Henri Pasonen

Palomuurin implementointi yritysverkkoon Cisco-ympäristössä

Opinnäytetyö
Tieto- ja viestintätekniikan koulutus

2018

Kaakkois-Suomen ammattikorkeakoulu

Tekijä/Tekijät	Tutkinto	Aika
Henri Pasonen	Insinööri (AMK)	Joulukuu 2018

Opinnäytetyön nimi	
Palomuurin implementointi yritysverkkoon Cisco-ympäristössä	39 sivua 0 liitesivua

Toimeksiantaja

Kaakkois-Suomen ammattikorkeakoulu Oy, ICTLAB

Ohjaaja

Martti Kettunen

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli tutkia, miten palomuurin voisi implementoida uudeksi osaksi olemassa olevan yritysverkon topologiaa. Tarkoituksena on myös kerätä materiaalia palomuuriratkaisuista olemassa olevan tieto- ja viestintätekniikan koulutuksen Big Picture of Internet -kurssin kehitystä varten. Palomuurin implementointi tuli toteuttaa siten, ettei yritysverkon alkuperäiseen topologiaan tarvitsisi puuttua muuten kuin palomuurin osalta ja ettei yritysverkon redundanttisuus kärsisi. Työssä tutkittiin palomuurin lisäämisen aiheuttamia lisätoimenpiteitä muualla topologiassa ja palomuuria kohdeltiin yritysverkon tietoturvaa parantavana konseptina, mutta palomuurin tietoturvaominaisuudet eivät olleet keskiössä.

Tietoturvan merkitys yritysverkoissa kasvaa jatkuvasti ja yrityksissä vaaditaan yhä enemmän henkilöstöä, joilla on riittävää ymmärrystä tietoverkkojen tietoturvallisuudesta. Työssä korostetaan yritysverkon palomuurin sisä- ja ulkopuolien välistä suhdetta ja kuinka palomuuri vaikuttaa yritysverkon toimintaan.

Työn alussa tutkittiin yleisellä tasolla palomuurien kehitystä ja merkitystä yritysverkoille. Samalla tutkittiin myös kampusverkon rakennetta. Työn käytännön osuudessa käsiteltiin suunniteltuja palomuuriratkaisuja topologiamuutosten osalta vanhan ja uuden topologian välillä sekä tutkittiin teoriatasolla ratkaisuissa käytettyjä protokollia.

Työlle asetetut tavoitteet saavutettiin suurimmilta osin onnistuneesti. Työn edistyessä painopiste siirtyi jatkuvasti enemmän BPI-kurssimateriaalin kehittämiseen. Tämä johti siihen, että joitain suunniteltuja palomuuriratkaisuja piti jättää pois, jotta voitiin keskittyä yhden ratkaisun hiomiseen. Tuloksena syntyi palomuurilla varustettu yritysverkon topologia, jonka tarkoituksena on toimia pohjana tulevissa BPI-kursseissa.

Asiasanat

Cisco, palomuuri, yritysverkko, tietoturva

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Henri Pasonen	Bachelor of Engineering	December 2018

Thesis title

Firewall implementation in an enterprise network in the Cisco environment

39 pages
0 pages of appendices

Commissioned by

South-Eastern Finland University of Applied Sciences, ICTLAB

Supervisor

Martti Kettunen

Abstract

The purpose of this thesis was to study how a firewall could be implemented as a new part of the topology of an existing enterprise network. The purpose is also to improve the existing Big Picture of Internet course material with the created firewall implementation. The implementation of the firewall was to be carried out without a need to modify the original topology of the enterprise network except for the firewall implementation and without affecting the redundancy of the enterprise network. The firewall was seen as a concept for improving the security of the enterprise network by investigating into any additional measures the firewall implementation would cause in the rest of the topology.

The importance of information security in enterprise networks is growing and companies require more and more personnel with sufficient understanding about the information security of networks. The work emphasizes the relationship between the internal and external zones of the firewalls and how the firewall affects the operations of the enterprise network.

At the beginning of the project, the development of the firewalls and their importance for enterprise networks was examined in general terms. At the same time, the structure of the enterprise network was also studied. The practical part of the thesis addressed planned firewall solutions for topology changes between the old and the new topologies and studied the solution protocols on a theoretical level.

The objectives set for the work were achieved for the most part successfully. As the work progressed, the focus shifted more and more to the development of BPI course material. This resulted in some planned firewall solutions being left out so as to focus on working with a single solution. The result was a new topology with a firewall for the enterprise network and this topology is to be used as a basis for future BPI courses.

Keywords

Cisco, firewall, enterprise network, information security

SISÄLLYS

KÄYTETYT LYHENTEET JA TERMIT

ALS/AL	Access Layer Switch
AS	Autonomous System
ASA	Adaptive Security Appliances
BGP	Border Gateway Protocol
BPI	Big Picture of Internet
CE	Customer Edge (Router)
DLS/DL	Distribution Layer Switch
FW	Firewall
FWaaS	Firewall as a Service
HSRP	Hot Standby Router Protocol
IGP	Interior Gateway Protocol
LACP	Link Aggregation Control Protocol
MPLS	Multiprotocol Label Switching
NGFW	Next-Generation Firewall
VLAN	Virtual Local Area Network
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network

1 JOHDANTO

Kaakkois-Suomen ammattikorkeakoulu Kotkan kampuksen tieto- ja viestintätekniikan tietoverkkojen koulutuslinja on viime vuosina painottunut jatkuvasti enemmän kyberturvallisuuden suuntaan. Vuonna 2019 aloittavilla tutkintonimikkeenä toimiikin ensimmäistä kertaa ”Insinööri (AMK), kyberturvallisuus”. Koulutuksen painottumissuunnan muutokset johtavat siihen, että kurssien materiaaleja pitäisi päivittää.

Big Picture of Internet, tästä eteenpäin BPI, on ensimmäisen vuoden tietoverkkotekniikan opiskelijoille tarkoitettu kilpailuhenkinen projektikurssi. Kurssin tarkoitus on toimia haasteena uusille opiskelijoille ja tutustuttaa heidät valitsemansa opintolinjan pääelementtiin eli toimivan tietoverkon rakentamiseen. Painottumissuunnan muuttuessa kurssikin tarvitsee uusia haasteita kyberturvallisuuden näkökulmasta. (Kettunen 2014, 90–96.)

Opinnäytetyön toimeksiantaja on Kaakkois-Suomen ammattikorkeakoulun, eli XAMK:n, Kotkan kampuksen ICTLAB. XAMK on korkeamman asteen koulutusinstituutti, joka muodostui vuonna 2017 Kymenlaakson ammattikorkeakoulun ja Mikkelin ammattikorkeakoulun yhdistyessä. XAMK:n Kotkan ICTLAB:ssa koulutetaan tulevaisuuden tietoverkkojen kyberturvallisuuden osaajia sekä peliohjelmoijia.

1.1 Opinnäytetyön tavoitteet

Opinnäytetyön ensisijaisena tavoitteena on suunnitella ja toteuttaa, kuinka olemassa olevaan verkkotopologiaan saisi lisättyä uutena osana palomuurikerroksen. Palomuurikerroksen lisääminen vaatii sen, että alkuperäisestä vain reitittimistä ja kytkimistä muodostuvaa topologiaa rikotaan. Tämä johtaa siihen, ettei alkuperäisen topologian laitteissa käytetyt asetukset ole enää toimivia. Uuden topologian laitteisiin tulee laittaa uudet asetukset, jotta verkon yhteydet olisivat taas kunnossa.

Työn tarkoituksena on, että järjestelmä olisi palomuurien lisäysten jälkeen edelleen toimiva, redundanttinen ja virheensietokykyinen. Työssä tullaan poh-

timaan, millaisia protokollia ja tekniikoita tällaisessa järjestelmässä voisi käyttää ja mitkä konfiguraatioratkaisut olisivat kohtalaisen yksinkertaiset toteuttaa ja kuvastaisivat todellisuutta. Saatuja tuloksia tultaisiin käyttämään tulevissa BPI-kursseissa, sillä uusi palomuurikerros palvelisi täydennyksenä nykyisen kurssin topologiassa. Ajatuksena on rakentaa palomuurien osalta kehykset uusien tietoverkkotekniikan kyberturvallisuuden opiskelijoiden kurssin materiaaleihin, jossa he ottavat ensimmäistä kertaa kunnolla kosketusta tietoverkkoihin.

Tämän opinnäytetyön tutkimusongelma on, kuinka palomuurit liitetään olemassa olevaan verkkoon vaikuttamatta liikaa muun yrityksen verkon toimintaan. Vastausta tutkimusongelmaan haetaan tutkimalla tapoja, joilla yritysverkosta lähtevän ja siihen saapuvan verkkoliikenteen saa kulkemaan palomuurin kautta. Samalla etsitään toimivaa keinoa palomuurin liittämiseksi verkkoon. Toimivuutta määritellään vertailemalla protokollien helppokäyttöisyyttä, joka tässä tapauksessa tarkoittaa protokollan tai protokollien laitteisiin konfiguroinnin yksinkertaisuutta. Koska työssä käytetään vain tietoliikenne- ja elektroniikkateollisuusyritys Ciscon laitteita, lopputulos ei ole täysin universaali.

Työ perustuu suurimmilta osin palomuurien implementointiin yritysverkon sisällä. Toisin sanoen kyseisessä tilanteessa yritys olisi oman palomuurikerroksensa haltija. Työssä tarkastellaan myös Firewall as a Service -vaihtoehtoa (FWaaS), jossa palomuuri tuodaankin palveluna palveluntarjoajan puolelta. Mainittu BPI-kurssi käsittelee myös ISP-puolen verkkoa, jolloin FWaaS on varteenotettava vaihtoehto palomuuriratkaisua mietittäessä.

1.2 Opinnäytetyön tietoperusta

Tämän opinnäytetyön aihetta sivuavia opinnäytetöitä löytyy Theseuksesta paljon. Ne opinnäytetyöt, joissa palomuuri ja/tai verkon suunnittelu ja sen rakentaminen olivat pääosassa, päätyivät lopulta lähemmän tarkastelun alle. Nämä opinnäytetyöt vaikuttivat olevan lähimpänä tämän opinnäytetyön aihetta: Mariia Miroshnichenkon (2018) Design and Configuration of a Factory Network, Konstantin Kaibijaisen (2013) Palomuurin suunnittelu ja käyttöönotto pienessä yritysverkossa sekä Timo Aroalhon (2013) Datakeskuksen tietoverkkojärjestelmä.

Theseuksessa esiintyvien tietoverkkoon ja tietoturvaan liittyvien opinnäytetöiden määrä ja tuoreus osoittavat, että verkon huolellinen suunnittelu ja tietoturvan huomioonottaminen suunnittelussa ovat tällä alalla tärkeitä taitoja. Esimerkiksi esineiden internetin (IoT) takia kyberturvallisuuden merkitys on jatkuvasti kasvussa. Samalla kun uusia laitteita pitäisi voida kytkeä verkkoon, myös yrityksen verkon rungon tulisi olla muokattavissa tarvittavia tietoturvaparannuksia varten. Tässä opinnäytetyössä ei keskitytä niinkään uuden verkon suunnitteluun, vaan vanhan topologian muokkaamiseen kyberturvallisuuden näkökulmasta.

1.3 Tutkimusmenetelmän valinta

Tämän opinnäytetyön aiheen synty perustuu kokonaan sille ajatukselle, että siitä syntyviä tuloksia voisi käyttää tietoverkkojen kyberturvallisuuden kurssimateriaalin kehittämisessä. Opinnäytetyön tutkimusotteeksi valikoituikin kehittämistutkimus. Kananen kertoo, että oikea käännös ”design research” -termille on kehittämistutkimus. Kehittämistutkimusta ei pidetä omana tutkimusmenetelmänään eikä sillä ole omaa metodologiaa. Kyseessä onkin useasta eri menetelmästä muodostuva kokonaisuus. Kehittämistutkimuksessa yhdistellään tarpeen mukaan kvalitatiivisia ja kvantitatiivisia tutkimusmenetelmiä. Tämä perustuu siihen, että kehittämistyötä on monenlaista ja muutosta voidaan saada aikaan erilaisilla tavoilla. (Kananen 2015a, 33.) Vaikka kehittämistutkimus onkin monimenetelmäinen, sen on mahdollista olla pelkästään kvalitatiivista tutkimusta. (Kananen 2017, 18).

Kehittämistutkimuksessa sanansa mukaisesti kehitetään jotain tuotetta, menetelmää, organisaatiota tms. (Kananen 2015a, 39). Tämän opinnäytetyön tapauksessa kehitetään vanhan kurssin materiaalia. Jos myös tarkastellaan Kanasen (2015b, 55) taulukkoa, kehittämistutkimus eli design research on oikeastaan ainoa lähestymistapa, jonka puitteisiin tämä opinnäytetyö sopii. Tässä työssä pyritään saamaan aikaan muutoksia kurssimateriaaliin ja työssä käsiteltävä teoria ja tarvittavat käytännön sovellukset ovat jatkuvassa vuorovaikutuksessa keskenään.

2 PALOMUURI

Tämän opinnäytetyön suurin yksittäinen osa-alue on palomuuri. Palomuuri on kehittynyt vuosien saatossa paljon. Tässä luvussa käsitellään palomuurin historiaa, nykytilannetta, erilaisia palomuurityyppejä sekä palomuurien merkitystä yrityksen tietoverkolle.

Palomuuri on tietoverkon turvajärjestelmä, mikä valvoo ja hallinnoi kaikkea itsensä lävitse kulkevaa verkkoliikennettä. Palomuurit joko estävät tai sallivat liikenteen kulkemisen itsensä lävitse perustuen siihen asetettuihin palomuurisääntöihin. Palomuureista voi ajatella, että ne muodostavat ikään kuin portin kahden valitun verkon välille. Yleensä palomuurin ”sisäpuolella” on luotettava kodin tai yrityksen sisäinen verkko ja ”ulkopuolella” epäluotettava verkko, kuten Internet. (Cisco 2018a.)

2.1 Palomuurin historia

Tietotekniikka on aina kehittynyt tietoturvan teknologioita nopeammin. Tietotekniikka lähti kunnolla kehittymään 1970-luvulla, kun ensimmäinen PC, eli personal home computer tai suomeksi kotitietokone valmistettiin. Ensimmäiset tietoturvan konseptit syntyivät kuitenkin myöhemmin. (Brazil 2017.) 1980-luvun puolivälissä eri alojen teknologioiden parissa toimiva Honeywell-yritys työskenteli yhdessä yhdysvaltalaisen tiedusteluvirasto NSA:n kanssa. Yhteistyön tarkoituksena oli saada aikaan tietoturvaltaan vahvennettu käyttöjärjestelmä, jonka nimeksi annettiin Logical Coprocessing Kernel, LOCK. Tämä oli ensimmäisiä tietoturvan vahventamiseen tarkoitettuja sovellutuksia ja kyseistä käyttöjärjestelmää käytettiin myöhemmin palomuureissa. (Devich 2015.)

Palomuurin esiaste kehitettiin aivan 1980-luvun lopussa, kun ensimmäiset Internetin kautta levinneet virukset olivat jo päässeet tekemään tuhojaan pari vuotta aiemmin. Morris-niminen virus saastutti 10 % silloisesta Internetiin kytketyistä laitteista ja tämä tapaus osoitti, että tietoverkkojen turvallisuuteen tulisi kiinnittää enemmän huomiota. (Devich 2015.) Nämä ensimmäiset palomuurit olivat reitittimiä, joita käytettiin jakamaan yritysverkko pienempiin pai-

kallisiin lähiverkkoihin. Tämä tarkoittaa sitä, että alkuperäinen isompi yritysverkko jaetaan pienempiin palasiin siten, ettei yhteen paikallisverkkoon kohdistuva hyökkäys tai ongelma leviä kaikkialle yritysverkkoon. (Avolio 1999.)

1990-luvulla tapahtui huomattavia kehitysaskeleita palomuurin osalta. Vuosikymmenen alussa kehitettiin reitittimiä, joihin pystyi asettamaan verkkoliikenteen suodattamissääntöjä. Tätä ominaisuutta kutsuttiin nimellä ”packet filtering” eli pakettisuodatus. Ensimmäiset luodut säännöt käytännössä sallivat kaiken liikenteen yritysverkosta muualle ja estivät kaiken muualta tulevan liikenteen yritysverkkoon. (Avolio 1999.)

Ensimmäinen kaupallinen palomuuri DEC valmistui DEC’s Network Systems Lab:n ja Palo Alton yhteistyön tuloksena. Tuote toimitettiin asiakkaalle vuonna 1991. DEC-palomuuria kuitenkin haluttiin kehittää paremmaksi ja muutamia kuukausia myöhemmin syntyi DEC SEAL, eli DEC Secure External Access Link. DEC SEAL:n julkaisun jälkeen myös muut yritykset alkoivat julkaista omia kaupallisia palomuurituotteita. (Avolio 1999.)

Myöhemmin ennen 1990-luvun puoliväliä kehitettiin ensimmäiset ”stateful” eli ”tilalliset” palomuurit. Check Point Software esitteli patentoimansa ”stateful inspection” -teknologian julkaisemalla FireWall-1-tuotteen. Tämä teknologia toimii edelleen perustana monille tietoverkon turvallisuuden teknologioille. (Checkpoint s.a.)

Tämän ”tilallisen” palomuurin suurimpia etuja olivat sen ylläpidon helppous ja kehittynyt palomuurisääntöjen luominen. Check Pointin palomuurissa oli oma graafinen käyttöliittymänsä, joten laitteen ylläpitäjän ei tarvinnut välttämättä osata käyttää tekstipohjaisia komentoja konsoli-ikkunassa. Tekstipohjaisissa laitteissa jokainen sääntö piti luoda erikseen ja yhteen sääntöön pystyi määrittelemään vain vähän asioita eikä tehtyjä sääntöjä voinut muokata jälkikäteen. Graafinen käyttöliittymä mahdollisti monimutkaisempien sääntöjen luomisen sekä vanhojen sääntöjen muokkaamisen tehden palomuurisääntöjen hallinnasta paljon tehokkaampaa. (Brazil 2017.)

Tilalliset palomuurit olivat pitkään melkein kuin standardi yritysten tietoverkon suojaamisessa. Haittaohjelmien kehittyessä ja tietoverkkohyökkäysten yleistyessä yritykset eivät enää pitäneet tietoverkkojensa turvaamista toissijaisena. Yrityksen ja asiakkaiden tietoja piti pystyä suojaamaan. Niinpä yritykset alkoivat hiljalleen sisältää tietoverkkojensa turvaamisen osaksi liiketoimintamallejaan 2000-luvun aikana. Haittaohjelmien kehittäminen ei kuitenkaan loppunut, hyökkäykset tietoverkkoihin jatkuivat ja nyt myös palomuurien yleistymisen takia eri tietoturvayritykset pyrkivät jatkuvasti hankkimaan isompaa jalansijaa markkinoilla. Tämä johti lopulta aivan uudenlaisen palomuurin syntymiseen, ja vuonna 2010 Palo Alto julkaisi uuden sukupolven palomuurin, jota kutsutaan myös nimellä NGFW. (Brazil 2017.)

2.2 Pakettisuodatin – Stateless

Kuten mainittu, ensimmäiset palomuurit olivat reitittimissä toimivia pakettisuodattimia. Normaalisti reititin ei välitä siitä, millaista dataa sen lävitse kulkee. Reitittimen tehtävä on ohjata siihen saapuva tietoliikenne, eli IP-paketit, oikeaan suuntaan. Reititin ei itsessään osaa tarkastaa IP-paketteja muuten kuin paketista luetun kohdeosoitteen osalta. Kuten nimi antaa ymmärtää, kohdeosoite on sen laitteen IP-osoite, jonne paketti on matkalla. Paketista luettua kohdeosoitetta verrataan reititysprotokollan tai -protokollien tekemään reititystauluun ja paketti ohjataan oikeaan suuntaan. (Zwicky ym. 2000, 165.)

Reitittimessä toimiva pakettisuodatin on kyberturvallisuuden näkökulmasta reitittimen äly. Reititin vain ohjaisi saapuvan paketin eteenpäin, mutta pakettisuodatin tarkastelee saapuvaa pakettia ennen päätöksen tekoa. Tavallisesti tarkastelun kohteena on IP-paketin lähde- tai kohdeosoite. Pakettisuodatin vertailee reititettävän paketin tietoja pakettisuodattimeen asetettuihin suodatussääntöihin ja näiden sääntöjen perusteella joko antaa reitittimen tehdä työnsä tai ”pudottaa” paketin, eli ei salli sen reitittämistä eteenpäin. (Zwicky ym. 2000, 165–166.)

Stateless eli tilaton pakettisuodatus on tehokas tapa tietoverkon suojaamiseen, jos tarkastelun kohteena on vain yksittäiset paketit. Pakettisuodattimella voidaan nimittäin estää yhden suodattamissäännön avulla kaikki liikenne halu-

tuista IP-osoiteryhmistä esimerkiksi yrityksen sisäverkon suuntaan. Pakettisuodattimen avulla määritellään, mitkä reitittimen portit ovat luotettavaa sisäpuolen verkkoa ja mikä epäluotettavaa ulkopuolen verkkoa. Otetaan esimerkkinä ”address-spoofing” eli IP-osoitteen väärentäminen. Tässä hyökkäysmuodossa niin sanotusta ulkoverkosta saapuva paketti väittää lähdeosoitteekseen jonkun sisäverkkoon kuuluvan osoitteen. Tässä ei kuitenkaan ole mitään järkeä, mutta ilman pakettisuodatinta reititin antaisi kyseisen paketin kulkea sisäverkkoon. Pakettisuodattimeen pystyy kuitenkin asettamaan sääntöjä, jotka estävät reitittimen ”ulkopuolelta” saapuvat sisäverkon osoitteet. Pakettisuodattimen heikkoudet tulevat esille silloin, kun täytyisi ottaa huomioon eri protokollia tai jos haluttaisiin monitoroida verkkoliikenteen tapahtumia. Näissä tilanteissa käytetään yleensä kehittyneempiä järjestelmiä, kuten välityspalvelinta. (Zwicky ym. 166–167.)

2.3 Pakettisuodatin – Stateful

Stateful eli tilallinen pakettisuodatin on edeltäjäänsä huomattavasti kehittyneempi. Siinä missä tilattomassa pakettisuodatuksessa tarkastelun kohteena oli aina yksi paketti, tilallinen pakettisuodatin kykenee seuraamaan itsensä kautta kulkevan yhteyden tilaa. Tilallisen pakettisuodattimen avulla pystytään myös tarkastelemaan protokollia ja asettamaan niille suodattamissääntöjä. Tilallista pakettisuodatinta kutsutaan myös dynaamiseksi pakettisuodattimeksi. Tämä nimitys tulee siitä, että tilallinen pakettisuodatin kykenee tarpeen vaatiessa muuttamaan toimintaansa tietyn yhteyden suhteen perustuen sen hetkiseen liikenteeseen. (Zwicky ym. 168–169.)

Tilallisen pakettisuodattimen toimintaa voi ymmärtää Transport Control Protocollan eli TCP:n kautta, sillä TCP on yhteyspohjainen protokolla. TCP seuraa yhteyttä muodostaessaan lähde- ja kohdeosoitteita sekä portteja.TCP muodostaa kahden laitteen välisen yhteyden ”kättelyllä”. Näitä kättelyn vaiheita kuvataan lyhenteillä SYN, SYN-ACK ja ACK. Lyhenteet tulevat sanoista synchronization ja acknowledgement. Yhteyttä avaava laite aloittaa kättelyn SYN-paketilla, vastaanottava laite vastaa siihen SYN-ACK-paketilla ja lopulta yhteyden aloittanut laite ilmoittaa SYN-ACK-paketin saapumisesta ACK-paketilla. Kättelyn päätyttyä yhteys laitteiden välillä on muodostettu. Kun yhteyttä ei

enää tarvita, se lopetetaan molempien laitteiden puolesta FIN- ja ACK-paketeilla. Kumpikin laitteista lähettää toiselle FIN-paketin ja ilmoittaa sen saapumisesta ACK-paketilla. (Wilkins 2013.) Tilallinen palomuuri seuraa kättelyn aikana ja yhteyden muodostamisen jälkeen pakettien käyttämiä lähde- ja kohdeosoitteita sekä portteja. Se vertaa itsestään poispäin lähtevän paketin tietoja saapuvan paketin tietoihin ja varmistaa, että saapuvan paketin tiedot vastaavat alkuperäisen lähetetyn paketin vastaanottajan tietoja. (Techopedia s.a.)

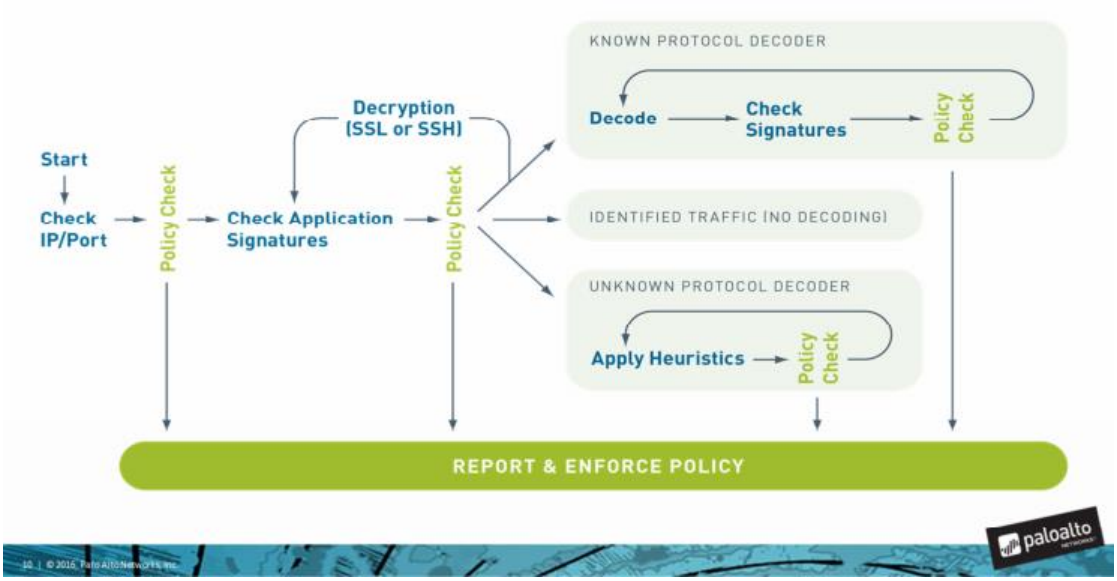
2.4 Uuden sukupolven palomuuri – NGFW

Tilallinen pakettisuodatin oli vielä varsin toimiva ratkaisu verkkojen suojaamiseen, kun sovellustason liikenne oli vielä kohtuullisen yksinkertaista ja perustui suurimmilta osin vakioina pysyviin porttinumeroihin. Tämä tarkoitti sitä, että kun palomuureissa esti tietyn portin, esti myös tietyn sovelluksen. Nykypäivänä Internet on kuitenkin paljon suurempi ja suuri osa yritysverkkojenkin liikenteestä kohdistuu Internetin sisältämiin palveluihin ja sovelluksiin. Perinteinen palomuuri ei ole enää turvallinen eikä välttämättä kannattavakaan ratkaisu, koska vanhat sovellusten porttisäännöt eivät ole enää päteviä. (Miller 2016, 23–25.)

Ongelmat porttien perusteella liikennettä suodattavissa palomuureissa tulee siinä, kun eri sovellukset käyttävätkin samaa porttia. Nämä perinteiset palomuurit eivät kykene erottelemaan sovelluksia toisistaan ja luottavat siihen, että tietty portti vastaa tiettyä sovellusta. Tämän lisäksi perinteinen palomuuri on kykenemätön erittelemään sovellusten ja palveluiden aiheuttamaa liikennettä sen perusteella, että olisiko liikenne hyödyksi tai haitaksi yrityksen verkolle. (Miller 2016, 25-26.)

NGFW-palomuurit ovat osa kolmannen sukupolven palomuuriteknologiaa, jolla pyritään turvaamaan verkot sovellustasolla. Tämä tarkoittaa sitä, että esimerkiksi TCP-yhteyksien muodostamisessa vaaditun kolmivaiheisen kättelyn aikana lähetettyjen kolmen paketin tarkastelu ei vielä riitä päätösten tekemiseen. Esimerkiksi TCP:tä käyttävä HTTP-protokolla lähettää NGFW-palomuurin kannalta merkityksellistä sovelluksen tietoa viidennessä paketissa ensimmäisestä kättelyn SYN-paketista katsottuna. (Palo Alto 2016, 9.)

NGFW-palomuuri pyrkii tunnistamaan tämän viidennen paketin sisältämän tiedon perusteella, mikä sovellus on kyseessä. Paketin sisältämää tieto käsitellään eri tavoilla riippuen siitä, kuinka palomuuri tunnistaa kyseisen tiedon. (Palo Alto 2016, 10.) Kuvassa 1 esitetään sovelluksen tunnistamisen vaiheet.



Kuva 1. Sovelluksen tunnistamisen vaiheet (Palo Alto 2016)

Kuvan 1 mukaan, palomuuri tarkistaa ensin paketin IP-osoitteen ja portin ja varmistaa, että paketti on niiltä osin kunnossa. Tämän jälkeen palomuuri analysoi pakettia perustuen sen kuljettaman sovelluksen sekä muodostetun yhteyden ominaisuuksiin. Näiden ominaisuuksien perusteella palomuuri katsoo, onko kyseessä tunnetun vai tuntemattoman protokollan avulla muodostettu yhteys. Jos paketin tiedot ovat salattuja SSL:n tai SSH:n avulla, palomuuri purkaa salauksen ja tarkastelee uudelleen sovelluksen ominaisuuksia ennen jatkopäätöksiä. Jos sovellus käyttää tunnettuja protokollia, palomuuri pyrkii tutkimaan ja purkamaan sovelluksen tietoja, kunnes sovellus on varmuudella tunnistettu esimerkiksi Facebookiksi. Jos sovellus käyttää palomuurille tuntemattomia protokollia, sovellus pyritään luokittelemaan sen käytöksen perusteella. Tätä toimenpidettä kutsutaan heuristiikaksi. (Palo Alto 2016, 10.)

Yksi NGFW-palomuurin ominaisuuksista on verkon käyttäjien tunnistaminen IP-osoitteen perusteella. Tämä mahdollistaa verkon hallinnoimisen jokaisen käyttäjän osalta erikseen. NGFW-palomuuri tekee yhteistyötä esimerkiksi yrityksen palvelimien kanssa kerätäkseen tarpeellisia tietoja verkon käyttäjistä. Nämä tiedot liittyvät usein käyttäjän rooliin yrityksessä. Näitä tietoja käytetään

tarpeen mukaan esimerkiksi silloin kun yritetään selvittää, ketkä käyttäjät ovat verkkokäyttäytymisellään mahdollisesti uhkia verkolle. Käyttäjien tietoja voidaan myös käyttää uusien palomuurisääntöjen muodostamiseen. Käyttäjien tunnistaminen tarjoaakin yrityksen IT-osastolle hyvän työkalun yrityksen sovelluskäytön säätelyyn. (Miller 2016, 36-37.)

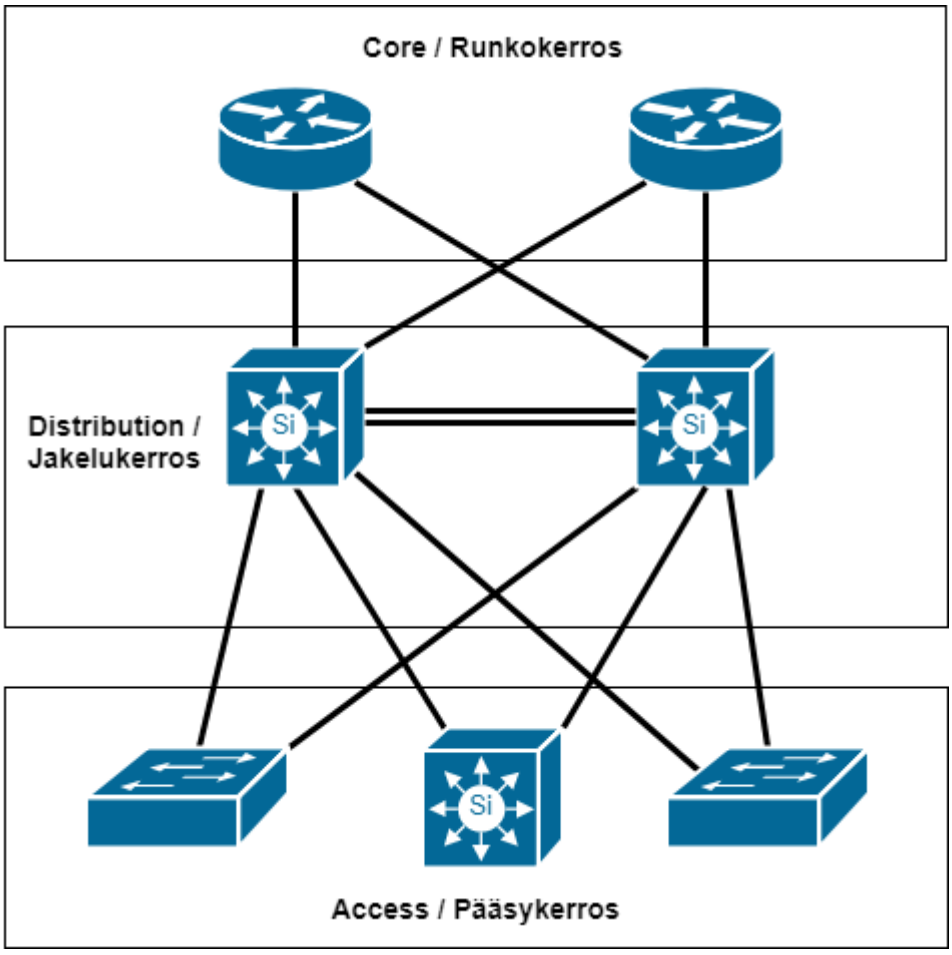
NGFW-palomuureissa käytetään sisällön tunnistusta (content identification), jonka avulla mahdollistetaan erilaisten uhkien torjuminen, URL-suodatus sekä tiedostojen ja tiedon suodatus. Uhkien torjumisella tarkoitetaan erilaisten haittaohjelmien pääsyn estämistä verkkoon. URL-suodatusta käytetään yhdessä aiemmin mainitun verkon käyttäjien tunnistuksen kanssa. Tämän avulla yrityksen IT-osasto pystyy monitoroimaan ja hallinnoimaan yrityksen verkon käyttöä jokaisen käyttäjän kohdalla erikseen. Tiedostojen suodatuksella mahdollistetaan tiedostojen luvattoman siirron estäminen. Tällä pyritään estämään tietovuotoja. (Miller 2016, 38-39.)

3 YRITYKSEN KAMPUSVERKKO

Yrityksen kampusverkko on tietoverkon näkökulmasta se yritysverkon osa, jonka kautta loppukäyttäjä, kuten työntekijä, pääsee käsiksi eri yritysverkon tarjoamiin palveluihin. Kampusverkon kautta loppukäyttäjä pääsee muodostamaan yhteyden tyypillisesti ensin yrityksen runkoverkkoon ja sitä kautta esimerkiksi yrityksen datakeskukseen, toisiin saman yrityksen kampusverkkoihin tai vaikka Internet-palveluntarjoajaan. (Cisco 2013.)

Ciscon suosittelema kampusverkon rakenne koostuu kolmesta pääkerroksesta, jotka ovat runko-, jakelu- ja pääsykerrokset. Vaihtoehtoisena neljäntenä osana on runkokerrokseen yhdistyvä yrityskampuksen palvelukerros, mutta tämän työn osalta keskitytään vain kolmeen mainittuun pääkerrokseen. Kuva 2 on Ciscon 2013 SAFE Reference Guiden Enterprise Campus -kappaleen Figure 5-1:n ja 5-2:n pohjalta tehty yksinkertaistettu malli, joka on toiminut myös tämän hetken BPI-kurssin kampusverkon topologiana. Kuvan topologia seuraa modulaarisen hierarkian mallia. Kyseisessä topologiassa eri tietoverkon ominaisuudet jaotellaan selkeisiin lohkoihin, joista lopullinen kokonaisuus rakennetaan. Tarkoituksena on saada aikaan virheensietokykyinen, skaalautuva

ja redundanttinen korkean käyttöasteen verkko. Skaalautuvuudella tarkoitetaan sitä, että verkkoon voidaan lisätä helposti uusia laitteita. Korkealla käyttöasteella tarkoitetaan sitä, että verkko pysyy mahdollisesti jatkuvasti toiminnassa ja kykenee sujuvasti palvelemaan mahdollisimman useaa käyttäjää. Redundanttisuudella tarkoitetaan sitä, että jos verkossa laite hajoaa tai yhteys kyseiselle laitteelle jollain tavalla menetetään, verkon liikenteelle on olemassa yksi tai useampi vaihtoehtoinen reitti. (Cisco 2013.)



Kuva 2. Ciscon suosittelema kampusverkon kolmijako (Cisco 2013)

Pääsykerroksessa eri päätelaitteet, kuten tietokoneet ja langattomat tukiasemat, yhdistetään yritysverkkoon. On tavallista, että pääsykerroksessa erilaisia laiteryhmiä jaotellaan virtuaalisiin lähiverkkoihin muun muassa turvallisuuden parantamiseksi. (Cisco 2013.) Kuvassa 2 nähdään, että jokainen pääsykerroksen laite on yhdistetty kahteen jakelukerroksen laitteeseen. Tällä pyritään saavuttamaan redundanttisuus pääsy- ja jakelukerroksen välille.

Jakelukerroksen voi ajatella olevan kampusverkon äly. Ensinnäkin se toimii liikennettä kontrolloivana pisteenä pääsykerroksen ja runkokerroksen välillä. Jakelukerroksessa ryhmitellään pääsykerroksen liikenne ja pyritään näin suojaamaan runkokerrosta ylimääräiseltä rasitukselta. Ilman jakelukerrosta kaikki pääsykerroksen liikenne menisi käsittelemättä runkokerrokseen ja sen sisältämät laitteet joutuisivat tekemään paljon enemmän töitä. Mitä enemmän pääsykerroksessa on laitteita, sitä enemmän syntyy liikennettä ja verkon toiminta hidastuu. Jakelukerroksessa on jo hoidettu pääsykerroksen liikenne ja näin runkokerroksen tarvitsee vaan reitittää saapuva liikenne eteenpäin. Toinen jakelukerroksen työ on liikenteen suodattaminen. Jakelukerroksen laitteisiin voi kuulua esimerkiksi palomuurit, joilla voidaan sallia tai estää liikennettä tarpeen mukaan. (Cisco 2013.)

Runkokerros on se piste, mihin kaikki yritysverkon palaset lopulta liittyvät. Runkokerroksen tehtävänä on hoitaa, että kaikki liikenne menee oikeaan suuntaan. Runkokerroksen avulla yritysverkko yhdistetään esimerkiksi Internet-palveluntarjoajaan. Koska yritysverkon liikenne on riippuvainen runkokerroksen toiminnasta, sen tulee olla nopea, virheensietokykyinen sekä redundanttinen. Runkokerroksen laitteiden konfiguraatiot tulisi myös pitää mahdollisimman yksinkertaisina käyttövirheiden minimoimiseksi. (Cisco 2013.)

4 KÄYTETYT PROTOKOLLAT JA TEKNOLOGIAT

4.1 Virtuaalilähiverkot ja IEEE 802.1Q

Virtuaalisten lähiverkkojen eli VLAN:ien avulla yrityksen fyysistä verkkoa voidaan jaotella pienempiin loogisiin kokonaisuuksiin perustuen esimerkiksi osaston tarkoitukseen. VLAN:n tarkoituksena on, että eri osastojen verkkoliikenne pystytään erottelemaan toisistaan. Tämä erottelu johtuu siitä, että jokainen VLAN muodostaa oman broadcast domainin. Broadcast domainin sisäiset laitteet kykenevät lähettämään toisilleen paketteja broadcastina. Tämä tarkoittaa sitä, että paketti lähetetään samanaikaisesti kaikille broadcast domainin sisäisille laitteille. Kaikki laitteet huomaavat lähetetyn paketin, mutta lopulta vain kohdelaite vastaanottaa paketin. (Froom & Frahim 2015, 42–44.) Broadcast domainien välinen viestintä vaatii reitittämistä. Tämä lisää tietoturvaa, koska näin voidaan säädellä fyysisen verkon laitteiden sisällä, mitkä VLAN:it voivat keskustella keskenään. (Cisco 2018b.)

IEEE 802.1Q

IEEE 802.1Q eli dot1q on standardi kytkimien välisten runkolinkkien muodostamiseksi. Runkolinkin avulla muodostetaan kahden laitteen välille yhteys, jossa sallitaan tavallisesti usean VLAN:n liikenteen kulkevan yhden fyysisen linkin läpi. Runkolinkkien avulla voidaan laajentaa VLAN:ien liikennöintialuetta halutulla tavalla verkon eri osiin. Runkolinkin muodostaminen tapahtuu siten, että kahden laitteen välisen linkin portit konfiguroidaan runkoporteiksi. Runkoporteissa määritetään linkillä sallitut VLAN:it. Kun IP-paketti saapuu runkoporttiin, sen ”headeriin” eli ”otsakkeeseen” lisätään tunniste. Tunniste sisältää tietoa siitä, mihin VLAN:iin paketti kuuluu ja näin se pystytään ohjaamaan oikeaan paikkaan runkolinkkien kautta. (Froom & Frahim 2015, 49.) Runkoporttien lisäksi käytetään pääsyportteja. Pääsyporteissa sallitaan vain yhden VLAN:n liikenne. (Cisco 2018c.)

4.2 HSRP-protokolla

Ciscon kehittämä Hot Standby Router Protocol eli HSRP on Ciscon vakiintunut tapa luoda korkean käyttöasteen tietoverkkoja (Cisco 2017a). HSRP:n avulla muodostetaan redundanttinen oletusyhdyskäytävä IP-osoitteilla varustetuille päätelaitteille. HSRP:n tuoma redundanttisuus johtuu siitä, että se käyttää useita reitittimiä. Tiettyyn HSRP-ryhmään valittujen reitittimien liityntärajapinnat toimivat yhdessä muodostaakseen yhden virtuaalisen reitittimen ja kyseiseen HSRP-ryhmään kuuluvien lähiverkkojen päätelaitteet tällöin kuvittelevat, että verkossa on vain yksi oletusyhdyskäytävä. Kun HSRP on konfiguroitu tarvittavan lähiverkon reitittimiin, se jakaa kyseisille reitittimille yhdet yhteiset MAC- ja IP-osoitteet. (Froom & Frahim 2015, 250.)

HSRP-ryhmässä voi olla kaksi tai useampi reititin. Tietylle liityntärajapinnalle voi kuitenkin olla vain yksi aktiivinen reititin. Tämä tarkoittaa sitä, että HSRP-ryhmässä reitittimet jaetaan tarvittavien liityntärajapintojen osalta active- ja standby-laitteisiin. Active-reititin toimii ryhmän reitittävänä laitteena. Active-reitittimen liityntärajapintaan kuuluvat päätelaitteet luulevat käyttävänsä yhtä ainoaa reititintä verkossa liikennöimiseen, mutta todellisuudessa Active-reititin hoitaa verkkoliikenteen ohjaamisen tarvittavaan suuntaan. Jos Active-reititin

esimerkiksi hajoaa, HSRP-ryhmän Standby-reititin muuttuu Active-reitittimeksi niille liityntärajapinnoille, jotka vielä äsken liikennöivät nyt hajonneen reitittimen kautta. HSRP-ryhmän reitittimet lähettävät toisilleen niin kutsuttuja hellopaketteja, joiden avulla ne huomaavat, jos jokin ryhmän reitittimistä on virhetilassa. (Cisco 2017a.) HSRP:lle löytyy myös vaihtoehtoisia protokollia, kuten Virtual Router Redundancy Protocol eli VRRP. VRRP on toiminnaltaan hyvin samankaltainen kuin HSRP, mutta se ei ole Ciscon kehittämä. (Froom & Frahim 2015, 275.)

4.3 OSPF-reititys

OSPF eli Open Shortest Path First on IETF:n kehittämä reititysprotokolla. OSPF:ää alettiin kehittämään 1980-luvun lopulla, kun siihen aikaan käytetty vanhempi reititysprotokolla RIP eli Routing Information Protocol ei enää riittänyt palvelemaan suuria ja jatkuvasti kasvavia tietoverkkoja. (Cisco 2012.) OSPF on “link-state” reititysprotokolla. Tämä tarkoittaa sitä, että OSPF:ää käyttävät reitittimet vaihtavat topologiatietojaan vain viereisten reititinnaapureiden kanssa. OSPF-laitteiden välillä levitetään link-state advertisement eli LSA-tietoja kokonaisten reititystaulupäivitysten sijasta, minkä takia OSPF-verkossa tapahtuvat muutokset havaitaan nopeasti. (Teare ym. 2015, 155.)

OSPF:n suurin etu muiden samankaltaisten ”link-state”-reititysprotokollien kanssa on se, että se tietää koko verkon topologian, riippuen tietenkin konfiguraatioista (Metaswitch s.a.). Tämä tietämys mahdollistaa sen, että OSPF pystyy tarkastelemaan eri reittejä verkon sisällä ja vertailemaan niitä reitin pituuden mukaan. OSPF käyttää Shortest Path First -algoritmia, jonka avulla se laskee lyhyimmän reitin eri verkon laitteiden välillä. (Teare ym. 2015, 155.)

4.4 LACP

LACP eli Link Aggregation Control Protocol on osa IEEE 802.3ad -standardia, jonka avulla voidaan muodostaa useasta laitteen fyysisestä portista yksi loogi-nen linkki. LACP toimii kontrolliprotokollana Link Aggregation Groupille eli LAG:lle. LACP:n tehtävänä on varmistaa, ettei LAG:tä muodostettaessa olla tehty konfiguraatiovirheitä. LACP:n konfiguraation tulee olla symmetrinen linkin molemmissa päissä tai linkki ei toimi. LACP:n avulla muodostetaan kahden

laitteen välille luotettava ja redundanttinen linkki. Jos joku LACP-linkin fyysisistä porteista kummassa tahansa laitteista menee syystä tai toisesta vikatilaan, linkki pysyy kuitenkin ylhäällä ja liikenne kulkee kyseisen linkin lävitse normaalisti. (Cisco 2018d.)

Ciscon oma versio LAG-teknologiasta on nimeltään EtherChannel. Samoin kuin LAG:n kanssa, EtherChannel yhdistää halutut fyysiset linkit yhdeksi loogiseksi linkiksi. LAG:n ja EtherChannelin ominaisuudet ovat samat, mutta Cisco painottaa EtherChannelin olevan tarkoitettu laitteiden välisen liikennöinnin nopeuden kasvattamiseen. Yhdellä EtherChannel-linkillä voidaan liikennöidä vain kahden laitteen välillä. (Froom & Frahim 2015, 94-95.)

LACP:n toiminnan edellytys on, että linkin molemmat päät ovat konfiguroitu samalla tavalla. Layer 2 -tason LACP vaatii, että molemmissa päissä sallitaan samojen VLAN:ien liikenne linkin lävitse. (Froom & Frahim 2015, 99.) Layer 3 -tason LACP-linkki vaatii, että muodostetun loogisen linkin molempien päiden fyysiset portit on muutettu reitittäviksi porteiksi, eli niille konfiguroidaan IP-osoitteet (Froom & Frahim 2015, 225).

4.5 BGP-protokolla

Border Gateway Protocol eli BGP on suurien verkkokokonaisuuksien välisten naapuruussuhteiden luomiseen tarkoitettu reititysprotokolla. Internet-palveluntarjoajat käyttävät BGP:tä muodostaakseen verkkojen reitityksen muiden palveluntarjoajien kanssa ja tuntemamme Internet toimii palveluntarjoajien välisten BGP-naapuruussuhteiden avulla. BGP:stä käytetään myös nimityksiä eBGP eli external BGP ja iBGP eli internal BGP riippuen siitä, mihin tarkoitukseen BGP-reititystä käytetään. BGP-reititys muodostetaan autonomisten systeemien eli AS:ien sisälle tai välille. Haluttu verkkokokonaisuus muodostaa yhden AS:n. Mainittu eBGP muodostetaan kahden eri AS:n välille ja iBGP toimii yhden AS:n sisällä. (Zhang & Bartell 2006, 5-9.)

BGP:ssä laitenaapurit vaihtavat keskenään kaikki BGP-reititystaulunsa tiedot, kun yhteys naapureiden välillä on ensimmäisen kerran muodostettu. Kun reititystaulussa tapahtuu muutos, BGP-reititin lähettää naapureilleen reititystaulu-

päivityksen vain muuttuneen reitin osalta. BGP-reitittimet eivät myöskään lähetä toisilleen muutosten välissä mitään BGP:hen liittyviä tietoja ja reititin mainostaa naapureilleen aina parhaimman reitin haluttuun kohdeverkkoon. (Cisco 2017b.)

4.6 MPLS ja VPLS

Normaalissa tapauksessa, kun IP-paketti siirtyy reitittimeltä toiselle, jokainen reititin joutuu tekemään oman päätöksensä paketin siirtämisestä eteenpäin. Yksi reititin joutuu aina käsittelemään IP-paketin eli otsakkeen, joka sisältää reitititintä kiinnostavan kohdeosoitteen lisäksi paljon reitittimen näkökulmasta turhaa tietoa. Reititin päättää kohdeosoitteen perusteella, mihin suuntaan paketti täytyy lähettää ja jokainen reitillä oleva reititin joutuu tekemään saman prosessin erikseen. (Guichard & Pepelnjak 2009, 5–6.)

MPLS on suunniteltu tämän prosessin helpottamiseksi. Jos verkossa käytetään Multiprotocol Label Switching -tekniikkaa (MPLS), päätös IP-paketin kuljetuksen suunnasta tehdään vain silloin kun se ensimmäisen kerran saapuu MPLS-verkon reunalle. MPLS-verkko muodostuu MPLS-nodeista, joita on jokaisessa MPLS-verkkoon kuuluvassa reitittimessä. Järjestyksessä ensimmäinen MPLS-node asettaa IP-paketille lyhyen vakiomittaisen arvon, jota kutsutaan nimellä ”label” tai suomeksi ”leima”. MPLS-verkon sisällä kulkeva paketti tunnistetaan tämän leimanumeron avulla eikä reitittimien tarvitse erikseen analysoida paketin otsaketta. MPLS ei itsessään kykene reitittämiseen, joten se tarvitsee toimiakseen jonkin reititysprotokollan tai staattisen reitityksen. Vierellä toimivan reititysprotokollan avulla MPLS-node vaihtaa reititystietojaan muiden MPLS-verkon laitteiden kanssa. (Guichard & Pepelnjak 2009, 11–13.)

MPLS:ää käytetään erityisesti operaattoreiden ja palveluntarjoajien keskuudessa erilaisten palveluiden luomiseksi, mutta MPLS on käytössä myös yritysverkoissa ja datakeskusten sisällä. MPLS:n avulla esimerkiksi palveluntarjoajat voivat luoda edullisia ja helposti skaalautuvia virtuaalisia yksityisverkko- eli VPN-palveluita. Yksi tällaisista VPN-palveluista on nimeltään Virtual Private LAN Service eli VPLS. (Jacob 2017.) VPLS on yksi muoto virtuaalisesta yksityisverkosta, VPN:stä. VPLS:n avulla palveluntarjoaja pystyy yhdistämään oman verkkonsa sisällä asiakkaan verkkoyhteyksiä yksityisesti. VPLS käyttää

MPLS:ää luodakseen loogisia reittejä fyysisten laitteiden sisällä pitääkseen eri asiakkaiden liikennettä erillään. (Lobo & Lakshman 2008, 529.) VPLS on yksi Layer 2 VPN -arkkitehtuurin muodoista. Yleensä Layer 2 VPN -arkkitehtuureissa käytetään kahden laitteen välistä viestintää, mutta VPLS:n avulla kyetään usean laitteen väliseen viestintään. Tämä tarkoittaa sitä, että VPLS:n vaikutuspiirissä olevat laitteet pystyvät lähettämään paketteja samanaikaisesti muille vaikutuspiirin laitteille. (Luo ym. 2008, 569–570.)

4.7 Cisco ASA Failover

Cisco Adaptive Security Appliances eli Cisco ASA -palomuurit ovat Ciscon tuoma lisä palomuurilaitteisiin. Tässä työssä käytetyt palomuurit ovat Cisco ASA -palomuureja. Cisco ASA -palomuureissa redundanttisuus saadaan aikaan Failover-ominaisuudella. Toisin kuin HSRP, Failover ei itsessään liity verkkoliikenteen ohjaamiseen. Failover on kahden ASA-palomuurin välillä toimiva laitteiden tilan tarkastaja. Failover monitoroi siihen konfiguroituja liityntärajapintoja. Jos toisessa palomuurilaitteessa tapahtuu jokin virhe, mikä voisi koskettaa Failoveria, se toimii sille asetettujen määritysten mukaisesti. (Cisco 2018e.)

Failover voidaan tehdä kahdella eri tavalla. Ensimmäinen on HSRP:n kaltainen Active/Standby-laitepari. Kyseisessä laiteparissa Active-laite toimii jatkuvasti reitittävänä laitteena ja Standby-laite odottaa hiljaa mahdollista virhetilannetta. Virhetilanteen sattuessa laitteiden Active/Standby-suhde muuttuu. Tämän jälkeen entinen Standby-laite hoitaa entisen Active-laitteen tehtävät kunnes entinen Active-laite on taas kunnossa. Active/Standby-laiteparin avulla liikenteen jakaminen palomuurilaitteiden välillä ei onnistu. Active/Standby-parin voi luoda sekä ASA:n single context että multiple context -tiloissa. Single context -tilalla tarkoitetaan sitä, että koko palomuurilaite on yksi fyysinen laite. Multiple context taas tarkoittaa sitä, että ASA-palomuurin voi jakaa useaan virtuaaliseen palomuuriin, jotka toimivat saman fyysisen palomuurin sisällä erossa toisistaan. (Cisco 2018e.)

Toinen tapa Failoverin muodostamiseen on Active/Active-laitepari. Tämä tapa vaatii multiple context -tilan käyttämistä. Active/Active-parissa palomuurilaitteisiin luodaan Failover-ryhmät, joihin eri multiple context -tilan mahdollistamat

security contextit määritetään. Failover-ryhmiä voi olla Ciscon mukaan kaksi. Active/Active-pari muodostuu, koska Failover-ryhmille asetetaan Active-laitteiksi eri palomuurit. Näin molemmat palomuurit pystyvät reitittämään. Virheen sattuessa Failover-toimii samalla tavalla kuin Active/Standby-parissa. Hajonneen Active-laitteen Failover-ryhmä siirtyy toimimaan kyseisen ryhmän entisen Standby-laitteen alle, kunnes sen ryhmän alkuperäinen Active-laite on taas kunnossa. Active/Active-pari mahdollistaa liikenteen jakamisen esimerkiksi eri virtuaalilähiverkoille. (Cisco 2018e.)

ASA-palomuurit tukevat kahta eri Failover-muotoa. Kuten palomuureissa, myös Failover voi olla joko stateless tai stateful eli tilaton tai tilallinen. Stateless Failover on passiivinen. Tämä tarkoittaa sitä, että jos palomuurissa tapahtuu virhe ja Failover muuttaa laitteiden suhteita, asiakkaat joutuvat muodostamaan yhteyden haluamaansa palveluun uudelleen. Stateful Failover sen sijaan lähettää jatkuvasti kyselyitä laiteparilleen, jossa se tarkistaa liityntärajapintojen ja laitteen tilan. Virheen sattuessa Stateful Failover kykenee lähettämään entiselle Standby-laitteelle huomattavasti enemmän tietoa. Stateful Failover tukee esimerkiksi reititystaulujen tiedon siirtämistä Active-laitteesta Standby-laitteelle. (Cisco 2018e.)

5 PALOMUURI YRITYSVERKOSSA

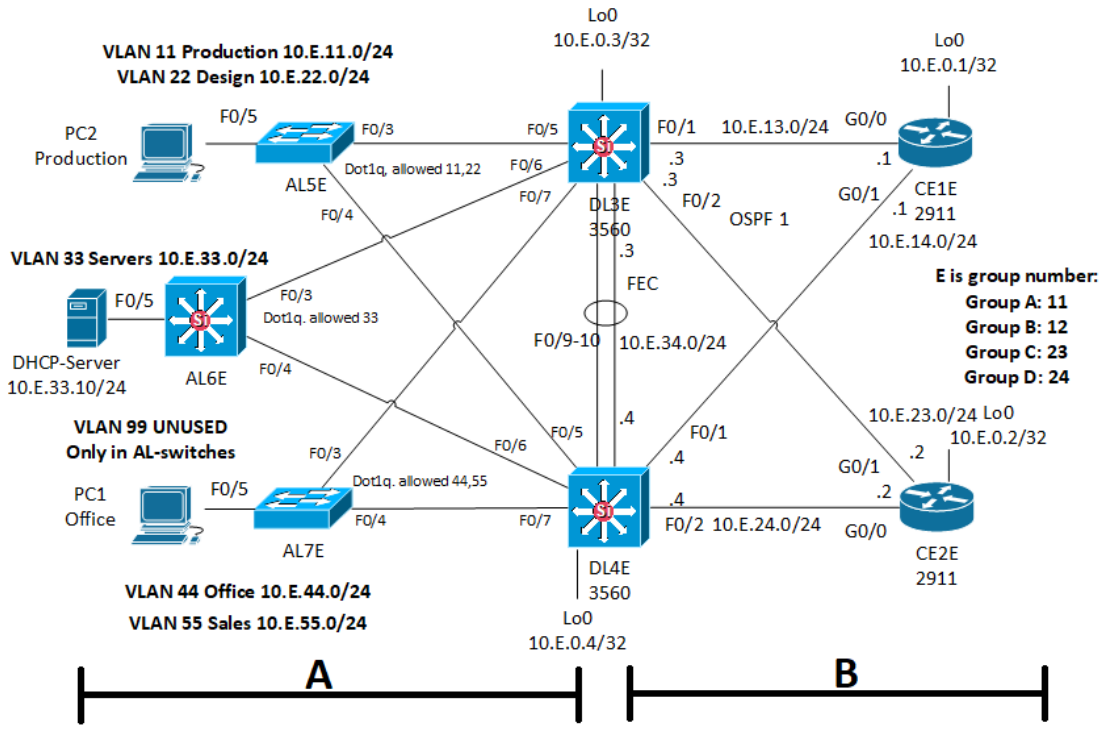
Käytännön osuudessa on pohdittu kahta erilaista tilannetta, kuinka yritysverkkoon voisi toteuttaa palomuuriratkaisun. Toinen näistä tilanteista on rakennettu ja testattu XAMK Kotka ICTLAB:n fyysisessä laboratoriossa oikeilla laitteilla ja toinen tilanteista on käsitelty vain ajatustasolla. Ratkaisut käsitellään siten, että aluksi esitellään kurssin alkuperäisen materiaalin topologia ja mitä tekniikoita siinä käytetään. Seuraavaksi kerrotaan yleisellä tasolla, mitä muutoksia on tehty, jotta palomuurit on saatu lisättyä uuteen topologiaan. Lopuksi avataan ratkaisussa käytetyt protokollat teoriatasolla ja kerrotaan, kuinka kyseisiä protokollia on konfiguroitu ratkaisussa käytettyihin laitteisiin. Molempien ratkaisujen pohjana toimivat BPI-kurssin materiaalit ja niissä on pyritty kunnioittamaan mahdollisimman paljon kurssin alkuperäistä rakennetta.

Ensimmäisessä ratkaisussa palomuurit sijoitettiin työssä aiemmin käsiteltyyn jakelukerrokseen. Tässä ratkaisussa on tarkoitus simuloida sitä tilannetta,

missä yritys itse omistaa fyysiset palomuurilaitteet. Jokaisessa kerroksessa täytyi tehdä joitain muutoksia, mutta suurin työ kohdistui jakelukerrokseen.

5.1 Lähtökohdat

Työn ensimmäisessä palomuuriratkaisussa palomuurilaitteet sijoitettiin yrityksen kampusverkon sisään jakelukerrokseen. Alkuperäisessä topologiassa asiakkaan kampusverkossa on viisi eri osastoille tarkoitettua virtuaalilähiverkkoa eli VLAN:ia tunnuksilla 11, 22, 33, 44 ja 55 sekä yksi tietoturvan parantamiseen tarkoitettu VLAN 99. VLAN 99:n tarkoituksena on se, että kuvan 3 laitteiden AL5E, AL6E ja AL7E käyttämättömät portit asetetaan VLAN 99:ään. Koska VLAN 99 jätetään konfiguroimatta, ei siihen asetettujen porttien kautta voi liikennöidä mihinkään suuntaan. Jokainen pääsykerroksen laite on yhdistetty kahteen DL-laitteeseen, joihin on konfiguroitu jokaiselle VLAN:lle HSRP-protokolla. Ajatuksena on se, että vaikka toinen DL-laitteista hajoaisi, HSRP:n avulla varmistetaan, että yhteys AL-laitteilta CE-laitteisiin säilyisi. Kuvassa 3 on esitetty BPI-kurssin yrityksen kampusverkon alkuperäinen topologia.



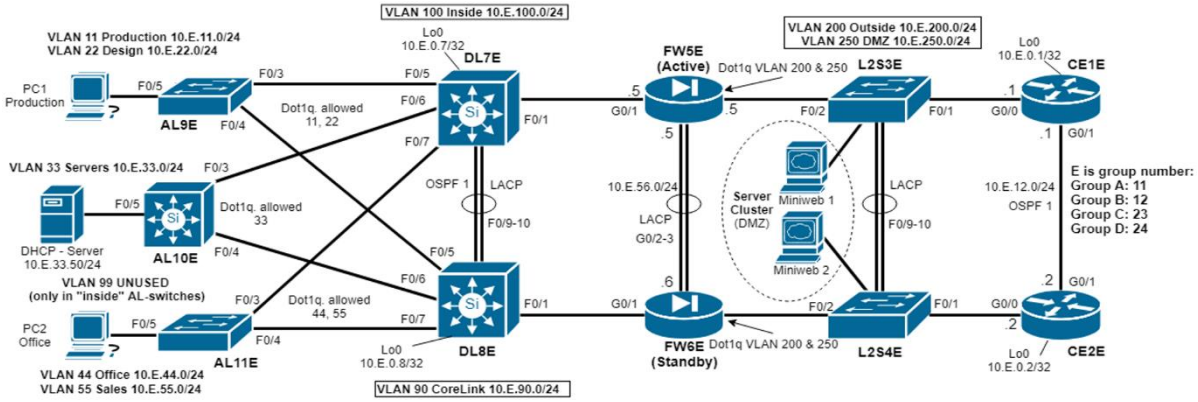
Kuva 3. BPI-kurssin yritysverkon alkuperäinen topologia

Kuten kuvassa 3 nähdään, DL- ja CE-laitteet on kytketty keskenään ristiin. Tällä varmistetaan redundanttisuus, eli vaikka joku laitteista hajoaisi, yhteys

palveluntarjoajan suuntaan säilyisi. DL- ja CE-laitteiden välinen yhteys varmistetaan OSPF-reititysprotokollalla. Ajatuksena on se, että OSPF-alueeseen kuuluvat laitteet mainostavat toisilleen kaikki tarvittavat verkot. Alkuperäisen topologian tapauksessa OSPF:n avulla mainostetaan kaikki VLAN:it, lukuun ottamatta VLAN:a 99, sekä kaikki DL–CE-välin linkkiverkot. Jos verrataan kuvaa 3 aikaisempaan kuvaan 2, voidaan huomata, että kuvan 3 vasemman puolen kuusi laitetta muodostavat pääsykerroksen, kuvan keskellä olevat DL-kytkimet muodostavat jakelukerroksen ja kuvan oikean puolen CE-reitittimet laitteet muodostavat runkokerroksen.

5.2 Tehdyt muutokset

Tässä ensimmäisessä palomuuriratkaisussa käytettiin paljon hyväksi BPI-kurssin yritysverkon alkuperäistä topologiaa sekä konfiguraatioita. Työssä pyrittiin pitämään tallessa niin paljon vanhaa kuin mahdollista ja topologian uusissa osissa on pyritty pitämään kiinni redundanttisuuden säilyttämisestä. Samalla pidettiin silmällä sitä, ettei uusi osuus toisi mukanaan liikaa lisämateriaalia. Kuvassa 4 nähdään uusi yritysverkko kokonaisuudessaan. Suurimmat muutokset kohdistuivat jakelukerrokseen. Verkon arkkitehtuurisesta näkökulmasta liitetyt palomuurit ja L2S-kytkimiin kytketyt Miniweb-palvelimet muodostavat uuden alueen, jota kutsutaan Internet Edgeksi (Cisco 2009).



Kuva 4. Muokatun yritysverkon valmis topologia

Pääsykerros pysyi muutamia VLAN-muutoksia lukuun ottamatta ennallaan. Jakelukerrokseen lisättiin kuvan 4 mukaisesti neljä uutta laitetta. Näistä kaksi ovat kuvaan merkityt FW-palomuurit ja toiset kaksi ovat L2S-kytkimet. Tämän lisäksi jakelukerrokseen täytyi luoda neljä uutta VLAN:ia. Runkokerroksessa

purettiin vanhan topologian kytkennät, konfiguroitiin HSRP ja muutettiin OSPF:n toimintaa alkuperäiseen topologiaan nähden.

HSRP-protokollan käyttö työssä

Tässä palomuuriratkaisussa HSRP on ollut tärkeässä roolissa. Se toimii redundanssiprotokollana luoden oletusyhdyskäytävän osoitteet kuvassa 4 nähtävien FW-palomuurien molemmilla puolilla. Fyysisellä tasolla HSRP-protokolla on konfiguroitu DL- ja CE-laitteisiin. DL-laitteiden sisällä HSRP on konfiguroitu VLAN:hin 11, 22, 33, 44, 55 ja 100. DL8 toimii aktiivisena laitteena VLAN:eille 44 ja 55, kun taas DL7 on aktiivinen laite muille neljälle VLAN:lle. Syyt jaottelun lievästä epätasapainosta löytyvät vanhasta BPI-kurssista, missä VLAN 100:aa ei vielä ollut. Vanhassa BPI-kurssissa verkon topologia mahdollisti liikenteen jakamisen tasaisemmin DL-laitteiden välillä, koska eri virtuaalilähiverkot pystyivät liikennöimään oman HSRP-ryhmän Active-reitittimen kautta. Tässä ratkaisussa DL8-laite ohjaa lopulta kaiken liikenteen DL7-laitteen kautta johtuen Failover-ominaisuudesta. HSRP:n liityntärajapintojen jaottelu on pidetty vanhan BPI-kurssimateriaalin mukaisena opetusta varten.

CE-laitteissa HSRP on konfiguroitu fyysisiin, L2S-kytkimiä kohti suuntaaviin portteihin. Active-reitittimeksi tälle VLAN 200 osoitealueella toimivalle HSRP-ryhmälle on asetettu CE1-laite. Oikeassa tilanteessa FW-palomuurien ja CE-reitittimien väliin ei tarvittaisi L2S-kytkimiä, mutta työssä käytetyt CE-reitittimet eivät pysty hoitamaan HSRP:tä oikein ilman niitä. Kytkimet eivät tee mitään muuta kuin mahdollistavat VLAN 200:n osoitealueen liikenteen FW- ja CE-laitteiden välillä sekä pitävät huolen HSRP:n toiminnasta. Taulukossa 1 nähdään HSRP:n konfigurointia varten vaaditut komennot tämän työn osalta.

Taulukko 1. HSRP:n konfigurointi liityntärajapintaan

Esimerkkikomento	Komennon selitys
standby 1 ip 10.24.100.1	Standby 1 määrittää, mihin HSRP-ryhmään komentoa ollaan asettamassa. Tässä kohdassa asetettava IP-osoite tulee olemaan HSRP-ryhmän 1 virtuaalisen reitittimen IP-osoite
standby 1 priority 150	Tällä komennolla määritetään, mikä laite toimii tietylle liityntärajapinnalle HSRP:n Active-laitteena. Suurimman prioriteetin (välillä 1 - 255) omaava laite valitaan HSRP-ryhmässä tietyn liityntärajapinnan Active-laitteeksi.
standby 1 preempt	Virhetilanteen sattuessa HSRP-ryhmän Active/Standby suhteet muuttuvat. Tällä komennolla laitteille kerrotaan, että alkuperäinen laite palautetaan Active-laitteeksi, kun virhetilanne on korjattu.
standby 1 timers msec 200 msec 750	Tällä komennolla säädetään HSRP:n *hellotime*- ja *holdtime*-ajastukset. Hellotime on hello-viestien lähetyksen välinen aika. Holdtime-ajastuksella kerrotaan, kuinka kauan laite odottaa ennen kuin se kertoo olevansa virhetilassa.

HSRP:n konfiguraatiot ovat kaikissa vaadituissa liityntärajapinnoissa IP-osoitteita ja Active-laitteen prioriteetteja lukuun ottamatta samanlaiset. Taulukossa nähtävä *standby 1 priority 150* asetetaan DL7-laitteessa VLAN 11, 22, 33 ja 100 liityntärajapintoihin, DL8-laitteessa VLAN 44, 55 ja CE1-laitteessa Inside-puolen fyysiseen porttiin. Palomuureista ulospäin lähtevälle liikenteelle näkyy nyt loogisesta näkökulmasta katsottuna CE-laitteisiin konfiguroidun HSRP:n luoma virtuaalisen reitittimen osoite. Tämä korvaa alkuperäisen topologian kytkennät, missä kaikki laitteet jakelu- ja runkokerroksen välissä oli yhdistetty kaapeleilla toisiinsa. Pääsykerroksen VLAN:it tarvitsevat palomuurin puolelta vielä paluuosoitteen. Tämä tapahtuu siten, että palomuurille kerrotaan kaikkien Inside-puolen suunnalla olevien virtuaalilähiverkkojen löytyvän VLAN 100 HSRP:n virtuaaliosoitteen kautta.

Cisco ASA Failover -ominaisuuden käyttö työssä

Tässä palomuuriratkaisussa käytettiin Stateful Active/Standby Failoveria. Aiemmin esitellyssä kuvassa 4 FW5 on laiteparin aktiivinen osapuoli. Ainakin Stateful Failover mahdollistaa sen, että tässä työssä vaaditut konfiguraatiot kopioituvat Active-laitteesta Standby-laitteeseen. Näin ollen FW6:ssa ei tarvinnut tehdä mitään muuta kuin konfiguroida Failover-asetukset. FW5:n Inside-puolen G0/1-porttiin on määritelty VLAN 100:n osoitealueeseen kuuluva IP-

osoite. Virheen sattuessa Failover hoitaa asian niin, että FW6:n Inside-puolen G0/1-portti saa kyseisen IP-osoitteen. Outside-puolella FW5:n fyysiseen G0/0-porttiin luodaan kaksi aliliityntäporttia G0/0.200 ja G0/0.250. G0/0.250 on tarkoitettu VLAN 250:lle, joka on palomuurien näkökulmasta dmz-alue. Molemmille aliliityntäporteille annetaan IP-osoite niiden omista VLAN-osoitealueista. Näin Inside-, Outside- ja dmz-alueiden väliset yhteydet pysyvät muun verkon näkökulmasta muuttumattomina. Dmz-alueen tarkoitus selitetään myöhemmin. Taulukossa 2 nähdään vaadittavat komennot tässä työssä muodostettuun Failover-pariin.

Taulukko 2. Failover-parin muodostaminen

Esimerkkikomento	Komennon selitys
failover lan unit primary	Tällä komennolla määritetään, kumpi laitteista on Active- ja kumpi Standby-laite. Standby-laitteessa *primary* korvataan sanalla *secondary*.
failover lan interface Failover Port-channel1	Asetetaan haluttu liityntärajapinta (port-channel 1) toimimaan Failover-parin paikallisverkon linkkinä. Tämä määritellään molemmissa Failover-parin laitteissa samalla tavalla.
failover link Failover Port-channel1	Määritetään haluttu liityntärajapinta, jonka kautta Stateful Failover -viestit kulkevat. Tämä määritellään vain Active-laitteeseen.
failover interface ip Failover 10.24.56.5 255.255.255.0 standby 10.24.56.6	Määritetään halutut IP-osoitteet Failover-parille. Tämä määritellään molemmissa Failover-parin laitteissa samalla tavalla.

Failover muodostettiin taulukon 2 mukaan LACP-linkkiin. Tässä ratkaisussa LACP:tä on käytetty melkein kaikissa saman tasoisten laitteiden välisissä kytkennöissä. Syynä on se, että linkeistä on tahdottu mahdollisimman redundanttiset. DL-kytkimien väliset ja L2S-kytkimien väliset LACP-linkit toimivat Layer 2 -tasolla. Ne ovat tässä ratkaisussa runkolinkkejä, joihin ei itsessään ole konfiguroitu mitään reititysominaisuuksia. Tässä työssä esimerkiksi DL-laitteiden linkkiin sallitaan VLAN:it 90 ja 100. FW-laitteiden välin LACP-linkki on Layer 3 -tason LACP. Taulukossa 3 nähdään, kuinka tässä ratkaisussa luotiin LACP-linkki DL-laitteiden välille.

Taulukko 3. LACP-linkin muodostaminen DL-laitteisiin

Esimerkkikomento	Komennon selitys
interface Port-channel1	Luodaan liityntärajapinta Port-channel 1.
switchport trunk encapsulation dot1q	Asetetaan kyseinen liityntärajapinta toimimaan dot1q-runkolinkkinä.
switchport mode trunk	Kerrotaan liityntärajapinnan olevan runkolinkki.
switchport trunk allowed vlan 90,100	Sallitaan runkolinkissä tiettyjen virtuaalilähiverkkojen liikenne.
interface range f0/9-10	Siirrytään konfiguroimaan haluttuja fyysisiä portteja.
channel-group 1 mode active	Asetetaan fyysiset portit halutun port-channelin alle. *mode active* asettaa LACP:n kyseiselle linkille.

Taulukossa 3 nähtävät komennot asetetaan molempiin DL-laitteisiin. Koska LACP-linkin molemmissa päissä on sama konfiguraatio, se katsoo linkkivälin olevan toimiva ja avaa yhteyden. L2S-kytkimien välissä LACP-linkin muodostaminen toimii lähes samalla tavalla, mutta kyseiselle linkille täytyy sallia vain VLAN 200.

OSPF-reitityksen käyttö työssä

Tässä palomuuriratkaisussa OSPF on konfiguroitu kuvan 4 mukaisesti kahteen paikkaan. Yksi OSPF-prosessi toimii DL-laitteiden välillä ja toinen prosessi toimii CE-laitteiden välillä. DL-laitteiden välisen OSPF-reitityksen tarkoitus on auttaa uuden reitin löytämisessä mahdollisen virhetilanteen aikana, kun HSRP vaihtaa laitteiden Active/Standby-tilaa. DL-laitteiden välinen OSPF-reititys toimii vain pääsykerroksen suuntaan. Laitteet muodostavat naapuruussuhteen DL-laitteiden välisen LACP-linkin kautta VLAN 90 -liityntärajapintojen välille. Työssä OSPF-mainostukseen otettiin mukaan kaikki muut virtuaaliset lähiverkot, paitsi VLAN 100.

CE-laitteiden välisen OSPF-reitityksen tarkoitus on ohjata yritysverkon ulkopuolelta saapuva liikenne kohti palomuuria ja sen takaa pääsykerroksesta löytyviä palveluita. OSPF-reitityksen avulla CE-laitteet kertovat toistensa kautta ulkopuolelta saapuvalle liikenteelle, kuinka päästä palomuurille eritoten virhetilanteen sattuessa. Jos Outside-alueen HSRP:n Active-reitittimelle kävisi jotain, yritysverkon sisältä pääsisi vielä liikennöimään ulospäin ISP-verkon

suuntaan, koska HSRP pitäisi asioista huolen. Ulkoapäin saapuvalle liikenteelle ei ole olemassa HSRP:tä, joten se ei enää pystyisi yhdistämään palomuurin takaisiin palveluihin. OSPF:n avulla ulkopuolelta saapuva liikenne pystytään kuitenkin ohjaamaan palomuurien suuntaan ja siitä aina palveluihin saakka. Taulukossa 4 nähdään vaadittuja komentoja OSPF:n konfiguroimiseksi tässä palomuuriratkaisussa.

Taulukko 4. OSPF-konfigurointi

Esimerkkikomento	Komennon selitys
router ospf 1	Tällä komennolla siirrytään komentolinjassa halutun OSPF-prosessin alle.
passive-interface default	Asetetaan kaikki liityntärajapinnat passiiviseksi, jotta ne eivät osallistuisi naapuruussuhteiden muodostamiseen.
no passive-interface vlan90	Asettaa halutun liityntärajapinnan osallistumaan naapuruussuhteen muodostamiseen.
ip ospf 1 area 0	Asetetaan halutun liityntärajapinnan sisällä. Määrittää kyseisen liityntärajapinnan toimimaan OSPF 1 -prosessissa halutulla alueella.

CE-laitteiden osalta vanhassa topologiassa kaikki jakelu- ja runkokerroksen linkit oli mainostettu OSPF:llä ja naapuruussuhteet haluttiin luoda runkokerroksen laitteiden kanssa. Nyt CE-laitteisiin on konfiguroitu staattinen reititys palomuurien Outside-puolen porttien Failover-osoitteeseen, johon kaikki yritysverkon ulkopuolelta saapuva liikenne reititetään normaalissa tilanteessa. OSPF pitää huolen vain yritysverkon ulkopuolelta saapuvan liikenteen reitityksestä virhetilanteen sattuessa. Uudessa ratkaisussa DL-laitteiden OSPF toimii DL-laitteiden välillä kaikille pääsykerroksen VLAN:lle sekä jakaa niille oletusreitin.

5.3 Ratkaisun testaaminen

Testausvaiheessa käytössä oli kaksi topologialtaan samanlaista yritysverkkoa ja niiden välissä täysin BPI-kurssin ohjeiden mukaan rakennettu palveluntarjoajan verkko. Ratkaisua testattiin kytkemällä kaksi Miniweb-palvelinta L2S-kytkimiin. Miniweb-palvelimia varten täytyi luoda dmz-alue. DMZ on palomuurin näkökulmasta määritelty aliverkko, johon laitetaan kaikki palvelut, joihin halutaan päästää ulkopuolelta tulevat yhteydet (Cisco s.a). DMZ-aluetta varten täytyi L2S-kytkimiin luoda uusi VLAN ja sallia kyseisen VLAN:n liikenne kytkimien ja palomuurien välillä. Palomuureihin luotiin aliliityntäportit VLAN 250:tä

varten ja konfiguroitiin dot1q-runkoporteiksi. Cisco ASA -palomuureissa aliliityntäportti luodaan seuraavalla esimerkkikomennolla ”interface GigabitEthernet 0/0.250”, jossa lopun 250 on yleensä sen VLAN:n ID, jonka käyttöön aliliityntäportti asetetaan. Aliliityntäportti konfiguroidaan dot1q-runkoportiksi komennolla ”vlan 250”.

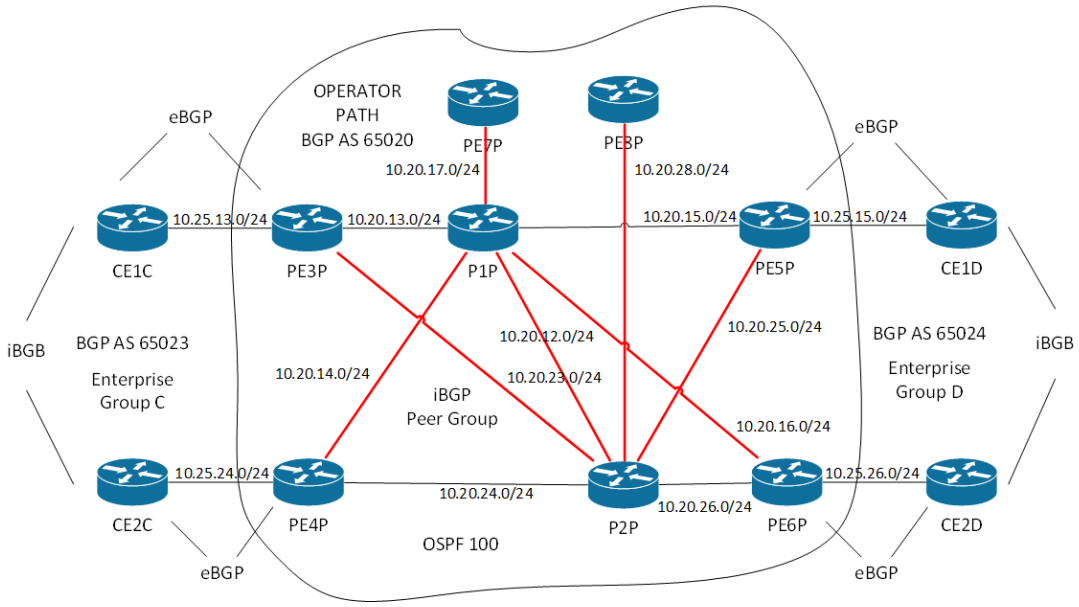
Toisen yritysverkon pääsykerroksessa oli virtuaalinen päätelaite, jonka tarkoitus oli päästä yhdistämään toisen yrityksen Miniweb-palveluun. Jos palomuureja ei yritysverkossa olisi, Miniweb-palvelu olisi vaarassa hyökkäyksille. Jotta Miniweb-palveluun yhdistäminen palomuurin läpi onnistui, palomuurissa tuli sallia yritysverkon ulkopuolelta saapuville yhteyksille vain http-yhteyksien muodostaminen kyseisen Miniweb-palvelimen osoitteeseen.

6 PALOMUURI PALVELUNA

6.1 Lähtökohdat

Voi olla, ettei yrityksellä ole mahdollisuutta lisätä palomuuria omaan verkkoon esimerkiksi kustannusten tai osaamisen puutteen vuoksi. Yritykselle voikin olla helpompaa ja halvempaa ostaa palomuuri palveluna palveluntarjoajalta. Tällaisessa tilanteessa yrityksen ei tarvitse huolehtia palomuurin toiminnasta juuri ollenkaan. Toisessa suunnitellussa palomuuriratkaisussa palomuuri laitettaisiin siis palveluntarjoajan verkkoon.

Tämä ratkaisu käydään läpi vain ajatustasolla eli kerrotaan, kuinka ratkaisu suunniteltiin tehtävän. Fyysisten laitteiden puutteiden takia työtä ei päästy tekemään käytännössä. Aluksi esitellään muutoksen kohteena oleva alkuperäinen topologia sekä siinä käytetyt vielä käsittelemättömät protokollat. Lopuksi käydään läpi suurpiirteittäin, miltä tämä ratkaisu olisi voinut näyttää. Kuvassa 5 nähdään alkuperäinen BPI-kurssin palveluntarjoajan verkon topologia.

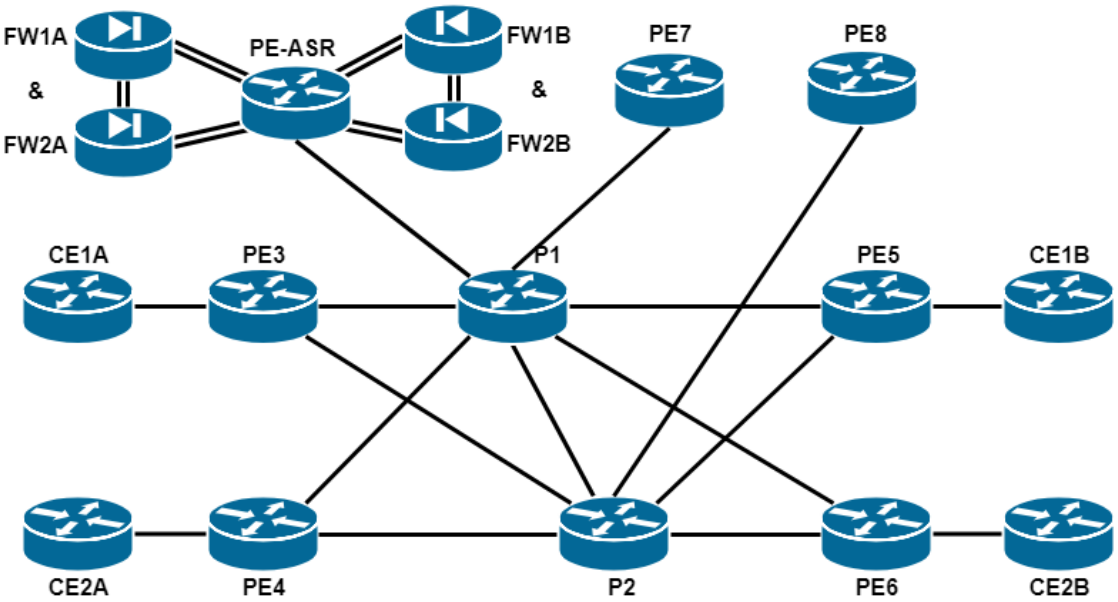


Kuva 5. BPI-kurssin ISP-verkon alkuperäinen topologia

Kuvassa 5 näkyvät CE-laitteet ovat samat yritysverkon reitittimet kuin aikaisemmassa ratkaisussa. Yritysverkon reitittimet kytketään palveluntarjoajan verkkoon BGP-reititysprotokollan avulla ja palveluntarjoajan omassa verkossa on konfiguroitu BGP-reititys. Verkossa on käytössä myös MPLS-menetelmä, jonka avulla palveluntarjoajan verkossa kaikkea liikennettä ei tarvitse jokaisen reitittimen kohdalla reitittää.

6.2 Palomuurin lisääminen palveluntarjoajan verkkoon

Kuten mainittu, tämä ratkaisu pystyttiin käsittelemään vain ajatustasolla. Ratkaisun suunnittelussa käytettiin apuna Uusitalon ja Lehtisen vuonna 2014 tekemää projektia, jossa käsiteltiin samankaltaista tilannetta, missä yritys ostaa palomuurin palveluna. Myös lehtori Vesa Kankareen kokemukset tällaisista ratkaisuista olivat isossa osassa lopullista suunnitelmaa hahmotettaessa. Kuvassa 6 nähdään suunniteltu uusi fyysinen topologia.



Kuva 6. Palomuuri palveluna –ratkaisun fyysinen topologia

Kuvasta 6 voidaan huomata, ettei topologia ole enää symmetrinen, kuten yritysverkon palomuuriratkaisussa. Syy tälle on siinä, että kuvan mukaisia palveluntarjoajan verkkoja tehdään BPI-kurssissa kaksi, ja kuvan PE-ASR-laitteita on käytettävissä vain kaksi. Tämän vuoksi palomuuripalvelun redundanttisuus kärsii. BPI-kurssin molempiin palveluntarjoajien verkkoihin yhdistyy kaksi yritysverkkoa ja palveluntarjoajien verkot yhdistetään toisiinsa PE7- ja PE8-laitteiden kautta. Molemmat palveluntarjoajan verkot saisivat tällöin yhden PE-ASR-laitteen, johon yhdistettäisiin kaksi palomuuriparia. Yksi palomuuripari palvelisi yhden yritysverkon tarpeita. PE-ASR-laite on tavallaan erillään muusta verkosta, sillä siinä aiheutuva mahdollinen virhetila sammuttaisi vain palomuuripalvelun. Palveluntarjoajan lompakon näkökulmasta tämä ei tietenkään olisi hyvä asia, mutta tietoliikenneyhteydet toimisivat vielä normaalisti palveluntarjoajan verkossa.

Ratkaisun looginen topologia jäi kokonaan työstön alle. Suunnitelmana oli kuitenkin käyttää palveluntarjoajan verkon valmista MPLS-verkkoa palomuuripalvelun luomiseen. MPLS:n avulla luotaisiin ASR-reitittimeen VPLS-palvelu, johon kunkin yrityksen palomuuripari kytkettäisiin.

Fyysisestä näkökulmasta palomuurit on asennettu syvälle palveluntarjoajan verkkoon. VPLS-palvelun avulla voidaan luoda yritysverkon suuntaan sellainen vaikutelma, että yritysverkon liikenne kulkee palveluntarjoajan verkkoon siirryttäessä suoraan palomuurin läpi. Loogisesta näkökulmasta palomuuripari

yhdistetään ASR-reitittimessä luotuun VPLS-kytkimeen. MPLS-leimojen avulla yritysverkosta lähtevä ja siihen saapuva liikenne ohjataan ensin VPLS-kytkimiin ja sieltä palomuurien kautta haluttuun kohteeseen.

7 JOHTOPÄÄTÖKSET

Tietoverkkojen ja niihin kytkettävien laitteiden määrä kasvaa jatkuvasti, koska teknologioiden kehittyessä verkot toimivat yhä paremmin entistä suuremmille asiakasmäärille. Sama ilmiö on nähtävissä pienemmässä mittakaavassa myös yritysverkkojen sisällä. Ihmiskunnan siirtyessä jatkuvasti lähemmäs IoT-aikakautta, jossa tietoverkkoihin liitetään sekä langallisesti että langattomasti niin pesukoneet kuin älyesineetkin, tietoturvauhkien määrä kasvaa niiden mukana. Verkostoituneessa yhteiskunnassamme yhä useampi yritys on riippuvainen omasta yritysverkostaan ja kyseisen verkon sisältämiä palveluita ja tietoja tulisi pystyä suojaamaan.

Opinnäytetyön aikana pyrittiin alun perin rakentamaan useampia palomuuriratkaisuja sekä yritysverkon sisälle että palveluksi palveluntarjoajan verkkoon. Tarkoituksena oli vertailla kehitettyjä ratkaisuja ja pohtia, mitkä olisivat kyseisten ratkaisujen heikkoudet ja vahvuudet. Näiden ratkaisujen pohjalta olisi lopulta valittu BPI-kurssia ajatellen paras vaihtoehto, jota olisi lähdetty työstämään tarkemmin kurssin materiaalin muuttamista varten. Kaikissa opinnäytetyöprosessin aikana syntyneissä ideoissa vaalittiin sekä verkon redundanttisuuden että alkuperäisten BPI-kurssin topologioiden säilyttämistä entisellään niin paljon kuin mahdollista.

Suurin osa suunnitelluista ratkaisuista unohdettiin tarpeettoman monimutkaisten konfiguraatioiden takia. Koska lopullisena tavoitteena oli ensimmäisen vuoden opiskelijoille tarkoitetun kurssin materiaalin päivittäminen, kyseisten ratkaisujen pitempi käsittely olisi ollut ajan haaskausta. Toinen lopullisten tulosten määrää rajoittanut tekijä oli lopulta aika. Tämän opinnäytetyön aihe syntyi, koska alamme on painottumassa jatkuvasti kyberturvallisuuden suuntaan. Vuodesta 2019 alkaen koulutuksemme kulkee nimellä kyberturvallisuus. Lopulta tässä työssä jouduttiin suoristamaan mutkia, jotta saatiin aikaan oikeita tuloksia.

Työssä keskityttiin eniten ratkaisuun, jossa palomuuri on yritysverkon sisällä. Kaakkois-Suomen ammattikorkeakoulun ICTLAB:n kannalta työstä saatu tulos on hyödyllinen. Kun ajankäyttö suunnattiin hyväksi havaitun ratkaisun hiomiseen ja testaamiseen, ratkaisun pohjalta syntyi oletettavasti luotettavampaa materiaalia. Palomuuri yritysverkossa -ratkaisun valintaa keskittymisen kohteeksi puolsi se, että alkuperäisessä BPI-kurssissa yritysverkon rakentaminen on ollut myös tärkeämmässä roolissa. Näin kurssimateriaalin kehittäminen kohdistui vanhan kurssin näkökulmasta oikeaan paikkaan. Mahdollisesti negatiivista asiassa on, että Palomuuri palveluna -ratkaisu jäi vain ajatustasolle. Näin ei päästy vertailemaan sitä, kumpi ratkaisuista olisi yksinkertaisempi toteuttaa. Vaikka molemmissa ratkaisuissa fyysisen topologian muutokset ovat vähäiset, varsinkin yritysverkon looginen topologia koki suuria muutoksia. Tämä näkyi uuden kurssimateriaalin ohjeistusta tehdessä. Lopullisessa ohjeistuksessa Miniweb-palvelimet jätettiin kokonaan pois. Syinä tälle olivat fyysisen laboratoriomme laitteiden tukemien ominaisuuksien vähäisyys sekä ohjeistuksen monimutkaisuuden lisääntyminen. Lopullisessa kurssimateriaalissa verkon ulkopuolelta saapuvia yhteyksiä testataan palomuurin Outside-puolen porttien avulla.

Yhtenä jatkokehitysmahdollisuutena on Palomuuri palveluna -ratkaisun toteuttaminen fyysisillä laitteilla sekä koko ratkaisun pohtiminen eri näkökulmista. Tämän opinnäytetyön aikana ratkaisun toteutus ICTLAB:n fyysisillä laitteilla on kuitenkin ongelmallinen, koska fyysisissä laitteissa on puutteita. Ensimmäinen ongelma on se, ettei olemassa olevia laitteita ole tarpeeksi redundanttisuuden säilyttämiseksi, olettaen että huomioon otetaan kaikki BPI-kurssin vaatimukset. Toinen ongelma on, että kuvan 6 topologian P1- ja P2-laitteissa ei ole tarpeeksi fyysisiä portteja eikä työhön käytettäväksi tarkoitetussa Cisco ASR920 -reitittimissä ole serial-portteja. Tällä hetkellä P1- ja P2-laitteet ovat Cisco 2801 -reitittimiä, joissa on käytössä kaksi Cisco WIC-2T 2-port Serial –moduulia. Jos nämä korvattaisiin Cisco HWIC-4ESW 4-port EtherSwitch 10BASE-T/100BASE-TX -moduuleilla, käytettävien porttien määrä nousisi neljästä kahdeksaan ja samalla kyseisissä laitteissa päästäisiin eroon vanhoista sarjaporteista. Moduulien vaihdos Cisco 2801 -laitteissa johtaisi siihen, että fyysisen laboratorion muihinkin reitittimiin tulisi hankkia sopivat moduulit.

Toisena jatkokehitysmahdollisuutena on ASA-palomuurien välisen Failover-parin nostaminen Active/Active-tilaan. Tämä mahdollistaisi verkkoliikenteen jakamisen palomuurien välillä. Tässäkin työssä mietittiin Active/Active-parin luomista, mutta lopulta sen katsottiin aiheuttavan liikaa ongelmia ja ylimääräistä työtä BPI-kurssia ajatellen. Alan keskustelupalstoilla oli myös useasti puhuttu siitä, ettei Failover Active/Active-pari ole yleisessä käytössä, sillä se aiheuttaa liikaa vaivaa suhteutettuna sen tuomiin hyötyihin.

LÄHTEET

Avolio, F. 1999. Firewalls and Internet Security. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-1/ipj-archive/article09186a00800c85ae.html [viitattu 15.10.2018].

Brazil, J. 2017. The life of the firewall – A history. WWW-dokumentti. Saatavissa: https://www.itproportal.com/features/the-life-of-the-firewall-a-history/ [viitattu 13.10.2018].

Checkpoint. s.a. Our History. WWW-dokumentti. Saatavissa: https://www.checkpoint.com/about-us/our-history/# [viitattu 19.10.2018].

Cisco. 2018a. What is a Firewall?. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html [viitattu 26.10.2018].

Cisco. 2018b. Cisco Connected Grid Ethernet Switch Module Interface Card Software Configuration Guide. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/switch_module_swcg/cgr-esm-configuration/config_vlans.html [viitattu 20.11.2018].

Cisco. 2018c. Cisco Nexus 5000 Series NX-OS Software Configuration Guide. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/AccessTrunk.html [viitattu 19.12.2018].

Cisco. 2018d. Cisco CPT Configuration Guide–CTC and Documentation Release 9.5.x and Cisco IOS Release 15.2(01). WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_5/configuration/guide/cpt95_configuration/cpt93_configuration_chapter_01011.html#concept_12EEFDC4EA904understandinglacp [viitattu 11.12.2018]

Cisco. 2018e. CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.9. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/general/asa-99-general-config.html [viitattu 11.12.2018].

Cisco. 2017a. Catalyst 3560 Software Configuration Guide, Release 12.2(52)SE. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swhsrp.html [viitattu 11.12.2018].

Cisco. 2017b. Border Gateway Protocol. WWW-dokumentti. Saatavissa: http://docwiki.cisco.com/wiki/Border_Gateway_Protocol [viitattu 12.12.2018].

Cisco. 2013. Cisco SAFE Reference Guide. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html [viitattu 17.11.2018].

Cisco. 2012. Open Shortest Path First. WWW-dokumentti. Saatavissa: http://docwiki.cisco.com/wiki/Open_Shortest_Path_First [viitattu 11.12.2018].

Cisco. 2009. Enterprise Internet Edge Design Guide. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/IE_DG.html [viitattu 17.12.2018].

Cisco. s.a. Configuring DMZ. WWW-dokumentti. Saatavissa: https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/ad1681599.html [viitattu 16.12.2018].

Devich, A. 2015. A Brief History of the Firewall. WWW-dokumentti. Saatavissa: https://www.illumio.com/blog/history-of-the-firewall#gsc.tab=0 [viitattu 13.10.2018].

Froom, R. & Frahim, E. 2015. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide. Indianapolis: Cisco Press.

Guichard, J. & Pepelnjak, I. 2009. MPLS and VPN Architectures. 12. painos. Indianapolis: Cisco Press.

Jacob, D. 2017. A Guide to MPLS VPN Fundamentals. WWW-dokumentti. Saatavissa: https://www.packetdesign.com/blog/a-guide-to-mpls-vpn-fundamentals/?cn-reloaded=1 [viitattu 12.12.2018].

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona: Opas opinnäytetyön ja pro gradun kirjoittajalle. Jyväskylä: JAMK University of Applied Sciences.

Kananen, J. 2015a. Kehittämistutkimuksen kirjoittamisen käytännön opas: Miten kirjoitan kehittämistutkimuksen vaihe vaiheelta. Jyväskylä: JAMK University of Applied Sciences.

Kananen, J. 2015b. Online Research for Preparing Your Thesis. Jyväskylä: JAMK University of Applied Sciences.

Kettunen, M. 2014. The big picture of the internet. Teoksessa Kiri, O., Huovi, T. & Malvela, P. (toim.) Learning Garden, Pedagogisia kukintoja LCCE –mallin reunamilla. Kymenlaakso University of Applied Sciences, 90-96.

Lobo, L. & Lakshman, U. 2006. MPLS Configuration on Cisco IOS Software. 2. painos. Indianapolis: Cisco Press.

Luo, W., Pignataro, C., Bokotey, D. & Chan, A. 2008. Layer 2 VPN Architectures. Indianapolis: Cisco Press.

Metaswitch. s.a. What is Open Shortest Path First (OSPF)?. WWW-dokumentti. Saatavissa: https://www.metaswitch.com/knowledge-center/reference/what-is-open-shortest-path-first-ospf [viitattu 11.12.2018].

Miller, L. 2016. Next-Generation Firewalls for Dummies. E-kirja. New Jersey: John Wiley & Sons Inc. Saatavissa: https://www.paloaltonetworks.com/resources/whitepapers/next-gen-firewall-for-dummies [viitattu 12.12.2018].

Palo Alto. 2016. Basic APP-ID. EDU-201-sertifikaatin koulutusmateriaali.

Techopedia. s.a. Stateful Inspection. WWW-dokumentti. Saatavissa: https://www.techopedia.com/definition/4129/stateful-inspection [viitattu 19.12.2018].

Teare, D., Vachon, B. & Graziani, R. 2015. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide. Indianapolis: Cisco Press.

Wilkins, S. 2013. Stateful Firewall Fundamentals: A Better, Easier, More Secure Firewall. WWW-dokumentti. Saatavissa: https://www.pluralsight.com/blog/it-ops/stateful-firewall-fundamentals [viitattu 19.12.2018].

Zhang, R. & Bartell, M. 2004. BGP Design and Implementation. 4. painos. Indianapolis: Cisco Press

Zwicky, E., Cooper, S. & Chapman, B. 2000. Building Internet Firewalls. 2. painos. California: O'Reilly.