Opinnäytetyö (AMK)

Tieto- ja viestintätekniikan koulutus

2018

Mikko Hovi

AKTIIVISEN CHECK POINT -PALOMUURIKLUSTERIN YLIHEITTO JA KONESALIN VAIHTO

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikan koulutus

Syksy 2018 | 38 sivua

Mikko Hovi

AKTIIVISEN CHECK POINT -PALOMUURIKLUSTERIN YLIHEITTO JA KONESALIN VAIHTO

Tämän opinnäytetyön tavoitteena oli dokumentoida projekti, jossa asiakasyrityksen vanha Check Point 4200 -palomuuriklusteri oli tarkoitus korvata uudemmilla Check Point 5100 -palomuureilla. Uudet palomuurit oli myös määrä asentaa eri konesaliin kuin missä tuotannossa oleva klusteri oli. 4200-palomuuriklusteri oli määritetty toimimaan High Availability -tilassa, jossa klusterin toinen palomuuri oli aktiivinen laite ja toinen varalaite. Palomuurit olivat aktiivikäytössä ja toimivat asiakkaan pääpalomuureina, eli kaikki asiakkaan tietoliikenne kulki niiden kautta. Opinnäytetyö tehtiin Tietokeskus Finland Oy:n toimeksiannosta.

Yliheiton tarkoituksena oli parantaa verkon toimintavarmuutta ja varautua verkkoliikenteen tulevaan kasvuun. Uudet laitteet olivat vanhoja suorituskykyisempiä, ja ne olivat laitevalmistajan palvelusopimuksen piirissä, mikä toisi lisäturvaa ongelmatilanteissa. Lisäksi tarkoituksena oli optimoida palomuurien hallintatietokanta yliheiton jälkeen poistamalla tarpeettomia sääntöjä sekä muita tietoja. Tällä tavoin saataisiin pienennettyä sisäverkon ja verkkolaitteiden kuormitusta, tehostettua palomuurien toimintaa ja parannettua asiakkaan verkon tietoturvaa.

Yliheiton testaamista varten rakennettiin virtuaalinen testiympäristö, jossa palomuurilaitteita simuloitiin virtuaalikoneiden avulla tuotantoverkoista erillään. Testiympäristön valmistuttua 4200-palomuureista siirrettiin järjestelmäasetukset ja hallintatietokanta ensin virtuaaliympäristöön ja sitten fyysisiin 5100-palomuureihin. Yliheiton valmistelua varten 5100-palomuurit asennettiin konesaliin, ja niiden tiedot tarkistettiin ja mukautettiin uuteen verkkoympäristöön. Kun laitteet oli liitetty hallintaverkkoon, varmistettiin, että palomuureihin on mahdollista ottaa etäyhteys konesaliverkon ulkopuolelta. Lisäksi uusien palomuurien vikasietoisuutta parannettiin muodostamalla 5100-klusterin palomuureista ja räkkikytkimistä Full Mesh -topologian mukainen verkko, joka takaisi liikenteen saumattoman kulun myös mittavammissa vikatilanteissa.

Vaikka projekti jäi kesken ja yliheittoa ei lopulta toteutettu, ei opinnäytetyötä varten käytetty aika kuitenkaan mennyt hukkaan, vaan sekä toimeksiantaja että asiakas saivat hyödyllistä tietoa projektin aikana laaditusta dokumentaatiosta. Lisäksi asiakkaan verkkokuvat sekä muuta asiakasdokumentaatiota päivitettiin, minkä ansiosta tulevien järjestelmänvalvojien ja muiden asiantuntijoiden on helpompaa perehtyä asiakkaan verkkoympäristön ominaispiirteisiin.

ASIASANAT:

palomuurit, Check Point, High Availability -klusterit, klusterointi, yliheitto, tietoturva

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2018 | 38 pages

Mikko Hovi

MIGRATION OF AN ACTIVE CHECK POINT HIGH AVAILABILITY FIREWALL CLUSTER

The aim of this thesis was to provide documentation for a project, in which an outdated Check Point 4200 firewall cluster was to be migrated to another data centre and replaced by Check Point 5100 firewalls. The 4200 firewalls were in use in production and configured as a High Availability cluster, in which one firewall was an active device and the other acted as the backup appliance. The appliances of the active cluster were used as the main firewalls of a medium-sized company. This means that the appliances handled and inspected all network traffic that originated in or was bound for the client's network environment. This thesis was written for Tietokeskus Finland Oy, a Finnish ICT service provider.

The objectives of the thesis were to improve stability in the client's network environment and to prepare for increase in future network traffic. The new appliances were also more robust than their predecessors and covered by manufacturer's 5-year warranty, which would provide additional protection should problems arise. Subsequent to this, after the migration would have been completed successfully, the management database of the firewalls was to be optimized by deleting outdated firewall rules and network objects as well as by rearranging the database. These measures would have reduced the workload on the networking devices, improved efficiency of the new firewalls and improved the overall security of the client's network.

A virtual testing environment was built to test the setup and to simulate the migration in an isolated environment before the actual migration would have taken place. When the testing environment was ready, the firewall configurations and the contents of the management database were first transferred from the 4200 appliances to the virtual environment and, after testing was over, to the 5100 appliances. The 5100 appliances were then installed in the data centre, after which their configurations were checked and adapted to the new environment. Then, after the firewalls were connected to the management network, the fault tolerance of the new cluster was improved by adopting a redundant fully meshed network topology between the appliances and rack switches.

Although the project remained unfinished and the migration could not be completed, the documentation created during the thesis project benefited both the client and Tietokeskus. In addition, the client's network diagrams and other documentation was updated as part of the thesis project, which facilitates the work of future network administrators and other specialists when they familiarize themselves with the intricacies of the client's network environment.

KEYWORDS:

Firewalls, Check Point, High Availability, clusters, migration, network security

SISÄLTÖ

KÄYTETYT LYHENTEET

Bash	Useissa Linux-jakeluissa käytössä oleva komentotulkki. (Bourne-again shell)
clish	Unixin kaltaisille käyttöjärjestelmille kehitetty komentotulkki, joka on oletusarvoisesti käytössä Check Pointin laitteissa. (Command Line Interface Shell)
CCP	Check Pointin omisteinen protokolla, jota klusterin laitteet käyttävät HA- ja synkronointitoimintojen hallinnassa [1]. (Cluster Control Protocol)
DHCP	Tietoverkon laitteiden IP-osoitteiden ja asetusten jakamisessa käytetty protokolla. (Dynamic Host Configuration Protocol)
DNS	Nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi. (Domain Name System)
FTP	TCP-protokollaa hyödyntävä tiedostonsiirtoprotokolla. (File Transfer Protocol)
GNS3	Verkkosimulaattori, jonka avulla voi rakentaa verkkotopologioita virtuaalialustalle. GNS3 tarjoaa valmiita laitemallipohjia (*template*), joihin käyttäjän on lisättävä laitevalmistajien omien käyttöjärjestelmien levykuvia pystyäkseen käyttämään simuloituja laitteita. (Graphical Network Simulator-3)
GUI	Graafinen käyttöliittymä. (Graphical User Interface)
HA	Tekniikka, jossa käytetään kahden tai useamman laitteen klusteria parantamaan järjestelmän vikasietoisuutta. HA-tilassa yksi laite on aktiivinen ja toinen varalaite, joka tarkkailee aktiivisen laitteen tilaa ja omaksuu sen roolin häiriön tai vian sattuessa. (High Availability)
HTTPS	TLS-salauksella vahvennettu, TCP-protokollaa hyödyntävä tiedonsiirtoprotokolla, jota käytetään tavallisimmin verkkoselainten ja verkkopalvelinten välisessä liikenteessä. (Hypertext Transfer Protocol Secure)
ICA	Sisäinen varmenne. Check Pointin hallintapalvelimissa sijaitseva, hallintapalvelimen asennuksen yhteydessä luotu varmenne, jota tarvitaan palomuurien ja hallintapalvelinten välisessä viestinnässä ja VPN-yhteyksien muodostamisessa [2]. (Internal Certificate Authority)
IP	Protokolla, joka vastaa IP-pakettien välittämisestä tietoverkoissa. Paketit välitetään lähettäjältä vastaanottajalle niille määritettyjen IP-osoitteiden perusteella. (Internet Protocol)

IPS	Tunkeutumisenestojärjestelmä, jonka tarkoitus on estää haitallinen liikenne kohdelaitteeseen tai -järjestelmään. IPS voi olla laite tai ohjelmisto. (Intrusion Prevention System)
LAN	Lähiverkko eli tietoverkko, joka kattaa rajatulla alueella verkkoon kytketyt laitteet. (Local Area Network)
MAC	Siirtoyhteyskerroksen osa, joka vastaa lähetettävän tiedon kehystämisestä siirtoa varten. MAC-osoite on Ethernet-verkossa verkkosovittimelle annettu kiinteä osoite, joka yksilöi laitteen ja sen valmistajan. (Media Access Control)
NAT	Osoitteenmuunnos. Menetelmä, jonka avulla rajallinen määrä julkisia IP-osoitteita voidaan jakaa laitteille, joille on määritetty ainoastaan yksityinen IP-osoite. (Network Address Translation)
NGFW	Seuraavan sukupolven palomuuri. Check Pointin terminologiassa NGFW on myös vanhempiin palomuureihin saatavana ollut palvelupaketti, joka sisälsi palomuurin perustoiminnot. Tarkempi kuvaus seuraavan sukupolven palomuureista on luvussa 2. (Next Generation Firewall)
NGTP	Check Pointin palomuurilaitteisiin tarkoitettu palvelupaketti, johon kuuluu palomuurin perustoimintojen lisäksi seuraavat *blade*-palvelut: IPS, Application Control, Antivirus, Anti-Bot, URL Filtering ja Email Security. (Next Generation Threat Prevention)
NGTX	Check Pointin tarjoama palvelupaketti, johon sisältyy NGTP-paketin lisäksi nollapäivähaavoittuvuuksilta suojaavat SandBlast Threat Emulation- ja SandBlast Threat Extraction -ominaisuudet. (Next Generation Threat Extraction)
RDP	Microsoftin kehittämä omisteinen protokolla, jonka avulla voi ottaa etäyhteyden toisiin tietokoneisiin tai virtuaalikoneisiin verkon yli. (Remote Desktop Protocol)
SCP	SSH-yhteyttä hyödyntävä turvallinen tiedostonsiirtoprotokolla. (Secure Copy Protocol)
SG	Check Pointin käyttämä nimitys laitepalomuureistaan. (Security Gateway)
SIC	Check Pointin palomuurien ja hallintapalvelimien välinen salattu hallintayhteys, joka perustuu kertakäyttöiseen salasanaan ja varmenteisiin. (Secure Internal Communication)
SMS	Check Pointin palomuurien hallintapalvelin, joka voi olla joko erillinen laite tai asennettuna palomuuriin. (Security Management Server)
SNMP	Tietoverkkoon liitettyjen laitteiden hallinnassa käytettävä protokolla, jonka avulla järjestelmänvalvojat voivat kerätä tietoa

	laitteista ja niiden tilasta. (Simple Network Management Protocol)
SSH	Protokolla, jota käytetään salatun tietoliikenneyhteyden muodostamiseen laitteiden välillä. (Secure Shell)
TCP	Tietoliikenneprotokolla, jonka avulla laitteet voivat muodostaa välilleen yhteyden. TCP-protokollaa voidaan pitää luotettavana siirtomenetelmänä, sillä siinä on erilaisia tarkistusmekanismeja varmistamassa, että lähetetyt tiedot tulevat perille oikeassa järjestyksessä. (Transmission Control Protocol)
TFTP	UDP-protokollaa hyödyntävä tiedostonsiirtoprotokolla. (Trivial File Transfer Protocol)
UDP	Tietoliikenneprotokolla, jota käyttävät laitteet eivät muodosta yhteyttä, mutta ne voivat silti siirtää tietoja. UDP-protokollaa käytettäessä ei ole varmuutta siitä, että lähetetyt tiedot ovat menneet perille, mutta se kuormittaa verkkoa selvästi vähemmän. (User Datagram Protocol)
VLAN	Virtuaalilähiverkolla tarkoitetaan loogista laiteryhmää, johon kuuluvat laitteet voivat olla eri fyysisissä lähiverkoissa. Virtuaalilähiverkot helpottavat tietoverkon ylläpitoa ja parantavat osaltaan tietoturvaa, sillä niitä voidaan käyttää myös yleislähetysten rajoittamiseen. (Virtual Local Area Network)
VPN	Virtuaalinen yksityisverkko on usein Internetin kautta muodostettu salattu verkkoyhteys, jossa yhteyden muodostavat laitteet toimivat kuin ne olisivat samassa lähiverkossa. (Virtual Private Network)

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena oli suorittaa asiakkaan aktiivikäytössä olevan Check Point -palomuuriklusterin yliheitto. Tässä työssä yliheitolla tarkoitetaan vanhan palomuurijärjestelmän korvaamista uudella ja uusien palomuurien käyttöönottoa siten, että asiakkaan verkon normaaliin toimintaan tarvittavat tiedot siirretään vanhoista laitteista uusiin. Opinnäytetyö tehtiin Tietokeskus Finland Oy:n toimeksiannosta.

Klusterin yliheitto oli tärkeä projekti, sillä kyseessä oli asiakkaan liiketoiminnan kannalta kriittinen laitekokoonpano, jonka vikasietoisuus ei ollut toivotulla tasolla. Aktiivisen klusterin laitteet alkoivat jo olla elinkaarensa päässä, ja lisäksi ne tuskin olisivat pitkään suoriutuneet alati kasvavasta tietoliikenteen määrästä, joten työ haluttiin aloittaa ripeästi. Aihe oli haastava opinnäytetyöksi, sillä asiakkaan verkkoympäristössä oli lukuisia yliheittoon vaikuttavia tekijöitä, jotka oli huomioitava jo yliheiton suunnittelussa.

Ensinnäkin aktiivisen klusterin palomuurit toimivat asiakkaan pääpalomuureina eli kaikki asiakkaan verkkoliikenne kulki niiden kautta. Toiseksi asiakkaalla oli liiketoimintaa eri mantereilla, ja palomuurien ylläpitotoimenpiteille ei ollut varattu säännöllistä huoltoajankohtaa, sillä lyhyetkin katkokset olisivat aiheuttaneet taloudellista vahinkoa. Tietokeskuksen asiantuntijat olivat lisäksi työllistettyjä muissa projekteissa, joten palomuurien yliheittoon haluttiin tietoverkkoihin ja tietoturvaan perehtynyt henkilö, joka keskittyisi päätoimisesti palomuuriprojektiin.

Opinnäytetyön tavoitteina oli tutustua Check Pointin palomuureihin, niiden käyttöjärjestelmiin ja ylläpitoon sekä laatia ja toteuttaa yliheittosuunnitelma. Yliheitto oli ensin määrä toteuttaa testiympäristössä eli testausta varten rakennetussa virtuaaliympäristössä, ja testauksen tarkoituksena oli kerätä kokemuksia laitteiden ja liikenteen käyttäytymisestä yliheiton aikana. Tämän jälkeen tarkoituksena oli analysoida tulokset ja toteuttaa yliheitto tuotannossa mahdollisimman pienin häiriöin tai jopa katkoksitta.

Salassapitovelvollisuuden vuoksi tekstistä ja kuvista on poistettu tai peitetty asiakastietoja, laitteiden nimiä, IP-osoitteita, palomuurisääntöjä sekä muita arkaluonteisia tietoja. Samasta syystä osa kuvista ja liitteet on jätetty kokonaan pois. Tässä opinnäytetyössä 4200-klusterin palomuureihin viitataan nimillä oldfw1 ja oldfw2 kun taas 5100-klusterin palomuureista käytetään nimiä newfw1 ja newfw2.

Opinnäytetyössä käsitelty aihe eli palomuurien yliheitto oli osa laajempaa projektia, jossa asiakkaan laitekantaa siirrettiin konesalista toiseen. Opinnäytetyöprojektin aikana oli samanaikaisesti käynnissä muitakin osaprojekteja, kuten palvelinten ja virtuaalikoneiden siirtoja, ja lisäksi asiakkaalle tehtiin tavanomaisia, sopimuksen mukaisia ylläpitotoimia. Opinnäytetyöprojektin ohessa tehtiin asiakkaalle myös verkkojen sekä laitteiden kartoitusta ja päivitettiin asiakasdokumentaatiota. Tässä opinnäytetyössä keskitytään vain palomuuriklusterin yliheittoon ja suoraan siihen liittyviin toimenpiteisiin – muut teemat on rajattu työn ulkopuolelle.

Lähdemateriaalin hankkiminen osoittautui ongelmalliseksi. Vaikka tässä työssä esitetyn kaltaisia toimenpiteitä on oletettavasti tehty lukuisia, tietoja tai kuvauksia niistä ei ole julkaistu tutkimuskirjallisuudessa. Tämä johtuu luultavimmin siitä, että palomuurijärjestelmien ja verkkojen tiedot ovat liikesalaisuuksia eikä kovin yksityiskohtaisia tietoja yliheitosta ole edes mahdollista julkaista tietoturvasyistä tai salassapitovelvollisuuden vuoksi. Lisäksi lähde- ja kohdejärjestelmät ovat lähes poikkeuksetta aina erilaiset, oli kyseessä sitten eri valmistajien laitteet tai jopa saman valmistajan eri mallit, ja ne on räätälöity kunkin yrityksen tarpeisiin. Tämän vuoksi yliheittoon voidaan antaa vain yleisiä suuntaviivoja.

Joitakin kuvauksia yliheitoista löytyi aiemmin julkaistuista opinnäytetöistä, mutta ne joko eivät käsitelleet Check Pointin laitteita tai sitten poikkesivat kysymyksenasettelultaan ja tavoitteiltaan tästä opinnäytetyöstä niin suuresti, ettei niitä ollut mahdollista hyödyntää. Paras apu löytyi Check Pointin keskustelupalstoilta, tietoturvaa ja Check Pointin palomuureja käsittelevistä blogikirjoituksista sekä valikoiduista ohjeartikkeleista. Valitettavasti eri lähteiden sisältämät tiedot olivat välillä ristiriitaisia, joten osaa toimenpiteistä oli vain kokeiltava käytännössä. Check Pointin palomuureja käsittelevää kirjallisuutta oli myös tarjolla niukalti, sillä jos Check Pointin laitevalmistajasertifiointeihin tähtäävät kirjat jätetään huomiotta, viimeinen yleisesti saatavilla oleva teos on vuodelta 2005. Lisäksi koska valtaosa Check Pointin teknisestä dokumentaatiosta oli ulottumattomissani Check Point -käyttäjätilin rajoitusten vuoksi, teoreettinen pohja opinnäytetyölle jäi melko ohueksi.

Tämä opinnäytetyö on jaoteltu siten, että luvussa 2 käsitellään palomuureja sekä niiden eroavaisuuksia yleisellä tasolla, luvussa 3 esitellään yliheittosuunnitelmat, luvussa 4 on dokumentoitu suunnitelman täytäntöönpano, luvussa 5 analysoidaan yliheiton tuloksia ja arvioidaan suunnitelman onnistumista ja luvussa 6 pohditaan tulosten merkitystä, niiden sovellettavuutta muihin hankkeisiin ja mahdollisia jatkotoimenpiteitä.

2 PALOMUURIT

2.1 Palomuurien toimintaperiaate

Palomuuri voi olla joko ohjelmistopalomuuri tai laitepalomuuri, jonka päätehtävä on tarkastella sen kautta kulkevaa liikennettä ja varmistaa että paketit, joiden halutaan pääsevän kohteeseensa, päästetään palomuurin läpi, ja paketit, joiden ei toivota pääsevän pidemmälle, hylätään [3, s. 9]. Tarkastelussa palomuuri käyttää ennalta määritettyjä sääntöjä, joita vastaan jokaista pakettia verrataan. Palomuuri käy sääntökantaa läpi sääntö kerrallaan säännöstä numero 1 alkaen, kunnes paketin sisältämiä tietoja käsittelevä sääntö löytyy [3, s. 1].

Palomuuri voidaan määrittää hallitsemaan ja ohjaamaan tietoliikennettä joko sisäverkossa tai ulkoverkon ja sisäverkon välillä, joista jälkimmäinen lienee huomattavasti yleisempi vaihtoehto.

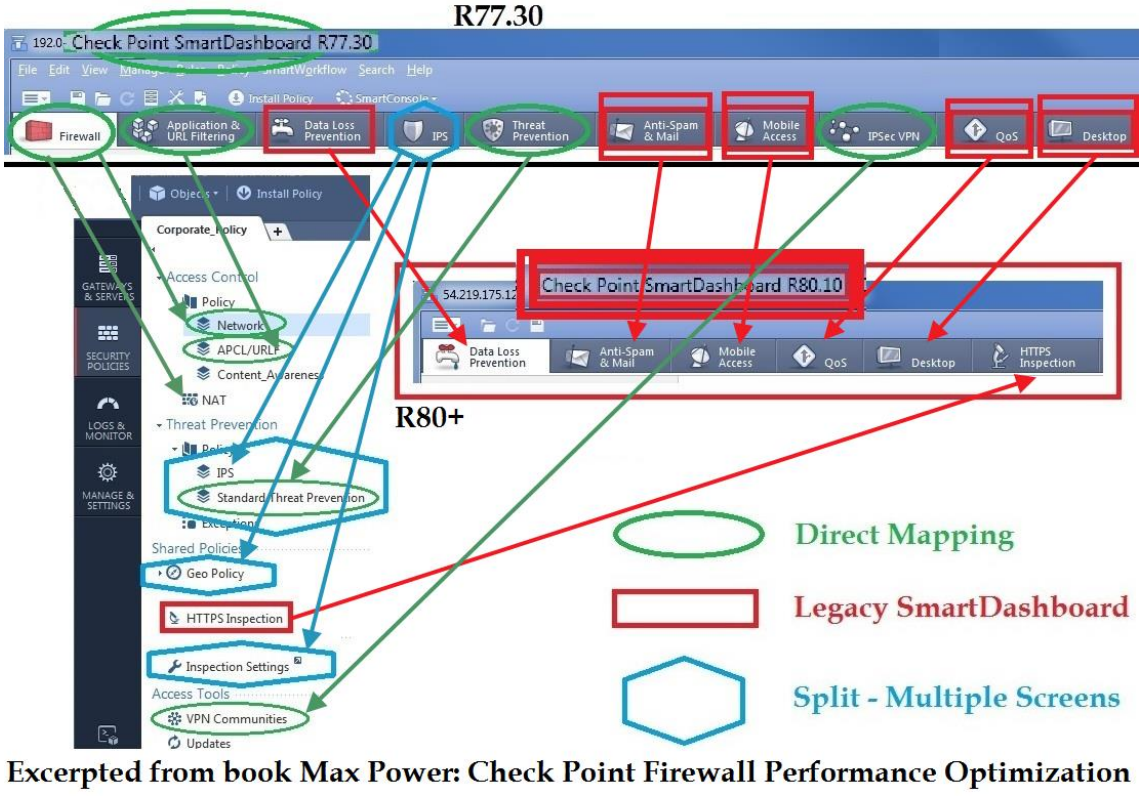
Moderni yritysverkoissa käytettävä palomuuri on monimutkainen laite, joka yhdistelee erillislaitteiden ja -järjestelmien toimintoja yhteen kokonaisuuteen. Tällainen niin kutsuttu seuraavan sukupolven palomuuri (NGFW) suoriutuu pakettien suodatuksen ja yhteyksien tilan tarkastelun lisäksi tunkeutumisen havaitsemis- ja estojärjestelmien tehtävistä ja kykenee lisäksi tarkkailemaan sovelluskerroksen liikennettä yksityiskohtaisesti [4].

2.2 Yleistä Check Pointin palomuureista

Kaikki Check Pointin tällä hetkellä markkinoimat palomuurit ovat seuraavan sukupolven palomuureja. Check Point -palomuuri muodostuu sekä laitteistosta että ohjelmistosta, jonka osaohjelmistoista eli moduuleista yritys käyttää termiä *blade*. Sillä todennäköisesti viitataan blade- eli korttipalvelimiin, erityiseen kehikkoon asennettaviin yksittäisiin palvelinlaitteisiin, jotka muodostavat palvelinkokonaisuuden. Check Point on pyrkinyt tuotteissaan modulaarisuuteen, minkä ansiosta asiakas voi perusominaisuuksien lisäksi valita palomuureihin ja hallintapalvelimiin erilaisia blade-moduuleja. Niitä ovat esimerkiksi palomuurilaitteissa verkkosivujen sisällön suodatukseen tarkoitettu *URL Filtering* -blade ja yrityssovellusten etäkäyttöä helpottava Mobile Access -blade sekä hallintapalvelimissa verkon ja verkkoon liitettyjen laitteiden valvontaan tarkoitettu *Check Point Monitoring* -blade.

Palomuurijärjestelmän tärkein osa on hallintatietokanta. Hallintatietokanta sisältää kaikki verkkoympäristössä käytettävät laitteet, verkot, protokollat, portit, IP-osoitteet, laiteryhmät, säännöt ja erillisten blade-moduulien määritykset eli käytännössä kaiken – laitteiden järjestelmäasetuksia lukuun ottamatta. Hallintapalvelin on mahdollista asentaa joko palomuuriin, jolloin palomuurista käytetään termiä *Standalone*, tai erilliseen palvelinlaitteeseen.

Palomuurin ja järjestelmäasetusten hallintaan käytetään komentoriviä ja graafista, verkkoselaimessa toimivaa GAiA Portal (WebUI) -käyttöliittymää, kun taas hallintapalvelinta hallitaan SmartDashboard-sovelluksella käyttöjärjestelmäversiossa R77.30 tai SmartConsole-sovelluksella käyttöjärjestelmäversiossa R80.10. Hallintapalvelimen komentoja on myös mahdollista suorittaa komentoriviltä tai R80.10-käyttöliittymäversiossa *Management API* -hallintarajapinnan kautta. Osaa toiminnoista voi käyttää ainoastaan komentoriviltä käsin, kun taas osa on käytettävissä vain selainkäyttöliittymässä. Tämä tekee laitteiden hallinnasta jossain määrin sekavaa, sillä aina ei ole selvää, mitä käyttöliittymää pitää käyttää esimerkiksi tietyn asetuksen määrittämiseen. Käyttöliittymien eroavaisuudet esitellään kuvassa 1.



Kuva 1. SmartDashboard- ja SmartConsole-käyttöliittymien vertailua [5].

Kuvasta käy ilmi, että R77.30-käyttöjärjestelmän SmartDashboard on suunniteltu selkeästi blade-arkkitehtuurin mukaan, sillä jokaista blade-moduulia varten on oma välilehtensä. Sitä vastoin R80.10-käyttöjärjestelmästä on kehitetty vähemmän hierarkkinen ja SmartConsoleen on yhdistetty aiempaa kiinteämmin hallintapalvelimen eri bladet. Lisäksi SmartConsolen kautta voi suoraan avata eri käyttöliittymäikkunoita, kuten halutun palomuurin GAiA Portal -näkymän tai clish-komentotulkin ilman erillistä SSH-yhteyttä.

2.3 Palomuurien vertailu

4200-palomuuriklusteri oli määritetty toimimaan *Standalone Full High Availability* (HA) -tilassa, mikä tarkoittaa, että kumpikin laite toimii sekä palomuurina (SG) että hallintapalvelimena (SMS). Tässä kokoonpanossa toinen palomuuri on aktiivinen eli se vastaa kaikista toiminnoista, ja toinen on varalaite, joka tarkkailee aktiivisen laitteen tilaa ja palomuurien välistä yhteyttä ja tarvittaessa ottaa itselleen aktiivisen laitteen roolin [6].

Check Point 4200 -palomuureissa on käyttöjärjestelmänä GAiA R77.30 ja Intel® Atom™ Dual-Core D525 -suoritin (1 Mt välimuistia, 1,80 GHz) ja 4 Gt keskusmuistia sekä kahdeksan 10/100/1000Base-T RJ45 -porttia. Laitteissa käytössä olevat lisenssit tarkistettiin komentoriviltä komennolla

```
cplic print ,
```

joka antoi tulosteeksi seuraavat lisenssitiedot:

```
CPAP-SG420X CPSB-FW CPSM-C-2 CPSB-VPN-HA CPSB-NPM CPSB-LOGS CPSB-IA-HA
CPSB-SSLVPN-5-HA CPSB-ADNC-HA CK-XX-XX-XX-XX-XX-XX.
```

Tulosteen mukaan laitteissa näytti olevan NGFW-palvelupaketti, johon sisältyi 4200-palomuurin laitelisenssi, *Firewall*-blade eli palomuuriohjelmisto, hallintapalvelinlisenssi 2 suoritinytimelle, *IPSec VPN* -blade, *Network Policy Management* -blade, *Logging and Status* -hallinta-blade, *Identity Awareness* -blade, 5 yhtäaikaisen käyttäjän *SSL VPN* -blade ja *Advanced Networking and Cluster* -blade. Lisäksi kaikki lisenssit oli asennettu HA-klusteria varten. Lisenssitiedoista kävi myös ilmi, että laitteiden palvelusopimus ei ollut enää voimassa, mutta laitteiden mukana toimitetut palomuuri- ja hallinnan blade -lisenssit eivät kuitenkaan vanhene, joten tieto ei edellyttänyt toimenpiteitä.

Check Point 5100 -palomuureissa on käyttöjärjestelmänä GAiA R80.10 ja Intel® Celeron® G1820 -suoritin (2 Mt välimuistia, 2,70 GHz) ja 8 Gt keskusmuistia sekä viisi

10/100/1000Base-T RJ45 -porttia. Laitteissa on perustoimintojen eli *Firewall*- ja *IPSec VPN* -moduulien sekä hallintapalvelimen eli *Network Policy Management* -bladen lisäksi NGTP-paketti, joka sisältää seuraavat bladet: *Application Control*, *URL Filtering*, *IPS*, *Antivirus*, *Anti-Bot* ja *Email Security*. Check Pointin Suomen edustaja tosin mainitsi, että näissä moduuleissa oli vain vuoden kokeilulisenssi, jonka voimassaolo oli alkanut laitteen hankinnasta. NGTP-paketin bladeja ei kuitenkaan ollut käytössä 4200-palomuureissa, joten näitä ei otettu käyttöön myöskään 5100-palomuureissa.

Laitteita vertailemalla kävi ilmi, että uusissa palomuureissa oli fyysisiä portteja kolme vähemmän kuin vanhoissa, mikä tarkoitti, että liitäntöjä oli jaettava useiden aliverkkojen kesken. Tämä ei välttämättä aiheuta ylikuormitusta palomuureihin, sillä uusien laitteiden suorituskyky on selvästi parempi kuin vanhojen. Lisäksi 4200-palomuureissa oli vapaana kaksi fyysistä liitäntää, joten vain yhden liitännän verkot oli jaettava muiden kesken. Tosin tällöin 5100-palomuureihin ei olisi jäänyt yhtään vapaata liitäntää tulevaa liikenteen kasvua varten, vaan uudet verkot olisi lisättävä jonkin fyysisen liitännän aliliitännöiksi tai, Check Pointin terminologian mukaan, VLAN-liitännöiksi.

Full HA -kokoonpano asettaa haasteita palomuurilaitteille, sillä niiden kuormitus on huomattavasti suurempi kuin hajautetussa kokoonpanossa, jossa palomuuri ja hallintapalvelin sijaitsevat eri laitteissa. Tämän vuoksi Full HA -laitteelta edellytetään huomattavasti suurempia laitteistoresursseja kuin pelkältä palomuurilta, koska hallintapalvelimen toiminnot kuormittavat laitteen suoritinta ja muistia. Hallintatietokannan koko ja verkon liikennemäärä ovat ratkaisevia laitteiden suorituskykyä vertailtaessa ja sopivaa laitetta valittaessa. Vaikka aiempi järjestelmänvalvoja oli tilannut tässä opinnäytetyössä tarkasteltavat laitteet ennen työn aloittamista, katsottiin silti tarpeelliseksi varmistua siitä, että laitteet olivat riittävän järeät suoriutumaan niille suunnitelluista tehtävistä.

Check Pointin R80.10-käyttöjärjestelmän julkaisutiedoissa oli maininta vähimmäislaitteistovaatimuksista, ja eri alustojen tietoja yhdistelemällä voitiin todeta, että palomuurin käyttö *Standalone*-tilassa edellyttää vähintään 2,6 GHz:n kellotaajuudella toimivaa Pentium IV -suoritinta ja kahdeksaa gigatavua keskusmuistia [7, s. 16–17]. Nämä edellytykset täyttyivät juuri ja juuri, joten 5100-palomuurit näyttivät kelpaavan 4200-palomuurien korvaajiksi.

3 YLIHEITON VALMISTELU JA MENETELMÄT

Yliheitossa sekä uusi että vanha järjestelmä ja niiden ominaisuudet on tunnettava hyvin, sillä monimutkaisiin järjestelmiin kohdistuvissa toimenpiteissä on vaarana, että jotain odottamatonta tapahtuu. Tällöin laitteiden hyvä tuntemus on eduksi. Yliheittovalmistelut aloitettiin tutustumalla palomuurivalmistajan oppaisiin ja itse palomuureihin, selvittämällä lukuisia yliheiton kannalta oleellisia asioita sekä laatimalla mahdollisimman kattava ja yksityiskohtainen suunnitelma yliheitosta. Suunnittelun lähtökohtana oli, että yliheitosta ei saisi koitua katkoksia asiakkaan verkkoliikenteeseen. Suunnittelun valmistuttua ja testauksen päätyttyä oli otettava yhteyttä asiakkaaseen ja sovittava tarkasti yliheiton aikataulusta, yliheitossa suoritettavista toimenpiteistä ja niiden laajuudesta sekä toimenpiteistä ongelma- tai vikatilanteissa.

3.1 Yliheittosuunnitelma

Suunnitelman mukaan yliheittoa on tarkoitus harjoitella testiympäristössä ennen laitteiden asentamista konesaliin ja varsinaisen yliheiton toteuttamista. Tällöin konfiguraatiomuutokset tehdään ja migraatio toteutetaan virtuaalikoneilla. Tämän jälkeen virtuaalikoneissa olevat tiedot siirretään fyysisiin laitteisiin, joiden toimivuus testataan ennen palomuurien käyttöönottoa tuotannossa.

Suunnitelman ensimmäisessä vaiheessa otetaan varmuuskopiot vanhoista 4200-mallin palomuureista testausta varten. Seuraavassa vaiheessa rakennetaan virtuaaliympäristö ja siirretään varmuuskopioidut tiedot virtuaalisille palomuureille, joissa on sama käyttöjärjestelmäversio (R77.30) kuin tuotannossa olevissa palomuureissa. Tämän jälkeen vanhoja palomuureja simuloivat virtuaalikoneet valmistellaan käyttöjärjestelmäpäivitystä varten Check Pointin omien työkalujen avulla eli niiden asetukset tarkistetaan, ja tarvittaessa niitä muokataan, jotta ne olisivat yhteensopivat uusien palomuurien käyttöjärjestelmän kanssa. Kun palomuurien asetukset ja hallintatietokannan yhteensopivuus on tarkistettu, otetaan vanhoista virtuaalipalomuureista varmuuskopio, joka siirretään uusia palomuureja simuloiviin virtuaalisiin palomuureihin, joissa on sama käyttöjärjestelmäversio (R80.10) kuin uusissa 5100-palomuureissa. Jos tämä sujuu ongelmitta, varmuuskopiot voidaan siirtää testiympäristöstä fyysisiin laitteisiin ja uusia palomuureja päästään

testaamaan siten, että ne ovat erillään tuotantoympäristöstä. Vasta tämän jälkeen – edellyttäen että testaus on onnistunut ja kaikki ongelmakohdat ratkaistu – voidaan päättää uusien palomuurien käyttöönotosta tuotannossa.

Ongelmatilanteiden varalle laadittiin varasuunnitelma, sillä aiempien kokemusten mukaan mittavan virtuaaliympäristön rakentaminen uudelle alustalle, jota muodostettaessa ei ole voitu ottaa huomioon verkkosimulaattoreiden vaatimuksia ja jonka asetuksia ei pysty tuotannollis-teknisistä syistä muokkaamaan, voi osoittautua haastavaksi. Varasuunnitelmana on ottaa varmuuskopio pelkästä hallintatietokannasta, valmistella se siirtoa varten ja siirtää tietokanta vanhasta palomuuriklusterista suoraan uuteen.

Viimeisenä vaihtoehtona olisi kaikkien tietojen siirtäminen uusiin palomuureihin käsityönä. Se olisi melko suoraviivainen vaihtoehto, mutta toimenpiteen edellyttämä työmäärä olisi melko suuri, ja todennäköisyys inhimillisten virheiden esiintymiselle olisi huomattava.

Kun laitteet ovat toimintakunnossa, ne on testattu ja niiden vikasietoisuus on toivotulla tasolla, sovitaan asiakkaan kanssa yliheiton aikataulusta sekä rauhoitusjaksosta, jonka aikana ei saa tehdä muutoksia palomuureihin tai verkkoympäristöön. Näin taataan yliheiton sujuminen mahdollisimman juohevasti ja ehkäistään mahdollisten ongelmatilanteiden syntyminen.

3.2 Vanhan palomuuriklusterin tietojen varmuuskopiointi

3.2.1 Varmuuskopiointisuunnitelma

Check Pointin suositusten mukaan lähde- ja kohdepalomuurien käyttöjärjestelmän, käyttöjärjestelmän version, koontiversion ja laitemallin on täsmättävä, jotta varmuuskopiointi onnistuisi [8]. Tässä kohtaa on myös huomioitava, että jos varmuuskopio otetaan GAiA Portal (WebUI) -käyttöliittymässä, käyttöjärjestelmäasetuksia ei varmuuskopioida, vaan ne on varmuuskopioitava erikseen [9, s. 84]. Käyttöjärjestelmäasetuksia ovat esimerkiksi liitäntöjen määritykset, DHCP- ja DNS-palvelinten tiedot, reitit, NetFlow-, aika- ja SNMP-asetukset sekä ajastetut tehtävät, reititysprotokollien tiedot ja käyttäjätiedot [9, s. 84].

Jos varmuuskopioiden siirto ei suju odotetusti, käynnistetään vianetsintä. Jos vikaa ei löydy, otetaan käyttöön varasuunnitelma. Tällöin kaikki yllä luetellut kohdat eivät kuitenkaan päde, koska varmuuskopioita voi muokata Check Pointin hallintatietokannan siirtoon laatiman työkalun avulla eri käyttöjärjestelmäversioon sopivaksi. Jos yliheitto sitä vastoin onnistuu suunnitellusti, voidaan siirtyä uuden palomuuriklusterin optimointiin ja muokata uusien muurien asetuksia ja palomuurisääntöjä vastaamaan paremmin nykytilannetta.

3.2.2 Erilaisten varmuuskopiointimenetelmien vertailu

Tilannekuva (snapshot)

Tilannekuva eli snapshot on kattava varmuuskopiointimenetelmä, joka tallentaa

- tiedostojärjestelmän, mukaan lukien käyttäjän muokkaamat tiedostot
- järjestelmäasetukset, kuten liitäntöjen asetukset ja reititystaulun
- ohjelmisto-bladet
- hallintatietokannan, jos tilannekuva otetaan laitteessa, johon on asennettu hallintapalvelin [10, s. 24].

Tilannekuva siis ottaa täydellisen levykuvan palomuurin kiintolevyn juuriosiosta, joten se on turhan raskas ja sisältää yliheiton kannalta turhia tietoja, kuten laitekohtaisia tietoja sekä palomuuriin asennettuja ajureita ja päivityksiä, jotka eivät välttämättä ole yhteensopivia kohdelaitteen kanssa [8]. Check Pointin mukaan tilannekuvaa voi käyttää laitteessa, joka on samantyyppinen ja -mallinen kuin laite, josta tilannekuva on otettu [9, s. 50]. Ohje jättää hieman epäselväksi, mitä laitetyyppi käytännössä tarkoittaa, mutta luultavimmin sillä tarkoitetaan ohjelmistoalustaa eli käyttöjärjestelmää, joka tässä tapauksessa on GAiA. Tilannekuva suositellaan ottamaan onnistuneen käyttöönoton jälkeen ja ennen käyttöjärjestelmäpäivityksiä [8].

Varmuuskopio (backup)

Varmuuskopio eli backup tallentaa hallintapalvelimen (SMS) tietokannan ja palomuurin (SG) käyttöjärjestelmäkonfiguraatiot [10, s. 23–24]. Hallintapalvelimen varmuuskopiota voi käyttää hallintapalvelimen kloonaamiseen eli uuden varapalvelimen luomiseen tai tietojen siirtämiseen toiseen laitteeseen päivitystä varten [11, s. 88–89].

Varmuuskopioiden siirtämiseen on käytössä kolme eri tapaa: TFTP, SCP ja FTP. Aiempi järjestelmänvalvoja oli määrittänyt automaattisen varmuuskopiointisuunnitelman, jossa oldfw1- ja oldfw2-palomuureista otetaan joka viikko varmuuskopiot, jotka sitten siirretään FTP:llä konesalin hallintakoneena toimivalle palvelimelle. Tätä tarkoitusta varten on myös luotu oma käyttäjätilinsä. Erilliseen varmuuskopiointiin ei siis ole välttämättä tarvetta, vaan varmuuskopiot ovat suoraan haettavissa hallintapalvelimelta. Jos varmuuskopioita tarvitsee luoda ja siirtää useammin, otetaan SSH-yhteys palvelimelta xxx.xx.xxx.xx halutun palomuurin sisäverkon IP-osoitteeseen (oldfw1: xxx.xx.xxx.xx ja oldfw2: xxx.xx.xxx.xx) sekä otetaan varmuuskopio ja siirretään se palvelimelle esimerkiksi komennolla

```
add backup tftp ip xxx.xx.xxx.xx .
```

TFTP:n käyttö on yksinkertaista eikä vaadi käyttäjän tai salasanan määrittämistä, pääsy palomuurin komentoriville riittää. Tietoturvan kannalta on toki järkevämpää käyttää tiedostojen siirtoon esimerkiksi SCP:tä, mutta tätä varten palomuurista on otettava käyttöön *expert*-tila ja vaihdettava komentotulkiksi *bash* palomuureissa oletusarvoisesti käytössä olevan *clish*-komentotulkin sijaan [12]. Järjestelmänvalvojan tili- tai käyttäjäasetuksia ei kuitenkaan kannata muokata, vaan SCP-tiedonsiirrossa voidaan joko hyödyntää vanhoissa palomuureissa ajastettua varmuuskopiointia varten määritettyä käyttäjää tai kirjautua sisään järjestelmänvalvojan tunnuksilla ja luoda uusi käyttäjä komentoriviltä seuraavasti:

```
add user scpuser uid 2600 homedir /home/scpuser
set user scpuser realname Scpuser
add rba role scpRole domain-type System readwrite-features expert
add rba user scpuser roles scpRole
set user scpuser gid 100 shell /usr/bin/scponly
set user scpuser password
save config
```
[13].

Näistä jälkimmäinen vaihtoehto on tietoturvan kannalta parempi, sillä siinä ei anneta *admin*-tason käyttöoikeuksia, vaan pääsy järjestelmään on rajallisempi. Tietoturvaa voi parantaa entisestään sallimalla *scpuser*-käyttäjälle pääsy ainoastaan omaan kotihakemistoon. Tällöin järjestelmänvalvoja voi kopioida siirrettävät tiedostot *scpuser*-käyttäjän kotihakemistoon eikä *scpuser*-käyttäjä pääse käsiksi muihin tiedostoihin [9, s. 53].

Kun käyttäjä on luotu ja komentotulkki vaihdettu, voidaan palomuuriin muodostaa SCP-yhteys esimerkiksi WinSCP-ohjelman avulla ja siirtää tiedostoja palomuurista konesalin hallintakoneena käytettävälle palvelimelle. Tämän jälkeen varmuuskopiot voi siirtää palvelimelta testiympäristöön joko jonkin luotettavan pilvipalvelun avulla tai Windowsin Kopioi > Liitä -ominaisuutta käyttäen suoraan RDP-yhteyden yli.

Järjestelmäasetusten kopiointi ja siirtäminen

Järjestelmäasetukset tallennetaan myös osana tilannekuvaa ja varmuuskopiota, mutta erikseen ne voi varmuuskopioida vain komentoriviltä käsin. Tällä menetelmällä saadaan talteen järjestelmäasetukset skriptitiedostona.

Asetukset sisältävä tiedosto luodaan komentoriviltä komennolla

```
save configuration <tiedoston nimi>,
```

joka luo tiedoston ja tallentaa sen kirjautuneena olevan käyttäjän kotihakemistoon eli esimerkiksi järjestelmänvalvojan tiliä käytettäessä kansioon ***/home/admin***. Tämän jälkeen skriptitiedosto siirretään palomuurista SCP-asiakasohjelman avulla hallintakoneelle ja sieltä edelleen kohdepalomuuriin järjestelmänvalvojan kotihakemistoon. Kohdepalomuurissa tiedosto otetaan käyttöön komentorivillä seuraavasti:

```
set clienv on-failure continue
load configuration <tiedoston nimi>
set clienv on-failure stop
save config
```
[14–15].

Klusterin tiedot

Palomuuriklusterista kannattaa myös ottaa talteen klusteritunniste eli Cluster Global ID. Tämä onnistuu komentoriviltä komennolla

```
cphaconf cluster_id get,
```

joka tulostaa tunnisteen komentorivi-ikkunaan [16]. Olemassa olevaa klusteritunnistetta voidaan käyttää, kun uusista palomuureista muodostetaan *High Availability* -klusteri. Li-

säksi on tarkistettava, ettei uudessa ja vanhassa palomuuriklusterissa ole käytössä samaa klusteritunnistetta tai, jos kumpikin klusteri on muodostettu samalla tunnisteella, niillä ei ole liitäntöjä samassa aliverkossa [17, s. 113].

3.2.3 Hallintatietokannan varmuuskopiointi

Hallintatietokanta on palomuuriklusterin toiminnan kannalta äärimmäisen tärkeä. Se sisältää kaikki palomuurien käyttämät säännöt, verkot, IP-osoitteet, VPN-yhteydet ja laitteet, joten ilman hallintatietokantaa palomuurit eivät toimi. Tässä luvussa esitellään hallintatietokannan varmuuskopiointiin tarkoitetut työkalut ja tarkastellaan niiden käyttöä. Hallintatietokannan varmuuskopioinnissa käytetään Check Pointin omaa hallintatietokannan siirtämiseen suunniteltua *Management Server Migration Tool* -työkalua.

Tätä työkalua voi käyttää sekä hallintatietokannan varmuuskopiointiin että käyttöjärjestelmäpäivitysten yhteydessä hallintatietokannan valmisteluun uutta käyttöjärjestelmäversiota varten. Työkalusta voi käyttää joko Check Pointin tukisivustolta ladattua uusinta versiota (**R80.10 Management Server Migration Tools for Gaia R7X.X to R80.10**) tai uusien palomuurien mukana toimitettua versiota, joka löytyy kansiosta ***/opt/CPsuite-R80/fw1/bin/upgrade_tools/***. Check Point suosittelee käyttämään uusinta versiota työkalusta, mutta tässä tapauksessa sitä ei voi käyttää [9, s. 58]. Vaatimuksena nimittäin on, että vanhan palomuuriklusterin hallintatietokannan siirtämiseen käytetään työkalun versiota, jonka pitää vastata uuden klusterin hallintapalvelimen käyttöjärjestelmän koontiversiota, joten työkalun kopiointi uusista palomuureista vanhoihin on helpoin ratkaisu – etenkin, kun uusimman version lataaminen edellyttää voimassaolevaa Check Pointin kumppanuussopimusta, mitä ei vielä opinnäytetyön tekohetkellä ollut.

Työkalut siirretään SCP:llä vanhan palomuuriklusterin pääasialliselle hallintapalvelimelle esimerkiksi kansioon ***$FWDIR/bin/upgrade_tools***. Ennen työkaluarkiston purkamista kannattaa luoda oma kansio vanhoja työkaluja varten ja siirtää vanhat versiot työkaluista sinne. Tämän jälkeen suoritetaan *pre_upgrade_verifier* -tarkistustyökalu, joka varmistaa, että hallintatietokanta ei aiheuta virheitä kohdelaitteessa, vaan että se on yhteensopiva uuden käyttöjärjestelmäversion kanssa. Tarkistustyökalu käynnistetään komennolla

```
./pre_upgrade_verifier -p $FWDIR -c R77 -t R80 -f R77_old_for_editing,
```

jossa parametreinä ovat hallintapalvelimen asennuskansio, sen laitteen käyttöjärjestelmäversio, jossa komento suoritetaan, kohdelaitteen käyttöjärjestelmäversio ja lopuksi työkalun käyttäjän määrittelemä nimi työkalun luomalle tiedostolle [9, s. 59].

Tarkistustyökalu siis analysoi hallintatietokannan, tarkistaa sen sopivuuden kohdejärjestelmässä ja tulostaa raportin ongelmakohdista, joita saattaa ilmetä siirrettäessä tietokantaa uusiin palomuureihin. Raportissa mainitut puutteet on niiden vakavuuden mukaan korjattava joko vanhan palomuuriklusterin hallintapalvelimessa tai siirron jälkeen uuden klusterin hallintapalvelimessa. Tietokanta viedään palomuurista komennolla

```
./migrate export tiedostonimi.tgz
```

ja siirretään SCP:llä palvelimelle. Ennen siirtämistä on tarkistettava, että SCP-ohjelma siirtää tiedostot binääritilassa [9, s. 86]. On tärkeää huomata, että Check Pointin suositusten mukaisesti ennen vientiä on joko pysäytettävä palomuurin toiminnot komennolla ***cpstop*** tai suljettava kaikki SmartConsole-yhteydet hallintapalvelimena toimivaan palomuuriin [9, s. 38; 83]. Näistä metodeista ***cpstop*** katkaisee kaikki yhteydet palomuuriin ja sulkee kaikki muut palvelut paitsi liikenteen suodatuksen, joten sitä ei voida tuotannossa olevalle palomuurille suorittaa. Ennen siirtoa on hyvä varmistaa, ettei SmartConsole-yhteyksiä hallintatietokantaan ole auki. Tämä onnistuu komentoriviltä komennolla

```
cpstat mg ,
```

joka tulostaa komentoriville syötteen, jossa on lueteltu aktiiviset hallintayhteydet hallintatietokantaan [18].

Ennen hallintatietokannan tuontia kohdelaitteeseen on myös hyvä tarkistaa, että hallintatietokannan varmuuskopion MD5-tarkistussummat ovat samat. Näin varmistetaan, että tietokanta ei ole korruptoitunut tai muuttunut siirron aikana. Tarkistussumman voi tulostaa näyttöön suorittamalla 4200-palomuurin komentorivin *expert*-tilassa komennon

```
md5sum $FWDIR/bin/upgrade_tools/tiedostonimi.tgz .
```

Näin saatua tarkistussummaa verrataan uuteen palomuuriin siirrettyyn tiedostoon suorittamalla sama komento 5100-palomuurissa [9, s. 86]. Jos tarkistussummat täsmäävät, hallintatietokanta on eheä ja kaikki on valmista tietokannan tuontia varten. Jos tarkistussummat eivät täsmää, tiedosto siirretään uudelleen ja tarvittaessa vaihdetaan tiedonsiir-

tomenetelmää. Jos tiedonsiirrossa käytetään SCP-asiakasohjelmaa, käytettävän sovelluksen asetuksissa on ennen hallintatietokannan siirtämistä valittava tiedonsiirtotavaksi **Binary**, jotta vältetään tietokannan korruptoituminen [9, s. 69].

Hallintatietokanta voidaan ottaa käyttöön uusissa palomuureissa, kun on varmistuttu tietokannan yhteensopivuudesta ja eheydestä. Tietokanta otetaan käyttöön komennolla

```
./migrate import tiedostonimi.tgz ,
```

jonka suorittaminen pysäyttää kaikki palomuurin palvelut (komento ***cpstop*** suoritetaan automaattisesti skriptin suorittamisen yhteydessä).

Tämän jälkeen varmistetaan tiedot ja tarkistetaan niiden toimivuus. Katso ohjeita Check Pointin asennusdokumentaatiosta [9, s. 58; 83]. Kannattaa varmistaa etenkin SYNC-verkon (oletuksena palomuurien LAN1-portti on tarkoitettu synkronointikäyttöön) osoitteet eli liitäntöjen IP-osoiteasetukset [9, s. 43].

3.3 Yliheiton toteutuksen suunnittelua

Kun hallintatietokanta ja järjestelmäasetukset on siirretty vanhoista palomuureista uusiin palomuureihin, selvitetään, miten palomuurien kuormantasaus ja klusterointi järjestetään. Helpoiten toteutettava vaihtoehto olisi muodostaa neljän palomuurin klusteri vanhoista palomuureista ja uusista palomuureista, ohjata liikenne uusien palomuurien kautta ja sammuttaa vanhat palomuurit yksi kerrallaan. Näin voitaisiin testata uusien palomuurien toimivuutta etukäteen, mutta kyseinen tapa ei ole ainakaan valmistajan suosittelema. Check Pointin ohjeissa mainitaan, että kaikissa klusterin palomuureissa on oltava ”samalla tavalla määritetty alusta,” mikä tarkoittanee laitemallia tai ohjelmistoversiota [17, s. 33]. Lisäksi Check Pointin suositusten mukaan klusterin palomuurien suorittimen, emolevyn, muistin ja liitäntöjen määrän sekä liitäntätyyppien on oltava identtiset [17, s. 57]. Myös käyttöjärjestelmän ja käyttöjärjestelmän koontiversion on täsmättävä, ja kaikissa laitteissa on oltava samat *hotfix*-päivitykset [17, s. 57; 137–138].

Teoriassa klusteriin on mahdollista lisätä eri mallisarjojen laitteita, kunhan palomuureissa on sama määrä fyysisiä suoritinytimiä [19]. Lisäksi 5100-palomuuriin on mahdollista asentaa R77.30-käyttöjärjestelmä, mutta se edellyttää valmistajan tarjoamaa muokattua käyttöjärjestelmäversiota [20]. Yksi toteutusvaihtoehto olisikin asentaa 5100-palomuu-

reihin GAiA R77.30 -käyttöjärjestelmä, siirtää niihin vanhojen palomuurien muokatut hallintatietokanta sekä järjestelmäasetukset ja muodostaa neljän palomuurin klusteri. Tämän jälkeen päivitettäisiin uusien 5100-palomuurien käyttöjärjestelmä uudelleen versioon R80.10 ja suoritettaisiin Check Pointin *Connectivity Upgrade*, jossa ennen päivitystä muodostetut yhteydet palomuuriin tai sen kautta eivät katkea päivityksen aikana [9, s. 88; 99]. Check Pointin kanta kuitenkin on, että 4200- ja 5100-laitemallien väliset erot saattaisivat estää klusterin muodostamisen neljän palomuurin kesken, vaikka teoreettisesti tällainen olisikin mahdollista. Käytännön sovelluksia esittämäni kaltaisesta kokoonpanosta ei kuitenkaan löydy, joten mielestäni tällaista järjestelyä ei voi suositella [19].

Toisena vaihtoehtona on, että yliheitto toteutettaisiin vaiheittain eli ensin yksi 5100-palomuuri asennettaisiin konesaliin ja kytkettäisiin verkkoon sekä toinen 4200-palomuureista sammutettaisiin. Jos palomuurit toimisivat odotetusti, yliheitto suoritettaisiin loppuun toistamalla samat toimenpiteet muille palomuureille. Tämä malli perustuu tilanteeseen, jossa vanhassa ja uudessa laitteessa olisi samat tiedot, jolloin osa liikenteestä ohjautuisi uudelle palomuurille, osa vanhalle. Ajatus ei kuitenkaan vaikuta houkuttelevalta, sillä tällöin klusterointi ja *High Availability* -ominaisuus eivät toimisi ja vikasietoisuus kärsisi liikaa.

Kolmas vaihtoehto on suunnitelma, jossa uusi 5100-palomuuriklusteri asennettaisiin vanhan 4200-klusterin rinnalle siten, että molemmat käyttäisivät samoja verkkoja mutta eri IP-osoitteita. Check Point ei tosin suosittele useiden klusterien käyttöä samassa virtuaalilähiverkossa (VLAN), mutta jos se on välttämätöntä, sekä klusterien välisessä hallintaliikenteessä käytettävän CCP-protokollan lähetys-MAC-osoitetta (Check Pointin terminologiassa MAC Magic ID) että synkronointiverkon liitäntöjen IP-osoitteita on muokattava uudessa klusterissa [16].

Kolmas vaihtoehto on näistä toteuttamiskelpoisin, koska vastaavasta tapauksesta on olemassa niin Check Pointin laatimat yksityiskohtaiset ohjeet kuin muiden järjestelmänvalvojien kokemuksia. Tässä vaihtoehdossa uudet palomuurit valmistellaan yliheittoa varten siirtämällä niihin tarvittavat tiedot vanhoista palomuureista. Tämän jälkeen uuden palomuuriklusterin klusteritunnistetta muokataan, jotta uusien palomuurien synkronointiverkon liikenne ei sekoitu vanhojen palomuurien synkronointiliikenteen kanssa. Lisäksi vaihdetaan uusien palomuurien nimet ja muokataan IP-osoitteita, jotta vältetään päällekkäisyydet vanhojen palomuurien kanssa. Myös palomuurisääntöjä on muokattava, jotta liikenne kulkisi uusien palomuurien läpi. Kun 5100-palomuurit on valmisteltu käyttöönottoa varten edellä mainitut seikat huomioiden, molemmat uuden klusterin palomuurit asennetaan paikoilleen konesaliin ja kytketään hallintaverkkoon. Lisäksi varmistetaan,

että SIC-yhteyden muodostaminen laitteiden välille onnistuu. Tarkemmat ohjeet tähän on annettu Check Pointin ohjeistuksessa [17, s. 111–114].

Vasta kun uudet palomuurit ovat täysin toimintakykyiset, sammutetaan vanhan klusterin palomuurit yksi kerrallaan, ja muutetaan uuden klusterin palomuurien nimet ja IP-osoitteet siten, että ne vastaavat tarkalleen vanhojen palomuurien tietoja. Tämä on tärkeä vaihe, sillä esimerkiksi VPN-yhteyksiä käyttäville päätelaitteille on syötetty vanhan palomuuriklusterin nimi- ja osoitetiedot, ja jos tiedot eivät täsmää, etäyhteyttä ei voi muodostaa palomuurien läpi. Lopuksi tarkkaillaan uuden klusterin toimintaa ja yliheiton onnistumista.

3.4 Palautussuunnitelma

Jos yliheitto ei syystä tai toisesta onnistuisi, oli laadittava palautussuunnitelma, jossa kuvataan toimenpiteet tilanteen saattamiseksi ennalleen. Yllä kuvattua toteutussuunnitelmaa (luvun 3.3 vaihtoehtoa kolme) noudatettaessa liikenteen siirtäminen takaisin vanhalle palomuuriklusterille olisi helppoa, sillä teoriassa tähän riittää uusien palomuurien sammuttaminen ja vanhojen käynnistäminen.

4 TOTEUTUS

Palomuuriklusteri oli asiakkaan liiketoiminnan kannalta kriittinen järjestelmä, joten yliheiton suorittaminen katkoksitta tai aiheuttamalla mahdollisimman lyhyt katkos tietoliikenneyhteyksiin oli olennaista. Tämän vuoksi testausympäristön rakentaminen aloitettiin aivan opinnäytetyön alkuvaiheessa, jotta yliheittoa voitaisiin hallitusti harjoitella tuotantoympäristön ulkopuolella.

Aluksi kartoitettiin aktiivisen palomuuriklusterin palomuurit tutkimalla niiden hallintatietokantaa. Tämän jälkeen mietittiin, mitä tietoja halutaan siirtää vanhoista palomuureista uusiin, miten tiedot siirretään, ja onko asetuksia muokattava, vai voiko ne ottaa sellaisinaan käyttöön. Kun vanhojen palomuurien asetukset ja hallintatietokannan sisältö oli kartoitettu, oli vertailtava laitteita ja selvitettävä, miten tiedot voidaan parhaiten siirtää uusiin palomuureihin.

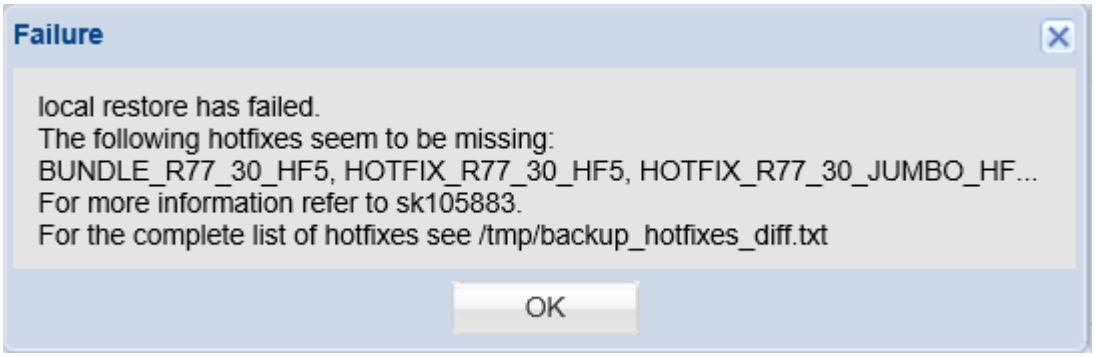
4.1 Yliheiton testaus virtuaaliympäristössä

Yliheittovalmistelut aloitettiin testausympäristön rakentamisella. Tähän ratkaisuun päädyttiin, koska aiemmin on saatu hyviä tuloksia virtuaaliympäristöjen rakentamisesta VMware-alustalle sekä verkkojen ja tietoverkkolaitteiden testaamisesta simulaattorin avulla. Ympäristö koostui virtuaalisista palomuureista, joissa oli samat käyttöjärjestelmät kuin 4200- ja 5100-palomuureissa, GNS3-verkkosimulaattorista ja VMware-sovelluksessa toimivasta GNS3-virtuaalikoneesta, joka ohjaa simulaattorin käskyt muille virtuaalisille laitteille. Ympäristön rakentaminen aloitettiin tavalliselle työasematietokoneelle, mutta pian huomattiin, että edes tehokkaan työaseman suorituskyky ei riitä R80.10-käyttöliittymän asentamiseen kahdelle virtuaalikoneelle. Tämän vuoksi pyydettiin Tietokeskuksen VMware-ympäristön ylläpitäjää varaamaan tarvittavat resurssit testiympäristön rakentamista varten.

Check Pointin käyttöjärjestelmäversioiden R77 ja R80.10 julkaisutiedoissa oli mainittu vähimmäislaitteistovaatimukset, joiden perusteella laskettiin tarvittavan vähintään 12 suoritinydintä, 25 Gt keskusmuistia ja 500 Gt levytilaa [7, s. 17; 21, s. 15–16]. Eri vaihtoehtojen punnitsemisen jälkeen päädyttiin lopulta ratkaisuun, jossa koko testiympäristö rakennetaan virtuaalialustalle ja kokoonpanosta jätetään pois GNS3-simulaattori ja -vir-

tuaalikone. Tällä tavoin saatiin yksinkertaistettua verkon topologiaa ja helpotettua vianmääritystä mahdollisissa ongelmatilanteissa, koska simulaattorin ja virtuaalikoneiden välisiä yhteyksiä ei tarvinnut ottaa huomioon. Seuraavaksi Tietokeskuksen konesalin VMware-ympäristöstä varattiin yllä mainitun laskelman mukaiset resurssit viidelle virtuaalikoneelle, joista neljä osoitettiin palomuureille ja yksi hallintakoneena toimivalle palvelinkoneelle. Hallintakoneena käytettävälle virtuaalikoneelle asennettiin käyttöjärjestelmäksi Windows Server 2016 sekä palomuurien hallinnassa ja ylläpidossa tarvittavat ohjelmistot.

Yliheittosuunnitelman mukaisesti tarkoitus oli siirtää vanhoista 4200-palomuureista otetut varmuuskopiot testiympäristön virtuaalipalomuureihin. Lähtökohtana oli, että koska käyttöjärjestelmä (R77.30) ja sen koontiversio (204) ovat identtiset molemmissa palomuureissa, varmuuskopion voi tuoda sellaisenaan testipalomuureihin ja ottaa niissä käyttöön. Aktiivisen klusterin palomuureille oli määritetty aikataulutettu varmuuskopiointi, jonka mukaisesti varmuuskopiot otetaan ja siirretään automaattisesti FTP-yhteyden avulla Espoossa sijaitsevassa konesalissa olevalle hallintakoneelle. Varmuuskopiot olivat siis valmiina, mutta niiden tuonti virtuaalisiin palomuureihin oli jo hankalampaa, sillä yritys tuotti kuvassa 2 näkyvän virheilmoituksen.



Kuva 2. Varmuuskopion tuonnin aiheuttama virheilmoitus virtuaalipalomuurissa.

Toisin sanoen 4200-palomuureihin oli asennettu *hotfix*-päivityksiä, joita ei ollut virtuaalisissa palomuureissa. Koska opinnäytetyön laatimishetkellä ei ollut voimassaolevaa kumppanuussopimusta Check Pointin kanssa, *hotfix*-päivityksiä ei voinut ladata.

Ratkaisuna kokeiltiin tilannekuvien siirtoa vanhoista palomuureista virtuaalisiin palomuureihin. Luvussa 3.2.2 esitettiin, että tilannekuvan voi siirtää, jos laitteet ovat samanmallisia ja -tyyppisiä ja jos lähde- ja kohdelaitteissa on sama käyttöjärjestelmä. 4200-palomuurissa ja virtuaalisessa palomuurissa on sama käyttöjärjestelmäversio, mutta toinen

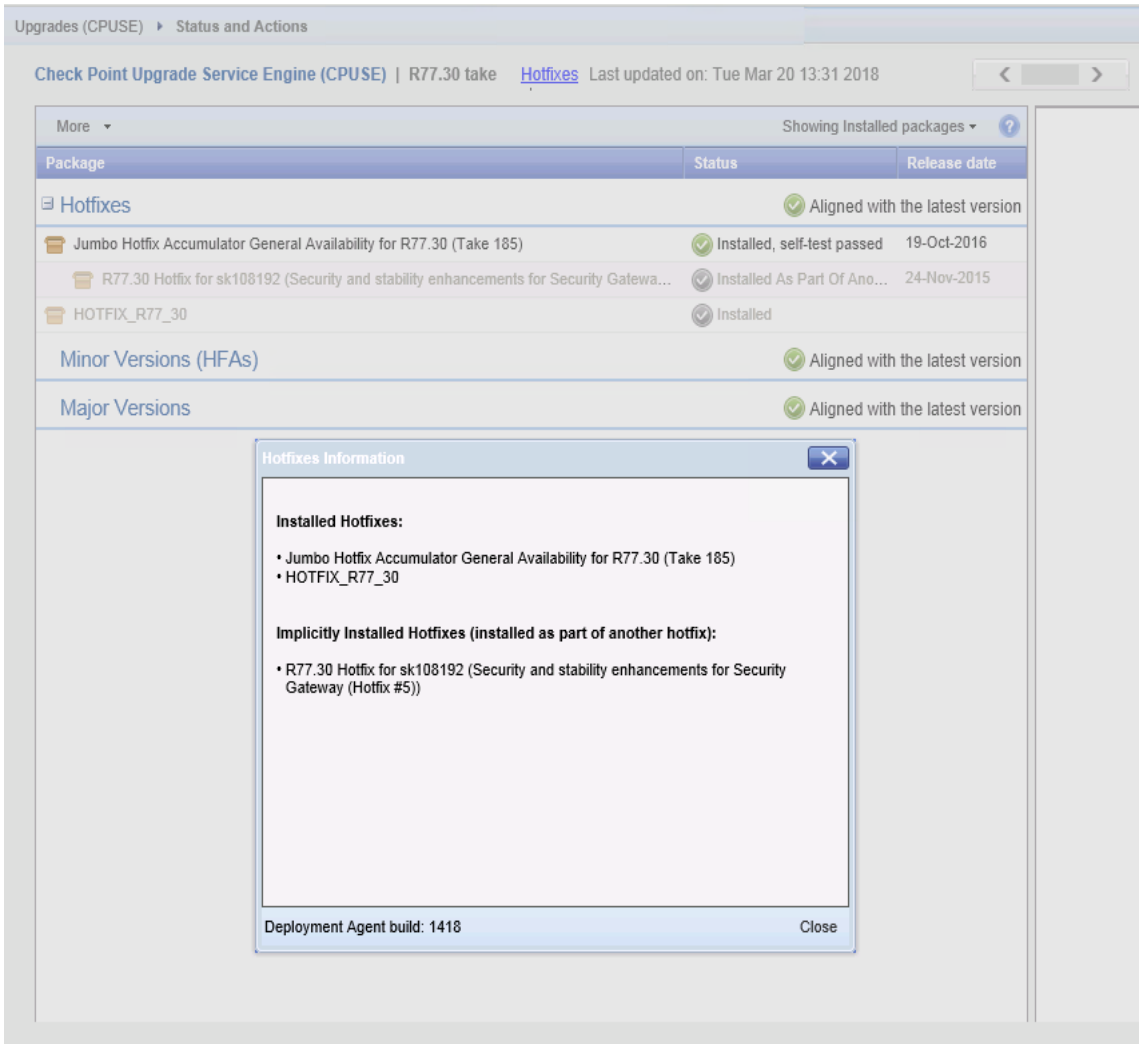
on laitealustalla ja toinen VMware-alustalla. Eräässä Check Pointin ohjeartikkelissa tosin mainitaan, että HA-klusterin muodostaminen fyysisestä laitteesta ja virtuaalikoneesta on mahdollista, joten tarkkojen tietojen puuttuessa tilannekuvan siirtoa oli vain testattava [22].

GAiA Portal (WebUI) -käyttöliittymän tilannekuvien hallinnassa (*Snapshot Management*) voi hallita ja luoda tilannekuvia sekä tuoda niitä laitteeseen tai viedä niitä laitteesta. Tilannekuvien ottaminen oli helppoa, mutta ongelmaksi muodostui niiden siirtäminen palomuurista hallintakoneelle. Tilannekuvien hallinnan vientitoiminto (*Export*) nimittäin pakkaa tilannekuvan ja tekee siitä kopion laitteen ***/var/log***-hakemistoon, joka on myös oma levyosionsa. Toimintoa suoritettaessa järjestelmä antoi virheilmoituksen, että laitteen levyaseman ***/var/log***-osiossa ei riitä tila toiminnon suorittamiseen. Check Pointin ohjeen mukaan kohdehakemistossa, johon tilannekuva viedään, pitää olla vapaata tilaa kaksi kertaa tilannekuvan koon verran, jotta vienti onnistuisi [23].

4200-palomuurien lokihakemistoon oli vuosien mittaan kertynyt lokeja sekä muita tiedostoja, joita olisi karsittava, mutta tietojen tarpeellisuus oli selvitettävä ennen poistamista. Levyosion läpikäynti osoitti, että ainakin kansiossa ***/var/log/opt/CPsuite-R77/fw1/log*** näytti olevan turhia tiedostoja sekä vanhoja asennuslokeja lokakuusta 2016 alkaen ja että automaattinen vanhojen lokien siivoustoiminto oli poistettu käytöstä. Levyosiota tutkittaessa ilmeni myös, että kansioissa ***/var/log/Cpda/backup*** ja ***/var/log/Cpda/repository*** on päivitystiedostoja eli ilmeisesti viimeisimmät laitteeseen asennetut päivitykset. Ennen vanhojen lokien poistamista kokeiltiin kuitenkin vielä kerran virtuaalipalomuurien päivittämistä ja varmuuskopioiden asentamista uudelleen. Komento

cpinfo -y all

tulostaa näyttöön kaikki Check Point -palomuuriin asennetut hotfix-päivitykset, ja suorittamalla komento sekä lähde- että kohdelaitteissa voitiin tarkistaa, onko laitteissa eri päivityspaketit [24]. Ensin tarkistettiin laitteiden väliset erot, minkä jälkeen päivityspaketit ladattiin ja yritettiin asentaa virtuaalisiin palomuureihin, mutta usean paketin asennus epäonnistui paketeista puuttuvasta tiedostosta aiheutuneen virheilmoituksen vuoksi (kuva 3).

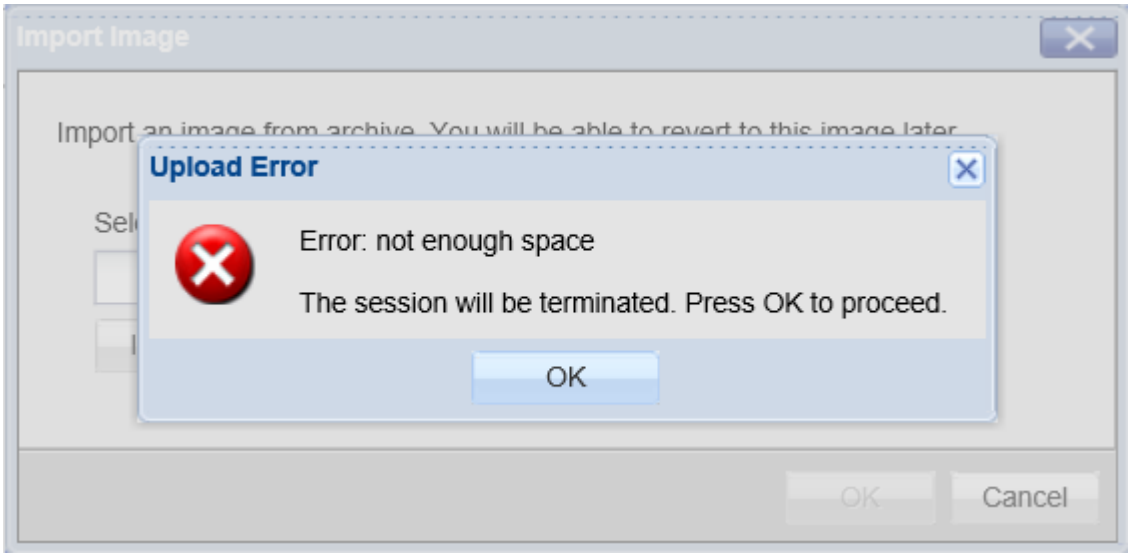


Kuva 3. Päivitysten asentamisen aiheuttama virheilmoitus virtuaalipalomuureissa.

Virheilmoituksen perusteella voitiin päätellä, että virhe aiheutui päivitysversioiden poikkeavuudesta, sillä 4200-palomuureihin oli asennettu *hotfix*-päivitys *Jumbo Hotfix Accumulator for R77.30 (Take 185)* eli päivitys, johon on kerätty useita järjestelmän eri palveluihin kohdistuvia vakautta ja laatua parantavia korjauksia [25]. Päivityksen lataaminen olisi tosin edellyttänyt kumppanuussopimusta Check Pointin kanssa, mutta koska sellaista ei ollut, korjauspäivityksiä ei voitu ladata eikä varmuuskopioita ollut näin ollen mahdollista ottaa käyttöön virtuaalipalomuureissa.

Seuraavaksi jatkettiin lokitiedostojen karsintaa ja yritettiin uudelleen tilannekuvien luontia. Check Pointin mukaan palomuurissa on oltava vapaata levytilaa kaksi kertaa tilannekuvan koon verran, joten vanhojen lokien poistamisessa noudatettiin tätä ohjetta [26]. Kun vanhan palomuuriklusterin lokitiedostoja oli karsittu, myös tilannekuvien ottaminen

onnistui, joten tilannekuvia ryhdyttiin siirtämään vanhan klusterin palomuureista testiympäristöön. Tilannekuvien luominen ja siirtäminen palomuureista hallintakoneelle sujui lähes ongelmitta, mutta niiden tuominen testiympäristöön ei onnistunut, sillä seurauksena oli jälleen virheilmoitus (kuva 4).



Kuva 4. Tilannekuvan tuonnin aiheuttama virheilmoitus virtuaalipalomuurissa.

Tuonti siis keskeytyi, koska virheilmoituksen mukaan virtuaalisen palomuurin levytila ei riitä tilannekuvan tuontiin. Valmistajan dokumentaatiossa, aihetta käsittelevissä blogeissa tai muissa ohjeissa ei ollut minkäänlaista mainintaa siitä, paljonko vapaata levytilaa tilannekuvan tuonti edellyttää, vaan kaikki artikkelit ja kirjoitukset käsittelivät vientiä. Lisäksi kohdepalomuurissa oli vapaana enemmän levytilaa kuin lähdepalomuurissa, joten todennäköisesti virheilmoitus kertoo jostain toisesta ongelmasta, jota en kuitenkaan onnistunut selvittämään. Tämä oli käytännössä viimeinen naula testiympäristön arkkuun, sillä kaikki keinot toimivan testausjärjestelmän luomiseen oli nyt käytetty.

4.2 5100-palomuurien valmistelu

Kun testiympäristön rakentamisesta oli luovuttu, seuraava vaihe oli yrittää siirtää järjestelmäasetukset ja hallintatietokanta aktiivisesta 4200-palomuuriklusterista 5100-palomuureihin.

Järjestelmäasetusten siirtäminen

Järjestelmäasetusten siirtäminen oli suoraviivainen toimenpide, joka tehtiin luvun 3.2.2 kohdan Järjestelmäasetusten kopiointi ja siirtäminen mukaisesti. Asetukset sisältävää skriptitiedostoa kuitenkin muokattiin tekstieditorissa poistamalla siitä liitäntöjen osoitteet ja määritetyt virtuaalilähiverkot sekä muuttamalla NTP-palvelimen tietoja ennen skriptin suorittamista kohdelaitteessa. Lisäksi muokattiin palomuureille määritettyä oletusreittiä, jotta vältettäisiin liikenteen tarpeeton ohjautuminen toiseen konesaliin. Lopuksi vielä tarkistettiin, että komennot ovat skriptitiedostossa asianmukaisessa järjestyksessä, ettei esimerkiksi käyttäjätietoja syötetä väärin. [27].

5100-palomuurien liitäntöjen osoitteet määritettiin graafisessa GAiA Portal (WebUI) -käyttöliittymässä, sillä tarkoituksena oli yhdistää useampi fyysinen liitäntä yhdeksi virtuaaliseksi liitännäksi tai liitäntäryhmäksi (Check Pointin terminologiassa *bond interface*), joka lisäksi määritettiin toimimaan HA-tilassa [9, s. 46–47]. Tämä liitäntäryhmä pilkottiin useampaan aliliitäntään, joille kullekin määritettiin oma aliverkkonsa. Tällä tavoin voitaisiin muodostaa vikasietoisempi yhteys synkronointiverkolle ja asiakkaan LAN-verkolle. Tässä kohtaa törmättiin myös pariin pulmaan. Ensinnäkin Check Pointin vaatimusten mukaisesti kytkinten, joihin palomuurit liitetään, *native VLAN* -asetuksena on oltava 1, jotta yhteys palomuureihin ei katkea [28]. Tämä ei ole yleensä suositeltavaa tietoturvan kannalta, mutta se voi olla perusteltua konesaleissa, joissa on useamman valmistajan laitteita kytkettynä samoihin kytkimiin. Toinen ongelma oli, että jos palomuurin synkronointiliitäntänä käytetään VLAN-liitäntää eli fyysisen liitännän aliliitäntää, synkronointi onnistuu ainoastaan siinä aliliitännässä, jonka VLAN-tunniste (VLAN ID) on pienin [29]. Tässä haasteeksi muodostui se, että lähes kaikki sopivan pieninumeroiset VLAN-tunnisteet olivat jo varattuja, mutta Check Pointin palomuureille löytyi kuin löytyikin sopiva VLAN Tietokeskuksen hallintaverkkojen joukosta.

Samalla tarkistettiin myös luvun 3.2.2 kohdan Klusterin tiedot mukaisesti aktiivisen klusterin klusteritunniste. Tarkistuksessa kävi ilmi, että vanhoissa 4200-mallin palomuureissa klusteritunnisteena on ollut 254, mikä on myös Check Pointin suosittelema arvo GAiA R80.10 -käyttöjärjestelmässä, sillä tällöin klusterien hallinnassa ja tietojen synkronoinnissa käytettävä CCP-protokolla toimii automaattitilassa [16]. R80.10-käyttöjärjestelmäversiossa klusteritunnisteen muuttaminen ei kuitenkaan ole suositeltavaa, vaan tunniste neuvotaan vaihtamaan ainoastaan, jos Check Pointin tuki näin kehottaa [17, s. 113–

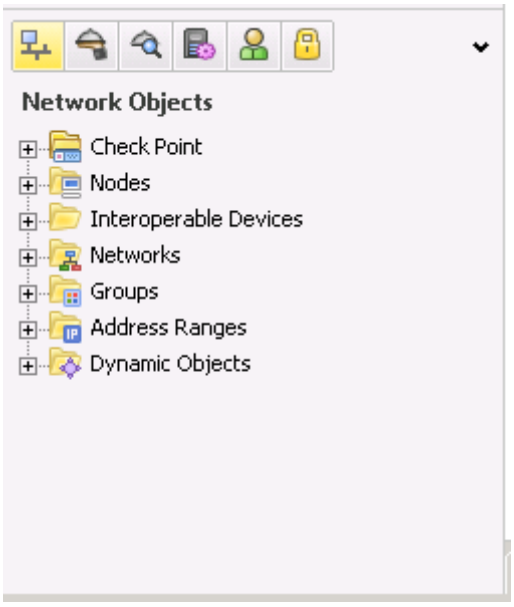
114]. Se, että kummassakin klusterissa oli käytössä sama klusteritunniste oli paitsi huonoa tuuria, aiheutti se myös lisää päänvaivaa, sillä synkronointiverkon liikenteen päätyminen tuotannossa oleviin palomuureihin olisi voinut aiheuttaa ikäviä seurauksia asiakkaan verkkoympäristössä. Havainnon seurauksena oli entistäkin tärkeämpää varmistaa, että räkkikytkimet eivät välitä synkronointiverkon liikennettä eteenpäin.

Hallintatietokannan siirtäminen

Koska hallintatietokannan vienti vanhoista palomuureista uusiin ei onnistunut, tietokannan tiedot oli siirrettävä käsin vanhasta palomuuriklusterista uuteen. Vaikka tietojen siirtäminen manuaalisesti oli työläs tapa, migraation toistaminen vanhan hallintatietokannan tiedoilla ei vaikuttanut kannattavalta eikä muita järkeviä työkaluja ollut käytössä. Olisi myös ollut mahdollista opiskella käyttämään Check Pointin omaa *Confwiz*-työkalua tai viedä tiedot hallintatietokannan kohteista .xml-muodossa, tuoda ne .csv-tiedostoon ja yrittää saada niitä lisättyä uusiin palomuureihin käyttämällä hallinnan ohjelmointirajapintaa (*Management API*), mutta pienempi vaiva oli luoda tiedot käsin uuden klusterin hallintatietokantaan ja vertailla sitten sitä vanhan tietokannan sisältöön.

Hallintatietokannan tietojen syöttämistä varten otettiin SmartDashboard-yhteys HA-klusterin varalaitteena toimivaan oldfw1-palomuuriin, valittiin ***Firewall***-välilehti ja sieltä kohta ***Policy***. Koska hallintatietokantaa käsiteltiin aktiivisena olevassa palomuuriklusterissa, tietoja oli järkevää tarkastella *Read Only* -tilassa, jotta voitiin välttää mahdollisten virhepainallusten aiheuttamat häiriöt.

Ennen sääntöjen luontia oli uuden palomuuriklusterin hallintapalvelimelle lisättävä tarvittavat verkot (***Networks***), palvelut (***Services***), *VPN Community* -kohteet, ryhmät (***Groups***) ja laitteet (***Nodes***). *VPN Community* on kokoelma palomuurilaitteita, jotka kykenevät muodostamaan VPN-tunnelin toisen päätelaitteen kanssa [30]. Termi voitaisiin virallisen käännöksen puuttuessa kääntää vaikkapa ryhmäksi.



Kuva 5. Verkkokohteet (***Network Objects***) -paneeli SmartDashboard-sovelluksessa.

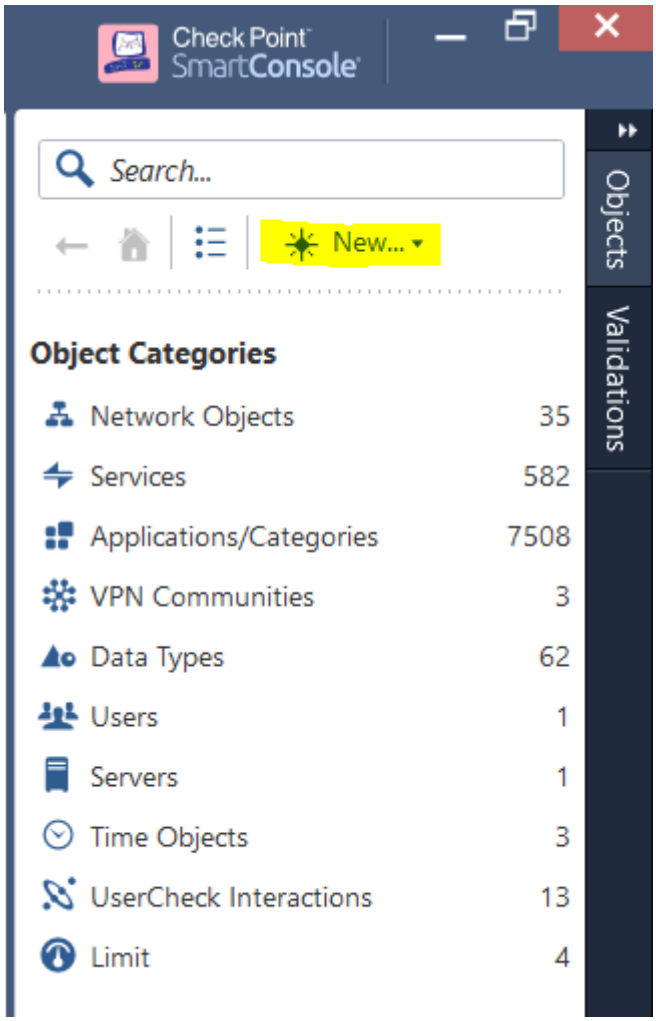
Tiedot haettiin SmartDashboardissa käyttämällä sovellusikkunan vasemmassa alareunassa olevaa navigaatiopaneelia (kuva 5). Paneelin yläreunan kuvakkeilla valittiin joko ***Network Objects***, ***Services*** tai ***VPN Communities***. ***Network Objects*** -näkymässä uuteen palomuuriklusteriin siirrettäviä kohteita oli kansioissa ***Nodes***, ***Interoperable Devices***, ***Networks*** ja ***Groups***. ***Service***-näkymässä oli järjestelmänvalvojan määrittelemät portit, joita käytettiin palomuurisäännöissä. ***VPN Communities*** -näkymän kohteista siirrettiin kaikki järjestelmänvalvojan määrittelemät ryhmät paitsi järjestelmän automaattisesti luomia kohteita ***MyIntranet*** ja ***RemoteAccess***.

Kohteiden siirtäminen oli VPN-asetuksia lukuun ottamatta melko suoraviivaista eli osoitteet ja määritykset tarkistettiin ja vastaava kohde luotiin uuteen hallintatietokantaan SmartConsolessa. Siirtämisen jälkeen tietoja verrattiin vielä kerran kohdelaitteen ja lähdelaitteen välillä, ettei niihin jäisi virheitä.

SmartDashboadissa vanhan palomuuriklusterin ***Advanced VPN Properties*** -välilehden kaikkia NAT-asetuksia ei päässyt näkemään *Read Only* -tilassa, vaan SmartDashboardiin oli kirjauduttava *Write*-tilassa, jotta voitiin tarkistaa kaikki VPN-yhteyksien asetukset. Nopein tapa oli napsauttaa sovellusikkunan alareunassa näkyvää ***Read Only Mode*** -linkkiä, josta saattoi valita, käynnistetäänkö SmartDashboard uudelleen *Write*-tilassa. Koska palomuuri oli määritetty tallentamaan automaattisesti hallintatietokantaan

tehdyt muutokset, piti VPN-yhteyksien tietojen kopioinnissa olla tarkkana, ettei vahingossa muokannut asetuksia.

SmartConsolessa uudet kohteet luotiin ***Objects***-valikossa (kuva 6), joka näkyi sovellusikkunan oikeassa reunassa. Esimerkiksi uusi verkko luodaan valitsemalla ***New...*** > ***Network...*** ja uusi palvelu valitsemalla ***New...*** > ***More*** > ***Service...*** > ***TCP...*** tai ***UDP...***



Kuva 6. Hallintatietokannan kohdevalikko (*Objects*).

R80.10-käyttöjärjestelmässä ei ole enää ***Nodes***-kohtaa, vaan yksittäisistä palvelimista ja työasemista käytetään termiä *host* (laite). Uusi laite luodaan valitsemalla ***New...*** > ***Host...***

VPN-ryhmän luonti oli hieman monivaiheisempi prosessi. Ensin oli luotava VPN-yhteyden toinen päätelaite valitsemalla ***New...*** > ***More*** > ***Network Object*** > ***More*** > ***Interoperable Device....*** ja syöttämällä ***Interoperable Device*** -ikkunassa laitteen tiedot. ***Topology***-välilehdellä valittiin ensin ***VPN-domain***-kohdassa ***Manually defined*** ja sitten valikosta oikea verkko. Tiedot hyväksyttiin ***OK***-painikkeella, minkä jälkeen siirryttiin luomaan VPN-ryhmä. VPN-ryhmä määritettiin valitsemalla ***New...*** > ***More*** > ***VPN Community...*** > ***Star Community...*** ja syöttämällä ***VPN Community*** -ikkunassa vanhan palomuuriklusterin hallintatietokannassa olleet tiedot. Vanhassa palomuuriklusterissa määritetty VPN-ryhmän topologia kävi ilmi, kun sen asetusikkuna avattiin SmartDashboardissa. Ikkunan otsikossa luki joko ***Star Community Properties*** tai ***Meshed Community Properties***.

Kun verkot, VPN-ryhmät, laitteet ja muut kohteet oli luotu ja määritetty, voitiin luoda palomuurisäännöt 5100-palomuurin hallintapalvelimessa. Uuden sääntötietokannan syntaksi oli onneksi samanlainen kuin vanhassa, joten sääntöjen luonti oli helppoa. Tässä vaiheessa ei vielä keskitytty hallintatietokannan optimointiin, sillä ensin oli selvitettävä muuttuneet IP-osoitteet ja verkot, ja lisäksi käytöstä poistettujen verkkojen ja laitteiden karsiminen hallintatietokannasta olisi edellyttänyt neuvottelua asiakkaan kanssa.

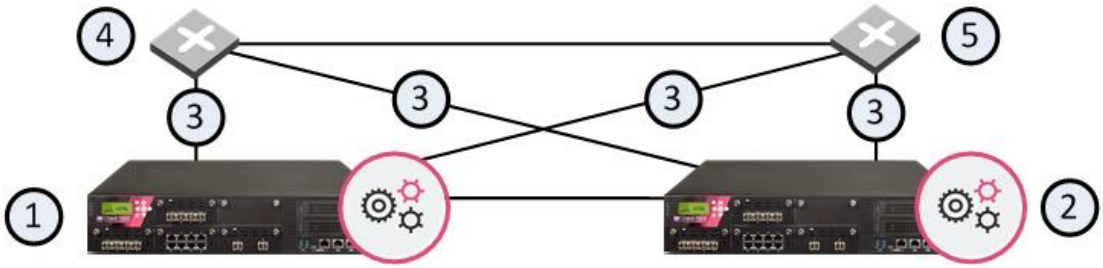
4.3 Palomuurien asennus konesaliin

Kun 5100-palomuurit siirrettiin ja asennettiin konesaliin, oli ennen niiden käynnistämistä varmistettava, että konesalin kytkimissä ei ollut sallittu liikennettä palomuureista virtuaalisiin lähiverkkoihin, jotka olivat käytössä toisen konesalin aktiivisena olevassa 4200-palomuuriklusterissa. Varmuuden vuoksi konesalien välisen yhteyden määrityksissä ei myöskään sallittu palomuurien synkronoinnissa käytettyjen virtuaalilähiverkkojen eikä asiakkaan julkisia osoitteita sisältävän verkon liikennettä. Muiden asiakkaan verkkojen liikennettä konesalien välillä ei tarvinnut rajoittaa. Lisäksi uusista palomuureista sammutettiin liitännät, joihin oli määritetty samoja osoitteita kuin mitä aktiivisessa klusterissa oli käytössä.

Palomuuriklusterille oli määritettävä sisäverkon, synkronointiverkon ja ulkoverkon IP-osoitteet, jotta klusterin muodostaminen onnistuisi. Siinä missä synkronointiverkolle riitti kaksi osoitetta, sisäverkolle ja ulkoverkolle tarvittiin kummallekin kolme IP-osoitetta, joista kaksi osoitettiin palomuurien liitäntöihin ja yksi varattiin klusterin virtuaalista IP-osoitetta varten. Tämä hankaloitti yliheittoa, sillä asiakkaan julkisessa verkossa ei ollut vapaita osoitteita eikä palomuureihin saisi yhteyttä ulkoverkosta ilman julkisia osoitteita.

Tässä tilanteessa ainoa ratkaisu olisi ollut siirtää julkisen verkon osoitteet vanhoista palomuureista uusiin, mutta näin päätettiin toimia vasta hieman ennen yliheiton suorittamista.

Tässä vaiheessa pantiin täytäntöön myös eräs vasta hetki ennen asennusta löydetty vikasietoisuutta parantava ja palomuurin fyysisiä liitäntöjä tehokkaasti hyödyntävä ratkaisu eli Check Pointin terminologian mukaan *Fully Meshed Redundancy*. Kuvasta 7 käy ilmi klusterin topologia.



Kuva 7. Esimerkki *Fully Meshed Redundancy* -topologiasta [17, s. 119].

Kuvassa numerot 1 ja 2 ovat newfw1- ja newfw2-palomuurit, numero 3 kuvaa laitteiden välistä kaapelointia sekä numerot 4 ja 5 ovat räkkikytkimiä, jotka on edelleen kytketty runkokytkimiin [17, s. 119]. Samalla kytkettiin luvussa 4.2 kuvatulla tavalla liitäntäryhmäksi yhdistetyt palomuurien LAN1- ja LAN2-liitännät eri räkkikytkimiin. Tällä tavoin haluttiin varmistaa, että HA-tilassa toimiva liitäntäryhmä jatkaa toimintaansa paitsi verkkokaapelin, liitännän tai palomuurin verkkokortin vikaantuessa myös toisen kytkimen pettäessä. Määritysten pääasiallisena tarkoituksena oli turvata palomuurien välisen synkronointiyhteyden toimivuus.

Seuraavaksi muutettiin muiden liitäntöjen osoitteita siten, että vanhan palomuuriklusterin laitteille määritettyjen verkkojen vapaana olevat IP-osoitteet tarkistettiin ja jokaisesta verkosta valittiin kaksi osoitetta uusille palomuureille ja yksi virtuaalinen osoite klusterille. Kun oli varmistuttu siitä, että 5100-palomuuriklusterin laitteet voitiin käynnistää turvallisesti ilman, että ne voisivat häiritä 4200-klusterin palomuureja, palomuurit käynnistettiin. Lisäksi lisättiin hallintatietokantaan sääntö, joka salli SSH- ja HTTPS-yhteydet palomuureihin Tietokeskuksen hallintaverkosta. Näin varmistettiin, että palomuureihin saa tarvittaessa etäyhteyden myös konesalin ulkopuolelta, jotta laitteiden hallinnointi olisi helpompaa.

5 TULOKSET

Lukuisista kokeiluista ja toimenpiteistä huolimatta opinnäytetyölle asetettuja tavoitteita ei saavutettu, vaan opinnäytetyöprojekti jäi kesken. Laitteisiin ja valmistajan oppaisiin perehtymiseen käytettiin runsaasti aikaa ja yliheittosuunnitelma oli erittäin yksityiskohtainen ja kattava. Varsinaisia virheitä valmistelussa ja toteutuksessa ei tehty, vaikka joitakin asioita olisi voinut ottaa paremmin huomioon jo suunnitteluvaiheessa. Lisäksi parempi perehtyminen Check Pointin tuotteisiin jo ennen opinnäytetyön aloittamista olisi todennäköisesti edesauttanut yliheiton saattamisessa loppuun.

Pääsyitä yliheiton eri vaiheissa koettuihin ongelmiin olivat Check Pointin kanssa solmittavan kumppanuussopimuksen rekisteröinnissä tai aktivoinnissa ilmenneet ongelmat ja käyttökelpoisten User Center- tai PartnerMAP-palvelun käyttäjätunnusten puute. Nämä seikat haittasivat niin yliheittotyökalujen, käyttöjärjestelmä- ja *hotfix*-päivitysten sekä levykuvien lataamista kuin valmistajan ohjeartikkeleiden lukemista ja syvällisempää perehtymistä Check Pointin laitteisiin sekä niiden määrityksiin.

5.1 Testauksen tulokset

Testausympäristön määrittäminen ja GAiA-käyttöjärjestelmän asentaminen virtuaalikoneisiin sujui odotetusti, mutta alusta pitäen ongelmana oli palomuurien välinen yhteys, sillä virtuaaliklusterin palomuurit eivät kyenneet muodostamaan SIC-yhteyttä eli salattua hallintayhteyttä, joka on edellytys klusterin muodostamiseen. Hallintapalvelimeen ei voinut muodostaa yhteyttä myöskään SmartDashboard-ohjelmiston avulla, jota käytetään palomuurisääntöjen hallintaan ja palomuuriklusterin muodostamiseen. Useita viikkoja kestäneen ongelmanratkaisun jälkeen, havaittiin laitevalmistajan sivuille hiljattain ilmestynyt ohjeartikkeli, jossa todettiin, että testauksessa käytettyyn GAiA-käyttöjärjestelmän levykuvaan oli jäänyt virhe. Virheen vuoksi palomuurien välisen yhteyden muodostamiseen vaadittava palomuurien sisäisen CA-sertifikaatin voimassaoloaika oli umpeutunut eikä sen päivittäminen onnistunut [31–32]. Check Point julkaisi korjauspäivityksen, ja virhe oli korjattuna myös uusimmassa GAiA-käyttöjärjestelmän levykuvassa, mutta päivityksen tai levykuvan lataaminen olisi edellyttänyt Check Point -kumppanuussopimusta ja toimivia Check Pointin User Center- tai PartnerMAP-palvelun käyttäjätunnuksia, joita ei opinnäytetyön tekohetkellä ollut.

5.2 Ongelmat palomuurien välisen hallintayhteyden muodostamisessa

Hallintatietokannan siirtäminen ei myöskään sujunut täysin ongelmitta, sillä tietokannan vienti hävitti uuden palomuuriklusterin hallintapalvelimelta kaikki aiemmat tiedot – myös laitteelle tallennetut varmuuskopiot tietokannasta, minkä ei olisi pitänyt olla mahdollista. Toinen odottamaton seuraus toimenpiteestä oli, että siirretty tietokanta korvasi palomuurin lisenssitiedot vanhojen palomuurien lisensseillä, minkä seurauksena hallintayhteys palomuurien välillä katkesi. Lisäksi SmartConsole-toimi ainoastaan *Read Only* -tilassa, joten muutosten tekeminen klusteriin tai muihin hallintatietokannan objekteihin ei onnistunut. Check Pointin *GUIDBedit*-työkalun avulla oli mahdollista muokata hallintatietokantaa ja poistaa virheelliset lisenssit, mutta hallintayhteyden muodostamiseen siitä ei ollut apua. Lopulta ainoaksi vaihtoehdoksi jäi palauttaa aktiivisena hallintapalvelimena toimiva newfw1-palomuuri tehdasasetuksiin. Koska varmuuskopiot olivat hävinneet, järjestelmäasetuksia oli muokattava käsin. Palomuuri- ja hallintaohjelmistojen uudelleenasennus onnistui, ja kun palomuuri ja hallintatietokanta olivat jälleen toiminnassa, seuraava toimenpide oli hallintayhteyden muodostaminen laitteiden välille. Tätä varten lisättiin kuvassa 8 näkyvät palomuurisäännöt, jotta kumpikaan palomuuri ei estäisi hallintayhteyden muodostamista.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1		Net_ Net_		Any	https ssh	Accept	None	
2				Any	Any	Accept	None	
3				Any	Any	Accept	None	
4			Any	Any	igmp	Accept	None	
5		Any		Any	icmp-requests	Accept	None	Policy...
6			Any	Any	ntp	Accept	None	
7	Cleanup rule	Any	Any	Any	Any	Drop	Log	Policy...

Kuva 8. Check Point 5100 -palomuurin hallintapalvelimen hallintasäännöt.

Ensin muokattiin synkronointiverkon osoitteita siten, että newfw1-palomuurin IP-osoitteeksi määritettiin xx.xxx.xxx.xxx/30 ja newfw2-palomuurin xx.xxx.xxx.xxx/30. Laitteet kytkettiin lisäksi toisiinsa ristikytkentäkaapelilla, jotta vältettäisiin synkronointiverkon liikenne palomuuriklusterien välillä. Tästä huolimatta palomuurit eivät saaneet yhteyttä toisiinsa eivätkä palomuurien välisen hallintayhteyden ongelmat ratkenneet. Lopulta useiden kokeilujen jälkeen päädyttiin tulokseen, että yhteys ei toimi, ellei palomuurien välissä ole kytkintä. Tätä kokeiltiin vaihtamalla synkronointiverkon osoitteeksi xx.xxx.xxx.xxx/29

ja palomuurien SYNC-porttien osoitteiksi xx.xxx.xxx.xxx ja xx.xxx.xxx.xxx, minkä jälkeen palomuurien väliin lisättiin kytkin, johon molemmat palomuurit kytkettiin. Kytkimen asetuksia ei muutettu, vaan kytkimenä käytettiin ei-hallittavaa kytkintä.

Heti kun kaapelit oli kytketty palomuurien ja kytkimien välille, palomuurit saivat yhteyden toisiinsa, mutta hallintayhteyden muodostaminen ei onnistunut. Tämän vuoksi nollattiin vielä SIC-tunniste, jota käytetään palomuurien välisen hallintayhteyden muodostamiseen. Nollaus tapahtui suorittamalla newfw2-palomuurin komentoriviltä expert-tilassa komennot

cp_conf sic init admin123456 norestart
cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"
cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"

sekä ottamalla SmartConsole-hallintayhteys newfw1-palomuuriin, valitsemalla hiiren oikella painikkeella **newfw2** > **Edit...** > **Communication...** > **Reset**, hyväksymällä valintaikkunan, syöttämällä newfw2-palomuuriin annetun uuden SIC-tunnisteen kohtaan **One-time password** ja valitsemalla **Initialize** [33].

Hallintayhteyden muodostaminen ei kuitenkaan onnistunut eikä laitteiden välinen synkronointi ottanut toimiakseen, vaan järjestelmä tulosti seuraavan virheilmoituksen: **Synchronization error: NGM failed to retrieve last publish time**. Virheilmoitus jäi mystiseksi, sillä tämän lisäksi ainoa johtolanka oli SIC-yhteyden muodostamisessa tulostunut virheilmoitus, jonka mukaan laitteiden välille ei ole mahdollista muodostaa TCP-yhteyttä. Kummankin klusterin palomuurin lokien läpikäynti, palveluiden uudelleenkäynnistys ja SIC:n nollaaminen uudelleen eivät kuitenkaan tuottaneet tulosta. Eräästä blogista löytyi kuitenkin kuvaus, jossa selviteltiin Check Pointin hallinnan ohjelmointirajapintaan liittyviä ongelmia [34]. Jostain syystä rajapinnan käynnistäminen uudelleen ja ***$FWDIR/scripts/cpm_status.sh***-skriptin suorittaminen kahdesti ratkaisi SIC-yhteyden muodostamiseen liittyvän ongelman ja hallintayhteyden muodostaminen palomuurien välille onnistui. Tästäkään huolimatta laitteiden välinen synkronointiyhteys ei toiminut eikä näin ollen myöskään *Management High Availability* -ominaisuus, mutta palomuurisääntöjen asentaminen molempiin palomuureihin näytti onnistuvan – tai ainakaan järjestelmä ei antanut virheilmoitusta.

Seuraavaksi kirjauduttiin SmartConsolella toiseen palomuuriin ja tarkasteltiin, miten asennetut säännöt siellä näkyvät. Yllättävää kyllä, yhtään palomuurisääntöä ei näkynyt

newfw2-palomuurin hallintatietokannassa, vaan siellä oli ainoastaan käytöstä poistettu alkusääntö, joka estää liikenteen palomuuriin. Tilanne tulkittiin niin, että hallintatietokannan siirtäminen korruptoi myös toisen palomuurin hallintapalvelimen jollain tavalla, sillä kaikki tarvittavat palvelut olivat käynnissä ja järjestelmän tietojen mukaan hallintapalvelin oli kunnossa. Kattavan vianetsinnän jälkeen lopulta myös newfw2-palomuuri palautettiin tehdasasetuksiin. Ennen palauttamista järjestelmäasetuksista otettiin varmuuskopio, ja palautuksen jälkeen koko käyttöjärjestelmä asennettiin uudelleen, ja toinen palomuuri määritettiin varahallintapalvelimeksi. Tämän jälkeen hallintayhteys toimi kuten pitikin ja myös hallintatietokannan synkronointi toimi ongelmitta palomuurien välillä. Ongelmiksi tässä vaiheessa jäivät klusteroinnin keskeneräisyys ja ajoittaiset hallintayhteyden katkokset aktiivisen palomuurin ja varalla olevan palomuurin välillä, mutta tästä huolimatta laitteet kannatti jo siirtää konesaliin.

5.3 Ongelmat lisensoinnissa ja valmistajan tukipalveluissa

Yksi opinnäytetyöprojektin etenemistä eniten haitanneista tekijöistä oli Check Pointin kanssa solmittavan palvelu- tai kumppanuussopimuksen puute. Asiaa alettiin edistää aivan opinnäytetyöprojektin alussa, koska järjestelmänvalvojilla ei ollut pääsyä Check Pointin User Center / PartnerMAP -palveluun, josta voi ladata valmistajan ohjeartikkeleita, yliheittotyökaluja tai palomuurien ohjelmistopäivityksiä. Keskusteluissa Check Pointin ja palomuurit toimittaneen tahon kanssa selvisi, että laitteisiin on olemassa viisivuotinen palvelusopimus, mutta sitä ei ole laitteissa aktivoitu. Aktivointi edellyttää, että laitteet ottavat yhteyden Check Pointin lisenssipalvelimeen, josta ne osaavat automaattisesti hakea lisenssi- ja palvelusopimustiedot. Toisin sanoen laitteiden kytkeminen Internetiin todennäköisesti korjaisi asian itsestään. Palomuureja ei kuitenkaan haluttu liittää julkiseen verkkoon ennen yliheittoa, sillä asiakkaalla ei ollut riittävästi vapaita julkisen verkon osoitteita, jotta kahdelle klusterille ja niiden jäsenille oltaisiin voitu määrittää kiinteät julkiset IP-osoitteet.

Lisenssi- ja sopimustiedot olisi kuitenkin ollut mahdollista hankkia myös offline-tilassa oleville laitteille Check Pointin käyttäjäportaalin kautta. Tätä varten Tietokeskukselle oli luotu käyttäjätunnukset User Center / PartnerMAP -palveluun mutta portaalin täysimääräinen käyttö olisi edellyttänyt kumppanuussopimusta ja sen tietojen linkittämistä luotuihin käyttäjätunnuksiin. Tämä ei onnistunut eikä ongelma ratkennut opinnäytetyöprojektin

aikana, joten suuri osa valmistajan laatimasta, palomuurien asennusta ja ylläpitoa käsittelevistä dokumentaatiosta oli ulottumattomissani.

5.4 Ongelmat palomuurien vikasietoisuudessa

Yksi valmistelun aikana havaituista ongelmista oli puutteellinen klusterointi, sillä järjestelmä ei ole vikasietoinen, jos palomuuriklusterin muodostaminen ei onnistu. Tämä ongelma saattaisi tosin ratketa itsestään, sillä Check Pointin suositusten mukaan klusterin muodostaminen edellyttää, että kummallakin klusterin palomuurilla sekä klusterilla itsellään on oltava yksi osoite niin ulkoverkossa, synkronointiverkossa kuin sisäverkossakin [17, s. 39]. Lisäksi epäiltiin, että ulkoverkon osoitteen on oltava julkinen ja sen on oltava yhteydessä Internetiin. Tämä ei tosin käynyt mistään ilmi eikä asiaa päästy testaamaan, sillä asiakkaalla ei ollut vapaita julkisen verkon IP-osoitteita.

Myöskään vikasietoisuuden parantamiseen tähdännyt liitäntäryhmä ei toiminut odotetusti, sillä laitteiden välisessä synkronointiyhteydessä ilmeni katkoksia, vaikka sääntömuutokset ja hallintatietokantaan lisätyt tiedot saatiin siirrettyä aktiiviselta laitteelta varalaitteelle. Tämäkin ongelma olisi saattanut ratketa muodostamalla palomuureista yhteyden johonkin ulkoverkon laitteeseen tai Internetiin, vaikka tälle oletukselle ei löytynytkään tukea lähteistä.

Kun kaikki vikasietoisuuteen vaikuttavat ongelmat olisi ratkaistu, palomuurien vikasietoisuus pitäisi vielä varmistaa testaamalla. Tämä onnistuisi aiheuttamalla toimivan klusterin aktiiviseen palomuuriin vikatilanne, jolloin pystyttäisiin tarkistamaan vikasietoisuuden toimivuus laiterikon tai yhteyskatkoksen sattuessa [35–37]. Tämän jälkeen olisi mahdollista jatkaa yliheittoa.

6 JOHTOPÄÄTÖKSET

Tämän opinnäytetyön tavoitteena oli asiakkaan Check Point 4200 -palomuuriklusterin yliheitto eli nykyisten palomuurien korvaaminen uudemmilla Check Point 5100 -palomuureilla ja vanhojen palomuurien tietojen siirtäminen uusiin palomuureihin. Uudet palomuurit oli myös tarkoitus asentaa eri konesaliin kuin käytössä olevan klusterin palomuurit.

Opinnäytetyön alussa perehdyttiin Check Pointin palomuurilaitteiden ominaisuuksiin sekä 4200- ja 5100-palomuurien välisiin eroihin. Valmistelu ja menetelmät -luvussa esiteltiin yliheittosuunnitelmat ja pohdittiin eri toteutusvaihtoehtoja, kun taas Toteutus-luvussa kerrottiin, mikä suunnitteluvaiheen vaihtoehdoista valittiin ja mitä toimenpiteitä yliheitossa tehtiin. Tulokset-luvussa esiteltiin toteutuneiden toimenpiteiden tulokset ja pyrittiin ratkaisemaan toteutuksen aikana ilmenneitä ongelmia.

Työn aihe vaikutti alussa hyvinkin selkeältä ja tarkkaan rajatulta, ja näytti siltä, että yliheitto saadaan hoidettua ripeästi siinä ajassa, joka projektille oli varattu. Kuten opinnäytetyöstäkin käy ilmi, työssä törmättiin melko pian lähes ylitsepääsemättömiin ongelmiin, ja lopulta yliheittoprojekti jäi kesken. Jos aikaa olisi ollut käytettävissä enemmän, yliheitto olisi todennäköisesti saatu suoritettua.

Opinnäytetyö osoitti, miten tärkeässä roolissa on laitteiden ja asiakkaan verkkoympäristön tuntemus. Vaikeudet opinnäytetyöprojektissa johtuivat osaksi kokemuksen puutteesta ja perehtymättömyydestä Check Pointin laitteiden ylläpitoon osaksi ulkoisista syistä eli palomuurien käyttöjärjestelmän virheistä ja asiakasympäristön haasteista. Lisähaasteita toivat myös puutteellinen dokumentaatio ja ennen kaikkea se, että opinnäytetyöprojektin aikana kumppanuussopimuksen tietoja ei saatu liitettyä aiemmin luotuun Check Pointin käyttäjätiliin. Viimeksi mainitun seikan vuoksi opinnäytetyö tehtiin käyttämättä Check Pointin ohjetietokantaa, yliheittotyökaluja sekä päivityksiä. Näistä lähtökohdista tarkasteltuna työn tuloksia voinee pitää hyvinä.

Aihetta käsittelevän tai sivuavan tutkimuskirjallisuuden puute yllätti. Tämä johtuu luultavasti siitä, että yliheitot ovat keskenään hyvinkin erilaisia eikä kovinkaan yksityiskohtaisia ohjeita ole edes mahdollista antaa. Laitteisto määritetään aina sen verkkoympäristön mukaan, johon se on asennettu, ja aihetta koskeva dokumentaatio koostuu järjestelmien ylläpitäjille suunnatuista, yritysten sisäisistä asiakirjoista tai sitten se on konsulttien ja palveluntarjoajien käytössä. Tällainen dokumentaatio kuuluu liikesalaisuuden piiriin, sillä

esimerkiksi palomuurisäännöt, käytössä olevat verkot, protokollat, ohjelmistot ja niitä varten avatut portit ovat arkaluontoista tietoa.

Vaikka yliheiton testaaminen virtuaaliympäristössä ei onnistunut, siitä saadut tulokset olivat hyödyllisiä. Asiakas oli tyytyväinen siihen, että verkkokuvaukset ja dokumentaatio oli saatettu ajan tasalle, ja toimeksiantajalle oli uutta verkkosimulaattorin käyttö testaustyökaluna. Modernit verkkosimulaattorit ovat monipuolisia, ja niihin on saatavana runsaasti valmiiksi määritettyjä malleja eri laitteiden simulointia varten, joten niiden käyttö varsinkin kriittisten laitteiden tai haastavissa ympäristöissä suoritettavien yliheittojen testaamiseen olisi perusteltua.

Koska kahta täysin samanlaista ympäristöä ei ole, tämän opinnäytetyön tulokset eivät ole suoraan sovellettavissa kuin Check Pointin palomuurien yliheittotilanteisiin tai ylläpitotoimenpiteisiin. Yleisohjeena voi kuitenkin sanoa, että yliheitto on mittava prosessi, joka on suunniteltava ja dokumentoitava huolellisesti. Suositeltavaa on myös yliheiton simulointi tai edes korvaavien laitteiden testaaminen tuotantoympäristöstä erillään olevassa ympäristössä.

Yliheiton jatkaminen edellyttäisi, että kumppanuussopimus- ja lisenssiasiat saadaan kuntoon Check Pointin kanssa. Sen jälkeen 5100-palomuureihin voidaan asentaa uusimmat päivityspaketit, ja niiden toimivuus testataan fyysisistä palomuureista ja virtuaalikoneista koostuvassa hybridiympäristössä. Testauksen jälkeen voidaan sopia asiakkaan kanssa ajankohta yliheitolle ja viimeistellä yliheitto opinnäytetyössä esitellyn suunnitelman mukaisesti. Mikäli sopimus- ja lisenssiasiat eivät etene, toinen vaihtoehto olisi korvata Check Pointin palomuurit toisen laitevalmistajan laitteilla ja käyttää toisen laitevalmistajan yliheittotyökaluja hallintatietokannan siirtämiseen korvaaviin palomuureihin. Jälkimmäinen vaihtoehto voi olla järkevä myös tilanteessa, jossa toisen laitevalmistajan palomuurien asentaminen ja ylläpito koetaan helpommiksi kuin Check Pointin laitteiden.

Jos yliheitto suoritetaan loppuun tässä opinnäytetyössä kuvatulla tavalla, yliheiton jälkeen tarkkaillaan 5100-klusterin palomuureja, liikennemääriä sekä palomuurisääntöjen käyttöä SmartConsolen osumalaskurin (*hit counter*) ja pakettienvalvontaominaisuuden avulla. Kerättyjen tietojen perusteella saadaan selville, onko hallintatietokannassa käyttämättömiä sääntöjä, VPN-yhteyksiä, verkkoja, laitteita tai portteja. Poistettavista tiedoista kerätään luettelo, joka lähetetään asiakkaalle hyväksyttäväksi. Kun turhat tiedot on poistettu, klusterin palomuurien toimintaa voidaan tehostaa järjestämällä palomuurisäännöt Check Pointin parhaat käytännöt -ohjeistuksen mukaisesti [38]. Lisäksi on

syytä laatia kattava varmuuskopiointisuunnitelma luvussa 3.2.2 annettujen ohjeiden mukaisesti, ja ottaa samalla GAiA Portal (WebUI) -käyttöliittymässä käyttöön ajastettu varmuuskopiointi, jossa tärkeimmät palomuurin ja hallintapalvelimen tiedot siirretään automaattisesti konesalin hallintakoneelle. Näin voidaan varautua myös tilanteisiin, joissa kummankaan palomuurin hallintatietokanta ei ole enää toimintakuntoinen.

LÄHTEET

[1] Check Point Software Technologies Ltd. *How does the Cluster Control Protocol function in working and failure scenarios for gateway clusters?*. [Verkkodokumentti]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/5990/FILE/sk31085_Cluster_Control_Protocol_Functionality.pdf.

[2] Check Point Software Technologies Ltd. *Security Management Server R76 Administration Guide – The Internal Certificate Authority*. [Verkkodokumentti]. 2016. [Viitattu 30.11.2018]. Saatavissa: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/13118.

[3] Steven Thomason. Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices. *Global Journal of Computer Science and Technology – Network, Web & Security*, 2012. Volume 12 Issue 13 Version 1.0. S. 47–50. ISSN 0975-4172 (verkkoversio). ISSN 0975-4350 (painettu).

[4] Alex X. Liu. *Firewall Design and Analysis*. Singapore: World Scientific Publishing Co Pte Ltd, 2010. 122 s. (Computer and Network Security – Vol. 4). ISBN-13 978-981-4261-65-4.

[5] Check Point Software Technologies Ltd. *"Max Power" Book Second Edition Released!*. [Verkkosivu]. Check Point CheckMates, 2018. [Viitattu 30.11.2018]. Saatavissa: https://community.checkpoint.com/message/28012-re-max-power-book-second-edition-released?commentID=28012#comment-28012.

[6] Check Point Software Technologies Ltd. *How to install Full HA cluster on Check Point appliances*. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk60443.

[7] Check Point Software Technologies Ltd. *Release Notes R80.10*. 2018.

[8] Check Point Software Technologies Ltd. Best Practices - Backup on Gaia OS. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902.

[9] Check Point Software Technologies Ltd. *Installation and Upgrade Guide R80.10*. 2017.

[10] Check Point Software Technologies Ltd. *Gaia Installation and Upgrade Guide R77*. 2018.

[11] Check Point Software Technologies Ltd. *Security Management Server Administration Guide R77 Versions*. 2016.

[12] Check Point Software Technologies Ltd. *File transfer from Gaia system to Gaia system over SCP fails with various errors*. [Verkkosivu]. 2018. [Viitattu 27.3.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk93085.

[13] Check Point Software Technologies Ltd. *HowTo - Creating an scpuser account on Gaia Clish. [Verkkosivu].* Check Point CheckMates, 2018. [Viitattu 30.11.2018]. Saatavissa: https://community.checkpoint.com/thread/5574-howto-creating-an-scpuser-account-on-gaia-clish.

[14] Check Point Software Technologies Ltd. *Backing up Gaia system level configuration*. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk102234.

[15] Check Point Software Technologies Ltd. *Gaia R76 Administration Guide – Introduction to the Command Line Interface*. [Verkkodokumentti]. 2014. [Viitattu 30.11.2018]. Saatavissa: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/75697.htm#o110107.

[16] Check Point Software Technologies Ltd. *Connecting multiple clusters to the same network segment (same VLAN, same switch)*. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk25977.

[17] Check Point Software Technologies Ltd. *ClusterXL Administration Guide R80.10*. 2018.

[18] Check Point Software Technologies Ltd. *How to check for connected SmartConsole administrators on a Smart Management Server / SmartCenter server*. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk59102.

[19] CPUG: The Check Point User Group. *Migrate Cluster 77.30 appliance to new 80.10 cluster applliance (Replace)*. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://www.cpug.org/forums/showthread.php/22325-Migrate-Cluster-77-30-appliance-to-new-80-10-cluster-applliance-%28Replace%29.

[20] Check Point Software Technologies Ltd. *Support Life Cycle Policy – Appliances Support*. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://www.checkpoint.com/support-services/support-life-cycle-policy/.

[21] Check Point Software Technologies Ltd. *R77 Release Notes*. 2014.

[22] Check Point Software Technologies Ltd. *Management High Availability restrictions*. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk39345.

[23] Check Point Software Technologies Ltd. *Gaia R77 Versions Installation and Upgrade Guide*. [Verkkodokumentti]. 2018. [Viitattu 27.3.2018]. Saatavissa: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/120709.

[24] Check Point Software Technologies Ltd. *How to get installed hotfix versions using CPInfo*. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk83860.

[25] Check Point Software Technologies Ltd. *Jumbo Hotfix Accumulator for R80.10 (R80_10_jumbo_hf)*. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk116380.

[26] Check Point Software Technologies Ltd. *"Cannot export snapshot, insufficient space in /var/log/." error when exporting a snapshot in Gaia Portal / Gaia Clish*. [Verkkosivu]. 2018. [Viitattu 25.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk115144.

[27] Check Point Software Technologies Ltd. *When running a saved configuration file, configuration does not complete as expected (or completes with errors)*. [Verkkosivu]. 2018. [Viitattu 4.12.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk107286.

[28] Check Point Software Technologies Ltd. *No connectivity over VLAN interfaces configured on a Bond interface on Check Point Security Gateway*. [Verkkosivu]. 2018. [Viitattu 25.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120684.

[29] Check Point Software Technologies Ltd. *Using VLAN on cluster Sync interfaces*. [Verkkosivu]. 2018. [Viitattu 25.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk34574.

[30] Check Point Software Technologies Ltd. *VPN R77 Versions Administration Guide – Introduction to VPN*. [Verkkodokumentti]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_VPN_AdminGuide/13894.

[31] Check Point Software Technologies Ltd. *Connectivity between SmartDashboard / SmartDomain Manager and Security Management / Multi-Domain Management Server R77.30 and below fails on fresh installation*. [Verkkosivu]. 2018. [Viitattu 30.11.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122612.

[32] Check Point Software Technologies Ltd. *Cannot Connect with SmartConsole to R77.30 or Earlier Management*. [Verkkosivu]. Check Point CheckMates, 2018. [Viitattu 30.11.2018]. Saatavissa: https://community.checkpoint.com/thread/6863-connection-cannot-be-initiated-please-make-sure.

[33] Check Point Software Technologies Ltd. *My Top 3 Check Point CLI commands*. [Verkkosivu]. Check Point CheckMates, 2018. [Viitattu 4.12.2018]. Saatavissa: https://community.checkpoint.com/thread/5319-my-top-3-check-point-cli-commands.

[34] Dhansham - Engineer's Notebook Checkpoint Firewalls Gaia. *R80.10 API – Troubleshooting*. [Verkkosivu]. 2018. [Viitattu 4.12.2018]. Saatavissa: http://dkcheckpoint.blogspot.fi/2018/02/r8010-api-troubleshooting.html.

[35] Expert Mode. *CheckPoint HA: How to force a failover (ClusterXL/VRRP)*. [Verkkosivu]. 2012. [Viitattu 5.4.2018]. Saatavissa: http://expert-mode.blogspot.fi/2012/06/checkpoint-ha-how-to-force-failover.html.

[36] FW Knowledge. *Manual Failover of the FW Cluster*. [Verkkosivu]. 2013. [Viitattu 5.4.2018]. Saatavissa: https://fwknowledge.wordpress.com/2013/04/04/manual-failover-of-the-fw-cluster/.

[37] Packet Pushers. *How To Force Failover / Failback of Check Point Cluster Members*. [Verkkosivu]. 2010. [Viitattu 5.4.2018]. Saatavissa: http://packetpushers.net/how-to-force-failover-failback-of-check-point-cluster-members.

[38] Check Point Software Technologies Ltd. *Best Practices - Rulebase Construction and Optimization*. [Verkkosivu]. 2018. [Viitattu 3.12.2018]. Saatavissa: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk106597.