Mika Hyppönen

Palomuurin sääntökantojen keskitetty optimointi

Algosec Firewall Analyzer

Metropolia Ammattikorkeakoulu
Insinööri AMK
Tietotekniikka
Insinöörityö
22.1.2017

Metropolia

Tiivistelmä

Tekijä(t) Otsikko Sivumäärä Aika	Mika Hyppönen Palomuurin sääntökantojen keskitetty optimointi 30 sivua 22.1.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Tietoturva-asiantuntija Masi Takamäki Lehtori Marko Uusitalo

Insinöörityön tavoitteena on tutkia nykypäivän ongelmia, jotka liittyvät palomuurien sääntökantoihin ja muutoksenhallintaan. Samalla tutkitaan, minkälaisia hyötyjä Algosec Firewall Analyzerilla olisi saavutettavissa kyseisten ongelmien ratkaisemiseksi. Tutkinnan pohjalta päätetään, olisiko kyseinen tuote sopiva Cygaten tuoteportfolioon ja käytettäväksi olemassaolevien asiakkaiden ympäristöissä.

Työ rajattiin käsittämään vain Algosec Firewall Analyzerin merkittävimpiä ominaisuuksia sääntökantojen optimoimiseen. Ominaisuuksien testaus suoritettiin laitevalmistajan tarjoamalla virtuaaliympäristöllä, joka asennettiin VMware Workstationille.

Asennus ja testaus sujui erittäin hyvin, ja saatuihin tuloksiin oltiin tyytyväisiä. Testauksen loputtua voitiin todeta, että Algosec olisi erittäin hyödyllinen laite usealle Cygaten asiakkaalle.

Avainsanat	Palomuuri, Algosec, Tietoturva, Virtuaaliympäristö

Metropolia

Abstract

Author(s) Title Number of Pages Date	Mika Hyppönen Centralized optimization for firewall rulesets. 30 pages 22 January 2017
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Masi Takamäki, Security Specialist Marko Uusitalo, Senior Lecturer

The purpose of the thesis was to investigate today's problems related to firewall rulesets and the change management. At the same time the aim was to explore what kind of benefits would be achieved to solve these issues using Algosec Firewall Analyzer. Also based on these findings the goal was to decide whether the product would be suitable for Cygate's product portfolio and for existing customer environments.

The study was defined only to include the most important Algosec Firewall Analyzer features to optimize the properties of rulesets and policies. The practical testing was conducted on a virtual environment that was provided by Algosec. The environment was installed on VMware Workstation.

The installation and testing went very well and the results were satisfying. After the testing was complete it was safe to say that the product would be very useful for multiple Cygate's customers.

Keywords	Firewall, Network Security, Algosec, Virtual Environment

Sisällys

1 Johdanto

Tämän insinöörityön tarkoituksena on tarkastella nykypäivän ongelmia suurissa yritysverkoissa, jotka liittyvät muutostenhallintaan ja palomuurien käsittelyyn. Samalla tutkintaan otetaan Algosec Firewall Analyzer ja katsotaan, minkälaisia työkaluja se tarjoaa palomuuriympäristöjen sääntökantojen hallintaan ja optimointiin. Tutkinnan pohjalta selvitetään, mikäli Algosec Firewall Analyzer olisi sopiva tuote Cygate Oy:n tuoteportfolioon ja sitä voitaisiin hyödyntää olemassa oleville asiakkaille.

Opinnäytetyön käytännön testaus suoritetaan laitevalmistajan tarjoaman virtuaaliympäristön avulla, joka simuloi mahdollisimman tarkasti kuvitteellisen yrityksen topologiaa. Ympäristössä suoritetaan muutamia testejä, joilla nähdään järjestelmän tarjoamat hyödyt käytännössä.

Työ rajattiin käsittämään vain tärkeimpiä Algosec Firewall Analyzerin tarjoamia työkaluja palomuurien sääntökantojen optimointiin.

2 Palomuurien kehitys ja mukana seuranneet haasteet

Palomuurit ovat olleet parin vuosikymmenen ajan tietoturvan perustana. Ensimmäisen sukupolven palomuurit kehitettiin 1980-luvun loppupuolella, kun ihmiset alkoivat ymmärtämään nousevien tietoturvauhkien muodostamaa ongelmaa. Ylläpitäjät halusivat erottaa yrityksen sisäisen verkon ulkopuolisesta verkosta, eli käytännössä Internetistä. Ensimmäisen sukupolven palomuurilla tämä tehtiin staattisella pakettien suodattamisella, joka tapahtui joko reitittimissä tai kytkimissä. Käytännössä tämä tarkoitti sitä, että palomuuri tarkasti jokaisen saapuvan ja lähtevän paketin yksitellen. Tarkastelussa katsottiin, mistä paketti on tulossa, minne se on menossa sekä mitä porttia ja protokollaa yhteydessä käytetään. Näitä tietoja verrattiin ylläpitäjän tekemään politiikkaan, jossa määriteltiin, mitkä yhteydet ovat sallittuja ja mitkä eivät. Tämän perusteella paketti joko päästettiin läpi tai sen eteneminen pysäytettiin.

Koska jokainen paketti tarkastettiin erikseen, kyseinen menetelmä ei ollut kovinkaan tehokas. Tämä johtui siitä, että palomuureilla ei ollut mitään käsitystä yhteyden tilasta, eli siitä, mitkä paketit saattoivat kuulua jo olemassa olevaan yhteyteen. Valitettavasti

ensimmäisen sukupolven palomuurit olivat myös varsin alttiita hyökkäyksille. Koska liikennettä tarkkailtiin vain osoitteiden tasolla, hakkerit pystyivät läpäisemään palomuurin liikennöimällä sellaisella osoitteella, joka oli sääntökannassa sallittuna lähteenä.

Koska haavoittuvuudet ensimmäisen sukupolven palomuurien kohdalla huomattiin varsin merkittäviksi, toisen sukupolven palomuurit saivat alkunsa varsin pian. Jo 1990-luvun alussa käytössä olivat ensimmäiset ns. tilalliset palomuurit. Nämä palomuurit tutkivat myös pakettien sisältöä, eivätkä pelkästään suodattaneet niitä osoitteiden perusteella. Toisen sukupolven palomuurilla olivat samat ominaisuudet kuin edeltäjälläkin, mutta niiden lisäksi palomuuri tallensi istunnon ja yhteyden tilan. Näin ollen päätelaitteiden muodostettua yhteyden palomuurin läpi kaikki samaan yhteyteen liittyvät myöhemmät paketit voitiin myös sallia molempiin suuntiin. Kun yhteyden tila oli tiedossa, saivat ylläpitäjätkin paremman kuvan verkossa tapahtuvasta liikenteestä, ja sääntökantojen muodostaminen oli yksinkertaisempaa. Toisen sukupolven palomuuritkaan eivät kuitenkaan vielä pystyneet erottamaan haitallista web-liikennettä normaalin joukosta. Tämä oli ongelma, johon tarvittiin seuraavaksi ratkaisu.

Internetin kasvaessa jo varsin yleiseksi maailmanlaajuisesti sai alkunsa palomuurien kolmas sukupolvi, sovelluspalomuurit. Ajan kuluessa sekä hyökkäävät menetelmät että sen johdosta myös palomuurit ovat siirtyneet OSI-mallissa jatkuvasti ylöspäin. Kun saavuttiin ylimmälle solvelluskerrokselle, saatiin vihdoin apu aikaisemmin mahdottomille web-hyökkäyksille. Kyseiset web-hyökkäykset pystyivät hyödyntämään olemassa olevia hyvin tunnettuja portteja kuten 80 (HTTP) sekä 443 (HTTPS), koska palomuurit eivät pystyneet erottamaan normaalia sovellusta ja haitallista liikennettä toisistaan. Sovelluspalomuurit pystyivät pureutumaan liikenteeseen paljon aikaisempaa tarkemmin ja mukautumaan liikenteeseen reaaliajassa. Laite esimerkiksi tarkkaili liikenteen prosessitunnisteita ja niiden perusteella selvitti, oliko kyseessä haitallista liikennettä. [13.]

2000-luvun lopussa kehitettiin nykyisinkin käytössä oleva uusin palomuurien sukupolvi ns. seuraavan sukupolven palomuuri. Varsinainen pakettien suodatus toimi kyseisissä laitteissa varsin samalla tavalla kuten sovelluspalomuureissakin, mutta seuraavan sukupolven palomuureihin tuli lisäksi paljon sellaisia ominaisuuksia, jotka aikaisemmin eivät olleet mahdollisia toteuttaa tai ne tehtiin erillisillä laitteilla. Ominaisuuksista

voidaan mainita muun muassa URL-suodatus, tunkeilijan havaitsemisjärjestelmä sekä kyky muokata palomuurin sääntöjä käyttäjäkohtaisesti tuomalla käyttäjät ulkoisista lähteistä. Tämän palveluiden keskitettävyyden ansiosta seuraavan sukupolven palomuurit ovatkin olleet valtava harppaus ylläpitäjien työtaakan vähentämiseksi. Tästä huolimatta kaiken kokoisilla yrityksillä on silti jatkuvasti haasteita sääntökantojen loogisuuden, latteiden suorituskyvyn ja tietoturvan takaamisen kanssa. Yritykset voivat tällaisissa tapauksissa lähteä etsimään apua yrityksen ulkopuolelta eivätkä pelkästään vaan lisää sisäisiä resursseja. [6; 7; 11; 13.]

2.1 Turvallisuuden takaaminen

Ihmiset, jotka ovat vastuussa palomuurien muutoksenhallinasta vaihtuvat ajan kuluessa ja jokaisella heistä on oma tyylinsä tehdä muutoksia sääntökantoihin. Toiset tarkastavat erikseen olemassa olevat säännöt tarkkaan uusien muutospyyntöjen tullessa ja pyrkivät hyödyntämään aikaisempia sääntöjä tehokkaasti. Toiset taas toteuttavat uuden avauspyynnön suoraan sellaisenaan uudella säännöllä. Jälkimmäisellä tavalla palomuurien sääntökannat paisuvat paljon ajan kuluessa. Samalla vaikeutuu mahdollinen vianetsintä, mikäli sellaiselle on tarvetta. Palomuurin suorituskyky laskee sitä mukaan, kuinka paljon sen tarvitsee käydä läpi sääntöjä jokaisen paketin kohdalla. [4.]

Kuormaa lisää myös sellaiset vanhat säännöt palomuureissa, joille ei ole enää edes käyttöä. Vanhoja avauksia on saatettu tehdä sellaisille henkilöille, jotka eivät ole enää yrityksen palveluksessa. Kenelläkään ylläpitäjällä ei ole aikaa käydä sääntökantoja läpi etsien tällaisia tapauksia.

Palomuurien muutoksenhallinta on nykyään erittäin tarkkaa ja vastuullista työtä. Usein muutospyynnöt saapuvat ylläpitäjille epäselvinä ja suurpiirteisinä. Ylläpitäjän vastuulle jää pitää huolta siitä, ettei avauksella ole huonoja seurauksia. Erittäin pieneltä vaikuttavalla muutoksella voi olla erittäin katastrofaalisia seurauksia. Väärin tehdyillä säännöllä, jolla on tarkoitus vain estää tietynlaista liikennettä, voidaan ajaa jopa koko yrityksen tuotanto alas. Herkissä ympäristöissä tämä voi tarkoittaa jopa satojen tuhansien eurojen menetyksiä tunnissa. Vaihtoehtoisesti huolimaton avaus voi myös altistaa verkon tietoturvauhille. [2.]

Palomuurien sääntökannan selkeys on tärkeä osa laitteen toimivuuden takaamista. Liian laajat avaukset, jotka sisältävät tarvitsemattomia portteja, käyttämättömät VPN-tunelit, päällekkäiset muuriavaukset ovat esimerkkejä riskeistä, jotka heikentävät laitteiden suorituskykyä ja mahdollisesti altistavat verkon käyttökatkoille. Yksi suurimmista suorituskykyä heikentävistä tekijöistä onkin sääntöjen sijainti sääntökannassa. Monesti usein käytössä oleva sääntö on sääntökannan pohjalla. Koska palomuuri käy säännöt läpi ylhäältä alaspäin, tarvitsee laitteen tällöin käydä paljon turhia sääntöjä läpi, ennen kuin saavutaan tuon usein käytettävän säännön kohdalle. Tämä aiheuttaa jatkuvasti lisää turhaa kuormaa palomuurille. Tällaiset ongelmat korostuvat isoissa yrityksissä, joiden verkko koostuu useista eri laitevalmistajien palomuureista

Esimerkkejä säännöistä, jotka aiheuttavat ongelmia:

- Liian sallivat säännöt. Säännöt joissa käytetään esimerkiksi ”Any” palveluna
- käyttämättömät säännöt
- säännöt joita ei käytetä, koska liikenne on jo sallittu aikaisemmin
- ajastetut säännöt jotka ovat umpeutuneet
- huonosti sääntökantaan sijoitetut säännöt.

2.2 Palomuurien auditointi

Pienemmillä yrityksillä tietoturvan takeeksi saattaa riittää se, että heillä on käytössään huippuluokkaa oleva palomuuri. Valitettavasti pelkästään palomuurin olemassaolo ei kuitenkaan tarkoita sitä, että asiat olisivat oikeasti mallillaan. Näissä yrityksissä palomuurien ylläpitäjillä ei välttämättä ole täyttä ymmärrystä siitä, miten sääntökantoja tulisi rakentaa, jotta voitaisiin varmistua tietoturvan pitävyydestä.

Suurissa yrityksissä ja varsinkin sellaisissa yrityksissä, jotka tarjoavat ulkoistetusti ylläpitopalvelua muille osapuolille, tulee tietoturvan ja osaamisen olla todistetusti huippuluokkaa. Tätä varten alalla käytetään erilaisia auditointeja ja niiden myötä yrityksille myönnetään sertifikaatteja todisteeksi siitä, että kaikki on kunnossa. Auditoinnit saattavat kestää useita päiviä ja tuona aikana yrityksen tietoturvaa testataan sekä haastatteluin että sisäisin tarkasteluin. Tarkasteluihin kuuluu muun muassa palomuurien sääntökantojen kunto. Esimerkiksi yritykset, jotka käsittelevät

luottokorttien maksuliikennettä tulee olla PCI (Payment Card Indystry) auditointi suoritettuna. [8.]

Ylläpitopalveluja tarjoavilta yrityksiltä saatetaan nykyään jo vaatia tiettyjä standardeja, esimerkiksi ISO/IEC 27001:tä. Tämän lisäksi harvinaisempia ja vaativimpia standardeja voidaan käyttää jopa kilpailuvalttina, jolla erotutaan muiden joukosta. Suomessa auditointeja suorittaa esimerkiksi Inspecta. [9; 10.]

Palomuurien sääntökantojen eheyden tarkastaminen vaatii erittäin yksityiskohtaista tarkastelua, jotta auditoinnin vaatimukset täytetään. Usein yrityksissä, jossa tarkastelua suoritetaan, työ saattaa viedä jopa viikon edestä työtunteja. Harvoissa yrityksissä ylläpitäjiltä löytyy tällaista aikaa laitettavaksi sivuun. Ulkopuolinen työkalu kuten Algosec mahdollistaa palomuurien auditointiin valmistautumisen vain tunneissa.

3 Algosec Firewall Analyzerin tarjoamat työkalut

Palomuurien sääntökannoissa on usein paljon sellaisia sääntöjä, joilla ei ole enää mitään merkitystä tuotannon kannalta. Ajan saatossa politiikasta tulee monimutkainen ja siitä puuttuu johdonmukaisuus. Tällaiset tilanteet aiheuttavat ylläpitäjille lisää vaivaa, ja samalla palomuurin suorituskyky laskee. Algosecin tarjoamilla työkaluilla voidaan kuitenkin tehokkaasti tarttua tähän haasteeseen.

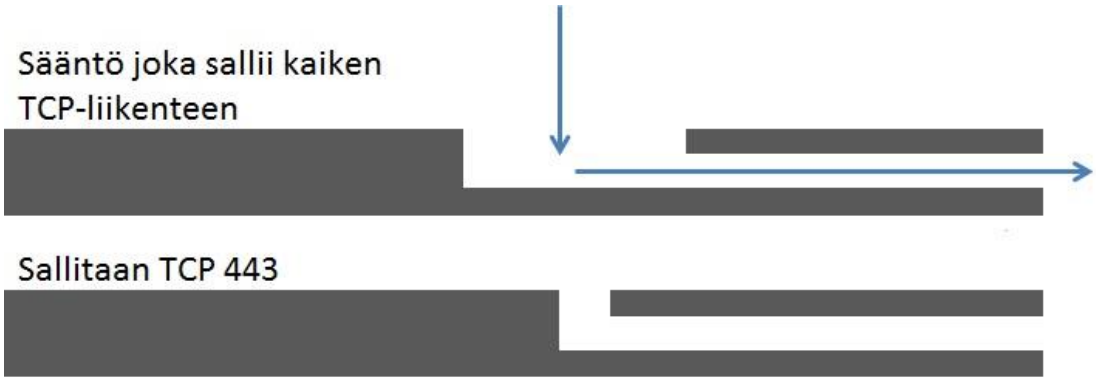
3.1 Palomuurisääntöjen siivous

Opinnäytetyö rajattiin tutkimaan tässä luvussa läpikäytäviä Algosec Firewall Analyzerin raportteihin perustuvia sääntökantojen optimointeja. Ominaisuuksien käyttöä tutkitaan tarkemmin varsinaisessa testiosuudessa.

3.1.1 Covered rules

Covered rules:it ovat sellaisia sääntöjä, joita ei koskaan tulla käyttämään, koska kyseistä sääntöä edeltää jo sellainen sääntö tai yhdistelmä sääntöjä, jotka tekevät päätöksen kyseisestä liikenteestä.

Jos sääntökannassa on esimerkiksi sääntö, joka sallii kaiken TCP-liikenteen, kaikki tämän jälkeen olevat tarkemmat TCP-liikennettä koskevat säännöt jäävät täysin koskematta.

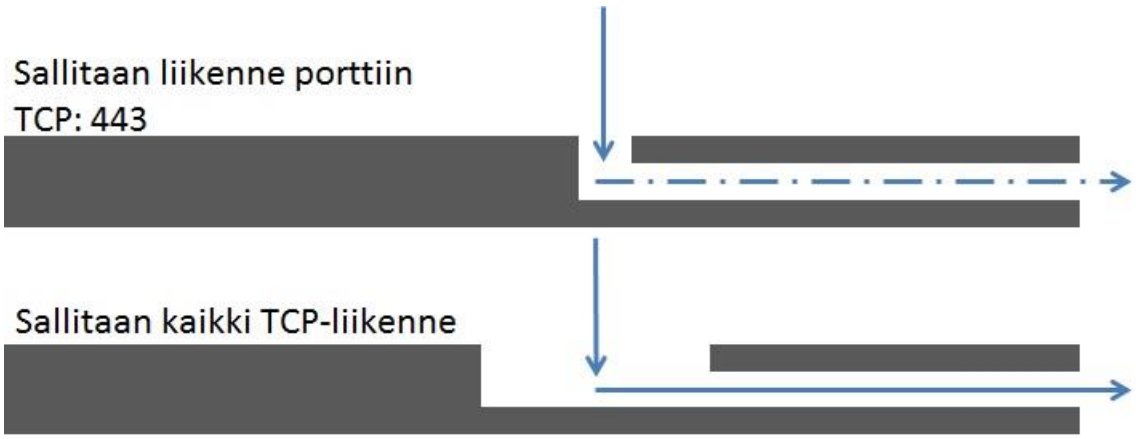


Kuva 1 Esimerkki säännöstä, jota ei tulla koskaan käyttämään.

Kyseisen esimerkin sääntöä, joka sallii TCP443-porttiin tulevan liikenteen, ei tulla koskaan käyttämään, koska yläpuolella oleva sääntö sallii jo kaiken TCP-liikenteen. Mielestäni tällaisessa tilanteessa olisi syytä tarkastella sääntökantaa ja miettiä, onko kaiken TCP-liikenteen salliva sääntö ylipäätään tarpeellinen sekä tietoturvallinen. Algosec Firewall Analyzer etsii laitteiden sääntökannoista tällaisia tapauksia ja ehdottaa täten turhien sääntöjen poistamista.

3.1.2 Redundant special case rules

Redundant special case rules on taas päinvastainen tilanne edeltävästä. Tällöin sääntökannassa on ylempänä sääntö, joka koskee tarkempaa liikennettä, mutta tämä sallitaan kuitenkin laajemmin alapuolella.



Kuva 2 Redundant special case rule käytännössä.

Tässä tapauksessa Algosec ehdottaa ylemmän säännön poistamista, koska kaikki TCP-liikenne on sallittu myöhemmin sääntökannassa. Järjestelmä tarkastaa myös kaikki näiden kahden säännön välissä olevat säännöt, ettei niiden joukossa ole mitään mikä vaikuttaisi liikenteeseen.

3.1.3 Unrouted rules

Unrouted rules tarkoittaa sellaisia sääntöjä, jotka koskevat liikennettä, jota ei ole reititetty kyseisen palomuurin läpi. Algosec tarkistaa kaikki käyttämättömät säännöt sekä säännöt, joissa on käyttämättömiä objekteja. Tämän jälkeen järjestelmä vertaa lähteitä ja kohteita niille annetuille zoneille. Mikäli näistä lähde tai kohde zoneista ei löydy kyseisiä objekteja, merkitään se reitittämättömäksi. Jos sääntö sisältää pelkkiä reitittämättömiä lähteitä tai kohteita, ehdottaa Algosec kyseisen säännön poistamista.

Tällä hetkellä kyseinen ominaisuus on tuettu seuraavissa zoneja hyödyntävissä laitteissa:

- Juniper SRX
- Juniper Netscreen
- Juniper NSM
- Palo Alto
- Fortigate

Reittittämättömiä sääntöjä syntyy helposti, jos yrityksen topologiassa tapahtuu muutoksia. Laitteita saatetaan muuttaa esimerkiksi konesalista toiseen, ja samalla verkon osoitteet vaihtuvat.

3.1.4 Consolidate similar rules

Consolidate similar rules eli samankaltaisten sääntöjen yhdistäminen. Isoissa ympäristöissä saatetaan esimerkiksi pyytää lukuisia avauksia eri verkoista samoille sähköpostipalvelimille. Mikäli ylläpitäjä ei tarkkaan tutki sääntökantaa etukäteen, saattaa hän tehdä lukuisia avauksia niin, että vain lähde muuttuu. Tällaisessa tapauksessa voitaisiin kaikki erilliset säännöt yhdistää yhdeksi isoksi säännöksi.

Algosec etsii palomuurien sääntökannoista samankaltaisia sääntöjä perustuen lähteeseen, kohteeseen sekä porttiin. Mikäli säännöissä kaksi näistä muuttujista ovat samoja ja molemmat säännöt ovat joko sallivia tai kieltäviä, voidaan ne yhdistää.

Lähde	Kohde	Portti
A	A	X
A	B	X

Lähde	Kohde	Portti
A	A+B	X

Kuva 3 Esimerkki samankaltaisista säännöistä, jotka voidaan yhdistää.

Kaksi ylläolevaa sääntöä voitaisiin yhdistää yhdeksi säännöksi, koska molemmissa on sama lähde ja portti.

3.1.5 Unused rules

Unused rules eli käyttämättömät säännöt ovat sellaisia sääntöjä, joihin ei ole tullut yhtään osumaa määrätyllä aikavälillä. Algosec tarkastaa, onko palomuurin lokiin kirjautunut yhtään osumaa kyseiseen sääntöön. Tämä tieto tallentuu Algosecin muistiin

ja sitä päivitetään joka kerta, kun uusi raportti ajetaan kyseiseltä palomuurilta. Mikäli sääntöön ei tule pidemmällä aikavälillä yhtään osumaa, ehdottaa Algosec sen poistamista. Tämä on erittäin hyvä ominaisuus, koska palomuurien omat lokit eivät välttämättä säily kovinkaan pitkään. Käyttämättömät säännöt ovat monesti erittäin vanhoja ja muutosten myötä verkon osoitteet ovat joko vaihtuneet tai poistuneet käytöstä.

3.2 Palomuurin suorituskyvyn parantaminen

Palomuurin suorituskykyyn vaikuttaa merkittävästi se, kuinka monta sääntöä laitteen on käytävä läpi, ennen kuin se tekee päätöksen siitä, mitä liikenteelle tehdään. Jotkin säännöt osuvat suureen osaan liikenteestä, kun taas joitain sääntöjä käytetään erittäin harvoin. Siirtämällä usein käytettävät säännöt politiikan alkuun voidaan huomattavasti parantaa laitteen suorituskykyä.

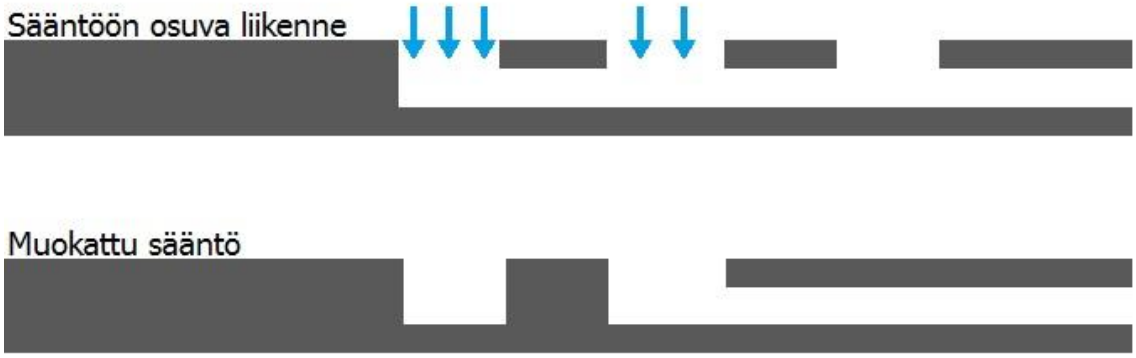
Algosec Firewall Analyzer käyttää sääntöjen uudelleenjärjestämistä varten erityistä RMPP-arvoa (Rules matched per packet). Kyseinen arvo kuvaa sitä, kuinka monta sääntöä palomuurin pitää keskimäärin käydä läpi, ennen kuin se tekee päätöksen. RMPP-arvo kuvaa usein melko tarkasti myös palomuurin suorittimen käyttöastetta. Mitä pienempi arvo on, sitä parempi.

Käytännöllisin työkalu sääntöjen uudelleen järjestämiseen Algosecilla on TOP10 optimizations. Kyseinen ominaisuus käy läpi palomuurin lokeja ja sääntökantaa ja etsii ne kymmenen sääntöä, joiden uudelleenjärjestämisellä saavutettaisiin suurin hyöty laitteen suorituskykyyn. Tällä on tarkoitus saada RMPP-arvo mahdollisimman matalaksi. Usein suuri suorituskyvyn parantuminen saavutetaan jo muutaman säännön sijaintia muuttamalla, joten koko sääntökannan uudelleenjärjestäminen ei välttämättä ole vaivan arvoista.

3.3 Turvallisuuden tiukentaminen

Algosec Firewall Analyzer tarjoaa erittäin merkittävän työkalun palomuurisääntöjen tietoturvan parantamiseen. Algosecin Intelligent Policy Tuner analysoi liikennettä pidemmällä aikavälillä ja tarkistaa, ovatko säännöt täsmällisesti tehtyjä. Mikäli tiettyyn

sääntöön, joka on tehty esimerkiksi avaamalla any-portti, osuu vain liikennettä muutamaan porttiin, havaitsee Algosec tämän ja suosittelee säännön tiukentamista.



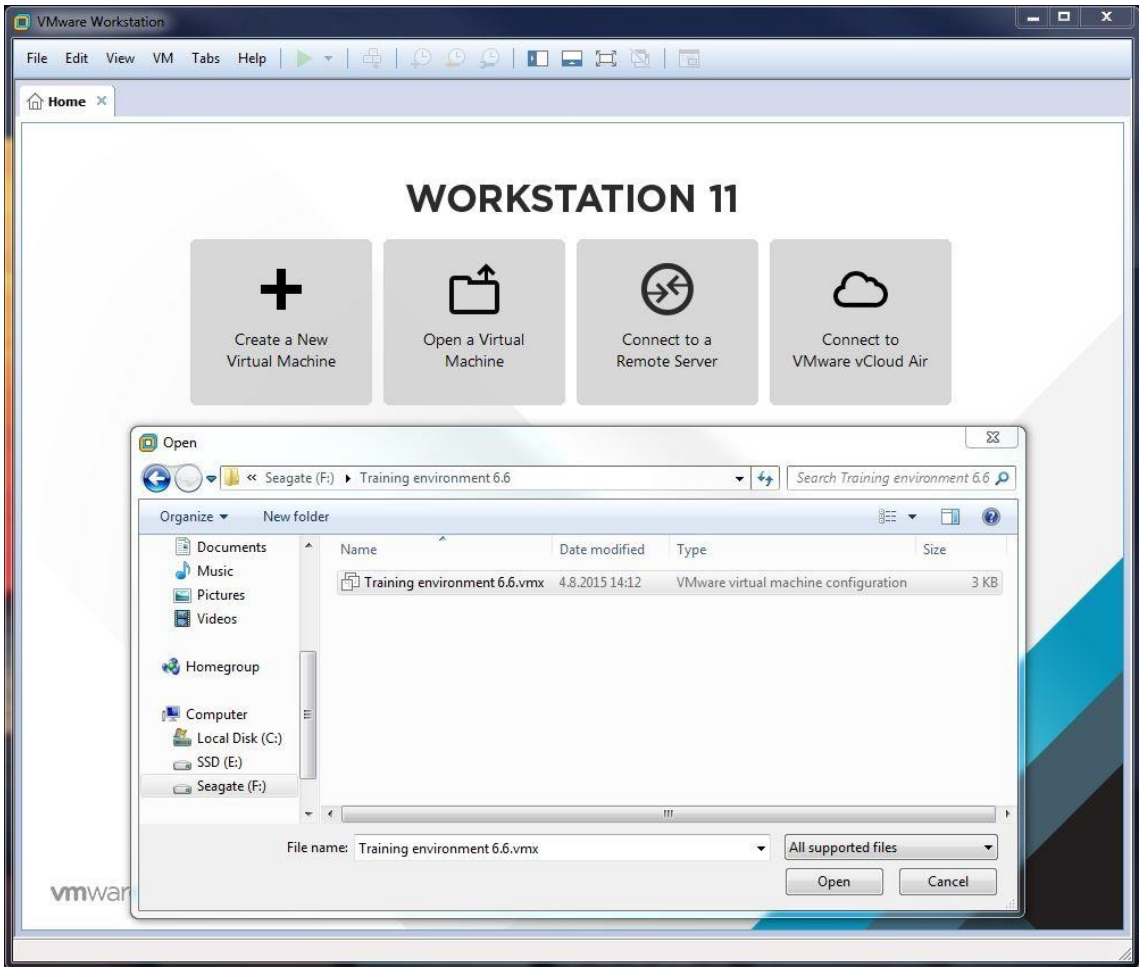
Kuva 4 Esimerkki säännöstä joka on liian salliva. Sääntö voidaan muokata niin, että turhia portteja ei ole sallittu.

Tällä tavalla varmistetaan, että palomuurissa on vain tuotannon kannalta merkittäviä avauksia eikä verkkoa altisteta hyökkäyksille. Kyseisen ominaisuuden käyttö luonnollisesti vaatii, että kaikki palomuurin säännöt ovat lokittavia sekä pidemmän aikavälin liikenteen analysoinnille.

4 Testiympäristö ja testaus

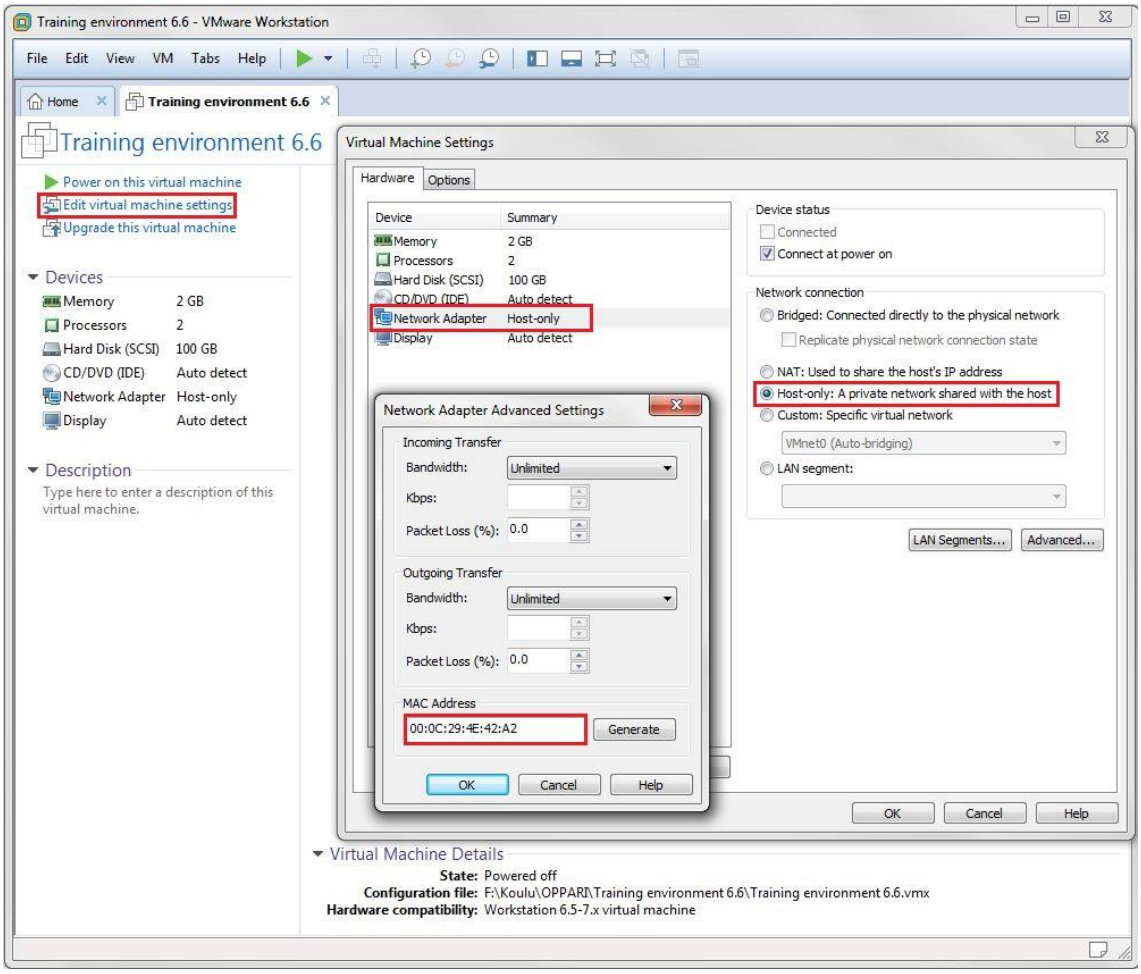
4.1 Testiympäristön asennus

Laitevalmistaja Algosec tarjosi tutustumiseen täysin virtualisoidun ympäristön. Testiympäristöä käyettiin Vmware Workstationilla aivan kuten mitä tahansa virtuaalikonetta.



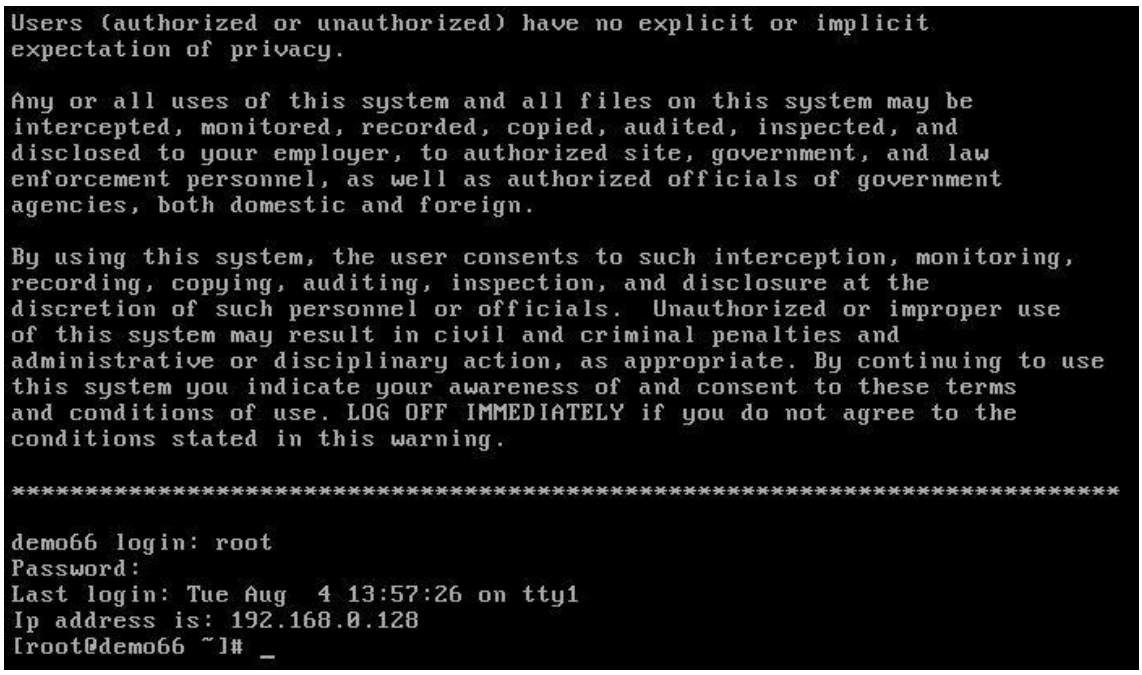
Kuva 5 testiympäristön asennuksen aloitus.

Testiympäristö avataan käyttöön vmx-tiedostosta, jonka Algosec tarjosi työtä varten. Kun tiedosto oli saatu avattua täytyi virtuaalikoneen verkkoadapteriin tehdä muutoksia, jotta ympäristöä voitaisiin käyttää oman tietokoneen selaimella.



Kuva 6 Virtuaalikoneen asetukset.

Verkkoadapterin tyypiksi vaihdettiin Host-only. Samalla tarkistettiinn, että MAC-osoite oli 00:0C:29:4E:42:A2. Tämä oli tärkeää siitä syystä, että lisenssi, jonka Algosec laitteelle generoi, oli tehty juuri tuolle osoitteelle. Tämän jälkeen virtuaalikone käynnistettiin.



Kuva 7 Valmiiseen virtuaalikoneeseen kirjautuminen.

Kun järjestelmä käynnistyi onnistuneesti, pyysi se sisäänkirjautumista. Järjestelmään kirjauduttiin oletuskäyttäjätunnuksella root ja salasanalla algosec. Kirjautumisen jälkeen järjestelmä ilmoitti IP-osoitteensa 192.168.0.128. Jatkossa virtuaalikoneeseen ei tarvinnut enää koskea, sillä graafiseen käyttöliittymään pääsi selaimella IP-osoitetta käyttäen.

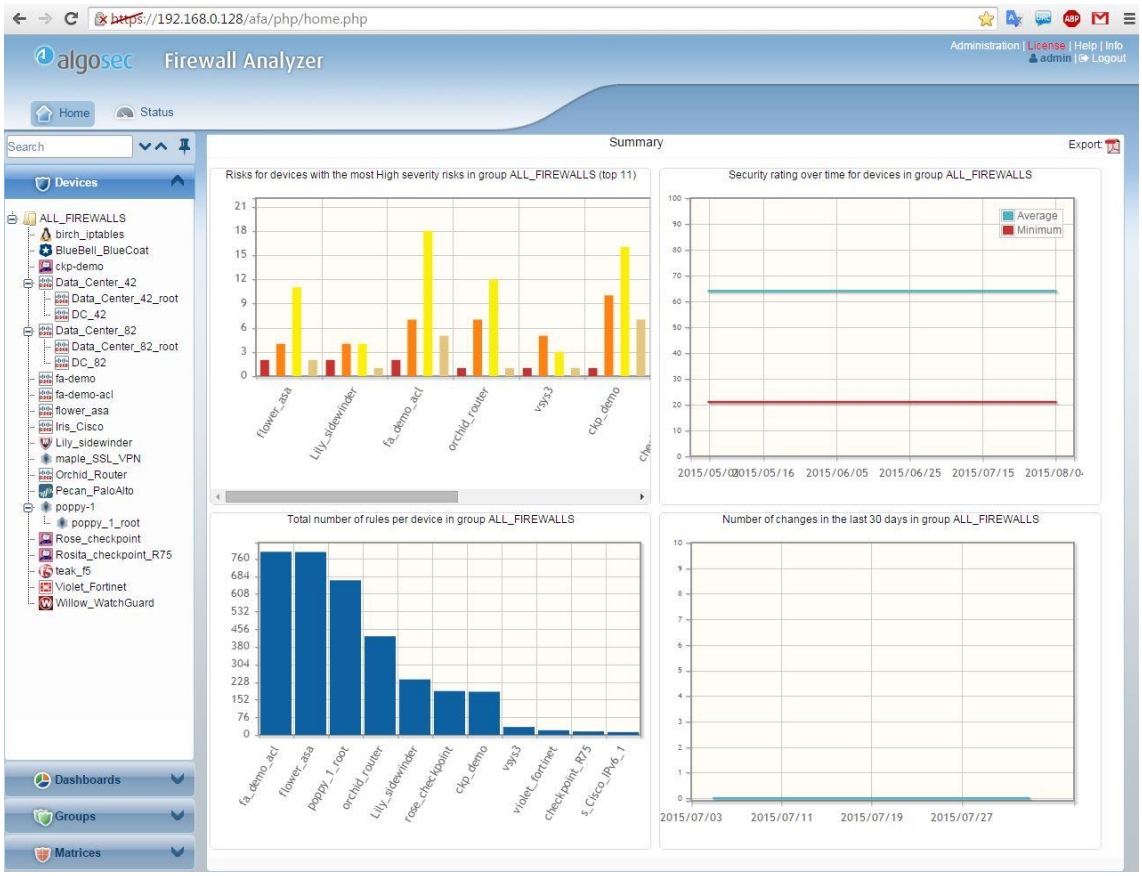
Selaimella yhdistettäessä osoitteeseen https://192.168.0.128 aukesi Algosec Security Management Suiten etusivu. Sivulta valittiin Firewall Analyzer.

Kuva 8 Algosec Security Management Suiten etusivu.

Tämän jälkeen Firewall Analyzer pyysi kirjautumaan sisään. Tällä kertaa oletuskäyttäjätunnus on admin ja salasana algosec.

Kuva 9 Kirjautuminen Algosec Firewall Analyzeriin.

Järjestelmään kirjauduttua aukesi graafisen käyttöliittymän etusivu.



Kuva 10 Algosec Firewall Analyzerin graafisen käyttöliittymän etusivu.

Kun Algosec Firewall Analyzer oli asennettu ja valmiina käyttöön, oli seuraava vaihe asentaa lisenssin. Graafisen käyttöliittymän etusivu ilmoitti lisenssin puuttumisesta punaisella tekstillä kuvaruudun oikeassa yläkulmassa.

Kuva 11 Puuttuva lisenssi ilmaistaan punaisella tekstillä.

Punaista lisenssitekstiä painettua päästiin katsomaan lisenssin tietoja.

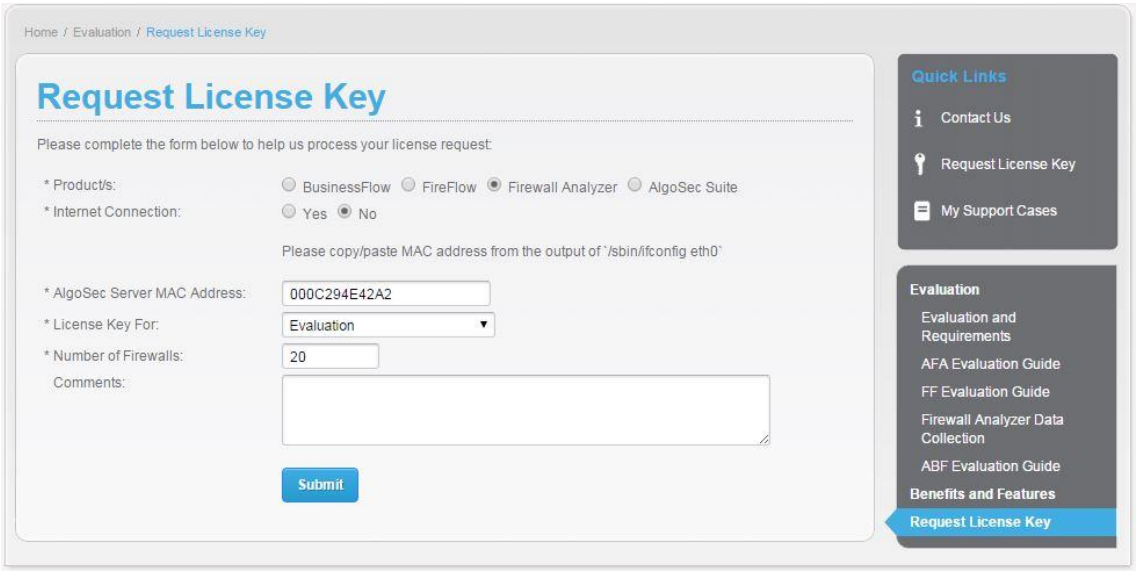
Kuva 12 Nykyiset lisenssitiedot.

Aluksi tiedot näyttivät tyhjää, koska lisenssiä ei ollut asennettu. Uuden lisenssin pystyi asentamaan painamalla Install License -nappia, jonka jälkeen valitaan haluttu lisenssitiedosto.

Kuva 13 Lisenssitiedoston asentaminen.

Lisenssivaihtoehtoja oli kaksi erilaista ja niitä pystyi anomaan Algosecin verkkosivuilta. Kun Algosec oli käsitellyt hakemuksen, lähettivät he lisenssitiedoston sähköpostiin. Ensimmäinen vaihtoehdoista oli online-lisenssi, ja sen asennus vaatii yhteyden Internettiin ja mahdollisesti proxyn konfiguroinnin. Kyseisen lisenssin voi aktivoida jo ennen virtuaaliympäristön asennusta. Toinen vaihtoehto oli hakea offline-lisenssi, joka on etukäteen aktivoitu lisenssi perustuen virtuaalikoneen MAC-osoitteeseen. Tämän

lisenssin asennus ei vaadi yhteyttä Internetiin. Molemmat lisenssit voidaan aktivoida vain kerran eikä niitä pysty käyttämään tämän jälkeen uudelleen. Mikäli vanhan lisenssin tilalle asentaa uuden, kirjoittuu se edellisen yli. Testiympäristöstä ei ollut yhteyttä Internetiin, joten testausta varten käytettiin Algoseciltä pyydettyä offline-lisenssiä.

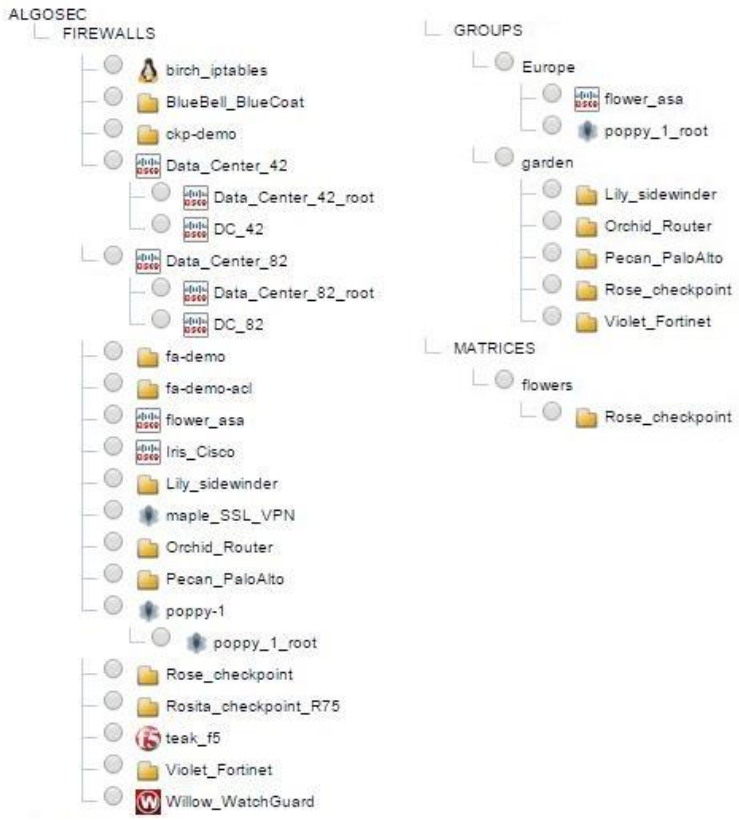


Kuva 14 Lisenssihakemuksen teko Algosecin verkkosivuilla.

Lisenssihakemuksen pystyi tekemään Algosecin verkkosivuilla osoitteessa https://portal.algosec.com/en/evaluation/request_license_key. Sivuille täytyi ensin luoda omat tunnukset, jotta anomuksen teko onnistui.

4.2 Testiympäristö ja topologia

Käytettävä testiympäristö oli sama, jota Algosec käyttää heidän omissa sertifikaattikoulutuksissa. Ympäristö koostui useista eri laitevalmistajien tuotteista ja laitteiden konfiguraatiot sekä politiikat oli määritelty virtuaalikoneen tiedostoissa. Käytännössä ympäristö simuloi kuvitteellisen yrityksen isoa verkkoa, jossa on osana palomuureja, reitittimiä, kuormantasaajia ja VPN-laitteita. Kuvassa 15 on listaus testiympäristöön kuuluneista laitteista.



Kuva 15 Testiympäristön laitteet.

4.2.1 Uuden laitteen lisääminen järjestelmään

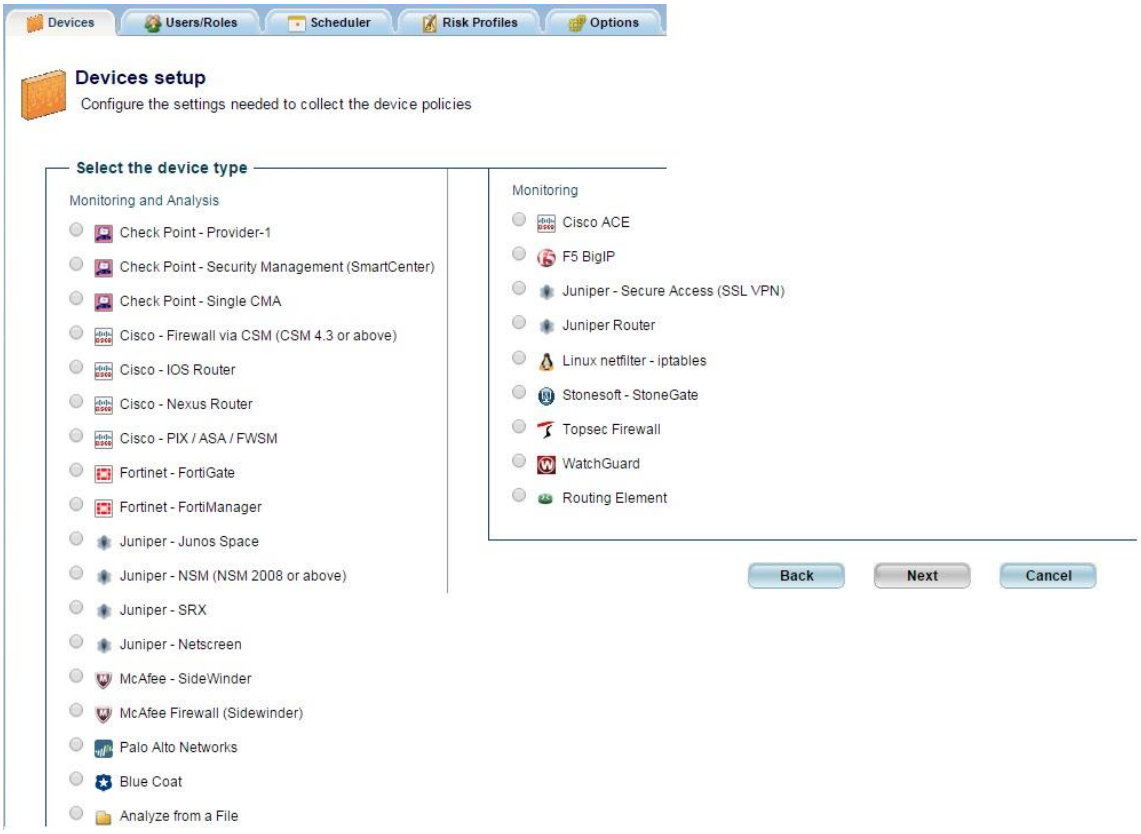
Laitteiden lisääminen järjestelmään onnistui graafisen käyttöliittymän Administration-valikon kautta.

Kuva 16 Administration-valikko löytyy etusivun oikeasta yläkulmasta.

Kyseisen valikon alta löytyi Devices-välilehti, josta uuden laitteen asennuksen pystyi aloittamaan.

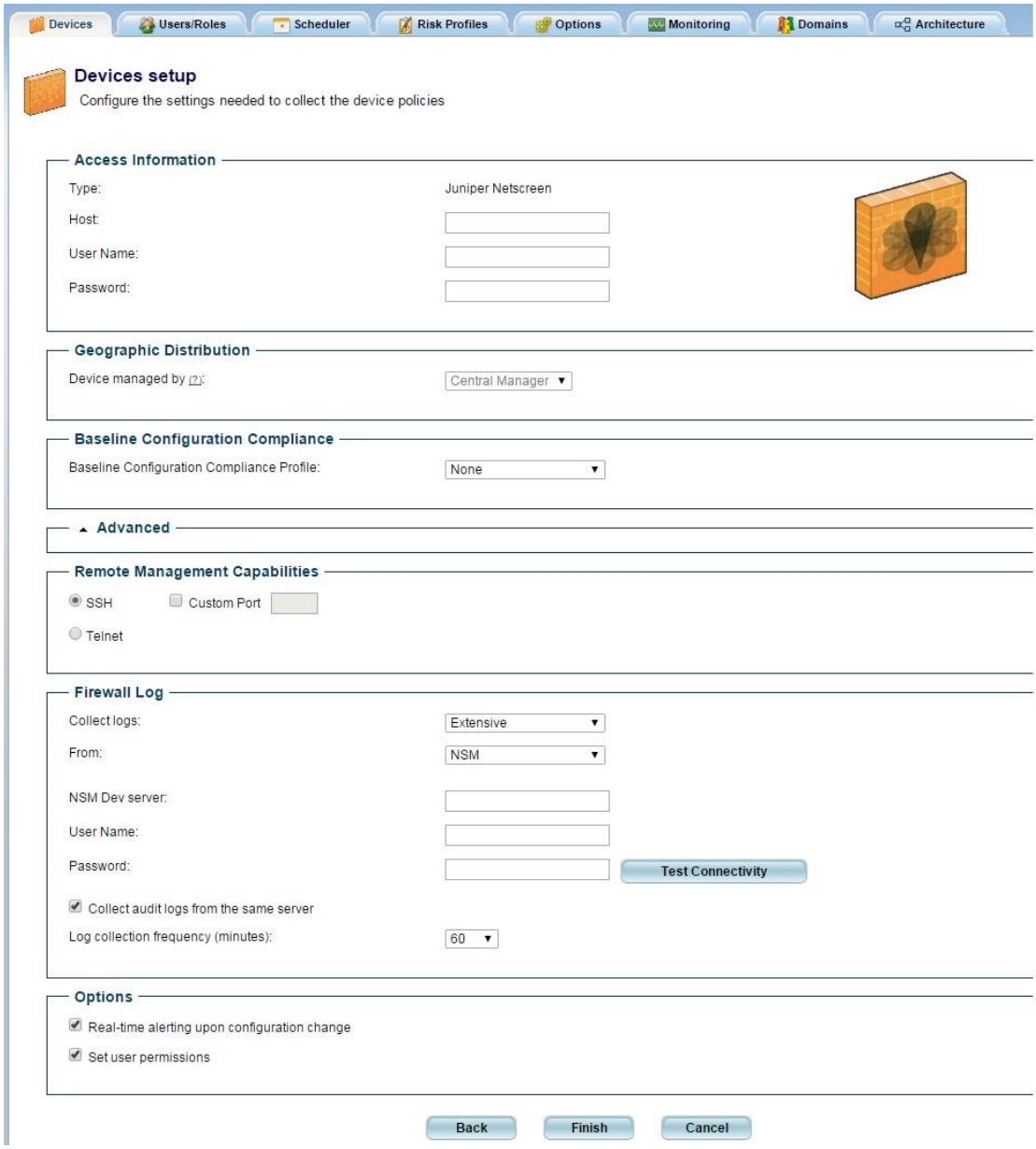
Kuva 17 Uuden laitteen tuonti järjestelmään.

Uuden laitteen asennuksen aloitettua aukesi valikko, josta täytyi valita kyseessä oleva laite. Laitteet oli jaoteltu kahteen ryhmään Monitoring and Analysis sekä Monitoring perustuen siihen, mitä ominaisuuksia kyseiselle laitteelle oli mahdollista saada.



Kuva 18 Asennettavan laitteen valinta.

Virtuaaliseen testiympäristöön ei pystytty lisäämään laitteita, mutta käytännössä lisäyksen tekeminen olisi ollut varsin helppoa. Device setup -sivulla syötetään kenttiin tarvittavat tiedot ja testataan yhteys laitteeseen.



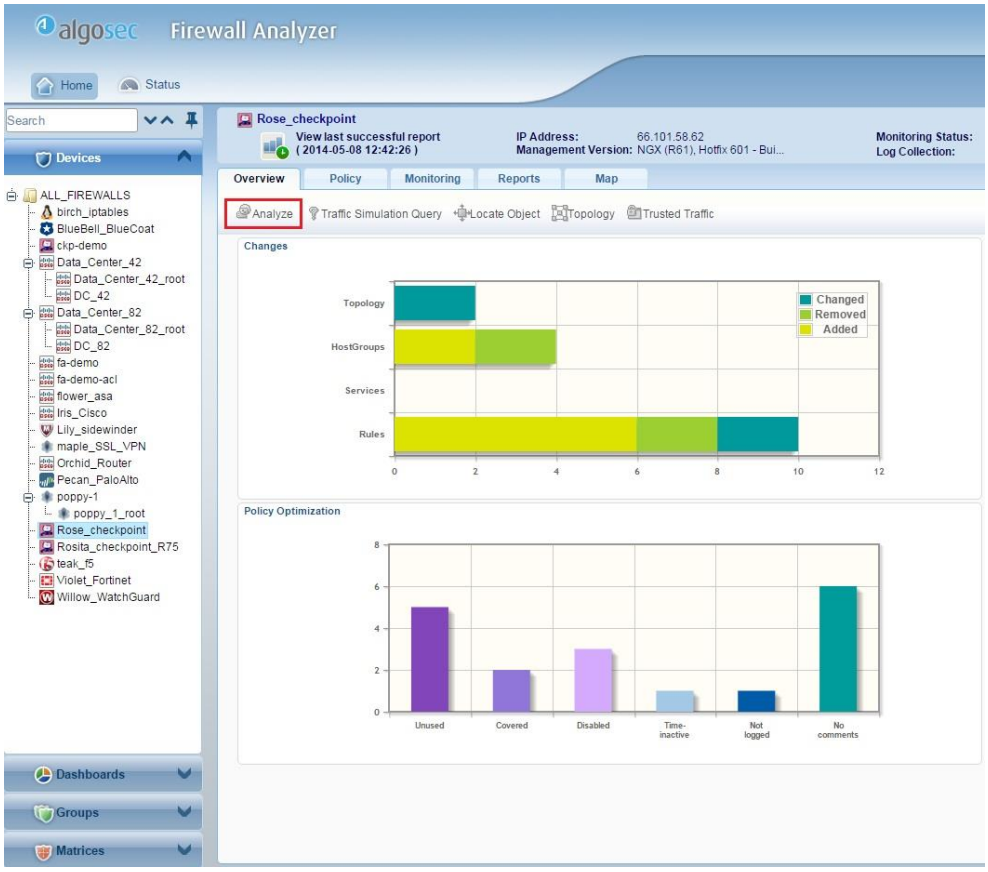
Kuva 19 Devices setup -sivu, johon syötetään tarvittavat laitteen tiedot.

Riittää, kun tiedossa on laitteen nimi ja käyttäjätunnukset, joilla laitteeseen pääsee kirjautumaan. Kun sivu on valmis, valitaan finish ja tämän jälkeen valitaan vielä käyttäjät, joilla on oikeus katsoa laitteen raportteja.

4.2.2 Raporttien luonti

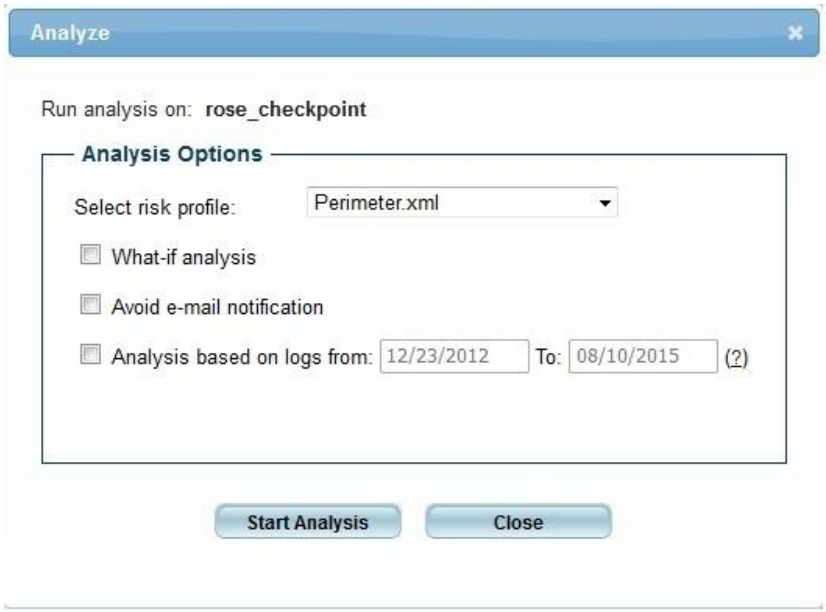
Algosec Firewall Analyzerin teho perustuu sen luomiin raportteihin laitteista. Raporteissa Algosec tarkistaa palomuurin lokin, konfiguraation ja politiikan. Valmiin raportin kautta voidaan suorittaa kaikki politiikan optimoinnit.

Raportin teko aloitettiin etusivulta ensin valitsemalla haluttu palomuuri vasemmasta laiteluettelosta ja sen jälkeen painamalla overview-valikosta löytyvää analyze-painiketta.



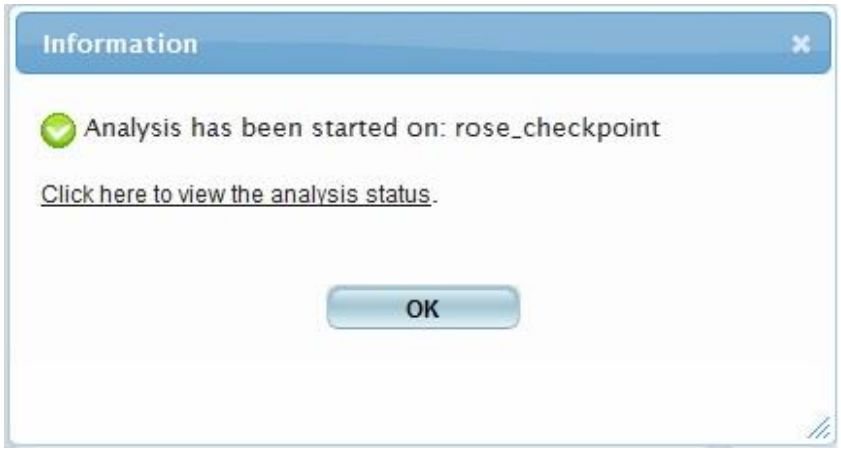
Kuva 20 Näkymä etusivulla, kun halutaan aloittaa raportin teko.

Tämän jälkeen järjestelmä kysyi, mitä lisävaihtoehtoja haluttiin käyttää ja mitä riskiprofiilia raportin tekoon käytetään. Riskiprofiilit ja niiden muokkaus ei kuulunut työn aihepiiriin, joten raportti tehtiin oletusarvoilla.



Kuva 21 Riskiprofiilin valinta ja muut lisävaihtoehdot raportin luontia varten.

Tämän jälkeen Algosec ilmoitti, että automaattinen tiedonkeruu on aloitettu ja analyysin edistymistä pystyi seuraamaan status-välilehdellä.



Kuva 22 Järjestelmä ilmoittaa analyysin alkaneen.

Kuva 23 Analyysin edistyminen näkyy status-välilehdellä. [2, s. 218.]

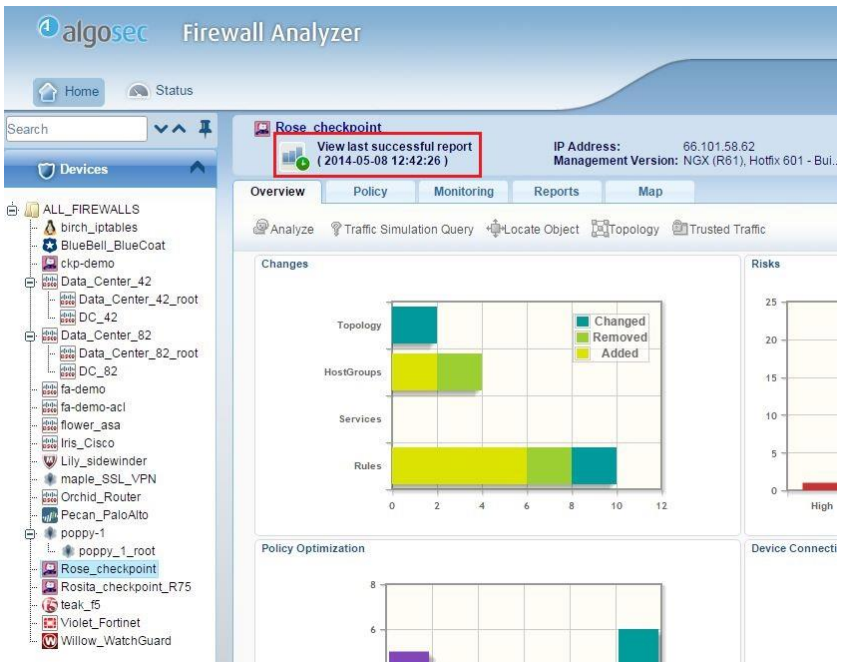
Status-välilehdeltä näki analyysin edistymisen ja mahdolliset virheilmoitukset. Mikäli halusi, pystyi analyysin teon myös keskeyttämään. Laitteesta riippuen analyysin teko saattoi viedä jopa kymmenen minuuttia.

Kun analyysi oli valmis ja raportti luettavissa, pystyi sen kautta hyödyntämään kaikkia Algosecin tarjoamia työkaluja.

4.3 Ominaisuuksien testaus käytännössä

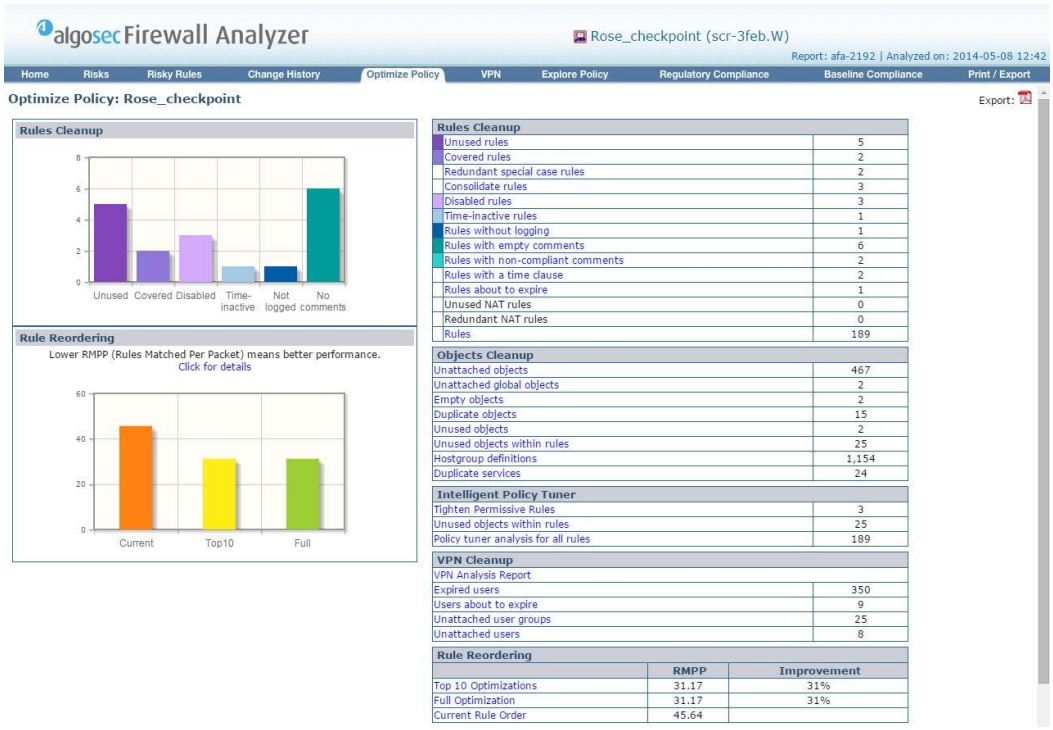
Algosec Firewall Analyzerin tekemien raporttien pohjalta päästiin hyödyntämään erilaisia työkaluja palomuurien sääntökantojen optimoimiseksi.

Raportteja pääsi katsomaan järjestelmän etusivun kautta. Ensin vasemmasta valikosta valittiin tutkittava palomuuri ja sen jälkeen valittiin uusin raportti.



Kuva 24 Uusimman raportin avaus etusivun kautta.

Valmis raportti piti sisällään monta eri osiota, joiden alta löytyivät kaikki tarvittavat työkalut. Koska työ käsitti vain sääntökannan optimoinnin, tarkasteltavat työkalut löytyivät Optimize Policy -valikon alta.

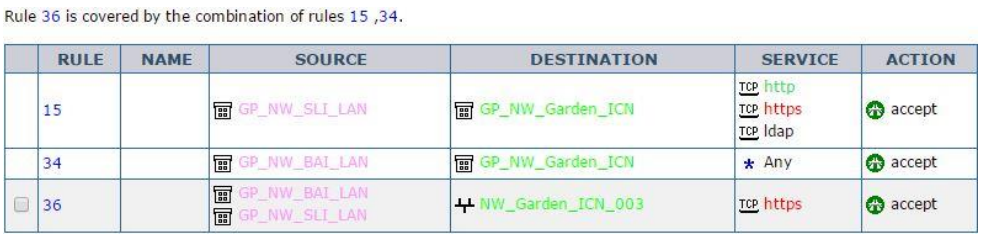


Kuva 25 Avattu raportti Optimize Policy -valikon kohdalla.

Seuraavaksi tutkitaan tarkemmin Optimize Policy -valikon alta löytyviä työhön valittuja työkaluja. Tarkasteluun valittiin yksi testiympäristön Check Point -palomuuri nimeltä Rose_checkpoint.

4.3.1 Covered rules

Covered rules -työkalulla Algosec näyttää välittömästi sellaiset säännöt, jotka täyttävät luvussa 3.1.1 läpikäydyt ehdot.


Rule 36 is covered by the combination of rules 15 ,34.

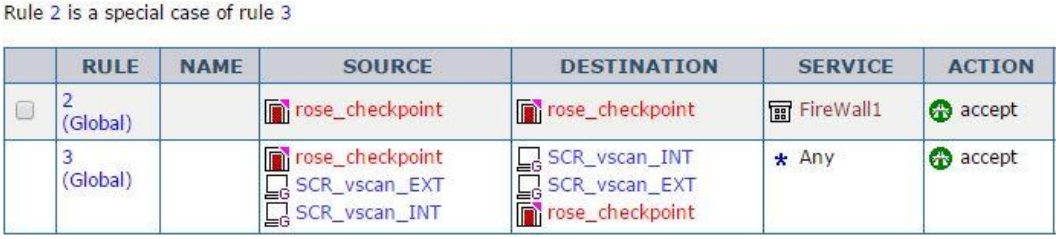
	RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION
	15		GP_NW_SLI_LAN	GP_NW_Garden_ICN	TCP http TCP https TCP ldap	accept
	34		GP_NW_BAI_LAN	GP_NW_Garden_ICN	* Any	accept
	36		GP_NW_BAI_LAN GP_NW_SLI_LAN	NW_Garden_ICN_003	TCP https	accept

Kuva 26 Covered rule -esimerkki testiympäristön palomuurilta Rose_checkpoint.

Kuvasta 26 huomataan, että säännöt 15 ja 34 muodostavat sellaisen yhdistelmän, että sääntö 36 voidaan poistaa. Esimerkissä GP_NW_Garden_ICN-ryhmä sisälsi verkon nimeltä NW_Garden_ICN_003. Kun sääntö poistettiin palomuurilta ja raportti ajettiin uudelleen, ei Covered rules -kohdassa ollut yhtään korjattavaa sääntöä.

4.3.2 Redundant special case rules

Redundant special case rules -valikkoa tarkasteltaessa Algosec löysi Rose_checkpoint-palomuurin sääntökannasta kuvan 27 säännöt.


Rule 2 is a special case of rule 3

	RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION
	2 (Global)		rose_checkpoint	rose_checkpoint	FireWall1	accept
	3 (Global)		rose_checkpoint SCR_vscan_EXT SCR_vscan_INT	SCR_vscan_INT SCR_vscan_EXT rose_checkpoint	* Any	accept

Kuva 27 Redundant special case rule Rose_checkpoint-palomuurilla.

Tässä tapauksessa Algosec havaitsi, että harmaalla pohjalla oleva sääntö 2 olisi syytä poistaa. Sääntö 3 sisältää rose_checkpoint -välisen liikenteen sallien kaikki portit, joten säännön 2 ollessa tarkempi, on se täysin turha.

4.3.3 Unrouted rules

Reitittämättömiä sääntöjä tarkasteltiin virtuaaliympäristön Palo Alto -palomuurilta. Pecan_PaloAlto -nimiseltä laitteelta löytyi kaikkiaan neljä reitittämätöntä sääntöä.

	NAME	FROM	SOURCE	USER	TO	DESTINATION	APPLICATION	SERVICE	ACTION
	Remote-1-internal_12	demo_dmz	Remote-1-internal_12	any	demo_dmz	Remote-2-internal10	any	SMTP	
	Remote_30_interna9	demo_dmz	Remote-30-internal_9	any	demo_internal	dns-int	any	any	
	UK_DNS	demo_external	Net_UK_DNS1	any	demo_internal	DMZ_grp135	any	ssh	
	icmp_inside	demo_external	Net_UK_DNS1	any	demo_internal	LAN	icmp	any	

Kuva 28 Reitittämättömät säännöt Pecan_PaloAlto -palomuurilla.

Jokaisessa säännössä oli nähtävissä joko lähde tai kohde, joka oli korostettu värillä. Korostettuja objekteja ei löytynyt palomuurin reitityksestä tai kyseisistä zoneista, joihin ne oli merkitty kuuluvaksi, ja täten liikenne näihin lähteisiin tai kohteisiin ei kulje kyseisen laitteen läpi. Nämä neljä sääntöä voitiin poistaa palomuurin sääntökannasta ilman, että se vaikutti mihinkään liikenteeseen. Säännöt olivat mahdollisesti peruja jostain vanhasta ympäristöstä, ja muutosten myötä ne oli unohdettu poistaa.

4.3.4 Samankaltaisten sääntöjen yhdistäminen

Rules Consolidation -kohtaa tutkittaessa Algosec löysi palomuurilta neljä sääntöä, jotka voitiin yhdistää kahdeksi.

RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION
34		GP_NW_BAI_LAN	GP_NW_Garden_ICN	* Any	accept
46		GP_NW_BAI_LAN	GP_NW_SLI_LAN	* Any	accept

RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION
22		GP_NW_SLI_LAN	GP_PC_Netware5	ICMP icmp-proto ICMP echo-reply ICMP echo-request	accept
30		GP_NW_SLI_LAN	GP_PC_Netware5	UDP snmp-161	accept

Kuva 29 Sääntöjä Rose_checkpoint -palomuurilta joita voitiin yhdistää.

Ylempää sääntöparia yhdisti sama lähde ja sama palvelu. Säännöt voitiin yhdistää yhdeksi, niin että sisällytettiin samaan sääntöön molemmat kohteet GP_NW_Garden_ICN sekä GP_NW_SLI_LAN. Näin saatiin karsittua yksi ylimääräinen sääntö pois palomuurilta.

Alemmassa sääntöparissa ainoana erona olivat käytettävät palvelut. Lisäämällä sääntöön 22 snmp-161 objektia, voitiin poistaa sääntö 30 turhana.

Tällaisia sääntöjä muodostuu usein tuotantoympäristöissä, jos sääntöjen laatija ei jaksa tarkasti käydä olemassaolevia sääntöjä läpi. Kyseinen työkalu onkin täten erittäin hyödyllinen lisä.

4.3.5 Käyttämättömät säännöt

Optimize Policy -valikon kohdasta Unused Rules löydettiin kaksi sääntöä, jotka Algosec oli määritellyt käyttämättömiksi.

Unused Rules
The analysis is based on logs from 25-Dec-2012 to 8-May-2014 (total: 263 days).
Log analysis is configured to include logs starting at most 500 days before the report date.
To change this setting (unlimited): login as administrator,
go to Administration > Options > Log Analysis

Policy: scr-3feb.W

No log records for the following rules

Select All Unused Rules

	RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION	COMMENT	LAST USE
	6		PC_Garden_ruoc4l.on.garden.net	rose_checkpoint	GP_TCP_Axent	accept	FireFlow #209: 6 month proj - contact Jim/InfoSec	N/A
	23		GP_NW_SLI_LAN	GP_PC_Garden_DNS	dns	accept	FireFlow #298: Garden employees at SLI point to Garden DNS	N/A

Kuva 30 Kaksi käyttämätöntä sääntöä, jotka Algosec löysi palomuurilta.

Tässä tapauksessa järjestelmä tutki palomuurin lokeja joulukuusta 2012 lähtien eikä tuona aikana sääntöihin tullut yhtään osumaa. Tämän perusteella voitiin todeta, että sääntöjen poistaminen oli erittäin turvallista ja näin saatiin sääntökantaa siivottua. Kyseisen ominaisuuden kanssa piti olla erittäin varovainen, koska mikäli tarkkailtava aikajakso oli asetettu liian lyhyeksi, voitiin vahingossa poistaa tärkeitäkin sääntöjä, joihin ei vain sattumalta tullut yhtään osumaa tarkkailujakson aikana.

4.3.6 Sääntöjen uudelleenjärjestäminen

Raportin lopusta löytyvän Rule Reordering -alaotsikon alta löydettiin työkalut, jotka auttoivat sääntöjen uudelleenjärjestämisessä. Kuten aikaisemmin mainittiin, sääntöjen uudelleenjärjestämisellä parannetaan palomuurin suorituskykyä.

Rule Reordering		
	RMPP	Improvement
Top 10 Optimizations	31.17	31%
Full Optimization	31.17	31%
Current Rule Order	45.64	

Kuva 31 Vaihtoehdot liittyen sääntöjen uudelleenjärjestämiseen.

Valikosta huomattiin jo suoraan että täydellistä sääntökannan uudelleenjärjestämistä ei tarvita. Top10 Optimizations -vaihtoehdolla saavutettiin täysin sama lopputulos.

Top 10 Rules to Move
The analysis is based on logs from 25-Dec-2012 to 8-May-2014 (total: 263 days).
Log analysis is configured to include logs starting at most 500 days before the report date.
To change this setting (unlimited): login as administrator,
go to Administration > Options > Log Analysis

	Instructions								IMPROVEMENT
1	Move rule 49 before rule 33								21%
	ORIGINAL RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION	COMMENT	DOCUMENTATION	
	49		GP_Dthomson	Shiva	Any	accept	FireFlow #345: MicroSoft Windows Update		
	33		ASF_GEO_Temp PC_SCR_scr0801_EXT	PC_SCR_scr0801_EXT ASF_GEO_Temp	pcANYWHERE http-8080 http	accept	FireFlow #320: Temp Entry for GeoSolutions Aug 1,2007 DT CS300701-82		
2	Move rule 50 before rule 33								9%
	ORIGINAL RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION	COMMENT	DOCUMENTATION	
	50	users	Citrix-Users@Any	TDE_3943_VML-WEB1_INT TDE_5403_eCommerce_INT	http https	Client Auth	FireFlow #511: remote users/HQ		
	33		ASF_GEO_Temp PC_SCR_scr0801_EXT	PC_SCR_scr0801_EXT ASF_GEO_Temp	pcANYWHERE http-8080 http	accept	FireFlow #320: Temp Entry for GeoSolutions Aug 1,2007 DT CS300701-82		

Kuva 32 TOP10 -sääntöjen kaksi ensimmäistä sääntöä.

Valitsemalla Top10 Optimizations voitiin tarkastella, mitä sääntöjä Algosec ehdotti uudelleenjärjestettäviksi. Kuvassa 32 on kaksi merkittävintä muutosta, joita järjestelmä ehdotti uudelleenjärjestettäviksi. Kuvasta nähdään, että listan ensimmäisellä muutoksella saavutetaan jo erittäin huomattava 21%:n parannus. Kun muutokset oli suoritettu palomuurille, voitiin raportti ajaa uudelleen. Tällöin merkittäviä parannusehdotuksia ei luonnollisesti enää löytynyt.

5 Yhteenveto

Insinöörityön suorittaminen onnistui alusta alkaen erittäin hyvin. Virtuaaliympäristö tarjosi joustavan tavan tutkia tarkasteltavan laitteen ominaisuuksia ja testata niitä käytännössä. Ongelmia työn suorittamisessa tuli ainoastaan siinä vaiheessa, kun tuotteen väliaikainen lisenssi umpeutui. Laitevalmistaja ei pystynyt tarjoamaan jälkikäteen vastaavaa lisenssiä, mutta työ saatiin tästä huolimatta suoritettua loppuun niiltä osin, kuin haluttiinkin. Eri ominaisuuksien lisätestaus ei vain enää ollut mahdollista.

Työn rajaaminen vain sääntökannan optimointiin todettiin järkeväksi ratkaisuksi, sillä laitteen muiden ominaisuuksien tutkiminen olisi laajentanut työtä valtavasti, eikä aika tähän olisi riittänyt.

Laitteeseen ja sen ominaisuuksiin tutustuttua tultiin siihen tulokseen, että Algosec Firewall Analyzer olisi erittäin hyödyllinen ja tarvittava lisä usean Cygaten asiakkaan ympäristöihin. Laitteen käyttöönotto toisi mukanaan huomattavia etuja ja tekisi se työskentelystä tehokkaampaa.

Lähteet

1 AlgoSec Firewall Analyzer User Guide. Verkkodokumentti. <https://portal.algosec.com/resources/download/?Section=vendor&file_id=271>. Luettu 3.8.2015.

2 Algosec next generation firewall policy management tips ebook. Verkkodokumentti. <http://www.slideshare.net/AlgoSec/the-big-colleaction-of-nextgeneration-firewall-policy-management-tips-e-book>. Luettu 3.8.2015.

3 Algosec suite brochure. Verkkodokumentti. <http://www.techmaxkenya.com/resources/AlgosecSuiteBrochure.pdf>. Luettu 3.8.2015.

4 Eguide to automating firewall. Verkkodokumentti. <https://www.algosec.com/wp-content/uploads/2016/03/The-eGuide-to-Automating-Firewall-Change-Control-WEB.pdf>. Luettu 3.8.2015

5 AlgoSec - Automating Firewall Management. Youtube. <https://www.youtube.com/watch?v=mG4_CTN9kbs>. Katsottu 3.8.2015.

6 Firewall (computing). Verkkodokumentti. <https://en.wikipedia.org/wiki/Firewall_(computing)>. Luettu 12.8.2015.

7 The Evolution of Firewalls. Verkkodokumentti. <http://www.informationweek.com/partner-perspectives/bitdefender/the-evolution-of-firewalls-past-present-and-future/a/d-id/1318814>. Luettu 13.5.2016.

8 Understanding PCI compliance auditing. Verkkodokumentti. <http://www.cio.com.au/article/400307/understanding_pci_compliance_auditing/>. Luettu 1.7.2017.

9 ISO/IEC 27001 – Information security management. Verkkodokumentti. <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>. Luettu 2.7.2016.

10 Tietoturvajärjestelmän sertifiointi. Verkkodokumentti. <http://www.inspecta.com/fi/Palvelut/Sertifiointi/Jarjestelmasertifiointi/Tietoturvajarjestelman-sertifiointi-ISO-IEC-27001/>. Luettu 2.7.2016.

11 Firewall Evolution from Packet Filter to Next Generation. Verkkodokumentti. <http://www.juniper.net/techpubs/en_US/learn-about/LA_FIrewallEvolution.pdf>. Luettu 14.5.2016.

12 Tunkeilijan havaitsemisjärjestelmä. Verkkodokumentti. <https://fi.wikipedia.org/wiki/Tunkeilijan_havaitsemisj%C3%A4rjestelm%C3%A4>. Luettu 5.5.2016.

13 Application firewall. Verkkodokumentti. <https://en.wikipedia.org/wiki/Application_firewall>. Luettu 5.5.2016.