LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

KESKITETTY PALOMUURIHALLINTA VIRTUAALIPALVELIMESSA

LAHDEN AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Syksy 2013
Yu Gang Zhou

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

ZHOU, YU GANG: Keskitetty palomuurihallinta virtuaalipalvelimessa

Tietoliikennetekniikan opinnäytetyö, 31 sivua, 2 liitesivua

Syksy 2013

TIIVISTELMÄ

Opinnäytetyön aiheena oli suunnitella ja toteuttaa keskitetty palomuurihallinta virtuaalipalvelimelle. Tavoitteena oli korvata tuotannossa olevat kaksi hallintajärjestelmää yhdellä järjestelmällä. Opinnäytetyö tehtiin toimeksiantona DNA Oy:lle.

Aluksi selvitettiin uuden hallintapalvelimen järjestelmävaatimukset, jotka olivat Windows 2008 Server, neliydinprosessori, 16 Gt keskusmuistia ja 100:n Gt kovalevy. Ainoat tuetut virtualisointiohjelmat olivat Vmware ESX ja ESXi. Sen jälkeen tehtiin VMware ESXi:llä virtuaalipalvelin, joka täytti vaatimukset. Palvelimen käyttöjärjestelmäksi valittiin Ciscon suosituksen mukaan Windows 2008 Server R2 SP1.

CSM 4.2 asennettiin onnistuneesti virtuaalipalvelimelle. Vanhan CSM-palvelimen tietokanta tuotiin uudelle CSM-palvelimelle käyttäen varmuuskopion palautusta. Uusi lisenssi piti asentaa CSM 4.2 -palvelimelle, koska vanha lisenssi ei ollut yhteensopiva uuden CSM:n kanssa. Toisen vanhan CSM:n tietokanta jouduttiin skannaamaan verkosta, koska CSM 4.2 oli bugi, joka aiheutti tietokannan viemisessä virheen, jos tietokanta oli tuotu toisesta palvelimesta. CSM 4.2 päivitettiin viimeiseen versioon 4.4 SP2. Testiksi luotiin joitakin palomuureja uudessa hallinnassa, jotta nähtiin, toimiko kaikki niin kuin piti. Testit onnistuivat hienosti. Opinnäytetyön tuloksena onnistuttiin pystyttämään keskitetty palomuurihallinta virtuaalipalvelimeen.

Avainsanat: CSM, palomuuri, virtualisointi, VMware ESXi, Windows 2008 Server

Lahti University of Applied Sciences
Degree Programme in Information Technology

ZHOU, YU GANG: Centralized firewall management in a virtual server

Bachelor's Thesis in Telecommunications, 31 pages, 2 appendices

Autumn 2013

ABSTRACT

The subject of this thesis was to design and implement a centralized firewall management for a virtual server. The objective was to replace two current management servers with one server. This was performed as an assignment for DNA Ltd.

The first task was to determine the system requirements for the new management server. They were Windows 2008 Server, quadcore prosessor, 16 GB RAM and 100 GB hard drive. The only supported virtualization software were VMware ESX and ESXi. Then a virtual server meeting the requirements was created using VMvare ESXi. Windows 2008 Server R2 SP1 was selected for OS as it was recommended by Cisco.

CSM 4.2 was installed successfully on the virtual server. Database from the older CSM was imported to the new CSM using the restore database method. A new license had to be installed to CSM 4.2 because the old license was not compatible with the new server. The database of the second old CSM had to be scanned from Network. There was a caveat in CSM 4.2, which caused exporting the database to fail if the database had been restored from another server. CSM 4.2 was updated to the latest version CSM 4.4 SP2. For testing purposes some firewalls were made in the new manager and deployed to see if everything worked as intended. The tests were a success. As a result of this thesis a centralized firewall management running in a virtual server was successfully set up.

Key words: CSM , firewall, virtualization, VMware ESXi, Windows 2008 Server

LYHENNELUETTELO

AAA	Authentication, Authorization and Accounting. Protokolla, jolla voidaan tunnistaa toinen osapuoli tietoverkossa.
ACL	Access Control List. Pääsylista.
ASA	Adaptive Security Appiance. Ciscon valmistama palomuuri.
AUS	Auto Update Server. Ciscon tietoturvaohjelmistossa käyttämä palvelin, jolla hallitaan PIX-palomuureja.
CLI	Command Line Interface. Tekstipohjainen -käyttöliittymä.
CPU	Central Processing Unit. Suoritin tai prosessori.
CSM	Cisco Security Manager. Ohjelmisto, jolla hallitaan Ciscon tietoturvalaitteita.
DNS	Domain Name System. Nimipalvelu.
FWSM	Firewall Services Module. Palomuuripalvelumoduuli. Moduulissa ajetaan yhtä tai useampaa palomuuria.
GHz	Gigahertsi. Prosessorin kellontaajuus eli nopeus.
Gt	Gigatavu (GB, Gigabyte). Muistin tai kovalevyn koko voidaan ilmaista gigatavuina.
GUI	Graphical User Interface. Graafinen käyttäjäliittymä. Käyttäjän ja ohjelman tai palvelimen välinen graafinen rajapinta.

HTTPS	Hyper Text Transfer Protocol Secure. Verkkopalvelimien käyttämä protokolla, jolla suojataan sisältö.
IDS	Intrusion Detection and Prevention System. Tunkeutujan havaitsemis- ja estojärjestelmä.
IP	Internet Protocol. IP-protokolla huolehtii tietoliikennepakettien toimittamisesta perille.
IPv4	Internet Protocol version 4. Käytetään 32-bittisiä osoitteita.
NAT	Network Address Translation. Verkko-osoitteen muutos toiseksi osoitteeksi.
NSM	Network Security and Manager. Juniper Networksin valmistama hallintajärjestelmä.
OS	Operating System. Käyttöjärjestelmä.
PAT	Port Address Translation. NAT-tyyppi, jossa useita IP-osoitteita muutetaan yhdeksi IP-osoitteeksi.
PIX	Private Internet eXchange. Ciscon valmistama palomuuri.
RADIUS	Remote Authentication Dial In User Service. Käytetään käyttäjän tunnistukseen AAA-protokollan kanssa.
RAM	Random Access Memory. Keskusmuisti. Tyhjenee virrankatkaisun yhteydessä.
RDP	Remote Desktop Protocol. Etätyöpöytäyhteys.

SP	Service Pack. Huoltopäivitys. Sisältää päivityksiä tai uudistuksia.
SPI	Stateful Packet Inspection. Tilallinen palomuuri.
TACACS+	Terminal Access Controller Access-Control System Plus. Käytetetään käyttäjän tunnistukseen AAA-protokollan kanssa.
TCP	Transmission Control Protocol. Yhteydellinen siirtoprotokolla. Lähettää hävinneet paketit uudestaan.
UDP	User Datagram Protocol. Yhteydetön siirtoprotokolla. Paketin perille menoa ei varmisteta.
VPN	Virtual Private Network. Virtuaalinen yksityisverkko.

SISÄLLYS

1 JOHDANTO

1.1 Työn tausta ja tavoitteet

Palomuureja hallitaan perinteisesti ottamalla suora yhteys palomuuriin käyttämällä komentokehote-käyttöliittymää tai graafista käyttöliittymää. Tämä on hyvä ja tehokas tapa, kun hallittavien palomuurien lukumäärä on pieni. Lukumäärän kasvaessa satoihin tai tuhansiin ei ole ylläpidon ja resurssien käytön kannalta järkevää yhdistää palomuureihin yksitellen.

Käyttämällä keskitettyä hallintajärjestelmää voidaan ylläpitää suuri määrä palomuureja yhdestä paikasta. Keskitetyssä hallinnassa nähdään kerralla kaikki palomuurit. Toimenpiteitä voidaan tehdä kerralla useaan palomuuriin tarvitsematta kirjautua erikseen yksittäiseen palomuuriin. Keskitetyllä hallinnalla säästetään aikaa ja kustannuksia.

Tämän opinnäytetyön tavoitteena on suunnitella ja pystyttää kohdeyritykselle keskitetty palomuurihallinta virtuaalipalvelimelle, jonka avulla hallitaan yrityksen asiakaspalomuureja. Tutkimusongelmana on selvittää, miten nykyiset erilliset hallintajärjestelmät saadaan yhteen suurempaan kokonaisuuteen. Keskitettynä hallintajärjestelmänä käytetään Cisco Security Manager -ohjelmistoa, joka tukee laajaa valikoimaa Ciscon tietoturvalaitteita.

1.2 Kohdeyrityksen esittely

Opinnäytetyö tehdään toimeksiantona valtakunnalliselle tietoliikennekonserni DNA Oy:lle. Yhtiö on syntynyt vuonna 1999, kun Finnet-ryhmän alueelliset puhelinyhtiöt perustivat matkapuhelinoperaattori DNA Finland Oy:n. DNA-liittymien myynti alkoi helmikuussa 2001. Nykyinen DNA Oy aloitti toimintansa 1.7.2007, kun emoyhtiö Finnet Oy:n ja kuuden puhelinyhtiön liiketoiminnot yhdistettiin. Matkaviestinliiketoiminnan ohelle tuli vahva kiinteän verkon liiketoiminta, joka sisältää puheen, datan, kaapeli-tv:n ja turvallisuuspalvelut. (DNA Oy 2013a.)

DNA Oy on laajentunut vuosien saatossa. Vuonna 2010 DNA osti Sanomalta Welhon liiketoiminnan. Welho on vahva toimija pääkaupunkiseudun kiinteässä verkossa. DNA on johtava kiinteän verkon toimija Oulun, Lahden, Turun, Porin ja Kuopion talousalueilla. Vuonna 2011 DNA osti tietoliikenne- ja tietoturvapalveluja tarjoavan Forte Netservices Oy:n, jonka palveluja käytetään 60 maassa. (DNA Oy 2013a.)

DNA Oy:n suurimmat omistajat 31.12.2012 ovat Finda Oy 32,56 %, Oulu ICT Oy 22,17 %, PHP Holding Oy 19,75 % ja KPY Sijoitus Oy 12,97 %. KPY Sijoitus Oy on ilmoittanut myyvänsä omistamansa osuudet Finda Oy:lle ja PHP Holding Oy:lle. Kaupan voimaantulon jälkeen Finda Oy:n omistus nousee 39,05 prosenttiin ja PHP Holding Oy:n nousee toiseksi suurimmaksi omistajaksi 26,24 prosentin omistuksella. (DNA Oy 2013c.) Yhtiön liikevaihto vuonna 2012 oli 769,2 miljoonaa euroa. Vuoden 2012 lopussa liittymämäärä oli 3 455 000 ja henkilöstöä 1427 (DNA Oy 2013b).

2 VERKKOJEN TIETOTURVA

2.1 Tietoturvateknologioita

Verkon tietoturvaa voidaan suunnitella monella eri tavalla. Tässä luvussa käydään läpi yleisimpiä suunnittelun periaatteita ja teknologioita.

Internet-liikenne käyttää TCP/IP-protokollaan, jossa data lähetetään pienissä osissa paketteina. Internetin alkuaikoina käytettiin yleisesti pakettisuodatusta. Nykyään yleisin toteutus perustuu verkon reunoilla olevien reitittimien pääsylistoihin. Pakettisuodatuksessa tutkitaan paketin sisältöä ja sovelletaan siihen määrättyjä sääntöjä, joiden perusteella paketti sallitaan tai pudotetaan. Ciscon reitittimissä pakettisuodatus perustuu pääsylistoihin (Access Control List eli ACL). ACL-listoja on kahta päätyyppiä. Standardissa pääsylistassa suodatetaan lähdeosoitteen perusteella. Laajennetussa pääsylistassa vertaillaan lähde- ja kohdeosoitteita ja valinnaisesti protokollaa ja porttinumeroa. (Thomas 2005, 89 -90.)

Yhteyssuodatuksessa (SPI) suodatusta tekevä laite, yleensä palomuuri, tarkkailee lähteviä paketteja. Kun lähtevä yhteys havaitaan, lisätään siitä tieto tauluun. Myöhemmin paketteja vastaanotettaessa verrataan niitä taulussa oleviin tietoihin. Jos paketit kuuluvat olemassa oleviin, kirjattuihin yhteyksiin, ne sallitaan. (Thomas 2005, 97.)

Sisältösuodattimilla voidaan suodattaa monia asioita. Yleisimpiä ovat pornografisen tai laittoman aineiston, roskapostin, virusten ja hyökkäyssivustojen suodattaminen. Sisällönsuodatus käyttää sääntöinään terminologia-, sana- tai fraasikirjastoa tai tietokantaa. Suodatusratkaisut voidaan jakaa kahteen pääluokkaan. Ne ovat asiakaspohjainen ja palvelinpohjainen suodatus. Asiakaspohjaisessa ratkaisussa yksittäisiin tietokoneisiin asennetaan ohjelma, joka tarkistaa sisällön ja suodattaa sen annettujen sääntöjen mukaan.

Palvelinpohjaisessa suodatuksessa sisällön suodatus tapahtuu palvelimella. Roskapostin suodatus on yleinen esimerkki tällaisesta suodatuksesta, sillä kaikki sähköpostit tulevat keskitettyyn palvelimeen, joten se on looginen paikka suodatukselle. (Thomas 2005, 108 - 111.)

AAA-protokollan kirjaimet tulevat sanoista Authentication (Todennus), Authorization (Valtuutus) ja Accounting (Tilastointi). Todennuksen tarkoitus on tunnistaa käyttäjä esimerkiksi verkkolaitteen käyttöoikeuden omaavaksi käyttäjäksi. Tunnustus tapahtuu esimerkiksi käyttäjätunnus-salasana-yhdistelmällä. Todennuksen jälkeen valtuutuksella varmistetaan käyttäjän oikeus palveluihin. Valtuutuksen avulla voidaan sallia tai kieltää tietyt palvelut käyttäjältä. Tilastoinnin avulla käyttäjästä kerätään tilastotietoja. Esimerkiksi käyttäjän suorittamista toiminnoista jää jäljet kellonaikoineen ja päivämäärineen. Kun AAA on konfiguroitu, voidaan sen kanssa käyttää ulkopuolisia turvapalvelimia, kuten RADIUS ja TACACS+. (Thomas 2005, 115 - 117.)

2.2 Palomuuri

Palomuuri on ohjelmisto- tai rautapohjainen turvajärjestelmä, joka kontrolloi verkkoliikennettä analysoimalla paketteja ja päättää tehtyjen sääntöjen perusteella sallitaanko paketit vai ei. Palomuuri luo suojan turvallisen sisäverkon ja internetin välille. Pakettisuodatuksen lisäksi monet palomuurit pystyvät myös tekemään reititystä ja osoitteenmuunnosta (Network Address Translation, NAT). (Wikipedia 2013a.)

Osoitteenmuunnosta ruvettiin tarvitsemaan kun IPv4 -osoiteavaruus, teoreettisesti 2^{32} osoitetta, rupesi internetin räjähdysmäisen kasvun takia olemaan riittämätön. Tämän johdosta osoitelohkoja varattiin yksityisiä verkkoja varten. Nämä lohkot ovat seuraavat:

- 10.0.0.0 – 10.255.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 192.168.255.255

Yksityiset verkot eivät reitity internetissä. Yksityisten osoitteiden avulla kaikille laitteille riittää sisäverkossa IP-osoite. Liikennöidessä ulospäin internettiin palomuuri tekee osoitteenmuunnoksen yksityisestä osoitteesta julkiseen osoitteeseen. (Thomas 2005, 99 - 101.)

Käytössä on useita NAT-tyyppejä:

- Staattinen NAT, jossa sisäverkon yksityinen IP-osoite muunnetaan aina samaan julkiseen IP-osoitteeseen.

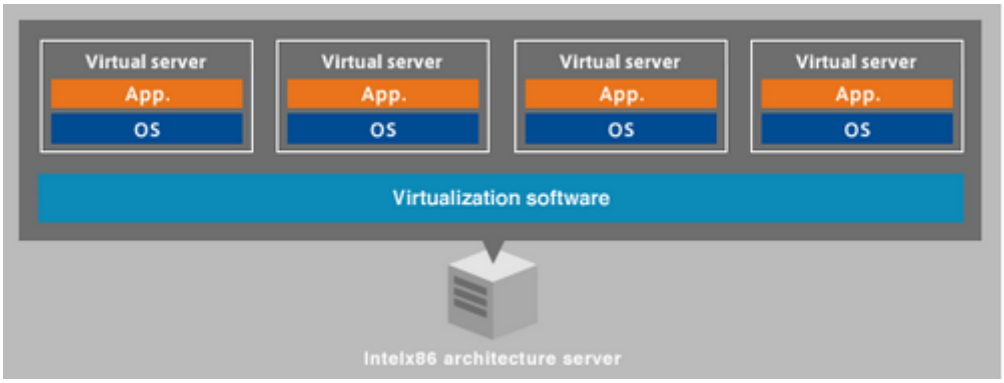
- Dynaaminen NAT, jossa sisäverkon osoitteet muutetaan johonkin poolissa olevaan julkiseen. Tässä tyypissä on mahdollista, että osoitteet loppuuvat, jos sisäverkon osoitteita on enemmän kuin julkisia osoitteita.

- Port Address Translation (PAT). PAT on yksi muoto dynaamisesta NAT-muunnoksesta. PAT sallii monen yksityisen IP-osoitteen muunnoksen yhdeksi julkiseksi IP-osoitteeksi. Tämän on mahdollista, koska PAT tekee osoitteen muunnoksen lisäksi porttimuunnoksen. Muunnoksista pidetään kirjaa, jotta paluuliikenne pystytään ohjaaamaan lähettäjälle. Julkisten osoitteiden säästämisen lisäksi NAT lisää verkon tietoturvaa, sillä NAT:n käyttö hankaloittaa hyökkäyskohteen verkkotopologian ja yhteyksien määrittelemistä, verkossa olevien järjestelmien lukumäärän selvittämistä sekä laitteiden tyypin ja käyttöjärjestelmän selvittämistä. (Thomas 2005. 102 - 103.)

3 PALVELINVIRTUALISOINTI

3.1 Virtualisoinnin hyödyt ja haitat

Palvelinvirtualisoinnissa yksi fyysinen palvelin jaetaan moneksi pienemmäksi virtuaalipalvelimeksi (kuvio 1). Virtualisoinnista hyötyy monella tavalla. Virtuaalipalvelit ovat erillään toisista. Niissä voidaan jokaisessa käyttää omaa käyttöjärjestelmää ja omia sovelluksia eikä yhden virtuaalipalvelin toiminta vaikuta muihin. Virtualisoinnin avulla saadaan resurssit käytettyä tehokkaaamin, sillä normaalisti palvelimien käyttöasteet ovat pieniä. Yhdistämällä monta virtuaalipalvelinta samalle fyysiselle palvelimelle säästetään käyttökustannuksissa, koska käytössä on vähemmän fyysisiä laitteita. (Webopedia 2013.)



KUVIO 1. Palvelinvirtualisointi (NEC 2012)

Virtualisoinnissa on olemassa omat ongelmansa. Yksi suuremmista haittapuolista on yhden pisteen vikaantuminen (Single point of failure). Palvelinvirtualisoinnissa tämä tarkoittaa sitä, että jos fyysinen palvelin tai sen virtualisointiohjelma kaatuu, kaataa se samalla kaikki siihen luodut virtuaalipalvelimet. Tämä kuulostaa vakavammalta kuin se todellisuudessa on. Redundanttikapasiteetilla ja säännöllisellä varmuuskopioinnilla saadaan riski torjuttua. (Georgieva 2013.)

Virtualisointi vaatii tehokkaan koneen. Jos palvelimessa, jonka resurssit jaetaan virtuaalikoneille, ei sisällä tarpeeksi RAM-muistia tai CPU-tehoa ei ole tarpeeksi, saattaa se vaikuttaa virtuaalikoneiden suorituskykyyn. (Georgieva 2013.)

Kaikki sovellukset eivät välttämättä toimi virtualisoituna tai niiden suorituskyky voi heiketä virtualisoinnissa. Tietokannat, joiden suorituskyvyn tiedetään voivan heikentyä virtualisoinnissa, ovat yleisin esimerkki. Tietokannat suorittavat usein levyoperaatioita. Jos levylle kirjoittamisessa tai levyltä lukemisessa on viivettä virtualisoinnin takia, se voi rampauttaa sovelluksen käyttökelvottomaksi. (Georgieva 2013.)

3.2 VMware ESX ja ESXi

VMware ESX ja ESXi ovat hypervisoreita eli ohjelmia, jotka jakavat yhden fyysisen palvelimen laskenta-, muisti-, kovalevy- ja verkkoresurssit monille virtuaalikoneille. VMware ESX ja ESXi ovat markkinoiden eniten käytettyjä hypervisoreita. VMware ESX ja VMware ESXi ovat niin sanottuja bare-metal arkkitehtuureja. Ne voidaan asentaa suoraan palvelimelle ilman että alustana tarvitsee olla käyttöjärjestelmää. (VMware, Inc. 2009.)

Ero VMware ESX:n ja ESXi:n välillä on arkkitehtuurissa ja VMwaren ESXi:n operatiivisessa hallinnassa. VMware ESX sisältää Linux-käyttöjärjestelmän nimeltä service console. Service consolen avulla suoritetaan jotkut hallintafunktiot, kuten skriptien ajaminen, kolmannen osapuolen agenttien asennus raudan monitorointia varten, varmuuskopiointi ja järjestelmän hallinta. VMwave ESXi:stä on poistettu service console, ja se on korvattu etäkomentorivikehote-käyttöliitymällä. Komentorivihallinnan lisäksi VMware ESX:n ja ESXi:n hallinta onnistuu myös VMware vSphere Client- tai VMware vCenter Server -ohjelmilla. (VMware, Inc. 2009.)

3.3 Hyper-V

Hyper-V on Microsoftin vastine VMwaren virtualisointiohjelmille. Hyper-V tuli alun perin Windows 2008 Serverin mukana. Hyper-V tarvitsee isäntäkäyttöjärjestelmän, jonka päällä hypervisor tekee virtualisoinnin. Myöhemmin Hyper-V:stä on tehty standalone-versio eli itsenäisesti toimiva versio nimeltään Hyper-V Server, joka ei vaadi isäntäkäyttöjärjestelmää. (Wikipedia 2013c.)

Hyper-V-arkkitehtuurissa virtualikoneet eristetään osioinnilla. Jokainen Hyper-V instanssi tarvitsee vähintään yhden vanhempiosion, jossa ajetaan tuettu Windows Server -palvelin. Vanhempiosio puolestaan luo lapsiosiot, joissa ajetaan vieraskäyttöjärjestelmät. (Wikipedia 2013c.)

Hyper-V tukee lähes kaikkia Windows-käyttöjärjestelmiä Windows XP:stä lähtien. Poikkeuksina ovat Home Editionit, jotka eivät toimi virtuaalisina. Myös joitakin Linux-distroja on tuettu, kuten Red Hat Enterprise Linuiax ja CentOsia. (Wikipedia 2013c.)

4 CISCO SECURITY MANAGER JA JUNIPER NETWORKS NETWORK AND SECURITY MANAGER

4.1 Cisco Security Manager

Cisco Security Manager (CSM) on kokonaisvaltainen hallintaratkaisu, joka tarjoaa keskitetyn hallinnan, monitoroinnin ja raportoinnin monille Ciscon tietoturvatuotteille. Tuettuja Ciscon laitteita ovat muun muassa seuraavat:

- Cisco PIX -palomuurit
- Cisco ASA -palomuurit
- Cisco Integrated Services Router (sisältää 800, 1800, 2800 ja 3800 sarjat)
- Cisco Integrated Services Router G2 (sisältää 1900, 2900 ja 3900 sarjat)
- Cisco Firewall Services Modules (FWSM-moduulit)
- Cisco Intrusion Prevension System (IPS) laitteet ja palvelumoduulit.

Lista Cisco Security Managerin tukemista laitteista liitteessä 1.
(Cisco 2013a).

Cisco Security Managerin ensisijaiset hyödyt ovat (Cisco 2013e):

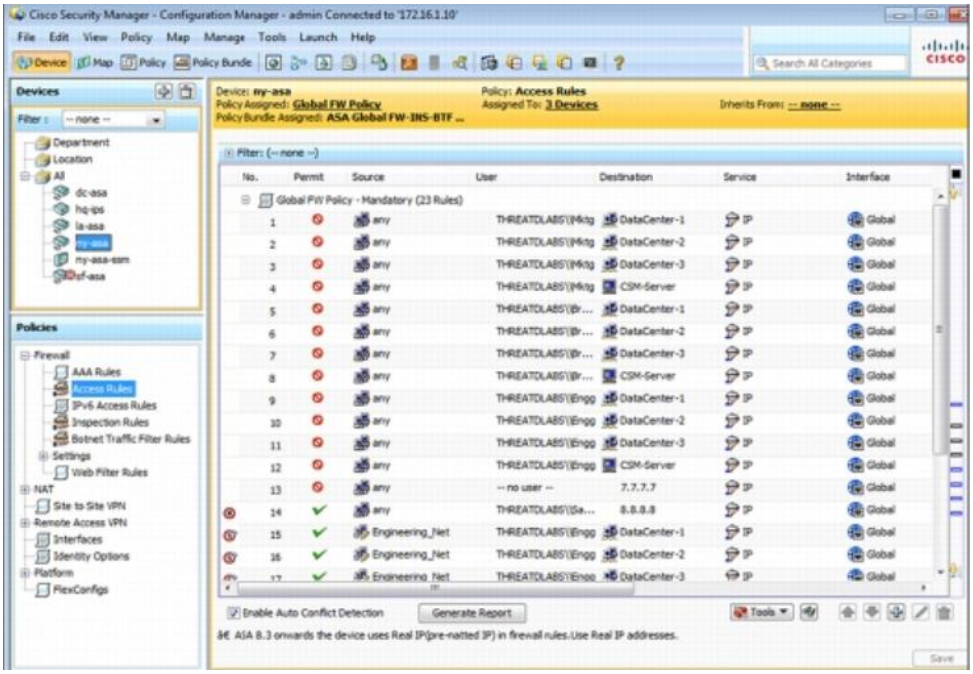
- Skaalautuva verkonhallinta. Soveltuu sekä pienille että suurille yrityksille, joilla tuhansia laitteita verkossa. Säännöt ja asetukset voi osoittaa yksittäiselle laitteelle, ryhmälle tai kaikille verkon laitteille.
- Useiden tietoturvateknologioiden provisiointi. Hallitsee VPN:n, palomuurin, IPS:n ja palvelumoduulit.
- Uudelleenkäytettävät objektit. Uudelleen käytetään kerran luotuja objekteja, jotka kuvaavat esimerkiksi verkko-osoitteita, sääntöjä ja asetuksia sen sijaan, että kirjoitetaan manuaalisesti.
- Laitteiden ryhmittäminen. Laitteet voi ryhmittää kuvaamaan organisaation rakennetta. Ryhmän laitteita pystyy hallitsemaan samanaikaisesti.

- Yhtenäinen käyttöliittymä yleisiin palomuuritoimintoihin. Yksi sääntötaulu kaikille alustoille (reitittimet, PIX, ASA, FWSM).

4.1.1 Cisco Security Managerin ohjelmat

Cisco Security Manager -ohjelmisto sisältää useita työkaluja. Itse CSM-palvelinta hallitaan selainpohjaisella käyttöliittymällä. Palvelinhallinnassa suoritetaan muun muassa käyttäjätilien hallinta, todennustavan valinta ja valitaan varmuuskopionnin asetukset. (Cisco 2013e.) Auto Update Serverin (AUS) avulla hallinnoidaan Ciscon PIX- ja ASA-palomuurien päivitys (Cisco 2013c).

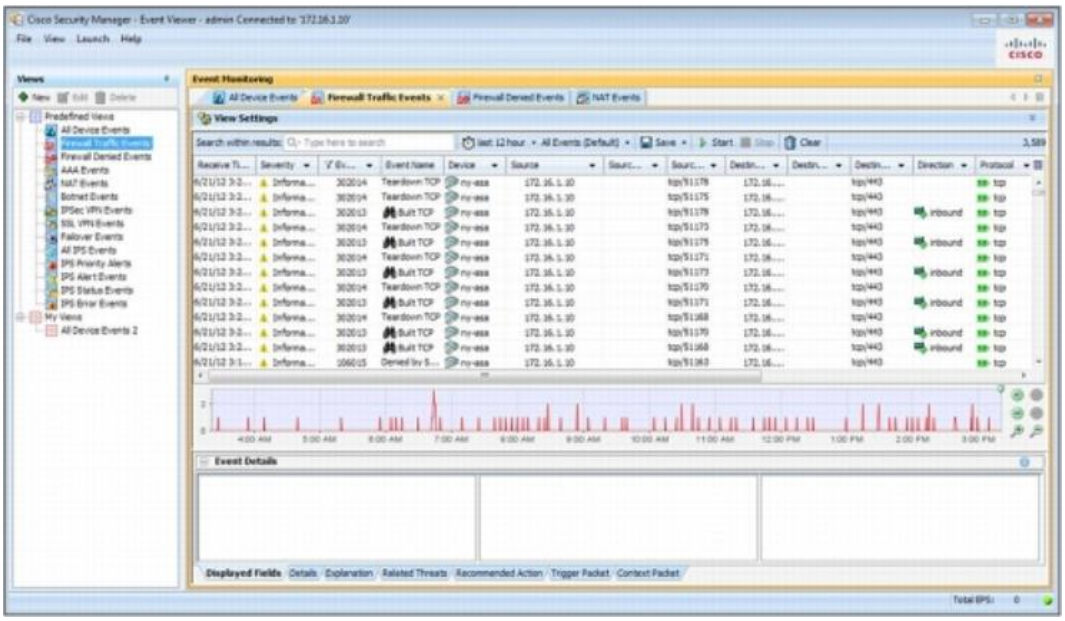
Laitteiden hallintaan ja konfiguroimiseen käytetään erillistä Cisco Security Manager Client -asiakasohjelmaa. CSM Client sisältää sulautetun ja täysin eristetyn Java-version. Se ei sekaannu selaimen asetuksiin eikä muihin Java-pohjaisiin ohjelmiin (Cisco 2013d). Asiakasohjelma sisältää useita osia.



KUVIO 2. Configuration Managerin näkymä (Cisco 2013a)

Configuration Managerin käyttöliittymä (kuvio 2) on selkeä ja helppokäyttöinen. Vasemmassa ylänurkassa on laitelista. Listan alapuolella on laitteen asetusvalikko. Keskellä nähdään laitteelle tehdyt määritykset, kuten pääsylistan säännöt. (Cisco 2013e.)

Event Viewerilla näkee ASA-, FWSM- ja IPS-laitteiden realiaikaiset ja historialliset tapahtumat (kuvio 3). Event Viewerin avulla voi suorittaa nopeasti tapahtuma-analyysin ja vianselvityksen. Filtteröinti ja hakutoiminto helpottaa mielenkiintoisten tapahtumien löytämistä. Event Viewerin ja Configuration Managerin välillä toimii linkitys. Esimerkiksi jos lokissa näkyy, että jonkin yhteys on estynyt tietyn pääsylistan säännön takia, pääsee linkityksen kautta suoraan siihen sääntöön Configuration Managerissa. (Cisco 2013e)



KUVIO 3. Event Viewerin näkymä (Cisco 2013a)

Report Manager luo yksityiskohtaisia raportteja ASA-, VPN- ja IPS-laitteista. Raportoitavat laitteet täytyy olla valittu tarkkailuun Event Viewerissä. Raportointi FWSM-moduuleista ei ole tuettu, vaikka FWSM-moduulit toimivat Event Viewerissa. Raportit voivat sisältää esimerkiksi yleisimmät hyökkäykset tai suurimmat kaistankäyttäjät. Valittavana on valmiita raporttipohjia tai ylläpitäjän määrittämiä raportteja, jotka täyttävät tietyt tarpeet. Raportin luomisen voi automatisoida tapahtuvan tiettyn aikaan ja lähetettäväksi tiettyyn sähköpostiosoitteeseen. (Cisco 2013e).

4.1.2 Lisenssit

Cisco Security Managerin käyttäminen vaatii lisenssin. Ilman lisenssiä ohjelmistoa voi käyttää vain 90 päivän ajan kokeiluversiona. Kokeiluversio toimii kuin Professional-lisenssi, mutta laitteiden määrä on rajoitettu 50 kappaleeseen. Cisco Security Managerissa voidaan käyttää kolmen tyyppisiä lisenssejä. Ne ovat Professional-, Standard- sekä Upgrade-lisenssit. Taulukossa 1 nähdään Professional-lisenssin ja Standard-lisenssin erot. (Cisco 2013d).

Add-on-lisenssejä (lisälisenssejä) ei voi käyttää Standard-lisenssin kanssa eikä myöskään kokeiluversiossa. Standard-lisenssissä on lisäksi rajatumpi laitteistotuki kuin Professional-lisenssissä. Standard-lisenssin voi päivittää Professional-lisenssiksi. CSM-ohjelmiston versiopäivitys vaatii Upgrade -lisenssin kun päivitetään CSM 3.x -versiosta CSM 4.x -versioon. Pääversion sisäiset päivitykset eivät vaadi lisenssin päivitystä. Lisenssien kuluvat niin, että Cisco Security Manager käyttää yhden lisenssin. Kukin CSM:n laiteinventaarioon lisätty fyysinen laite, turvallisuuskonteksti tai virtuaalinen sensori syö yhden lisenssin.
(Cisco 2013d.)

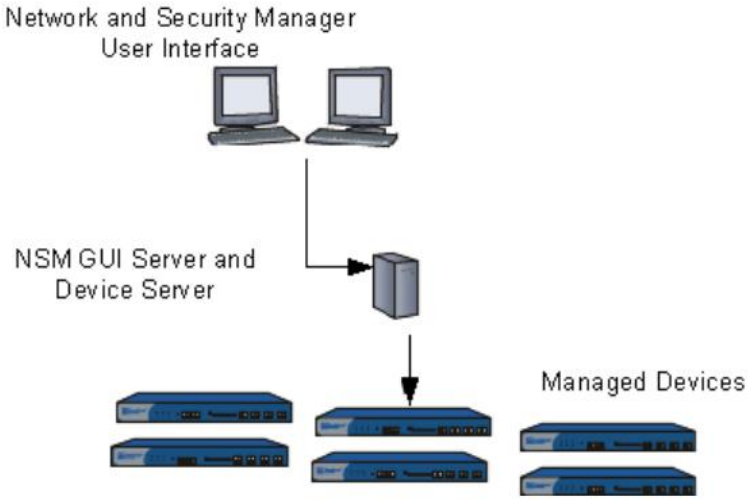
TAULUKKO 1. Lisenssien erot (Cisco 2013d)

Feature	Supported in Professional?	Supported in Standard?
Support of incremental ("add-on") device license packages in increments of 50, 100, and 250 devices	Yes	No
Support for the management of Cisco Catalyst 6500 and 7600 Series switches and associated services modules	Yes	No
Support for the management of firewall service modules	Yes	No
Support for temporary licenses (licenses with an expiration date)	Yes	No (only permanent licenses are supported)

4.2 Juniper Networks Network and Security Manager

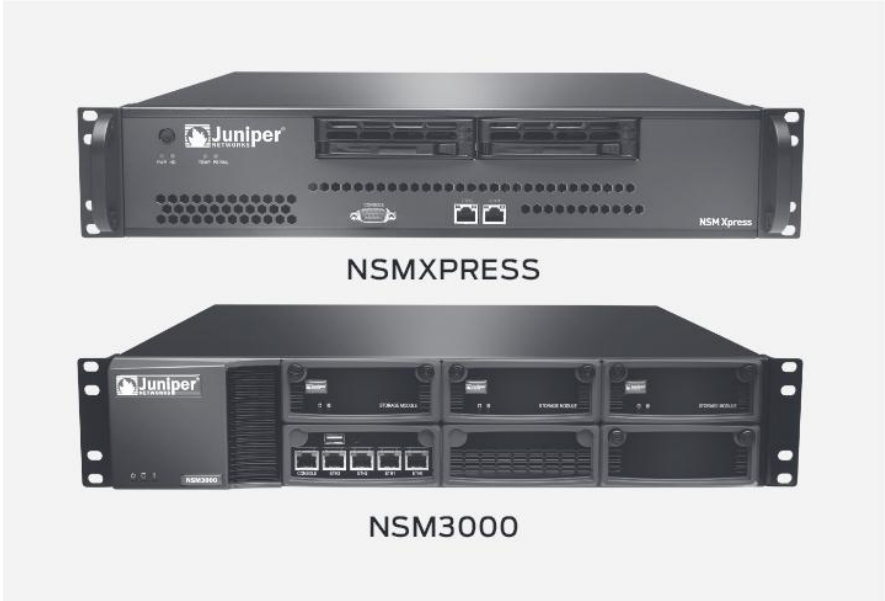
Network and Security Manager (NSM) on Juniper Networksin hallintaratkaisu valmistajan omille reitittimille, kytkimille, palomuurille, VPN:lle ja IDS-laitteille. NSM on skaalautuva ja joustava. Ratkaisu sopii niin yrityksen sivukonttoriin kuin suureen datakeskukseen. NSM voidaan toteuttaa joko ohjelmistopohjaisena palvelimelle tai käyttää dedikoitua laitetta. NSM tarjoaa keskitetyn hallinnan lisäksi muun muassa Log Viewerin realiaikaiseen tarkkailuun ja Report Managerin raportointiin. (Juniper 2013c.)

NSM:n arkkitehtuuri koostuu laitepalvelimesta, GUI-palvelimesta ja user interface (UI) -käyttäjäliittymästä (kuvio 4). Joustavuuden ja suorituskyvyn ylläpitämiseksi laitteiden vuorovaikutuksen ja lokivarastoinnin hoitaa laitepalvelin. Kaikki konfigurointi-informaatio sijaitsee GUI-palvelimella. Kustannustehokkaassa ja yksinkertaisessa ratkaisussa laitehallinta ja GUI-hallinta voivat olla samalla palvelimella. Suorituskykyisessä ja joustavassa ratkaisussa ne ovat eri palvelimilla. UI-käyttäjäliittymä toimii pääsypisteenä toimintoihin molemmissa toteutuksissa. (Juniper 2013b.)



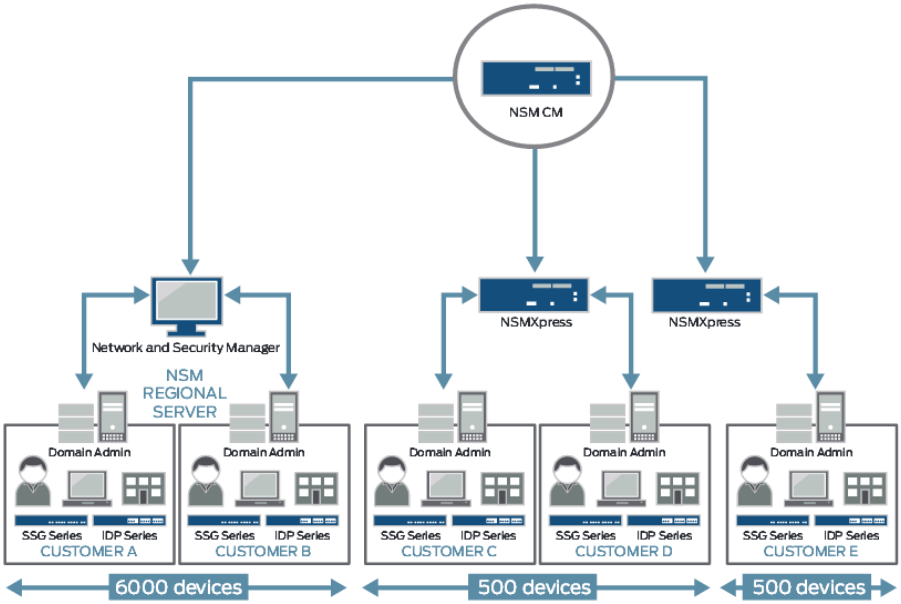
KUVIO 4. Network and Security Managerin arkkitehtuuri (Juniper 2013b)

Dedikoituina laitteina Juniper tarjoaa NSMXpress ja NSM3000 (kuvio 5). Dedikoitujen laitteiden etuina ovat kovennettu käyttöjärjestelmä, selainpohjainen hallinta, tietokannan varmuuskopiointi ja roolitus eli laite voi toimia alueellisena palvelimena tai keskusmanagerina (Juniper 2013a). Käyttöjärjestelmän kovetus tarkoittaa sitä, että se on vain tiettyä tarkoitusta varten. Tarpeettomat ohjelmat, palvelut ja tietoliikenneportit on suljettu tai poistettu. (Wikipedia 2013b.)



KUVIO 5. Dedikoidut NSM -laitteet (Juniper 2013a)

NSMXpress on tarkoitettu pienille ja keskisuurille yrityksille. Sen kapasiteetti riittää 500 laitteen hallintaan. NSM3000 soveltuu suurille yrityksille. Sen kapasiteetti skaalautuu 1500 laitteeseen. Yhdessä NSM Central Managerin kanssa voidaan rakentaa keskitetty hallinta, joka skaalautuu jopa 6000 laitteelle (kuvio 6). (Juniper 2013a.)



KUVIO 6. Keskitetty NSM-hallintajärjestelmä (Juniper 2013b)

4.3 CSM ja NSM vertailu

CSM ja NSM ovat ominaisuuksilta hyvin samankaltaisia. Kummallakin ohjelmistolla hallitaan laitevalmistajan omia tuotteita. Yhteisiä toimintoja ovat keskitetty laitehallinta, monitorointi ja raportointi. Suurin ero on järjestelmävaatimuksissa. CSM-palvelinohjelmisto vaatii käyttöjärjestelmäksi Windows Server -palvelimen. NSM-palvelin puolestaan vaatii Solaris 10:n tai Red Hat Enterprise Linuxin.

Virtualisoinnin puolella CSM tukee virallisesti VMware ESX- ja ESXi-ohjelmia. Dokumentoinnin mukaan NSM ei tue virtualisointia eikä sitä suositella. Rautavaatimukset ovat NSM:lla paljon maltillisemmat kuin CSM:lla (taulukko 2). (Juniper 2013b.)

TAULUKKO 2. CSM:n ja NSM:n järjestelmävaatimukset (Cisco 2013d; Juniper 2013b)

Komponentti	CSM 4.4	NSM 2012.2
CPU	Intel Quadcore Xeon 5500 sarja tai parempi	Sun Microsystems UltraSPARC III (Cu) 1,2 GHz tai parempi
RAM	16 Gt	4 Gt
Kovalevy	Suositus 100 Gt	Suositus 80 Gt
Virtuaalimuisti	24 Gt	8 Gt

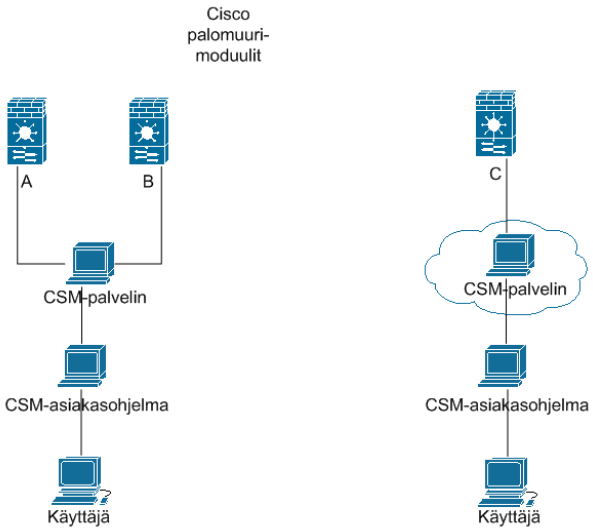
5 KESKITETYN HALLINTAPALVELIMEN PYSTYTTÄMINEN

5.1 Toteutuksen vaatimukset ja tavoitteet

Opinnäytetyön tavoitteena oli päivittää kohdeyrityksen DNA Oy:n nykyiset palomuurien hallintajärjestelmät ja yhdistää ne yhdeksi kokonaisuudeksi. Yrityksen nykyisessä toteutuksessa yksi hallintajärjestelmä oli tehty fyysiselle Windows Server -palvelimelle ja toinen hallintajärjestelmä oli tehty virtuaaliseen Windows Server -palvelimeen. Molemmissa hallintajärjestelmissä käytettiin CSM 3.x -ohjelmistoa (Cisco Security Manager). Vaatimuksena oli päästä eroon fyysisestä palvelimesta, sillä sen ylläpitäminen oli kallista, koska laiterikon varalta piti varastossa olla varalaitteet.

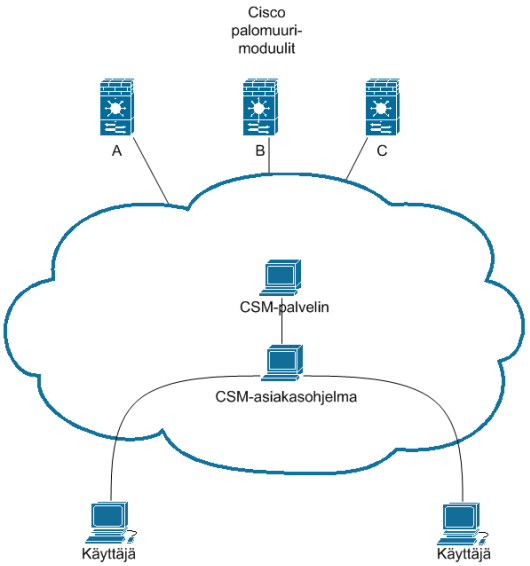
Parhaaksi vaihtoehdoksi katsottiin virtuaalipalvelimeen siirtymistä, koska DNA:lla oli jo olemassa edellytykset virtualisointiin. Uudelle virtuaalipalvelimelle tarvittiin vain CSM-ohjelmiston mukaisten järjestelmävaatimusten allokointi. Virtualisoinnin lisäksi selvitettiin, mitä CSM-ohjelmiston päivitys vaatii.

Kuviossa 7 nähdään nykyinen toteutus. Yllälaidassa ovat Cisco palomuurimoduulit A, B ja C, joissa asiakaspalomuurit sijaitsivat. Nykyisessä toteuksessa oli kaksi erillistä hallintajärjestelmää, jotka eivät olleet yhteydessä toisiinsa. Palomuurimoduuleita A ja B hallittiin fyysiseltä CSM-palvelimelta. Kun haluttiin tehdä muutoksia palomuurimoduuleissa A tai B olevaan asiakaspalomuuriin, käyttäjä otti yhteyden vasemmanpuoliseen CSM-asiakasohjelmaan. Käyttäjän tekemät muutokset ajettiin palomuurimoduuleihin A ja B. Palomuurimoduulia C hallittiin virtuaaliselta CSM-palvelimelta. Kyseistä palvelinta hallittiin oikeanpuolisen CSM-asiakasohjelman kautta.



KUVIO 7. Nykyinen palomuurihallintajärjestelmien toteutus

Kuviossa 8 nähdään tavoitetila, johon opinnäytetyössä pyrittiin. Palomuurimoduulit pysyivät samoissa paikoissa. Kuvion keskellä oleva pilvi kuvaa virtuaaliympäristöä. Pilven sisällä oleva CSM-palvelin ja CSM-asiakasohjelma ovat virtuaalisia. Tavoitetilassa oli yksi CSM-palvelin, jonka kautta hallittiin kaikkia palomuurimoduuleja. Käyttäjät pääsivät tekemään muutoksia kaikkiin kolmeen palomuurimoduuliin yhdestä paikasta.



KUVIO 8. Palomuurihallintajärjestelmän tavoitetila

5.2 Cisco Security Manager -palvelin

5.2.1 Virtuaalisen Windows -palvelimen asennus

CSM-palvelinohjelmiston versioksi valittiin viimeisin versio 4.4.
CSM-palvelin oli tarkoitus pystyttää virtuaalipalvelimeen, joten aluksi selvitettiin, mitä CSM 4.4 virtualisointi vaati. Asennusohjeessa kerrottiin, että tuettuina olivat virtualisointiohjelmat VMware ESX 4.1, VMware ESXi 4.1, VMware ESXi 5.0 tai ESXi 5.1. DNA:lla oli vaadittava virtualisointiohjelma.

CSM-ohjelmisto asennettiin suosituksen mukaan Windows 2008 R2 Enterprise Server SP1 - 64bit -virtuaalipalvelimelle. Palvelin täyttää CSM 4.4:n vaatimukset (taulukko 3).

TAULUKKO 3. CSM 4.4 vaatimukset ja suositukset (Cisco 2013d)

Käyttöjärjestelmä OS	Suositus: Windows 2008 R2 Enterprise Server SP1 - 64bit Tukee myös: Windows Server 2008 Enterprise (Service Pack 2) 64bit Englanti ja japani ovat ainoat tuetut kielet.
Prosessori	Intel Quadcore Xeon 5500 sarja tai parempi.
Muisti (RAM)	16 Gt minimi kaikkien ominaisuuksien käytössä. Vähempi muistin määrä vaikuttaa joidenkin ominaisuuksien käyttöön.
Kovalevy	Suositus: 100 Gt käyttöjärjestelmäosiolle. 150 Gt ohjelmistolle (Security Managerille).
IP-osoite	Staattinen IP-osoite. Dynaamiset IP-osoitteet eivät ole tuettuna.

Windows 2008 Server -virtuaalipalvelinta ei asennettu opinnäytetyöntekijän toimesta vaan virtuaalipalvelimen teki yrityksen virtuaalikoneista huolehtinut henkilö taulukossa 3 olevien vaatimusten ja suositusten pohjalta. Virtuaalipalvelimen luonnin aikana annettiin palvelimelle staattinen IP-osoite. DNS-nimipalveluun lisättiin luotu virtuaalipalvelin. DNS:n avulla palvelimelle voitiin antaa helposti muistettava nimi. Palvelimeen päästiin nyt IP-osoitteen lisäksi nimellä. Staattisen IP-osoitteen lisäksi tehtiin Windowsille pääkäyttäjätunnukset. Kun luotu Window 2008 Server -palvelin oli käynnistetty, tarkistettiin, että palvelin toimi ja että sen suorituskyky oli määritysten mukainen. Sen jälkeen palvelimelle sallittiin etäyhteys tuotantopalvelimelta. Kaikki opinnäytetyössä virtuaalipalvelimelle tehdyt toimenpiteet tehtiin etäyhteydellä.

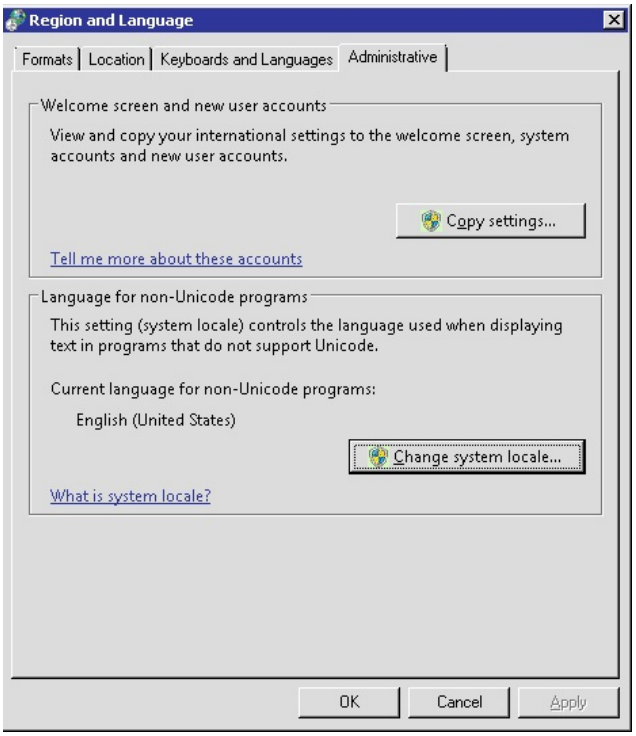
5.2.2 Cisco Security Manager -ohjelmiston asennus

CSM-ohjelmiston asennus Windows-palvelimelle suoritettiin RDP-yhteydellä. Tuotantopalvelimelta, josta oli sallittu etäyhteys palvelimelle, käynnistettiin etäistunto palvelimelle ja kirjauduttiin sisään pääkäyttäjätunnuksilla. CSM-ohjelmistojen asennustiedostot olivat ladattavissa valmistajan internetsivuilta www.cisco.com. Asennustiedoston lataaminen vaati Cisco-tilin, joka sisälsi vaadittavan palvelusopimuksen.

Vaikka palvelimen CSM-ohjelmiston versioksi oli valittu 4.4, aluksi piti asentaa versio CSM 4.2. CSM 4.2 versio piti asentaa sen, jotta vanhan palvelimen tietokannan sai siirrettyä CSM 4.2 versioon, mutta ei suoraan CSM 4.4 versioon. Ciscolta saatiin 3.x to 4.2 -päivityslisenssi ja hieman suuntaa antavaa ohjeistusta. Ciscolla ei ollut tällaisesta päivityksestä ennakkotapausta. Asennuksen jälkeen CSM 4.2 version pystyi päivittämään 4.4 versioon samalla lisenssillä.

CSM 4.2 asennustiedoston koko oli noin 1,33 Gt. CSM-ohjelmiston asennus- ja käyttöohjeiden lataamiseen ei vaadittu Cisco-tiliä. Asennustiedosto ladattiin palvelimen paikalliselle levylle. Asennustiedosto oli pakattu. Sen purkamiseen käytettiin palvelimella ollutta WinZip-työkalua. Purretuista tiedostoista ajettiin asennusohjelma Setup.exe.

Jos palvelimella oli jo olemassa CSM-ohjelmisto, asennus kysyi, haluttiinko ottaa siitä varmuuskopio. Jos Windows-palvelimen sijainti ja kieliasetukset olivat muuta kuin CSM:n vaatimat englanti tai japani, niin asennus keskeytyi virheilmoituksella, jossa pyydettiin laittamaan asetukset kuntoon. Asetukset korjattiin avaamalla Control Panel → Region and Language. Formats-välilehdellä valittiin valikosta English (United States). Location -välilehdellä valittiin sijainniksi United States. Keyboards and Languages -välilehdellä valittiin näppäimistön kieleksi English (United States). Administrative-välilehdellä Language for non-Unicode programs kohtaan valittiin English (United States) (kuvio 9).



KUVIO 9. Palvelimen kieliasetukset

Sijainti- ja kieliasetuksiin tehdyjen muutosten jälkeen päästiin asennuksen seuraavaan vaiheeseen, jossa kysyttiin kohde, mihin ohjelmisto asennetaan. Kohdekansioksi valittiin käyttöjärjestelmästä erillä oleva levyosio.

Seuraavassa vaiheessa kysyttiin, mitkä ohjelmistot haluttiin asentaa. CiscoWorks Common Services 4.0 oli valmiiksi valittuna, eikä sitä voi muuttaa. Valittavana oli Security Manager 4.2 ja AUS (Auto Update Server) 4.2. Asennettaviksi valittiin molemmat. Seuraavaksi kysyttiin lisenssitietoja. Vaihtoehtoina oli antaa polku lisenssitiedostolle tai selata siihen. Jos lisenssitietoja ei halunnut antaa, pystyi myös valitsemaan Evaluation Only, joka sallii 90 päivän kokeilun. Valittiin Evaluation Only.

Seuraavaksi luotiin admin-tunnukselle salasana. Salasanan piti olla vähintään viisi merkkiä pitkä. Lopuksi tuli yhteenveto asennuksesta. Asennus suoritettiin painamalla Install. Asennusprosessi kesti puolisen tuntia. Kun asennus oli valmis, Windows vaati uudelleenkäynnistyksen. CSM-ohjelmisto käynnistyi automaattisesti Windowsin uudelleenkäynnistyksen jälkeen. Windowsin työpöydältä löytyi asennuksen jälkeen Cisco Security Manager -niminen pikakuvake. Pikakuvakkeesta päästiin CSM:n selainhallintaan (kuvio 10). Tunnuksina käytettiin asennusvaiheessa luotuja admin-tunnuksia.

KUVIO 10. Cisco Security Managerin kirjautumisikkuna

5.2.3 Varmuuskopion palauttaminen

Cisco Security Manageriin voitiin palauttaa omasta palvelimesta tai muista Cisco Security Managereista otettu varmuuskopio. Opinnäytetyössä CSM 4.2 palvelimelle palautettiin fyysisestä CSM 3.x palvelimesta otettu varmuuskopio. CSM 3.x palvelimen varmuuskopio sisälsi kaiken tiedon palvelimelta mukaan lukien lisenssit. Varmuuskopion palauttaminen tehtiin Windowsin omalla komentokehotteella. Varoituksena varmuuskopion palauttaminen tyhjentää käytössä olevan CSM-palvelimen tietokannan täydellisesti, joten sitä on käytettävä harkitusti. Varmuuskopion pitää olla paikallisella levyllä.

Komentokehotteessa lopetettiin ensi kaikki CSM -prosessit komennolla:

net stop crmdmgtd

Varmuuskopio palautettiin komennolla:

D:\Progra~1\CSCOpx\bin\perl D:\Progra~1\CSCOpx\bin\restorebackup.pl -d D:\backups

Komennon syntaksi on liitteessä 2. Palautusprosessi kysyi haluttiinko varmasti tehdä palautus. Vastattiin yes eli kyllä. Koska varmuuskopio oli CSM 3.x -palvelimelta, palautusprosessi ilmoitti myös sen, että vanha lisenssi ei toimi uudessa palvelimessa vaan palautuksen jälkeen pitää syöttää uusi lisenssi.

Jos varmuuskopion palautus sujui onnistuneesti, loppuun tuli viesti onnistuneesta palautuksesta. Jos palautus epäonnistui, niin prosessi keskeytyi virheilmoituksella. Palautuksen keskeytyessä tai mennessä virheeseen CSCOpx -kansioon jää backup.LOCK -tiedosto, joka estää uuden palautusprosessin ajamisen. Yksinkertainen ratkaisu tähän oli poistaa backup.LOCK -tiedosto. Tiedoston poistamisen jälkeen varmuuskopion palautusta pystyi ajamaan uudestaan.

Onnistuneen palautuksen jälkeen CSM-prosessit käynnistettiin uudelleen komennolla:

net start crmdmgtd

Opinnäytetyössä onnistuttiin palauttamaan CSM 3.x varmuuskopio CSM 4.2 palvelimelle. Seuraavaksi tarkastettiin tietokannan eheys. Heti aluksi havaittiin CSM-palvelimen hallintanäkymästä että autentikointi moodiksi oli vaihtunut TACACS+, joka oli käytössä CSM 3.x palvelimella. Ennen palautusta moodi oli CiscoWorks Local eli palvelimen paikalliset tunnukset. Asiakaspalomuurien tietokannan eheyden tarkistamiseksi piti asentaa CSM-asiakasohjelmisto. Tietokantaa verrattiin tuotannossa olevan CSM 3.x tietokantaan ja todettiin, että palautus onnistui.

5.3 Cisco Security Manager -asiakasohjelma

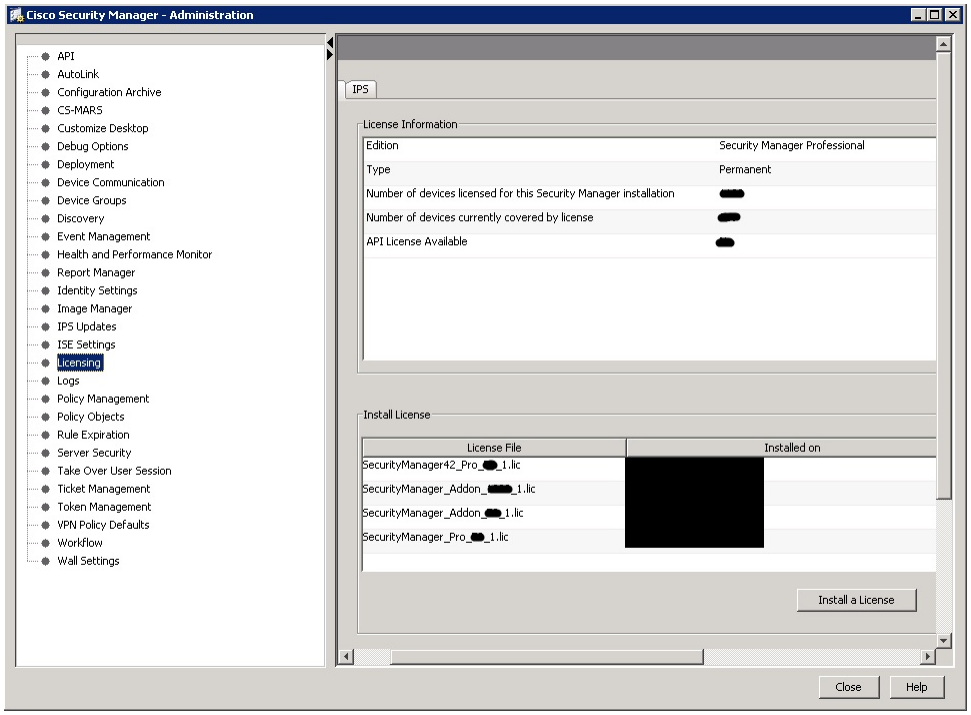
5.3.1 Asiakasohjelman asennus

CSM -asiakasohjelman sai ladattua CSM-palvelimen kautta. Kun CSM-palvelimen hallintaan kirjautui sisään, aukesi näkymä, jossa pystyi valitsemaan asiakasohjelman asennuksen, Auto Update Server tai järjestelmän ylläpito. Valitsemalla asiakasohjelman asennuksen pystyi ajamaan asennustiedoston tai tallentamaan sen kovalevylle. Ciscon suositus oli, että asiakasohjelma ajetaan eri palvelimelta tai työasemalta kuin missä CSM -palvelin on, jotta asiakasohjelma ei kuluttaisi palvelimen resursseja. Tässä vaiheessa asiakasohjelma asennettiin samalle palvelimelle. Käyttöönottovaiheessa olisi tarkoitus ajaa asiakasohjelma toiselta palvelimelta. Asiakasohjelma kysyi asennuksen aikana CSM palvelimen DNS nimeä tai staattista IP-osoitetta ja protokollaa. Annettiin palvelimen nimi ja protokollaksi valittiin HTTPS. Asiakasohjelman käyttäminen vaati, että selaimessa sallittiin ponnahdusikkunat ja Javascript.

5.3.2 Lisenssin lisääminen

Ilman lisenssiä ei pystynyt käyttämään asiakasohjelmaa, sillä heti kun yritettiin yhdistää asiakasohjelmalla CSM-palvelimelle tuli ilmoitus että palvelimella ei ole lisenssiä. Jos tässä vaiheessa ei syöttänyt lisenssiä, ei pääsyt eteenpäin. Tässä vaiheessa syötettiin palvelimelle Ciscolta saatu 3.x to 4.2 -päivityslisenssi. Lisenssin lisäys onnistui ja CSM-asiakasohjelmalla saatiin yhteys CSM -palvelimeen.

Lisenssien hallinta tehtiin asiakasohjelman kautta. Hallintanäkymästä valittiin Tools → Security Manager Administration → Licensing. Lisenssien hallinnassa (kuvio 11) nähtiin palvelimen lisenssitiedot. License Information alta nähtiin lisenssin tyyppi, lisenssien kokonaismäärä sekä käytössä olevien lisenssien määrän. Install License alta nähtiin asennetut lisenssit. Siellä näkyi myös vanha CSM 3.x lisenssi vaikka se ei toimi CSM 4.x palvelimessa. Install a License-painikkeesta pystyi lisäämään uusia lisenssejä.



KUVIO 11. Lisenssien hallinta

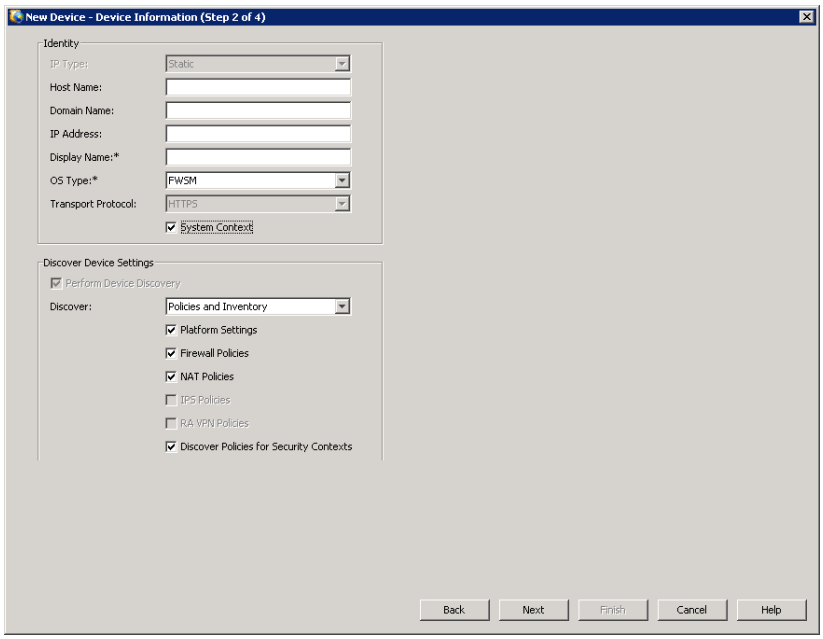
5.3.3 Laitteiden lisääminen inventaarioon

Laitteiden lisääminen inventaarioon tehtiin asiakasohjelman kautta. Tarkoituksena oli aluksi tuoda virtuaalisen CSM 3.x -palvelimen tietokanta CSM 4.2 palvelimelle. Tämä olisi vaatinut virtuaalisen CSM 3.x -palvelimen päivitystä 4.2 versioon, jotta tietokanta olisi ollut yhteensopiva. Tutkittaessa tätä vaihtoehtoa törmättiin CSM 4.2 version julkaisuhuomioissa kohtaan:

CSCtr32994 Device export failing when db restored from another server

Huomio tarkoitti sitä, että jos tietokanta oli palautettu toisesta palvelimesta, laitteita vieminen epäonnistuu. Tämä esti tietokannan tuomisen virtuaaliselta CSM 3.x palvelimelta. Vaihtoehdoksi jäi palomuurimoduulin lisääminen suoraan CSM 4.2 -palvelimelle verkosta. Asiakasohjelman hallinnassa valittiin hiiren oikealla napilla New Device → Add Device From Network.

Seuraavassa vaiheessa (kuvio 12) annettiin palomuurimoduulin nimi ja hallinnan IP-osoite. OS Type-kohtaan valittiin FWSM. System Context kohta valittiin myös, sillä palomuurimoduuli sisälsi useita kontekseja eli asiakaspalomuureja. Discovery -kohtaan valittiin Policies and Inventory. Rastitetaan kaikki mahdolliset valinnat. Näillä asetuksilla lisätty palomuurimoduuli sisältää kaiken tiedon. Yksittäisiä asiakasmuureja ei tarvinnut erikseen lisätä. Palomuurimoduulin lisääminen kesti useita tunteja. Kestoon vaikutti moduulin sisällä olevien asiakaspalomuurien määrä.



KUVIO 12. Uuden laitteen lisääminen verkosta

5.4 CMS-palvelimen päivitys ja testaus

CSM 4.2 palvelin päivitettiin lopuksi uusimpaan 4.4 SP2 versioon. CSM 4.4 asentaminen voitiin tehdä suoraan 4.2 version päälle. Lisenssit ja tietokanta säilyivät päivityksessä. Kun 4.4 versio oli asennettu, siihen päivitettiin SP2. Päivityspaketti ladattiin Ciscon sivuilta. Asennusohjelma tunnisti automaattisesti Windowsilla olleen CSM 4.4 ohjelmiston ja osasi päivittää siihen SP2. Palvelinohjelmiston päivityksen takia piti päivittää myös asiakasohjelma, sillä se vaati toimiakseen saman versionumeron kuin palvelimella oli. Aluksi ladattiin CSM 4.4 hallinnan kautta asiakasohjelman asennustiedosto. Asiakasohjelma 4.4:n asennus menee automaattisesti 4.2 version päälle. Ensimmäisellä kerralla kun ohjelmalla yhdistettiin CSM 4.4 SP2 -palvelimelle, täytyi asiakasohjelma päivittää SP2 versioon. Päivityksen jälkeen päästiin taas hallintaan kiinni.

CSM 4.4 SP2 -palvelimeen tehtiin testausvaiheessa jokaiselle palomuurimoduulille yksi palomuuri. Kun palomuuri luotiin asiakasohjelmassa, se ei ole vielä luotu palomuurimoduuliin. Asiakasohjelmassa valittiin File → Submit and Deploy. Tämä jälkeen päästiin valitsemaan minkä palomuurin muutokset haluttiin ajaa. Ajansäästämiksi kannatti valita ainoastaan palomuurit, joihin oli tehty muutoksia. Ennen muutosten ajamista näytettiin yhteenveto muutoksista mitä oltiin ajamassa. Kun testipalomuurit oli ajettu palomuurimoduuleihin, käytiin moduulien CLI-hallinnassa varmistamassa että testipalomuurit todella olivat ilmestyneet.

Lopuksi testattiin varmuuskopioiden ottamista. Palvelimesta pystyi ottamaan varmuuskopion heti tai tietyin väliajoin. Asetuksissa määritettiin hakemisto, mihin varmuuskopiot tehdään, generaatioiden lukumäärä, kellonaika ja toisto (heti, päivittäin, viikoittain tai kuukausittain). Esimerkiksi jos generaatioiden lukumääräksi asetettiin kaksi ja toistoksi päivittäin, kolmannen päivä varmuuskopio tehtiin ensimmäisen päivän varmuuskopion tilalle. Neljännen päivän varmuuskopio meni toisena päivänä tehdyn varmuuskopion tilalle ja niin edelleen. Generaatioiden määrä kannatti pitää kohtuusena sillä yhden varmuuskopion koko on palomuurien määrästä riippuen noin 1 Gt tai suurempi.

5.5 Toteutuksen onnistumisen arviointi

Opinnäytetyössä onnistuttiin täyttämään työlle asetetut tarpeet ja vaatimukset. Usean hallintajärjestelmän verkosta päästiin tulokseen, jossa on yksi virtuaalipalvelimella oleva hallintapalvelin. Kyseiseltä palvelimelta voitiin tehdä keskitetysti ylläpitotehtäviä kaikkiin asiakaspalomuureihin, jotka olivat palomuurimoduuleissa. Kirjallisen työn tekemisen aikana ei yrityksessä vielä tehty päätöstä opinnäytetyön ottamisesta tuotantokäyttöön. Alustavien keskustelujen perusteella työ tullaan ottamaan käyttöön, sillä vanhoista hallintapalvelimista haluttiin tosissaan eroon.

Opinnäytetyössä ei tarvinnut tehdä yksin kaikkea, sillä osan tarvittavista asioista teki muut yrityksen työntekijät, jotka olivat niistä vastuussa. Näitä asioita olivat lisenssien tilaaminen ja virtuaalipalvelimen luominen. Ne tehtiin kuitenkin opinnäytetyön tekijän antamien vaatimusten pohjalta. Alku- ja testausvaiheessa auttoivat palomuureja ylläpitäneet henkilöt, sillä heillä oli parempi asiantuntemus hallintajärjestelmistä.

Ajanhallinnasta löytyi eniten parannettavaa. Toimeksiannon alussa tehtiin opinnäytetyön tekemiselle aikataulu. Aikataulu petti pahasti monesta syystä. Päälimmäisinä syinä olivat opinnäytetyöntekijän ajankäytön priorisointi ja passiivisuus. Opinäytetyön tekeminen olisi pitänyt priorisoida korkeammalle kuin muiden työtehtävien tekeminen. Aikataulusta olisi pitänyt pitää tiukemmin kiinni ja olla paljon aktiivisempi asioiden eteenpäin viemisessä. Aikataulun pettämiseen vaikutti myös osittain opinnäytetyön tekijästä riippumattomat asiat kuten lisenssien saamisen venyminen.

6 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli pystyttää virtuaalipalvelimelle Cisco Security Manager -ohjelmisto, jonka kautta verkonylläpitäjät pystyvät keskitetysti suorittamaan ylläpitotehtäviä palomuureihin. Uuden järjestelmän oli tarkoitus korvata vanha toteutus, jossa verkossa oli yksi fyysinen ja yksi virtuaalinen palomuurien hallintapalvelin.

Opinnäytetyön teoriaosuudessa pyrittiin kertomaan verkon tietoturvasta, palvelinvirtualisoinnista ja esiteltiin kahden verkkolaitevalmistajan hallintaohjelmistoja: Cisco Security Manager ja Juniper Networks Network and Security Manager. Verkon tietoturvassa käytiin läpi joitakin tietoturvateknologioita, kuten eri pakettisuodatuksen tyyppejä, AAA -protokollaa, palomuurin toimintaa ja NAT-osoitteenmuunnosta. Palvelinvirtualisoinnissa kerrottiin virtualisoinnin hyödyt ja ongelmat. Virtualisointiarkkitehtuureina esiteteltiin kaksi yleisintä käytössä olevaa ohjelmaa: VMware ESX sekä VMware ESXi. Niiden lisäksi kerrottiin hieman kilpailija Microsoftin Hyper-V-arkkitehtuurista. Cisco Security Managerin ja Network and Security Managerin esittelyissä kerrottiin ohjelmistojen käyttötarkoituksista. Lisenssitiedosta kerrottiin miten ne toimivat ja mitkä laitteet syövät lisenssejä.

Käytännön osuudessa suunniteltiin ja pystytettiin virtuaalipalvelin, johon asennettiin käyttöjärjestelmäksi Windows 2008 R2 Enterprise Server SP1. Windowsille asennettiin sen jälkeen CSM 4.2 -ohjelmisto. Vanhan fyysisen CSM-palvelimen tietokanta vietiin CSM 4.2 -palvelimelle tekemällä varmuuskopion palautus. Kun tietokanta oli todettu ehjäksi, päivitettiin CSM 4.2 uusimpaan versioon CSM 4.4 SP2. Lopuksi uutta hallintajärjestelmää testattiin tekemällä testimuureja ja levittämällä muurit moduuleihin. Testaus onnistui hyvin.

Keskitettyjen hallintajärjelmien käyttäminen on nyt ja tulevaisuudessa merkittävässä osassa. Yrityksillä, varsinkin tietoliikennealalla on paljon erilaisia verkkolaitteita. Laitteiden hallinta ja ylläpito vie suurimman osan ylläpitäjän työajasta. Keskitetyllä hallintajärjestelmällä saadaan kustannussäästöjä, kun järjestelmiä on vain yksi. Ylläpitäjien ajankäyttö tehostuu kun yhdestä paikasta pääsee hallitsemaan kaikkia laitteita, eikä tarvitse kirjautua yksittäiseen laitteeseen. Keskitetty hallintajärjestelmä helpottaa myös verkkokuvan hahmottamista, kun samankaltaisia laitteita tai samalla alueella olevat laitteet voidaan hallinnassa laittaa samaan ryhmään ja muutokset voidaan suorittaa kerralla kaikkiin ryhmän laitteisiin.

LÄHTEET

Cisco Systems, Inc. 2013a. Cisco Security Manager 4.4 Data Sheet. Cisco Systems, Inc. [viitattu 11.11.2013]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/data_sheet_c78-727090.html

Cisco Systems, Inc. 2013b. Cisco Security Solutions. Cisco Systems, Inc. [viitattu 17.11.2013]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/brochure_c02-518424.pdf

Cisco Systems, Inc. 2013c. CiscoWorks Auto Update Server Datasheet. Cisco Systems, Inc. [viitattu 11.11.2013]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps3993/product_data_sheet09186a00800e79ca.html

Cisco Systems, Inc. 2013d. Installation Guide for Cisco Security Manager 4.4. Cisco Systems, Inc. [viitattu 10.11.2013]. Saatavissa: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.4/installation/guide/instl.pdf

Cisco Systems, Inc. 2013e. User Guide for Cisco Securit Manager 4.4. Cisco Systems, Inc. [viitattu 17.11.2013]. Saatavissa: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.4/user/guide/CSMUserGuide.pdf

DNA Oy. 2013a. DNA Oy -konsernin historia. DNA Oy [viitattu 9.11.2013]. Saatavissa: https://www.dna.fi/DNAOy/TietoaDNAsta/dnanhistoria/Sivut/Default.aspx

DNA Oy. 2013b. Kasvua ja kehitystä usealla rintamalla. DNA Oy [viitattu 9.11.2013]. Saatavissa: http://annualreporting.dna.fi/2012/vuosi-2012

DNA Oy. 2013c. Omistajat. DNA Oy [viitattu 9.11.2013]. Saatavissa: https://www.dna.fi/DNAOy/TietoaDNAsta/Omistajat/Sivut/Default.aspx

Georgieva, T. 2013. Disadvantages of Virtualization. Suite101 Media [viitattu 11.11.2013]. Saatavissa: http://suite101.com/a/disadvantages-of-virtualization-a170745

Juniper Networks, Inc. 2013a. Network and Security Manager Appliances (NSMXpress and NSM3000). Juniper Networks, Inc [viitattu 17.11.2013]. Saatavissa: http://www.juniper.net/us/en/local/pdf/datasheets/1000204-en.pdf

Juniper Networks, Inc. 2013b. Network and Security Manager Installation Guide. Juniper Networks, Inc [viitattu 17.11.2013]. Saatavissa: http://www.juniper.net/techpubs/software/management/security-manager/nsm2010_2/nsm-admin-guide.pdf

Juniper Networks, Inc. 2013c. Network and Security Manager Overview. Juniper Networks, Inc [viitattu 17.11.2013]. Saatavissa: http://www.juniper.net/us/en/products-services/software/network-management-software/nsm/#overview

NEC. 2012. Server Virtualization. NEC [viitattu 11.11.2013]. Saatavissa: http://www.nec-itplatform.com/-Server-Virtualization#topmenu

Thomas, T. 2005. Verkkojen tietoturva. Helsinki: Edita Prima Oy.

VMware, Inc. 2009. VMware ESX and VMware ESXi. VMware, Inc. [viitattu 11.11.2013]. Saatavilla: http://www.vmware.com/files/pdf/VMware-ESX-and-VMware-ESXi-DS-EN.pdf

Webopedia. 2013. Server virtualization. Webopedia [viitattu 17.11.2013]. Saatavissa: http://www.webopedia.com/TERM/S/server_virtualization.html

Wikipedia. 2013a. Firewall (computing). Wikipedia [viitattu 11.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/Firewall_%28computing%2

Wikipedia. 2013b. Hardening (computing). Wikipedia [viitattu 17.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/Hardening_%28computing%29

Wikipedia. 2013c. HyperV. Wikipedia [viitattu 17.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/HyperV

LIITTEET

LIITE 1

CISCO MANAGERIN TUETUT LAITTEET

Cisco PIX Security Appliances
Cisco ASA 5500 and ASA 5500-X Series Adaptive Security Appliances
Cisco Integrated Services Routers (including 800, 1800, 2800, and 3800 Series) Cisco Integrated Services Routers G2 (including 1900, 2900, and 3900 Series)
Cisco ASR 1000 Series Aggregation Service Routers
Cisco 7600 Series Routers
Cisco 7500 Series Routers
Cisco 7300 Series Routers
Cisco 7200 Series Routers
Cisco 7100 Series Routers
Cisco 3200 Series Routers
Cisco 2600 Series Routers
Cisco Catalyst 6500 Series Firewall Services Modules (FWSMs)
Cisco Catalyst 6500 Series VPN Services Modules (VPN SMs)
Cisco 7600 Series/Catalyst 6500 Series IPsec VPN Shared Port Adapters (VPN SPAs)
Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM-2)
Cisco IPS 4200 Series Sensors
Cisco AIP-SSM for Cisco ASA 5500 Series
Cisco AIP-SSC for Cisco ASA 5500 Series
Cisco IPS AIM for Integrated Services Routers
Cisco IPS Module for Access Routers Network Module - Cisco Intrusion Detection System (NM-CIDS)
Cisco Catalyst 3550, 3560, 3560E, 3750, 3750 Metro, 4500, 4948, and 4948 10 Gigabit Ethernet Switches

LIITE 2

VARMUUSKOPION PALAUTUKSEN SYNTAKSI

*$NMSROOT****bin*****perl** *$NMSROOT****bin*****restorebackup.pl** *[**-t** temporary_directory][**-gen** generationNumber]* ***-d*** *backup_directory [**-h**]*

Jossa,

$NMSROOT - täysi polku Common Services:n asennushakemistoon (oletus on C:\Program Files\CSCOpx).

-t *temporary_directory* - (Valinnainen) Hakemisto tai tiedosto, jossa palautusohjelma säilyttää väliaikaiset tiedostot. Oletuksena hakemisto on *$NMSROOT*\tempBackupData.

-gen *generationNumber* - (Valinnainen) Varmuuskopion generaatio, jonka haluat palauttaa. Oletuksena käytetään viimeisintä. Jos generaatioita on 1-5, 5 on viimeisin.

-d *backup_directory* - Hakemisto, joka sisältää palautettavan varmuuskopion.

-h - (Valinnainen) Antaa apua. Kun käytetään ***-d*** *backup_directory* kanssa näyttää oikean syntaksin ja saatavilla oleva generaatiot.