Juha Tiikkaja

TYÖASEMIEN TIETOTURVALLISUUDEN OPTIMOINTI POLICY MANAGER -OHJELMISTON AVULLA

Insinöörityö
Kajaanin ammattikorkeakoulu
Tekniikan ja liikenteen ala
Tietoturvan koulutusohjelma
Kevät 2013

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Tekniikan ja liikenteen ala	Koulutusohjelma Tietotekniikan koulutusohjelma
Tekijä(t) Juha Tiikkaja	
Työn nimi Työasemien tietoturvallisuuden optimointi Policy Manager ohjelmiston avulla	
Vaihtoehtoiset ammattiopinnot Tietoturvateknologia	Ohjaaja(t) Raili Simanainen
	Toimeksiantaja Aaro Pääkkönen/Miika Lippojoki
Aika Kevät 2013	Sivumäärä ja liitteet 29+7

Tämän insinöörityön tavoitteena oli perehtyä F-Securen Policy Manager -tuotteeseen ja Kainuun ammattiopiston työasemien tietoturvallisuuden nykytilaan. Perehtymisen pohjalta käytössä olevaa ohjelmistoa tuli muokata niin, että tuotteesta saadaan organisaatiolle paras mahdollinen hyöty.

Opinnäytetyön alussa kerrotaan, mitä tietoturvallisuudella ja työasemien keskitetyllä hallinnalla tarkoitetaan. Teoriaosassa kuvataan virustorjuntaohjelmiston tärkeimpiä ominaisuuksia, joita voidaan hallita keskitetysti. Työssä esitellään yleisimpiä työasemien keskitettyyn hallintaan tarkoitettuja sovelluksia. Teoriaosassa esitellään myös F-Securen tuotteiden keskitettyyn hallintaan tarkoitettu Policy Manager Console -ohjelmisto.

Insinöörityön käytännön osuus sisältää suppean työasemien tietoturvallisuuden nykytilanteen kartoituksen. Kartoituksen avulla pyritään kuvaamaan organisaation työasemien nykytilannetta ja esittämään mahdollisia heikkoja kohtia tietoturvallisuuden kannalta. Kartoituksen pohjalta on pyritty esittämään kehitysideoita ja hyviä käytänteitä, joilla toimintaa voidaan tehostaa.

Työasemien tietoturvallisuutta tehostettiin muokkaamalla Policy Managerin avulla virustorjunnan ja palomuurin asetuksia. Palomuurisääntöjen avulla sallittiin organisaation tarvitsemaa verkkoliikennettä. Henkilöstön kannettaviin työasemiin määriteltiin turvallisuustason automaattinen valinta sen mukaan, missä verkossa työasema sijaitsee. Työn tuloksena virustorjuntaohjelmiston ja palomuurin asetuksia muokattiin vastaamaan organisaation toiveita. Työasemien nykytilanteen kartoittamisen avulla löydettiin kehitysideoita, joiden pohjalta organisaation tietoturvallisuutta voidaan tehostaa.

Kieli	Suomi
Asiasanat	Tietoturva, Keskitetty hallinta, F-Secure Policy Manager
Säilytyspaikka	☒ Verkkokirjasto Theseus ☒ Kajaanin ammattikorkeakoulun kirjasto

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

THESIS ABSTRACT

School School of Engineering	Degree Programme Information Technology
Author(s) Juha Tiikkaja	
Title Optimizing workstations information security by Policy Manager	
Optional Professional Studies Information Security	Instructor(s) Raili Simanainen
	Commissioned by Aaro Pääkkönen/Miika Lippojoki
Date Spring 2013	Total Number of Pages and Appendices 29+7

The purpose of this Bachelor's thesis was to get familiar with the F-Secure Policy Manager product and the current state of workstation data security level in the Kainuu Vocational College. Based on the findings, anti-virus and firewall software were configured to meet the needs of the organization.

First, the thesis describes information security and centralized management concepts. The theoretical part focuses on describing the key functions of anti-virus software together with some applications and methods which can be used for centralized management of workstations. It also introduces Policy Manager software, which can be used to manage all F-Secure products.

The practical part of the thesis contains a survey of the current situation of workstation data security. The purpose of studying the current situation is to improve the workstation data security by revealing potential weak points. The thesis also contains changes that were made in the firewall and the anti-virus software.

As a result Policy Manager settings, firewall rules and security levels were configured. Some weaknesses were found by studying the current situation of the workstation data security. The end of the thesis contains some development ideas how to improve the data security of the workstations.

Language of Thesis	Finnish
Keywords	Information Security, Data Security, Centralized management, F-Secure Policy Manager
Deposited at	☒ Electronic library Theseus ☒ Library of Kajaani University of Applied Sciences

SISÄLLYS

SYMBOLILUETTELO

BIOS	Basic Input-Output System. Tietokoneohjelma, joka käynnistää käyttöjärjestelmän tietokoneen käynnistämisen yhteydessä.
FTP	File Transfer Protocol. Tiedonsiirtoprotokolla kahden tietokoneen välillä.
Host	Nimitys työasemalle, jota hallitaan Policy Manager -ohjelmistolla
HTTP	Hypertext Transfer Protocol. Selaimille ja webpalvelimille tarkoitettu tiedonsiirtoprotokolla.
Policy	Joukko sääntöjä, jotka ilmaisevat, kuinka arkaluontoista tietoa käsitellään ja hallitaan.
Policy Domain	Joukko Host-koneita, joissa vallitsevat samankaltaiset tietoturva-asetukset.
POP	Post Office Protocol. Protokolla sähköpostiviestin noutamiseen palvelimelta
SCCM	System Center Configuration Manager. Microsoftin julkaisema ohjelmisto Windows-käyttöjärjestelmällä toimivien koneiden hallintaan.
SMTP	Simple Mail Transfer Protocol. Protokolla, jota käytetään sähköpostiviestin lähettämiseen
TCP	Transmission Control Protocol. Tietoliikenneprotokolla, joka vaatii molemmilta tietokoneilta internet-yhteyden.

1 JOHDANTO

Kainuun ammattiopisto on Kainuun maakunta -kuntayhtymän omistama liikelaitos. Se järjestää toisen asteen koulutusta nuorille ja aikuisopiskelijoille. Vakituisia toimipaikkoja sijaitsee Kajaanissa, Kuhmossa, Kuusamossa, Suomussalmella ja Vuokatissa. Tämän lisäksi aikuiskoulutuksen toimipisteitä sijaitsee Sotkamossa, Vantaalla ja Virossa. Organisaatiossa on noin 500 työntekijää, 2600 nuorta opiskelijaa ja vuositasolla noin 5500 aikuista, joista noin 700 on oppisopimusopiskelijoita. [1.]

Tämän insinöörityön tavoitteena on parantaa Kainuun ammattiopiston työasemien tietoturvallisuutta. Työn teoriaosassa perehdytään tietoturvallisuuden määritelmään, virustorjuntaohjelmiston keskeisimpiin toimintoihin sekä yleisellä tasolla työasemien keskitettyyn hallintaan. Työssä kuvataan tärkeimpiä työasemien keskitetyn hallinnan sovelluksia sekä perehdytään F-Securen Policy Manager Console -ohjelmistoon.

Työasemien tietoturvaa on pyritty parantamaan muokkaamalla virustorjunta- ja palomuurin ohjelmiston asetuksia. Työasemien tietoturvallisuuden nykytilanteesta on tehty kartoitus, jonka avulla on pyritty etsimään mahdollisia haavoittuvuuksia ja heikkouksia. Kartoituksen pohjalta esitetään kehitysideoita ja hyviä käytäntöjä, joilla tietoturvallisuutta voidaan parantaa.

2 TIETOTURVALLISUUS JA KESKITETTY HALLINTA

Tässä luvussa perehdytään tietoturvallisuuden määritelmään ja tietoturvan eri osatekijöihin. Kerrotaan, mitä työasemien keskitetyllä hallinnalla tarkoitetaan ja kuvataan eri toimenpiteitä, joita keskitetyn hallinnan ratkaisuilla voidaan tehdä.

2.1 Tietoturvallisuuden määritelmä

Tietoturvallisuudella tarkoitetaan yritykselle arvokkaan tiedon suojaamista erilaisilta tietoturvauhilta. Tavoitteena on pitää tieto luotettavana, nopeasti saatavilla ja vain tietoon oikeutettujen henkilöiden käytettävissä. Tiedon suojaamista koskevia määritelmiä on usein laajennettu sisältämään myös tietojen käsittelyssä tarvittavat laitteet sekä tietoliikennemenetelmät. Tietojärjestelmien halutaan myös kiistämättömästi kertovan järjestelmässä olevan tiedon luoja. [2, s. 4.]

Klassinen tietoturvallisuuden määritelmä sisältää kolme osatekijää, joita ovat luottamuksellisuus, käytettävyys ja eheys. Luottamuksellisuuden varmistamisella tarkoitetaan, että tieto on suojattu ulkopuolisilta henkilöiltä, jolloin vain tietoon oikeutettu henkilö saa käsitellä niitä. Käytettävyydellä tarkoitetaan, että järjestelmässä oleva tieto on saatavissa oikeassa muodossa ja tarpeeksi nopeasti. Eheydellä tarkoitetaan, että tieto pysyy oikeana eikä siihen tule tahallisia tai tahattomia virheitä. Klassista tietoturvallisuuden määritelmää on laajennettu sisältämään myös kiistämättömyys ja pääsynvalvonta. Kiistämättömyydellä tarkoitetaan, että tietojärjestelmä tunnistaa sitä käyttäneen henkilön, jolloin varmistetaan tiedon alkuperä ja tarvittaessa osoitetaan tietojen luvaton käyttö. Pääsynvalvonnalla tarkoitetaan erilaisia keinoja, joilla rajoitetaan laitteistojen, tietojärjestelmien sekä tietoliikenneyhteyksien käyttöä. [2, s. 4–5.]

Tietoturvallisuuden arviointi, kehitys ja ylläpito on jatkuvaa toimintaa, jolloin se mielletään prosessimuotoiseksi työksi. Yhtenä tietoturvallisuustyön tavoitteena on luoda organisaatiolle toimiva tietoturvapolitiikka. Tietoturvapolitiikka on dokumentti, joka ohjaa organisaation tietoturvakäytäntöjä ja tietoturvallisuusprosessia. Se laaditaan kuvaamaan eri liiketoimintaprosessien edellyttämää tietojen turvaamisastetta ja menetelmiä, joilla haluttuun turvallisuustasoon pyritään. Tietoturvapolitiikassa ilmenee myös se, kuinka tietoturvallisuutta hallinnoi-

daan ja kehitetään. Tietoturvapolitiikan laatiminen on ylimmän johdon vastuulla, ja se laaditaan yleisellä tasolla. Koska tietoturvapolitiikan tarkoituksena on toimia joko keskipitkän tai pitkän aikavälin ohjeena (5–10 vuotta), siihen ei voida sisällyttää tietoturvallisuuden toteutukseen liittyviä yksityiskohtia. Tekniset yksityiskohdat ja käytänteet, joilla haluttuun tietoturvallisuuden tasoon pyritään, kuvataan tarkemmin tietoturvasuunnitelmassa. [2, s. 7–9.]

2.2 Keskitetty hallinta

Keskitetyllä hallinnalla tarkoitetaan useiden työasemien hallintaa ja ylläpitoa yhdestä paikasta käsin. Erilaiset ohjelmistotyökalut mahdollistavat ohjelmistopäivitysten ja sovellusten jakamisen työasemiin. Myös käyttäjäoikeuksia ja työaseman ominaisuuksia voidaan muokata käyttötarkoitukseen sopivaksi. Keskittämällä työasemien hallinta säästetään aikaa ja resursseja, sillä muutoksia ei tarvitse tehdä jokaiselle työasemalle erikseen.

Työasemien vakioinnilla tarkoitetaan, että käyttöjärjestelmän asetukset ja sovelluskokoonpanot määritellään yhtenäisiksi. Tämä mahdollistaa erilaisten työasemakokoonpanojen paremman hallittavuuden. Rikkoutuessaan työasema voidaan nopeasti vaihtaa uuteen samanlaiseen työasemaan. [2, s. 133.]

Tietoturvan kannalta työasemien vakioinnissa on oleellista, että työasemissa olevia palveluita rajataan työtehtävästä riippuen. Hakalan, Vainion ja Vuorisen [2, s. 133] mukaan käyttöjärjestelmän asennuksen jälkeen sellaiset palvelut, joita käyttäjät eivät tarvitse, tulisi sammuttaa.

”Käyttöjärjestelmän asennuksen jälkeen järjestelmästä sammutetaan ne palvelut, joita ei tarvita. Etenkin verkon muille järjestelmille ja käyttäjille suunnatut ylimääräiset palvelut pitää sammuttaa” [2, s. 133].

Keskitetyn hallinnan ratkaisuja käytetään usein sovellusten asentamiseen työasemille. Asennettavasta ohjelmasta tehdään asennuspaketti, joka asennetaan keskitetyn hallinnan sovelluksen avulla työasemiin. Ohjelmia ei tarvitse asentaa yksitellen työasemiin, jolloin säästetään merkittävästi aikaa ja resursseja. Ohjelmat asennetaan täsmälleen samoilla asetuksilla, mikä helpottaa ITC-tuen työtä.

Käyttöjärjestelmiin ja sovelluksiin julkaistaan ajoittain erilaisia päivityksiä. Päivitykset voivat olla tietoturvapäivityksiä, joilla korjataan ohjelmistossa olevia tietoturva-aukkoja. Päivityksillä

voidaan myös korjata muita ohjelmistossa esiintyviä virheitä. [2, s. 135.] Keskitetyn hallinnan ratkaisut helpottavat päivitysten asentamista samoilla periaatteilla kuin itse ohjelmienkin asennus. Päivitykset voidaan helposti jakaa ja asentaa työasemiin keskitetysti.

Etähallintaohjelmistojen avulla voidaan tehostaa työasemien ylläpitoa. Etähallinnalla tarkoitetaan toisen työaseman hallitsemista omalla työasemalla verkon kautta. Esimerkiksi järjestelmänvalvoja voi etähallintaohjelmiston avulla ottaa yhteyden verkossa olevaan koneeseen ja hallita sitä kuin omaa työasemaansa.

2.3 Virustorjuntaohjelmiston keskeiset toiminnot

Käytettävästä tietoturvaohjelmistosta riippuen hallintasovelluksen avulla voidaan esimerkiksi jakaa uusia ohjelmistoversioita ja saada raportteja järjestelmän tilasta. Hallintasovelluksella voidaan myös määrittää virustorjuntaohjelmassa ja palomuurissa vallitsevat asetukset sekä automatisoida virustorjunnan eri toimintoja.

Virus- ja haittaohjelmistojen torjunta perustuu pääosin tunnistetietokantaan. Virustunniste on eräänlainen viruksen allekirjoitus, joka viittaa vain tiettyyn virukseen. Virustorjuntaohjelma vertaa tarkistuksen aikana epäilyttävää tiedostoa virustunnistetietokannassa oleviin tietoihin ja löytää viruksen yhtenevyyksien perusteella. Virustorjuntaohjelmisto ei kykene tunnistamaan sellaisia haittaohjelmia, joista tunnistetietoja ei ole vielä tullut. Tämän vuoksi virustunnisteet tulisi aina olla ajan tasalla. [2, s. 135.]

Päivityksiä virustunnistetietokantaan voidaan jakaa esimerkiksi erillisen välityspalvelimien avulla, jolloin vähennetään kuormaa palvelimelta. Joissain tapauksissa on myös mahdollista asettaa työasemat etsimään ja jakamaan päivityksiä muille samassa verkossa oleville työasemille.

Virustentarkistus voidaan suorittaa sekä manuaalisesti että reaaliaikaisena tarkistuksena. Manuaalinen tarkistus vaatii sen, että käyttäjä erikseen käynnistää virustarkistuksen. Manuaalinen virustarkistus voidaan myös automatisoida, jolloin varmistetaan, että tarkistus tapahtuu säännöllisin väliajoin. Toinen tekniikka on reaaliaikainen virustarkistus, joka tutkii järjestelmää jatkuvasti sen käytön aikana. Tällöin virustorjuntaohjelmisto yrittää löytää haittaohjelmia

niiden käyttäytymisen perusteella. Reaaliaikainen tarkistus suojaa konetta sellaisilta haittaohjelmilta, joista ei vielä ole tullut virustunnisteita. Virusten löytäminen perustuu järjestelmässä ilmeneviin muutoksiin, jotka virustorjuntaohjelmisto huomaa haittaohjelman aiheuttamaksi.

Osa virustorjuntaohjelmista antaa epäilyttävän ohjelman toimia eräänlaisessa suojatussa tilassa, jolloin ohjelma ei voi vahingoittaa järjestelmää. Virustorjunta analysoi ohjelman käyttäytymisen ja käyttäjän määrittelemien asetusten pohjalta sen, sallitaanko ohjelman tehdä muutoksia järjestelmään. Yleensä tarkistuksen asetuksista voidaan määritellä, mitä tiedostotyyppejä tarkistetaan. Virustarkistus tulisi määritellä koskemaan kattavasti kaikkia tiedostotyyppejä ja pakattuja tiedostoja.

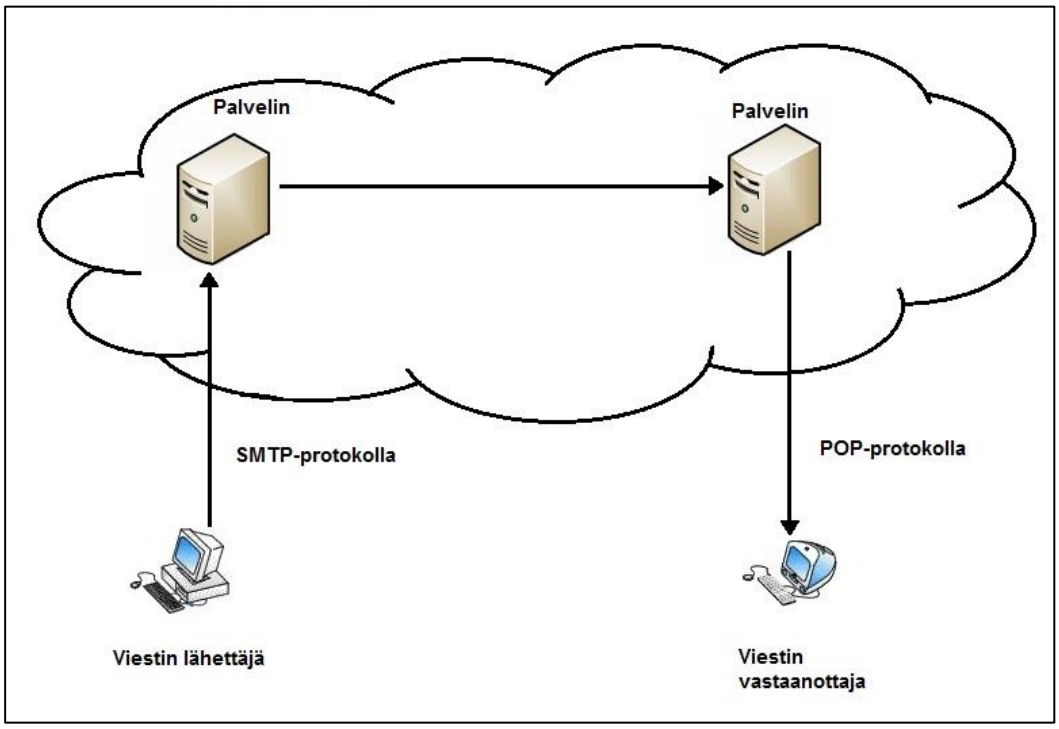
Virustarkastuksen lisäksi monessa ohjelmistossa on mahdollista säätää vakoiluohjelmien tarkistukseen liittyviä asetuksia. Vakoiluohjelma eli spyware on haittaohjelma, joka asentaa itsensä työasemaan käyttäjän tietämättä. Tämän jälkeen ohjelma toimii taustalla keräten tietoa käyttäjästä ja tietokoneesta. Vakoiluohjelmien avulla voidaan esimerkiksi seurata, mitä ohjelmia työasemilla on ajettu ja millä verkkosivuilla on vierailtu. [3, s. 136.] Vakoiluohjelmat voivat varastaa arkaluontoista tietoa, kuormittavat tietojärjestelmää sekä lähettävät selaimeen mainoksia ja ponnahdusikkunoita.

Viruskaranteeni on virustorjuntaohjelmiston varaama paikka kiintolevyltä, jossa olevat tiedostot ovat eristettyinä muista tietokoneen tiedostoista. Virustorjuntaohjelmisto on ainut sovellus, joka voi käyttää karanteenissa olevia tiedostoja. Viruskaranteenia käytetään virusten varastointiin esimerkiksi silloin, kun virustorjuntaohjelma löytää haittaohjelman, jota käyttäjä ei halua tai voi poistaa. Karanteenia voidaan käyttää myös kaikkien epäilyttävien tiedostojen varastointiin myöhempää tutkimista varten. Käyttäjä voi myös esimerkiksi varastoida kopioita käyttöjärjestelmän toiminnan kannalta oleellisista tiedostoista viruskaranteeniin. [4.] Viruskaranteeniin tulisi asettaa aika, jota vanhemmat kohteet poistetaan automaattisesti karanteenista. Automaattinen karanteenin tyhjennys auttaa säästämään levytilaa työasemilta ja samalla varmistaa karanteenin tyhjentämisen säännöllisesti.

Osa haittaohjelmista leviää sähköpostin liitetiedostojen välityksellä. Haittaohjelman sisältävä liitetiedosto on varustettu viestin vastaanottajaa kiinnostavalla nimellä tai kuvakkeella. Ava-

tessa liitetiedostoa haittaohjelma aktivoituu. Yleistä on myös viestin lähettäjätietojen väärentäminen, jolloin vastaanottaja ei osaa epäillä viestin aitoutta. [5.] Haittaohjelma jatkaa leviämistään lähettämällä viestejä muihin tililtä löytyviin sähköpostiosoitteisiin. Pahimmassa tapauksessa haittaohjelma voivat tuhota ja varastaa tiedostoja, kuormittaa työasemaa sekä avata tietojärjestelmään takaovia. Takaovien avulla voidaan ohittaa esimerkiksi palomuuri ja muita verkon turvallisuuteen liittyviä palveluita [5].

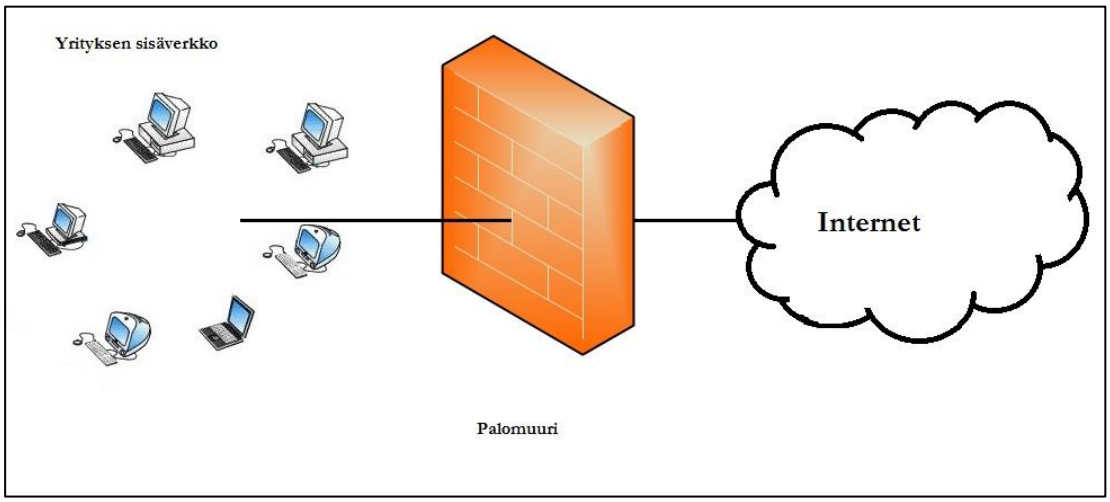
Sähköpostijärjestelmä (kuva 1) koostuu verkosta, postitoimistoista sekä käyttäjän postiohjelmasta. Postitoimisto on palvelin, joka ottaa vastaan käyttäjiensä postit ja jakaa ne käyttäjien postilaatikoihin. Postilaatikko sijaitsee palvelimella, josta käyttäjä voi lukea tai hakea viestinsä omalle työasemalleen. Postipalvelin voi olla yrityksen omassa verkossa tai ulkoistettuna esimerkiksi internetoperaattorille. Viestiä lähettäessä sähköpostiohjelmisto ottaa yhteyden omaan postitoimisto-palvelimeen, jonka jälkeen palvelin etsii sähköpostiosoitteessa olevan domain-nimen perusteella vastaanottajan postitoimisto-palvelimen. Jokaiseen domain-nimeen liittyy mail exchange -tietue, joka kertoo kyseiseen domainiin saapuvaa sähköpostia käsittelevän palvelimen IP-osoitteen. Postitoimistojen välillä kulkevaa liikennettä voidaan pitää turvallisena, mutta haavoittuvia osia ovat postitoimistot ja sen käyttäjien väliset yhteydet. [3, s. 216–217.]



Kuva 1. Sähköpostiviestin lähetys

Usein haittaohjelmat käyttävät hyväkseen selaimessa olevia tietoturva-aukkoja. Tämän vuoksi virustorjuntaohjelmat sisältävät selainsuojan, joka tutkii selaimen ja verkon välistä liikennettä. Ohjelmistosta riippuen voidaan määrittää ennalta ne toimenpiteet, joita tehdään, kun havaitaan haittaohjelma tai kun tarkistus epäonnistuu. Osa virustorjuntaohjelmista ilmoittaa sivun turvallisuuden ja antaa käyttäjälle mahdollisuuden määritellä sellaisia sivustoja, joita voidaan pitää turvallisina. Selainsuojan avulla voidaan myös usein estää selaimen pääsy vaarallisina pidetyille verkkosivustoille. Estämällä tarpeettomia ja mahdollisesti vaarallisia verkkosivustoja voidaan ehkäistä haittaohjelmien leviämistä työasemiin selaimen kautta.

Palomuuria (kuva 2) voidaan pitää suodattimena sisäverkon ja ulkoisen verkon välillä. Se pyrkii estämään haittaohjelmien leviämisen tarkkailemalla sen läpikulkevaa verkkoliikennettä ja päästämällä vain harmittomat paketit läpi.



Kuva 2. Palomuurin toimintaperiaate

Yksinkertaisimmillaan palomuuri voi olla pakettisuodatin, jolloin se tutkii IP-pakettien lähtö- ja kohdeosoitteet sekä porttinumeron. Palomuuriin voidaan tehdä sääntöjä, joilla määritellään, mitkä portit ja osoitteet ovat missäkin tilanteissa sallittuja. Jos paketti ei täsmää yhteenkään sääntöön, se hylätään [3, s. 316.]

Palomuuri voi olla myös dynaaminen pakettisuodatin. Silloin palomuuri tarkkailee pakettien sisältöä sekä niiden keskinäistä järjestystä. Palomuuri analysoi aktiivisten TCP-yhteyksien tilaa, hyväksyen vain loogisesti oikeat paketit. Näin voidaan torjua palvelunestohyökkäykset sekä mahdolliset yritykset väärentää ulkopuolisen työaseman IP-osoite kuulumaan yrityksen sisäverkkoon. [3, s. 317–318.]

Palomuuri sääntöjen avulla voidaan sallia, rajoittaa tai estää palveluita. Sääntöjä luodessa järjestelmänvalvojan tulisi sallia vain kaikkein välttämättömimmät palvelut, kieltää muut ja tarvittaessa lisätä uusia palveluita. Vaihtoehtoinen tapa on kieltää vaarallisina pidettävät palvelut ja sallia kaikki muut. Tämä ei kuitenkaan ole suositeltavaa, sillä nyt turvallisina pidetyt palvelut voivat sisältää tietoturvariskejä tulevaisuudessa. [6.]

Sovellustenhallinnan avulla voidaan sallia luotettavana pidettäviä sovelluksia ja estää epäilyttävien sovellusten pääsy verkkoon. Se suojaa etenkin sellaisilta haittaohjelmilta, jotka pyrkivät lähettämään tietoa verkkoon. Esimerkiksi troijalaiset virukset voivat avata takaoven tietojärjestelmään, jonka jälkeen hyökkääjä voi ottaa työaseman haltuunsa.

Sovellusten hallintaa voidaan käyttää palomuurisääntöjen tarkentamiseen. Yleensä palomuurisäännöissä määriteltyjä estoja verkkoliikenteeseen ei voida ohittaa sovellusten hallinnan kautta. Palomuurin säännöissä voidaan esimerkiksi sallia tietyn tyyppinen verkkoliikenne ja sovellusten hallinnan avulla voidaan rajoittaa erikseen ne sovellukset, jotka saavat käyttää tätä sääntöä hyväkseen. [6.]

Hakalan, Vainion ja Vuorisen [2, s. 136] mukaan ongelmatilanteessa virustorjuntaohjelmisto suorittaa joko sille määritetyn automaattisen toimenpiteen tai kysyy käyttäjältä jatkotoimenpiteitä. Tietoturvallisuuden kannalta ohjelmistot tulisi kuitenkin määritellä niin, ettei käyttäjän itse tarvitse tehdä valintoja.

Asetuksista tulisi etenkin rajata käyttäjän mahdollisuuksia tehdä muutoksia virustorjunta ohjelmistoon. Esimerkiksi käyttäjällä ei saisi olla oikeutta poistaa virustorjuntaohjelmaa työasemaltaan, sulkea palomuuria tai keskeyttää päivitysten latausta. Työaseman tulisi myös säännöllisin väliajoin tarkastaa, onko palvelimelta asetettu siihen muutoksia. Vahingon sattuessa tieto virustartunnasta tulisi saada tietoturvasta vastaavien henkilöiden tietoon mahdollisimman nopeasti. Keskitetyn hallinnan sovellukset mahdollistavat hälytyksen lähettämisen ja raporttien reaaliaikaisen seuraamisen.

Työasemien tietoturvallisuuden kehittämisen ja ylläpidon kannalta on oleellista saada säännöllisesti tietoa järjestelmästä. Erilaisten raporttien avulla voidaan muodostaa tehokkaasti kokonaiskuva järjestelmän tilanteesta. Raporttien avulla voidaan havaita tartunnat ja paikantaa ne työasemat, joissa haittaohjelmia esiintyy. Raporttien avulla voidaan myös varmistaa, että käytössä olevat ohjelmistoversiot ovat ajan tasalla.

2.4 Muita keskitetyn hallinnan sovelluksia

Esimerkiksi Microsoft tarjoaa yritysasiakkaille System Centre 2012 Endpoint Protection -ohjelmistoa. Ohjelmisto on rakennettu System Centre Configuration Manager 2012

-ohjelmiston päälle ja mahdollistaa työasemien virustorjunnan keskitetyn hallinnan. Virustorjuntaohjelmisto on toteutettu samalla tekniikalla kuin yksittäisille työasemille tarkoitettu Microsoft Security Essentials -virustorjuntaohjelmisto. [7.]

Työasemasta joudutaan usein rajaamaan pois ylimääräisiä palveluita ja määrittelemään käyttäjälle sopivat käyttöoikeudet tietojärjestelmään. Näitä voidaan säätää kattavasti esimerkiksi ryhmäkäytäntöjen eli Group Policyn avulla.

Ryhmäkäytäntöasetukset on tarkoitettu ensisijaisesti keskitetyksi hallintavälineeksi jota käytetään Active Directory -hakemiston kautta [8]. Ryhmäkäytäntö on työkalu Windows-käyttöjärjestelmällä toimivien työasemien asetusten ja käyttäjäoikeuksien määrittelyyn. Sillä voidaan esimerkiksi luoda tietynlaiset työpöytämääritykset halutuille käyttäjäryhmälle tai joukolle tietokoneita, muokata käyttäjän oikeuksia tietojärjestelmään, ajaa komentosarjoja sekä asentaa, poistaa tai päivittää sovelluksia työasemiin. Tehdyt ryhmäkäytäntöasetukset sijaitsevat ryhmäkäytäntöobjekteissa (GPO), jotka kohdistetaan Active Directory -säiliöihin: toimipaikka, toimialue tai organisaatioyksikkö. [9.]

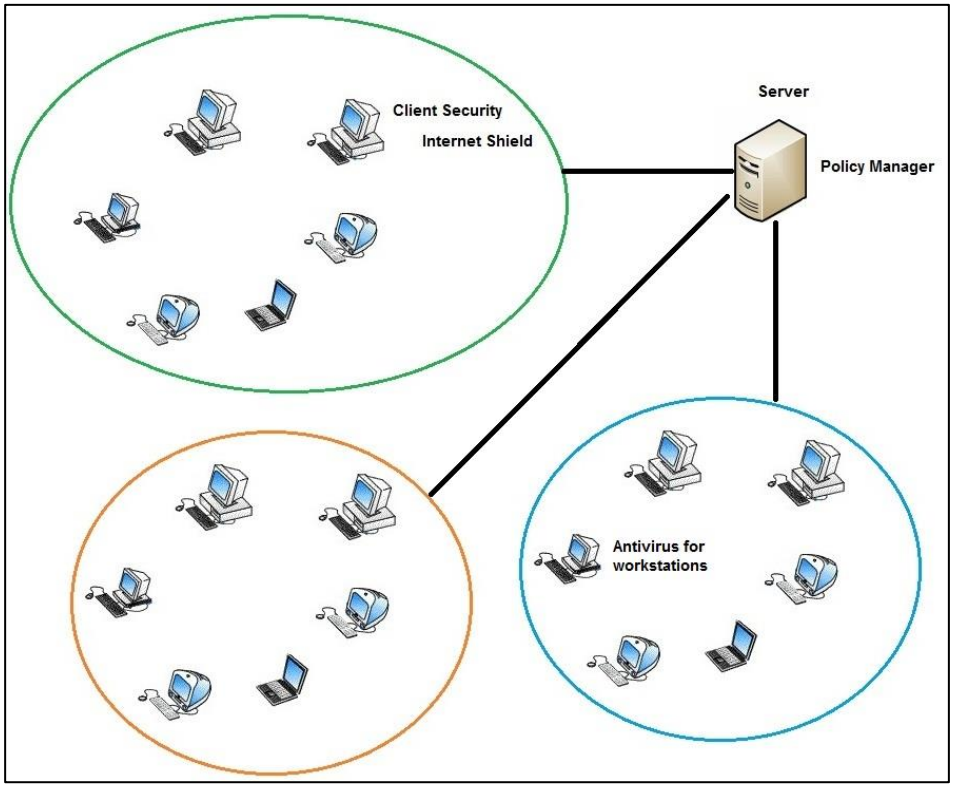
Monet ryhmäkäytäntöasetukset rajoittavat toimintaa, mutta niillä parannetaan tietoturvaa haittaohjelmien varalta. Periaatteessa kaikki ryhmäkäytäntöasetukset voitaisiin tehdä suoraan rekisterimuutoksina, jolloin käsittely olisi huomattavasti työläämpää ja vaarallisempaa kuin hallintaohjelman käyttö. [8.]

2.5 Policy Manager

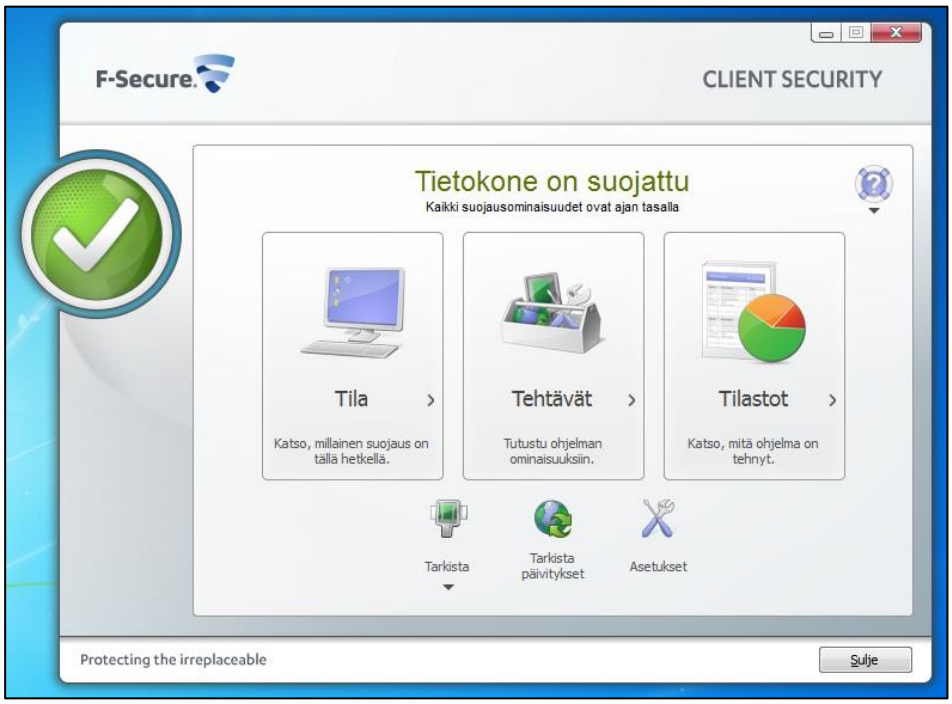
Policy Manager Console on F-Securen julkaisema ohjelmisto työasemien tietoturvan keskitettyyn hallintaan. Ohjelmistolla voidaan hallita kaikkia F-Securen yrityslisenssituotteita [9]. Policy Manager Console asennetaan palvelimelle, jonka kautta sitä voidaan käyttää tietoturvamenettelyiden määrittämiseen ja niiden jakamiseen organisaation sisällä. Kuvassa 3 on esitetty Policy Managerin yleinen toimintaperiaate, jossa organisaation työasemat on jaettu eri Policy Domaineihin. Työasemien käyttötarkoituksesta riippuen Policy Domaineihin voidaan määrittää erilaiset tietoturva-asetukset. Client Security (kuva 4) on F-Securen julkaisema vi-

rustorjuntaohjelmisto työasemiin. Client Security -käyttöliittymä on työaseman käyttäjälle näkyvä osa virustorjuntaohjelmistoa. Se vastaa yksittäisen työaseman tietoturvasta.

Suojatun yhteyden varmistaminen palvelimella olevan Policy Manager Consolen ja host -työaseman välillä perustuu digitaaliseen allekirjoitukseen. Se toteutetaan ”admin.pub” ja ”admin.prv” avainparin avulla. Avaimet luodaan Policy Manager Consolen asennuksen yhteydessä. ”Admin.pub”-tiedosto toimii julkisena avaimena, johon hallittavana olevalla työasemalla tulee olla pääsy. Julkisen avaimen lisäksi tarvitaan salainen admin.prv-avain. Avaimet toimivat parina, ja jos toinen avain menetetään, joudutaan luomaan uusi avainpari. [10.]

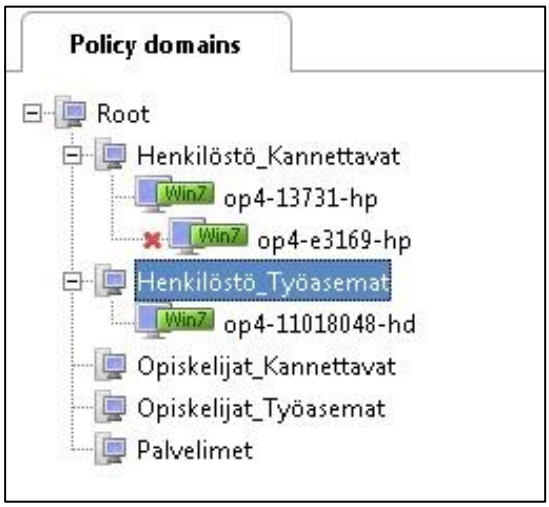


Kuva 3. Policy Managerin toimintaperiaate



Kuva 4. Client Security-käyttöliittymä

Palvelimella sijaitsevaan Policy Manager Consoleen voidaan rakentaa Policy Domain-rakenne, jonka avulla organisaation työasemat voidaan jakaa useampiin eri haaroihin. Näin erityyppisiin työasemiin voidaan määritellä halutunlaiset tietoturva-asetukset ja käytännöt. Policy Domain tree (kuva 5) rakentuu root-tasosta ja sen alle lisätyistä haaroista. Muutokset periytyvät ylemmästä haarasta alempiin haaroihin ja niihin lisättyihin työasemiin. Root-tasolla tehdyt muutokset tulevat voimaan kaikissa haaroissa ja sen kautta kaikissa työasemissa.



Kuva 5. Policy Domains

Policy Managerista voidaan valita kaksi eri tilaa, jossa muutoksia asetetaan. Antivirus mode on yksinkertaistettu tila, jossa hallitaan pääasiallisesti Client Security- ja Antivirus for Workstations -ohjelmistoja. Advanced mode on paljon kattavampi kokonaisuus, jossa voidaan säätää Client Securityn kaikkia ominaisuuksia, jotka eivät ole esillä normaalissa antivirus modessa. Advanced mode on tarkoitettu kaikkien F-Securen tuotteiden keskitettyyn hallintaan. [11.]

F-Securen palomuuri sisältää joukon turvallisuustasoja, joista jokaiselle tasolle on ennalta määritellyt palomuurisäännöt. Näiden sääntöjen avulla voidaan määrittää, millaista verkkoliikennettä sallitaan työasemassa. Työaseman käyttötarkoituksesta, yrityksen tietoturvapolitiikasta sekä käyttäjän taidoista ja kokemuksesta riippuen voidaan valita koneelle parhaiten sopiva tietoturvataso. Alla olevassa taulukossa (taulukko 1) on kerrottu Policy Managerissa oletuksena esiintyvät turvallisuustasot sekä yleinen kuvaus tason turvallisuusasetuksista.

Taulukko 1. Policy Managerissa oletuksena olevat turvallisuustasot

Turvallisuus taso	Kuvaus
Mobile	Sallii normaalin verkon selailun ja tiedoston haun. HTTP, HTTPS, FTP, sähköposti ja Usenet news liikenteen. VPN ja SSH ovat myös sallittuja. Kaikki muu on kielletty. Kielletty saapuva TCP-liikenne aiheuttaa hälytyksiä.
Home	Sallii kaiken lähtevän TCP-liikenteen ja FTP tiedostojen haun. Kaikki muu on kielletty Kielletty saapuva TCP-liikenne aiheuttaa hälytyksiä.
Office	Sallii kaiken lähtevän TCP-liikenteen ja FTP-tiedostojen haun. Kaikki muu on oletuksena kielletty ja vain haittaohjelmat aiheuttavat hälytyksiä.
Strict	Sallii lähtevän verkko selailun, sähköposti, ja NEWS-liikenteen, salatun liikenteen, FTP-liikenteen ja etäpäivitykset
Custom	Vapaasti muokattavissa oleva turvallisuustaso. Ei alkuperäisiä asetuksia.
Disabled	Palomuuri pois käytöstä
Network quarantine	Sallii vain automaattisten päivitysten lataamisen ja yhteydet Policy Manager palvelimeen. Kaikki muut verkkoyhteydet on estetty.

Turvallisuustasojen lisäksi palomuuriasetuksista voidaan säätää verkkoliikenteen suodatus, palomuurisäännöt sekä verkkopalveluihin liittyvät asetukset. Verkkoliikenteen suodatus voidaan määrittää kolmeen eri tilaan. Normal-tilassa turvallisuustasoon määriteltyjen asetusten mukainen suodatus on käytössä, bypass-tila ohittaa palomuurin eli sallii kaiken liikenteen ja ohjelmat. Block-tila estää kaiken verkkoliikenteen. [9.] Network quarantine on palomuurin ominaisuus, jonka avulla voidaan rajoittaa tai estää host-koneilta verkkoon pääsy, jos virus-

tunnisteet ovat määriteltyä aikaa vanhempia tai realtime scanning -toiminto on sammutettuna [12].

Voimassa olevia palomuurisääntöjä voidaan asettaa Firewall rules -välilehdellä. Sääntö voi sallia, rajoittaa tai estää palveluita. Jokaiselle turvallisuus tasolle asetukset tulee säätää erikseen. Kaikkiin paitsi custom-tasolle on valmiiksi määriteltyjä palomuurisääntöjä. Säännöt periytyvät Root-tasolta, joka tulee olla valittuna sääntöjä muokatessa. [12.]

Firewall services -välilehdeltä säädetään verkkopalveluiden asetuksia. Verkkopalvelulla tarkoitetaan internetissä olevaa sisältökokonaisuutta. Esimerkiksi yhden internetosoitteen takaa löytyvistä sivuista ja sisällöstä muodostunutta kokonaisuutta voidaan kutsua verkkopalveluksi.[13, s. 14–15.] Palveluita kuvataan usein sen mukaan, mitä protokollaa ja porttia ne käyttävät [14].

3 NYKYTILANTEEN KARTOITUS

Tässä osiossa tarkastellaan Kainuun ammattiopiston työasemien nykytilannetta tietoturvan kannalta. Nykytilanteen kartoittamisen tavoitteena on tuoda esiin suojattavia kohteita ja mahdollisia puutteita. Kartoituksen pohjalta voidaan kehittää keinoja näiden puutteiden korjaamiseksi.

3.1 Nykytilanne Kainuun ammattiopistolla

Kainuun ammattiopistolla työasemien tietoturvaa hallitaan ja ylläpidetään keskitetysti F-Securen Policy Manager 10 -ohjelmiston avulla. Työasemiin on käyttöjärjestelmän asennuksen yhteydessä asennettu Client Security, joka vastaa työaseman tietoturvasta. Tietokoneita on järjestelmässä arviolta noin 3000 kappaletta. Koneet on jaettu Policy Managerin useisiin eri haaroihin, joissa vallitsevat erilaiset tietoturva-asetukset.

Kulunvalvonta on hoidettu organisaatiossa hyvin. Työasemat sekä palvelimet ovat lukituissa tiloissa, joihin vain niihin oikeutetuilla henkilöillä on pääsy. Yrityksessä on myös käytössä kameravalvonta. Henkilökunta tunnistetaan henkilökortin perusteella, joka on aina työntekijän mukana. Käyttäjällä on henkilökohtainen käyttäjätunnus ja salasana, joilla suoritetaan kirjautuminen työasemaan. Tietokoneiden BIOS on suojattu salasanalla. Käyttäjäoikeuksia hallitaan Group Policyllä.

Admin-oikeudet ovat vain järjestelmän ylläpitäjillä. Tämän lisäksi osalle henkilökuntaa on annettu heidän käytössään oleviin kannettaviin työasemiin tehokäyttäjän oikeudet, jotka vastaavat melkein pääkäyttäjien oikeuksia. Tarkoituksena on se, että käyttäjät voivat asentaa tarvitsemiaan ohjelmia koneelle, mutta eivät kuitenkaan voi ohittaa esimerkiksi käyttäjätunnusten hallintaoikeuksia.

Varmuuskopiointia varten henkilöstöllä on käytössä oma verkkoasema työtiedostoja varten. Henkilökunta voi myös käyttää ulkoisia kovalevyjä ja muistitikkuja tiedostojensa varmuuskopiointiin. Palvelinten osalta on käytössä varmistusnauhasetti, jossa on säännöllinen kierto.

Nauhoilta voidaan palauttaa esimerkiksi puoli vuotta vanhaa tietoa takaisin. Osa palvelimista on virtuaalisia, jolloin C-asema ei muodostu kriittiseksi.

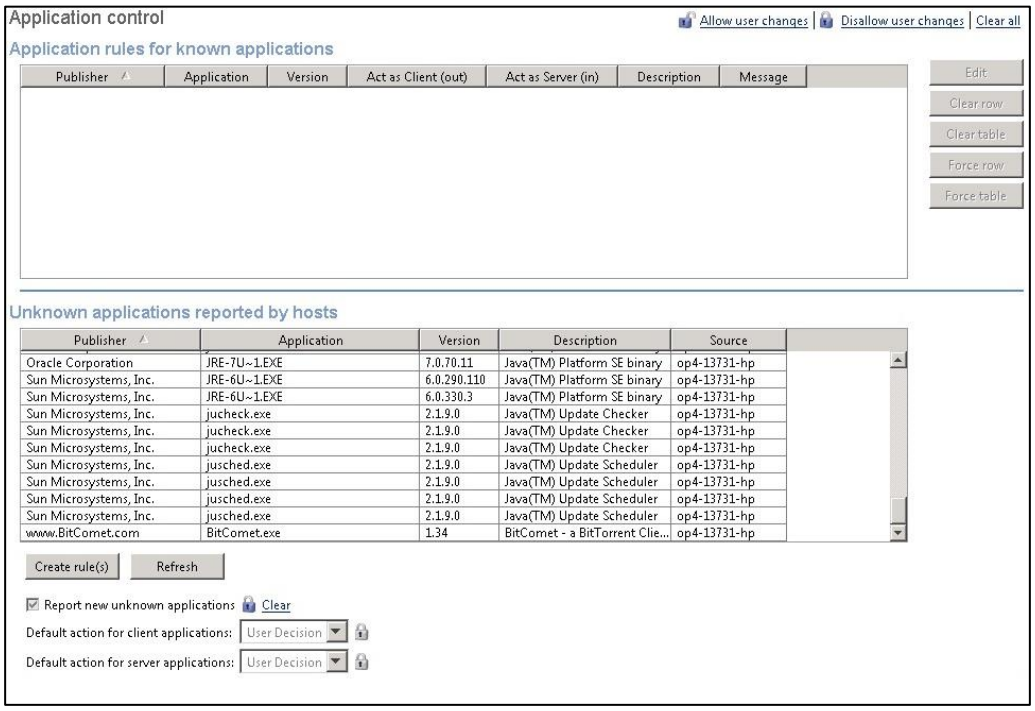
Sähköpostilaatikot sijaitsevat palvelimella, josta niiden sisältö synkronoidaan työasemaan. Tällöin esimerkiksi tietokoneen kovalevyn hajotessa postikanta synkronoidaan tietokoneeseen ja sähköposteja ei menetetä.

3.2 Mahdolliset ongelmakohdat

Policyjen perusasetukset periytyvät root-tasolta, mutta tämän lisäksi kuhunkin haaraan on aina tilanteen mukaan tehty muokkauksia. Hallintahaaroja on luotu tarpeen mukaan, ja niiden nimeämisestä puuttuu yksiselitteisyys. Nykyisellään vallitseva järjestelmä ei ole niinkään riskialtis, mutta koneiden kuuluminen eri haaroihin tekee järjestelmästä sekavan. Tämä johtuu siitä, että samoille käyttäjille tarkoitettuja työasemia löytyy useista eri paikoista. Esimerkiksi jos halutaan tehdä muutos kaikkiin opiskelijakoneisiin, joudutaan säätämään asetuksia useaan eri haaraan. Tämä aiheuttaa järjestelmän valvojalle lisää vaivaa verrattuna siihen, että muutokset voitaisiin tehdä kerralla. Pahimmassa tapauksessa osa koneista voi jäädä epähuomiossa haluttujen muutosten ulkopuolelle, jolloin niissä vallitsevat asetukset jäävät vanhentuneiksi ja saattavat näin muodostaa tietoturvariskejä.

Toimialueen työasemien tilaraportteja ei seurata säännöllisesti. Tämän vuoksi Host-työasemat eivät ole aina ajan tasalla. Yrityksessä on käytössä Client Securityn 9.32-version lisäksi myös muita vanhempia versioita. Nämä versiot osoittautuvat hitaiksi ja hankaliksi käyttää etenkin vanhemmilla koneilla, joissa ei ole tarpeeksi suorituskykyä.

Policy Managerin sovellusten hallintaa on vaikea ylläpitää, sillä tuntemattomien sovellusten taulukko (kuva 6) täyttyy ohjelmien eri versioista. Esimerkiksi Java-ohjelmistosta tulee useita päivityksiä, joiden kaikki versiot listautuvat taulukkoon. Taulukon ylläpito osoittautuu erittäin vaikeaksi. Nykyisellään vallitsevana käytäntönä on, että käyttäjä valitsee, sallitaanko sovellus vai ei.



Kuva 6. Sovellusten hallinta

Palomuurisääntöjen luomisesta puuttuu suunnitelmallisuus, jolloin käytännöt voivat olla hyvin epämääräisiä. Esimerkiksi palomuurisääntöjä luodaan aina tarpeen tullen. Palomuurista avataan tarvittavat portit yleensä silloin, kun huomataan jokin este organisaation toiminnassa. Palomuurisäännöt on nimetty epämääräisesti, koska missään ei ole määritelty tiettyä käytäntöä, jolla ne tulisi luoda.

Henkilökunnan työasemien osalta tulisi huomioida, ettei työasemissa ole automaattista uloskirjautumista. Salasanojen vaihtoa työasemiin ei vaadita säännöllisin väliajoin. Tällä hetkellä salasanan tulee sisältää kirjaimia ja numeroita, eikä salasanaa asettaessa vaadita erikoismerkkejä tai isoja kirjaimia.

Vaikka henkilöstöllä on käytössä verkkoasema, joihin voi tallentaa tiedostoja, osa työntekijöistä silti käyttää myös tietokoneen C-asemaa tiedostojen tallentamiseen. Tällöin työaseman kiintolevyn hajotessa tiedostoja on hankala, tai jopa mahdoton palauttaa. Henkilökuntaa tulisi tämän vuoksi ohjeistaa ottamaan tärkeistä tiedostoistaan varmuuskopioita säännöllisin väliajoin ja käyttämään omaa verkkoasemaa niiden varastointiin.

Sähköpostia voi kertyä käyttäjälle niin paljon, että palvelimelle määritelty levytila ei riitä. Yleensä tässä tilanteessa käyttäjät tekevät oman työaseman C-asemalle postiarkistoja, joihin sähköpostit varastoidaan. Kiintolevyn hajotessa nämä postiarkistot tuhoutuvat, ellei käyttäjä ole itse huolehtinut niiden varmuuskopioinnista.

4 POLICY MANAGERIN KONFIGUROINTI

Tässä luvussa kuvataan palomuurisääntöihin ja turvallisuustasoille tehtyjä muutoksia. Työasemien tietoturvallisuuden nykytilanteen kartoittamisen perusteella on pyritty esittämään hyviä käytäntöjä ja kehitysideoita tietoturvallisuuden tehostamiseksi.

4.1 Lähtötilanne

Insinöörityön tavoitteena oli tehostaa käytössä olevaa virustorjuntaohjelmistoa. Työssä muutettiin ohjelmiston asetuksia ja testattiin ohjelmiston eri toimintoja. Muutoksia ei voitu tehdä suoraan käytössä olevalle palvelimelle, koska se olisi häirinnyt organisaation normaalia toimintaa. Tämän vuoksi Policy Manager Console oli asennettu toiselle palvelimelle, jossa työn alussa ei ollut testikoneen lisäksi muita hallittavia työasemia. Työn lopuksi kaikki ammattiopiston työasemat lisätään vähitellen tällä palvelimella olevaan Policy Manager Consoleen.

Policy Managerin Policy Domain -rakenne oli suunniteltu valmiiksi, ja siihen kuului viisi eri hallintahaaraa, joita ovat opiskelija kannettavat, opiskelija työasemat, henkilöstö kannettavat, henkilöstö työasemat sekä palvelimet. Rakenteen tarkoitus on vähentää ylimääräisiä haaroja ja jakaa työasemat ryhmiin, joihin ne kuuluvat.

4.2 Työasemien lisääminen Policy Manager Consoleen

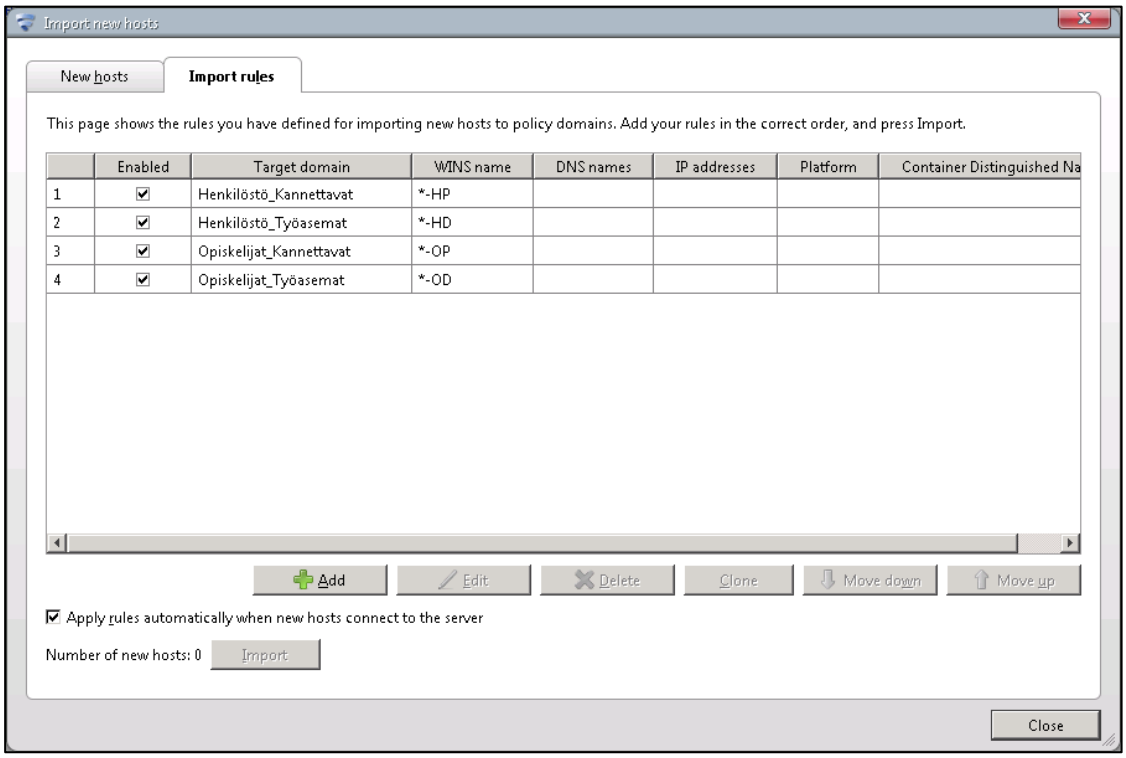
Client Security -ohjelmasta tehdään Policy Managerilla asennuspaketti, joka jaetaan ja asennetaan työasemiin keskitetysti. Paketin jakamiseen voidaan käyttää Policy Manageria. Asentaminen on kuitenkin käytännössä osoittautunut helpommaksi suorittaa työasemien käyttöjärjestelmän asennuksen yhteydessä SCCM:n avulla. Tätä menettelytapaa halutaan käyttää jatkossakin.

Client Security -ohjelman asentamisen jälkeen työasemat lisätään Policy Domain-rakenteeseen, joka voidaan toteuttaa monella eri tavalla. Esimerkiksi aktiivihakemiston mu-

kainen rakenne ja siinä olevat työasemat voidaan tuoda Policy Manageriin. Työasemia voidaan hakea toimialueelta tai yksitellen esimerkiksi niiden IP-osoitteen perusteella. Työasemien tuomiseen voidaan asettaa sääntöjä, joiden perusteella työasemat hakeutuvat oikeaan paikkaan. Kainuun ammattiopiston työasemat on nimetty hyvin yksiselitteisesti. Työaseman nimestä voidaan nähdä rakennus ja luokka, jossa tietokone sijaitsee. Työaseman nimen loppuosasta (taulukko 3) nähdään, onko työasema pöytäkone vai kannettava sekä henkilöstön vai opiskelijoiden käytössä. Kuvassa 7 nähdään sääntötaulukko, jossa työasemat on ohjattu hakeutumaan Policy Domain -rakenteeseen niiden nimen loppuosan perusteella.

Taulukko 2. Työasemien nimien päätteet

Työaseman nimen pääte	**Käyttäjäryhmä**
-OP	opiskelija kannettava
-OD	opiskelija pöytäkone
-HP	henkilökunta kannettava
-HD	henkilökunta pöytäkone

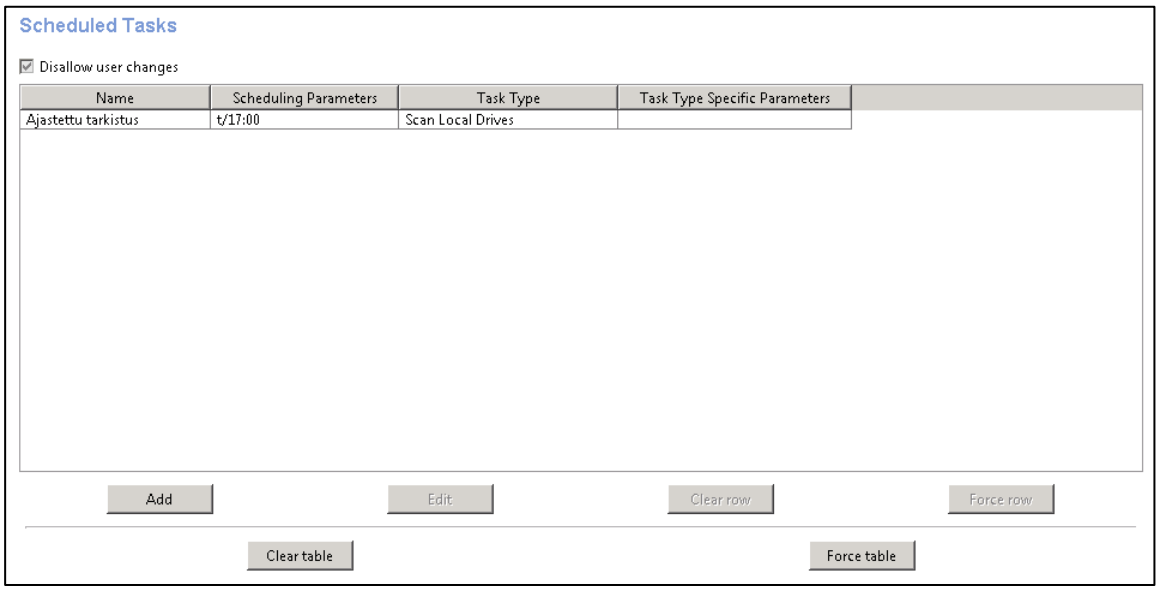


Kuva 7. Työasemien määräytyminen eri hallintahaaroihin.

4.3 Virustorjunta- ja palomuuriohjelmiston konfigurointi

Palomuurisäännöt pyritään määrittämään niin, että Kainuun ammattiopiston tarjoamat palvelut on taattu kaikille käyttäjäryhmille. Etenkin opiskelijakoneissa tietoturva-asetukset määritellään niin, että virustorjunnan ja palomuuriohjelmiston asetusten muokkaaminen on rajattua. Käyttäjän tulee päästä suorittamaan virustarkistus ja hakemaan uudet virustunnisteet. Käyttäjällä ei saisi olla oikeutta poistaa tai sulkea virustorjuntaohjelmistoa. Virustunnisteiden ja ohjelmiston päivitysten lataamista ei myöskään saisi katkaista. Opiskelijoiden käytössä olevista työasemista voitaisiin esimerkiksi estää verkkoon pääsy, jos virustunnistetiedot eivät ole ajan tasalla. Tietyissä tapauksissa opiskelijoiden sääntöä voitaisiin muokata siltä osin, että työasemista estetään internetiin pääsy. Tämäntyyppisiä työasemia on esimerkiksi autopuolen opiskelijoiden käytössä. Näillä työasemilla on tarkoitus päästä vain palvelimella sijaitsevaan autodata-ohjelmistoon. Työasemat on tarkoitettu pelkästään autodatan käyttämistä varten, jolloin niistä voitaisiin estää selaimen käyttö.

Policy Managerin ajastetut tehtävät toiminnolla luokkien työasemiin asetettiin automaattinen virustarkistus. Luokkien työasemat on asetettu olemaan arkisin päällä klo 20.00 asti. Virustarkistus tapahtuu päivittäin klo 17.00, jolloin se ei häiritse normaalia työskentelyä työasemalla.

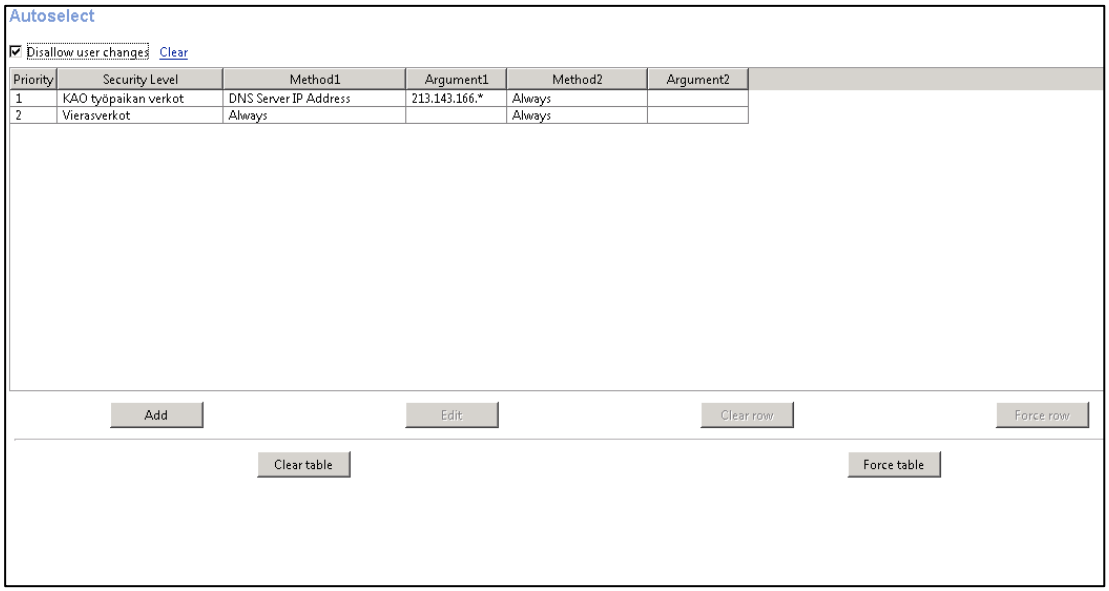


Kuva 8. Ajastettu virustarkistus

ICT-tuki tarvitsee palomuurin osalta kaikki mahdolliset avaukset, jotka takaavat toimivan etähallinnan. Nykyisellään olevassa järjestelmässä on varattu ICT-tuelle oma IP-osoitealue. Niihin on valmiiksi määritelty sääntö, joka sallii kaiken liikenteen molempiin suuntiin. Uudelle palvelimelle määritellään samankaltainen sääntö samalle IP-osoitealueelle.

Henkilöstön osalta nykyiset oletussäännöt ovat hyvät. Ne voidaan ottaa käyttöön uudessa Policy Managerissa sellaisenaan. Henkilöstön työasemissa voi olla vapaammat asetukset, verrattuna opiskelijoiden käytössä oleviin koneisiin. Etenkin henkilökunnan kannettaviin työasemiin asennetaan paljon käyttäjän toimesta ohjelmia, joihin tarvitaan järjestelmänvalvojan oikeuksia. Tämä on ratkaistu antamalla henkilöstölle kannettaviin työasemiin tehokäyttäjän oikeudet, jotka mahdollistavat ohjelmien asentamisen. Kannettavat työasemat siirtyvät verkosta toiseen, jolloin käyttäjällä tulisi olla enemmän oikeuksia tehdä muutoksia koneen asetuksiin.

Henkilöstön kannettavien työasemien palomuurin turvallisuustasot haluttiin määritellä niin, että koulun verkossa työasemassa on käytössä perusasetukset. Kun työntekijä vie koneen pois toimialueelta esimerkiksi omaan kotiverkkoonsa, turvallisuustaso vaihtuu ja palomuuri ottaa käyttöön tiukemmat turvallisuusasetukset. Tämä toteutettiin muokkaamalla F-Securen palomuurin Home- ja Office-turvallisuustasoja. Office-turvallisuustaso nimettiin uudelleen ”KAO työpaikan verkot”, joka on käytössä Kainuun ammattiopiston toimialueella. Home-turvallisuustaso nimettiin uudelleen ”Vierasverkot”, joka on käytössä kaikissa muissa verkoissa. Turvallisuustason valinta tehdään autoselection-toiminnolla, joka valitsee käytössä olevan turvallisuustason DNS-serverin IP-osoitteen perusteella.



Kuva 9. Turvallisuustason automaattinen valitseminen

5 TULOSTEN TARKASTELU

Policy Managerin Policy Domain-rakennetta oli muutettu yksiselitteisemmäksi. Tällä tavalla ohjelmiston käytettävyys selkeytyy huomattavasti. Muutoksia ei enää tarvitse tehdä useisiin eri paikkoihin ja eri käytössä olevat työasemat on helppo löytää omasta paikastaan.

Palomuuri- ja virustorjuntaohjelmiston oletusasetuksiin tehtiin muokkauksia. Valmiit turvallisuustasot Home ja Office nimettiin uudelleen ”KAO työpaikan verkot” ja ”Vierasverkot” -nimisiksi. Henkilöstön kannettaville työasemille asetettiin automaattinen turvallisuustason valinta, riippuen siitä, oliko työasema Kainuun ammattiopiston toimialueella vai asiakkaan kotiverkossa. Luokkien työasemille määriteltiin kerran päivässä tapahtuva ajastettu virustarkistus.

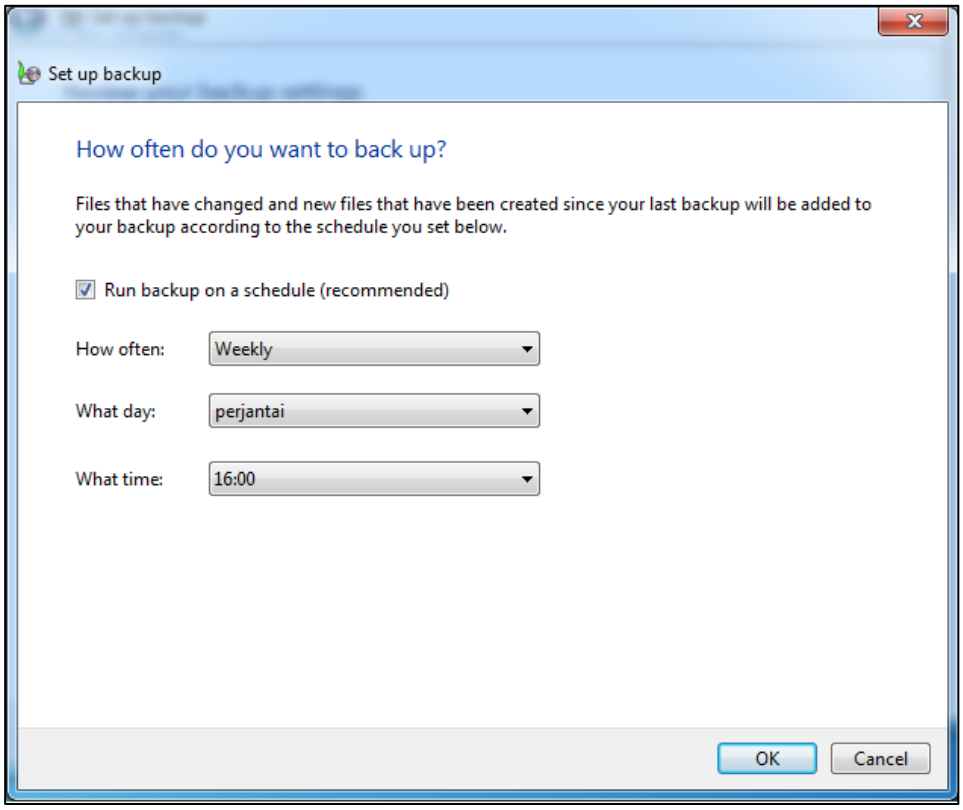
Työasemien tietoturvallisuuden nykytilanteeseen perehdyttiin tekemällä siitä suppea kartoitus. Kartoituksessa kuvattiin organisaation työasemien ja tietoturvallisuuden nykytilannetta. Perehtymisen perusteella pyrittiin löytämään heikkoja kohtia ja käytäntöjä jonka pohjalta voidaan esittää kehitysideoita, joilla tietoturvaa voidaan parantaa.

Sovellusten hallinta Policy Managerissa osoittautui ongelmalliseksi. Nykyisellään vallitsevana käytäntönä on se, että käyttäjä päättää, sallitaanko sovellus vai ei. Tämä jää vallitsevaksi menettelytavaksi. Jonoja voisi vähentää esimerkiksi se, että ylläpitäjä seuraa tilannetta säännöllisin väliajoin. Säännöllisen tilaraporttien seuraamisen avulla saadaan Client Security-ohjelmien versiot pysymään ajan tasalla.

Työasemien salasanat tulisi asettaa vähintään 8 merkkiä pitkiksi, niiden tulisi sisältää pieniä ja suuria kirjaimia, numeroita sekä erikoismerkkejä. Salasanat voidaan myös asettaa vaihtumaan säännöllisesti. Henkilökuntaa voidaan ohjeistaa käyttämään esimerkiksi salasanalauseita, jotka helpottavat salasanan muistamista.

Henkilöstön työasemiin tulisi asettaa koneiden automaattinen lukkiutuminen esimerkiksi 5–10 minuuttia työaseman käyttämättömänä olon jälkeen. Tämä parantaa tietoturvaa estämällä ulkopuolisten henkilöiden pääsyn työaseman kautta esimerkiksi verkkoasemille sekä käyttäjän tiedostoihin.

Mahdollisten laiterikkojen varalta henkilöstön tulisi suorittaa tiedostojensa varmuuskopiointia säännöllisin väliajoin. Esimerkiksi Windows 7-käyttöjärjestelmässä olevalla varmuuskopioi ja palauta -toiminnolla voidaan asettaa automaattinen tiedostojen varmuuskopiointi. Kopiot voidaan tallentaa esimerkiksi kannettavalle kiintolevylle, USB-tikulle, verkkoon, CD- tai DVD-asemalle. Käyttäjä voi itse valita, mistä tiedostoista hän haluaa ottaa varmuuskopiot ja kuinka usein varmuuskopioita otetaan (kuva 11). Tämän jälkeen Windows hoitaa tärkeiden tiedostojen varmuuskopioinnin käyttäjän asettamien määrittelyjen mukaan automaattisesti.



Kuva 10. Automaattisen varmuuskopioinnin määritys.

6 YHTEENVETO

Työn tavoitteena oli perehtyä F-Securen Policy Manager -tuotteeseen ja sen käyttöasteeseen organisaatiossa. Perehtymisen pohjalta suoritettiin muutoksia Policy Domain -rakenteeseen, palomuuri- ja virustorjuntaohjelmiston asetuksiin. Tarkoituksena oli saada organisaatiolle paras mahdollinen hyöty käytettävästä ohjelmistosta. Työasemien tietoturvallisuutta pyrittiin parantamaan tekemällä nykytilanteen kartoitus, jonka avulla etsittiin mahdollisia haavoittuvuuksia ja heikkouksia. Työssä on kuvattu kartoituksen pohjalta löytyneitä kehitysideoita. Kehitysideoita olivat mm. salasanojen monimuotoisuuden lisääminen, säännöllinen vaihto, työasemien automaattinen lukkiutuminen ja henkilöstön ohjeistaminen varmuuskopioiden ottamiseen.

Työn toteutusosassa kuvataan Policy Manager Consoleen tehtyjä muutoksia. Ajoitettujen tehtävien avulla luokkien työasemille asetettiin ajastettu virustarkistus. Palomuurisääntöjä pyrittiin miettimään ja asettamaan kullekin käyttäjäryhmälle sopiviksi. Palomuurisääntöjen avulla sallittiin ICT-tuen ja Netop-luokanhallinta ohjelman tarvitsema verkkoliikenne. Palomuurin turvallisuustasot Office ja Home nimettiin henkilöstön kannettaviin työasemiin kuvaavimmiksi KAO työpaikanverkot ja Vierasverkot. Henkilöstön kannettaviin työasemiin määriteltiin turvallisuustasot, jotka vaihtuivat automaattisesti työntekijän siirtäessä työasemansa toimialueelta toiseen verkkoon.

LÄHTEET

1 Kainuun ammattiopisto. viitattu 27.11.2012 [WWW-sivusto]
<http://www.kao.fi/fi/info/kainuun-ammattiopisto.html>

2 Hakala, M., Vainio, M., Vuorinen, O. Tietoturvallisuuden käsikirja. 1., painos. Porvoo: WS Bookwell, 2006. 421 s. ISBN 951-846-273-9.

3 Järvinen, P. Tietoturva & yksityisyys. 1., painos. Porvoo: WS Bookwell, 2002. 434 s. ISBN 951-846-152-X

4 Avast Antivirus. Yleistä viitattu 08.01.2013 [WWW-sivusto]
<http://avast.helpmax.net/fi/viruskaranteeni/yleista/>

5 Viestintävirasto cert-fi. viitattu 12.02.2013 [WWW-sivusto]
<http://www.cert.fi/ohjeet/2002/P_1.html>

6 F-Secure. Configuring Internet Shield. Viitattu 20.11.2012 [WWW-sivusto]
<http://www.f-secure.com/en_EMEA/downloads/documentation/online-help/pm/900/configuring_internet_shield/concepts/configuring_internet_shield.html>

7 Microsoft. System Center 2012 Endpoint Protection. Viitattu 27.11.2012 [WWW-sivusto]
<http://www.microsoft.com/en-US/server-cloud/system-center/endpoint-protection-2012.aspx>

8 Micropc. Ryhmäkäytännöt tukevat turvaa. Viitattu 12.02.2013 [WWW-sivusto]
<http://mikropc.net/nettilehti/pdf/0311200548.pdf>

9 F-Secure. Tuotteet ja palvelut. Viitattu 20.11.2012 [WWW-sivusto]
<http://www.f-secure.com/fi/web/business_fi/products/management/solution>

10 F-Secure Client Security. Quick Installation Guide. Viitattu 19.02.2013 [WWW-sivusto]

<http://www.f-secure.com/en/c/document_library/get_file?uuid=a8587a88-e258-4aad-b587-acf0ae93f41a&groupId=30743>

11 F-Secure. Viitattu 20.11.2012 [WWW-sivusto] <http://www.f-secure.com/en_EMEA/downloads/documentation/online-help/pm/1000/index.html>

12 F-Secure Policy Manager 10 ohjelmisto

13 Jussila, M. Leino, A. Verkkoviestinnän käsikirja. Hämeenlinna: Karisto Oy, 1999. 215 s. ISBN 952-5123-14-6

14 F-Secure. Advanced features: Internet Shield Viitattu 20.11.2012 [WWW-sivusto] <http://www.f-secure.com/en_EMEA/downloads/documentation/online-help/pm/900/advanced_internet_shield/concepts/advanced_is.html>

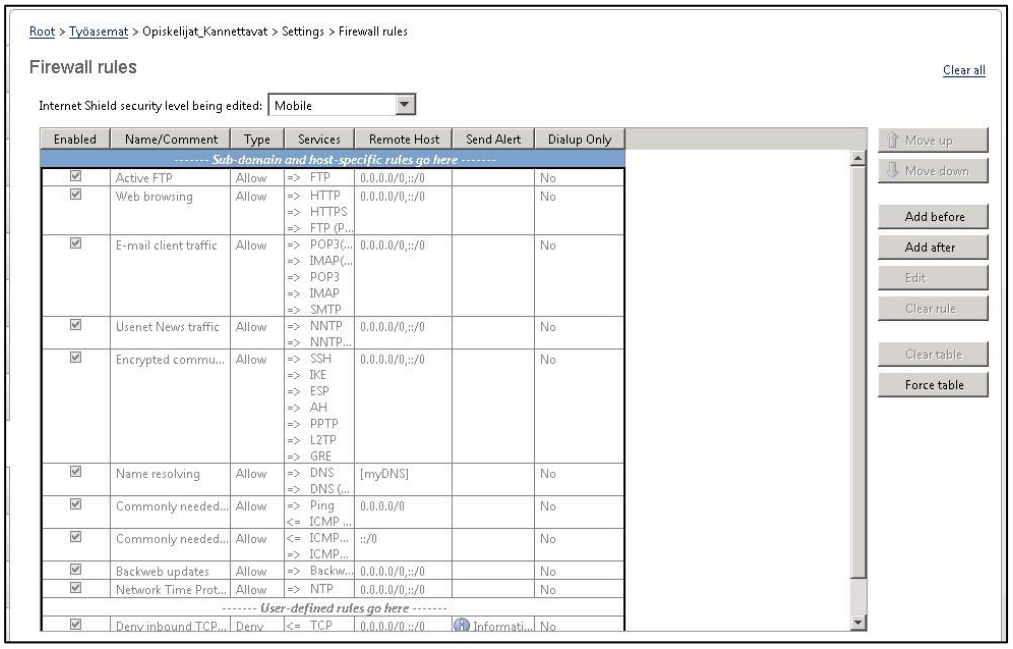
LIITTEET

LIITE 1 - Palomuurisääntöjen lisääminen

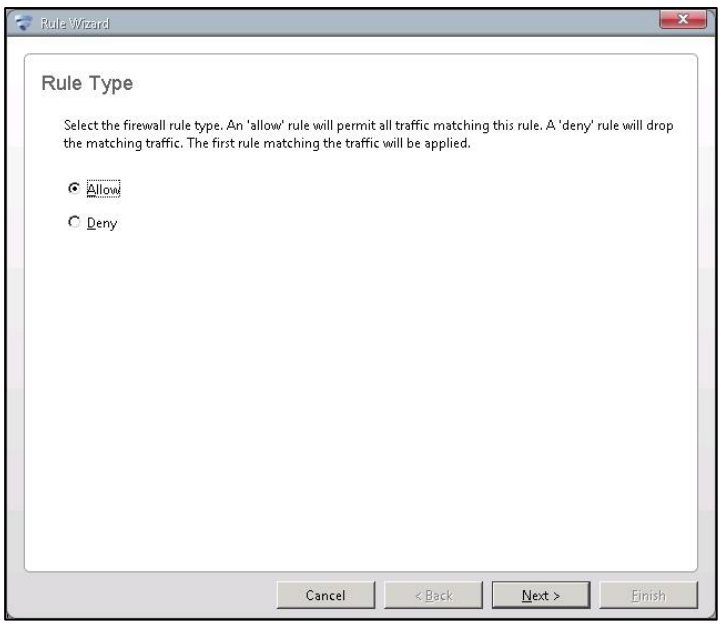
LIITE 2 - Palomuurin turvallisuustasojen automaattinen valinta

LIITE 3 - Virustarkistuksen ajastaminen

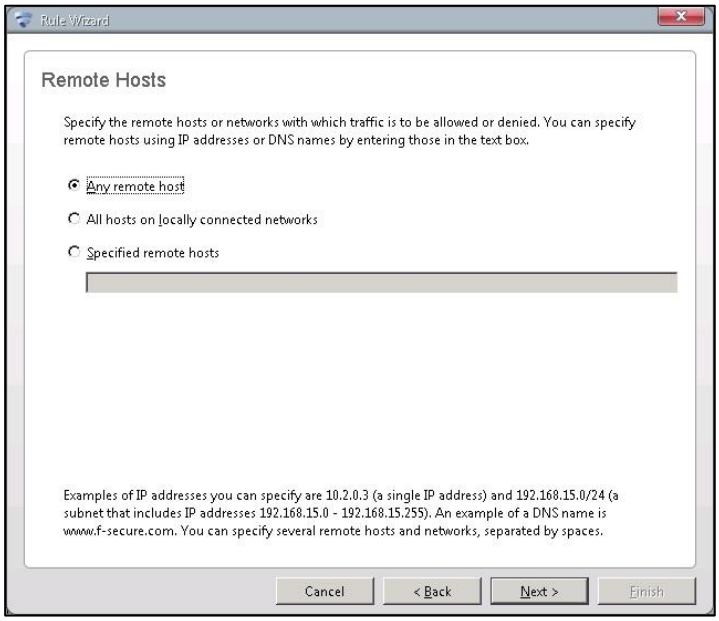
Palomuurisääntöjä määriteltiin ITC-tuen tarvitsemalla liikenteelle ja Netop-luokanhallinta ohjelman tarvitsemalle liikenteelle. Kullakin turvallisuustasolla vallitsevia palomuurisääntöjä asetetaan Policy Manager Console ohjelmiston Firewall rules-välilehdeltä. Add before- ja add after-painikkeet avaavat Rule Wizardin, jonka avulla palomuurisääntöjä voidaan lisätä.



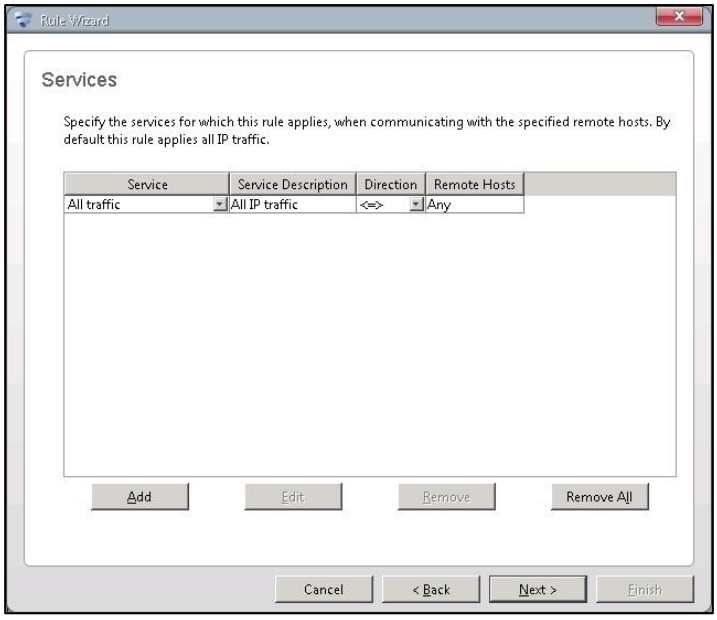
Sääntö voidaan asettaa joko sallimaan, tai estämään verkkoliikennettä.



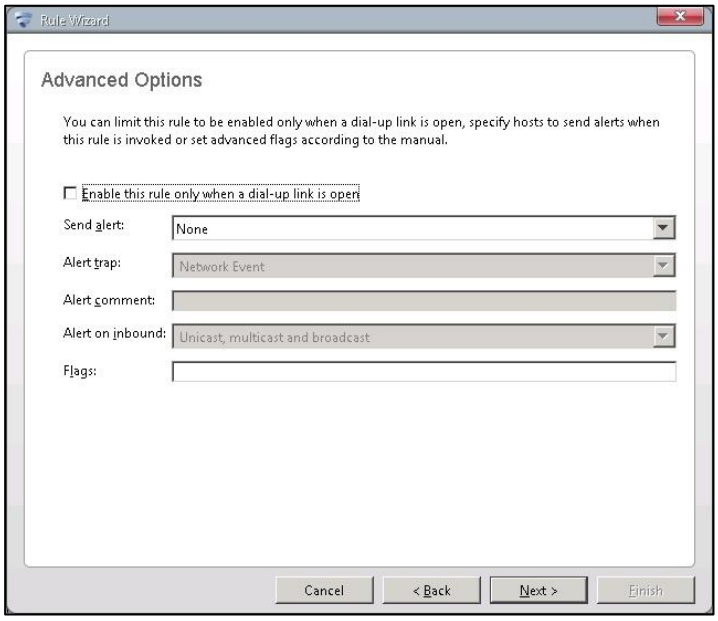
Tämän jälkeen valitaan mitä työasemia sääntö koskee. Sääntö voidaan asettaa voimaan kaikissa hallittavissa koneissa tai esimerkiksi vain tietyissä koneissa IP-osoitteen perusteella.



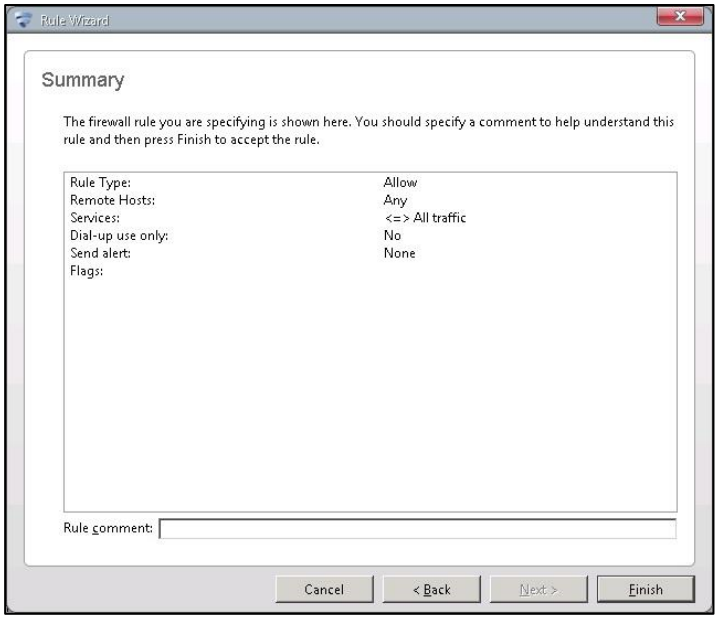
Seuraavaksi määritellään mihin suuntaan ja mitä liikennettä sääntö koskee. Yksittäisiä palveluita voidaan lisätä niin paljon kuin tarvitaan. Sääntö voi koskea host-koneelta lähtevää, saapuvaa tai kaikkea liikennettä.



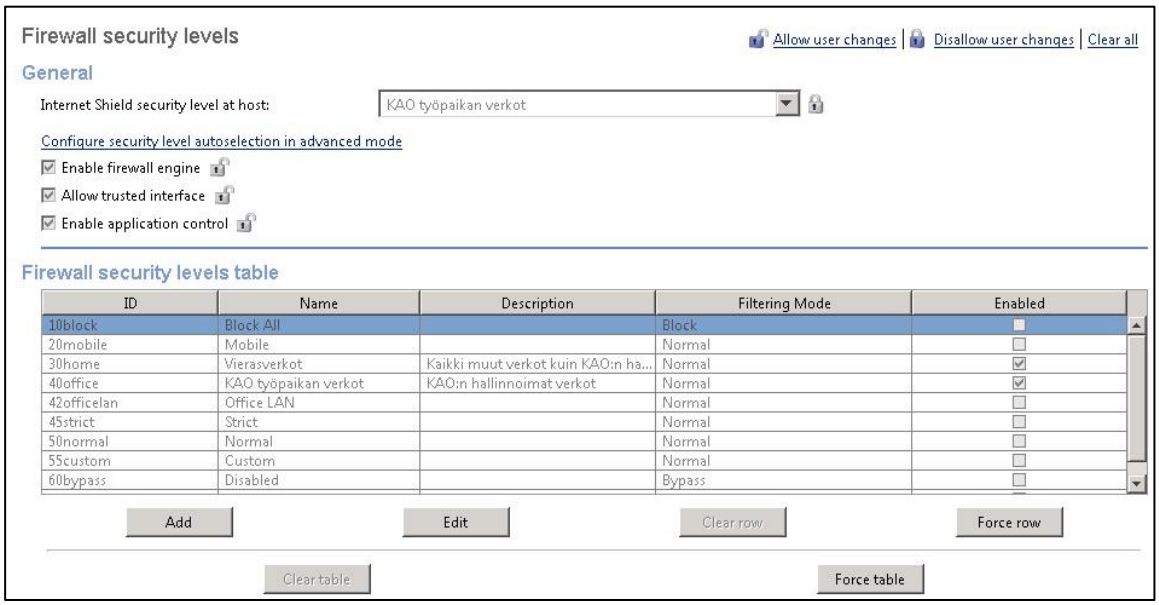
Sääntöön voidaan lisätä hälytys, joka ilmoittaa, kun säännön mukaista liikennettä havaitaan työasemissa.



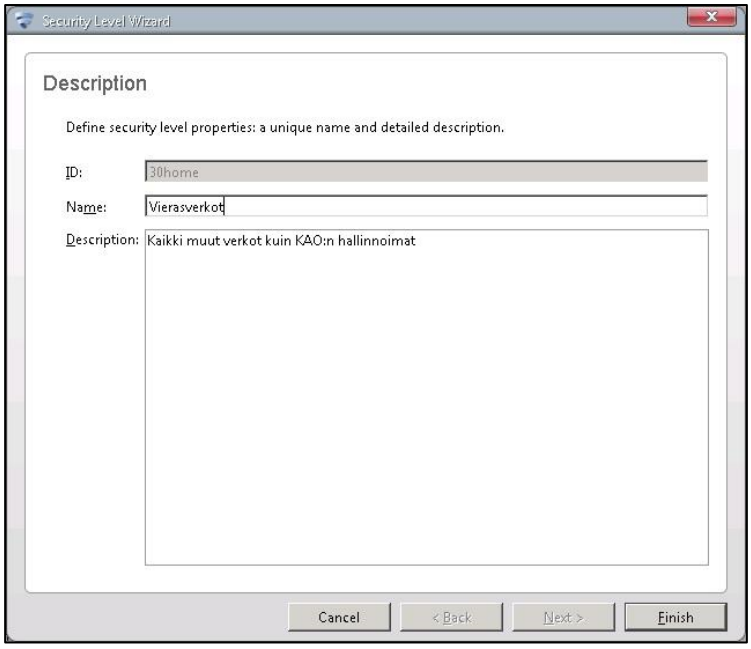
Lopuksi tulee yhteenveto, jossa nähdään luotu sääntö.



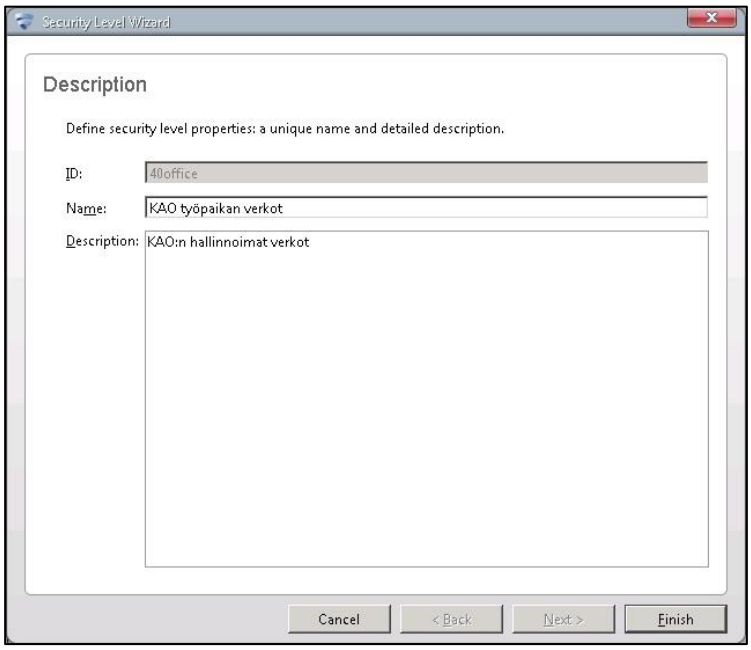
Henkilöstön kannettavien työasemien tietoturvaa pyritään parantamaan turvallisuustasojen avulla. Turvallisuustasoja voidaan muokata Edit-painikkeella.



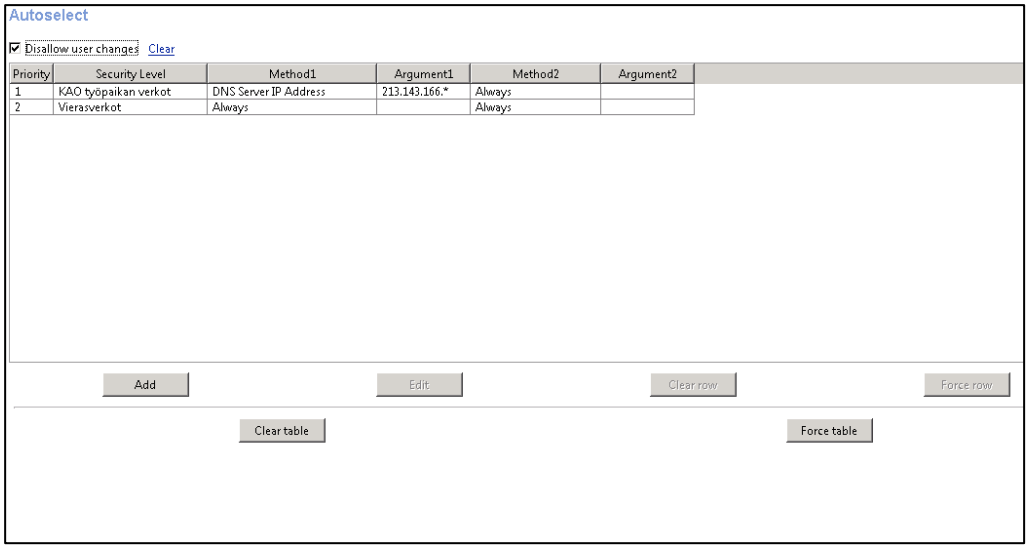
Home-turvallisuustaso muutettiin Vierasverkot nimiseksi.



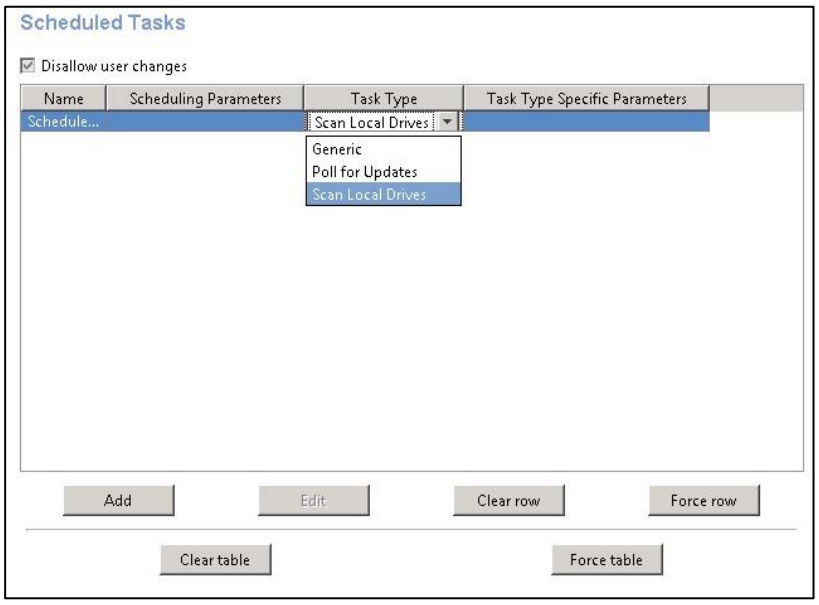
Office-taso nimettiin KAO työpaikanverkot.



Turvallisuustason automaattinen valinta tehdään määrittelemällä sääntö advanced modessa. Sääntö koostuu kahdesta tilasta Method 1/ Argument 1 sekä Method 2/Argument 2. Kun Host-kone arvioi molempien tilojen arvoksi tosi, säännössä määritelty turvallisuustaso otetaan käyttöön. Sääntöä arvioidaan aina kun huomataan muutoksia verkon tilassa, jolloin sääntö, jolla on korkein prioriteetti, otetaan käyttöön. Tämä on siltä varalta, että taulukkoon on lisätty useita sääntöjä, joilla on samat tilat. Jos toinen argumentti ei saa arvoa tosi, turvallisuustaso ei vaihdu. Sääntö taulukon loppuun tehdään sääntö, jossa molemmat methodit asetetaan always tilaan.



Työasemille voidaan määrittää ajastettuja tehtäviä, joiden avulla työasemille voidaan asettaa ajastettu virustarkistus, päivitysten jakaminen sekä muita yleisiä tehtäviä. Alla olevasta taulukosta nähdään parametrit, joita ajastetulle tehtävälle voidaan asettaa. Niiden avulla voidaan tarkasti ajoittaa milloin tehtävä suoritetaan.



Parametri	Merkitys	Esimerkki
/a	suorittaa tehtävän käynnistyessä	/a
/l	sisään kirjautuessa	/l
/o	suoritetaan vain kerran	/o
/t	suorittaa tehtävän haluttuna kellon aikana.	/t14:23
/ti	suorittaa tehtävän koneen ollessa käyttämättömänä määritellyn ajan	/ti30
/b	ilmaisee ensimmäisen päivän jolloin ajoitettu tehtävä on voimassa	/bYYYY-MM-DD
/e	ilmaisee viimeisen päivän jolloin tehtävä on voimassa	/eYYYY-MM-DD
/r	suorittaa tehtävän kerran, päivittäin, viikottain, kuukasittain	/ronce, /rdaily, /weekly, /monthly
/s	suorittaa tehtävän haluttuna päivänä	/s1/s20/s30