Tampereen ammattikorkeakoulu

F-Secure Policy Managerin käyttöönotto

Oskari Jaakkola

OPINNÄYTETYÖ
Lokakuu 2019

Tietojenkäsittely
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkkopalvelut

JAAKKOLA, OSKARI:
F-Secure Policy Managerin käyttöönotto

Opinnäytetyö 45 sivua, joista liitteitä 8 sivua
Lokakuu 2019

Opinnäytetyön tavoitteena oli ottaa käyttöön Combitech Oy:n uudessa ympäristössä virustorjuntohjelma ja laitekohtainen palomuuri. Tarkoituksena oli konfiguroida ympäristöön F-Secure Policy Manager. Uuteen ympäristöön haluttiin viranomaisen suojaustason IV-luokitus. Luokituksen saamiseksi ympäristössä pitää olla laitekohtainen palomuuriratkaisu.

Ympäristöön otettiin käyttöön F-Secure Policy Manager 14.20. F-Secure Policy Manager on asennettu RHEL 8 -käyttöjärjestelmää käyttävälle virtuaalikoneelle. RHEL 8 ja F-Secure Policy Manager 14.20 yhteensopivuudesta ei ollut tietoa työn alussa, mutta yhteensopivuuden kanssa ei ilmennyt ongelmia. Kun komponentit oli todettu toimintakuntoisiksi, selvitettiin F-Secure Policy Managerin ominaisuudet. Käyttöönotettiin Combitech Oy:n lisenssiin kuuluvat hyödyllisiksi todetut ominaisuudet.

Lopputuloksena oli päätelaitteiden virustorjunnasta ja palomuurista vastaava työkalu, jota voidaan hallita järjestelmänvalvojien työasemilta. Ympäristössä on verkkopalomuuri, joka vähentää F-Secure Policy Managerin hyödyllisyyttä. Tämä ei tee F-Secure Policy Managerista turhaa, koska se on pakollinen suojaustason IV-luokituksen saamiseksi. Tämän lisäksi on hyvä muistaa, että tietoturva koostuu kerroksista, eikä yksikään lisäkerros ole turha.

Asiasanat: F-Secure, virustorjunta, tietoturva, käyttöönotto

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme int Business Information Systems
Network Services

JAAKKOLA, OSKARI:
Deployment of F-Secure Policy Manager

Bachelor's thesis 45 pages, appendices 8 pages
October 2019

The goal of this thesis was to deploy antivirus software and a host-based firewall into Combitech Oy's new network. The aim of this thesis was to configure F-Secure Policy Manager into the network, which will be protection level IV network. In order to get the official protection level IV classification, a network must have host-based firewall deployed.

F-Secure Policy Manager is version 14.20 and it runs on virtual machine with the new RHEL 8 operating system. There was no official statement about the compatibility of Policy Manager 14.20 and RHEL 8 at the time of the deployment. In the end, there were no compatibility issues between the two. After all Policy Manager's components were installed, the research into its features began. Features that were deemed useful and were included in Combitech Oy's license were implemented.

The end result was a tool, which can be used to control the endpoint firewalls and antivirus software. The network also has a firewall device, which does most of the network protection, making Policy Manager less useful. It does not render Policy Manager fully useless, as it is needed in order to get the protection level IV classification for the network. It is also important to keep in mind that information security is based on layers and therefore no layer is useless.

Key words: F-Secure, antivirus, information security, deployment

SISÄLLYS

LYHENTEET JA TERMIT

AD	Active Directory
CA	Certificate Authority
GPO	Group Policy Object
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LDAP	Lighweight Directory Access Protocol
PKI	Public Key Infrastucture
PM	Policy Manager
PMC	Policy Manager Console
PMCS	Policy Manager Client Security
PMS	Policy Manager Server
PMSS	Policy Manager Server Security
SSL	Secure Sockets Layer

1 JOHDANTO

F-Secure Policy Manager on F-Securen tarjoama virustorjuntakokonaisuus yrityksille. Policy Managerin avulla voidaan keskitetysti hallita Windows-työasemien ja palvelimien palomuureja, sekä asentaa erilaisille päätelaitteille niille sopiva virustorjuntaratkaisu. Yhdellä palvelimella on varsinainen Policy Manager Server -ohjelma. Policy Manager Serveriä hallinnoidaan Policy Manager Consolella. Päätelaitteille asennetaan jokin virustorjuntaohjelma, esimerkiksi Client Security Windows-työasemille tai Server Security Windows-palvelimille. Policy Managerista asennettiin versio 14.20, Client Securitysta versio 14.10 ja Server Securitysta versio 14.00. Opinnäytetyössä käsitellään vain F-Secure Policy Manageria, eikä muuta ympäristöä.

Opinnäytetyön toimeksiantajana toimi Combitech Oy. Combitech Oy on alkujaan suomalainen yritys, joka on osa kansainvälistä Saab konsernia. Combitech Oy on rakentanut uutta ympäristöä, johon halutaan suojaustason IV-luokitus.

Mikäli liikenne poistuu aliverkostaan, se menee verkkopalomuurin läpi. Ympäristössä on verkkopalomuuri, mutta saadakseen virallisen ST IV-luokituksen, ympäristön työasemilla on oltava oma ohjelmistopalomuuri. Windowsin oma palomuuri täyttää tämän ehdon. Sen hallitseminen GPO:lla on kankeaa, joten ympäristöön päätettiin ottaa käyttöön F-Secure Policy Manager.

Ympäristöä käyttävät ohjelmoijat. Tästä seuraa muutamia tavallisuudesta poikkeavia asetuksia. Jotta ohjelmoijat voisivat asentaa ja käyttää tarvitsemiaan ohjelmia, täytyy heidän tunnuksillaan olla paikallisen järjestelmänvalvojan oikeudet. Työasemilla tulee olemaan ohjelmoijien tekemiä ohjelmia, joita virustorjuntaohjelmat eivät tunnista. Tästä voi koitua ongelmia, jos tuntemattomien ohjelmien suoritusoikeuksia rajoitetaan liikaa.

2 TAUSTAA

Combitech Oy on Pohjoismaissa operoiva kyberturvallisuuteen keskittyvä yritys, joka on osa Saab konsernia. Suomessa Combitech Oy:ltä löytyy toimipiste Espoosta, Tampereelta, Jyväskylästä ja Säkylästä. Työntekijöitä näissä neljässä eri toimipisteessä on yhteensä yli 80. (Combitech verkkosivut – Tietoja meistä.)

Toimin Combitech Oy:llä Tampereen toimipisteessä ICT-tukihenkilönä. Combitech Oy:lla on nyt rakennettu suojaustason IV -ympäristöä. Asensin sinne F-Secure Policy Managerin. Ympäristön arkaluontoisuuden vuoksi opinnäytetyön kaikista kuvista poistettiin IP-osoitteet sekä palvelinten ja työasemien nimet.

Suojaustasoja on neljä: ST IV, ST III, ST II ja ST I. Jotta ympäristö voi saada ST X (X on muuttuja) -luokituksen, sen täytyy täyttää tietyt vaatimukset. Nämä vaatimukset löytyvät Katakrista. ST I:tä ei ole Katakrissa määritelty. Katakri on viranomaisille tehty auditointityökalu, jolla valvotaan yritysten kykyä käsitellä ja säilyttää viranomaisten salassa pidettävää tietoa oikein. (Katakri 2015.) Tämän opinnäytetyön kannalta merkittävin säädös Katakrissa on: ”Tarjottavat (erityisesti verkko)palvelut on minimoitu ja rajattu vain välttämättömiin. On lisäksi käytössä verkkoliikenteen vain välttämättömään rajaava (host-based) palomuuriratkaisu.” (Katakri 2015. s. 42.) Tämä tarkoittaa, että ST IV -ympäristössä on oltava laitekohtainen palomuuriratkaisu.

Katakri ei aseta tietoturvalle vaatimuksia, vaan sen vaatimukset perustuvat olemassa olevaan lainsäädäntöön sekä kansainvälisiin tietoturvallisuusvelvoitteisiin. Katakrin vaatimukset jaetaan kolmeen eri osa-alueeseen. (Katakri 2015.)

Ensimmäinen osa-alue koskee turvallisuusjohtamista, joka tarkoittaa organisaation turvallisuusjohtamisen valmiuksien sekä kyvykkyyden varmistamista. Salassa pidettävien tietojen fyysisen käyttöympäristön vaatimukset kuvataan toisessa osa-alueessa. Kolmas osa-alue koskee salassa pidettävien tietojen teknistä tietoturvallisuutta. (Katakri 2015.) Ainoastaan kolmas osa-alue vaikuttaa tähän opinnäytetyöhön.

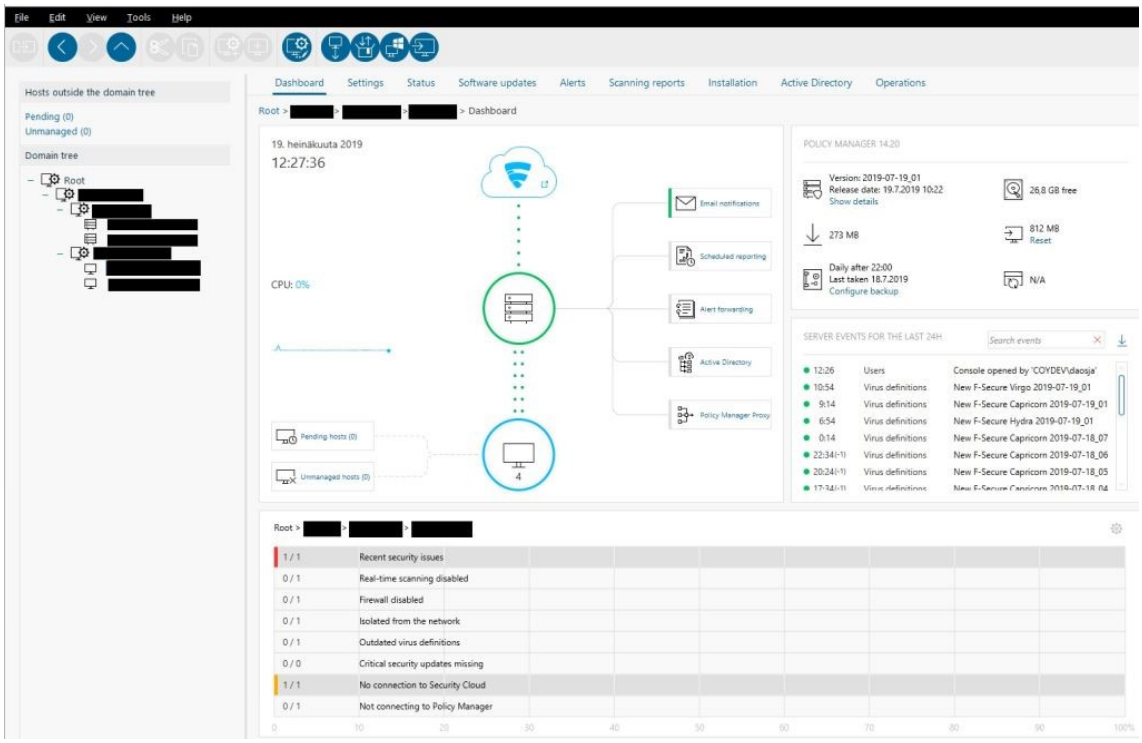
3 F-SECURE POLICY MANAGER

3.1 Yleistä

F-Secure Policy Manager on F-Securen tarjoama virustorjuntaratkaisu yritysympäristöön. Virustorjuntaohjelmat tarkastelevat tieto koneella olevia ohjelmia, ja vertaavat niitä tunnettujen viruksien tietokaantaansa. Jos ohjelman koodi muistuttaa virusta, virustorjuntaohjelma varoittaa käyttäjää ja estää epäilyttävän ohjelman toiminnan. Virustorjuntaohjelmien reagointi viruksiin on yleensä muokattavissa. Käyttäjä/järjestelmänvaloja voi määritellä mikä tunnistetaan virukseksi ja miten sellaisen kanssa toimitaan. Usein etenkin yrityksen kehitysympäristössä tulee vastaan poikkeuksia, kuten jokin yrityksen oma ohjelma. Poikkeuksellisten tilanteiden takia virustorjuntaohjelman säännöstössä on sallittava toimintoja, joita ei sallittaisi oletusasetuksilla.

Yritysympäristön vaatimukset eroavat suuresti kotikäytöstä. Kotona on mahdollista ladata virustorjuntaohjelma ja antaa sen tehdä työnsä. Malli ei toimi yrityksellä, jolla voi olla käytössä satoja työasemia. Virustorjuntaohjelman asentaminen ja tämän säännöstön muokkaaminen erikseen jokaisella työasemalla olisi liian työlästä. Tämän takia yrityksillä on yleensä jokin F-Secure Policy Managerin kaltainen työkalu, joka mahdollistaa kaikkien yrityksen koneiden virustorjunnan keskitetyn hallinnan.

F-Secure Policy Manager 14.xx ja sen tarjoama virustorjuntaohjelma Client Security 14.xx poikkeavat aikaisemmista versioista. Aikaisemmissa versioissa työasemien palomuurina on käytetty F-Securen omaa palomuuriohjelmaa. Tästä on luovuttu ja nyt F-Secure Policy Manager hallinnoi Windows-päätelaitteissa oletuksena olevaa Windows Defender -palomuuria. Yksinkertaistettuna F-Secure Policy Manager on työkalu, jolla hallitaan keskitetysti päätelaitteiden palomuureja ja virustorjuntaohjelmia. Alla olevassa kuvassa 1 on käyttökunnossa olevan Policy Managerin käyttöliittymä.



KUVA 1. Käyttökunnossa olevan Policy Manager 14.20:n käyttöliittymä

3.2 Sertifikaatti

Pelkistettynä sertifikaatti on digitaalinen passi. Sertifikaatteja käytetään tietotekniikassa tunnistautumiseen ja tiedon salaamiseen. Salaaminen perustuu algoritmeihin ja avaimiin. Tieto muutetaan algoritmilla epäluettavaan muotoon. Algoritmeissa käytetään avaimia lopputuloksen arvaamattomuuden saavuttamiseksi. Avaimia on asymmetrisiä ja symmetrisiä.

Asymmetriset avaimet luodaan aina pareittain. Pari muodostuu julkisesta avaimesta ja yksityisestä avaimesta. Julkiset avaimet ovat avoimesti saatavilla kaikille. Yksityistä avainta ei jaeta. (Rouse 2018.)

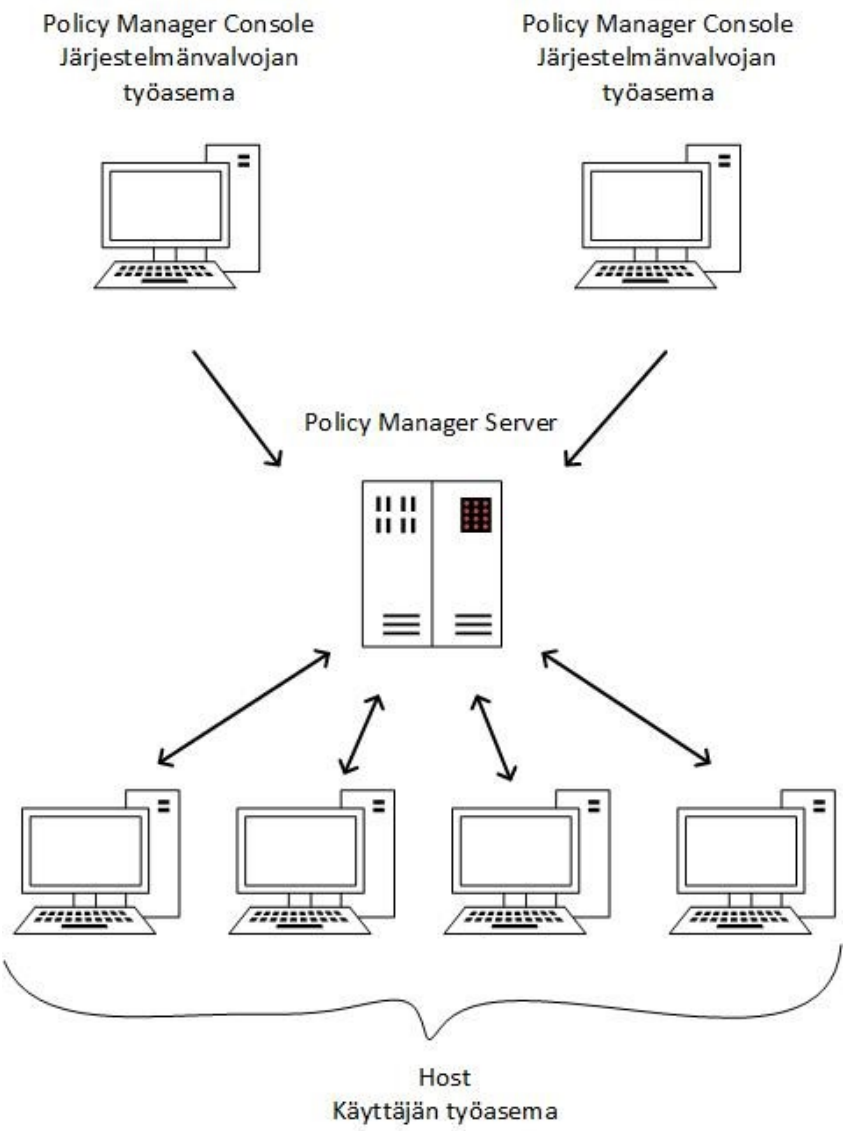
Tietoa salataan valitulla algoritmilla. Algoritmin yksi muuttuja on julkinen avain. Salauksen voi purkaa ainoastaan julkista avainta vastaavalla yksityisellä avaimella. Näin ainoastaan viestin tarkoitettu vastaanottaja voi lukea viestin.

Vähemmän turvallinen vaihtoehto on symmetrinen avain, jossa käytetään samaa avainta tiedon salaamiseen ja salauksen purkamiseen. Tämä on huomattavasti nopeampaa kuin asymmetrinen salaaminen. Usein asymmetristä avainta käytetään symmetrisen avaimen neuvotteluun ja viemiseen kummallekin osapuolelle. Sitten symmetristä avainta voidaan käyttää nopeaan tiedon salaamiseen ja purkamiseen.

Sertifikaatit jakavat sertifikaatin omistajan julkista avainta (Rouse 2018). Certificate Authority (CA) eli sertifikaatti auktoriteetti allekirjoittaa sertifikaatteja. Kun taho luottaa johonkin sertifikaatti auktoriteettiin se luottaa kaikkiin tämän sertifikaatti auktoriteetin allekirjoittamiin sertifikaatteihin. Usein verkossa on oma sertifikaatti auktoriteetti, johon kaikki ympäristön laitteet luottavat. Näin ympäristön laitteet luottavat toisiinsa, mutta eivät mihinkään ylimääräiseen. Tämä lisää myös tiedon salaamisen hallintaa.

3.3 Rakenne

F-Secure Policy Manager koostuu Serveristä, Consolesta ja hosteista. Serveri on varasto ajettaville päivityksille ja menettelytavoille. Consolella vuorostaan hallitaan tätä varastoa. Kuva 2 visualisoi komponenttien välisiä suhteita. Policy Managerin hallinnan piirissä olevia päätelaitteita kutsutaan hosteiksi. Hosteille asennetaan sen käyttöjärjestelmälle sopiva Policy Managerin tarjoama virustorjuntaohjelma. Tämän ohjelman mukana työasemalle asentuu Management Agent. Management Agent kommunikoi Policy Managerin muiden komponenttien kanssa ja pitää työaseman Policy Manageriin liittyvät ohjelmistopäivitykset, virustunnisteet ja menettelytavat ajan tasalla. Policy Managerista löytyy myös Web Reporting, joka on Policy Manager Serverin mukana tuleva web-pohjainen raportointityökalu. Tämän avulla saadaan statistiikkaa hostien tilanteesta.



KUVA 2. Policy Managerin komponenttien väliset suhteet

3.3.1 Policy Manager Server

Server on säilö menettelytavoille ja ohjelmistopaketeille (Policy Manager - Admin guide), joita järjestelmänvalvojat haluavat asentaa hosteille. Lista PMS (Policy Manager Server) vaatimuksista on liitteessä 1.

PMS:iin ei tarvitse juurikaan koskea asennuksen jälkeen. PMS on vain käynnissä ja Policy Manager Consolella tehdään kaikki muutokset. PMS välittää tietoa hosteille käyttäen pääsääntöisesti https-protokollaa, mutta esimerkiksi virustunnisteiden päivitykset siirretään http-protokollalla.

3.3.2 Policy Manager Console

Policy Manager Console on java-pohjainen ohjelma, joka voidaan asentaa yhdelle tai useammalle työasemalle. Ympäristössä johon PM (Policy Manager) asennettiin PMS on omalla koneella ja PMC (Policy Manager Console) löytyy järjestelmänvalvojan/järjestelmänvalvojien työasemilta. On myös mahdollista asentaa PMS ja PMC samalle koneelle. Koko lista PMC:n järjestelmävaatimuksista löytyy liitteestä 2. PMC:llä määritellään F-Secure Policy Managerin toiminta. PMC:n avulla järjestelmänvalvoja voi määritellä käyttäjien oikeuksia, järjestellä hostit loogisiin ryhmiin (policy domaineihin), tarkastella hostien statuksia, käsitellä hälytyksiä, hallita etäasennuksia ja katsella raportteja. Järjestelmänvalvojan luomat menettelytavat voivat kohdistua yhteen hostiin tai kokonaiseen policy domainiin. Policy domain sisältää useita hosteja. (Policy Manager - Admin Guide.)

Hosteja voidaan lisätä monella eri tavalla Policy Manageriin. Näitä voidaan tuoda suoraan Windows-toimialueesta tai Active Directorysta (Policy Manager – Admin Guide). Uudet potentiaaliset hostit voidaan myös tuoda automaattisesti säännöllä. Jotta päätelaite näkyy potentiaalisena hostina siellä on oltava Policy Managerilta saatu virustorjuntaohjelma (Client/Server/linux Security tai vastaava). On myös mahdollista tuoda hosti täysin manuaalisesti, eli luoda hosti ennen kuin siltä löytyy Policy Managerilta saatu virustorjuntaohjelma.

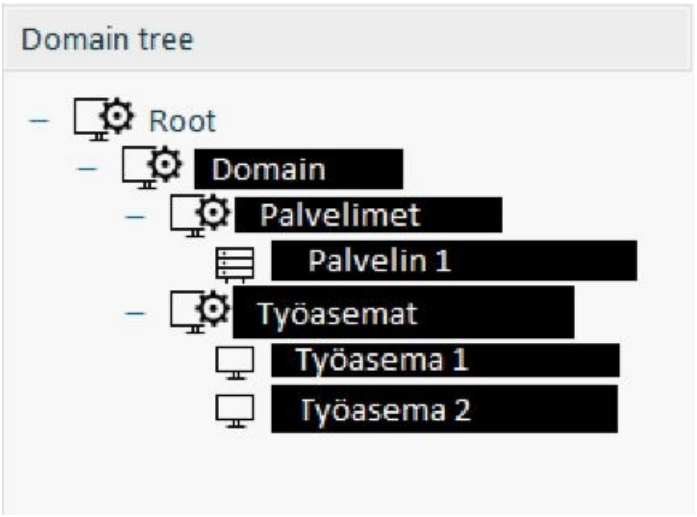
Ohjelmistopaketteja voidaan jakaa hosteille PMC:n avulla usealla eri tavalla. Ohjelmistopaketeilla tarkoitetaan erilaisille päätelaitteille suunnattuja suojausohjelmia. Näitä ovat esimerkiksi Server Security ja Client Security. Tämmöisen ohjelmistopaketin voi muuntaa Policy Managerilla msi-tiedostoksi ja sen jälkeen se voidaan työntää hostille. Ohjelmiston voi myös ladata msi-tiedostona esimerkiksi USB-muistitikulle, viedä työasemalle ja asentaa paikallisesti.

3.3.3 Host

Host on suojattava päätelaite. Hostille asennetaan Policy Managerilta saatava virustorjuntaohjelma, jonka mukana asentuu Management Agent. Management

Agent tekee koneelle tarvittavat muutokset. Agentti pitää päätelaitteen PM:iin liittyvät asetukset ja menettelytavat ajan tasalla.

Kun päätelaitteelle on asennettu jokin Policy Managerin virustorjuntaohjelmista, se voidaan tuoda PMC:lla hostiksi. Tämän jälkeen sen toimintaa voidaan hallita ja määritellä. Hostien säännöstöä ja menettelytapoja voidaan määritellä yksilökohtaisesti tai hostit voidaan jakaa ryhmiin. Kaikki ryhmän hostit saavat sille ryhmälle määritetyt policyt. Näitä ryhmiä kutsutaan policy domaineiksi. Policy domaineja voi olla sisäkkäin (kuva 3), jolloin säännöt periytyvät.



KUVA 3. ”Palvelimet” -policy domainilla on oletusarvona ”Domain” -policy domainin asetukset.

Myös palvelin voi olla hosti. Palvelimille ei voi asentaa Windows-työasemille suunnattua Client Security -virustorjuntaohjelmaa. Palvelimille on Server Security -virustorjuntaohjelma, joka toimii pääsäännöllisesti Windows-palvelimilla. Lista Server Security -ohjelmaa tukevista käyttöjärjestelmistä ja laitteiston vaatimuksista löytyy liitteestä 3.

3.3.4 Web Reporting

F-Secure Policy Managerilla on web-pohjainen raportointijärjestelmä. Tällä järjestelmänvalvoja voi luoda kuvallisia raportteja, joista näkee mitkä hostit ovat haavoittuvaisia tai saastuneita. Raportit pohjautuvat tietoon, jota hosteilla olevat

Management Agentit lähettävät PMS:lle. Raportit voidaan myös muuttaa HTML- tai PDF -tiedostoiksi. (Policy Manager – Admin Guide.)

3.4 Ominaisuudet

F-Securen sivuilla on lista Policy Managerin ominaisuuksista. Ominaisuuksiksi on listattu ohjelmiston jakaminen, menettelytapojen hallinta ja konfiguroiminen sekä tapahtumien/suorituskyvyn/tehtävien hallinta (Policy Manager – Admin Guide).

Ohjelmiston jakaminen ominaisuutena tarkoittaa ohjelmistopakettien keskitettyä asentamista päätelaitteille. Policy Managerilla voidaan keskitetysti asentaa- esimerkiksi PMCS (Policy Manager Client Security) hosteille, sekä päivittää niiden virustunnisteita. (Policy Manager – Admin Guide.)

Keskitetty menettelytapojen hallinta ja konfiguroiminen mahdollistaa sen, että hostit saavat PMS:ltä tietoturvaa koskettavat menettelytavat. Menettelytapoja määrittelevien tiedostojen yhtenäisyys varmistetaan ohjelmien tapaan digitaalisella allekirjoituksella (Policy Manager – Admin Guide).

Policy Managerilla tapahtumien hallinta tarkoittaa tapahtumien lokitusta joko kolmannen osapuolen syslog-palvelimelle tai Windowsin omaan Event Viewer -ohjelmaan. Lokeja voidaan myös lähettää sähköpostina. (Policy Manager – Admin Guide.)

Tehtävien hallinta on erilaisten virusskannauksien määrittelyä ja hallintaa. Skannauksia voi suorittaa Policy Managerilla etäältä tai paikallisesti. (Policy Manager – Admin Guide.)

Policy Managerissa on paljon erilaisia ominaisuuksia/asetuksia. Monet näistä tekevät osin samoja asioita. Kaikki ominaisuudet eivät toimi kaikilla päätelaitteilla.

3.4.1 DeepGuard

DeepGuard on hosti-kohtainen IPS (Intrusion Prevention System) (Policy Manager – Admin Guide). IPS tarkkailee hostilla käynnissä olevien ohjelmien toimintaa. Mikäli ohjelman toiminta on epäilyttävää DeepGuard estää sen. Tämä eroaa klassisesta virustorjunnasta, koska se ei tarkastele pelkästään ohjelman koodia, vaan myös tämän toimintaa.

DataGuard on DeepGuardin lisäominaisuus. DataGuard estää epäluotettavia ohjelmia tekemästä muutoksia kansioihin. Järjestelmänvalvoja voi määritellä mitkä kansiot DataGuard suojaa ja mitkä ohjelmat luokitellaan luotettaviksi. (Policy Manager – Admin Guide.)

3.4.2 Application control

Järjestelmänvalvoja voi estää ohjelmien/skriptien asentamisen ja ajamisen hosteilla Application control -ominaisudeen avulla. Tämä ominaisuus on saatavilla ainoastaan PMCS versiossa 14.00 ja sitä uudemmissa. (Policy Manager – Admin Guide.)

3.4.3 Web traffic HTTP Scanning

HTTP-skannauksella voidaan suojata hostia http-verkkoliikenteestä saatavilta viruksilta. HTTP Scanning skannaa sisään tulevan liikenteen, ja poistaa virukset. HTTP-skannaus voidaan konfiguroida antamaan käyttäjälle ilmoitus, kun virus on estetty. Skanneri antaa eri sivuille erilaisia luokituksia. Luokituksia ovat seuraavat: Unknown/unrated, safe, unsafe, suspicious ja malicious. (Policy Manager-Admin Guide.)

Unknown/unrated tarkoittaa sitä, että sivun osoitetta ei ole vielä arvioitu tai siihen ei saada yhteyttä testin aikana. Safe tarkoittaa sivun osoitteen olevan turvallinen ja käyttäjä voi tietoisesti ladata sieltä mitä tahansa. Suspicious-luokituksen saa-

neet sivustot ovat yhdistetty epärehelliseen ja/tai spämmiä muistuttavaan toimintaan. Malicious tarkoittaa sivuston olevan epäluotettava. Tämän luokituksen saaneilta sivustoilta on löytynyt erilaisiin hyökkäyksiin liittyviä elementtejä (esimerkiksi skriptejä/koodia/phisausta). (Policy Manager – Admin Guide.)

Policy Manager tarjoaa myös mahdollisuuden manuaaliseen skannaukseen. Manuaalinen skannaus käynnistetään skannattavalta päätelaitteelta, eikä PMC kautta. Tälläisella skannauksella voi skannata koko systeemin, vain yhden tiedoston tai vain yhden levyn. Manuaalisia skannauksia voidaan myös ajastaa. (Client Security For Windows - Guide.) Client Securityn voi myös laittaa skannaamaan reaaliajassa, jolloin kevyt skanneri on jatkuvasti päällä. Avattuja ja käytössä olevia tiedostoja skannataan tällöin koko ajan hiljaisesti taustalla. (Policy Manager – Admin Guide.)

3.4.4 Selaimen suojaaminen

Browsing protection -ominaisuus estää käyttäjän pääsyn epäilyttäville ja/tai kielletyille sivuille. Browsing protectionin toiminta pohjautuu nettisivuijen luotettavuuteen. Arvio luotettavuudesta tulee F-Securen keräämän tiedon perusteella. (Client Security for Windows - Guide.)

3.4.5 Device Control

Device Control on laitteiston hallintaan tarkoitettu ominaisuus. Tällä voidaan estää haitallisten laitteiden liittäminen tietojärjestelmään. Monet tietoturvallisuuteen liittyvät rikokset ovat perustuneet saastuneen USB-muistitikun kytkemiseen yrityksen tietokoneeseen. Tämän kaltaisia inhimillisiä (tai tahallisia) virheitä pyritään estämään Device Control -ominaisuudella. Kun estetty laite liitetään hostiin Device Control laittaa liitetyn laitteen pois päältä estäen tämän pääsyn järjestelmään (Policy Manager – Admin Guide).

3.4.6 Automaattiset päivitykset

Automaattiset päivitykset takaavat sen, että virustorjuntaohjelma pysyy ajan tasalla. Tietoturvaohjelmiin tulevat päivitykset keskittyvät usein paikkaamaan tietoturva-aukkoja, eli päivittämättä jättäminen on tietoturvariski.

Hallitut hostit voidaan konfiguroida hakemaan tietoturvapäivitykset vain, jos niillä on Software Updater päällä. Hostit voivat hakea päivityksiä Policy Manager Serveriltä kolmella eri tavalla: always, if possible ja never. Always pakottaa hostit hakemaan päivitykset aina PMS:ltä. If possible vuorostaan laittaa hostit hakemaan päivityksiä PMS:ltä jos mahdollista, muussa tapauksessa hosti etsii päivityksiä internetistä. Never vaihtoehto pakottaa hostit hakemaan päivitykset aina internetistä. (Policy Manager – Admin Guide.)

3.4.7 Rapid Detection & Response

Rapid Detection & Response on F-Securen älykäs päätelaitteen suojaamiseen tarkoitettu järjestelmä. Se asentaa kevyitä sensoreita valvottavalla päätelaitteelle, jotka tarkkailevat eri ohjelmien toimintaa. Monet hyökkäykset tapahtuvat nykyään ilman erillistä haittaohjelmaa. Tälläisiin hyökkäyksiin voi varautua Rapid Detection & Response -ominaisuudella. (Policy Manager – Admin Guide.)

4 KÄYTTÖÖNOTTO

4.1 Server

Policy Manager Server asennettiin virtuaalikoneelle, jolla on 4GB RAM, 4-core cpu ja 40GB levytilaa. Virtuaalikoneen käyttöjärjestelmäksi valittiin RHEL 8. Tämä oli riski, koska F-Secure ei ollut viellä julkaissut virallista tiedotetta RHEL 8 ja Policy Manager 14.20:n yhteensopivuudesta. PMS 14.20 asentui RHEL 8:lle ilman ongelmia.

Varsinainen asennus onnistui Policy Manager – Admin Guiden ohjeita seuraamalla. Kun pohjalla oleva virtuaalikone oli saatu valmiiksi (laitettu verkkoasetukset, kovennettu ja liitetty toimialueeseen) piti asentaa libstdc++.i686 niminen paketti. Tämän jälkeen oli mahdollista asentaa varsinainen Policy Manager Server. Asennus tapahtui hakemalla F-Securen sivuilta downloads osiosta ”policy manager 14.20 for linux” ja sieltä valittiin rpm päätteinen tiedosto. Sitten tämä rpm-tiedosto siirrettiin WinSCP ohjelmalla RHEL 8 virtuaalikoneelle. Kun rpm-tiedosto oli koneella PMS asennus aloitettiin komennolla:

```
rpm -i fspms-<version_number>.<build number>-1.x86_64.rpm
```

Kun asennus oli valmis, PMS konfiguroiminen aloitettiin komennolla:

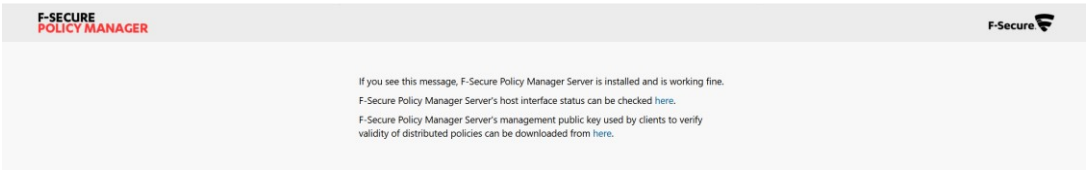
```
/opt/f-secure/fspms/bin/fspms-config
```

Tätä seurasi muutamia kysymyksiä liittyen esimerkiksi siihen mitä portteja Policy Manager tulee käyttämään ja administrator-tilin salasanan asettaminen. Kysymyksiin vastaamisen jälkeen konfiguraatio oli valmis. Policy Manager Serverin tila tarkastettiin komennolla:

```
/etc/init.d/fspms status
```

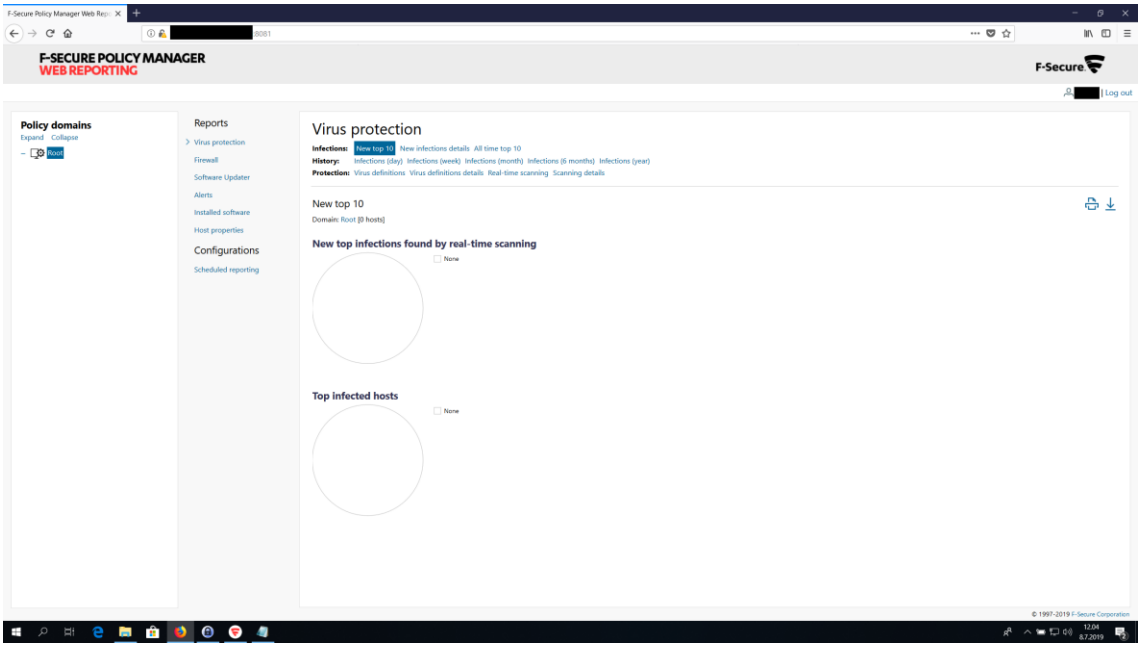
Käyttöön otettiin oletusportit eli 80, 443, 8080 ja 8081. Porttia 80 (http) käytetään virustunnisteiden ja muun yleisen tiedon kuljettamiseen hostien ja PMS välillä. Portti 443 (https) on varattu hostien ja PMS:n väliseen salattuun liikenteeseen. Ylläpitäjät hallinnoivat Policy Manageria PMC:n avulla, joka on yhteydessä PMS:n porttiin 8080. Web Reporting sijaitsee PMS koneella portissa 8081. Nämä portit piti avata myös PMS koneen palomuurista.

Serverin asennuksen toimivuuden voi tarkistaa menemällä selaimella virtuaalikoneen osoitteeseen porttiin 443. Kuvassa 4 näkyy mitä sivulla lukee, mikäli asennus on onnistunut.



KUVA 4. Ilmoitus onnistuneesta F-Secure Policy Manager Serverin asennuksesta

Web Reporting tulee Policy Manager Serverin asennuksen yhteydessä, eikä vaadi erillistä konfiguraatiota. PMS asennuksen jälkeen varmistettiin Web Reporting (kuva 5) toimivuus, menemällä PMS:in osoitteeseen porttiin 8081.

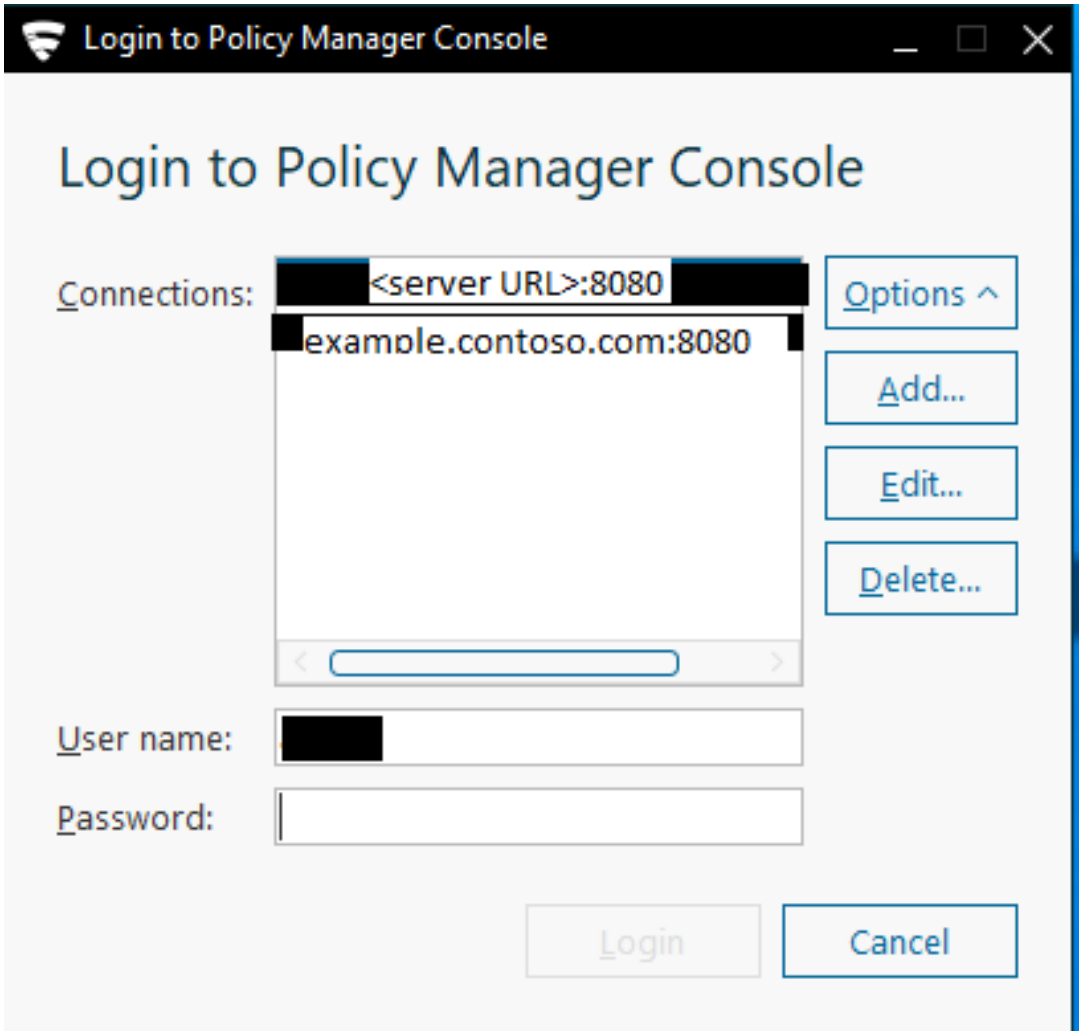


KUVA 5. Juuri käyttöönotettu Web Reporting ilman ainuttakaan hostia

4.2 Console

F-Secure Policy Manager Consolen asentaminen aloitettiin lataamalla asennuspaketti F-Securen sivuilta, downloads osiosta “Policy Manager for Windows”. Ohjatussa asennuksessa komponenteiksi valittiin vain “console”, koska serveri

oli jo erillisellä koneella. Ohjatun asennuksen jälkeen PMC oli käyttökunnossa. Policy Manager Consoleen (kuva 6) syötettiin tunnukset, jonka jälkeen päästiin hallinnoimaan Policy Manageria.



KUVA 6. F-Secure Policy Manager Consoleen sisäänkirjautuminen

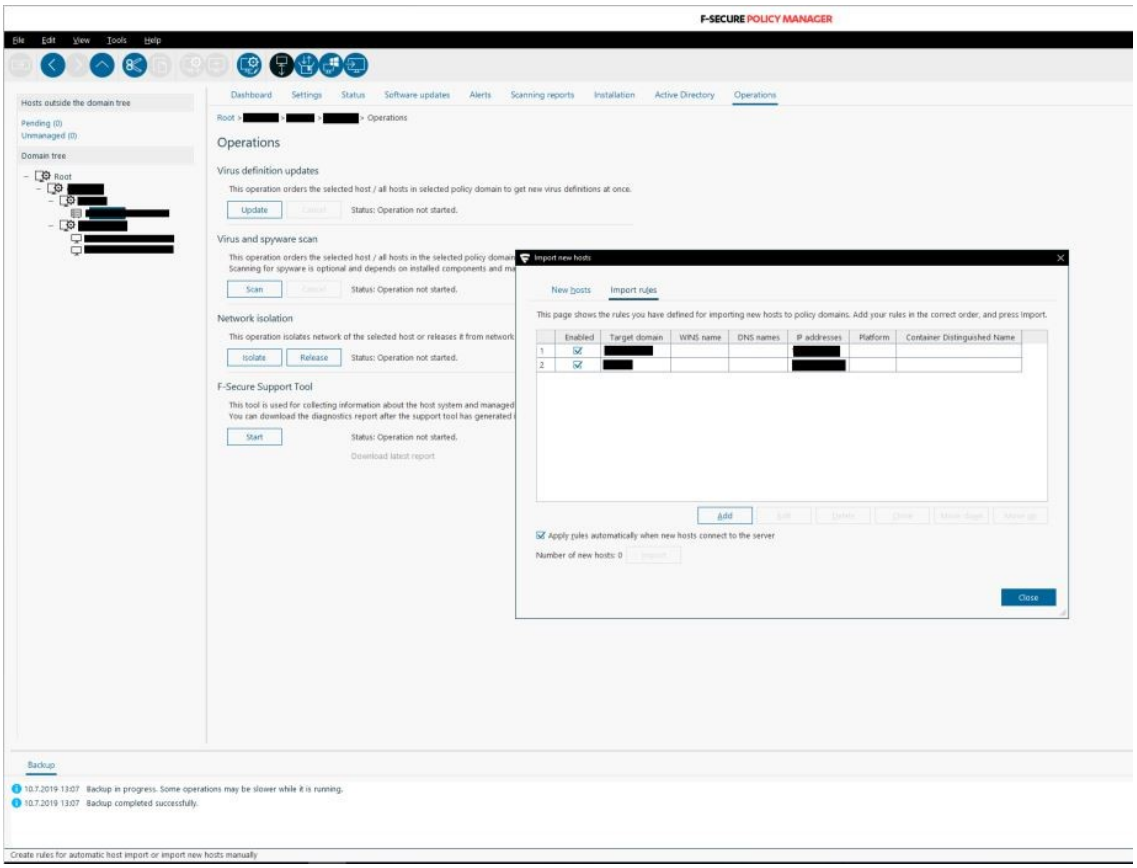
4.3 Työaseman/palvelimen suojaaminen

Ympäristössä käytetään Windows-työasemia ja muutamia Windows-palvelimia. Windows-työasemille F-Secure tarjoaa Client Security virustorjuntaohjelman ja Windows-palvelimille Server Securityn. Kun virustorjuntaohjelma on asennettu ja yhteydet toimivat, hosti voidaan tuoda Policy Managerin hallinnan piiriin.

Aluksi Client/Server Securityn asennettiin manuaalisesti muutamalla päätelaitteelle. Manuaalisella tarkoitetaan asennustiedoston viemistä päätelaitteelle. Kun

LDAPS (LDAP over SSL) saatiin käyttöön (tästä enemmän kappaleessa 4.6.2) oli mahdollista työntää Client/Server Security halutuille päätelaitteille. Jotta ohjelman työntäminen päätelaitteelle toimii, sillä täytyy olla File Sharing päällä. Tämän saa päälle avaamalla File Explorerin ja menemällä network osioon. Mikäli File sharing ei ole päällä File Explorer ilmoittaa: ”File sharing is turned off”. File sharing -ominaisuuden saa päälle klikkaamalla tätä ilmoitusta.

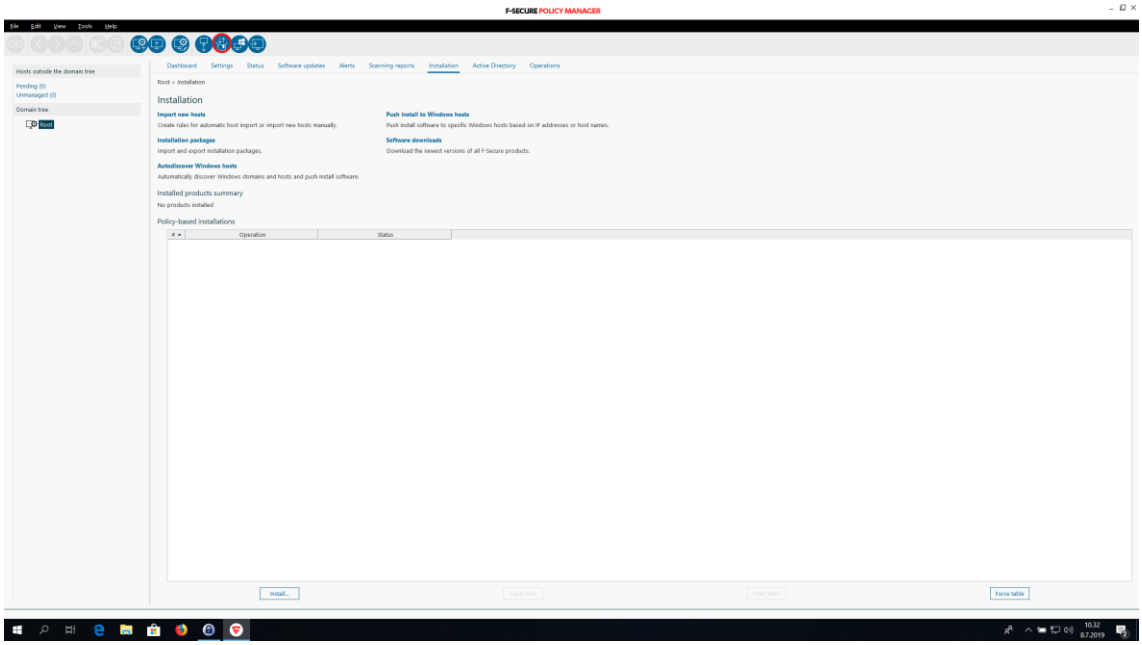
Palvelimet laitettiin yhteen policy domainiin ja työasemat toiseen. Työasemille ja palvelimille halutaan harvoin samoja asetuksia, esimerkiksi palomuurin suhteen. Tätä prosessia automatisoitiin tekemällä ”import hosts” -työkalulla sääntöjä (kuva 7). Yhden säännön mukaan kaikki tuotavat hostit, joiden ip-osoite on x.x.x.0/24 aliverkossa (työasemien aliverkko) menevät työasemille suunnattuun policy domainiin. Toisen säännön mukaan hostit, joiden ip-osoite on x.x.y.0/24 (palvelin aliverkko) aliverkossa menevät palvelimille suunnattuun policy domainiin. Kun asiaankuuluvalla virustorjuntaohjelmalla varustettu päätelaite ottaa yhteyttä PMS:iin, se menee automaattisesti oikeaan policy domainiin ja saa sille sopivat asetukset.



KUVA 7. Import rules ikkuna

4.3.1 Client Security

Ensin F-Securen sivuilta downloads osiosta ladattiin Client Security 14.10 jar-tiedosto. Ladattu jar-tiedosto tuotiin pakettienhallinta työkalulla (kuva 8) Policy Manageriin, jonka jälkeen jar-tiedoston pystyi lataamaan msi-tiedostona. Tämä msi-tiedosto siirrettiin halutulle työasemalle ja asennettiin ohjatun asennuksen avulla. Ennen msi-tiedoston tekemistä on hyvä tarkistaa että ”settings” osion centralized management-välilehdellä on oikeat tiedot. Täällä määritellään muun muassa mistä osoitteesta PMS löytyy. Kun PMCS oli asennettu ja verkkopalomuuriin oli tehty tarvittavat avaukset, työaseman pystyi tuomaan PM:n hallinnan piiriin klikkaamalla ”import host”. Tuonnin sääntöjen asettamisen jälkeen tämä tapahtui automaattisesti.



KUVA 8. PMC näkymä, jossa pakettienhallinta työkalu ympyröity punaisella

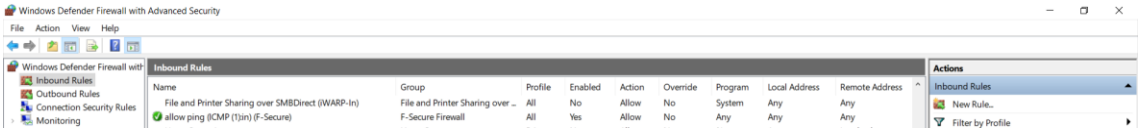
4.3.2 Server Security

Server Securityn asentaminen meni samalla tavalla kuin Client Securityn. F-Securen sivuilta ladattiin Server Security 14.00 jar-tiedosto. Se tuotiin Policy Manageriin. Tämän jälkeen tehtiin msi-tiedosto samalla tavalla kuin Client Securityn

kanssa. Tämä msi-tiedosto vietiin halutulle palvelimelle. Msi-tiedostosta aukesi ohjattu asennus, jonka suorittamisen jälkeen palvelimen pystyi tuomaan hallittavaksi hostiksi.

4.4 Palomuuri

Policy Manager 14.xx käyttää hyväksi Windowsin omaa palomuuria, eikä asenna sen tilalle omaa. Policy Manageriin tehdään palomuuriprofiili, joka asetetaan halutulle hostille. Hostilla voi olla vain yksi profiili. Hostin paikalliseen palomuurisäännöstöön ilmestyy profiilissa määritellyt säännöt (kuva 9). Tämä tarkoittaa sitä, että paikallisesti tehdyt säännöt ovat yhdenvertaisia Policy Managerilla tehtyjen sääntöjen kanssa.



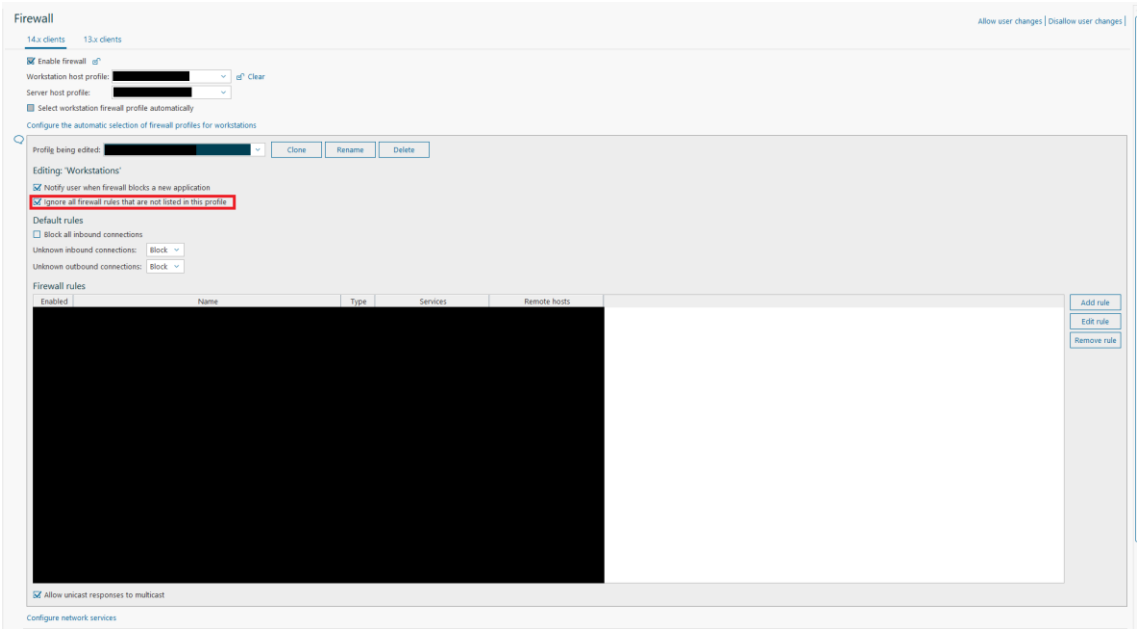
KUVA 9. Policy Managerilla tehty sääntö hostin palomuurilla

Windowsin palomuuri ei katso sääntöjen järjestystä. Yleensä säännöstöä käydään läpi ylhäältä alas rivi riviltä ja toimitaan ensimmäisenä vastaantulevan liikenteeseen täsmäävän säännön mukaan. Windowsin palomuuri käy aina koko listan läpi ja katsoo mitkä kaikki säännöt koskevat liikennettä. Kielto säännöt ovat etusijalla. Liikenteen osuessa sekä kieltävään että sallivaan sääntöön, liikenne kielletään.

Ympäristössä johon F-Secure Policy Managerin asennettiin, käyttäjillä on paikallisen järjestelmänvalvojan oikeudet. Käyttäjät voivat tällöin tehdä avauksia paikalliseen palomuuriin (tämä on tosin kiellettyä yrityksen säännöissä), mikä on tietoturvariski. Käyttäjä voi muuttaa paikalliselta palomuurilta PM:lla määriteltyä sääntöä, mutta tämä sääntö muuttuu parin sekunnin päästä takaisin. Toisinsanoen Policy Managerilla määritellyt säännöt ovat turvassa käyttäjiltä mutta paikallinen palomuuri kokonaisuudessaan ei.

Ongelmaksi muodostui kuinka estää käyttäjiä tekemästä ylimääräisiä avauksia palomuuriin. Yleistä ”kiellä kaikki” sääntöä ei voitu tehdä; koska kieltävät säännöt ovat etusijalla, mitään liikennettä ei sallittaisi. Hostien paikallisen palomuurin säännöt yritettiin ottaa pois käytöstä Group Policylla. Kyseinen Group Policy asetus löytyy Group Policy editorista Computer configuration -> Policies -> Windows Settings -> Security Settings -> Windows Defender Firewall with Advanced Security. Täältä löytyy vaihtoehto “do not apply local firewall rules”. Tämä kuulostaa hyvältä, mutta myös PM:lla määritellyt säännöt lasketaan lokaaleiksi säännöiksi. Mikäli tämä asetus otetaan käyttöön, hosteilta ei saa enää yhteyttä mihinkään. Jos liikenteeseen ei oteta mitään kantaa säännöstössä, se hylätään. Koska hostilla ei ollut sääntöjä niin kaikki liikenne hylättiin oletusarvona.

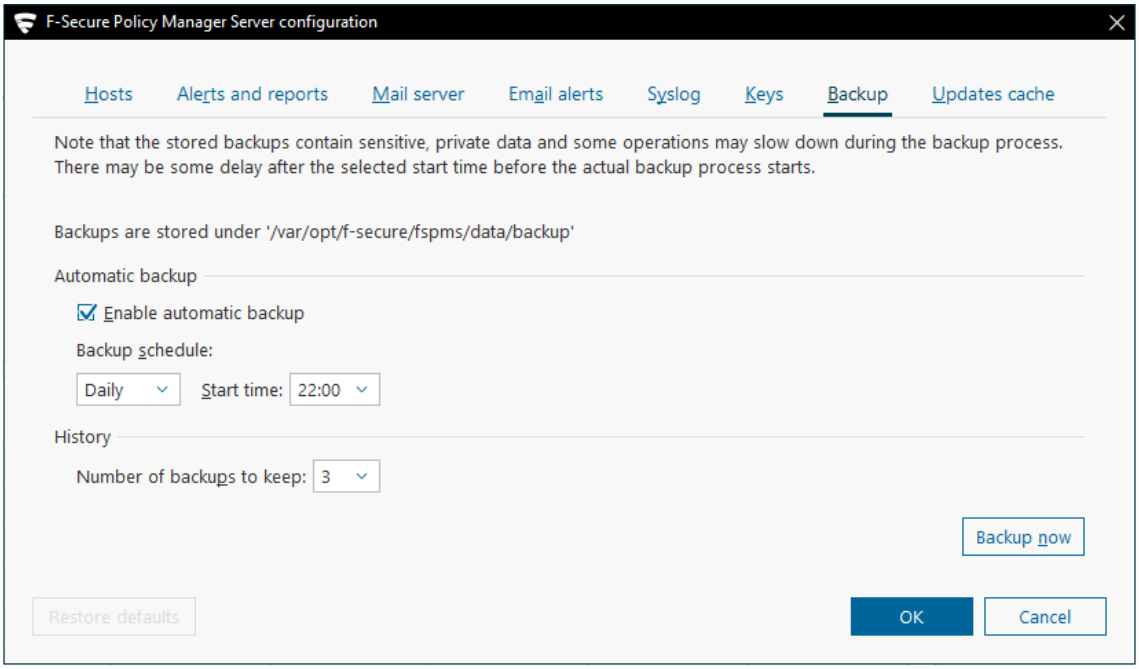
Oikea ratkaisu tähän oli laittaa päälle Policy Managerilla palomuuriprofiilista ”ignore all firewall rules that are not listed in this profile” (kuva 10). Työasemilta sallittiin ulospäin lähtevä liikenne varsin kattavasti, mutta työasemia kohti menevä liikenne rajattiin tarkasti.



KUVA 10. Palomuuri asetukset Policy Managerilla

4.5 Varmuuskopiointi

F-Secure Policy Managerille pystyy konfiguroimaan automaattisen varmuuskopioinnin. Tämä varmuuskopiointi ei varmuuskopioi koko konetta, vaan ainoastaan PMS-tietokannan. PMS konfiguroitiin ottamaan tietokannastaan varmuuskopio joka ilta kello 22:00 ja säilyttämään kolme viimeisintä kopiota. Konfiguraatio tapahtui valitsemalla vasemmasta yläreunasta tools, ja sieltä ”server configuration”. Täältä valittiin Backup-välilehti (kuva 11), johon asetukset määriteltiin.



KUVA 11. Server configuration -työkalun Backup-välilehti

Tämän lisäksi myöhemmin konfiguroidaan kattavampi varmuuskopiointi siihen tarkoitetulla erillisellä järjestelmällä. Erillisen varmuuskopionnin konfigurointia ei käsitellä tässä opinnäytetyössä.

4.6 Sertifikaatti

F-Secure Policy Manager luo asennusvaiheessa itse itselleen allekirjoittamansa sertifikaatin. Muut palvelut eivät luota tähän sertifikaattiin, jolloin esimerkiksi selain huomauttaa aina virheellisestä sertifikaatista. Tämän voisi kiertää lisäämällä Policy Managerin sertifikaatin työasemille luotettuihin sertifikaatteihin, mutta tämä

ei ole elegantti ratkaisu. Policy Managerille tehtiin uusi sertifikaatti. Ympäristössämme on oma PKI (Public Key Infrastructure). On toivottavaa, että kaikki mahdollinen allekirjoitetaan omalla sertifikaatti auktoriteetilla.

4.6.1 Sertifikaatin vaihto

En mene tässä uuden sertifikaatin luomiseen, koska tähän on paljon ohjeita internetissä. Kerron kuinka PM:n sertifikaatti saadaan vaihdettua. Keytool ohjelma, jonka avulla uusi sertifikaatti lisätään oikeaan sertifikaattisäilöön, löytyy Policy Manager Serverillä sijainnista /opt/f-secure/fspms/jre/bin/. Sertifikaattisäilön koko polku on /var/opt/f-secure/fspms/data/fspms.jks. PMS:n luotetut juuritason CA:t ovat tiedostossa /opt/f-secure/fspms/jre/lib/security/cacerts.

Uuden sertifikaatin tulee olla PKCS12 muodossa. Mikäli sertifikaatti on esimerkiksi pem-tiedosto, se voidaan konvertoida oikeaan muotoon komennolla:

```
sudo openssl pkcs12 -export -out <pkcs12cert_nimi>.p12 -in <sertifikaattisi>.pem -inkey <sertifikaattisi_avain>.key
```

Uuden sertifikaatin tuominen Policy Managerin sertifikaattisäilöön tapahtuu komennolla:

```
sudo /opt/f-secure/fspms/jre/bin/keytool -importkeystore -deststorepass superPASSWORD -destkeypass superPASSWORD -destkeystore /var/opt/f-secure/fspms/data/fspms.jks -srckeystore <pkcs12cert_nimi>.p12 -srcstoretype PKCS12 -srcstorepass <store_pass>
```

Tämän jälkeen kannattaa tarkistaa, että sertifikaatti on todella mennyt sertifikaattisäilöön komennolla:

```
sudo /opt/f-secure/fspms/jre/bin/keytool -list -v -keystore /var/opt/f-secure/fspms/data/fspms.jks
```

Yllä oleva komento tulostaa komentoriville fspms.jks-tiedoston sisällön. Siellä on nyt kaksi sertifikaattia. PMS:n itse allekirjoitettu sertifikaatti ja juuri tuotu PCKS12-sertifikaatti. Tässä vaiheessa kannattaa ottaa ylös PCKS12-sertifikaatin alias.

Seuraavaksi poistetaan PMS:n itse allekirjoitettu sertifikaatti komennolla:

```
sudo /opt/f-secure/fspms/jre/bin/keytool -delete -alias fspms -keystore
/var/opt/f-secure/fspms/data/fspms.jks
```

Nyt sertifikaatti repositoriossa pitäisi olla jäljellä enää sinne juuri siirretty PCKS12-sertifikaatti. Tällä hetkellä sertifikaatin alias on jokin (oletusarvona ”1”) ja se pitää muuttaa ”fspms”:ksi. Aliaksen muuttaminen tapahtuu komennolla:

```
sudo /opt/f-secure/fspms/jre/bin/keytool -changealias -alias “1” -desta-
lias “fspms” -keypass <store_pass> -keystore /var/opt/f-se-
cure/fspms/data/fspms.jks -storepass superPASSWORD
```

Sertifikaatti on nyt oikeassa paikassa oikealla aliaksella. Tämän jälkeen käynnistetään fspms-palvelu uudelleen komennolla:

```
/etc/init.d/fspms restart
```

Mikäli sertifikaatti on kunnossa ja komennoissa on käytetty oikeita salasanoja, fspms-palvelu käynnistyy normaalisti. Sertifikaatin voi helposti tarkistaa menemällä osoitteeseen PMS:n osoitteeseen ja katsoa huomauttaako selain sertifikaatista.

4.6.2 Luotettu juuritason CA

Käyttöön haluttiin LDAP:n turvallinen versio eli LDAPS. Tätä varten PMS pitää luottaa AD:n sertifikaattiin. Luottosuhde tehdään lisäämällä luotettuihin juuritason CA:hin sen CA:n sertifikaatti (.crt muodossa), joka on allekirjoittanut AD:n sertifikaatin.

Ensin siirretään juuritason CA:n sertifikaatti winSCP:llä PMS:lle. Tämän jälkeen se tuodaan sille tarkoitettuun sertifikaattirepositorioon komennolla:

```
sudo /opt/f-secure/fspms/jre/bin/keytool -importcert -keystore /opt/f-se-
cure/fspms/jre/lib/security/cacerts -file <root_ca_name>.crt
```

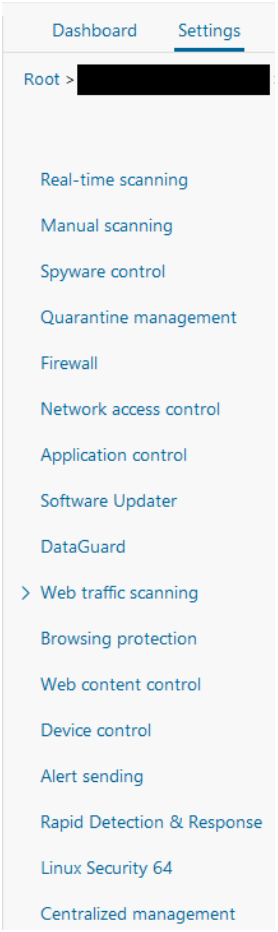
Sitten fsmps-palvelu käynnistetään uudelleen komennolla:

```
/etc/init.d/fspms restart
```

Tämän jälkeen LDAPS toimii. LDAPS:ia voidaan käyttää esimerkiksi AD synkronointisääntöjen tekemiseen. Ympäristössämme sitä käytettiin käyttäjien tuontiin suoraan AD:sta. Näin järjestelmänvalvojat voivat käyttää toimialueelle tehtyjä käyttäjiään, eikä tarvitse tehdä erikseen paikallisia käyttäjiä PM:lle. Tuonti tapahtui valitsemalla PMC:n ylälaidassa sijaitsevasta valikosta tools ja sieltä ”Users”. Täältä löytyi vaihtoehto ”Import from Active Directory” ja syötettiin toimialueen järjestelmänvalvojan tunnuksen tiedot. Sitten valittiin käyttäjäryhmä, jonka tunnuksilla haluttiin kirjautua PM:iin.

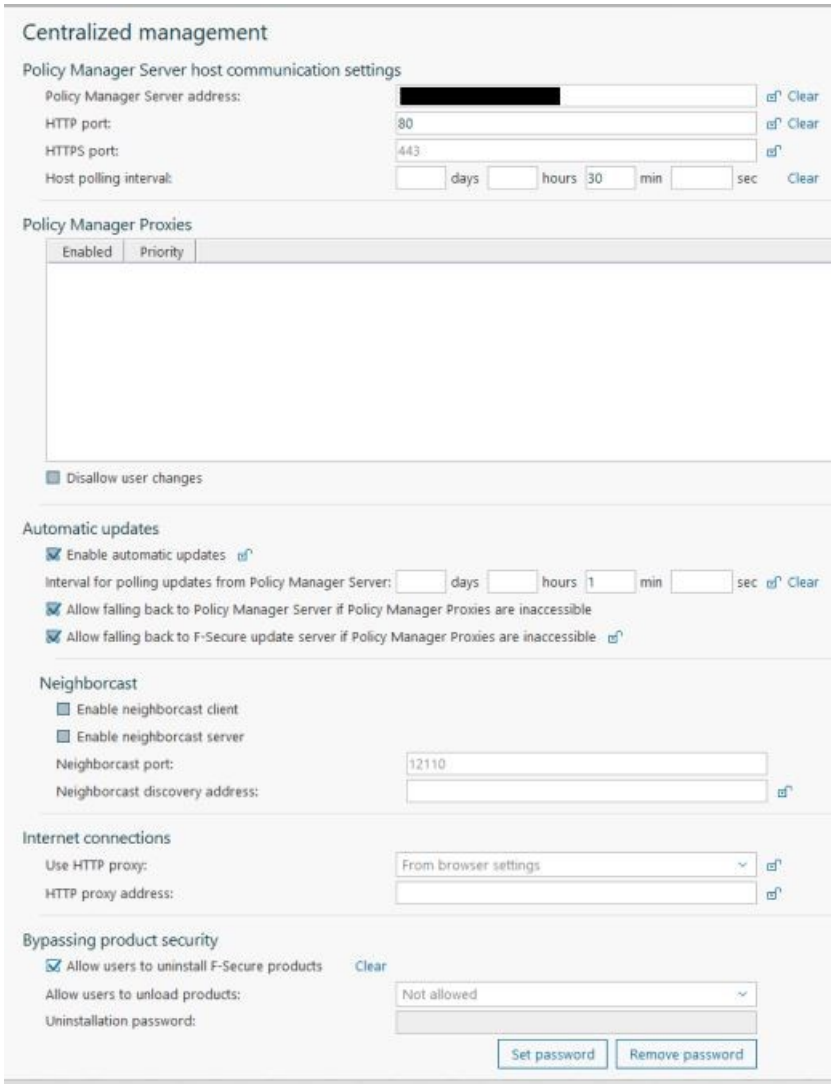
4.7 Asetukset

Policy Managerin ominaisuuksia otetaan käyttöön ja säädetään PMC:llä settings osiosta (kuva 12). Policy Managerilla näkyy kaikki asetukset/ominaisuudet, vaikka osa tarvitsee F-Secure Client/Server Security Premium-lisenssin. Lista PMCS/PMSS lisenssien eroista ominaisuuksien suhteen löytyy liitteistä 5 ja 6.



Kuva 12. Policy Managerin asetukset

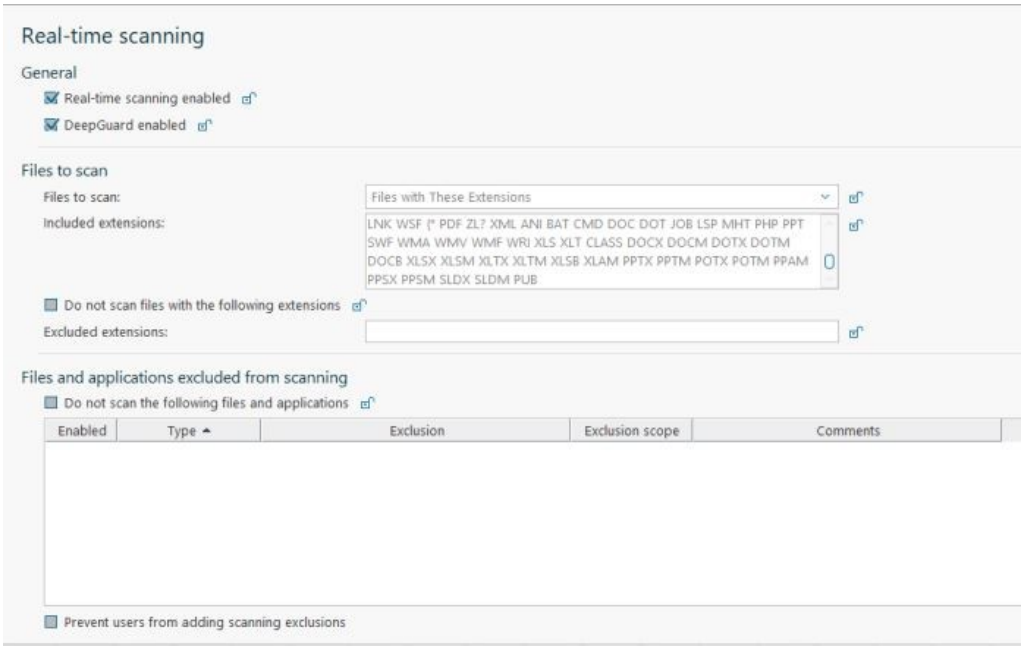
Centralized management osiosta (kuva 13) löytyvät asetukset, joiden perusteella päätelaite ottaa yhteyden PMS:iin. Hostit ovat säännöllisesti yhteydessä PMS:iin. Näin nähdään, jos joku hosti on pudonnut pois verkosta syystä tai toisesta. PMS laitettiin kyselemään hostien tilaa 30 minuutin välein. Verkossamme on vähän hosteja, mikä mahdollistaa päivitysten hakemisen PMS:ltä minuutin välein. Mikäli hosteja olisi paljon tästä koituisi turhaan ruuhkaa verkkoon. Neighborcast on ympäristössämme täysin turha ja potentiaalinen tietoturvariski, joten sitä ei otettu käyttöön. Neighborcastin ollessa käytössä hostit saavat edelleen tiedon uusista päivityksistä PMS:ltä, mutta eivät lataa tiedostoja sieltä vaan lähtevät kyselemään niitä lähiverkostaan. Mikäli lähiverkosta löytyy hosti, jolla on tarvittavat tiedostot ja neighborcast päällä, tiedostot haetaan tältä toiselta hostilta PMS:n sijaan.



KUVA 13. Centralized Management asetukset

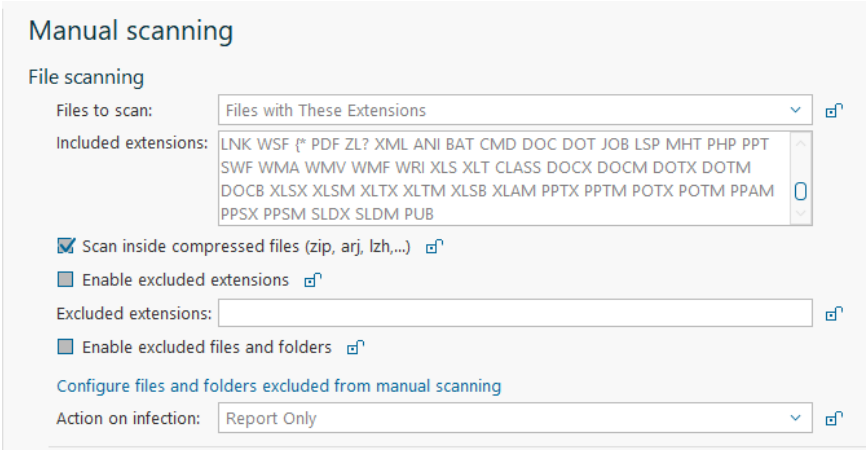
4.7.1 Käyttöönotetut ominaisuudet

Käyttöön otettiin Real-time scanning, koska ei ollut mitään syytä olla ottamatta sitä käyttöön. Reaaliaikaisen skannauksen asetukset laitettiin alla olevan kuvan 14 mukaisesti.



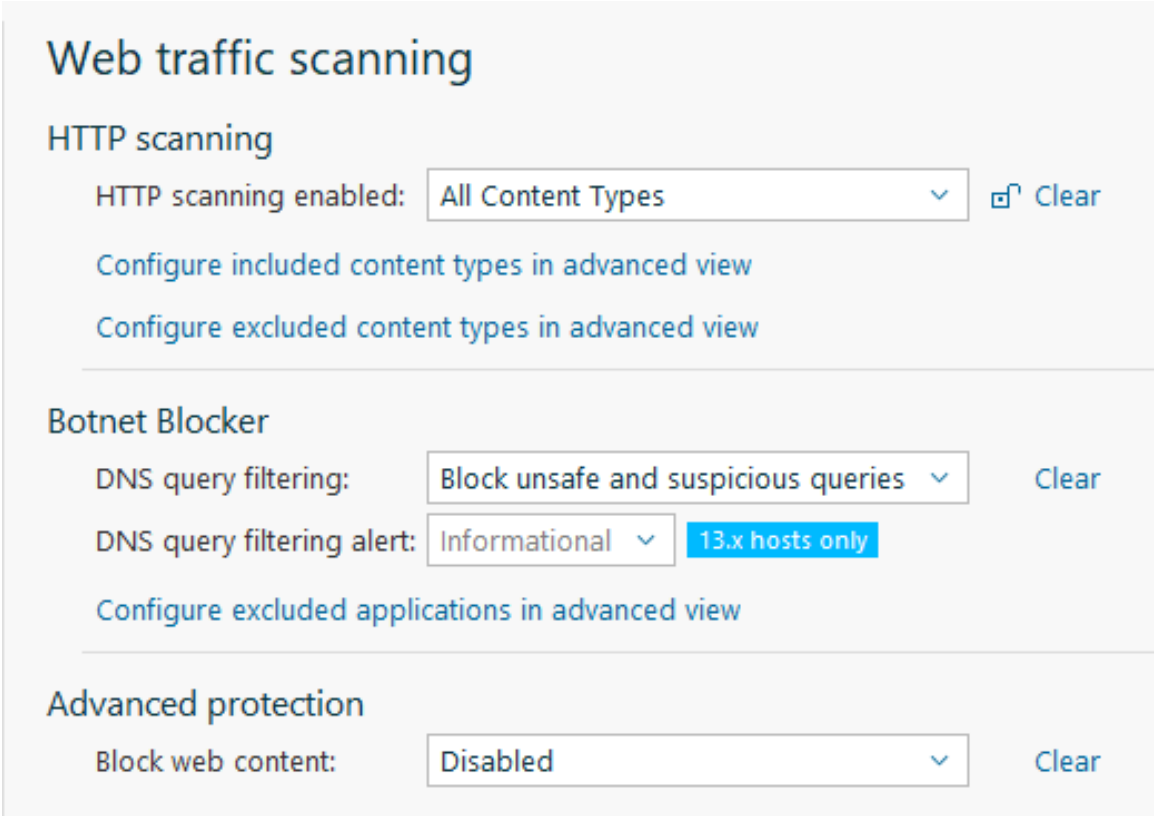
KUVA 14. Real-time scanning -ominaisuuden asetukset

Myös Manual scanning on hyvä olla. Olisi tietoturvan kannalta parasta, jos kaikki internetistä ladatut tiedostot skannattaisiin varmuuden vuoksi myös manuaalisesti. Kuvassa 15 manuaalisen skannauksen asetukset.



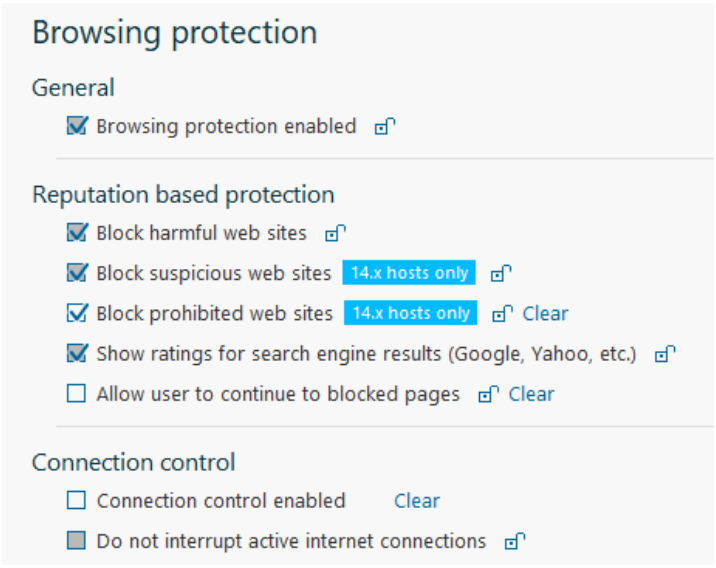
KUVA 15. Manual scanning -ominaisuuden asetukset

Kunnollinen verkkopalomuuri tekee Web traffic scanning -ominaisuudesta melko turhan. Tämä laitettiin silti päälle koska se on yksi kerros tietoturvaa lisää. Advanced Protection -ominaisuutta ei laitettu päälle, koska se tekisi tismalleen samaa mitä verkkopalomuuri tekee jo. Advanced protection löytyy Web traffic scanning asetuksista (kuva 16).



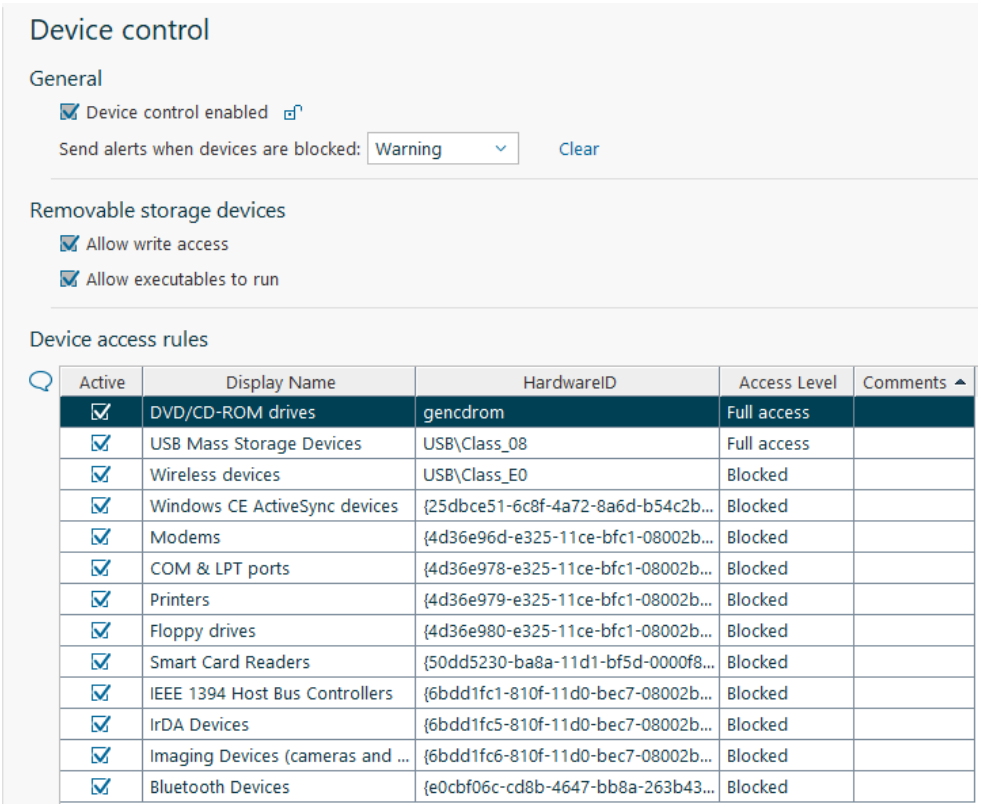
KUVA 16. Web traffic scanning -ominaisuuden asetukset

Browsing protection -ominaisuus laitettiin päälle, mutta sen lisäominaisuus Connection control olisi vaatinut Premium-lisenssin, mitä ympäristössämme ei ollut. Browsing protection -ominaisuuden asetukset kuvassa 17.



KUVA 17. Browsing protection -ominaisuuden asetukset

Device control -ominaisuus otettiin käyttöön, jotta käyttäjät eivät liittäisi turhia laitteita työasemiinsa. Kuvassa 18 näkyy minkälaisia laitteita päätelaitteisiin voi laittaa kiinni ja mitä ei. Ympäristössämme kenelläkään ei pitäisi olla esimerkiksi wifi-laitetta kiinni koneessa. Device control -ominaisuudella estetään ylimääräisten ja potentiaalisesti haitallisten laitteiden liittäminen työasemiin ja niiden kautta verkkoon.



Active	Display Name	HardwareID	Access Level	Comments
☑	DVD/CD-ROM drives	gencdrom	Full access	
☑	USB Mass Storage Devices	USB\Class_08	Full access	
☑	Wireless devices	USB\Class_E0	Blocked	
☑	Windows CE ActiveSync devices	{25dbce51-6c8f-4a72-8a6d-b54c2b...	Blocked	
☑	Modems	{4d36e96d-e325-11ce-bfc1-08002b...	Blocked	
☑	COM & LPT ports	{4d36e978-e325-11ce-bfc1-08002b...	Blocked	
☑	Printers	{4d36e979-e325-11ce-bfc1-08002b...	Blocked	
☑	Floppy drives	{4d36e980-e325-11ce-bfc1-08002b...	Blocked	
☑	Smart Card Readers	{50dd5230-ba8a-11d1-bf5d-0000f8...	Blocked	
☑	IEEE 1394 Host Bus Controllers	{6bdd1fc1-810f-11d0-bec7-08002b...	Blocked	
☑	IrDA Devices	{6bdd1fc5-810f-11d0-bec7-08002b...	Blocked	
☑	Imaging Devices (cameras and ...	{6bdd1fc6-810f-11d0-bec7-08002b...	Blocked	
☑	Bluetooth Devices	{e0cbf06c-cd8b-4647-bb8a-263b43...	Blocked	

KUVA 18. Device control -ominaisuuden asetukset

4.7.2 Käyttöönottamatta jääneet ominaisuudet

Kaikkia ominaisuuksia ei otettu käyttöön. Iso osa näistä ominaisuuksista vaatisi Premium-lisenssin. Tällaisia ominaisuuksia olivat Application control, Software updater, Dataguard ja Web content control.

Asetuksista löytyi myös muutamia ominaisuuksia, jotka ovat vain PMCS 13.xx virustorjuntaohjelmalla varustettuja hosteja varten. Näille ei ole mitään käyttöä, koska ympäristössämme kaikilla hosteilla on PMCS 14.10. Asetuksista löytyviä ominaisuuksia, jotka sopivat vain vanhemmille versioille olivat Spyware control, Network access control ja Alert sending.

5 POHDINTA

Ympäristössä on nyt yksi Policy Manager Server ja jokaisen järjestelmänvalvojan työasemalla on Policy Manager Console. Käyttäjien työasemat ovat tuotu hosteiksi. Windows-palvelimille on asennettu Server Security ja Windows-työasemille Client Security. Windows-hostien palomuurien säännöt tulevat Policy Managerilta. Uudet potentiaaliset hostit tuodaan Policy Managerin hallinnan piiriin automaattisesti. Policy Manager käyttää ympäristön sertifikaatti auktoriteetin allekirjoittamaa sertifikaattia. Kaikki ympäristön kannalta merkitykselliset ominaisuudet ovat käytössä.

Työ onnistui hyvin. Policy Manager toimii ympäristössä oikein ja se saatiin käyttöön aikataulun mukaisesti. Todellisuudessa konfiguraatio ei tule ikinä olemaan kokonaan valmis, koska sitä pitää jatkuvasti muuttaa käyttäjien ja ympäristön tarpeiden mukaan.

Pidin siitä miten konkreettinen ja selkeä opinnäytetyön aihe oli. Aiheen rajaus oli suhteellisen helppoa, koska päätin keskittyä puhtaasti Policy Manageriin. Aihe olisi voinut helposti lähteä laajenemaan turhaan, jos olisin alkanut kertoa laajemmin esimerkiksi eri protokollista tai PKI:n toiminnasta.

Internetistä löytyy jo F-Securen omat melko kattavat ohjeet Policy Managerin ominaisuuksiin ja asentamiseen. F-Securelta löytyy tosin varsin heikosti tietoa sertifikaatin vaihdosta. Tästä raportista löytyvä ohjeistus sertifikaatin vaihtoon on mielestäni raportin arvokkain osa.

Käyttöönoton aikana ympäristössä oli ainoastaan muutama käyttäjä. Olisi ollut hyvä tarkkailla ja tutkia Policy Managerin toimintaa siinä vaiheessa, kun ympäristössä on enemmän käyttäjiä. Vasta siinä vaiheessa näkee mitä haittaohjelmia/ongelmia/virheitä Policy Manager havaitsee, vai onko se ympäristössä vain ST IV-luokituksen saamiseksi. Tämä olisi auttanut Policy Managerin todellisen hyödyllisyyden arvioinnissa.

Policy Managerin toimintaa pitäisi kehittää verkossa, jossa on ssl-purku päällä. Hostien ja PMS:n välinen kommunikaatio ei toimi ollenkaan, jos välissä on ssl-purku. Kaikki ympäristön salattu liikenne haluttaisiin purkaa, mutta tällä hetkellä se ei ole mahdollista.

LÄHTEET

Client Security for Windows – Guide. Luettu 10.5.2019 https://help.f-secure.com/product.html#business/client-security/14.10/en/concept_88784CE3BD5246F5898817F3660AA948-14.10-en

Combitech Oy verkkosivut – Tietoja meistä. Luettu 20.7.2019 https://combitech.fi/tietoja/

F-Secure For Business Release Notes. Luettu 13.5.2019 https://help.f-secure.com/product.html#business/releasenotes-business/latest/en/products_bs-latest-en

Policy Manager – Admin Guide. Luettu 24.4.2019 https://help.f-secure.com/product.html#business/policy-manager/14.00/en/concept_0C321E9CB5994555A9B0A0B793DD5E98-14.00-en

Puolustusministeriö – Katakri 2015. Luettu 20.7.2019 https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

Server Security. Luettu 12.5.2019 https://help.f-secure.com/product.html#business/server-security/14.00/en

Rouse, M. 2018. Techtarget verkkosivut – digital certificate. Luettu 8.10.2019 https://searchsecurity.techtarget.com/definition/digital-certificate

LIITTEET

Liite 1. Policy Manager Server järjestelmävaatimukset

Operating system:	Microsoft Windows: Windows Server 2008 SP1 (64-bit); Standard, Enterprise, Web Server, Small Business Server or Essential Business Server editions Windows Server 2008 R2 with or without SP1; Standard, Enterprise or Web Server editions Windows Server 2012; Essentials, Standard or Datacenter editions Windows Server 2012 R2; Essentials, Standard or Datacenter editions Windows Server 2016; Essentials, Standard or Datacenter editions Windows Server 2019; Essentials, Standard or Datacenter editions (Server Core is supported) Linux (only 64-bit versions of all distributions listed are supported): Red Hat Enterprise Linux 6, 7 CentOS 6, 7 openSUSE Leap 43.2 SUSE Linux Enterprise Server 11, 12 SUSE Linux Enterprise Desktop 11, 12 Debian GNU Linux 8, 9

	Ubuntu 14.04, 16.04, 18.04
Processor:	Dual-core 2GHz CPU or higher.
Memory:	2 GB RAM.
Disk space:	10 GB of free disk space. For managing Premium clients, an additional 10 GB of space is required for serving software updates.
Network:	100 Mbit network.
Browser:	Firefox, Internet Explorer, Google Chrome

(Policy Manager - Admin Guide.)

Liite 2. Policy Manager Console järjestelmävaatimukset

Operating system:	Microsoft Windows: Windows 7 (64-bit) with or without SP1; Professional, Enterprise or Ultimate editions Windows 8 (64-bit), any edition Windows 8.1 (64-bit), any edition Windows 10 (64-bit) Windows Server 2008 SP1 (64-bit); Standard, Enterprise, Web Server, Small Business Server or Essential Business Server editions Windows Server 2008 R2 with or without SP1; Standard, Enterprise or Web Server editions Windows Server 2012; Essentials, Standard or Datacenter editions Windows Server 2012 R2; Essentials, Standard or Datacenter editions Windows Server 2016; Essentials, Standard or Datacenter editions Windows Server 2019; Essentials, Standard or Datacenter editions Note: Server Core installation option is not supported. Linux (only 64-bit versions of all distributions listed are supported): Red Hat Enterprise Linux 6, 7 CentOS 6, 7 openSUSE Leap 43.2 SUSE Linux Enterprise Server 11, 12 SUSE Linux Enterprise Desktop 11, 12

	Debian GNU Linux 8, 9 Ubuntu 14.04, 16.04, 18.04
Processor:	2 GHz or higher CPU.
Memory:	1 GB of RAM.
Disk space:	300 MB of free disk space.
Display:	Minimum 16-bit display with resolution of 1024x768 (32-bit color display with 1280x1024 or higher resolution recommended).
Network:	100 Mbit network.

(Policy Manager - Admin Guide.)

Liite 3. Server Security tuetut käyttöjärjestelmät

- Microsoft® Windows Server 2008 R2
- Microsoft® Small Business Server 2011, Standard edition
- Microsoft® Small Business Server 2011, Essentials
- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2012 Essentials
- Microsoft® Windows Server 2012 R2
- Microsoft® Windows Server 2012 R2 Essentials
- Microsoft® Windows Server 2012 R2 Foundation
- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core
- Microsoft® Windows Server 2019 Standard
- Microsoft® Windows Server 2019 Essentials
- Microsoft® Windows Server 2019 Datacenter
- Microsoft® Windows Server 2019 Core

Note: Windows Server 2016 Nano is not supported.

All Microsoft Windows Server editions are supported except:

- Windows Server for Itanium processor
- Windows HPC editions for specific hardware
- Windows Storage editions
- Windows MultiPoint Server
- Windows Home Server

Note: All operating systems are required to have the latest Service Pack installed.

Note: For performance and security reasons, you can install the product only on an NTFS partition.

Supported terminal servers

F-Secure Server Security supports the following terminal server platforms:

- Microsoft Windows Terminal/RDP Services (on the above mentioned Windows Server platforms)
- Citrix® XenApp 5.0
- Citrix® XenApp 6.0
- Citrix® XenApp 6.5
- Citrix® XenApp 7.5, 7.6

(Server Security.)

Liite 4. Client Security 14.10 lisenssien ominaisuudet

Feature	F-Secure Client Security Standard	F-Secure Client Security Premium
Virus & spyware protection	•	•
DeepGuard™	•	•
DataGuard		•
Application control		•
Web traffic scanning	•	•
Firewall	•	•
Browsing protection	•	•
Botnet Blocker	•	•
Device control	•	•
Offload Scanning Agent	•	•
Software Updater		•
Connection control		•
Web content control		•
Rapid Detection & Response	•	•

(F-Secure Client Security 14.10 Release Notes.)

Liite 5. Server Security 14.00 lisenssien ominaisuudet

Feature	F-Secure Server Security	F-Secure Server Security Premium
Virus & spyware protection	•	•
DeepGuard™	•	•
DataGuard		•
Application control		•
Firewall	•	•
Web traffic scanning	•	•
Browsing protection	•	•
Software Updater		•
Offload Scanning Agent	•	•
Rapid Detection & Response	•	•

(F-Secure Server Security 14.00 Release Notes.)