

Joni Louhelainen

Asiakaskäytössä olevan palomuurialustan vaihto

Insinööritö 27.4.2009

Ohjaaja: manager Jani Anttila

Ohjaava opettaja: lehtori Erik Pätynen

Tekijä Otsikko	Joni Louhelainen Asiakaskäytössä olevan palomuurialustan vaihto
Sivumäärä Aika	48 sivua 27.4.2009
Koulutusohjelma	tietotekniikka
Tutkinto	insinööri (AMK)
Ohjaaja Ohjaava opettaja	manager Jani Anttila lehtori Erik Pätynen
<p>Insinöörit­yössä vaihdetaan Capgemini Finland Oy:n palomuurialusta, jossa toimii virtualisoituina asiakkaiden palomureja, toiselle alustalle. Nykyinen palomuurialusta, Nokia IP1220 -palomuu­ri, on tarkoitettu laitteistoksi varsinaiselle palomuuriohjelmistolle Check Point VPN-1/FireWall-1 VSX:lle. Uudeksi palomuurialustaksi valittiin Juniper ISG1000 -palomuu­ri ilman kolmannen osapuolen palomuuriohjelmistoja.</p> <p>Työssä asiakkaiden virtualisoidut palomuurit vaihdetaan uudelle palomuurialustalle yksi kerrallaan. Työtä varten perustettiin työryhmä, jonka jäsenien kesken asiakkaat jaettiin. Palomuurialustan vaihto on kokonaisuudessaan ryhmätyö, vaikka työ varsinaisesti tehdään asiakaskohtaisesti itsenäisesti. Vaihdon työt jakaantuvat valmistelu- ja toteutusvaiheisiin, joista suurin työ tehdään valmisteluvaiheessa. Valmisteluvaiheessa mm. suunnitellaan asiakkaan uusi palomuuriympäristö uudelle alustalle, piirretään uudet verkkokuvat, luodaan uudet sääntökannat uudelle alustalle sekä valmistaudutaan varsinaiseen toteutukseen. Kattavien valmistelujen myötä varsinaiset toteutukset, eli asiakkaiden virtuaalisten palomuurien vaihdot uudelle alustalle, ovat onnistuneet toistaiseksi hyvin.</p>	
Hakusanat	palomuu­ri, Nokia, IP1220, Check Point, Juniper, ISG1000

Author Title	Joni Louhelainen Changing a customer's firewall platform
Number of Pages Date	48 27 April 2009
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Instructor Supervisor	Jani Anttila, Manager Erik Pätynen, Lecturer
<p>In this thesis the Capgemini Finland Oy's firewall platform, where clients' virtualized firewalls reside, will be changed for another platform. The current firewall platform, Nokia IP1220 -firewall, is meant to be hardware for the actual firewall software Check Point VPN-1/FireWall-1 VSX. The new firewall platform is Juniper ISG1000 without any third party firewall software.</p> <p>The clients' virtualized firewalls will be changed for the new firewall platform one at a time. For the task a work group was created and the clients were assigned to different members of the group. The changing of the platform is group work as general, although the work is done independently for every customer. The work of the change is split into a preparation and implementation phase, where most of the work is done in the preparation phase. The work in the preparation phase includes planning the client's firewall environment for the new platform, drawing the new network diagrams, creating the policies for the new platform and preparing for the implementation. With inclusive preparations, the implementations, which is changing the platform of the the clients' virtual firewalls, have been done well so far.</p>	
Keywords	firewall, Nokia, IP1220, Check Point, Juniper, ISG1000

Lyhenteet, käsitteet ja määritelmät

3DES	<i>Triple Data Encryption Standard</i> . Salausmenetelmä, jota käytetään tietotekniikassa. Kehittyneempi versio DES-salausmenetelmästä.
AES	<i>Advanced Encryption Standard</i> . Lohkosalausmenetelmä, jota käytetään tietotekniikassa.
ASIC	<i>Application-Specific Integrated Circuit</i> . Integroitu piiri, joka on mukautettu tiettyä käyttöä varten.
BGP	<i>Border Gateway Protocol</i> . Reititysprotokolla, joka on mm. Internetin tärkein reititysprotokolla.
CLI	<i>Command-Line Interface</i> . Komentopohjainen käyttöliittymä esim. ohjelmiston hallintaan.
CLM	<i>Customer Log Module</i> . Check Pointin Provider-1 -ratkaisun komponentti yksittäisen palomuurin lokitiedostoille, jota säilytetään MLM:llä. Sisältää palomuurien keräämät lokit.
CMA	<i>Customer Management Add-on</i> . Check Pointin Provider-1 -ratkaisun komponentti yksittäisen palomuurin virtuaaliselle hallintakoneelle, jota säilytetään MDS:llä. CMA:n kautta voidaan muokata esim. sääntöjä asiakkaan palomuurille.
DES	<i>Data Encryption Standard</i> . Salausmenetelmä, jota käytetään tietotekniikassa.
DHTML	<i>Dynamic HTML</i> . Termi erilaisille tekniikoille, joilla mm. lisätään interaktiivisuutta ja animaatioita staattisille HTML-sivustoille.
DIP	<i>Dynamic IP</i> . Juniperin palomuuressa käytetty metodi lähdeosoitteen muuntamiseen.
EVR	<i>External Virtual Router</i> . Check Point -palomuurin käyttämä virtuaalinen reititin.
FreeBSD	BSD-Unixiin perustuva vapaa käyttöjärjestelmä.
FTP	<i>File Transfer Protocol</i> . Tiedonsiirtoprotokolla.
GUI	<i>Graphical User Interface</i> . Graafinen käyttöliittymä esim. ohjelmiston hallintaan.

HotSwap	HotSwap-termillä tarkoitetaan tekniikkaa, jolla voidaan vaihtaa järjestelmän komponentteja sammuttamatta itse järjestelmää.
HSRP	<i>Hot Standby Router Protocol</i> . Ciscon omistama protokolla, jolla edistetään varmennetun järjestelmän viansietokykyä luomalla virtuaalinen yhdyskäytävän osoite, jota kautta liikenne kulkee, vaikka jokin varmentavista laitteista viottuisi.
ICMP	<i>Internet Control Message Protocol</i> . Kontrolliprotokolla, jolla voidaan lähettää erilaisia viestejä esim. yhteyden testaamista varten.
IDP	<i>Intrusion Detection & Prevention</i> . Järjestelmä, joka havaitsee ja suojaa verkkoon suuntautuvia hyökkäysyrityksiä.
IKE	<i>Internet Key Exchange</i> . Avaimenvaihtoprotokolla salattujen yhteyksien neuvotteluun sekä autentikointiin.
IP	<i>Internet Protocol</i> . Internet-protokolla.
IPSec	<i>IP Security Architecture</i> . Sisältää tietoliikenneprotokollia Internet-yhteyksien turvaamiseen.
IPSO	Nokian käyttöjärjestelmä, jota käytetään mm. Nokian palomuuressa. Perustuu FreeBSD-käyttöjärjestelmään.
ISG	<i>Integrated Security Gateway</i> . Juniperin palomuurimallisto suuremmille yritysille ja konesaliverkoille.
IVR	<i>Internal Virtual Router</i> . Check Point -palomuurin käyttämä virtuaalinen reititin.
MD5	<i>Message-Digest algorithm 5</i> . Kryptografiassa käytetty algoritmi, jolla luodaan 128-bittisiä tiivistettä.
MDG	<i>Multi-Domain GUI</i> . Check Pointin Provider-1 -ratkaisun käyttöliittymä usean palomuurin hallintaan.
MDS	<i>Multi-Domain Server</i> . Check Pointin Provider-1 -ratkaisun yksi pääkomponenteista. Palvelin, joka pitää sisällään CMA:t eli palomuurien virtuaaliset hallintakoneet.
MIP	<i>Mapped IP</i> . Juniperin palomuuressa käytetty metodi kohdeosoitteen muuntamiseen.
MLM	<i>Multi-Domain Log Module</i> . Check Pointin Provider-1 -ratkaisun yksi pääkomponenteista. Palvelin, joka pitää sisällään CLM:t eli lokitiedot.

NAT	<i>Network Address Translation</i> . Internet-tekniikka, jolla voidaan muuntaa IP-osoitteita.
NAT-DST	Juniperin palomuuureissa käytetty metodi kohdeosoitteen muuntamiseen.
NAT-SRC	Juniperin palomuuureissa käytetty metodi lähdeosoitteen muuntamiseen.
NSM	<i>Network Security and Manager</i> . Ent. Netscreen Security Manager. Juniperin valmistama hallintasovellus, jolla voidaan hallita useita fyysisiä sekä virtuaalisia palomuuureja keskitetysti.
PAT	<i>Port Address Translation</i> . Internet-tekniikka, jolla voidaan muuntaa yhteyksissä käytettäviä porttinumeroita.
PCI	<i>Peripheral Component Interconnect</i> . Tietokoneväylä, jonka avulla tietokoneisiin saadaan liitettyä lisälaitteita.
PCMCIA	<i>Personal Computer Memory Card International Association</i> . Tietokoneen laajennuskorttipaikan tyyppi.
PMC	<i>PCI Mezzanine Card</i> . PCI-kortin tapainen lisälaittekortti, joka asennetaan tietokoneen emolevylle vertikaalisesti.
PPU	<i>Packet Processing Unit</i> . Juniperin ohjelmoitavissa oleva mikroprosessori.
ScreenOS	Juniperin käyttöjärjestelmä, jota käytetään mm. Juniperin palomuuureissa.
SHA-1	<i>Secure Hash Algorithm</i> . Kryptografiassa käytetty algoritmi, jolla luodaan tiivisteitä.
SSH	<i>Secure Shell</i> . Verkkoprotokolla, jonka avulla saadaan siirrettyä tietoa turvallisesti kahden verkossa olevan laitteen välillä.
SSL	<i>Secure Sockets Layer</i> . Salausprotokolla, jolla voidaan suojata Internet-sovelluksien tietoliikennettä.
STP	<i>Spanning Tree Protocol</i> . Protokolla silmukoiden estämiseen kahdennetuissa ympäristöissä.
TCP	<i>Transmission Control Protocol</i> . Tietoliikenneprotokolla.
U	Laitetelineen mittayksikkö, jolla kerrotaan laitteen korkeus, joka on tarkoitettu asennettavaksi 19- tai 23-tuuman laitetelineeseen. 1 U on korkeudeltaan 44,45 mm.

VIP	<i>Virtual IP.</i> Juniperin palomuuressa käytetty metodi kohdeosoitteen muuntamiseen.
VLAN	<i>Virtual LAN.</i> Virtuaalilähiverkko, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin.
VPN	<i>Virtual Private Network.</i> Tapa, jolla voidaan yhdistää eri verkkoja keskenään julkisen verkon esim. Internetin yli.
VRF	<i>Virtual Routing and Forwarding.</i> Tekniikka, jolla saadaan muodostettua samalle reitittimelle useita eri reititystauluja.
VRRP	<i>Virtual Router Redundancy Protocol.</i> Protokolla, jolla edistetään varmennetun järjestelmän viansietokykyä luomalla virtuaalinen yhdyskäytävän osoite, jota kautta liikenne kulkee, vaikka jokin varmentavista laitteista viottuisi.
VS	<i>Virtual Systems.</i> Check Pointin virtuaalinen palomuuuri. Toimii kuten normaali palomuuuri.
VSX	Lyhenne Check Pointin virtuaalipalomuuri-ohjelmistolle Check Point VPN-1/FireWall-1 VSX:lle.
VSYS	<i>Virtual Systems.</i> Juniperin virtuaalinen palomuuuri. Toimii kuten normaali palomuuuri.
WebUI	Web-pohjainen käyttöliittymä esim. ohjelmiston hallintaan.

Sisällys

Tiivistelmä

Abstract

Lyhenteet, käsitteet ja määritelmät

1 Johdanto	9
2 Palomuurialustojen esittely	9
2.1 Nykyinen palomuurialusta, Nokia IP1220	10
2.1.1 Palomuurialustan kokoonpano	11
2.1.2 Check Point -ohjelmisto	12
2.1.3 Palomuurialustan hallintasovellukset	13
2.1.4 Palomuurialustan virtualistointi Check Pointin VSX-ohjelmistolla	16
2.2 Tuleva palomuurialusta, Juniper ISG1000	17
2.2.1 Palomuurialustan kokoonpano	18
2.2.2 Palomuurialustan pääkomponentit	19
2.2.3 Pakettien kulku palomuurialustan läpi	20
2.2.4 Palomuurialustan hallintasovellukset	22
2.2.5 Palomuurialustan virtualistointi	23
3 Konesali- ja asiakasverkkojen esittely	25
3.1 Konesaliverkon runko ja sen toiminnallisuus	25
3.2 Asiakasverkon toiminnallisuus	28
3.2.1 Yhteydet asiakasverkosta ulospäin	30
3.2.2 Asiakasverkko Nokian palomuurialustalla	30
3.2.3 Asiakasverkko Juniperin palomuurialustalla	32
3.2.4 Sisäverkon ja VSYS:n välinen eteinen	33
4 Asiakkaan palomuurialustan vaihto	35
4.1 Valmistelut palomuurialustan vaihtoa varten	35
4.1.1 Valmistelut uusia linkkiverkkoja varten	35
4.1.2 Uuden verkkokuvan ja VSYS:n luonti	36
4.1.3 Sääntöjen luonti asiakkaan VSYS:lle	37
4.1.4 NAT-säännöt yleisesti ja niiden luonti asiakkaan VSYS:lle	39
4.1.5 Reititykset asiakkaan VSYS:llä	41
4.2 Testaus	42
4.3 Toteutus	43
5 Yhteenveto	45
Lähteet	46

1 Johdanto

Tämä insinöörityö on kooste Capgemini Finland Oy:n sisäisestä palomuuriprojektista, jossa tarkoituksena on vaihtaa asiakaskäytössä oleva palomuurialusta kokonaan nykyiseltä alustalta toiselle. Vaihdeettavalla palomuurialustalla toimii virtuaalisesti useita eri asiakkaiden palomuuureja, jotka ovat käytössä heidän omissa verkoissaan ja toimivat niissä palomuurin lisäksi asiakkaiden verkkojen omina reitittiminä. Palomuurialusta on lähes kaikkien asiakkaiden verkkojen keskipiste, jota kautta heidän tietoliikenteensä pääasiallisesti kulkee.

Insinöörityössä käydään aluksi läpi nykyinen ja tuleva palomuurialusta toimintoiheen ja hallintasovelluksineen. Laite-esittelyjen jälkeen esitellään Capgeminin konesali- ja asiakasverkkoja, jotta lukijalle muodostuisi kuva, kuinka asiakkaiden yhteydet toimivat ja kuinka palomuurialustan vaihto ylipäänsä vaikuttaa asiakkaiden verkkoihin. Yleisen verkkoesittelyn jälkeen paneudutaan itse palomuurialustan vaihdon työvaiheisiin aina valmistelusta itse vaihtoon.

2 Palomuurialustojen esittely

Capgeminin pääasiallisena palomuurialustana asiakkaiden palomuuureille toimii Nokia IP1220 -palomuri. Palomuurialustoja on kaksi kappaletta redundanttisuuden takia. Ne ovat kahdennettu aktiivi-passiivimenetelmällä. Tällä menetelmällä vain toinen palomuurialusta on aktiivinen eli toisen palomuurialustan vikaantuessa liikenne siirtyy automaattisesti kulkemaan toisen palomuurialustan kautta. Kuormanjakoa ei näin ollen toteuteta palomuurialustojen kesken. Asiakkaiden palomuurit toimivat virtuaalisina palomuurialustalla, joten lähes jokaisella asiakkaalla on oma eristetty palomuri käytössä.

Palomuurialustan vaihto tuli ajankohtaiseksi, sillä nykyisen Nokia IP1220 -palomuurin suorituskyky ei enää riitä vastaamaan nykyisiä tarpeita. Palomuurialustan kautta kulkeva liikenne on vuosien myötä kasvanut niin suureksi, että uusien virtuaalimuurien

luominen palomuurialustalle ei ole enää suositeltavaa. Lisäksi uusien virtuaalimuurien lisenssit ovat huomattavasti kalliimpia kuin muiden valmistajien vastaavat. Joka tapauksessa uusia virtuaalimuureja varten olisi pitänyt vaihtaa koko palomuurialusta. Jos uudeksi palomuurialustaksi olisi valittu uudempi malli Nokialta, kustannuksia olisi tullut palomuurialustan hankinnan ja edellä mainittujen lisenssimaksujen lisäksi myös Nokialla ajettavan palomuuriohjelmiston päivityksestä. Nokian palomuurialustalla toimii kolmannen osapuolen palomuuriohjelmisto.

Uudeksi palomuurialustaksi valittiin Juniperin valmistama ISG1000-palomuuri, joka on hankinta-, huoltosopimus- ja lisenssikustannuksineen huomattavasti halvempi kuin Nokian palomuurit Check Point -ohjelmistoineen. Lisäksi ISG1000-palomuurin suorituskyky on todettu suoriutumaan helposti nykyisestä liikennemäärästä. Se sisältää myös kasvuvaraa uusia virtuaalimuureja varten. Nämä Juniperin palomuurit, joita Nokian tapaan on kaksi kappaletta redundanttisuuden takia, ovat jo toiminnassa Capgeminin konesalissa. Tähän työhön ei sisälly uuden palomuurialustan asennus eikä konfigurointi.

2.1 Nykyinen palomuurialusta, Nokia IP1220

Capgeminiillä on vielä toistaiseksi käytössä asiakkaiden palomuurialustana kaksi Nokia IP1220 -palomuuria, jotka muodostavat keskenään kahdennetun klusterin. Nokia esitteli tämän mallin markkinoille 24.5.2004. Palomuurit toimivat alustana kolmannen osapuolen, Check Pointin, valmistamalle VPN-1/Firewall-1 -ohjelmistolle, joka hoitaa varsinaisen palomuurin työn. Keskitettyyn hallintaan Capgeminiillä käytetään Check Pointin Provider-1 -ratkaisua, jolla pystyy keskitetysti hallinnoimaan kaikkia Check Pointin muureja, sekä fyysisiä että virtuaalisia.

Check Point ilmoitti 22.12.2008 allekirjoittaneensa sopimuksen, jolla se saa haltuunsa Nokian tietoturvalaiteliiketoiminnan. Näin ollen Nokian palomuurit kuuluvat nykyään Check Pointille. [1.]

2.1.1 Palomuurialustan kokoonpano

Nokia IP1220 on perinteinen laitetelineeseen asennettava laitteistopohjainen palomuuuri, joka tehokkuudellaan vastaa suurten yritysten ja palveluntarjoajien tarpeisiin.

Käytännössä laite on pitkälti kuin normaaliin työasemakäyttöön tarkoitettu tietokone, jonka komponentit ovat tarkkaan valittu tarkoitukselleen sopivaksi. Käyttöjärjestelmänä laitteessa toimii Nokia IPSO, joka perustuu räätälöityyn FreeBSD-käyttöjärjestelmään. Suhteellisen vapaasti konfiguroitavan käyttöjärjestelmänsä myötä palomuruuriin voi asentaa kolmannen osapuolen ohjelmistoja kuten Check Pointin, joita on saatavilla myös muun muassa Windows-pohjaisiin työasemiin. [2; 3.]

Peruskokoonpanolla Nokia IP1220 -palomuuuri sisältää yhden gigatavun muistia, joka on laajennettavissa kahteen gigatavuun asti, sekä neljä integroitua 10 / 100 megabitin verkkoliitäntää. Peruskokoonpano on kuitenkin helposti laajennettavissa muistin lisäksi myös PCMCIA-korteilla, joille palomuuuri tarjoaa kaksi paikkaa tyyppi II:n kortteja varten. Näiden lisäksi palomuruuriin saa verkkojen kasvaessa lisää verkkoliitäntöjä PMC-korteilla, joita laitteeseen saa asennettua neljä kappaletta. Näillä laajennuskorteilla palomuruuriin saa vaikka 20 kappaletta 10 / 100 megabitin verkkoliitäntää tai vaihtoehtoisesti kahdeksan 1000 megabitin liitäntää. [3.]

PMC on lyhenne sanoista PCI mezzanine card, ja se on yksinkertaisuudessaan PCI-kortti, joka asennetaan laitteen emolevyille vertikaalisesti, toisin kuin normaaleissa pöytäkoneissa, joissa PCI-kortti asennetaan pystysuoraan emolevyyn nähden. Tällä asettelulla säästetään laitteen korkeudessa, jolla taas säästetään tilaa konesalin laitetelineissä. PMC-korttien ansiota Nokia IP1220 -palomuuuri on vain 2 U korkea. U on laitetelineyksikkö, jolla ilmoitetaan laitteen korkeus, joka on tarkoitettu asennettavaksi 19- tai 23-tuuman laitetelineisiin. 1 U on korkeudeltaan 44,45 mm jolloin 2 U on 88,90 mm korkea. Nokian tuotetiedoissa laitteelle on merkitty korkeudeksi 2 U:n lisäksi 8,79 cm. [3; 5, s. 10; 6.]

Laajennettavuuden lisäksi Nokia IP1220 -palomuuuri hallitsee kahdentamisen useilla eri tasoilla. Itse palomuurin kahdennus verkkokäyttöön on tuettu Nokia IPSO -käyttöjär-

jestelmässä VRRP:llä (Virtual Router Redundancy Protocol). VRRP vastaa Ciscon HSRP:tä (Hot Standby Router Protocol), jolla luodaan yksi yhteinen osoite virtuaaliselle yhdyskäytävälle useille eri laitteille. Sama yhdyskäytävän osoite toimii edelleen normaalisti, vaikka jokin VRRP:n takana olevista laitteista hajoaisi. VRRP:n lisäksi Nokia IPSO tarjoaa laitteiden kahdentamiseen Nokia IP Clusteringia, joka on toteutettu VRRP:n päälle ja joka tuo mukanaan virtuaalisen yhdyskäytävän osoitteen lisäksi muun muassa kuormanjaon, joka jakaa liikennettä laitteiden kesken. VRRP:n ja Nokia IP Clusteringin lisäksi palomuuuri tukee laitetasolla HotSwap-tekniikkaa, eli komponentti voidaan sekä poistaa että korvata laitteen ollessa toiminnassa. Tekniikka on tuettu edellä mainituille PMC-korteille, virtayksikölle ja tuulettimelle sekä peilatuille kovalevyille. Palomuuuri tukee kovalevyjen peilausta, jolla varmistetaan tietojen säilyvyys ja tuotannon jatkuvuus, jos toinen kovalevy hajoaa. [3; 7; 8.]

Tietojen tallentamisessa Nokia IP1220 -palomuuuri tukee konfigurointien tallennukseen kovalevy- tai flash-muistiin pohjautuvaa tallennusta. Palomuuria voidaan käyttää myös hybriditilassa, jolloin molemmat mediat ovat käytössä. Tässä tilassa palomuuuri käyttää flash-muistia Nokia IPSO -käyttöjärjestelmälle sekä Check Pointin ohjelmistoille, jolloin kovalevy jää käyttöön muun muassa konfiguraatio- ja lokitiedostoille. [3.]

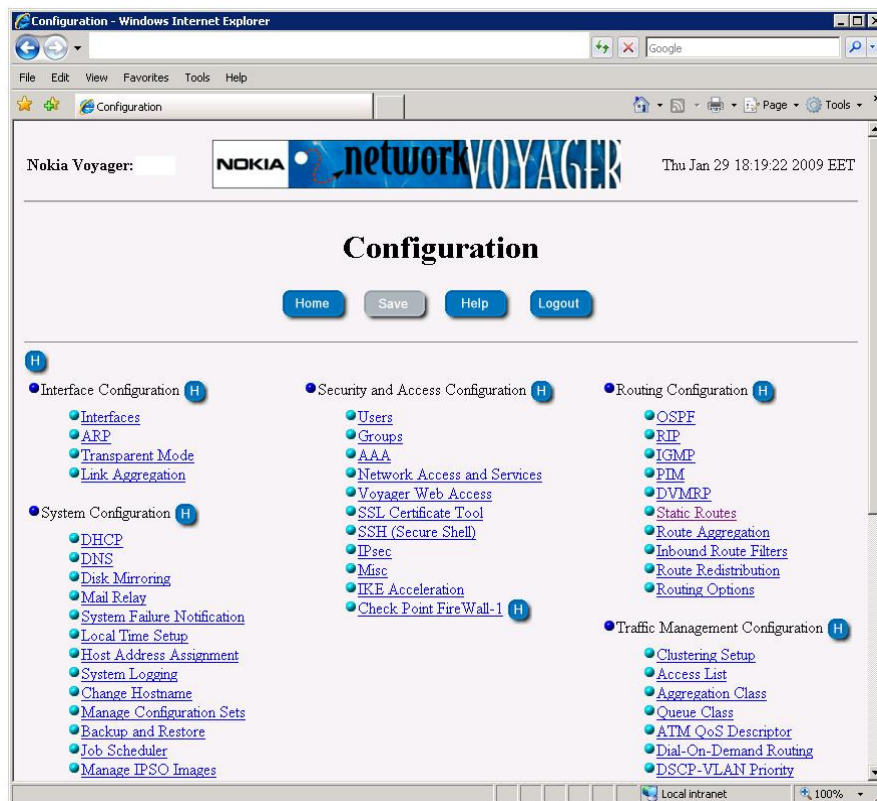
2.1.2 Check Point -ohjelmisto

Koska Nokia IP1220 palomuurissa on joustava käyttöjärjestelmä ja laitteisto, voidaan siihen asentaa kolmannen osapuolen ohjelmia aivan kuten esimerkiksi normaaleihin Windows-pohjaisiin työasemiin. Moni ostaakin Nokian palomuurin melkeinpä pelkästään sen vuoksi, että siihen saa asennettua Check Point VPN-1/FireWall-1 -ohjelmiston, joka suorittaa varsinaiset palomuuurioperaatiot. Nokian kehittäjät ovat työskennelleet Check Pointin kanssa hyvin läheisesti ja Nokian palomuuureja saa tilattua myös Check Point VPN-1/FireWall-1 -ohjelmisto esiasennettuna. Kyse ei ole siis mistä tahansa kolmannen osapuolen ohjelmistosta, vaan hyvässä yhteistyössä rakennetusta kokonaisuudesta. Muutoin Check Pointin ohjelmistoja voidaan asentaa vaikka Windows-käyttöjärjestelmälle, jolloin Windows-koneesta voi rakentaa palomuurin.

Sanomattakin on selvää, että Check Pointin ajamiseen Nokian tarkkaan rakennettu palomuurialusta vie voiton Windows-pohjaisesta työasemasta. [5, s. 152.]

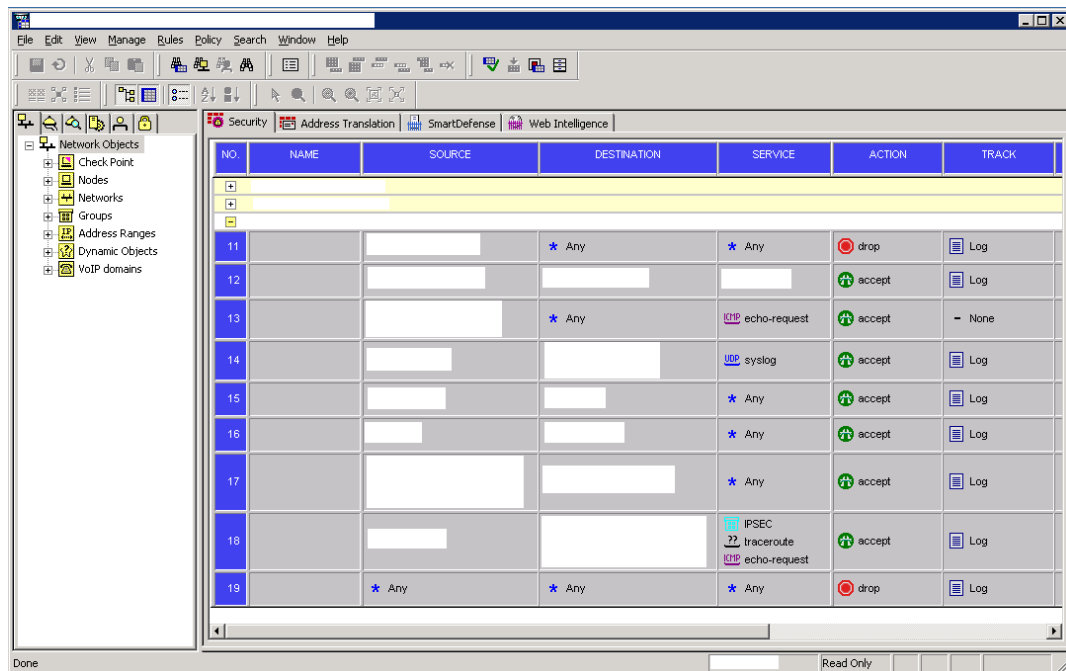
2.1.3 Palomuurialustan hallintasovellukset

Nokia IP1220 -palomuurin hallinta tapahtuu komentopohjaisten sääntöjen ja konfiguraatioiden syöttämisellä Nokia IPSO -käyttöjärjestelmään, joka perustuu FreeBSD-käyttöjärjestelmään. Näin ollen komennot ja käyttöjärjestelmän yleinen käyttäytyminen vastaa pitkälti Linux- / Unix-käyttöjärjestelmää. Mikäli komentojen syöttäminen ei miellytä, on toisena vaihtoehtona Web-pohjainen Nokia Network Voyager (kuva 1), joka korvaa komentojen syöttämisen graafisella käyttöliittymällä ja jota hallitaan Internet-selaimella. Nämä ovat yksittäisen laitteen hallintaan tarkoitettuja sovelluksia, mutta mikäli halutaan hallita samalla sovelluksella useampia laitteita, tarjoaa Nokia siihen Nokia Horizon Manageria. [3; 9.]



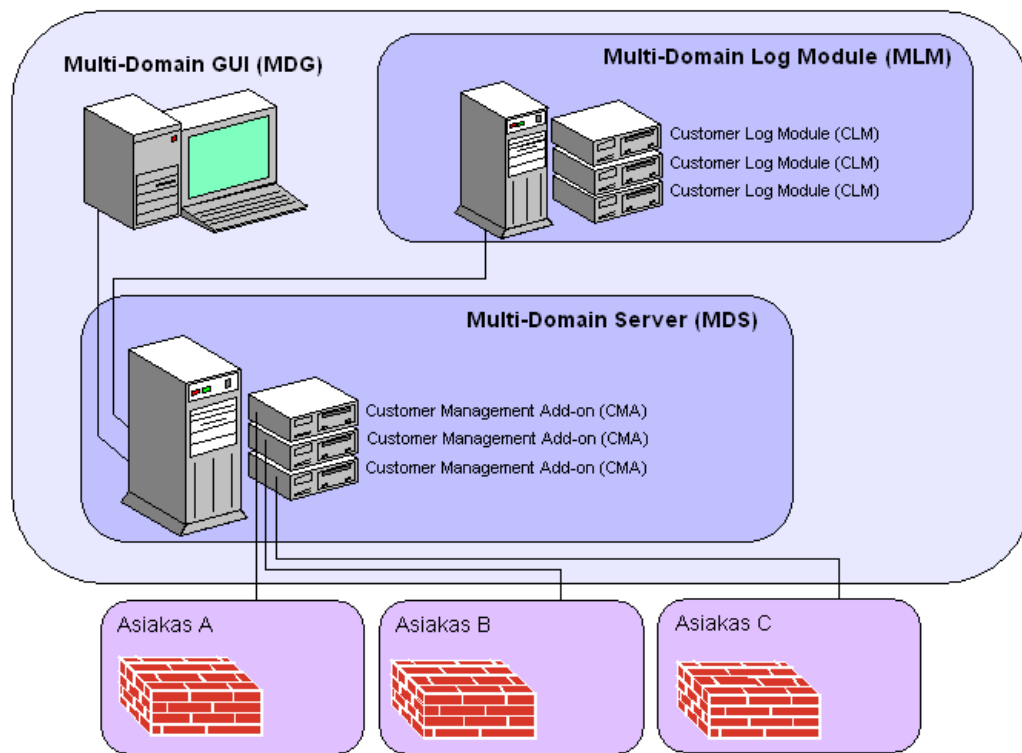
Kuva 1. Nokia Network Voyager -hallintasovellus.

Mikäli Nokian palomuurille on asennettu Check Pointin ohjelmisto, esimerkiksi VPN-1/Firewall-1, onnistuu sen hallinnointi pätevillä Check Pointin graafisilla hallintatyökaluilla, jotka voidaan asentaa erilliselle Windows-pohjaiselle työasemalle. Hallintatyökaluista voinee mainita SmartDashboardin (kuva 2), jolla hallitaan pitkälti koko palomuuria sääntökantoineen. Lisäksi mainitsemisen arvoinen työkalu on SmartView Tracker lokitietojen tutkimiseen. Mikäli palomureja on useita, fyysisinä tai virtuaalisina, tarjoaa Check Point kaikkien palomuurien keskitettyyn hallintaan Provider-1 -ratkaisua. Provider-1:n avulla voidaan yhdestä hallintakoneesta ottaa hallintayhteydet kaikkiin hallittaviin Check Point -palomureihin, olivat ne sitten fyysisiä tai virtuaalisia. [10; 11.]



Kuva 2. Check Pointin hallintatyökalu SmartDashboard.

Check Pointin Provider-1 -ratkaisun pääkomponentit ovat MDS- (Multi-Domain Server) ja MLM-palvelimien (Multi-Domain Log Module) lisäksi varsinaiseen hallinnoimiseen käytettävä MDG (Multi-Domain GUI), jonka avulla yhteydet eri komponentteihin otetaan (kuva 3). [11; 13.]



Kuva 3. Provider-1:n komponentit [11].

MDS-palvelin pitää sisällään virtuaaliset hallintakoneet eli CMA:t (Customer Management Add-on) jokaiselle fyysiselle ja virtuaaliselle palomuurille. CMA kattaa Check Pointin SmartCenterin ohjelmistot, joihin kuuluu muun muassa edellä mainitut SmartDashboardin ja SmartView Trackerin. CMA:iden kautta päästään muokkaamaan sääntöjä asiakkaan palomuurille normaaliin tapaan SmartDashboardia käyttämällä. [11; 13.]

MLM on MDS-palvelinta vastaava palvelin lokitiedostoille. MLM-palvelin sisältää asiakkaiden lokitiedot omissa asiakaskohtaisissa CLM:eissä (Customer Log Module). Lokien kerääminen saadaan myös kahdennettua MDS-palvelimen kanssa, jota voidaan käyttää varapalvelimena. CLM:ien kautta päästään asiakkaiden lokeja tutkimaan SmartView Trackeriä käyttämällä. [11; 13.]

2.1.4 Palomuurialustan virtualistointi Check Pointin VSX-ohjelmistolla

Check Point VPN-1/FireWall-1 VSX tai pelkkä VSX on ohjelmisto palomuurialustan virtualisointiin, jolla saadaan ajettua useita virtuaalimuureja omassa eristetyssä ympäristössä yhdellä varsinaisella fyysisellä palomuurialustalla. VSX-ohjelmiston saa muiden Check Pointin ohjelmistojen tapaan asennettua Nokian palomuurialustan lisäksi myös muun muassa Windows-pohjaisille työasemille. [14.]

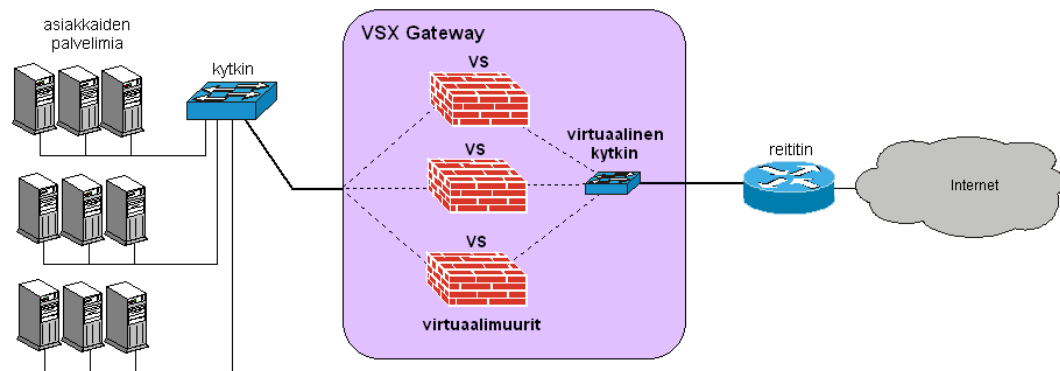
Ilman virtuaalimuureja jokaiselle asiakkaalle täytyisi asentaa oma fyysinen palomuri. Tämä tulisi kalliiksi, sillä jokaisesta fyysisestä palomuurista koituisi hankinta-, lisenssi-, ja ylläpitokustannuksia aina huoltosopimuksista konesalipaikan tuomiin kuluihin. Kaikkien asiakkaiden liikennettä voidaan toki ajaa yhden fyysisen palomuurinkin läpi ilman virtualisointia, mutta tällöin käytössä olisi pelkästään yksi sääntökanta, jonka ylläpitäminen kaikille asiakkaille olisi vaikeaa ja tehotonta. [15.]

VSX-ohjelmisto tarjoaa virtuaaliset komponentit, jotka toimivat kuten oikeat verkkolaitteet. Nämä komponentit käsittävät varsinaisen palomuurin eli Check Point VPN-1/FireWall-1 -ohjelmiston lisäksi muun muassa reitittimet, kytkimet sekä verkkokaapelit. Käyttämällä VSX-ohjelmiston tarjoamia virtuaalisia komponentteja saadaan rakennettua verkkotopologia, joka vastaa toimivuudeltaan täysin fyysisiä laitteita, mutta säästää huomattavasti kustannuksien lisäksi myös konesalitilaa. [14.]

Virtuaalimuurien käyttö ei myöskään ole ilmaista, vaikka huomattavasti halvempaa ja kaikin puolin helpompaa, koska kaikki toiminta tapahtuu yhdellä alustalla.

Virtuaalimuureja varten tarvitaan ohjelmiston lisäksi myös lisenssit virtuaalimuurien ylläpitämiseen. Check Point myy näitä lisenssejä 10, 25, 50, 100 tai 250 virtuaalimuurin käytölle. Myös virtuaalimuurien hallintaa helpottamista varten kannattaa hankkia keskitetty hallinta, esimerkiksi Check Pointin Provider-1. Virtuaalimuureja voi myös hallita yksittäin kuten normaaleja fyysisiä palomuuureja, mutta mikäli virtuaalimuureja on useita, se ei enää välttämättä ole tehokasta. [15.]

VSX Gatewayn, jolla tarkoitetaan varsinaista palomuurialustaa eli tässä tapauksessa Nokia IP1220:aa, sisältämiä virtuaalimuureja kutsutaan VS:ksi (Virtual System), jotka ovat täydellisiä virtualisoituja versioita normaalista Check Point VPN-1/FireWall-1 -ohjelmistosta. Liikenne VS:lle toteutuu VLAN:ien avulla, joten yhdestä palomuurin fyysisestä liitännästä saadaan kulkemaan vaikka kaikkien virtuaalimuureja käyttävien asiakkaiden liikenne (kuva 4). [16.]



Kuva 4. VSX Gatewayn toimintaa havainnollistava kuva [14].

VSX-ohjelmiston virtuaalimuureille kaikki konfigurointi reitityksiä myöten tehdään SmartDashboardilla. Mitään ei tehdä virtuaalimuureille Nokia IPSO:lla, sillä VSX-ohjelmiston virtuaalimuurit ovat toteutettu täysin Check Pointin ohjelmistolla. Fyysisiä Nokian palomureja, joissa toimii Check Point VPN-1/FireWall-1 -ohjelmisto ilman virtualisointia mahdollistavaa VSX:ää, voi vielä konfiguroida IPSO:n kautta normaalisti. [14.]

2.2 Tuleva palomuurialusta, Juniper ISG1000

Capgeminin konesaliin on hankittu vuoden 2007 keväällä kaksi Juniperin valmistamaa ISG1000-palomuuria, jotka Juniper esitteli markkinoille 9.5.2006. Näiden palomuurien muodostamalle kahdennetulle klusterille on tarkoitus siirtää asiakkaiden virtuaalimuurit Nokian palomuuriklusterilta. Kolmannen osapuolen ohjelmistoja Juniperin palomureille ei saa, vaan kaikki toteutetaan Juniperin omalla ScreenOS-käyttöjärjestelmällä.

Keskittynä hallintasovelluksena Capgeminiä on käytössään Juniperin valmistama Network and Security Manager -ohjelmisto (NSM), jolla voidaan hallita useita fyysisiä sekä virtuaalisia palomuuureja keskitetysti Check Pointin Provider-1:n tapaan. [17.]

2.2.1 Palomuurialustan kokoonpano

Juniper ISG1000 (Integrated Security Gateways) on laitetelineeseen asennettava palomuuritarkoitukseen tarkasti rakennettu laitteistopohjainen palomuuuri, joka tarjoaa verkko- ja sovellusturvaa suurille yrityksille sekä konesaliverkoille. Kun Nokia IP1220 oli FreeBSD-käyttöjärjestelmään perustuvan Nokia IPSO:n ja kolmannen osapuolen asennettavien ohjelmien kanssa enemmänkin pelkkä alusta palomuuriohjelmistoille, on Juniper ISG1000 enemmän kokonainen palomuuripaketti laitteistoineen sekä ohjelmistoineen. Käyttöjärjestelmänä laitteessa toimii Juniperin oma ScreenOS-käyttöjärjestelmä.

Juniper ISG1000 -palomuuuri sisältää peruskokoonpanolla neljä 10 / 100 / 1000 megabitin kupariverkkoliitännää. Verkkoliitännät ovat laajennettavissa liitännäkorteilla, joille Juniper ISG1000 -palomuurin etupaneelissa on kaksi lisäliitännäpaikkaa. Laajennuskortteja on saatavilla muun muassa neljän tai kahdeksan 10 / 100 megabitin kupariverkkoliitännällä, kahdella 10 / 100 / 1000 megabitin kupariverkkoliitännällä ja kahdella tai neljällä gigabitin kuituverkkoliitännällä. Lisäksi nykyään on saatavilla laajennuskortti yhdellä 10 gigabitin kuituverkkoliitännällä. Liitännäkortteja yhdistelemällä saadaan Juniper ISG1000 -palomuuriin lisättyä haluttu määrä erilaisia verkkoliitännöitä. [19; 20.]

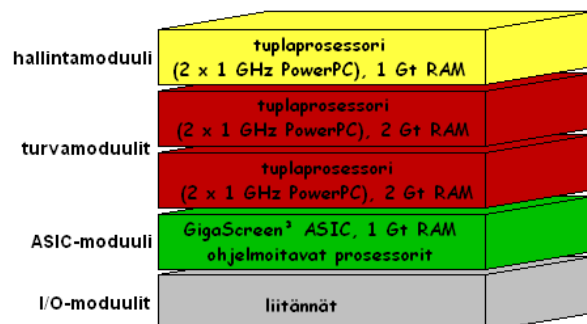
Verkkoliitännöjen lisäksi Juniper ISG1000 -palomuuria saadaan laajennettua Flash-muistikortilla, jolle on palomuurin etupaneelissa varattu yksi PCMCIA-paikka. PCMCIA-paikkaan voidaan asentaa yhden tai kahden gigatavun Flash-muisti. Muistille voidaan tallentaa muun muassa lokitiedostoja, konfiguraatioita tai ScreenOS-käyttöjärjestelmän asennustiedostoja. [19.]

Palomuurin varsinainen laajennettavuus saavutetaan kotelon sisäpuolelle asennettavilla turvamoduuleilla (Security Modules), jotka asennetaan palomuuriin samaan tapaan kuin PCI-kortit pöytäkoneeseen. Turvamoduuleja saa Juniper ISG1000 -palomuuriin asennettua kaksi kappaletta, joille molemmille on varattu omat tuplaprosessorit (kaksi 1 GHz:n PowerPC-prosessoria) sekä omaa muistia aina kahteen gigatavuun asti. Tällä varustelulla turvamoduuleilla tapahtuva toiminta ei kuormita muita prosesseja lainkaan, eivätkä ne näin ollen muodosta pullonkauloja verkkoon. Turvamoduuleilla saadaan asennettua palomuuriin ylimääräisiä turvasovelluksia (Security Applications). Tällä hetkellä turvamoduulina on saatavilla IDP-moduuli (Intrusion Detection & Prevention), joka kiihdyttää palomuurin suorittamia hyökkäyksen havaitsemis- ja estotoimintoja.

Edellä mainittujen laajennettavuuksien lisäksi Juniperin ISG1000 -palomuurissa on AC- tai DC-virtalähteet kahdennettu ja toteutettu HotSwap-tekniikalla, joten toisen vikaantuessa se voidaan vaihtaa palomuurin ollessa toiminnassa. Lisäksi tuuletinrima tukee myös HotSwap-tekniikkaa. [19.]

2.2.2 Palomuurialustan pääkomponentit

Juniper ISG1000 -palomuurin varsinaisina pääkomponentteina toimii rungon ja liitäntöjen lisäksi ASIC-moduuli, hallintamoduuli (Management Module) ja edellisessä luvussa mainitut turvamoduulit. Kuva 5 havainnollistaa komponenteilla muodostuvaa järjestelmäarkkitehtuuria. [19.]



Kuva 5. Juniper ISG1000:n järjestelmäarkkitehtuuri [19].

Juniper ISG1000 -palomuurin sydämenä toimii ASIC-moduuli GigaScreen³. ASIC-moduuli käy läpi kaikki sisään tulevat paketit samalla suorittaen niille monimutkaisia tehtäviä. ASIC-moduulin palomuuriprosessointi kattaa muun muassa istuntojen läpikäynnin, TCP-tarkistussumman tarkistamisen, osoite- ja porttimuunnokset yms. Lisäksi ASIC-moduuli hallitsee VPN-ominaisuuksista muun muassa IPSec-protokollan prosessoinnin yleisesti, salauksen (DES, 3DES sekä AES aina 256 bitin avaimen pituuteen) sekä tiivistet (SHA-1 ja MD5). Palomuri- ja VPN-ominaisuuksien lisäksi ASIC-moduuli avustaa IDP-prosessissa suorittamalla istuntojen läpikäyntiä sekä tekemällä kuormanjakoa palomuurin turvamuulien kesken. Kaiken tämän ASIC-moduuli suorittaa täysin itsenäisesti, eikä se näin ollen toimi pelkkänä keskusyksikön avustajana. [19.]

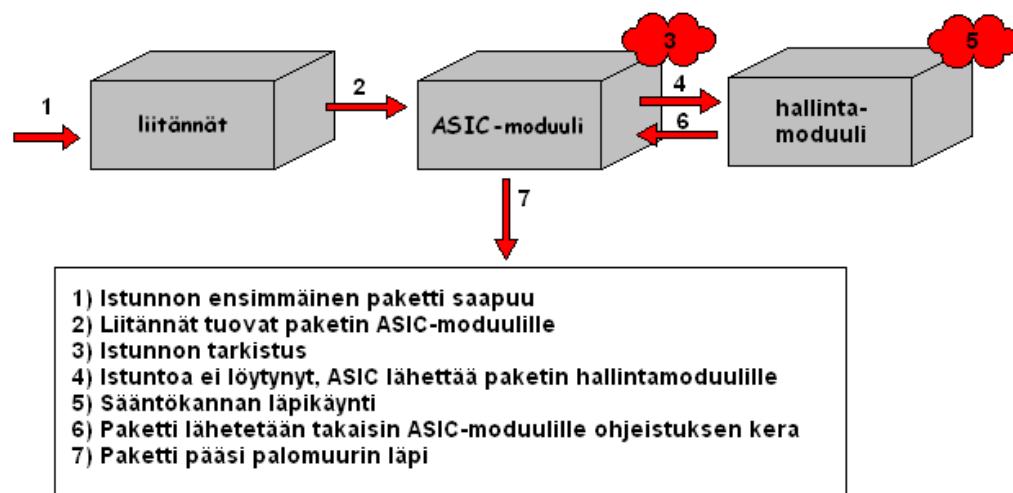
Lisäksi ASIC-moduuli sisältää kahden tyyppisiä ohjelmoitavissa olevia mikroprosessoreja, 32-bittisiä prosessoreja sekä 32-bittisiä Juniperin PPU:ita (Packet Processing Unit). Näitä voidaan tarpeen tullessa päivittää ohjelmistopäivityksillä vaikka tukemaan erilaisia uusia paketinprosessointialgoritmeja. Tällä hetkellä näitä prosessoreja käytetään muun muassa kiihdyttämään SYN flood -hyökkäyksen suojausta. [19.]

Hallintamoduuli käsittelee nimensä mukaisesti hallintaan liittyviä prosesseja. Sen oma tuplaprosessori (kaksi 1 GHz:n PowerPC-prosessoria) sekä oma gigatavun muisti (laajennettavissa kahteen gigatavuun) pitävät huolen, että palomuri on saavutettavissa kovimmankin palvelunestohyökkäyksen aikana. Omien prosessoriensä ansiosta myöskään palomuurin hallinta ei kuormita varsinaista palomuuriprosessia. Normaalin hallinnan (WebUI, CLI, lokien tarkastelu jne.) lisäksi hallintamoduuli käsittelee muun muassa istuntojen luomista eli istuntojen ensimmäisten pakettien prosessointia sekä IKE-neuvotteluja VPN-yhteyksien luomisessa. [19.]

2.2.3 Pakettien kulku palomuurialustan läpi

Paketti saapuu verkkoliitännästä ensin ASIC-moduulille, joka tarkastaa, kuuluuko kyseinen paketti jo johonkin olemassa olevaan istuntoon. Mikäli paketti ei kuulu

mihinkään istuntoon, se lähetetään hallintamoduulille, joka ensin tarkastaa, täsmääkö paketti jonkin hyökkäyksen piirteisiin. Tämän jälkeen käydään sääntökanta läpi ja tarkastetaan, täsmääkö paketti johonkin sääntöön. Sopivan sallivan säännön löytyessä luodaan paketin liikenteelle istunto ja paketti lähetetään takaisin ASIC-moduulille ohjeistuksen kera, kuinka pakettia sekä tulevia istuntoon kuuluvia paketteja käsitellään. Ohjeistukset voivat sisältää esimerkiksi osoitemuunnoksia tai vain käskyn päästää paketti läpi ilman muutoksia. Kuvassa 6 läpikäydään uuden istunnon prosessi. [19.]



Kuva 6. Uuteen istuntoon kuuluvan paketin kulkeminen komponenttien läpi [19.]

Mikäli paketti kuuluu jo johonkin olemassa olevaan istuntoon, se päästetään suoraan läpi jo ASIC-moduulista, kunhan ensin mahdolliset istuntoon kohdistuvat toimenpiteet on tehty (esim. osoitemuunnos). Taulukkoa istunnoista ylläpidetään muistissa, joka on suoraan kytköksissä ASIC-moduuliin. Näin ollen vain istunnon ensimmäinen paketti käy hallintamoduulin kautta pyörittämässä, jolloin saadaan vähennettyä hallintamoduulin kuormaa reilusti ja korotettua palomuurin kokonaismääräistä ulosantia. [19.]

Mikäli turvamoduulit olisivat käytössä, opastaisi hallintamoduuli ASIC-moduulia lähettämään uuden paketin turvamoduuliin, josta paketti palaisi ASIC-moduulin kautta ulos. Olemassa olevaan istuntoon kuuluvat paketit kiertäisivät ASIC-moduulista

suoraan turvamoduulille kiertämättä hallintamoduulin kautta samoin kuten ilman turvamoduuleitakin. [19.]

2.2.4 Palomuurialustan hallintasovellukset

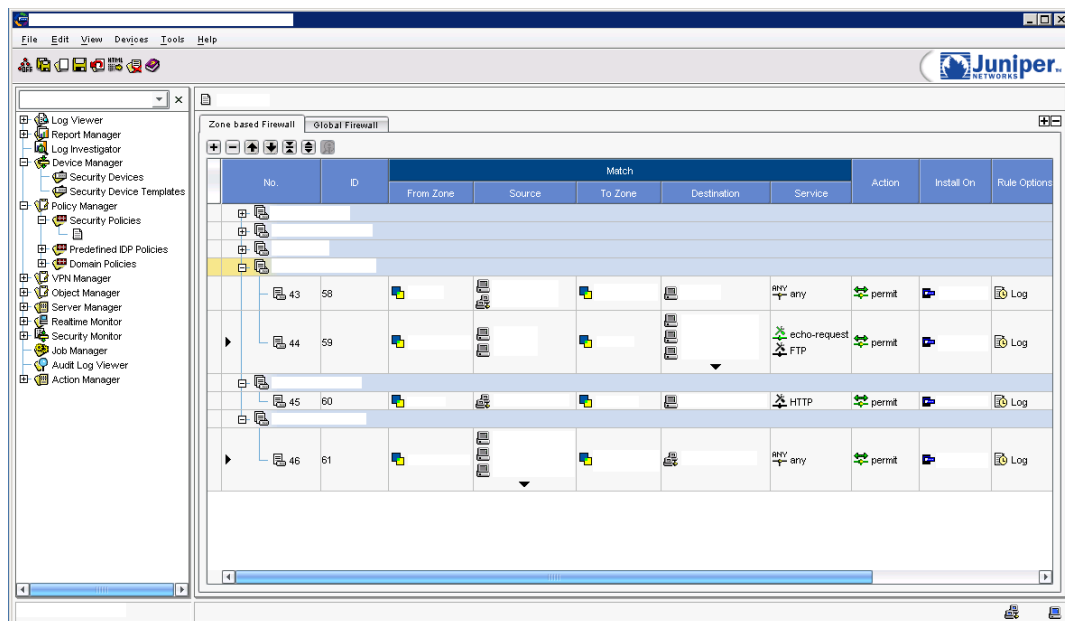
Juniperin ScreenOS-käyttöjärjestelmän konfigurointia ja hallintaa voi suorittaa kolmella eri tavalla, CLI:llä eli komentopohjaisella käyttöliittymällä, Web-pohjaisella WebUI:lla tai keskitetyllä hallintasovelluksella Network and Security Managerilla (NSM), joka tunnettiin ennen nimellä NetScreen Security Manager. [21, s. 91.]

Komentopohjaiseen käyttöliittymään pääsee käsiksi kolmella eri tavalla, verkon kautta käyttämällä joko suojaamatonta telnet-yhteyttä tai suojattua SSH-yhteyttä tai suoraan kytkemällä esimerkiksi kannettavan sarjakaapelilla palomuurin konsoliporttiin.

Komentopohjainen käyttöliittymä on kaiken hallinnan runko, ja esimerkiksi WebUI ja NSM lähettävät palomuurille normaaleja komentoja niillä konfiguroitaessa. [21, s. 91–92.]

Komentopohjaisen käyttöliittymän lisäksi yksittäisen palomuurin perushallintasovellus on Web-pohjainen käyttöliittymä eli WebUI. WebUI:hin pääsee käsiksi normaalilla Internet-selaimella joko salaamattomalla tai SSL-salatulla yhteydellä. WebUI-käyttöliittymä pitää sisällään menu-palkin, joka voidaan konfiguroida näkymään DHTML:llä tai Javalla. Java on oletuksena. [21, s. 92.]

Useiden palomuurien, fyysisten ja virtuaalisten, keskitettyyn hallintaan Juniper tarjoaa omaa Network and Security Manager (NSM) -hallintasovellusta (kuva 7), jolla voidaan hallita täysin jokaista siihen liitettyä palomuuria aina laitekonfiguraatiosta sääntökantoihin. NSM:n arkkitehtuuri rakentuu laitepalvelimesta (Device Server), GUI-palvelimesta sekä itse käyttöliittymästä, josta varsinaiset konfiguraatiot tehdään. Laitepalvelin säilöo lokit sekä hoitaa laitteiden vuorovaikutuksen, kun taas kaikki konfiguraatioinformaatio sijaitsee GUI-palvelimella. Laite- ja GUI-komponentit voidaan myös pitää samalla palvelimella. [22.]

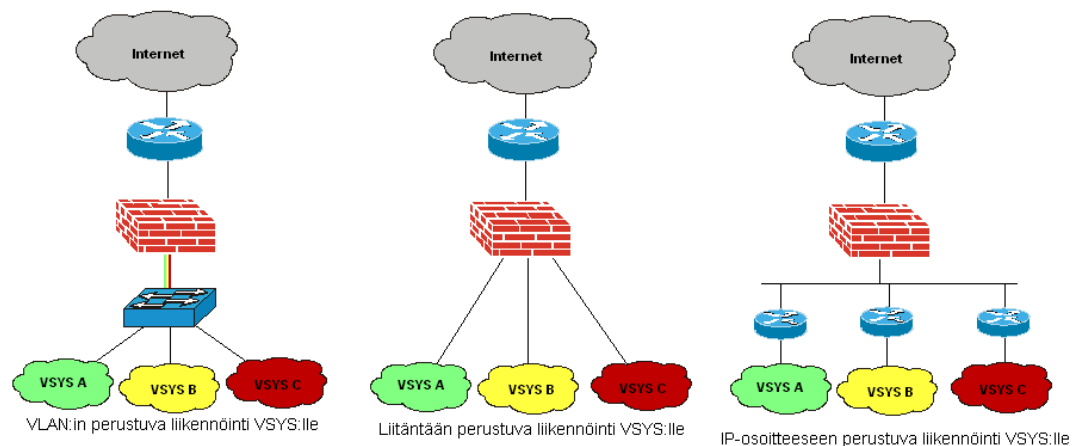


Kuva 7. Juniperin Network and Security Manager (NSM) -hallintasovellus.

2.2.5 Palomuurialustan virtualistointi

Virtualisoinnin idea Juniperissa on sama kuin kaikissa muissakin laitteissa, eli jaetaan varsinainen fyysinen laite useammaksi virtuaaliseksi laitteeksi. Juniper-palomuuressa virtualisoituja laitteita kutsutaan nimellä VSYS (Virtual Systems). Jokainen VSYS pitää sisällään omat virtuaaliset reitittimet, osoitekirjat, sääntökannat, hallinnat sekä alueensa. Ne käyttäytyvät aivan kuten normaalit fyysiset palomuurit ja ovat täysin eristettyjä muista virtuaalimuureista. [23.]

Vaikka virtuaalimuurit ovat täysin eristettyjä muista muureista, voi niillä silti olla jaettuja resursseja, kuten esimerkiksi untrust-alue, joka on yleensä jaettu yhteys Internetiin. Tämän sekä muiden yleisien konfiguraatioiden hallinta suoritetaan Root VSYS:stä. Varsinainen liikennöinti virtuaalimuureille voidaan toteuttaa VLAN:lla, liitännöillä tai IP-osoitteen perusteella (kuva 8). [23.]



Kuva 8. Eri liikennöintimenetelmät virtuaalimuureille eli VSYS:lle [23].

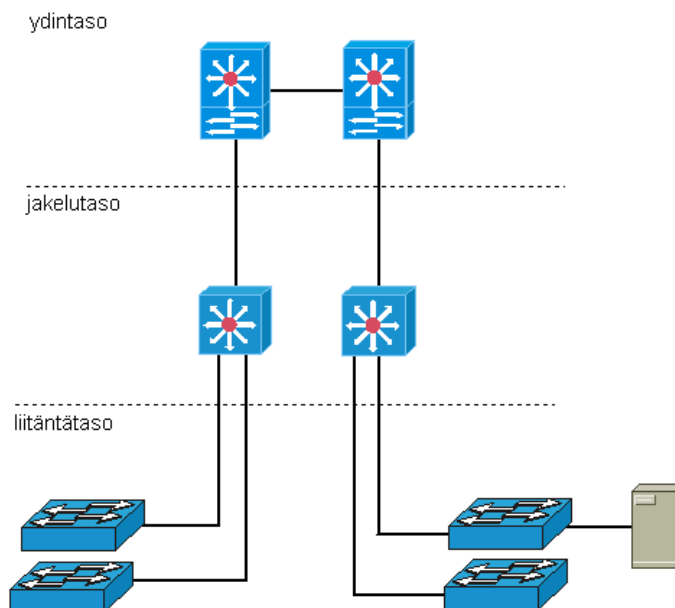
Varsinaiseen virtualisointiin ei tarvita erillistä ohjelmaa, kuten Check Pointilla on (oma erillinen VSX-ohjelmisto), vaan virtualisoinnin voi suorittaa palomuurin omalla ScreenOS-käyttöjärjestelmällä suoraan. Virtualisointiin tarvitaan kuitenkin erillinen lisenssi, joita Juniper myy muun muassa 10, 25, 100, 250 virtuaalimuurin käytölle. [24.]

Jokaisella VSYS:llä on oma eristetty WebUI, jonka kautta virtuaalimuurin konfigurointi ja sääntökannan ylläpitäminen suoritetaan. Eristetyn WebUI:n ja joustavien käyttäjätunnusten ansiota oikeuksia erillisille virtuaalimuureille voidaan myös jakaa asiakkaille ilman pelkoa siitä, että he pääsevät tarkastelemaan muiden asiakkaiden samalla alustalla toimivia virtuaalimuureja. Virtuaalimuurien konfigurointi onnistuu helposti myös komentopohjaisella käyttöliittymällä tai Juniperin keskitetyn hallintasovelluksen, NSM:n, kautta, jolle saadaan myös luotua joustavia käyttäjätunnuksia. [23.]

3 Konesali- ja asiakasverkkojen esittely

3.1 Konesaliverkon runko ja sen toiminnallisuus

Capgeminin konesaliverkon rungon rakenne pohjautuu Ciscon kolmitasoiseen hierarkiamalliin (kuva 9), joka nimensä mukaisesti perustuu kolmeen eri tasoon: ydin-, jakelu- sekä liitântätasoon. Jokaisella tasolla on oma vastuualueensa: ydintaso on verkon selkäranka, jakelutasolla suoritetaan reititykset ja liitântätasolla liikennöidään muun muassa palvelimille. Tasojen määritykset ovat kuitenkin vain loogisia, eikä niihin haeta fyysisiä laitteita. Näin ollen sama laite voi suorittaa vaikka kahden eri tason toimintoja. [25, s. 47.]



Kuva 9. Ciscon kolmitasoinen hierarkiamalli [25, s. 47].

Hierarkiaa ylhäältä alaspäin tarkasteltaessa on ensimmäisenä ydintaso, joka on koko verkon selkäranka. Ytimen tarkoituksena on pelkästään siirtää paketteja niin nopeasti kuin mahdollista. Ydintasolla ei tehdä mitään, mikä voisi hidastaa pakettien kulkua kuten pääsilystojen käyttöä tai pakettisuodatuksia. Nämä ovat seuraavan tason, eli

keskellä toimivan jakelutason tehtäviä. Pääsylistojen ja pakettisuodatuksien lisäksi jakelutasolla hoidetaan muun muassa reitityksiä, mahdollisia tietoturva-asioita (esim. osoitemuunnokset) ja reititystaulujen jakelut eri reititysprotokollien kesken. Alimpana hierarkiassa toimii liitântätaso, jossa varsinaiset palvelimet ja työasemat sijaitsevat. [25, s 47–49.]

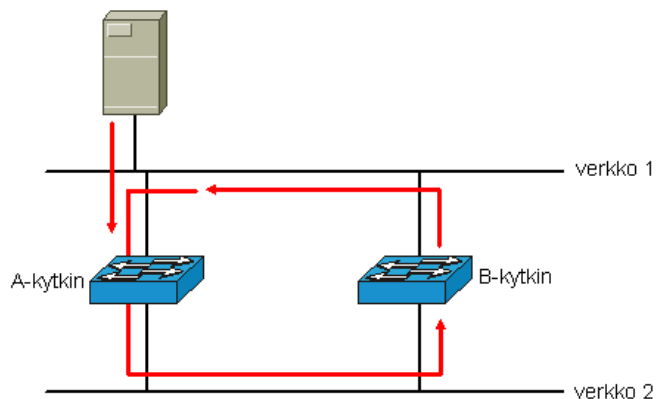
Kun kolmitasoinen hierarkiamalli on tarkoitettu helpottamaan verkon hallintaa ja hahmottamista, niin varsinaista helpotusta liikennöintiin tuo verkkojen virtualisointi käyttämällä VLAN:a eli virtuaalilähiverkkoja. VLAN:ien avulla saadaan luotua useista fyysisistä porteista loogisia yhteislähetysalueita, vaikka fyysiset portit voivat sijaita kaukana toisistaan aivan eri kytkimillä. VLAN:ien käyttö siis mahdollistaa samassa VLAN:ssa olevien laitteiden keskinäisen kommunikoinnin siirtokerroksella. Samassa kytkimessä voi siis olla useiden eri asiakkaiden palvelimia ilman, että ne tietävät toistensa olemassaolosta. Näin ollen jokaisella asiakkaalla ei tarvitse olla omaa nimettyä kytkintä. Mikäli halutaan liikennöidä eri VLAN:ien välillä, tarvitaan toimenpiteeseen verkkokerroksella toimiva kytkin tai reititin. [26, s. 129–131.]

VLAN:ien lisäksi myös reititystauluja saadaan virtualisoitua, jolloin niitä voi olla useampia samalla reitittimellä. Tämä toteutetaan käyttämällä VRF- eli Virtual Routing and Forwarding -tekniikkaa. Tekniikan ansiosta reititystaulut pysyvät helposti hallittavissa eikä jokaiselle reititystaululle tarvitse hankkia erillistä reititintä. [27.]

Tehokkuuden, eli virtualisoinnin, lisäksi täytyy konesaliverkossa toimia myös käyttövarmuus eli kahdennus. Tämä on toteutettu yksinkertaisimmillaan siten, että on hankittu jokaista ydin- ja jakelukytkintä kahdet kappaleet sekä vedetty verkkokaapelit kahdesti kytkimeltä toiselle. Toisen kytkimen liitännän, verkkokaapelin tai kytkimen rikkoontuessa yhteydet toimivat vielä toisen varmistavan vastaavan kautta.

Valitettavasti verkon kahdennusta ei voi toteuttaa aivan niin helposti, että vedetään toinen kaapeli kytkimeltä toiselle. Mikäli näin tehdään, syntyy verkkoon silmukka. Silmukka siis syntyy, kun kytkimeltä on kaksi reittiä toiselle kytkimelle. Esimerkki silmukasta nähdään kuvasta 10. Kun yhteislähetyskehys saapuu A-kytkimelle, lähettää

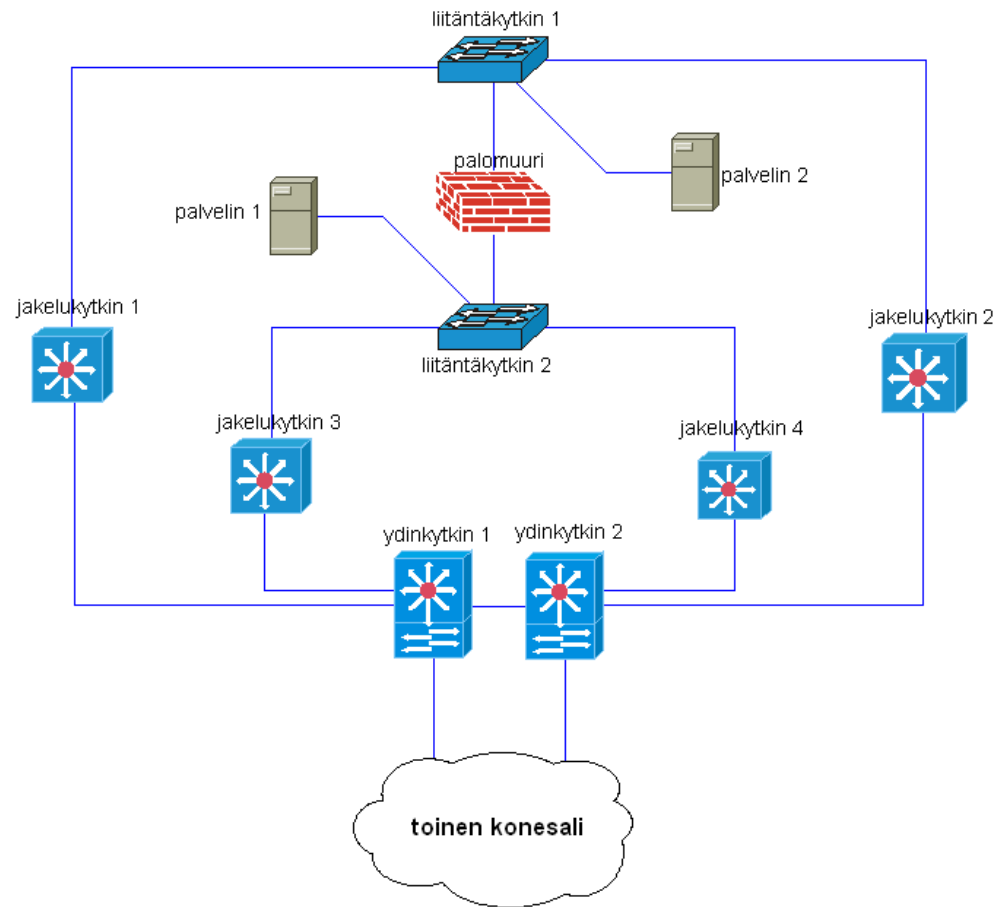
se tämän kehyksen eteenpäin kytkimen jokaisesta liitännästä paitsi siitä, josta kehys vastaanotettiin. Kuvan tapauksessa kehys kulkeutui A-kytkimelle yläkautta, joten yhteislähetyskehys kulkeutuu B-kytkimelle alakautta. Normaalin toimintatavan mukaisesti tämä yhteislähetyskehys lähetetään taas jokaisesta B-kytkimen liitännästä ulos, paitsi siitä josta se vastaanotettiin. Tällöin kehys kulkeutuu yläkautta takaisin A-kytkimelle. Tämä yhteislähetyskehyksen eteenpäin lähettäminen jatkuu näiden kytkimien välillä loputtomiin. Silmukka on syntynyt A- ja B-kytkimien välille, joka lopulta hidastaa verkon toiminnan käyttökelvottomaksi. [25, s. 504–505; 28.]



Kuva 10. Yhteislähetyskehyksellä aiheutettu silmukka [25, s. 504].

Edellä mainittu esimerkki silmukan syntymisestä voidaan estää STP-protokollalla (Spanning Tree Protocol), joka erilaisten määrityksien ja algoritmien avulla sulkee toisen varmistavan liitännän, jolloin liikenne kulkee vain toista kaapelia pitkin. Mikäli yhteys tämän kaapelin kautta jostain syystä katkeaa, avautuu suljettu liitäntä ja liikenne pääsee kulkemaan sitä kautta. [28.]

Kuva 11 näyttää yksinkertaistetun, mutta havainnollistavan kuvan konesaliverkon rakenteesta. Kuvassa näkyvä toinen konesalipilvi vie yhteydet konesaliin, joka sijaitsee aivan toisessa rakennuksessa. Lisäksi kuvassa näkyvän palomuurin paikalle voidaan kuvitella kumpi tahansa palomuurialustoista, sillä Juniper-palomuurialusta on kytketty konesaliverkon liitäntäkytkimille samoin kuin Nokia-palomuurialusta.



Kuva 11. Capgeminin konesaliverkon siirtokerroksen yksinkertaistettu rakenne.

3.2 Asiakasverkon toiminnallisuus

Asiakkaan palvelimien liikennöinti asiakasverkon sisällä toimii molemmilla palomuurialustoilla samoin periaattein. Asiakkaan virtuaalimuuri toimii yleisesti asiakasverkon keskipisteenä toimien palomuurin toimintojen lisäksi myös reitittimenä, jonka reititystaulu sisältää kaikki tarpeelliset reititykset asiakkaan yhteyksille. Liikenne asiakkaan virtuaalimuurille saapuu siirtokerroksella VLAN:ien avulla palomuurialustan jaetun fyysisen liitännän kautta. Verkkokerroksella liikenne saapuu palvelimien oletusyhdykskäytävän mukaisesti virtuaalimuurin virtuaaliseen liitäntään. Asiakkaan omat verkot ovat verkkokerroksella kytketty suoraan virtuaalimuuriin kiinni, joten niiden reititykset muodostuvat virtuaalimuurin reititystauluun automaattisesti.

Asiakasverkon ja ulkomaailman väliset yhteydet toimivat palomuurialustoilla eri tavoin ja siihen palataan seuraavassa luvussa.

Samassa verkossa eli VLAN:ssa olevien palvelimien välinen liikenne ei kulje oletusyhdykäytävän eli virtuaalimuurin kautta, sillä liikenne ei tarvitse reititystä. Paketti lähtee palvelin 1:stä liitäntäkytkin 2:een, josta se kulkeutuu jakelukytkimille 3 ja 4. Paketti voi kulkea vain toiselle jakelukytkimelle, sillä STP-protokolla on sulkenut toisen yhteyden estääkseen silmukoiden muodostumisen kahdennetussa ympäristössä. Jakelukytkimen jälkeen paketti kulkeutuu ydinkytkimien kautta jakelukytkimille 1 ja 2, joiden kautta paketti kulkeutuu aina liitäntäkytkin 1:n kautta palvelin 2:een. Paketti kulkee pitkälti siirtokerroksella. Fyysisesti paketti kulkee pitkän matkan, mutta loogisesti hyvin lyhyen (ks. kuva 11).

Eri verkoissa eli VLAN:eissa olevien palvelimien välinen liikenne tarvitsee reitityksen. Tällöin liikenne kulkee palvelimien oletusyhdykäytävän mukaisesti virtuaalimuurin virtuaalisten liitäntöjen kautta. Paketti lähtee palvelin 1:stä palvelimen oletusyhdykäytävää kohti. Siirtokerroksella paketti saapuu palomuurialustan jaetun fyysisen verkkoliitännän kautta, jonka kautta kulkeutuvat myös muiden asiakkaiden paketit. Mikäli kyseessä on uusi istunto, virtuaalimuuri käy sääntökannan paketille läpi tarkistaakseen, onko yhteys sallittu. Mikäli yhteys on sääntökannan mukaan sallittu, käy virtuaalimuuri läpi reititystaulun, jonka avulla se tietää, minne paketti seuraavaksi lähetetään. Koska palvelin 2:n verkko on virtuaalimuurissa kiinni, löytyy oikea reitti automaattisesti. Paketti siis lähetetään siitä virtuaalisesta liitännästä ulos, jossa tämä palvelin 2:n verkko sijaitsee. Siirtokerroksella paketti lähtee taas palomuurialustan fyysisestä jaetusta liitännästä. Paketti kulkee siirtokerroksella VLAN:ien avulla virtuaalimuurille, ja verkkokerroksella virtuaalimuuri reitittää paketin oikeaan verkkoon (ks. kuva 11).

3.2.1 Yhteydet asiakasverkosta ulospäin

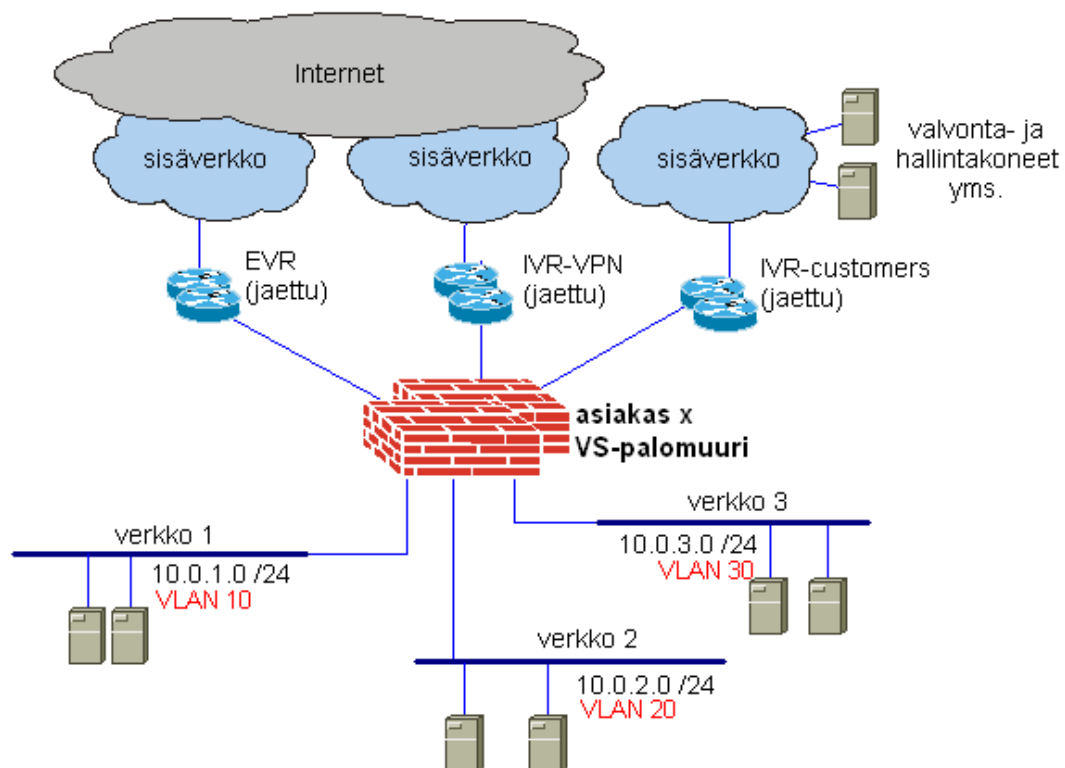
Asiakasverkossa ja asiakasverkon ulkopuolella sijaitsevien palvelimien välinen liikenne käyttää jotain virtuaalimuurin kolmesta virtuaalisten liitännöiden tarjoamasta reitistä. Virtuaalimuurilta löytyy erilliset reitit Internetin, VPN-keskittimien ja Capgeminin sisäverkon suuntaan. Reitti Internetiin on asiakkaan suora yhteys Internetiin, ja se käyttää Capgeminin asiakkaille tarkoitettua Internet-liittymää. Tätä kautta voidaan myös Internetistä ottaa yhteyttä esimerkiksi asiakkaan web-palvelimeen julkisen osoitteen avulla, mikäli yhteys on sallittu virtuaalimuurilla. VPN-keskittimien kautta asiakas voi liikennöidä VPN-tunnelissa esimerkiksi oman ja asiakkaan kumppanin verkon välillä. Capgeminin sisäverkosta saadaan yhteydet siellä sijaitseville palvelimille, kuten esimerkiksi hallinta- ja valvontapalvelimille. Vaikka liikenne jokaisesta reitistä kulkee tavalla tai toisella Capgeminin sisäverkossa, on sisäverkossa oleville palvelimille luotu oma reitti. Tämän avulla asiakasverkon ja sen ulkopuolisen verkon välisiä reitityksiä saadaan selkeytettyä huomattavasti. Asiakkaalla voi olla myös omia yhteyksiään ulospäin esimerkiksi oman Internet-yhteyden kautta. Edellä mainittujen reittien käyttö on toteutettu palomuurialustoilla eri tavoin.

3.2.2 Asiakasverkko Nokian palomuurialustalla

Edellisessä luvussa mainitut reitit ulkopuolella sijaitseville palvelimille on jaettu yleisesti palomuurialustalla jokaisen virtuaalimuureja käyttävän asiakkaan kesken. Nokian palomuurialustalla Check Point -ohjelmistossa virtuaalimuureja kutsutaan VS:ksi. Liikenne ei kulje asiakasverkon ulkopuolelta suoraan asiakkaan VS:lle VLAN:ien avulla, vaan tässä tapauksessa liikenne kulkee oikealle VS:lle IP-osoitteiden perusteella. Jotta liikenne saadaan reititettyä kohdeosoitteen perusteella oikean asiakkaan VS:lle, tarvitaan reitittimiä. Jokaiselle reitille on varattu yhteiset virtuaaliset reitittimet palomuurialustan eteisessä, eli näitä virtuaalisia reitittimiä on kolme kappaletta. EVR (External Virtual Router) on virtuaalinen reititin, jonka kautta liikenne kulkee asiakkaan ja Internetin välillä. IVR-VPN (Internal Virtual Router) on virtuaalinen reititin asiakkaan ja VPN-keskittimien välillä. IVR-customers on

virtuaalinen reititin asiakkaan ja Capgeminin sisäverkon välillä. Nämä virtuaaliset reitittimet sisältävät reititystaulut, joiden oletusreitti on aina palomuurialustalta ulospäin. Asiakkaiden verkoille reitittimien reititystauluissa on staattiset reitit asiakkaiden VS:n suuntaan.

Kuva 12 näyttää yksinkertaistetun kuvan asiakkaan verkon rakenteesta VS:llä. Kun verkosta 1 liikennöidään verkkoon 2, liikenne käy palomuurin kautta. Sääntökannan tarkistuksen jälkeen sallittu liikenne kulkee reititystaulun mukaisesti. Samassa verkossa olevien palvelimien liikenne ei kulje palomuurin kautta. Asiakkaan virtuaalimuurin reititystaulun oletusreitti on yleensä Internetin suuntaan eli EVR-reitittimelle, mutta jos halutaan ottaa yhteys esimerkiksi VPN-tunnelin takana olevalle palvelimelle, tehdään kyseiselle palvelimelle staattinen reitti VPN-keskittimien suuntaan IVR-VPN-reitittimen kautta.

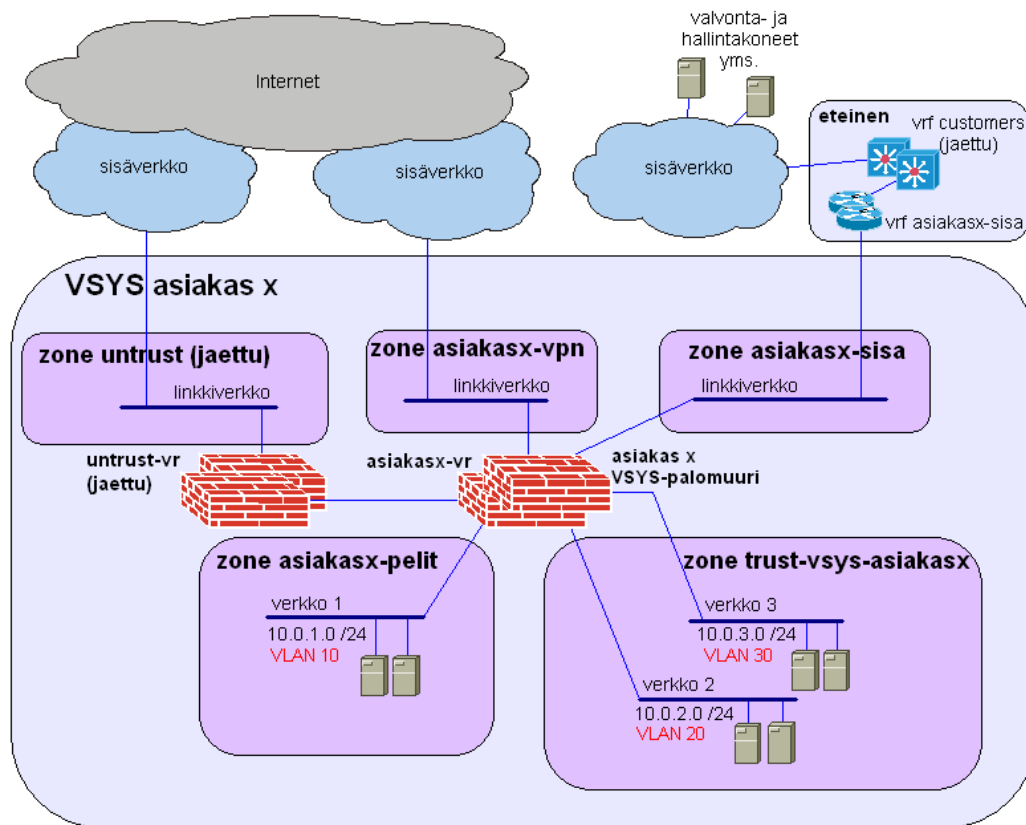


Kuva 12. Asiakkaan verkon yksinkertaistettu rakenne Check Pointilla.

3.2.3 Asiakasverkko Juniperin palomuurialustalla

Juniper-palomuurialustalla asiakkaalla on omat suorat linkkiverkot virtuaalimuurilta sekä VPN-keskittimien että Capgeminin sisäverkon suuntaan. Juniperin palomuurialustalla virtuaalimuureja kutsutaan VSYS:ksi. Liikenne kulkee suoraan virtuaalimuurin virtuaalisen liitännän IP-osoitteen perusteella oikealle VSYS:lle, joten ylimääräisiä reitittämiä palomuurialustalla ei tarvita. Ainoastaan Internetin ja VSYS:n välillä palomuurialustan eteisessä on edelleen yhteinen virtuaalinen reititin, untrust-vr, joka korvaa Nokia-palomuurialustalla olleen EVR:n. Untrust-vr:llä on EVR:n tapaan oletusreitti palomuurialustalta ulospäin, ja reitit asiakkaiden verkkoihin on tehty staattisin reitein kohti asiakkaiden VSYS:ä. VSYS:n oletusreitinnä toimii usein untrust-vr, joten liikennöinti esimerkiksi VPN-tunnelin takana sijaitseville palvelimille täytyy erikseen reitittää. Reititykset osoittavat tällä kertaa linkkiverkon suuntaan Nokian palomuurialustalla olleen IVR-VPN-reitittimen sijaan. Myös VSYS:n ja Capgeminin sisäverkon välisellä liikenteellä on oma eteisensä, mutta se ei sijaitse palomuurialustalla. Tämä eteinen esitellään seuraavassa luvussa.

Nokian palomuurialustaan verrattuna Juniper tuo suorien linkkiverkkojen lisäksi uutta toiminnallisuutta zoneilla eli alueilla. Alueet lisäävät asiakkaiden verkkojen tietoturvaa yleisesti, sillä verkot voidaan jaotella erilaisiin alueisiin esimerkiksi tietoturvasoilla heikko, normaali ja korkea. Tämä myös helpottaa verkon hallintaa, sillä uutta palvelinta asennettaessa voidaan se heti määritellä johonkin tietoturvassoon kuuluvaksi, jolloin palomuurin sääntökannassa sille voi olla jo valmiina tiettyjä sääntöjä alueellisesti. Lisäksi alueet nopeuttavat sääntökannan läpikäymistä, sillä Juniper-palomuuri tarkastaa aluksi lähde- ja kohdepalvelimien alueet ja käy säännöt läpi vain niistä säännöistä, joiden lähde- ja kohdealueet vastaavat näitä. Kuva 13 näyttää asiakkaan verkon VSYS:n rakenteen lisäksi verkkojen alueellistamisen. [21, s. 164.]

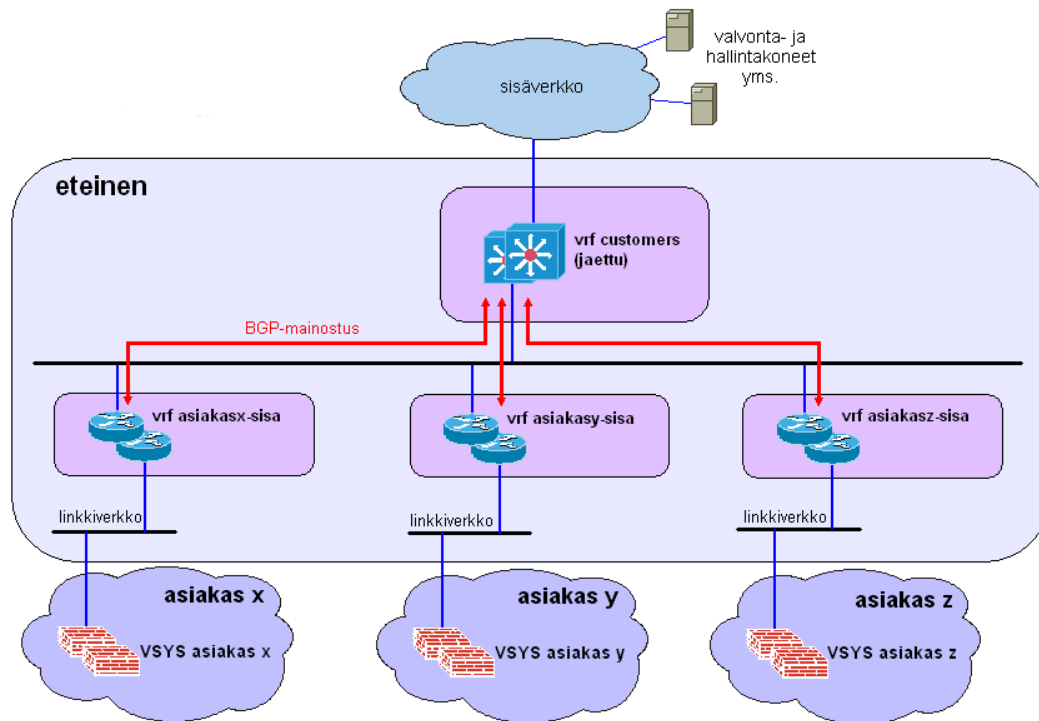


Kuva 13. Asiakkaan verkon yksinkertaistettu rakenne Juniperilla.

3.2.4 Sisäverkon ja VSYS:n välinen eteinen

Nokian palomuurialustalla liikenne Capgeminin sisäverkon sisältä muun muassa hallinta- ja valvontapalvelimilta saapui palomuurialustan virtuaaliselle IVR-customers -reitittimelle palvelimesta riippuen milloin minkäkin sisäverkon sisällä toimivan reitittimen ja linkkiverkon kautta. Sisäverkon liikennöinti asiakkaiden virtuaalimuureille on Juniperin palomuurialustan käyttöönnotossa suunniteltu uudestaan ja se on toteutettu käyttämällä erillistä eteistä jo ennen varsinaista palomuurialustaa (kuva 14). Eteinen on luotu kahdella virtuaalisella reititystaululla eli VRF:llä sisäverkossa sijaitseville reitittimille, joiden kautta yhteydet asiakas- ja sisäverkossa olevien palvelimien kesken kulkevat. Jokaisella asiakkaalla on oma VRF (esim. kuvassa oleva asiakasx-sisa), joka pitää sisällään staattiset reitit VSYS:n suuntaan asiakkaan verkkoihin. Lisäksi eteisessä on yksi yleinen jaettu VRF, customers, joka sisältää staattiset reitit sisäverkon suuntaan

sisäverkossa oleville palvelimille. Varsinaiset yhteydet asiakkaan sekä sisäverkon palvelimien kesken, eli näiden kahden VRF:n kesken, luodaan BGP-reititysprotokollalla sekä pääsilystoilla.



Kuva 14. Sisä- ja asiakasverkon välinen eteinen ennen palomuurialustaa.

Käytetään esimerkkinä kuvassa 14 näkyvää asiakas x:ää. BGP-protokolla mainostaa asiakasx-sisa-VRF:ssä olevat asiakasverkon staattiset reitit yleiselle customers-VRF:lle. Verkot, jotka halutaan BGP-protokollan mainostuksella lisätä yleiselle customers-VRF:lle, täytyy ensin sallia yleisen VRF:n pääsilystalla. Mainostus toimii samoin myös toiseen suuntaan eli customers-VRF:n sisältämät reitit mainostuvat asiakasx-sisa-VRF:lle. Asiakkaan VRF:n pääsilystalla sallitaan vain ne Capgeminin sisäverkossa sijaitsevat verkot, joita asiakas tarvitsee. Pääsilystojen avulla hallitaan BGP-protokollalla tapahtuvaa reittien mainostusta. Mikäli pääsilystoja ei olisi, jokaisen asiakkaan VRF:llä olisi koko customers-VRF:n massiivinen reititystaulu. Jotta liikenne toimisi asiakas- ja sisäverkon välillä, täytyy tarvittavat reititykset vielä tehdä asiakkaan VSYS:illä osoittamaan kohti asiakkaan VRF:ää. Vaikka eteisreititys kuulostaa monimutkaiselta, helpottaa se reititystaulujen yleistä hallintaa huomattavasti.

4 Asiakkaan palomuurialustan vaihto

4.1 Valmistelut palomuurialustan vaihtoa varten

Koska Nokia IP1220 -palomuurialustalla ajettavan Check Point VPN-1/FireWall-1 VSX -palomuuriohjelmiston VS-virtuaalimuureja käyttäviä asiakkaita on useita, joilla on oma ympäristönsä omine sääntökantoineen ja yhteyksineen, on asiakkaat jaettu eri työntekijöiden kesken. Työtä varten on perustettu vuoden 2009 alussa työryhmä, jotta koko palomuurialustan vaihto kaikkine asiakkaineen onnistuisi tehokkaasti. Työnjakoa varten pidettiin alustava palaveri aiheesta. Lisäksi muutaman kerran kuussa on pidetty erilaisia tilannekatsauspalavereita, joissa on käyty läpi työn edistymistä sekä jaettu erilaisia vinkkejä ja huomioita yleisesti työhön liittyen. Jokainen työryhmässä oleva hoitaa itsenäisesti muiden töidensä ohella nimetyn asiakkaan tai nimettyjen asiakkaiden palomuurivaihdon valmistelun ja sen toteuttamisen ja on tästä vastuullinen. Koska jokainen toimeksianto tehdään pitkälti itsenäisesti ja jokaisella on oma työtapansa, on hyvä jakaa esimerkkejä ja vinkkejä yhteisissä palavereissa tai sähköpostitse. Kokonaisuudessaan työ on hyvässä hengessä suoritettavaa ryhmätyötä.

Koska palomuurialustan vaihdosta aiheutuu yleisesti katkoksia asiakkaan verkkoihin, tulee vaihdon olla asiakkaan hyväksymä. Työ on hyvä aloittaa kertomalla asiakkaalle, mistä on kyse ja miksi näin tehdään. Myöhemmin, kun työn valmistelu on jo hyvällä mallilla, voidaan asiakkaalle ehdottaa päivämäärää itse palomuurialustan vaihdolle. Yleensä vaihdos tehdään viikonloppuyönä, mutta joissain tapauksissa voi arki-iltakin olla mahdollinen. Tämä riippuu pitkälti asiakkaan yhteyksistä ja mielipiteestä asiaan.

4.1.1 Valmistelut uusia linkkiverkkoja varten

Koska Juniper ISG1000 -palomuurille on tarkoituksena luoda suorat linkkiverkot asiakkaan virtuaalimuurilta ulospäin lähteille yhteyksille, täytyy nämä uudet linkkiverkot ensin suunnitella sekä varata tarvittavat verkot ja VLAN:t niitä varten. Tämän jälkeen ne voidaan luoda sisäverkossa sijaitseville reitittimille, sillä liikenne ei

vielä niiden kautta reitity. Ainoastaan Internetin ja asiakasverkon välinen liikenne kulkee palomuurin eteisessä olevan yhteisen virtuaalisen reitittimen untrust-vr:n kautta. Jokainen asiakas käyttää tämän reitittimen ja sisäverkon välillä olevaa linkkiverkkoa yhteisesti. Linkkiverkosta on varattu jokaiselle asiakkaalle yksi IP-osoite, jonka taakse voidaan suorittaa osoitemuunnos, kun asiakkaan verkosta liikennöidään Internetin suuntaan.

Linkkiverkkojen varaaminen onnistuu varaamalla sopivan kokoinen käyttämätön verkkolohko Capgeminin IP-taulukoista. Samalla onnistuu myös tarvittavan VLAN:n varaus linkkiverkkoa varten. Linkkiverkkoja tarvitaan asiakkaalle yleensä kaksi, VPN-keskittimien ja palomuurin välille sekä Capgeminin sisäverkon ja palomuurin välille. Kaikilla asiakkailla ei tosin välttämättä ole VPN-palvelua, jolloin he eivät linkkiverkkoa VPN-keskittimien välille tarvitse.

Luvussa 3.2.4 kerrottiin sisäverkon ja asiakkaan virtuaalimuurin välissä olevasta eteisestä. Eteistä varten täytyy luoda yleinen VRF sekä asiakkaan oma VRF. Nämä luodaan sisäverkon reitittimille. Kun VSYS:n ja sisäverkon välinen linkkiverkko on reitittimille normaalisti luotu, sen VLAN sisällytetään asiakkaan VRF:lle, jolloin linkkiverkon kautta kulkeva liikenne reitittyy tämän VRF:n reititystaulun mukaisesti. Varsinaiset reititykset asiakkaan verkkoihin voidaan luoda asiakkaan VRF:llä staattisilla reitityksillä ja lisäksi ne voidaan jo mainostaa BGP:llä pääsylistojen avulla yleiselle VRF:lle. Saman voi toteuttaa toisinpäin, eli mainostetaan yleiseltä VRF:ltä pääsylistojen avulla asiakkaan tarvitsemat sisäverkon palvelimet kohti asiakkaan VRF:ää. Varsinaisessa vaihdossa sisäverkosta tarvittavat yhteydet (esim. hallinta- ja valvontayhteydet) reititetään kohti yleistä VRF:ää, jolloin liikenne alkaa kulkea asiakkaan virtuaalimuurille oikein.

4.1.2 Uuden verkkokuvan ja VSYS:n luonti

Asiakkaan nykyisestä verkkokuvasta täytyy tehdä suunnitelma, miltä asiakkaan verkko tulee Juniperin palomuurialustalla näyttämään. Käytännössä tämä tarkoittaa sitä, että asiakkaan nykyiseen verkkoon täytyy kehittää aluesuunnitelma, eli mikä verkko kuuluu

mihinkin alueeseen. Kuvasta 13 nähtiin yleinen alueellistaminen asiakkaan verkossa. Jokaisella asiakkaalla on oletuksena jaettu untrust- sekä trust-vsyst-asiakas-alue. Trust-vsyst-asiakas-alue luodaan automaattisesti asiakkaan VSYS:iin, kun VSYS Juniper-palomuurille luodaan. Untrust-alue on jo luotuna ja käytössä, sillä se on yleisesti jaettu. Näiden kahden alueen lisäksi lähes kaikilla asiakkailla on alueet ulospäin lähteville linkkiverkoille eli alueet asiakas-vpn ja asiakas-sisa. Asiakkailla voi myös olla omia alueita, esimerkiksi asiakkaan omiin ulospäin lähteviin yhteyksiin, joille voidaan luoda esimerkiksi oma asiakas-outside-alue. Joka tapauksessa alueet täytyy suunnitella verkkokuvaan mahdollisimman viimeistellysti, jotta niitä ei tarvitse myöhemmin korjata.

Verkkokuvaan piirrettäessä on alueiden lisäksi hyvä suunnitella valmiiksi asiakkaan verkkojen liitännät, eli mitä palomuurin fyysistä liitännää käytetään missäkin asiakkaan virtuaalisessa liitännässä. Asiakkaan verkko voi olla esimerkiksi liitännän 1/0.11 takana, mikä kertoo, että liikenne tulee Juniperin fyysisestä liitännästä 1/0 ja kulkee asiakkaan virtuaalisen liitännän 1/0.11 läpi. Eri verkkoja kannattaa tuoda eri fyysisten liitännöiden kautta, jolloin kaikki liikenne ei tule samasta fyysisestä liitännästä sisään. Tällä saadaan toteutettua pieni manuaalinen kuormanjako.

Kun verkkokuva on luotu, voidaan Juniperissa luoda asiakkaan virtuaalimuuri eli VSYS. VSYS:n käyttöönotto onnistuu WebUI:lla muutamalla napsautuksella tai CLI:ltä muutamalla komennolla. Ainoa asia, joka luontivaiheessa täytyy tietää, on nimi tulevalle VSYS:lle. Kun VSYS on luotu, voidaan verkkokuvaan suunnitellut alueet ja liitännät luoda, jolloin ne ovat palomuurilla valmiina. [21, s. 729–730.]

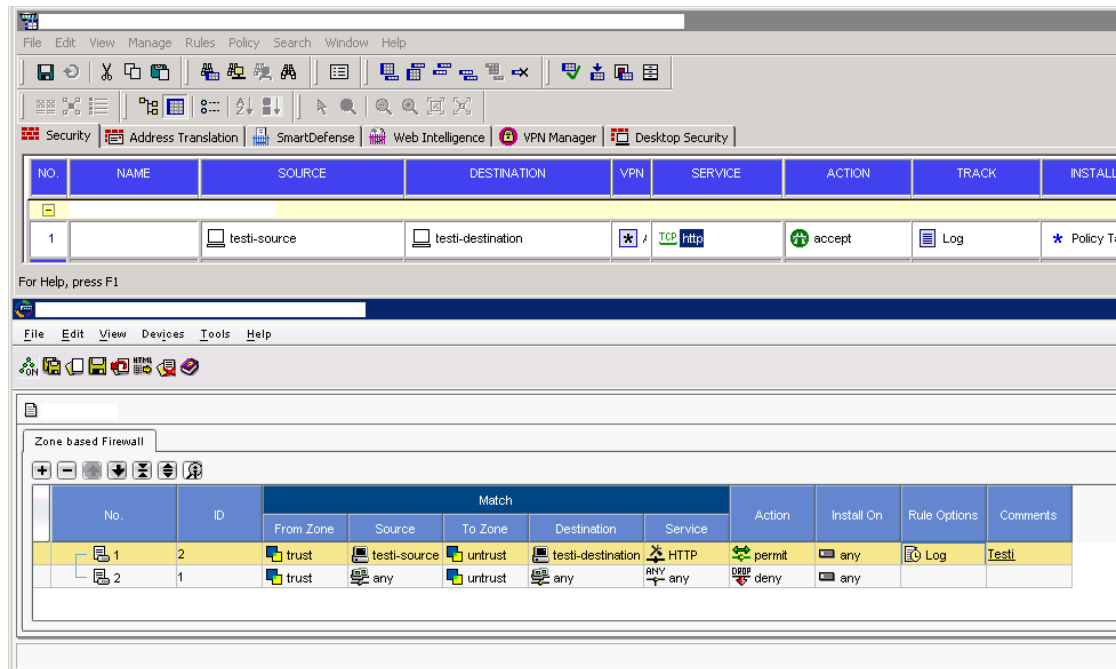
4.1.3 Sääntöjen luonti asiakkaan VSYS:lle

Vaikka erilaisia konvertointiohjelmiä sääntökantojen konvertoimiseen Check Pointilta Juniperiin on, ei niitä työssä käytetä. Kyseisiin ohjelmistoihin ei kannata luottaa niin paljoa, että niillä voisi konvertoida kaikkien asiakkaiden sääntökannat ja kopioida ne Juniperille. Joka tapauksessa pitäisi kokonaan tarkistaa, mitä ja miten ohjelma lopulta konvertoi säännöt. Lisäksi uudet säännöt pitäisi ymmärtää hyvin, jotta toteutusvaiheen

mahdollisessa vikatilanteessa ongelma ratkeaisi nopeasti. Samassa ajassa, kun konvertoituja sääntöjä käydään läpi ja korjataan mahdollisia virheitä, kopioidaan sääntökanta käsin Check Pointilta Juniperille mahdollisesti joitain sääntöjä hieman karsien. Lisäksi Check Pointilla ei ole sääntöjen alueita kuten Juniperilla ja yhteyksien osoitemuunnokset on toteutettu eri tavoin.

Sääntöjen kopioimista voi helpottaa tuomalla Check Pointin objektit asiakkaan VSYS:lle suoraan käyttämällä CLI:tä. Käytännössä tämä tapahtuu tuomalla Check Pointin objektit normaaliin Excel-taulukkaan, mitä varten Nokian IPSO:lle on asennettu oma ohjelmansa. Taulukkoon saadaan Check Pointilta tuotua IP-osoitteet, objektien nimet, kommentit sekä palveluja varten tarvittavat portit. Juniperia varten objekteille täytyy vielä miettiä oikeat alueet. Kun objektit on saatu taulukkoon, voidaan ne helposti muokata ScreenOS-komennoiksi esimerkiksi *set address "trust-vsysis-asiakas" "testiobjekti-1" 10.1.1.1 255.255.255.255 "Asiakkaan testipalvelin"* tai *set service "asiakas-http" protocol tcp src-port 1-65535 dst-port 81*. Muokkaamisen jälkeen kaikki objektit eli rivit voidaan kopioida asiakkaan VSYS:lle käyttämällä ScreenOS-käyttöjärjestelmää komentopohjaisesti. Jotta objektit saadaan näkymään oikein myös NSM:ään, täytyy muutoksien jälkeen VSYS tuoda NSM:lle kokonaisuudessaan, jolloin muutokset päivittyvät myös sinne.

Varsinainen sääntöjen luonti tehdään yksi kerrallaan ottamalla mallia Check Pointin säännöistä (kuva 15). Check Pointilla on myös omiin virtuaalimuureihin liittyviä avauksia, jotka voidaan olla tuomatta Juniperille. Osoitemuunnoksien tekeminen kuvataan seuraavassa luvussa.



Kuva 15. Hallintasovellukset. Ylhäällä Check Pointin SmartDashboard, alhaalla Juniperin NSM.

4.1.4 NAT-säännöt yleisesti ja niiden luonti asiakkaan VSYSLle

Check Pointilla on osoitemuunnoksille eli NAT-säännöille oma NAT-sääntökantansa. Varsinaisen sääntökannan läpikäymisen jälkeen Check Point käy sallitulle yhteydelle läpi NAT-sääntökannan. Mikäli yhteydelle löytyy vastine NAT-sääntökannasta, sille suoritetaan osoitemuunnos NAT-säännön mukaisesti. Jos IP-osoitteesta 1.1.1.1 sallitaan siis sääntökannassa FTP-yhteys osoitteeseen 2.2.2.2, käydään yhteydelle sääntökannan läpikäymisen jälkeen NAT-sääntökanta läpi, löytyykö sieltä esimerkiksi osoitemuunnos kaikelle liikenteelle, jonka kohde on 2.2.2.2. Juniperissa NAT-säännöt toteutetaan jo varsinaisessa säännössä. Mikäli edellä olevaan esimerkkiin siis halutaan tehdä osoitemuunnos Juniperilla, kyseinen toimenpide lisätään vain tähän sääntöön, ei erilliselle NAT-sääntökannalle. [29, s. 2–3; 30, s. 231–232.]

Check Pointilla NAT-metodeja on kaksi: Static ja Hide NAT. Static NAT on tarkoitettu yksi yhteen osoitemuunnosta varten, eli yleensä sitä käytetään sisäverkossa olevaan palvelimeen pääsyyn julkisen osoitteen avulla. Hide NAT on Check Pointin PAT (Port

Address Translation) eli porttimuunnos, jolla voidaan piilottaa useita sisäverkon palvelimia tai käyttäjiä yhden julkisen osoitteen taakse. Tämä onnistuu yhteyksien porttimuunnoksilla. Check Pointilla NAT-säännössä oleva IP-osoite voi olla mikä vain, ja sääntö voidaan toteuttaa jokaisella liitännällä jokaiseen suuntaan. Rajoituksia ei ole. [29, s. 2–3.]

Juniperilla NAT-metodeja on useita. Kohdeosoitteen muunnoksen voi suorittaa MIP:llä (Mapped IP), VIP:llä (Virtual IP) tai sääntöpohjaisella NAT-DST:llä. NAT-DST on yksisuuntainen ja tekee osoitemuunnoksen lisäksi myös porttimuunnoksen. NAT-DST on suunniteltu korvaamaan MIP- ja VIP-metodit ja sitä käytetään usein, sillä NAT-DST tukee minkä tahansa osoitteen käyttöä NAT-osoitteena, eikä sitä ole sidottu mihinkään liitântään. Mikäli NAT-osoitteena käytetään osoitetta, joka asiakkaalla ei ole normaalisti käytössä, täytyy tämä kyseinen NAT-osoite reitittää asiakkaan VSYS:n suuntaan, jotta paketti saapuu asiakkaan muurille oikein. NAT-DST tehdään pelkästään sääntöön, jossa se halutaan toteuttaa. [30, s. 232, 241, 243.]

MIP on kaksisuuntainen staattinen osoitemuunnos, joka konfiguroidaan sisääntulevalle liitännälle ja säännölle, jossa muunnos halutaan toteuttaa. Yleensä MIP-metodia käytetään demilitarisoidulla alueella oleville palvelimille, kuten web-palvelimille. Vanhemmissa ScreenOS-versioissa MIP-osoitteena voidaan käyttää julkista osoitetta muistakin verkoista kuin sisääntulevan liitännän verkosta vain jos tämä sisääntuleva liitântä on untrust-alueella. VIP-metodilla voidaan tehdä staattisia porttimuunnoksia sisääntulevassa liitännässä ja sitä voidaan käyttää muuntamaan kaksi eri julkista IP-osoitetta osoittamaan yhden sisäverkon palvelimen kahteen eri porttiin, joissa voi toimia eri palveluja. Käytännössä julkinen IP-osoite 1.1.1.1 voi osoittaa palvelimen 192.168.1.1 porttiin 80, kun taas julkinen IP-osoite 1.1.1.2 voi osoittaa saman palvelimen porttiin 81. Vanhemmissa ScreenOS-versioissa VIP-osoitteen verkko tuli olla untrust-alueella ja osoitteen oli oltava samassa verkossa sisääntulevan liitännän kanssa. [30, s. 232, 241, 243–244.]

Lähdeosoitteen muunnokseen Juniper tarjoaa sääntöpohjaista NAT-SRC:tä, joka on synonyymi DIP:lle (Dynamic IP). DIP:n lisäksi ulos lähtevä liitântä voidaan asettaa

NAT-tilaan, jolloin kaikki ulos lähtevä liikenne muunnetaan liitännän IP-osoitteen taakse. NAT-tilaa ei suositella kuin kahden liitännän palomuuureille. [30, s. 232, 256–257.]

NAT-SRC tai DIP suorittaa lähdeosoitteen ja porttimuunnoksen ulos lähtevällä liitännällä ja yleisin käyttö tälle on piilottaa yhden julkisen osoitteen taakse useita sisäverkon osoitteita. DIP-osoite konfiguroidaan ulos lähtevälle liitännälle ja sääntöön, jossa muunnos halutaan toteuttaa. Mikäli DIP-osoitteena halutaan käyttää osoitetta jostakin muusta verkosta kuin liitännän verkosta, johon DIP-konfiguroidaan, pitää liitännälle konfiguroida Extended IP (tai Extended DIP) eli pidennetty IP. Tällä Extended IP:llä voidaan liitännään asettaa ns. vale-IP, jota voidaan käyttää DIP-osoitteena normaalisti. Vastapäässä reitityksien täytyy huomioida Extended IP:n osoite. [30, s. 232, 236.]

Asiakkaiden säännöissä on yleisesti käytetty sääntöpohjaisia NAT-SRC- ja NAT-DST-metodeja. Check Pointilta täytyy tarkkaan haravoida, mitkä säännöt osuvat NAT-sääntökannan NAT-sääntöihin, jotta ne osataan luoda Juniperin sääntökannalle oikein. Tämän takia voi Juniperin sääntökannassa joutua karsimaan joitain Check Pointin yleisluontoisia sääntöjä, jotta osoitemuunnokset voidaan tehdä oikein.

4.1.5 Reititykset asiakkaan VSYS:llä

Virtuaalimuurien eli VSYS:ien reititystaulun oletusreitinnä toimii reitti Internetin suuntaan eli jaetulle virtuaaliselle untrust-vr -reitittimelle, josta liikenne jatkaa Capgeminin sisäverkon kautta kohti Internetiä. Jotta liikenne osaisi Internetistä tulla takaisin asiakkaan VSYS:lle, täytyy untrust-vr -reitittimelle tehdä staattiset reitit asiakkaan jokaiselle julkiselle verkolle. Reitityksessä liikenne näille verkoille osoitetaan kulkemaan kohti asiakkaan VSYS:ä. Nämä reititykset tehdään VSYS:n alta untrust-vr:lle, jolloin kyseiset reitit eivät näy tältä jaetulta reitittimeltä esimerkiksi muiden asiakkaiden VSYS:stä. Tämä toimenpide piilottaa reitit muilta tällä jaetulla reitittimellä.

Edellä oleva untrust-vr-reititys voidaan toteuttaa etukäteen, sillä Internetistä tuleva liikenne ei vielä reitity sisäverkossa olevilla reitittimillä Juniperille. Nämä reititykset muutetaan reitittymään Juniperin suuntaan vasta palomuurin vaihdossa. Lisäksi kaikki muut yhteydet sisäverkosta, eli yhteydet VPN-keskittimiltä Juniperille ja yhteydet sisäverkon palvelimilta yleiseen VRF:ään, reititetään vasta palomuurin vaihdossa. Komennot näiden vanhojen reitityksien poistoon ja uusien reitityksien luomiselle voidaan tehdä valmiiksi tekstitiedostoon, josta ne voidaan kopioida suoraan reitittimille, kun palomuurialusta vaihdetaan. Lisäksi tehdään tekstitiedosto paluureitityksistä eli tehdään vastaavat reititykset toisinpäin. Paluutiedostossa on siis komennot uusien reitityksien poistamiseksi ja vanhojen reitityksien palauttamiseksi, jolloin komennot voidaan suoraan kopioida reitittimille. Tällöin paluu Check Pointille onnistuu hyvin nopeasti, mikäli jokin meni vikaan.

4.2 Testaus

Koska VSYS:n toimivuutta asiakkaan sääntökantoihin on mahdotonta testata, sillä asiakkaan verkkoympäristöt sisältävät useita erilaisia palvelimia eri palveluineen, palomuurivaihdos tehdään ilman kattavaa testausta. Muutamien NAT-osoitteiden toimivuutta on testattu ennen vaihtoa, jotta voidaan olla varmoja niiden toimivuudesta myös tuotannossa. Mikäli yhteydet eivät jostain syystä toimi uudella palomuurilla oikein eikä ratkaisua vaihdon aikana asiaan löydy, on paluu vanhalle muurille helppoa. Näin ongelmaa voidaan selvittää rauhassa ja mahdollisesti testata tätä toimimatonta yhteyttä erikseen. Kun ongelma yhteyksien toimimattomuuteen on saatu ratkaistua, voidaan asiakkaan kanssa sopia uusi aika palomuurialustan vaihdolle. Seuraavan luvun lopussa kerrotaan, kuinka paluu vanhalle muurille on valmisteltu ja kuinka se voidaan tarpeen vaatiessa toteuttaa.

4.3 Toteutus

Varsinainen työ itse vaihdossa on vain kopioida ennalta valmistellut ja dokumentoidut komennot oikeille kytkimille ja reitittimille. Komennot poistavat ensin yhteydet asiakkaan VS:ään, jonka jälkeen ne siirretään kulkemaan asiakkaan VSYS:lle.

Siirtokerroksella liitántäkytkimiltä poistetaan asiakkaan VLAN:t niistä liitännöistä, joihin Nokian palomuurit ovat kytketty. Tämän jälkeen asiakkaan palvelimien liikenne ei enää oletusyhdydskäytävän mukaisesti mene Nokian palomuurissa olevalle asiakkaan VS:lle. Seuraavaksi asiakkaan VLAN:t lisätään niihin liitántäkytkimien liitántöihin, joihin Juniperin palomuurit on kytketty ja joiden kautta liikenne kulkee asiakkaan virtuaalisille liitännöille. VLAN:ien lisäämisen jälkeen asiakkaan palvelimien liikenne kulkee oletusyhdydskäytävän mukaisesti Juniperin fyysisten liitántöjen kautta kohti asiakkaan virtuaalisia liitántöjä. VSYS:n virtuaalisissa liitännöissä käytetään edelleen samoja IP-osoitteita, jotka olivat VS:llä käytössä. Päällekkäisyyksiä IP-osoitteissa ei tule, koska yhteydet VS:lle ovat tarkoituksellisesti poikki.

Siirtokerroksen VLAN:ien poistojen ja -lisäyksien jälkeen asiakkaan yhteydet toimivat asiakkaan palvelimien kesken, mikäli sääntökanta on tehty VSYS:lle oikein. Tämän jälkeen on aika paneutua verkkokerrokseen ja reitityksiin. Mikäli VSYS:n reititykset on etukäteen oikein tehty, liikenne kulkee ulospäin oikein VSYS:n reititystaulujen mukaisesti. Yhteydet eivät silti toimi, sillä liikenne takaisinpäin kulkee vielä VS:lle sisäverkossa sijaitsevien reitittimien reititystaulujen mukaisesti. Valmisteluvaiheessa valmisteltujen ja dokumentoitujen komentojen avulla vanhat reititykset saadaan helposti poistettua, jonka jälkeen sisäverkossa oleville reitittimille voi lisätä uudet reitit osoittamaan kohti asiakkaan uutta VSYS:ä. Uusien reitityksien lisäämisen jälkeen liikenne tulee ulkopuolelta oikein asiakkaan VSYS:lle, jolloin yhteyksien tulisi toimia.

Kaikki edellä oleva eli varsinainen vaihto suoritetaan ajankohtana, joka on asiakkaan kanssa erikseen sovittu. Koska vaihdosta joka tapauksessa aiheutuu hetkellisiä katkoksia asiakkaan yhteyksiin, suoritetaan vaihdot yleensä asiakkaasta riippuen viikonloppuisin tai arki-iltais. Ongelmatilanteissa katkokset voivat kestää pidempääkin, mikä pitää

ajankohtaa ehdottaessa huomioida. Varsinainen vaihto ei kuitenkaan vielä ole ohi, sillä yhteyksiä pitää testata. Verkkopuolelta palvelimien yhteyksien testaus ICMP-paketeilla ja lokien seuranta ei riitä, sillä vaikka palvelin itse vastaisikin paketteihin mainiosti, voi palvelimessa toimiva palvelu olla silti toimimaton. Testauksia varten tarvitaan tietoliikenneasiantuntijan lisäksi joko Capgeminin sisältä palvelinasiantuntijoita tai vaihtoehtoisesti asiakkaan omia asiantuntijoita testaamaan yhteyksiä. Kun jokin palvelu todetaan testauksessa toimimattomaksi, pyritään se saman tien korjaamaan. Ongelma voi johtua yksinkertaisesti vaikka sääntökannasta uupuneesta säännöstä tai osoitemuunnoksen puuttumisesta.

Kun kaikki yhteydet ovat todettu toimiviksi, voidaan vaihto todeta onnistuneeksi. Vaihdon jälkeen palomuuria ylläpidetään normaaliin tapaan, mutta tällä kertaa toimenpiteet tehdään VS:n sijaan VSYS:lle. Asiakkaan CMA voidaan Provider-1:stä näin ollen sammuttaa, jottei sieltä lisättäisi epähuomiossa uusia sääntöjä. Lisäksi onnistuneen vaihdon jälkeen on syytä siivota muut asiakkaan VS:ään liittyneet konfiguraatiot esimerkiksi käyttämättömäksi jääneet VLAN:t liitännäkytkimiltä, joita kautta asiakkaan liikenne ennen VS:lle kulki.

Mikäli jokin kriittinen yhteys ei kaikesta huolimatta ala VSYS:llä toimia, on paluu VS:lle yhtä helppo kuin VSYS:lle siirtyminen. Paluuta varten komennot on valmisteluvaiheessa tarkkaan dokumentoitu, joten niiden syöttäminen tarvittaville kytkimille ja reitittimille onnistuu helposti. Paluukomennoissa on huomioitu uusien VLAN:ien ja reitityksien poisto sekä niiden lisäykset, kuten ne olivat ennen vaihtoa. Paluun jälkeen liikenne kulkee taas asiakkaan VS:lle kuin ennenkin, jolloin toimimattomien yhteyksien pitäisi palata jälleen normaaliin tilaan. Paluun jälkeen selvitetään, mikä vaihdossa epäonnistui ja mahdollisesti testataan toimimattomia yhteyksiä testiympäristössä. Kun ongelma on selvitetty, voidaan vaihtoa yrittää uudestaan.

5 Yhteenveto

Tätä kirjoittaessa on kolme asiakkaan Nokian palomuurialustalla toimivaa VS:ää siirretty onnistuneesti Juniperin palomuurialustan VSYS:lle. Kaikki vaihdot onnistuivat hyvin lukuun ottamatta muutamaa inhimillistä erehdystä valmisteluvaiheessa. Esimerkkinä mainittakoon asiakkaan VS:llä ollut Internet-liikennöintiä varten yleinen palomuurisääntö, jonka lähdepalvelimista avattiin tiettyjä portteja kaikkialle. Sääntö luotiin Juniperiin käyttäen kohdealueena untrust-aluetta eli Internetiä. VS:llä tästä yleisestä säännöstä kulki myös muutama yhteys VPN-keskittimen suuntaan, jotka eivät VSYS:llä säännön kohdealueen takia toimineetkaan. Tämä sekä muut vastaavanlaiset pienet haasteet selvitettiin nopeasti palomuurivaihdon aikana, eikä niistä koitunut varsinaista haittaa. Työ on edennyt hyvin ja näiden kolmen asiakkaan kohdalla toteutus on onnistunut suunnitelmien mukaisesti. Asiakkaiden palomuurien hallinta jatkuu normaalisti VSYS:n kautta eikä asiakkaalle itselleen näkyvää muutosta, lukuun ottamatta lyhyitä katkoksia, vaihdoksesta tullut.

Työn suurin haaste on ajankäyttö, koska työ tehdään muiden töiden ohella. Vaikka itse toteutus ei vie muutamaa tuntia kauempaa, kuluu valmisteluihin huomattavasti enemmän aikaa. Valmisteluissa täytyy kiinnittää erityistä huomiota muun muassa NAT-sääntöjen sekä erilaisten yleisten sääntöjen (edellä kuvattu tapaus) toimivuuteen, sillä ne on palomuurialustoilla eri tavoin toteutettu. Huolellinen valmistelu vie aikaa, mutta estää ongelmatilanteiden syntymisen itse vaihdon aikana, mikä voi säästää aikaa jälkeenpäin.

Muiden asiakkaiden sääntökantojen kopiointi Nokian palomuurialustalta Juniperille on täydessä vauhdissa eikä varsinainen vaihtokaan ole ongelma, koska kolmen palomuurin vaihdon jälkeen työryhmällä on kokemuksia jaettavana itse toteutuksesta. Kaikkien VS:ien pitäisi olla siirretty VSYS:lle alkukesän 2009 aikana, jonka jälkeen koko Nokian palomuurialusta voidaan purkaa konesalista. Nykyisellä tahdilla suunnitellussa aikataulussa pysytään.

Lähteet

- 1 Check Point Signs Agreement to Acquire Nokia's Security Appliance Business. (WWW-dokumentti.) Check Point Software Technologies Ltd. <http://www.checkpoint.com/press/2008/checkpoint_to_acquire_nokia_sab_221208.html>. Päivitetty 22.12.2008. Luettu 2.2.2009.
- 2 List of Nokia products. (WWW-dokumentti.) Wikipedia. <http://en.wikipedia.org/wiki/List_of_Nokia_products#Security_solutions>. Päivitetty 4.2.2009. Luettu 5.2.2009.
- 3 Nokia IP Security Solutions, Nokia IP1220. (WWW-dokumentti.) Nokia. <http://europe.nokia.com/NOKIA_BUSINESS_26/Europe/Products/Security_Products/Firewall_VPN/Nokia_IP1220/nokia_ip1220_datasheet_emea.pdf>. Päivitetty 16.8.2006. Luettu 26.1.2009.
- 4 Nokia Network Security, Product Summary Guide. (WWW-dokumentti.) Nokia. <http://www.nokiaforbusiness.com/Page%20Content/Mobilize%20your%20business/Knowledge%20center/Guides/Nokia_NetworkSecurityProductSummaryGuide_PUBLIC_03JUN08.pdf>. Päivitetty 13.6.2008. Luettu 26.1.2009.
- 5 Hourihan, Kyle X., Kligerman, Daniel, Bautts, Tony, Shimonski, Robert J., Greene, Kevin, Amon, Cherie & Maxwell, Doug. Nokia Network Security Solutions Handbook. Yhdysvallat: Syngress Publishing, Inc., 2002.
- 6 Rack unit. (WWW-dokumentti.) Wikipedia. <http://en.wikipedia.org/wiki/Rack_unit>. Päivitetty 3.2.2009. Luettu 5.2.2009.
- 7 Nokia IP Clustering. (WWW-dokumentti.) Nokia. <http://www.nokiaforbusiness.com/Page%20Content/Mobilize%20your%20Business/Knowledge%20Center/White%20Papers/WhitePaper_IPClustering.pdf>. Päivitetty 30.1.2007. Luettu 26.1.2009.
- 8 Virtual Router Redundancy Protocol. (WWW-dokumentti.) Wikipedia. <<http://en.wikipedia.org/wiki/VRRP>>. Päivitetty 27.1.2009. Luettu 27.1.2009.
- 9 Alustanhallinta. (WWW-dokumentti.) Computerlinks Oy. <<http://www.computerlinks.fi/html/nokia.php?spid=1207>>. 2009. Luettu 28.1.2009.
- 10 SmartCenter. (WWW-dokumentti.) Check Point Software Technologies Ltd. <http://www.checkpoint.com/products/downloads/smartcenter_datasheet.pdf>. Päivitetty 26.2.2008. Luettu 28.1.2009.
- 11 Provider-1/SiteManager-1. (WWW-dokumentti.) Check Point Software Technologies Ltd. <http://www.checkpoint.com/products/downloads/provider-1_datasheet.pdf>. Päivitetty 5.3.2007. Luettu 3.2.2009.

- 12 Check Point Software: SmartDashBoard. (WWW-dokumentti.) Check Point Software Technologies Ltd.
<http://www.checkpoint.com/products/smartcenter/smartcenter_management.html>. 2009. Luettu 28.1.2009.
- 13 Check Point Offers Provider-1 NG FP-1 for Managing Multiple Firewalls. (WWW-dokumentti.) Network computing.
<<http://www.networkcomputing.com/1306/1306sp6.html>>. Päivitetty 18.2.2002. Luettu 3.2.2009.
- 14 Check Point VSX, Version NGX R60. (WWW-dokumentti.) Check Point Software Technologies Ltd.
<http://updates.checkpoint.com/fileserver/ID/5591/FILE/CheckPoint_VSX_NGX_UserGuide.pdf>. 2006. Luettu 2.2.2009.
- 15 Virtual Firewalls part 1. Checkpoint VSX. (WWW-dokumentti.) NetLeets.
<<http://www.netleets.com/2008/09/vsx.htm>>. 2008. Luettu 2.2.2009.
- 16 VPN-1/FireWall-1 VSX. (WWW-dokumentti.) Check Point Software Technologies Ltd. <http://www.securitytechnet.com/resource/rsc-center/vendor-wp/checkpoint/vsx_ds.pdf>. 2003. Luettu 2.2.2009.
- 17 Juniper Networks Secures and Assures Networks with Eight Security Platforms and Major Threat Control Enhancements. (WWW-dokumentti.) Juniper Networks, Inc. <<http://www.juniper.net/company/presscenter/pr/2005/pr-050509.html>>. 2005. Luettu 6.2.2009.
- 18 Juniper Networks ISG Series / ISG Series GPRS. (WWW-dokumentti.) Juniper Networks, Inc.
<http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/isg_series_slash_gprs/>. 2009. Luettu 6.2.2009.
- 19 Juniper Networks ISG Series. (WWW-dokumentti.) Juniper Networks, Inc.
<<http://www.juniper.net/products/integrated/dsheet/110036.pdf>>. 2008. Luettu 6.2.2009.
- 20 Integrated Security Gateway (ISG) Series Architecture. (WWW-dokumentti.) Juniper Networks, Inc.
<http://www.juniper.net/solutions/literature/white_papers/200117.pdf>. 2004. Luettu 6.2.2009.
- 21 Cameron, Rob, Woodberg, Brad, Madwachar, Mohan Krishnamurthy, Swarm, Mike, Wyler, Neil R., Albers, Matthew & Bonnel, Ralph. Configuring Juniper Networks NetScreen & SSG Firewalls. Yhdysvallat: Syngress Publishing, Inc, 2007.

- 22 Juniper Networks Network and Security Manager. (WWW-dokumentti.) Juniper Networks, Inc. <<http://www.juniper.net/products/integrated/dsheet/110018.pdf>>. 2008. Luettu 10.2.2009.
- 23 Virtualization Technologies Overview. (WWW-dokumentti.) Juniper Networks, Inc. <http://www.juniper.net/solutions/literature/white_papers/200103.pdf>. 2005. Luettu 11.2.2009.
- 24 Virtual Firewalls part 2. Juniper Vsys. (WWW-dokumentti.) NetLeets. <<http://www.netleets.com/2008/10/vsys.htm>>. 2008. Luettu 11.2.2009.
- 25 Lammle, Todd. CCNA, Cisco Certified Network Associate. Yhdysvallat: John Wiley and Sons, 2007.
- 26 Menga, Justin. CCNP Self-Study: Switching. Yhdysvallat: Cisco Press, 2004.
- 27 VRF. (WWW-dokumentti.) Wikipedia. <<http://en.wikipedia.org/wiki/VRF>>. Päivitetty 5.1.2009. Luettu 21.2.2009.
- 28 Understanding Spanning Tree Protocol - the Fundamental Bridging Algorithm. (WWW-dokumentti.) O'Reilly Media. <http://www.oreillynet.com/pub/a/network/2001/03/30/net_2nd_lang.html>. Päivitetty 30.3.2001. Luettu 21.2.2009.
- 29 Noble, Jim, Maxwell, Doug, Hourihan, Kyle X., Stephens, Robert, Stiefel, Barry J., Amon, Cherie & Tobkin, Chris. Check Point NG VPN-1/FireWall-1 Advanced Configuration and Troubleshooting. Yhdysvallat: Syngress Publishing, Inc., 2003.
- 30 Brunner, Stefan, Davar, Vik, Delcourt, David, Draper, Ken, Kelly, Joe & Wadhwa, Sunil. ScreenOS Cookbook. Yhdysvallat: O'Reilly Media Inc, 2008.