Väinö Hyppänen

Palomuuripalvelu

Opinnäytetyö
Tieto- ja viestintätekniikan koulutus

2021

Kaakkois-Suomen
ammattikorkeakoulu

Tekijä/Tekijät	Tutkinto	Aika
Väinö Hyppänen	Insinööri (AMK)	Toukokuu 2021
Opinnäytetyön nimi Palomuuripalvelu		29 sivua 0 liitesivua
Toimeksiantaja Kaakkois-Suomen ammattikorkeakoulu Oy		
Ohjaaja Martti Kettunen		

Tiivistelmä

Opinnäytetyön tavoitteena oli tutkia, kuinka palomuuripalvelu voidaan luoda ja lisätä osaksi palveluntarjoajan verkkoa. Palomuuripalvelun toteuttamisen takia tarpeellista oli myös selvittää, kuinka verkkoliikenne asiakasverkosta saataisiin ohjattua verkkoon lisättävälle palomuurille. Työn tarkoituksena oli integroida luotu palomuuripalvelu tieto- ja viestintätekniikan Big Picture of Internet-kurssin materiaaliin. Ratkaisun tarvitsee olla ensimmäisen ja kolmannen vuoden opiskelijoiden tehtävissä, mistä johtuen reitityksen monimutkaisuutta tarvitsi yksinkertaistaa. Toteutuksessa on hyödynnetty Kaakkois-Suomen ammattikorkeakoulun virtuaalilaboratoriojärjestelmää.

Opinnäytetyön alkuvaiheessa perehdyttiin palomuuripalveluun. Tässä vaiheessa ilmeni merkittäviä palomuuripalveluita olevan kahta eri tyyppiä, joista toinen hyödyntää fyysisiä palomuurilaitteita ja toinen virtualisoitua ympäristöä. Työn tarkoituksena oli hyödyntää oikeita palomuurilaitteita, joten virtualisointiin perustuva palvelu jätettiin teoreettiselle tasolle.

Työn toteutus siirtyi virtuaalilaboratorioon käytettävissä olevien fyysisten laitteiden rajoitteista johtuen. Big Picture of Internet-kurssin palveluntarjoajaverkon reunalle lisättiin tarvittavat reitittimet ja palomuurilaitteisto. Verkkoliikenteen reititys palomuurille saatiin teoreettisella tasolla suunniteltua, mutta sen toimivuutta ei saatu varmistettua.

Työn tavoitteita ei saavutettu kokonaisuudessaan. Erilaisten palomuuripalveluiden eroja saatiin selvennettyä ja palveluntarjoajan verkon topologiaan saatiin lisättyä palomuuripalvelun tarvitsemat laitteet. Työstä jäi puuttumaan toimiva konfiguraatio, mistä johtuen työn tuloksia ei voida suoraan hyödyntää BPI-kurssin sisällön laajentamisessa.

Asiasanat

Palomuuripalvelu, palveluntarjoajaverkko, tietoturva, reititys

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Väinö Hyppänen	Bachelor of Engineering	May 2021

Thesis title

Managed Firewall Service

29 pages
0 pages of appendices

Commissioned by

South-Eastern Finland University of applied sciences

Supervisor

Martti Kettunen

Abstract

The main purpose of this thesis was to investigate a way to create and integrate a managed firewall service to a pre-existing service provider network. Due to the nature of a managed firewall service, it was also necessary to research a way to route the network traffic of a customer through a service provider network to a firewall. The resulting firewall service was to be integrated with Big Picture of Internet course material to be studied by first- and third-year students. This made it necessary to keep the solution simple and easy to teach and implement.

The beginning phase of the thesis was used to get familiarized with firewall services. During this phase it became clear that there were two main types of firewall services, one of which uses physical firewall devices and another that relies on virtualizing the firewall. As the purpose of this thesis was to use physical devices, the service based on virtualization was left to a theoretical level.

The implementation of the work was moved to the virtual laboratory system of South-Eastern Finland University of applied sciences due to the limitations of the available physical devices. Necessary devices to create a managed firewall service were added to the topology of the service provider network in BPI course material. Routing of the network traffic was completed on theoretical level, but full functionality could not be confirmed.

The objectives of this thesis were accomplished only partially. The differences between a firewall as a service and a managed firewall service were clarified and the devices required by managed firewall service were added to the service provider network. A functional configuration for the routing of customer network traffic through service provider network was not finished, therefore the results of this thesis cannot be directly used in the BPI course material.

Keywords

Managed firewall service, service provider network, information security, routing

SISÄLLYS

TERMIT JA LYHENTEET

BPI	Big Picture of Internet
VPN	Virtual Private Network
QoS	Quality of Services
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
UTM	Unified Threat Management
WAF	Web Application Firewall
ICMP	Internet Control Message Protocol
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
MPLS	Multiprotocol Label Switching
VPLS	Virtual Private LAN Service
LAN	Local Area Network
FWaaS	Firewall as a Service
IP	Internet Protocol
HTTP	Hypertext Transfer Protocol
SDN	Software-defined Networking
NGFW	Next-Generation Firewall
ACL	Access Control List
TCP	Transmission Control Protocol
DPI	Deep Packet Inspection
SSL	Security Sockets Layer
FEC	Forwarding Equivalence Class
LSP	Label Switched Path
CoS	Class of Service
TC	Traffic Control
EXP	Experimental
TTL	Time To Live

1 JOHDANTO

Tieto- ja viestintätekniikan koulutuslinja Kaakkois-Suomen ammattikorkeakoulussa on painottunut vuosi vuodelta yhä enemmän kyberturvallisuuteen. Koulutuksen nimeä on vaihdettu kuvaamaan tätä muutosta, joten vuonna 2019 uudet opiskelijat aloittavat koulutuslinjalla ”Insinööri (AMK), Kyberturvallisuus”. Kyberturvallisuusuhkien lisääntyessä on tärkeää kouluttaa alalle henkilöitä, jotka kykenevät lieventämään näiden uhkien tuomia riskejä, sekä luomaan uhkien torjumiseen kykeneviä tietoverkkojärjestelmiä. Palomuurit toimivat yhtenä osa-alueena näitä uhkia vastaan.

Perinteisesti palomuurit ovat olleet fyysisiä laitteita yritysten konesaleissa toteutettuna joko sovelluspohjaisena palvelimena tai tarkoitukseen rakennettuna fyysisenä laitteena. Yritysmaailman muuttuessa yhä enemmän riippuvaiseksi internetistä tarvitsevat yritykset myös vaativampia palomuuriratkaisuja, joten palomuurin ostaminen palveluntarjoajalta palveluna on yhä houkuttelevampi vaihtoehto. Markkinoilla on tarjolla ainakin kahta erilaista palvelutyyppiä, joista toinen on palveluntarjoajan tarjoama palomuuripalvelu (Managed Firewall Service), missä palvelu tuotetaan kierrättämällä yrityksen tietoliikenne palveluntarjoajan konesalissa sijaitsevien fyysisten palomuurilaitteiden kautta. Sopimuksesta riippuen, myös palomuurin ylläpito, päivitykset ja konfigurointi ovat kokonaan tai osittain palveluntarjoajan vastuulla. Toinen on FWaaS (Firewall as a Service), palomuuripalvelu, jossa palomuurin tehtävät hoidetaan pilvipalvelussa. FWaaS on palvelutyypiltään huomattavasti erilainen verrattuna aiempaan palveluna tarjottuun palomuuriin. FWaaS toimii pilvessä ja ei ole rajoittunut palomuurilaitteiden määrän mukaisesti, sillä se saa suorituskykynsä pilvilaskennan avulla.

Opinnäytetyö toteutetaan työn toimeksiantajan, Kaakkois-Suomen ammattikorkeakoulun, laitteilla Kotkan kampuksen ICTLABin tiloissa. Tästä johtuen käytettävissä olevat laitteet rajoittuvat Ciscon laitteistoihin. Työn aikana tullaan myös hyödyntämään koulun CyberLab-oppimisympäristössä olevaa Virtual-Lab-virtuaalilaboratoriojärjestelmää, jonka avulla koulun opiskelijat kykenevät harjoittelemaan tietoverkkojen luomista myös virallisen opetusajan ulkopuolella käyttäen omia päätelaitteitaan.

Ensimmäisen vuoden opiskelijoita on useamman vuoden ajan tutustutettu koulutuksen sisältöön tiimityöskentelyä vaativalla kilpailuhenkisellä projektikurssilla Big Picture of Internet, jatkossa BPI. Kyseisellä kurssilla opiskelijat jaetaan tiimeihin, jotka koostuvat ensimmäisen ja kolmannen vuoden opiskelijoista. Kolmannen vuoden opiskelijoiden tehtävänä on opastaa sekä auttaa ensimmäisen vuoden opiskelijoita kurssin aikana ja ensimmäisen vuoden opiskelijoiden tehtävänä on luoda toimiva yritysverkko sekä palveluntarjoajaverkko. (Kettunen 2014.)

Palomuuria käsitteleviä opinnäytetöitä löytyy Theseuksesta paljon, mutta palveluna tuotettua palomuuria käsitteleviä opinnäytetöitä on erittäin vähän. Palomuureihin pohjautuvien opinnäytetöiden joukosta tarkasteluun valikoitui Henri Pasosen (2018) opinnäytetyö *Palomuurin implementointi yritysverkkoon Cisco-ympäristössä*. Opinnäytetyö käsittelee palomuurikerroksen lisäämistä yritysverkon topologiaan säilyttäen olemassa olevan verkon toiminnallisuuden ja redundanttisuuden. Tuomas Paavolan (2016) opinnäytetyö *Sophos-palomuuri palveluna* käsittelee laajemmin palomuuripalvelua ja on sisällöltään lähimpänä tämän opinnäytetyön aihetta. Marko Vatasen (2009) opinnäytetyö *Operaattoritasoisen reitityksen ja VPLS:n toteutus SpiderNetiin* käsittelee syvällisemmin teknologioita, joita myös tässä opinnäytetyössä tullaan tarvitsemaan ja tästä syystä se valikoitui tarkastelun alaiseksi.

1.1 Opinnäytetyön tavoitteet

Koulutuslinjan painotuksen muuttuessa yhä enemmän kyberturvallisuuden suuntaan täytyy olemassa olevia kursseja myös täydentää. Tästä johtuen BPI-kurssin sisältöön on lisätty palomuurit. Tämän opinnäytetyön tavoitteena on luoda toimiva palomuuripalvelu, jonka kautta asiakasverkon verkkoliikenne kierrätetään ennen internetiin pääsyä ja jonka kautta myös internetistä tuleva liikenne kulkee ennen asiakasverkkoon pääsyä. Työssä tullaan hyödyntämään BPI-kurssikokonaisuuden palveluntarjoajapuolen verkkotopologiaa, johon palomuuripalvelu rakennetaan ja jota tarjotaan BPI-kokonaisuuden yritysverkoille. Tulevat muutokset vaativat fyysisten laitteiden lisäämistä topologiaan sekä näiden konfiguroinnin. Lisäksi olemassa oleviin laitteisiin täytyy lisätä tarvittavia toimintoja, jotta palvelu saadaan toimimaan. Työtä varten täytyy miet-

tiä mitä tekniikoita ja protokollia työn toteuttamiseen tarvitaan, jotta yritysverkon liikenne saadaan kulkemaan palveluntarjoajaverkon puolella olevan palomuurin kautta ja mikä olisi optimaalisin tapa konfiguroida kyseinen kokonaisuus. Työn tekoa rajoittaa toimeksiantajan laitevalikoima, joka koostuu kokonaan Ciscon valmistamista laitteista ja täten sekä työ että sen lopputulos myös rajoittuvat Cisco-laitteista koostuvaan ympäristöön. Opinnäytetyön tutkimusongelmana on, kuinka palomuuripalvelu toteutetaan palveluntarjoajan verkossa.

1.2 Tutkimusmenetelmän valinta

Tutkimuksen alkuvaiheisiin kuuluu työssä käytettävän tutkimusotteen valinta. Tämän tutkimusotteen mukaisesti ryhdytään ratkaisemaan tutkimuskysymyksiä sekä -ongelmaa. Yleistä kuitenkin on, että tutkimuksen aihealue ja laatu määrittelevät sopivimman tutkimusmenetelmän. (Kananen 2014, 51.) Kehittämistutkimus valikoitui opinnäytetyön tutkimusmenetelmäksi, sillä työn tarkoituksena on perehtyä, kuinka palveluntarjoaja voi luoda palomuurin yritysasiakkaalle palveluna ja kuinka tämä luotu palvelu saadaan lisättyä jo olemassa olevaan BPI-kokonaisuuteen.

Kehittämistutkimus on suomalaisten luoma versio toimintatutkimuksesta ja usein näiden välillä ei tehdä eroa, sillä molemmat pyrkivät muutokseen. Toimintatutkimuksen piirteisiin kuuluu havainnoiva tiedonkeruu. Havainnointi tiedonkeruumenetelmänä on osa kvalitatiivista tutkimusta ja toimintatukimusta lähinnä on osallistuva havainnointi. Toimintatutkimuksessa kuitenkin pyritään muuttamaan jotain, joten mikäli tutkimus ei sisällä myös muutoksen tekoa, ei tutkimusmenetelmä saavuta toiminta- tai kehittämistutkimuksen määritelmää. (Kananen 2014, 58.)

Kehittämistutkimus yhdistelee kvalitatiivista ja kvantitatiivista tutkimusta ja täten se on yhdistelmä erilaisia tutkimus- ja kehittämismenetelmiä, ei oma menetelmänsä. Vaikka kehittämistutkimuksessa muutetaan jotakin, esimerkiksi menetelmiä tai organisaatioita, ei kaikki muutostyö ole kehittämistutkimusta. Kehittämistutkimus vaatii myös tutkimusosion muutostyön lisäksi. (Kananen 2017, 18.)

Kehittämistutkimus ja kehittämistyö ovat lähellä toisiaan. Kehittämistyötä tapahtuu jatkuvasti organisaatioissa ja kehittämistyöstä tulee tieteellisempää ja täten muuttuu kehittämistutkimukseksi, kun työtä tehdessä työ dokumentoidaan ja käytetään tieteellisiä menetelmiä tuottamaan uutta luotettavaa tietoa. (Kananen 2012, 20–21.)

2 PALOMUURI

Tämän opinnäytetyön aihealueesta johtuen palomuuri on työn keskeisimpiä osa-alueita verkkotekniikoiden lisäksi. Tämä luku sisältää tietoa ja teoriaa palomuureista, niiden historiasta sekä toimintatavoista ja eri palomuurityypeistä.

Palomuuria voi kuvailla monin eri tavoin, sitä voi esimerkiksi verrata rajavartijaan. Palomuuri suodattaa verkkoliikennettä esimääriteltyjen turvallisuuskäytäntöjen mukaisesti ja suojaa verkkoa ulkopuolisilta hyökkäyksiltä. Oletussääntöjen mukaisesti palomuurit estävät kaiken verkkoliikenteen, joten niihin täytyy erikseen luoda sääntöjä, joilla haluttu liikenne sallitaan ja joilla ei-haluttu liikenne estetään. Verkkoliikenteen suodatus toimii vertailemalla saapuneiden IP-pakettien sisältöä määriteltyihin sääntöihin. IP-paketti saa jatkaa matkaansa vain, mikäli sen sisältö on säännön mukaisesti sallittua. Jos paketin sisältö täsmää kieltolistojen sisältöön, ei kyseistä pakettia päästetä liikkumaan määränpäähänsä. Mikäli palomuurille saapuu paketti, joka ei täsmää minkään säännön kanssa, sitä ei päästetä eteenpäin. (Stewart 2014, 44–45.)

Barracuda Networks (s.a.) kertoo, että palomuurit sijaitsevat verkon reunalla toimien yhteyskäytävänä sisä- ja ulkoverkkojen välillä. Kun palomuuri on asianmukaisesti konfiguroitu, kykenee se pitämään virukset, hakkerit ja ei-toivotut käyttäjät ulkopuolella ja samanaikaisesti päästämään sallitut käyttäjät käyttämään tarvitsemiansa resursseja. Verkon käytön rajoittamisen lisäksi palomuurit kykenevät pitämään lokia kaikesta verkkoon tulevasta ja sieltä lähtevästä liikenteestä sekä hallinnoimaan etäyhteyksiä todennussertifikaattien ja turvallisten kirjautumisien kautta. Puhtaasti palomuurikäyttöön tehdyt laitteistopohjaiset palomuurit ovat yleensä tarkoitettu yrityskäyttöön, mutta usein myös palomuureja löytyy sisäänrakennettuina muista verkkolaitteista, kuten reitittimistä. Ohjelmistopohjaiset palomuurit ovat joko tietokoneille asennettuja ohjel-

mistoja tai käyttöjärjestelmien tai verkkolaitteiden valmistajien toimittamia ohjelmistoja. Ohjelmistopohjaiset palomuurit kykenevät suojaamaan järjestelmiä yksinkertaisilta tunkeutumishyökkäyksiltä mutta ovat suuremmissa hankaluuksissa hienostuneempien tunkeutumisyritysten kanssa. (Barracuda s.a.)

2.1 Palomuurien Historiaa

Maailmanlaajuinen viestintä avasi ovet tunkeutumisille verkkoon kytkettyihin kotikäyttäjien tietokoneisiin sekä yritysten tietokoneisiin. Kasvavat huolet tietoturvasta ajoivat tietoverkkojen tietoturvan kehitystä ja johtivat ensimmäisiin palomuureihin. (Thompson-Melanson 2015.)

Tietotekniikka on olemassaolonsa ajan kehittynyt tietoturvaa nopeammin ja 1990-luvun puolella tietoturvauhkia alkoi ilmaantua, jolloin Check Point Technologies julkaisi pakettisuodatinpalomuurin (Stateful Firewall). Samaan aikaan markkinoilla oli myös reitittimiin sisällytettyjä pakettisuodattimia sekä välityspalvelimia. Vaikka välityspalvelimet tarjosivat hyvän tietoturvan, olivat niiden yrityksille aiheuttamat vaikutukset liian negatiivisia verrattuna kilpaileviin toteutuksiin. (Brazil 2017.)

Pakettisuodatinpalomuurit olivat suhteellisen yksinkertaisia laitteita, mutta ne loivat pohjan nykypäivän erittäin monitahoisille tietoturvateknologioille. 1990-luvun loppupuolella markkinoille ilmaantui useita rinnakkaisprojekteja kuten Snort (IPS, Intrusion Prevention System), joiden päätarkoituksena oli kehittää tietoturvatekniikoita. Samaan aikaan toimintoja kuten VPN ja QoS lisättiin jo olemassa oleviin tietoturvaratkaisuihin luoden pohjaa tulevaisuuden palomuurilaitteille. (Brodbeck 2015b.)

Pakettisuodatinpalomuurien suosiota 1990-luvulla selittää niiden helppo hallinnointi aikana, jolloin verkkotekniikka kehittyi nopeasti. Tällöin kehittyi myös nykyään asiakkaille kolme tärkeää palomuurien osa-aluetta, jotka ovat turvallisuus, suorituskyky ja käytettävyys. Check Pointin graafinen käyttöliittymä helpotti palomuurisääntöjen tekoa ja sen vallankumouksellisin ominaisuus oli mahdollisuus useampaan lähdeosoitteeseen, useampaan kohdeosoitteeseen ja useampaan palveluun kullakin suodatussääntörivillä. Graafinen käyttöliittymä antoi myös kyvyn editoida olemassa olevia sääntöjä (Brazil 2017.)

Internetin suosion kasvaessa useat ohjelmat ja palvelut alkoivat keskittää toimintaansa verkkoon. Tämä nostatti tarvetta HTTP-protokollaan pohjautuvien järjestelmien suojaamiselle ja tätä varten markkinoille ilmestyi ratkaisuksi Web Application Firewall (WAF), joka myös sisällytettiin UTM:ien ominaisuuksiin. UTM (Unified Threat Management) tiivisti useita eri toimintoja ja tietoturvaominaisuuksia yhteen pakettiin, mutta tämä tuotti suorituskykyongelmia. Vuonna 2008 Palo Alto Networks esitteli markkinoille konseptin seuraavan sukupolven palomuureista (NGFW, Next Generation Firewall), joka ratkaisi UTM:ien suorituskykyongelmat sekä lisäsi näkyvyys- ja sovelluspohjaiset hallintakeinot. Vuotta myöhemmin Gartner teki määritelmän seuraavan sukupolven palomuureista. (Brodbeck 2015b.)

Yritysten välinen kilpailu loi palomuurista korvaamattoman osan tietoturva-alaa. Pilvi- ja SDN ympäristöjen yleistyessä palomuurin rooli tulee laajenemaan ja palomuuri tulee pysymään kriittisenä osana tietoverkkoja tulevaisuudessakin. (Brazil 2017.)

2.2 Palomuurityypit

2.2.1 Tilalliset ja tilattomat palomuurit

Tilattomat (stateless) ja tilalliset (stateful) pakettisuodatinpalomuurit loivat pohjan nykypäivänä käytettäville kehittyneemmille palomuureille. Tilallisia palomuureja käytetään yhä yleensä niin, ettei ne ole näkyvissä tai hallittavissa järjestelmänvalvojille tai turvallisuusanalyytikoille. Yksinkertaistettuna pakettisuodatus tapahtuu tarkastelemalla IP-pakettien otsakkeita, vertailemalla sen sisältöä luotuihin sääntöihin joiden perusteella paketti joko päästetään eteenpäin tai hylätään. (Brodbeck 2017.)

Tilattomia pakettisuodattimia kutsutaan myös pääsylistoiksi (ACL, Access Control List). Tilaton palomuuri määrittelee yhdestä tai useammasta säännöstä koostuvan sarjan, jota kutsutaan suodatusehdoksi. Suodatusehto määrittää, mitä paketille tehdään, kun ehdot täsmäävät paketin sisällön kanssa. Tilaton pakettisuodatin tyypillisesti asetetaan verkkolaitteen liitäntään mihin on konfiguroitu jonkin protokollan ominaisuuksia. Tilattoman palomuurin voi aset-

taa verkkolaitteen sisään tulevaan liittimeen, ulostulevaan liittimeen tai molempiin. Pääsylistojen perustarkoituksena on parantaa turvallisuutta suodattamalla verkossa kulkevia IP-paketteja. Tilattoman palomuurin tyypillinen käyttötarkoitus on suojata laitteen resursseja ja prosesseja tuntemattomilta tai haitallisilta paketeilta. (Routing Policies, Firewall Filters, and Traffic Policers Feature Guide 2019, 582–583.)

Tilallisen palomuurin keskeisin muutos oli ohjata suodatus yhteyteen, joka mahdollisti liikenteen sallimisen yhteyksien pohjalta. Tämä toiminnallisuus tunnetaan tilataulukkona. Tilallinen palomuuri nostattaa toimintaympäristönsä tietoturvaa huomattavasti, sillä yhteyden luomisessa käytettyjä parametreja voidaan jäljittää. Tilataulukko päivittyy luodun yhteyden muutoksien mukaan varmistaen yhteyden turvallisuuden ja eheyden. (Brodbeck 2017.)

Tilallinen palomuuri kykenee seuraamaan ja ylläpitämään jokaisen sen läpi kulkevan yhteyden tilaa. Tilallisen palomuurin läpi pyrkivää liikennettä kuitenkin vertaillaan palomuurisääntöihin ja tilallinen prosessi alkaa vain, mikäli tarkastettu liikenne on sallittua. Tilallisen palomuurin toimintatavan esimerkkinä voidaan käyttää TCP-yhteyttä (Transmission Control Protocol) käyttävää verkkoliikennettä. TCP seuraa yhteyttään lähde- ja kohdeosoitteiden, porttinumeroiden ja IP-lippujen perusteella. TCP-yhteys luodaan yhteyden osapuolien välisellä kolmiosaisella kättelyllä. Aluksi yhteyttä luova laite lähettää SYN-paketin (Synchronization) ja tästä jää merkintä palomuurin tilataulukkoon. Mikäli yhteyttä luova laitteen sallitaan pääsevän palomuurin läpi, lähettää palomuuri SYN-ACK-paketin (Acknowledgement) takaisin ja lisää tämän tiedon tilataulukkoon. Lopuksi yhteyttä luova laite lähettää palomuurille ACK-paketin, palomuuri merkitsee yhteyden tilaksi *established,* jonka jälkeen verkkoliikenne laitteiden välillä kulkee vapaasti. Palomuuri ylläpitää tätä yhteyttä niin kauan, kun yhteys pysyy *established*-tilassa. (Wilkins 2013.)

Mikäli käytössä on yhteydetön protokolla kuten UDP, on tilallisen palomuurin hankalampi seurata yhteyden tilaa. Yhteydettömällä protokollalla ei ole tilaa, joten tilallinen palomuuri joutuu seuraamaan kyseistä yhteyttä näennäistilallisesti käyttäen hyödykseen juuri sille yhteydelle ominaisia kohtia. UDP:n kanssa tämä joudutaan tekemään IP-osoitteiden ja laitteiden porttinumeroiden

perusteella. UDP ei myöskään sisällä ominaisuutta, jolla se ilmoittaisi yhteyden päättymisestä, joten yleensä UDP-yhteyden tiedot tyhjennetään tilataulukosta märitetyn ajanjakson jälkeen. UDP ei myöskään kykene korjaamaan yhteysongelmia itse, vaan se käyttää ICMP:tä (Internet Control Message Protocol) virheiden korjaamiseen. Mikäli palomuuri ei päästä UDP-yhteyden tarvitsemaa ICMP-liikennettä läpi, ei UDP kykene palautumaan virhetilanteesta. Tämän takia tilalliset palomuurit joutuvat ottamaan huomioon yhteydettömien protokollien tarvitsemat avustavat teknologiat tehdessään päätöksiä mikä liikenne saa kulkea palomuurin läpi. (Northcutt ym. 2005, Chapter 3.)

2.2.2 Välityspalvelinpalomuurit

Välityspalvelinpohjaiset palomuurit (Proxy Firewall) ovat rooliltaan samankaltaisia tilallisten palomuurien kanssa. Molemmat palomuurityypit kontrolloivat verkkoliikennettä esiasetettujen sääntöjen mukaisesti. Välityspalvelinpalomuuri toimii välittäjänä jokaiselle sen läpi menevälle yhteydelle. Välityspalvelin ei ohjaa liikennettä laitteelta toiselle, vaan välityspalvelinta käyttävät laitteet luovat yhteyden välityspalvelimelle ja välityspalvelin luo uuden yhteyden haluttuun kohteeseen. Tämä estää suoran yhteyden luomisen välityspalvelinta käyttävien laitteiden välille ja parantaa tietoturvaa, sillä nämä laitteet eivät ole suorassa yhteydessä keskenään. (Northcutt ym. 2005, Chapter 4.)

Välityspalvelin voi sääntöjen valvonnan lisäksi naamioida liikennettä vastaanottavan laitteen sijainnin. Välityspalvelimien ansiosta ulkopuoliset tietokoneet kykenevät keräämään rajallista tietoa yhteydessä olevasta verkosta, sillä ne ovat yhteydessä vain välityspalvelimeen. Välityspalvelin voi heikentää verkon suorituskykyä, sillä saapuvien yhteyksien lopettaminen, uusien yhteyksien luominen ja näiden suodatus kasvattavat verkon vasteaikaa, tehden joidenkin sovellusten käyttämisen välityspalvelimen läpi mahdottomaksi. (Greene & Butler 2019.)

Välityspalvelimet toteutetaan usein pienenä ryhmänä luotettuja erityisohjelmistoja, joista jokainen tukee jotain tiettyä ohjelmistoprotokollaa. Nämä ohjelmat kykenevät tekemään erittäin tarkan tietoturva-analyysin välittämästään protokollasta, tarjoten tilallista palomuuria paremman tietoturvan. Tämä tietoturva-

hyöty rajoittuu vain välityspalvelimen tuntemiin protokolliin. Mikäli välityspalvelimella ei ole erityistä tukea käytettävälle protokollalle, välityspalvelin ei kykene tekemään syvempää analyysiä sen läpi menevälle liikenteelle. (Northcutt ym. 2005, Chapter 4.)

2.2.3 Pakettien syvätarkastus

Pakettien syvätarkastaminen, DPI (Deep Packet Inspection), mahdollistaa verkkoliikenteen analysoinnin reaaliaikaisesti ja sen erottelun IP-pakettien sisällön mukaan. Aikaisemmat ratkaisut suodattivat liikennettä pakettien otsikoiden (header) mukaisesti. DPI mahdollistaa tämän lisäksi IP-pakettien sisältämän datan tarkastamisen. (Telecommunication Engineering Center s.a., 1.)

Tarkastamalla IP-pakettien sisältämää dataa DPI-laitteet voivat tunnistaa käytössä olevan ohjelman tai protokollan. Liikenteen sisällön tunnistamisen avulla voidaan luoda rajoituksia verkkoliikenteelle, tai muokata liikenteen kulkua. DPI:n avulla voidaan karsia verkossa kulkevia viruksia pysäyttämällä virukseksi tunnistettujen pakettien liikkumisen. (Anderson 2007.)

Tunnistepohjaisella tarkastuksella DPI kykenee tekemään tarpeellisia toimenpiteitä, mikäli verkkoliikenteessä tunnistetaan poikkeavaa käytöstä tai käynnissä oleva hyökkäys. Tunnistepohjaisen tarkastuksen toimintatapa on samankaltainen välityspalvelimien erityisohjelmistojen kanssa. IDS tarvitsee tiedon analysoitavan protokollan toimintaperiaatteesta kyetäkseen analysoimaan ja vertailemaan liikenteen dataa. Tämä vaatii laitteelta myös paljon laskennallista tehoa, sillä IP-paketin dataosio sisältää paljon tietoa. (Brodbeck 2015a.)

DPI suunniteltiin alun perin turvaamaan paikallisia lähiverkkoja ei-toivotulta liikenteeltä tavallisten palomuurien rinnalle, sillä yritysverkon sisä- ja ulkopuolen rajoittamisesta on tullut hankalaa web-sovellusten kehittymisen ansiosta, mistä johtuen lähiverkossa liikkuvan datan tarkastamisesta on tullut tarpeellista. Hyödyntämällä pakettien syvätarkastamista verkkoa voidaan hallinnoida tarkemmin. Verkon ruuhkautumista voidaan estää erottelemalla eri verkkoliikennetyyppejä, kuristamalla kaistaa liialliselta liikenteeltä ja priorisoimalla tarpeellinen liikenne. (Telecommunication Engineering Center s.a., 4.)

2.2.4 UTM

Ennen UTM-laitteiden kehittämistä turvallisuusala vaikutti kehittyvän suuntaan, jossa jokaista uhkaa varten tarvittaisiin uusi erillinen teknologia. Tästä johtuen syntyi tilanteita, missä verkonhallinta oli monimutkaisempaa, kalliimpaa ja hankalampaa hallita (Tam ym. 2013, 20).

Tarve saattaa yhä enemmän eri tietoturvamekanismeja yhteen ratkaisuun loi pohjan UTM-järjestelmän käsitteelle. Ensisijaisesti tämä on markkinanimitys yksittäisille laitteille, jotka sisältävät useampia ominaisuuksia, kuten välityspalvelin, VPN ja IDS/IPS-järjestelmät. Vaikka useampien ominaisuuksien sisällyttäminen yhteen laitteeseen voi vaikuttaa helpolta ratkaisulta tietoturvahaasteisiin, vaatii laite sitä enemmän suorituskykyä mitä enemmän ominaisuuksia siihen sisällytetään. (Brodbeck 2015a.)

UTM-palomuurin rajoittavaksi tekijäksi voidaan korostaa suorituskykyongelmat. Kaikkien tietoturvaominaisuuksien keskittämisen ongelmat näkyvät yrityksissä, missä käytössä olevien laitteistojen suorituskyky ei ole riittävä yrityksen verkolle. Pienemmät yritykset, joiden verkkoliikenne ei ole raskasta voivat hyötyä näistä laitteista paljon. Yksittäinen laite on usein halvempi kuin usea erikoistunut laite ja yritysverkossa, jonka liikenne ei ole raskasta, kykenee yksittäinen UTM-laite käsittelemään verkon liikennettä ilman suorituskykyongelmia. (Brodbeck 2018.)

Ilman UTM-laitetta verkon liikenne joutuu todennäköisesti kulkemaan useamman eri tietoturvajärjestelmän lävitse. Usein näiden järjestelmien toiminnot ovat toiminnoiltaan vastaavanlaisia ja niiden lävitse kulkevat yhteydet tarkastetaan uudelleen jokaisen järjestelmän kohdalla ennen kuin ne päästetään liikkumaan eteenpäin. UTM-laitteen avulla verkon tehokkuutta voidaan kasvattaa tarkastamalla jokainen yhteys vain kerran. UTM-laitteet helpottavat verkon ongelmanratkaisua, sillä kaikki tarvittava tieto verkon tilanteesta löytyy yhdestä paikasta. (Tam ym. 2013, 23–24.)

2.2.5 Seuraavan sukupolven palomuuri

Seuraavan sukupolven palomuuri (Next Generation Firewall, NGFW) kehitettiin korjaamaan UTM-laitteiden toimintakyvyn heikkoudet suorituskykyisessä

yhtenäisessä kokonaisuudessa. UTM-palomuurin ominaisuuksia on jätetty sisällyttämättä seuraavan sukupolven palomuureihin, varmistaen hyvät laajennettavuusmahdollisuudet suuriin ympäristöihin. Pakettien syvätarkastuksen ja ohjelmistojen läpinäkyvyyden kehittymisen ansiosta seuraavan sukupolven palomuuri mahdollistaa dynaamisempien ja tehokkaampien suodatussääntöjen luomisen. (Brodbeck 2018.)

Esimerkkinä ohjelmien läpinäkyvyyden tuomista hyödyistä on mahdollisuus erotella ohjelman tai verkkosivun eri osa-alueita mitä sallia tai kieltää sen sijaan, että se joko sallittaisiin tai kiellettäisiin kokonaan. Seuraavan sukupolven palomuurit kykenevät havaitsemaan liikennepohjaisen ohjelman tyypin ohjelman käyttämän portin ja protokollan lisäksi. Tämän ansiosta seuraavan sukupolven palomuuri kykenee tunnistamaan ohjelman, vaikka ohjelma ei käyttäisikään sen vakioportteja. (Brodbeck 2015a.)

Seuraavan sukupolven palomuurilla ja UTM-palomuurilla on merkittäviä eroja mutta niiden ymmärtämisessä on vielä vaikeuksia. Tähän on vaikuttanut UTM-teknologian kehittyminen. Seuraavan sukupolven palomuurien katsotaan soveltuvan hyvin ympäristöihin, joissa verkkoliikenne on intensiivistä. Näissä verkoissa tietoturvajärjestelmien erottaminen toisistaan on tärkeää ympäristön sietokyvyn ja skaalautuvuuden kannalta. (Brodbeck 2018.)

2.2.6 FWaaS

FWaaS (Firewall as a Service) on pilvi- tai hybridipohjainen monitoimintoinen palomuuripalvelu. FWaaS tarjoaa yksinkertaisemman ja joustavamman arkkitehtuurin siirtämällä useita yritystasoisia palomuuriominaisuuksia osittain tai kokonaan pilveen. (Young & D'Hoinne 2017.)

FWaaS on pohjimmiltaan erilainen palvelu verrattuna hallinnoituun palomuuripalveluun (Managed firewall service). SSL liikenteen suuri kasvu aiheuttaa ongelmia palomuurilaitteiden suorituskyvylle ja aiheuttaa ennalta-arvaamatonta tarvetta päivittää palomuurilaitteita suorituskykyisempiin. Palveluntarjoajat ovat jo pitkään tarjonneet palomuuripalveluja, joissa palvelu toteutetaan fyysi-

sillä palomuurilaitteilla. FWaaS on pilvilaskentaa hyödyntävä looginen palomuuri, jonka suorituskyky skaalautuu käyttäjän tarpeiden mukaan. (Greenfield 2017.)

Toisien palomuuriratkaisuiden suurena ongelmana ovat vastaan tulevat suorituskykyrajoitteet, ja laitteiden tuen loppuminen laitteen elinkaaren tullessa päätökseen. FWaaS tarjoaa näille palomuureille vaihtoehtoisen, kaiken kattavan ratkaisun. Ydinajatus FWaaS-tyyppisessä palomuuripalvelussa on tarjota täysi tietoturvapaketti pilvipalveluna, jonka avulla päästään eroon tavallisten verkkolaitteiden huolto- ja ylläpitotehtävistä. FWaaS ohjaa yritysverkon liikenteen pilveen, yhdistäen kaiken liikenteen yhteen kaiken kattavaan palomuuriin. (Greenfield 2018.)

FWaaSilla on huomattavia etuja vanhoihin järjestelmiin verrattuna. Näitä ovat yksinkertaisempi hallinnointi ja mahdollisuus tarkastaa usean verkon yli kulkevaa liikennettä. Tämän lisäksi palvelun asiakkailla ei ole rajoitteita suorituskyvyn kanssa ja FWaaS pysyy aina ajan tasalla palveluntarjoajan pitäessä huolen kaikista päivityksistä ja suorituskyvyn pitämisestä tarvittavalla tasolla. (Greenfield 2018.)

3 TEKNOLOGIAT

3.1 MPLS

MPLS-verkon keskeisin ominaisuus on useiden eri verkkoliikennetyyppien tunnelointimahdollisuus ydinverkon läpi. MPLS-tunnelissa vain liikenteen sisäänmeno- ja ulostuloreitittimet tietävät tunnelin läpi kulkevasta liikenteestä tarpeelliset tiedot liikenteen reitittämistä varten. MPLS-verkon ydinlaitteet liikuttavat MPLS-kapseloituja paketteja ottamatta kantaa pakettien sisältöön. MPLS suojaa liikennettä dataväärennykseltä, sillä MPLS-tunneliin voidaan injektoida dataa vain tunnelin alkupäässä. (Minei & Lucek 2008, 6)

MPLS-verkko koostuu reunareitittimistä ja ydinreitittimistä. Reitittimien välille rakennetaan yksisuuntaisia LSP-tunneleita, joita käyttämällä sisääntuloreitittimeen tuleva liikenne voidaan ohjata oikeaan ulostuloreitittimeen. Reunareititin määrittää, mihin FECiin saapuvat paketit kuuluvat. Paketteja, jotka ovat kulke-

massa samaan määränpäähän samaa reittiä pitkin ja joiden edelleenlähetykseen kohdistetaan samat toimenpiteet, pidetään kuuluvan samaan FECiin. Samaan FECiin kuuluvat paketit edelleenlähetetään samalla MPLS-tunnuksella. MPLS kykenee kuljettamaan useaa eri liikennetyyppiä saman LSP:n sisällä. Tämän ansiosta kaikki liikenne tiettyjen reunareitittimien välillä voidaan sisällyttää yhteen tunneliin. LSP:n sisällä kulkeva liikenne tekee edelleenlähetyspäätökset MPLS-tunnisteen perusteella, mistä johtuen MPLS-verkon ydinlaitteiden ei tarvitse tallentaa tunneleissa kulkevan liikenteen reititystietoja. (Minei & Lucek 2008, 6–7.)

MPLS-tunniste koostuu neljästä kentästä, joita ovat Label, TC, S ja TTL. MPLS-tunnisteen rakennetta on esitetty taulukossa 1. MPLS-verkon edelleenlähetys toimii 20-bittisen Label-kentän sisällön perusteella. TC/EXP-kentän tietoja käytetään määrittelemään paketin CoS-arvot. (Minei & Lucek 2008, 7.) Vuonna 2009 tämä kenttä uudelleennimettiin TC-kentäksi ja kaikki siihenastiset viittaukset EXP-kenttään viittaavat nyt TC-kenttään. (Andersson & Asati 2009, 5). S-kenttä, bottom of stack-bitti joka asetetaan pohjimmaiseen MPLS-tunnisteeseen. TTL-kenttää käytetään ehkäisemään silmukoiden syntymistä. Sen arvoa vähennetään jokaisella hypyllä reitittimien välillä ja paketti hylätään, mikäli tämä arvo laskee nollaan. (Minei & Lucek 2008, 7.)

Taulukko 1. MPLS-tunnisteen rakenne

Label	TC/EXP	S	TTL

Sisääntuloreititin asettaa yhden tai useamman MPLS-tunnisteen verkkoon saapuville paketeille. Tämä tunniste määrittää mihin LSP:hen saapunut paketti asetetaan. Sisääntuloreititin määrittää myös mihin ulosmenoreitittimeen ja sen LSP:hen liikenne ohjataan. Seuraava reititin määrittää paketin Label-kentälle uuden arvon ja jatkaa sen uudelleenlähetystä. Label-kenttää vaihtamalla MPLS-verkko ohjaa tunneloidun liikenteen reunalta reunalle. (Minei & Lucek 2008, 7–8.)

3.2 EoMPLS

MPLS on palveluntarjoajien käyttämä teknologia, jonka avulla toteutetaan useita toiminnallisuuksia, kuten QoS, tunnisteenvaihto ja palvelutasot. Ethernet over MPLS, lyhenne EoMPLS, on Ciscon luoma ratkaisu MPLS:n laajentamiseksi. EoMPLS mahdollistaa palveluntarjoajalle helpomman laajentuvuuden ja asiakkaalle mahdollisuuden ohjata oman verkkoliikenteen suoraan palveluntarjoajan verkon läpi. (Deal 2003, 118.)

EoMPLS:n avulla ethernet-kehyksien lähettäminen onnistuu MPLS-verkon yli. EoMPLS tunneloi OSI-mallin toisen kerroksen ethernet-liikennettä palveluntarjoajan kolmannella kerroksella olevan ytimen läpi. MPLS-pakettien sisälle paketoidaan toisten protokollien PDU:t (Protocol Data Unit) ja nämä ohjataan eteenpäin MPLS-verkossa. EoMPLS:n mahdollistama toisen kerroksen dataliikenne mahdollistaa esimerkiksi dynaamisten reititysprotokollien käytön datakeskuksien välillä. (MPLS Applications User Guide 2021, 1675–1676.)

EoMPLS:n avulla voi luoda TLS-yhteyden (Transport Layer Security) asiakkaan ethernet-yhteyksille. TLS luo loogisen yhteyden kahden kohteen välille, näkyen asiakkaalle osana ethernetiä. EoMPLS:n pohjautuessa kolmannen kerroksen prosesseihin, toisen kerroksen hallinnointi ja ongelmien korjaus ei jää palveluntarjoajan tehtäväksi. (Deal 2003, 118.)

3.3 OSPF

Tämä luku perustuu Huntin (2002, 184–188) kirjan kappaleeseen Interior Routing Protocols.
Open Shortest Path First (OSPF) on link-state-tyyppinen protokolla. Tämän tyyppinen protokolla jakaa verkkoon tietoa naapurilaitteistaan. Verkolla tarkoitetaan tässä tapauksessa laajimmillaan yhtä autonomista järjestelmää (AS). OSPF on sisäinen reititysprotokolla ja sen tarkoituksena on luoda verkkoliikenteen reititys autonomisen järjestelmän sisälle. OSPF luo autonomisen järjestelmän sisäisen hierarkian reititysalueille. Tämän hierarkian osia ovat alueet, runkoverkko ja tynkäalue (stub-area). Alueet ovat tietyistä verkkolaitteista koostuvia kokonaisverkon osia. Verkon jakaminen alueisiin on tarpeellista vain suurempien autonomisten järjestelmien kohdalla. Runkoverkko yhdistää auto-

nomisen järjestelmän eri alueet samaan verkkoon ja jakaa reititystiedot alueiden välillä. Tästä johtuen kaikkien alueiden tulee olla liitettynä runkoverkkoon. Tynkäalueella on vain yksi reititin alueen reunalla. Tästä johtuen tynkäalueelta on vain yksi reitti ulos ja tynkäalueen reunareititin voi mainostaa itseään oletusreittinä. Link-state protokollien ongelmana on niiden verkosta keräämä suuri määrä reitittimien välistä dataa, mistä johtuen verkkoliikenteen reitin laskemiseen voi mennä paljon aikaa. Tästä datasta reitittimet luovat itselleen tietokannan verkosta, jonka osana ne ovat. Jokainen OSPF-reititin hyödyntää tätä tietokantaa kaavion luomiseksi verkosta, joka toimii karttana koko OSPF-verkolle kyseisen reitittimen näkökulmasta. Tämä kartta sisältää tietoa OSPF-verkon jokaisesta reitittimestä, sekä niiden naapurireitittimistä. Tietokannan data kerätään ja jaetaan yksinkertaisesti käyttämällä Hello-paketteja. OSPF-reititin lähettää Hello-paketteja verkkoon ja kuuntelee naapurireitittimien lähettämiä vastaavia paketteja. Kun naapurireitittimet saavat lähetettyä ja vastaanotettua Hello-paketteja toisiltaan, lisäävät nämä reitittimet toisensa omille naapurilistoilleen. Tämän jälkeen OSPF-reititin mainostaa kaikki naapurinsa verkkoon LSA-viestinnällä (Link-State Advertisement). LSA sisältää kaikkien naapureiden osoitteet ja kustannuksen kyseisen naapurin saavuttamiseksi LSA:n lähettäneeltä reitittimeltä. Mainostaminen tapahtuu lähettämällä LSA-tiedot eteenpäin kaikista porteista, paitsi siitä, mistä reititin on vastaanottanut LSA-tietoja. Reitittimet tallentavat kopion vastaanottamistaan LSA-paketeista ja tämän jälkeen hylkäävät samanlaiset LSA:t. Tällä tavalla OSPF-verkko välttää turhan liikenteen luomisen. OSPF-verkko ylläpitää itseään automaattisesti. Reitittimet lähettävät Hello-paketteja säännöllisesti. Mikäli jokin verkon reititin ei lähetä tai vastaanota Hello-paketteja, OSPF olettaa joko tämän linkin naapurille tai koko naapurireitittimen olevan alhaalla. Tässä tilanteessa reitittimet päivittävät naapurilistansa ja jakavat päivitetyn LSA:n OSPF-verkkoon. Tämän jälkeen jokainen reititin laskee verkosta luomansa kartan uudelleen päivitetyillä tiedoilla.

OSPF-verkon tehokkuutta voidaan lisätä hyödyntämällä nimettyä reititintä (Designated router). Tämä reititin pitää kaikkia OSPF-verkon reitittimiä naapureinaan ja samanaikaisesti muut reitittimet pitävät vain tätä nimettyä reititintä naapurinaan. Näin saadaan link-state-tietokantaa pidettyä pienempänä, samalla nopeuttaen OSPF-verkon kokonaisuuden laskentaa. Hyödyntämällä alueita ja nimitettyjä reitittimiä, OSPF-verkko kykenee laskemaan reitin verkkoliikenteelle nopeammin.

4 PALOMUURIPALVELUIDEN TYYPIT JA VALINTA TYÖHÖN

Palomuurin tarjoaminen ylläpidettävänä palveluna (Managed Firewall Service) on vanhempi keino toteuttaa palomuuripalvelu. Tämän tyyppisessä palvelussa palomuurilaitteiden hankkimiskustannukset tulevat palveluntarjoajalle ja asiakasyritykset voivat vuokrata näiden laitteiden toimintakykyä oman verkkoliikenteensä suodattamista varten. Palveluntarjoajan asiakkailta tämä poistaa tarpeen ostaa palomuurilaitteita omiksi, sekä siirtää vastuun niiden toimivuudesta palveluntarjoajalle. Tämäntyyppisen palomuuripalvelun suurimpia haasteita on sen skaalautuvuus. Salattu liikenne yleistyy jatkuvasti ja sen tarkastaminen on perinteisille palomuureille salaamatonta liikennettä huomattavasti raskaampaa. Tästä johtuen yksittäinen palomuurilaite kykenee suodattamaan rajallisen määrän liikennettä. Ainoa keino kasvattaa liikenteen käsittelykykyä on ostaa lisää palomuurilaitteita kattamaan tarpeen kasvaneen liikenteen suodattamiselle, eikä tämä ratkaisu ongelmaa ole nopea. Tästä johtuen tämän tyyppinen palomuuripalvelu ei ole joustava, tarkoittaen sitä, että se ei kykene vastaamaan hetkelliseen verkkoliikenteen suureen kasvuun.

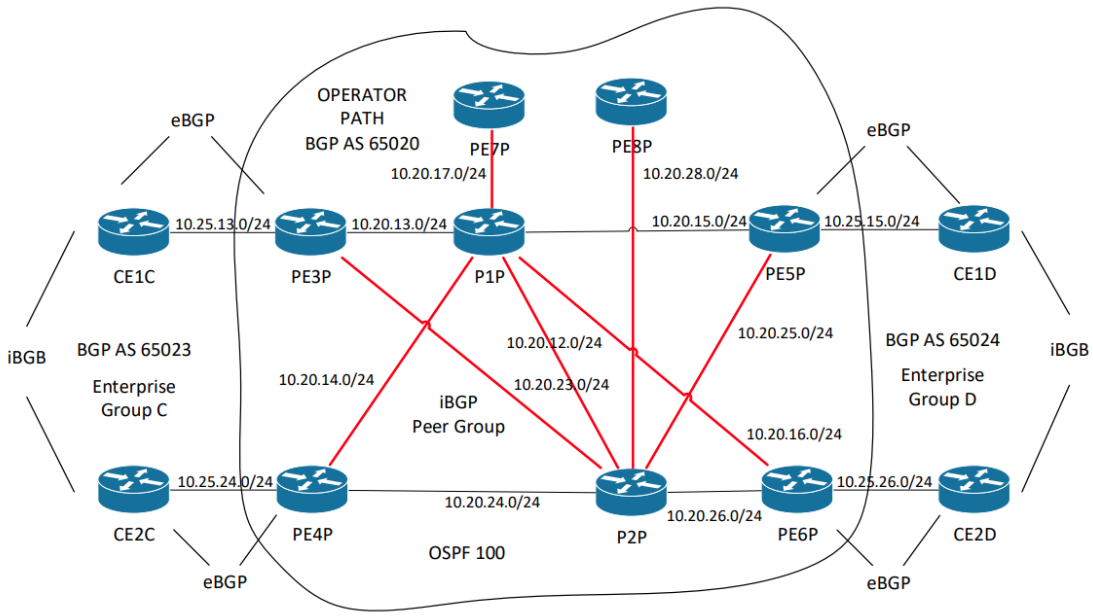
FWaaS on uudempi keino luoda palomuuripalvelu ja se pyrkii tarjoamaan ylläpidettävän palomuuripalvelun rajoituksiin ratkaisun ja kuitenkin pitää sen hyödyt. FWaaS toimii pilvipalveluna ja sen palomuuriratkaisut virtualisoituina. Palveluntarjoajalle tämä tarkoittaa sitä, että sen tarvitsee ylläpitää samaan aikaan monimutkaisempaa ja yksinkertaisempaa datakeskusta ja varmistaa, että datakeskuksen suorituskyky vastaa sitä, mitä asiakkaille on luvattu heidän ostamassa palomuuripalvelupaketissa. Palvelun ylläpito tulee yksinkertaisemmaksi palveluntarjoajalle, sillä ylläpidettävien fyysisten laitteiden monimuotoisuus vähenee ja monimutkaisemmaksi useampien tarpeellisten ohjelmistojen takia. Toimiva FWaaS kuitenkin tarjoaa ylläpidettävän palomuuripalvelun ominaisuuksien lisäksi myös saumattoman toimivuuden myös tilanteessa, jossa yrityksen verkkoliikenne kasvaa hetkellisesti.

Työhön valikoitui palveluntarjoajan ylläpitämä palomuuripalvelu, sillä BPI-kurssissa on haluttu käyttää mahdollisimman paljon fyysisiä laitteita, tarkoituksena havainnollistaa myös datakeskuksien toimintaa opiskelijoille. Pohjana on käytetty BPI-kurssin palveluntarjoajaverkkoa, johon on lisätty palomuurilaite havainnollistamaan aikaisemmin kuvaillun palvelun luomista. Todellisuudessa vastaavanlaisessa palvelussa olisi käytössä useampia palomuurilaitteita,

mutta laitteiden suurella määrällä ei ole konseptin todennuksen kannalta merkitystä. Ratkaisu on saatu osittain tehtyä, osan siitä jäädessä teoreettiselle tasolle. Toteutusosiossa käydään ensin läpi BPI-kurssin palveluntarjoajaverkon toimintaa ja lisätään tähän kokonaisuuteen palomuuri. Tämän jälkeen käsitellään asiakasverkon liikenteen ohjausta palomuurille, josta liikenne ohjataan palveluntarjoajan verkon läpi internetiin. Tässä yritysverkossa on myös haluttu käyttää yksinkertaista MPLS-verkkoa opetustarkoituksessa ja sitä hyödyntämällä valitun tyyppinen palomuuripalvelu on yksinkertaisempi lisätä kokonaisuuteen. FWaaS-ratkaisu hukuttaisi BPI-kurssin tarkoituksen yksinkertaistettuna ensimmäisen ja kolmannen vuoden opiskelijoiden välisenä tiimipohjaisena kurssina ja vaatisi laajempaa tuntemusta virtualisoinnista.
Työ on toteutettu Kaakkois-Suomen ammattikorkeakoulun ICTLAB:in virtuaalilaboratoriojärjestelmässä fyysisten laitteiden määrällisten ja toiminnallisten rajoitteiden vuoksi.

5 TOTEUTUS

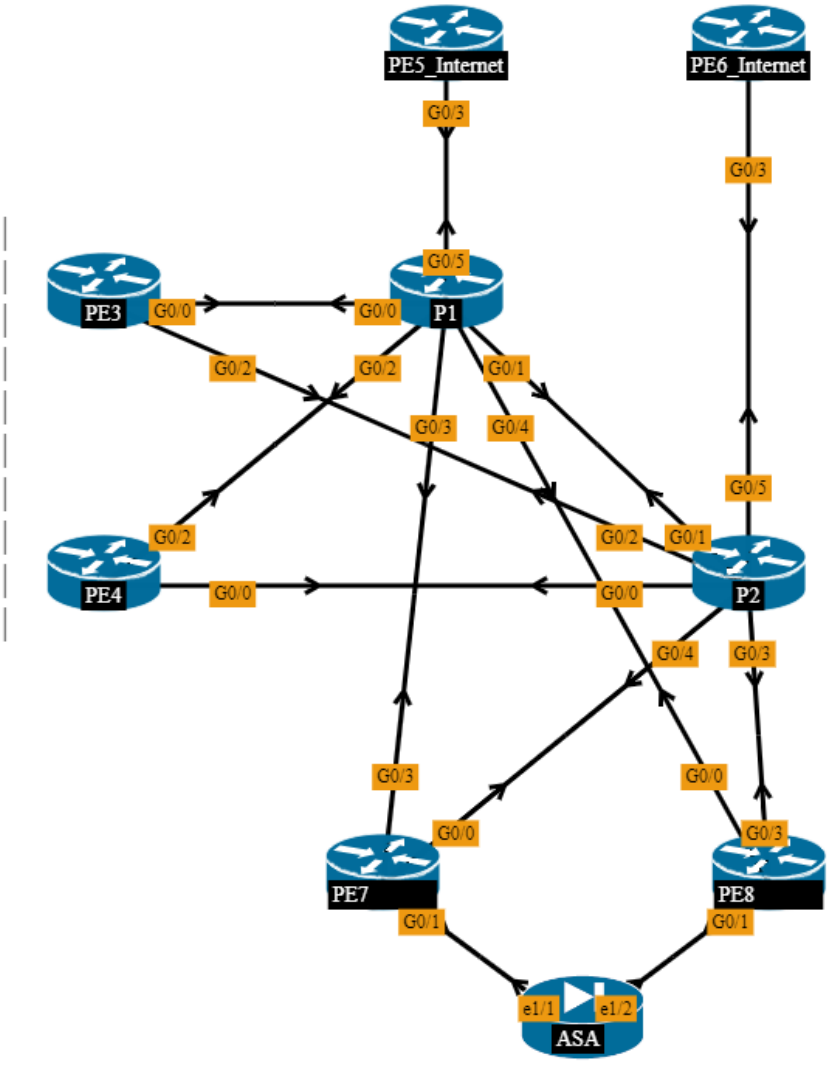
Kuva 1 näyttää pohjalla olevan verkon topologian. P-alkuiset reitittimet kuuluvat palveluntarjoajan verkkoon, joista P1P ja P2P muodostavat verkon ytimen ja PE-reitittimet toimivat verkon reunalla. CE-reitittimet kuuluvat asiakasverkkoihin, toimien näiden verkkojen reunareitittiminä.



Kuva 1. Alkuperäinen palveluntarjoajaverkon topologia

Kuten kuvasta 1 näemme, on palveluntarjoajan verkon ydinreitittimet kytketty verkon muihin reitittimiin, luoden tästä verkosta redundanttisen yhdessä käytössä olevien protokollien kanssa. Palveluntarjoajan verkossa on käytössä myös MPLS, jota hyödyntämällä yhteys palomuurille on tarkoitus luoda. Tässä esimerkissä käytössä oleva IGP (Interior Gateway Protocol) on OSPF ja asiakasverkko on yhdistettynä palveluntarjoajan verkkoon BGP:n avulla.

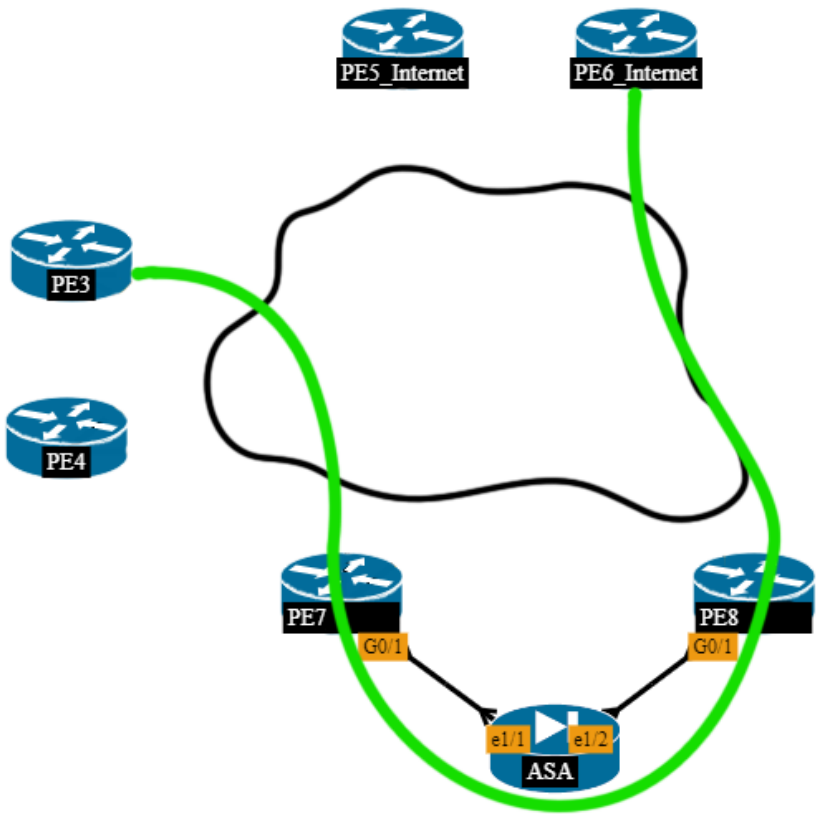
Asiakasverkon yhteys palveluntarjoajan verkkoon on kahdennettu. Kahdentamisella varmistetaan asiakkaan verkkoyhteyden toimivuus myös tilanteessa, missä toinen yhteyksistä katkeaisi esimerkiksi laiterikon tai kaapelin katkeamisen vuoksi. Palveluntarjoajan verkossa on myös varmistettu verkon toimivuus vikatilanteessa redundanttisella suunnittelulla.



Kuva 2. Topologiaan tehty lisäys

Palomuuripalvelu lisättiin palveluntarjoajan verkon reunalle, tätä havainnollistettu kuvassa 2. Reunareitittimet PE7 ja PE8 yhdistettiin molempiin ydinreitittimiin redundanttisuuden saavuttamiseksi. Kuten kuvasta 2 näkyy, on topologiasta karsittu pois toisen puolen asiakasverkko ja sen puolen reunareitittimet näkymän yksinkertaistamiseksi.

Yhteys palomuurille tuodaan käyttämällä EoMPLS-tunnelia reunareitittimeltä reunareitittimelle. Tunneli kahdennetaan molempien ydinreitittimien kautta, näin pyritään varmistamaan yhteyden toimivuus myös tilanteessa, jossa toinen linkeistä katkeaisi. Tunnelia varten luodaan aliliityntäportit (subinterface) yhdistettäviin portteihin, käytetään esimerkkinä PE3-reitittimen G0/0-porttia ja reitittimen PE7 G0/3-porttia. Molemmille luodaan aliliityntäportit, joille EoMPLS/pseudowire-komennot lisätään.



Kuva 3. Looginen reitti

Kuvassa 3 havainnollistetaan liikenteen kulkemaa reittiä. Pilven alle jäävät ydinreitittimet toimivat siltana halutunlaiselle yhteydelle. Tässä tapauksessa on asiakkaalle luotu EoMPLS-tunneli palomuuriin kiinnitetylle reunareitittimelle. Asiakkaalle tämän on tarkoituksena toimia, kuin palomuuri olisi osana omaa verkkoa, hallintamahdollisuuksien laajuuden jäävän sovittavaksi palveluntarjoajan ja asiakkaan kesken.

Palomuurilta yhteys voidaan reitittää normaalisti, tässä esimerkissä PE8-reitittimeltä, ydinverkon läpi internetiin hyödyntäen ydinverkon protokollia. Kuvan 3 esimerkissä palomuurin (ASA) INSIDE-liikenne kulkee PE7-reitittimen kautta ja OUTSIDE-liikenne kulkee PE8-reitittimen kautta. Ratkaisun redundanttisuutta voisi lisätä hyödyntämällä aliliityntäportteja palomuurilla. Tässä tapauksessa INSIDE ja OUTSIDE-liikenne saataisiin kulkeutumaan samaa fyysistä linkkiä pitkin ja ratkaisu kestäisi toisen linkin katkeamisen. Tämä myös mahdollistaisi toisen EoMPLS-tunnelin luomisen varayhteydeksi PE8-reitittimelle. Tällöin verkkoliikenne pysyisi toimintakuntoisena tilanteessa, missä PE7 tai PE8-reititin menisi toimintakyvyttömäksi. Mikäli aliliityntäportteja ei haluta käyttää, voi saman lopputuloksen saavuttaa lisäämällä toinen fyysinen yhteys palomuurin ja reunareitittimen välille. Tässä tapauksessa toinen linkki olisi varattu palomuurin INSIDE-liikenteelle ja toinen OUTSIDE-liikenteelle. Todellisessa tilanteessa aliliityntäporttien käyttäminen olisi todenmukaisempi vaihtoehto, sillä palomuurilaitteilla on hyvin rajallinen määrä fyysisiä liityntäportteja. Aliliityntäportteja hyödyntämällä yksittäinen palomuurilaite kykenee tarjoamaan enemmän yhteyksiä, kuin olisi mahdollista pelkkiä fyysisiä portteja käyttämällä. Kuvailtuja keinoja käyttämällä työn määrä lisääntyisi kuitenkin huomattavasti ja BPI-kurssipohjaan tehtävän lisäyksen laajuus kasvaisi huomattavasti, joten yksinkertaisempi ratkaisu on tässä tilanteessa parempi vaihtoehto.

6 JOHTOPÄÄTÖKSET JA POHDINTA

Tarve toimiville ja turvallisille tietoverkoille kasvaa jatkuvasti ja kyberturvallisuus alkaa tulemaan yhä laajemmin esille alan koulutuksissa, kuten myös tavallisessa maailmassa jatkuvasti yleistyvien tietomurtojen myötä. Kyberturvallisuus käsitteenä on laaja ja tämän käsitteen yhtenä osa-alueena ovat palomuurit monimuotoisine ratkaisuineen. Yritykset voivat hoitaa verkkoyhteyksiensä ylläpidon itse, jolloin kaikki vastuu yhteyksien turvallisuudesta voi jäädä tämän yrityksen hoidettavaksi. Tämä puolestaan tarkoittaa tarvetta ammattilaisten palkkaamiseen hoitamaan yrityksen verkkoyhteyksiä. Joillekin yrityksille tämä ei ole toteuttamiskelpoinen ratkaisu, jolloin heillä on mahdollista kääntyä verkkoyhteyksien toteutuksen kanssa näihin erikoistuneen yrityksen puoleen. Osan verkkolaitteista on sijaittava yrityksen tiloissa, mutta joitakin osuuksia voi ulkoistaa yhteistyökumppaneille, kuten esimerkiksi palomuurit.

Ulkoistettavia palomuuriratkaisuja ovat ainakin perinteisempi palomuuripalvelu, jossa palomuurit sijaitsevat palveluntarjoajan datakeskuksessa ja asiakkaan liikenne ohjataan näiden laitteiden läpi sekä FWaaS, Firewall as a Service, joka puolestaan on pilvipalvelupohjainen palomuuriratkaisu. FWaaS uudempana teknologiana tulee todennäköisesti syrjäyttämään perinteisemmät palomuuripalvelut, sillä se ei vaadi palveluntarjoajalta yhteen asiaan erikoistuneiden fyysisten laitteiden hankkimista palvelua varten, vaan palvelu voidaan toteuttaa laitteilla, jotka samanaikaisesti ylläpitävät myös muita palveluita.

Tämän opinnäytetyön aikana oli tarkoituksena luoda hallinnoitu palomuuripalvelu lisäten se BPI-kurssin palveluntarjoajaverkkoon ilman, että konfiguraatiokokonaisuus monimutkaistuisi liikaa. BPI on yhteiskurssi ensimmäisen ja kolmannen vuoden opiskelijoille ja tässä opinnäytetyössä on osittain käsitelty asioita, jotka tulevat opiskelijoille eteen vasta kolmannen vuoden aikana. Tästä johtuen myös palomuuripalvelun luomisprosessin täytyi olla kokonaisuutena yksinkertaistetumpi, jotta kolmannen vuoden opiskelijat pystyisivät ohjeistamaan ensimmäisen vuoden opiskelijoita paremmin. Tarkoituksena oli myös luoda ohjeistus tämän palomuuripalvelun luomiseksi Kaakkois-Suomen ammattikorkeakoulun ICTLAB:n virtuaaliympäristössä, sillä fyysisiä laitteita ei olisi saatavilla tarpeeksi paljoa täyttä toteutusta varten. Eteen tulleiden aikarajoitteiden vuoksi konfiguraatioiden täysi testaus jäi kuitenkin puutteelliseksi ja täten opinnäytetyön tavoitetta ei saavutettu. Mikäli tätä aihetta tulevaisuudessa jatketaan, tarvitsee konfiguraatioiden toimivuus varmistaa tai muuttaa, mikäli käytettävä käyttöjärjestelmä eroaa komennoiltaan huomattavasti Ciscon IOS XE:stä, kuten esimerkiksi Ciscon IOS XR.

LÄHTEET

Anderson, N. 2007. Deep packet inspection meets 'Net neutrality, CALEA. WWW-dokumentti. Saatavissa: https://arstechnica.com/gadgets/2007/07/deep-packet-inspection-meets-net-neutrality/ [viitattu 25.4.2019].

Andersson, L. & Asati, R. 2009. Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field. Internet Engineering Task Force. PDF-dokumentti. Saatavissa: https://tools.ietf.org/pdf/rfc5462.pdf [viitattu 17.6.2019].

Barracuda Networks s.a. What are Network Firewalls. WWW-dokumentti. Saatavissa: https://www.barracuda.com/glossary/network-firewall [viitattu 8.4.2019].

Brazil, J. 2017. The life of the firewall – A history. ITProPortal. WWW-dokumentti. Saatavissa: https://www.itproportal.com/features/the-life-of-the-firewall-a-history/ [viitattu 9.4.2019].

Brodbeck, C. 2015a. Definition of Firewall: Enhance your security knowledge. OSTEC. WWW-dokumentti. Saatavissa: https://ostec.blog/en/perimeter/firewall-definition [viitattu 24.4.2019].

Brodbeck, C. 2015b. Firewall: History. OSTEC. WWW-dokumentti. Saatavissa: https://ostec.blog/en/perimeter/firewall [viitattu 9.4.2019].

Brodbeck, C. 2017. Firewall: stateless and stateful filtering mechanisms. WWW-dokumentti. Saatavissa: https://ostec.blog/en/perimeter/firewall-stateful-stateless [viitattu 17.4.2019].

Brodbeck, C. 2018. NGFW and UTM Firewall: Find out the main differences. WWW-artikkeli. Saatavissa: https://ostec.blog/en/perimeter/firewall-utm-ngfw-differences [viitattu 26.4.2019].

Deal, R. 2003. Bcmsn Exam Cram 2: Exam 642-811. Que. E-kirja. Saatavissa: https://flylib.com/books/en/2.247.1/ [viitattu 29.4.2021].

Greenfield, D. 2017. FWaaS or Managed Firewall Services: What's the Difference? WWW-artikkeli. Saatavissa: https://www.catonetworks.com/blog/fwaas-or-managed-firewall-services-whats-the-difference/ [viitattu 15.3.2019].

Greenfield, D. 2018. Firewall as a Service vs UTM. WWW-artikkeli. Saatavissa: https://www.catonetworks.com/blog/firewall-as-a-service-vs-utm/ [viitattu 2.5.2019].

Greene, T. & Butler, B. 2019. What is a firewall? How they work and how they fit into enterprise security. WWW-artikkeli. Saatavissa: https://www.networkworld.com/article/3230457/what-is-a-firewall-perimeter-stateful-inspection-next-generation.html [viitattu 24.4.2019].

Hunt, C. 2002. TCP/IP Network Administration. Kolmas painos. Sebastopol: O'Reilly Media.

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona: Opas opinnäytetyön ja pro gradun kirjoittajalle. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2014. Verkkotutkimus Opinnäytetyönä: Laadullisen ja määrällisen verkkotutkimuksen opas. Jyväskylä: Jyväskylän ammattikorkeakoulu, 51, 58.

Kananen, J. 2012. Kehittämistutkimus Opinnäytetyönä: Kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kettunen, M. 2014. The Big Picture of Internet -Project. Kotka: Kaakkois-Suomen ammattikorkeakoulu. PDF-dokumentti. Saatavissa: https://www.ict-lab.fi/images/tietoverkkotekniikka/tekstit/BIG_PICTURE_OF_INTERNET_peda.pdf [viitattu 19.3.2019].

Minei, I. & Lucek, J. 2008. MPLS-Enabled Applications – Emerging Developments and New Technologies. Toinen painos. Chichester, West Sussex: John Wiley & Sons.

Northcutt, S., Zeltser, L., Winters, S., Kent, K. & Ritchey, R. 2005. Inside Network Perimeter Security, Second Edition. E-Kirja. Saatavissa: https://learning.oreilly.com [viitattu 18.4.2019].

MPLS Applications User Guide. 2021. Sunnyvale: Juniper Networks, Inc. PDF-dokumentti. Saatavissa: https://www.juniper.net/documentation/us/en/software/junos/mpls/mpls.pdf [viitattu 29.4.2021].

Routing Policies, Firewall Filters, and Traffic Policers Feature Guide. 2019. Sunnyvale: Juniper Networks, Inc. PDF-dokumentti. Päivitetty 3.4.2019. Saatavissa: https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-policy/config-guide-policy.pdf [viitattu 17.4.2019].

Stewart, J. 2014. Network Security, Firewalls and VPNs. Toinen painos. Burlington: Jones & Bartlett Learning.

Tam, K., Salvador, M., McAlpine, K., Basile, R., Matsugu, B. & More, J. 2013. UTM Security with Fortinet – Mastering FortiOS. Waltham, MA: Elsevier, Inc.

Telecommunication Engineering Center s.a. White paper on Deep Packet Inspection. PDF-dokumentti. Saatavissa: http://tec.gov.in/pdf/Studypaper/White%20paper%20on%20DPI.pdf [viitattu 24.4.2019].

Thompson-Melanson, J. 2015. Learn About Firewall Evolution from Packet Filter to Next Generation. PDF-dokumentti. Päivitetty tammikuu 2015. Saatavissa: https://www.juniper.net/documentation/en_US/learn-about/LA_FIrewallEvolution.pdf [viitattu 15.4.2019].

Wilkins, S. 2013. Stateful Firewall Fundamentals: A Better, Easier, More Secure Firewall. WWW-artikkeli. Saatavissa: https://www.pluralsight.com/blog/it-ops/stateful-firewall-fundamentals [viitattu 17.4.2019].

Young, G. & D'Hoinne, J. 2017. Hype Cycle for Threat-Facing Technologies, 2017. PDF-dokumentti. Saatavissa: https://www.gartner.com/en/documents/3762274 [viitattu 30.4.2019].