McAfee®

VirusScan® Plus 2007

AntiVirus, Firewall & AntiSpyware

Käyttöopas

Sisältö

LUKU 1

Johdanto

McAfee VirusScan Plus Suite suojaa tietokonettasi ja tiedostojasi viruksilta, vakoiluohjelmilta ja hakkereilta. Voit selata Web-sivustoja ja ladata tiedostoja turvallisesti tietäen, että McAfee on aina käynnissä, aina päivitetty ja aina suojaamassa. McAfeen luotettava suojaus torjuu uhkat ja hakkerit automaattisesti ja pitää tietokoneesi puhtaana ja suojassa. McAfee helpottaa myös suojaustilan tarkastelua, virusten ja vakoiluohjelmien varalta tarkistamista, ja tuotteiden ajantasaisuuden varmistamista uudistetun McAfee Security Centerin avulla. Sen lisäksi saat tilauksesi mukana uusimmat McAfee-ohjelmistot ja -päivitykset automaattisesti.

VirusScan Plus sisältää seuraavat ohjelmat:

- SecurityCenter
- VirusScan
- Personal Firewall
- Network Manager
- EasyNetwork (vain kolmen käyttäjän lisenssi)
- SiteAdvisor

LUKU 2

McAfee SecurityCenter

McAfee SecurityCenter on helppokäyttöinen ympäristö, jossa McAfeen käyttäjät voivat ottaa tietoturvatilauksensa käyttöön, hallita sitä ja määrittää sen asetukset.

SecurityCenter on myös tietopankki, jossa on tietoja virushälytyksistä, tuotteista, tuesta ja tilauksista, ja se mahdollistaa McAfeen Web-sivustossa olevien työkalujen käytön ja uutisten lukemisen yhdellä näppäimen painalluksella.

Tässä luvussa

Ominaisuudet

McAfee SecurityCenter tarjoaa seuraavat uudet toiminnot ja edut:

Uudelleensuunniteltu suojaustila

Voit helposti tarkastaa tietokoneesi suojaustilan, etsiä päivityksiä ja korjata mahdollisia tietoturva-aukkoja.

Jatkuvat päivitykset ja uudet tuoteversiot

Asenna päivittäiset päivitykset automaattisesti. Kun uusi McAfee-ohjelmistoversio on saatavilla, tilaajana saat sen automaattisesti ilman lisäkustannuksia, jotta suojauksesi on aina ajan tasalla.

Reaaliaikaiset hälytykset

Suojahälytykset ilmoittavat virusesiintymistä ja tietoturvauhista sekä tarjoavat toimintavaihtoehtoja uhkien poistamiseen ja neutralointiin sekä lisätietoja uhista.

Helppokäyttöinen suojaus

Useat uudistusvaihdot auttavat pitämään McAfee-suojauksesi ajan tasalla.

Suorituskykytyökalut

Poista käyttämättömät tiedostot, eheytä käytetyt tiedostot ja käytä järjestelmän palautusta, jotta voit pitää tietokoneen suorituskyvyn parhaana mahdollisena.

Oikeaa online-tukea

McAfeen tietoturva-ammattilaiset tarjoavat tukipalveluja puhelimen, sähköpostin ja Internet-keskusteluohjelmien välityksellä.

Suojatun selauksen suojaus

Jos McAfee SiteAdvisor -selainlaajennus on asennettu, se auttaa suojaamaan sinua vakoiluohjelmilta, roskapostilta, viruksilta ja verkkohuijauksilta arvioimalla Web-hakutuloksissa luetellut Web-sivustot tai sivut, joilla olet käynyt. Voit tarkastella yksityiskohtaisia turvallisuusarviomäärityksiä, jotka näyttävät sivuston sähköpostikäytäntöjä, ladattavia tiedostoja, verkkoyhteyksiä sekä ponnahdusikkunoiden ja kolmansien osapuolten seurantaevästeiden kaltaisia häiriötekijöitä koskevien testien tulokset.

LUKU 3

SecurityCenterin käyttäminen

Voit käynnistää SecurityCenterin napsauttamalla McAfee SecurityCenterin kuvaketta, joka sijaitsee tehtäväpalkin oikeassa reunassa olevalla Windowsin ilmaisinalueella tai Windowsin työpöydällä.

Kun avaat SecurityCenterin, Koti-ikkuna näyttää tietokoneen suojauksen tilan ja antaa mahdollisuuden päivitysten, tarkistusten (jos McAfee VirusScan on asennettu) ja muiden yleisten tehtävien nopeaan suorittamiseen:

Otsikko

Ohje

Tarkastele ohjelman ohjetiedostoa.

Vasen sarake

Päivitä

Suojaudu uusilta uhilta päivittämällä tuotteesi.

Tarkista

Jos McAfee VirusScan on asennettu, voit tarkistaa tietokoneen manuaalisesti.

Yleiset tehtävät

Suorita yleisiä tehtäviä: palaa Koti-ikkunaan, tarkastele äskettäisiä tapahtumia, hallitse tietokoneverkkoa (jos käytät verkon hallintaan kykenevää tietokonetta) ja ylläpidä tietokonetta. Jos McAfee Data Backup on asennettu, voit myös varmuuskopioida tietosi.

Asennetut komponentit

Katso, mitkä tietoturvapalvelut huolehtivat tietokoneesi turvallisuudesta.

Pääikkuna

Suojauksen tila

Olenko suojattu? -kohdassa voit tarkastella tietokoneen yleistä suojauksen tilaa. Sen alapuolella näet tilan eriteltynä suojausluokan ja -tyypin mukaan.

SecurityCenterin tiedot

Tarkista, koska tietokone on päivitetty viimeksi, koska se on tarkistettu viimeksi (jos McAfee VirusScan on asennettu) ja koska tilaus umpeutuu.

Tässä luvussa

SecurityCenterin kuvakkeiden toiminta

SecurityCenterin kuvakkeet ilmestyvät tehtäväpalkin oikeassa reunassa olevalle Windowsin ilmaisinalueelle. Niiden avulla voit tarkistaa, onko tietokoneesi täysin suojattu, tarkastella käynnissä olevan tarkistuksen tilaa (jos McAfee VirusScan on asennettu), hakea päivityksiä, tarkastella äskettäisiä tapahtumia, ylläpitää tietokonetta ja pyytää tukea McAfeen Web-sivustosta.

Avaa SecurityCenter ja käytä lisäominaisuuksia

Kun SecurityCenter on käynnissä, tehtäväpalkin oikeassa reunassa olevalle Windowsin ilmaisinalueelle ilmestyy SecurityCenter M -kuvake.

SecurityCenterin avaaminen tai lisäominaisuuksien käyttäminen:

- Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella ja valitse yksi seuraavista:
  - Avaa SecurityCenter
  - Päivitykset
  - Pikalinkit

    Alivalikossa on linkit Koti-, Tarkastele äskettäisiä tapahtumia-, Verkonhallinta-, Ylläpidä tietokonetta- ja Data Backup -valikkovaihtoehtoihin (jos asennettu).
  - Vahvista tilaus

    (Tämä kohde ilmestyy näyttöön sen jälkeen, kun ainakin yhden tuotteen tilaus on umpeutunut.)
  - Päivityskeskus
  - Asiakastuki

Tarkista suojauksen tila

Jos tietokone ei ole täysin suojattu, tehtäväpalkin oikeassa reunassa olevalle Windowsin ilmaisinalueelle ilmestyy suojauksen tilan kuvake. Suojauksen tilan mukaan kuvake voi olla punainen tai keltainen.

Suojauksen tilan tarkistaminen:

- Avaa SecurityCenter napsauttamalla suojauksen tilan kuvaketta ja korjaa mahdolliset ongelmat.

Tarkista päivitysten tila

Jos olet hakemassa päivityksiä, tehtäväpalkin oikeassa reunassa olevalle Windowsin ilmaisinalueelle ilmestyy päivityskuvake .

Päivitysten tilan tarkistaminen:

- Napsauttamalla päivityskuvaketta voit tarkastella päivitysten tilaa työkaluvihjeenä.

Suojauksen tilan toiminta

Tietokoneen yleinen suojauksen tila on ilmoitettu Security Centerin **Olenko suojattu?** -kohdassa.

Suojauksen tila ilmaisee, onko tietokone täysin suojattu uusia tietoturvauhkia vastaan, kuten myös sen, vaativatko ongelmat huomiota ja miten ne voi ratkaista. Jos ongelma vaikuttaa useampaan suojausluokkaan, ongelman ratkaiseminen voi palauttaa useamman luokan täysin suojattuun tilaan.

Suojauksen tilaan vaikuttavat muun muassa ulkoiset tietoturvauhat, tietokoneeseen asennetut tietoturvatuotteet, Internetiä käyttävät tuotteet sekä kyseisten tietoturva- ja Internet-tuotteiden asetukset.

Oletusarvoisesti nämä ei-kriittiset suojausongelmat ohitetaan automaattisesti ja niitä ei seurata yleisessä suojauksen tilassa, jos roskapostin torjuntaa ja sisällön estämistä ei ole asennettu. Jos suojausongelman perässä on **Ohita**-linkki, voit halutessasi ohittaa ongelman, jos olet varma, että et halua korjata sitä.

Olenko suojattu?

SecurityCenterin **Olenko suojattu?** -kohdassa voit tarkastella tietokoneen yleistä suojauksen tilaa:

- Näyttöön ilmestyy **Kyllä**, jos tietokoneesi on täysin suojattu (vihreä).
- Näyttöön ilmestyy **Ei**, jos tietokoneesi on osittain suojattu (keltainen) tai suojaamaton (punainen).

Voit ratkaista useimmat suojausongelmat automaattisesti valitsemalla suojauksen tilan vierestä **Korjaa**. Jos yksi tai useampi suojausongelma ei ratkea ja vaatii toimenpiteitä, napsauta ongelman perässä olevaa linkkiä ja suorita suositeltu toimenpide.

Suojausluokkien ja -tyyppien toiminta

SecurityCenterin **Olenko suojattu?** -kohdassa voit tarkastella suojauksen tilaa seuraavien suojausluokkien ja -tyyppien mukaan jaoteltuna:

- Tietokone ja tiedostot
- Internet ja verkko
- Sähköposti ja pikaviesti
- Käytönvalvonta-asetukset

SecurityCenterissä näkyvät suojaustyypit vaihtelevat asennettujen tuotteiden mukaan. Esimerkiksi Tietokoneen kunto -suojaustyyppi ilmestyy näyttöön silloin, kun McAfee Data Backup -ohjelmisto on asennettu.

Jos luokalla ei ole suojausongelmia, se on vihreässä tilassa. Jos valitset vihreän luokan, oikealle ilmestyy käyttöön otettujen suojaustyyppien luettelo, jota seuraa ohitettujen ongelmien luettelo. Jos ongelmia ei ole, niiden tilalla näkyy virusilmoitus. Voit myös muuttaa kyseisen luokan asetuksia valitsemalla **Määritä**.

Jos luokan kaikki suojaustyypit ovat vihreässä tilassa, myös luokan tila on vihreä. Samalla tavalla yleinen suojauksen tila on vihreä, jos kaikki suojausluokat ovat vihreässä tilassa.

Jos jokin suojausluokka on keltaisessa tai punaisessa tilassa, voit ratkaista suojausongelmat korjaamalla tai ohittamalla ne. Tällöin tila muuttuu vihreäksi.

Tietokone ja tiedostot -suojauksen toiminta

Tietokone ja tiedostot -suojausluokka muodostuu seuraavista suojaustyypeistä:

- **Virustorjunta** – Reaaliaikainen tarkistussuojaus suojaa tietokonetta viruksia, matoja, Troijan hevosia, epäilyttäviä komentosarjoja, sekahyökkäyksiä ja muita uhkia vastaan. Se tarkistaa ja yrittää puhdistaa tiedostot (muun muassa .exe-muotoiset pakatut tiedostot, käynnistyslohkon, muistin ja kriittiset tiedostot) automaattisesti, kun sinä tai tietokone yritätte käyttää niitä.
- **Vakoiluohjelmien torjunta** – Vakoiluohjelmien torjunta havaitsee, estää ja poistaa vakoiluohjelmat, mainosohjelmat ja muut mahdollisesti ilman lupaasi henkilökohtaisia tietoja keräävät ja lähettävät ohjelmat nopeasti.
- **SystemGuards** – SystemGuards havaitsee tietokoneeseen tehdyt muutokset ja varoittaa niistä. Voit tämän jälkeen tarkastella muutoksia ja päättää, haluatko sallia ne.
- **Windows-suojaus** – Windows-suojaus näyttää tietokoneen Windows-päivitysten tilan. Jos McAfee VirusScan on asennettu, puskurin ylivuotosuojaus on myös käytettävissä.

Yksi Tietokone ja tiedostot -suojaukseen vaikuttavista tekijöistä on ulkoiset virusuhat. Esimerkiksi suojaako käyttämäsi virustorjuntaohjelmisto sinua virusesiintymiltä? Muita tekijöitä ovat virustorjuntaohjelmiston asetukset ja se, onko tietokone päivitetty uusimmilla tunnistusallekirjoitustiedostoilla, jotka auttavat suojaamaan tietokonetta uusilta uhilta.

Avaa Tietokone ja tiedostot -asetusikkuna

Jos **Tietokone ja tiedostot** -luokassa ei ole ongelmia, voit avata asetusikkunan tietoikkunasta.

Tietokone ja tiedostot -asetusikkunan avaaminen:

1. Valitse Koti-ikkunasta **Tietokone ja tiedostot**.
2. Valitse oikeasta ikkunasta **Määritä**.

Internet ja verkko -suojauksen toiminta

Internet ja verkko -suojausluokka muodostuu seuraavista suojaustyypeistä:

- **Palomuurisuojaus** – Firewall suojaa tietokonetta tietomurroilta ja ei-toivotulta tietoliikenteeltä. Se auttaa hallitsemaan saapuvia ja lähteviä Internet-yhteyksiä.
- **Langaton suojaus** – Langaton suojaus suojaa kodin langatonta verkkoa tietomurroilta ja tietojen sieppaamiselta. Jos olet muodostanut yhteyden ulkoiseen langattomaan verkkoon, suojauksesi taso vaihtelee kuitenkin kyseisen verkon suojaustason mukaan.
- **Web Browsing Protection** – Web-selauksen suojaus piilottaa mainokset, ponnahdusikkunat ja piilojäljitteet tietokoneella Internetiä selattaessa.
- **Phishing-huijausten torjunta** – Phishing-huijausten torjunta auttaa estämään petolliset Web-sivustot, jotka tavoittelevat henkilökohtaisia tietoja sähköpostiviestien ja pikaviestiohjelmien hyperlinkkien avulla, sekä ponnahdusikkunoiden ja muiden keinojen avulla.
- **Henkilökohtaisten tietojen suojaus** – Henkilökohtaisten tietojen suojaus estää arkaluonteisten ja luottamuksellisten tietojen julkistamisen Internetissä.

Avaa Internet ja verkko -asetusikkuna

Jos **Internet ja verkko** -luokassa ei ole ongelmia, voit avata asetusikkunan tietoikkunasta.

Internet ja verkko -asetusikkunan avaaminen:

1. Valitse Koti-ikkunasta **Internet ja tiedostot**.
2. Valitse oikeasta ikkunasta **Määritä**.

Sähköposti ja pikaviesti -suojauksen toiminta

Sähköposti ja pikaviesti -suojausluokka muodostuu seuraavista suojaustyypeistä:

- **Sähköpostisuojaus** – Sähköpostisuojaus tarkistaa saapuvat ja lähtevät sähköpostiviestit ja liitteet automaattisesti ja yrittää poistaa niissä olevat virukset, vakoiluohjelmat ja mahdolliset uhat.
- **Roskapostin torjunta** – Roskapostin torjunta auttaa estämään ei-toivottujen sähköpostiviestien toimittamisen Saapuvat-kansioosi.
- **Pikaviestisuojaus** – Pikaviestisuojaus tarkistaa saapuvien pikaviestien liitteet automaattisesti ja yrittää poistaa niissä olevat virukset, vakoiluohjelmat ja mahdolliset uhat. Se estää myös pikaviestipalvelimia vaihtamasta haitallisia sisältöjä tai henkilökohtaisia tietoja Internetissä.
- **Suojatun selauksen suojaus** – Jos McAfee SiteAdvisor -selainlaajennus on asennettu, se auttaa suojaamaan sinua vakoiluohjelmilta, roskapostilta, viruksilta ja verkkohuijauksilta arvioimalla vierailemasi tai Web-hakutuloksissa luetellut Web-sivustot. Voit tarkastella yksityiskohtaisia turvallisuusarviomäärityksiä, jotka näyttävät sivuston sähköpostikäytäntöjä, ladattavia tiedostoja, verkkoyhteyksiä sekä ponnahdusikkunoiden ja kolmansien osapuolten seurantaevästeiden kaltaisia häiriötekijöitä koskevien testien tulokset.

Avaa Sähköposti ja pikaviesti -asetusikkuna

Jos **Sähköposti ja pikaviesti** -luokassa ei ole ongelmia, voit avata asetusikkunan tietoikkunasta.

Sähköposti ja pikaviesti -asetusikkunan avaaminen:

1. Valitse Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse oikeasta ikkunasta **Määritä**.

Käytönvalvonta-asetukset-suojauksen toiminta

Käytönvalvonta-asetukset-suojausluokka muodostuu seuraavasta suojaustyypistä:

- **Käytönvalvonta-asetukset** – Käytönvalvonta-asetukset estävät käyttäjiä katselemasta ei-toivottuja Internet-sisältöjä estämällä mahdollisesti vahingolliset Web-sivustot. Käyttäjien Internet-tapahtumia ja -käyttöä voidaan myös valvoa ja rajoittaa.

Avaa Käytönvalvonta-asetukset-asetusikkuna

Jos **Käytönvalvonta-asetukset**-luokassa ei ole ongelmia, voit avata asetusikkunan tietoikkunasta.

Käytönvalvonta-asetukset-asetusikkunan avaaminen:

1. Valitse Koti-ikkunasta **Käytönvalvonta-asetukset**.
2. Valitse oikeasta ikkunasta **Määritä**.

Suojausongelmien korjaaminen

Useimmat suojausongelmat voidaan ratkaista automaattisesti. Jos yksi tai useampi ongelma ei kuitenkaan poistu, ne on ratkaistava.

Korjaa suojausongelmat automaattisesti

Useimmat suojausongelmat voidaan ratkaista automaattisesti.

Suojausongelmien korjaaminen automaattisesti:

- Valitse suojauksen tilan vierestä **Korjaa**.

Korjaa suojausongelmat manuaalisesti

Jos yksi tai useampi suojausongelma ei ratkea automaattisesti, napsauta ongelman perässä olevaa linkkiä ja suorita suositeltu toimenpide.

Suojausongelmien korjaaminen manuualisesti:

- Valitse yksi seuraavista vaihtoehdoista:
  - Jos tietokoneelle ei ole suoritettu täydellistä tarkistusta viimeisen 30 päivän aikana, tarkista tietokone manuaalisesti valitsemalla suojauksen tilan pääikkunan vasemmalta puolelta **Tarkista**. (Tämä valikkovaihtoehto ilmestyy näyttöön, jos McAfee VirusScan on asennettu.)
  - Jos tunnistusallekirjoitustiedostot (DAT) ovat vanhentuneet, päivitä suojauksesi valitsemalla suojauksen tilan pääikkunan vasemmalta puolelta **Päivitä**.
  - Jos ohjelmaa ei ole asennettu, asenna se valitsemalla **Hanki täydellinen suojaus**.
  - Jos ohjelmasta puuttuu osia, asenna se uudelleen.
  - Jos täydellinen suojaus edellyttää ohjelman rekisteröintiä, rekisteröi se valitsemalla **Rekisteröi nyt**. (Tämä valikkokohde ilmestyy näyttöön, jos yksi tai useampi ohjelma on vanhentunut.)
  - Jos ohjelma on vanhentunut, tarkista tilisi tila valitsemalla **Vahvista tilaus nyt**. (Tämä valikkokohde ilmestyy näyttöön, jos yksi tai useampi ohjelma on vanhentunut.)

SecurityCenterin tietojen tarkasteleminen

Suojauksen tila -ikkunan alaosassa olevassa SecurityCenterin tiedot -kohdassa voit määrittää SecurityCenterin asetukset ja tarkastella McAfeen tuotteiden viimeistä päivitystä, viimeistä tarkistusta (jos McAfee VirusScan on asennettu) ja tilauksen päättymiseen liittyviä tietoja.

Avaa SecurityCenter-asetusikkuna

Käytön helpottamiseksi voit muuttaa asetuksiasi Koti-ikkunasta, kun avaat SecurityCenter-asetusikkunan.

SecurityCenter-asetusikkunan avaaminen:

- Valitse Koti-ikkunassa olevasta **SecurityCenterin tiedot** -kohdasta **Määritä**.

Tarkastele asennettujen tuotteiden tietoja

Voit tarkastella asennettujen tuotteiden luetteloa, jossa näkyvät tuoteversiot ja viimeisten päivitysten ajankohdat.

McAfeen tuotteiden tietojen tarkasteleminen

- Avaa tuotetietoikkuna valitsemalla Koti-ikkunassa olevasta **SecurityCenter-tiedot** -kohdasta **Näytä tiedot**.

Lisävalikon käyttäminen

Kun avaat SecurityCenterin ensimmäisen kerran, Perusvalikko avautuu vasemmalla olevaan sarakkeeseen. Jos olet kokenut käyttäjä, voit avata sen sijaan yksityiskohtaisemman komentovalikon valitsemalla **Lisävalikko**-vaihtoehdon. Käytön helpottamiseksi viimeksi käytetty valikko näytetään SecurityCenterissä, kun se avataan seuraavan kerran.

Lisävalikossa on seuraavat kohteet:

- Koti
- Raportit ja lokitiedostot (sisältää äskettäisten tapahtumien luettelon ja lokit viimeisen 30, 60 ja 90 päivän ajalta)
- Määritä
- Palauta
- Työkalut

LUKU 4

SecurityCenterin asetusten määrittäminen

SecurityCenter näyttää tietokoneen yleisen suojauksen tilan, mahdollistaa McAfee-käyttäjätilien luomisen, asentaa automaattisesti uusimmat tuotepäivitykset ja ilmoittaa sinulle julkisista virusesiintymistä, tietoturvauhista ja tuotepäivityksistä automaattisesti hälytyksellä ja merkkiäänellä.

SecurityCenter-asetukset-ikkunassa voit muuttaa seuraavia Security Centerin asetuksia:

- Suojauksen tila
- Käyttäjät
- Automaattiset päivitykset
- Hälytykset

Tässä luvussa

Suojauksen tilan asetusten määrittäminen

Tietokoneen yleinen suojauksen tila on ilmoitettu Security Centerin **Olenko suojattu?** -kohdassa.

Suojauksen tila ilmaisee, onko tietokone täysin suojattu uusia tietoturvauhkia vastaan, kuten myös sen, vaativatko ongelmat huomiota ja miten ne voi ratkaista.

Oletusarvoisesti nämä ei-kriittiset suojausongelmat ohitetaan automaattisesti ja niitä ei seurata yleisessä suojauksen tilassa, jos roskapostin torjuntaa ja sisällön estämistä ei ole asennettu. Jos suojausongelman perässä on **Ohita**-linkki, voit halutessasi ohittaa ongelman, jos olet varma, että et halua korjata sitä. Jos päätät myöhemmin korjata aikaisemmin ohitetun ongelman, voit lisätä sen suojauksen tilaan seurantaa varten.

Määritä ohitettujen ongelmien asetukset

Voit ottaa ongelmat huomioon tai jättää ne huomiotta seuratessasi tietokoneen yleistä suojauksen tilaa. Jos suojausongelman perässä on **Ohita**-linkki, voit halutessasi ohittaa ongelman, jos olet varma, että et halua korjata sitä. Jos päätät myöhemmin korjata aikaisemmin ohitetun ongelman, voit lisätä sen suojauksen tilaan seurantaa varten.

Ohitettujen ongelmien asetusten määrittäminen:

1. Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
2. Laajenna **Suojauksen tila** -ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
3. Toimi Ohitetut ongelmat -ikkunassa seuraavasti:
   - Jos haluat ottaa aikaisemmin ohitetut ongelmat suojauksen tilassa huomioon, poista niiden valintaruutujen valinnat.
   - Jos haluat jättää aikaisemmin ohitetut ongelmat suojauksen tilassa huomiotta, valitse niiden valintaruudut.
4. Valitse **OK**.

Käyttäjäasetusten määrittäminen

Jos käytät McAfeen ohjelmia, jotka vaativat tiettyjä käyttöoikeuksia, kyseiset käyttöoikeudet vastaavat oletusasetuksena tietokoneen Windows-käyttäjätilien käyttöoikeuksia. Voit yksinkertaistaa näiden ohjelmien käyttäjien hallintaa siirtymällä milloin tahansa käyttämään McAfee-käyttäjätilejä.

Jos siirryt käyttämään McAfee-käyttäjätilejä, Käytönvalvonta-asetukset-ohjelmassa olevat käyttäjänimet ja käyttöoikeudet tuodaan automaattisesti. Kun siirryt käyttämään McAfee-käyttäjätilejä ensimmäisen kerran, sinun on kuitenkin luotava järjestelmänvalvojan tili. Sen jälkeen voit luoda uusia McAfee-käyttäjätilejä ja määrittää niiden asetukset.

Siirry McAfee-käyttäjätileihin

Oletusarvoisesti käytät Windows-käyttäjätilejä. Voit kuitenkin siirtyä käyttämään McAfee-käyttäjätilejä, jolloin uusia Windows-käyttäjätilejä ei enää tarvitse luoda.

Siirtyminen McAfee-käyttäjätileihin:

1. Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
2. Laajenna **Käyttäjät**-ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
3. Jos haluat käyttää McAfee-käyttäjätilejä, valitse **Vaihda**.

Kun siirryt käyttämään McAfee-käyttäjätilejä ensimmäisen kerran, sinun on luotava järjestelmänvalvojan tili (sivu 23).

Luo järjestelmänvalvojan tili

Kun siirryt käyttämään McAfee-käyttäjätilejä ensimmäisen kerran, sinua kehotetaan luomaan järjestelmänvalvojan tili.

Järjestelmänvalvojan tilin luominen:

1. Kirjoita salasana **Salasana**-tekstiruutuun ja kirjoita se uudelleen **Vahvista salasana** -tekstiruutuun.
2. Valitse salasanan palautuskysymys luettelosta ja kirjoita salaisen kysymyksen vastaus **Vastaus**-tekstiruutuun.
3. Valitse **Käytä**.

   Kun olet valmis, käyttäjätilin tyyppi päivitetään ikkunassa lisäämällä siihen mahdolliset Käytönvalvonta-asetukset-ohjelman käyttäjänimet ja käyttöoikeudet. Jos olet määrittämässä käyttäjätilien asetuksia ensimmäisen kerran, näyttöön ilmestyy Hallitse käyttäjiä -ikkuna.

Määritä käyttäjäasetukset

Jos siirryt käyttämään McAfee-käyttäjätilejä, Käytönvalvonta-asetukset -ohjelmassa olevat käyttäjänimet ja käyttöoikeudet tuodaan automaattisesti. Kun siirryt käyttämään McAfee-käyttäjätilejä ensimmäisen kerran, sinun on kuitenkin luotava järjestelmänvalvojan tili. Sen jälkeen voit luoda uusia McAfee-käyttäjätilejä ja määrittää niiden asetukset.

Käyttäjäasetusten määrittäminen

1. Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
2. Laajenna **Käyttäjät**-ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
3. Valitse **Käyttäjätilit**-kohdasta **Lisää**.
4. Kirjoita käyttäjänimi **Käyttäjänimi**-tekstiruutuun.
5. Kirjoita salasana **Salasana**-tekstiruutuun ja kirjoita se uudelleen **Vahvista salasana** -tekstiruutuun.
6. Valitse **Aloituskäyttäjä**-valintaruutu, jos haluat uuden käyttäjän kirjautuvan automaattisesti sisään, kun SecurityCenter käynnistyy.
7. Valitse **Käyttäjätilin tyyppi** -kohdasta kyseiselle käyttäjälle tilin tyyppi ja valitse **Luo**.

   Huomaa: Kun olet luonut käyttäjätilin, sinun on määritettävä sille Käytönvalvonta-asetukset-kohdasta rajoitetun käyttäjän asetukset.

8. Jos haluat muokata käyttäjän salasanaa, automaattista sisäänkirjausta tai tilin tyyppiä, valitse luettelosta käyttäjän nimi ja sitten **Muokkaa**.
9. Kun olet valmis, valitse **Käytä**.

Palauta järjestelmänvalvojan salasana

Jos unohdat järjestelmänvalvojan salasanan, voit palauttaa sen.

Järjestelmänvalvojan salasanan palauttaminen:

1. Napsauta SecurityCenter M -kuvaketta hiiren kakkospainikkella ja valitse **Vaihda käyttäjää**.
2. Valitse **Käyttäjänimi**-luettelosta **Järjestelmänvalvoja** ja sitten **Unohditko salasanasi?**
3. Anna vastaus salaiseen kysymykseen, jonka valitsit järjestelmänvalvojan salasanan luomisen yhteydessä.
4. Valitse **Lähetä**.

   Unohdettu järjestelmänvalvojan salasanasi ilmestyy näyttöön.

Muuta järjestelmänvalvojan salasanaa

Jos sinun on vaikeata muistaa järjestelmänvalvojan salasanaa tai epäilet sen joutuneen vääriin käsiin, voit muuttaa sen.

Järjestelmänvalvojan salasanan muuttaminen:

1. Napsauta SecurityCenter M -kuvaketta hiiren kakkospainikkella ja valitse **Vaihda käyttäjää**.
2. Valitse **Käyttäjänimi**-luettelosta **Järjestelmänvalvoja** ja sitten **Vaihda salasana**.
3. Kirjoita nykyinen salasanasi **Vanha salasana** -tekstiruutuun.
4. Kirjoita uusi salasanasi **Salasana**-tekstiruutuun ja kirjoita se uudelleen **Vahvista salasana** -tekstiruutuun.
5. Valitse **OK**.

Päivitysasetusten määrittäminen

Kun olet muodostanut yhteyden Internetiin, SecurityCenter hakee päivityksiä automaattisesti kaikille McAfee-palveluille neljän tunnin välein ja asentaa uudet tuotepäivitykset automaattisesti. Voit kuitenkin hakea päivityksiä myös manuaalisesti napsauttamalla SecurityCenter-kuvaketta, joka sijaitsee tehtäväpalkin oikeassa reunassa olevalla Windowsin ilmaisinalueella.

Hae päivityksiä automaattisesti

Kun olet muodostanut yhteyden Internetiin, SecurityCenter hakee päivityksiä automaattisesti neljän tunnin välein. Voit kuitenkin määrittää SecurityCenterin antamaan ilmoituksen ennen päivitysten lataamista tai asentamista.

Päivitysten automaattinen hakeminen:

1. Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
2. Laajenna **Automaattiset päivitykset ovat käytössä** -ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
3. Valitse Päivitysvalinnat-ikkunasta yksi seuraavista:
   - Asenna päivitykset automaattisesti ja ilmoita, kun tuote päivitetään (suositus) (sivu 27)
   - Lataa päivitykset automaattisesti ja ilmoita, kun ne ovat valmiina asennettaviksi (sivu 28)
   - Ilmoita ennen päivitysten lataamista (sivu 28)
4. Valitse **OK**.

Huomaa: Parhaan mahdollisen suojan takaamiseksi McAfee suosittelee, että annat SecurityCenterin hakea ja asentaa päivitykset automaattisesti. Jos haluat kuitenkin päivittää tietoturvapalvelut vain manuaalisesti, voit poistaa automaattiset päivitykset käytöstä (sivu 29).

Lataa ja päivitä päivitykset automaattisesti

Jos valitset SecurityCenterin Päivitysvalinnat-kohdasta **Asenna päivitykset automaattisesti ja ilmoita, kun palvelut päivitetään (suositus)**, SecurityCenter lataa ja asentaa päivitykset automaattisesti.

Lataa päivitykset automaattisesti

Jos valitset SecurityCenterin Päivitysvalinnat-kohdasta **Lataa päivitykset automaattisesti ja ilmoita, kun ne ovat valmiina asennettaviksi**, SecurityCenter lataa päivitykset automaattisesti ja ilmoittaa sinulle, kun ne ovat valmiina asennettaviksi. Voit tällöin halutessasi asentaa päivityksen tai siirtää päivitystä (sivu 29).

Automaattisesti ladatun päivityksen asentaminen:

1. Valitse hälytyksen saatuasi **Päivitä tuotteet nyt** ja sitten **OK**.

   Kehotettaessa sinun on kirjauduttava Web-sivustoon ja vahvistettava tilauksesi ennen latauksen aloittamista.

2. Kun tilauksesi on vahvistettu, lataa ja asenna päivitys valitsemalla Päivitykset-ikkunasta **Päivitä**. Jos tilauksesi on umpeutunut, valitse hälytyksen saatuasi **Uudista tilaukseni** ja toimi kehotteiden mukaan.

Huomaa: Joissakin tapauksissa sinua kehotetaan viimeistelemään päivitys käynnistämällä tietokone uudelleen. Tallenna työt ja sulje kaikki ohjelmat ennen uudelleenkäynnistystä.

Ilmoita ennen päivitysten lataamista

Jos valitset Päivitysvalinnat-ikkunasta **Ilmoita ennen päivitysten lataamista**, SecurityCenter ilmoittaa sinulle ennen päivitysten lataamista. Voit tällöin halutessasi ladata ja asentaa tietoturvapalveluiden päivityksen hyökkäysuhan välttämiseksi.

Päivityksen lataaminen ja asentaminen:

1. Valitse hälytyksen saatuasi **Päivitä tuotteet nyt** ja sitten **OK**.
2. Kirjaudu kehotettaessa Web-sivustoon.

   Päivitys latautuu automaattisesti.

3. Valitse hälytyksen saatuasi **OK**, kun päivitys on asennettu.

Huomaa: Joissakin tapauksissa sinua kehotetaan viimeistelemään päivitys käynnistämällä tietokone uudelleen. Tallenna työt ja sulje kaikki ohjelmat ennen uudelleenkäynnistystä.

Poista automaattiset päivitykset käytöstä

Parhaan mahdollisen suojan takaamiseksi McAfee suosittelee, että annat SecurityCenterin hakea ja asentaa päivitykset automaattisesti. Jos haluat kuitenkin päivittää tietoturvapalvelut vain manuaalisesti, voit poistaa automaattiset päivitykset käytöstä.

Huomaa: Muista hakea päivitykset manuaalisesti (sivu 30) ainakin kerran viikossa. Jos et hae päivityksiä, uusimmat tietoturvapäivitykset eivät suojaa tietokonettasi.

Automaattisten päivitysten poistaminen käytöstä:

1. Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
2. Laajenna **Automaattiset päivitykset ovat käytössä** -ikkuna napsauttamalla sen vieressä olevaa nuolta.
3. Valitse **Ei käytössä**.
4. Vahvista muutos valitsemalla **Kyllä**.

   Tila päivitetään otsikkoon.

Jos et hae päivityksiä manuaalisesti seitsemään päivään, saat tästä muistuttavan hälytyksen.

Siirrä päivitykset

Jos olet liian kiireinen etkä ehdi päivittää tietoturvapalveluita juuri silloin, kun saat hälytyksen, voit pyytää myöhempää muistutusta tai ohittaa hälytyksen.

Päivityksen siirtäminen:

- Toimi seuraavasti:
  - Valitse hälytyksen saatuasi **Muistuta myöhemmin** ja sitten **OK**.
  - Valitse **Sulje tämä hälytys** ja sulje hälytys ryhtymättä toimenpiteisiin valitsemalla **OK**.

Hae päivityksiä manuaalisesti

Kun olet muodostanut yhteyden Internetiin, SecurityCenter hakee päivityksiä automaattisesti neljän tunnin välein ja asentaa uudet tuotepäivitykset. Voit kuitenkin hakea päivityksiä myös manuaalisesti napsauttamalla SecurityCenter-kuvaketta, joka sijaitsee tehtäväpalkin oikeassa reunassa olevalla Windowsin ilmaisinalueella.

Huomaa: Parhaan mahdollisen suojan takaamiseksi McAfee suosittelee, että annat SecurityCenterin hakea ja asentaa päivitykset automaattisesti. Jos haluat kuitenkin päivittää tietoturvapalvelut vain manuaalisesti, voit poistaa automaattiset päivitykset käytöstä (sivu 29).

Päivitysten manuaalinen hakeminen:

1. Varmista, että tietokoneesi on muodostanut yhteyden Internetiin.
2. Napsauta SecurityCenter M -kuvaketta hiiren kakkospainikkeella tehtäväpalkin oikeassa reunassa olevalla Windowsin ilmaisinalueella ja napsauta sitten **Päivitykset**-kohtaa.

   Sillä välin kun SecurityCenter tarkistaa päivityksiä, voit suorittaa sillä muita tehtäviä.

   Käytön helpottamiseksi tuotteen kuvake ilmestyy tehtäväpalkin oikeassa reunassa olevalle Windowsin ilmaisinalueelle. Kun SecurityCenter on valmis, kuvake katoaa automaattisesti.
3. Kirjaudu kehotettaessa Web-sivustoon ja vahvista tilauksesi.

Huomaa: Joissakin tapauksissa sinua kehotetaan viimeistelemään päivitys käynnistämällä tietokone uudelleen. Tallenna työt ja sulje kaikki ohjelmat ennen uudelleenkäynnistystä.

Hälytysasetusten määrittäminen

SecurityCenter ilmoittaa julkisista virusesiintymistä, tietoturvauhkista ja tuotepäivityksistä automaattisesti hälytyksellä ja merkkiäänellä. Voit kuitenkin määrittää SecurityCenterin näyttämään vain välitöntä huomiota vaativat hälytykset.

Määritä hälytysasetukset

SecurityCenter ilmoittaa julkisista virusesiintymistä, tietoturvauhkista ja tuotepäivityksistä automaattisesti hälytyksellä ja merkkiäänellä. Voit kuitenkin määrittää SecurityCenterin näyttämään vain välitöntä huomiota vaativat hälytykset.

Hälytysasetusten määrittäminen:

1. Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
2. Laajenna **Hälytykset**-ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
3. Valitse Hälytysasetukset-ikkunasta yksi seuraavista:
   - **Hälytä julkisista virusesiintymistä tai tietoturvauhista**
   - **Näytä tiedottavat hälytykset, kun tietokoneen havaitaan olevan pelitilassa**
   - **Soita ääni hälytyksen esiintyessä**
   - **Näytä McAfee-aloitusnäyttö Windowsin käynnistyessä**
4. Valitse **OK**.

Huomaa: Jos haluat poistaa tulevat tiedottavat hälytykset käytöstä itse hälytyksestä, valitse **Älä näytä tätä hälytystä uudelleen** -valintaruutu. Voit ottaa ne myöhemmin uudelleen käyttöön Tiedottavat hälytykset -ikkunassa.

Määritä tiedottavien hälytysten asetukset

Tiedottavat hälytykset ilmoittavat tapahtumista, jotka eivät vaadi välitöntä huomiota. Jos poistat tulevat tiedottavat hälytykset käytöstä itse hälytyksestä, voit ottaa ne Tiedottavat hälytykset -ikkunassa uudelleen käyttöön.

Tiedottavien hälytysten asetusten määrittäminen:

1. Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
2. Laajenna **Hälytykset**-ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
3. Valitse **SecurityCenter-asetukset**-ikkunasta **Tiedottavat hälytykset**.
4. Poista **Piilota tiedottavat hälytykset** -kohdan valinta ja poista sitten luettelosta niiden hälytysten valintaruutujen valinnat, jotka haluat näyttää.
5. Valitse **OK**.

LUKU 5

Yleisten tehtävien suorittaminen

Voit suorittaa yleisiä tehtäviä: palata Koti-ikkunaan, tarkastella äskettäisiä tapahtumia, hallita tietokoneverkkoa (jos käytät verkon hallintaan kykenevää tietokonetta) ja ylläpitää tietokonetta. Jos McAfee Data Backup on asennettu, voit myös varmuuskopioida tietosi.

Tässä luvussa

Suorita yleisiä tehtäviä

Voit suorittaa yleisiä tehtäviä: palata Koti-ikkunaan, tarkastella äskettäisiä tapahtumia, ylläpitää tietokonetta, hallita tietokoneverkkoa (jos käytät verkon hallintaan kykenevää tietokonetta) ja varmuuskopioida tietosi (jos McAfee Data Backup on asennettu).

Yleisten tehtävien suorittaminen:

- Toimi Perusvalikon **Yleiset tehtävät** -kohdassa seuraavasti:
  - Jos haluat palata Koti-ikkunaan, valitse **Koti**.
  - Jos haluat tarkastella tietoturvaohjelmiston äskettäin havaitsemia tapahtumia, valitse **Äskettäiset tapahtumat**.
  - Jos haluat poistaa käyttämättömiä tiedostoja, eheyttää tietoja ja palauttaa tietokoneen aikaisemmat asetukset, valitse **Ylläpidä tietokonetta**.
  - Jos haluat hallita tietokoneverkkoa, valitse **Verkonhallinta**, jos käytät verkon hallintaan kykenevää tietokonetta.

    Network Manager tarkkailee verkkosi tietokoneita mahdollisten tietoturva-aukkojen varalta, ja sen avulla voit tunnistaa verkon tietoturvaongelmat helposti.
  - Jos haluat luoda tiedostoistaisi varmuuskopioita, valitse **Data Backup**, jos McAfee Data Backup on asennettu.

Automaattinen varmuuskopiointitoiminto tallentaa salatut kopiot tärkeimmistä tiedostoistasi CD- ja DVD-levyille, USB-asemille sekä ulkoisille kiintolevyasemille ja verkkoasemille.

Vihje: Käytön helpottamiseksi voit suorittaa yleisiä tehtäviä myös kahdesta muusta paikasta (Lisävalikon **Koti**-kohdasta ja tehtäväpalkin oikeassa reunassa olevan SecurityCenter M -kuvakkeen **Pikalinkit**-valikosta). Voit myös tarkastella äskettäisiä tapahtumia ja yksityiskohtaisia lokeja tyypeittäin Lisävalikon **Raportit ja lokit** -kohdassa.

Tarkastele äskettäisiä tapahtumia

Äskettäiset tapahtumat kirjataan, kun tietokoneessa tapahtuu muutoksia. Esimerkkejä tästä ovat suojaustyypin ottaminen käyttöön tai poistaminen käytöstä, uhan poistaminen tai Internet-yhteysyrityksen estäminen. Voit tarkastella 20:tä viimeisintä tapahtumaa ja niiden tietoja.

Lisätietoja tapahtumista on kunkin tuotteen ohjetiedostossa.

Äskettäisten tapahtumien tarkasteleminen:

1. Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit** ja sitten **Tarkastele äskettäisiä tapahtumia**.

   Äskettäiset tapahtumat ilmestyvät luetteloon yhdessä päiväyksen ja lyhyen kuvauksen kanssa.

2. Valitse **Äskettäiset tapahtumat** -kohdasta tapahtuma, jota haluat tarkastella tarkemmin Lisätiedot-ikkunassa.

   Mahdolliset toimenpiteet ilmestyvät **Haluan**-kohtaan.

3. Jos haluat tarkastella tapahtumien yksityiskohtaisempaa luetteloa, valitse **Tarkastele lokia**.

Ylläpidä tietokonetta automaattisesti

Voit vapauttaa arvokasta kiintolevytilaa ja optimoida tietokoneen suorituskyvyn ajoittamalla tietokoneen suorittamaan QuickClean- ja levyn eheytystehtävät säännöllisin väliajoin. Näiden tehtävien avulla voit poistaa, tuhota ja eheyttää tiedostoja ja kansioita.

Tietokoneen automaattinen ylläpito:

1. Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit** ja sitten **Ylläpidä tietokonetta**.
2. Valitse **Tehtävien ajoitus** -kohdasta **Käynnistä**.
3. Valitse toimintojen luettelosta **QuickClean** tai **Levyn eheytys**.
4. Toimi seuraavasti:
   - Jos haluat muuttaa olemassa olevaa tehtävää, valitse se ja sitten **Muokkaa**. Toimi näytön ohjeiden mukaan.
   - Jos haluat luoda uuden tehtävän, kirjoita sen nimi **Tehtävän nimi** -tekstiruutuun ja valitse **Luo**. Toimi näytön ohjeiden mukaan.
   - Jos haluat poistaa tehtävän, valitse se ja sitten **Poista**.
5. **Tehtävän yhteenveto** -kohdassa voit tarkastella, koska tehtävä on suoritettu viimeksi, koska se suoritetaan seuraavan kerran ja mikä sen tila on.

Ylläpidä tietokonetta manuaalisesti

Manuaalisia ylläpitotehtäviä suorittamalla voit poistaa käyttämättömiä tiedostoja, eheyttää tietoja tai palauttaa tietokoneen aikaisemmat asetukset.

Tietokoneen manuaalinen ylläpito:

- Toimi seuraavasti:
  - Jos haluat käyttää QuickClean-toimintoa, napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit**, sitten **Ylläpidä tietokonetta** ja lopuksi **Käynnistä**.
  - Jos haluat käyttää levyn eheytystoimintoa, napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit**, sitten **Ylläpidä tietokonetta** ja lopuksi **Analysoi**.
  - Jos haluat käyttää järjestelmän palautustoimintoa, valitse Lisävalikosta **Työkalut**, sitten **Järjestelmän palautus** ja lopuksi **Käynnistä**.

Poista käyttämättömiä tiedostoja ja kansioita

QuickClean-toiminnolla voit vapauttaa arvokasta kiintolevytilaa ja optimoida tietokoneen suorituskyvyn.

Käyttämättömien tiedostojen ja kansioiden poistaminen:

1. Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit** ja sitten **Ylläpidä tietokonetta**.
2. Valitse **QuickClean**-kohdasta **Käynnistä**.
3. Toimi näytön ohjeiden mukaan.

Eheytä tiedostoja ja kansioita

Tiedostot pirstoutuvat, kun tiedostoja ja kansioita poistetaan ja uusia tiedostoja lisätään. Pirstoutuminen hidastaa levyn käyttöä ja heikentää tietokoneen yleistä suorituskykyä, vaikka yleensä ei kovinkaan merkittävästi.

Levyn eheytystä käyttämällä voit kirjoittaa tiedoston uudelleen kiintolevyn peräkkäisille sektoreille ja siten nopeuttaa käyttöä ja hakua.

Tiedostojen ja kansioiden eheyttäminen:

1. Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit** ja sitten **Ylläpidä tietokonetta**.
2. Valitse **Levyn eheytys** -kohdasta **Analysoi**.
3. Toimi näytön ohjeiden mukaan.

Palauta tietokoneen aikaisemmat asetukset

Palautuspisteet ovat tilannevedoksia tietokoneesta, jotka Windows tallentaa säännöllisin väliajoin ja aina merkittävien tapahtumien yhteydessä (esimerkiksi kun ohjelma tai ohjain asennetaan). Voit kuitenkin luoda myös omia palautuspisteitä ja nimetä ne milloin tahansa.

Palautuspisteiden avulla voit kumota tietokoneelle vahinkoa aiheuttaneet muutokset ja palauttaa aikaisemmat asetukset.

Tietokoneen aikaisempien asetusten palauttaminen:

1. Valitse Lisävalikosta **Työkalut** ja sitten **Järjestelmän palautus**.
2. Valitse **Järjestelmän palautus** -kohdasta **Käynnistä**.
3. Toimi näytön ohjeiden mukaan.

Hallitse verkkoa

Jos tietokoneesi kykenee verkon hallintaan, Network Managerin avulla voit tarkkailla verkkosi tietokoneita mahdollisten tietoturva-aukkojen varalta, ja sen avulla voit tunnistaa verkon tietoturvaongelmat helposti.

Jos tietokoneen suojauksen tilaa ei valvota tässä verkossa, tietokone ei kuulu verkkoon tai se on verkon laite, joka ei kuulu hallinnan piiriin. Lisätietoja on Network Managerin ohjetiedostossa.

Verkon hallinta:

1. Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit** ja sitten **Verkonhallinta**.
2. Napsauta verkkokartassa tätä tietokonetta esittävää kuvaketta.
3. Valitse **Haluan**-kohdasta **Valvo tätä tietokonetta**.

Hanki lisätietoja viruksista

Virustietokanta ja viruskartta tarjoavat useita mahdollisuuksia:

- Lisätietoja viimeisimmistä viruksista, sähköpostivirushuijauksista ja muista tietoturvauhkista.
- Hanki ilmaisia virusten poistotyökaluja, joiden avulla voit korjata tietokoneesi.
- Saat reaaliaikaisia karttanäkymiä siitä, miten viimeisimmät virukset leviävät tietokoneissa maailman ympäri.

Lisätietojen hankkiminen viruksista:

1. Valitse Lisävalikosta **Työkalut** ja sitten **Virustietoja**.
2. Toimi seuraavasti:
   - Tutki viruksia maksuttoman McAfee-virustietokannan avulla.
   - Tutki viruksia McAfeen Web-sivustossa olevan maailman viruskartan avulla.

LUKU 6

McAfee QuickClean

Kun surffaat Internetissä, tietokoneeseen kertyy nopeasti ylimääräistä roskamateriaalia. Turvaa tietosuojasi ja poista Internetin sekä sähköpostin kautta tuleva tarpeeton materiaali QuickClean-pikapuhdistusohjelman avulla. QuickClean tunnistaa ja poistaa tiedostoja, joita kerääntyy surffatessa, esimerkiksi evästeitä, sähköposteja, latauksia ja henkilötietoja sisältäviä historiatietoja. Ohjelma parantaa tietosuojaasi tarjoamalla turvallisen tavan poistaa näitä tietoja.

QuickClean poistaa myös ei-toivottuja ohjelmia. Määritä poistettavat tiedostot, niin voit poistaa turhan materiaalin ja säilyttää tarpeelliset tiedot.

Tässä luvussa

QuickClean-ohjelman toiminnot

Tässä osassa kuvaillaan QuickClean-ohjelman toimintoja.

Ominaisuudet

QuickClean-ohjelma on tehokas ja helppokäyttöinen työkalu, joka poistaa turvallisesti digitaalisen roskamateriaalin. Voit vapauttaa arvokasta levytilaa ja saat käyttöön tietokoneen parhaan mahdollisen suorituskyvyn.

LUKU 7

Tietokoneen puhdistaminen

QuickClean-ohjelman avulla voit turvallisesti poistaa tiedostoja ja kansioita.

Kun selaat Internetiä, selain kopioi jokaisen Internet-sivun ja sen kuvat kiintolevyllä olevaan välimuistiin. Tämän jälkeen selain voi ladata sivun nopeasti, jos palaat siihen. Tiedostojen tallentaminen välimuistiin on käytönnöllistä, jos käyt usein samoilla Internet-sivuilla, eikä niiden sisältö muutu usein. Useimmiten välimuistiin tallennetut tiedostot eivät kuitenkaan ole hyödyllisiä, ja ne voi poistaa.

Voit poistaa useita eri kohteita seuraavilla puhdistusohjelmilla.

- Roskakorin tyhjennysohjelma: Tyhjentää Windows-roskakorin.
- Väliaikaisten tiedostojen poisto-ohjelma: Poistaa väliaikaisten tiedostojen kansioihin tallennetut tiedostot.
- Pikakuvakkeiden puhdistusohjelma: Poistaa rikkinäiset pikakuvakkeet ja pikakuvakkeet, joihin ei liity mitään ohjelmaa.
- Hävinneiden tiedostopirstaleiden puhdistusohjelma: Poistaa kadonneet tiedostopirstaleet tietokoneesta.
- Rekisterin puhdistusohjelma: Poistaa Windows-rekisteritiedot ohjelmista, jotka on poistettu tietokoneesta.
- Välimuistin tyhjennysohjelma: Poistaa välimuistiin tallennetut tiedostot, joita kertyy Internetiä selatessa. Tämäntyyppiset tiedostot tallentuvat tavallisesti väliaikaisina Internet-tiedostoina.
- Evästeiden poisto-ohjelma: Poistaa evästeet. Tämäntyyppiset tiedostot tallentuvat tavallisesti väliaikaisina Internet-tiedostoina.
  Evästeet ovat pieniä tiedostoja, joita Web-selain tallentaa tietokoneeseen Web-palvelimen pyynnöstä. Aina kun avaat Web-sivun Web-palvelimelta, selaimesi lähettää evästeen takaisin palvelimeen. Nämä evästeet voivat toimia tunnisteina, joiden avulla Web-palvelin voi jäljittää avaamasi sivut sekä sen, kuinka usein käyt niillä.
- Selainhistorian tyhjennysohjelma: Poistaa selaimen historiatiedot.
- Outlook Express- ja Outlook-ohjelmien poistettujen ja lähetettyjen sähköpostien poisto-ohjelma: Poistaa sähköpostit lähetettyjen ja poistettujen sähköpostien kansioista Outlook-ohjelmissa.

- Viimeksi käytettyjen kohteiden poisto-ohjelma: Poistaa tietokoneeseen tallentuneet viimeksi käytetyt kohteet, kuten Microsoft Office -asiakirjat.
- ActiveX- ja Plug-in-laajennusten poisto-ohjelma: Poistaa ActiveX- ja Plug-in-laajennukset.
  ActiveX on teknologia, jota käytetään ohjelman komponenttien suorittamiseen. ActiveX-komponentti voi lisätä painikkeen ohjelman käyttöliittymään. Useimmat komponentit ovat harmittomia, mutta jotkut henkilöt voivat hyödyntää ActiveX-tekniikkaa tietojen kaappaamiseen tietokoneesta.
  Plug-in-laajennukset ovat pieniä ohjelmia, jotka kytkeytyvät suurempiin sovelluksiin ja lisäävät niihin toimintoja. Plug-in-laajennukset antavat Web-selaimen käyttää ja suorittaa HTML-asiakirjoihin upotettuja tiedostoja, jotka ovat selaimen tunnistamattomassa muodossa (esimerkiksi animaatio-, video- ja äänitiedostot).
- Järjestelmän palautuspisteiden poisto-ohjelma: Poistaa vanhat järjestelmän palautuspisteet tietokoneesta.

Tässä luvussa

QuickClean-ohjelman käyttäminen

Tässä osassa kerrotaan, kuinka QuickClean-pikapuhdistusohjelmaa käytetään.

Tietokoneen puhdistaminen

Voit poistaa käyttämättömät tiedostot ja kansiot, vapauttaa levytilaa ja tehostaa tietokoneen toimintaa.

Tietokoneen puhdistaminen:

1. Valitse Lisävalikosta **Työkalut**.
2. Valitse **Ylläpidä tietokonetta** ja valitse sitten **McAfee QuickClean** - **Käynnistä**.
3. Tee toinen seuraavista:
   - Hyväksy luettelon oletuspuhdistusohjelmat valitsemalla **Seuraava**.
   - Valitse tai poista haluamasi puhdistusohjelmat ja valitse sitten **Seuraava.** Valitsemalla Viimeksi käytettyjen kohteiden poisto-ohjelma -kohdasta **Asetukset** voit poistaa käytöstä haluamasi puhdistusohjelmat.
   - Palauta oletuspuhdistusohjelmat valitsemalla **Palauta oletusasetukset** ja valitse sitten **Seuraava**.
4. Kun analyysi on suoritettu, vahvista tiedostojen poistaminen valitsemalla **Seuraava**. Voit laajentaa luetteloa, jotta näet puhdistettavat tiedostot ja niiden sijainnin.
5. Valitse **Seuraava**.
6. Tee jokin seuraavista:
   - Hyväksy oletusasetus **Ei, haluan poistaa tiedostot perinteisellä Windowsin poistomenetelmällä** valitsemalla **Seuraava**.
   - Valitse **Kyllä, haluan poistaa tiedostot turvallisesti käyttämällä Shredder-ohjelmaa** ja määritä tyhjennyskerrat. Shredder-ohjelmalla poistettuja tiedostoja ei voi palauttaa.
7. Valitse **Valmis**.
8. Tarkasta **Pikatyhjennyksen yhteenveto** -näytöstä poistettujen rekisteritiedostojen määrä ja puhdistuksen vapauttama levytila.

LUKU 8

McAfee Shredder

Poistetut tiedostot voi palauttaa tietokoneeseen vielä roskakorin tyhjentämisen jälkeenkin. Kun poistat tiedoston, Windows merkitsee tilan levyasemaan vapaaksi levytilaksi, mutta tiedosto on yhä asemassa. Tietokoneen jäljitystyökalujen avulla voit palauttaa verotiedot, työhakemuksen ansioluettelot ja muut poistamasi asiakirjat. Shredder-ohjelma parantaa tietosuojaasi poistamalla ei-toivotut tiedostot turvallisesti ja pysyvästi.

Jos haluat poistaa tiedoston pysyvästi, aiempi tiedosto on korvattava uusilla tiedoilla. Microsoft® Windows ei poista tiedostoja turvallisesti, sillä kaikki tiedostotoiminnot ovat erittäin hitaita. Asiakirjan hävittäminen ei aina takaa, ettei tiedostoa voisi palauttaa, sillä jotkut ohjelmat tekevät avoimista asiakirjoista väliaikaisia piilokopioita. Jos hävität vain asiakirjat, jotka näkyvät Windowsin® Resurssienhallinnassa, asiakirjoista voi yhä olla väliaikaisia kopioita.

Huomaa: Shredder-ohjelmalla poistettuja tiedostoja ei varmuuskopioida. Et voi enää palauttaa tiedostoja, jotka on poistettu Shredder-ohjelmalla.

Tässä luvussa

Shredder-ohjelman toiminnot

Tässä osassa kuvaillaan Shredder-ohjelman toimintoja.

Ominaisuudet

Shredder-ohjelmalla voit poistaa roskakorin sisällön, väliaikaiset Internet-tiedostot, Web-sivuhistorian, tiedostoja ja kansioita sekä tyhjentää levyasemia.

LUKU 9

Ei-toivottujen tiedostojen poistaminen Shredder-ohjelmalla

Shredder-ohjelma parantaa tietosuojaasi poistamalla turvallisesti ja pysyvästi ei-toivotut tiedostot, kuten roskakorin sisällön, väliaikaiset Internet-tiedostot ja Web-sivuhistorian. Voit valita tiedostoja ja kansioita poistettavaksi tai selata niitä.

Tässä luvussa

Shredder-ohjelman käyttäminen

Tässä osassa kerrotaan, kuinka Shredder-ohjelmaa käytetään.

Tiedostojen ja kansioiden poistaminen sekä levyasemien tyhjentäminen

Tiedostot voivat yhä sijaita tietokoneessa, vaikka tyhjennät roskakorin. Shredder-ohjelma kuitenkin poistaa tiedot pysyvästi, eivätkä hakkerit pääse niihin käsiksi.

Tiedostojen ja kansioiden poistaminen ja levyasemien tyhjentäminen:

1. Valitse Lisävalikosta **Työkalut** - **Shredder**.
2. Tee jokin seuraavista:
   - Poista tiedostoja ja kansioita valitsemalla **Poistaa tiedostoja ja kansioita**.
   - Poista levyasemia valitsemalla **Tyhjentää koko levyn**.
3. Valitse jokin seuraavista poistamistasoista:
   - **Nopea**: Poistaa valitut kohteet kerran.
   - **Perusteellinen**: Poistaa valitut kohteet 7 kertaa.
   - **Mukautettu**: Poistaa valitut kohteet 10 kertaa. Mitä suurempi poistomäärä, sitä parempi tiedostojen poiston tietosuoja on.
4. Valitse **Seuraava**.
5. Tee jokin seuraavista:
   - Jos olet poistamassa tiedostoja, valitse **Valitse tuhottava(t) tiedosto(t)** -luettelosta **Roskakorin sisältö**, **Väliaikaiset Internet-tiedostot** tai **Web-sivustohistoria**. Jos olet tyhjentämässä levyasemaa, napsauta asemaa.
   - Valitse **Selaa**, siirry poistettavien tiedostojen kohdalle ja valitse ne.
   - Kirjoita poistettavien tiedostojen polku **Valitse tuhottava(t) tiedosto(t)** -luetteloon.
6. Valitse **Seuraava**.
7. Suorita toiminto loppuun valitsemalla **Valmis**.
8. Valitse **Valmis**.

LUKU 10

McAfee Network Manager

McAfee® Network Manager esittää graafisen näkymän kotiverkon tietokoneista ja osista. Network Managerin avulla voit valvoa kunkin verkkosi hallitun tietokoneen suojauksen tilaa ja korjata raportoituja tietoturvan puutteita.

Voit tutustua Networkin Managerin suosituimpiin ominaisuuksiin, ennen kuin alat käyttää sitä. Lisätietoja näiden ominaisuuksien määrittämisestä ja käyttämisestä on Network Managerin ohjeessa.

Tässä luvussa

Ominaisuudet

Network Manager tarjoaa seuraavat ominaisuudet:

Graafinen verkkokartta

Network Managerin verkkokartta tarjoaa graafisen näkymän muiden tietokoneiden ja kotiverkon osien suojaustilasta. Kun teet muutoksia verkkoosi (esimerkiksi lisäät siihen tietokoneen), verkkokartta tunnistaa muutokset. Voit päivittää verkkokarttaa, nimetä sen uudelleen ja mukauttaa näkymää näyttämällä tai piilottamalla verkkokartan osia. Voit myös tarkastella verkkokartassa näkyviin osiin liittyviä tietoja.

Etähallinta

Voit hallita kotiverkkosi tietokoneiden suojaustilaa Network Managerin verkkokartan avulla. Voit kutsua tietokoneen hallittuun verkkoon, valvoa hallitun tietokoneen suojaustilaa ja korjata tunnettuja tietoturvan puutteita verkkosi etätietokoneelta.

Network Managerin kuvakkeiden toiminta

Seuraavassa taulukossa kuvataan Network Managerin verkkokartassa yleisesti käytettyjä kuvakkeita.

Kuvake	Kuvaus
	Kuvaa verkossa olevaa hallittua tietokonetta
	Kuvaa hallittua tietokonetta, joka ei ole verkossa
	Kuvaa hallinnan piiriin kuulumatonta tietokonetta, johon on asennettu McAfee 2007 -tietoturvaohjelmisto
	Kuvaa hallinnan piiriin kuulumatonta tietokonetta, joka ei ole verkossa
	Kuvaa verkossa olevaa tietokonetta, johon ei ole asennettu McAfee 2007 -tietoturvaohjelmistoa, tai tuntematonta verkkolaitetta
	Kuvaa tietokonetta, joka ei ole verkossa ja johon ei ole asennettu McAfee 2007 -tietoturvaohjelmistoa, tai tuntematonta verkkolaitetta, joka ei ole verkossa
	Määrittää. että vastaava kohde on suojattu ja kytketty
	Määrittää, että vastaava kohde vaatii huomiota
	Määrittää, että vastaava kohde vaatii huomiota ja yhteys on katkaistu
	Kuvaa langatonta kotireititintä
	Kuvaa tavallista kotireititintä
	Kuvaa Internetiä, kun yhteys on muodostettu
	Kuvaa Internetiä, kun yhteys on katkaistu

LUKU 11

Hallitun verkon määrittäminen

Voit määrittää hallitun verkon käyttämällä verkkokartan kohteita ja lisäämällä jäseniä (tietokoneita) verkkoon.

Tässä luvussa

Verkkokartan käyttäminen

Aina kun kytket tietokoneen verkkoon, Network Manager analysoi verkon tilan ja määrittää reitittimen asetukset, Internet-tilan ja sen, onko verkossa jäseniä (hallittuja tai hallinnan piiriin kuulumattomia). Ellei jäseniä löydy, Network Manager olettaa, että nyt kytkettävä tietokone on verkon ensimmäinen tietokone ja tekee tietokoneesta automaattisesti järjestelmänvalvojan oikeuksin varustetun jäsenen. Oletusarvoisesti verkon nimeen sisältyy ensimmäisen verkkoon liittyvän tietokoneen, johon on asennettu McAfee 2007 -tietoturvaohjelmisto, työryhmän tai toimialueen nimi. Voit kuitenkin nimetä verkon uudelleen milloin tahansa.

Kun teet muutoksia verkkoosi (esimerkiksi lisäät siihen tietokoneen), voit mukauttaa verkkokarttaa. Voit esimerkiksi päivittää verkkokarttaa, nimetä sen uudelleen ja mukauttaa näkymää näyttämällä tai piilottamalla verkkokartan osia. Voit myös tarkastella verkkokartassa näkyviin osiin liittyviä tietoja.

Verkkokartan käyttäminen

Voit käyttää verkkokarttaa käynnistämällä Network Managerin SecurityCenterin yleisten tehtävien luettelosta. Verkkokartta on graafinen esitys kotiverkon tietokoneista ja osista.

Verkkokartan käyttäminen:

- Valitse Perus- tai Lisävalikosta **Verkonhallinta**. Verkkokartta näkyy oikeanpuoleisessa ikkunassa.

Huomaa: Kun käytät verkkokarttaa ensimmäistä kertaa, sinua pyydetään luottamaan verkon muihin tietokoneisiin, ennen kuin verkkokartta tulee näkyviin.

Päivitä verkkokartta

Voit päivittää verkkokartan milloin tahansa, esimerkiksi kun toinen tietokone liittyy hallittuun verkkoon.

Verkkokartan päivittäminen:

1. Valitse Perus- tai Lisävalikosta **Verkonhallinta**. Verkkokartta näkyy oikeanpuoleisessa ikkunassa.
2. Valitse **Haluan**-kohdasta **Päivitä verkkokartta**.

Huomautus: Päivitä verkkokartta -linkki on käytettävissä vain, kun verkkokartalta ei ole valittu kohteita. Voit poistaa kohteen valinnan napsauttamalla valittua kohdetta tai napsauttamalla verkkokartan valkoista kohtaa.

Verkon nimeäminen uudelleen

Oletusarvoisesti verkon nimeen sisältyy ensimmäisen verkkoon liittyvän tietokoneen, johon on asennettu McAfee 2007 -tietoturvaohjelmisto, työryhmän tai toimialueen nimi. Voit vaihtaa nimeä, ellei se ole soveltuva.

Verkon nimeäminen uudelleen:

1. Valitse Perus- tai Lisävalikosta **Verkonhallinta**. Verkkokartta näkyy oikeanpuoleisessa ikkunassa.
2. Valitse **Haluan**-kohdasta **Verkon nimeäminen uudelleen**.
3. Kirjoita verkon nimi **Nimeä verkko uudelleen** -ruutuun.
4. Valitse **OK**.

Huomautus: Nimeä verkko uudelleen -linkki on käytettävissä vain, kun verkkokartalta ei ole valittu kohteita. Voit poistaa kohteen valinnan napsauttamalla valittua kohdetta tai napsauttamalla verkkokartan valkoista kohtaa.

Verkkokartan kohteiden näyttäminen ja piilottaminen

Oletusarvoisesti kaikki kotiverkkosi tietokoneet ja osat näkyvät verkkokartalla. Jos sinulla on piilotettuja kohteita, saat ne näkyviin milloin tahansa. Vain hallinnan piiriin kuulumattomat kohteet voidaan piilottaa, hallittuja tietokoneita ei voi piilottaa.

Jos haluat saada...	Valitse Perus- tai Lisävalikosta **Verkonhallinta** ja tee näin...
...kohteen piilotettua verkkokartalta	Napsauta verkkokartalla näkyvää kohdetta ja valitse **Haluan**-kohdasta **Piilota tämä**. Valitse vahvistusvalintaikkunasta **Kyllä**.
...kohteen näkyviin verkkokartalle	Valitse **Haluan**-kohdasta **Näytä piilotetut kohteet**.

Kohteen tietojen tarkasteleminen

Voit tarkastella yksityiskohtaisia tietoja mistä tahansa verkkosi kohteesta valitsemalla kohteen verkkokartalta. Näitä tietoja ovat muun muassa osan nimi, sen suojauksen tila ja muut osan hallintaan tarvittavat tiedot.

Kohteen tietojen tarkasteleminen:

1. Napsauta verkkokartalla näkyvää kohteen kuvaketta.
2. **Tiedot**-kohdassa voit tarkastella kohteen tietoja.

Hallittuun verkkoon liittyminen

Tietokoneen täytyy olla verkon luotettu jäsen, ennen kuin sitä voidaan etähallita tai sille voidaan myöntää oikeus etähallita toisia verkon tietokoneita. Verkon jäsenyyden uusille tietokoneille myöntää verkossa jo oleva jäsen, jolla on järjestelmänvalvojan käyttöoikeudet. Jotta varmistetaan, että vain luotetut tietokoneet voivat liittyä verkkoon, täytyy sekä myöntävän että liittyvän tietokoneen todentaa toisensa.

Kun tietokone liittyy verkkoon, järjestelmä pyytää sitä paljastamaan McAfee-suojaustilansa muille verkon tietokoneille. Jos tietokone suostuu paljastamaan suojaustilansa, siitä tulee verkon *hallittu* jäsen. Jos tietokone ei suostu paljastamaan suojaustilaansa, siitä tulee *hallinnan piiriin kuulumaton* verkon jäsen . Hallinnan piiriin kuulumattomat verkon jäsenet ovat tavallisesti vierailevia tietokoneita, jotka haluavat käyttää muita verkon ominaisuuksia (kuten tiedostojen tai tulostinten jakamista).

Huomaa: Jos tietokoneeseen on asennettu muita McAfee-verkko-ohjelmia, kuten McAfee Wireless Network Security tai EasyNetwork, tietokone tunnistetaan hallittavaksi tietokoneeksi myös näiden ohjelmien osalta. Network Managerissa määritetty oikeustaso koskee kaikkia McAfee-verkko-ohjelmia. Lisätietoja vieraan käyttöoikeuksista, täysistä käyttöoikeuksista ja järjestelmänvalvojan käyttöoikeuksista McAfee-verkko-ohjelmissa on ohjelmien mukana toimitetuissa käyttöohjeissa.

Hallittuun verkkoon liittyminen

Kun saat kutsun liittyä verkkoon, voit joko hyväksyä tai hylätä kutsun. Voit määrittää myös, haluatko tämän ja muiden tietokoneiden valvovan toistensa suojausasetuksia (esimerkiksi ovatko tietokoneen virustorjuntapalvelut ajan tasalla).

Hallittuun verkkoon liittyminen:

1. Valitse kutsun valintaikkunasta **Salli tämän ja muiden tietokoneiden valvoa toistensa suojausasetuksia** -valintaruutu, jos haluat toisten hallitun verkon tietokoneiden valvovan tietokoneesi suojausasetuksia.
2. Valitse **Liity**.
   Kun hyväksyt kutsun, kaksi pelikorttia tulee näkyviin.
3. Vahvista, että kortit ovat samat kuin sinut hallittuun verkkoon kutsuneella tietokoneella näkyvät kortit.
4. Valitse **Vahvista**.

Huomaa: Jos sinut hallittuun verkkoon kutsuneen tietokoneen näytössä näkyvät kortit eivät ole samat kuin suojausvarmistuksen valintaikkunassa näkyvät kortit, hallitun verkon turvallisuus on uhattuna. Verkkoon liittyminen saattaa altistaa tietokoneesi turvallisuusriskeille, joten valitse suojausvarmistuksen valintaikkunasta **Hylkää**.

Tietokoneen kutsuminen hallittuun verkkoon

Jos hallittuun verkkoon lisätään tietokone tai verkossa on hallinnan piiriin kuulumaton tietokone, voit kutsua ne liittymään hallittuun verkkoon. Vain tietokoneet, joilla on järjestelmänvalvojan oikeudet verkossa, voivat kutsua toisia tietokoneita liittymään verkkoon. Kun lähetät pyynnön, määrität samalla liittyvälle tietokoneelle myönnettävän oikeustason.

Tietokoneen kutsuminen liittymään hallittuun verkkoon:

1. Napsauta verkkokartalla näkyvää hallinnan piiriin kuulumattoman tietokoneen kuvaketta.
2. Valitse **Haluan**-kohdasta **Valvo tätä tietokonetta**.
3. Valitse Kutsu tietokone liittymään hallittuun verkkoon -valintaikkunasta jokin seuraavista:
   - **Myönnä vieraan käyttöoikeudet**
     Vieraan käyttöoikeuksilla tietokone voi käyttää verkkoa.
   - **Myönnä täydelliset käyttöoikeudet kaikkiin hallitun verkon sovelluksiin**
     Täydellisillä käyttöoikeuksilla (kuten vieraan käyttöoikeuksilla) tietokone voi käyttää verkkoa.

- **Myönnä järjestelmänvalvojan käyttöoikeudet kaikkiin hallitun verkon sovelluksiin**
  Järjestelmänvalvojan käyttöoikeuksilla tietokone voi käyttää verkkoa järjestelmänvalvojan oikeuksin. Niillä varustettu tietokone voi myös myöntää käyttöoikeuden muille tietokoneille, jotka haluavat liittyä hallittuun verkkoon.

4 Valitse **Kutsu**.
Kutsu liittyä hallittuun verkkoon lähetään tietokoneelle. Kun tietokone hyväksyy kutsun, kaksi pelikorttia tulee näkyviin.

5 Vahvista, että kortit ovat samat kuin hallittuun verkkoon kutsutussa tietokoneessa näkyvät kortit.

6 Valitse **Myönnä käyttöoikeudet**.

Huomaa: Jos hallittuun verkkoon kutsutun tietokoneen näytössä näkyvät kortit eivät ole samat kuin suojausvarmistuksen valintaikkunassa näkyvät kortit, hallitun verkon turvallisuus on uhattuna. Käyttöoikeuden myöntäminen tälle tietokoneelle saattaa altistaa toiset tietokoneet vaaroille, joten valitse suojausvarmistuksen valintaikkunasta **Hylkää**.

Lakkaa luottamasta verkon tietokoneisiin

Jos olet vahingossa suostunut luottamaan toiseen verkon tietokoneeseen, voit lopettaa luottamisen.

Verkon tietokoneeseen luottamisen lopettaminen:

- Valitse **Haluan**-kohdasta **Lopeta tämän verkon tietokoneisiin luottaminen**.

Huomaa: Lopeta tämän verkon tietokoneisiin luottaminen -linkki on valittavissa vain, jos verkkoon ei ole liittynyt muita hallittuja tietokoneita.

LUKU 12

Verkon etähallinta

Kun olet asentanut hallitun verkon, voit etähallita verkon tietokoneita ja osia Network Managerin avulla. Voit valvoa tietokoneiden ja osien tilaa ja oikeustasoja sekä korjata tietoturvan puutteita.

Tässä luvussa

Tilan ja oikeuksien valvonta

Hallitussa verkossa on kahdentyyppisiä jäseniä: hallittuja jäseniä ja hallinnan piiriin kuulumattomia jäseniä. Hallitut jäsenet sallivat muiden verkon tietokoneiden valvoa McAfee-suojaustasoaan, hallinnan piiriin kuulumattomat eivät. Hallinnan piiriin kuulumattomat verkon jäsenet ovat tavallisesti vierailevia tietokoneita, jotka haluavat käyttää muita verkon ominaisuuksia (kuten tiedostojen tai tulostinten jakamista). Toinen hallitun verkon tietokone voi kutsua hallinnan piiriin kuulumattoman tietokoneen hallituksi tietokoneeksi. Samoin hallitusta tietokoneesta voidaan tehdä hallinnan piiriin kuulumaton milloin tahansa.

Hallituilla tietokoneilla on joko järjestelmänvalvojan, täydet tai vieraan käyttöoikeudet. Järjestelmänvalvojan oikeuksilla hallitut tietokoneet voivat hallita toisten hallittujen tietokoneiden suojaustilaa verkossa ja myöntää toisille tietokoneille verkon jäsenyyksiä. Täysillä käyttöoikeuksilla ja vieraan käyttöoikeuksilla tietokoneet voivat vain käyttää verkkoa. Voit muokata tietokoneen oikeustasoa milloin tahansa.

Hallittuun verkkoon kuuluu myös laitteita (esimerkiksi reitittimiä), joita voit myös hallita Network Managerin avulla. Voit myös määrittää ja muokata laitteen näytön ominaisuuksia verkkokartalla.

Tietokoneen suojauksen tilan valvominen

Jos tietokoneen suojauksen tilaa ei valvota verkossa (joko koska tietokone ei ole verkon jäsen tai se ei kuulu hallinnan piiriin), sen valvontaa voi pyytää.

Tietokoneen suojauksen tilan valvominen:

1. Napsauta verkkokartalla näkyvää hallinnan piiriin kuulumattoman tietokoneen kuvaketta.
2. Valitse **Haluan**-kohdasta **Valvo tätä tietokonetta**.

Tietokoneen suojauksen tilan valvomisen lopettaminen

Voit lopettaa yksityisen verkon hallitun tietokoneen suojauksen tilan valvomisen. Tietokoneesta tulee tällöin hallinnan piiriin kuulumaton.

Tietokoneen suojauksen tilan valvomisen lopettaminen:

1. Napsauta verkkokartalla näkyvää hallitun tietokoneen kuvaketta.
2. Valitse **Haluan**-kohdasta **Lopeta tämän tietokoneen valvonta**.
3. Valitse vahvistusvalintaikkunasta **Kyllä**.

Hallitun tietokoneen oikeuksien muokkaaminen

Voit muokata hallitun tietokoneen oikeuksia milloin tahansa. Oikeuksien avulla voit määrittää, mitkä tietokoneet valvovat toisten verkon tietokoneiden suojauksen tilaa (suojausasetuksia).

Hallitun tietokoneen oikeuksien muokkaaminen

1. Napsauta verkkokartalla näkyvää hallitun tietokoneen kuvaketta.
2. Valitse **Haluan**-kohdasta **Muuta tämän tietokoneen käyttöoikeuksia**.
3. Määritä, voivatko hallitun verkon tietokoneet valvoa toistensa suojauksen tilaa valitsemalla tai poistamalla valinta käyttöoikeuksien muuttamisen valintaikkunan valintaruudusta.
4. Valitse **OK**.

Laitteen hallitseminen

Voit hallita laitetta käyttämällä sen hallinnan Web-sivua Network Managerista käsin.

Laitteen hallitseminen:

1. Napsauta verkkokartalla näkyvää laitteen kuvaketta.
2. Valitse **Haluan**-kohdasta **Ota tämä laite hallintaan**. Laitteen hallinnan Web-sivu aukeaa selaimeen.
3. Kirjoita kirjautumistietosi selaimeen ja määritä laitteen suojausasetukset.

Huomaa: Jos laite on Wireless Network Securityn suojaama langaton reititin tai yhteyspiste, sen suojausasetusten määrittämiseen on käytettävä Wireless Network Securityä.

Laitteen näytön ominaisuuksien muokkaaminen

Kun muokkaat laitteen näytön ominaisuuksia, voit muuttaa laitteen näyttönimeä verkossa ja määrittää, onko laite langaton reititin.

Laitteen näytön ominaisuuksien muokkaaminen:

1. Napsauta verkkokartalla näkyvää laitteen kuvaketta.
2. Valitse **Haluan**-kohdasta **Muokkaa laitteen ominaisuuksia**.
3. Voit määrittää laitteen näyttönimen kirjoittamalla nimen **Nimi**-ruutuun.
4. Voit määrittää laitteen tyypin napsauttamalla toista seuraavista:
   - **Reititin**
     Tämä vastaa tavallista kotireititintä.
   - **Langaton reititin**
     Tämä vastaa langatonta kotireititintä.
5. Valitse **OK**.

Tietoturvan puutteiden korjaaminen

Järjestelmänvalvojan oikeuksilla varustetut tietokoneet voivat valvoa verkossa olevien toisten hallittujen tietokoneiden McAfee-suojaustasoa ja korjata raportoituja tietoturvan puutteita. Jos esimerkiksi hallitun tietokoneen McAfee-suojaustaso ilmaisee, ettei virustorjunta ole käytössä, toinen järjestelmävalvojan oikeuksin varustettu hallittu tietokone voi *korjata* tämän tietoturvan puutteen ottamalla virustorjunnan käyttöön etäyhteyden kautta.

Kun korjaat tietoturvan puutteita etäyhteyden kautta, Network Manager korjaa useimmat raportoidut ongelmat automaattisesti. Tietyt tietoturvan puutteet saattavat kuitenkin vaatia manuaalisia toimia paikalliselta tietokoneelta. Tässä tapauksessa Network Manager korjaa ne ongelmat, jotka se pystyy korjaamaan etäyhteyden kautta, ja pyytää korjaamaan loput ongelmat kirjautumalla kyseisessä tietokoneessa SecurityCenteriin ja noudattamalla tarjottuja suosituksia. Joissakin tapauksissa suositeltava korjaustapa on McAfee 2007 -tietoturvaohjelmiston asentaminen etätietokoneeseen tai verkon tietokoneisiin.

Korjaa tietoturvan puutteet

Network Managerin avulla voit korjata automaattisesti useimmat hallittujen tietokoneiden tietoturvan puutteet etäyhteyttä käyttäen. Jos esimerkiksi virustorjunta on poistettu käytöstä etätietokoneesta, voit ottaa sen automaattisesti käyttöön Network Managerin avulla.

Tietoturvan puutteiden korjaaminen:

1. Napsauta verkkokartalla näkyvää kohteen kuvaketta.
2. Kohteen suojauksen tila näkyy **Lisätiedot**-kohdassa.
3. Valitse **Haluan**-kohdasta **Tietoturvan puutteiden korjaaminen**.
4. Kun tietoturvan puutteet on korjattu, napsauta **OK**-painiketta.

Huomaa: Vaikka Network Manager korjaa automaattisesti useimmat tietoturvan puutteet, joidenkin puutteiden korjaus edellyttää SecurityCenterin käynnistämistä kyseisessä tietokoneessa ja tarjottujen suositusten noudattamista.

McAfee-tietoturvaohjelmiston asentaminen etätietokoneisiin

Jos yksi tai useampi verkkosi tietokone ei käytä McAfee 2007 -tietoturvaohjelmistoa, niiden suojauksen tilaa ei voida valvoa etäyhteyden kautta. Jos haluat valvoa kyseisiä tietokoneita etäyhteydettä käyttäen, niihin täytyy asentaa McAfee-tietoturvaohjelmisto.

McAfee-tietoturvaohjelmiston asentaminen etätietokoneisiin:

1. Siirry etätietokoneen selaimella osoitteeseen http://download.mcafee.com/us/.
2. Asenna McAfee 2007 -tietoturvaohjelmisto tietokoneeseen noudattamalla näytössä näkyviä ohjeita.

LUKU 13

McAfee VirusScan

VirusScan tarjoaa kattavan, luotettavan ja päivitetyn suojauksen viruksia ja vakoiluohjelmia vastaan. VirusScan suojaa tietokonetta viruksia, matoja, troijalaisia, epäilyttäviä komentosarjoja, tietomurto-ohjelmistoja, puskurin ylivuotoja, sekahyökkäyksiä, vakoiluohjelmia, mahdollisia haittaohjelmia ja muita uhkia vastaan McAfeen palkitun tarkistustekniikan avulla.

Tässä luvussa

Ominaisuudet

Tämä VirusScan-ohjelmistoversio sisältää seuraavat ominaisuudet.

Virustorjunta

Tiedostojen reaaliaikainen tarkistus tarkistaa tiedostot, kun sinä tai tietokoneesi käyttää niitä.

Tarkista

Etsii viruksia ja muita uhkia kiintolevyasemista, levykkeiltä ja yksittäisistä tiedostoista ja kansioista. Voit myös tarkistaa kohteen napsauttamalla sitä hiiren kakkospainikkeella.

Vakoilu- ja mainosohjelmien tunnistustoiminto

VirusScan tunnistaa ja poistaa vakoiluohjelmia, mainosohjelmia ja muita ohjelmia, jotka saattavat vaarantaa tietosuojasi ja heikentää järjestelmäsi suorituskykyä.

Automaattiset päivitykset

Automaattiset päivitykset suojaavat tietokonettasi viimeisimpiä tunnistettuja ja tunnistamattomia tietoturvauhkia vastaan.

Nopea taustatarkistustoiminto

Nopeat, huomaamattomat tarkistukset tunnistavat ja tuhoavat viruksia, troijalaisia, matoja, vakoiluohjelmia, mainosohjelmia, soitto-ohjelmia ja muita uhkia häiritsemättä työskentelyäsi.

Reaaliaikaiset suojaushälytykset

Suojaushälytykset ilmoittavat merkittävistä virusesiintymistä ja tietoturvauhkista ja tarjoavat toimintoja, joiden avulla voit poistaa tai neutraloida uhkia ja lukea niitä koskevia lisätietoja.

Tunnistus- ja puhdistustoiminnot useissa tulokohdissa

VirusScan valvoo ja puhdistaa tietokoneesi tärkeimpiä tulokohtia: sähköpostiviestejä, pikaviestien liitteitä ja Internet-latauksia.

Sähköpostin valvonta matomaisten toimintojen varalta

WormStopper™ estää troijalaisia lähettämästä matoja muihin tietokoneisiin sähköpostiviesteissä ja kysyy käyttäjältä luvan, ennen kuin tuntemattomien sähköpostiohjelmien sallitaan lähettää viestejä.

Komentosarjojen valvonta matomaisten toimintojen varalta

ScriptStopper™ estää tunnettujen, vahingollisten komentosarjojen suorittamisen tietokoneessasi.

McAfee X-ray for Windows

McAfee X-ray tunnistaa ja tuhoaa tietomurto-ohjelmistoja ja muita ohjelmia, jotka eivät näy Windowsissa.

Puskurin ylivuotosuojaus

Puskurin ylivuotosuojaus suojaa järjestelmää puskurin ylivuodoilta. Puskurin ylivuotoja esiintyy, kun epäilyttävät ohjelmat tai prosessit yrittävät tallentaa tietokoneen puskuriin (tietojen väliaikaiselle tallennusalueelle) enemmän tietoja kuin mitä siihen mahtuu. Tämä vioittaa vierekkäisissä puskureissa olevia kelvollisia tietoja tai korvaa ne.

McAfee SystemGuards -toiminnot

SystemGuards-toiminnot tarkkailevat tietokonettasi tiettyjen tapahtumien varalta, jotka saattavat viitata virusten, vakoiluohjelmien tai hakkereiden toimintaan.

LUKU 14

Virustorjunnan hallinta

Voit hallita reaaliaikaisia virustorjunta-, vakoiluohjelmien torjunta-, SystemGuards- ja komentosarjasuojaustoimintoja. Voit esimerkiksi poistaa tarkistustoiminnon käytöstä tai määrittää, mitä kohteita haluat tarkistaa.

Ainoastaan käyttäjät, joilla on järjestelmänvalvojan oikeudet, voivat muokata lisäasetuksia.

Tässä luvussa

Virustorjunnan käyttäminen

Kun virustorjunta (reaaliaikainen tarkistustoiminto) käynnistetään, se valvoo tietokonettasi jatkuvasti virustapahtumien varalta. Reaaliaikainen tarkistustoiminto tarkistaa tiedostot joka kerta, kun sinä tai tietokoneesi käyttää niitä. Kun virustorjuntatoiminto tunnistaa tartunnan saaneen tiedoston, se yrittää puhdistaa tiedoston tai poistaa sen. Jos tiedostoa ei voi puhdistaa tai poistaa, hälytys kehottaa sinua suorittamaan jatkotoimenpiteitä.

Vastaavat aiheet

- Mitä suojaushälytykset ovat? (sivu 103)

Virustorjuntatoiminnon poistaminen käytöstä

Jos poistat virustorjuntatoiminnon käytöstä, tietokonettasi ei valvota virustapahtumien varalta. Jos sinun täytyy keskeyttää virustorjunta, varmista, että et ole yhteydessä Internetiin.

Huomaa: Virustorjunnan poistaminen käytöstä poistaa myös reaaliaikaisen vakoiluohjelma-, sähköposti- ja pikaviestiohjelmasuojauksen käytöstä.

Virustorjuntatoiminnon poistaminen käytöstä:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **Virustorjunta**-kohdassa **Ei käytössä**.
4. Suorita jokin seuraavista toiminnoista Vahvistus-valintaikkunassa:
   - Jos haluat käynnistää virustorjuntatoiminnon automaattisesti uudelleen tietyn ajanjakson kuluttua, valitse **Ota reaaliaikainen tarkistus uudelleen käyttöön, kun aika on kulunut** -valintaruutu ja valitse haluamasi aika luettelosta.
   - Jos haluat estää virustorjuntatoimintoa käynnistymästä uudelleen tietyn ajanjakson kuluttua, tyhjennä **Ota virustorjunta uudelleen käyttöön, kun aika on kulunut** -valintaruutu.

5 Valitse **OK**.

Jos reaaliaikainen suojaus on määritetty käynnistymään Windowsin käynnistyessä, tietokoneesi on suojattu, kun käynnistät sen uudelleen.

Vastaavat aiheet

- Reaaliaikaisen suojauksen määrittäminen (sivu 74)

Virustorjuntatoiminnon käyttöönottaminen

Virustorjuntatoiminto valvoo tietokonettasi jatkuvasti virustapahtumien varalta.

Virustorjuntatoiminnon käyttöönottaminen:

1 Valitse Lisävalikon kohta **Määritä**.

2 Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.

3 Valitse **Virustorjunta**-kohdassa **Käytössä**.

Reaaliaikaisen suojauksen määrittäminen

Voit halutessasi muokata reaaliaikaista virustorjuntatoimintoa. Voit esimerkiksi tarkistaa vain ohjelmatiedostot ja asiakirjat tai poistaa reaaliaikaisen tarkistuksen käytöstä Windowsin käynnistyessä (ei suositeltavaa).

Reaaliaikaisen suojauksen määrittäminen

Voit halutessasi muokata reaaliaikaista virustorjuntatoimintoa. Voit esimerkiksi tarkistaa vain ohjelmatiedostot ja asiakirjat tai poistaa reaaliaikaisen tarkistuksen käytöstä Windowsin käynnistyessä (ei suositeltavaa).

Reaaliaikaisen suojauksen määrittäminen:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **Virustorjunta**-kohdassa **Lisäasetukset**.
4. Valitse tai tyhjennä seuraavat valintaruudut:
   - **Tarkista tuntemattomat virukset heuristiikan avulla**: Tiedostoja verrataan tunnettujen virusten allekirjoituksiin, jotta voitaisiin tunnistaa merkkejä tunnistamattomista viruksista. Tämä vaihtoehto tarjoaa perusteellisimman tarkistuksen, mutta se on yleensä hitaampi kuin tavallinen tarkistus.
   - **Tarkista levyasema, kun järjestelmä suljetaan**: Levyasema tarkistetaan, kun suljet tietokoneesi.
   - **Tarkista vakoiluohjelmat ja mahdolliset haittaohjelmat**: Vakoiluohjelmat, mainosohjelmat ja muut mahdollisesti ilman lupaa tietoja keräävät ja lähettävät ohjelmat tunnistetaan ja poistetaan.
   - **Tarkista ja poista seurantaevästeet**: Evästeet, jotka mahdollisesti keräävät ja lähettävät tietoja ilman lupaa tunnistetaan ja poistetaan. Evästeet toimivat käyttäjien tunnisteina heidän vieraillessa Web-sivustoissa.
   - **Tarkista verkkoasemat**: Verkkoon liitetyt asemat tarkistetaan.
   - **Ota käyttöön puskurin ylivuotosuojaus**: Jos puskurin ylivuototapahtuma tunnistetaan, se estetään ja sinulle näytetään hälytysilmoitus.
   - **Käynnistä reaaliaikainen tarkistus, kun Windows käynnistyy (suositus)**: Reaaliaikainen suojaus otetaan käyttöön joka kerta, kun käynnistät tietokoneen, vaikka poistaisit sen käytöstä yhden istunnon ajaksi.

5 Napsauta toista seuraavista painikkeista:

- **Kaikki tiedostot (suositus)**: Jokainen tietokoneesi käyttämä tiedostotyyppi tarkistetaan. Käytä tätä toimintoa, jos haluat suorittaa perusteellisimman tarkistuksen.
- **Vain ohjelmatiedostot ja asiakirjat**: Ainoastaan ohjelmatiedostot ja asiakirjat tarkistetaan.

6 Valitse **OK**.

Vakoiluohjelmasuojauksen käyttäminen

Vakoiluohjelmasuojaus poistaa vakoilu- ja mainosohjelmia ja muita mahdollisia haittaohjelmia, jotka keräävät ja lähettävät tietoja ilman käyttäjän myöntämää lupaa.

Vakoiluohjelmasuojauksen poistaminen käytöstä

Jos poistat vakoiluohjelmasuojauksen käytöstä, luvattomasti tietoja kerääviä ja lähettäviä mahdollisia haittaohjelmia ei tunnisteta.

Vakoiluohjelmasuojauksen poistaminen käytöstä:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **Vakoiluohjelmasuojaus**-kohdassa **Ei käytössä**.

Vakoiluohjelmasuojauksen käyttöönottaminen

Vakoiluohjelmasuojaus poistaa vakoilu- ja mainosohjelmia ja muita mahdollisia haittaohjelmia, jotka keräävät ja lähettävät tietoja ilman käyttäjän myöntämää lupaa.

Vakoiluohjelmasuojauksen käyttöönottaminen:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **Vakoiluohjelmasuojaus**-kohdassa **Käytössä**.

SystemGuards-toimintojen käyttäminen

SystemGuards-toiminnot tunnistavat tietokoneeseesi tehdyt mahdollisesti luvattomat muutokset ja varoittavat niistä. Voit tämän jälkeen tarkastella muutoksia ja päättää, haluatko sallia ne.

SystemGuards-toiminnot on luokiteltu seuraavasti.

Ohjelma

Ohjelmien SystemGuards-toiminnot tunnistavat käynnistystiedostojen, tiedostotunnisteiden ja määritystiedostojen muutokset.

Windows

Windowsin SystemGuards-toiminnot tunnistavat Internet Explorerin asetusten muutokset, kuten selainmääritteiden ja suojausasetusten muutokset.

Selain

Selaimen SystemGuards-toiminnot tunnistavat Windows®-palveluiden, sertifikaattien ja määritystiedostojen muutokset.

SystemGuards-toimintojen poistaminen käytöstä

Jos poistat SystemGuards-toiminnot käytöstä, tietokoneeseesi tehtyjä mahdollisesti luvattomia muutoksia ei tunnisteta.

Kaikkien SystemGuards-toimintojen poistaminen käytöstä:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **SystemGuard-suojaus**-kohdassa **Ei käytössä**.

SystemGuards-toimintojen käyttöönottaminen

SystemGuards-toiminnot tunnistavat tietokoneeseesi tehdyt mahdollisesti luvattomat muutokset ja varoittavat niistä.

SystemGuards-toimintojen käyttöönottaminen:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **SystemGuard-suojaus**-kohdassa **Käytössä**.

SystemGuards-toimintojen määrittäminen

Voit halutessasi muokata SystemGuards-toimintoja. Voit päättää, että tapahtumista hälytetään ja ne kirjataan lokiin tapahtumakohtaisesti tai että tapahtumat ainoastaan kirjataan lokiin tai että SystemGuard-toiminto poistetaan käytöstä.

SystemGuards-toimintojen määrittäminen

Voit halutessasi muokata SystemGuards-toimintoja. Voit päättää tapahtumakohtaisesti miten tapahtumista hälytetään ja miten tapahtumat kirjataan lokiin, tai että tapahtumat ainoastaan kirjataan lokiin, tai että SystemGuard-toiminto poistetaan käytöstä.

SystemGuards-toimintojen määrittäminen:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **SystemGuard-suojaus**-kohdassa **Lisäasetukset**.
4. Valitse jokin SystemGuards-luettelon luokka näyttääksesi luettelon liitetyistä SystemGuards-toiminnoista ja niiden tilasta.
5. Napsauta SystemGuard-toiminnon nimeä.
6. Voit näyttää lisätietoja SystemGuard-toiminnosta **Lisätiedot**-kohdassa.
7. Suorita jokin seuraavista toimenpiteistä **Haluan**-kohdassa:
   - Valitse **Näytä hälytykset**, jos haluat, että muutoksen tapahtuessa näytetään hälytysilmoitus ja tapahtuma kirjataan lokiin.
   - Valitse **Muutokset ainoastaan kirjataan lokiin**, jos haluat, että mitään toimenpidettä ei suoriteta, kun muutos tunnistetaan. Tässä tapauksessa muutos ainoastaan kirjataan lokitiedostoon.
   - Valitse **Poista SystemGuard-toiminto käytöstä** poistaaksesi SystemGuard-toiminnon käytöstä. Sinulle ei näytetä hälytystä muutoksen tapahtuessa ja tapahtumaa ei kirjata lokitiedostoon.
8. Valitse **OK**.

Miten SystemGuards-toiminnot toimivat?

SystemGuards-toiminnot tunnistavat tietokoneeseesi tehdyt mahdollisesti luvattomat muutokset ja varoittavat niistä. Voit tämän jälkeen tarkastella muutoksia ja päättää, haluatko sallia ne.

SystemGuards-toiminnot on luokiteltu seuraavasti.

Ohjelma

Ohjelmien SystemGuards-toiminnot tunnistavat käynnistystiedostojen, tiedostotunnisteiden ja määritystiedostojen muutokset.

Windows

Windowsin SystemGuards-toiminnot tunnistavat Internet Explorerin asetusten muutokset, kuten selainmääritteiden ja suojausasetusten muutokset.

Selain

Selaimen SystemGuards-toiminnot tunnistavat Windows®-palveluiden, sertifikaattien ja määritystiedostojen muutokset.

Tietoja ohjelmien SystemGuards-toiminnoista

Ohjelmien SystemGuards-toiminnot tunnistavat seuraavat tapahtumat.

ActiveX-asennukset

Tunnistaa Internet Explorerilla ladatut ActiveX-ohjelmat. ActiveX-ohjelmia ladataan Web-sivustoista, ja ne tallennetaan tietokoneen C:\Windows\Downloaded Program Files- tai C:\Windows\Temp\Temporary Internet Files -kansioon. Niihin viitataan myös rekisterissä niiden CLSID-tunnuksella (pitkä numerosarja aaltosulkeiden välissä).

Internet Explorer käyttää säännöllisesti monia kelvollisia ActiveX-ohjelmia. Jos et ole varma ActiveX-ohjelman toiminnasta, voit poistaa sen tietokoneesta vahinkoja aiheuttamatta. Jos tarvitset ohjelmaa myöhemmin, Internet Explorer lataa sen automaattisesti, kun palaat sitä vaativaan Web-sivustoon seuraavan kerran.

Käynnistystiedostot

Valvoo käynnistysrekisteriavaimiin ja -kansioihin tehtyjä muutoksia. Windowsin rekisterin käynnistysrekisteriavaimet ja Käynnistä-valikon käynnistyskansiot tallentavat ohjelmien polkuja tietokoneeseen. Näissä sijainneissa luetteloidut ohjelmat ladataan Windowsin käynnistyessä. Vakoiluohjelmat tai muut mahdolliset haittaohjelmat yrittävät usein latautua automaattisesti, kun Windows käynnistyy.

Windows Shell Execute Hook -ohjelmat

Valvoo Explorer.exe-tiedostoon ladattavien ohjelmien luetteloon tehtyjä muutoksia. Shell Execute Hook on ohjelma, joka latautuu explorer.exe Windows-käyttöliittymään. Shell Execute Hook -ohjelma vastaanottaa kaikki tietokoneessa suoritettavat suorituskomennot. Kaikki explorer.exe-käyttöliittymään ladatut ohjelmistot voivat suorittaa myös muita tehtäviä ennen toisen ohjelman todellista käynnistämistä. Vakoiluohjelmat tai muut mahdolliset haittaohjelmat voivat käyttää Shell Execute Hook -ohjelmia estääkseen tietoturvaohjelmia toimimasta.

Shell Service Object Delay Load -luettelo

Valvoo Shell Service Object Delay Load -luettelon tiedostojen muutoksia. Explorer.exe-tiedosto lataa kyseisen luettelon tiedostot tietokoneen käynnistyessä. Koska explorer.exe on tietokoneen käyttöliittymä, se käynnistyy aina ja lataa tässä avaimessa mainitut tiedostot. Nämä tiedostot ladataan käynnistystoiminnon alussa ennen käyttäjän toimenpiteitä.

Tietoja Windows SystemGuards -toiminnoista

Windows SystemGuards -toiminnot tunnistavat seuraavat tapahtumat.

Pikavalikon käsittelijät

Estää Windowsin pikavalikoiden luvattomat muutokset. Näiden valikoiden avulla voit napsauttaa tiedostoa hiiren kakkospainikkeella ja suorittaa kyseistä tiedostoa koskevia toimintoja.

AppInit DLL-tiedostot

Estää Windowsin AppInit.DLL-tiedostojen luvattomat muutokset. AppInit_DLL-tiedostojen rekisteriarvo sisältää luettelon tiedostoista, jotka ladataan user32.dll-tiedoston latautuessa. AppInit_DLL-arvossa olevat tiedostot ladataan Windows-käynnistystoiminnon alussa, jolloin mahdollisesti haitalliset .DLL-tiedostot voivat piiloutua ennen käyttäjän toimenpiteitä.

Windowsin Hosts-tiedosto

Valvoo tietokoneen Hosts-tiedoston muutoksia. Hosts-tiedostoa käytetään tiettyjen toimialuiden nimien uudelleenohjaamiseen tiettyihin IP-osoitteisiin. Kun esimerkiksi käyt sivustossa www.esimerkki.com, selain tarkistaa Hosts-tiedoston, löytää sivustoon example.com viittaavan merkinnän ja siirtyy kyseisen toimialueen IP-osoitteeseen. Jotkin vakoiluohjelmat yrittävät muuttaa Hosts-tiedostoa ja ohjata selaimesi toiseen sivustoon tai estää ohjelmistoasi päivittymästä kunnolla.

Winlogon Shell

Valvoo Winlogon-käyttöliittymää. Tämä käyttöliittymä ladataan, kun käyttäjä kirjautuu sisään Windowsiin. Käyttöliittymä on Windowsin ensisijainen hallintakäyttöliittymä ja se on tavallisesti Windowsin Resurssienhallinta (explorer.exe). Windows-käyttöliittymä voidaan kuitenkin yhdistää helposti myös toiseen ohjelmaan. Tällöin jokin toinen ohjelma kuin Windows-käyttöliittymä käynnistetään aina, kun käyttäjä kirjautuu sisään.

Winlogon User Init

Valvoo Windowsin kirjautumistietoihin tehtyjä muutoksia. HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit-avain määrittää mikä ohjelma käynnistetään, kun käyttäjä on kirjautunut sisään Windowsiin. Oletusohjelma palauttaa käyttäjänimelle määritetyn profiilin, fontit, värit ja muut asetukset. Vakoiluohjelmat ja muut mahdolliset haittaohjelmat saattavat yrittää käynnistyä lisäämällä itsensä tähän avaimeen.

Windows-protokollat

Valvoo verkkoprotokolliin tehtyjä muutoksia. Jotkin vakoiluohjelmat tai muut mahdolliset haittaohjelmat ohjaavat tietokoneen tapaa lähettää ja vastaanottaa tietoja. Tämä tapahtuu Windows-protokollien suodattimien ja käsittelijöiden avulla.

Winsock-kerrostettujen palvelujen tarjoajat

Valvoo kerrostettujen palvelujen tarjoajia, jotka saattavat kaapata verkossa siirrettäviä tietoja ja muuttaa tai uudelleenohjata niitä. Luvallisia LSP:itä ovat muun muassa käytönvalvontaohjelmistot, palomuurit ja muut tietoturvaohjelmat. Vakoiluohjelmat voivat käyttää LSP:itä Internet-tapahtumien valvontaan ja tietojen muuttamiseen. Jotta et joudu asentamaan käyttöjärjestelmää uudelleen, poista vakoiluohjelmat ja haitalliset kerrostettujen palvelujen tarjoajat McAfee-ohjelmien avulla.

Windows-käyttöliittymän avoimet komennot

Estää Windows-käyttöliittymän (explore.exe) avoimien komentojen muutokset. Shell Open Command -komennot sallivat tiettyjen ohjelmien suorittamisen aina tietyn tyyppistä tiedostoa suoritettaessa. Esimerkiksi mato voi yrittää käynnistyä automaattisesti aina, kun .exe-sovellus suoritetaan.

Shared Task Scheduler

Valvoo SharedTaskScheduler-rekisteriavainta, joka sisältää luettelon niistä ohjelmista, jotka suoritetaan Windowsin käynnistyessä. Jotkin vakoiluohjelmat tai muut mahdolliset haittaohjelmat muokkaavat tätä avainta ja lisäävät itsensä luetteloon ilman lupaa.

Windows Messenger -palvelu

Valvoo Windows Messenger -palvelua, joka on Windows Messengerin dokumentoimaton toiminto, jonka avulla käyttäjät voivat lähettää ponnahdusviestejä. Jotkin vakoiluohjelmat tai muut mahdolliset haittaohjelmat yrittävät ottaa palvelun käyttöön ja lähettää turhia mainoksia. Palvelua voidaan käyttää myös koodien etäsuorittamiseen hyödyntämällä tunnettua suojausongelmaa.

Windowsin Win.ini-tiedosto

Win.ini-tiedosto on tekstipohjainen tiedosto, joka sisältää luettelon niistä ohjelmista, jotka suoritetaan Windowsin käynnistyessä. Tiedostossa oleva ohjelmien lataamiseen tarkoitettu syntaksi tukee Windowsin aikaisempia versioita. Useimmat nykyiset ohjelmat eivät käytä win.ini-tiedostoa ohjelmien lataamiseen. Jotkin vakoiluohjelmat tai muut mahdolliset haittaohjelmat ovat kuitenkin suunniteltu hyödyntämään tätä vanhempaa syntaksia ja lataamaan itsensä Windowsin käynnistyessä.

Tietoja selaimen SystemGuards-toiminnoista

Selaimen SystemGuards-toiminnot tunnistavat seuraavat tapahtumat.

Selainapuohjelman objektit

Valvoo selainapuohjelman objekteihin tehtäviä lisäyksiä. Selainapuohjelman objektit ovat ohjelmia, jotka toimivat Internet Explorerin plug-in-laajennuksina. Vakoiluohjelmat ja selaimen kaappaajat käyttävät usein selainapuohjelmien objekteja mainosten näyttämiseen tai käyttäjän selaintoimintojen seuraamiseen. Monet kelvolliset ohjelmat, kuten tavalliset hakutyökalurivit, käyttävät myös selainapuohjelmien objekteja.

Internet Explorerin palkit

Valvoo Internet Explorerin palkkiohjelmien luetteloon tehtyjä muutoksia. Explorer-palkki on Haku-, Suosikit- ja Historia-ruutujen kaltainen ruutu, joka näkyy Internet Explorer -selaimessa tai Windowsin Resurssienhallinnassa.

Internet Explorerin plug-in-laajennukset

Estää vakoiluohjelmia asentamasta Internet Explorerin plug-in-laajennuksia. Internet Explorerin plug-in-laajennukset ovat ohjelmistolaajennuksia, jotka ladataan Internet Explorerin käynnistyessä. Vakoiluohjelmat käyttävät usein Internet Explorerin plug-in-laajennuksia mainosten näyttämiseen tai käyttäjän selaintoimintojen seuraamiseen. Kelvolliset plug-in-laajennukset parantavat Internet Explorer -selaimen toimintaa.

Internet Explorer ShellBrowser

Valvoo Internet Explorer ShellBrowser -esiintymän muutoksia. Internet Explorer ShellBrowser sisältää Internet Explorer -esiintymän tietoja ja asetuksia. Jos näitä asetuksia muutetaan tai uusi ShellBrowser lisätään, uusi ShellBrowser voi ottaa Internet Explorerin kokonaan hallintaansa ja lisätä uusia toimintoja, kuten työkalurivejä, valikoita ja painikkeita.

Internet Explorer WebBrowser

Valvoo Internet Explorer WebBrowser -esiintymän muutoksia. Internet Explorer WebBrowser sisältää Internet Explorer -esiintymän tietoja ja asetuksia. Jos näitä asetuksia muutetaan tai uusi WebBrowser lisätään, uusi WebBrowser voi ottaa Internet Explorerin kokonaan hallintaansa ja lisätä uusia toimintoja, kuten työkalurivejä, valikoita ja painikkeita.

Internet Explorer URL Search Hook -objektit

Valvoo Internet Explorerin URL Search Hook -objekteihin tehtyjä muutoksia. URL Search Hook -objektia käytetään silloin, kun kirjoitat osoitteen selaimen sijaintikenttään ilman osoitteen http://- tai ftp://-protokollaa. Kun kirjoitat tällaisen osoitteen, selain voi käyttää UrlSearchHook-objektia hakeakseen kirjoittamasi sijainnin Internetistä.

Internet Explorerin URL-osoitteet

Valvoo Internet Explorerin valmiiksi määritettyjen URL-osoitteiden muutoksia. Tämä estää vakoiluohjelmia tai muita mahdollisia haittaohjelmia muuttamasta selainasetuksia ilman lupaa.

Internet Explorerin rajoitukset

Valvoo Internet Explorerin rajoituksia, jotka antavat järjestelmänvalvojalle mahdollisuuden estää käyttäjää muuttamasta Internet Explorerin kotisivua tai muita asetuksia. Nämä toiminnot ovat käytettävissä vain silloin, kun järjestelmänvalvoja on ottanut ne tarkoituksellisesti käyttöön.

Internet Explorerin suojausvyöhykkeet

Valvoo Internet Explorerin suojausvyöhykkeitä. Internet Explorerissa on neljä valmiiksi määritettyä suojausvyöhykettä: Internet, Paikallinen intranet, Luotettavat sivustot ja Kielletyt sivustot. Jokaisella suojausvyöhykkeellä on oma valmiiksi määritetty tai mukautettu suojausasetuksensa. Suojausvyöhykkeet ovat joidenkin vakoiluohjelmien tai muiden mahdollisten haittaohjelmien kohteita, sillä suojaustason alentaminen sallii näiden ohjelmien ohittaa suojaushälytykset ja toimia huomaamatta.

Internet Explorerin luotettavat sivustot

Valvoo Internet Explorerin luotettavia sivustoja. Luotettavien sivustojen luettelo on niiden Web-sivustojen hakemisto, jotka olet merkinnyt luotettaviksi. Tämä luettelo on joidenkin vakoiluohjelmien ja mahdollisten haittaohjelmien kohteena, sillä sen avulla epäilyttävät sivustot voidaan merkitä luotettavaksi ilman käyttäjän myöntämää lupaa.

Internet Explorer -käytäntö

Valvoo Internet Explorer -käytäntöjä. Näitä käytäntöasetuksia muuttavat yleensä järjestelmänvalvojat, mutta vakoiluohjelmat voivat käyttää niitä hyväkseen. Muutokset voivat estää sinua muuttamasta kotisivua tai piilottamasta Työkalut-valikon Internet-asetukset-valintaikkunan välilehtiä.

Komentosarjojen tarkistustoiminnon käyttäminen

Komentosarjat voivat luoda, kopioida tai poistaa tiedostoja. Komentosarjat voivat myös avata Windowsin rekisterin.

Komentosarjojen tarkistustoiminto estää tunnettujen, vahingollisten komentosarjojen suorittamisen tietokoneessa automaattisesti.

Komentosarjojen tarkistustoiminnon poistaminen käytöstä

Jos poistat komentosarjojen tarkistustoiminnon käytöstä, epäilyttäviä komentosarjoja ei tunnisteta.

Komentosarjojen tarkistustoiminnon poistaminen käytöstä:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **Komentosarjatarkistussuojaus**-kohdassa **Ei käytössä**.

Komentosarjojen tarkistustoiminnon käyttöönottaminen

Komentosarjojen tarkistustoiminto näyttää käyttäjälle hälytysilmoituksen, jos komentosarjan suorittaminen luo, kopioi tai poistaa tiedostoja tai avaa Windowsin rekisterin.

Komentosarjojen tarkistustoiminnon käyttöönottaminen:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **Komentosarjatarkistussuojaus**-kohdassa **Käytössä**.

Sähköpostisuojauksen käyttäminen

Sähköpostisuojaus tunnistaa ja estää saapuvien (POP3) ja lähtevien (SMTP) sähköpostiviestien ja liitetiedostojen uhkia, kuten viruksia, troijalaisia, matoja, vakoiluohjelmia, mainosohjelmia ja muita uhkia.

Sähköpostisuojauksen poistaminen käytöstä

Jos poistat sähköpostisuojauksen käytöstä, saapuvien (POP3) ja lähtevien (SMTP) sähköpostiviestien ja liitetiedostojen mahdollisia uhkia ei tunnisteta.

Sähköpostisuojauksen poistaminen käytöstä:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Sähköposti & viestit**.
3. Valitse **Sähköpostisuojaus**-kohdassa **Ei käytössä**.

Sähköpostisuojauksen käyttöönottaminen

Sähköpostisuojaus tunnistaa saapuvien (POP3) ja lähtevien (SMTP) sähköpostiviestien ja liitetiedostojen uhkia.

Sähköpostisuojauksen käyttöönottaminen:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Sähköposti & viestit**.
3. Valitse **Sähköpostisuojaus**-kohdassa **Käytössä**.

Sähköpostisuojauksen määrittäminen

Sähköpostisuojauksen asetusten avulla voit tarkistaa saapuvat ja lähtevät sähköpostiviestit matojen varalta. Madot kopioituvat ja kuluttavat järjestelmäresursseja, mikä heikentää tietokoneen suorituskykyä tai keskeyttää tehtäviä. Madot voivat lähettää itsensä kopioita sähköpostiviesteissä. Ne saattavat esimerkiksi yrittää edelleenlähettää sähköpostiviestejä yhteystietoluettelossasi oleville henkilöille.

Sähköpostisuojauksen määrittäminen

Sähköpostisuojauksen asetusten avulla voit tarkistaa saapuvat ja lähtevät sähköpostiviestit matojen varalta.

Sähköpostisuojauksen määrittäminen:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Sähköposti & viestit**.
3. Valitse **Sähköpostisuojaus**-kohdassa **Lisäasetukset**.
4. Valitse tai tyhjennä seuraavat valintaruudut:
   - **Tarkista saapuvat sähköpostiviestit**: Saapuvat (POP3) sähköpostiviestit tarkistetaan mahdollisten uhkien varalta.
   - **Tarkista lähtevät sähköpostiviestit**: Lähtevät (SMTP) sähköpostiviestit tarkistetaan mahdollisten uhkien varalta.
   - **Ota WormStopper käyttöön**: WormStopper estää sähköpostiviestien madot.
5. Valitse **OK**.

Pikaviestisuojauksen käyttäminen

Pikaviestisuojaus tunnistaa saapuvien pikaviestien liitetiedostojen uhkia.

Pikaviestisuojauksen poistaminen käytöstä

Jos poistat pikaviestisuojauksen käytöstä, saapuvien pikaviestien liitetiedostojen uhkia ei tunnisteta.

Pikaviestisuojauksen poistaminen käytöstä

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Sähköposti & viestit**.
3. Valitse **Pikaviestisuojaus**-kohdassa **Ei käytössä**.

Pikaviestisuojauksen käyttöönottaminen

Pikaviestisuojaus tunnistaa saapuvien pikaviestien liitetiedostojen uhkia.

Pikaviestisuojauksen käyttöönottaminen:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Sähköposti & viestit**.
3. Valitse **Pikaviestisuojaus**-kohdassa **Käytössä**.

LUKU 15

Tietokoneen manuaalinen tarkistaminen

Voit etsiä viruksia ja muita uhkia kiintolevyasemilta, levykkeiltä ja yksittäisistä tiedostoista ja kansioista. Kun VirusScan löytää epäilyttävän tiedoston, se yrittää puhdistaa sen, ellei kyseessä ole mahdollinen haittaohjelma. Jos VirusScan ei pysty puhdistamaan tiedostoa, voit eristää tai poistaa sen.

Tässä luvussa

Manuaalinen tarkistaminen

Voit halutessasi suorittaa manuaalisen tarkistuksen milloin tahansa. Jos esimerkiksi olet juuri asentanut VirusScanin, voit suorittaa tarkistuksen varmistaaksesi, että tietokoneessasi ei ole viruksia tai muita uhkia. Tai jos olet poistanut reaaliaikaisen tarkistuksen käytöstä, voit suorittaa tarkistuksen varmistaaksesi, että tietokoneesi on yhä turvallinen.

Tarkistaminen manuaalisten tarkistusasetusten avulla

Tämän tyyppinen tarkistus käyttää manuaalisesti määrittämiäsi tarkistusasetuksia. VirusScan tarkistaa myös pakattujen tiedostojen (.zip, .cab jne.) sisällä olevat tiedostot, mutta se laskee pakatun tiedoston yhdeksi tiedostoksi. Myös tarkistettujen tiedostojen lukumäärä voi vaihdella, jos olet poistanut väliaikaiset Internet-tiedostot edellisen tarkistuksen jälkeen.

Tarkistaminen manuaalisten tarkistusasetusten avulla:

1. Valitse Perusvalikon kohta **Tarkista**. Kun tarkistus on suoritettu, yhteenveto näyttää tarkistettujen ja tunnistettujen kohteiden lukumäärän, puhdistettujen kohteiden lukumäärän ja edellisen tarkistuksen ajankohdan.
2. Valitse **Lopeta**.

Vastaavat aiheet

- Manuaalisten tarkistusten määrittäminen (sivu 94)

Tarkistaminen ilman manuaalisia tarkistusasetuksia

Tämä tarkistustoiminto ei käytä manuaalisesti määrittämiäsi tarkistusasetuksia. VirusScan tarkistaa myös pakattujen tiedostojen (.zip, .cab jne.) sisällä olevat tiedostot, mutta se laskee pakatun tiedoston yhdeksi tiedostoksi. Myös tarkistettujen tiedostojen lukumäärä voi vaihdella, jos olet poistanut väliaikaiset Internet-tiedostot edellisen tarkistuksen jälkeen.

Tarkistaminen ilman manuaalisia tarkistusasetuksia:

1. Valitse Lisävalikon kohta **Koti**.
2. Valitse Koti-ruudun kohta **Tarkista**.
3. Valitse **Tarkistettavat sijainnit** -kohdassa tarkistettavien tiedostojen, kansioiden ja asemien valintaruudut.
4. Valitse **Asetukset** -kohdassa tarkistettavien tiedostotyyppien valintaruudut.
5. Valitse **Tarkista nyt**. Kun tarkistus on suoritettu, yhteenveto näyttää tarkistettujen ja tunnistettujen kohteiden

lukumäärän, puhdistettujen kohteiden lukumäärän ja edellisen tarkistuksen ajankohdan.

6 Valitse **Lopeta**.

Huomaa: Näitä asetuksia ei tallenneta.

Tarkistaminen Windowsin Resurssienhallinnassa

Voit tarkistaa valitsemiasi tiedostoja, kansioita ja asemia virusten ja muiden uhkien varalta Windowsin Resurssienhallinnassa.

Tiedostojen tarkistaminen Windowsin Resurssienhallinnassa:

1 Avaa Windowsin Resurssienhallinta.

2 Napsauta tarkistettavaa tiedostoa, kansiota tai asemaa hiiren kakkospainikkeella ja valitse sitten **Tarkista**. Kaikki oletustarkistusasetukset on valittu, jotta tarkistus suoritetaan mahdollisimman perusteellisesti.

Manuaalisten tarkistusten määrittäminen

Kun suoritat manuaalisen tai ajoitetun tarkistuksen, voit määrittää tarkistettavat tiedostotyypit, tarkistettavat sijainnit sekä tarkistuksen suoritusajankohdan.

Tarkistettavien tiedostotyyppien määrittäminen

Voit halutessasi määrittää tarkistettavat tiedostotyypit.

Tarkistettavien tiedostotyyppien määrittäminen:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **Virustorjunta**-kohdassa **Lisäasetukset**.
4. Valitse Virustorjunta-ruudun kohta **Manuaalinen tarkistus**.
5. Valitse tai tyhjennä seuraavat valintaruudut:
   - **Tarkista tuntemattomat virukset heuristiikan avulla**: Tiedostoja verrataan tunnettujen virusten allekirjoituksiin, jotta voitaisiin tunnistaa merkkejä tunnistamattomista viruksista. Tämä vaihtoehto tarjoaa perusteellisimman tarkistuksen, mutta se on yleensä hitaampi kuin tavallinen tarkistus.
   - **Tarkista .zip- ja muut pakatut tiedostot**: Tunnistaa ja poistaa viruksia .zip-tiedostoista ja muista pakatuista tiedostoista. Joskus virusten tekijät sijoittavat viruksia .zip-tiedostoon ja asettavat sitten kyseisen .zip-tiedoston toisen .zip-tiedoston sisälle, jotta virustorjuntaohjelmat eivät tunnistaisi niitä.
   - **Tarkista vakoiluohjelmat ja mahdolliset haittaohjelmat**: Vakoiluohjelmat, mainosohjelmat ja muut mahdollisesti ilman lupaa tietoja keräävät ja lähettävät ohjelmat tunnistetaan ja poistetaan.
   - **Tarkista ja poista seurantaevästeet**: Evästeet, jotka mahdollisesti keräävät ja lähettävät tietoja ilman lupaa tunnistetaan ja poistetaan. Evästeet toimivat käyttäjien tunnisteina heidän vieraillessa Web-sivustoissa.
   - **Tarkista tietomurto-ohjelmistot ja muut vaikeasti havaittavat ohjelmat**: Tunnistaa ja poistaa kaikki tietomurto-ohjelmistot ja muut ohjelmat, jotka eivät näy Windowsissa.
6. Napsauta toista seuraavista painikkeista:
   - **Kaikki tiedostot (suositus)**: Jokainen tietokoneesi käyttämä tiedostotyyppi tarkistetaan. Käytä tätä toimintoa, jos haluat suorittaa perusteellisimman tarkistuksen.
   - **Vain ohjelmatiedostot ja asiakirjat**: Ainoastaan ohjelmatiedostot ja asiakirjat tarkistetaan.

7 Valitse **OK**.

Tarkistettavien sijaintien määrittäminen

Voit määrittää manuaalisten ja ajoitettujen tarkistusten sijainnit.

Tarkistettavan sijainnin määrittäminen:

1 Valitse Lisävalikon kohta **Määritä**.

2 Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.

3 Valitse **Virustorjunta**-kohdassa **Lisäasetukset**.

4 Valitse Virustorjunta-ruudun kohta **Manuaalinen tarkistus**.

5 Valitse **Oletustarkistussijainti**-kohdassa tiedostot, kansiot ja asemat, jotka haluat tarkistaa.

   Jotta tarkistus suoritetaan mahdollisimman perusteellisesti, varmista, että **Tärkeät tiedostot** -kohta on valittu.

6 Valitse **OK**.

Tarkistusten ajoittaminen

Voit ajoittaa perusteellisia tarkistuksia etsimään tietokoneestasi viruksia ja muita uhkia tietyin aikavälein.

Tarkistuksen ajoittaminen:

1 Valitse Lisävalikon kohta **Määritä**.

2 Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.

3 Valitse **Virustorjunta**-kohdassa **Lisäasetukset**.

4 Valitse Virustorjunta-ruudun kohta **Ajoitettu tarkistus**.

5 Varmista, että **Ota käyttöön ajoitettu tarkistus** on valittu.

6 Valitse sen viikonpäivän viereinen valintaruutu, jolloin haluat suorittaa tarkistuksen.

7 Määritä tarkistuksen aloitusaika napsauttamalla aloitusaikaluettelon arvoja.

8 Valitse **OK**.

Vihje: Voit palauttaa oletusajoitukset valitsemalla **Palauta.**

LUKU 16

VirusScanin hallinta

Voit poistaa kohteita luotetuista luetteloista, hallita eristettyjä ohjelmia, evästeitä ja tiedostoja, näyttää tapahtumia ja lokeja ja tehdä ilmoituksia epäilyttävistä tapahtumista McAfeelle.

Tässä luvussa

Luotettujen listojen hallinta

Kun merkitset SystemGuard-toiminnon, ohjelman, puskurin ylivuodon tai sähköpostiohjelman luotettavaksi, kyseinen kohde lisätään luotettujen luetteloon, jotta sitä ei enää tunnisteta.

Jos merkitset ohjelman luotetuksi vahingossa tai haluat, että ohjelma tunnistetaan, sinun täytyy poistaa se kyseisestä luettelosta.

Luotettujen listojen hallinta

Kun merkitset SystemGuard-toiminnon, ohjelman, puskurin ylivuodon tai sähköpostiohjelman luotettavaksi, kyseinen kohde lisätään luotettujen luetteloon, jotta sitä ei enää tunnisteta.

Jos merkitset ohjelman luotetuksi vahingossa tai haluat, että ohjelma tunnistetaan, sinun täytyy poistaa se kyseisestä luettelosta.

Kohteiden poistaminen luotettujen luetteloista:

1. Valitse Lisävalikon kohta **Määritä**.
2. Valitse Määritä-ruudun kohta **Tietokone & tiedostot**.
3. Valitse **Virustorjunta**-kohdassa **Lisäasetukset**.
4. Valitse Virustorjunta-ruudun kohta **Luotetut luettelot**.
5. Valitse luotettu SystemGuard-toiminto, ohjelma, puskurin ylivuoto tai sähköpostiohjelma luettelossa näyttääksesi sen kohteet ja niiden luotettavuustilat.
6. Voit näyttää kohteen lisätietoja **Lisätiedot**-kohdassa.
7. Valitse jokin toiminto **Haluan**-kohdassa.
8. Valitse **OK**.

Eristettyjen ohjelmien, evästeiden ja tiedostojen hallinta

Eristettyjä ohjelmia, evästeitä ja tiedostoja voidaan palauttaa, poistaa tai lähettää McAfeelle analysoitavaksi.

Eristettyjen ohjelmien, evästeiden ja tiedostojen palauttaminen

Jos tarpeellista, voit palauttaa eristettyjä ohjelmia, evästeitä ja tiedostoja.

Eristettyjen ohjelmien, evästeiden ja tiedostojen palauttaminen:

1. Valitse Lisävalikon kohta **Palauta**.
2. Valitse tarpeen mukaan Palauta-ruudun kohta **Ohjelmat ja evästeet** tai **Tiedostot**.
3. Valitse eristetyt ohjelmat, evästeet tai tiedostot, jotka haluat palauttaa.
4. Jos haluat lisätietoja eristetystä viruksesta, napsauta sen tunnistusnimeä **Lisätiedot**-kohdassa. Viruksen kuvaus näytetään virustietokannassa.
5. Valitse **Haluan**-kohdassa **Palauta**.

Eristettyjen ohjelmien, evästeiden ja tiedostojen poistaminen

Voit halutessasi poistaa eristettyjä ohjelmia, evästeitä ja tiedostoja.

Eristettyjen ohjelmien, evästeiden ja tiedostojen poistaminen:

1. Valitse Lisävalikon kohta **Palauta**.
2. Valitse tarpeen mukaan Palauta-ruudun kohta **Ohjelmat ja evästeet** tai **Tiedostot**.
3. Valitse eristetyt ohjelmat, evästeet tai tiedostot, jotka haluat poistaa.
4. Jos haluat lisätietoja eristetystä viruksesta, napsauta sen tunnistusnimeä **Lisätiedot**-kohdassa. Viruksen kuvaus näytetään virustietokannassa.
5. Valitse **Haluan**-kohdassa **Poista**.

Eristettyjen ohjelmien, evästeiden ja tiedostojen lähettäminen McAfeelle

Voit lähettää eristettyjä ohjelmia, evästeitä ja tiedostoja McAfeelle analysoitavaksi.

Huomaa: Jos lähettämäsi eristetty tiedosto ylittää tiedostojen enimmäiskokorajoituksen, tiedosto voidaan hylätä. Useimmissa tapauksissa näin ei kuitenkaan tapahdu.

Eristetyn ohjelman tai tiedoston lähettäminen McAfeelle:

1. Valitse Lisävalikon kohta **Palauta**.
2. Valitse tarpeen mukaan Palauta-ruudun kohta **Ohjelmat ja evästeet** tai **Tiedostot**.
3. Valitse eristetyt ohjelmat, evästeet tai tiedostot, jotka haluat lähettää McAfeelle.
4. Jos haluat lisätietoja eristetystä viruksesta, napsauta sen tunnistusnimeä **Lisätiedot**-kohdassa. Viruksen kuvaus näytetään virustietokannassa.
5. Valitse **Haluan**-kohdassa **Lähetä McAfeelle**.

Viimeisimpien tapahtumien ja lokien näyttäminen

Viimeisimmät tapahtumat ja lokit näyttävät kaikkien asennettujen McAfee-tuotteiden tapahtumia.

Voit nähdä viimeiset 30 merkittävää tietokoneessasi tapahtunutta tapahtumaa Viimeisimpien tapahtumien luettelossa. Voit myös palauttaa estettyjä ohjelmia, ottaa reaaliaikaisen tarkistuksen uudelleen käyttöön ja merkitä puskurin ylivuototapahtumia luotettaviksi.

Voit myös näyttää lokitiedostoja, jotka tallentavat kaikki viimeisen 30 päivän tapahtumat.

Tapahtumien näyttäminen

Voit nähdä viimeiset 30 merkittävää tietokoneessasi tapahtunutta tapahtumaa Viimeisimpien tapahtumien luettelossa. Voit myös palauttaa estettyjä ohjelmia, ottaa reaaliaikaisen tarkistuksen uudelleen käyttöön ja merkitä puskurin ylivuototapahtumia luotettaviksi.

Tapahtumien näyttäminen:

1. Valitse Lisävalikon kohta **Raportit & lokit**.
2. Valitse Raportit & lokit -ruudun kohta **Viimeisimmät tapahtumat**.
3. Valitse tapahtuma, jonka haluat näyttää.
4. Voit näyttää tapahtuman tiedot **Lisätiedot**-kohdassa.
5. Valitse jokin toiminto **Haluan**-kohdassa.

Lokien näyttäminen

Lokit tallentavat kaikki viimeisen 30 päivän tapahtumat.

Lokien näyttäminen:

1. Valitse Lisävalikon kohta **Raportit & lokit**.
2. Valitse Raportit & lokit -ruudun kohta **Viimeisimmät tapahtumat**.
3. Valitse Viimeisimmät tapahtumat -ruudun kohta **Näytä loki**.
4. Valitse lokityyppi, jonka haluat näyttää ja valitse sitten loki.
5. Voit näyttää lokin tiedot **Lisätiedot**-kohdassa.

Anonyymien tietojen automaattinen raportointi

Voit lähettää tietoja mahdollisista haittaohjelmista, viruksista ja hakkereiden jäljitystiedoista anonyymisti McAfeelle. Tämä toiminto on käytettävissä ainoastaan asennuksen aikana.

Mitään henkilökohtaisia tietoja ei kerätä.

Raportointi McAfeelle

Voit lähettää tietoja mahdollisista haittaohjelmista, viruksista ja hakkereiden jäljitystiedoista anonyymisti McAfeelle. Tämä toiminto on saatavissa ainoastaan asennuksen aikana.

Anonyymien tietojen automaattinen raportointi:

1. Hyväksy **Lähetä nimettömät tiedot** -oletustoiminto VirusScan-asennuksen aikana.
2. Valitse **Seuraava**.

Mitä suojaushälytykset ovat?

Jos reaaliaikainen tarkistustoiminto tunnistaa uhkan, hälytys tulee näyttöön. Reaaliaikainen tarkistustoiminto näyttää suojaushälytyksen ja yrittää poistaa useimmat virukset, troijalaiset ja madot automaattisesti. Mahdollisten haittaohjelmien ja SystemGuards-toimintojen ilmetessä reaaliaikainen tarkistustoiminto tunnistaa tiedoston tai muutoksen ja näyttää suojaushälytyksen. Puskurin ylivuotojen, seurantaevästeiden ja komentosarjatoimintojen ilmetessä reaaliaikainen tarkistustoiminto estää tapahtumat automaattisesti ja näyttää suojaushälytyksen.

Nämä hälytykset voidaan jakaa kolmeen eri ryhmään.

- Punaiset hälytykset
- Keltaiset hälytykset
- Vihreät hälytykset

Voit valita, miten tunnistettuja tiedostoja ja sähköposteja, epäilyttäviä komentosarjoja, mahdollisia matoja, mahdollisia haittaohjelmia, SystemGuards-toimintoja ja puskurin ylivuotoja hallitaan.

Hälytysten hallinta

McAfee käyttää useita erilaisia hälytyksiä, joiden avulla voit hallita järjestelmäsi suojausta. Nämä hälytykset voidaan jakaa kolmeen eri ryhmään.

- Punaiset hälytykset
- Keltaiset hälytykset
- Vihreät hälytykset

Punaiset hälytykset

Punainen hälytys vaatii käyttäjän vastauksen. Joissain tapauksissa McAfee ei pysty päättelemään automaattisesti, kuinka tiettyihin tapahtumiin täytyy vastata. Tällöin punainen hälytys kuvaa kyseessä olevan tapahtuman ja antaa käyttäjälle yhden tai useamman valittavan vaihtoehdon.

Keltaiset hälytykset

Keltainen hälytys on ei-kriittinen ilmoitus, joka yleensä vaatii käyttäjän antaman vastauksen. Keltainen hälytys kuvaa kyseessä olevan tapahtuman ja antaa käyttäjälle yhden tai useamman valittavan vaihtoehdon.

Vihreät hälytykset

Useimmissa tapauksissa vihreä hälytys antaa perustietoja tapahtumasta, eikä vaadi käyttäjän vastausta.

Hälystysasetusten määrittäminen

Jos et halua näyttää hälytystä ja muutat myöhemmin mielesi, voit halutessasi muokata asetusmäärityksiä siten, että hälytys näytetään jatkossa. Lisätietoja hälytysasetusten määrittämisestä löydät SecurityCenter-ohjeesta.

LUKU 17

Lisäohjeet

Tästä osasta löydät vastaukset usein kysyttyihin kysymyksiin ja ohjeet vianmääritystilanteisiin.

Tässä luvussa

Usein kysytyt kysymykset

Tämä osa sisältää vastauksia useimmin kysyttyihin kysymyksiin.

Uhka on tunnistettu, mitä minun täytyy tehdä?

McAfee käyttää hälytyksiä auttaakseen sinua hallitsemaan järjestelmäsi suojausta. Nämä hälytykset voidaan jakaa kolmeen eri ryhmään.

- Punainen hälytys
- Keltainen hälytys
- Vihreä hälytys

Voit valita miten tunnistettuja tiedostoja ja sähköposteja, epäilyttäviä komentosarjoja, mahdollisia matoja, mahdollisia haittaohjelmia, SystemGuards-toimintoja ja puskurin ylivuotoja hallitaan.

Lisätietoja tietynlaisten uhkien hallinnasta löydät virustietokannasta osoitteesta: http://us.mcafee.com/virusInfo/default.asp?affid=.

Vastaavat aiheet

- Mitä suojaushälytykset ovat? (sivu 103)

Voinko käyttää VirusScan-ohjelmistoa Netscape-, Firefox- ja Opera-selainten kanssa?

Voit käyttää Netscape-, Firefox- tai Opera-selainta oletusselaimenasi, mutta sinulla täytyy olla Microsoft Internet Explorer 6.0 tai uudempi asennettuna tietokoneeseesi.

Täytyykö minun olla yhteydessä Internetiin, jotta voin suorittaa tarkistuksen?

Sinun ei tarvitse olla yhteydessä Internetiin tarkistuksen suorittamiseksi, mutta sinun kannattaa muodostaa Internet-yhteys vähintään kerran viikossa, jotta voit vastaanottaa McAfee-päivitykset.

Tarkistaako VirusScan sähköpostien liitetiedostot?

Jos olet ottanut käyttöön reaaliaikaisen tarkistuksen ja sähköpostisuojauksen, kaikki liitetiedostot tarkistetaan sähköpostiviestin saapuessa.

Tarkistaako VirusScan zip-pakatut tiedostot?

VirusScan tarkistaa .zip-tiedostot ja muut pakatut tiedostot.

Miksi lähtevien sähköpostiviestien tarkistamisessa tapahtuu virheitä?

Kun lähteviä sähköpostiviestejä tarkistetaan, seuraavantyyppisiä virheitä voi tapahtua:

- Protokollavirhe. Sähköpostipalvelin on hylännyt sähköpostiviestin.
  Jos tapahtuu protokollavirhe tai järjestelmävirhe, kyseisen istunnon jäljellä olevat sähköpostiviestit käsitellään ja lähetetään palvelimeen.
- Yhteysvirhe. Sähköpostipalvelinyhteys on katkaistu.
  Jos tapahtuu yhteysvirhe, varmista, että tietokoneesi on yhteydessä Internetiin, ja yritä sitten lähettää viesti uudelleen sähköpostiohjelmasi **Lähetetyt viestit** -luettelosta.
- Järjestelmävirhe. Tiedostonkäsittelyvirhe tai muu järjestelmävirhe on tapahtunut.
- Salatun SMTP-yhteyden virhe. Sähköpostiohjelmasi salattu SMTP-yhteys on tunnistettu.
  Jos salatun SMTP-yhteyden virhe tapahtuu, poista sähköpostiohjelmasi salattu SMTP-yhteys käytöstä varmistaaksesi, että sähköpostiviestisi tarkistetaan.

Jos sähköpostiviestien lähettämisessä tapahtuu aikakatkaisuja, poista lähtevien sähköpostiviestien tarkistus tai sähköpostiohjelmasi salattu SMTP-yhteys käytöstä.

Liittyvät aiheet

- Sähköpostisuojauksen määrittäminen (sivu 88)

Vianmääritys

Tämä osa sisältää ohjeita, joiden avulla voit ratkaista yleisiä ongelmia.

Virusta ei voi puhdistaa tai poistaa

Joidenkin virusten esiintyessä tietokone täytyy puhdistaa manuaalisesti. Käynnistä tietokone uudelleen ja yritä sitten tarkistaa järjestelmä uudelleen.

Jos tietokoneesi ei voi puhdistaa tai poistaa virusta, katso lisäohjeita virustietokannasta osoitteessa: http://us.mcafee.com/virusInfo/default.asp?affid=.

Jos tarvitset lisäapua, ota yhteys McAfeen asiakastukeen McAfeen Web-sivustossa.

Huomaa: Viruksia ei voi poistaa CD- ja DVD-levyiltä tai kirjoitussuojatuilta levykkeiltä.

Kohdetta ei voi poistaa edes uudelleenkäynnistyksen jälkeen

Kun olet tarkistanut ja poistanut kohteita, joissakin tilanteissa tietokone täytyy käynnistää uudelleen.

Jos kohdetta ei ole poistettu tietokoneen uudelleenkäynnistyksen jälkeen, lähetä tiedosto McAfeelle.

Huomaa: Viruksia ei voi poistaa CD- ja DVD-levyiltä tai kirjoitussuojatuilta levykkeiltä.

Liittyvät aiheet

- Eristettyjen ohjelmien, evästeiden ja tiedostojen hallinta (sivu 99)

Komponentteja puuttuu tai ne ovat vioittuneita

Joissakin tilanteissa VirusScan saattaa asentua virheellisesti:

- Tietokoneessasi ei ole riittävästi levytilaa tai muistia. Varmista, että tietokoneesi vastaa ohjelman suorittamiseen vaadittavia järjestelmävaatimuksia.
- Internet-selaimesi on määritetty virheellisesti.
- Internet-yhteytesi ei toimi oikein. Tarkista yhteys. Muussa tapauksessa yritä muodostaa yhteys myöhemmin uudelleen.
- Tiedostoja puuttuu tai asennus epäonnistui.

Paras ratkaisu on ratkaista nämä mahdolliset ongelmat ja asentaa sitten VirusScan uudelleen.

LUKU 18

McAfee Personal Firewall

Personal Firewall on edistynyt tapa suojata tietokonetta ja henkilökohtaisia tietoja. Personal Firewall muodostaa muurin tietokoneen ja Internetin välille ja valvoo Internet-tietoliikennettä taustalla epäilyttävien tapahtumien varalta.

Tässä luvussa

Ominaisuudet

Personal Firewall tajoaa täydellisen lähtevän ja saapuvan tietoliikenteen palomuurisuojauksen ja myöntää käyttöoikeudet luotettaville ohjelmille automaattisesti sekä suojaa järjestelmäsi vakoiluohjelmia, troijalaisia ja salakuunteluyrityksiä vastaan. Palomuurin avulla voit suojautua luotauksilta ja hyökkäyksiltä, valvoa Internet- ja verkkotapahtumia, saada hälytyksiä vihamielisistä ja epäilyttävistä tapahtumista, saada yksityiskohtaisia tietoja Internet-tietoliikenteestä sekä täydentää virustorjuntaa.

Suojaustasot, vakio ja muokattu

Suojaudu tietomurroilta ja epäilyttävältä toiminnalta käyttämällä palomuurin oletusarvoisia suojausasetuksia tai mukauta palomuuria vastaamaan omia turvallisuustarpeitasi.

Reaaliaikaiset suositukset

Voit saada dynaamisesti suosituksia, jotka auttavat päättämään, sallitaanko ohjelman muodostaa yhteys Internetiin tai luotetaanko verkkotietoliikenteeseen.

Ohjelmien älykäs hallinta

Hallitse ohjelmien pääsyä Internetiin hälytysten ja tapahtumalokien avulla tai määritä pääsyoikeuksia määrätyille ohjelmille palomuurin Ohjelmien käyttöoikeudet -ikkunasta.

Pelien suojelu

Estä tietomurtoyritysten ja epäilyttävien toimintojen hälytyksiä häiritsemästä sinua pelatessasi koko ruudun tilassa ja määritä palomuuri näyttämään hälytykset, kun olet lopettanut pelaamisen.

Tietokoneen käynnistyksenaikainen suojaus

Palomuuri suojaa tietokonettasi tietomurtoyrityksiltä, mahdollisilta haittaohjelmilta ja verkkotietoliikenteeltä, ennen kuin Windows avautuu.

Järjestelmäpalveluportin hallinta

Järjestelmäpalveluportit voivat toimia tietokoneesi takaporttina. Palomuurin avulla voit luoda ja hallita joidenkin ohjelmien vaatimia järjestelmäpalveluportteja.

Tietokoneen yhteyksien hallinta

Aseta luotettaviksi tai estetyiksi etäyhteyksiä ja IP-osoitteita, jotka voivat ottaa yhteyden tietokoneeseesi.

HackerWatchin tietojen integrointi

HackerWatch on turvallisuustietojen keskus, joka seuraa yleisiä hakkerointi- ja tietomurtokaavoja sekä tarjoaa tuoreinta tietoa tietokoneesi ohjelmista. Voit tarkastella yleisten turvallisuustapahtumien ja Internet-porttien tilastoja.

Lukitse palomuuri

Estää kaiken saapuvan ja lähtevän Internet-tietoliikenteen välittömästi.

Palauta palomuuri

Palauttaa palomuurin alkuperäiset suojausasetukset välittömästi. Jos Personal Firewall ei toimi halutulla tavalla etkä saa sitä korjatuksi, voit palauttaa palomuurin oletusasetuksiinsa.

Kehittynyt troijalaisten tunnistus

Yhdistää ohjelmien yhteyksien hallinnan parannettuun tietokantaan tunnistaakseen ja estääkseen mahdollisesti vihamielisten sovellusten, kuten troijalaisten, pääsyn Internetiin ja henkilökohtaisten tietojen levittämisen.

Tapahtumien kirjaaminen lokiin

Määritä, otetaanko lokiin kirjaaminen käyttöön, ja jos otetaan, niin mitä tapahtumatyyppejä kirjataan. Tapahtumalokin kirjaamisen avulla voit tarkastella saapuvia ja lähteviä tapahtumia. Voit tarkastella myös havaittuja tietomurtotapahtumia.

Internet-tietoliikenteen valvonta

Tarkastele helppolukuisia graafisia karttoja, joista näkyy vihamielisten hyökkäysten lähde ja maailmanlaajuinen tietoliikenne. Näet lisäksi yksityiskohtaisia tietoja lähteenä olevan IP-osoitteen omistajasta sekä sen maantieteellisen sijainnin. Voit myös analysoida saapuvaa ja lähtevää tietoliikennettä, valvoa ohjelmien yhteyskaistan käyttöä ja ohjelmien toimintaa.

Tietomurtojen estäminen

Suojaa yksityisyyttäsi tarjoamalla mahdollisten Internet-uhkien tietomurtojen eston. McAfee käyttää heuristis-tyyppisiä toimintoja tarjotessaan kolmannen asteen suojatason estämällä kohteita, jotka näyttävät hyökkäyksen oireita tai vaikuttavat hakkerointiyrityksiltä .

Hienostunut tietoliikenneanalyysi

Voit tarkastella sekä saapuvaa että lähtevää Internet-tietoliikennettä ja ohjelmien yhteyksiä, myös niitä, jotka kuuntelevat aktiivisesti avoimia yhteyksiä. Tämän avulla voit nähdä ohjelmat, jotka saattavat olla alttiina tietomurroille.

Firewallin käynnistäminen

Firewallin käynnistämisen jälkeen tietokone on suojattu tietomurroilta ja ei-toivotulta tietoliikenteeltä. Olet lisäksi valmis käsittelemään hälytyksiä ja hallitsemaan tunnettujen ja tuntemattomien ohjelmien saapuvaa ja lähtevää Internet-käyttöä. Suositukset ja Normaali-tietoturvataso otetaan automaattisesti käyttöön.

Voit poistaa Firewallin käytöstä Internet- ja verkkomääritykset -ikkunasta, mutta tällöin tietokone ei ole suojassa tietomurroilta ja ei-toivotulta tietoliikenteeltä, etkä myöskään voi hallita saapuvia ja lähteviä Internet-yhteyksiä tehokkaasti. Jos sinun on poistettava palomuurisuojaus käytöstä, tee se väliaikaisesti ja vain silloin, kun se on aivan välttämätöntä. Voit ottaa Firewallin käyttöön myös Internet- ja verkkomääritykset -ikkunasta.

Firewall poistaa Windowsin® palomuurin automaattisesti käytöstä ja asettaa itsensä oletuspalomuuriksi.

Huomaa: Määritä palomuuri avaamalla Internet ja verkko -asetusikkuna.

Käynnistä palomuurisuojaus

Palomuurin ottaminen käyttöön suojaa tietokoneesi tietomurtoja ja ei-toivottua tietoliikennettä vastaan, sekä auttaa sinua hallitsemaan saapuvia ja lähteviä Internet-yhteyksiä.

Palomuurin ottaminen käyttöön:

1. Toimi McAfee SecurityCenter -ikkunassa seuraavasti:
   - Valitse **Internet ja verkko** ja sitten **Määritä**.
   - Valitse **Lisävalikko**, sitten **Koti**-valikosta **Määritä** ja lopuksi **Internet ja verkko**.
2. **Internet- ja verkkomääritykset** -ikkunassa, kohdan **Palomuurisuojaus** alla, paina **Käytössä**.

Pysäytä palomuurisuojaus

Palomuurisuojauksen poistaminen käytöstä saattaa tietokoneen alttiiksi tietomurroille ja ei-toivotulle tietoliikenteelle. Jos palomuurisuojausta ei ole otettu käyttöön, et voi hallita saapuvia ja lähteviä Internet-yhteyksiä.

Palomuurin poistaminen käytöstä:

1 Toimi McAfee SecurityCenter -ikkunassa seuraavasti:

- Valitse **Internet ja verkko** ja sitten **Määritä**.
- Valitse **Lisävalikko**, sitten **Koti**-valikosta **Määritä** ja lopuksi **Internet ja verkko**.

2 **Internet- ja verkkomääritykset** -ikkunassa, kohdan **Palomuurisuojaus** alla, paina **Ei käytössä**.

Hälytysten käsitteleminen

Firewall käyttää erilaisia hälytyksiä auttaakseen sinua hallitsemaan tietoturvaa. Nämä hälytykset voidaan jakaa neljään pääryhmään:

- Estetty troijalainen -hälytys
- Punainen hälytys
- Keltainen hälytys
- Vihreä hälytys

Hälytyksissä on myös tietoja, jotka auttavat käyttäjää päättämään, miten hälytyksiä pitää käsitellä, tai miten tietokoneessa käytettävistä ohjelmista voi saada tietoja.

Tietoja hälytyksistä

Firewallissa on neljä perushälytystyyppiä. Joissakin hälytyksissä on myös tietoja, jotka helpottavat tietokoneessa suoritettavien ohjelmien käytön oppimista tai niihin liittyvien tietojen hankkimista.

Estetty troijalainen -hälytys

Troijan hevonen näyttää luvalliselta ohjelmalta, mutta se voi aiheuttaa tietokoneelle vahinkoa tai sallia tietokoneen luvattoman käytön. Firewall antaa troijalaishälytyksen, kun se havaitsee ja estää tietokoneessa olevan Troijan hevosen ja suosittelee tietokoneen tarkistamista uusien uhkien välttämiseksi. Tämä hälytys esiintyy jokaisella tietoturvatasolla, Avoin-tasoa lukuun ottamatta. Hälytystä ei esiinny, jos suositukset on poistettu käytöstä.

Punainen hälytys

Yleisin hälytystyyppi on punainen hälytys, joka vaatii yleensä vastausta käyttäjältä. Firewall ei joissakin tapauksissa pysty määrittämään ohjelma- tai verkkotapahtumille sopivaa toimenpidettä, joten hälytys kuvailee ensin kyseiset ohjelma- tai verkkotapahtumat ja antaa sitten yhden tai useamman vaihtoehdon, joihin käyttäjän on vastattava. Jos suositukset on otettu käyttöön, ohjelmat lisätään Ohjelmien käyttöoikeudet -ikkunaan.

Seuraavat hälytysten kuvaukset ovat kaikkein yleisimmät:

- **Ohjelma pyytää lupaa muodostaa yhteys Internetiin**: Firewall havaitsee ohjelman, joka yrittää muodostaa yhteyden Internetiin.
- **Ohjelmaa on muokattu**: Firewall havaitsee ohjelman, joka on muuttunut jollakin tavalla, ehkä online-päivityksen seurauksena.
- **Ohjelma on estetty**: Firewall estää ohjelman, sillä se on Ohjelmien käyttöoikeudet -ikkunan luettelossa.

Vaihtoehdot vaihtelevat asetusten ja ohjelma- tai verkkotapahtumien mukaan, mutta niistä yleisimmät ovat seuraavat:

- **Myönnä käyttöoikeudet**: Myönnä tietokoneessa olevalle ohjelmalle oikeudet käyttää Internetiä. Sääntö lisätään Ohjelmien käyttöoikeudet -sivulle.
- **Myönnä lupa muodostaa yhteys vain tällä kertaa**: Myönnä tietokoneessa olevalle ohjelmalle väliaikaiset oikeudet käyttää Internetiä. Uuden ohjelman asentaminen voi vaatia yhteyden muodostamista vain kerran.

- **Estä käyttöoikeudet**: Estä ohjelmaa käyttämästä Internetiä.
- **Myönnä vain lähtevien yhteyksien käyttöoikeudet**: Myönnä vain lähtevä Internet-yhteys. Tämä hälytys esiintyy yleensä silloin, kun tietoturvatasoksi on asetettu Tiukka tai Vaikeasti havaittava.
- **Luota tähän verkkoon**: Salli verkosta saapuva ja lähtevä tietoliikenne. Verkko lisätään Luotettavat IP-osoitteet -kohtaan.
- **Älä luota tähän verkkoon tällä kertaa**: Estä verkosta saapuva ja lähtevä tietoliikenne.

Keltainen hälytys

Keltainen hälytys on ei-kriittinen ilmoitus Firewallin havaitsemasta verkkotapahtumasta. Esimerkiksi **Havaittiin uusi verkko** -hälytys ilmestyy näyttöön, kun Firewall suoritetaan ensimmäisen kerran tai kun tietokone, johon Firewall on asennettu, liitetään uuteen verkkoon. Voit itse päättää, haluatko luottaa verkkoon vai et. Jos verkkoon luotetaan, Firewall sallii tietoliikenteen kaikista muista verkossa olevista tietokoneista, ja verkko lisätään luotettavien IP-osoitteiden luetteloon.

Vihreä hälytys

Useimmissa tapauksissa vihreä hälytys antaa perustietoja tapahtumasta, ja se ei vaadi käyttäjältä vastausta. Vihreitä hälytyksiä esiintyy tavallisesti silloin, kun tietoturvatasoksi on asetettu Normaali, Tiukka, Vaikeasti havaittava tai Lukitus. Vihreiden hälytysten kuvaukset ovat seuraavat:

- **Ohjelmaa on muokattu**: Ilmoittaa, että ohjelmaa, jolle olet aikaisemmin myöntänyt oikeudet käyttää Internetiä, on muokattu. Voit halutessasi estää ohjelman, mutta jos et vastaa, hälytys katoaa työpöydältä ja ohjelman käyttöoikeudet säilyvät.
- **Ohjelmalle on myönnetty lupa muodostaa yhteys Internetiin**: Ilmoittaa, että ohjelmalle on myönnetty lupa muodostaa yhteys Internetiin. Voit halutessasi estää ohjelman, mutta jos et vastaa, hälytys katoaa ja ohjelma jatkaa Internetin käyttöä.

Käyttäjätuki

Monissa Firewallin hälytyksissä on lisätietoja, jotka auttavat sinua hallitsemaan tietokoneen tietoturvaa. Niihin kuuluvat muun muassa seuraavat:

- **Lisää tietoja tästä ohjelmasta**: Avaa McAfeen maailmanlaajuinen tietoturvaa käsittelevä Web-sivusto, jos haluat saada lisätietoja ohjelmasta, jonka Firewall on havainnut tietokoneessa.

- **Kerro McAfeelle tästä ohjelmasta**: Lähetä McAfeelle tietoja tuntemattomasta tiedostosta, jonka Firewall on havainnut tietokoneessa.
- **McAfee suosittelee**: Hälytysten käsittelyyn liittyviä neuvoja. Hälytys voi esimerkiksi suositella, että myönnät ohjelmalle käyttöoikeudet.

Tiedottavien hälytysten hallinta

Firewall antaa mahdollisuuden tiedottavien hälytysten näyttämiseen tai piilottamiseen tiettyjen tapahtumien aikana.

Näytä hälytykset pelaamisen aikana

Oletusarvoisesti Firewall estää tiedottavia hälytyksiä ilmestymästä näyttöön koko näytön tilassa pelattaessa. Voit kuitenkin määrittää Firewallin asetukset siten, että Firewall näyttää tiedottavat hälytykset pelaamisen aikana, kun se havaitsee tietomurtoyrityksen tai muuta epäilyttävää toimintaa.

Hälytysten näyttäminen pelaamisen aikana:

1. Valitse Yleiset tehtävät -ikkunasta **Lisävalikko**.
2. Valitse **Määritä**.
3. Valitse SecurityCenter-asetusikkunasta **Hälytykset**.
4. Valitse **Lisäasetukset**.
5. Valitse **Hälytysasetukset**-ikkunasta **Näytä tiedottavat hälytykset, kun tietokoneen havaitaan olevan pelitilassa**.

Piilota tiedottavat hälytykset

Tiedottavat hälytykset ilmoittavat tapahtumista, jotka eivät vaadi välitöntä huomiota.

Tiedottavien hälytysten piilottaminen:

1. Valitse Yleiset tehtävät -ikkunasta **Lisävalikko**.
2. Valitse **Määritä**.
3. Valitse SecurityCenter-asetusikkunasta **Hälytykset**.
4. Valitse **Lisäasetukset**.
5. Valitse **SecurityCenter-asetukset**-ikkunasta **Tiedottavat hälytykset**.
6. Toimi **Tiedottavat hälytykset** -ikkunassa seuraavasti:
   - Valitse piilotettava hälytystyyppi.
   - Piilota tiedottavat hälytykset valitsemalla **Piilota tiedottavat hälytykset**.
7. Valitse **OK**.

LUKU 19

Palomuurisuojauksen asetusten määrittäminen

Firewall tarjoaa useita tapoja hallita tietoturvaa ja mukauttaa tietoturvatapahtumiin ja hälytyksiin vastaamisen tapaa.

Kun asennat Firewallin ensimmäisen kerran, tietoturvatasoksi asetetaan Normaali. Tämä riittää turvaamaan useimpien käyttäjien tietoturvaa koskevat vaatimukset. Firewallissa on kuitenkin myös muita tasoja, jotka vaihtelevat erittäin rajoittavista erittäin salliviin.

Halutessasi voit saada Firewallissa myös hälytyksiin ja ohjelmien Internet-käyttöön liittyviä suosituksia.

Tässä luvussa

Firewallin tietoturvatasojen hallinta

Voit määrittää tietoturvatasojen asetukset ja päättää, kuinka paljon haluat hallita palomuuria ja vastata hälytyksiin, kun Firewall havaitsee ei-toivottua tietoliikennettä sekä saapuvia ja lähteviä Internet-yhteyksiä. Oletusarvoisesti käytössä on Normaali-tietoturvataso.

Kun Normaali-tietoturvataso on asetettu ja suositukset on otettu käyttöön, punaiset hälytykset antavat mahdollisuuden myöntää käyttöoikeudet tuntemattomille ja muutetuille ohjelmille tai estää ne. Kun palomuuri havaitsee tunnettuja ohjelmia, näyttöön ilmestyy vihreitä tiedottavia hälytyksiä ja käyttöoikeudet myönnetään automaattisesti. Käyttöoikeuksien myöntäminen sallii ohjelman muodostaa lähteviä yhteyksiä ja kuunnella pyytämättömiä saapuvia yhteyksiä.

Yleisesti voidaan sanoa, että rajoittavien tietoturvatasojen (Vaikeasti havaittava ja Tiukka) kohdalla käytetään enemmän asetuksia ja näytetään enemmän hälytyksiä, joihin käyttäjän on vastattava.

Firewallissa on kuusi tietoturvatasoa. Rajoittavimmasta vähiten rajoittavaan nämä tasot ovat seuraavat:

- **Lukitus**: Estää kaikki Internet-yhteydet.
- **Vaikeasti havaittava**: Estää kaikki saapuvat Internet-yhteydet.
- **Tiukka**: Hälytykset kehottavat sinua vastaamaan jokaiseen saapuvaan ja lähtevään Internet-yhteyspyyntöön.
- **Normaali**: Antaa hälytyksen, kun tuntemattomat tai uudet ohjelmat pyytävät oikeuksia Internetin käyttöön.
- **Luottava**: Sallii kaikki saapuvat ja lähtevät Internet-yhteydet ja lisää ne automaattisesti Ohjelmien käyttöoikeudet -ikkunaan.
- **Avoin**: Sallii kaikki saapuvat ja lähtevät Internet-yhteydet.

Firewall antaa sinulle myös mahdollisuuden palauttaa tietoturvataso välittömästi normaaliksi Palauta palomuurisuojauksen oletusasetukset -ikkunassa.

Aseta tietoturvatasoksi Lukitus

Palomuurin tietoturvatason asettaminen Lukitus-tilaan estää kaikki saapuvat ja lähtevät verkkoyhteydet, mukaan lukien yhteydet Web-sivustoihin, sähköpostiin ja tietoturvapäivityksiin. Tällä tietoturvatasolla on sama vaikutus kuin Internet-yhteyden katkaisemisella. Tällä asetuksella voit estää portit, jotka olet valinnut avattaviksi Järjestelmäpalvelut-ikkunassa. Lukitus-tilassa hälytykset voivat edelleen kehottaa sinua estämään ohjelmia.

Palomuurin tietoturvatason asettaminen Lukitus-tilaan:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Siirrä Tietoturvataso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Lukitus**.
3. Valitse **OK**.

Aseta tietoturvatasoksi Vaikeasti havaittava

Palomuurin tietoturvatason asettaminen Vaikeasti havaittava -tilaan estää avoimia portteja lukuun ottamatta kaikki saapuvat yhteydet. Tämä asetus piilottaa tietokoneen Internetissä kokonaan. Kun tietoturvatasoksi on asetettu Vaikeasti havaittava, palomuuri hälyttää, kun uudet ohjelmat yrittävät muodostaa lähteviä Internet-yhteyksiä tai saavat saapuvia yhteyspyyntöjä. Estetyt ja lisätyt ohjelmat näkyvät Ohjelmien käyttöoikeudet -ikkunassa.

Palomuurin tietoturvatason asettaminen Vaikeasti havaittava -tilaan:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Siirrä Tietoturvataso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Vaikeasti havaittava**.
3. Valitse **OK**.

Aseta tietoturvatasoksi Tiukka

Kun tietoturvatasoksi on asetettu Tiukka, palomuuri ilmoittaa, kun uudet ohjelmat yrittävät muodostaa lähteviä Internet-yhteyksiä tai saavat saapuvia yhteyspyyntöjä. Estetyt ja lisätyt ohjelmat näkyvät Ohjelmien käyttöoikeudet -ikkunassa. Kun tietoturvatasoksi on asetettu Tiukka, ohjelma pyytää vain kulloinkin tarvittavaa käyttöoikeutta, esimerkiksi oikeutta vain lähtevään tietoliikenteeseen, jonka voit myöntää tai estää. Jos ohjelma tarvitsee myöhemmin sekä saapuvaa että lähtevää yhteyttä, voit myöntää ohjelmalle täydet käyttöoikeudet Ohjelmien käyttöoikeudet -ikkunassa.

Palomuurin tietoturvatason asettaminen Tiukka-tilaan:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Siirrä Tietoturvataso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Tiukka**.
3. Valitse **OK**.

Aseta tietoturvatasoksi Normaali

Normaali on oletusarvoinen ja suositeltu tietoturvataso.

Kun palomuurin tietoturvatasoksi asetetaan Normaali, Firewall valvoo saapuvia ja lähteviä yhteyksiä ja hälyttää, kun uudet ohjelmat yrittävät käyttää Internetiä. Estetyt ja lisätyt ohjelmat näkyvät Ohjelmien käyttöoikeudet -ikkunassa.

Palomuurin tietoturvatason asettaminen Normaali-tilaan:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Siirrä Tietoturvataso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Normaali**.
3. Valitse **OK**.

Aseta tietoturvatasoksi Luottava

Palomuurin tietoturvatason asettaminen Luottava-tilaan sallii kaikki saapuvat ja lähtevät yhteydet. Luottava-tilassa palomuuri myöntää automaattisesti käyttöoikeudet kaikille ohjelmille ja lisää ne Ohjelmien käyttöoikeudet -ikkunan sallittujen ohjelmien luetteloon.

Palomuurin tietoturvatason asettaminen Luottava-tilaan:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Siirrä Tietoturvataso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Luottava**.
3. Valitse **OK**.

Hälytyksiin liittyvien suositusten asetusten määrittäminen

Voit määrittää, miten haluat Firewallin hälyttävän ohjelmista, jotka yrittävät muodostaa Internet-yhteyden. Firewall voi lisätä suosituksia hälytyksiin, jättää ne pois tai näyttää ne.

Suositusten ottaminen käyttöön auttaa sinua päättämään, miten hälytyksiä kannattaa käsitellä. Kun suositukset on otettu käyttöön (ja tietoturvatasoksi on asetettu Normaali), Firewall myöntää tai estää tunnettujen ohjelmien käyttöoikeudet sekä hälyttää ja antaa toimenpidesuosituksia, kun se kohtaa tuntemattomia ja mahdollisesti vaarallisia ohjelmia.

Kun suositukset on poistettu käytöstä, Firewall ei automaattisesti myönnä tai estä Internetin käyttöä eikä se myöskään anna toimenpidesuosituksia.

Kun Firewallin asetukset on määritetty siten, että suositukset ainoastaan näytetään, hälytys kehottaa sinua myöntämään tai estämään käyttöoikeudet, mutta se antaa toimenpidesuosituksen.

Ota suositukset käyttöön

Suositusten ottaminen käyttöön auttaa sinua päättämään, miten hälytyksiä kannattaa käsitellä. Kun suositukset on otettu käyttöön, Firewall myöntää tai estää ohjelmien käyttöoikeudet automaattisesti ja hälyttää tunnistamattomista ja mahdollisesti vaarallisista ohjelmista.

Suositusten ottaminen käyttöön:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Tietoturvataso-ikkunan **Suositukset**-kohdasta **Ota suositukset käyttöön**.
3. Valitse **OK**.

Poista suositukset käytöstä

Kun poistat suositukset käytöstä, et enää saa hälytysten käsittelyä ja ohjelmien käyttöoikeuksien hallintaa helpottavia hälytyksiä. Jos suositukset poistetaan käytöstä, Firewall jatkaa ohjelmien käyttöoikeuksien myöntämistä ja estämistä sekä hälyttää tunnistamattomista ja mahdollisesti vaarallisista ohjelmista. Jos Firewall havaitsee uuden ohjelman, jota se pitää epäilyttävänä tai jonka tiedetään olevan mahdollisesti vaarallinen, se estää automaattisesti ohjelmaa käyttämästä Internetiä.

Suositusten poistaminen käytöstä:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Tietoturvataso-ikkunan **Suositukset**-kohdasta **Poista suositukset käytöstä**.
3. Valitse **OK**.

Näytä vain suositukset

Suositusten näyttäminen auttaa sinua päättämään, miten tunnistamattomia ja mahdollisesti vaarallisia ohjelmia koskevia hälytyksiä kannattaa käsitellä. Kun suositusten arvoksi on asetettu **Vain näyttö**, palomuuri näyttää hälytysten käsittelemistä koskevia tietoja, mutta toisin kuin **Ota suositukset käyttöön** -asetusta käytettäessä, suosituksia ei oteta automaattisesti käyttöön eikä ohjelman käyttöoikeuksia myönnetä tai estetä automaattisesti. Sen sijaan hälytykset toimivat suosituksina, jotka auttavat sinua päättämään ohjelmien käyttöoikeuksien myöntämisestä tai estämisestä.

Vain suositusten näyttäminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Tietoturvataso-ikkunan **Suositukset**-kohdasta **Vain näyttö**.
3. Valitse **OK**.

Firewallin suojauksen optimointi

Tietokoneen suojaus voi pettää monesta syystä. Jotkin ohjelmat voivat esimerkiksi yrittää muodostaa Internet-yhteyden ennen Windowsin® käynnistymistä. Taitavat tietokoneen käyttäjät voivat myös lähettää ping-pyynnön tietokoneellesi määrittääkseen, onko tietokoneesi verkossa. Firewallin avulla voit puolustautua molempia tietomurtoyrityksiä vastaan sallimalla käynnistyssuojauksen käyttöönoton ja estämällä ICMP ping -pyynnöt. Ensimmäinen asetus estää ohjelmia pääsemästä Internetiin Windowsin käynnistyessä ja toinen estää ping-pyynnöt, jotka auttavat muita käyttäjiä havaitsemaan tietokoneesi verkossa.

Vakioasennusasetuksiin kuuluu yleisimpien tietomurtoyritysten, kuten palvelunestohyökkäysten ja tietoturva-aukkojen, automaattinen havaitseminen. Käyttämällä vakioasennusasetuksia varmistut, että olet suojassa näiltä hyökkäyksiltä ja tarkistuksilta. Tietomurtojen havainnointi -ikkunassa voit kuitenkin poistaa yhden tai usean hyökkäyksen tai tarkistuksen automaattisen havaitsemisen.

Suojaa tietokonetta käynnistyksen aikana

Firewall pystyy suojaamaan tietokonetta Windowsin käynnistyessä. Käynnistyssuojaus estää kaikki uudet ohjelmat, jotka vaativat käyttöoikeutta Internetiin, mutta joille ei ole sitä aikaisemmin myönnetty. Kun Firewall on käynnistynyt, se näyttää niitä ohjelmia koskevat hälytykset, jotka pyysivät Internetin käyttöoikeuksia käynnistyksen aikana. Voit tällöin päättää niiden myöntämisestä tai estämisestä. Jos haluat käyttää tätä toimintoa, tietoturvatason asetukseksi on valittava jokin muu kuin Avoin tai Lukitus.

Tietokoneen suojaaminen käynnistyksen aikana:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Tietoturvataso-ikkunan Suojausasetukset-kohdasta **Salli käynnistyssuojaus**.
3. Valitse **OK**.

Huomaa: Estettyjä yhteyksiä ja tietomurtoja ei kirjata, jos käynnistyssuojaus on käytössä.

Määritä ping-pyyntöjen asetukset

ICMP-kaiutuspyyntöviestejä lähettävän ja vastaanottavan ping-työkalun avulla tietokoneen käyttäjät voivat määrittää, onko jokin tietty tietokone liitetty verkkoon. Voit määrittää Firewallin asetukset estämään tai sallimaan tietokoneen käyttäjien lähettämät ping-pyynnöt.

ICMP ping -pyyntöjen asetusten määrittäminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Toimi Tietoturvataso-ikkunan **Tietoturva-asetukset**-kohdassa seuraavasti:
   - Valitse **Salli ICMP ping -pyynnöt**, jos haluat sallia verkossa olevan tietokoneen havaitsemisen ping-pyyntöjen avulla.
   - Poista **Salli ICMP ping -pyynnöt** -kohdan valinta, jos haluat estää verkossa olevan tietokoneen havaitsemisen ping-pyyntöjen avulla.
3. Valitse **OK**.

Määrittele tietomurtojen havainnoinnin asetukset

Tietomurtojen havainnointi (IDS) valvoo datapaketteja epäilyttävien datansiirtojen tai siirtomenetelmien varalta. IDS analysoi tietoliikennettä ja datapaketteja ja pyrkii löytämään niistä hyökkääjien tietoliikenteeseen viittaavaa toimintaa. Esimerkiksi kun Firewall havaitsee ICMP-paketteja, se analysoi ne epäilyttävän tietoliikenteen varalta vertailemalla ICMP-liikennettä tunnettuihin hyökkäysmalleihin. Firewall vertaa paketteja allekirjoitustietokantaan ja jos se pitää paketteja epäilyttävinä tai vaarallisina, se poistaa ne loukkaavasta tietokoneesta sekä mahdollisesti kirjaa tapahtuman.

Vakioasennusasetuksiin kuuluu yleisimpien tietomurtoyritysten, kuten palvelunestohyökkäysten ja tietoturva-aukkojen, automaattinen havaitseminen. Käyttämällä vakioasennusasetuksia varmistut, että olet suojassa näiltä hyökkäyksiltä ja tarkistuksilta. Tietomurtojen havainnointi -ikkunassa voit kuitenkin poistaa yhden tai usean hyökkäyksen tai tarkistuksen automaattisen havaitsemisen.

Tietomurtojen havainnoinnin asetusten määrittäminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Tietomurtojen havainnointi**.
3. Toimi **Havaitse tietomurtoyritykset** -kohdassa seuraavasti:
   - Valitse nimi hyökkäyksen automaattista havainnointia tai tarkistamista varten.
   - Poista nimi, jos haluat poistaa hyökkäyksen automaattisen havainnoinnin tai tarkistuksen käytöstä.
4. Valitse **OK**.

Määritä Firewallin suojauksen tilan asetukset

SecurityCenter jäljittää ongelmat, jotka liittyvät tietokoneen yleisen suojauksen tilaan. Voit kuitenkin määrittää Firewallin asetukset siten, että se ohittaa tietyt tietokoneeseen liittyvät ongelmat, jotka voivat vaikuttaa suojauksen tilaan. Voit määrittää SecurityCenterin asetukset siten, että se ohittaa ongelmat, kun Firewallin tietoturva-asetukseksi on asetettu Avoin, kun Firewall-palvelu ei ole käytössä tai kun tietokoneeseen ei ole asennettu vain lähtevää tietoliikennettä valvovaa palomuuria.

Firewallin suojauksen tilan asetusten määrittäminen

1. Valitse Yleiset tehtävät -ikkunasta **Lisävalikko**.
2. Valitse **Määritä**.
3. Valitse SecurityCenter-asetusikkunasta **Hälytykset**.
4. Valitse **Lisäasetukset**.
5. Valitse Yleiset tehtävät -ikkunasta **Lisävalikko**.
6. Valitse **Määritä**.
7. Valitse SecurityCenter-asetukset-ikkunasta **Suojauksen tila**.
8. Valitse Lisäasetukset.
9. Valitse Ohitetut ongelmat -ikkunasta yksi tai useampi seuraavista vaihtoehdoista:
   - **Palomuurin suojaustasoksi on määritetty Avoin.**
   - **Palomuuripalvelu ei ole käytössä.**
   - **Lähtevää palomuuria ei ole asennettu tietokoneeseen.**
10. Valitse **OK**.

Firewallin lukitseminen ja palauttaminen

Lukitus on hyödyllinen ominaisuus käyttäjille, jotka käsittelevät tietokoneeseen liittyviä hätätapauksia, joiden on estettävä kaikki tietoliikenne tietokoneessa olevien ongelmien eristämiseksi ja määrittämiseksi tai jotka ovat epävarmoja ja joiden on selvitettävä, miten ohjelman Internet-käyttöä hallitaan.

Lukitse Firewall välittömästi

Firewallin lukitseminen estää kaiken saapuvan ja lähtevän Internet-tietoliikenteen välittömästi. Se estää etäyhteyden muodostamisen tietokoneeseesi ja estää kaikkia tietokoneesi ohjelmia muodostamasta Internet-yhteyksiä.

Firewallin välitön lukitseminen ja kaiken tietoliikenteen estäminen:

1. Ota **Perusvalikko** tai **Lisävalikko** käyttöön ja valitse Koti- tai Yleiset tehtävät -ikkunasta **Lukitse palomuuri**.
2. Valitse Lukitse palomuuri -ikkunasta **Lukitus**.
3. Valitse valintaikkunasta **Kyllä** ja vahvista, että haluat estää kaiken saapuvan ja lähtevän tietoliikenteen välittömästi.

Firewallin lukituksen poistaminen välittömästi

Firewallin lukitseminen estää kaiken saapuvan ja lähtevän Internet-tietoliikenteen välittömästi. Se estää etäyhteyden muodostamisen tietokoneeseesi ja estää kaikkia tietokoneesi ohjelmia muodostamasta Internet-yhteyksiä. Kun olet lukinnut Firewallin, voit avata sen lukituksen tietoliikenteen sallimiseksi.

Firewallin lukituksen välitön avaaminen ja kaiken tietoliikenteen salliminen:

1. Ota **Perusvalikko** tai **Lisävalikko** käyttöön ja valitse Koti- tai Yleiset tehtävät -ikkunasta **Lukitse palomuuri**.
2. Valitse Lukitse palomuuri -ikkunasta **Poista lukitus**.
3. Valitse valintaikkunasta **Kyllä** ja vahvista, että haluat poistaa Firewallin lukituksen ja sallia tietoliikenteen.

Palauta Firewallin asetukset

Voit palauttaa Firewallin alkuperäiset suojausasetukset nopeasti. Oletusasetusten palauttaminen asettaa tietoturvatasoksi normaalin, ottaa suositukset käyttöön, tyhjentää luotettavien ja estettyjen IP-osoitteiden luettelot ja poistaa kaikki ohjelmat Ohjelmien käyttöoikeudet -ikkunasta.

Firewallin alkuperäisten asetusten palauttaminen:

1. Ota **Perusvalikko** tai **Lisävalikko** käyttöön ja valitse Koti- tai Yleiset tehtävät -ikkunasta **Palauta palomuurin oletusasetukset**.
2. Valitse Palauta palomuurin oletusasetukset -ikkunasta **Palauta oletusasetukset**.
3. Valitse Palauta palomuurin oletusasetukset -ikkunasta **Kyllä** ja vahvista, että haluat palauttaa palomuurin oletusasetukset.

Aseta tietoturvatasoksi Avoin

Palomuurin tietoturvatason asettaminen Avoin-tilaan sallii palomuurin myöntää käyttöoikeudet kaikille saapuville ja lähteville yhteyksille. Jos haluat myöntää käyttöoikeudet aikaisemmin estetyille ohjelmille, käytä Ohjelmien käyttöoikeudet -ikkunaa.

Palomuurin tietoturvatason asettaminen Avoin-tilaan:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Siirrä Tietoturvataso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Avoin**.
3. Valitse **OK**.

Huomaa: Aikaisemmin estettyjen ohjelmien estoa jatketaan, kun palomuurin tietoturvatasoksi asetetaan **Avoin**. Jos haluat estää tämän, voit muuttaa ohjelman säännöksi **Täydet käyttöoikeudet**.

LUKU 20

Ohjelmien ja käyttöoikeuksien hallinta

Firewallin avulla voit luoda käyttöoikeuksia nykyisille ja uusille ohjelmille, jotka vaativat saapuvia ja lähteviä Internet-yhteyksiä, ja hallita niitä. Firewallin avulla ohjelmille voidaan myöntää täydelliset tai vain lähtevän tietoliikenteen sallivat käyttöoikeudet. Ohjelmien käyttöoikeudet voidaan myös estää.

Tässä luvussa

Internet-käyttöoikeuden myöntäminen ohjelmille

Jotkin ohjelmat, kuten Internet-selaimet, vaativat Internet-käyttöoikeutta toimiakseen kunnolla.

Firewallin Ohjelmien käyttöoikeudet -sivulla voit

- myöntää ohjelmille käyttöoikeudet
- myöntää ohjelmille vain lähtevän tietoliikenteen käyttöoikeudet
- estää ohjelmien käyttöoikeudet.

Voit myöntää ohjelmille täydelliset tai vain lähtevän tietoliikenteen käyttöoikeudet myös lähtevien ja äskettäisten tapahtumien lokeista.

Myönnä ohjelmalle täydet käyttöoikeudet

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Personal Firewallissa on luettelo ohjelmista, joille myönnetään automaattisesti täydet käyttöoikeudet, mutta näitä käyttöoikeuksia voi muuttaa.

Täysien Internet-käyttöoikeuksien myöntäminen ohjelmalle:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
3. Valitse **Ohjelmien käyttöoikeudet** -kohdasta ohjelma, jonka asetuksena on **Estetty** tai **Vain lähtevien yhteyksien käyttöoikeudet**.
4. Valitse **Toiminto**-kohdasta **Myönnä täydet käyttöoikeudet**.
5. Valitse **OK**.

Myönnä uudelle ohjelmalle täydet käyttöoikeudet

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Firewallissa on luettelo ohjelmista, joille myönnetään automaattisesti täydet käyttöoikeudet, mutta voit lisätä myös uuden ohjelman ja muuttaa sen käyttöoikeuksia.

Täysien Internet-käyttöoikeuksien myöntäminen uudelle ohjelmalle:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse **Firewall**-ikkunasta **Ohjelmien käyttöoikeudet**.
3. Valitse **Ohjelmien käyttöoikeudet** -kohdasta **Lisää sallittu ohjelma**.
4. Hae ja valitse **Lisää ohjelma** -kohdasta ohjelma, jonka haluat lisätä.
5. Valitse **Avaa**.
6. Valitse **OK**.

   Juuri lisätty ohjelma ilmestyy **Ohjelmien käyttöoikeudet** -kohtaan.

Huomaa: Voit muuttaa juuri lisätyn ohjelman käyttöoikeuksia samalla tavalla kuin nykyisen ohjelman käyttöoikeuksia: valitse ohjelma ja sitten **Toiminto**-kohdasta **Myönnä vain lähtevien yhteyksien käyttöoikeudet** tai **Estä käyttöoikeudet**.

Myönnä täydet käyttöoikeudet äskettäisten tapahtumien lokista

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Voit valita ohjelman äskettäisten tapahtumien lokista ja myöntää sille täydet oikeudet Internetin käyttöön.

Täysien käyttöoikeuksien myöntäminen ohjelmalle äskettäisten tapahtumien lokista:

1. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse ensin tapahtuman kuvaus Äskettäiset tapahtumat -ikkunasta ja sitten **Myönnä täydet käyttöoikeudet**.
3. Valitse Ohjelmien käyttöoikeudet -valintaikkunasta **Kyllä** ja vahvista, että haluat myöntää ohjelmalle täydet käyttöoikeudet.

Vastaavat aiheet

- Tarkastele lähteviä tapahtumia (sivu 166)

Myönnä täydet käyttöoikeudet lähtevien tapahtumien lokista

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Voit valita ohjelman lähtevien tapahtumien lokista ja myöntää sille täydet oikeudet Internetin käyttöön.

Täysien Internet-käyttöoikeuksien myöntäminen ohjelmalle lähtevien tapahtumien lokista:

1. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
3. Valitse **Internet & verkko** ja valitse sitten **Lähtevät tapahtumat**.
4. Valitse ensin Lähtevät tapahtumat -ikkunasta IP-lähdeosoite ja sitten **Myönnä käyttöoikeudet**.
5. Valitse Ohjelmien käyttöoikeudet -valintaikkunasta **Kyllä** ja vahvista, että haluat myöntää ohjelmalle täydet oikeudet Internetin käyttöön.

Vastaavat aiheet

- Tarkastele lähteviä tapahtumia (sivu 166)

Vain lähtevän tietoliikenteen käyttöoikeuksien myöntäminen

Jotkin tietokoneeseen asennetut ohjelmat vaativat vain lähteviä Internet-yhteyksiä. Firewallin avulla voit myöntää ohjelmille vain lähtevän tietoliikenteen käyttöoikeudet.

Myönnä ohjelmalle vain lähtevän tietoliikenteen käyttöoikeudet

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Personal Firewallissa on luettelo ohjelmista, joille myönnetään automaattisesti täydet käyttöoikeudet, mutta näitä käyttöoikeuksia voi muuttaa.

Vain lähtevän tietoliikenteen sallivien oikeuksien myöntäminen ohjelmalle:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
3. Valitse **Ohjelmien käyttöoikeudet** -kohdasta ohjelma, jonka asetuksena on **Estetty** tai **Täydet käyttöoikeudet**.
4. Valitse **Toiminto**-kohdasta **Myönnä vain lähtevien yhteyksien käyttöoikeudet**.
5. Valitse **OK**.

Myönnä vain lähtevän tietoliikenteen oikeudet äskettäisten tapahtumien lokista

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Voit valita ohjelman äskettäisten tapahtumien lokista ja myöntää sille oikeudet vain lähtevien Internet-yhteyksien käyttöön.

Vain lähtevän tietoliikenteen käyttöoikeuksien myöntäminen ohjelmalle äskettäisten tapahtumien lokista:

1. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse ensin tapahtuman kuvaus Äskettäiset tapahtumat -ikkunasta ja sitten **Myönnä vain lähtevien yhteyksien käyttöoikeudet**.
3. Valitse Ohjelmien käyttöoikeudet -valintaikkunasta **Kyllä** ja vahvista, että haluat myöntää ohjelmalle vain lähtevän tietoliikenteen käyttöoikeudet.

Vastaavat aiheet

- Tarkastele lähteviä tapahtumia (sivu 166)

Myönnä vain lähtevän tietoliikenteen käyttöoikeudet lähtevien tapahtumien lokista

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Voit valita ohjelman lähtevien tapahtumien lokista ja myöntää sille oikeudet vain lähtevien Internet-yhteyksien käyttöön.

Vain lähtevän tietoliikenteen käyttöoikeuksien myöntäminen ohjelmalle lähtevien tapahtumien lokista:

1. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
3. Valitse **Internet & verkko** ja valitse sitten **Lähtevät tapahtumat**.
4. Valitse ensin Lähtevät tapahtumat -ikkunasta IP-lähdeosoite ja sitten **Myönnä vain lähtevien yhteyksien käyttöoikeudet**.
5. Valitse Ohjelmien käyttöoikeudet -valintaikkunasta **Kyllä** ja vahvista, että haluat myöntää ohjelmalle vain lähtevän tietoliikenteen käyttöoikeudet.

Vastaavat aiheet

- Tarkastele lähteviä tapahtumia (sivu 166)

Ohjelmien Internet-käyttöoikeuden estäminen

Firewall antaa sinulle mahdollisuuden estää ohjelmia käyttämästä Internetiä. Varmista, että ohjelman estäminen ei vaikuta häiritsevästi verkkoyhteyteen tai johonkin muuhun ohjelmaan, joka vaatii Internet-käyttöoikeutta toimiakseen kunnolla.

Estä ohjelman käyttöoikeudet

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Personal Firewallissa on luettelo ohjelmista, joille myönnetään automaattisesti täydet käyttöoikeudet, mutta nämä käyttöoikeudet voi estää.

Ohjelman Internet-käyttöoikeuksien estäminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
3. Valitse **Ohjelmien käyttöoikeudet** -kohdasta ohjelma, jonka asetuksena on **Täydet käyttöoikeudet** tai **Vain lähtevien yhteyksien käyttöoikeudet**.
4. Valitse **Toiminto**-kohdasta **Estä käyttöoikeudet**.
5. Valitse **OK**.

Estä uuden ohjelman käyttöoikeudet

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Personal Firewallissa on luettelo ohjelmista, joille myönnetään automaattisesti täydet käyttöoikeudet, mutta voit lisätä myös uuden ohjelman ja estää sitä käyttämästä Internetiä.

Uuden ohjelman Internet-käytön estäminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
3. Valitse **Ohjelmien käyttöoikeudet** -kohdasta **Lisää estetty ohjelma**.
4. Hae ja valitse **Lisää ohjelma** -kohdasta ohjelma, jonka haluat lisätä.
5. Valitse **Avaa**.
6. Valitse **OK**.

   Juuri lisätty ohjelma ilmestyy **Ohjelmien käyttöoikeudet** -kohtaan.

Huomaa: Voit muuttaa juuri lisätyn ohjelman käyttöoikeuksia samalla tavalla kuin nykyisen ohjelman käyttöoikeuksia: valitse ohjelma ja sitten **Toiminto**-kohdasta **Myönnä vain lähtevien yhteyksien käyttöoikeudet** tai **Myönnä täydet käyttöoikeudet**.

Estä käyttöoikeudet äskettäisten tapahtumien lokista

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Äskettäisten tapahtumien lokista voit kuitenkin halutessasi estää ohjelmia käyttämästä Internetiä.

Ohjelman käyttöoikeuksien estäminen äskettäisten tapahtumien lokista:

1. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse ensin tapahtuman kuvaus Äskettäiset tapahtumat -ikkunasta ja sitten **Estä käyttöoikeudet**.
3. Valitse Ohjelmien käyttöoikeudet -valintaikkunasta **Kyllä** ja vahvista, että haluat estää ohjelman.

Vastaavat aiheet

- Tarkastele lähteviä tapahtumia (sivu 166)

Ohjelmien käyttöoikeuksien poistaminen

Varmista ennen ohjelman käyttöoikeuksien poistamista, että tämä ei vaikuta tietokoneen toimintaan tai verkkoyhteyteen.

Poista ohjelman käyttöoikeudet

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Personal Firewallissa on luettelo ohjelmista, joille myönnetään automaattisesti täydet käyttöoikeudet, mutta voit myös poistaa automaattisesti ja manuaalisesti lisätyt ohjelmat.

Uuden ohjelman käyttöoikeuksien poistaminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
3. Valitse **Ohjelmien käyttöoikeudet** -kohdasta ohjelma.
4. Valitse **Toiminto**-kohdasta **Poista ohjelman käyttöoikeudet**.
5. Valitse **OK**.

   Ohjelma poistetaan Ohjelman käyttöoikeudet -ikkunasta.

Huomaa: Firewall estää muuttamasta joitakin ohjelmia himmentämällä tai poistamalla toimintoja käytöstä.

Perehtyminen ohjelmiin

Jos et ole varma, mitä ohjelmien käyttöoikeuksia kannattaa käyttää, McAfeen HackerWatch-sivustossa on päätöksen tekemistä helpottavia tietoja.

Hanki ohjelmatietoja

Monet tietokoneeseen asennetut ohjelmat vaativat saapuvia ja lähteviä Internet-yhteyksiä. Personal Firewallissa on luettelo ohjelmista, joille myönnetään automaattisesti täydet käyttöoikeudet, mutta näitä käyttöoikeuksia voi muuttaa.

Firewall voi auttaa sinua ohjelman Internet-käytön myöntämiseen tai estämiseen liittyvien päätösten tekemisessä. Varmista, että olet muodostanut Internet-yhteyden ja että selain käynnistää McAfeen HackerWatch-sivuston. Siinä on ajan tasalla olevia tietoja ohjelmista, Internet-käytön vaatimuksista ja tietoturvauhista.

Ohjelmatietojen hankkiminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
3. Valitse **Ohjelmien käyttöoikeudet** -kohdasta ohjelma.
4. Valitse **Toiminto**-kohdasta **Lisätietoja**.

Hae ohjelmatietoja lähtevien tapahtumien lokista

Personal Firewallin avulla voit hankkia tietoja lähtevien tietojen lokissa olevista ohjelmista.

Varmista ennen tietojen hankkimista, että sinulla on käytössäsi Internet-yhteys ja Internet-selain.

Ohjelmatietojen hankkiminen lähtevien tapahtumien lokista:

1. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
3. Valitse **Internet & verkko** ja valitse sitten **Lähtevät tapahtumat**.
4. Valitse ensin Lähtevät tapahtumat -ikkunasta IP-lähdeosoite ja sitten **Lisätietoja**.

   Voit tarkastella ohjelman tietoja HackerWatch-sivustossa. HackerWatch tarjoaa ajan tasalla olevia tietoja ohjelmista, Internet-käytön vaatimuksista ja tietoturvauhista.

Vastaavat aiheet

- Tarkastele lähteviä tapahtumia (sivu 166)

LUKU 21

Järjestelmäpalveluiden hallinta

Toimiakseen kunnolla tiettyjen ohjelmien (muun muassa Web-palvelinten ja tiedostonjakelupalvelinten ohjelmien) täytyy hyväksyä pyytämättömiä yhteyksiä muista tietokoneista tähän tarkoitukseen varattujen järjestelmäpalveluporttien kautta. Tavallisesti Firewall sulkee nämä järjestelmäpalveluportit, sillä järjestelmän haavoittuvuus johtuu useimmiten juuri niistä. Etätietokoneyhteydet edellyttävät kuitenkin, että nämä järjestelmäpalveluportit ovat auki.

Tämä luettelo esittää yleisten palveluiden käyttämät vakioportit.

- Tiedonsiirtoprotokolla (FTP), portit 20–21
- Postipalvelin (IMAP), portti 143
- Postipalvelin (POP3), portti 110
- Postipalvelin (SMTP), portti 25
- Microsoftin hakemistopalvelin (MSFT DS), portti 445
- Microsoftin SQL-palvelin (MSFT SQL), portti 1433
- Etätuki-/päätepalvelin (RDP), portti 3389
- Etäproseduurikutsut (RPC), portti 135
- Suojattu Web-palvelin (HTTPS), portti 443
- Universal Plug and Play (UPNP), portti 5000
- Web-palvelin (HTTP), portti 80
- Windows File Sharing (NETBIOS), portit 137–139

Tässä luvussa

Järjestelmäpalveluporttien asetusten määrittäminen

Tietokoneen palvelun etäkäyttö edellyttää palvelun ja siihen liittyvän avattavan portin määrittämistä. Valitse palvelu ja avaa portti vain silloin, kun olet varma, että portin täytyy olla auki. Portin avaaminen on vain harvoin tarpeellista.

Salli olemassa olevan järjestelmäpalveluportin käyttö

Järjestelmäpalvelut-ikkunasta voit avata tai sulkea olemassa olevan portin, niin että verkkopalvelun etäyhteys tietokoneeseesi sallitaan tai estetään. Avoin järjestelmäpalveluportti saattaa altistaa tietokoneen Internetin tietoturvauhille, joten avaa portti vain tarvittaessa.

Järjestelmäpalveluportin käytön salliminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Järjestelmäpalvelut**.
3. Valitse **Avaa järjestelmäpalveluportti** -kohdasta järjestelmäpalvelu portin avaamiseksi.
4. Valitse **OK**.

Estä olemassa olevan järjestelmäpalveluportin käyttö

Järjestelmäpalvelut-ikkunasta voit avata tai sulkea olemassa olevan portin, niin että verkkopalvelun etäyhteys tietokoneeseesi sallitaan tai estetään. Avoin järjestelmäpalveluportti saattaa altistaa tietokoneen Internetin tietoturvauhille, joten avaa portti vain tarvittaessa.

Järjestelmäpalveluportin käytön estäminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Järjestelmäpalvelut**.
3. Poista **Avaa järjestelmäpalveluportti** -kohdasta järjestelmäpalvelu portin sulkemiseksi.
4. Valitse **OK**.

Määritä uuden järjestelmäpalveluportin asetukset

Järjestelmäpalvelut-ikkunassa voit lisätä uuden järjestelmäpalveluportin, jonka avaamalla tai sulkemalla voit puolestaan sallia tai estää tietokoneen verkkopalvelun etäkäytön. Avattu järjestelmäpalveluportti voi saattaa tietokoneen alttiiksi Internetin tietoturvauhille, joten avaa portti vain silloin, kun se on välttämätöntä.

Uuden järjestelmäpalveluportin luominen ja sen asetusten määrittäminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Järjestelmäpalvelut**.
3. Valitse **Lisää**.
4. Määritä **Lisää porttikokoonpano** -kohdassa seuraavat:
   - ohjelman nimi
   - saapuvan liikenteen TCP/IP-portit
   - lähtevän liikenteen TCP/IP-portit
   - saapuvan liikenteen UDP-portit
   - lähtevän liikenteen UDP-portit.
5. Voit vaihtoehtoisesti myös kuvailla uuden kokoonpanon.
6. Valitse **OK**.

   Juuri määritetty järjestelmäpalveluportti ilmestyy **Avaa järjestelmäpalveluportti** -kohtaan.

Muokkaa järjestelmäpalveluporttia

Avattu tai suljettu portti sallii tai estää tietokoneen verkkopalvelun käytön. Järjestelmäpalvelut-ikkunassa voit muokata olemassa olevan portin saapuvia ja lähteviä tietoja. Jos portin tiedot annetaan virheellisesti, järjestelmäpalvelu ei toimi.

Järjestelmäpalveluportin muokkaaminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Järjestelmäpalvelut**.
3. Valitse järjestelmäpalvelu ja sitten **Muokkaa**.
4. Määritä **Lisää porttikokoonpano** -kohdassa seuraavat:
   - ohjelman nimi
   - saapuvan liikenteen TCP/IP-portit
   - lähtevän liikenteen TCP/IP-portit
   - saapuvan liikenteen UDP-portit

- lähtevän liikenteen UDP-portit.

5 Voit vaihtoehtoisesti myös kuvailla muokatun kokoonpanon.

6 Valitse **OK**.

Muokattu järjestelmäpalveluportti ilmestyy **Avaa järjestelmäpalveluportti** -kohtaan.

Poista järjestelmäpalveluportti

Avattu tai suljettu portti sallii tai estää tietokoneen verkkopalvelun käytön. Järjestelmäpalvelut-ikkunassa voit poistaa olemassa olevan portin ja siihen liittyvän järjestelmäpalvelun. Sen jälkeen, kun järjestelmäpalvelu on poistettu Järjestelmäpalvelut-ikkunasta, etätietokoneet eivät enää pääse käyttämään tietokoneen etäpalvelua.

Järjestelmäpalveluportin poistaminen:

1 Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.

2 Valitse Firewall-ikkunasta **Järjestelmäpalvelut**.

3 Valitse ensin järjestelmäpalvelu ja sitten **Poista**.

4 Valitse **Järjestelmäpalvelut**-valintaikkunasta **Kyllä** ja vahvista, että haluat poistaa järjestelmäpalvelun.

Järjestelmäpalveluportti ei enää näy Järjestelmäpalvelut-ikkunassa.

LUKU 22

Tietokoneyhteyksien hallinta

Voit määrittää Firewallin hallitsemaan tietokoneen etäyhteyksiä luomalla etätietokoneiden IP-osoitteisiin perustuvia sääntöjä. Tietokoneille, joiden IP-osoitteet ovat luotettavia, voidaan myöntää lupa muodostaa yhteys käyttäjän tietokoneeseen, kun taas tietokoneita, joiden IP-osoitteet ovat tuntemattomia, epäilyttäviä tai epäluotettavia, voidaan estää muodostamasta yhtes käyttäjän tietokoneeseen.

Kun sallit yhteyden, varmista, että tietokone, johon luotat, on turvallinen. Jos tietokone, johon luotat, on madon tai muun mekanismin tartuttama, voit tietokoneesi olla alttiina tartunnalle. McAfee suosittelee lisäksi, että luotat vain tietokoneisiin, jotka ovat palomuurin sekä ajantasaisen virustorjuntaohjelman suojaamia. Firewall ei kirjaa tietoliikennettä eikä luo tapahtumahälytyksiä luotettavien IP-osoitteiden luettelossa oleville IP-osoitteille.

Tietokoneita, joiden IP-osoite on tuntematon, epäilyttävä tai joka ei ole luetettava, voidaan estää ottamasta yhteyttä tietokoneeseesi

Koska palomuuri estää kaiken ei-toivotun tietoliikenteen, tavallisesti ei ole tarpeellista estää IP-osoitteita. IP-osoite tulee estää vain, jos olet varma, että määrätty Internet-yhteys on jonkin uhan aiheuttaja. Varmista, ettet estä tärkeitä IP-osoitteita, kuten DNS- tai DHCP-palvelinta tai muita Internet-palveluntarjoajan palvelimia. Suojausasetuksissa voidaan määrittää, että palomuuri hälyttää, kun se havaitsee tapahtuman estetystä tietokoneesta.

Tässä luvussa

Tietokoneyhteyksiin luottaminen

Voit lisätä, muokata ja poistaa luotettavia IP-osoitteita Luotettavat ja estetyt IP-osoitteet -ikkunan **Luotettavat IP-osoitteet** -kohdassa.

Luotettavat ja estetyt IP-osoitteet -ikkunan **Luotettavat IP-osoitteet** -luettelosta voit sallia kaiken tietoliikenteen määrätystä tietokoneesta omaan tietokoneeseesi. Palomuuri ei kirjaa lokiin tietoliikennettä tai luo tapahtumahälytyksiä IP-osoitteista, jotka ovat **Luotettavat IP-osoitteet** -luettelossa.

Firewall luottaa kaikkiin luettelossa oleviin IP-osoitteisiin ja päästää luotettavista IP-osoitteista peräisin olevan tietoliikenteen aina palomuurin läpi kaikkiin portteihin. Firewall ei kirjaa luotettavien IP-osoitteiden tapahtumia. Firewall ei suodata eikä analysoi luotettavaa IP-osoitetta käyttävän tietokoneen ja käyttäjän tietokoneen välisiä tapahtumia.

Kun sallit yhteyden, varmista, että tietokone, johon luotat, on turvallinen. Jos tietokone, johon luotat, on madon tai muun mekanismin tartuttama, voit tietokoneesi olla alttiina tartunnalle. McAfee suosittelee lisäksi, että luotat vain tietokoneisiin, jotka ovat palomuurin sekä ajantasaisen virustorjuntaohjelman suojaamia.

Lisää luotettava tietokoneyhteys

Firewallin avulla voit lisätä luotettavan tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

Luotettavat ja estetyt IP-osoitteet -ikkunan **Luotettavat IP-osoitteet** -luettelosta voit sallia kaiken tietoliikenteen määrätystä tietokoneesta omaan tietokoneeseesi. Palomuuri ei kirjaa lokiin tietoliikennettä tai luo tapahtumahälytyksiä IP-osoitteista, jotka ovat **Luotettavat IP-osoitteet** -luettelossa.

Tietokoneet, jotka muodostavat yhteyden luotettavista IP-osoitteista, voivat aina muodostaa yhteyden tietokoneeseesi. Ennen kuin lisäät, muokkaat tai poistat luotettavia IP-osoitteita, varmista, että osoitteet ovat turvallisia.

Luotettavan tietokoneyhteyden lisääminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
3. Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Luotettavat IP-osoitteet**.
4. Valitse **Lisää**.
5. Toimi **Lisää IP-osoitteen luotettavuussääntö** -kohdassa seuraavasti:
   - Valitse **Yksittäinen IP-osoite** ja anna IP-osoite.
   - Valitse **IP-osoitealue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin.
6. Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.
7. Kirjoita vaihtoehtoisesti kuvaus säännöstä.
8. Valitse **OK**.
9. Valitse Lisää IP-osoitteen luotettavuussääntö -valintaikkunasta **Kyllä** ja vahvista, että haluat lisätä luotettavan tietokoneyhteyden.

   Juuri lisätty IP-osoite ilmestyy **Luotettavat IP-osoitteet** -kohtaan.

Lisää luotettava tietokone saapuvien tapahtumien lokista

Voit lisätä luotettavan tietokoneyhteyden ja siihen liittyvän IP-osoitteen saapuvien tapahtumien lokista.

Tietokoneet, jotka muodostavat yhteyden luotettavista IP-osoitteista, voivat aina muodostaa yhteyden tietokoneeseesi. Ennen kuin lisäät, muokkaat tai poistat luotettavia IP-osoitteita, varmista, että osoitteet ovat turvallisia.

Luotettavan tietokoneyhteyden lisääminen saapuvien tapahtumien lokista:

1. Varmista, että lisävalikko on käytössä. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
3. Valitse **Internet & verkko** ja valitse sitten **Saapuvat tapahtumat**.
4. Valitse ensin Saapuvat tapahtumat -ikkunasta IP-lähdeosoite ja sitten **Luota tähän osoitteeseen**.
5. Valitse Lisää IP-osoitteen luotettavuussääntö -valintaikkunasta **Kyllä** ja vahvista, että haluat luottaa IP-osoitteeseen.

   Juuri lisätty IP-osoite ilmestyy **Luotettavat IP-osoitteet** -kohtaan.

Vastaavat aiheet

- Tapahtumien kirjaus (sivu 164)

Muokkaa luotettavaa tietokoneyhteyttä

Firewallin avulla voit muokata luotettavaa tietokoneyhteyttä ja siihen liittyvää IP-osoitetta.

Tietokoneet, jotka muodostavat yhteyden luotettavista IP-osoitteista, voivat aina muodostaa yhteyden tietokoneeseesi. Ennen kuin lisäät, muokkaat tai poistat luotettavia IP-osoitteita, varmista, että osoitteet ovat turvallisia.

Luotettavan tietokoneyhteyden muokkaaminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
3. Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Luotettavat IP-osoitteet**.
4. Valitse ensin IP-osoite ja sitten **Muokkaa**.
5. Toimi **Lisää IP-osoitteen luotettavuussääntö** -kohdassa seuraavasti:
   - Valitse **Yksittäinen IP-osoite** ja anna IP-osoite.
   - Valitse **IP-osoitealue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin.
6. Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.
7. Kirjoita vaihtoehtoisesti kuvaus säännöstä.
8. Valitse **OK**.

   Muokattu IP-osoite ilmestyy **Luotettavat IP-osoitteet** -kohtaan.

Poista luotettava tietokoneyhteys

Firewallin avulla voit poistaa luotettavan tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

Tietokoneet, jotka muodostavat yhteyden luotettavista IP-osoitteista, voivat aina muodostaa yhteyden tietokoneeseesi. Ennen kuin lisäät, muokkaat tai poistat luotettavia IP-osoitteita, varmista, että osoitteet ovat turvallisia.

Luotettavan tietokoneyhteyden poistaminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
3. Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Luotettavat IP-osoitteet**.
4. Valitse ensin IP-osoite ja sitten **Poista**.
5. Valitse **Luotettavat ja estetyt IP-osoitteet** -valintaikkunasta **Kyllä** ja vahvista, että haluat poistaa luotettavan tietokoneyhteyden **Luotettavat IP-osoitteet** -kohdasta.

Tietokoneyhteyksien estäminen

Voit lisätä, muokata ja poistaa luotettavia IP-osoitteita Luotettavat ja estetyt IP-osoitteet -ikkunan **Estetyt IP-osoitteet** -kohdassa.

Tietokoneita, joiden IP-osoite on tuntematon, epäilyttävä tai joka ei ole luetettava, voidaan estää ottamasta yhteyttä tietokoneeseesi

Koska palomuuri estää kaiken ei-toivotun tietoliikenteen, tavallisesti ei ole tarpeellista estää IP-osoitteita. IP-osoite tulee estää vain, jos olet varma, että määrätty Internet-yhteys on jonkin uhan aiheuttaja. Varmista, ettet estä tärkeitä IP-osoitteita, kuten DNS- tai DHCP-palvelinta tai muita Internet-palveluntarjoajan palvelimia. Suojausasetuksissa voidaan määrittää, että palomuuri hälyttää, kun se havaitsee tapahtuman estetystä tietokoneesta.

Lisää estetty tietokoneyhteys

Firewallin avulla voit lisätä estetyn tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

Tietokoneita, joiden IP-osoite on tuntematon, epäilyttävä tai joka ei ole luetettava, voidaan estää ottamasta yhteyttä tietokoneeseesi

Koska palomuuri estää kaiken ei-toivotun tietoliikenteen, tavallisesti ei ole tarpeellista estää IP-osoitteita. IP-osoite tulee estää vain, jos olet varma, että määrätty Internet-yhteys on jonkin uhan aiheuttaja. Varmista, ettet estä tärkeitä IP-osoitteita, kuten DNS- tai DHCP-palvelinta tai muita Internet-palveluntarjoajan palvelimia. Suojausasetuksissa voidaan määrittää, että palomuuri hälyttää, kun se havaitsee tapahtuman estetystä tietokoneesta.

Estetyn tietokoneyhteyden lisääminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
3. Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Estetyt IP-osoitteet**.
4. Valitse **Lisää**.
5. Toimi Lisää IP-osoitteen estosääntö -kohdassa seuraavasti:
   - Valitse **Yksittäinen IP-osoite** ja anna IP-osoite.
   - Valitse **IP-osoitealue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin.

6 Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.

7 Kirjoita vaihtoehtoisesti kuvaus säännöstä.

8 Valitse **OK**.

9 Valitse **Lisää IP-osoitteen estosääntö** -valintaikkunasta **Kyllä** ja vahvista, että haluat lisätä estetyn tietokoneyhteyden.

Juuri lisätty IP-osoite ilmestyy **Estetyt IP-osoitteet** -kohtaan.

Muokkaa estettyä tietokoneyhteyttä

Firewallin avulla voit muokata estettyä tietokoneyhteyttä ja siihen liittyvää IP-osoitetta.

Tietokoneita, joiden IP-osoite on tuntematon, epäilyttävä tai joka ei ole luetettava, voidaan estää ottamasta yhteyttä tietokoneeseesi

Koska palomuuri estää kaiken ei-toivotun tietoliikenteen, tavallisesti ei ole tarpeellista estää IP-osoitteita. IP-osoite tulee estää vain, jos olet varma, että määrätty Internet-yhteys on jonkin uhan aiheuttaja. Varmista, ettet estä tärkeitä IP-osoitteita, kuten DNS- tai DHCP-palvelinta tai muita Internet-palveluntarjoajan palvelimia. Suojausasetuksissa voidaan määrittää, että palomuuri hälyttää, kun se havaitsee tapahtuman estetystä tietokoneesta.

Estetyn tietokoneyhteyden muokkaaminen:

1 Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.

2 Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.

3 Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Estetyt IP-osoitteet**.

4 Valitse ensin IP-osoite ja sitten **Muokkaa**.

5 Toimi **Lisää IP-osoitteen luotettavuussääntö** -kohdassa seuraavasti:

- Valitse **Yksittäinen IP-osoite** ja anna IP-osoite.
- Valitse **IP-osoitealue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin.

6 Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.

7 Kirjoita vaihtoehtoisesti kuvaus säännöstä.

Valitse **OK**. Muokattu IP-osoite ilmestyy **Estetyt IP-osoitteet** -kohtaan.

Poista estetty tietokoneyhteys

Firewallin avulla voit poistaa estetyn tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

Tietokoneita, joiden IP-osoite on tuntematon, epäilyttävä tai joka ei ole luetettava, voidaan estää ottamasta yhteyttä tietokoneeseesi

Koska palomuuri estää kaiken ei-toivotun tietoliikenteen, tavallisesti ei ole tarpeellista estää IP-osoitteita. IP-osoite tulee estää vain, jos olet varma, että määrätty Internet-yhteys on jonkin uhan aiheuttaja. Varmista, ettet estä tärkeitä IP-osoitteita, kuten DNS- tai DHCP-palvelinta tai muita Internet-palveluntarjoajan palvelimia. Suojausasetuksissa voidaan määrittää, että palomuuri hälyttää, kun se havaitsee tapahtuman estetystä tietokoneesta.

Estetyn tietokoneyhteyden poistaminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
3. Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Estetyt IP-osoitteet**.
4. Valitse IP-osoite ja sitten **Poista**.
5. Valitse **Luotettavat ja estetyt IP-osoitteet** -valintaikkunasta **Kyllä** ja vahvista, että haluat poistaa estetyn tietokoneyhteyden **Estetyt IP-osoitteet** -kohdasta.

Estä tietokone saapuvien tapahtumien lokista

Voit estää tietokoneyhteyden ja siihen liittyvän IP-osoitteen saapuvien tapahtumien lokista.

Saapuvien tapahtumien lokissa olevat IP-osoitteet estetään. Osoitteen estäminen ei siten lisää tietoturvaa, paitsi jos tietokone käyttää tarkoituksella avattuja portteja tai jos tietokoneessa on ohjelma, jolle on myönnetty oikeudet Internetin käyttöön.

Lisää IP-osoite **Estetyt IP-osoitteet** -luetteloon vain silloin, jos olet tarkoituksella avannut yhden tai useamman portin ja jos uskot, että kyseistä osoitetta on estettävä käyttämästä avattuja portteja.

Voit käyttää kaiken saapuvan Internet-tietoliikenteen IP-osoitteet sisältävää saapuvien tapahtumien sivua sellaisten IP-osoitteiden estämiseen, joiden uskot olevan epäilyttävien tai ei-toivottujen Internet-tapahtumien taustalla.

Luotettavan tietokoneyhteyden estäminen saapuvien tapahtumien lokista:

1. Varmista, että lisävalikko on käytössä. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
3. Valitse **Internet & verkko** ja valitse sitten **Saapuvat tapahtumat**.
4. Valitse ensin Saapuvat tapahtumat -ikkunasta IP-lähdeosoite ja sitten **Estä tämä osoite**.
5. Valitse **Lisää IP-osoitteen estosääntö** -valintaikkunasta **Kyllä** ja vahvista, että haluat estää IP-osoitteen.

   Juuri lisätty IP-osoite ilmestyy **Estetyt IP-osoitteet** -kohtaan.

Vastaavat aiheet

- Tapahtumien kirjaus (sivu 164)

Estä tietokone tietomurtojen havainnoinnin tapahtumien lokista

Voit estää tietokoneyhteyden ja siihen liittyvän IP-osoitteen tietomurtojen havainnoinnin tapahtumien lokista.

Tietokoneita, joiden IP-osoite on tuntematon, epäilyttävä tai joka ei ole luetettava, voidaan estää ottamasta yhteyttä tietokoneeseesi

Koska palomuuri estää kaiken ei-toivotun tietoliikenteen, tavallisesti ei ole tarpeellista estää IP-osoitteita. IP-osoite tulee estää vain, jos olet varma, että määrätty Internet-yhteys on jonkin uhan aiheuttaja. Varmista, ettet estä tärkeitä IP-osoitteita, kuten DNS- tai DHCP-palvelinta tai muita Internet-palveluntarjoajan palvelimia. Suojausasetuksissa voidaan määrittää, että palomuuri hälyttää, kun se havaitsee tapahtuman estetystä tietokoneesta.

Tietokoneyhteyden estäminen tietomurtojen havainnoinnin tapahtumien lokista:

1. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
3. Valitse **Internet & verkko** ja valitse sitten **Tietomurtojen havainnoinnin tapahtumat**.
4. Valitse ensin Tietomurtojen havainnoinnin tapahtumat -ikkunasta IP-lähdeosoite ja sitten **Estä tämä osoite**.
5. Valitse **Lisää IP-osoitteen estosääntö** -valintaikkunasta **Kyllä** ja vahvista, että haluat estää IP-osoitteen.

   Juuri lisätty IP-osoite ilmestyy **Estetyt IP-osoitteet** -kohtaan.

Vastaavat aiheet

- Tapahtumien kirjaus (sivu 164)

LUKU 23

Kirjaus, valvonta ja analyysi

Firewall tarjoaa monipuolisia ja helppolukuisia menetelmiä Internet-tapahtumien ja tietoliikenteen kirjaukseen, valvontaan ja analysointiin. Internet-tietoliikenteen ja tapahtumien ymmärtäminen helpottaa Internet-yhteyksien hallintaa.

Tässä luvussa

Tapahtumien kirjaus

Firewall antaa sinun määrittää, haluatko ottaa kirjauksen käyttöön tai poistaa sen käytöstä. Jos kirjaus on käytössä, voit määrittää, minkätyyppisiä tapahtumia kirjataan. Tapahtumien kirjauksen avulla voit tarkastella äskettäisiä tapahtumia, sekä saapuvia että lähteviä. Voit tarkastella myös havaittuja tietomurtotapahtumia.

Tapahtumalokin asetusten määrittäminen

Palomuuritapahtumien ja -toiminnan jäljittämiseksi voit valita tarkasteltavien tapahtumien tyypit ja määrittää niiden asetukset.

Tapahtumien kirjauksen asetusten määrittäminen:

1. Valitse Internet- ja verkkomääritykset -ikkunasta **Lisäasetukset**.
2. Valitse Firewall-ikkunasta **Tapahtumalokin asetukset**.
3. Toimi Tapahtumalokin asetukset -ikkunassa seuraavasti:
   - Ota tapahtumien kirjaus käyttöön valitsemalla **Kirjaa tapahtuma lokiin**.
   - Poista tapahtumien kirjaus käytöstä valitsemalla **Älä kirjaa tapahtumaa lokiin**.
4. Määritä **Tapahtumalokin asetukset** -ikkunassa kirjattavien tapahtumien tyypit. Tapahtumien tyyppejä ovat muun muassa seuraavat:
   - ICMP ping -pyynnöt
   - estetyistä IP-osoitteista saapuva tietoliikenne
   - järjestelmäpalveluporttien tapahtumat
   - tuntemattomien porttien tapahtumat
   - tietomurtojen havainnointitapahtumat (IDS).
5. Jos haluat estää tiettyjen porttien kirjaamisen, valitse **Älä kirjaa tapahtumia seuraavista porteista** ja anna yksittäisten porttien numerot pilkuilla erotettuina tai porttialueet väliviivoilla yhdistettyinä, esimerkiksi `137-139, 445, 400-5000`.
6. Valitse **OK**.

Tarkastele äskettäisiä tapahtumia

Jos kirjaus on otettu käyttöön, voit tarkastella äskettäisiä tapahtumia. Äskettäiset tapahtumat -ikkunassa näkyy tapahtuman päivämäärä ja kuvaus. Äskettäiset tapahtumat -ikkunassa näytetään vain niitä ohjelmia koskevat tapahtumat, jotka on estetty käyttämästä Internetiä.

Firewallin äskettäisten tapahtumien tarkasteleminen:

- Valitse Yleiset tehtävät -ikkunan **Lisävalikko**-kohdasta **Raportit ja lokit** tai **Tarkastele äskettäisiä tapahtumia**. **Tarkastele äskettäisiä tapahtumia** -asetuksen voit vaihtoehtoisesti valita myös Perusvalikon Yleiset tehtävät -kohdasta.

Tarkastele saapuvia tapahtumia

Jos kirjaus on otettu käyttöön, voit tarkastella ja lajitella saapuvia tapahtumia.

Saapuvien tapahtumien lokissa on seuraavat kirjausluokat:

- päivämäärä ja aika
- IP-lähdeosoite
- isännän nimi
- tietojen ja tapahtuman tyyppi.

Palomuurin saapuvien tapahtumien tarkasteleminen:

1. Varmista, että lisävalikko on käytössä. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
3. Valitse **Internet & verkko** ja valitse sitten **Saapuvat tapahtumat**.

Huomaa: Saapuvien tapahtumien lokissa voit luottaa, estää ja jäljittää IP-osoitteen.

Vastaavat aiheet

- Lisää luotettava tietokone saapuvien tapahtumien lokista (sivu 154)
- Estä tietokone saapuvien tapahtumien lokista (sivu 160)
- Jäljitä tietokone saapuvien tapahtumien lokista (sivu 170)

Tarkastele lähteviä tapahtumia

Jos kirjaus on otettu käyttöön, voit tarkastella lähteviä tapahtumia. Lähteviin tapahtumiin kuuluvat muun muassa lähtevän yhteyden muodostamista yrittävän ohjelman nimi, tapahtuman päivämäärä ja aika sekä ohjelman sijainti tietokoneessa.

Palomuurin lähtevien tapahtumien tarkasteleminen:

1. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
3. Valitse **Internet & verkko** ja valitse sitten **Lähtevät tapahtumat**.

Huomaa: Voit myöntää ohjelmalle täydet tai vain lähtevän tietoliikenteen käyttöoikeudet lähtevien tapahtumien lokista. Voit myös etsiä muita tietoja ohjelmasta.

Vastaavat aiheet

- Myönnä täydet käyttöoikeudet lähtevien tapahtumien lokista (sivu 138)
- Myönnä vain lähtevän tietoliikenteen käyttöoikeudet lähtevien tapahtumien lokista (sivu 140)
- Hae ohjelmatietoja lähtevien tapahtumien lokista (sivu 145)

Tarkastele tietomurtojen havainnoinnin tapahtumia

Jos kirjaus on otettu käyttöön, voit tarkastella saapuvia tapahtumia. Tietomurtojen havainnoinnin tapahtumat näyttävät päivämärän ja ajan, IP-lähdeosoitteen ja tapahtuman isännän nimen. Loki kuvailee myös tapahtuman tyypin.

Tietomurtojen havainnoinnin tapahtumien tarkasteleminen:

1. Valitse Yleiset tehtävät -ikkunasta **Tapahtumat ja lokit**.
2. Valitse Äskettäiset tapahtumat -kohdasta **Tarkastele lokia**.
3. Valitse ensin **Internet ja verkko** ja sitten **Tietomurtojen havainnoinnin tapahtumat**.

Huomaa: Tietomurtojen havainnoinnin tapahtumien lokissa voit estää ja jäljittää IP-osoitteen.

Vastaavat aiheet

- Estä tietokone tietomurtojen havainnoinnin tapahtumien lokista (sivu 161)
- Jäljitä tietokone tietomurtojen havainnoinnin tapahtumien lokista (sivu 171)

Tilastotietojen käsitteleminen

Firewall hyödyntää McAfeen HackerWatch-tietoturvasivustoa ja tarjoaa tilastotietoja maailman Internet-tietoturva- ja -porttitapahtumista.

Tarkastele maailman tietoturvatapahtumien tilastotietoja

HackerWatch seuraa Internet-tietoturvatapahtumia maailmanlaajuisesti, ja voit tarkastella niitä SecurityCenterissä. Seurantatiedoissa ovat mukana tapahtumat, joista on ilmoitettu HackerWatchille viimeisen 24 tunnin, 7 päivän ja 30 päivän aikana.

Maailman tietoturvatapahtumien tilastotietojen tarkasteleminen:

1. Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
2. Valitse Työkalut-ikkunasta **HackerWatch**.
3. Tarkastele tietoturvatapahtumien tilastotietoja **Tapahtumien seuranta** -kohdassa.

Tarkastele maailman Internet-porttitapahtumia

HackerWatch seuraa Internet-tietoturvatapahtumia maailmanlaajuisesti, ja voit tarkastella niitä SecurityCenterissä. Siellä näytetään tietoja muun muassa tärkeimpien tapahtumien porteista, jotka on ilmoitettu HackerWatchille viimeisen seitsemän päivän aikana. Tavallisesti tietoja näytetään HTTP-, TCP- ja UDP-porteista.

Maailman porttitapahtumien tarkasteleminen:

1. Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
2. Valitse Työkalut-ikkunasta **HackerWatch**.
3. Tarkastele tärkeimpien tapahtumien porttitapahtumia **Äskettäiset porttitapahtumat** -kohdassa.

Internet-tietoliikenteen jäljittäminen

Firewall tarjoaa useita vaihtoehtoja Internet-tietoliikenteen jäljittämiseen. Näiden vaihtoehtojen avulla voit jäljittää verkkotietokoneen maantieteellisesti, hankkia toimialueeseen ja verkkoon liittyviä tietoja sekä jäljittää tietokoneita saapuvien tapahtumien ja tietomurtojen havainnoinnin tapahtumien lokeista.

Jäljitä verkkotietokone maantieteellisesti

Visuaalisen jäljityksen avulla voit etsiä tietokoneen, joka on muodostamassa tai yrittää muodostaa yhteyden omaan tietokoneeseesi. Maantieteelliseen etsimiseen käytetään tietokoneen nimeä tai IP-osoitetta. Visuaalinen jäljitys mahdollistaa myös verkon ja rekisteröintitietojen käytön. Visuaalista jäljitystä käyttämällä saat näkyviin maailmankartan, joka näyttää tiedonsiirron todennäköisimmän reitin lähdetietokoneen ja oman tietokoneesi välillä.

Tietokoneen maantieteellinen etsiminen:

1. Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
2. Valitse Työkalut-ikkunasta **Visuaalinen jäljitys**.
3. Kirjoita tietokoneen IP-osoite ja valitse **Jäljitä**.
4. Valitse **Visuaalinen jäljitys** -kohdasta **Karttanäkymä**.

Huomaa: Silmukkaa käyttäviä, yksityisiä tai virheellisiä IP-osoitteita sisältäviä tapahtumia ei voi jäljittää.

Hanki tietokoneen rekisteröintitiedot

Voit hankkia tietokoneen rekisteröintitiedot SecurityCenteristä visuaalisen jäljityksen avulla. Tiedot sisältävät toimialueen nimen, rekisteröijän nimen ja osoitteen sekä hallinnoinnista vastaavan yhteyshenkilön tiedot.

Tietokoneen toimialuetietojen hankkiminen:

1. Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
2. Valitse Työkalut-ikkunasta **Visuaalinen jäljitys**.
3. Kirjoita tietokoneen IP-osoite ja valitse **Jäljitä**.
4. Valitse **Visuaalinen jäljitys** -kohdasta **Rekisteröijänäkymä**.

Hanki tietokoneen verkkotiedot

Voit hankkia tietokoneen verkkotiedot SecurityCenteristä visuaalisen jäljityksen avulla. Verkkotiedot sisältävät yksityiskohtaisia tietoja verkosta, jossa toimialue sijaitsee.

Tietokoneen verkkotietojen hankkiminen:

1. Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
2. Valitse Työkalut-ikkunasta **Visuaalinen jäljitys**.
3. Kirjoita tietokoneen IP-osoite ja valitse **Jäljitä**.
4. Valitse **Visuaalinen jäljitys** -kohdasta **Verkkonäkymä**.

Jäljitä tietokone saapuvien tapahtumien lokista

Saapuvat tapahtumat -ikkunassa voit jäljittää IP-osoitteen, joka on saapuvien tapahtumien lokissa.

Tietokoneen IP-osoitteen jäljittäminen saapuvien tapahtumien lokista:

1. Varmista, että lisävalikko on käytössä. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
3. Valitse **Internet & verkko** ja valitse sitten **Saapuvat tapahtumat**.
4. Valitse ensin Saapuvat tapahtumat -ikkunasta IP-lähdeosoite ja sitten **Jäljitä tämä osoite**.
5. Valitse Visuaalinen jäljitys -ikkunassa yksi seuraavista:
   - **Karttanäkymä**: Etsi tietokone maantieteellisesti valitun IP-osoitteen perusteella.
   - **Rekisteröijänäkymä**: Etsi toimialuetiedot valitun IP-osoitteen perusteella.
   - **Verkkonäkymä**: Etsi verkkotiedot valitun IP-osoitteen perusteella.
6. Valitse **Valmis**.

Vastaavat aiheet

- Internet-tietoliikenteen jäljittäminen (sivu 169)
- Tarkastele saapuvia tapahtumia (sivu 165)

Jäljitä tietokone tietomurtojen havainnoinnin tapahtumien lokista

Tietomurtojen havainnoinnin tapahtumat -ikkunassa voit jäljittää IP-osoitteen, joka on tietomurtojen havainnoinnin tapahtumien lokissa.

Tietokoneen IP-osoitteen jäljittäminen tietomurtojen havainnoinnin tapahtumien lokista:

1. Valitse Yleiset tehtävät -ikkunasta **Raportit& Lokit**.
2. Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
3. Valitse **Internet & verkko** ja valitse sitten **Tietomurtojen havainnoinnin tapahtumat**. Valitse ensin Tietomurtojen havainnoinnin tapahtumat -ikkunasta IP-lähdeosoite ja sitten **Jäljitä tämä osoite**.
4. Valitse Visuaalinen jäljitys -ikkunassa yksi seuraavista:
   - **Karttanäkymä**: Etsi tietokone maantieteellisesti valitun IP-osoitteen perusteella.
   - **Rekisteröijänäkymä**: Etsi toimialuetiedot valitun IP-osoitteen perusteella.
   - **Verkkonäkymä**: Etsi verkkotiedot valitun IP-osoitteen perusteella.
5. Valitse **Valmis**.

Vastaavat aiheet

- Internet-tietoliikenteen jäljittäminen (sivu 169)
- Kirjaus, valvonta ja analyysi (sivu 163)

Jäljitä valvottu IP-osoite

Jäljittämällä valvotun IP-osoitteen voit luoda maantieteellisen yleiskatsauksen, joka näyttää tiedonsiirron todennäköisimmän reitin lähdetietokoneen ja oman tietokoneesi välillä. Lisäksi voit hankkia IP-osoitteen rekisteröinti- ja verkkotiedot.

Ohjelmien käyttämän kaistanleveyden valvonta:

1. Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
2. Valitse Työkalut-ikkunasta **Tietoliikenteen valvonta**.
3. Valitse **Tietoliikenteen valvonta** -kohdasta **Aktiiviset ohjelmat**.
4. Valitse ohjelma ja sen jälkeen ohjelman nimen alla oleva IP-osoite.
5. Valitse **Ohjelmien tapahtumat** -kohdasta **Jäljitä tämä IP-osoite**.
6. **Visuaalinen jäljitys** -kohdassa voit tarkastella maailmankarttaa, joka näyttää tiedonsiirron todennäköisimmän reitin lähdetietokoneen ja oman tietokoneesi välillä. Lisäksi voit hankkia IP-osoitteen rekisteröinti- ja verkkotiedot.

Huomaa: Jos haluat tarkastella uusimpia tilastotietoja, valitse **Visuaalinen jäljitys** -kohdasta **Päivitä**.

Vastaavat aiheet

- Internet-tietoliikenteen valvonta (sivu 173)

Internet-tietoliikenteen valvonta

Firewall tarjoaa useita tapoja Internet-tietoliikenteen valvontaan, muun muassa seuraavat:

- **Tietoliikenneanalyysin kaaviot**: Kuvaavat viimeisintä saapuvaa ja lähtevää Internet-tietoliikennettä.
- **Tietoliikenteen käytön kaaviot**: Näyttävät prosentteina, kuinka suuren osan kaistanleveydestä aktiivisimmat ohjelmat ovat käyttäneet viimeisen 24 tunnin aikana.
- **Aktiiviset ohjelmat**: Näyttää tietokoneen tällä hetkellä eniten verkkoyhteyksiä käyttävät ohjelmat ja niiden käyttämät IP-osoitteet.

Tietoja tietoliikenneanalyysin kaaviosta

Tietoliikenneanalyysin kaaviot ovat numeerisia ja graafisia esityksiä saapuvasta ja lähtevästä Internet-tietoliikenteestä. Tietoliikenteen valvonta näyttää lisäksi ohjelmat, jotka käyttävät tietokoneessasi eniten verkkoyhteyksiä ja IP-osoitteet, joihin ohjelmat ovat yhteydessä.

Tietoliikenneanalyysi-ikkunassa voit tarkastella äskettäistä saapuvaa ja lähtevää Internet-tietoliikennettä sekä tiedonsiirron nykyistä, keskimääräistä ja suurinta mahdollista nopeutta. Voit tarkastella myös tietoliikenteen määrää, esimerkiksi Firewallin käynnistämisen jälkeistä tietoliikenteen määrää sekä tietoliikenteen kokonaismäärää kuluvan kuukauden ja edellisten kuukausien aikana.

Tietoliikenneanalyysi-ikkuna näyttää tietokoneen reaaliaikaiset Internet-tapahtumat, kuten äskettäisen saapuvan ja lähtevän Internet-tietoliikenteen määrän ja tiedonsiirtonopeuden, yhteysnopeuden sekä Internetin kautta siirrettyjen tavujen yhteismäärän.

Yhtenäinen vihreä viiva osoittaa saapuvan liikenteen nykyisen tiedonsiirtonopeuden. Vihreä pisteviiva osoittaa saapuvan liikenteen keskimääräisen tiedonsiirtonopeuden. Jos nykyinen ja keskimääräinen tiedonsiirtonopeus ovat samat, kaaviossa ei ole pisteviivaa. Yhtenäinen viiva osoittaa sekä keskimääräisen että nykyisen tiedonsiirtonopeuden.

Yhtenäinen punainen viiva osoittaa lähtevän liikenteen nykyisen tiedonsiirtonopeuden. Punainen pisteviiva osoittaa lähtevän liikenteen keskimääräisen tiedonsiirtonopeuden. Jos nykyinen ja keskimääräinen tiedonsiirtonopeus ovat samat, kaaviossa ei ole pisteviivaa. Yhtenäinen viiva osoittaa sekä keskimääräisen että nykyisen tiedonsiirtonopeuden.

Vastaavat aiheet

- Analysoi saapuvaa ja lähtevää tietoliikennettä (sivu 174)

Analysoi saapuvaa ja lähtevää tietoliikennettä

Tietoliikenneanalyysin kaaviot ovat numeerisia ja graafisia esityksiä saapuvasta ja lähtevästä Internet-tietoliikenteestä. Tietoliikenteen valvonta näyttää lisäksi ohjelmat, jotka käyttävät tietokoneessasi eniten verkkoyhteyksiä ja IP-osoitteet, joihin ohjelmat ovat yhteydessä.

Saapuvan ja lähtevän tietoliikenteen analysoiminen:

1. Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
2. Valitse Työkalut-ikkunasta **Tietoliikenteen valvonta**.
3. Valitse **Tietoliikenteen valvonta** -kohdasta **Tietoliikenneanalyysi**.

Vihje: Jos haluat tarkastella uusimpia tilastotietoja, valitse **Tietoliikenneanalyysi**-kohdasta **Päivitä**.

Vastaavat aiheet

- Tietoja tietoliikenneanalyysin kaaviosta (sivu 173)

Valvo ohjelman kaistanleveyttä

Voit tarkastella ympyräkaaviota, joka näyttää prosentteina, kuinka suuren osan kaistanleveydestä aktiivisimmat ohjelmat ovat käyttäneet viimeisen 24 tunnin aikana. Ympyräkaavio esittää visuaalisesti kunkin ohjelman käyttämän kaistanleveyden suhteellisen määrän.

Ohjelmien käyttämän kaistanleveyden valvonta:

1. Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
2. Valitse Työkalut-ikkunasta **Tietoliikenteen valvonta**.
3. Valitse **Tietoliikenteen valvonta** -kohdasta **Tietoliikenteen käyttö**.

Vihje: Jos haluat tarkastella uusimpia tilastotietoja, valitse **Tietoliikenteen käyttö** -kohdasta **Päivitä**.

Valvo ohjelmatapahtumia

Voit tarkastella saapuvia ja lähteviä ohjelmatapahtumia, kuten etätietokoneiden yhteyksiä ja portteja.

Ohjelmien käyttämän kaistanleveyden valvonta:

1. Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
2. Valitse Työkalut-ikkunasta **Tietoliikenteen valvonta**.
3. Valitse **Tietoliikenteen valvonta** -kohdasta **Aktiiviset ohjelmat**.
4. Voit tarkastella seuraavia tietoja:
   - Ohjelmatapahtumien kaavio: Valitse ohjelma, jonka tapahtumien kaaviota haluat tarkastella.
   - Kuunteluyhteys: Valitse kuunneltava kohde ohjelman nimen alta.
   - Tietokoneyhteys: Valitse IP-osoite ohjelman nimen, järjestelmäprosessin tai palvelun alta.

Huomaa: Jos haluat tarkastella uusimpia tilastotietoja, valitse **Aktiiviset ohjelmat** -kohdasta **Päivitä**.

LUKU 24

Perehtyminen Internet-tietoturvaan

Firewall hyödyntää McAfeen HackerWatch-tietoturvasivustoa ja tarjoaa ajan tasalla olevia tietoja ohjelmista ja maailman Internet-tapahtumista. HackerWatchista löydät myös HTML-muotoisen opetusohjelman Firewallista.

Tässä luvussa

Käynnistä HackerWatch-opetusohjelma

Lisätietoja Firewallista saat SecurityCenterissä olevasta HackerWatch-opetusohjelmasta.

HackerWatch-opetusohjelman käynnistäminen:

1. Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
2. Valitse Työkalut-ikkunasta **HackerWatch**.
3. Valitse **HackerWatch-resurssit**-kohdasta **Katso opetusohjelma**.

LUKU 25

McAfee EasyNetwork

McAfee® EasyNetwork mahdollistaa suojatun tiedostojen jakamisen, yksinkertaistaa tiedostonsiirtoa ja automatisoi tulostimen jakamisen kotiverkkosi tietokoneiden kesken.

Voit tutustua EasyNetworkin suosituimpiin ominaisuuksiin, ennen kuin alat käyttää sitä. Lisätietoja näiden ominaisuuksien määrittämisestä ja käyttämisestä on EasyNetworkin ohjeessa.

Tässä luvussa

Ominaisuudet

EasyNetworkissä on seuraavat ominaisuudet.

Tiedostojen jakaminen

EasyNetworkin avulla voit helposti jakaa tietokoneessasi olevia tiedostoja toisiin verkon tietokoneisiin. Kun jaat tiedostoja, myönnät toisille tietokoneille lukuoikeuden kyseisiin tiedostoihin. Vain hallitun verkon jäsentietokoneet (eli täysillä tai järjestelmänvalvojan oikeuksilla varustetut tietokoneet) voivat jakaa tiedostoja tai lukea toisten jäsentietokoneiden jakamia tiedostoja.

Tiedostonsiirto

Voit lähettää tiedostoja toisiin hallitun verkon jäsentietokoneisiin. Kun vastaanotat tiedoston, se näkyy EasyNetworkin Saapuneet-kansiossa. Saapuneet-kansio on väliaikainen tallennuspaikka kaikille tiedostoille, jotka on lähetetty sinulle toisista verkon tietokoneista.

Automaattinen tulostimen jakaminen

Kun olet liittynyt hallittuun verkkoon, EasyNetwork jakaa automaattisesti tietokoneeseesi liitetyt paikalliset tulostimet ja käyttää jaetun tulostimen nimenä tulostimen nykyistä nimeä. Se havaitsee myös toisten verkon tietokoneiden tulostimet ja sallii noiden tulostimien määrittämisen ja käyttämisen.

LUKU 26

EasyNetworkin asentaminen

Ennen kuin EasyNetworkin ominaisuuksia voi käyttää, ohjelma on käynnistettävä ja hallittuun verkkoon on liityttävä. Liittymisen jälkeen voit poistua verkosta milloin tahansa.

Tässä luvussa

EasyNetworkin käynnistäminen

Oletusarvoisesti järjestelmä kehottaa käynnistämään EasyNetworkin heti asennuksen jälkeen, mutta voit käynnistää EasyNetworkin myöhemminkin.

EasyNetworkin käynnistäminen

Oletusarvoisesti järjestelmä kehottaa käynnistämään EasyNetworkin heti asennuksen jälkeen, mutta voit kuitenkin käynnistää EasyNetworkin myöhemminkin.

EasyNetworkin käynnistäminen:

- Valitse **Käynnistä**-valikosta **Ohjelmat**, **McAfee** ja valitse **McAfee EasyNetwork**.

Vihje: Jos olet luonut asennuksen yhteydessä työpöytä- ja pikakäynnistyskuvakkeet, voit käynnistää EasyNetworkin myös kaksoisnapsauttamalla työpöydällä olevaa McAfee EasyNetwork -kuvaketta tai napsauttamalla tehtäväpalkin oikeassa reunassa sijaitsevalla ilmaisinalueella McAfee EasyNetwork -kuvaketta.

Hallittuun verkkoon liittyminen

SecurityCenterin asentamisen jälkeen tietokoneeseen lisätään taustalla suoritettava verkkoagentti. Verkkoagentti vastaa EasyNetworkissä kelvollisen verkkoyhteyden havaitsemisesta, jaettavien paikallisten tulostimien havaitsemisesta ja verkon tilan valvonnasta.

Ellei verkkoon, johon olet liittynyt, ole liittynyt muita verkkoagenttia suorittavia tietokoneita, järjestelmä tekee sinusta automaattisesti verkon jäsenen ja kehottaa sinua määrittämään, onko verkko luotettava. Ensimmäisenä verkkoon liittyvänä tietokoneena tietokoneesi nimi sisällytetään verkon nimeen. Voit kuitenkin muuttaa verkon nimeä milloin tahansa.

Kun tietokone liittyy verkkoon, kaikille muille verkon tietokoneille lähetetään erillinen liittymispyyntö. Pyyntö voidaan hyväksyä miltä tahansa tietokoneelta, jolla on verkonvalvojan oikeudet. Myöntäjä voi myös määrittää verkkoon liittyvien tietokoneiden oikeuksien tason, esimerkiksi vieraan käyttöoikeudet (vain tiedostonsiirto-oikeus) tai täydet/järjestelmänvalvojan käyttöoikeudet (tiedostonsiirto- ja tiedostonjako-oikeudet). Järjestelmänvalvojaoikeuksin varustetut tietokoneet voivat myöntää EasyNetworkissä käyttöoikeudet muille tietokoneille ja hallita oikeuksia (eli ylentää tai alentaa tietokoneita). Täysillä käyttöoikeuksilla varustetut tietokoneet eivät voi suorittaa kyseisiä järjestelmänvalvojan tehtäviä. Lisäksi järjestelmä suorittaa tietokoneelle turvallisuustarkastuksen, ennen kuin se voi liittyä verkkoon.

Huomaa: Jos tietokoneeseen on asennettu muita McAfee-verkko-ohjelmia, kuten McAfee Wireless Network Security tai Network Manager, tietokone tunnistetaan hallittavaksi tietokoneeksi myös näiden ohjelmien osalta. Tietokoneelle määritetty oikeuksien taso koskee kaikkia McAfee-verkko-ohjelmia. Lisätietoja vieraan käyttöoikeuksista, täysistä käyttöoikeuksista ja järjestelmänvalvojan käyttöoikeuksista McAfee-verkko-ohjelmissa on ohjelmien mukana toimitetuissa käyttöohjeissa.

Verkkoon liittyminen

Kun tietokone liittyy luotettavaan verkkoon ensimmäistä kertaa EasyNetworkin asentamisen jälkeen, näyttöön tulee kehotusikkuna, jossa kysytään, haluatko liittyä hallittuun verkkoon. Kun tietokone hyväksyy liittymiskutsun, lähetetään pyyntö kaikille verkon tietokoneille, joilla on järjestelmänvalvojan oikeudet. Pyyntöön tarvitaan hyväksyntä, ennen kuin tietokone voi jakaa tulostimia ja tiedostoja tai lähettää ja kopioida tiedostoja verkossa. Jos tietokone on verkon ensimmäinen tietokone, se saa automaattisesti verkon järjestelmänvalvojan oikeudet.

Verkkoon liittyminen:

1. Valitse Jaetut tiedostot -ikkunasta **Kyllä, liity verkkoon nyt**. Kun verkon järjestelmänvalvoja-tietokone hyväksyy pyyntösi, näyttöön tulee viesti, jossa kysytään sallitaanko tämän ja muiden verkon tietokoneiden hallita toistensa suojausasetuksia.
2. Jos haluat sallia tietokoneen ja muiden verkon tietokoneiden keskinäisen suojausasetusten hallitsemisen, valitse **Kyllä**, muussa tapauksessa valitse **Ei**.
3. Varmista, että myöntävän tietokoneen näytössä näkyvät samat pelikortit kuin suojausvarmistuksen valintaikkunassa ja valitse **Vahvista**.

Huomaa: Jos myöntävän tietokoneen näytössä näkyvät kortit eivät vastaa suojausvarmistuksen valintaikkunassa näkyviä kortteja, hallitun verkon turvallisuus on uhattuna. Verkkoon liittyminen saattaa altistaa tietokoneesi turvallisuusriskeille, joten valitse suojausvarmistuksen valintaikkunasta **Hylkää**.

Verkon käyttöoikeuksien myöntäminen

Kun tietokone pyytää oikeutta liittyä hallittuun verkkoon, muille verkon järjestelmänvalvojatietokoneille lähetetään viesti. Ensimmäisenä viestiin vastaavasta tietokoneesta tulee myöntäjä. Myöntäjä päättää tietokoneelle myönnettävän käyttöoikeustyypin: vieras, täydet oikeudet tai järjestelmänvalvoja.

Verkon käyttöoikeuksien myöntäminen:

1. Valitse jokin seuraavista valintaruuduista:
   - **Myönnä vieraan käyttöoikeudet**: Sallii käyttäjän lähettää tiedostoja muihin tietokoneisiin, mutta ei salli tiedostojen jakamista.
   - **Myönnä täydelliset käyttöoikeudet kaikkiin hallitun verkon sovelluksiin**: Sallii käyttäjän lähettää ja jakaa tiedostoja.

- **Myönnä järjestelmänvalvojan käyttöoikeudet kaikkiin hallitun verkon sovelluksiin**: Sallii käyttäjän lähettää ja jakaa tiedostoja, myöntää käyttöoikeuksia toisille tietokoneille ja muuttaa toisten tietokoneiden oikeuksien tasoja.

2 Valitse **Myönnä käyttöoikeudet**.

3 Varmista, että tietokoneen näytössä näkyvät samat pelikortit kuin suojausvarmistuksen valintaikkunassa ja valitse **Vahvista**.

Huomaa: Jos tietokoneen näytössä näkyvät kortit eivät vastaa suojausvarmistuksen valintaikkunassa näkyviä kortteja, hallitun verkon turvallisuus on uhattuna. Käyttöoikeuden myöntäminen kyseiselle tietokoneelle saattaa altistaa tietokoneesi tietoturvariskeille, joten valitse suojausvarmistuksen valintaikkunasta **Hylkää**.

Nimeä verkko uudelleen

Oletusarvoisesti verkon nimi sisältää ensimmäisen siihen liittyneen tietokoneen nimen, mutta voit kuitenkin muuttaa verkon nimeä milloin tahansa. Kun nimeät verkon uudelleen, EasyNetworkissä näkyvä verkon kuvaus muuttuu.

Verkon nimeäminen uudelleen:

1. Valitse **Valinnat**-valikosta **Määritä**.
2. Kirjoita verkon nimi Määritä-valintaikkunan **Verkon nimi** -ruutuun.
3. Valitse **OK**.

Hallitusta verkosta poistuminen

Jos liityt hallittuun verkkoon ja päätät, ettet enää halua kuulua verkkoon, voit poistua verkosta. Voit liittyä verkkoon uudelleen milloin tahansa jäsenyydestäsi luovuttuasi. Tarvitset kuitenkin uuden liittymisluvan ja turvallisuustarkastus suoritetaan uudelleen. Lisätietoja on kohdassa Hallittuun verkkoon liittyminen (sivu 183).

Hallitusta verkosta poistuminen

Voit poistua hallitusta verkosta, johon olet aiemmin liittynyt.

Hallitusta verkosta poistuminen:

1. Valitse **Työkalut**-valikosta **Poistu Verkosta**.
2. Valitse Poistu verkosta -valintaikkunasta sen verkon nimi, josta haluat poistua.
3. Valitse **Poistu verkosta**.

LUKU 27

Tiedostojen jakaminen ja lähettäminen

EasyNetworkin avulla voit helposti jakaa ja lähettää tietokoneessasi olevia tiedostoja toisiin verkon tietokoneisiin. Kun jaat tiedostoja, myönnät toisille tietokoneille lukuoikeuden kyseisiin tiedostoihin. Vain hallitun verkon jäsentietokoneet (eli täysillä tai järjestelmänvalvojan oikeuksilla varustetut tietokoneet) voivat jakaa tiedostoja ja lukea toisten jäsentietokoneiden jakamia tiedostoja.

Tässä luvussa

Tiedostojen jakaminen

EasyNetworkin avulla voit jakaa tietokoneessasi olevia tiedostoja helposti toisiin verkon tietokonesiin. Kun jaat tiedostoja, myönnät toisille tietokoneille lukuoikeuden kyseisiin tiedostoihin. Vain hallitun verkon jäsentietokoneet (eli täysillä tai järjestelmänvalvojan oikeuksilla varustetut tietokoneet) voivat jakaa tiedostoja ja lukea toisten jäsentietokoneiden jakamia tiedostoja. Jos jaat kansion, järjestelmä jakaa automaattisesti kaikki kansion sisältämät tiedostot ja alikansiot. Kansioon myöhemmin lisättäviä tiedostoja ei kuitenkaan jaeta. Jos jaettu kansio poistetaan, se poistuu myös Jaetut tiedostot -ikkunasta. Voit lopettaa tiedoston jakamisen milloin tahansa.

Voit käyttää jaettua tiedostoa kahdella tavalla: avaamalla tiedoston suoraan EasyNetworkistä tai kopioimalla tiedoston tietokoneeseesi ja avaamalla sen sitten. Jos jaettujen tiedostojen luettelo on pitkä, voit hakea jaettua tiedostoa tai tiedostoja, joita haluat käyttää.

Huomautus: EasyNetworkillä jaettuja tiedostoja ei voi käyttää toisesta tietokoneesta käsin Windowsin Resurssienhallinnan avulla. EasyNetworkin tiedostojen jakaminen suoritetaan suojattuja yhteyksiä pitkin.

Tiedoston jakaminen

Kun jaat tiedoston, se on niiden hallitun verkon jäsentietokoneiden saatavilla, joilla on täydet tai järjestelmänvalvojan oikeudet.

Tiedoston jakaminen:

1. Etsi Windowsin Resurssienhallinnassa tiedosto, jonka haluat jakaa.
2. Vedä tiedosto Windowsin Resurssienhallinnasta EasyNetworkin Jaetut tiedostot -kansioon.

Vihje: Voit jakaa tiedoston myös valitsemalla **Työkalut**-valikosta **Jaa tiedostot**. Siirry Jakaminen-valintaikkunassa kansioon, jossa jaettava tiedosto sijaitsee, valitse tiedosto ja valitse sitten **Jaa**.

Tiedoston jakamisen lopettaminen

Jos jaat tiedostoa hallitussa verkossa, voit lopettaa jakamisen milloin tahansa. Kun lopetat tiedoston jakamisen, toiset hallitun verkon tietokoneet eivät voi enää käyttää sitä.

Tiedoston jakamisen lopettaminen:

1. Valitse **Työkalut**-valikosta **Lopeta tiedostojen jakaminen**.
2. Valitse Lopeta jakaminen -valintaikkunasta tiedosto, jonka jakamisen haluat lopettaa.
3. Napsauta **Älä jaa** -painiketta.

Jaetun tiedoston kopioiminen

Voit kopioida jaettuja tiedostoja mistä tahansa hallitun verkon tietokoneesta omaan tietokoneeseesi. Tällöin käytössäsi on kopio tiedostosta, vaikka tiedostoa jakanut tietokone lopettaisi jakamisen.

Tiedoston kopioiminen:

- Vedä tiedosto EasyNetworkin Jaetut tiedostot -ikkunasta Windowsin Resurssienhallintaan tai Windowsin työpöydälle.

Vihje: Voit kopioida jaetun tiedoston myös valitsemalla sen EasyNetworkissä ja valitsemalla sitten **Työkalut**-valikosta **Kopioi kohteeseen**. Siirry Kopioi kohteeseen -valintaikkunassa kansioon, johon haluat kopioida tiedoston, valitse se ja napsauta **Tallenna**-painiketta.

Jaetun tiedoston hakeminen

Voit hakea tiedostoa, joka on ollut jaettuna joko omassa tietokoneessasi tai jossakin toisessa verkon jäsentietokoneessa. Kun kirjoitat hakuehtoja, Jaetut tiedostot -ikkunassa näkyvät hakuasi vastaavat tulokset.

Jaetun tiedoston hakeminen:

1. Valitse Jaetut tiedostot -ikkunasta **Haku**.
2. Valitse **Sisältää**-luettelosta jokin seuraavista vaihtoehdoista:
   - **Sisältää sanat**: Hakee tiedostojen tai tiedostopolkujen nimiä, jotka sisältävät kaikki **Tiedoston tai tiedostopolun nimi** -luettelossa määrittämäsi sanat missä tahansa järjestyksessä.
   - **Sisältää minkä tahansa sanoista**: Hakee tiedostojen tai tiedostopolkujen nimiä, jotka sisältävät **Tiedoston tai tiedostopolun nimi** -luettelossa määrittämiäsi sanoja missä tahansa järjestyksessä.

- **Sisältää merkkijonon**: Hakee tiedostojen tai polkujen nimiä, jotka sisältävät **Tiedoston tai tiedostopolun nimi** -luettelossa määrittämäsi koko lauseen.

3 Kirjoita tiedoston tai tiedostopolun nimi osittain tai kokonaan **Tiedoston tai tiedostopolun nimi** -luetteloon.

4 Valitse **Tyyppi**-luettelosta jokin seuraavista tiedostotyypeistä:

- **Mikä tahansa**: Hakee kaikkia jaettuja tiedostotyyppejä.
- **Asiakirja**: Hakee kaikkia jaettuja asiakirjoja.
- **Kuvatiedosto**: Hakee kaikkia jaettuja kuvatiedostoja.
- **Videoleike**: Hakee kaikkia jaettuja videoleiketiedostoja.
- **Äänitiedosto**: Hakee kaikkia jaettuja äänitiedostoja.

5 Valitse **Mistä**- ja **Mihin**-luetteloiden avulla aikaväli, jonka aikana tiedosto on luotu.

Tiedostojen lähettäminen toisiin tietokoneisiin

Voit lähettää tiedostoja toisiin hallitun verkon jäsentietokoneisiin. Ennen tiedoston lähettämistä EasyNetwork tarkistaa, että vastaanottavassa tietokoneessa on riittävästi vapaata levytilaa.

Kun vastaanotat tiedoston, se näkyy EasyNetworkin Saapuneet-kansiossa. Saapuneet-kansio on väliaikainen tallennuspaikka kaikille toisista verkon tietokoneista sinulle lähetetyille tiedostoille. Jos EasyNetwork on auki, kun vastaanotat tiedoston, tiedosto näkyy heti Saapuneet-kansiossa. Muussa tapauksessa viesti näkyy tehtäväpalkin oikeassa reunassa sijaitsevalla Windowsin ilmaisinalueella. Jos et halua nähdä vastaanoton ilmoitusviestejä, voit ottaa ne pois käytöstä. Jos Saapuneet-kansiossa on jo samanniminen tiedosto, uuden tiedoston nimen perään lisätään numeerinen erotin. Tiedostot säilyvät Saapuneet-kansiossa, kunnes hyväksyt ne (eli kopioit ne tietokoneeseesi).

Tiedoston lähettäminen toiseen tietokoneeseen

Voit lähettää tiedoston suoraan toiseen hallitun verkon tietokoneeseen jakamatta sitä. Ennen kuin vastaanottavan tietokoneen käyttäjä voi katsella tiedostoa, se täytyy tallentaa paikalliseen sijaintiin. Lisätietoja on kohdassa Tiedoston hyväksyminen toisesta tietokoneesta (sivu 194).

Tiedoston lähettäminen toiseen tietokoneeseen:

1. Etsi Windowsin Resurssienhallinnassa tiedosto, jonka haluat lähettää.
2. Vedä tiedosto Windowsin Resurssienhallinnasta EasyNetworkissä aktiivisena olevan tietokoneen kuvakkeen päälle.

Vihje: Voit lähettää tietokoneeseen useita tiedostoja painamalla CTRL-näppäintä tiedostoja valitessasi. Voit lähettää tiedostoja myös valitsemalla **Työkalut**-valikosta **Lähetä**, valitsemalla tiedostot ja napsauttamalla sitten **Lähetä**-painiketta.

Tiedoston hyväksyminen toiselta tietokoneelta

Jos toinen hallitun verkon tietokone lähettää sinulle tiedoston, sinun täytyy hyväksyä se (tallentamalla se johonkin tietokoneessasi olevaa kansioon). Jos EasyNetwork ei ole auki tai näkyvissä kun tietokoneeseesi lähetetään tiedosto, saat ilmoitusviestin, joka näkyy tehtäväpalkin oikeassa reunassa sijaitsevalla Windowsin ilmaisinalueella. Avaa EasyNetwork napsauttamalla ilmoitusviestiä, niin pääset käyttämään tiedostoa.

Tiedoston vastaanottaminen toisesta tietokoneesta:

- Napsauta **Vastaanotettu**-painiketta ja vedä tiedosto EasyNetworkin Saapuneet-kansiosta Windowsin Resurssienhallinnan kansioon.

Vihje: Voit vastaanottaa tiedoston toisesta tietokoneesta myös valitsemalla tiedoston EasyNetworkin Saapuneet-kansiosta ja valitsemalla sitten **Työkalut**-valikosta **Hyväksy**. Siirry Hyväksy kansioon -valintaikkunassa siihen kansioon, johon haluat tallentaa vastaanottamasi tiedostot, valitse se ja napsauta **Tallenna**-painiketta.

Ilmoituksen saaminen tiedoston lähettämisestä

Voit saada ilmoituksen, kun toinen hallitun verkon tietokone lähettää sinulle tiedoston. Jos EasyNetwork ei ole auki tai se ei ole näkyvissä, ilmoitusviesti näkyy tehtäväpalkin oikeassa reunassa sijaitsevalla Windowsin ilmaisinalueella.

Ilmoituksen saaminen tiedoston lähettämisestä:

1. Valitse **Valinnat**-valikosta **Määritä**.
2. Valitse Määritä-valintaruudusta **Ilmoita, kun joku toinen tietokone lähettää tiedostoja** -valintaruutu.
3. Valitse **OK**.

LUKU 28

Tulostinten jakaminen

Kun olet liittynyt hallittuun verkkoon, EasyNetwork jakaa automaattisesti tietokoneeseesi liitetyt paikalliset tulostimet. Lisäksi se havaitsee toisten verkon tietokoneiden tulostimet ja sallii kyseisten tulostimien määrittämisen ja käyttämisen.

Tässä luvussa

Jaettujen tulostinten käyttäminen

Kun olet liittynyt hallittuun verkkoon, EasyNetwork jakaa automaattisesti tietokoneeseesi liitetyt paikalliset tulostimet ja käyttää jaetun tulostimen nimenä tulostimen nykyistä nimeä. Lisäksi se havaitsee toisten verkon tietokoneiden tulostimet ja sallii kyseisten tulostimien määrittämisen ja käyttämisen. Jos olet määrittänyt tulostinohjaimen tulostamaan verkon tulostuspalvelimen kautta (esimerkiksi langaton USB-tulostuspalvelin), EasyNetwork tulkitsee tulostimen paikalliseksi tulostimeksi ja jakaa sen verkossa. Voit lopettaa tulostimen jakamisen milloin tahansa.

EasyNetwork havaitsee myös kaikkien muiden verkon tietokoneiden jakamat tulostimet. Jos se havaitsee etätulostimen, jota ei ole vielä kytketty tietokoneeseesi, Jaetut tiedostot -ikkunassa näkyy **Saatavilla olevat verkkotulostimet** -linkki, kun avaat EasyNetworkin ensimmäisen kerran. Sen avulla voit asentaa saatavilla olevia tulostimia tai poistaa tietokoneeseen jo kytkettyjen tulostimien asennuksia. Voit myös päivittää verkossa havaittujen tulostimien luettelon.

Jos et ole vielä liittynyt hallittuun verkkoon, mutta olet kytkeytynyt siihen, voit käyttää jaettuja tulostimia Windowsin Ohjauspaneelin kautta.

Tulostimen jakamisen lopettaminen

Voit lopettaa tulostimen jakamisen milloin tahansa. Jäsenet, jotka ovat asentaneet tulostimen, eivät voi enää tulostaa sillä.

Tulostimen jakamisen lopettaminen:

1. Valitse **Työkalut**-valikosta **Tulostimet**.
2. Valitse Hallitse tulostimia -valintaikkunasta sen tulostimen nimi, jonka jakamisen haluat lopettaa.
3. Napsauta **Älä jaa** -painiketta.

Saatavilla olevan verkkotulostimen asentaminen

Hallitun verkon jäsenenä voit käyttää verkon jaettuja tulostimia. Ennen käyttöä on asennettava kyseisen tulostimen käyttämä tulostinohjain. Jos tulostimen omistaja lopettaa tulostimen jakamisen sen jälkeen kun olet asentanut sen, et voi enää tulostaa kyseisellä tulostimella.

Saatavilla olevan verkkotulostimen asentaminen:

1. Valitse **Työkalut**-valikosta **Tulostimet**.
2. Valitse tulostimen nimi Saatavilla olevat verkkotulostimet -valintaikkunasta.
3. Napsauta **Asenna**-painiketta.

LUKU 29

Liitteet

Termisanasto luettelee ja määrittää McAfee-tuotteissa useimmin käytetyt tietoturvatermit.

Tietoja McAfeesta -sivu sisältää lakeihin liittyvää tietoa McAfee Corporationista.

Sanasto

8

802.11

Kokoelma langattoman lähiverkkotekniikan IEEE-standardeja. 802.11 määrittää langattoman asiakkaan ja tukiaseman tai kahden langattoman asiakkaan välisen maanpäällisen jakeluliittymän. 802.11 sisältää useita eri määrityksiä, kuten 802.11a-standardin, jonka avulla voidaan käyttää jopa 54 Mbps verkkoyhteyksiä 5 Ghz kaistassa, 802.11b-standardin, jonka avulla voidaan käyttää jopa 11 Mbps verkkoyhteyksiä 2,4 Ghz kaistassa, 802.11g-standardin, jonka avulla voidaan käyttää jopa 54 Mbps verkkoyhteyksiä 2,4 Ghz kaistassa sekä 802.11i:n, joka on kokoelma erilaisia Ethernet-verkkojen suojausstandardeja.

802.11a

802.11-standardin laajennus, jota käytetään langattomissa lähiverkoissa ja jonka avulla tietoa voidaan siirtää jopa 54 Mbps nopeudella 5 Ghz kaistassa. Vaikka tiedonsiirron nopeus on suurempi kuin 802.11b-standardissa, laajennuksen kantoalue on paljon pienempi.

802.11b

802.11-standardin laajennus, jota käytetään langattomissa lähiverkoissa ja jonka avulla tietoa voidaan siirtää jopa 11 Mbps nopeudella 2,4 Ghz kaistassa. 802.11b on tällä hetkellä yleisimmin käytetty langattoman tiedonsiirron standardi.

802.11g

802.11-standardin laajennus, jota käytetään langattomissa lähiverkoissa ja jonka avulla tietoa voidaan siirtää jopa 54 Mbps nopeudella 2,4 Ghz kaistassa.

802.1x

Wireless Home Network Security ei tue tätä standardia. Tavallisten ja langattomien verkkojen IEEE-todennusstandardi, jota käytetään useimmiten 802.11-standardin langattomien verkkoyhteyksien yhteydessä. Tämä standardi tarjoaa vahvan, molemminpuolisen todennuksen asiakkaan ja todennuspalvelimen välillä. Lisäksi 802.1x tarjoaa dynaamisen käyttäjä- ja istuntokohtaisen WEP-avaimen, joka poistaa staattisia WEP-avaimia käyttävien verkkojen hallintavaatimukset ja turvallisuusriskit.

A

arkistointi

Tarkkailtavien tiedostojen varmuuskopiointi paikallisesti CD- tai DVD-levylle, USB-asemalle, ulkoiselle kiintolevyasemalle tai verkkoasemalle.

arkistointi

Tarkkailtavien tiedostojen varmuuskopiointi paikallisesti CD- tai DVD-levylle, USB-asemalle, ulkoiselle kiintolevyasemalle tai verkkoasemalle.

asiakas

Sovellus, joka toimii henkilökohtaisessa tietokoneessa tai työasemassa ja käyttää palvelinta tiettyjen toimintojen suorittamiseen. Esimerkiksi sähköpostiasiakas on sovellus, jonka avulla voit lähettää ja vastaanottaa sähköpostia.

avain

Kirjaimista ja/tai numeroista muodostuva sarja, jota kaksi laitetta käyttävät niiden välisen viestinnän todentamiseen. Molemmilla laitteilla täytyy olla sama avain. Katso myös kohdat WEP, WPA. WPA2, WPA-PSK ja WPA2-PSK.

avainsana

Sana, jonka avulla voidaan määrittää varmuuskopioidun tiedoston suhde tai yhteys muihin tiedostoihin, joille on määritetty sama avainsana. Avainsanojen määrittäminen tiedostoille tekee Internetissä julkaistujen tiedostojen etsimisestä helpompaa.

D

DNS

Akronyymi, joka tulee sanoista Domain Name System (toimialueen nimijärjestelmä). Hierarkinen järjestelmä, jossa Internetin isännillä on sekä toimialueen nimiosoite (kuten bluestem.prairienet.org) että IP-osoite (kuten 192.17.3.4). Käyttäjät käyttävät toimialueen nimiosoitetta ja se käännetään automaattisesti numeeriseksi IP-osoitteeksi, jota käyttävät pakettien reititysohjelmistot. DNS-nimet muodostuvat päätason toimialueesta (kuten .com, .org ja .net), alemman tason toimialueesta (yrityksen, yhteisön tai henkilön sivuston nimi) ja mahdollisesti yhdestä tai useammasta alitoimialueesta (alemman tason toimialueen palvelimet). Katso myös kohdat DNS-palvelin ja IP-osoite.

DNS-palvelin

Toimialueen nimijärjestelmäpalvelimen lyhenne. Tietokone, joka vastaa toimialueen nimi (DNS) -pyyntöihin. DNS-palvelin ylläpitää tietokantaa isäntätietokoneista ja niiden IP-osoitteista. Jos DNS-palvelimeen lähetetään pyyntö esimerkiksi nimellä apex.com, palvelin palauttaa Apex-yhtiön IP-osoitteen. DNS-palvelin tunnetaan myös nimellä nimipalvelin. Katso myös kohdat DNS ja IP-osoite.

E

eristäminen

Kun epäilyttävä tiedosto tunnistetaan, se asetetaan eristykseen. Voit sitten suorittaa asianmukaisen toiminnon.

ESS (laajennettu palvelukokoelma)

Kahden tai useamman verkon kokoelma, joka muodostaa yhtenäisen aliverkon.

eväste

Webissä käytettävä tietolohko, jonka Web-palvelin tallentaa asiakasjärjestelmään. Kun käyttäjä palaa samaan Web-sivustoon, selain lähettää evästeen kopion takaisin palvelimeen. Evästeitä käytetään käyttäjien tunnistamiseen, palvelimen ohjaamiseen, jotta se lähettää mukautetun version pyydetystä Web-sivusta, käyttäjän tilitietojen lähettämiseen ja muihin hallinnollisiin käyttötarkoituksiin.

Evästeiden avulla Web-sivustot muistavat kuka sinä olet ja pitävät kirjaa siitä, kuinka paljon vierailijoita Web-sivustossa on käynyt, milloin he ovat vierailleet ja mitä sivuja he ovat näyttäneet. Evästeet auttavat myös yrityksiä mukauttamaan Web-sivustonsa sinua varten. Useat Web-sivustot vaativat käyttäjänimeä ja salasanaa tiettyjen sivujen käyttämiseen, ja lähettävät evästeen tietokoneeseesi, jotta sinun ei tarvitse kirjautua sisään jokaisella vierailukerralla. Evästeitä voidaan kuitenkin käyttää myös haitallisiin käyttötarkoituksiin. Internetin mainosyritykset käyttävät usein evästeitä päätelläkseen mitä sivustoja sinä käytät useimmiten ja julkaisevat sitten mainoksia suosikki-Web-sivustoissasi. Ennen kuin hyväksyt sivuston evästeet, varmista, että sivusto on luotettava.

Vaikka evästeet ovat monen laillisen yrityksen tietolähde, ne voivat olla myös hakkereiden tietolähde. Useat verkkokauppoja sisältävät Web-sivustot laittavat luottokortti- ja muita henkilökohtaisia tietoja evästeisiin, jotta asiakkaiden on helpompi tehdä ostoksia. Valitettavasti evästeet saattavat sisältää tietoturva-aukkoja, joiden avulla hakkerit voivat päästä käsiksi asiakkaiden tietokoneisiin tallennettujen evästeiden sisältämiin tietoihin.

H

hallittu verkko

Kotiverkko, jossa on kahdentyyppisiä jäseniä: hallittuja jäseniä ja hallinnan piiriin kuulumattomia jäseniä. Hallitut jäsenet sallivat muiden verkon tietokoneiden valvoa McAfee-suojaustasoaan, hallinnan piiriin kuulumattomat eivät.

I

Internet

Internet sisältää valtavan määrän toisiinsa liitettyjä verkkoja, jotka käyttävät TCP/IP-protokollaa tiedonsiirtoon ja etsimiseen. Internet perustuu Yhdysvaltojen puolustusministeriön 1960-luvun lopulla ja 1970-luvun alussa rahoittamaan yliopistojen ja korkeakoulujen tietokoneiden muodostamaan verkkoon, jota kutsuttiin ARPANET:ksi. Tänä päivänä Internet on maailmanlaajuinen verkko, joka sisältää lähes 100 000 itsenäistä verkkoa.

Intranet

Yleensä organisaation sisäinen yksityinen verkko, joka toimii samalla tavoin kuin Internet. Nykyinen käytäntö on, että opiskelijat ja työntekijät voivat muodostaa Intranet-yhteyden kampusten ja yritysten tilojen ulkopuolelta. Palomuurit, sisäänkirjautumistoiminnot ja salasanat ovat suunniteltu järjestelmien suojaamiseksi.

IP-huijausyritys

IP-paketin IP-osoitteiden väärentäminen. Tätä huijauskeinoa käytetään useissa erilaisissa hyökkäyksissä, kuten istunnon kaappauksissa. Sitä käytetään usein myös roskapostiviestien otsikoiden väärentämiseen, jotta viestejä ei voida jäljittää.

IP-osoite

Internet-protokollaosoite tai IP-osoite on ainutkertainen numerosarja, joka koostuu neljästä pistein eritellystä osasta (esim. 63.227.89.66). Jokaisella Internetin tietokoneella aina suurimmasta palvelimesta matkapuhelimen kautta verkkoyhteyttä käyttävään kannettavaan tietokoneeseen on oma yksilöivä IP-osoitteensa. Kaikilla tietokoneilla ei ole toimialueen nimeä, mutta jokaisella tietokoneella on IP-osoite.

Seuraava luettelo sisältää muutamia epätavallisia IP-osoitetyyppejä:

- Reitittämättömät IP-osoitteet: Näitä IP-osoitteita kutsutaan myös henkilökohtaiseksi IP-tilaksi. Näitä osoitteita ei voi käyttää Internetissä. Yksityiset IP-osoitelohkot ovat 10.x.x.x, 172.16.x.x - 172.31.x.x ja 192.168.x.x.
- Silmukka-IP-osoitteet**:** Silmukkaosoitteita käytetään testitarkoituksiin. Tähän IP-osoitelohkoon lähetetty tietoliikenne palautuu suoraan takaisin paketin luoneeseen laitteeseen. Se ei koskaan poistu laitteesta ja sitä käytetään pääasiassa laitteistojen ja ohjelmistojen testaamiseen. Silmukka-IP-osoitelohko on 127.x.x.x.

Tyhjä IP-osoite: Tämä on virheellinen osoite. Kun tämä osoite näkyy, se viittaa siihen, että tietoliikenteellä on tyhjä IP-osoite. On itsestään selvää, että tämä ei ole tavallista, ja se useimmiten viittaa siihen, että liikenteen lähettäjä yrittää tahallaan salata tietoliikenteen lähdeosoitetta. Lähettäjä ei voi vastaanottaa vastauksia tietoliikenteeseen, ellei pakettia vastaanota sovellus, joka pystyy ymmärtämään paketin sisällön ja tulkitsemaan kyseistä sovellusta koskevia yksityiskohtaisia ohjeita. Mikä tahansa IP-osoite, joka alkaa nollalla (0.x.x.x) on tyhjä IP-osoite. Esimerkiksi 0.0.0.0 on tyhjä IP-osoite.

J

jaettu salaisuus

Katso myös kohta RADIUS. Suojaa RADIUS-viestien arkaluontoisia osia. Jaettu salaisuus on salasana, jonka todentaja ja todennuspalvelun jakavat jollakin suojatulla keinolla.

jakaminen

Toiminto, jonka avulla sähköpostiviestin vastaanottajat voivat ladata varmuuskopioituja tiedostoja rajoitetun ajanjakson aikana. Kun tiedosto jaetaan, lähetetään tiedoston varmuuskopioitu versio sähköpostiviestin vastaanottajille. Viestin vastaanottajat saavat sähköpostiviestin McAfee Data Backupilta, jossa heille kerrotaan jaettavista tiedostoista. Sähköpostiviesti sisältää linkin, josta jaettavat tiedostot voidaan ladata.

julkaiseminen

Varmuuskopioidun tiedoston julkaiseminen Internetissä.

K

kaistanleveys

Tiedon määrä, joka voidaan siirtää tietyssä ajassa. Digitaalisten laitteiden kaistanleveys ilmoitetaan useimmiten bitteinä per sekunti (bps) tai tavuina per sekunti. Analogisten laitteiden kaistanleveys ilmoitetaan värähdyksinä sekunnissa tai hertseinä (Hz).

kieltoluettelo

Haitallisten Web-sivustojen luettelo. Web-sivusto voidaan sijoittaa kieltoluetteloon, jos se sisältää petollisia toimintoja tai yrittää käyttää hyväkseen selaimen tietoturva-aukkoja lähettääkseen mahdollisia haittaohjelmia käyttäjän tietokoneeseen.

kirjasto

Data Backup -käyttäjien julkaisemien tiedostojen online-tallennealue. Kirjasto on Internetin Web-sivusto, jota voi käyttää kuka tahansa Internet-käyttäjä.

komentosarja

Komentosarjat voivat luoda, kopioida tai poistaa tiedostoja. Ne voivat avata myös Windowsin rekisterin.

kuva-analyysi

Estää mahdollisesti sopimattomia kuvia tulemasta näkyville. Kuvat estetään kaikilta muilta käyttäjiltä, paitsi aikuisikäryhmän jäseniltä.

Käyttöpiste

Verkkolaite, jonka avulla 802.11-standardia käyttävät asiakkaat voivat muodostaa yhteyden lähiverkkoon. Käyttöpisteet laajentavat langattoman verkon käyttöaluetta. Käyttöpisteitä kutsutaan joskus myös langattomiksi reitittimiksi.

käytönvalvonta-asetukset

Käytönvalvonta-asetuksilla voit määrittää sisältöluokitukset Web-sivustoille ja sisällöille, joita käyttäjä voi katsella, sekä rajoittaa Internet-käytön ajankohtaa ja kestoa. Käytönvalvonta-asetuksilla voit myös rajoittaa käyttäjien pääsyä Web-sivustoihin ja sallia tai estää käytön ikäryhmien käyttöoikeuksien tai salasanojen perusteella.

L

Langaton lähiverkko (WLAN)

Katso myös kohta Lähiverkko. Lähiverkko, johon voidaan muodostaa langaton yhteys. Lähiverkko käyttää korkeataajuuksisia radioaaltoja johtojen sijaan solmujen väliseen viestintään.

langaton verkkopiste

Tietty maantieteellinen sijainti, jossa mobiileja yhteyksiä käyttävät vierailijat voivat käyttää julkisia langattomia laajakaistaverkkopalveluja langattoman käyttöpisteen avulla. Langattomat verkkopisteet (hotspots) sijaitsevat usein suuria ihmismääriä sisältävissä paikoissa kuten lentokentillä, rautatieasemilla, kirjastoissa, satamissa, messukeskuksissa ja hotelleissa. Langattomat verkkopisteet toimivat tavallisesti hyvin rajoitetulla käyttöalueella.

langaton verkkosovitin

Sisältää vaadittavat virtapiirit, joiden avulla tietokone tai muu laite voi keskustella langattoman reitittimen kanssa (eli luoda yhteyden langattomaan verkkoon). Langattomat verkkosovittimet voidaan rakentaa laitteiston päävirtapiirien yhteyteen tai ne voivat olla erillisiä lisälaitteita, jotka lisätään laitteeseen liittämällä ne sopivaan porttiin.

Langattomat PCI-verkkosovitinkortit

Liittää työaseman verkkoon. Kortti asetetaan tietokoneen PCI-korttipaikkaan.

Langattomat USB-verkkosovitinkortit

Langattomat USB-verkkosovitinkortit tarjoavat laajennettavan Plug-and-Play-sarjakäyttöliittymän. Tämä liittymä tarjoaa standardinmukaisen, halvan langattoman yhteyden oheislaitteille, kuten näppäimistöille, hiirille, peliohjaimille, tulostimille, skannereille, tallennuslaitteille ja videokonferenssikameroille.

luvattomat käyttöpisteet

Käyttöpiste, jonka toiminnalle yritys ei ole myöntänyt lupaa. Ongelma on siinä, että luvattomat käyttöpisteet eivät usein noudata langattomien lähiverkkojen suojauskäytäntöjä. Luvaton käyttöpiste mahdollistaa avoimen suojaamattoman käyttöliittymän yrityksen verkkoon fyysisesti kontrolloidun tilan ulkopuolelta.

Oikein suojatussa langattomassa lähiverkossa luvattomat käyttöpisteet aiheuttavat enemmän vahinkoa kuin luvattomat käyttäjät. Jos yritys käyttää toimivia todennusmekanismeja, luvattomat langattoman lähiverkon käyttäjät eivät todennäköisesti pysty käyttämään yrityksen arvokkaita liiketoimintaresursseja. Ongelmia syntyy kuitenkin silloin, kun yrityksen työntekijä tai hakkeri liittää verkkoon luvattoman käyttöpisteen. Lähes kuka tahansa käyttäjä, jolla on käytössään 802.11-laite pystyy käyttämään yrityksen lähiverkkoa luvattoman käyttöpisteen avulla. Tällä tavoin he pääsevät hyvin lähelle yrityksen tärkeitä resursseja.

Lähiverkko

Tietokoneverkko, joka kattaa suhteellisen pienen alueen. Useimmat lähiverkot ovat rajoitettu yksittäiseen rakennukseen tai rakennusten muodostamaan ryhmään. Kuitenkin yksi lähiverkko voidaan liittää muihin lähiverkkoihin minkä tahansa välimatkan päästä puhelin- ja radioaaltojen avulla. Tällä tavalla yhdistettyjen lähiverkkojen järjestelmää kutsutaan suuralueverkoksi. Useimmat lähiverkot liittävät työasemat ja henkilökohtaiset tietokoneet toisiinsa yksinkertaisten keskittimien tai valitsimien avulla. Jokaisella lähiverkon solmulla (yksittäisellä tietokoneella) on oma suorittimensa, jonka avulla se suorittaa ohjelmia, mutta se voi myös käyttää tietoja ja laitteita (esim. tulostimia) missä tahansa lähiverkon sisällä. Tämä tarkoittaa sitä, että useat käyttäjät voivat jakaa kalliita laitteita, kuten laser-tulostimia, sekä tietoja. Käyttäjät voivat myös käyttää lähiverkkoa viestiäkseen toistensa kanssa, esimerkiksi lähettämällä sähköpostia tai käyttämällä keskusteluohjelmia.

M

MAC (MAC-osoite tai viestin todennuskoodi)

Jos haluat lisätietoja ensimmäisestä termistä, katso kohta MAC-osoite. Viestin todennuskoodi on koodi, jota käytetään määritetyn viestin tunnistamiseen (esim. RADIUS-viestin tunnistamiseen). Koodi on yleensä kryptograafisesti vahva hajautuskokoelma viestin sisältämistä tiedoista, joka sisältää ainutlaatuisen arvon, jonka avulla koodin suojaus voidaan varmistaa.

MAC-osoite

Alemman tason osoite, joka on määritetty verkkoa käyttävälle fyysiselle laitteelle.

mahdollinen haittaohjelma

Vakoilu- ja mainosohjelmat ja muut ohjelmat, jotka keräävät ja lähettävät tietoja ilman käyttäjän myöntämää lupaa ovat mahdollisia haittaohjelmia.

MAPI-tili

Akronyymi, joka tulee sanoista Messaging Application Programming Interface. Microsoftin käyttöliittymämääritys, jonka avulla eri viestintä- ja työryhmäsovellukset (kuten sähköposti, ääniviesti ja faksi) toimivat yhden asiakkaan kautta, kuten esimerkiksi Exchange-asiakkaan kautta. Tästä syystä MAPI:a käytetään usein yritysympäristöissä, jos yritys käyttää Microsoft Exchange Serveriä. Kuitenkin monet ihmiset käyttävät myös Microsoft Outlookia henkilökohtaisen sähköpostinsa lukemiseen.

mato

Mato on itseään kopioiva virus, joka piileskelee tietokoneen aktiivisessa muistissa ja voi lähettää itsensä kopioita sähköpostiviesteissä. Madot kopioituvat ja kuluttavat järjestelmäresursseja, hidastaen tietokoneen suorituskykyä tai keskeyttäen tehtäviä.

melko tärkeät tarkkailukohteet

Tietokoneellasi sijaitseva kansio, jonka muutoksia McAfee Data Backup tarkkailee. Jos määrität melko tärkeän tarkkailukohteen, McAfee Data Backup varmuuskopioi ainoastaan kyseisen kansion tarkkailtavien tiedostotyyppien mukaiset tiedostot, ilman alihakemistoja.

MITM-hyökkäys

Hyökkääjä salakuuntelee julkisen avaimenvaihdon viestejä ja lähettää ne sitten uudelleen, vaihtaen oman julkisen avaimensa pyydetyn tilalle siten, että alkuperäiset viestien lähettäjät näyttävät yhä keskustelevan suoraan toistensa kanssa. Hyökkääjä käyttää ohjelmaa, joka näyttää olevan asiakkaan palvelin ja palvelimen asiakas. Hyökkäystä saatetaan käyttää yksinkertaisesti siksi, että hyökkääjä pääsee näkemään viestejä tai että hän voi muokata viestejä ennen niiden uudelleenlähettämistä. Termi MITM (Man-in-the-middle)on peräisin pallopelistä, jossa pelaajat yrittävät heittää pallon suoraan toisilleen ja välissä oleva pelaaja yrittää siepata pallon.

MSN-tili

Akronyymi, joka tulee sanoista Microsoft Network. Online-palvelu ja Internet-portaali. Tämä on Web-pohjainen tili.

O

online-varmuuskopiovarasto

Online-palvelimen sijainti, jonne tarkkailtavat tiedostot tallennetaan varmuuskopioinnin jälkeen.

otsikko

Otsikko on viestiin lisättävää tietoa, joka säilyy viestissä sen koko elinajan. Otsikko kertoo Internet-ohjelmistolle kuinka viesti tulee toimittaa, mihin osoitteeseen viestin vastaukset tulee lähettää, mikä on kyseisen sähköpostiviestin yksilöivä tunniste sekä muita viestiä koskevia hallinnollisia tietoja. Otsikkokenttien esimerkkejä ovat: Vastaanottaja, lähettäjä, CC, päivämäärä, aihe, viestin tunniste ja vastaanotettu.

P

pakkaus

Toiminto, jonka avulla tietoja (tiedostoja) pakataan muotoon, joka minimoi niiden tallentamiseen tai siirtämiseen vaadittavan levytilan määrän.

palauttaminen

Tiedoston kopion noutaminen online-varmuuskopiovarastosta tai arkistosta.

palomuuri

Järjestelmä, joka on kehitetty estämään luvattomia saapuvia ja lähteviä yhteyksiä yksityisessä verkossa. Palomuureja on sekä laitteistoina että ohjelmistoina, sekä niiden yhdistelminä. Palomuureja käytetään usein luvattomien Internet-käyttäjien estämiseen, jotta he eivät pysty muodostamaan yhteyttä Internetiin liitettyihin yksityisiin verkkoihin, kuten Intranet-verkkoihin. Kaikki Intranetin saapuvat ja lähtevät viestit kulkevat palomuurin läpi. Palomuuri tutkii jokaisen viestin ja estää ne viestit, jotka eivät vastaa määritettyä suojausehtoja. Palomuuria pidetään henkilökohtaisten tietojen ensisijaisena suojauskeinona. Tietoturvallisuuden lisäämiseksi tietoja voidaan myös salata.

palvelin

Tietokone tai ohjelmisto, joka tarjoaa tiettyjä palveluja muissa tietokoneissa suoritettaville ohjelmille. Internet-palveluntarjoajasi postipalvelin on ohjelmisto, joka käsittelee kaikkia palveluntarjoajan käyttäjien saapuvia ja lähteviä sähköpostiviestejä. Lähiverkon palvelin on laitteisto, joka muodostaa verkon pääsolmun. Siinä voi olla myös ohjelmisto, joka tarjoaa tiettyjä palveluja, tietoja tai muita toimintoja kaikille siihen liitetyille asiakastietokoneille.

Palvelun esto

Internetin palvelunestohyökkäys on tapahtuma, jossa käyttäjältä tai yhteisöltä estetään jonkin resurssin palvelujen käyttö, joita he normaalisti pystyvät käyttämään. Tavallisesti palvelun menettäminen tarkoittaa kykenemättömyyttä käyttää tiettyä verkkopalvelua, kuten sähköpostia tai kaikkien verkkoyhteyksien ja palveluiden väliaikaista menettämistä. Pahimmassa tapauksessa esimerkiksi Web-sivusto, jolla on miljoonia käyttäjiä voi joutua keskeyttämään toimintansa. Palvelunestohyökkäys voi myös tuhota tietokonejärjestelmän ohjelmia ja tiedostoja. Vaikka palvelunestohyökkäykset ovat tavallisesti tarkoituksellisia ja haitallisia, niitä voi joskus tapahtua myös vahingossa. Palvelunestohyökkäys on tietokonejärjestelmien tietoturvauhka, joka ei tavallisesti aiheuta tietovarkauksia tai muita suojauksen menetyksiä. Kyseiset hyökkäykset voivat kuitenkin aiheuttaa kohdehenkilölle tai yritykselle huomattavia taloudellisia tappioita tai aikaavieviä korjaustöitä.

perusteksti

Mikä tahansa viesti, joka ei ole salattu.

phishing-huijaus

Phishing-huijaus on huijausyritys, jossa hakkeri pyrkii varastamaan tärkeitä tietoja, kuten luottokortti- ja sosiaaliturvanumeroita, käyttäjätunnuksia ja salasanoja. Phishing-huijausyrityksessä mahdollisille uhreille lähetetään virallisen näköinen sähköpostiviesti, jonka lähettäjä näyttää olevan uhrin Internet-palveluntarjoaja, pankki tai usein käyttämä verkkokauppa. Sähköpostiviestejä saatetaan lähettää valituissa luetteloissa oleville henkilöille tai missä tahansa luettelossa oleville henkilöille sillä oletuksella, että osa viestin vastaanottajista todella sattuu omistamaan tilin väärennetyssä organisaatiossa.

pika-arkistointi

Ainoastaan niiden tarkkailtavien tiedostojen arkistoiminen, jotka ovat muuttuneet viimeisimmän täydellisen tai pika-arkistoinnin jälkeen.

ponnahdusikkunat

Pieniä ikkunoita, jotka tulevat näyttöön muiden ikkunoiden päälle. Ponnahdusikkunoita käytetään useimmiten mainosten näyttämiseen Web-selaimissa. McAfee estää ponnahdusikkunat, jotka ladataan automaattisesti, kun Web-sivu ladataan selaimeesi. McAfee ei estä ponnahdusikkunoita, jotka ladataan, kun napsautat linkkiä.

POP3-tili

Akronyymi, joka tulee sanoista Post Office Protocol 3. Useimmilla kotikäyttäjillä on POP3-tili. Tämä on POP-standardin nykyversio, jota käytetään yleisesti TCP/IP-verkoissa. POP3-tili tunnetaan myös tavanomaisena sähköpostitilinä.

portti

Paikka, johon tieto kulkee tietokoneelle tai tietokoneelta, esimerkiksi tavallinen analoginen modeemi kytkettynä sarjaporttiin. TCP/IP-yhteyksien porttien numerot ovat virtuaalisia arvoja, joita käytetään tietoliikenteen erottelemiseen sovelluskohtaisiin tietovirtoihin. Portit ovat määritetty standardiprotokollille, kuten SMTP:lle ja HTTP :lle siten, että ohjelmat tietävät mihin porttiin niiden kannattaa yrittää muodostaa yhteys. TCP-pakettien kohdeportti viittaa etsittävään sovellukseen tai palvelimeen.

PPPoE

Akronyymi, joka tulee sanoista Point-to-Point Protocol Over Ethernet. Useat Internet-palveluntarjoajat käyttävät PPPoE:ta, koska protokolla tukee PPP:ssä usein käytettyjä protokollatasoja ja todennusta, ja PPPoE:n avulla voidaan muodostaa Point-to-Point-yhteys Ethernetin normaalisti monipisteisessä arkkitehtuurissa.

protokolla

Sovittu muoto, jonka avulla tietoa siirretään kahden laitteen välillä. Käyttäjän näkökulmasta protokollien ainoa kiinnostava puoli on se, että käyttäjän tietokoneen tai laitteen täytyy tukea oikeita protokollia, jos he haluavat kommunikoida muiden tietokoneiden kanssa. Protokolla voidaan ottaa käyttöön joko laitteistossa tai ohjelmistossa.

puskurin ylivuoto

Puskurin ylivuotoja esiintyy, kun epäilyttävät ohjelmat tai prosessit yrittävät tallentaa tietokoneen puskuriin (tietojen väliaikaiselle tallennusalueelle) enemmän tietoja kuin mitä siihen mahtuu. Tämä vioittaa vierekkäisissä puskureissa olevia kelvollisia tietoja tai korvaa ne.

R

RADIUS (Remote Access Dial-In User Service)

Protokolla, jonka avulla käyttäjät voidaan todentaa. Protokollaa käytetään useimmiten etäyhteyksien yhteydessä. Protokolla kehitettiin alunperin etäkäyttöpalvelimia varten, mutta nykyään sitä käytetään useissa erilaisissa todennusympäristöissä, kuten esimerkiksi langattoman verkon käyttäjän jaetun salaisuuden todentamisessa 802.1x-standardin yhteydessä.

reaaliaikainen tarkistus

Tiedostot tarkistetaan virusten ja muiden haitallisten mekanismien varalta, kun sinä tai tietokoneesi käytät niitä.

reititin

Verkkolaite, joka edelleenlähettää paketteja verkosta toiseen. Reitittimet perustuvat sisäisiin reititystaulukoihin ja ne lukevat jokaisen saapuvan paketin ja päättävät sitten miten paketti lähetetään eteenpäin. Lähtevien pakettien lähetysosoite reitittimessä määräytyy paketin lähde- ja kohdeosoitteen, sekä verkkoliikenteen tilatietojen, kuten verkon käytön, kustannusten ja heikkojen yhteyksien perusteella, Reittimiä kutsutaan joskus myös käyttöpisteiksi.

roaming

Toiminto, jonka avulla voidaan siirtyä yhden käyttöpisteen käyttöalueelta toiselle ilman palvelukatkoja tai yhteyden menetyksiä.

S

salasana

Useimmiten aakkosnumeerinen koodi, jonka avulla voit käyttää tietokonetta, tiettyä ohjelmaa tai Web-sivustoa.

Salasanasäilö

Henkilökohtaisten salasanojesi suojattu tallennesäilö. Sen avulla voit tallentaa salasanasi luottaen siihen, että kukaan muu käyttäjä, ei edes McAfee-valvoja tai järjestelmänvalvoja, saa niitä käyttöönsä.

salattu teksti

Tietoja, jotka ovat salattu. Salattu teksti ei ole lukukelpoista ennen kuin se on muunnettu perustekstiksi (salaamattomaksi) salausavaimen avulla.

salaus

Toiminto, jossa tietoa muunnetaan tekstistä koodiksi muuttaen tietoa siten, että henkilöt, jotka eivät tiedä kuinka salaus puretaan eivät voi lukea sitä.

sanakirjahyökkäys

Sanakirjahyökkäykset suoritetaan siten, että käyttäjän salasana yritetään päätellä kokeilemalla useita erilaisia tietyn luettelon sisältämiä sanoja. Hyökkääjät eivät yritä kaikkia mahdollisia sanayhdistelmiä manuaalisesti, vaan käyttävät työkaluja, jotka yrittävät tunnistaa käyttäjän salasanan automaattisten toimintojen avulla.

selain

Asiakasohjelma, joka tekee pyyntöjä Web-palvelimille Internetissä HTTP-protokollan (Hypertext Transfer Protocol) avulla. Web-selain näyttää sisällön käyttäjälle graafisessa muodossa.

sisältöluokitus-ryhmät

Ikäryhmä, johon käyttäjä kuuluu. Sisältö luokitellaan (eli se on saatavissa tai estetty) käyttäjän sisältöluokitusryhmän perusteella. Sisältöluokitusryhmiä ovat: nuori lapsi, lapsi, nuorempi teini-ikäinen, vanhempi teini-ikäinen ja aikuinen.

SMTP-palvelin

Akronyymi, joka tulee sanoista Simple Mail Transfer Protocol. TCP/IP-protokolla, jonka avulla viestejä voidaan lähettää verkon tietokoneesta toiseen. Tätä protokollaa käytetään Internetissä sähköpostin reitittämiseen.

solmu

Verkkoon liitetty yksittäinen tietokone.

SSID-tunnus

Langattoman lähiverkon alijärjestelmän laitteiden verkon nimi. Perustekstinä oleva 32 merkin merkkijono, joka lisätään kaikkiin langattoman lähiverkon pakettien otsikkoihin. SSID-tunnus erottaa langattomat lähiverkot toisistaan, joten kaikkien verkon käyttäjien täytyy toimittaa sama SSID-tunnus käyttääkseen tiettyä käyttöpistettä. SSID-tunnus estää asiakaslaitteita, joilla ei ole verkon SSID-tunnusta käyttämästä verkkoa. Käyttöpisteet lähettävät kuitenkin SSID-tunnuksensa julkisesti oletusasetuksena. Vaikka SSID-tunnuksen julkaisu on pois käytöstä, hakkerit voivat silti tunnistaa verkon SSID-tunnuksen nuuskintatyökalujen avulla.

SSL-protokolla

Netscapen kehittämä protokolla henkilökohtaisten asiakirjojen lähettämiseen Internetissä. SSL-protokolla salaa SSL-yhteyden välityksellä lähetettävät tiedot julkisen avaimen avulla. Sekä Netscape Navigator että Internet Explorer käyttävät ja tukevat SSL-protokollaa ja useat Web-sivustot käyttävät protokollaa vastaanottaessaan luottamuksellisia käyttäjätietoja, kuten luottokorttien numeroita. URL-osoitteet, jotka vaativat SSL-yhteyden alkavat tekstillä https: tavanomaisen http:n sijaan.

synkronointi

Voit ratkaista varmuuskopioitujen tiedostoversioiden ja paikalliselle tietokoneelle tallennettujen tiedostoversioiden ristiriidat synkronoinnin avulla. Tiedostot kannattaa synkronoida silloin, kun online-varmuuskopiovarastossa oleva tiedostoversio on uudempi kuin muilla tietokoneilla oleva tiedostoversio. Synkronointi päivittää tietokoneillasi olevan tiedoston online-varmuuskopiovarastossa olevalla tiedostoversiolla.

SystemGuard-toiminto

SystemGuards-toiminnot tunnistavat tietokoneeseen tehdyt luvattomat muutokset ja varoittavat niistä.

sähköposti

Sähköinen posti, Internetin tai yrityksen lähiverkon tai suuralueverkon kautta lähetetyt viestit. EXE- (suoritettavat tiedostot) tai VBS-muodossa (Visual Basic -komentosarjat) olevat tiedostot ovat yhä kasvavassa määrin suosiossa virusten ja troijalaisten levityskeinona.

sähköpostiasiakas

Sähköpostitili. Esimerkiksi Microsoft Outlook tai Eudora.

T

tapahtuma

Tapahtumat IP-osoitteesta 0.0.0.0

Jos näet tapahtumia IP-osoitteesta 0.0.0.0, siihen on kaksi todennäköistä syytä. Ensimmäinen ja tavanomaisin syy on, että jostain syystä tietkoneesi on vastaanottanut huonosti muotoutuneen paketin. Internet ei ole aina 100 % luotettava, joten huonoja paketteja saattaa esiintyä. Koska palomuuri näkee paketit ennen kuin TCP/IP-protokolla voi vahvistaa ne, se saattaa raportoida paketit tapahtumana.

Toinen tilanne voi tapahtua, kun lähde-IP-osoite on tekaistu tai väärennetty. Huijausyrityspaketit saattavat viitata siihen, että joku yrittää tarkistaa tietokonettasi etsiessään troijalaisia. On tärkeää muistaa, että palomuuri estää yrityksen.

Tapahtumat IP-osoitteesta 127.0.0.1

Tapahtumat luetteloivat joskus lähde-IP-osoitteekseen osoitteen 127.0.0.1. On tärkeää huomata, että tämä IP-osoite on erityistapaus, jota kutsutaan silmukkaosoitteeksi.

Huolimatta siitä, mitä tietokonetta käytät, 127.0.0.1 viittaa aina paikalliseen tietokoneeseen. Tämä osoite tunnetaan myös nimellä localhost, koska tietokoneen nimi "localhost" palauttaa aina IP-osoitteen 127.0.0.1. Tarkoittaako tämä, että tietokoneesi yrittää murtautua itse itseensä? Onko joku troijalainen tai vakoiluohjelma ottamassa tietokoneesi haltuunsa? Ei todennäköisesti. Useat lailliset ohjelmat käyttävät silmukkaosoitetta komponenttien väliseen viestintään. Esimerkiksi useat henkilökohtaiset posti- ja Web-palvelimet antavat sinun määrittää ne Web-käyttöliittymän avulla, jota voidaan useimmiten käyttää http://localhost/-osoitteen kautta.

Palomuuri kuitenkin sallii näiden ohjelmien lähettämän tietoliikenteen, joten jos näet tapahtumia IP-osoitteesta 127.0.0.1, se todennäköisesti tarkoittaa sitä että lähde-IP-osoite on tekaistu tai väärennetty. Huijausyrityspaketit ovat useimmiten merkkejä siitä, että joku tarkistaa järjestelmääsi etsiessään troijalaisia. On tärkeää muistaa, että palomuuri estää tämän huijausyrityksen. On itsestään selvää, että IP-osoitteesta 127.0.0.1 tulevien tapahtumien raportoiminen ei ole tarpeellista.

Kuten sanottua, jotkut ohjelmat, kuten esimerkiksi Netscape 6.2 ja sitä uudemmat versiot vaativat, että lisäät IP-osoitteen 127.0.0.1 **Luotettavien IP-osoitteiden** luetteloon. Näiden ohjelmien komponentit keskustelevat keskenään sellaisella tavalla, että palomuuri ei pysty päättelemään, onko tietoliikenne paikallista.

Esimerkiksi jos käytät Netscape 6.2:a ja et merkitse osoitetta 127.0.0.1 luotettavaksi, et pysty käyttämään selaimen ystäväluetteloa. Tästä syystä jos näet tietoliikennetapahtumia osoitteesta 127.0.0.1 ja kaikki tietokoneesi ohjelmat toimivat normaalisti, voit turvallisesti estää kyseisen liikenteen. Jos kuitenkin jonkun ohjelman, kuten Netscapen käytössä esiintyy ongelmia, lisää IP-osoite 127.0.0.1 palomuurin **Luotettavien IP-osoitteiden** luetteloon ja selvitä, ratkeaako ongelma tällä tavoin.

Jos IP-osoitteen 127.0.0.1 lisääminen **Luotettavien IP-osoitteiden** luetteloon korjaa ongelman, sitten sinun täytyy harkita seuraavia vaihtoehtoja: jos merkitset osoitteen 127.0.0.1 luotettavaksi ohjelma toimii oikein, mutta olet alttiimpi huijausyrityshyökkäyksille. Jos et merkitse osoitetta luotettavaksi, ohjelma ei toimi oikein, mutta suojauksesi kyseistä haitallista tietoliikennettä vastaan pysyy ennallaan.

Lähiverkon tietokoneista saapuvat tapahtumat

Useimmissa yritysten lähiverkkojen määrityksissä voit merkitä kaikki lähiverkkosi tietokoneet luotettaviksi.

Yksityisistä IP-osoitteista saapuvat tapahtumat

IP-osoitteita, jotka ovat muodossa 192.168.xxx.xxx, 10.xxx.xxx.xxx ja 172.16.0.0 - 172.31.255.255 kutsutaan reitittämättömiksi tai yksityisiksi IP-osoitteiksi. Nämä IP-osoitteet eivät koskaan poistu verkostasi ja ne voidaan useimmiten merkitä luotettaviksi.

192.168-lohkoa käytetään Microsoftin Internet-yhteyden jakamisen yhteydessä. Jos käytät jaettua Internet-yhteyttä ja näet tapahtumia tästä IP-lohkosta, sinun kannattaa lisätä IP-osoite 192.168.255.255 **Luotettavien IP-osoitteiden** luetteloon. Tämä merkitsee koko 192.168.xxx.xxx-lohkon luotettavaksi.

Jos et ole yksityisessä verkossa ja näet tapahtumia näistä IP-osoitealueista, lähde-IP-osoite saattaa olla tekaistu tai väärennetty. Huijausyrityspaketit ovat useimmiten merkki siitä, että joku yrittää tarkistaa järjestelmääsi etsiessään troijalaisia. On tärkeää muistaa, että palomuuri estää tämän huijausyrityksen.

Koska yksityiset IP-osoitteet ovat erillisiä Internetissä käytettävistä IP-osoitteista, näiden tapahtumien raportoimisesta ei ole mitään hyötyä.

tarkkailtavat tiedostotyypit

Tarkkailtavat tiedostotyypit ovat tiedostotyyppejä (esimerkiksi .doc ja .xls), jotka McAfee Data Backup varmuuskopioi tai arkistoi tarkkailukohteissa.

tarkkailukohteet

Tietokoneen kansiot, joita McAfee Data Backup tarkkailee.

tavallinen sähköpostitili

Useimmillä kotikäyttäjillä on tämän tyyppinen tili. Katso myös kohta POP3-tili.

TKIP-protokolla

Pikakorjauskeino, jolla voidaan korjata WEP-suojauksen tietoturva-aukkoja, erityisesti salausavainten uudelleenkäyttöön liittyviä aukkoja. TKIP-protokolla vaihtaa väliaikaisia avaimia 10 000 paketin välein. Tämä tarjoaa dynaamisen jakelukeinon, joka parantaa verkon suojausta huomattavasti. TKIP-suojaus aloitetaan 128-bittisellä väliaikaisella avaimella, joka jaetaan verkon asiakkaiden ja käyttöpisteiden välillä. TKIP-protokolla yhdistää väliaikaisen avaimen asiakaskoneen MAC-osoitteen kanssa ja lisää sitten huomattavan suuren 16 oktetin alustusvektorin, joka luo avaimen, jolla tiedot salataan. Tämä toiminto takaa, että jokainen asema käyttää eri avainvirtaa tietojen salaamiseen. TKIP-protokolla käyttää RC4:ää salauksen suorittamiseen. WEP käyttää myös RC4:ää.

todennus

Henkilön tunnistusmenetelmä, joka useimmiten perustuu käyttäjänimeen ja salasanaan. Todennuksen avulla voidaan varmistaa, että henkilö on kuka hän väittää olevansa, mutta menetelmässä ei määritetä todennettavan henkilön käyttöoikeuksia.

toimialue

Verkkoyhteyden osoite, joka esittää osoitteen omistajan nimen hierarkisessa muodossa: palvelin.yhteisö.tyyppi. Esimerkiksi osoite www.whitehouse.gov toimii Valkoisen talon Web-palvelimen tunnisteena, joka on Yhdysvaltojen hallintojärjestelmän osa.

Troijan hevonen

Troijalaiset ovat ohjelmia, jotka esiintyvät vaarattomina ohjelmina. Troijalaiset eivät ole viruksia, koska ne eivät kopioi itseään, mutta ne saattavat olla aivan yhtä tuhoisia.

tärkeä tarkkailukohde

Tietokoneesi kansio (ja kaikki sen alihakemistot), jonka muutoksia McAfee Data Backup tarkkailee. Jos määrität tärkeän tarkkailukohteen, McAfee Data Backup varmuuskopioi kaikki kyseisen kansion ja sen alihakemistojen tarkkailtavien tiedostotyyppien mukaiset tiedostot.

täydellinen arkistointi

Käyttäjän määrittämien tarkkailtavien tiedostotyyppien ja sijaintien tietojen täydellinen arkistoiminen.

ulkoinen kiintolevyasema

Kiintolevyasema, joka sijaitsee tietokoneen kotelon ulkopuolella.

URL

URL tulee sanoista Uniform Resource Locator. URL on Internet-osoitteiden standardimuoto.

valkoinen lista

Sallittujen Web-sivustojen luettelo. Luettelon Web-sivustojen käyttö on sallittua, koska ne eivät sisällä haitallisia toimintoja.

wardriver-verkkovarkaat

Tunkeutujia, jotka käyttävät kannettavia tietokoneita, erityisohjelmistoja ja laitteita ja ajelevat ympäri kaupunkeja, esikaupunkialueita ja liikealueita etsiessään salakuunneltavia langattomia tietoliikenneyhteyksiä.

varmuuskopiointi

Tarkkailtavien tiedostojen varmuuskopioiminen suojattuun online-palvelimeen.

Web-bugit

Pieniä grafiikkatiedostoja, jotka voivat upottaa itsensä HTML-sivuihisi ja sallia luvattoman lähteen asettaa evästeitä tietokoneeseesi. Nämä evästeet voivat sitten lähettää tietoja luvattomalle lähteelle. Web-bugeja kutsutaan myös pikselitunnisteiksi, läpinäkyviksi GIF-tiedostoiksi ja näkymättömiksi GIF-tiedostoiksi.

WEP

Salaus- ja todennusprotokolla, joka kehitettiin osana 802.11-standardia. Protokollan ensimmäiset versiot perustuivat RC4-salaustekstiin ja sisälsivät merkittäviä tietoturva-aukkoja. WEP yrittää suojata tiedot salaamalla radioaaltojen välityksellä siirrettäviä tietoja siten, että ne ovat suojattuja, kun niitä siirretään verkon yhdestä päätepisteestä toiseen. Viime aikoina on kuitenkin huomattu, että WEP-salaus ei ole aivan niin turvallinen kuin aiemmin on uskottu.

verkkoasema

Levy- tai nauha-asema, joka on liitetty useiden käyttäjien jakaman verkon palvelimeen. Verkkoasemia kutsutaan joskus etäasemiksi.

verkkokartta

Network Managerin graafinen esitys kotiverkon tietokoneista ja osista.

Verkkokortti

Kortti, joka liitetään kannettavaan tietokoneeseen tai muuhun laitteeseen ja jonka avulla laite voidaan liittää lähiverkkoon.

verkkoon

Kun liität kaksi tai useampia tietokoneita toisiinsa, luot verkon.

Wi-Fi (Wireless Fidelity)

Termi, jota käytetään yleisesti kaikista 802.11-standardin verkoista, oli kysessä sitten 802.11b-, 802.11a-, dual-band-verkko tai joku muu verkko. Termiä käyttää Wi-Fi Alliance -yhteistyöjärjestö.

Wi-Fi Alliance

Organisaatio, jonka muodostavat johtavat langattomien laitteistojen ja ohjelmistojen valmistajat, tavoitteenaan 1) kaikkien 802.11-standardiin perustuvien tuotteiden yhteentoimivuuden varmistaminen ja 2) Wi-Fi-termin promotointi kaikkien 802.11-standardiin perustuvien langattomien lähiverkkotuotteiden kansainvälisenä brändin nimenä kaikilla markkinoilla. Organisaatio toimii yhteistyöjärjestönä, testauslaboratoriona ja selvitystoimistona toimittajille, jotka haluavat promotoida tuotteiden yhteentoimivuutta ja toimialan kasvua.

Vaikka kaikkia 802.11a/b/g-tuotteita kutsutaan nimellä Wi-Fi, vain tuotteet, jotka ovat läpäisseet Wi-Fi Alliancen testit saavat käyttää tuotteistaan nimitystä Wi-Fi Certified (Wi-Fi-varmennettu). Wi-Fi Certified on rekisteröity tavaramerkki. Tuotteissa, jotka ovat läpäisseet testit tulee olla paketoinnissaan tunnistava leima, jossa lukee, että tuote on Wi-Fi-varmennettu. Tuotteen leimassa täytyy näkyä myös tuotteen käyttämä radiotaajuus. Järjestö tunnettiin aiemmin nimellä Wireless Ethernet Compatibility Alliance (WECA), mutta se muutti nimeään lokakuussa 2002, jotta nimi vastaisi paremmin Wi-Fi-brändiä, jonka järjestö haluaa luoda.

Wi-Fi Certified (Wi-Fi-varmennettu)

Mitkä tahansa tuotteet, jotka ovat testattu ja hyväksytty Wi-Fi Certified -tuotteiksi (rekisteröity tavaramerkki) Wi-Fi Alliancen toimesta, ovat yhteensopivia toistensa kanssa, vaikka ne olisivat eri valmistajien tuotteita. Wi-Fi Certified -tuotteen käyttäjä voi käyttää minkä tahansa valmistajan käyttöpistettä minkä tahansa valmistajan asiakasohjelmistolla, edellyttäen, että asiakasohjelmisto on myös Wi-Fi Certified -tuote. On kuitenkin tyypillistä, että mitkä tahansa langattomat tuotteet, jotka käyttävät samaa radiotaajuutta (esim. 2,4 GHz / 802.11b tai 11g, 5 GHz / 802.11a) toimivat toistensa kanssa, vaikka ne eivät ole Wi-Fi Certified -tuotteita.

WPA

Määritysstandardi, joka lisää nykyisten ja tulevien langattomien lähiverkkojärjestelmien tietosuojaa ja käyttöoikeuksien hallintaa erittäin paljon. Standardi on suunniteltu toimimaan olemassaolevissa laitteistoissa ohjelmistopäivityksenä, koska WPA on kehitetty IEEE 802.11i-standardin pohjalta ja on yhteensopiva sen kanssa. Kun WPA on asennettu oikein, se tarjoaa langattomien lähiverkkojen käyttäjille korkeatasoisen suojauksen ja varmistuksen siitä, että vain luvalliset verkkokäyttäjät voivat muodostaa yhteyden verkkoon.

WPA-PSK

Erikoislaatuinen WPA-tila, joka on suunniteltu kotikäyttäjille, jotka eivät vaadi vahvaa yritystason tietosuojaa ja eivät käytä todennuspalvelimia. Tässä tilassa kotikäyttäjä antaa aloitussalanan manuaalisesti aktivoidakseen suojatun langattoman verkkoyhteyden esijaetun avaintilan, ja vaihtaa sitten verkon jokaisen langattoman tietokoneen ja käyttöpisteen salasanaa säännöllisesti. Katso myös kohdat WPA2-PSK ja TKIP.

WPA2

Katso myös kohta WPA. WPA2 on WPA-tietosuojastandardin päivitys, joka perustuu 802.11i IEEE -standardiin.

WPA2-PSK

Katso myös kohdat WPA-PSK ja WPA2. WPA2-PSK on samankaltainen kuin WPA-PSK ja se perustuu WPA2-standardiin. WPA2-PSK:n yleinen ominaisuus on se, että laitteet tukevat usein monia erilaisia salaustoimintoja (esim. AES, TKIP) samanaikaisesti, kun vanhemmat laitteet useimmiten tukivat vain yhtä salaustoimintoa kerralla (eli kaikkien laitteiden täytyi käyttää samaa salaustoimintoa).

VPN (Virtual Private Network)

Verkko, joka muodostuu julkisten linjojen avulla yhdistettävistä solmuista. On olemassa lukuisia järjestelmiä, joiden avulla voidaan luoda verkkoja käyttämällä Internetiä tiedonsiirtokeinona. Nämä järjestelmät käyttävät salausta ja muita suojausmekanismeja varmistaakseen, että ainoastaan luvalliset käyttäjät voivat käyttää verkkoa ja että verkon tietoja ei voida salakuunnella.

välimuistipalvelin

Palomuurin osa, joka hallitsee lähiverkon saapuvaa ja lähtevää Internet-tietoliikennettä. Välimuistipalvelin voi parantaa verkon suorituskykyä toimittamalla usein pyydettyjä tietoja, kuten suosittuja Web-sivuja, ja suodattamalla ja hylkäämällä pyyntöjä, joita verkon omistaja ei pidä asianmukaisina, kuten yksityistiedostojen luvatonta käyttöä koskevia pyyntöjä.

välityspalvelin

Tietokone tai tietokoneessa suoritettava ohjelmisto, joka toimii verkon ja Internetin välisenä suojamuurina ja näyttää ainoastaan yhden verkko-osoitteen ulkopuolisille sivustoille. Koska välityspalvelin toimii kaikkien verkon sisäisten tietokoneiden suojamuurina, se suojaa käyttäjien verkkoidentiteettiä, silti kuitenkin mahdollistaen Internet-yhteyksien muodostamisen. Katso myös kohta Välimuistipalvelin.

väsytysmenetelmähyökkäys

Tunnetaan myös nimellä väsytysmenetelmämurtautuminen. Sovellusohjelmien käyttämä yritys ja erehdys -menetelmä, jonka avulla yritetään purkaa salattua tietoa, kuten salasanoja sinnikkäällä yrittämisellä älykkäiden strategioiden sijaan. Samalla tavalla kuin rikollinen saattaa murtautua kassakaappiin yrittämällä mahdollisimman monia erilaisia yhdistelmiä, väsytysmenetelmämurtautuminen yrittää murtaa salauksen kokeilemalla kaikkia mahdollisia sallittujen merkkien yhdistelmiä. Väsytysmenetelmää pidetään erehtymättömänä, joskin aikaa vievänä murtautumiskeinona.

yhdistetty yhdyskäytävä

Laite, joka yhdistää langattoman käyttöpisteen, reitittimen ja palomuurin toiminnot. Jotkut laitteet saattavat sisältää myös suojausparannuksia ja siltausominaisuuksia.

Tietoja McAfeesta

McAfee, Inc.:n pääkonttori sijaitsee Santa Clarassa, Kaliforniassa. McAfee on yksi maailman johtavista tietomurtojen esto- ja tietoturvariskien hallintasovellusten valmistajista. McAfee toimittaa luotettavia ratkaisuja ja palveluita, jotka suojaavat järjestelmiä ja verkkoja ympäri maailman. McAfeen kokemus tietoturvakysymyksissä ja tehokas tuotekehitys tuottavat sovelluksia, joiden avulla kotikäyttäjät, yritykset, julkisen sektorin laitokset ja palveluntarjoajat pystyvät torjumaan hyökkäyksiä, estämään haittayrityksiä ja kehittämään ja parantamaan tietoturvaansa jatkuvasti.

Copyright

Hakemisto

I

J

K

L

M

N

O

P

Q

R

S

T

U

V,W

Y