Opinnäytetyö (AMK)

Tietojenkäsittelyn koulutusohjelma

Yrityksen tietoliikenne ja tietoturva

2014

Hannu-Pekka Leukumaa

KESKITETYN VIRUSTORJUNNAN TOTEUTTAMINEN F-SECURE POLICY MANAGERILLA

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittelyn koulutusohjelma | Yrityksen tietoliikenne ja tietoturva

Kesäkuu 2014 | 37 sivua

Esko Vainikka

Hannu-Pekka Leukumaa

KESKITETYN VIRUSTORJUNNAN TOTEUTTAMINEN F-SECURE POLICY MANAGERILLA

Tämän opinnäytetyön tarkoituksena on kehittää Turun ammattikorkeakoulun Lemminkäisenkadun toimipisteen laboratorioverkon tietoturvaa. Lisäksi tavoitteena on saada lukijalle tietoa virustorjunnan välttämättömyydestä ja keskitetyn virustorjunnan hyödyllisyydestä. Opinnäytetyössä tutustutaan sekä teorian että käytännön avulla virustorjuntaan ja sen keskitettyyn hallintaan.

Työn teoriaosuus koostuu virustorjunnan perusteista sekä sen keskitetyn hallinnan esittelemisestä. Keskitetty hallinta ja keskitetty virustorjunta muodostavat työn tietoperustan, joka tukee soveltavaa osuutta.

Soveltavassa osuudessa asennettiin keskitetysti hallitut virustorjuntaohjelmistot verkon tietokoneisiin. Ohjelmistojen asennuksia ja järkevää ylläpitoa varten tehtiin keskitetylle hallinnalle vaatimusmäärittelyn pohjalta kohdeympäristöön sopiva rakenne. Asennukset toteutettiin käyttämällä F-Securen keskitetyn hallinnan työkalua, Policy Manageria.

F-Secure Policy Managerilla on tarkoituksena jatkossa huolehtia ympäristön virustorjunnan ylläpidosta samalla parantaen merkittävästi verkon tietoturvaa. Lisäksi sillä voidaan pienentää järjestelmänvalvojan työtaakkaa virustorjunnasta huolehtimisessa.

ASIASANAT:

Keskitetty hallinta, virustorjunta, virustorjuntaohjelmisto.

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Techology | Business Data communications and Information Security

June 2014 | 37 pages

Esko Vainikka

Hannu-Pekka Leukumaa

REALIZATION OF CENTRALIZED MANAGEMENT FOR ANTIVIRUS SOFTWARE WITH F-SECURE POLICY MANAGER

The objective of the present Bachelor's thesis is to improve the information security of Turku University of Applied Sciences' laboratory network in the Lemminkäisenkatu campus. In addition, this thesis aims to add to the reader's understanding of the indispensability of antivirus management and the usefulness of centralized management for antivirus software. The thesis explores antivirus software and centralized management for antivirus software both from the perspective of theory and practice.

The theoretical part consists of the basics of antivirus protection and an introduction to centralized management. Centralized management and centralized antivirus protection constitute a large part of the theory, which supports the empirical part of the thesis.

In the empirical part, centrally managed antivirus software was installed on network computers. A suitable organization for the target environment of centralized management was made based on the requirements specification and for the installation of software and administration of the network. The installations were executed with Policy Manager, F-Secure's tool for centralized management.

In the future, the aim of F-Secure Policy Manager is to take care of the administration of environment's antivirus software, while substantially improving the information security of the network and decreasing the resources needed for taking care of the antivirus.

KEYWORDS:

Centralized management, antivirus, antivirus software.

SISÄLTÖ

LIITTEET

KUVAT

1 JOHDANTO

Tämä opinnäytetyö tehdään Turun ammattikorkeakoulun toimeksiannosta. Opinnäytetyön tarkoituksena on tutustua keskitettyyn virustorjuntaan ja samalla asentaa se Lemminkäisenkadun toimipisteen laboratorioverkkoon. Tavoitteena opinnäytetyössä on, että sen luettuaan ymmärtäisi virustorjunnan välttämättömyyden ja keskitetyn virustorjunnan hyödyllisyyden. Opinnäytetyöhön on kirjoitettu F-Secure Policy Managerista kattava paketti, joka kattaa melko yksityiskohtaiset ohjeet asennuksesta käyttöönottoon. Valmista opinnäytetyötä voi siis käyttää apuna asennettaessa keskitettyä virustorjuntaratkaisua samantyyppiseen verkkoon.

Keskitetty virustorjunta on nykypäivänä yrityksille ja organisaatioille tärkeä tietoturvan apuväline. Se tarjoaa mahdollisuuden hallinnoida kaikkia työasemia kerralla, jolloin ylläpitäjän ei tarvitse käydä paikallisesti joka koneella päivittämässä ja tarkastamassa virustorjunnan tilaa. Ilman keskitettyä virustorjunnan hallintaa ylläpito ei välttämättä ehdi tehdä kaikkia virustorjuntaan liittyviä asioita, mikä heikentää verkon virustorjuntaa.

Koulun laboratorioverkko on nimeltään Labraverkko ja se on erillään Turun ammattikorkeakoulun omasta Windows-verkosta. Labraverkko on käytössä muutamassa luokassa ja tutkimusprojektissa. Opinnäytetyössä Labraverkkoon asennetaan F-Secure Policy Manager, joka on keskitetyn tietoturvan hallintatyökalu. Työ aloitetaan tekemällä vaatimusmäärittely, jolla selvitetään, mitä Policy Managerilta halutaan ja mihin kaikkialle se Labraverkossa ulotetaan.

Opinnäytetyön tutkimusote on konstruktiivinen tutkimusote, jonka lopputuloksena on toimiva ratkaisu dokumentteineen. Ominaista konstruktiiviselle tutkimukselle on tiivis vuoropuhelu käytännön ja teorian välillä (Lukka 2014). Opinnäytetyössä kuvataan työn eri vaiheet lähtötilanteesta ohjelmiston käyttöönottoon. Opinnäytetyössä kerrotaan, mitä on tehty ja perustellaan käytetyt valinnat. Työn aikana tein paljon "mitä mistäkin napista tapahtuu" -kokeiluja, koska en ole aiemmin käyttänyt kyseessä olevaa ohjelmaa. F-Secure Policy Managerin asen-

nuksessa ja konfiguroinnissa käytetään apuna F-Securen Policy Manager Administrator’s guidea. Lisäksi saan apua työhön haastattelemalla ammattikorkeakoulun IT-vastaavia. Omien kokeilujen ja haastatteluiden perusteella selvitetään parhaat ratkaisut kohdeympäristön asennukseen.

2 VIRUSTORJUNNAN PERUSTEET

2.1 Haittaohjelmat

Virukset ovat haittaohjelmia, kuten myös madot, troijalaiset ja vakoiluohjelmat. Haittaohjelmat saastuttavat tietokoneita ja järjestelmiä. Ne voivat muun muassa kerätä tietokoneilta tärkeitä tietoja ja käyttää tietokonetta levittämään roskapostia. Ne voivat myös aiheuttaa vahinkoa tietokoneelle tai järjestelmälle, esimerkiksi rikkomalla tietokoneen tai hidastamalla sen käyttökelvottomaksi. (Tietoturvaopas 2014a.) Viruksia ja haittaohjelmia tekevät ohjelmoijat etsivät koko ajan uusia tapoja tunkeutua tietokoneisiin ja järjestelmiin. Samaan aikaan virustorjuntayritykset ja niiden virusanalyytikot yrittävät tunnistaa haittaohjelmia ja löytää keinoja paikata niiden aiheuttamat tai hyödyntämät tietoturva-aukot.

Haittaohjelmien jaottelu on vaikeaa ja termistöstä on monia versioita, koska yleistä yhteisymmärrystä ei kaikista termeistä ole. Eri haittaohjelmissa esiintyy myös paljon päällekkäisyyksiä. Haittaohjelmat voidaan jakaa eri ryhmiin sen perusteella, tarvitseeko se isäntäohjelman vai toimiiko se itsenäisenä ohjelmana, ja onko ohjelma replikoituva vai ei. (Stallings & Brown 2008, 216.) Haittaohjelmat on jaoteltu eri kategorioihin liitteessä 4 olevassa taulukossa.

Termi virustorjunta on hieman harhaanjohtava, koska nykyiset virustorjuntaohjelmistot sisältävät komponentit muidenkin haittaohjelmien torjuntaan. Siksi käytänkin opinnäytetyössäni termejä virus ja virustorjunta tarkoittaen haittaohjelmia ja niiden torjuntaa.

Melkein kaikki yleisimmät haittaohjelmat voi torjua nykypäivän virustorjuntaohjelmistoilla. Jos verkkoon on lisäksi asennettu vielä erillinen palomuuri, on verkon käyttäminen jo melko turvallista. Myös Windowsin oman palomuurin voi pitää päällä, jolloin erillistä palomuuriohjelmistoa ei yksittäisille tietokoneille tarvita. Palomuurin asetuksia voi tarvittaessa muokata, mutta sitä ei tarvitse kokonaan ottaa pois käytöstä. Esimerkiksi opinnäytetyöni aikana Windowsin palomuuri aiheutti päänvaivaa useita kertoja, mutta ongelmista selvittiin konfiguroimalla palomuurin asetuksia tai sammuttamalla se hetkellisesti.

Pitää kuitenkin aina muistaa, että täydellistä suojausta viruksia ja haittaohjelmia vastaan ei ole eikä tule. Ideaalitilanne olisi, että virukset eivät pääsisi järjestelmään vaan ne torjuttaisiin ennen tartuntaa. Tuo tilanne on kuitenkin käytännössä mahdotonta saavuttaa, koska virukset ovat askeleen edellä antivirusohjelmia. Reaaliaikainen virustorjunta (ennaltaehkäisy) voi kuitenkin huomattavissa määrin vähentää virushyökkäyksiä. Virustorjuntaohjelmistojen valmistajilla onkin reaaliaikaisesti viruksia torjuvia komponentteja ohjelmistoissaan ja niitä kehitetään koko ajan, koska tietokantapohjainen virustorjunta ei voi millään pysyä virusten kanssa samassa vauhdissa. (SearchSecurity 2014.) Ennaltaehkäisyn jälkeen seuraavaksi paras lähestymistapa on viruksen paikallistaminen tietokoneelta tartunnan jälkeen, viruksen identifiointi ja viruksen poisto kaikkialta järjestelmästä. Tähän pystyy uusimmat virustietokantapäivitykset saanut virustorjuntaohjelmisto sen jälkeen, kun viruksen tiedot on saatu virustietokantaan. (Stallings & Brown 2008, 226-227.) Nykyisin virukset saadaan tietokantoihin nopeasti ja tietokannat päivittyvätkin jopa useita kertoja päivässä. Osoitteesta http://www.f-secure.com/dbtracker/ näkee F-Securen virustietokannan viimeisimmät päivitykset.

2.2 Tausta virustorjuntaohjelmistojen synnylle

Vuosien kuluessa virusten tekijöiden tavoitteet ovat muuttuneet. Aikaisemmin viruksen tekijät saattoivat haluta vain pilailla, tai kuten maailman ensimmäisen PC-viruksen ”Brainin” tapauksessa, suojata tuotettaan piratismilta. Virus latautui, kun laiton kopio ohjelmasta käynnistettiin. (Mentalfloss 2013.) Virukset saattoivat olla vain näyttöön ilmestyviä kuvia tai jotain muuta kohtuullisen harmitonta, mutta ne paljastivat paljon vahingollisemman toiminnan uhkat. Viruksia alkoivat tehdä entistä useammat ja ne kehittyivät samassa tahdissa tietokoneverkkojen kanssa. (Norton Advisor 2014.) ”Pilailuviruksia” esiintyy edelleen, mutta yhä lisääntyvät toimijat tuovat mukanaan myös uusia tarkoitusperiä.

Tietoturvaohjelmistot ja niiden päivittäminen nousivat tietokoneiden verkottumisen myötä paljon tärkeämmiksi kuin aikaisemmin. Kun tietokoneet verkottuvat ja ovat siten yhteydessä toisiinsa, haittaohjelmatkin pääsevät leviämään huomattavasti nopeammin kuin esimerkiksi levykkeiden mukana. (Norton Advisor 2014.)

2.3 Käyttöjärjestelmän ja sovellusohjelmien päivitys

Suuri osa tietokoneiden tietoturvasta tulee muuta kautta kuin tietoturvaohjelmistojen mukana. Haittaohjelmat hyödyntävät käyttöjärjestelmän ja ohjelmistojen tietoturva-aukkoja, minkä vuoksi niidenkin päivittäminen on todella tärkeää. Käyttöjärjestelmän ja ohjelmistojen päivitykset sisältävät paljon tietoturva-aukkojen korjauksia. Virustorjunta on periaatteessa vain lisäapuna estämässä ja ennakoimassa haittaohjelmien liikkeitä.

3 KESKITETTY HALLINTA: TAUSTA JA OHJELMISTOT

Tässä luvussa kerrotaan keskitettyjen hallintatyökalujen taustasta ja synnystä, ja esitellään muutama Microsoftin keskitetyn hallinnan palvelu. Opinnäytetyön aiheena on keskitetty virustorjunta, joten siinä keskitytään tietoturvayritysten tarjoamiin keskitettyihin ratkaisuihin selvittämällä F-Secure Policy Managerin keskeisimmät ominaisuudet ja vertailemalla sitä hieman kilpailijoiden tarjoamiin ohjelmistoihin.

3.1 Ohjelmistojen tausta

Tietokoneiden verkottuminen mahdollisti keskitettyjen ratkaisujen käytön tietokoneiden hallinnassa. Kun käyttöjärjestelmien päivitykset ja ylläpito voidaan hoitaa kätevästi keskitetysti, automaattisesti ja kustannustehokkaasti, olisi niiden hoitaminen hitaasti jokaisella koneella yksitellen ajan- ja rahanhukkaa. Myös tietoturvayritykset tarjoavat keskittyä hallintaa pitämään ohjelmistonsa ajan tasalla, minkä lisäksi ne tarjoavat nykyisin muidenkin osapuolten ohjelmistojen päivitysten hallintaa.

3.2 Microsoftin keskitetyt ratkaisut järjestelmänhallinnalle

SCCM

Microsoftin System Center Configuration Manager eli SCCM -järjestelmänhallintatuotteella voi keskitetysti hallita suuria ryhmiä tietokoneita. Sen ominaisuuksiin kuuluvat etähallinta, päivitysten hallinta, ohjelmistojen jakelu, käyttöjärjestelmien jakelu sekä laitteisto- ja ohjelmistoinventaario. (Microsoft 2014a.)

WSUS

WSUS (Windows Server Update Service) on myös Microsoftin palvelu. Se on ilmainen päivitystenhallintatyökalu, jota voi käyttää Windows Server -käyttöjärjestelmillä. WSUS lataa päivitykset Windows Update -palvelusta ja tämän jälkeen jakaa ne verkon tietokoneille. (Microsoft 2014b.)

Kuten luvussa 2 kerrottiin, käyttöjärjestelmän ja sovellusohjelmien päivittäminen on iso osa tietoturvaa. Keskitetty hallinta parantaa tietoturvaa mahdollistaen nopeat päivitykset koko organisaation verkon tietokoneisiin kerralla.

Group Policy

Group Policy on Microsoftin keskitetyn hallinnan työkalu Active Directory -ympäristössä. Sen avulla voi konfiguroida tietokoneiden käyttöjärjestelmää mahdollistaen erilaisia spesifioituja asetuksia eri ryhmien tietokoneille ja/tai eri ryhmien käyttäjille. (Microsoft 2014c.)

3.3 F-Secure Policy Manager

Tässä luvussa esitellään lyhyesti F-Secure Policy Manager. Opinnäytetyön soveltavassa osuudessa tutustutaan tarkemmin Policy Managerin ominaisuuksiin, kun Turun ammattikorkeakoulun laboratorioverkkoon asennetaan ja konfiguroidaan F-Secure Policy Manager Server ylläpitämään tietokoneiden tietoturvaohjelmistoa, F-Secure Client Securityä.

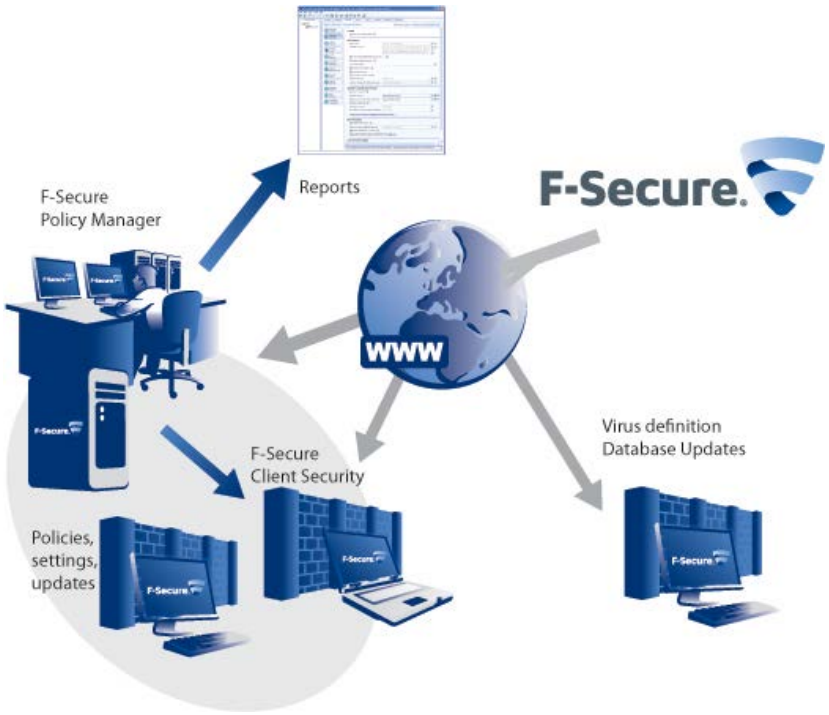
F-Secure on tietoturvaratkaisuja ja pilvipalveluja tarjoava suomalainen yritys. F-Secure mainostaa kotisivuillaan olleensa ensimmäinen keskitetyn hallinnan tietoturva-alalle tuonut yritys (F-Secure 2014a). Jo pitemmän aikaa kaikki suurimmat tietoturvayritykset ovat tarjonneet keskitettyjä palveluja. Kun tietoturvayritykset myyvät tietoturvaohjelmistoja yrityksille, puhutaan yleisesti keskitetystä tietoturvasta tai ainakin kyseinen palvelu kattaa sen.

F-Secure Policy Managerin keskeisimpiä ominaisuuksia ovat automaatio, Microsoft Active Directoryn toisinto, tuki useille käyttäjille ja Software Updater (F-Secure 2014a):

- Automaation avulla säästetään aikaa, joka voidaan käyttää tärkeämpiin tietoturva-asioihin, kun Policy Manager käsittelee automaattisesti päivittäiset toiminnot kuten uusien verkkoasemien tuonnin ja tarpeettomien poiston (F-Secure 2014a).
- Active Directoryn toisinto selkeyttää rakenteen ymmärtämistä, kun se on samanlainen kuin muuallakin verkossa.
- Policy Managerissa on tuki useille eri käyttäjille, joilla kaikilla on omat käyttöoikeutensa. Admin-käyttäjä voi esimerkiksi antaa käyttäjälle oikeudet koko Policy Manager Serverin hallintaan tai vain tiettyihin sen rakenteen osiin. (F-Secure 2014a.)
- Software Updater mahdollistaa Windowsin ja kolmansien osapuolten ohjelmistojen kuten mm. Javan, Adobe Flashin, OpenOfficen ja monien muiden yleisessä käytössä olevien ohjelmistojen päivitysten tarkastamisen ja päivittämisen (F-Secure 2014e, 4).

Tämän keskitetyn hallinnan työkalun keskeisiä ominaisuuksia on myös monipuolinen raportointi ja skaalautuvuus pienyrityksistä suuryrityksiin. Lisäksi Policy Managerin kautta voi hoitaa ohjelmistojen jakelut työasemiin ja palvelimiin sekä tietoturvakäytäntöjen välityksen niihin. Kaikki tapahtuu keskitetysti Policy Managerin käyttöliittymän, Consolen, kautta. (F-Secure 2014d.)

Kuvassa 1 on esitetty Policy Managerin toimintaperiaate tämän opinnäytetyön tasolla. Hallinnan piiriin kuuluu ainoastaan Windows-koneita. Kuvassa näkyy vain yksi F-Secure Policy Manager -yksikkö, mutta lopullisessa toteutuksessa se jakaantuu kahteen komponenttiin: F-Secure Policy Manager Serveriin ja F-Secure Policy Manager Consoleen, jolta hallitaan Policy Manager Serveriä. Policy Manager Serveriä voi hallita paikallisesti myös palvelinkoneelta, jos siihen on asennuksen yhteydessä asennettu myös Policy Manager Console, tai etänä samassa verkossa olevalta koneelta, johon on asennettu erikseen F-secure Policy Manager Console.



Kuva 1. F-Secure Policy Managerin toiminta (Abacus 2014).

3.4 Kilpailijat

Kaikilla suurimmilla kaupallisilla tietoturvaohjelmistojen valmistajilla on keskitetyn hallinnan ratkaisuja. Eroavaisuudet eri valmistajien ohjelmistojen välillä ovat pieniä ja jokaista palvelua mainostetaan minuuteissa asennetuksi. Tietoturvayrityksille keskitetty hallinta on yksi yrityksen tietoturvan osa-alue ja eritasoiset ratkaisut yrityksille sisältävätkin keskitetyn hallinnan työkalun. Muun muassa F-Securen Business Suite sisältää Policy Managerin. Valittavana ovat tuotteet pienille ja suuremmille yrityksille. Ratkaisu voi olla erillinen palvelimelle asennettu palvelu, jolta jaetaan tietoturvakäytäntöjä verkon koneille oman käyttöliittymän kautta (F-secure Policy Manager) tai kuten Kaspersky Small Office Security, joka sisältää Management Consolen samassa paketissa muiden tuotteiden kanssa. Seuraavassa on listattuna isoimpien kilpailijayritysten keskitettyjä virustorjuntaratkaisuja.

- **Symantec.** Endpoint Protection Family. Tuetut käyttöjärjestelmät ovat Windows, MAC ja Linux. (Symantec 2014.)

- **Kaspersky.** Endpoint security. Pienemmille yrityksille tarkoitettu ohjelmisto kulkee nimellä Small office security. (Kaspersky 2014.)

- **McAfee.** McAfee ePolicy Orchestrator. Skaalautuu kaikenkokoisiin yrityksiin. (McAfee 2014.)

Selaillessa eri tietoturvayritysten sivuja voi tuskastua helposti. Tuotteita on todella paljon ja kaikilla on omia nimityksiään eri suojauksille. Kaikki myös mainostavat olevansa helppokäyttöisiä ja nopeita ottaa käyttöön. En tässä työssä kuitenkaan vertaile näitä tuotteita keskenään. Halutessaan mahdollisimman yksinkertaisen ja kustannustehokkaan ratkaisun omalle yritykselleen, pitää ensin määrittää, mitä haluaa suojata ja kuinka paljon suojattavia kohteita on. Tämän jälkeen voi katsoa esimerkiksi internetistä eri ohjelmistojen käyttövideoita, koska niistä saa hyvän kuvan kyseisistä tuotteista.

4 KESKITETTY VIRUSTORJUNTA LABRAVERKOSSA

4.1 Taustaa ja lähtötilanne

Labraverkko

Labraverkkoa käytetään opetuskäyttöön eri opintojaksoilla, jolloin voidaan testata tietokoneita ja niiden tietoturvaa suljetussa ympäristössä vaarantamatta koulun pääverkon tietoturvaa. Se on siis erillään ammattikorkeakoulun Windows-verkosta. Labraverkkoon kuuluvat kahden luokkahuoneen (B155 ja B162) tietokoneet, sekä WISE-projektin, Kansalaisen mikrotuen ja Bio-alojen käytössä olevat tietokoneet. Kuvassa 2 on kuvattu Labraverkko.

Kuva 2. Labraverkko (Lampikoski 2014). (SALATTU)

Labraverkko on kokenut paljon muutoksia: AD-verkkoa on yksinkertaistettu, virustorjunnat ovat vaihtuneet, palomuuri on vaihtunut ja verkkokytkimiä on vaihdettu. Eri tilat on eriytetty omiin virtuaali-LANeihin, mikä helpottaa verkon seu-

raamista ja samalla ne eivät pääse häiritsemään toisiaan. Labraverkkoa on selkeytetty paljon. Tällä hetkellä myös muita opiskelijoita on tekemässä opinnäytetöinä siihen liittyviä kehitystöitä, joihin kuuluvat mm. verkon parantaminen ja tietoturvan kehitys sekä samalla sen hallinnoinnin ja päivitysten asentamisen helpottaminen. Nämä parannukset sisältävät mm. WSUS:n, SCCM:n ja Group Policyn käyttöönoton sekä tämän opinnäytetyön yhteydessä F-Secure Policy Managerin asennuksen ja testaamisen.

Labraverkon virustorjuntana oli ennen opinnäytetyön aloittamistakin F-Secure Client Security eli sama sovellus, joka siinä tulee olemaan myös tämän opinnäytetyön jälkeen. Tällä hetkellä jokaisella tietokoneella on kuitenkin itsenäinen Client Security-ohjelmisto, eli ohjelmisto- ja viruspäivitykset pitää hoitaa jokaisella tietokoneella paikallisesti.

4.2 Vaatimusmäärittely

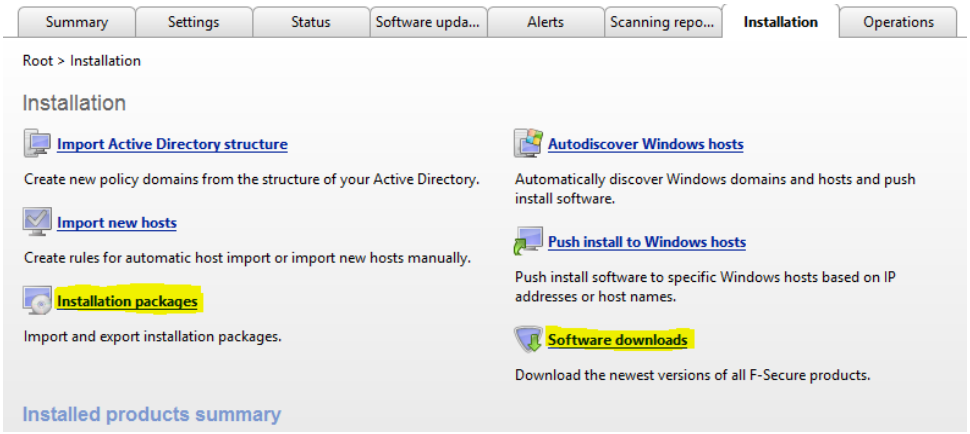
Tässä luvussa kerrotaan, mitä opinnäytetyöllä halutaan saavuttaa, mihin vaatimuksiin sen pitää vastata ja mitä rajauksia tehdään.

Tässä opinnäytetyössä tavoitteena on helpottaa Labraverkon virustorjunnan hallinnointia asentamalla siihen F-Securen keskitetty tietoturvan hallintatyökalu. F-Secure Policy Manager pitää huolen siitä, että tietokoneet saavat viimeisimmät ohjelmisto- ja virustietokantapäivitykset nopeasti ja vaivattomasti. Keskitetyn virustorjunnan mukana verkon kuormitus vähenee ja tiedonsaanti ja tietoturva paranevat. Järjestelmänvalvojan ei tarvitse enää huolehtia erikseen jokaisen tietokoneen virustorjunnasta, vaan kaiken voi tehdä etänä ja keskitetysti.

Keskitettyä virustorjuntaratkaisua ei ole tarkoitus toteuttaa koko Labraverkkoon, vaan sitä rajataan hieman tarpeen mukaan. Alustava rajaus koski ainoastaan Bio-alojen käytössä olevia tietokoneita, joita järjestelmänvalvoja ei halunnut ottaa mukaan toteutukseen. Niinpä keskitetyn virustorjunnan haluttiin kattavan luokkahuoneiden B155 ja B162, KMT:n ja WISE-projektin koneet. Se rajasi tietokoneiden määrän noin 50 koneeseen.

Ympäristön lisäksi rajaus tehdään käytettäviin ohjelmistoihin. Labraverkon koneet ovat pääasiassa Windows-koneita, lukuun ottamatta muutaman opettajan käyttämää Mac-kannettavaa ja KMT:n yhtä Linux-konetta. Opinnäytetyössä ei oteta huomioon Mac-tietokoneita, koska F-Secure Policy Manager ei niitä tue. Tässä asiassa suurimpien kilpailijoiden ratkaisut olisivat olleet parempia, koska ne tukevat Mac-tietokoneita. Myöskään Laboratorioverkon palvelimiin ei ainakaan vielä tehdä asennuksia. Vaatimuksena on siis asentaa tietokoneisiin haittaohjelmien torjunta, jota pystytään hallitsemaan keskitetysti. F-Securen tuotteilla on myös mahdollista pitää keskitetysti ajan tasalla käyttöjärjestelmät ja kolmansien osapuolten sovellukset (F-Secure 2014c), mutta Labraverkossa niiden päivittäminen hoidetaan ainakin toistaiseksi muuta kautta. Asennettavat ohjelmistot ovat F-secure Policy Manager, F-Secure Client Security ja F-Secure Linux Security. Opinnäytetyön soveltavan osuuden katsotaan olevan valmis, kun ohjelmistojen asennus on suoritettu ja toimivuus testattu.

F-Secure Client Securitystä on kaksi versiota, Standard ja Premium. Premium-versio sisältää Software Updater-ominaisuuden. Se tarkkailee sekä Windowsin että kolmansien osapuolten ohjelmistojen päivityksiä ja mahdollistaa niiden päivittämisen. Kuten aikaisemmin mainitsin, ominaisuutta ei toistaiseksi oteta käyttöön, joten asennuksessa käytetään Client Security Standardia. Myöhemmin järjestelmänvalvoja voi halutessaan asentaa Premiumin ohjelmistopäivityksenä kuten muitakin F-Securen tuotteita, jotka saa helposti ladattua suoraan Policy Manageriin ja asennettua sitä kautta koneille (Kuva 3).



Kuva 3. Ohjelmistojen lataukset Policy Managerista.

4.3 Testiympäristön luonti

Päätimme yhdessä järjestelmänvalvojan kanssa Policy Managerin olevan hyvä asentaa virtuaalikoneelle ja luoda sille testiympäristö luokkaan B155, ja sen jälkeen siirtää virtuaalikone tuotantopalvelimelle. Testiympäristöön luotiin aluksi virtuaalikoneita, joilla tutustuttiin Policy Managerin käyttöön. Sen jälkeen testiympäristöön tuotiin Labraverkon fyysisiä koneita. Alkuperäisenä tarkoituksena oli luoda testiympäristöön valmis Labraverkon Policy Manager -domainin rakenne eli lopulta testiympäristö ei siis olisi ollut testiympäristö vaan valmis ympäristö, joka olisi siirretty ESXi-palvelimelle ylläpidettäväksi. Asennusten jatkuessa kuitenkin selvisi, että testiympäristö on parempi pitää testiympäristönä ja tehdä asennus tuotantopalvelimelle alusta alkaen uudelleen. Ohjelman käytön opettelu ja siihen tutustuminen hoidettiin testiympäristössä ja sen jälkeen asennukset olikin helppo tehdä tuotantopalvelimelle.

Testiympäristö tehtiin B155-luokan tietokoneelle. Aloitin tarkistamalla, että tietokoneeseen on asennettu viimeisin VMware Workstation -ohjelmisto, eli versio 10. Ennen virtuaalikoneiden luontia on tarkistettava Policy Managerin Administrator’s guidesta järjestelmän minimivaatimukset Policy Manager -palvelimelle (Kuva 4).

Processor:	P4 2Ghz or multi-core 3GHz CPU, depending on the operating system and the size of the managed environment.
Memory:	1 - 2 GB RAM, depending on the operating system and the size of the managed environment.
Disk space:	6 - 10 GB of free disk space, depending on the size of the managed environment.
Network:	100 Mbit network.
Browser:	• Firefox 3.6 or newer

Kuva 4. Policy Manager Server -järjestelmän minimivaatimukset (F-Secure 2013, 9).

Virtuaalipalvelin

Kuvan 4 vaatimusten lisäksi Policy Manager Server vaatii tietysti myös käyttöjärjestelmän. Microsoft Windows-käyttöjärjestelmäksi käy käytännössä jokainen versio Windows Server 2003, 2008 ja 2012 -käyttöjärjestelmistä. Policy Manager Serverin voi asentaa myös useille Linux-jakeluille. Valitsin käyttöjärjestelmäksi Windows Server 2012 Standardin, sillä se on käyttöjärjestelmistä uusin ja olen käyttänyt sitä aikaisemminkin.

VMware Workstationilla luotiin virtuaalikone, johon asetettiin 2048 MB muistia ja 25 GB levytilaa. Virtuaalipalvelin on tarkoitus siirtää käyttöönotossa ESXi-palvelimelle, joten levytilaa luodessa valittiin ”split virtual disk into multiple files”. Se tarkoittaa virtuaalilevyn jakamista useiksi tiedostoiksi, mikä helpottaa siirtoa myöhemmin palvelimelle. Kun virtuaalikone oli luotu, asennettiin siihen Windows Server 2012 Standard Edition. Imagen sai ladattua Microsoft Dreamspark-palvelusta, josta opiskelijat saavat ladata tiettyjä Microsoftin ohjelmistoja käytettäväkseen. Asennuksessa valittiin palvelin käyttöliittymän kanssa. Asennus suoritettiin onnistuneesti loppuun.

Halusin liittää palvelimen heti Labraverkkoon, jotta pääsisin alusta asti kunnolla tutustumaan Policy Managerin ominaisuuksiin. Liittääkseni palvelimen Labraverkon domainiin, täytyi VMware Workstationin asetuksista palvelimen verkkokortti vaihtaa NATista ”sillattuun yhteyteen”. Näin VMware ei antanut minulle uutta IP-osoitetta vaan muodosti yhteyden suoraan Labraverkkoon. Liittääkseni palvelimen Labraverkon domainiin täytyi ohjauspaneelista valita ”System properties” -sivu ja sieltä vaihtaa tietokoneen nimi ja toimialueen jäsenyys. Nimesin tietokoneen FSPMsrv:ksi ja liityin laboratorioverkon toimialueeseen. Toimialueliitokseen tarvittiin toimialueen järjestelmänvalvojan oikeudet.

Client-koneet

Testiympäristöön tarvitaan tietenkin myös testikoneita, joihin asennetaan Policy Managerilla hallittava virustorjuntaohjelmisto. Päätin ainakin aluksi tehdä tes-

tiympäristöön kaksi Windows 7 -virtuaalikonetta, joihin asennuksia ja konfiguraatioita lähdetään tekemään. Asensin virtuaalikoneet ja niihin käyttöjärjestelmät, minkä lisäksi liitin virtuaalikoneet samalla tavalla toimialueeseen kuin virtuaalipalvelimenkin. Testiympäristön viimeisessä versiossa ei kuitenkaan käytetty kuin yhtä virtuaalikonetta. Laboratorioverkon suljetun ympäristön vuoksi pystyin ottamaan mukaan testiympäristöön myös fyysisiä koneita, joilla pystyi testaamaan ympäristön toimivuuden. Testiympäristössä oli lopulta kaksi B155-luokan konetta ja yksi virtuaalikone, kaikki Windows 7 käyttöjärjestelmällä varustettuina.

5 F-SECURE POLICY MANAGER: ALKUTOIMET JA TUTUSTUMINEN OHJELMISTOON

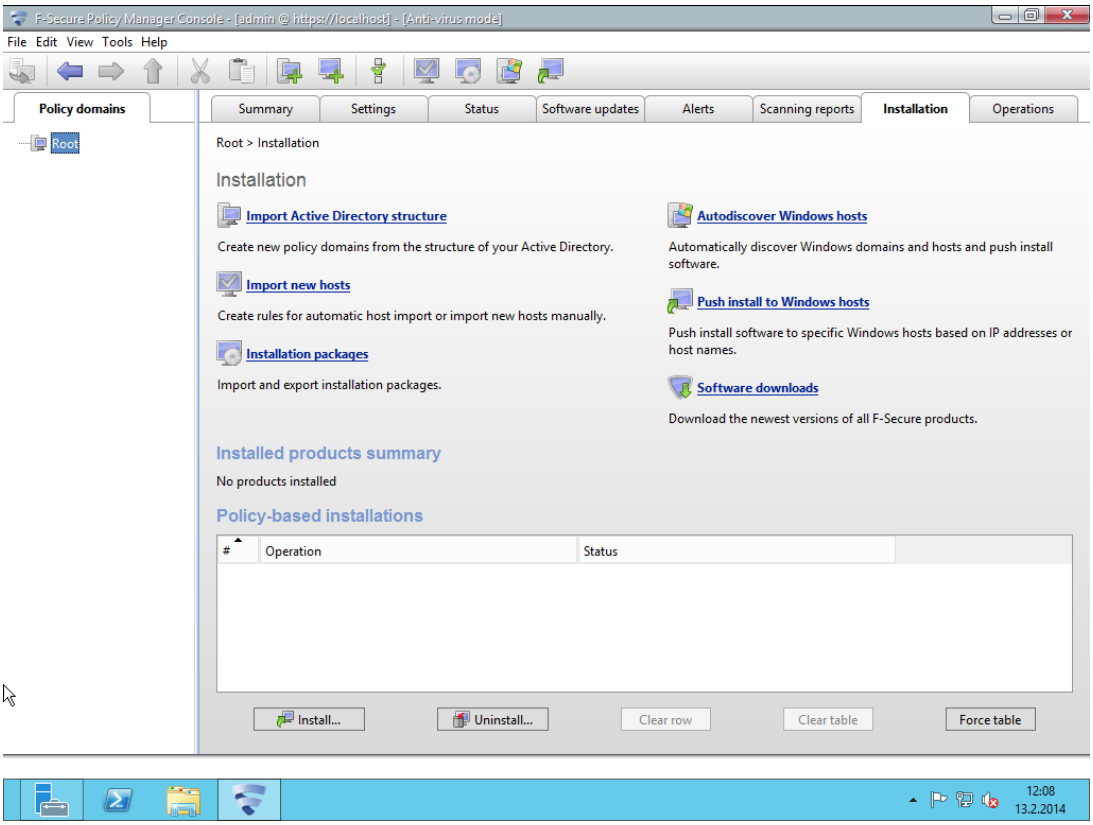
Testiympäristön virtuaalikoneiden tultua valmiiksi aloitin tutustumisen F-Secure Policy Manageriin. Policy Manager asennettiin Windows Server 2012 -virtuaalikoneelle. Yksityiskohtaiset asennuskuvat ja selostukset löytyvät opinnäytetyön liitteestä 1. Itse ohjelman asennus on todella yksinkertainen ja helppo.

Tässä luvussa käydään läpi Policy Managerin alkutoimet, kuten käyttäjien luonti, rakenteen luonti ja rekisteröinti. Lisäksi esitellään joitain ominaisuuksia, kuten eri tavat tuoda hosteja Policy Manageriin sekä ohjelmistojen jakelu- ja asennustavat.

5.1 Rakenteen luonti

Policy Domains

Kuvassa 5 näkyy Policy Manager Consolen päänäkymä, joka aukeaa, kun kirjautuu sisään F-Secure-palvelimeen. Vasemmalle Policy domains -otsikon alle tulee Policy Managerin rakenne. Policy domain on periaatteessa ryhmä, johon voi asettaa haluttuja käytäntöjä eli policyja. Käytännöt tulevat käyttöön kaikissa ryhmän koneissa eli hosteissa. Root domain, joka on kuvassa valittuna, on ”ylin ryhmä”. Se pitää sisällään kaikki ryhmät ja hostit. Rootin alle tehdyt ryhmät ovat subdomaineja. Kun asettaa policyn Root domainiin, kyseinen policy tulee käyttöön kaikissa subdomaineissa ja kaikissa hosteissa – policyt ovat siis periytyviä. Periytyvyys tarkoittaa, että kukin Policy domain perii automaattisesti ”ylemmän domainin” asetukset, mutta periytyviä asetuksia voidaan muuttaa subdomainin hosteilta muuttamalla kyseisen subdomainin policyja. Myös suoraan yksittäisiin hosteihin voi tehdä policyja, jotka tulevat käyttöön vain kyseisiin koneisiin. (F-Secure 2013, 15.)

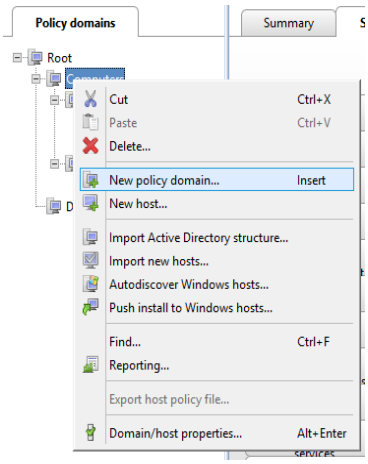


Kuva 5. F-Secure Policy Manager -päänäkymä.

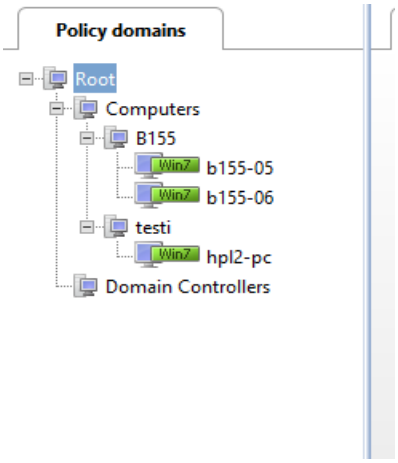
Tuki Active Directorylle

Ohjelmisto tukee Microsoft Active Directorya, mikä mahdollistaa verkon Active Directory -rakenteen toisinnon F-secure Policy Manageriin (F-Secure 2014a). Se on helppo tapa tehdä rakenne, joka on samanlainen kuin Active Directoryn rakenne. Tämä kannattaa tehdä ainakin suurissa yritysverkoissa, joiden domaineissa on paljon eri koneryhmiä, mikäli samat ryhmät halutaan säilyttää myös Policy Managerin rakenteessa, jotta niihin voi asettaa ryhmäkohtaisia policyja. Labraverkkoon tehtiin myös AD-liitäntä, mutta Labraverkon AD:ssä ei ollut kuin kaksi ryhmää: Computers ja Domain Controllers. Koska työn vaatimusmäärittelyssä mietittiin ryhmäkohtaisia policyjä, niin ei riitä, että olisi ainoastaan yksi ryhmä ”Computers”, jonka alla kaikki hostit olisivat. Valmiiseen rakenteeseen halutaan omat ryhmänsä eri luokille ja WISE-projektin koneille, joten tuotantopalvelimeen tehdyssä F-Secure -palvelimessa ei käytetty Active Directoryn toisintoa.

Policy domainien alle voi luoda omia subdomaineja painamalla Policy domainin kohdalla hiiren oikeaa näppäintä ja valitsemalla ”New policy domain...”, kuten kuvassa 6 osoitetaan. Kuvassa 7 näkyy Labraverkkoon luotu testiympäristö: AD-rakenne ja manuaalisesti luodut subdomainit B155 ja testi.



Kuva 6. Subdomainin luonti.



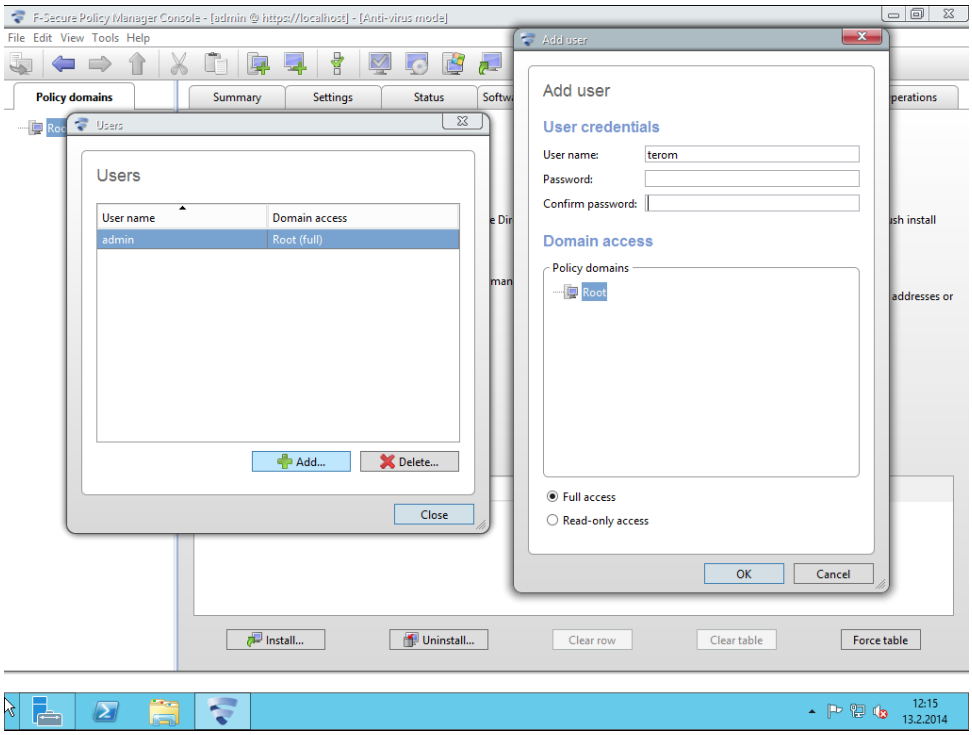
Kuva 7. Testiympäristö.

5.2 Käyttäjien luonti

Käyttäjät

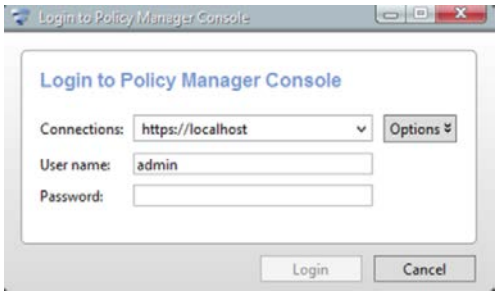
Policy Manageria voivat käyttää useat eri käyttäjät. Pääkäyttäjä eli admin-tili luodaan Policy Managerin asennuksen yhteydessä. Muut käyttäjät luodaan Policy Manager Consolen kautta. Uusille käyttäjille voi antaa joko full access eli root-oikeudet tai vain read-only-oikeudet. Lisäksi käyttäjälle voi antaa oikeudet kaikkiin domaineihin valitsemalla Domain Access ikkunasta Root domainin, tai vain tietyn subdomainin oikeudet valitsemalla kyseisen subdomainin. Vain root-oikeudet omaava voi rekisteröidä tuotteen, luoda tai poistaa hostien tuontisääntöjä, tuoda manuaalisesti uusia hosteja, tuoda ja poistaa tuotteiden asennuspaketteja, tuoda ja viedä allekirjoitusavaimia tai tuoda Active Directory -rakenteita. (F-Secure 2013, 26.)

Kuvassa 8 näkyy ensimmäisen käyttäjätilin luonti Labraverkon Policy Manager Serverille. Labraverkon järjestelmänvalvojalle annetaan Full access -oikeudet koko domainiin.



Kuva 8. Käyttäjän luonti.

Käyttäjä kirjautuu omalla tunnuksellaan Policy Manager Serveriin Consolen käynnistyksessä. Jos organisaatiolla on useita eri Policy Manager Servereitä, niitä kaikkia voi hallita saman Consolen kautta. Halutulle palvelimelle kirjaudutaan lisäämällä uusi yhteys options-valikosta (kuva 9). Osoite palvelimelle on Policy Managerin HTTPS URL. Jos sille halutaan kirjautua muualta kuin paikallisesti, pitää osoitteeksi aina vaihtaa kyseisen Policy Manager Serverin HTTPS URL-osoite. Testiympäristössä Policy Manager Server ja Console asennettiin samalle tietokoneelle, joten serverille kirjaudutaan paikallisella osoitteella https://localhost.



Kuva 9. Policy Manageriin kirjautuminen.

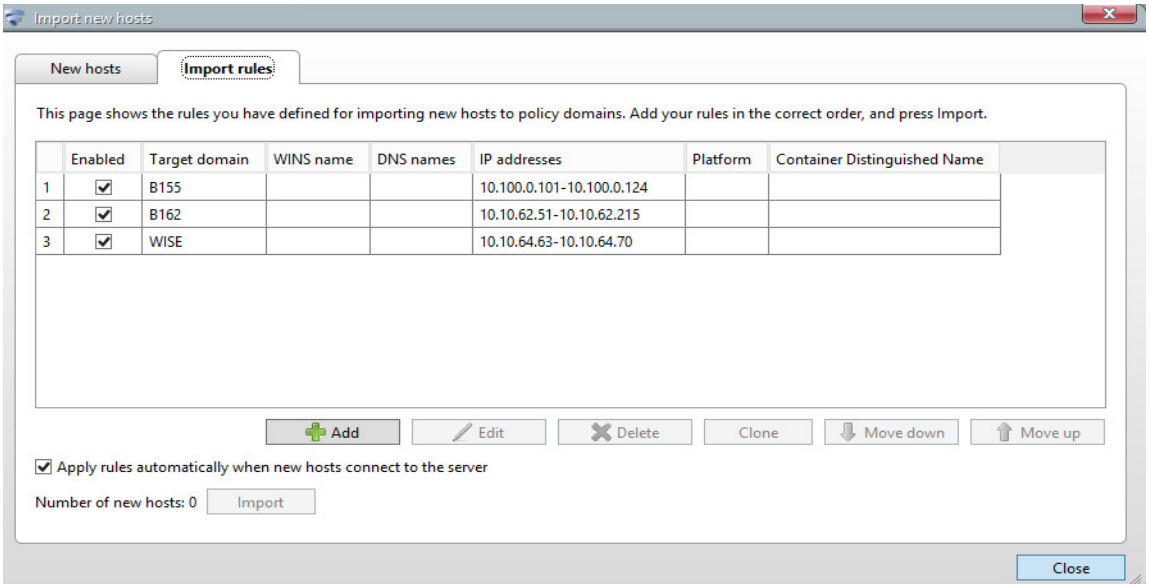
5.3 Policy Managerin rekisteröinti

F-Secure Policy Managerissa on 30 päivän ilmainen kokeilujakso, jonka jälkeen se pitää rekisteröidä. Rekisteröintiin tarvitsee asiakasnumeron, joka löytyy tuotteen mukana tulleesta lisenssisertifikaatista. Kokeilujakson loppuessa palvelimeen ei voi enää muodostaa yhteyttä, mutta client-koneille asennetut sovellukset kuitenkin toimivat ja asetukset pysyvät muuttumattomina. (F-Secure 2013, 14.)

5.4 Hostien tuonti Policy domainiin ja ohjelmistojen jakelu

Import rules

Mielestäni helpoin tapa lisätä hostit Policy Manageriin on käyttää import rules eli tuontisäännöt -vaihtoehtoa. Ne ovat Policy Manager palvelimeen asetettavia sääntöjä, joiden avulla uudet Clientit saadaan automaattisesti oikeaan Policy domain -ryhmään. Tuontisäännöiksi asetin eri lähiverkkojen IP-osoitealueet (Kuva 10). Kun Client Security asennetaan hosteille, asettaa Policy Manager kyseisen hostin automaattisesti IP-osoitteen perusteella oikeaan ryhmään eli target domainiin.



Kuva 10. Import rules.

Muita mahdollisuuksia tuoda hosteja Policy domain -rakenteeseen ovat:

- Autodiscover Windows hosts: etsii verkosta automaattisesti Windows-koneet ja mahdollistaa asennuksen aloituksen.
- Active Directory -toisinto: hyvä tapa isoissa, paljon eri ryhmiä sisältävissä verkoissa.
- Import new hosts: uudet hostit voidaan tuoda Policy domainiin eri kriteerien avulla, kuten tuontisäännöissäkin, vaikkapa IP-osoitteen perusteella.

Push installation

Push installation to Windows hosts -ominaisuuden avulla halutun ohjelmiston asennuksen saa tehtyä hostille suoraan IP-osoitteen tai hostin nimen perusteella. Autodiscover Windows hosts -ominaisuus toimii samoin kuin push installation -ominaisuus, mutta siinä hostit valitaan listasta ja jatketaan sen jälkeen asennukseen. Kohdehostien valinnan jälkeen alkaa halutun sovelluksen asennus. Ensin valitaan haluttu asennuspaketti installation packages -listasta (Liite 2), minkä jälkeen asennus suoritetaan normaalisti ohjeiden mukaan. (F-Secure 2013, 33.)

Local installation

Ohjelmistot voidaan asentaa myös paikallisesti koneille, minkä jälkeen ohjelmisto ottaa yhteyden Policy Manager -palvelimeen. Asennus toimii siten, että haluttu asennuspaketti ladataan ensin Policy Manageriin. Installation packages -listasta valitaan haluttu paketti ja painetaan ”export”-painiketta. Tämän jälkeen käydään läpi normaalit asennusvaiheet ja valitaan paikka, mihin halutaan tallentaa kustomoitu asennuspaketti. Asennuspaketin voi jakaa koneille käyttämällä vaikka Windows Group Policya.

Tässä opinnäytetyössä paikallista asennusta käytettiin asentaessa WISE-projektin koneita. Valmiiksi konfiguroitu Client Security -asennuspaketti ladattiin Policy Managerista USB-tikulle, jolta Client Security asennettiin koneille. Tämän jälkeen Client Security otti automaattisesti yhteyden Policy Manageriin.

Policy-based installation

Hosteille, joissa on jo jokin F-Secure Policy Managerin kautta tehty asennus, eli koneessa on jo F-Secure Management Agent, on mahdollista tehdä asennuksia käytäntöjen mukana. Policy-based-asennuksessa ohjelmistosta luodaan spesifioitu asennuspaketti ja asennuksesta kirjoitetaan tieto policy-tiedostoihin.

Asennuspaketti ja policy-tiedostot allekirjoitetaan avainparilla. Kun hostin Management Agent tarkastaa uudet käytännöt Policy Managerista, huomaa se asennuskäytännön ja aloittaa asennuksen. (F-Secure 2013, 35.) Tätä asennusmenetelmää ei käytetty tässä opinnäytetyössä, koska Policy Manageriin yhdistettyä Management Agentia ei ollut vielä missään koneessa.

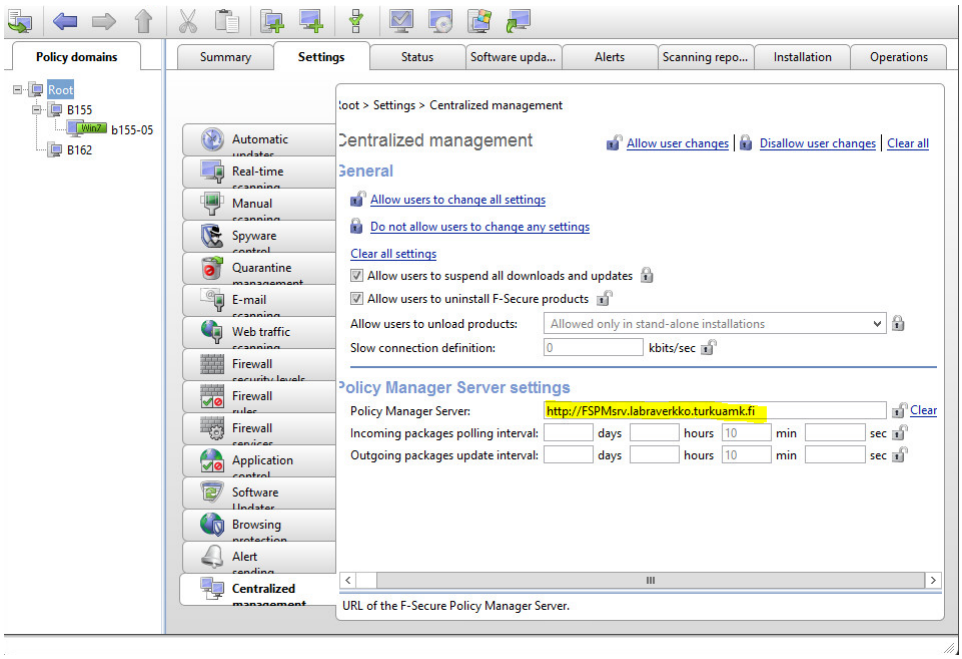
6 ASENNUSTEN VAIHEET JA KÄYTÄNTÖJEN KONFIGUROINTI

6.1 Muutokset alkuperäiseen suunnitelmaan

Opinnäytetyön alkuperäinen suunnitelma oli luoda ensin testiympäristö. Tarkoituksena oli, että siitä muodostuisi lopullinen ympäristö, joka vasta käyttöönotossa siirrettäisiin tuotantopalvelimelle. Alkuperäisestä suunnitelmasta poikettiin ja asennus tuotantopalvelimelle tehtiin kokonaan uudelleen. Tapaamisessa ammattikorkeakoulun IT-tukihenkilön kanssa selvisi, että uudelleenasennus on helpompi ja järkevämpi vaihtoehto kuin siirtää koko ympäristö toiselle palvelimelle. Testiympäristön siirto tuotantopalvelimelle olisi pitänyt hoitaa asentamalla uusi F-Secure Policy Manager Server palvelimelle ja käynnistämällä siinä testiympäristön palvelimesta otettu varmuuskopio. Sen jälkeen testiympäristön koneet olisi pitänyt saada ottamaan yhteys uuteen palvelimeen. Testiympäristössä Clientit ottivat yhteyttä IP-osoitteen perusteella palvelimeen. Tästä muodostuisi ongelma, jos palvelimen IP-osoite vaihtuisi, koska clientit eivät silloin enää löytäisi uuden IP-osoitteen omaavaa palvelinta. Ratkaisu olisi ollut luoda testiympäristön palvelimelle sellainen käytäntö, joka toimittaisi uuden F-Secure-palvelimen IP-osoitteen hosteille. Myös uusi avainpari olisi tarvittu. Tämä olisi ollut F-Securen tukisivustojen mukaan mahdollista, mutta hieman mutkikasta ja toimiminenkin vaikutti epävarmalta.

Katsoin siis parhaimmaksi, että asennan kokonaan uuden Windows Serverin Workstationiin ja siirrän sen heti ESXi-palvelimelle. Tällä kertaa käytin Windows Server 2012 R2 -käyttöjärjestelmää. Asensin palvelimen samalla tavalla kuin testiympäristössäkin, mutta levytilan pienensin 20 gigatavuun. Windows Serverin siirto onnistui helposti Workstationilla. Ensin muodostettiin yhteys ESXi-palvelimeen ”connect remote server”-napilla. Sitten valittiin oikealla hiiren napilla siirrettävä palvelin, valittiin manage ja sitten upload. Sen jälkeen valittiin kohdepalvelin ja datastore, minkä jälkeen painettiin ”finish” ja palvelin kopioitui ESXi:lle. Palvelimen siirron jälkeen asensin F-Secure Policy Manager Serverin

palvelimelle (Liite 1). Palvelimelle annettiin verkossa kaksi kiinteää IP-osoitetta. Tällä kertaa Policy Manager -palvelimen osoitteena en käyttänyt IP-osoitetta vaan DNS-nimeä, joten IP-osoitteen vaihtuessa hostit pystyvät silti DNS-nimen perusteella löytämään oikean palvelimen ja muodostamaan yhteyden siihen. Kuvassa 11 näkyy kaikille hosteille toimitettu Policy Manager -palvelimen osoite. Osoite on oletuskäytäntö, joten se toimitetaan oletuksena myös kaikissa asennuksissa.



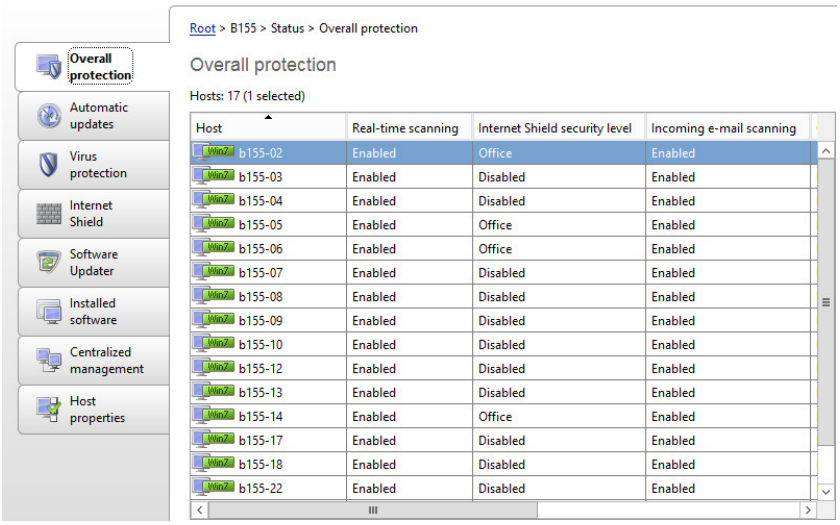
Kuva 11. Policy Manager Serverin yhteysosoite (oletuskäytäntö).

6.2 Client Security -asennuksen vaiheet

Ensimmäisenä latasin F-Securen sivuilta uuden version Client Securitystä. Aloitin asennukset testiympäristöstäkin tutuiksi tulleilla koneilla B155-05 ja B155-06 ”puskemalla” niihin uuden, täydellä lisenssillä varustetun Client Securityn. Sen jälkeen yritin työntää asennuksen ensimmäisen kerran B162-luokan koneelle, mikä ei kuitenkaan onnistunut. Syynä oli yksinkertaisesti se, että koneen Windows-palomuuri esti asennuksen. Koska Labraverkossa ei ole vielä Group Policy käytössä, jouduttiin Windows-palomuuri ottamaan pois käytöstä kaikista koneista erikseen.

B162-luokan asennukset onnistuivat yhdellä kerralla sen jälkeen, kun Windows-palomuuri oli poistettu käytöstä. Myös B155-luokan muutamissa tietokoneissa oli Windows-palomuuri päällä, joten sieltäkin se piti poistaa käytöstä ennen asennuksia.

Aloittaessani asennukset kaikille B155-luokan tietokoneille asennus meni ensimmäisellä kerralla läpi vain kahteen tietokoneeseen 24:stä. Syyksi selvisi tietokoneissa ollut itsenäinen F-Secure Client Security 9, jonka palomuuri esti yhteydenoton Policy Manager -palvelimelta ja siten uudelleenasennuksenkin. Onnistuakseni asentamaan uuden keskitetysti hallitun Client Securityn hosteille, jouduin sallimaan kaiken liikenteen aikaisemmasta Client Securityn palomuurista eli disabloimaan palomuurin. Kuvassa 12 näkyy, kuinka uuden Client Securityn asennuksen jälkeen tämä sääntö oli edelleen voimassa, jolloin tietokoneiden palomuurit sallivat kaiken liikenteen. Sainkin siis heti lähettää hosteille uuden käytännön, jotta palomuurit alkaisivat taas toimia. Kuvasta 12 havaitaan, että joillekin tietokoneille uusi käytäntö (Internet Shield security level: Office) on mennyt jo perille, kun taas osalla Internet Shield on vielä tilassa ”Disabled”.

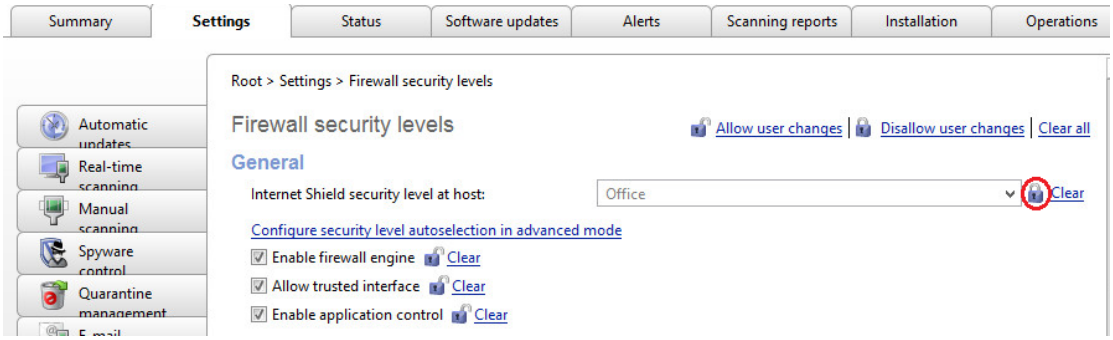


Kuva 12. Palomuurit disabloituna perintönä aikaisemmalta Client Securityltä.

6.3 Käytäntöjen muokkaus ja jakelu

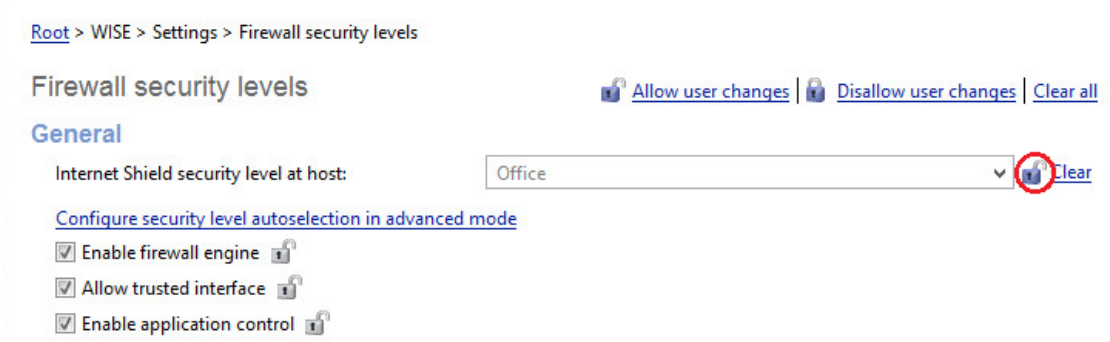
Tässä luvussa kuvataan, mitä käytäntöjä asetin Policy domains -ryhmille. Eri ryhmille asetettiin alustavasti samat yksinkertaiset käytännöt, mutta WISE-ryhmän koneille jätettiin palomuurin konfigurointimahdollisuus auki. Käytäntöjen muokkaus on melko helppoa, koska Policy Managerin ominaisuudet on selkeästi jaoteltu ja nimetty. Käytäntöjen voimaantulon edellytyksenä on, että ne jaetaan hosteille. Jako tapahtuu painamalla Policy Managerin vasemmassa ylälaidassa olevaa Policy distribution -painiketta. Intervalli käytäntöjen päivittymisessä on 10 minuuttia.

Kuvassa 13 näkyy, kuinka palomuuri on lukittu Root-tasolla Office-asentoon eli kaikkien subdomainienkin (B155, B162, WISE) hostien palomuurit on lukittu käyttäjiltä. Koneiden käyttäjät eivät voi sammuttaa tai muokata palomuuria.



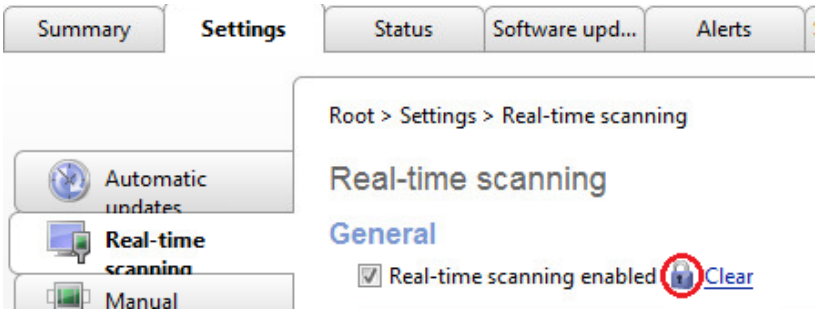
Kuva 13. Palomuuri lukossa.

Kuvassa 14 taas näkyy, kuinka WISE-ryhmältä on erikseen aukaistu palomuuri konfiguroitavaksi, joten he voivat tarvittaessa sallia liikennettä palomuurin läpi. Kuvassa 14 näkyy myös Policy Managerin sääntöjen periytyvyys. Yleiset käytännöt kannattaa asettaa Rootille, jolloin ne periytyvät kaikkiin subdomaineihin. Subdomainin asetuksissa niitä voi sitten erikseen muokata, jolloin vaikutusta muihin domaineihin ei ole.



Kuva 14. Palomuuri muokattavissa.

Kuvassa 15 näkyy reaaliaikaisen virustorjunnan lukitseminen Root-tasolla. Käyttäjät eivät voi sammuttaa virusskanneria.



Kuva 15. Reaaliaikainen virusskanneri toiminnassa ja lukossa Root-tasolla.

7 JATKOTOIMENPITEET JA YHTEENVETO

Tavoitteena opinnäytetyössä oli ottaa käyttöön keskitetty virustorjunta koulun opetuskäyttöön tarkoitetussa laboratorioverkossa. Keskitettyyn hallintaan valittiin F-Secure Policy Manager ja laboratorion tietokoneiden virustorjuntaohjelmistoksi F-Secure Client Security.

Alkuperäinen tarkoitus oli ottaa F-Secure Policy Manager käyttöön hieman laajemmin, sekä laajemmassa ympäristössä että ominaisuuksiltaan. Kansalaisen mikrotuen tietokoneiden liittäminen Policy Managerin hallinta-alueeseen kuitenkin suljettiin pois, koska järjestelmänvalvoja ei halunnut kyseisestä lähiverkosta mitään liikennettä muuhun laboratorioverkkoon. Myöskään Software Updater -ominaisuutta ei otettu käyttöön, koska kyseiset päivitykset on tulevaisuudessa tarkoitus hoitaa toisilla työkaluilla. Nämä mahdollisuudet ovat kuitenkin edelleen olemassa ja jatkotoimenpiteinä helppo toteuttaa. Tietokoneita voi lisätä verkkoon todella helposti ja Software Updaterinkin saa käyttöön myöhemmin halutessaan.

Ohjelmistot testattiin ensin VMwaren virtualisointiohjelmistoilla luodussa testiympäristössä. Testien jälkeen F-Secure Policy Manager asennettiin ESXi-palvelimelle. B155- ja B162-luokkien koneisiin Client Security -ohjelmisto asennettiin Policy Managerin Push installation -menetelmällä, jolla kaikki tietokoneet saa asennettua kerralla. WISE-projektin tietokoneisiin ohjelmisto asennettiin paikallisesti USB-tikulta. Ohjelmistojen asennukset onnistuivat melko nopeasti. Ohjelmistojen asennusten ja Policy Manager -palvelimen konfiguraatioiden jälkeen Policy Manager alkoi heti ilmoitella mahdollisista haittaohjelmista useassa verkon tietokoneessa. Policy Managerin kautta näkee helposti saastuneen tietokoneen tiedot ja selkeän rakenteen ansiosta koneiden sijainnit voi heti nähdä. Haittaohjelmat voi poistaa heti Policy Managerin käyttöliittymän kautta.

Jatkotoimenpiteinä järjestelmänvalvojan täytyy tutustua Policy Manageriin ja toimittaa haluamansa käytännöt hosteille. Tämän opinnäytetyön yhtenä tuotoksena on, että palomuurit on asetettu perustasolle (Office), jonka on katsottu ja

päätetty riittäväksi omalta osaltaan suojaamaan tietoturvallista työntekemistä. WISE-projektin koneissa mahdollisuus palomuurin sammuttamiseen jätettiin. Muualla palomuuri on mahdollista ottaa pois käytöstä vain Policy Managerin kautta. Myös automaattiset päivitykset ja virusten reaaliaikaiset skannaukset lukittiin, jotta käyttäjät eivät niitä voi sulkea.

Mielestäni opinnäytetyö onnistui kohtuullisesti ja täytti ainakin tavoitteensa tuoda keskitetty virustorjunta laboratorioverkkoon. Miettiessäni, mitä olisin tehnyt toisin, olisin tehnyt huomattavasti selkeämmän määrittelyn siitä, missä ja mitä ohjelmistoja otetaan käyttöön. Olisin voinut myös oma-aloitteisesti yrittää saada keskitetyt virustorjunnat asennetuksi palvelinkoneille. Teoriaosuus olisi voinut painottua vielä paljon selkeämmin Policy Managerin ominaisuuksiin. Kaiken kaikkiaan olen melko tyytyväinen työhön ja varsinkin siihen, että opin paljon keskitetystä tietoturvasta.

LÄHTEET

Abacus 2014. Abacus Computing: F-Secure products and technologies. Viitattu: 11.6.2014. http://www.abacus.co.me/f-secure_En.htm.

F-Secure 2013. Policy Manager Administrator's guide. Viitattu: 15.4.2014. http://download.f-secure.com/webclub/pm11_adminguide_eng.pdf.

F-Secure 2014a. Hallinta - Yleistä. Viitattu: 4.4.2014. http://www.f-secure.com/fi/web/business_fi/products/management/overview.

F-Secure 2014b. Keskeiset ominaisuudet. Viitattu: 4.4.2014. http://www.f-secure.com/fi/web/business_fi/products/management/features.

F-Secure 2014c. Pöytäkoneet ja kannettavat. Viitattu: 4.4.2014. http://www.f-secure.com/fi/web/business_fi/products/desktops/overview.

F-Secure 2014d. Hallinta – Ratkaisu. Viitattu: 20.4.2014. http://www.f-secure.com/fi/web/business_fi/products/management/solution.

F-Secure 2014e. F-Secure Software Updater. Viitattu: 22.5.2014. http://www.f-secure.com/en/c/document_library/get_file?uuid=65e7a77b-f083-416e-b778-ac6fea7c9c85&groupId=30743.

Kaspersky 2014. Products - For Business. Viitattu: 27.5.2014. http://www.kaspersky.com/business-security.

Lampikoski, J. 2014. Turun ammattikorkeakoulun Lemminkäisenkadun toimipisteen laboratorio-verkon kehitys. AMK-opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. Turku: Turun ammatti-korkeakoulu.

Lukka, K. 2014. Konstruktiivinen tutkimusote. Viitattu: 5.6.2014 http://www.metodix.com/fi/sisallys/04_virtuaalikirjasto/dokumentit/aineistot/konstruktiivinentutkimusote.

McAfee 2014. Products & solutions. Viitattu 5.6.2014. http://www.mcafee.com/us/products/epolicy-orchestrator.aspx#vt=vtab-Overview.

Mentalfloss 2013. Going Viral: How Two Pakistani Brothers Created the First PC Virus. Viitattu: 6.3.2014. http://mentalfloss.com/article/12462/going-viral-how-two-pakistani-brothers-created-first-pc-virus.

Microsoft 2014a. System Center 2012 R2 Configuration Manager. Viitattu: 27.5.2014. http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2-configuration-manager/.

Microsoft 2014b. Windows Server Update Services. Viitattu: 27.5.2014. http://technet.microsoft.com/fi-fi/windowsserver/bb332157.

Microsoft 2014c. Group Policy. Viitattu: 27.5.2014. http://technet.microsoft.com/fi-fi/windowsserver/bb310732.aspx.

Norton Advisor 2014. Computer Virus History. Viitattu: 30.3.2014. http://www.nortonadvisor.com/knowledge-center/computer-virus-history.html.

PC tools 2014. What is a Rootkit Virus? Viitattu: 25.5.2014. http://www.pctools.com/security-news/what-is-a-rootkit-virus/.

SearchSecurity 2014. Antivirus vendors go beyond signature-based antivirus. Viitattu: 29.5.2014. http://searchsecurity.techtarget.com/magazineContent/Antivirus-vendors-go-beyond-signature-based-antivirus.

Stallings, W. & Brown, M. 2008. Computer Security. New Jersey: Pearson Education, Inc.

Symantec 2014. Products. Viitattu: 27.5.2014. http://www.symantec.com/products-solutions/.

Tietoturvaopas 2014a. Haittaohjelmat. Viitattu: 27.5.2014. http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haittaohjelmat.html.

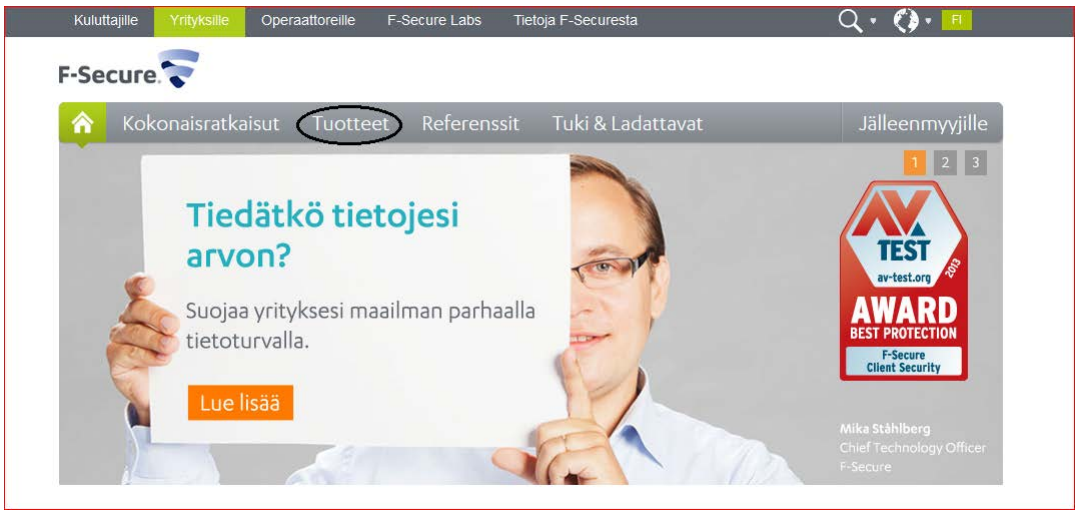
Tietoturvaopas 2014b. Miten haittaohjelmilta suojaudutaan? Viitattu: 25.5.2014. http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haitoiltasuojautuminen.html.

F-Secure Policy Manager - Lataus ja asennus

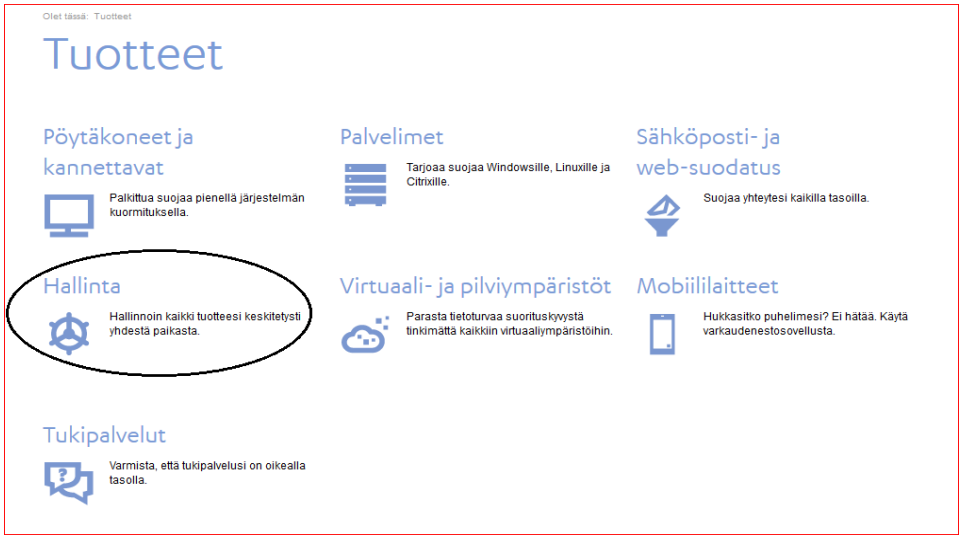
Lataus

Kannattaa ensin tutustua F-secure Policy Managerin ilmaisversioon. Ilmaisversiota voi kokeilla 30 päivää, jonka jälkeen sen voi ostaa ja rekisteröidä. Ilmaisversion aikana tehdyt asennukset ja konfiguraatiot säilyvät oston jälkeenkin.

Policy Managerin asennustiedosto löytyy osoitteesta www.f-secure.com. Siirry ylhäältä välilehdestä Yrityksille-sivulle ja valitse sieltä ”Tuotteet”.

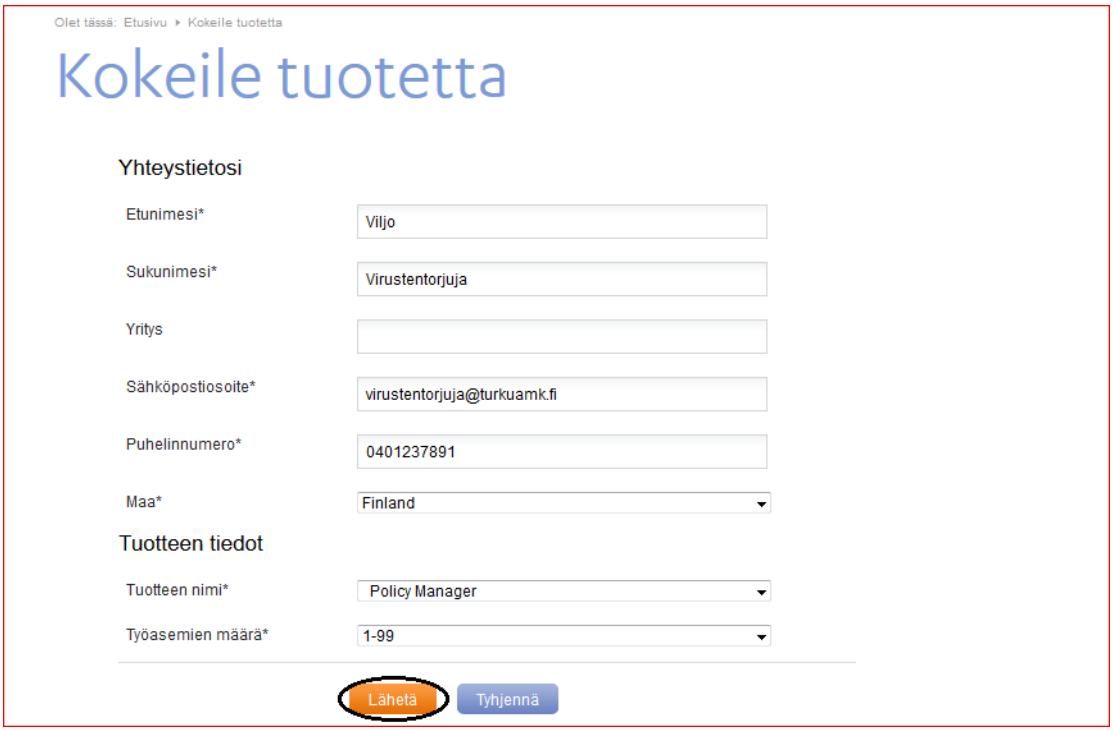


Seuraavalta sivulta valitse ”Hallinta”, joka vie sinut F-Secure Policy Managerin esittelysivulle.

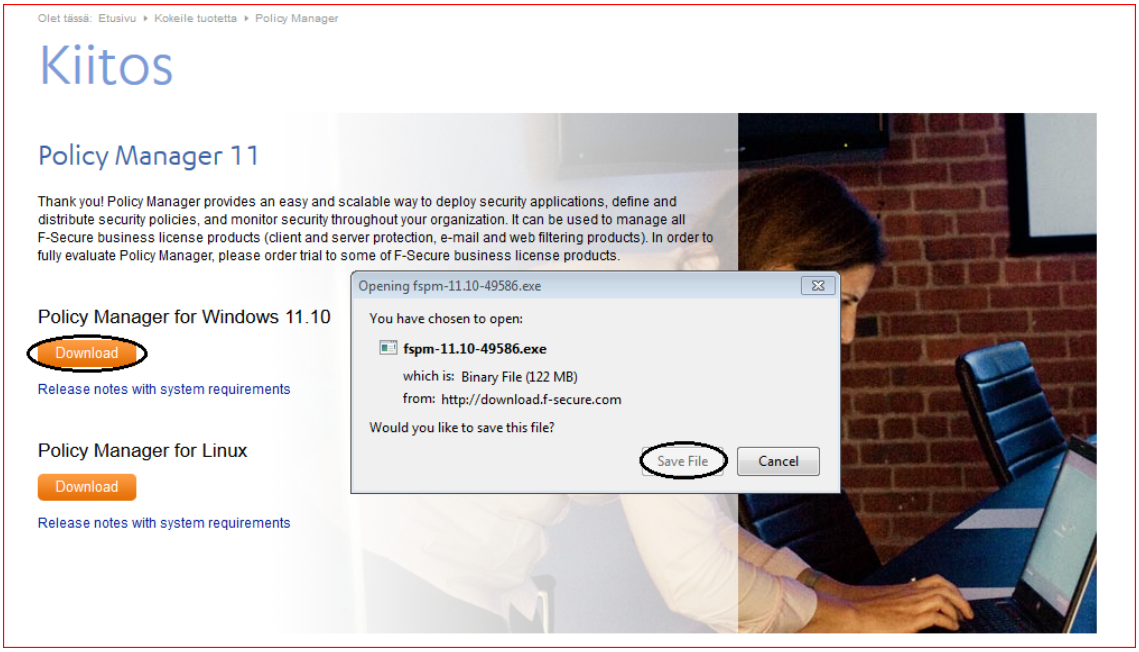


Hallinta-sivulla voit tutustua tuotteeseen. Ilmaisen kokeiluversion ladataksesi klikkaa yläkulmasta ”ilmainen kokeiluversio” -linkkiä.

Tämän jälkeen syötä omat ja haluamasi tuotteen tiedot seuraavalle sivulle, ja paina ”Lähetä”.



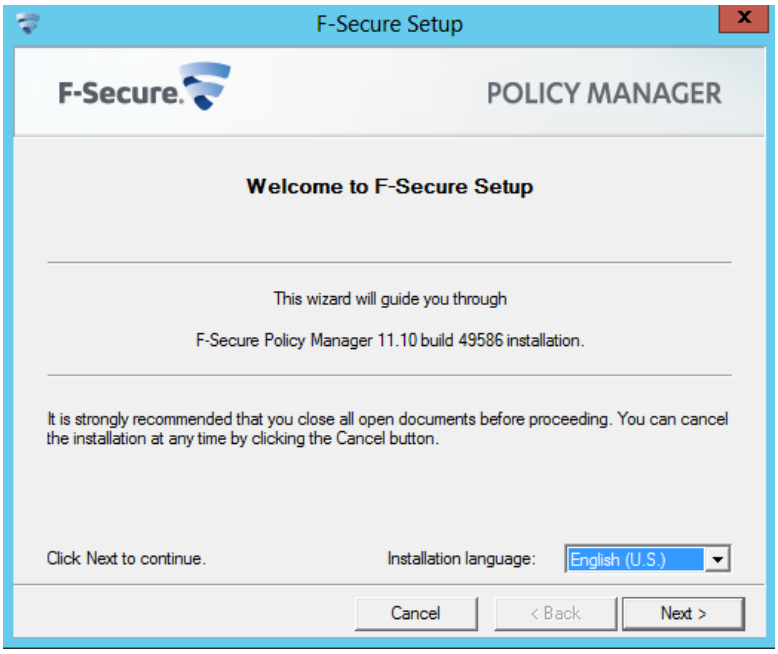
Seuraavaksi lataa Policy Manager painamalla ”Download”- ja Save File-painikkeita.



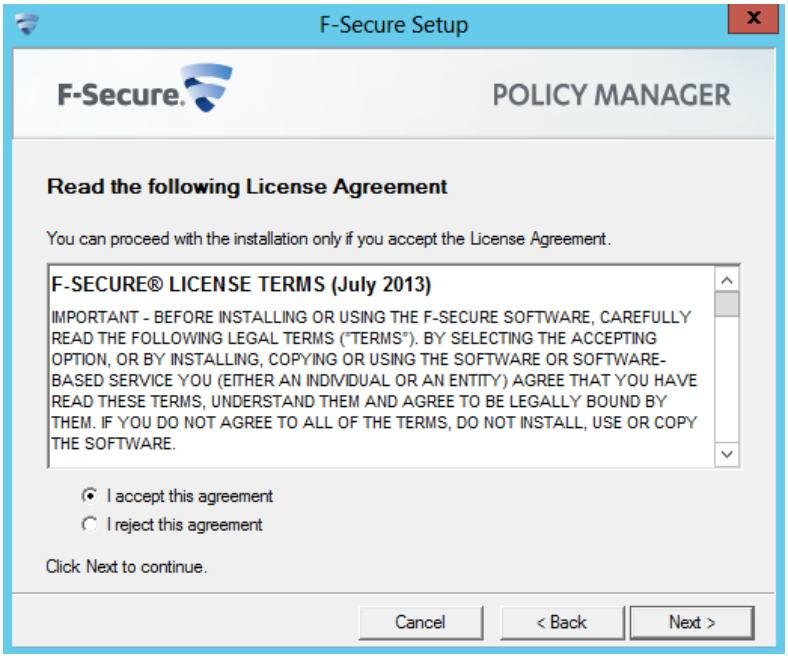
Asennus

F-secure Policy Managerin asennus on erittäin yksinkertainen.

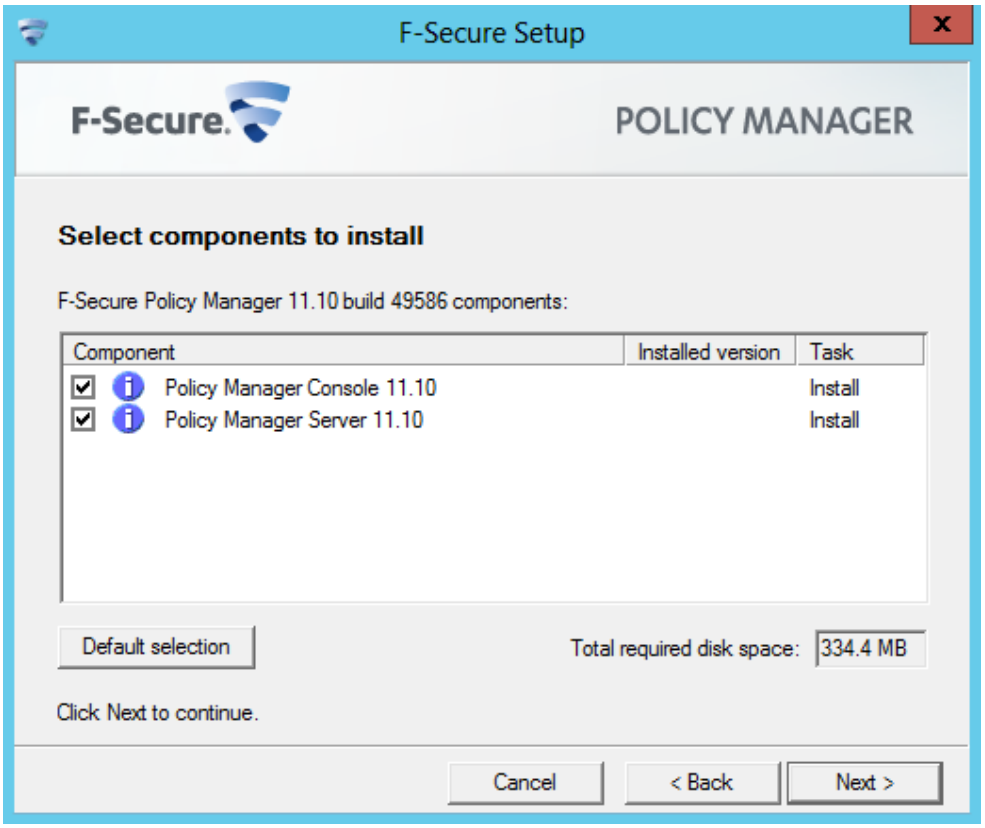
Asennuksen ensimmäisessä ikkunassa valitse kieli ja paina ”Next”.



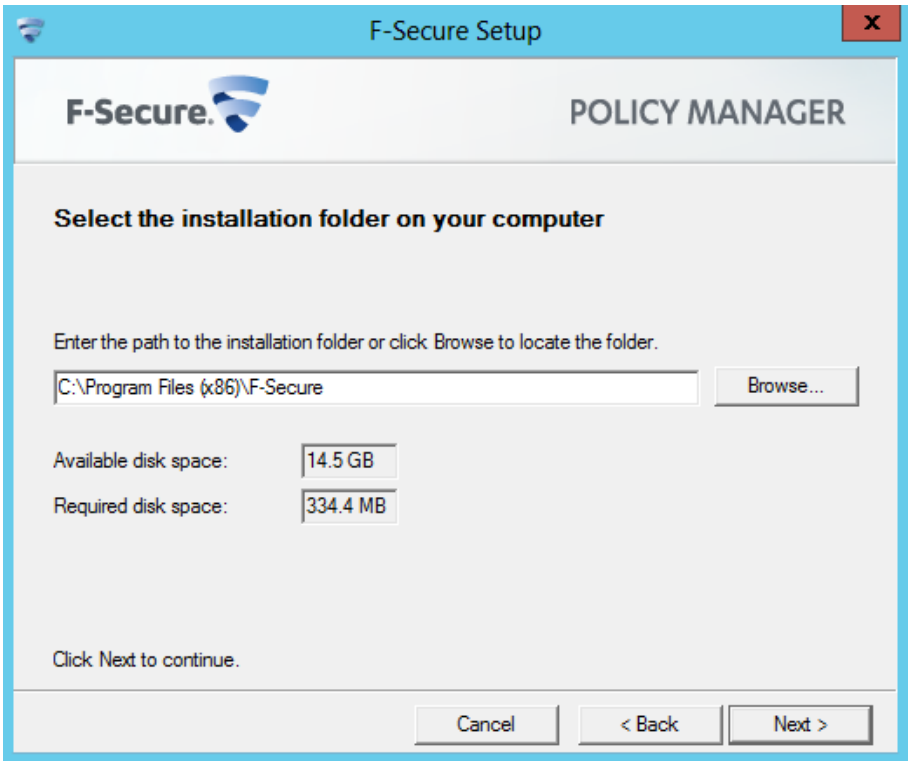
Hyväksy lisenssisopimus ja paina ”Next”.



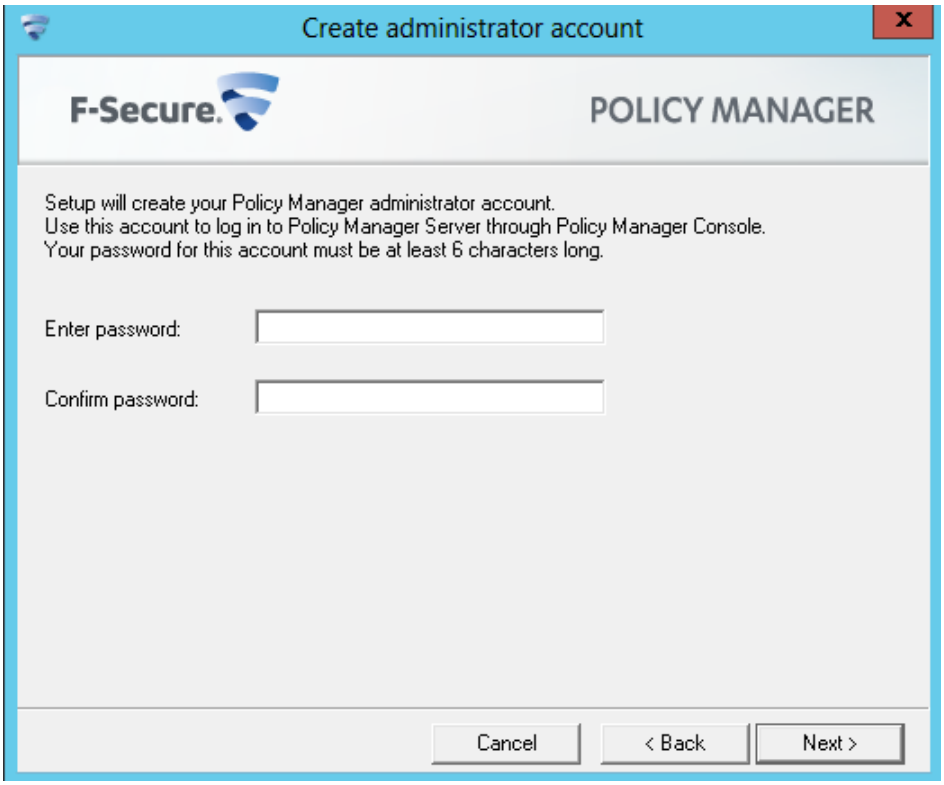
Seuraavaksi pitää valita, haluatko asentaa koneelle sekä Policy Manager Serverin sekä Policy Managerin konsolin. Valitse molemmat, jos haluat hallita Policy Manager Serveriä samalta koneelta, mihin se on asennettu. Voit myös valita ainoastaan Policy Manager Serverin ja asentaa hallintakonsolin jollekin toiselle koneelle. Tein asennuksen virtuaalikoneelle, jossa pääsin asennuksen jälkeen heti tutustumaan tuotteeseen, joten asensin molemmat. Valinta ei ole lopullinen, vaan myöhemmin konsolin voi asentaa jollekin toiselle koneelle ja ottaa sieltä yhteyden serveriin.



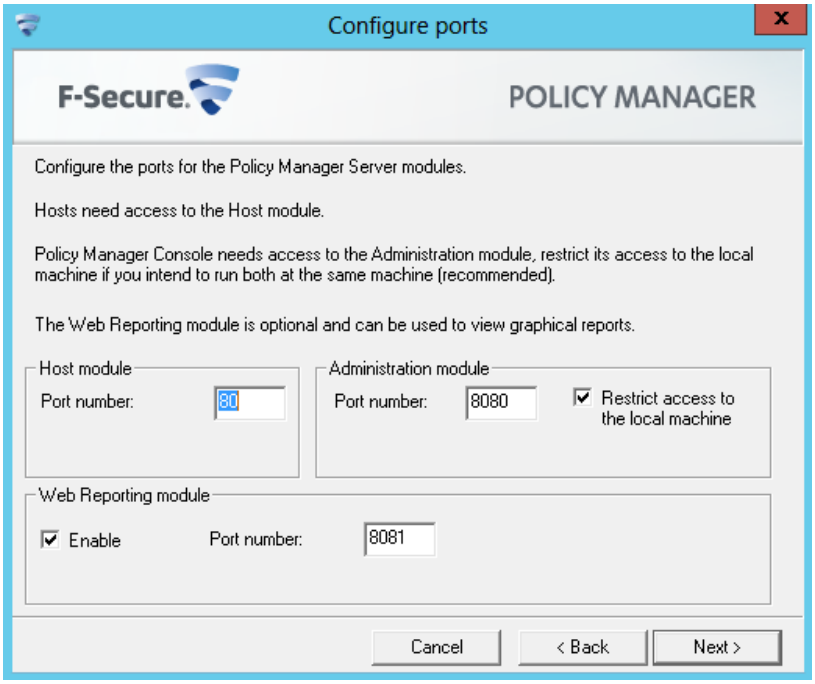
Seuraavaksi valitaan asennuskansio. F-Secure Policy Managerin Administrator´s guidessa on esitetty järjestelmän vaatimukset ja levytilasuositus on 6-10 GB riippuen hallittavan ympäristön laajuudesta. Paina ”Next”.



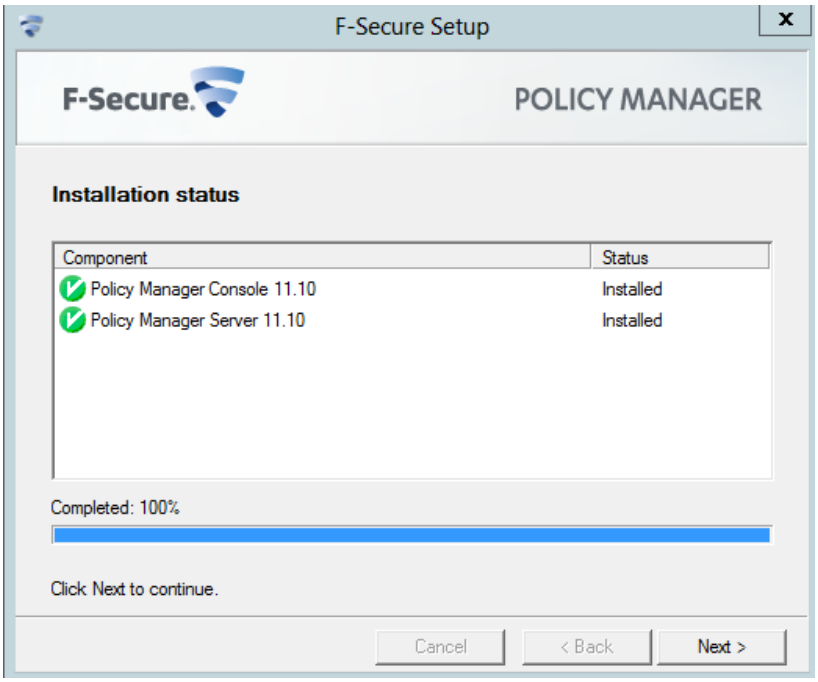
Seuraavaksi luodaan Policy Managerin admin-tunnus, jolla kirjaudutaan asennuksen jälkeen konsolin kautta serverille. Aseta salasana ja paina ”Next”.



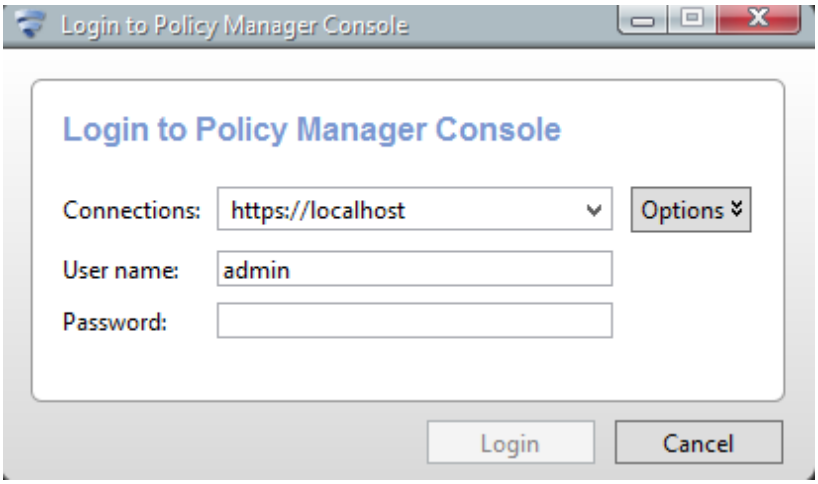
Sitten konfiguroidaan portit serverin eri moduuleihin. Pidän portit oletuksena, ja koska asensin sekä Policy Manager Serverin ja konsolin samalle koneelle, laitan ruksin kohtaan ”Restrict access to the local machine”. Haluan asentaa myös Web Reporting -moduulin, joten laitan ruksi kohtaan ”enable”. Paina ”Next”.



Asennus on valmis. Paina ”Next”.

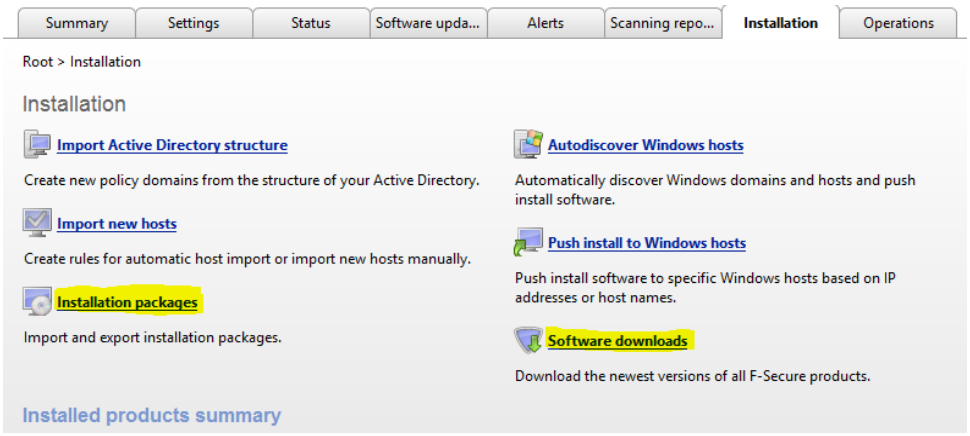


Asennuksen jälkeen aukeaa Policy Manager Consolen Login-ikkuna. Käyttäjätunnus on admin ja salasana aikaisemmin luomasi salasana. Koska kyseinen Policy Manager Server ja Console ovat samalla koneella, palvelimen osoite on https://localhost. Jos palvelimelle halutaan kirjautua muualta kuin paikallisesti, pitää osoitteeksi vaihtaa Policy Manager -palvelimen HTTPS URL-osoite.

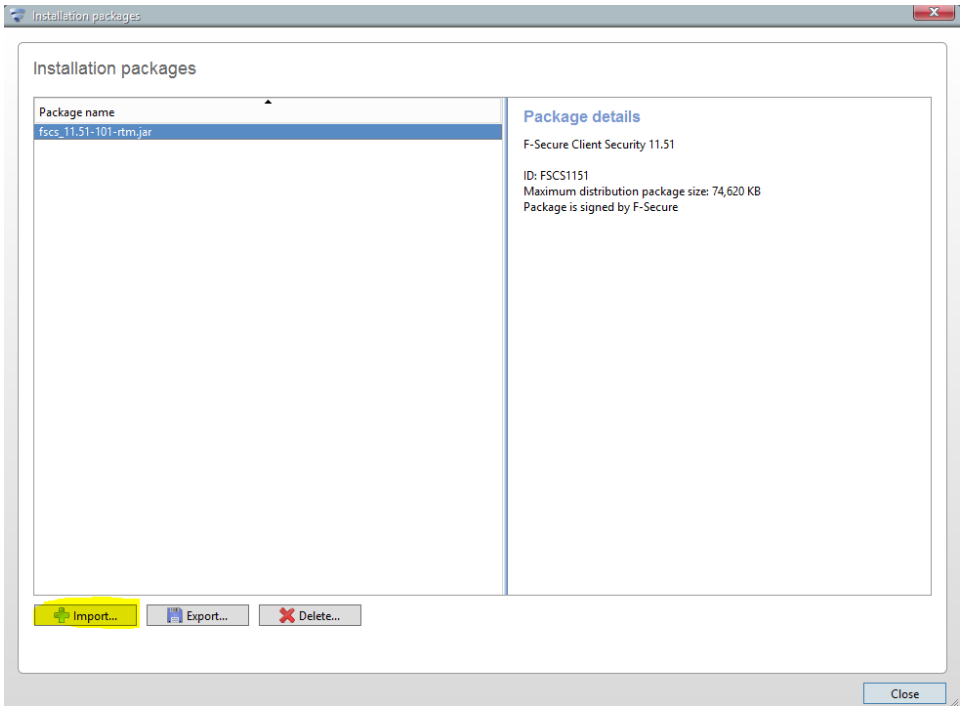


Asennuspakettien lataus

Asennuksiin tarvitaan asennuspaketit. Asennuspaketit saa suoraan F-Securen nettisivuilta klikkaamalla Software downloads-kuvaketta. Nappi ohjaa F-Securen ladattavat-sivulle, josta ladataan haluttu asennuspaketti. Latasin sieltä F-Secure Client Security 11.51 -ohjelmiston. Tämän jälkeen klikataan Installation packages-kuvaketta, jolloin uusi ikkuna aukeaa.



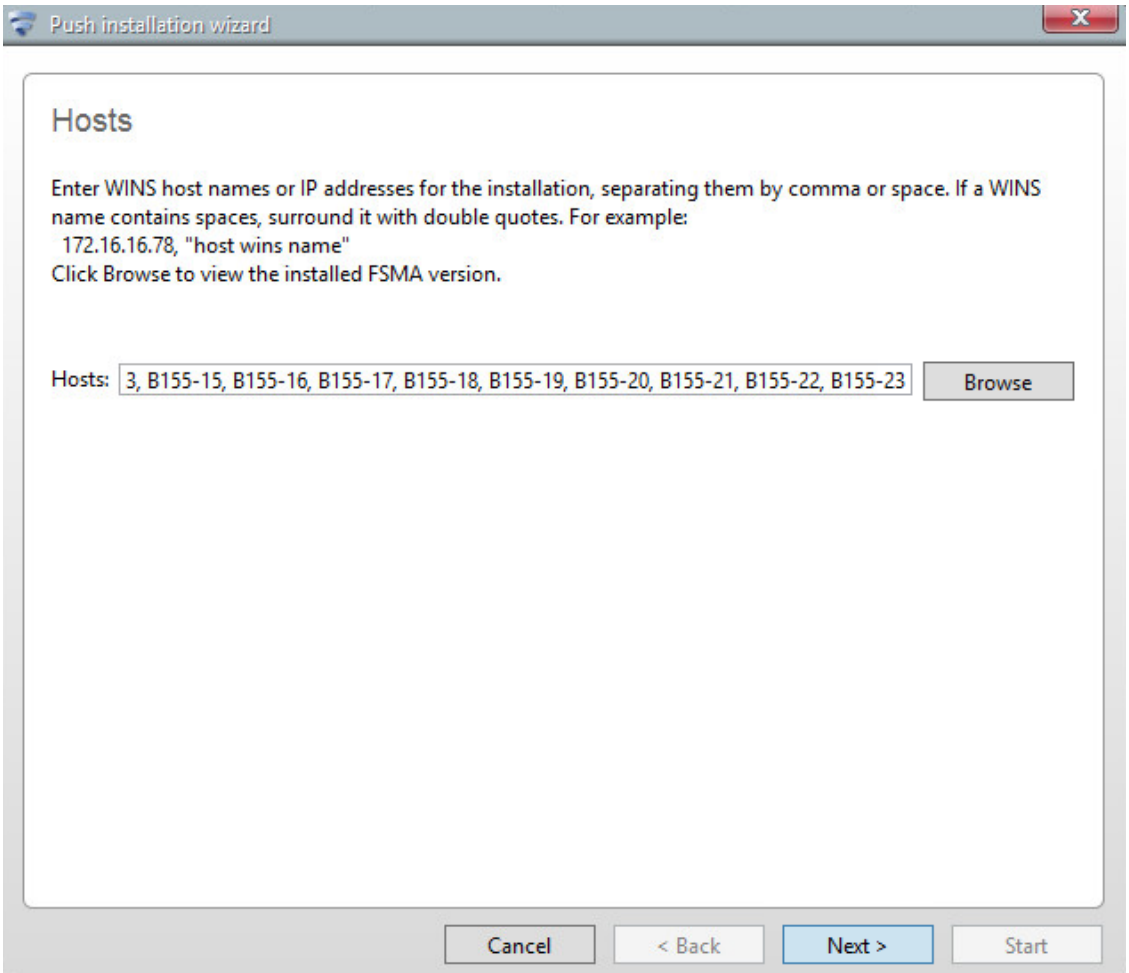
Klikkaamalla painiketta Import aukeaa kansionäkymä, josta etsitään aikaisemmin ladattu tiedosto. Tämän jälkeen paketti on valmis asennettavaksi halutulla menetelmällä.



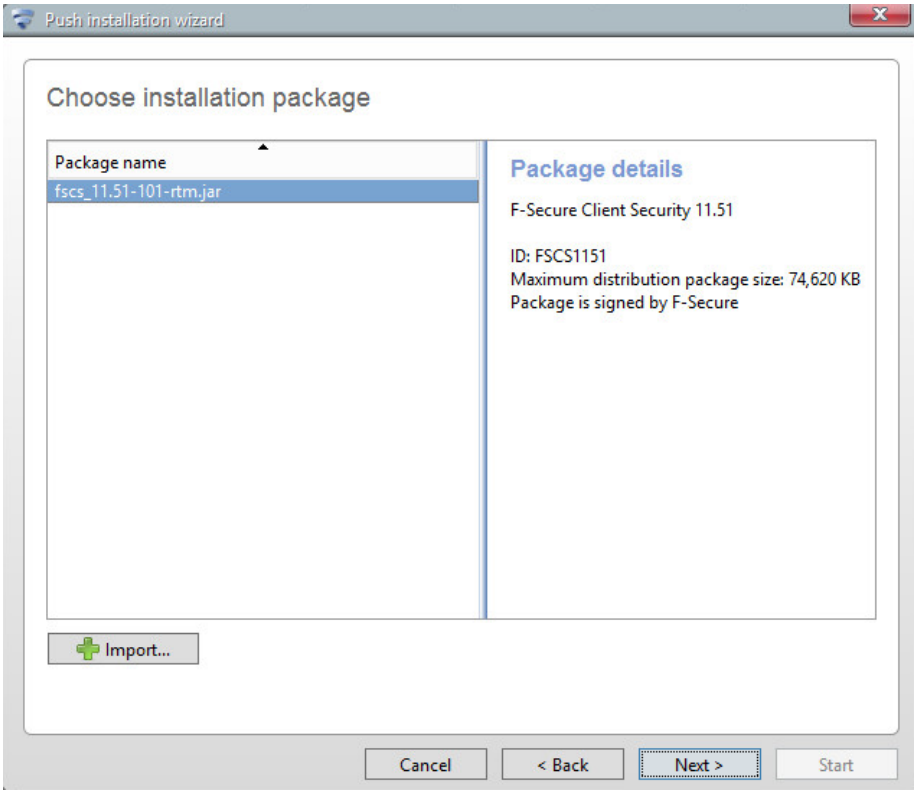
Push installation kuvina

Käytin luokkien B155 ja B162 Client Security -asennuksiin push installation-ominaisuutta. Tässä esimerkkinä luokan B155 asennus.

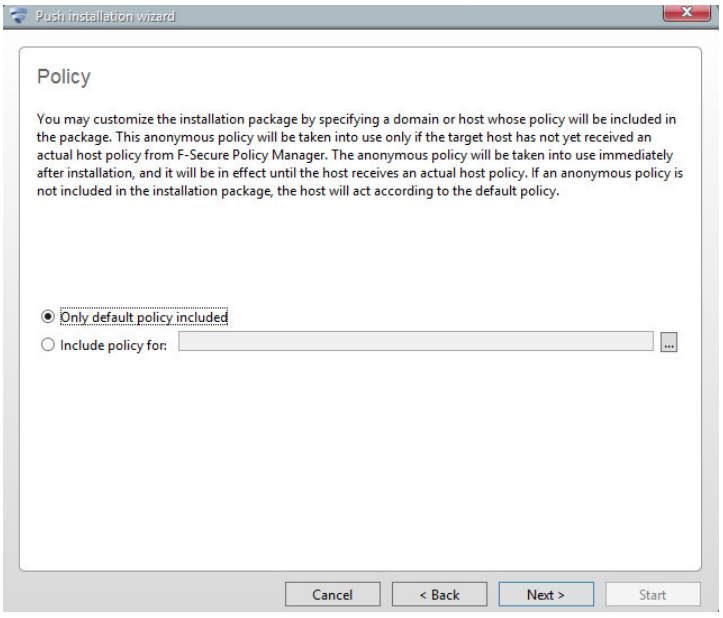
Ensimmäisessä vaiheessa määritellään hostit, joihin asennus tehdään. Asennettavat koneet voidaan valita joko host-nimen tai IP-osoitteen perusteella kirjoittamalla kyseinen kriteeri Hosts-kenttään. Asensin ohjelmistot host-nimen perusteella.



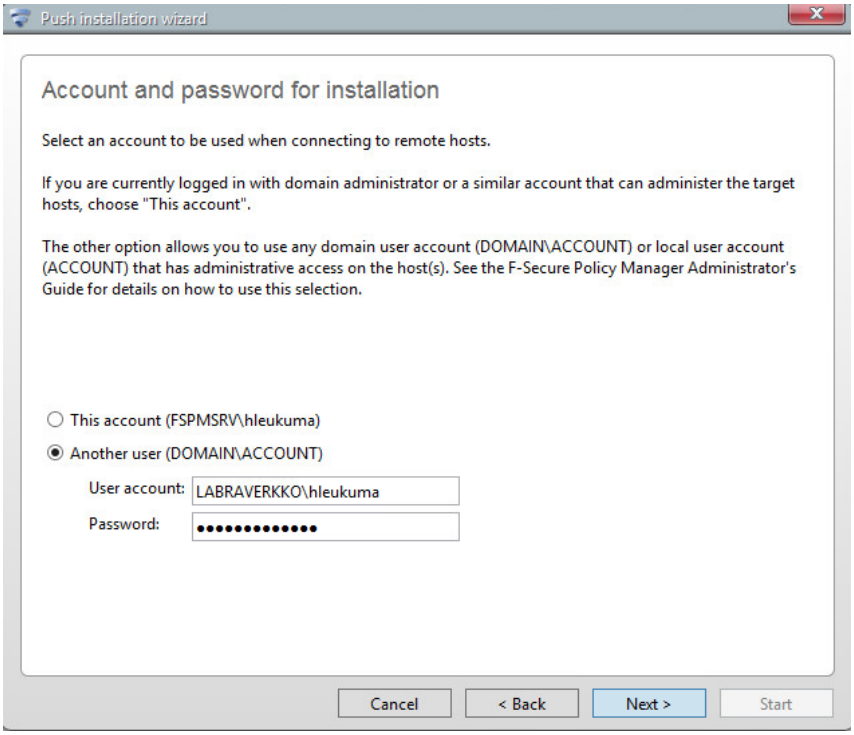
Valitaan haluttu asennuspaketti listasta ja painetaan ”Next”.



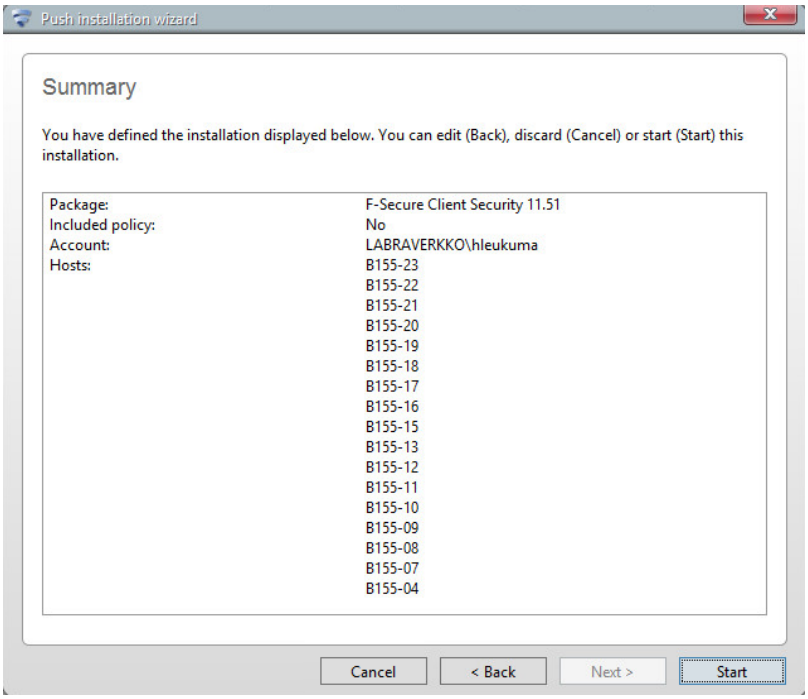
Seuraavassa vaiheessa pakettiin voi liittää jonkin Policy domainin käytännön, joka tulee voimaan heti asennuksen jälkeen. Minä en liittänyt paketteihin mitään käytäntöjä, koska käytössä oli muutenkin vasta oletuskäytännöt. Valinnan jälkeen painetaan ”Next”.



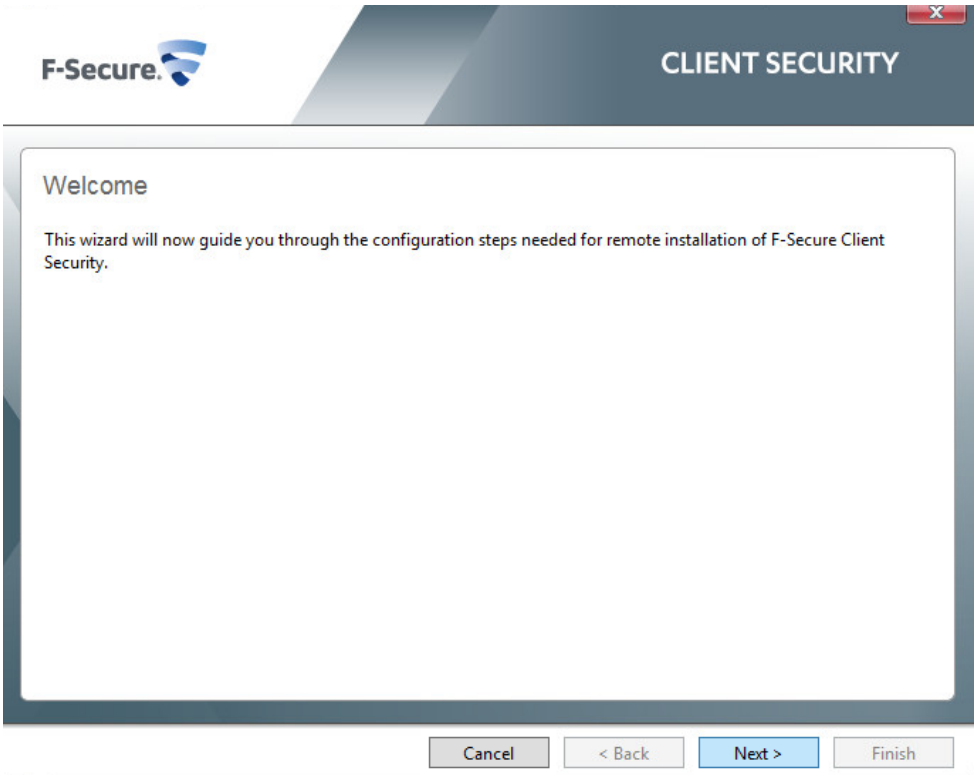
Asennuksen voi suorittaa vain joko domainin tai hostin Administrator-tunnuksilla. Labraverkossa kaikilla on Admin-oikeudet koneisiin. Painetaan ”Next”.

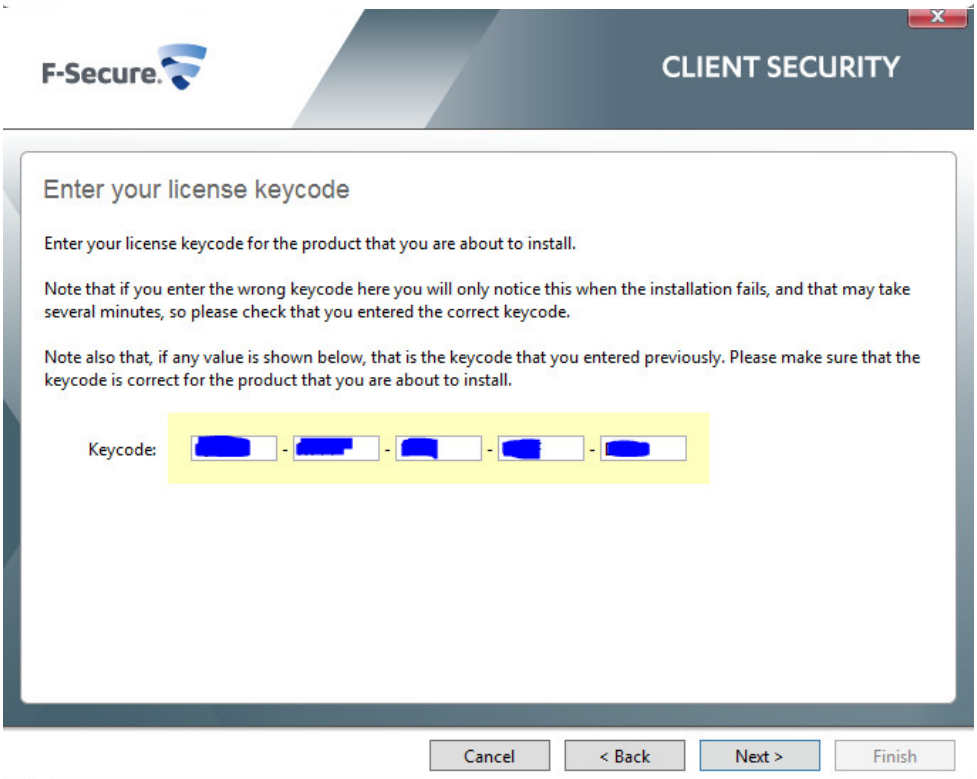


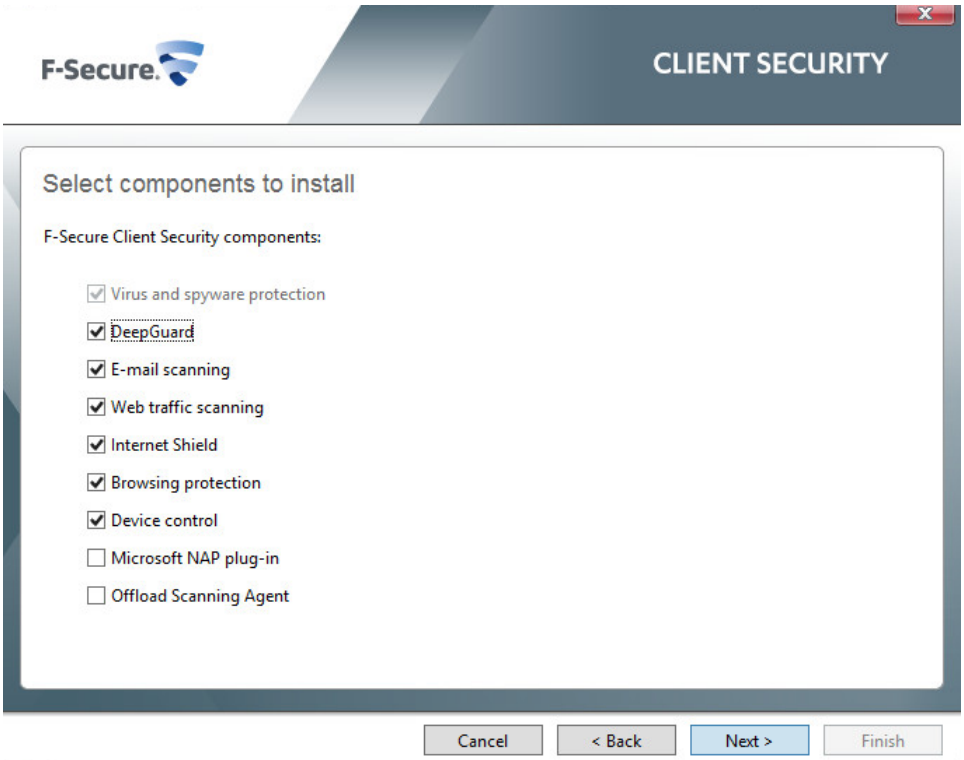
Ennen asennuksen aloitusta näytetään vielä yhteenvetosivu asennuksesta. Painetaan ”Start”. Tämän jälkeen käynnistyy Client Securityn asennus.

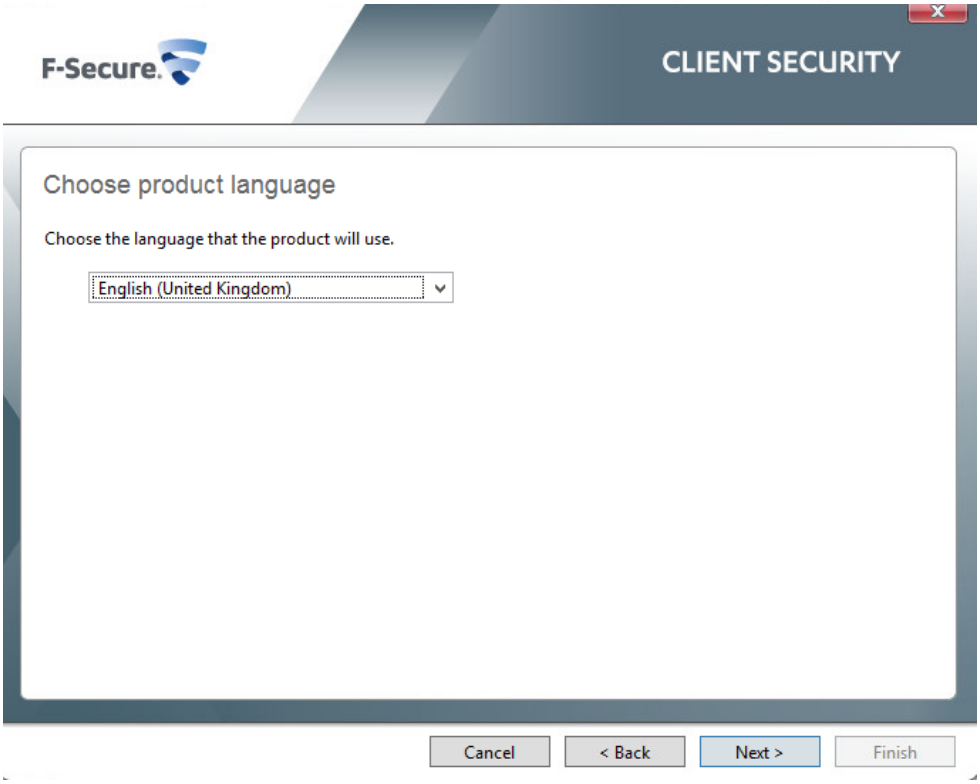


Client Security -asennus

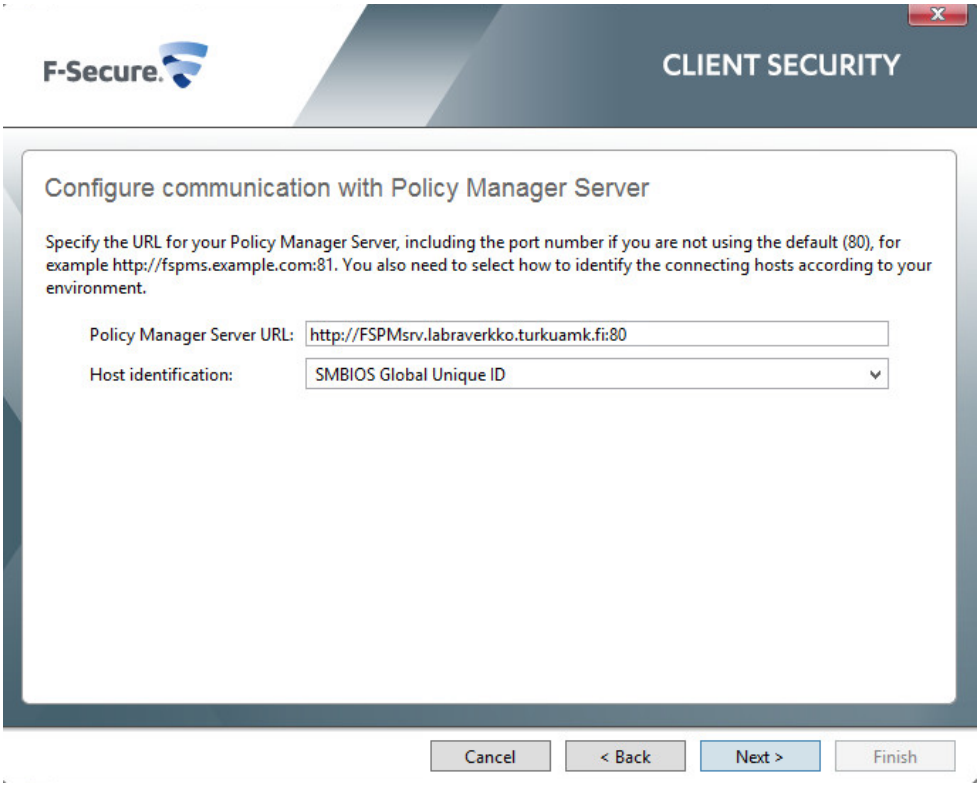


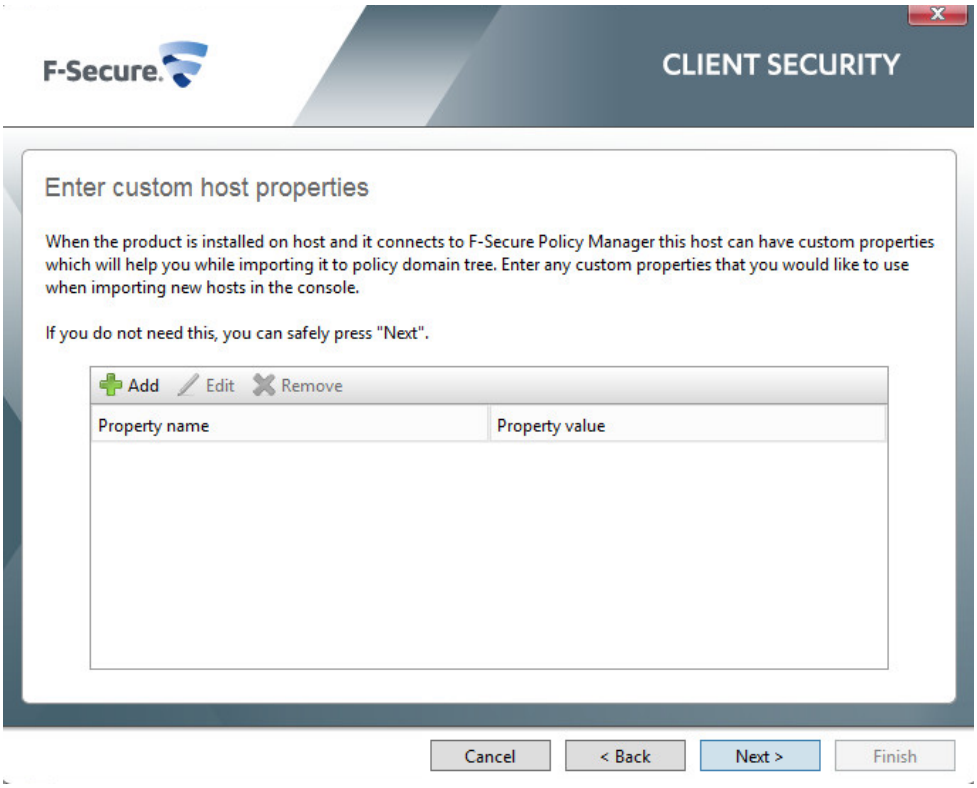


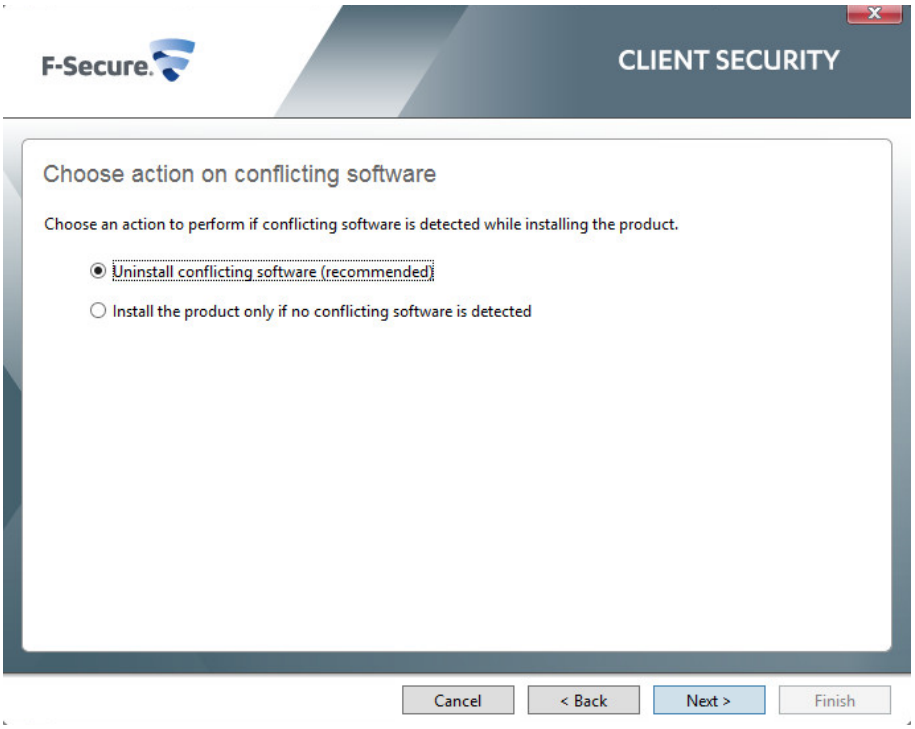

F-Secure.
CLIENT SECURITY
Select components to install
F-Secure Client Security components:
Virus and spyware protection
DeepGuard
E-mail scanning
Web traffic scanning
Internet Shield
Browsing protection
Device control
Microsoft NAP plug-in
Offload Scanning Agent
Cancel
< Back
Next >
Finish


F-Secure.
CLIENT SECURITY
Choose product language
Choose the language that the product will use.
English (United Kingdom)
Cancel
< Back
Next >
Finish

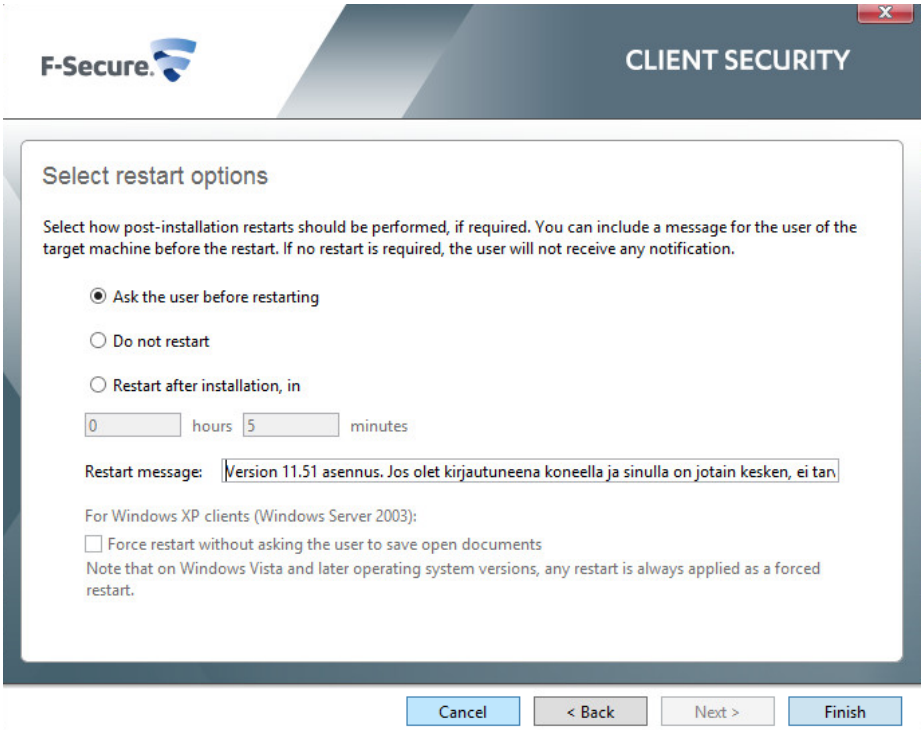
Annetaan Client Securitylle Policy Manager -palvelimen osoite.



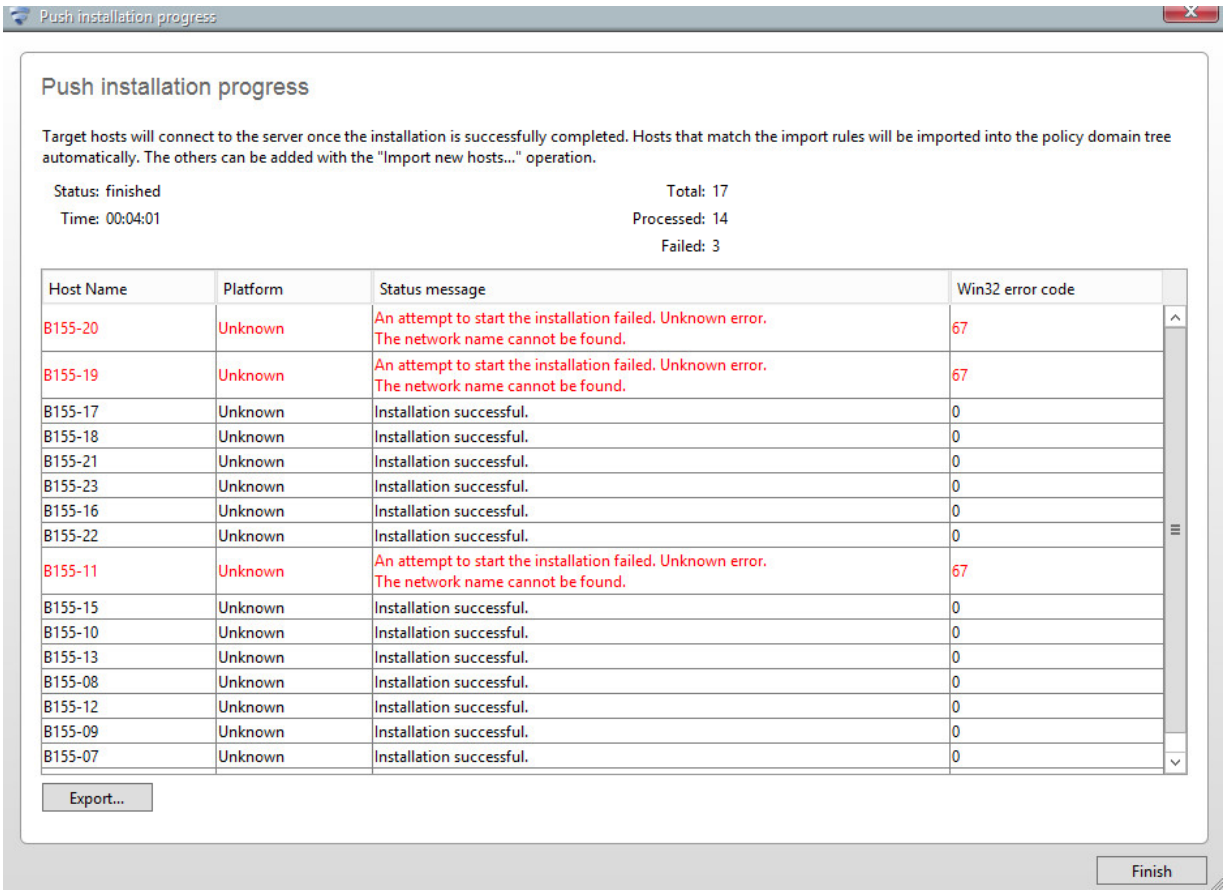




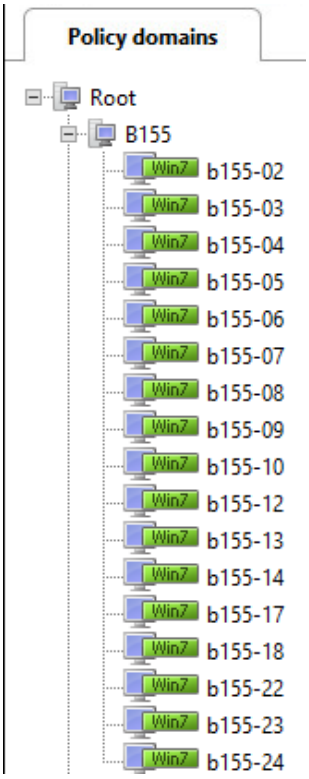
Asennuksen lopussa saa valita käynnistyykö kone uudelleen heti asennuksen jälkeen vai kysytäänkö käyttäjältä, milloin kone käynnistetään uudelleen. Koska asennushetkellä koneilla oli käyttäjiä, halusin asennuksen kysyvän heiltä uudelleenkäynnistyksestä viestin kera.



Alla olevassa kuvassa näkyy asennusten tilanne, kun asennus on valmis. Mustalla on merkitty onnistuneet asennukset ja punaisella epäonnistuneet. Tässä kyseisessä tapauksessa virheitä aiheutti Windowsin palomuuri sekä aikaisemman F-Securen ohjelmiston palomuuri hostilla. Vaikka asennus osaa poistaa aikaisemman päällekkäisen F-Securen ohjelmiston, ei sillä ole oikeuksia ohittaa sen palomuuria. Joten ennen asennusta kaikki koneilla olevat palomuurit pitää ottaa pois käytöstä tai avata tarvittavat portit.



Viimeisessä kuvassa näkyy Policy Domainiin tulleet hostit, joihin on nyt asennettu Client Security. Ne menivät suoraan subdomainin B155 alle tuontisääntöjen mukaisesti. Puuttuvat hostit asensin tämän jälkeen kunhan ensin otin niistä palomuurit pois käytöstä.


Policy domains
Root
B155
Win7 b155-02
Win7 b155-03
Win7 b155-04
Win7 b155-05
Win7 b155-06
Win7 b155-07
Win7 b155-08
Win7 b155-09
Win7 b155-10
Win7 b155-12
Win7 b155-13
Win7 b155-14
Win7 b155-17
Win7 b155-18
Win7 b155-22
Win7 b155-23
Win7 b155-24

Nimi	Kuvaus	Leviämistapa ja turvatoimet	Replikoituva	Itsenäinen
Virus	Viruksia on useita erityyppisiä ja nimisiä, kuten esim. tiedostovirukset, käynnistyslohkovirukset, makrovirukset ja piilovirukset (Stallings & Brown 2008, 224). Yhteistä niillä on, että ne on suunniteltu leviämään ohjelmien kautta. Virukset voivat kantaa ”pay-loadia”, joka voi aiheuttaa kaikkea tiedostojen ja ohjelmien tuhoamisesta harmittomiin kuviin ruudulla. (Stallings & Brown 2008, 220)	Virukset leviävät ohjelmien kautta, jotka voivat olla piilotettuina sähköpostin liitetiedostoon (suoritettavaan tiedostoon tai dokumenttiin), levykkeen käynnistyslohkoon tai muistitikkuun (Tietoturvaopas 2014b). Virukset eivät tarvitse verkkoa levitäkseen vaan ne leviävät tarttumalla ohjelmasta toiseen (Stallings & Brown 2008, 220). Virukset havaitaan ja poistetaan virustorjuntaohjelmistoilla, joissa on nykyään myös ennaltaehkäiseviä reaaliaikaisia virustorjuntakomponentteja.	Kyllä	Ei
Mato	Madot on suunniteltu leviämään ja lisääntymään verkossa. Pelkästään leviämään suunniteltu mato voi aiheuttaa suurta haittaa viemällä verkon kaistaa. Mato voi myös sisältää ”pay-loadin”, joka voi mm. poistaa tiedostoja, avata takaoven koneelle tai sisältää niin kutsutun Troijan hevosen. (Stallings & Brown 2008, 231.)	Mato leviää järjestelmästä järjestelmään verkossa. Saavuttuaan kohteeseensa mato aktivoituu. Se replikoituu ja leviää seuraavaan kohteeseen verkossa. Mato etsii verkkoon kytkettyjen tietokoneiden tietoturva-aukkoja tai saattaa yrittää levitä sähköpostin välityksellä lähettämällä itsensä kaikkiin osoitekirjan osoitteisiin. Nykyaikaisissa virustorjuntaohjelmissa on suojaus matoja vastaan. (Stallings & Brown 2008, 231.)	Kyllä	Kyllä
Troijalainen	Ohjelma, joka esittää olevansa jokin hyödyllinen sovellus tai rutiininomainen päivitys, mutta sisältääkin koodia, jolla on jokin toinen tavoite. Se voi antaa hakkerille luvattoman etäyhteyden koneelle, varastaa tietoa tai aiheuttaa muita harmeja järjestelmälle. (Stallings & Brown 2008, 218.)	Käyttäjä asentaa ohjelman, mutta ei tiedä piilotetusta koodista. Troijalainen käynnistyy heti tai loogisena pommina tietyllä hetkellä. Troijalainen voi olla vaikea huomata. Se voi myös aiheuttaa selvää koneen hidastumista. Turvatoimena kannattaa olla tietoinen asentamiensa ohjelmien alkuperästä.	Ei	Ei
Looginen pommi	Käyttäjän tietämättä ohjelmaan sijoitettu koodi, joka ehtojen täyttyessä laukaisee luvattoman toimen. Se voi poistaa ja muuttaa tiedostoja tai aiheuttaa muuta vahinkoa. (Stallings & Brown 2008, 218.)	Mikä tahansa ohjelma voi olla looginen pommi, jos ohjelmaan on piilotettu koodi joka aktivoituu määritetyllä hetkellä ja käyttäjä on tietämätön siitä.	Ei	Ei
Mainos- ja vakoiluohjelmat	Ohjelmat, jotka käyttäjän tietämättä keräävät tietoja koneelta ja välittävät ne eteenpäin. Se voi aiheuttaa myös pop-up-mainoksia ja yrittää ohjata käyttäjän halutulle sivulle. Lisäksi vakoiluohjelmat voivat avata takaoven tietokoneelle. (Tietoturvaopas 2014a.)	Leviävät Ilmaisohjelmien mukana (Tietoturvaopas 2014a). Melkein kaikki kaupalliset virustorjuntaohjelmistot löytävät vakoilu- ja mainosohjelmat.	Ei	Kyllä ja Ei
Takaovi	Mikä tahansa mekanismi, joka ohittaa normaalin käyttäjän todennuksen mahdollistaen luvattoman pääsyn ohjelmaan (Stallings & Brown 2008, 216-217).	Leviävät madon tai rootkitin mukana. Se voi olla myös sovelluskehitystä varten tehty ”maintenance hook”, joka ohittaa pitkän tunnistautumisprosessin. Turvatoimiin täytyy keskittyä jo sovelluskehityksessä. Myös ohjelmistopäivitykset ovat tärkeitä ehkäisykeinoja. (Stallings & Brown 2008, 216- 217.)	Ei	Ei
Rootkit	Rootkit ei itse ole haitallinen vaan se pyrkii piilottamaan muiden haittaohjelmien ”pay-loadin” virustorjuntaohjelmalta. (PC tools 2014)	Hyökkääjä asentaa rootkitin joko automaattisesti tai manuaalisesti koneeseen saatuaan sen ensin hallintaansa. Rootkit on vaikea havaita, koska se aktivoituu jo ennen kuin käyttöjärjestelmä käynnistyy. Markkinoilla on erillisiä rootkittien poisto-ohjelmia, mutta myös nykyiset virustorjuntaohjelmistot pääsevät pintaa syvemmälle. (PC tools 2014)	Ei	Ei