thesis Choosing a firewall for a laptop	**Number of pages and appendices** 57
Supervisors Titta Ahlberg	

The purpose of this thesis was to find the best applicable firewall for laptop users who manage the data security of their laptop, in this case firewall, themselves. In addition, the thesis clarified some concepts as for stateful firewalls. These concepts included e.g. the task, mode of operation, mechanisms, control, logs and application control of the firewall.

The empirical section compared three different stateful firewalls which were Windows 7 Enterprise operating system firewall, F-Secure Internet Security 2012 firewall and Comodo firewall. In regard to these firewalls, the study investigated how these three firewalls differ from each other when comparing their additional data security features and their default firewall rules. Furthermore, the study looked into how the log files of these firewalls are different in terms of features and how configurable they are.

These three firewalls were installed, one at a time, on a Windows 7 laptop and observations were made of the firewalls and their additional data security features. In addition to that, firewalls were port scanned with Nmap port scanner to simulate hacker traffic.

The thesis concludes that Windows 7 Enterprise firewall is the most recommendable firewall choice for laptop data protection.

Key words
Firewall, Data security, Laptop, Windows 7

Sisällys

1 Johdanto

Tutkimuksesta on hyötyä sellaiselle kannettavan tietokoneen käyttäjille, esimerkiksi opiskelijalle, jolla on henkilökohtainen kannettava tietokone, jonka tietoturva-asiat (tässä tapauksessa palomuuri) on hänen itsensä hoidettavanaan. Nykypäivänä jokainen tietokone tarvitsee palomuurin, joten sen valinta on välttämätön, mutta erityisesti tästä tutkimuksesta on hyötyä käyttäjälle, joka haluaa kehittää osaamistaan ja ymmärtämistään palomuurien suhteen sen lokitietoja tarkkailemalla. Myös käyttäjä, joka on vasta hankkimassa omaa kannettavaa tietokonetta, voi kokea hyödyksi tutkimuksen osuuden, jossa vertaillaan näiden kolmen tutkittavan palomuurin eri lisäominaisuuksia. Tutkimus on suunnattu liikkuvalle ja aktiiviselle kannettavan tietokoneen käyttäjälle, jolla kannettava on ”aina” mukana, esimerkiksi Internetin ja sähköpostin käyttöä varten missä tahansa vieraassa verkossa.

Tutkimuskysymykset:

1) Miten tutkimukseen valitut palomuurit eroavat ominaisuuksiltaan sekä palomuurisääntöjen oletusasetuksiltaan?
2) Miten palomuurien lokitiedostot eroavat ominaisuuksiltaan ja kuinka konfiguroitavissa ne ovat?

2 Tietoturvan periaatteet

Tietoturva on nykysuomalaiselle päivittäinen asia. Se liittyy lähes jokaisen meistä päivittäiseen elämään. Käytämme tietokoneita, sähköpostia, matkapuhelinta, pankkipalveluita ja kanta-asiakaskortteja luottaen, että ne toimivat ja että ne säilyttävät omat tietomme muiden ulottumattomissa. Edellä mainituissa esimerkeissä käsitellään suuri määrä henkilökohtaisia sekä erittäin henkilökohtaisia tietoja meistä, joiden joutuminen vääriin käsiin ei missään nimessä olisi toivottavaa. Helposti käy niin, että ihmiset ymmärtävät tietoturvan tärkeyden vasta sitten, kun pahin on jo tapahtunut: tietokone on varastettu, sähköpostit on luettu, Internet selaimen historiatiedot rekisteröity tai liikkuminen kaupungilla jäljitetty matkapuhelimen sijaintitietojen perusteella. Varsinkin meillä Suomessa, jossa olemme uuden tekniikan edelläkävijöitä, vaara on konkreettinen, koska meiltä puuttuu uuteen tekniikkaan liittyvä kriittisyys ja julkinen keskustelu. Tietoyhteiskunnan myötä yhä useampi arkipäivän askare siirtyy verkossa hoidettavaksi ja näin ollen hyödyntää tietotekniikkaa. (Järvinen 2002, 17.)

Tietoturva koostuu kolmesta eri osa-alueesta, jotka ovat:

- tiedon luottamuksellisuus (confidentiality)
- tiedon eheys (integrity)
- tiedon saatavuus (availability)

Kaikki nämä osa-alueet käsittelevät tietoa sen eri muodoissa: tiedostoina (esimerkiksi dokumentit), tiedonsiirtona (esimerkiksi sähköpostiviestit) tai bittien joukkona (esimerkiksi koneen keskusmuistissa käsittelyssä oleva tieto). Seuraavassa tarkastellaan yllä mainittuja osa-alueita tarkemmin.

2.1 Tiedon luottamuksellisuus

Tiedon luottamuksellisuudella tarkoitetaan sitä, että tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen käytettävissä. Toisin sanoen pyritään siihen, että kukaan ei pääse käyttämään tietoa, jota hänen ei ole tarkoitettu käyttää. Valtuutettujen käyttäjien tunnistamiseen käytetään todentamista, ja valtuuttamattomien käyttäjien pääsy tietoon estetään salauksen avulla. Todennus- ja salausmenetelmiä on useita, mutta lähtökohtana voidaan pitää, että mitä turvallisempi menetelmä, sitä varmemmin tieto säilyy luottamuksellisena.

2.2 Tiedon eheys

Tiedon eheydellä tarkoitetaan sitä, että tieto on pysynyt oikeana ja ajantasaisena eli ettei mikään ulkopuolinen taho ole pystynyt sitä luvatta muuttamaan. Tiedon muuttaminen käsittää niin tiedon päivittämisen kuin kokonaan tuhoamisenkin. Tiedon eheyttä pyritään turvaamaan tarkistussummilla, lokitiedostoilla, tiedonsiirron protokollilla sekä erilaisilla sisäisillä tarkastuksilla ja tarkistusohjelmilla, esimerkiksi virustorjuntaohjelmat. Tiedon eheyden rikkomisen keinoja on useita. Esimerkiksi virukset rikkovat tiedon eheyttä samoin hakkerit, jotka murtautuvat www-sivuille ja muuttavat siellä olevaa tietoa.

2.3 Tiedon saatavuus

Tiedon saatavuus tarkoittaa tietojärjestelmien toimivuutta. Tietojärjestelmien toiminnan turvaaminen on olennaisin asia tiedon saatavuudessa. Järjestelmien ja koneiden pitää olla päällä, ja niissä oleva tieto saatavilla aina kun sitä tarvitaan. Verkkopalveluissa se tarkoittaa, että tiedon pitää olla saatavilla 24 tuntia vuorokaudessa seitsemänä päivänä viikossa. Tärkein keino saatavuuden varmistamiseen on tiedostojen varmuuskopiointi, sillä koneista ja yhteyksistä niihin ei ole hyötyä, jos niissä säilöttynä oleva tieto ei ole saatavilla. Toinen saatavuutta varmistava keino on laitteiden turvaaminen tekniikan avulla, esimerkiksi UPS-laite sähkökatkojen varalta. Tiedon tai palvelun saatavuutta voidaan häiritä esimerkiksi tarkoituksellisella ylikuormituksella (palvelunestohyökkäys), jolla pyritään estämään palvelun normaali toiminta tai tiedon normaali saatavilla oleminen. (Järvinen 2002, 22–24.)

3 Kannettavan tietokoneen tietoturva

Edellä on havainnollistettu tietoturvan peruspilarit. Seuraavaksi käsitellään näitä peruspilareita kannettavan tietokoneen näkökulmasta.

3.1 Tiedon luottamuksellisuus kannettavassa tietokoneessa

Kannettavassa tietokoneessa tiedon luottamuksellisuus tarkoittaa sitä, että kukaan muu kuin kannettavan omistaja tai hänen valtuuttamansa henkilö ei pääse kannettavan tiedostoihin tai järjestelmiin käsiksi.

Yksi keino varmistaa edellä mainittu luottamuksellisuus on luoda kaikille kannettavan tietokoneen käyttäjille oma käyttäjätili. Tällöin on tunnettava sekä käyttäjätilin tunnus, että sitä vastaa-

va salasana, jotta saa käyttöoikeuden. Usein käyttäjätunnus on johdettu suku- ja etunimestä, joten se on melko helposti pääteltävissä. Tästäkin syystä salasanan on oltava salainen koodi, eikä esimerkiksi käyttäjän syntymäajasta johdettu merkkijono tms. Salasana ei ole erityisen hyvä tietoturvajärjestely, koska sen ongelmat riippuvat ennen muuta ihmisestä. Tästäkin huolimatta salasanoja käytetään tiedon luottamuksellisuuden ylläpitämiseksi erittäin paljon ja tämä taas johtuu siitä, että se on käytännössä ainoa käyttökelpoinen vaihtoehto. Kannettavan tietokoneen käyttäjätunnuksen salasanaa valittaessa tulee muistaa että:

- hyvä salasana ei löydy sanakirjoista eikä se ole kenenkään nimi
- huono salasana ei muutu hyväksi lisäämällä sen jatkoksi numeroita
- hyvä salasana on riittävän pitkä (8 merkkiä on aivan liian vähän, 15 merkkiä on sopiva lähtökohta)
- hyvää salasanaa ei ole kierrätetty eri palveluissa

(CERT-FI – Vaihda salasanasi vahvempiin)

Kannettavan tietokoneen tiedon luottamuksellisuuden säilyttämiseksi käytettävään käyttäjätilin salasanaan tulee valita isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä. Näin varmistetaan salasanan mahdollisimman vaikea murtaminen. Salasanan vaihtamisesta voidaan kannettavan tietokoneen käyttäjätilin hallinnassa asettaa omat sääntönsä ja suositeltavaa sekä yleistä on, että salasana asetetaan vaihdettavaksi 30 päivän välein. Yksi syy vaihtamiseen on se, että hakkerit yleensä käyttävät murtamiaan salasanoja vain vähän, jottei murto tulisi ilmi. Salasanan säännöllisellä vaihtamisella vaikeutetaan hakkereiden onnistumista sekä rajoitetaan onnistuneiden salasanan murtojen vaikutuksia. (Korpela 2005, 121–131.)

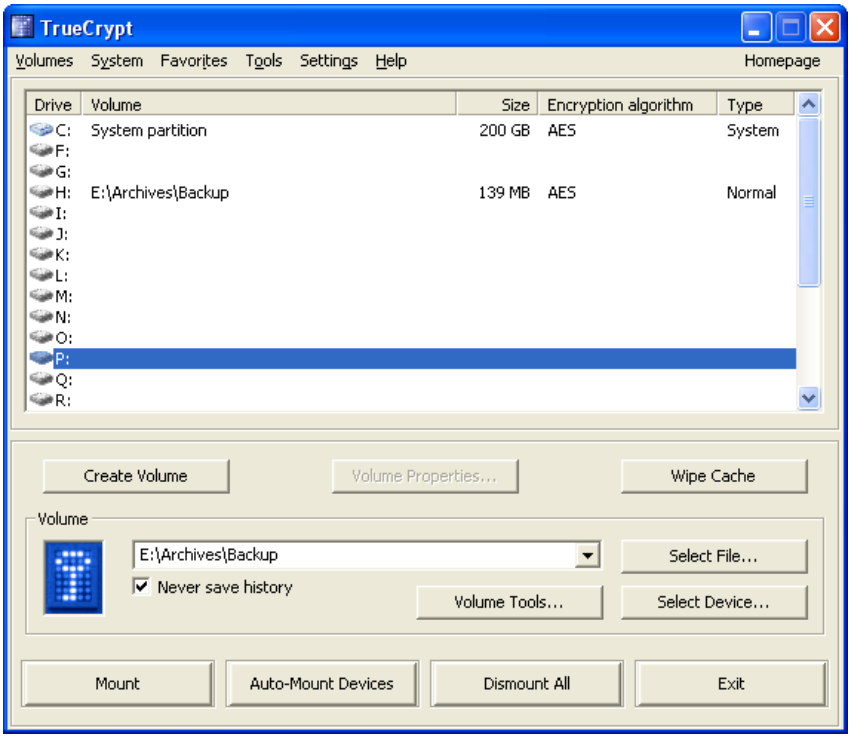
Toinen tärkeä asia kannettavan tietokoneen tiedon luottamuksellisuuden ylläpitämisessä tulee esille ohjelmia asentaessa tai päivitettäessä. Ohjelmien asentaminen tai päivittäminen vaatii järjestelmäylläpitäjän oikeuksia. Tämä johtuu siitä, että ohjelmaa asennettaessa tai päivitettäessä siihen liittyviä tiedostoja on sijoitettava järjestelmän kansioon johon ei tavallisella käyttäjätunnuksella ole oikeutta tehdä muutoksia. Järjestelmäylläpitäjän oikeuksia taas ei ole järkevää käyttää koko ajan, koska kannettavan tietokoneen peruskäyttö onnistuu ilman näitä oikeuksia ja lisäksi järjestelmänvalvojana toimiva henkilö voi tehdä epähuomiossa vahinkoa kannettavan tietokoneen tiedostoille tai järjestelmille. Tämän takia järjestelmävalvojalla tulee olla myös tavallinen käyttäjän oikeuksin varustettu käyttäjätili, jota käytetään kaikkeen missä näitä laajempia oikeuksia ei tarvita. Kuitenkin, kun uusi ohjelma tai päivitys on asennettu, sitä on järkevintä testata tavallisena käyttäjänä, koska jos ohjelma esimerkiksi onkin virus tai haittaohjelma, se ei

pysty tekemään sen enempää vauriota kannettavan tietokoneen tiedon luottamuksellisuuteen, kuin mitä tavallisella käyttäjätunnuksella pystyy. (Korpela 2005, 140.)

Kolmas merkittävä asia kannettavan tietokoneen tiedon luottamuksellisuuden saavuttamiseksi on tietojen salaaminen. Kannettavan tietokoneen tiedot on tallennettu kovalevylle, ja tätä kovalevyä ei pystytä täydellisesti suojaamaan käyttäjätileillä ja salasanoilla. Tästä syystä on järkevää ainakin harkita kannettavan tietokoneen kovalevyn tietojen salausta.

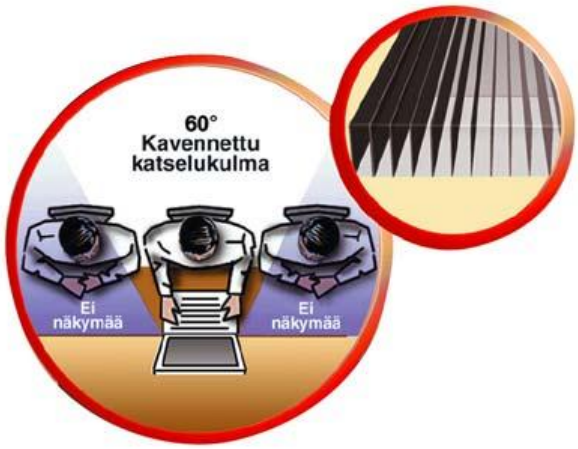
Tietojen salaamisella tarkoitetaan kannettavan tietokoneen kovalevyllä olevien tietojen salaamista salausohjelman avulla. Tämä henkilökohtaisten tai muiden tärkeiden ja arkaluontoisten tietojen salaaminen tulee kysymykseen erityisesti, kun käytössä on kannettava tietokone. (Tietoturvaopas – Tietoturvaohjelmat)

Hyvä esimerkki salausohjelmasta, jolla nämä henkilökohtaiset tai muut tärkeät ja arkaluontoiset tiedot kannettavasta tietokoneesta voi salata, on TrueCrypt. Se on ilmainen ja yhteensopiva muun muassa Windows – käyttöjärjestelmän kanssa. Tällä ohjelmalla voi salata kokonaisia levyosioita tai vaihtoehtoisesti tehdä ns. säiliötiedostoja, jotka näkyvät omana levyasemanaan. TrueCrypt on reaaliaikainen salausohjelma, joka tarkoittaa sitä, että tiedostot salataan juuri ennen kuin ne tallennetaan ja vastaavasti salaus puretaan juuri ennen kuin tiedosto avataan. Salatulle kiintolevylle / levyosiolle talletettua tiedostoa ei voi avata salaamattomana, jos ei tiedä salauksen avaamiseen tarvittavaa salasanaa / avainta. Tämä ohjelma ei talleta salaamatonta tietoa minnekään kovalevylle salausprosessin aikana, vaan se käyttää tietokoneen muistia väliaikaiseen tallennukseen. Kuviossa 1 näkyy TrueCrypt ohjelman perusnäkymä, jossa on valittu salatuksi levyosioiksi E:\Archives\Backup – kansio. ”Create Volume” – napista voi halutessaan helposti tehdä uuden salatun osion. (TrueCrypt – Beginner’s Tutorial)



Kuvio 1: TrueCrypt – ohjelman perusnäkymä (TrueCrypt – Beginner's Tutorial)

Edellä on mainittu kolme keskeistä asiaa kannettavan tietokoneen tietojen luottamuksellisuuden takaamiseksi, mutta toki on muitakin yksittäisiä asioita, joita tulee ottaa huomioon. Tiedon luottamuksellisuuteen vaikuttaa ihan yksinkertaisesti myös se, että näkeekö ulkopuoliset kannettavan tietokoneen ruudun kun sitä käytetään julkisessa tilassa esimerkiksi junassa. Sivullisia voi estää näkemästä ruutua hankkimalla ruudun suojaksi ns. tietoturvasuojan, joka kaventaa näytön katselukulmaa niin, että sen näkee vain suoraan edestäpäin ja läheltä katsottuna. Kuviossa 2 on havainnollistettu tietoturvasuojan toimintaperiaate, eli edes kannettavan tietokoneen ruudun vierestä ei näe ruudun sisältöä. (Staples Finland Oy – Näyttöjen tietoturvasuojat)



Kuvio 2: Tietoturvasuojan toiminta (Staples Finland Oy – Näyttöjen tietoturvasuojat)

Lisäksi on tärkeää varautua myös fyysisiin tietoturvauhkiin kannettavan tietokoneen tietojen luottamuksellisuuden takaamiseksi eli on syytä lukita kannettava tietokone ns. vaijerilukolla aina, kun se on mahdollista. Vaijerilukon avulla kannettava tietokone lukitaan sen rungossa sijaitsevan lukituskolon kautta, kuten kuviossa 3 on nähtävissä. Esimerkiksi kirjastossa tai Internet kahvilassa on hyvä harkita kannettavan tietokoneen lukitsemista vaikka pöydänjalkaa tai jotain muuta kiinteää apuvälinettä hyväksikäyttäen. Vaijerilukkoja on saatavilla monenlaisia, esimerkiksi avaimella lukittavia tai numeroyhdistelmällä lukittavia. Lisäksi on olemassa tuplavaijerilukkoja, joilla voi lukita kaksi laitetta samalla lukolla. (Visiolink Oy – Datalaitteiden lukitus)

Kuvio 3: Vaijerilukon toiminta (Visiolink Oy – Datalaitteiden lukitus)

3.2 Tiedon eheys kannettavassa tietokoneessa

Jotta kannettavan tietokoneen tiedot pysyvät eheänä, oikeanlaisena, ajantasaisena ja muuttumattomana, tulee sen käyttöjärjestelmän sekä käyttöjärjestelmän päälle asennettujen ohjelmien toimivuus taata. Niiden tietoturva on tärkein asia tiedon eheyden saavuttamiseksi, kun kyseessä on kannettava tietokone.

Windows käyttöjärjestelmä on laaja ohjelmisto, joka koostuu useista eri osista ja johon kuuluu myös Internet Explorer -selain sekä Windows Live Mail -sähköpostiohjelma. Käyttöjärjestelmässä sekä sen ohjelmissa on virheitä, kuten käytännössä kaikissa ohjelmissa on. Osa virheistä on tietoturva-aukkoja, jotka vaarantavat tiedon eheyden. Tämän takia ohjelmiin, mukaan lukien käyttöjärjestelmä, tehdään päivityksiä ja huoltopaketteja. Huoltopaketit ovat isompia muutoksia ja niitä tulee harvemmin, kun taas päivitykset ovat pienempiä ja useammin ilmestyviä ja niissä tyypillisesti paikkaillaan löytyneitä tietoturva-aukkoja aiheuttavia virheitä. Näiden tiedon eheyttä turvaavien korjausten ajan tasalla pitämiseksi on syytä käyttää Windows Update -palvelua esimerkiksi määrittelemällä kannettava tietokone hakemaan korjaukset automaattisesti.

Windows Update on Microsoft Windows – käyttöjärjestelmää käyttäville tietokoneille tarkoitettu palvelu, jonka kautta asennetaan ilmestyneet korjaukset. Valittavana on kaksi tapaa:

- automaattinen päivitys, jossa Windows hakee korjaukset automaattisesti
- manuaalinen päivitys, jossa korjausten haku jää käyttäjän vastuulle

Automaattipäivityksessä haetaan Microsoftin kriittisiksi luokitellut päivitykset ja huoltopaketit automaattisesti ja valittavana on muutama eri tapa niiden asennukseen:

- automaattinen asennus, jossa voidaan valita päivä ja aika jolloin korjaukset haetaan ja haun jälkeen asennetaan
- automaattinen lataus, jossa korjaukset vain haetaan tietokoneelle valmiiksi mutta ei asenneta
- automaattinen ilmoitus, jossa saatavilla olevista uusista korjauksista ilmoitetaan mutta niitä ei haeta saati asenneta.

Yllämainittujen lisäksi on siis olemassa myös vaihtoehto, jossa korjauksista ei edes ilmoiteta eli tässä tapauksessa niistä pitää huolehtia täysin manuaalisesti. Tämä on huono ja ei suositeltava vaihtoehto mutta toki täysin toimiva myös kunhan tietokoneen käyttäjä muistaa säännöllisesti käydä Windows Update – sivulla tarkistamassa, onko korjauksia saatavilla. Huolimatta siitä kumpaa tapaa käyttää on syytä käydä Windows Update – sivulla kuitenkin säännöllisesti sillä sitä kautta voi asentaa myös sellaisia korjauksia, joita ei ole luokiteltu kriittisiksi. Nämä ovat pääasiassa järjestelmän toimintoja laajentavia täydennyksiä eivätkä virheiden korjauksia, mutta yhtä kaikki nämä korjaukset auttavat pitämään kannettavan tietokoneen eheänä. (Korpela 2005, 32–37.)

Yksin käyttöjärjestelmän ja siihen kuuluvien ohjelmien tietoturvan hoitaminen ei vielä riitä, vaan varmistaakseen kannettavassa tietokoneessa olevan tiedon eheyden pitää ottaa huomioon useita muitakin asioita. Näistä tärkeimmät ovat tietoturvaa parantavat ohjelmat kuten virustorjunta- ja palomuuri-ohjelmat. Virus on tietokoneohjelma tai ohjelman osa, jonka tarkoitus on tuhota tai muuttaa esimerkiksi kannettavassa tietokoneessa olevia tietoja tai muuten haitata toimintaa. Virukset leviävät monin eri tavoin, mutta pääasiassa sähköpostin liitetiedostojen tai Internet -sivujen kautta. Viruksilta suojautuminen edellyttää sitä varten kehitetyn ohjelman käyttöä, eli virustorjuntaohjelman käyttöä. Kannettavaan tietokoneeseen on siis asennettava virustorjunta ohjelma. Virustorjuntaohjelman toiminta perustuu siihen, että se tunnistaa viruk-

set tunnettujen ominaisuuksien perusteella. Tästä syystä on ensiarvoisen tärkeää, että myös virustorjuntaohjelmaa pidetään jatkuvasti ajan tasalla. Virustorjuntaohjelmassa on niin sanottu virustietokanta, jossa on tieto tunnetuista viruksista ja aina kun löytyy uusi virus, sen tiedot lisätään ohjelman toimittajan virustietokantaan. Kannettavan tietokoneen virustorjuntaohjelman virustietokanta tulee siis päivittää joka päivä toimittajan virustietokantaa vastaavaksi, jotta ohjelman toimintaan voi luottaa. Tämän päivityksen voi myös määrittää tapahtumaan automaattisesti. (Korpela 2005, 63–65.)

Kolmas erittäin tärkeä asia kannettavan tietokoneen tietojen eheyden turvaamiseksi on valvoa sekä kontrolloida tietoliikennettä kannettavan tietokoneen ja ulkomaailman välillä. Tätä varten kannettavaan tietokoneeseen tarvitaan palomuuri. Palomuuri on ohjelma, joka valvoo ja kontrolloi verkkoliikennettä niin ettei kukaan voi näkymättömästi käyttää kannettavaa tietokonetta verkon kautta. Näin se estää myös mahdollisesti koneeseen päässeitä viruksia ottamasta yhteyttä ulospäin. Palomuuri ja virustorjunta täydentävät toisiaan mutta eivät korvaa toisiaan. Molemmat siis tarvitaan. Kun virustorjunta suojaa kannettavassa tietokoneessa olevia ohjelmia ja tiedostoja niin palomuuri estää ulkopuolisia ”komentamasta” kannettavassa tietokoneessa olevia ohjelmia asiattomalla tavalla. Kannettavassa tietokoneessa, joka on liitettynä verkkoon, on useita liittymiä, eli portteja, jota kautta tietoliikenne voi kulkea. Palomuuri valvoo näitä portteja käytännössä sulkemalla ne ja päästämällä läpi vain sellaisen liikenteen, jonka tietää olevan sallittua. (Korpela 2005, 86–87.)

3.3 Tiedon saatavuus kannettavassa tietokoneessa

Lyhyesti kerrattuna tiedon saatavuudella siis tarkoitetaan tietojärjestelmien toimivuutta. Kannettavassa tietokoneessa tietojärjestelmä on käytännössä koko kannettavan tietokoneen sisältö eli tiedostot, jotka sen kovalevyllä sijaitsevat. Näin ollen tärkein yksittäinen asia tiedon saatavuuden turvaamiseksi kannettavassa tietokoneessa on tietojen varmuuskopiointi.

Tyypillisesti kannettavan tietokoneen kovalevyllä on sen käyttäjän valokuvia, muistiinpanoja sekä muita henkilökohtaisia sekä tärkeitä tiedostoja. Jos näistä ei oteta varmuuskopiota, ne on hyvin vaikea saada takaisin jos esimerkiksi kannettavan tietokoneen kovalevy hajoaa. Hajonneen kovalevyn tietoja voidaan jossain tapauksissa saada palautettua mutta tämmöinen toimenpide on erittäin kallis. Tämän takia on syytä huolehtia, että varmuuskopiointi tehdään säännöllisesti, sillä se on paljon helpompi ja kustannuksiltaan pienempi operaatio kuin edellä mainittu tiedostojen palauttaminen rikkoutuneelta kovalevyltä. Kovalevyn rikkoutumisen lisäksi toisena uhkana kovalevyn tiedoille on eri ohjelmien sekä käyttöjärjestelmän päivitykset, jois-

sa toisinaan on vikoja, jotka saattavat vaarantaa tallennettuja tiedostoja. Näin tosin tapahtuu ani harvoin.

Varmistukset on tärkeä jakaa kahteen eri osioon, jotka ovat:

- järjestelmän varmistukset
- työtiedostojen varmistukset

Järjestelmän varmistamisella taataan kannettavan tietokoneen käytettävyys mahdollisimman vähin katkoin eli vastataan fyysisiin uhkiin, kuten konerikkoihin, haittaohjelmien aiheuttamiin ongelmiin ja varkauksiin. Työtiedostojen varmistamisella taasen taataan kannettavan tietokoneen työn jatkuvuus, säilyvyys ja osittain siirrettävyyskin. Koska työtiedostot eivät ole riippuvaisia järjestelmästä, ne voidaan esimerkiksi kannettavan tietokoneen vaihtuessa siirtää helposti uuteen järjestelmään. Molemmissa tapauksissa varmistukset kannattaa automatisoida jos siihen on mahdollisuus ja lisänä tälle kannettavan tietokoneen käyttäjä voi ottaa erikseen ylimääräisiä varmistuksia manuaalisesti, kun kokee sen olevan tarpeellista. Lisäksi on syytä varmistaa varmistusten toimivuus eli käytännössä testata miten järjestelmän tai työtiedostojen palauttaminen onnistuu.

Järjestelmän varmistusta ei tarvitse tehdä yhtä usein kuin työtiedostojen varmistus on syytä tehdä. On kannettavan tietokoneen käyttäjän harkinnan mukaista, kuinka suurena ja aikaa vievänä työnä hän näkee mahdollisen koko järjestelmän uudelleen rakentamisen. Tämä tarkoittaa käyttöjärjestelmän ja ohjelmien asennusta, niihin päivitysten hakemista Internetistä sekä työtiedostojen palauttamista uusittuun järjestelmään. Hyvä tapa on tehdä kannettavan tietokoneen järjestelmävarmistus kahdesti vuodessa sekä aina ennen isompia käyttöjärjestelmän päivityksiä (esimerkiksi Service Packeja) ja muista isompia asennuksia. Ensimmäinen järjestelmävarmistus kannattaa aina ottaa heti järjestelmän perusasennuksen jälkeen. Tätä varmistusta on syytä säilyttää kannettavan tietokoneen elinkaaren loppuun asti, koska sen avulla voidaan aina palata ns. alkupisteeseen. Varmistuksista on syytä säilyttää muitakin versioita, kuin uusin. Tämä puhtaasti sen takia, että jos esimerkiksi jokin haittaohjelma on päässyt pesiytymään kannettavaan tietokoneeseen, se on saattanut olla järjestelmässä jo pidempään passiivisena jolloin on tarpeen löytää järjestelmävarmistus niin pitkän ajan takaa, jossa tätä haittaohjelmaa ei vielä kannettavassa tietokoneessa ollut.

Työtiedostojen varmistaminen tulee siis olla tiheämpää kuin järjestelmän. Työtiedostojen varmistustarve kannettavassa tietokoneessa määräytyy käytännössä niiden tärkeyden mukaan – jos käyttäjä päivittää tärkeää tiedostoa päivittäin, on siitä syytä ottaa varmuuskopio päivittäin. Koskaan ei voi tietää milloin kovalevy hajoaa vai hajoaako ollenkaan. Kun työtiedostojen varmistus on automatisoitu riittää, että talteen otetaan vain tiedostot, jotka ovat muuttuneet. Näin vältetään varmistettavan tiedostomäärän kasvamista turhan suureksi sekä varmistukseen käytettävän ajan kasvamista. On myös syytä huomata, että työtiedoston kopioiminen samassa kannettavassa tietokoneessa sijaitsevan saman kovalevyn eri kansioon ei suojaa mahdolliselta kovalevyn rikkoutumiselta – varmistus pitää siis tehdä eri medialle.

Tiedon saatavuuden varmistamiseksi otettavien varmistusten tallennusmedioita löytyy monenlaisia. Kaikki eivät sovi kaikkiin tarkoituksiin joskaan mikään ei varmastikaan yksinään sovi jokaiseen tarkoitukseen. Seuraavassa on esitelty yleisimmät vaihtoehdot tallennusmedioiksi:

- optiset mediat, eli kirjoitettavat CD, DVD ja Blu-ray – levyt
- muistitikut ja -kortit
- ulkoinen, erillinen kiintolevy
- sisäinen, lisäkiintolevy
- A4 paperivarmistus eli esimerkiksi valokuvien tulostaminen paperille ja kansiointi
- tallennuspalvelut Internetissä (esimerkiksi Saunalahden Holvi-palvelu)

Yllä esitellyistä vaihtoehdoista varmasti jokainen kannettavan tietokoneen käyttäjä, joka haluaa varmistaa tietojensa saatavuuden löytää käyttötarkoituksiinsa sopivimman. Merkitsevää on tallennusmedian koko, medialle siirtämisen nopeus sekä joissain tapauksissa myös median siirreltävyys. (MicroPC 12 / 2008, 24–27.)

Automaattisen varmistuksen kannettavan tietokoneen tietojen saatavuuden varmistamiseksi voi järjestää esimerkiksi Saunalahden Holvi-palvelulla, joka itsessään on ilmainen mutta on osa maksullista palvelukokonaisuutta. Tämä palvelu tekee varmistukset kannettavasta tietokoneesta automaattisesti, turvallisesti ja huomaamattomasti. Käyttäjän valitsemat tiedostot pakataan, salataan ja siirretään turvaan Saunalahden palvelimella olevalle verkkolevylle, johon vain käyttäjällä on pääsy. Lisäksi tuon verkkolevyn tiedoista otetaan varmuuskopio. Palvelua varten kannettavalle tietokoneelle tulee asentaa ohjelma, joka suorittaa varmistuksen käyttäjän määrittelemällä tavalla. (Saunalahti – Holvi backup)

4 Kannettavan tietokoneen palomuuri

Yksi tärkeimmistä tietoturvaa ylläpitävistä tekijöistä kannettavassa tietokoneessa on palomuuri. Palomuureja on monenlaisia mutta tässä keskitytään ohjelmalliseen tilalliseen palomuuriin, joka asennetaan kannettavaan tietokoneeseen valvomaan sekä ulos- että sisäänpäin kulkevaa liikennettä.

4.1 Palomuurin tehtävä

Palomuuri on ohjelma tai laite, joka valvoo ja rajoittaa tietokoneen ja muun maailman välistä liikennettä. Sillä pyritään estämään tietokoneen luvaton ja näkymätön käyttö verkon kautta. Se myös ehkäisee mahdollisia tietokoneessa olevia viruksia ottamasta yhteyttä ulospäin. (Korpela 2005, 86.)

Etenkin kannettavassa tietokoneessa jota oletettavasti liikutellaan paljon ja joka oletettavasti on yhteydessä säännöllisesti eri julkisiin verkkoihin, palomuurin tärkeys korostuu. Liikkuva käyttäjä käyttää kannettavaansa nykypäivänä verkossa lähes koko ajan riippumatta siitä missä hän kannettavansa kanssa on. Hän ei voi luottaa verkkoon johon kannettavansa liittää, josta syystä palomuurin on oltava pitävä sekä oikein konfiguroitu, että se täyttää tehtävänsä.

4.2 Palomuurin toimintatapa

Palomuuri tarkistaa jokaisen paketin, joka kulkee sen läpi. Jos se pystyy toteamaan, että paketti ei ole sallittu tai on uhkaava, se hylkää paketin eli estää paketin pääsyn läpi. Vastaavasti, jos pakettia ei todeta kielletyksi tai uhkaavaksi, se päästetään läpi jatkamaan kohti kohdettaan. Huomioitavaa on, että siis myös sellaiset uhkaavat paketit joita palomuuri ei tunnista, pääsevät läpi. Niistä paketeista joita palomuuri ei päästä läpi, se pitää kirjaa eli kirjoittaa lokitiedostoa. Tätä lokitiedostoa tulee palomuurin ylläpitäjän tutkia säännöllisesti, koska se antaa erityisen tärkeää tietoa erityyppisistä uhkaavista paketeista. (Panko 2008, 251–252.)

Edellä on kuvattu palomuurin toimintatapa kaikessa yksinkertaisuudessaan. Tämän lisäksi palomuurin toimintatapaan liittyy lokitiedot sekä sääntölistat. Näistä ominaisuuksista kerrotaan tarkemmin seuraavissa kappaleissa mutta jo tässä yhteydessä on syytä mainita, että myös nämä kaksi ominaisuutta ovat olennaisia ja tärkeitä palasia palomuurin toiminnassa.

4.3 Palomuurimekanismit

Palomuuri siis suodattaa liikennettä ja riippuen palomuurista, käyttää siihen erilaisia menetelmiä. Näitä menetelmiä ovat muun muassa tilaton ja tilallinen pakettisuodattaminen, osoitemuunnos (engl. NAT, Network Address Translation) sekä sovellustason suodatus (engl. Proxy). (Panko 2008, 254–268.)

4.4 Tilallinen pakettisuodatin

Tässä työssä keskitytään siis tilalliseen pakettisuodattimeen eli palomuuriin, joka asennetaan kannettavaan tietokoneeseen. Keskeistä tilallisen pakettisuodattimen toiminnassa on tila. Se keskittyy eri tiloihin kahden ohjelman välisessä yhteydessä. Seuraavassa yksinkertainen esimerkki, jossa kuvitellaan kaksi eri tilaa:

1. tila, jossa yritetään avata yhteys toiseen ohjelmaan/tietokoneeseen
2. tila, jossa yhteys on avattu ja kommunikointi on meneillään.

Ensin siis selvitetään paketista joka saapuu, että onko se avaamassa yhteyttä vai ei. Jos paketti tulee sisäverkosta ja on yhteyttä avaamassa oleva paketti, oletuksena on, että yhteyden avaus on sallittu. Jos halutaan estää sisäverkon yhteyksiä, ne pitää kieltää erikseen sääntölistan avulla. Jos paketti tulee ulkoverkosta ja on yhteyttä avaamassa oleva paketti, se on oletuksena kielletty jolloin vastaavasti sääntölistalla pitää olla kiellon kumoava merkintä, jos yhteyden avaamisen halutaan olevan sallittu.

Suurin osa paketeista on kuitenkin meneillään olevaa kommunikointia. Niihin tilallinen pakettisuodatin suhtautuu tehokkaasti: jos paketti on osa meneillään olevaa ja aiemmin hyväksyttyä yhteyttä se päästetään läpi ja vastaavasti jos se ei ole, niin sitä ei päästetä. Tämä ominaisuus tekee tilallisesta palomuurista nopean ja mahdollistaa sen käytön myös silloin, kun liikennettä on paljon. Toisaalta niitä paketteja, jotka yrittävät avata yhteyden, tilallinen pakettisuodatin ei käsittele kovinkaan yksinkertaisesti. Näitä paketteja on – kuten mainittu – onneksi kuitenkin vähän, joten tämä ei tee tilallisesta palomuurista hidasta tai käyttökelvotonta.

Tietoliikenteessä normaali tapa yhteydelle on socket, joka nimeää ohjelman, portin sekä IP-osoitteen. Socket kirjoitetaan IP -osoitteena jonka perässä on kaksoispiste sekä portin numero, esimerkiksi 10.3.47.16:4400. Yhteys on kahdessa eri tietokoneessa olevien ohjelmien välinen

linkki, joka koostuu kahdesta socketista – sisäisestä ja ulkoisesta. Tätä tapaa yhteyksissä käyttää myös tilallinen pakettisuodatin. (Panko 2008, 258–259.)

Aiemmin kerrottiin siis paketeista, jotka yrittävät avata yhteyttä sekä paketeista, jotka eivät yritä avata yhteyttä ja ovat todennäköisesti jo olemassa olevan yhteyden kommunikointi-paketteja. Seuraavaksi käydään läpi mitä näillä eri paketeilla tarkoitetaan, miten tilallinen palomuuri niitä käsittelee ja miten se tunnistaa ne.

4.4.1 Paketit jotka eivät yritä avata yhteyttä

Kun paketti, joka ei yritä avata yhteyttä saapuu, tilallinen palomuuri tarkistaa onko se osa olemassa olevaa aiemmin hyväksyttyä yhteyttä. Tämä tarkistus tapahtuu tutkimalla yhteystaulua johon on merkattu kaikki olemassa olevat hyväksytyt yhteydet sekä niiden tyyppi, lähde IP -osoite, lähdeportti, kohde IP -osoite, kohdeportti sekä yhteyden tila. Jos paketti on osa olemassa olevaa yhteyttä eli löytyy yhteystaulusta, se päästetään läpi ja vastaavasti jos ei ole, sitä ei päästetä läpi ja tämä kirjoitetaan lokitauluun. (Panko 2008, 260–261.)

4.4.2 Paketit jotka yrittävät avata yhteyden

Oletuksena tilallinen palomuuri sallii yhteyksien avaamiset sisäverkosta ulkoverkkoon, koska on yleisesti hyväksyttävää ottaa yhteys niin päin. Kun näin tapahtuu eli yhteys sallitaan, merkataan tämä muodostettu yhteys yhteystauluun. Toinen oletus on, että tilallinen palomuuri estää kaikki yhteydenavausyritykset ulkoverkosta sisäverkkoon, koska on normaalia että vain tiedetyt ulkoiset tietokoneet ovat hyväksyttyjä avaamaan yhteys sisäverkon tietokoneisiin. (Panko 2008, 262–263.)

4.5 Sääntölistat

Jo aiemmin mainitut sääntölistat ovat olennainen osa palomuurin konfigurointia sellaiseksi, että se sekä suojaa tietoturvamielessä, että mahdollistaa oikeat halutut yhteydet. Sääntölista tehdään siihen tarkoitukseen, että sen avulla saadaan tilallinen palomuuri toimimaan vastoin oletussääntöjä eli muokataan ne halutunlaisiksi. Oletussääntönä kun esimerkiksi on estetty kaikki ulkoa sisäänpäin tulevat yhteyden avausyritykset, niin sääntölistan avulla luodaan tähän yksittäinen poikkeus. Esimerkiksi sallitaan sisäänpäin tulevan paketin avata yhteys tiettyyn palveluun, kuten Skype – ohjelmassa. Toinen hyvä esimerkki ulkoisen yhteyden sisäverkkoon päästämisestä on sellainen, jossa ulkoisten tietokoneiden tulee päästä sisäverkkoon kaupan-

käynti – palvelimelle. Toki myös joitain yhteyksiä sisäverkosta ulkoverkkoon on estettävä. Tämmöinen voi olla esimerkiksi yhteys tunnetulle kalastelu – sivustolle.

Sääntölistoilla siis muokataan palomuurin oletusyhteysasetuksia sekä sisään – että ulospäin kulkevan liikenteen osalta ja ne koostuvat useista eri säännöistä, pääsääntöisesti näin:

- Oletussääntö sisältä ulospäin tehtävien yhteydenavausyritysten suhteen on, että kaikki on sallittu, joten sääntölistalle kirjataan ne sisäiset yhteydet ja tilanteet joissa yhteyden avaaminen estetään.
- Oletussääntö ulkoa sisäänpäin tehtävien yhteydenavausyritysten suhteen on, että kaikki on kielletty, joten sääntölistalle kirjataan ne ulkoiset yhteydet ja tilanteet joissa yhteyden avaaminen sallitaan.

Tyypillisesti sääntölistat käsittävät TCP ja UDP – porttien numerot. On olemassa tunnetut porttinumerot joiden tiedetään kuuluvan tietyille ohjelmille. Esimerkiksi on yleisesti tiedossa, että HTTP portin numero on 80. Tilallinen palomuuri estää oletuksena TCP ja UDP – yhteydet näiden yleisesti tiedossa olevien porttien kautta.

Taulukko 1: Esimerkki sisäänpäin tulevan liikenteen sääntölistasta (Panko 2008, 264)

Access Control List for Ingress	
1.	If TCP destination port = 80 or TCP destination port = 443, then Allow Connection *[Pass all HTTP traffic to any webserver]*
2.	If TCP destination port = 25 AND IP destination address = 60.47.3.35, then Allow Connection *[Pass all SMTP traffic to a specific host (mail server)]*
3,	If IP protocol = 51, AND IP destination address = 60.47.3.77, then Allow Connection *[Pass all encrypted ESP traffic to the firm's IPsec gateway]*
4.	Deny ALL *[Deny all other externally initiated connections; this is the default behavior]*

Sääntölistaa tukee niin sanottu ”jos-niin” formaatti. Tämä tarkoittaa sitä, että jos tietty paketti täyttää tietyt arvot eli se sopii luotuun sääntöön, niin tilallinen palomuuri toimii tietyllä tavalla tämän paketin kohdalla. Esimerkiksi niin, että se päästää paketin avaamaan yhteyden jos paketti on TCP paketti ja on yrittämässä avata yhteyttä tunnettuun HTTP porttiin 80, kuten taulukon 1 ensimmäinen sääntö määrää. Taulukon 1 toisessa säännössä taas hyväksytään TCP paketit, jotka tulevat porttiin 25 (portti 25 on tunnettu porttinumero sähköpostipalvelimelle) ja tiettyyn tämän palomuurin takana olevaan sähköpostipalvelimen osoitteeseen. Sääntölistalla voi olla vaikka kuinka paljon sääntöjä mutta mitä enemmän niitä on, sitä monimutkaisempi ja

haastavampi sitä on ymmärtää. Kuten useaan otteeseen on mainittu, oletussääntö on, että kaikki ulkoapäin tulevat yhteysavauspyynnöt on kielletty. Tämä ilmenee taulukon 1 viimeiseltä riviltä eli kohdasta neljä. Eli sääntölistalla listataan ensin poikkeukset ja lopulta viimeisellä rivillä kerrotaan oletustoimintatapa. (Panko 2008, 262–265.)

4.6 Palomuurin hallinta

Palomuuri ei toimi automaattisesti kuten halutaan vaan sen toimintaan saattaminen vaatii huolellista suunnittelua, toteuttamista sekä päivittäistä hallinnointia. Varsinkin hallinnointi on tärkeä osa varmistettaessa, että palomuuri tarjoaa halutun suojan luvatonta läpikulkua sen läpi. Hyvän suunnittelun tuloksena muodostuu palomuuripolitiikka mikä kertoo karkealla ja korkealla tasolla, miten palomuuri konfiguroidaan. Palomuuripolitiikka saattaa kertoa esimerkiksi, että mikä tahansa HTTP yhteys joka tulee Internetistä, voidaan muodostaa ainoastaan eteisverkon palvelimiin. Politiikan avulla sitten rakennetaan varsinaiset säännöt, eli pääsynvalvontalistat. Se kertoo palomuurille miten toimia eri tilanteissa. Sääntölistoja saattaa olla ihmisen vaikea ymmärtää. Tämän takia on tärkeää tehdä myös politiikka, joka kertoo karkeammalla ja ihmisläheisemmällä tasolla saman asian.

Suunnittelun ja toteuttamisen valmistuttua on myös hyvä testata palomuurin toiminta käytännössä. Tämän voi tehdä esimerkiksi porttiskannerilla jolla voi helposti tutkia, mitkä portit ovat auki ja mitkä eivät. Toinen vaihtoehto on yrittää päästä ulospäin sivulle joille pääsy on palomuurin pääsynvalvontalistan mukaan estetty. (Panko 2008, 284-288.)

4.7 Palomuurin lokien ymmärtäminen

Palomuurin lokien seuraaminen on erittäin aikaa vievää ja samalla tärkeää, jotta oppisi ymmärtämään vallitsevia uhkia. Hyvä tapa on käydä lokit läpi vähintään päivittäin ja tilanteesta riippuen jopa useamminkin. Lokitiedosto on useimmiten jaettu sarakkeisiin, kuten taulukosta 2 selviää.

Taulukko 2: Esimerkki palomuurin lokitiedostosta

Järjestysnumero	Aikaleima	Sääntö	Lähde IP	Kohde IP	Palvelu
1	12:03:004	Pääsyn esto web - palvelimelle	128.171.17.3	60.17.14.8	HTTP
2	12:03:010	Pääsy ulkoverkosta sisäver-	14.8.23.96	60.8.123.56	FTP

		kon FTP - palvelimelle			
3	12:04:122	Kielletty tiedus-telupaketti	1.124.82.6	60.14.42.68	ICMP
4	12:04:132	Kielletty tiedus-telupaketti	1.124.82.6	60.14.42.69	ICMP

Taulukon 2 esimerkki palomuurin lokitiedostosta kertoo jokaisesta paketista kuusi eri informaatiota:

- ensimmäinen sarake kertoo tapahtuman järjestysnumeron, jonka avulla on helppo seurata tapahtumia kronologisessa järjestyksessä.
- toinen sarake kertoo tapahtuman tarkan ajan.
- kolmas sarake kertoo säännön, joka aiheutti paketin hylkäämisen. Kaikki lokit eivät kerro säännön nimeä.
- neljäs ja viides sarake kertovat mistä IP - osoitteesta paketti tuli ja mihin IP - osoitteeseen se oli menossa.
- kuudes sarake kertoo mitä palvelua paketti tavoitteli.

Lokeista on erityisesti syytä poimia epänormaalit merkinnät. Sen, mikä on epänormaalia, oppii näkemään kun seuraa lokeja säännöllisesti. Esimerkiksi jos yhdestä tietystä IP- osoitteesta tulee useita hylättyjä paketteja, on syytä tutkia asiaa tarkemmin. Yhtenä vaihtoehtona on luoda sääntö, jonka avulla kaikki paketit kyseisestä IP- osoitteesta hylätään mutta jos tapaus vaikuttaa hyökkäykseltä, voidaan kyseistä IP – osoitteesta tuleville paketeille määritellä tarkempi lokikirjoitus. Näitä lokeja tutkimalla on mahdollista selvittää ovatko paketit hyökkäyspaketteja vai eivät.

Yksi hyvä tapa on kerätä tilastot joka päivältä, jolloin esimerkiksi näkee montako epäonnistunutta DNS – kyselyä keskimäärin tapahtuu päivässä. Sitten jos jonain päivänä vastaavia kyselyjä on moninkertainen määrä verrattuna tilastojen mukaiseen keskiarvoon, on niitä syytä tutkia normaalia tarkemmin.

Normaalisti palomuuri kirjoittaa lokia vain paketeista jotka hylätään. Monissa palomuureissa on kuitenkin mahdollisuus konfiguroida palomuuri keräämään enemmän lokitietoja, esimerkiksi myös läpipäässeistä paketeista. Tämä luonnollisesti tekee palomuurin lokien tutkimisen paljon haasteellisemmaksi, sillä rivejä on selvästi enemmän, mutta erityisesti tarkempi lokin keräys vaikuttaa lokitiedoston kokoon ja sitä kautta levytilan määrään, jota kyseinen tiedosto varaa. On siis syytä miettiä kuinka tarkkaa lokitietoa on tarpeen kerätä mutta samalla on tar-

peen huomioida, että kannettavan tietokoneen kannalta läpipäässeet paketit ovat paljon merkityksellisempiä ja sitä kautta pahimmillaan myös vaarallisempia, kuin hylätyt paketit. (Panko 2008, 289–293.)

4.8 Sovelluskontrolli

Sääntölistan lisäksi työasemassa oleva palomuuri voi tehdä suodatuspäätökset myös verkkoa käyttävän sovelluksen perusteella. Näissä tapauksissa suodatuspäätöksen tekee palomuurin rinnalle rakennettu sovelluskontrolli –ohjelma. Se on ohjelma, joka valvoo jokaisen ei-tunnetun ohjelman suorittamista kannettavassa tietokoneessa. Se analysoi tiedostojen sisältöä ja ohjelmien toimintaa sekä estää uudet ja vielä määrittämättömät virukset ja muut haitalliset ohjelmat, jotka yrittävät tehdä haitallisia muutoksia tietokoneeseen. Aina kun ohjelma jota sovelluskontrolli ei tunne aiotaan suorittaa, se kysyy käyttäjältä luvan ja jos lupaa ei anneta, se estää ohjelman suorittamisen. Perusidea on kuitenkin se, että kaikki tunnetut ohjelmat saavat automaattisesti luvan suorittamiseen jolloin kannettavan tietokoneen käyttäjälle tulee mahdollisimman vähän kysymyksiä konfigurointiin liittyen. Edellä mainittujen lisäksi sovelluskontrolli valvoo käyttöjärjestelmään kuuluvia sekä kannettavalle tietokoneelle erikseen asennettuja sovelluksia ja niiden yhteyksiä ulospäin.
(Comodo – Comodo Internet Security Help)

5 Tutkimusaineisto ja – menetelmä

Tutkimuksessa vertaillaan kolmea eri tilallista palomuuria, jotka ovat sopivia kannettavan tietokoneen palomuuriksi. Näiden valittujen palomuurien ominaisuuksia tutkitaan ja vertaillaan ja tämän lisäksi perehdytään tarkasti niiden lokinkeräys vaihtoehtoihin. Ominaisuudet esitellään niin, että ne listataan kaikkien kolmen palomuurin osalta tuloksissa, josta ne on helppo lukea ja tehdä valinta oman käyttötarpeen mukaan. Lokinkeräyksestä tehdään syvällisempi tutkimus, jossa verrataan muun muassa oletusasetuksia sekä lokitiedoston konfigurointi mahdollisuuksia.

Tutkimus on rajattu niin, että käyttöjärjestelmään - joka on Windows 7 - ei keskitytä lainkaan, vaan ainoastaan tutkitaan näitä kolmea eri tilallista palomuuria. Myöskään käyttöjärjestelmän mukaan kuuluvia ohjelmia (esimerkiksi Internet Explorer ja Windows Live Mail) ei esitellä, vaikka niitä tutkimuksen tukena käytetäänkin. Tutkimus toteutetaan kannettavan tietokoneen avulla. Tämä kannettava tietokone on IBM Lenovo T60, jossa on Intel Core Duo 1.83 GHz prosessori, 1.5 GB RAM muistia sekä siis Windows 7 Enterprise 32-bit SP1 käyttöjärjestelmän kokeiluversio. Testikannettavaan siis asennetaan yksi palomuuri kerrallaan tutkimuksen toteut-

tamista varten. Toisin sanoen käyttöjärjestelmä on pelkkä alusta yhdelle palomuurille kerrallaan, eli väline tutkimukselle.

Tutkimuksessa käytetään myös Nmap Security Scanner porttiskanneria sekä toista kannettavaa tietokonetta, johon se on asennettu. Porttiskannerilla simuloidaan hakkeriliikennettä testikannettavaan ja tehdään sillä tapaa havaintoja siitä, miten tutkittavat palomuurit näyttävät lokeissaan kyseisen sisäänpäin tulevan porttiskannauksen.

5.1 Tutkittavien palomuurien esittely

Tutkittaviksi palomuureiksi on valittu:

- Windows 7 Enterprise -käyttöjärjestelmän mukana tuleva palomuuri
- F-Secure Internet Security 2012
- Comodo Firewall

Tutkimukseen valittiin kolme erilaista palomuuria, jotka kuitenkin kaikki pystyvät tarjoamaan tarvittavan suojan kannettavaan tietokoneeseen. Valinta kohdistui yhteen käyttöjärjestelmän lisenssin mukana tulevaan, yhteen kaupalliseen eli maksulliseen ja yhteen ilmaiseen palomuuriin.

5.1.1 Windows 7 Enterprise palomuuri

Tutkimuksessa asennetaan Windows 7 Enterprise – käyttöjärjestelmä ja tarkastellaan sen mukana tulevaa palomuuria. Itse Windows 7 – asennus on siis rajattu pois tutkimuksesta, jossa keskitytään vain palomuuriin ja sen ominaisuuksiin sekä lokeihin. Windows 7 Enterprise – käyttöjärjestelmästä asennetaan 30 päivän kokeiluversio, jotta tutkimus voidaan suorittaa.

Windows XP Service Pack 2:sta alkaen Windows – käyttöjärjestelmän mukana tulee palomuuri jota siis kutsutaan Windowsin omaksi palomuuriksi. Aiemmissa Windows -versioissa ei käytännössä ole ollut omaa palomuuria ollenkaan tai itse asiassa Windows XP – versiossa on, mutta se on hyvin rajoittunut. Tämä XP Service Pack 2:n mukana tullut on siis käytännössä ensimmäinen, jota voidaan palomuuriksi kutsua. Myös tämä palomuuri on niin sanottu tilallinen pakettisuodatin, jossa on oletuksena kaikki sisäänpäin tulevat paketit kielletty. Tässä käyttöjärjestelmäpäivityksen mukana tulevassa palomuurissa käyttäjä voi itse tehdä lisäyksiä sääntölistalle graafisen käyttöliittymän avulla.

5.1.2 F-Secure Internet Security 2012 palomuuri

Kaupallisista palomuureista on valittu F-Securen palomuuri osittain sen takia, että se on suomalainen tuote ja osittain sen takia, että F-Secure on erittäin käytetty palomuuri myös kannettavissa tietokoneissa sekä opetuskäytössä. F-Secure Internet Securityn ensimmäinen versio julkaistiin vuonna 2006 ja siitä eteenpäin sen kehitys sekä suosion kasvaminen on ollut nopeaa. Vuonna 2011 F-Secure Internet Security 2011 valittiin AV Comparativesin vuoden tuotteeksi. AV Comparatives on riippumaton valikoituja virustorjuntaohjelmia vertaileva sivusto, joten valintaa voidaan pitää merkittävänä ja arvostettavana saavutuksena.

F-Secure Internet Security 2012 – palomuurista asennetaan 30 päivän kokeiluversio, joka pitää sisällään kaikki samat ominaisuudet kuin täysiversiossakin on.

5.1.3 Comodo Firewall

Comodo on yhdysvaltalainen yritys joka on perustettu vuonna 1998. Toimipaikkoja on myös Euroopassa ja Aasiassa. Yrityksen missio on ”luottamuksen luominen”. Ensimmäinen versio Comodo Firewall – palomuurista on julkaistu vuonna 2005. Comodo tarjoaa myös maksullisia tuotteita aivan kuten F-Secure, esimerkiksi Comodo Internet Security, jossa on palomuurin lisäksi mm. virustorjunta sekä paljon muita tietoturvaa parantavia lisäohjelmia.

Comodo Firewall on tutkittavista palomuureista ainoa, joka on täysin ilmainen. Tämän takia on mielenkiintoista nähdä poikkeaako se ominaisuuksiltaan merkittävästi verrattuna kahteen maksulliseen palomuuriin. Myös se onko tämän palomuurin lokinkirjoitus ominaisuudet ja niiden konfigurointi mahdollisuudet selvästi rajoittuneempia kuin muissa tutkittavissa palomuureissa, on erittäin mielenkiintoista nähdä.

5.2 Tutkimuskriteerit

Seuraavassa avataan tutkimuskysymykset, joita on tässä tutkimuksessa kaksi. Molempien kohdalla kerrotaan miten varsinainen tutkimus tehdään ja mitä asioita selvitetään. Myös tutkimuksen kannalta oleelliset asiat esitellään.

5.2.1 Miten tutkimukseen valitut palomuurit eroavat tietoturvaa parantavilta lisäominaisuuksiltaan sekä palomuurisääntöjen oletusasetuksiltaan?

Ensimmäinen vertailtava asia näitä kolmea palomuuria tutkittaessa on niiden muut tietoturvaominaisuudet. Usein palomuurin mukana – varsinkin kun kyse on kaupallisista palomuureista – on mahdollista hankkia myös muita tietoturvan kannalta oleellisia ohjelmia kuten esimerkiksi:

- haittaohjelmien suodatus
- roskapostin suodatus
- lapsilukko
- virustorjunta
- tiedostojen salaus

Toki näitä lisäominaisuuksia on myös ilmaisten palomuurien mukana ja siksi on hyvä selvittää, miten nämä tutkittavaksi valitut palomuurit eroavat toisistaan tässä suhteessa.

Ominaisuuksien vertailu toteutetaan tässä tutkimuksessa niin, että ensin tutustutaan jo valittujen kolmen palomuurin dokumentaatioon, josta oletettavasti selviää myös nämä mahdolliset tietoturvaa parantavat lisäominaisuudet. Tämän jälkeen kukin palomuuri vuorollaan asennetaan tutkimuksessa apuna käytettävään kannettavaan tietokoneeseen ja tehdään havaintoja muun muassa seuraavista asioista:

- onko ylipäänsä mitään lisäominaisuuksia saatavilla?
- pitääkö dokumentaatio paikkansa lisäominaisuuksien suhteen?
- voiko asennuksessa valita ottaako näitä lisäominaisuuksia käyttöön vai ei?
- voiko vain osan lisäominaisuuksista ottaa käyttöön / jättää pois käytöstä?

Oleellista näitä lisäominaisuuksia tutkittaessa on tietysti se onko niitä ylipäänsä edes olemassa, mutta vielä oleellisempaa on se minkä verran niiden käyttöä voi kannettavan tietokoneen käyttäjä itse hallita.

Ominaisuuksien vertailun lisäksi tässä tutkimuskysymyksessä siis selvitetään myös näiden kolmen vertailtavan palomuurin oletusasetukset palomuurisäännöille. Näistä palomuurisääntöjen oletuksista selvitetään seuraavat asiat:

- mitkä yhteydet on oletuksena sallittu sisäänpäin (vai onko mitään)?
- onko kaikki liikenne ulospäin oletuksena sallittu, kuten tilallisissa palomuureissa usein on?
- onko sovelluskontrolli oletuksena päällä ja voiko sen kytkeä pois päältä?
- oppiiko palomuurin sovelluskontrolli sallitut yhteydet käyttäjän sovelluskäytön mukana?

Nämä oletussäännöt selviävät palomuureista asennuksen jälkeen, kun tarkistetaan mitä kunkin palomuurin säännöstössä kerrotaan. Sovelluskontrolli sen sijaan testataan niin, että ensin tarkistetaan onko se päällä ja jos on, niin voiko sen laittaa pois päältä? Lisäksi lähetetään tietokoneen sähköpostiohjelmasta sähköpostia ja testataan näin miten sovelluskontrolli siihen reagoi ja jos se pyytää lupaa yhteyden avaamiseen, annetaan se. Tämän jälkeen suljetaan sähköposti ja tehdään sama uudestaan sekä kiinnitetään huomiota siihen, muistaako palomuuri ensimmäisellä sähköpostin lähettämiskerralla hyväksytyn yhteyden.

5.2.2 Miten palomuurien lokitiedostot eroavat ominaisuuksiltaan ja kuinka konfiguroitavissa ne ovat?

Toinen erittäin mielenkiintoinen ja merkityksellinen asia näitä kolmea palomuuria tutkittaessa on niiden lokitiedostot. Kuten aiemmin mainittua lokitiedostojen säännöllinen seuraaminen on hyvin tärkeää tietoturvan kannalta. Ja kun lokia seuraa oppii näkemään ja ymmärtämään jos meneillään on jotain normaalista poikkeavaa. Tämä on suurin yksittäinen syy, miksi lokien tutkiminen on valittu yhdeksi osaksi tätä tutkimusta.

Tutkimuksessa siis ensin selvitetään millaista lokinkirjoitusta kukin palomuuri tekee oletusasetuksin. Tämän lisäksi tarkistetaan onko lokinkirjoitus konfiguroitavissa esimerkiksi tarkemmaksi kuin oletusasetus. Myös se selviää kirjoittaako palomuuri lokia vain hylätyistä paketeista vai myös hyväksytyistä sekä se, että onko tämä asetus palomuurin järjestelmävalvojan konfiguroitavissa.

Lokitiedoston konfiguroitavuus selviää joko palomuurien dokumentaatiosta tai todennäköisimmin kokeilemalla. Jokaiselle tutkittavalle palomuurille tehdään testejä, joilla selvitetään lokinkirjoituksen oletusasetusten erot.

Oleellista lokinkirjoitusta tutkittaessa on se kuinka monipuolista lokia palomuurista saadaan talteen joko oletuksena tai viimeistään lokinkirjoitusasetuksia konfiguroimalla. Mielenkiintoista on myös nähdä eroaako kaupallisen tuotteen ja ei kaupallisen tuotteen konfiguroitavuus merkittävästi. Testien perusteella pyritään myös saamaan käsitys siitä millaista lokia palomuurit kirjoittavat testeissä tapahtuvan niin sanotun ”normaaliliikenteen” ollessa kyseessä. Tämä normaali liikenne tarkoittaa siis juuri sellaista liikennettä mitä liikkuva kannettavan tietokoneen käyttäjä muodostaa kannettavasta sisään ja ulospäin eli päivitysten hakemista, Internetin nettipankissa käymistä ja sähköpostin lähetystä ja vastaanottoa. Lisäksi saadaan käsitys siitä millaista lokia testattavat palomuurit kirjoittavat, kun simuloidaan hakkeriliikennettä Nmap – porttiskannerin avulla.

6 Tutkimuksen toteutus

Seuraavassa esitellään miten tutkimus toteutettiin, testit tehtiin sekä tulokset kerättiin.

6.1 Tutkittavien palomuurien ominaisuudet ja oletusasetukset

Ensin siis tutustuin tutkimukseen valittujen palomuurien dokumentaatioon pyrkimyksenä selvittää vastauksia tutkimuskysymykseen. Lähdin tekemään tätä dokumentaatioihin tutustumista kyseisten tuotteiden Internet-sivuilta ja lisäksi käytin apuna hakukoneita.

Dokumentaatiota jossa kerrottaisiin Windows 7 palomuurin lisäominaisuuksista, oli vaikea löytää Microsoftin sivuilta. Toinen ongelma oli, että hakuni tuottivat useita tuloksia ja oli vaikeaa löytää tätä tietoa mitä Windows 7 palomuurista halusin. F-Securen kohdalla sen sijaan tietoa tuotteesta löytyi heidän Internet sivultaan helposti ja nopeasti ja sain nopeasti selville mitä lisäominaisuuksia heidän tuotteeseen kuuluu. Comodon kohdalla taas tiedon ja dokumentoinnin löytäminen vaikeutui sillä heidän Internet sivuillaan oli helposti löydettävissä dokumentaatiota ja lisätietoa vain heidän kaupallisesta tuotteestaan – ei tästä ilmaisversiosta, joka tähän testiin oli valittu.

Dokumentaation etsimisen ja siihen tutustumisen jälkeen tein siis asennukset testikannettavaan. Ensimmäistä tutkittavaa palomuuria ei tarvinnut asentaa, koska se on siis osa Windows 7 käyttöjärjestelmää eli Windowsin oma palomuuri. Varmistin vain, että se on päällä ennen kuin testini tein. F-Secure Internet Security 2012 palomuurin asensin oletusasetuksin. Samoin toimin Comodo Firewall –palomuurin kohdalla. Toki aina poistin edellisen palomuurin asennuksen testikannettavasta ennen uuden asennusta ja Windowsin oman palomuurin ollessa kyseessä

riitti siis pelkkä palomuurin pois päältä laittaminen. Asennuksia tehdessä kiinnitin huomiota oletusasetuksiin, kirjasin kaikki havaintoni talteen sekä otin kuvaruutukopioita eri vaiheista tutkimustuloksien esittelyä varten.

Jokaisen palomuurin kohdalla, kun asennus (tai Windows 7 palomuurin kohdalla käyttöönotto) oli tehty, avasin ohjelman ja katsoin onko olemassa sovelluskontrolli ominaisuutta ja jos oli, oliko se oletuksena päällä vai ei. Jos sovelluskontrolli kuului testattuun palomuuriin, lähetin testikannettavan Windows Live Mail 2011 -sähköpostiohjelmalla sähköpostin. Tästä tapahtumasta tein havaintoja eli miten sovelluskontrolli tähän reagoi ja mahdollisen reagoinnin jälkeen suljin sähköpostiohjelman, sekä käynnistin testikannettavan kokonaan uudestaan. Nämä toimet tein, jotta selviäisi oliko palomuurin sovelluskontrolliin jäänyt talteen sallittu yhteys sähköpostipalvelimeen. Sovelluskontrollin lisäksi tarkistin onko palomuureissa valmiina joitain yhteyksiä sallittuna ulos- tai sisäänpäin. Tämän tarkistuksen tein tutkimalla palomuurien pääsylistoja asennuksen jälkeen.

6.2 Palomuurien lokitiedostojen eroavaisuus ja konfiguroitavuus

Koska ensimmäisessä tutkimuskysymyksessä perehdytään tutkittavien palomuurien dokumentaatioon ja tehdään niistä havaintoja, päätin että on mielekkäämpää etsiä tähän toiseen tutkimuskysymykseen vastauksia eri tavalla, eli kokeilemalla. Tätä päätöstä tuki oletus siitä, että dokumentaatio ei ole niin tarkalla tasolla että siitä selviäisi millaiset ovat lokinkeruun oletusasetukset ja kuinka tarkasti niitä voi säätää. Katsoin siis ensin kaikista tutkittavista palomuureista tarkemmin sanoen niiden hallintakonsolista tms., millaiset ovat lokinkirjoituksen oletusasetukset. Tämän jälkeen tein kaikille tutkittaville palomuureille kolme testiä, jotka on kuvattu seuraavaksi:

1. Tarkistin manuaalisesti Windowsin ohjauspaneelin kautta onko Microsoft Update – palvelussa tarjolla uusia päivityksiä kannettavaan tietokoneeseeni ja katsoin miten tuo päivitysten tarkistus näkyy palomuurin lokissa? Tämän jälkeen tein havaintoja näkyikö tämä manuaalinen saatavilla olevien päivitysten tarkistus palomuurin lokissa jotenkin ja jos näkyi, niin miten?

2. Kävin kannettavan tietokoneen oletusselaimella verkkopankissa, jolloin osa liikenteestä tapahtui HTTPS – protokollalla. Tämän jälkeen tutkin toimenpiteestä muodostunutta lokia ja havainnoin lokin muodostumista kiinnittäen erityishuomion siihen, että oliko varmenteen tarkistamisesta muodostunut merkintä lokiin?

3. Kolmantena testinä simuloin sisäänpäin tulevaa hakkeriliikennettä Nmap Security Scanner -porttiskannerin avulla, jolla skannasin testikannettavan portteja ja tutkin miten kyseinen skannaus näkyi palomuurien lokeissa. Samalla tein lokeista havaintoja esimerkiksi että onko eri palomuurien välillä eroja siinä, miten portit olivat oletuksena auki tai kiinni.

Luonnollisesti jos tutkittavan palomuurin lokiasetukset olivat oletuksena niin, että lokia ei kirjoiteta, vaihdoin tämän asetuksen ennen yllä kuvailtuja testejä niin, että lokia syntyy.

Testien aikana tapahtui oleellinen muutos F-Secure Internet Security 2012 palomuurin saatavuuteen, joka aiheutti sen että jouduin tekemään osan testeistä eri versiota vasten. Tapahtui siis niin, että kun minulla oli vielä F-Secure Internet Security 2012 version testit tekemättä tutkimuskysymys 2:n osalta F-Secure päivitti versionsa 2013 versioon, eikä 2012 versio ollut enää ollenkaan saatavilla. Olennaista tässä on se, että tuosta F-Secure Internet Security 2013 versiosta oli poistettu palomuuri kokonaan ja sillä ohjataan tähän versioon rakennetun käyttöliittymän kautta Windowsin omaa palomuuria. Koska halusin kuitenkin tehdä testini loppuun F-Securen tuotteella, olin yhteydessä heihin ja sain heiltä tietää, että F-Secure Client Security 2012 tuotteessa on teknisesti lähestulkoon sama palomuuri, kuin F-Secure Internet Security 2012 versiossa oli. Näin ollen käytin viimeisiin testeihini tuota Client Securityn palomuuria.

7 Tutkimustulokset

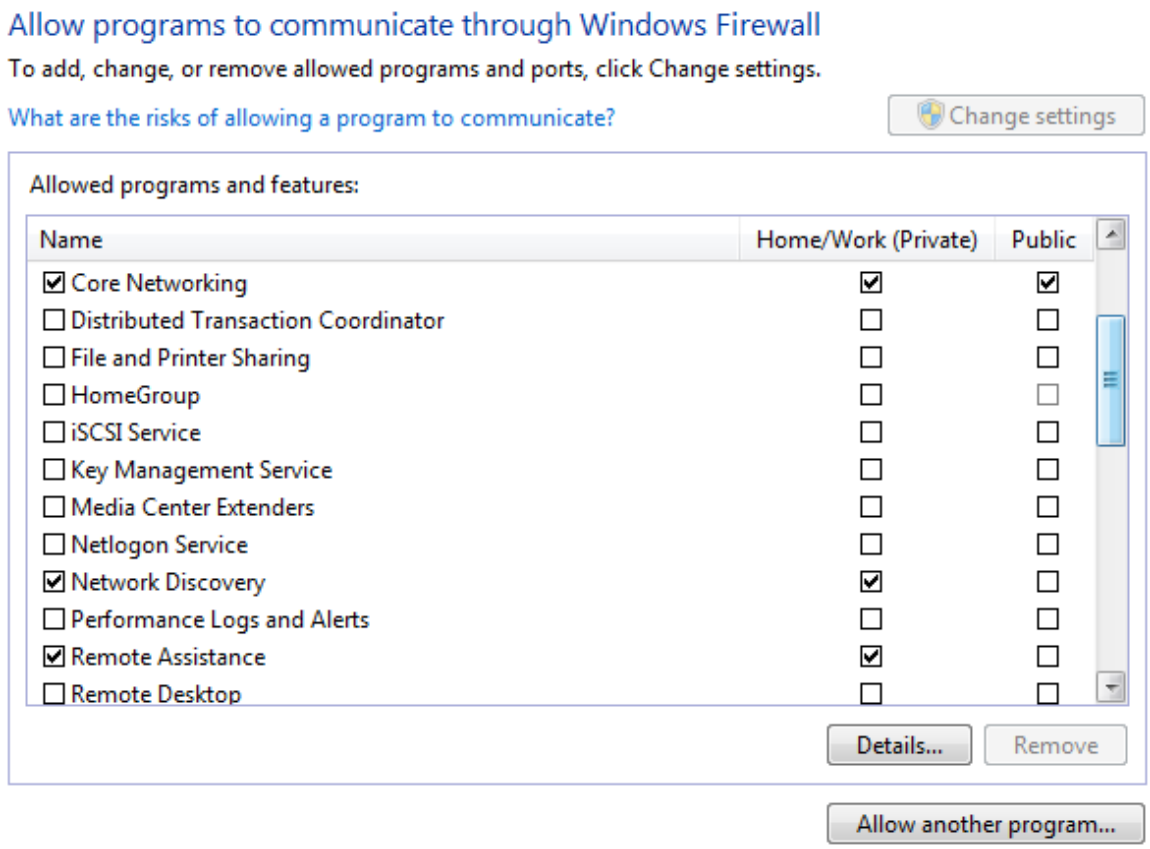
7.1 Tutkimuskysymys 1

7.1.1 Windows 7 Enterprise palomuuri

Tutustuttuani löytämääni Windows 7 palomuurin dokumentaatioon Microsoftin sivuilla olin siinä uskossa, että tämä palomuuri ei pidä sisällään mitään lisäominaisuuksia. Jatkoin siis testiä eteenpäin ja ”asensin” palomuurin. Asennuksesta ei sanan varsinaisessa merkityksessä voida puhua, koska Windows 7 palomuuria ei oikeasti tarvitse asentaa sillä se kuuluu Windows 7 käyttöjärjestelmään automaattisesti. Se tarvitsee vain aktivoida käyttöön eli laittaa päälle. Tämä kävi helposti Windowsin ohjauspaneelin kautta.

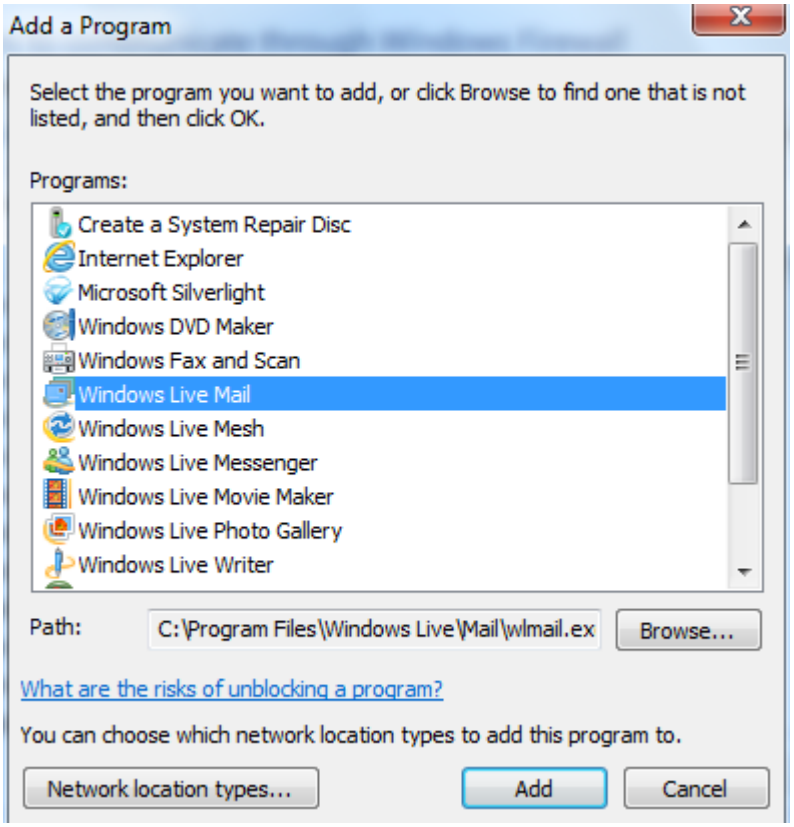
Laitettuani Windows 7 palomuurin päälle ja hetken palomuuria tutkittuani tein havainnon että tässä palomuurissa on sittenkin yksi lisäominaisuus nimittäin eräänlainen sovelluskontrolli, jota

ei saa erikseen pois päältä ja joka pitää sisällään myös tiettyjen Windowsin ominaisuuksien kontrolloinnin. Muita lisäohjelmia ei ole, jonka uskoisin johtuvan siitä että Microsoftilla on esimerkiksi virustorjuntaohjelma erikseen. Sovelluskontrolli oli oletusasetuksin päällä ja siinä oli valmiina liuta sovelluksia, joista osan oli jo valmiiksi sallittu ottaa vastaan yhteyksiä läpi palomuurin. ”Läpi palomuurin” tarkoittaa Windows 7 palomuurin kyseessä ollessa että yhteys sisäänpäin on sallittu, sillä tämä sovelluskontrolli kontrolloi vain sisäänpäin tulevia yhteyksiä. Se toimii siis niin että sovellukset, jotka ovat listalla sallittuna, saavat ottaa vastaan yhteyksiä ulkoa sisäänpäin. Kuten kuviosta 4 selviää, Windows 7 palomuurissa oli oletuksena sallittu yhteys palomuurin läpi tietyille lähinnä Windowsin toimivuuteen vaikuttaville sovelluksille tai ominaisuuksille. Muille tällä ”sallittujen ohjelmien ja ominaisuuksien” listalla valmiina oleville ohjelmille/ominaisuuksille voi halutessaan helposti antaa kyseisen oikeuden. Huomionarvoista on myös se, että Windows 7 palomuurissa on kolme erilaista verkkoprofiilia. Nämä ovat yksityiset koti- ja työverkot sekä julkinen verkko. Mm. sovelluskontrollin asetuksia, kuten kaikkia muitakin Windows 7 palomuurin asetuksia, voi muokata per profiili.



Kuvio 4: Windows 7 palomuurin sovelluskontrolli

Lisäksi jos sovellusta, jolle halutaan lisätä oikeudet läpäistä palomuuri, ei löydy valmiina listalta, on se helppo lisätä ”Allow another program…” – napista jolloin aukeaa kuviossa 5 näkyvä ikkuna.



Kuvio 5: Sovelluksen lisääminen

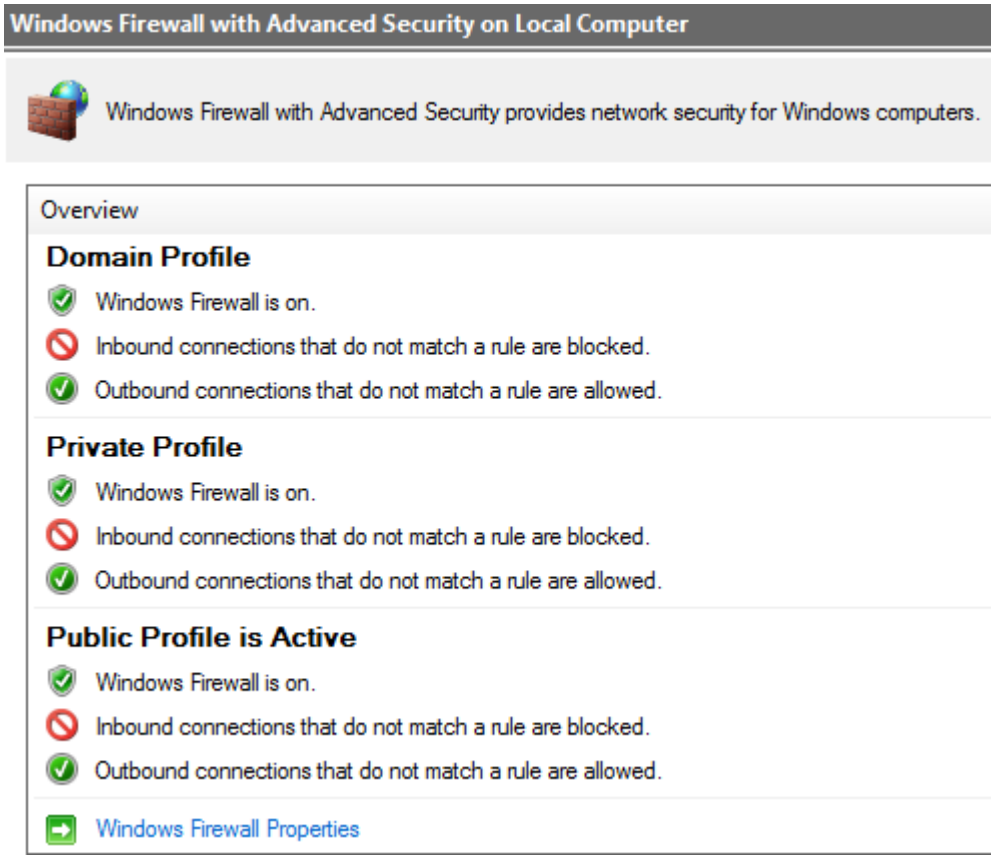
Kannettavassa tietokoneessa on harvoin tarvetta lisätä tätä kautta ohjelmia listalle joilta sallitaan ottaa yhteyksiä vastaan palomuurin läpi, koska useimmiten ohjelman asennusohjelma luo itse tarvittavat säännöt sovelluskontrolliin kunhan asentaja – eli käyttäjä – antaa asennusohjelmalle luvan tehdä näin.

Windows Live Mail – ohjelmaa ei ollut Windows 7 palomuurissa automaattisesti määritelty läpäisemään palomuuri. En kuitenkaan lisännyt sitä manuaalisesti, koska seuraava testini oli avata kyseinen ohjelma ja lähettää siitä sähköpostia sekä havainnoida miten Windows 7 palomuuri ja etenkin sen sovelluskontrolli tähän reagoi.

Sähköpostin avaaminen ja lähettäminen sujui ilman mitään ilmoituksia Windows 7 palomuurilta tai sovelluskontrollilta. Tämän jälkeen vielä käynnistin testikannettavan uudestaan ja kokeilin uudestaan. Sain edelleen saman lopputuloksen eli sähköpostin lähettäminen onnistui ja mitään ilmoituksia ei tullut. Ilmoituksia ei tullut sen takia, koska kaikki yhteydet ulospäin ovat Windows 7 palomuurissa oletusasetuksin sallittuja.

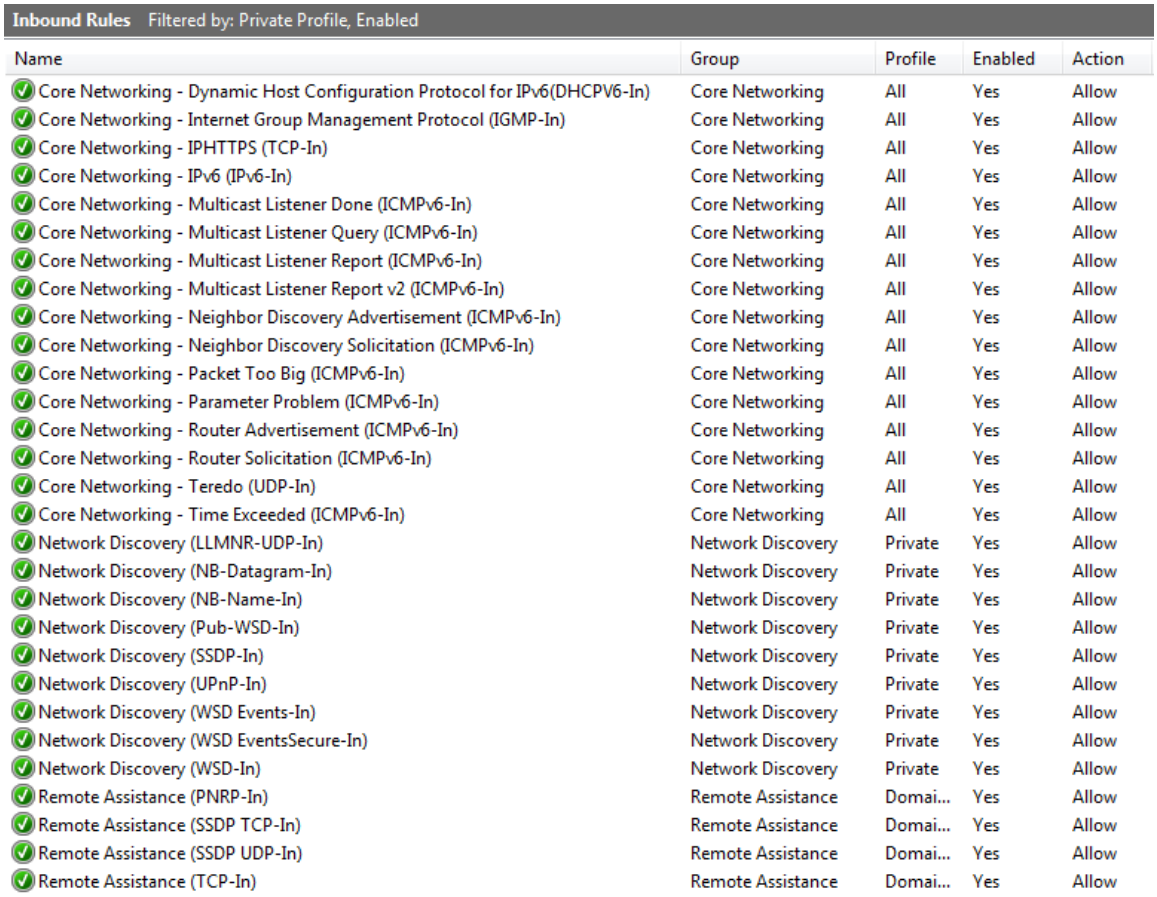
Sähköpostitestin jälkeen tarkastelin vielä Windows 7 palomuurin oletusasetuksia koskien yhteyksiä ulos- ja sisäänpäin. Kuten aiemmin on mainittu, tilallisen pakettisuodattimen oletussään-

nöt ovat, että kaikki liikenne ulospäin on sallittua ja kaikki liikenne sisäänpäin on kiellettyä ja niin on myös Windows 7 palomuurin oletusasetuksissa, kuten kuviosta 6 selviää.



Kuvio 6: Windows 7 palomuurin oletussäännöt

Kuviosta 6 selviää myös, että testatessani aktiivisena profiilina oli ”public” profiili eli Windows 7 palomuuri käytti yhteyteeni oletussääntöjä, jotka on tehty profiilille jossa kannettavaa tietokonetta käytetään yleisessä verkossa, esimerkiksi Internet-kahvilassa. Nämä mainitsemani sisäänpäin tulevan liikenteen oletussäännöt sisältävät tietysti poikkeuksia, joita siis kontrolloidaan sääntölistalla. Kuviossa 7 näkyy Windows 7 palomuurin ”public” profiilin sääntölistan oletusasetukset koskien sisäänpäin kulkevaa liikennettä. Tämä tarkoittaa, että kun kaikki sisäänpäin tuleva liikenne - paitsi sääntölistalla mainitut – on kielletty, niin kuviossa 7 näkyvät ovat nimenomaan sallittuja eli niitä sääntölistalla mainittuja. Kaikki liittyvät tavalla tai toisella Windowsin toimintaan.



Inbound Rules Filtered by: Private Profile, Enabled

Name	Group	Profile	Enabled	Action
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)	Core Networking	All	Yes	Allow
Core Networking - Internet Group Management Protocol (IGMP-In)	Core Networking	All	Yes	Allow
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Done (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Query (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Report (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Report v2 (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Parameter Problem (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Router Advertisement (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes	Allow
Network Discovery (LLMNR-UDP-In)	Network Discovery	Private	Yes	Allow
Network Discovery (NB-Datagram-In)	Network Discovery	Private	Yes	Allow
Network Discovery (NB-Name-In)	Network Discovery	Private	Yes	Allow
Network Discovery (Pub-WSD-In)	Network Discovery	Private	Yes	Allow
Network Discovery (SSDP-In)	Network Discovery	Private	Yes	Allow
Network Discovery (UPnP-In)	Network Discovery	Private	Yes	Allow
Network Discovery (WSD Events-In)	Network Discovery	Private	Yes	Allow
Network Discovery (WSD EventsSecure-In)	Network Discovery	Private	Yes	Allow
Network Discovery (WSD-In)	Network Discovery	Private	Yes	Allow
Remote Assistance (PNRP-In)	Remote Assistance	Domai...	Yes	Allow
Remote Assistance (SSDP TCP-In)	Remote Assistance	Domai...	Yes	Allow
Remote Assistance (SSDP UDP-In)	Remote Assistance	Domai...	Yes	Allow
Remote Assistance (TCP-In)	Remote Assistance	Domai...	Yes	Allow

Kuvio 7: Windows 7 palomuurin sääntölista

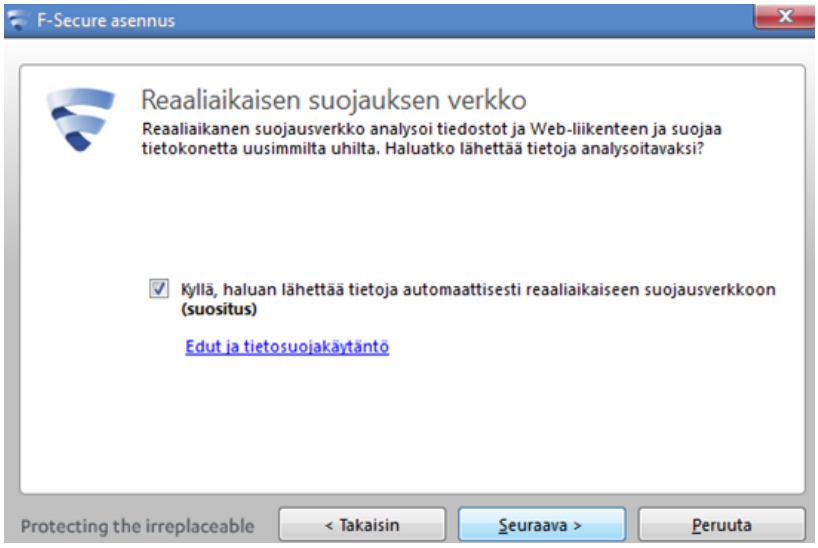
Jos manuaalisesti luo uuden säännön jolla sallii esimerkiksi liikenteen ulkoa sisäänpäin virustorjuntaohjelmaan, ilmestyy se automaattisesti myös ”Allowed programs and features” – listalle (katso kuvio 4).

7.1.2 F-Secure Internet Security 2012 palomuuri

F-Securen kotisivulta löytyi kattavasti tietoa heidän tuotteistaan, myös tästä palomuurin sisältävästä F-Secure Internet Security 2012 – kokonaisuudesta. Latasin 30 päivän ilmaisen kokeiluversion, joka sisältää siten kaikki samat ominaisuudet kuin maksullinenkin versio mutta ei toimi enää 30 päivän käytön jälkeen ellei lisenssiä osta. F-Secure Internet Security – paketin tärkeimmät ominaisuudet selviävät lataussivulta poimitusta kuviosta 8.

Kuvio 8: F-Secure Internet Security ominaisuudet (F-Secure Internet Security 2012 – Kokeile ilmaiseksi)

Kun asensin tuon kokeiluversion kiinnitin huomioni siihen, että ainoa yllämainituista ominaisuuksista minkä asennus oli valinnanvaraista, oli tuo selauksen suojaus, eli oikeammalta nimeltään reaaliaikaisen suojauksen verkko. Kuviosta 9 selviää myös, että F-Secure suosittelee kyseisen lisäominaisuuden asentamista, vaikka se tosiaan vapaaehtoista onkin:



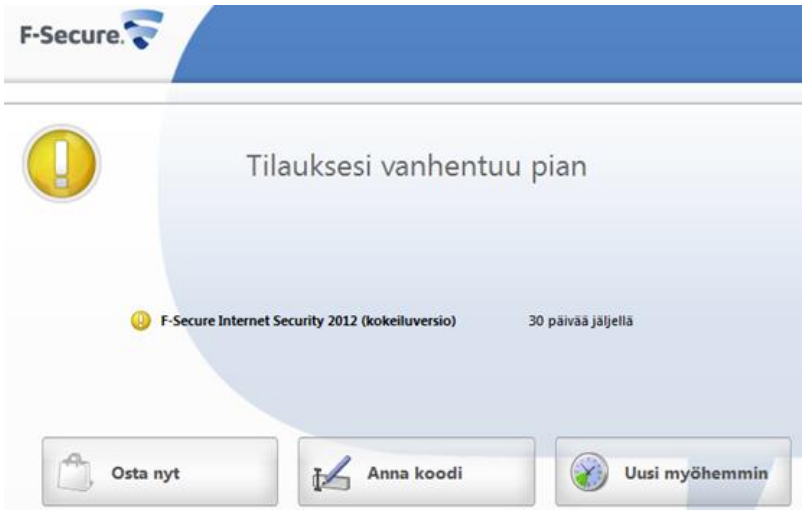
Kuvio 9: F-Securen reaaliaikainen suojausverkko 1

Tästä lisäominaisuudesta löytyi myös kattavasti lisätietoa jo ennen kuin asennusta tarvitsi edes jatkaa, kun painoin yllä kuviossa 9 olevaa ”Edut ja tietosuojakäytäntö” – linkkiä. Se avasi selaimeen kuviossa 10 näkyvän tietosivun.

Kuvio 10: F-Securen reaaliaikainen suojausverkko 2

Kyse on siis F-Securen omasta verkkopalvelusta, joka tunnistaa vaarattomat sovellukset ja Internet-sivustot sekä tarjoaa suojaa haittaohjelmia ja Internet-sivustojen heikkouksien hyödyntämistä vastaan. Tämä lisäominaisuus myös vähentää tarpeettomia hälytyksiä epäilyttävistä sovelluksista, jotka eivät oikeasti ole haitallisia.

Muista luvatuista ominaisuuksista ei näkynyt viitteitä asennuksen aikana mutta heti asennuksen valmistuttua näytölle tuli ilmoitus (katso kuvio 11), josta selvisi, että käytössä on kokeiluversio sekä se montako päivää kokeilua on jäljellä.



Kuvio 11: F-Securen kokeiluversion muistutus

Reaaliaikaisen suojausverkon ja palomuurin lisäksi F-Secure Internet Security 2012 tuote pitää siis sisällään myös liudan muita ominaisuuksia jotka kaikki ovat kytkettävissä myös pois käytöstä, vaikka näin ei asennuksen yhteydessä voikaan tehdä.

Virus- ja vakoiluohjelmien tarkistus tarkistaa myös sähköpostien virukset ja on oletusasetuksin päällä. Se on myös otettavissa pois päältä joko kokonaan tai sähköpostitarkistuksen osalta. Tämä lisäohjelma tarkistaa kaikki tiedostot kun niitä otetaan käyttöön ja estää sellaisten tiedostojen käytön, jotka sisältävät haittaohjelmia.

Tietomurtojen esto on yksi lisäominaisuuksista ja myös tämän saa halutessaan pois päältä. Se suojaa verkkohyökkäyksiltä, jotka on suunnattu tietokoneen avoimille porteille, käyttämällä ennalta määritettyjä sääntöjä niiden tunnistamiseen. Tämä lisäohjelma eroaa palomuurista siinä, että se estää vain sellaisen tietoliikenteen, jota se pitää haitallisena. Täten ei haitalliseksi tulkittu tietoliikenne pääsee portista läpi. Tämän lisäominaisuuden saa myös kirjoittamaan lokia tapahtumista mutta tämä lokinkirjoitus ei ole oletusasetuksin päällä.

Kuten yllämainitut, myös sähköpostisuodatus –lisäominaisuus on oletusasetuksin asennettuna päällä. Se suojaa sähköpostia tunnistamalla roskapostit ja siirtämällä ne roskakansioon.

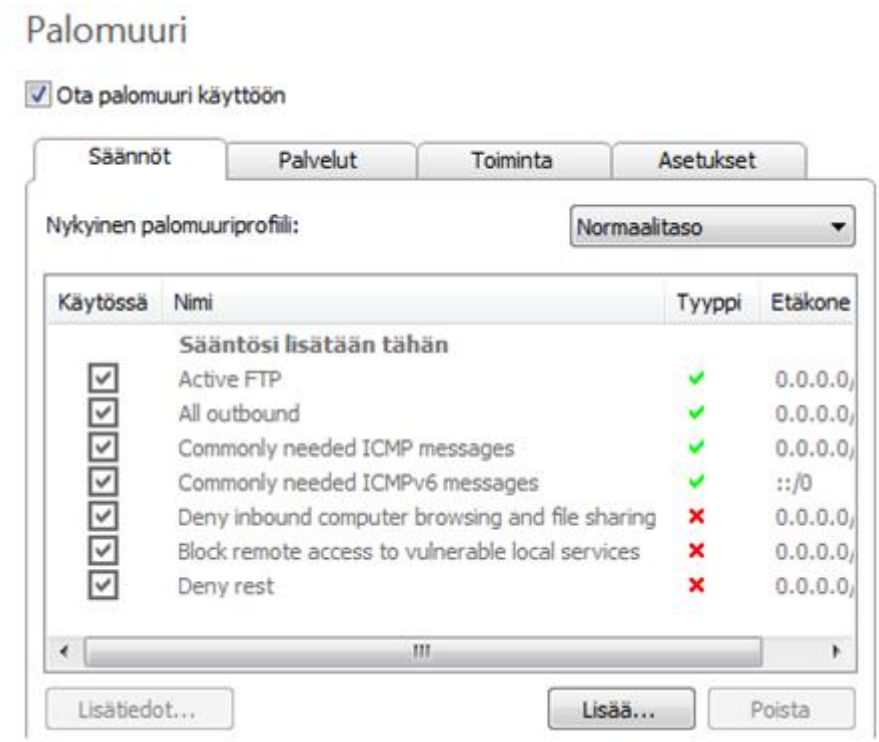
Ainoa lisäominaisuus, joka ei ollut oletuksena päällä, oli puhelinverkkoyhteyden hallinta. Sillä voidaan estää tai sallia puhelinverkkoyhteydet valittuihin numeroihin.

Lapsilukko –lisäohjelmalla, joka myös on oletusasetuksin päällä, voi estää tietyiltä koneen käyttäjiltä tai käyttäjäryhmiltä pääsyn valitsemilleen Internet-sivuille tai vaikka rajoittaa koko Internetin käytön esimerkiksi kellon tai sivuston aihealueen mukaan.

F-Securessa on myös oma sovelluskontrolli – lisäohjelma, jonka nimi on Deep Guard. Se on hyvin samanlainen kuin sovelluskontrollit pääasiassa ovat eli se valvoo tietokoneen sovelluksia ja niiden yhteyksiä. Deep Guard on oletuksena päällä ja sen voi ottaa pois käytöstä niin halutessaan ”Sovellusten hallinta” –ohjelman asetuksista.

Asennuksen jälkeen tarkastelin palomuurin oletusasetuksia. Ne löytyivät todella helposti sillä kaikkien F-Secure Internet Security 2012 ohjelmien asetukset löytyvät samasta paikasta. Palomuurin asetukset –ikkunasta oli selkeästi havaittavissa, että oletusasetuksin kaikki liikenne ulospäin on sallittua. Sisäänpäin kaikki liikenne paitsi yleiset ICMP – viestit, on kielletty. Alla

näkyvästä kuviosta 12 selviää nämä säännöt ja on hyvä huomata myös, että koko palomuurin saa helposti pois päältä ottamalla pois rastin kohdasta ”ota palomuuri käyttöön”.



Kuvio 12: F-Secure palomuurin oletussäännöt

Seuraavaksi testasin sovelluskontrollin eli lähetin testikannettavan sähköpostiohjelmasta, Windows Live Mail – ohjelmasta sähköpostin ja tein havaintoja miten Deep Guard siihen reagoi. Se ei reagoinut mitenkään näkyvästi. Tämä johtui siitä, että sovellusten hallinta – ohjelman oletusasetukset ovat sellaiset, että Deep Guard sallii automaattisesti tuntemiensa sovellusten yhteydet ulos- ja sisäänpäin, kuten kuviosta 13 selviää.

Kuvio 13: F-Secure sovellushallinnan oletusasetukset

Deep Guard siis tunnisti käyttämäni Windowsin oman sähköpostiohjelman ja antoi sen ottaa yhteyden kysymättä lupaa. Kun vaihdoin asetuksen kohtaan ”Kysy kaikista sovelluksista” (kat-

so kuvio 13) ja kokeilin uudestaan avata sähköpostiohjelmaa, niin sain Deep Guardin reagoimaan kuviossa 14 näkyvällä tavalla.

Kuvio 14: F-Secure sovelluskontrollin yhteyskysymys

Tuohon kun vastasin ”Luotan sovellukseen. Salli yhteys molempiin suuntiin”, sain lähetettyä sähköpostia ja kyseinen ohjelma lisättiin sallittujen sovellusten listalle. Koska Windows Live Mail oli heti asennuksen jälkeen sovelluskontrollissa sallittuna ohjelmana, olin varma että se on siellä myös testikannettavani uudelleen käynnistyksen jälkeen, ja näin tosiaan kävikin.

7.1.3 Comodo Firewall

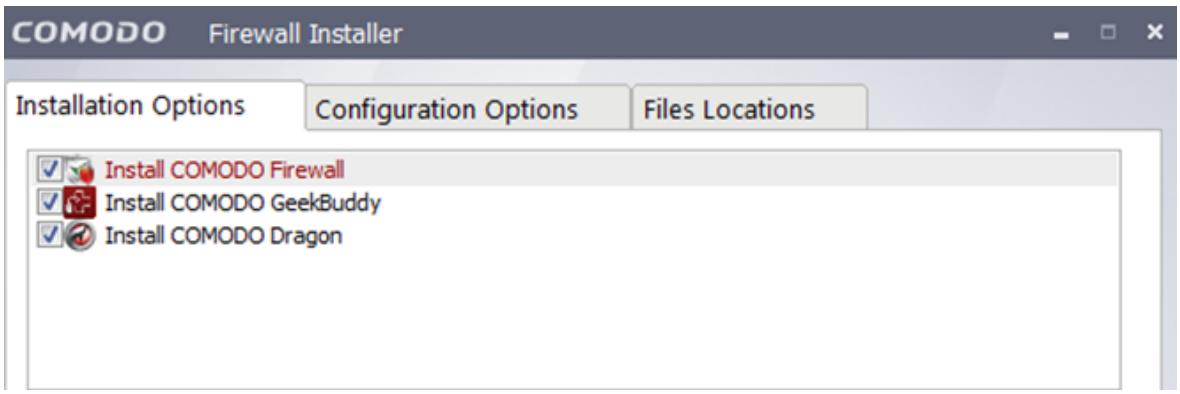
Comodo palomuurin kotisivulta löytyi melko kattavasti tietoa lisäominaisuuksista joita heidän kaupallinen Comodo Antivirus + Firewall – tuote sisältää, mutta tästä ilmaisversiosta ei juuri tietoa löytynyt. Löysin ainoastaan alla näkyvän kuvion 15 ja se kertoo vain palomuurin ominaisuuksista yleisellä tasolla.

Kuvio 15: Comodo Firewall ominaisuudet (Comodo Firewall – Palomuurin lataussivu)

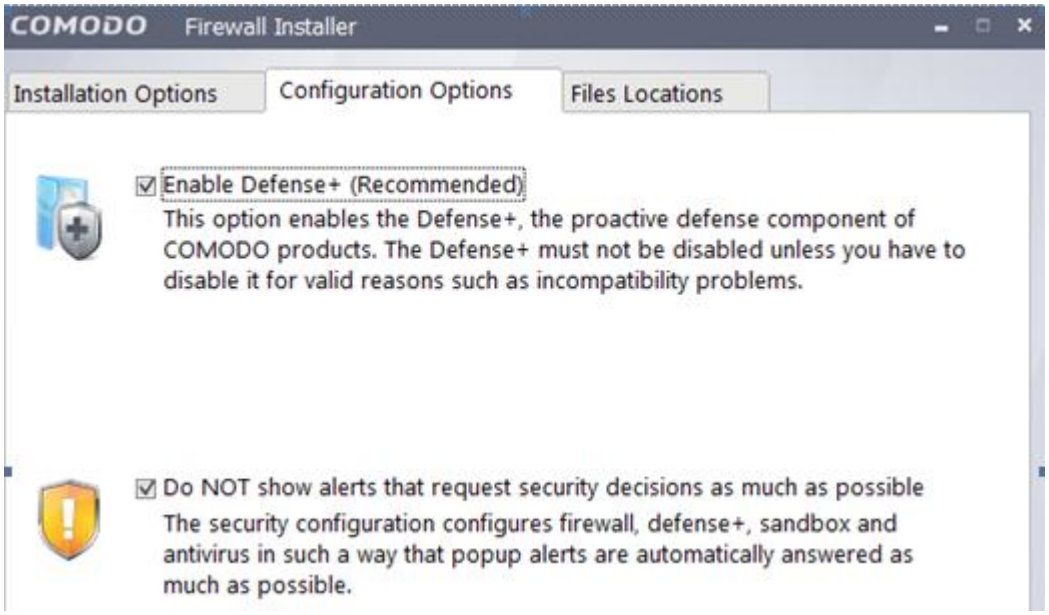
Comodo Firewallin asennuksessa oletusasetuksin huomasin, että varsinaisen palomuurin mukana tulee kolme lisäominaisuutta:

- Comodo GeekBuddy
- Comodo Dragon
- Defense+

Näistä ei huomannut mitään tietoa Comodon internet –sivulta ilmaisen Comodo Firewall –tuotteen yhteydessä. Näiden lisäominaisuuksien asennus oli siis oletuksena päällä, mutta tuotteen olisi voinut asentaa myös ilman näitä käyttämällä ”customize installation” –vaihtoehtoa. Kuvioissa 16 ja 17on nähtävissä asennuksen oletusasetukset sekä vaihtoehdot.



Kuvio 16: Comodo Firewall customize installer 1 (Comodon asennus)



Kuvio 17: Comodo Firewall customize installer 2 (Comodon asennus)

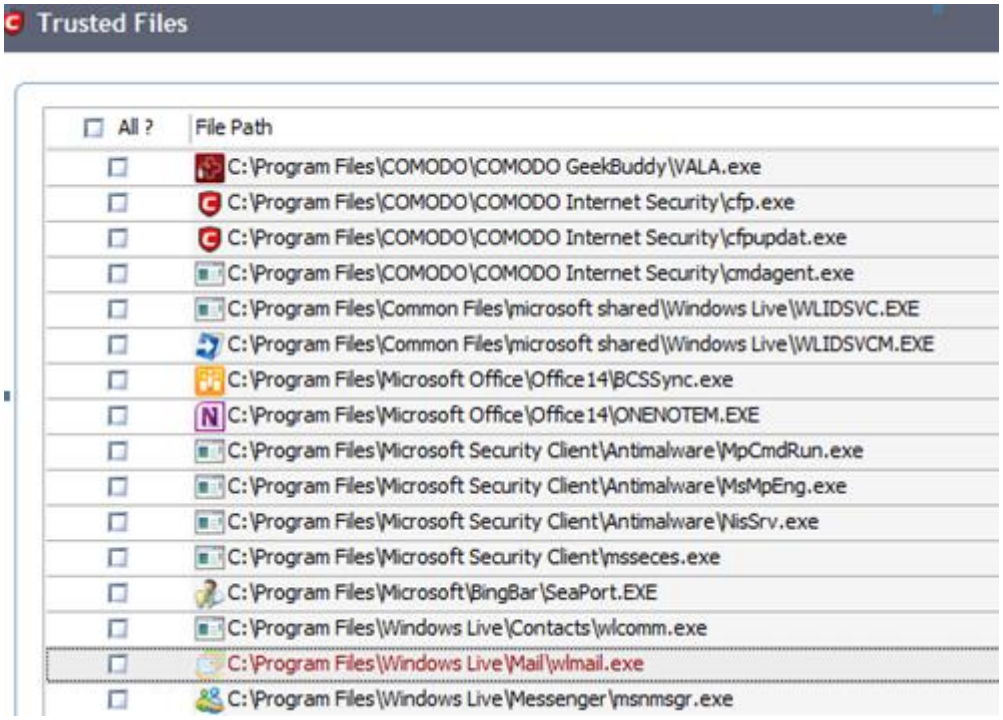
Asensin siis Comodo Firewallin oletusasetuksin, jolloin pääsin tutkimaan myös mitä nämä oletuksena asentuvat lisäominaisuudet ovat. Kun asennus oli valmis, huomasin että tuotteesta asentui myös kattava dokumentaatio, jota en Comodon internetsivulta löytynyt. Dokumentaatio löytyi Comodo Firewallin ”Help” –kohdasta.

Comodo GeekBuddy on Comodon oma tukipalvelu, josta saa tukea milloin tahansa ja kaikkiin tietokoneongelmiin ei siis vain tämän tuotteen ongelmiin. Esimerkiksi siis sähköpostitilin luonti, ohjelmien asennus ja/tai konfigurointi, varmuuskopioiden otto ja mikä tahansa muu tietokoneongelma kuuluvat tämän tuotteen palveluun. Yhteydenotto tukihenkilöön tapahtuu joko pikaviestitse tai puhelimella. Comodo GeekBuddy on kuitenkin maksullinen tuote, vaikka ilmaisen Comodo Firewallin mukana oletuksena asentuukin.

Comodo Dragon on Comodon oma internetselain jonka käyttö on toki ilmaista ja heidän oman mainoksensa mukaan nopeaa sekä turvallista. En testannut tätä Comodo Firewallin lisäosaa tämän enempää, koska se olisi mennyt tutkimukseni aiheen ohi.

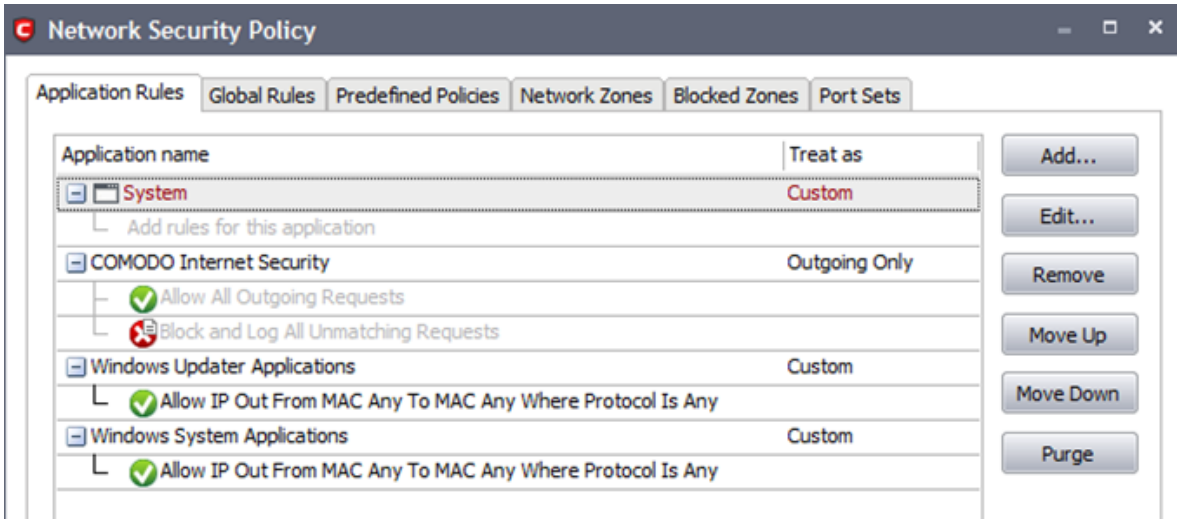
Comodon sovelluskontrolli –lisäohjelmana toimii Defence+ -niminen ohjelma. Se valvoo jokaisen ei-tunnetun ohjelman suorittamista kannettavassa tietokoneessa kuten sovelluskontrollit tekevät ja kysyy tarvittaessa luvan ohjelman ottamiin yhteyksiin. Kuviossa 17 näkyy, että oletusasetuksin tämä Defence+ -ohjelma asennetaan niin, että käyttäjälle tulee mahdollisimman vähän kysymyksiä liittyen Defence+ -ohjelman konfigurointiin eri sovellusten osalta. Näin asennettuna Comodo konfiguroi itse mahdollisimman suuren osan. Näin kaikki tunnetut sovellukset saavat luvan suorittamiseen. Tämä kävi myös Windows Live Mail – sähköpostioh-

jelman kanssa eli testissäni avasin kyseisen ohjelman ja lähetin sähköpostia siitä. Defence+ ei kysynyt mitään ja kun tutkin asiaa tarkemmin, huomasin että kyseisen sovelluksen suorittava tiedosto (wlmail.exe) löytyi jo Defence+:n sallittujen ohjelmien listalta (katso kuvio 18). Kuten kuviosta 18 näkyy, samalla listalla oli myös useita muita tunnettuja sovelluksia jo valmiina. Ilmeisesti Comodon asennusohjelma oli skannannut kannettavan tietokoneen ohjelmat asennusvaiheessa. Comodon sovelluskontrollin eli Defence+:an toiminta ei muuttunut tästä mitenkään, kun käynnistin testikannettavani ja kokeilin sähköpostin lähettämistä uudestaan.



Kuvio 18: Comodo Firewall - sallittuja ohjelmia (Defence+ hallinnointi)

Lisäksi selvitin Comodo Firewallista siis palomuurin oletussäännöt. Ne löytyivät varsin helposti, kun avasin Comodon hallintaikkunan ja sieltä palomuuri –välilehden. Comodo Firewallissa on oletuksena sääntö, että kaikki liikenne ulospäin on sallittua, kun taas sisäänpäin tuleva liikenne on kaikilta osin kielletty, kuten kuviossa 19 näkyy.

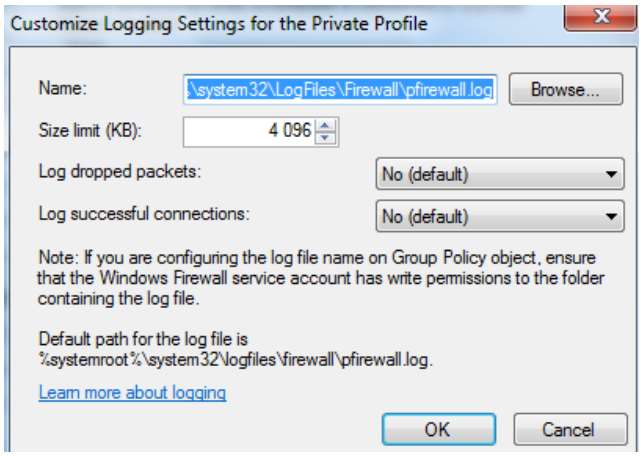


Kuvio 19: Comodo Firewall palomuurisäännöt (Comodo Firewall hallinnointi)

7.2 Tutkimuskysymys 2

7.2.1 Windows 7 Enterprise palomuuri

Windows 7 palomuurin lokinkirjoituksen oletusasetukset olivat kaikilla profiileilla sellaiset, että lokia ei kirjoiteta ollenkaan. Ei siis paketeista, joita palomuuri ei päästä läpi, eikä paketeista jotka palomuuri päästää läpi. Nämä kaksi vaihtoehtoa olivat erikseen konfiguroitavissa, kuten kuviossa 20 on nähtävillä.

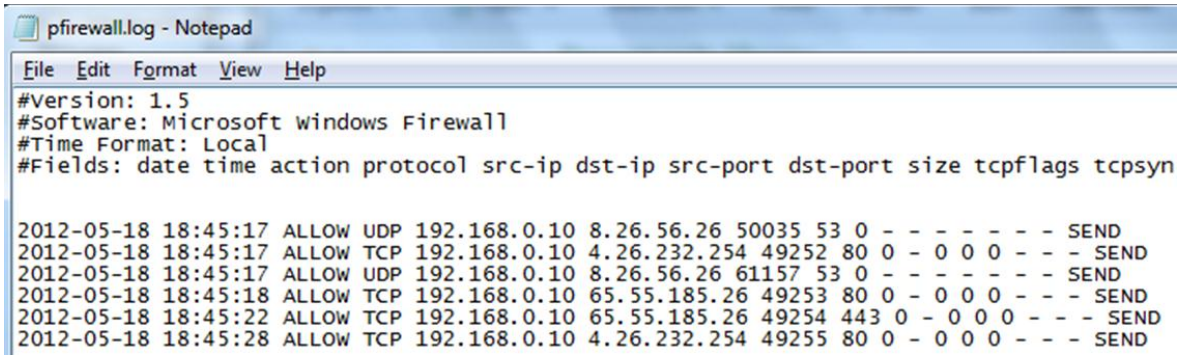


Kuvio 20: Windows 7 palomuurin lokit

Kuviosta 20 selviää muut konfiguroitavissa olevat asiat Windows 7 palomuurin lokiasioissa, eli lokitiedoston sijainti sekä maksimikoko. Seuraavaa testiä varten vaihdoin siis asetukset niin, että sekä läpi päästetyistä, että estetyistä paketeista kirjoitetaan lokia.

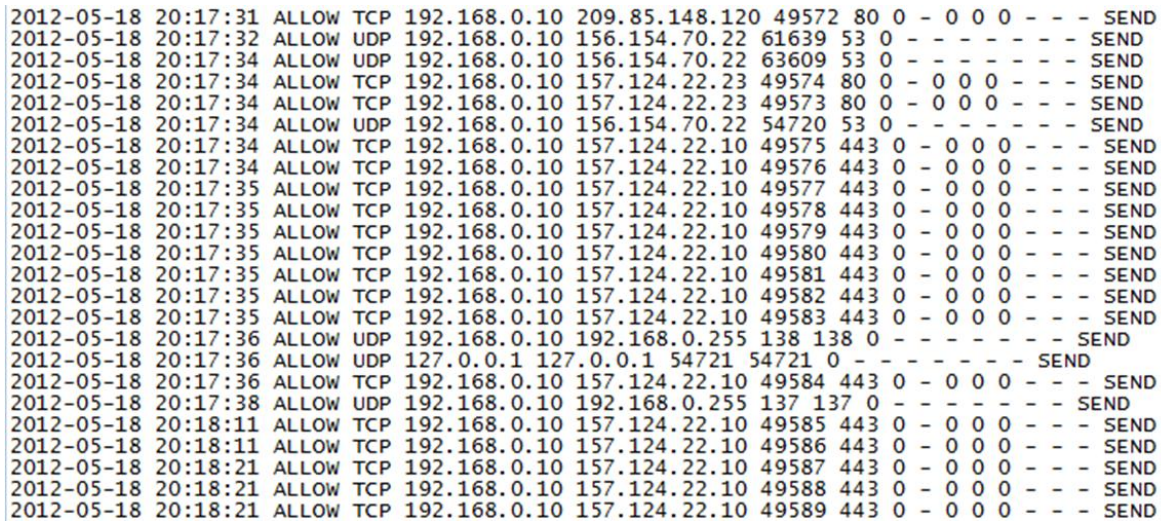
Lokinkirjoitusasetusten vaihtamisen jälkeen kokeilin manuaalisesti onko Windows Update – palvelussa testikannettavalleni päivityksiä saatavilla. Kuviossa 21 on tuosta testistä muodostunut lokitiedosto. Siitä käy ilmi päivän ja kellonajan lisäksi tapahtuma, käytetty protokolla, lähde

IP-osoite, kohde IP-osoite, lähde- ja kohde-portit sekä muita yhteyteen liittyviä tietoja. Kuvio 21 kertoo, että ensin yhteys on otettu IP-osoitteeseen 8.26.56.26 ja sen porttiin 53. Tämän jälkeen on tapahtunut muita yhteydenottoja, jotka kaikki liittyvät tekemääni tarkastukseen.



Kuvio 21: Windows 7 palomuurin Windows Update lokia

Edellisen testin jälkeen muokkasin taas hieman lokinkirjoitusasetuksia seuraavaa testiäni varten. Huomasin edellisessä testissä, että Windows 7 palomuuri kirjoittaa paljon lokia, josta syystä otin lokinkirjoituksen pois estettyjen pakettien kohdalla. Näin uskoin saavani paremmin tulkittua syntyvää lokitiedostoa. Testini oli siis avata kannettavan tietokoneeni oletusselaimella yhteys verkkopankkiin ja kirjautua sinne katsomaan tilitietoja. Kuviossa 22 näkyy ote tässä testissä näillä lokinkirjoitusasetuksilla muodostuneesta lokitiedostosta.



Kuvio 22: Windows 7 palomuurin pankkilokia

Ensimmäinen rivi näyttää kuinka yhteys on avattu IP-osoitteeseen 209.85.148.120 ja sen porttiin 80, joka on Googlen eli testikannettavani selaimen kotisivun osoite. Seuraavan rivin IP-osoite ja portti kertovat yhteydestä tässä testissä käytetyn verkkopankin (Osuuspankki) nimipalveluun. Seuraava tärkeä asia lokista on sen seitsemäs rivi, jossa käytetty portti on muuttunut 443:een, joka on tunnettu porttinumero HTTPS –protokollalle. Tätä protokollaa käytetään

tiedon suojattuun siirtoon. Tässä vaiheessa on tapahtunut varmenteen tarkistus ja sen jälkeen tieto on kulkenut tuon saman 443 portin kautta.

Kolmas testini tämän tutkimuskysymyksen selvittämiseen oli siis käyttää Nmap – porttiskanneria simuloimaan sisäänpäin tulevaa liikennettä ja havainnoida millaista lokia siitä syntyy. Tein kyseisellä ohjelmalla niin sanotun TCP connect skannauksen, jossa TCP yhteyden vaatima kolmivaiheinen kättely pyritään viemään loppuun asti, mikäli mahdollista. Ennen testiä vaihdoin kuitenkin taas lokinkirjoitusasetukset takaisin sellaisiksi, että estetyistä sekä läpi päästetyistä paketeista jää lokiin merkintä. Tämän skannauksen tulos näkyy alla olevassa kuviossa 23 eli yksikään tuhannesta ensimmäisestä portista jotka skannattiin ei ollut auki.

```
C:\>nmap -sT 192.168.0.15

Starting Nmap 6.00 ( http://nmap.org ) at 2012-09-17 21:25 FLE Daylight Time
Nmap scan report for 192.168.0.15
Host is up (0.031s latency).
All 1000 scanned ports on 192.168.0.15 are filtered
MAC Address: 00:1B:77:6E:0C:4C (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 65.00 seconds
```

Kuvio 23: Windows 7 palomuurin Nmap tulokset 1

Tuo että skannauksen tulos sanoo porttien olevan ”filtered” tarkoittaa sitä, että Nmap ei voi määrittää onko portti olemassa vai ei. Jos se on olemassa, niin siihen ei siis pääse. Kuviossa 24 näkyy ote Windows 7 palomuurin lokista, joka muodostui testistäni.

```
2012-09-17 21:25:56 DROP TCP 192.168.0.11 192.168.0.15 11540 135 48 S 3903058631 0 64512 - - - RECEIVE
2012-09-17 21:25:56 DROP TCP 192.168.0.11 192.168.0.15 11541 554 48 S 3961008844 0 64512 - - - RECEIVE
2012-09-17 21:25:57 DROP TCP 192.168.0.11 192.168.0.15 11542 554 48 S 3766001006 0 64512 - - - RECEIVE
2012-09-17 21:25:57 DROP TCP 192.168.0.11 192.168.0.15 11543 135 48 S 2478143733 0 64512 - - - RECEIVE
2012-09-17 21:25:57 DROP TCP 192.168.0.11 192.168.0.15 11544 445 48 S 3480534065 0 64512 - - - RECEIVE
2012-09-17 21:25:58 DROP TCP 192.168.0.11 192.168.0.15 11557 139 48 S 2995957457 0 64512 - - - RECEIVE
2012-09-17 21:25:58 DROP TCP 192.168.0.11 192.168.0.15 11562 139 48 S 2286285961 0 64512 - - - RECEIVE
2012-09-17 21:26:11 DROP TCP 192.168.0.11 192.168.0.15 11998 49153 48 S 855135471 0 64512 - - - RECEIVE
2012-09-17 21:26:11 DROP TCP 192.168.0.11 192.168.0.15 12003 49153 48 S 283167268 0 64512 - - - RECEIVE
2012-09-17 21:26:29 DROP TCP 192.168.0.11 192.168.0.15 12551 49152 48 S 1382551540 0 64512 - - - RECEIVE
2012-09-17 21:26:29 DROP TCP 192.168.0.11 192.168.0.15 12556 49152 48 S 648264907 0 64512 - - - RECEIVE
2012-09-17 21:26:40 DROP TCP 192.168.0.11 192.168.0.15 12700 49154 48 S 3487223247 0 64512 - - - RECEIVE
2012-09-17 21:26:40 DROP TCP 192.168.0.11 192.168.0.15 12706 49154 48 S 3677312709 0 64512 - - - RECEIVE
2012-09-17 21:26:40 DROP TCP 192.168.0.11 192.168.0.15 12740 2869 48 S 2780560828 0 64512 - - - RECEIVE
2012-09-17 21:26:40 DROP TCP 192.168.0.11 192.168.0.15 12746 2869 48 S 3788899040 0 64512 - - - RECEIVE
2012-09-17 21:26:43 DROP TCP 192.168.0.11 192.168.0.15 12706 49154 48 S 3677312709 0 64512 - - - RECEIVE
2012-09-17 21:26:43 DROP TCP 192.168.0.11 192.168.0.15 12700 49154 48 S 3487223247 0 64512 - - - RECEIVE
2012-09-17 21:26:43 DROP TCP 192.168.0.11 192.168.0.15 12746 2869 48 S 3788899040 0 64512 - - - RECEIVE
2012-09-17 21:26:43 DROP TCP 192.168.0.11 192.168.0.15 12740 2869 48 S 2780560828 0 64512 - - - RECEIVE
2012-09-17 21:26:49 DROP TCP 192.168.0.11 192.168.0.15 12706 49154 48 S 3677312709 0 64512 - - - RECEIVE
2012-09-17 21:26:49 DROP TCP 192.168.0.11 192.168.0.15 12700 49154 48 S 3487223247 0 64512 - - - RECEIVE
2012-09-17 21:26:49 DROP TCP 192.168.0.11 192.168.0.15 13183 49156 48 S 3889727477 0 64512 - - - RECEIVE
2012-09-17 21:26:49 DROP TCP 192.168.0.11 192.168.0.15 12740 2869 48 S 2780560828 0 64512 - - - RECEIVE
2012-09-17 21:26:49 DROP TCP 192.168.0.11 192.168.0.15 12746 2869 48 S 3788899040 0 64512 - - - RECEIVE
2012-09-17 21:26:49 DROP TCP 192.168.0.11 192.168.0.15 13188 49156 48 S 2050473850 0 64512 - - - RECEIVE
2012-09-17 21:26:54 DROP TCP 192.168.0.11 192.168.0.15 13343 49155 48 S 1932476011 0 64512 - - - RECEIVE
2012-09-17 21:26:54 DROP TCP 192.168.0.11 192.168.0.15 13348 49155 48 S 96572954 0 64512 - - - RECEIVE
2012-09-17 21:26:56 DROP TCP 192.168.0.11 192.168.0.15 13413 49167 48 S 152959515 0 64512 - - - RECEIVE
2012-09-17 21:26:56 DROP TCP 192.168.0.11 192.168.0.15 13418 49167 48 S 3060261690 0 64512 - - - RECEIVE
2012-09-17 21:27:00 DROP TCP 192.168.0.11 192.168.0.15 13531 10243 48 S 427982852 0 64512 - - - RECEIVE
2012-09-17 21:27:00 DROP TCP 192.168.0.11 192.168.0.15 13536 10243 48 S 3036672418 0 64512 - - - RECEIVE
```

Kuvio 24: Windows 7 palomuurin Nmap lokia

Lokin kahdeksas sarake vasemmalta oikealle katsottuna kertoo kohdeportin johon skannaus on tehty. Olennaisinta lokista kuitenkin on huomata, että kaikki yritykset riippumatta lähde- tai kohdeportista, on estetty.

Saadakseni varmuuden palomuurin toiminnasta sekä hieman erilaisuutta tuloksiin, päätin vielä testata toisella tapaa. Suljin Windows 7 palomuurin kokonaan ja suoritin samanlaisen TCP connect skannauksen. Kuten pitikin, tulos oli erilainen. Kuviosta 25 näkyy, kuinka auki olevia portteja löytyi 12 kpl ja loput 988 porttia oli kiinni. Tästä huomaa hyvin konkreettisesti kuinka tärkeä palomuuri kannettavassa tietokoneessa on.

```
C:\>nmap -sT 192.168.0.15

Starting Nmap 6.00 ( http://nmap.org ) at 2012-09-17 21:19 FLE Daylight Time
Nmap scan report for 192.168.0.15
Host is up (1.0s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49167/tcp open  unknown
MAC Address: 00:1B:77:6E:0C:4C (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 209.28 seconds
```

Kuvio 25: Windows 7 palomuurin Nmap tulokset 2

7.2.2 F-Secure Client Security 2012 palomuuri

Kuten aiemmin mainittu tämän osuuden testit minun piti tehdä F-Secure Internet Security 2012 ohjelman palomuurilla, mutta sitä ei ollut enää testejä aloittaessani saatavilla versiopäivityksen johdosta. Tästä syystä käytin seuraavaksi kuvatuissa testeissä F-Secure Client Security 2012 ohjelman palomuuria, joka F-Securelta saadun tiedon mukaan on ”teknisesti melkein sama kuin Internet Security 2012 versiossa”. Näin ollen tein siis tämän osion testini eri palomuurilla kuin alun perin olin suunnitellut.

F-Secure Client Security 2012 versiossa lokinkirjoitus on jaettu periaatteessa kahteen osaan, eli tapahtumalokiin ja pakettilokiin. Tosin näiden lisäksi palomuurilla on erikseen hälytysloki joka kerää lokiin merkinnät liikenteestä, joka aiheuttaa hälytyksen palomuurissa. Tähän lokiin tulee seuraavat tiedot hälytyksestä:

- Hälytyksen kuvaus
- Toimenpide (esimerkiksi että palomuuri on estänyt paketin)

- Aika
- Suunta, eli koskeeko hälytys sisään vai ulospäin menossa ollutta pakettia
- Protokolla
- Palomuurin palvelu johon tämä hälytys liittyy
- Lähde IP osoite ja portti
- Kohde IP osoite ja portti

Tämä palomuurin hälytysloki on oletuksena päällä jos palomuurikin on päällä ja sitä ei voi erikseen ottaa pois päältä.

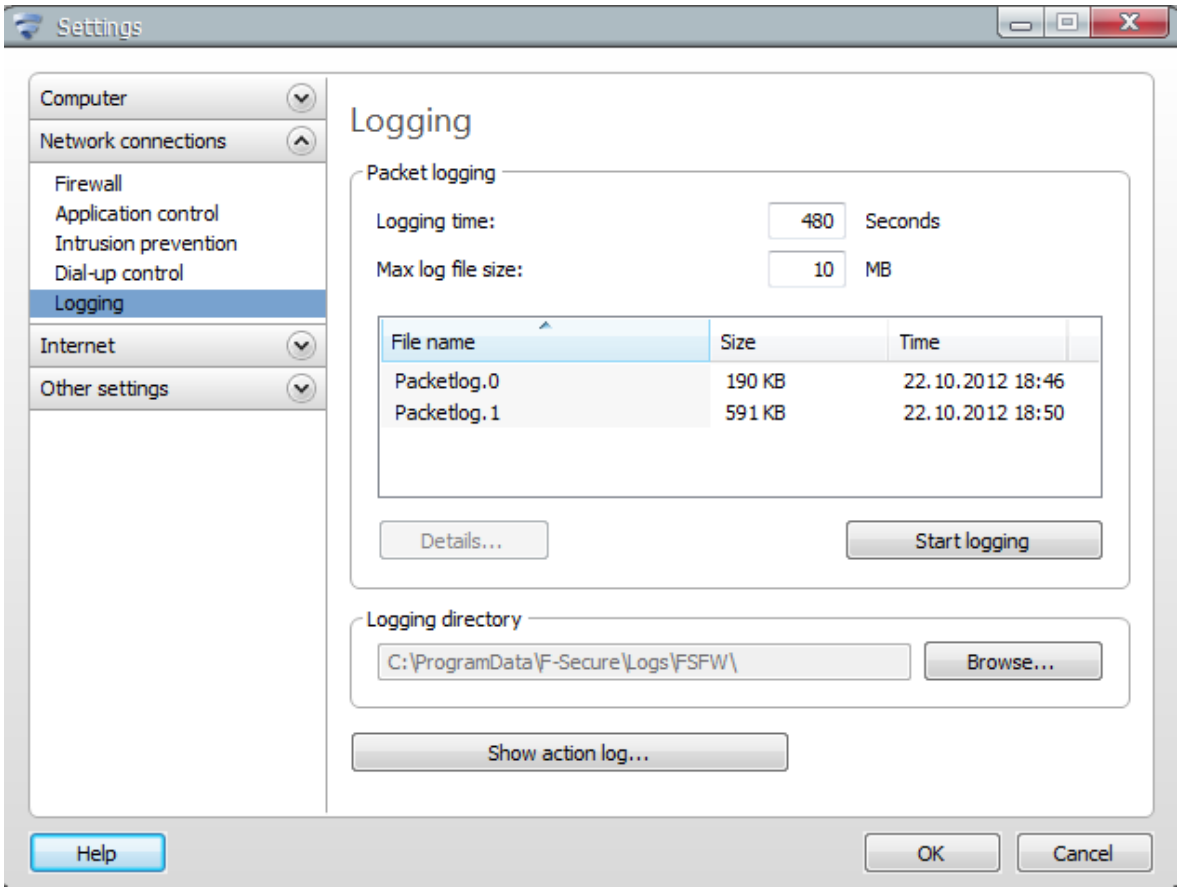
Tapahtumalokiin kirjataan avatut yhteydet sekä muuttuneet palomuurisäännöt. Esimerkkinä avatusta yhteydestä käy vaikka kun käyttäjä antaa palomuurille luvan, että tietty kannettavassa tietokoneessa oleva ohjelma saa itse hallinnoida yhteyksiä palomuurin läpi. Kun tämä kyseinen ohjelma sitten ottaa yhteyden vastaan palomuurin läpi eli sisäänpäin, se tapahtuma kirjautuu tapahtumalokiin avattuna yhteytenä. Lokin maksimikoko on 10 megabittiä ja kun se tulee vastaan, poistetaan merkintöjä vanhimmasta päästä. Myös tämä loki on oletuksena päällä eikä sitä voi ottaa pois päältä.

Pakettiloki on tarkoitettu kokeneimmille käyttäjille ja on oletuksena pois päältä. Sillä voi tutkia ja kerätä tietoa verkkoliikenteestä, joka menee palomuurin läpi. Tätä lokia on hyvä käyttää esimerkiksi silloin kun on tehnyt uuden oman palomuurisäännön ja haluaa tarkistaa miten se vaikuttaa liikenteeseen. Toinen hyvä käyttötapa on epäilyttävän verkkoliikenteen tutkiminen. Pakettiloki laitetaan päälle ennalta määrätyksi ajaksi ja tuo aika määritellään asetuksissa sekunteina, kuten kuvion 26 ”Logging time” – kentästä näkee. Lokille annetaan myös maksimikoko kohdassa ”Max log file size” (katso kuvio 26). Itse loki käynnistetään napista ”Start logging” (katso kuvio 26). Tämän jälkeen pakettiloki kerää tuon ennalta määrätyn sekuntiajan mukaan tietoa seuraavasti:

- Aika sekunneissa siitä hetkestä kun loki laitettiin päälle
- Mitä paketille tehtiin (oletus on että estetään pääsy palomuurin läpi) eli jos paketti päästetään läpi, annetaan arvo ”No” ja jos paketti on estetty, arvo on ”Yes”. Lisäksi samassa kentässä on myös merkinnät ”In” ja ”Out”, jotka tarkoittavat joko sisäänpäin tai ulospäin kulkenutta liikennettä
- Protokolla
- Lähde IP-osoite

- Kohde IP-osoite
- Paketin otsikon tunnistetiedot
- Niin sanottu TTL eli Time To Live arvo, joka kertoo kuinka monen verkkolaitteen läpi paketti pääsee ennen kuin se hävitetään
- Paketin kokonaispituus
- Paketin kuvaus

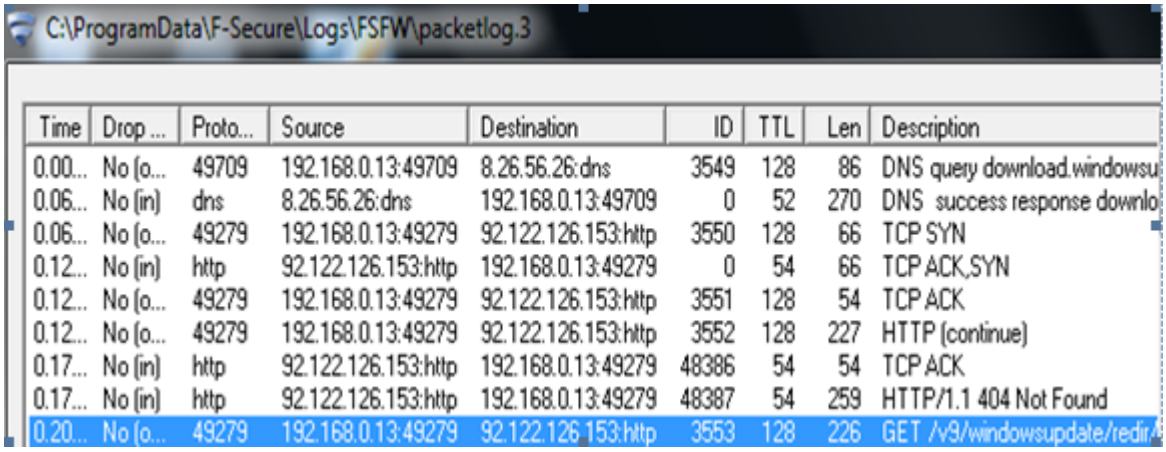
Kuviossa 26 näkyy F-Securen valikko, josta pakettilokin asetukset määritellään ja loki käynnistetään. Samasta kuviosta näkee myös kohdan, josta pääsee katsomaan aiemmin mainittua tapahtumalokia (Show action log).



Kuvio 26: F-Securen lokiasetukset

Seuraavaa testiäni varten päätin katsoa tässä tapauksessa molempia lokeja eli tapahtuma- sekä pakettilokia. Testihän oli hakea Windows Update – palvelusta päivitykset manuaalisesti ja katsoa miten se näkyy lokeilla. Tätä testiä varten siis tapahtumaloki oli jo oletuksena päällä ja lisäksi käynnistin pakettilokin, jotta saisin mahdollisimman kattavat lokit tästä testistäni. Laitoin pakettilokin kestoksi 480 sekuntia, jonka uskoin riittävän sekä maksimikooksi samoin perustein 10 MB.

Testin tuloksena tapahtumalokiin tuli vain merkintä, että testikannettavani svchost.exe – ohjelmalle oli avattu yhteys ulospäin. Muita merkittäviä merkintöjä ei lokilla ollut. Tämän takia keskityin pakettilokiin. Siellä merkintöjä riittikin runsaasti, vaikka testini kesti vain noin 5 sekuntia. Alla olevassa kuviossa 27 näkyy ote tuon testin aikana muodostuneesta pakettilokista, jonka siis itse ”nauhoitin”.

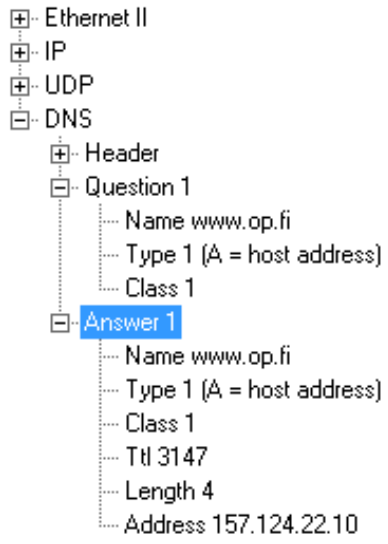

C:\ProgramData\F-Secure\Logs\FSFW\packetlog.3

Time	Drop ...	Proto...	Source	Destination	ID	TTL	Len	Description
0.00...	No (o...	49709	192.168.0.13:49709	8.26.56.26:dns	3549	128	86	DNS query download.windowsu
0.06...	No (in)	dns	8.26.56.26:dns	192.168.0.13:49709	0	52	270	DNS success response downlo
0.06...	No (o...	49279	192.168.0.13:49279	92.122.126.153:http	3550	128	66	TCP SYN
0.12...	No (in)	http	92.122.126.153:http	192.168.0.13:49279	0	54	66	TCP ACK,SYN
0.12...	No (o...	49279	192.168.0.13:49279	92.122.126.153:http	3551	128	54	TCP ACK
0.12...	No (o...	49279	192.168.0.13:49279	92.122.126.153:http	3552	128	227	HTTP (continue)
0.17...	No (in)	http	92.122.126.153:http	192.168.0.13:49279	48386	54	54	TCP ACK
0.17...	No (in)	http	92.122.126.153:http	192.168.0.13:49279	48387	54	259	HTTP/1.1 404 Not Found
0.20...	No (o...	49279	192.168.0.13:49279	92.122.126.153:http	3553	128	226	GET /v9/windowsupdate/redir

Kuvio 27: F-Securen Windows Update lokia

Kuvion 27 kaksi ensimmäistä riviä kertovat että testikannettavan IP – osoitteesta on tehty DNS kysely, jonka tarkoituksen on ollut selvittää Windows Update – palvelun IP – osoite. Tämä osoite on saatu tietoon, jonka jälkeen kolmannelta riviltä alkaen on aloitettu yhteyden muodostaminen tuohon osoitteeseen. Kuvion 27 lokin alimmalla rivillä näkyy, kun yhteys on muodostunut HTTP – porttiin ja IP – osoitteeseen 92.122.126.153. Myös ”Description” – kentän tekstistä näkyy, että yhteys on valmiina.

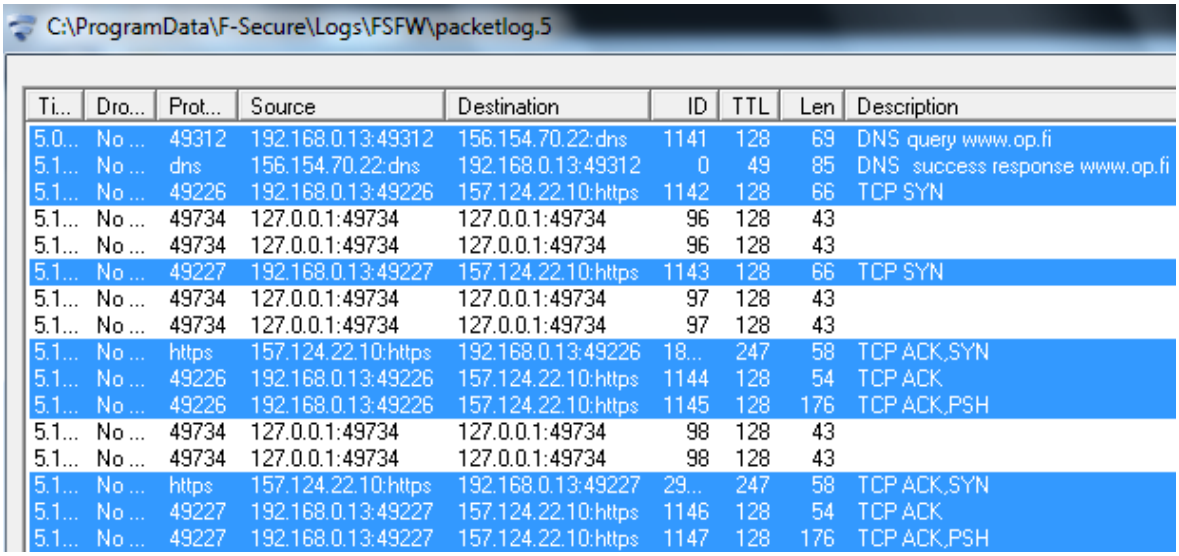
Seuraavassa testissäni, joka oli verkkopankissa käynti, päätin käyttää pelkästään pakettilokia, sillä huomasin sen olevan erittäin kattava ja selkeä. Avasin siis testikannettavan Internet Explorer selaimen jolla menin verkkopankkiin, kirjauduin sisään ja selasin tilitietojani. Tämän jälkeen pysäytin pakettilokin keräämisen ja aloin tutkia tuloksia. Lokilta näkyy jälleen, kuinka ensin testikannettavani on lähettänyt DNS kyselyn selvittääkseen mikä on www.op.fi – sivun IP – osoite. Kuviosta 28, joka on poimittu pakettilokilta, näkyy tarkemmin mitä tuossa DNS kyselyssä tapahtuu.



Kuvio 28: F-Securen pankkiloki 1

DNS kyselyssä siis yksinkertaisesti lähetetään kysymys www.op.fi sivun osoitteesta, kuten kuvion 28 kohdassa ”Question 1” näkyy ja saadaan vastaus että se on 157.124.22.10, kuten saman kuvion ”Answer 1” – kohdasta selviää.

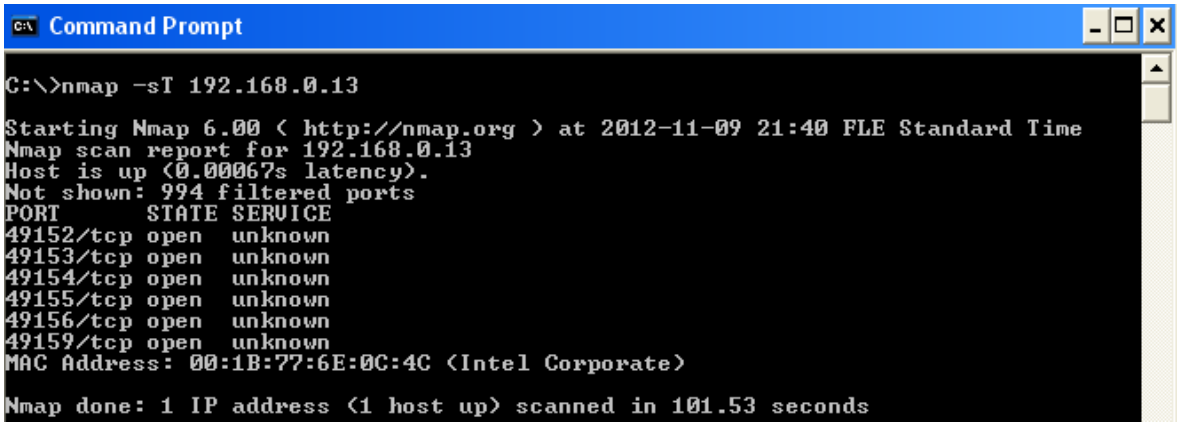
Kuviossa 29 on ote pakettilokista kokonaisuudessaan. Kuviosta näkyy, että kaksi ensimmäistä riviä ovat siis tuota DNS kyselyä jota yllä kuviossa 28 selvitettiin tarkemmin. Sen jälkeen kun osoite verkkopankkiin on saatu selville, liikenne on vaihdettu salatuksi, eli käyttämään HTTPS protokollaa jo yhteyttä sivustolle muodostettaessa. Kuviossa 29 tummennettuna ovat yhteyden muodostuksen kannalta tärkeimmät rivit. Ne koskevat nimenomaan tuota yhteyden muodostamista sekä sivustolle kirjautumista.



Kuvio 29: F-Securen pankkiloki 2

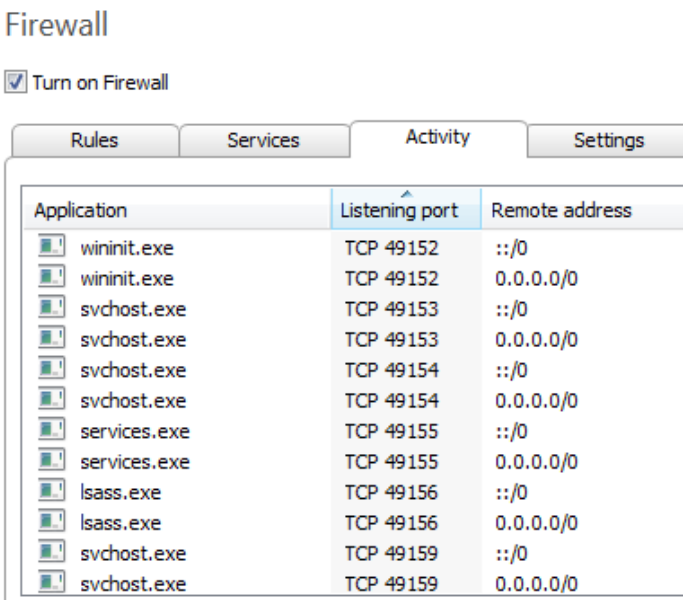
Kolmantena testinä tein sitten porttiskannauksen Nmap – porttiskannerilla, simuloiden tällä sisään tulevaa hakkeriliikennettä. Tein jälleen TCP Connect – skannauksen mutta sitä ennen

laitoin F-Secure Internet Security 2012 palomuurin pakettilokin päälle, jotta saisin kattavat tulokset. Kuviossa 30 on kuvaruutukaappaus Nmap – ohjelman tuloksista ja siitä selviää, että skannatuista 1000 portista auki oli 6. Loput 994 porttia olivat kiinni tai niiden tila jäi epäselväksi.



Kuvio 30: F-Securen Nmap tulokset

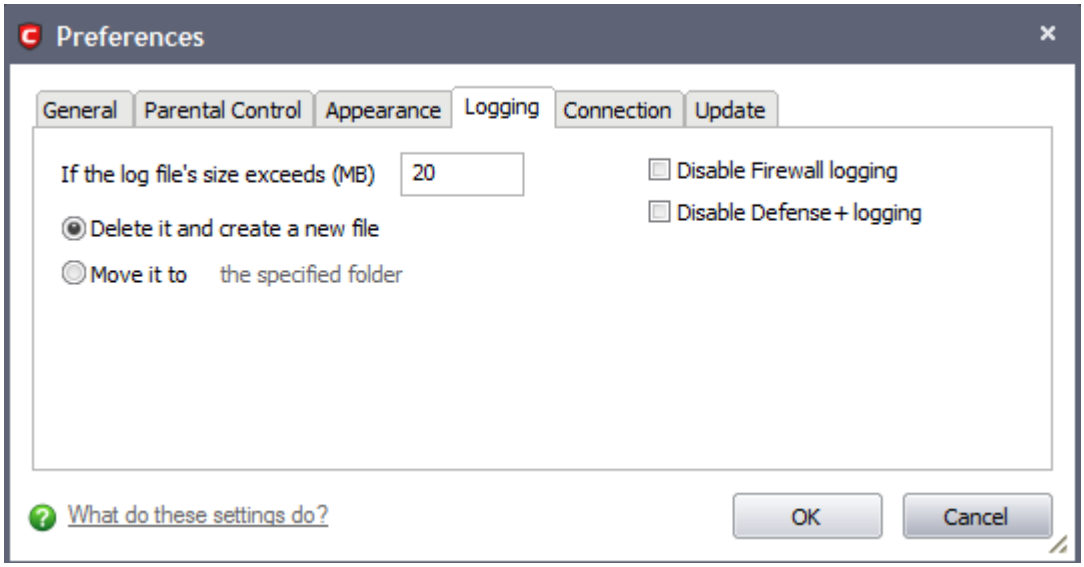
F-Securen palomuurin ”activity” – kohdasta eli kohdasta, joka näyttää olemassa olevat yhteydet poimin alla näkyvän kuvion 31. Poiminta on tehty Nmap – testin aikana eli tuo selittää miksi kuviossa 30 näkyvät portit olivat auki. Ja kun kuviosta 31 katsoo saraketta ”application” selviää, että mikä ohjelma on pitänyt porttia auki. Kaikki neljä eri ohjelmaa (wininit.exe, svchost.exe, services.exe ja lsass.exe) liittyvät Windows käyttöjärjestelmän toimintaan, joten on loogista, että nuo portit ovat auki.



Kuvio 31: F-Securen Nmap testin aikaiset yhteydet

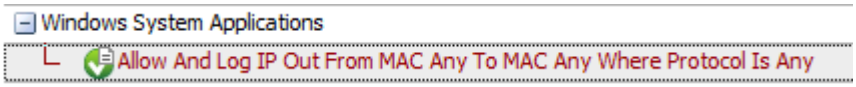
7.2.3 Comodo Firewall

Comodo palomuurin lokinkirjoituksen oletusasetukset ovat sellaiset, että lokia kirjoitetaan vain jos sisäänpäin tulevia yhteyksiä estetään. Tämä tarkoittaa siis sitä, että kun kaikki ulospäin menevä liikenne on sallittua, siitä ei lokia muodostu. Lokia pystyy konfiguroimaan per sääntö sekä yleisesti koko ohjelman asetuksista. Yleisesti muutettavissa on lokitiedoston maksimikoko, sekä se mitä tehdään, kun tuo maksimikoko saavutetaan. Vaihtoehtoina tähän on, että järjestelmä poistaa lokitiedoston kokonaan tai siirtää sen haluttuun kansioon. Lisäksi erikseen pystyy poistamaan palomuurin ja/tai sovelluskontrollin lokinkirjoituksen käytöstä kokonaan. Kuviossa 32 näkyy Comodon asetusten loki – välilehti, josta yllä mainitut asetukset ovat säädettävissä.

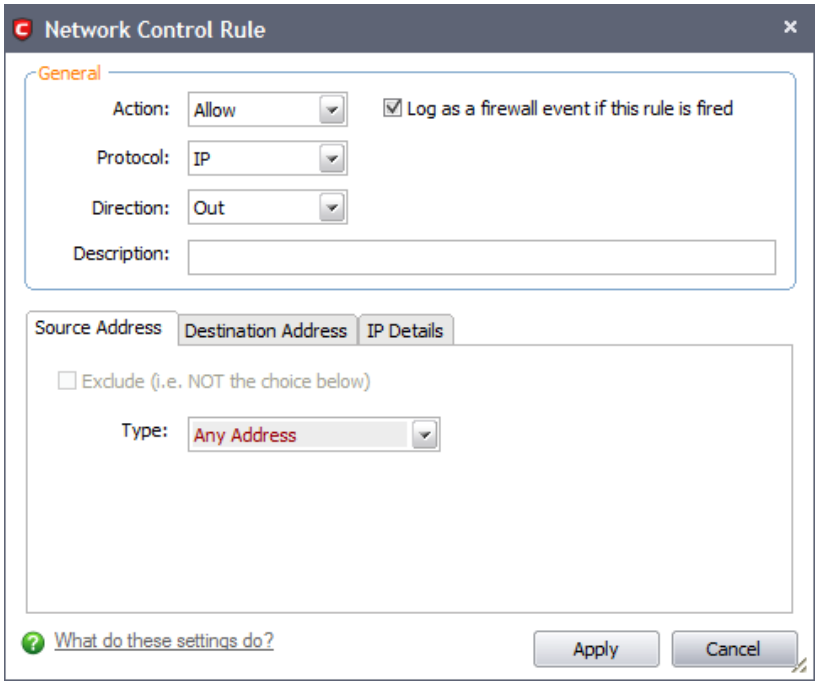


Kuvio 32: Comodon lokiasetukset

Muutin seuraavaa testiäni varten oletusasetuksia yhden palomuurisäännön kohdalla eli sen, joka salli kaiken liikenteen Windowsin systeemi sovelluksilta joihin Windows Update kuuluu. Muutin kyseisen säännön lokiasetuksia niin, että lokia kirjoitetaan myös sallittujen yhteyksien kohdalla. Kuviossa 33 näkyy ensin sääntö, jonka lokinkirjoitusasetuksia muutin sekä kuviossa 34 tarkemmin mitä muutin eli laitoin ruksin kohtaan ”Log as a firewall event if this rule is fired”. Tämän asetuksen avulla muodostui lokia jos tämä sääntö toteutuu (oletusasetuksin tuo ruksi oli siis pois päältä).

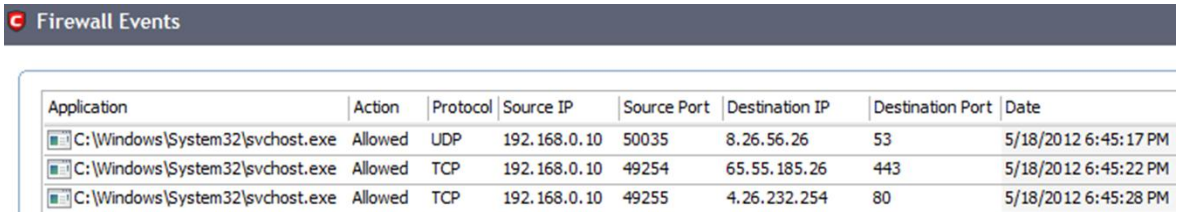


Kuvio 33: Comodo palomuurisääntö 1



Kuvio 34: Comodo palomuurisääntö 2

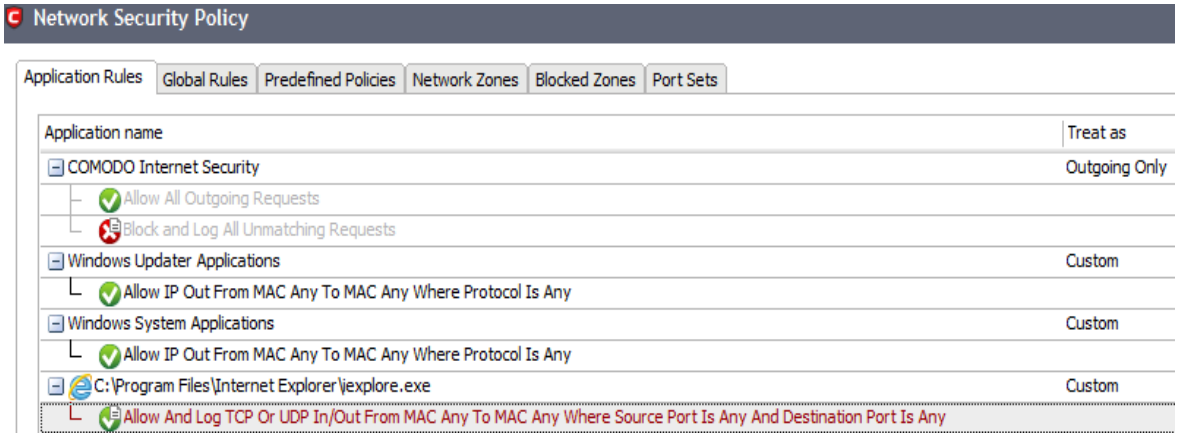
Tämän muutoksen avulla sain siis lokia muodostumaan seuraavaa testiäni varten, joka siis oli että tarkistin manuaalisesti Windows Updatesta onko päivityksiä saatavilla. Alla näkyvässä kuviossa 35 on ote lokista. Lokia on muodostunut siitä, kun testikannettavani on ottanut yhteyden Microsoft Update – palveluun. Lokista selviää että yhteyden on ottanut svchost.exe ohjelma, jonka avulla Windows suorittaa monia toimintoja kuten esimerkiksi tämän saatavilla olevien päivitysten tarkistamisen. Seuraavat sarakkeet kertovat mitä on tapahtunut, millä protokollalla ja mistä IP-osoitteesta ja portista mihin IP-osoitteeseen ja porttiin. Myös päiväys kellonaikoineen on tallentunut lokille. Kuvion 35 lokia tutkimalla selviää että ensin yhteys on muodostettu IP -osoitteeseen 8.26.56.26 ja porttiin 53. Tämä on DNS kyselyn lokimerkintä eli testikoneeni IP -osoitteesta on lähtenyt kysely verkkoon, jonka tavoitteena on ollut selvittää Windows Update – palvelun IP -osoite. Tämän jälkeen on muodostettu kaksi muuta yhteyttä eri IP -osoitteisiin ja portteihin. Nämä ovat liittyneet tuohon saatavilla olevien päivitysten tarkistukseen ja molemmat koskevat HTTP ja HTTPS portteja, eli 80 ja 443.



Kuvio 35: Comodo Windows update lokia

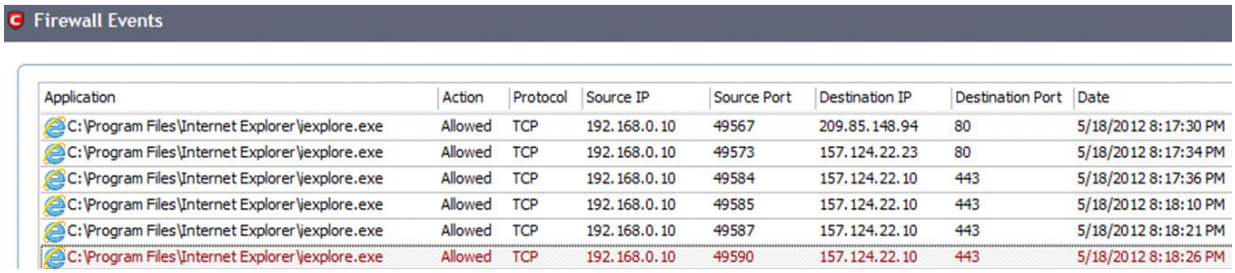
Seuraavaksi testasin millaista jälkeä lokeihin muodostuu kun kävin verkkopankissa katsomassa tilini saldon. Jälleen ennen testiä oli tarpeen muokata lokinkirjoituksen asetuksia, koska muu-

ten ei lokia olisi syntynyt ollenkaan. Tämä sen takia että Comodon oletusasetuksissa on määritelty, että kun ulospäin on kaikki liikenne sallittua, siitä ei lokia kirjoiteta. Muokkasin sääntölistaa niin että Internet Explorerin liikenteestä kirjoitetaan lokia, kuten kuviosta 36 kahdelta alimmalta riviltä näkyy.



Kuvio 36: Comodon muokattu sääntölista

Tämän jälkeen tein itse testin eli avasin selaimen, jonka aloitussivu oli www.google.fi ja sen latautumisen jälkeen kirjoitin osoiteriville www.op.fi ja jatkoin siitä kirjautumalla verkkopankkiini. Hetken päästä kirjauduin ulos ja suljin selaimen. Kuvio 37 näyttää millaista lokia tuosta syntyi.



Kuvio 37: Comodo pankkiloki

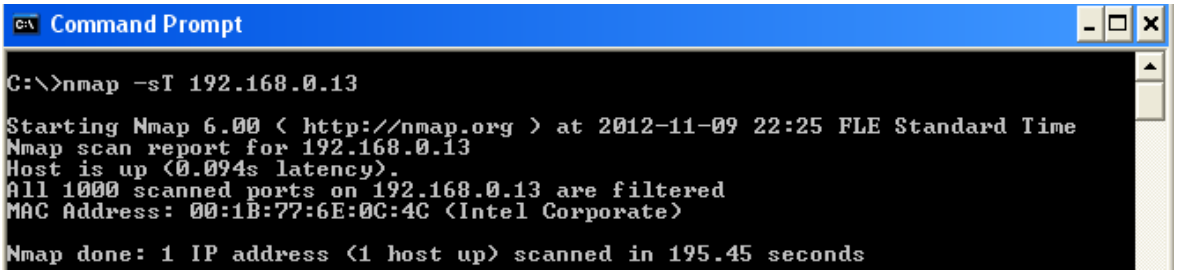
Kuviossa 37 näkyvä loki kertoo, että ensin on avattu yhteys IP-osoitteeseen 209.85.148.94 ja porttiin 80, jonka selvitin olevan Googlen osoite. Tämän jälkeen siirryin siis www.op.fi sivulle, joka näkyy seuraavalla rivillä lokissa, eli edelleen on käytössä portti 80. Kolmannella rivillä näkyy selvästi kun liikenne on muutettu käyttämään HTTPS –protokollaa ja sen tunnettua porttia 443. Tästä voin siis varmistua, että kirjautumiseni verkkopankkiini käytti HTTPS – protokollaa jota käytetään tiedon suojattuun siirtoon.

Kolmannessa eli Nmap – porttiskannerilla tehdyssä testissä simuloin siis sisäänpäin tulevaa hakkeriliikennettä edelleen TCP Connect – skannauksella, jotta kaikkien kolmen Nmap – testini tulokset olisivat vertauskelpoisia keskenään. Comodon kohdalla en muuttanut oletusase-

tuksia mitenkään ennen tätä testiä ja Comodon sovelluskontrolli reagoikin tähän testiini välittömästi. Eli ilmoitus jossa kysyttiin sisäänpäin tulevalle liikenteelle hyväksyntää tai hylkäystä, ponnahti testikannettavani ruudulle. Hylättyäni yhteyden huomasin, että samanlaisia ilmoituksia ponnahti ruudulle useampia Nmap porttiskannauksen ollessa käynnissä. Vastasin kaikkiin samoin kuin ensimmäiseen eli hylkäsin ne. Kuviossa 38 näkyy esimerkki ensimmäisestä ilmoituksesta.

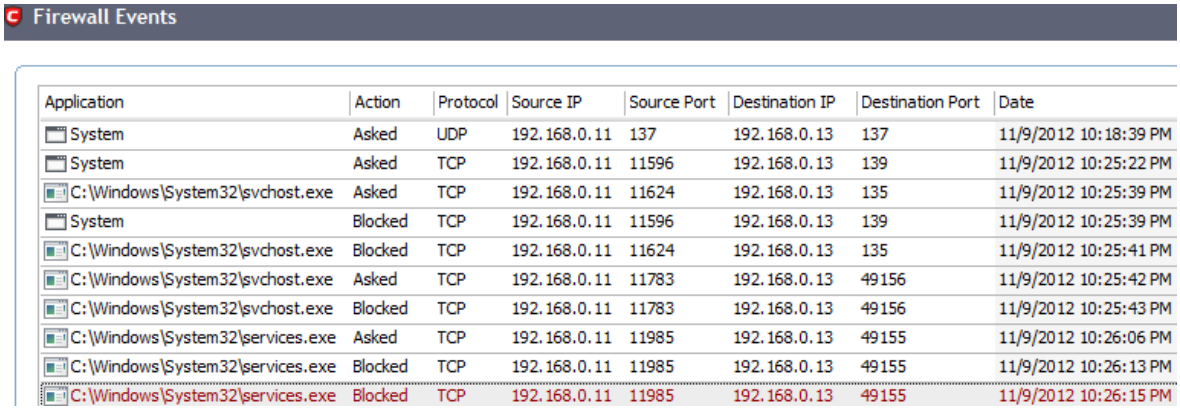
Kuvio 38: Comodo sovelluskontrollin ilmoitus

Ilmoitus siis kysyy annanko Internetistä tulevalle yhteyspyynnölle luvan avata yhteys svchost.exe – ohjelmaan. Kuten mainittu vastasin tähän sekä kaikkiin Nmap – skannauksen aikana tulleisiin vastaaviin kysymyksiin ”Block”. Kuviosta kannattaa huomioida myös kohta ”Remember my answer”, jonka ruksaamalla Comodo muistaa käyttäjän vastauksen tämän ohjelman kohdalla eikä tämän jälkeen enää kysy uudestaan saman ohjelman ollessa kyseessä. Nmapin skannattua testikoneeni kuvaruutukaappaus sen tuloksista näytti kuvion 39 mukaiselta.



Kuvio 39: Comodon Nmap tulokset

Kuvio 39, jossa on kuvaruutukaappaus Nmapin tuloksista, kertoo siis että skannaus on tehty 1000 porttiin ja tulos on, että kaikki ovat ”filtered”. Tämä taas tarkoittaa sitä, että Nmap ei voi määrittää onko portti olemassa vai ei. Jos se on olemassa, niin siihen ei siis pääse. Kuviossa 40 näkyy mitä Comodon loki kertoi tekemästäni porttiskannauksesta.



Application	Action	Protocol	Source IP	Source Port	Destination IP	Destination Port	Date
System	Asked	UDP	192.168.0.11	137	192.168.0.13	137	11/9/2012 10:18:39 PM
System	Asked	TCP	192.168.0.11	11596	192.168.0.13	139	11/9/2012 10:25:22 PM
C:\Windows\System32\svchost.exe	Asked	TCP	192.168.0.11	11624	192.168.0.13	135	11/9/2012 10:25:39 PM
System	Blocked	TCP	192.168.0.11	11596	192.168.0.13	139	11/9/2012 10:25:39 PM
C:\Windows\System32\svchost.exe	Blocked	TCP	192.168.0.11	11624	192.168.0.13	135	11/9/2012 10:25:41 PM
C:\Windows\System32\svchost.exe	Asked	TCP	192.168.0.11	11783	192.168.0.13	49156	11/9/2012 10:25:42 PM
C:\Windows\System32\svchost.exe	Blocked	TCP	192.168.0.11	11783	192.168.0.13	49156	11/9/2012 10:25:43 PM
C:\Windows\System32\services.exe	Asked	TCP	192.168.0.11	11985	192.168.0.13	49155	11/9/2012 10:26:06 PM
C:\Windows\System32\services.exe	Blocked	TCP	192.168.0.11	11985	192.168.0.13	49155	11/9/2012 10:26:13 PM
C:\Windows\System32\services.exe	Blocked	TCP	192.168.0.11	11985	192.168.0.13	49155	11/9/2012 10:26:15 PM

Kuvio 40: Comodo Nmap lokia

Kuvion 40 lokista näkyy siis mihin kaikkiin palveluihin ja portteihin Nmap on skannauksessa yrittänyt ottaa yhteyttä ja ”action” kohdassa näkyy kun Comodo on kysynyt lupaa yhteyksien avaamisille ja seuraavilla rivillä vastauksia kysymyksiin, joka on siis aina ollut kieltävä. Niistä on tullut tuohon sarakkeeseen tapahtumiksi ”Blocked”.

8 Johtopäätökset

Seuraavassa vertaillaan ja analysoidaan molempiin tutkimuskysymyksiin saatuja vastauksia tehtyjen testien perusteella sekä esitetään johtopäätöksiä näistä.

Ensimmäisessä tutkimuskysymyksessähän oli tarkoituksena selvittää tutkittavista palomuureista niiden tietoturvaa parantavat lisäominaisuudet sekä tilallisen palomuurin oletussäännöt. Lisäominaisuuksiltaan nämä kolme palomuuria olivat melko erilaiset, vaikka yhteinen tekijä löytyikin. Se oli sovelluskontrolli ja nimenomaan sellainen, joka oletusasetuksin palomuuria asennettaessa kuului asennukseen ja oli siis asennuksen jälkeen oletuksena päällä. Mielenkiintoista sovelluskontrollin osalta oli myös se, että kahdessa palomuurissa sen sai halutessaan pois päältä vaikka palomuuri edelleen jäi päälle, mutta Windows 7 palomuurissa näin ei voinut tehdä eli jos halusi sen pois päältä, piti ottaa koko palomuuri pois käytöstä.

Muista lisäominaisuuksista huomionarvoista oli se, että ne vaihtelivat palomuureittain selvästi. Windows 7 palomuurissa ei ollut mitään lisäominaisuuksia, minkä uskon johtuvan siitä että Microsoftilla on sellaisia omina erillisinä tuotteinaan esimerkiksi virustorjunta. Comodossa oli

kaksi lisäominaisuutta, jotka olivat pettymyksiä. Toinen oli Comodon oma Internet selain johon en sen enempää ota kantaa, koska en sitä tutkinut ja toinen oli tukipalvelu joka osoittautui maksulliseksi, joten en sitäkään testannut. Hyvää näissä Comodon lisäpalveluissa oli se että niitä ei ollut pakko asentaa. F-Securessa sen sijaan oli useitakin lisäominaisuuksia esimerkiksi virustorjunta. Lisäominaisuuksista huonoimman arvosanan antaisin Comodolle, kun taas Windows 7 palomuuri sekä F-Secure olivat mielestäni tässä suhteessa hyviä.

Toinen ensimmäisessä tutkimuskysymyksessä selvitettävä asia oli tilallisen palomuurin oletussäännöt sekä sovelluskontrollin testaus sähköpostia lähettämällä. Kaikkien kolmen palomuurin oletussäännöissä liikenne ulospäin oli kokonaan sallittu. Sisäänpäin saapuvassa liikenteessä oli pieniä eroavaisuuksia mutta ei mitään suurta ja merkittävää. Kaikissa palomuureissa sisäänpäin tuleva liikenne oli oletuksena kielletty mutta sovelluskontrolli sai antaa itse oikeuksia tunnistamilleen ohjelmille avata yhteyksiä ja siten ottaa vastaan liikennettä sisäänpäin palomuurin läpi. Tähän asiaan liittyi myös testini, jossa lähetin sähköpostia Windowsin omalla sähköpostiohjelmalla, eli Live Mail – ohjelmalla. Kaikkien kolmen palomuurin sovelluskontrolli toimi käyttäjän kannalta miellyttävästi eli sovelluskontrolli tunnisti Windows Live Mail – ohjelman ja antoi sen toimia kuten sen pitääkin, ilman ylimääräisiä ilmoituksia käyttäjälle.

Ensimmäiseen tutkimuskysymykseen vastauksia etsiessäni havainnoin toki muitakin asioita näistä kolmesta palomuurista. Sellaisiakin joita en edes varsinaisesti tutkinut. Näistä on syytä mainita erityisesti Windows 7 palomuurin erittäin hyvä ominaisuus jolla saa helposti napin painalluksella palautettua oletusasetukset sekä oletuspalomuurisäännöt. Tämä pienentää kynnystä tehdä itse uusia palomuurisääntöjä ja sitä kautta oppia koko ajan lisää palomuurista, kun aloitustilanteen voi aina helposti palauttaa. Vastaava mutta toisensuuntaisen havainnon tein Comodo palomuurista. Siinä itse tehdyn palomuurisäännön/sääntöjen jälkeen palomuurin palauttaminen alkutilanteeseen ei todellakaan ollut näin helppoa. Toki myös Windows 7 palomuurin eduksi voi mainita sen tosiseikan, että sitä ei tarvitse erikseen asentaa, koska se kuuluu osana Windows käyttöjärjestelmään ja sen voi ottaa käyttöön napin painalluksella.

Toisessa tutkimuskysymyksessä ensimmäinen asia oli etsiä vastauksia tutkittavien palomuurien lokinkirjoituksen oletusasetuksiin, konfiguroitavuuteen sekä itse lokinkirjoitukseen. Kaikissa kolmessa palomuurissa oli mahdollista saada lokia muodostumaan monipuolisesti vaikka lokia ei välttämättä oletuksena kirjoitettukaan, kuten esimerkiksi Windows 7 palomuurin kohdalla oli. Windows 7 palomuurin lokista on syytä mainita myös se, että sitä ei voinut ollenkaan tyhjentää, kuten Comodon kohdalla oli mahdollista tehdä vaan sitä kontrolloitiin lokitiedoston

maksimikoon asettamisella. Windows 7 palomuurin eduksi on kuitenkin sanottava, että vaikka sen lokitiedosto ja sen lukeminen ei ollut kovinkaan käyttäjäystävällistä, niin sen ainoa lokitiedosto kuitenkin antoi varsin monipuolista tietoa palomuurin liikenteestä. Windows 7 palomuuri siis muodosti vain yhtä lokitiedostoa, kun F-Secure sekä Comodo tuottivat useaa eri lokia, jopa oletuksena. Comodolla oli oma loki palomuurille ja oma sovelluskontrollille. Lokin keräysasetusten konfigurointi kuitenkin oli melko epäselvää ja muutosten teko haastavaa. Loki sinällään oli myös monipuolista ja erittäin hyvä asia oli, että sen sai halutessaan tyhjennettyä kokonaan. F-Secure oli lokinkirjoitusominaisuuksiltaan mielestäni paras palomuuri. Siinä oli normaalien lokien lisäksi käytettävissä niin sanottu pakettiloki. Tämä erikseen päälle laitettava ja myös monipuolinen loki on erittäin käyttökelpoinen uusia palomuurisääntöjä laadittaessa. F-Securen pakettilokin sai päälle vain käyttäjän toimesta, joten sillä saattoi helposti tallettaa lokille ongelman aiheuttaneen tilanteen toistamalla sen pakettilokinkirjoituksen ollessa päällä. Pakettilokiin muodostui merkinnät sekä sisään, että ulospäin tapahtuneesta liikenteestä.

Toisen tutkimuskysymyksen toinen osa oli tehdä muutamia käytännön testejä, joilla saatiin lisäkokemusta lokinkirjoituksesta sekä havaintoja simuloidusta hakkeriliikenteestä. Windows Update ja verkkopankki – testeistä tehtyjen lokihavaintojen perusteella F-Securen lokinkirjoitus oli edelleen ensiluokkaista. Kaikki palomuurit tekivät näissä testeissä paljon lokia, mutta Comodo palomuurissa piti itse luoda erikseen lokinkirjoitukseen sääntö, jotta lokia sai näistä testeistä muodostumaan. Windows 7 palomuurin loki taasen oli vähemmän selkeää kuin F-Securen. F-Securen ensiluokkaisuutta perustelen muun muassa sillä, että sen lokissa oli erikseen myös ”description” eli ”kuvaus” – kenttä, joka kertoi tekstimuodossa mitä missäkin lokin kohdassa oli tapahtunut. Kaikkien palomuurien kohdalla sekä Windows Update – tarkastuksesta että verkkopankkiin kirjautumisesta jäi kaikesta huolimatta asianmukaiset lokimerkinnät eli siinä suhteessa eroavaisuuksia ei ollut. Kuten aiemmin mainittu, toisilla palomuureilla ne vaan olivat hieman sekavammat kuin toisilla ja yhdessä palomuurissa (Comodo) piti itse tehdä toimenpiteitä, että loki saatiin aikaiseksi.

Viimeisenä osana toista tutkimuskysymystä simuloin siis Nmap – porttiskannerilla hakkeriliikennettä tutkittavia palomuureja vastaan. Windows 7 sekä Comodo palomuuri antoivat tulokset että kaikki portit ovat joko kiinni tai niiden tilaa ei voida selvittää. Molempien kohdalla tämä oli todennettavissa myös lokeista. F-Secure sen sijaan näytti, että 6 porttia olisi auki ja loput 994 skannatusta tuhannesta portista olisivat kiinni tai selvittämättömiä (katso kuvio 30). Myös F-Securen loki tuki tätä Nmap – porttiskannerin antamaa tulosta. Kun selvitin, että kaikki nämä kuusi auki ollutta porttia olivat Windows käyttöjärjestelmän toimintaan liittyviä

portteja, saatoin todeta että myös F-Secure oli tietoturvamielessä toimiva palomuuri. Näiden tekemieni testien perusteella tietoturva oli kaikissa palomuureissa kohdallaan eikä testattuja palomuureja voi laittaa järjestykseen sen perusteella, että joku olisi vähemmän luotettava kuin toinen.

8.1 **Suositukset**

Tutkimuksen perusteella minulle muodostui hyvin selkeä kuva näistä kolmesta palomuurista. Ensimmäisenä totean ja haluan korostaa, että näillä testeillä mitattuna kaikki kolme ovat siis tietoturvamielessä luotettavia eikä ole syytä epäillä, että vääränlaista liikennettä pääsisi kannettavaan tietokoneeseen, jossa on joku näistä palomuureista käytössä. Toki aina pitää olla tarkkana ja suuri osa tietoturvaa on lopulta kuitenkin käyttäjän vastuulla. Myös palomuurin lokeja on tarpeellista tutkia aika ajoin, kuten työssäni aiemmin on tuotu esille.

Windows 7 palomuuri sekä F-Securen palomuuri olivat mielestäni kokonaisuutta katsoen käyttäjäystävällisempiä kuin Comodo, jonka käyttöliittymä oli tietyllä tapaa sekava ja monimutkainen. Comodo kuitenkin ainoana täysin ilmaisena palomuurina on hyvä edistyneemmälle käyttäjälle, joskin sen tarjoamat lisäominaisuudet olivat turhia tai maksullisia. Windows 7 palomuuri on selkeä ja helppokäyttöinen vaikkakin lokin lukeminen on ehkä hieman hankalaa ainakin aluksi. F-Secure kirjoittaa useaa eri lokia, mutta niitä on helppo lukea.

Kuten mainittu, tutkimukseni aikana F-Secure julkaisi uudemman version F-Secure Internet Security – tuotteestaan ja siinä ei enää ollut omaa palomuuria ollenkaan. F-Secure on siis siirtynyt käyttämään Windowsin palomuuria ja ohjaamaan sitä omalla käyttöliittymällään. Nopea vilkaisu F-Securen kilpailijoiden tuotteisiin osoitti, että tämä on palomuurien nykysuunta, eli myöskään esimerkiksi Norton ei käytä enää omaa palomuuria, vaan on tehnyt uusimmassa versiossaan samanlaisen ratkaisun. Viimeistään tämän perusteella voidaan todeta, että Windowsin oma palomuuri on luotettava ja suositeltava kun tietoturva-alan suuret yrityksetkin luottavat siihen omien tuotteidensa käytössä.

Suositukseni näistä kolmesta vertaillusta palomuurista kohdistuu täten Windows 7 Enterprise käyttöjärjestelmän mukana tulevaan palomuuriin, joka on kokonaisvaltaisesti katsottuna paras. Käyttäjälle, joka ei halua palomuurilta kuin varman suojan uhkia ja haitallisia yhteyksiä vastaan, se on riittävä palomuuri. Lisäksi edistyneemmälle käyttäjälle siinä on riittävästi mahdollisuuksia konfiguroida lokinkirjoitusta sekä tutkia sitä. Erityisesti pidin Windows 7 palomuurin ominai-

suudesta jolla sai helposti palautettua palomuurin oletusasetukset. Kun vielä lisäksi mainitaan sen toimiva sovelluskontrolli, joka ei vaadi käyttäjältä turhia toimia, on suositukseni perusteltu.

Lähteet

CERT-FI – Vaihda salasanasi vahvempiin. Luettavissa: https://www.cert.fi/tietoturvanyt/2011/11/ttn201111141503.html. Luettu: 20.02.2012

Comodo Firewall – Palomuurin lataussivu. Luettavissa: http://personalfirewall.comodo.com/free-download.html. Luettu: 06.04.2012

Comodo – Comodo Internet Security Help http://help.comodo.com/topic-72-1-284-2945-Defense+-Tasks---Introduction.html. Luettu: 23.05.2012

F-Secure Internet Security 2012 – Kokeile ilmaiseksi. Luettavissa: http://www.f-secure.com/fi/web/home_fi/protection/internet-security/trial. Luettu: 23.04.2012

Järvinen P. 2002. Tietoturva & yksityisyys. 2. painos. Docendo Finland Oy. Jyväskylä.

Korpela J. 2005. Kodin tietoturvaopas. 1. painos. Docendo Finland Oy. Jyväskylä.

Microsoft Windowsin palomuuri – Windows 7 ominaisuudet. Luettavissa: http://windows.microsoft.com/fi-FI/windows7/products/features/windows-firewall. Luettu 25.04.2012

Panko R. 2010. Corporate Computer and Network Security. 2. painos. Pearson Education Inc. New Jersey.

Saunalahti – Holvi backup. Luettavissa: http://isog.pp.fi/holvi.html. Luettu 25.09.2011.

Staples Finland Oy – Näyttöjen tietoturvasuojat. Luettavissa: http://www.lindell.fi/?id=129. Luettu: 22.09.2011.

Tietoturvaopas – Tietoturvaohjelmat. Luettavissa: http://www.tietoturvaopas.fi/ohjelmatjayhteydet/tietoturvaohjelmat.html. Luettu: 13.06.2011.

TrueCrypt – Beginner's Tutorial. Luettavissa: http://www.truecrypt.org/docs/. Luettu 22.09.2011.

Uski J. 2008. Turvaa perintösi jälkipolville. MicroPC 2008/12. s. 24-27.

VisioLink Oy – Datalaitteiden lukitus. Luettavissa: http://www.visiolink.fi/lukitus.htm. Luettu 22.09.2011.