Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Aku Leskinen

Testilaboratorion palomuurilaitteiden päivitys

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

23.5.2019

Tekijä(t) Otsikko Sivumäärä Aika	Aku Leskinen Testilaboratorion palomuurilaitteiden päivitys 26 sivua 23.5.2019
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Osaamisaluepäällikkö Janne Salonen Tuoteryhmäpäällikkö yrityksen henkilö

Opinnäytetyö tehtiin työelämälähtöisenä projektina, jossa testilaboratorion vanhentuneet palomuurilaitteet päivitettiin uudempaan laitemalliin.

Työn suurin osuus oli tekninen asennustyö, jossa tehdasasetuksilla olevat palomuurilaitteet kytkettiin ja konfiguroitiin toimimaan tuotantokäyttöön kelpaavaksi toimivaksi kokonaisuudeksi. Vanhan ympäristön verkkotopologiaa, reititystä ja palomuurisäännöstöä käytettiin hyväksi uuden ympäristön rakentamisessa siltä osin kuin se uusien laitteiden muuttuneiden ominaisuuksien mukaan oli mahdollista.

Työ alkoi verkkoympäristön suunnittelulla ja verkkokuvien piirtämisellä, jonka jälkeen laitteet asennettiin testilaboratorioon. Tärkeä osa työtä oli myös Junos käyttöjärjestelmään tutustuminen koska sitä ei ollut aiemmin laboratoriossa käytetty. Tuotantokäyttöön kelpaavan ympäristön rakentaminen täysin konfiguroimattomista laitteista oli haastavaa ja aikaa vievää työtä.

Ympäristö rakennettiin viranomaisen Kansallisen Turvallisuusauditointikriteeristön (Katakri) mukaisesti ja sillä oli suuri vaikutus laitteiden konfiguraatioihin ja laitevalintojen tekemiseen.

Rakennettu ympäristö saatiin toimimaan odotuksia vastaavalla tavalla ja sitä voitaisiin jatkossa käyttää Katakri-vaatimuksiin sitoutuneen tai muun tietoturvaa arvostavan yrityksen tietoliikenneverkon rakentamisen mallina.

Avainsanat	palomuuri, reititys, tietoturva, Katakri

Author(s) Title Number of Pages Date	Aku Leskinen Test laboratory firewall upgrade 26 pages 23 May 2019
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data networks
Instructor(s)	Janne Salonen, Head of Department (ICT) Company employee, Product group manager

Subject for this final year project came from work related project in which test laboratory end of life firewalls needed upgrade to a newer hardware.

Biggest part of the final year project was the technical installation work. Firewalls with factory default settings were connected and configured to form well-functioning environment that would be suitable for production use. Network topology, routing and firewall policies from old environment were used as a base configuration for this work.

Work began with planning and drawing out network diagrams following the actual installation of all equipment in the test laboratory. One of the important learning goals was the Junos operating systems which was not used in the laboratory earlier. Installing the environment from zero configuration to a production capable network was laborious and time-consuming work.

Device configurations had to meet the national security audit criteria, which had big impact to the final configuration and the selection of devices that could be used.

Finally, goals were achieved as planned and the environment that was built could be used as a secure model for any organizations network. Especially organizations who are committed to national security audit criteria or those who value network security in general, could be the possible customers.

Keywords	firewall, routing, network security, audit

Sisällys

Lyhenteet

ALG	Application Layer Gateway. Ohjelma, joka tarkastelee OSI-mallin 7 kerroksen liikennettä.
EOL	End Of Life. Tuote jonka elinkaari on loppunut.
GARP	Gratuitous Address Resolution Protocol. Atribuuttien verkossa rekisteröimiseen käytetty protokolla.
HA	High Availability. Järjestelmän korkea saatavuus.
ICMP	Internet Control Message Protocol. TCP/IP perheeseen kuuluva kontrolliprotokolla.
IDS	Intrusion Detection System. Tunkeutumisen havaitsemisjärjestelmä.
IKE	Internet Key Exhange. Avainten vaihto.
IP	Internet Protocol. Internet protokolla.
IPsec	Internet Protocol Security. Joukko TCP/IP perheeseen kuuluvia protokollia.
IPS	Intrusion Prevention System. Tunkeutumisen estojärjestelmä.
Katakri	Viranomaisen kansallinen turvallisuusauditointikriteeristö.
L2	Layer 2 in OSI-model. Osi-mallin 2 kerros.
L3	Layer 3 in OSI-model. Osi-mallin 3 kerros.
MAC	Media Access Control Address. Verkkosovittimen ethernet-verkossa yksilöivä osoite.
NAT	Network Address Translation. Osoitteenmuutostekniikka.
OSI-malli	Open system Interconnection Reference Model. Tiedonsiirtoprotokollia kuvaava malli.
RE	Routing Engine. Reititin.

RETH	Redundant Ethernet interface. Redundanttinen portti.
RSA	River-Shamir-Adleman Cryptosystem. Network Security company. Salausalgoritmi. Tietoturvaan erikoistunut yritys.
UTM	Unified Threat Management. Juniperin käyttämä uhkienhallintatyökalu.
VPN	Virtual Private Network. Virtuaalinen salattu verkkoyhteys.

1 Johdanto

Opinnäytetyön tehtävänä oli työpaikan testilaboratorion palomuurilaitteiden päivittäminen uudempaan laitemalliin. Testiympäristön vanhat End Of Life (EOL) Juniper SSG-520 -palomuuriklusterit korvattiin Juniper SRX-550 -palomuureilla. Kyseessä oli ensisijaisesti teknologia tai niin sanottu “rautapäivitys” jossa verkkoympäristö ja palomuurisäännöstö säilyivät ennallaan. Testiympäristön tarkoitus on kokeilla ja testata laitteistoa ja niiden valmiutta mahdollista tuotantokäyttöä varten.

Vanha ympäristö muodostui kolmesta palomuuriklusterista, joiden välille oli rakennettu IPSEC Virtual Private Network (VPN) -yhteys. Yksi klustereista simuloi datakeskuksen palomuuria, jonka takana pääosa verkkoympäristön palveluista sijaitsi. Kaksi muuta klusteria simuloivat pienempiä käyttöpaikkoja, jotka olivat yhteydessä datakeskukseen sekä toisiinsa datakeskuksen kautta. VPN-yhteydet oli rakennettu palomuurien eteen sijoitetuilla erillisillä salaimilla. Palomuuriklusterit olivat yhteydessä toisiinsa salainten muodostaman VPN-tunnelin kautta. Koska salainten rooli oli pelkästään VPN-yhteyden muodostaminen ja ne olivat palomuurien kannalta katsottuna lähes näkymättömät, niiden konfiguraatiota ei lähemmin tarkasteltu tässä työssä.

Vanhojen SSG-520 -palomuurien käyttöjärjestelmä oli NetScreen ja uusissa SRX-550 -palomuureissa oli Junos. Käyttöjärjestelmän vaihtuminen toi joitain haasteita konfiguraation siirtämiseen. Palomuurisäännöstön suuren koon takia sääntökonfiguraation siirtämiseen käytettiin osittain Juniperin kääntötyökalua, joka käänsi Netscreen-komennot Junos-komennoiksi. Laitteiden muu peruskonfiguraatio tehtiin alusta asti kokonaan uusiksi. Peruskonfiguraatiolla tarkoitetaan muun muassa porttien, IP-osoitteiden, Security Zone-asetusten, kovennusten ja reitityksen konfiguraatiota.

Vanha palomuuriympäristö oli rakennettu viranomaisen kansallisen turvallisuusauditointikriteeristön (Katakri) vaatimusten mukaisesti ja tämä täytyi huomioida myös uutta ympäristöä rakennettaessa.

Työ aloitettiin suunnittelulla ja verkkokuvan piirtämisellä, jonka jälkeen laitteet asennettiin testilaboratorioon. Lopputuloksena oli toimiva verkkoympäristö, joka oli valmis tuotantokäyttöön.

2 Ympäristön kuvaus

Testiympäristö muodostui datakeskuksesta, jonka palvelimilla suurin osa verkon käyttämistä palveluista sijaitsi sekä kahdesta muusta käyttöpisteestä. Verkon rakenteena oli tähtitopologia, jossa kaikki verkkoliikenne kulki ensin datakeskukseen, josta se reititettiin edelleen eteenpäin, mikäli kohteena oli jokin muu kuin datakeskuksessa sijaitseva palvelu. Verkkoympäristö olisi tällaisenaan soveltunut minkä tahansa yrityksen tietoliikenneverkoksi, vaikka tähtitopologia ei vikasietoisuutensa puolesta olekaan paras mahdollinen ratkaisu. Solmuverkko (Mesh network) olisi vikasietoisin, koska siinä kaikki käyttöpaikat olisivat yhteydessä suoraan toisiinsa. Solmuverkossa yhden käyttöpaikan vikaantuminen ei lamauttaisi koko verkkoa.

Työasemaverkkoja oli kaikilla kolmella käyttöpaikalla. Datakeskuksen työasemien pääsy palvelinverkkoihin toteutettiin suoraan datakeskuksen lähiverkossa ja käyttöpisteiden liikenne reititettiin datakeskukseen VPN-tunneleita pitkin. Kaikkien työasemaverkkojen ja palvelinverkkojen väliset palomuurisäännöt oli tehty deny all -periaatteella, jossa vain harkitut ja tarpeelliset palvelut oli sallittu ja kaikki muu verkkoliikenne kielletty. Työasemien ja palvelinten välisen verkkoliikenteen turvallisuutta oli lisäksi parannettu lisäämällä palomuurisääntöihin erillinen RSA-autentikaatiokerros. Kun työaseman käyttäjän verkkoliikenne osuu palomuurisääntöön niin liikenne ohjataan vielä erilliselle autentikointipalvelimelle. Vasta käyttäjän tunnistauduttua palvelimelle sääntö sallii liikenteen kohteeseen.

Katakri-vaatimusten mukaisesti kaikki verkkolaitteet ja palvelimet on asetettu lähettämään lokitietonsa keskitettyyn lokienhallintajärjestelmään.

3 Palomuurien toiminta

3.1 Tilattomat ja tilalliset palomuurit

Palomuurit ovat olleet jo pitkään tärkeä osa yritysten ja organisaatioiden tietoverkkoa. On tavallista, että myös tavallisen kodin verkkoa suojataan palomuurilla. Palomuuri toimii verkon “vartijana” suojatessaan sisäverkkoa ulkomaailmalta ja sillä voidaan rajata ja valvoa lähiverkon omaa sisäistä verkkoliikennettä.

Verkkojen välisen liikenteen rajaamiseen käytetään perinteisesti lähde ja kohde IP osoitteita, porttinumeroita ja protokollatyyppiä. Palomuuri tarkastaa sen lävitse kulkevan liikenteen ja päättää mitkä datapaketit sallitaan ja mitkä estetään. Periaatteet siitä minkä tyyppinen liikenne halutaan sallia ja mikä kieltää määritellään palomuurisäännöstössä (firewall policy) tai pääsylistoissa (access list).

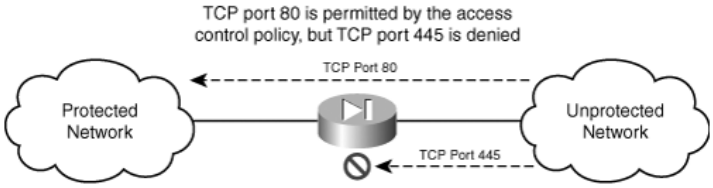
Internetissä tiedetään olevan paljon palomuureja, jotka on suunniteltu huonosti ja niiden konfiguraatiossa on virheitä. Tämän takia konfiguraation suunnittelu ja tuotannossa olevien laitteiden säännölliset tarkastukset ovat tärkeitä. [1]

Palomuurin olisi pystyttävä suorittamaan vähintään seuraavat tehtävät:

- Verkkoliikenteen hallinta ja kontrollointi
- Verkossa olevien resurssien suojaaminen
- Liikenteen välittäjänä toimiminen
- Autentikointi
- Tapahtumien hallinta ja tallentaminen. [2]

Pakettien tarkastuksessa (packet inspection) data tarkastetaan ja prosessoidaan jotta voidaan päätellä, tuleeko kyseinen liikenne sallia vai kieltää. Ensimmäisen sukupolven tilattomat (Packet-filtering Firewall) palomuurit toimivat tällä perusteella ja käyttävät suodatuksessa seuraavia elementtejä:

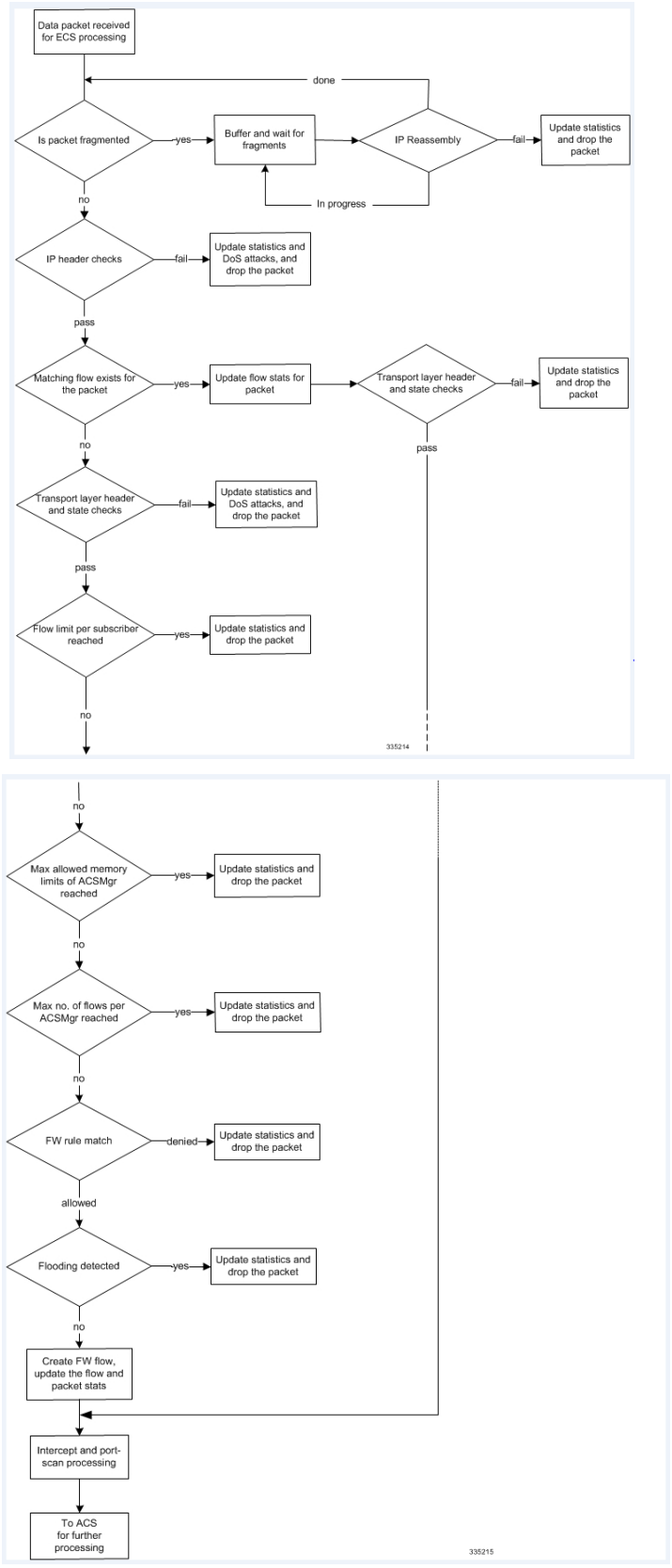
- Lähde IP-osoite
- Lähde portti
- Kohde IP-osoite
- Kohde portti
- IP-protokolla
- IP-paketin otsikkokentän tiedot. (data flags, sequence number, checksums ja payload information)



Kuva 1, Palomuuri estää ei-sallitun palvelun ulkoverkosta. [2]

Tilaton palomuuri tarkastaa jokaisen paketin ja tekee päätöksensä jatkokäsittelystä sen perusteella. Tilallinen palomuuri (Stateful Firewall) tarkastaa tämän lisäksi aikaisemmin hyväksyttyjä paketteja selvittääkseen kuuluuko liikenne jo aikaisemmin aloitettuun keskusteluun. Tilallinen palomuuri voi estää paketin saapumisen ulkoverkosta sisäverkkoon kahden laitteen välillä, ellei sisäverkon laite ole ensin ottanut yhteyttä ulkoverkon laitteeseen. Tästä johtuu se, että tilallisissa palomuureissa palomuuriavauksia ei tarvitse tehdä kahteen suuntaan koska paluuliikenne sallitaan osana olemassa olevaa keskustelua tai sessiota. Jos sisäverkossa oleva tietokone lähettää ICMP-paketin internetissä olevaan Googlen DNS-osoitteeseen niin tarvitaan vain yksi sääntö palomuuriin: lähde IP-osoite 192.168.1.50, kohde IP-osoite 8.8.8.8 ja protokolla ICMP. Jos kyseessä olisi perinteinen tilaton palomuuri, avaus tulisi tehdä myös toiseen suuntaan, joka sallisi osoitteen 8.8.8.8 ICMP-vastauksen takaisin sisäverkkoon.

Seuraava kaavio havainnollistaa pakettien prosessointia tilallisessa palomuurissa:

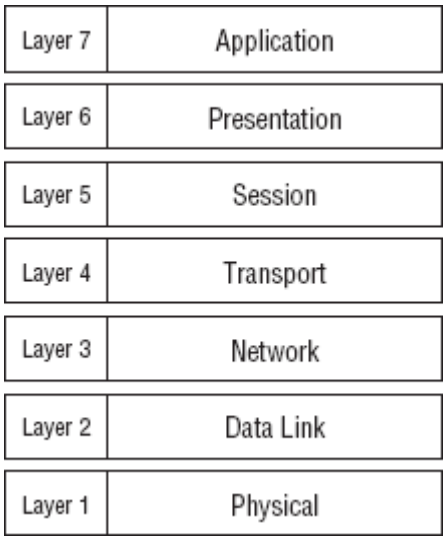


Kuva 2, IP-paketin käsittely tilallisessa palomuurissa. [3]

3.2 OSI-malli

OSI-viitemalli on ISO:n kansainvälinen standardi ISO/IEC 7498-1. Sitä on usein käytetty tietoliikenteen käsitemallina havainnollistamaan kuinka tiedonsiirtoprotokollat yhdistyvät toisiin seitsemässä eri kerroksessa. Mallissa ylempi kerros käyttää alemman kerroksen palveluja ja tarjoaa palveluja eteenpäin itseään ylemmälle kerrokselle. Kullakin kerroksella on käytössään tiettyjä protokollia. OSI-malli on kehitetty tietoliikennejärjestelmien suunnitteluun. Mallista on myös apua käytännön työelämässä, kun tehdään esimerkiksi vianselvitystä tietoliikenneympäristössä. Vianselvityksen aikana voidaan viitata esim. L2 (kerros 2) tai L3 (kerros 3) -kerroksiin, jolloin on selvää mitä osaa verkosta ja sen laitteista kulloinkin tarkoitetaan. [4]

OSI-mallin seitsemän kerrosta ovat:



Kuva 3, OSI-malli [4].

Tässä työssä liikuttiin suurimmaksi osaksi OSI-mallin kerroksilla 2 ja 3.

4 Vikasietoinen järjestelmä

Sekä vanhan että uuden ympäristön palomuurit toimivat HA (High Availability) -klusterissa. HA tarkoittaa, että järjestelmän saatavuus tai vikasietoisuus pyritään pitämään

mahdollisimman korkealla tasolla ja että palvelussa esiintyisi mahdollisimman vähän katkoksia. Klassinen esimerkki palvelun korkeasta saatavuudesta on puhelimen käyttö. Hyväksymme ehkä sen, että puhelinverkon ei tarvitse toimia vuoden jokaisena päivänä tai tuntina mutta odotamme sen kuitenkin toimivan joka kerta kun haluamme soittaa puhelun.

Vikasietoisuus voi tarkoittaa esimerkiksi kahdennettuja komponentteja, jotka turvaavat laitteen toiminnan tai kahdennettua järjestelmää, joka taas turvaa palveluita. Vikasietoisuutta on oltava aina komponentti tasolta järjestelmä tasolle saakka mutta lopulta kaikki tähtää siihen, että yritys ja sen palvelut ovat käyttäjien saatavilla mahdollisimman suuren osan ajasta.

Viiden yhdeksikön (Five 9s) konsepti kuvaa saatavuuden mittaamista vuoden aikana. Viisi yhdeksikköä kuvaan prosenttilukuna aikaa jona järjestelmän tulisi olla saatavilla vuoden aikana. [5]

Taulukko 1, Viisi yhdeksikköä. [5]

Availability	Downtime in one year
90%	876 hours
99%	87.6 hours
99.9%	8.76 hours
99.99%	52.6 minutes
99.999%	5.26 minutes
99.9999%	31.5 seconds

Tässä työssä rakennetun ympäristön tapauksessa kussakin klusterissa oli aina kaksi palomuuria. Jos toinen laite hajoaa tai lakkaa toimimasta, liikenne siirtyy (failover) toiselle laitteelle eikä palveluun tule katkosta tai katkos on mahdollisimman lyhyt. Testiympäristön Juniper SRX-500 -klusteri konfiguroitiin toimimaan aktiivi / passiivi tilassa, jolloin vain aktiivinen laite välittää liikennettä. Passiivinen laite tarkkailee aktiivisen laitteen tilaa ja on vikatilanteen syntyessä valmis ottamaan aktiivisen laitteen roolin.

4.1 Juniper SRX palomuurien vikasietoisuus

4.1.1 Klusteri ID (Cluster ID)

Klusterilla täytyy olla oma uniikki klusteri ID, joka on jaettu jokaisen klusterin jäsenen kesken. ID on tärkeä jäsenten kommunikoidessa keskenään. ID:tä käytetään myös Reth (Redundant Ethernet interface) -porttien MAC-osoitteiden määrittelyssä. Yhteensä viisitoista Klusteri ID:tä on käytettävissä klusteria luotaessa. [6]

4.1.2 Noodi ID (Node ID)

Noodi ID:tä käytetään klusterissa olevan laitteen tunnistamiseen. ID:tä voi olla vain kaksi: noodi 0 ja noodi 1. Noodi 0 on niin sanottu pohja noodi. Noodi 0 on klusterin ensimmäinen porttinumeroa kuvaava noodi ja noodi 1 toinen ja viimeinen noodi klusterissa. [6]

4.1.3 Redundanssiryhmä (Redundancy group)

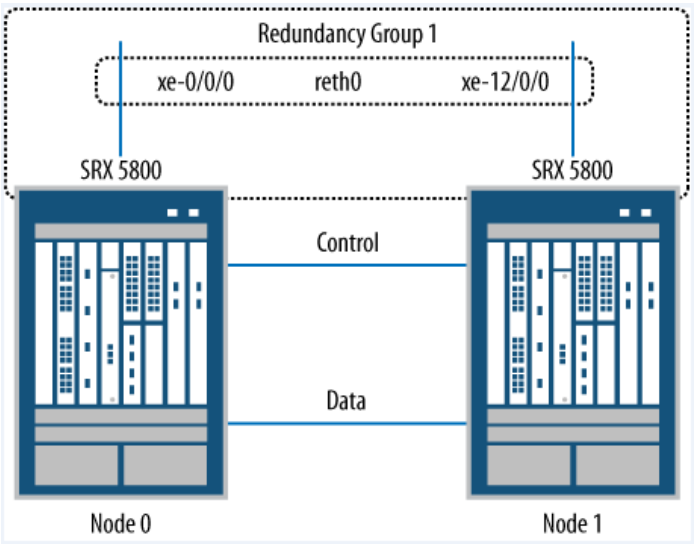
HA-klusterin tarkoitus on varmistaa resurssien käytettävyys vikatilanteessa. Redundanssiryhmä on kokoelma resursseja, joiden täytyy siirtyä laitteelta toiselle vikatilanteen sattuessa. Vain toinen klusterin noodi voi olla vastuussa redundanssiryhmästä mutta toisaalta yksi noodi voi olla samanaikaisesti primääri noodi usealle redundanssiryhmälle.

Redundanssiryhmään sijoitetaan kaksi osiota: 1. kontrolli taso (Control plane) sekä 2. laitteen portit (Interfaces). Oletusryhmä on ryhmä 0 joka edustaa kontrolli tasoa. Ryhmän 0 isäntä (Master) noodi on aina se, jolla on aktiivinen reititin (Routing Engine). Aktiivinen reititin kontrolloi data osiota sekä on vastuussa uuden konfiguraation tuomisesta laitteelle. Aktiivinen reititin määrää kaikesta mitä laitteelle tapahtuu. [6]

Redundanssiryhmä 1 ja sitä suuremmat ryhmät sisältävät laitteen data osion ja sekä vähintään yhden kahdennetun reth -portin (Redundant Ethernet Interface). Reth-portti on pseudo-portti tai virtuaalinen portti, johon klusterin yksi fyysinen portti pari on sidottu. Reth-portti on isäntä (redundant parent) johon fyysinen portti (child interface) sidotaan. Juniper SRX-550 -mallissa voi olla enintään 58 reth-porttia. [7]

Aktiivisen noodin fyysinen portti vastaa kaikesta liikenteestä ja passiivisen noodin portin lävitse ei kulje liikennettä lainkaan. [10]

Kuvassa 4 vasemmanpuoleinen laite on noodi 0 ja oikeanpuoleinen laite noodi 1. Noodin 0 fyysinen xe-0/0/0-portti on sidottu reth0-porttiin ja noodissa 1 sidotaan vastaavasti fyysinen portti xe-12/0/0. Reth0 kuuluu esimerkissä redundanssiryhmään 1. Noodi 0 linkki on aktiivinen ja noodin 1 linkki on valmiudessa mutta sen läpi ei kulje liikennettä. Noodin 0 mennessä vikatilaan noodi 1 ottaa aktiivisen roolin ja lähettää gratuitous ARP (GARP) -viestin. Molemmat reth-portin noodit käyttävät samaa MAC-osoitetta. GARP-viestin jälkeen ympäröivät kytkimet oppivat, että uusi portti on saanut reth portille kuuluvan MAC -osoitteen ja näin L2-tasolla verkkoliikenne voi jatkua. Koska sama MAC-osoite säilyy, muiden ympäröivien laitteiden ei tarvitse opetella uutta osoitetta. [6]



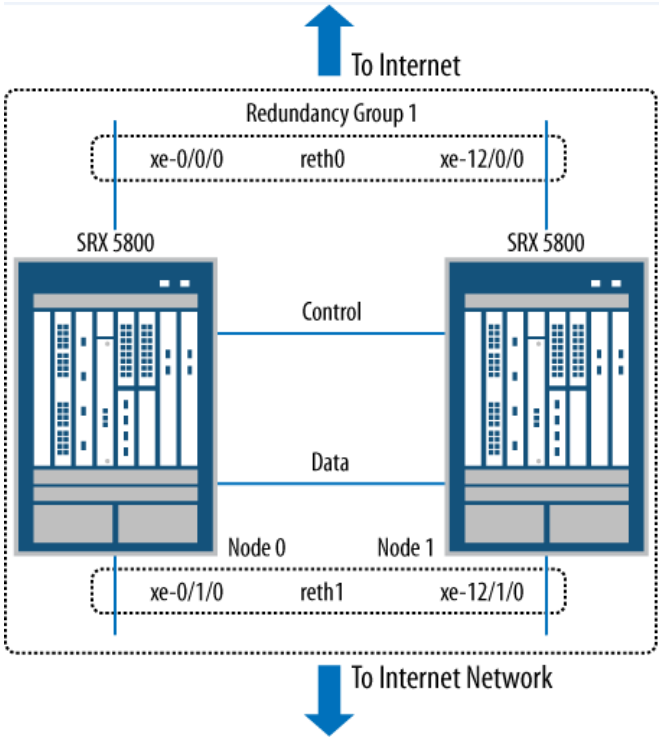
Kuva 4, Redundanssiryhmän fyysiset portit [6].

4.1.4 Aktiivi / passiivi tila

Aktiivi / passiivi tilassa ensimmäisen SRX:n data-osio (Data plane) välittää liikennettä, kun taas toisen SRX:n data-osio ei välitä mitään. Vikatilanteessa SRX käyttää redundanssiryhmää ja yhtä tai useampaa porttia korjatakseen tilanteen.

Kuvassa 5 noodi 0 on aktiivinen. Tässä konfiguraatiossa on kaksi reth-porttia reth 0 jonka suunta on internettiin ja reth 1, joka kytkeytyy sisäverkkoon. Aktiivinen noodi 0 synkronoi

istuntotaulun (Session table) passiivisen noodin kanssa. Sessiotaulun synkronointi on tärkeää koska vikatilanteessa aktiiviseksi tulevan noodin ei tarvitse tehdä synkronointia uudelleen ja liikenne saadaan nopeammin ja näkymättömämmin siirtymään toiselle laitteelle. [6]



Kuva 5, RETH portit sisä- ja ulkoverkon suuntiin. [6]

5.0 PALOMUURIN HALLINTA

Juniper SRX-550 palomuureissa hallintaan käytetään fxp0-porttia, joka on kytköksissä reitittimeen (RE). Sekundaarisen noodin hallinta edellyttää, että joko fxp0 tai jokin muu fyysinen portti on konfiguroitu käyttöön. Fxp0-portti mahdollistaa laitteen turvallisen hallinnan ja portin pitäisi toimia aina, siitä huolimatta mitä verkossa tapahtuu. Myös laitteen hallintasovellukset kuten Network and Security Manager (NSM) tai tässä työssä käytetty Junos Space toimivat parhaiten, kun laitteet ovat yhteydessä niihin fxp0-portin kautta. [6]

Klusteria muodostettaessa klusterin noodien väliseen kommunikointiin käytetään fxp1-porttia. Fxp1-portti mahdollistaa laitteiden keskinäisen kommunikoinnin ja se on vastuussa konfiguraation synkronoinnista noodien välillä. Juniper suosittelee, että fyysisestä

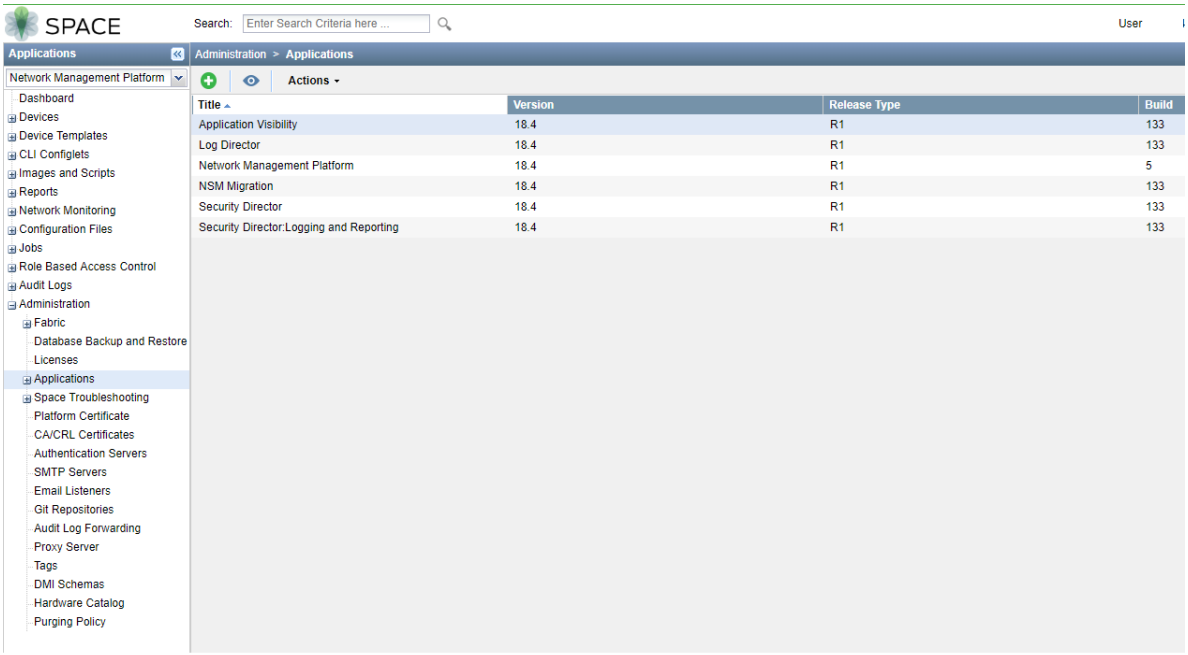
portista 0/0 konfiguroidaan hallintaan käytettävä fxp0-portti ja fyysisestä 0/1 portista konfiguroidaan fxp1-portti. [8]

Fabric on fyysinen yhteys kahden noodin välillä, joka kytketty noodien fyysisiin ethernet -portteihin. Fabric toimii datalinkkinä noodien välillä. Noodille saapuva liikenne, joka on tarkoitettu prosessoitavaksi toisella noodilla, lähetetään eteenpäin fabric-linkkiä pitkin. Samoin noodilla prosessoitu liikenne, joka on tarkoitettu välitettäväksi eteenpäin toisen noodin kautta, kulkee fabric-linkin kautta. Klusterin pakettien välitys (Packer Forwarding Engine) käyttää fabric-datalinkkiä liikenteen välittämiseen sekä järjestelmän dynaamisen tilan synkronointiin. Fabric-linkki on myös vastuussa eri operaatioiden kuten NAT, IPsec ja ALG-sessiotilojen synkronoinnista. Fabric-linkin konfiguroimiseen voidaan käyttää mitä tahansa fyysistä porttia. [7]

5.1 Junos Space

5.1.1 Network Management Platform

Testilaboratoriossa käyttöön otettu Junos Space palomuurien hallintaohjelma koostuu kolmesta osasta: Network Management Platform, Security Director ja Security Director Logging and Reporting. Network Management Platform toimii nimensä mukaisesti hallintaohjelman alustana, jonka päälle tarvittavia ohjelmia voidaan asentaa. Security Director sisältää palomuurisäännöt ja se on ohjelmista tärkein ja käytetyin. Security Director Logging and Reporting kerää lokitietoa palomuuriympäristöstä. Lokien kerääminen on Katakri:n mukaisesti pakollinen osa palomuuriympäristöä. Lokipalvelin mahdollistaa myös lokihistorian käytön vianselvityksessä ja helpottaa näin palomuurin lävitse kulkevan liikenteen tarkkailua.

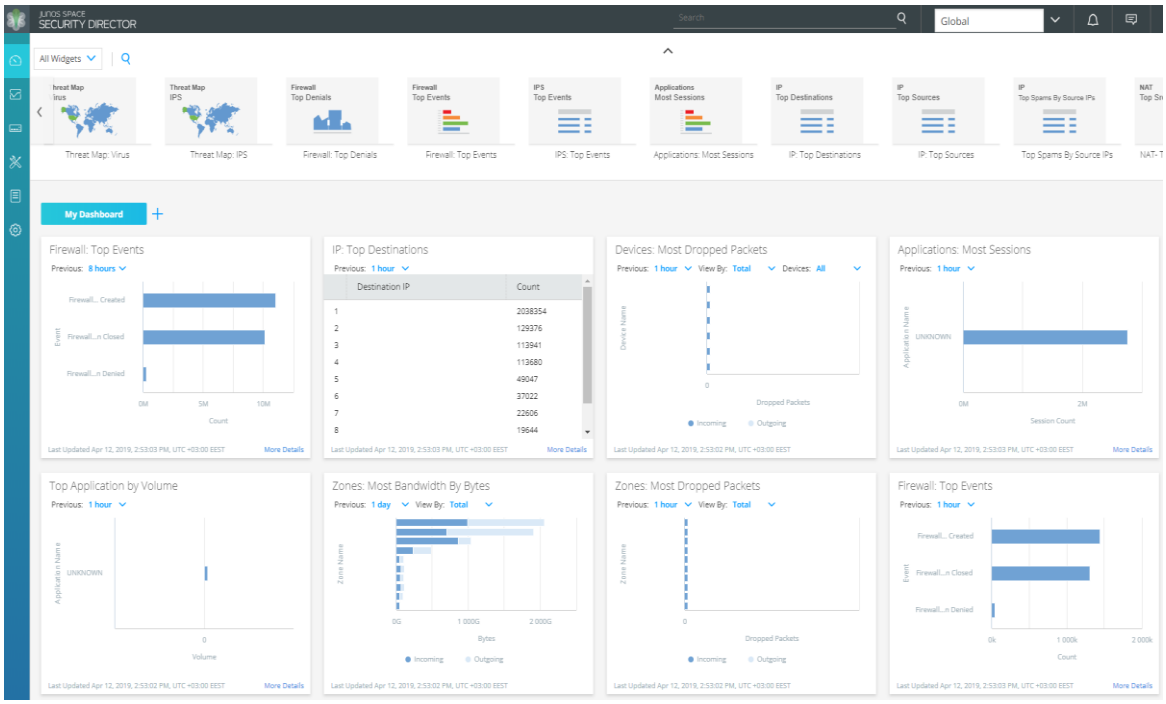


Kuva 6, Junos Space Network Management Platform.

Alustaan asennettiin tätä työtä varten myös NSM Migration-ohjelma, jota käytettiin palomuurisääntöjen siirtämiseen vanhasta NSM-hallintaohjelmasta.

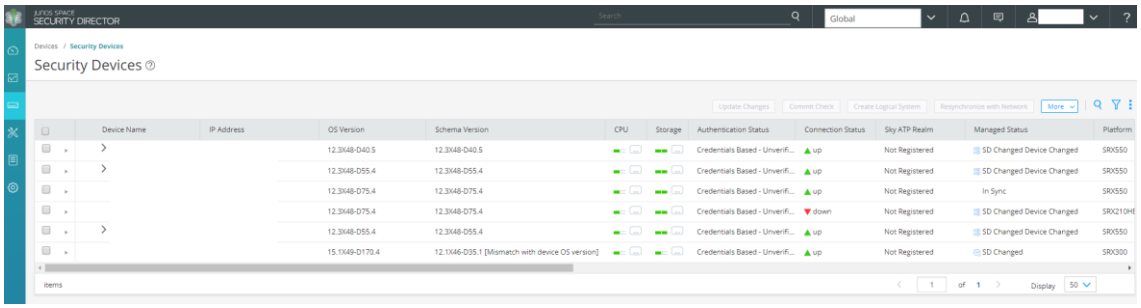
5.1.2 Security Director

Security Directorin oletus sivulla avautuva Dashboard sisältää ikkunoita, jotka keräävät statistiikkaa palomuurin eri tapahtumista. Ikkunoita voi vaihdella oman käyttötarpeen mukaisesti.



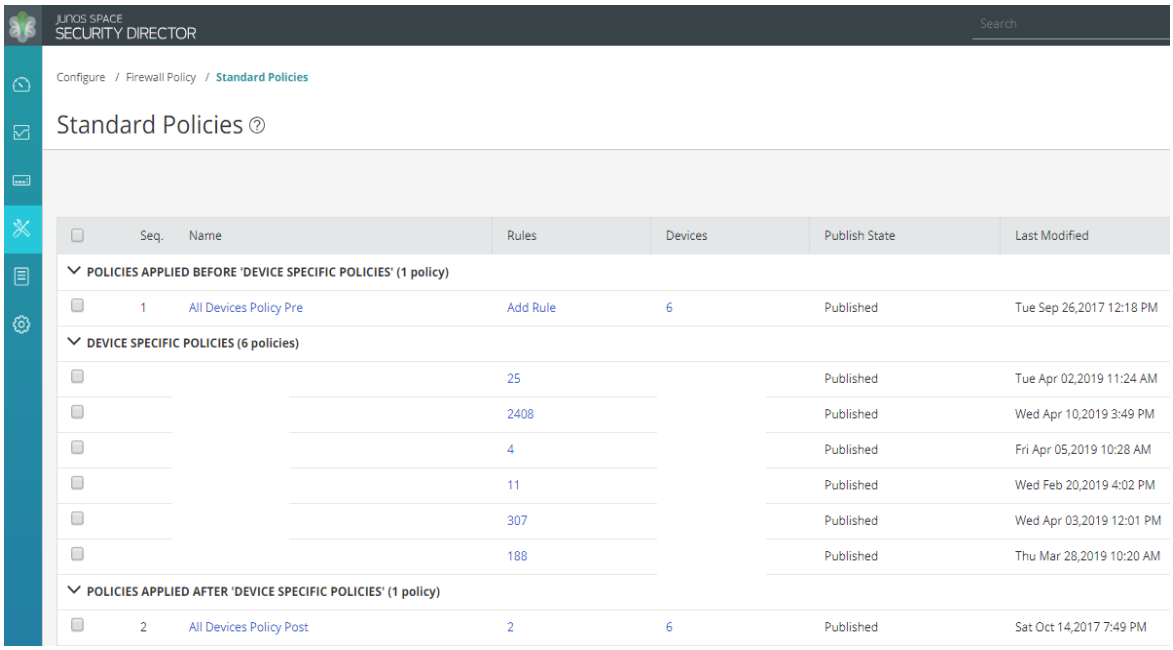
Kuva 7, Security Director Dashboard.

Devices-kohdasta laitteille voi suorittaa erilaisia operaatioita, valvoa prosessorin ja muistin käyttöä sekä tarkastella yhteyden tilaa hallintaohjelman ja laitteiden välillä.



Kuva 8, Firewalls in Security Director.

Migraation jälkeen palomuurisäännöt saatiin näkyviin Security Directorin Standard Policies-näkymään. Datakeskuksen palomuurin sääntökanta oli isoin ja siinä oli yhteensä 2408 sääntöä. Security Director jaottelee säännöt kolmeen eri ryhmään. Ensimmäisenä ovat säännöt, jotka tulevat voimaan ennen laitekohtaisia sääntöjä. Toinen ryhmä sisältää palomuurilaitteille asennettavat säännöt, jossa pääosa varsinaisista säännöistä sijaitsee. Viimeisessä ryhmässä ovat laitesääntöjen jälkeiset säännöt. Tässä ryhmässä voidaan määritellä globaali kaiken liikenteen kieltävä (deny-all) -sääntö, joka pysäyttää kaiken sellaisen liikenteen, joka ei ole vielä osunut mihinkään muuhun sääntöön.

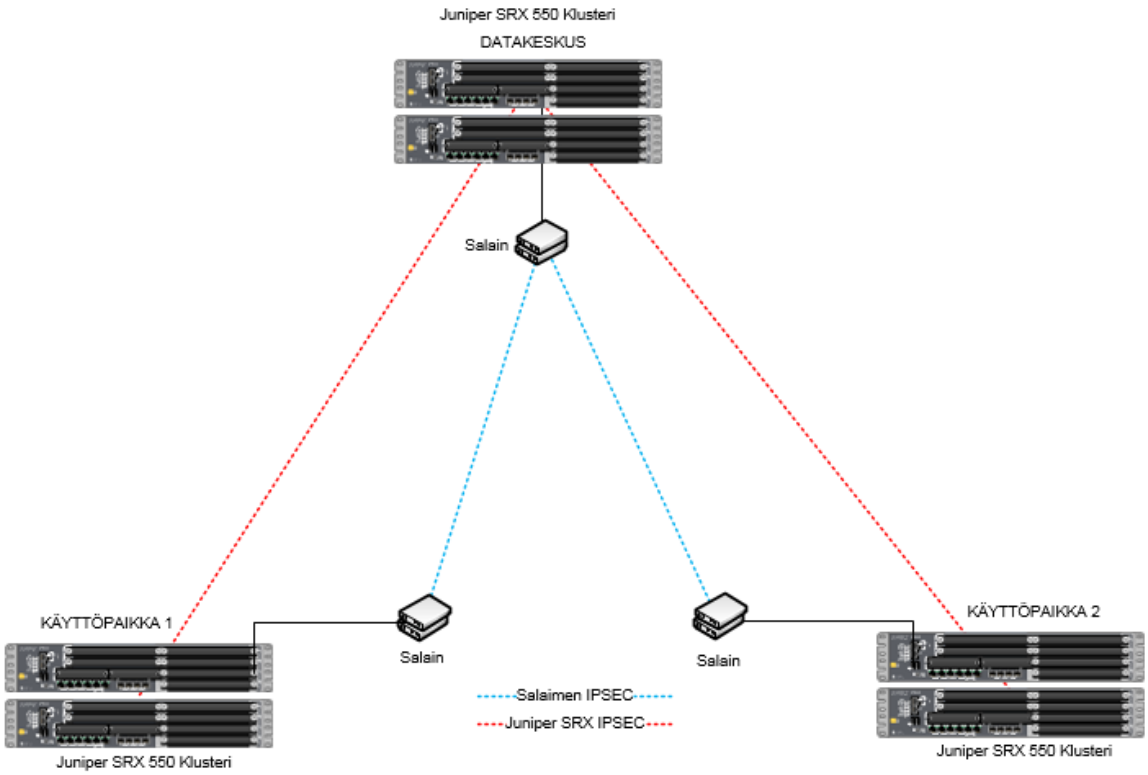


Kuva 9, Palomuurisäännöt Security Directorissa.

Palomuurisääntöjen lisäksi Configure-kohdassa voidaan määrittää IPS, NAT ja UTM -asetuksia, luoda VPN-yhteyksiä ja konfiguroida ajastettuja sääntöjä. [11]

6 Laboratorion verkkotopologia

Laboratorioympäristö rakennettiin kuvan 10 mukaisesti. Käyttöpaikoille asennettiin Juniper SRX-500-klusterit, joiden välille konfiguroitiin IPSec VPN-tunnelit. Palomuurien eteen asennettiin salaimet, joiden välillä oli myös IPSec VPN-tunnelit vahvalla salausalgoritmilla. Palomuurien VPN-tunneli kulkee salainten muodostaman VPN-tunnelin sisällä. Topologiakuvan selkeyttämiseksi tunnelit on piirretty kuvaan toisistaan erilleen.



Kuva 10, Laboratorion verkkotopologia.

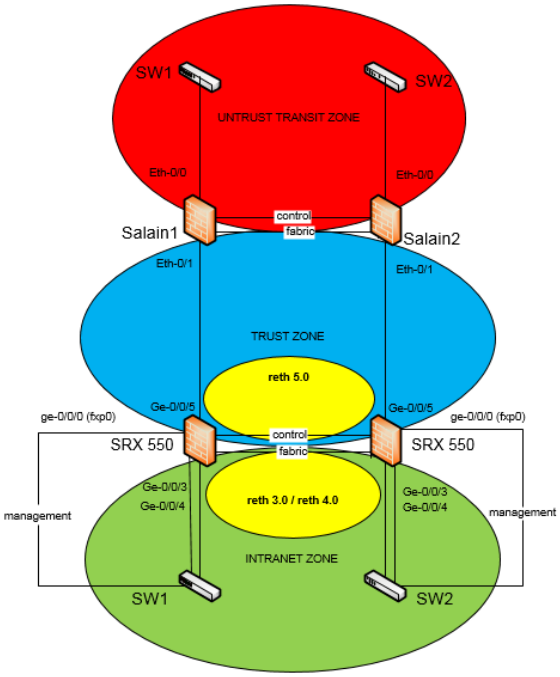
Palomuurissa salausalgoritmejä on neljä eri vaihtoehtoa:

- `3des-cbc`—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.
- `aes-128-cbc`—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- `aes-192-cbc`—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- `aes-256-cbc`—Advanced Encryption Standard (AES) 256-bit encryption algorithm.

Kuva 13, Juniper SRX-550 salausalgoritmi vaihtoehdot. [12]

6.1 Laboratorioympäristön kytkennät

Fyysiset kytkennät tehtiin kuvan 11 mukaisesti. Kuva havainnollistaa myös miten fyysiset portit sijoittuvat eri Security Zone-vyöhykkeille:



Kuva 11, Laboratorion fyysiset kytkennät.

7 Katakri

Ympäristö rakennettiin Katakri-vaatimusten mukaisesti, joten sillä oli vaikutuksia suunnitteluun ja laitteiden lopulliseen konfiguraatioon.

> “Katakri on viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset.”

Katakri antaa viitekehyksen tietoturvallisen ympäristön rakentamisesta, mutta ei määrittele teknisiä yksityiskohtia tai laitteiden asetuksia.

7.1 Katakri vaatimukset

Katakri tarkastelee organisaation tietoturvaa laaja-alaisesti mutta tähän työhön poimittiin Katakri:sta vain ne kohdat, jotka koskevat tietoliikenneverkkoa ja näin ollen vaikuttivat selvästi laboratorioympäristön suunnitteluun ja lopulliseen toteutukseen. Katakri esittää seuraavia vaatimuksia tietoliikenneympäristön toteuttamiseen:

> ”Onko tietoliikenneverkon rakenne turvallinen?”
>
> 1) ”Tietojenkäsittely-ympäristö on fyysisesti tai loogisesti erotettu ja valvottu verkko, josta ei ole suoria liittymiä alemman suojaustason verkkoihin. Viranomainen voi tapauskohtaisesti hyväksyä valvotun ja rajatun yhteyden määriteltyihin vastaavan suojaustason järjestelmiin.” [9]

Ympäristö rakennettiin niin että siinä ei ole yhdyskäytävää alemman suojaustason verkkoon. Päivityksiä varten konfiguroitiin IPSec-valmius alemman suojaustason verkkoon, jota voitaisiin tietyin ehdoin ja auditoituna käyttää tietoturva ja laitepäivitysten tuomiseen.

> 2) ”Tiettyihin viranomaisen suojaustason III tietojärjestelmiin voidaan tuoda tietoa viranomaisen hyväksymän yhdyskäytäväratkaisun (esim. vain yksisuuntaisen liikenteen sallivan datadiodin) kautta.” [9]

Ympäristöön konfiguroitiin valmius, joka mahdollistaisi liitoksen erilliseen verkkoon, jossa käytettäisiin datadiodia tiedon tuomiseen yksisuuntaisesti. Datadiodi toimii yksisuuntaisesti koska siitä on katkaistu lähettävä portti ja jätetty pelkästään vastaanottava portti. Käytännössä tämä voitaisiin toteuttaa valokuituyhteydellä, josta lähettävä kuitupari on irrotettu. Näin liikenne ei voisi koskaan liikkua korkeamman suojaustason verkosta matalamman suojaustason verkkoon.

> 4) ”Tietyt viranomaisen tietojärjestelmät koostuvat suuresta määrästä tietyn suojaustason tietoa ja näissä järjestelmissä asiakokonaisuus nousee luokitukseltaan usein yksittäistä tietoa korkeampaan suojaustasoluokkaan (kasautumisvaikutus, esim. suuri määrä suojaustason IV tietoa voi muodostaa yhdistettynä suojaustason III tietovarannon). Viranomainen voi tapauskohtaisesti hyväksyä rajatun ja valvotun pääsyn osaan tällaisen järjestelmän tietosisällöstä myös luokkaa alemman suojaustason hyväksytyistä järjestelmistä. Hyväksyttävä toteutus edellyttää yleisten suojausmenetelmien lisäksi muun muassa pääsyn rajaamista vain tehtävässä tarvittavaan yksittäiseen tai suppeaan osaan tietosisällöstä, havainnointi- ja torjuntakykyä poikkeavien/luvattomien käyttötapausten (esim. suuret määrät tietohakuja) varalle ja sitä, että järjestelmään tehdyistä tietohauista jää lainmukaisesti säilöttävä tallenne, josta voidaan jälkikäteen yksilöidä mm. tapahtuman (esim. tietohaku) suorittanut henkilö.” [9]

Ympäristön käyttäjiä ohjeistettaisiin käyttämään kaikessa kommunikaatiossa pienintä mahdollista tietomäärää, joka on tarpeellista asian hoitamiseksi. Esimerkiksi IP-osoitteita tai viittauksia käytettyyn teknologiaan tulisi välttää tiedon kasautumisvaikutuksen estämiseksi. Laboratorioympäristöön tehtiin myös valmius keskitetyn lokien hallintajärjestelmän liittämiselle, joka keräisi lokitietoa käytännössä kaikista verkon tapahtumista. Suurin osa verkossa olevista laitteista on myös konfiguroitu lähettämään lokitietoa lokienhallintajärjestelmään. Liitosta alemman suojaustason verkkoon valvottaisiin IDS-järjestelmällä, joka yhdessä keskitetyn lokienhallintajärjestelmän kanssa muodostaisi kattavan kuvan verkon tapahtumista. Kaikkea lokitietoa olisi valmius säilyttää vähintään kahden vuoden ajan.

> ”Ovatko palomuurien ja vastaavien liikennettä suodattavien laitteiden säännöstöt hyvien tietoturvaperiaatteiden mukaisia? Miten on varauduttu yleisimpiin nykyisiin verkkohyökkäyksiin?” [9]

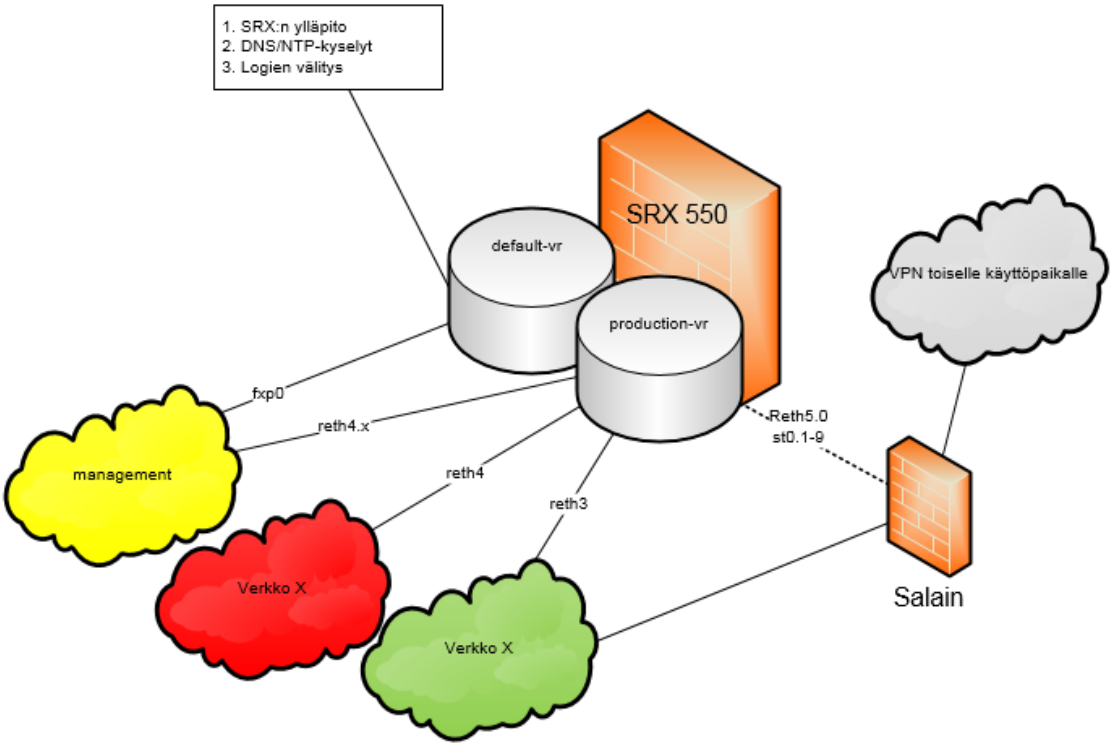
> ”Perustason vaatimukset soveltuen, lähinnä vyöhykkeiden sisällä ja/tai rajoilla, vrt. I 401:n määritykset.
> 1) ”Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny). Säännöstöt sallivat vain erikseen määritellyn, toiminnalle välttämättömän liikennöinnin. 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin. 3) Organisaatiopalomuurin takana sisäverkossa olevien työasemien, kannettavien tietokoneiden ja vastaavien ohjelmistopalomuurit sallivat vain erikseen määriteltyjen, toiminnalle välttämättömien ohjelmistojen/protokollien liikennöinnin. 4) Estetyt paketit kirjataan lokiin (vrt. I 504.0). Mikäli teknisesti mahdollista, kirjauksesta on voitava yksilöidä lähettäjätaho esim. MAC-osoitteen tarkkuudella. 5) Web-selailua suodatetaan toimintavaatimusten mukaisesti. 6) Yleisiin verkkohyökkäyksiin on varauduttu: a) Osoitteiden väärentäminen (spoofing) estetty. b) Liikenne, joka käyttää IP-lisämääreitä (IP options) ja erityisesti lähdereititystä (source routing), on oletuksena estetty kaikissa verkkolaitteissa. c) Proxy ARP -toiminnallisuus on estetty kaikissa verkkolaitteissa. d) Liikenne, jonka lähde- tai kohdeosoite on lähiverkon broadcast-osoite, on estetty. e) Liikenne, jonka lähde- tai kohdeosoitteena on 127.0.0.1 tai 0.0.0.0, on estetty. f) SNMP-liikenne sallitaan vain erikseen määritellyistä lähteistä. g) On määritetty mitä ICMP-liikennettä sallitaan. Erityisesti on huomioitava, että ICMP-tyypin 3 (unreachable) liikenne tulee estetyksi. h) Varattuja osoitteita (RFC 1918) käyttävä liikenne, joka joko saapuu organisaation verkon ulkopuolelta tai suuntaa sinne, on estetty. i) Palomuurit on konfiguroitu kokoamaan sirpaloituneet (fragment) paketit ennen suodatuspäätöksen tekemistä. j) Palvelunestohyökkäysten (DoS, DDoS, roskapostitulva) uhka on arvioitu ja tarpeelliset torjunta- ja ehkäisykeinot toteutettu.” [9]

Palomuurien osalta edellä mainitut kohdat on tarkastettu ja on todennettu, että vain erikseen sallittu liikenne pääsee kulkemaan palomuurien lävitse ja kaikki muu liikenne estetään. Työasemia testilaboratorioon asennettiin vain muutama. Työasemiin oli asennettu virustorjuntaohjelmat. Keskitetty lokienhallintajärjestelmä keräisi kattavasti tietoa verkkoliikenteestä ja tuottaisi hälytyksen, jos sallimatonta liikennettä havaittaisiin. Myös erillinen

IDS (Intrusion Detection System) -järjestelmä liitettynä lokienhallintajärjestelmään rikastaisi verkon tilannekuvaa.

> ”Onko hallintayhteydet suojattu asianmukaisesti?”
>
> 1) ”Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua. 2) Verkon aktiivilaitteisiin sallitaan hallintayhteydenotot vain erikseen määritellyistä lähteistä tai vain fyysisesti laitteeseen kytkeytymällä. Vrt. etähallintavaatimus I 704.0.” [9]

Hallintayhteydet eriytettiin kuvan 12 mukaisesti omaan erilliseen virtuaalireitittimeen. Hallintayhteydet ovat näin omassa reititystaulussaan. Lisäksi hallintaan pääsyä rajattiin sallimalla yhteydet vain tietyille IP-osoitteille ja käyttäjätunnuksille. Yhteiskäyttötunnuksien käyttöä ei sallittu lainkaan ja niiden käyttö aiheuttaisi hälytyksen lokienhallintajärjestelmässä.



Kuva 12, Hallintayhteyden eriyttäminen.

> ”Miten verkon aktiivilaitteet on kovennettu?”
>
> ”Perustason vaatimusten lisäksi:
> 1) Verkkolaitteiden lokeista on pystyttävä jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta. 2) Kytkimien käyttämättömät portit on poistettu käytöstä. ” [9]

Palomuurit kovennettiin Juniperin parhaiden käytäntöjen mukaisesti ja kaikista verkkolaitteista suljettiin käyttämättömät portit. Tuotantoympäristöön asennettava lokijärjestelmä tallentaisi kaikki laitteille kirjautumiset. Junos Space palomuurien hallintasovellus tallentaa laitteille suoritetut toimenpiteet.

> ”Miten verkkoa, järjestelmiä ja niiden käyttöä valvotaan? Onko resurssit mitoitettu toimintavaatimusten mukaisiksi?”
>
> ”Perustason vaatimusten lisäksi:
> Käytössä oltava menettely hyökkäyksen / väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan (vrt. I 107.0 ja I 504.0). Verkkoliikennettä tarkkaillaan vähintään sillä tarkkuudella, että havaitaan a) merkittävät poikkeamat työasemien ja palvelinten liikennemäärissä, b) normaalitilaan nähden poikkeavat protokollat, c) luvattomien yhteyksien yritykset (esim. vyöhykkeiden välisessä yhdyskäytävässä).” [9]

Keskitetyn lokijärjestelmän valvonta tulisi resursoida niin että hälytykset ja poikkeamat havaitaan mahdollisimman nopeasti ja niihin ehdittäisiin reagoida ajoissa.

8 Konfiguraatiot

SRX-550 palomuurien peruskonfiguraatio koostui useista osa-alueista, joista on tämän kappaleen kuvissa esitelty vain oleellisimmat kohdat. Konfiguraatiossa esiintyvät IP-osoitteet ja asetusten nimet on tietoturvasyistä muutettu.

8.1 Porttikonfiguraatio

Komennolla ”show interfaces terse” saadaan yleislistaus käytössä olevista porteista:

```
Interface               Admin Link Proto    Local
ge-0/0/3.12             up    up   aenet    --> reth3.12
ge-0/0/3.15             up    up   aenet    --> reth3.15
ge-9/0/3.12             up    up   aenet    --> reth3.12
ge-9/0/3.15             up    up   aenet    --> reth3.15
reth3.12                up    up   inet     x.x.x.x/24
reth3.15                up    up   inet     x.x.x.x/24
fab0                    up    up
fab0.0                  up    up   inet     x.x.x.x/24
fab1                    up    up
fab1.0                  up    up   inet     x.x.x.x/24
fxp0                    up    up
fxp0.0                  up    up   inet     x.x.x.x/24
reth5                   up    up
reth5.0                 up    up   inet     x.x.x.x/24
st0                     up    up
st0.0                   up    up   inet
st0.1                   up    up   inet
st0.2                   up    up   inet
st0.3                   up    up   inet
st0.5                   up    up   inet
```

Kuva 13, palomuurilaitteen portit

8.2 Security zone-asetukset

Junos palomuureihin voidaan konfiguroida useita loogisia vyöhykkeitä (security zone) joilla laitteen portteja ja aliverkkoja voidaan segmentoida toisistaan erillisiksi osiksi. Jokaisen portin täytyy toimiakseen kuulua johonkin vyöhykkeeseen. Vyöhykkeille voidaan määritellä eri palveluja (service), joista yhteyksiä sallitaan. [13]

```
set security zones security-zone esimerkkizone interfaces reth3.12 host-inbound-traffic system-services dhcp
set security zones security-zone esimerkkizone interfaces reth4.13 host-inbound-traffic system-services dhcp
set security zones security-zone esimerkkizone interfaces reth4.13 host-inbound-traffic system-services ping
```

Kuva 14, Vyöhykkeiden määrittely.

8.3 Screen-asetukset

Junos Screen-asetusten avulla verkkoon kohdistuvia hyökkäyksiä voidaan havaita ja niitä voidaan estää. Screen-asetusten raja-arvoja voidaan säätää komentoriviltä tai Junos Space-hallintaohjelmasta. Testilaboratorion palomuureilla käytettiin oletusarvoja.

```
set security screen ids-option default-screen icmp fragment
set security screen ids-option default-screen icmp large
set security screen ids-option default-screen icmp flood
set security screen ids-option default-screen icmp ping-death
set security screen ids-option default-screen ip bad-option
set security screen ids-option default-screen ip record-route-option
set security screen ids-option default-screen ip timestamp-option
set security screen ids-option default-screen ip security-option
set security screen ids-option default-screen ip stream-option
set security screen ids-option default-screen ip source-route-option
set security screen ids-option default-screen ip loose-source-route-option
set security screen ids-option default-screen ip strict-source-route-option
set security screen ids-option default-screen ip unknown-protocol
set security screen ids-option default-screen ip tear-drop
set security screen ids-option default-screen tcp syn-fin
set security screen ids-option default-screen tcp tcp-no-flag
set security screen ids-option default-screen tcp syn-frag
set security screen ids-option default-screen tcp syn-flood
set security screen ids-option default-screen tcp land
set security screen ids-option default-screen tcp winnuke
```

Kuva 15, Screen-asetukset.

8.4 Palomuurisäännöt

Palomuurisäännöt koostuvat vähintään neljästä lausekerivistä: Lähdeosoite, kohdeosoite, palvelu ja toimenpide. Toimenpide (action) voi olla joko salliva tai kieltävä.

```
set security policies from-zone zone1 to-zone zone2 policy 1 match source-address x.x.x.x/32
set security policies from-zone zone1 to-zone zone2 policy 1 match destination-address x.x.x.x/32
set security policies from-zone zone1 to-zone zone2 policy 1 match application https
set security policies from-zone zone1 to-zone zone2 policy 1 then permit
```

Kuva 16, Palomuurisäännöt.

8.5 IPsec VPN

VPN-yhteyksien konfiguraatio muodostuu kahdesta osasta. Ensimmäinen osa on IKE-asetus (Internet Key Exchange), jossa määritellään yhdistelmä parametrejä, joita käytetään avainten vaihdossa. Toisessa osassa määritellään IPSec-asetukset.

8.5.1 IKE policy

Tässä työssä käytettiin manuaalisesti asetettuja avaimia sekä kiinteitä IP-osoitteita VPN-yhteyden molemmissa päissä. Onnistunut IKE-neuvottelu on edellytys IPSec-yhteyden

onnistumiselle. IKE-asetuksessa määritetään myös vastapään laitteen IP-osoite ja portti, jota käytetään yhteyden muodostamiseen. [14]

```
set security ike proposal example-phase1-proposal authentication-method pre-shared-keys
set security ike proposal example-phase1-proposal dh-group group20
set security ike proposal example-phase1-proposal authentication-algorithm sha-256
set security ike proposal example-phase1-proposal encryption-algorithm aes-256-cbc

set security ike policy phase1-policy mode main
set security ike policy phase1-policy proposals phase1-proposal
set security ike policy phase1-policy pre-shared-key ascii-text

set security ike gateway gw_example_location address x.x.x.x
set security ike gateway gw_example_location external-interface reth5
```

Kuva 17, IKE asetukset.

8.5.2 IPSec policy

IPSec-asetuksissa määritellään varsinaiset salausasetukset sekä VPN-yhteyden muodostamiseen käytetyt portit. Junos käyttää VPN-yhteyden muodostamiseen st0.x -nimistä porttia (tunnel interface).

```
set security ipsec proposal example-phase2-proposal protocol esp
set security ipsec proposal example-phase2-proposal authentication-algorithm hmac-sha-256-128
set security ipsec proposal example-phase2-proposal encryption-algorithm aes-256-cbc
set security ipsec policy example-phase2-policy perfect-forward-secrecy keys group20
set security ipsec policy example-phase2-policy proposals updates-phase2-proposal

set security ipsec vpn example_location bind-interface st0.2
set security ipsec vpn example_location ike gateway gw_example_location

set security ipsec vpn example_vpn df-bit copy
set security ipsec vpn example_vpn vpn-monitor optimized
set security ipsec vpn example_vpn ike proxy-identity local x.x.x.x/32
set security ipsec vpn example_vpn ike proxy-identity remote x.x.x.x/32
set security ipsec vpn example_vpn ike ipsec-policy example-phase2-policy
set security ipsec vpn example_vpn establish-tunnels immediately
```

Kuva 18, IPSec-asetukset.

8.6 Käyttäjät

Yhteiskäyttötunnuksien käyttöä ei sallittu, joten laitteille kirjautuminen onnistuu vain ennalta määrätyille käyttäjille.

```
set system login user username full-name "Keijo konffaaja"
set system login user username uid 2001
set system login user username class admin
```

Kuva 19, Käyttäjätunnukset.

8.7 Lokien lähetys

Lokien lähetys keskitettyyn lokienhallintajärjestelmään on yksi tärkeimmistä konfiguraation osista. Vain lokitietoa seuraamalla voidaan kattavasti seurata verkon tapahtumia, laitteille suoritettuja komentoja ja havaita asiaton liikenne verkossa. Katakri:n mukaan lokitietoa tulee säilyttää kahden vuoden ajan ja tapahtumia voidaan hakea järjestelmästä helposti koko säilytyksen ajalta. Lokitieto lähetetään lokipalvelimelle UDP-protokollalla portissa 514.

```
set security log mode stream
set security log format sd-syslog
set security log source-address x.x.x.x
set security log transport protocol udp
set security log stream space format sd-syslog
set security log stream space host x.x.x.x
set security log stream space host port 514
set security log stream siem format binary
set security log stream siem host x.x.x.x
set security log stream siem host port xx
```

Kuva 20, Lokien lähetys keskitettyyn lokienhallintajärjestelmään.

8.8 Reititys

Palomuurien reititys jaettiin kahteen eri reititystauluun. Routing options on Junos käyttöjärjestelmän oletuksena käyttämä reititystaulu, johon tässä työssä konfiguroitiin hallintayhteys. Varsinaista hyötyliikennettä sisältävät verkot liitettiin erikseen luotuun virtuaalireitittimeen.

```
ROUTION OPTIONS

set routing-options static route 0.0.0.0/0 next-hop x.x.x.x
set routing-options static route x.x.x.x/32 next-table transit-vr.inet.0
set routing-options static route x.x.x.x/32 next-table transit-vr.inet.0

ROUTING INSTANCES

set routing-instances transit-vr instance-type virtual-router
set routing-instances transit-vr interface reth3.12
set routing-instances transit-vr interface reth3.15
set routing-instances transit-vr routing-options static route x.x.x.x/32 next-hop x.x.x.x
set routing-instances transit-vr routing-options static route x.x.x.x/32 next-hop x.x.x.x
```

Kuva 21, Reitityksen konfiguraatio.

8.9 Kovennukset

Verkkolaitteiden kovennukset (hardening) ovat tärkeä osa turvallista tietoverkkoa. Kovennuksilla tarkoitetaan laitteen oletusasetusten muuttamista turvallisemmiksi. Oletuksena sallitut protokollat poistetaan, avoimet fyysiset portit suljetaan ja kirjautumisyritysten sallitut maksimimäärät vaihdetaan. Kovennukset suojaavat verkon laitteita ja näin myös koko tietoverkkoa ulkopuolisilta.

```
set system login password format sha1
set system services ssh root-login deny
set system services ssh protocol-version v2
set system services ssh connection-limit 3
set system services ssh rate-limit 5

set system login retry-options tries-before-disconnect 3
set system login retry-options backoff-threshold 2
set system login retry-options backoff-factor 6
set system login retry-options minimum-time 30
set system login class admin idle-timeout 10
set system login class admin login-alarms
set system login class admin permissions all

set system time-zone Europe/Helsinki
set system authentication-order radius
set system authentication-order password
set system location country-code FI
set system ports console log-out-on-disconnect
set system ports auxiliary disable
```

Kuva 22, Kovennusten konfiguraatio.

Tiivistelmä ja johtopäätökset

Tuotantokäyttöön tarkoitetun verkkoympäristön perusteellinen mallintaminen ja testaaminen laboratorioympäristössä ovat tärkeitä vakaan ja toimivan kokonaisuuden aikaansaamiseksi. Uusi ympäristö saatiin rakennettua uusilla palomuureilla toimivaksi ja vaatimuksia vastaavaksi kokonaisuudeksi, jossa vanhan ympäristön tärkeimmät periaatteet säilyivät.

Uusien tehdasasetuksilla olevien laitteiden käyttökuntoon konfiguroiminen oli haastavaa ja vaati paljon valmistajan dokumentaatioon perehtymistä. Tämä tarjosi kuitenkin hyvän tilaisuuden tutustua Junos käyttöjärjestelmään, jota ei ollut aiemmin käytetty testilaboratoriossa. Uuden käyttöjärjestelmän perusteellinen opettelu tarkoittaisi jatkossa todennäköisesti saman laitevalmistajan laitteiden suosimista. Tällöin aikaa ei kuluisi niin paljon itse käyttöjärjestelmän opetteluun.

Käytettävissä oleva aika ja resurssit kuitenkin rajasivat työn laajuutta. Kattavamman testauksen aikaansaamiseksi laboratorioon olisi voinut rakentaa enemmän järjestelmiä, palvelimia ja työasemia, joilla verkkoa ja sen palveluja olisi voitu testata. Tässä työssä joillekin kyseisille testattaville järjestelmille rakennettiin vain valmius; järjestelmien käytännön testausta olisi voinut tehdä enemmän, jos laitteita olisi ollut enemmän saatavilla.

Tässä työssä rakennettua ympäristöä voisi jatkossa käyttää Katakri-vaatimuksiin sitoutuneen tai muun tietoturvaa arvostavan yrityksen tietoliikenneverkon rakentamisen mallina. Resursseista riippuen verkon topologian voisi rakentaa vikasietoisemmaksi ja testivaiheessa laboratorioon voisi liittää lisää testattavia järjestelmiä.

Lähteet

1 Firewall Design and Analysis 2010, Alex X Liu.

2 Firewall Fundamentals, by Ido Dubrawsky; Wes Noonan Published by Cisco Press, 2006.

3 Cisco Documentation. <https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-1/SFW/21-1-PSF-Admin/21-1-PSF-Admin_chapter_01.html>. Luettu 22.3.2019.

4 Networking Self-Teaching Guide: OSI, TCP/IP, LANs, MANs, WANs, Implementation, Management, and Maintenance, by Richard Bramante; James Edwards Published by John Wiley & Sons, 2009.

5 JUNOS High Availability by Senad Palislamovic; James Sonderegger; Orin Blomberg; Kieran Milne Published by O'Reilly Media, Inc., 2009.

6 Junos Security by Timothy Eberhard; James Quinn; Rob Cameron; Patricio Giecco; Brad Woodberg Published by O'Reilly Media, Inc., 2010.

7 Juniper Documentation. <https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-redundant-ethernet-interfaces.html>. Luettu 3.4.2019.

8 Juniper Documentation. <https://www.juniper.net/documentation/en_US/release-independent/junos/topics/concept/services-gateway-srx550-built-in-ethernet-port.html>. Luettu 9.4.2019.

9 Puolustusministeriö. Verkkoaineisto. <https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille>. Luettu 20.2.2019.

10 Juniper Documentation. <https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-active-passive-deployments.html#jd0e88>. Luettu12.5.2019.

11 Juniper Documentation. <https://www.juniper.net/documentation/en_US/junos-space16.1/information-products/pathway-pages/junos-space-security-director-pwp.html>. Luettu 12.5.2019.

12 Juniper Documentation. <https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/services-ipsec-proposals-configuring.html>. Luettu 12.5.2019.

13 Juniper Documentation. <https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-zone-configuration.html>. Luettu 22.5.2019.

14 Juniper Documentation. <https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/services-ike-policies-configuring.html> Luettu 22.5.2019.