jamk.fi

Kuormantasausjärjestelmien vertailu

Mikko Lehtomäki

Opinnäytetyö
Maaliskuu 2017
Tekniikan ja liikenteen ala
Insinööri (AMK), Tietotekniikan koulutusohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Lehtomäki, Mikko	Opinnäytetyö, AMK	Maaliskuu 2017
	Sivumäärä 41 + 3	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Kuormantasausjärjestelmien vertailu

Tutkinto-ohjelma
Tietotekniikan koulutusohjelma

Työn ohjaaja(t)
Juha Jokinen, Sampo Kotikoski

Toimeksiantaja(t)
Suomen Erillisverkot Oy
Henri Tikkanen

Tiivistelmä

Opinnäytetyön toimeksiantajana oli Suomen Erillisverkot Oy. Erillisverkot tuottaa ICT-palveluita viranomaisille ja huoltovarmuuskriittisille toimijoille. Liikenne- ja käyttäjämäärän noustessa myös Erillisverkoille oli tullut tarve miettiä kuormantasausvaihtoehtoja tuleviin ja nykyisiin palveluihin.

Työn tavoitteena oli toteuttaa kuormantasaajien vertailu kahdessa ennalta määritetyssä käyttötapauksessa. Vertailu toteutettiin kolmen erilaisen kuormantasaajajärjestelmän (F5, HAProxy ja NetScaler) välillä toimeksiantajan pyynnöstä. Kuormantasauksen lisäksi järjestelemiltä vaadittiin tiettyjä ominaisuuksia kuten sovellussuojaus, palomuuraus ja SSL VPN.

Opinnäytetyö toteutettiin vertailemalla ominaisuuksia ja testaamalla järjestelmiä. Testaaminen suoritettiin virtuaaliympäristössä laitteiden puuttumisen vuoksi.

Tuloksena vertailusta saatiin jokaisen kuormantasausjärjestelmän hyvät ja huonot puolet molemmille käyttötapauksille. Tulosten pohjalta toimeksiantaja voi tulevissa hankkeissaan miettiä sopivan ratkaisun kyseisiin projekteihin vertailua hyödyntäen.

Avainsanat (asiasanat)
Kuormantasausjärjestelmä, F5, HAProxy, NetScaler, Erillisverkot

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Lehtomäki, Mikko	Bachelor's thesis	March 2017
		Language of publication: Finnish
	Number of pages 41 + 3	Permission for web publication: x

Title of publication
Comparison of load balancing systems

Degree programme
Information Technology

Supervisor(s)
Juha Jokinen, Sampo Kotikoski

Assigned by
Suomen Erillisverkot Oy
Henri Tikkanen

Abstract

The bachelor's thesis was assigned by State Security Networks Group. State Security Networks Group provides secure and reliable ICT services for public authorities and other critical operators of national security. The amount of traffic and users has been increasing enormously, which why State Security Networks Group had to think about load balancing for their current and future projects.

The goal of the thesis was to compare three load balancing systems in two use cases. The load balancing systems were F5 Networks, HAProxy and Citrix NetScaler. Besides load balancing, the required features included DoS protection, firewall and SSL VPN.

The thesis was carried out by comparing features and testing load balancing systems. All testing was conducted in a virtual environment due to the lack of devices.

The outcome of the thesis presents the advantages and disadvantages of chosen load balancing system in both use cases. Based on the results, the assigner can use this comparison to help them with their choices in future projects.

Keywords/tags (subjects)
Load balancing system, F5, HAProxy, NetScaler, State Security Networks Group

Miscellaneous

Sisältö

Kuviot

Taulukot

Lyhenteet

ADC	Application Delivery Controller
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
HAProxy	High Availability Proxy
ISO	International Organization for Standardization
MAS	Management and Analytics System
NAT	Network Address Translation
OSI	Open Systems Interconnection
SD-WAN	Software Defined Wide Area Network
SSL	Secure Sockets Layer
SSO	Single Sign-on
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
Virve	Viranomaisverkko
VPN	Virtual Private Network
WAF	Web application firewall

1 Johdanto

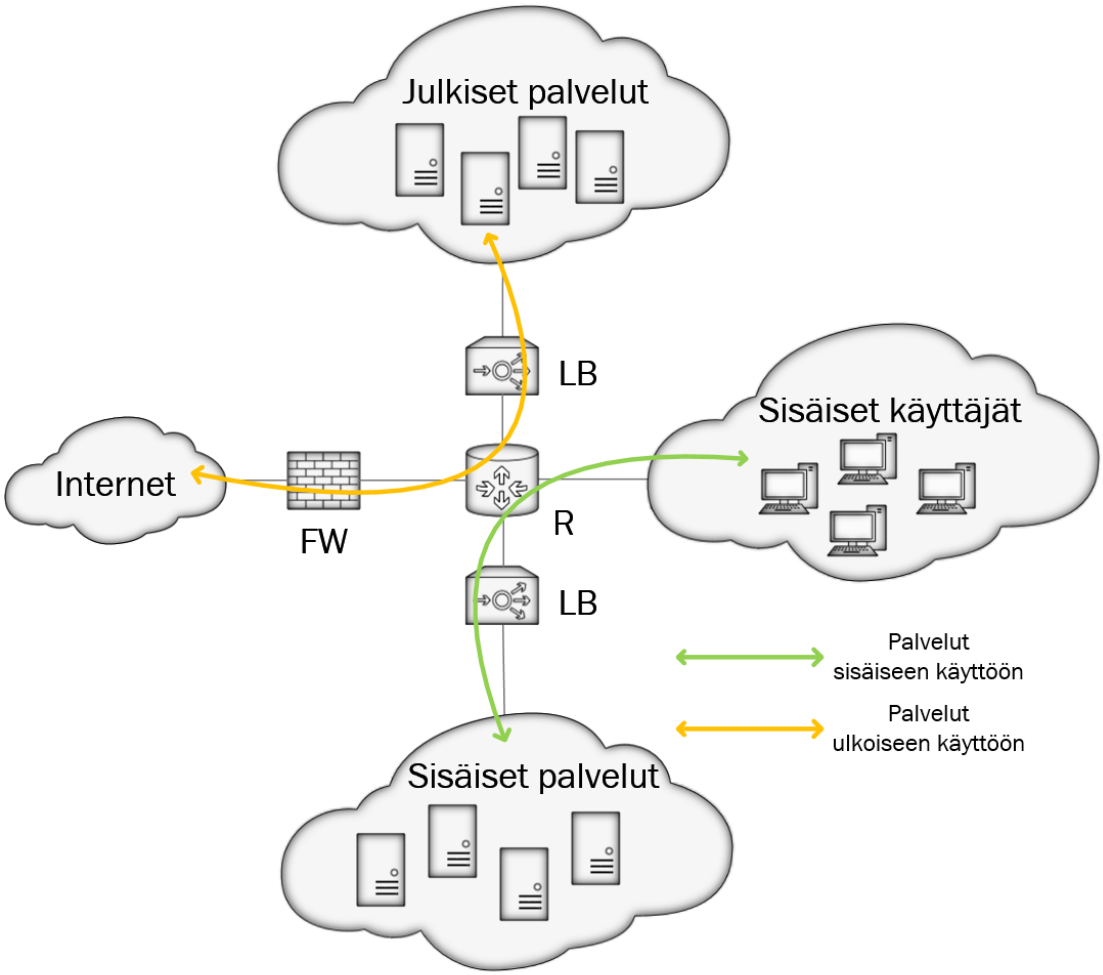
1.1 Toimeksiantaja

Opinnäytetyössä toimeksiantaja toimi Suomen Erillisverkot Oy. Erillisverkot on sataprosenttisesti Suomen valtion omistuksessa oleva yritys, joka tuottaa viranomaisille toimintavarmat ICT-palvelut. Erillisverkot on perustettu v.1999, vastaamaan virvanomaisverkon (Virven) toiminnasta. Virve otettiin käyttöön maanlaajuisesti v.2002. Erillisverkkojen suurimpia asiakkaita ovat huoltovarmuuskriittiset yritykset kuten televiestintä- ja energiatoimiala, ministeriöt, pelastustoimi, poliisi, puolustusvoimat, hätäkeskuslaitokset ja sosiaali- ja terveystoimi. Erillisverkkoihin kuuluvat tytäryhtiöt VIRVE Tuotteet ja Palvelut Oy, Suomen Turvallisuusverkko Oy, Leijonaverkot Oy ja Johtotieto Oy. (Erillisverkot n.d.)

1.2 Toimeksianto ja tavoitteet

Toimeksiantona on vertailla kolmea erilaista kuormantasausjärjestelmää kahdessa erilaisessa käyttötapauksessa. Kuviossa 1 on esitetty kyseiset käyttötapaukset. Oranssilla nuolella on kuvattu ulkoverkosta tuleva liikenne käytettäville palveluille. Tilanne voidaan ajatella tavallisena web-palvelimena. Vihreä nuoli kuvaa liikennettä sisäisille palveluille. Sisäisiä palveluita ovat mm. intranet, sähköposti ja sovellukset.

Opinnäytetyön tavoitteena on selvittää eri kuormantasausjärjestelmien hyvät ja huonot puolet Erillisverkkojen määrittämiin tarpeisiin. Opinnäytetyöstä Erillisverkot saa pohjan tulevia hankintoja varten.



Kuvio 1. Kuormantasaus sisäiselle ja ulkoiselle palvelulle/palveluille

1.3 Tarpeet

Liikenne- ja käyttäjämäärän nousun vuoksi Erillisverkoille on tullut tarve kartoittaa kohtaako nykyisten ja tulevien palveluiden määritykset tulevaisuuden vaatimuksia.

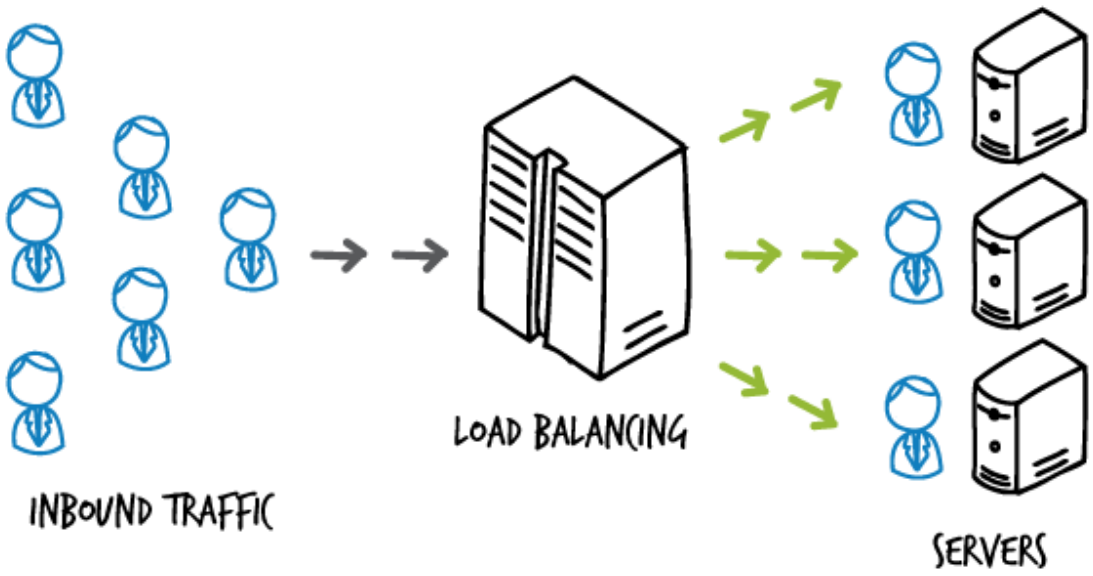
Kun asiakkaina toimivat kriittiset toimijat (esim. poliisi ja puolustusvoimat), on verkon turvallisuus taattava parhain mahdollisin keinoin.

Sen vuoksi kuormantasaajalta vaaditaan palomuurauksen lisäksi sovellussuojausta verkko- ja kuljetuskerroksessa. Sovelluskerroksen suojaus ei ole pakollista, mutta on kuitenkin suositeltavaa. Turvallisuuden lisäksi asiakkaat arvostavat korkeaa saatavuutta ja eheyttä.

Käyttäjien käsitellessä hyvin arkaluontaista materiaalia, ei tietoja voi kuljettaa selkokielisenä. Sen vuoksi SSL-salaus on vaadittu ominaisuus vertailtavilta järjestelmiltä.

2 Kuormantasaus

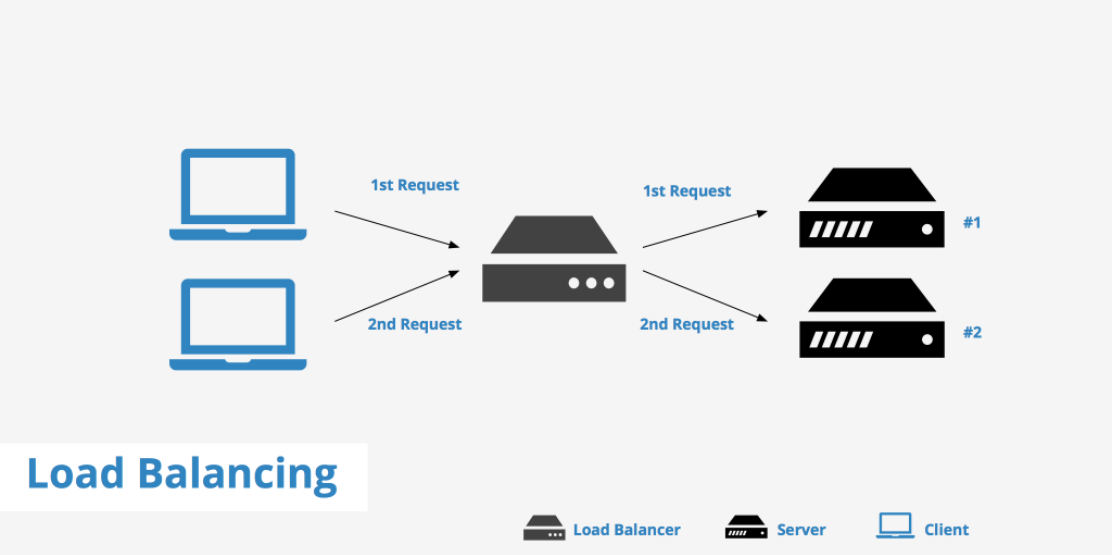
Kuormantasauksen ideana on se, että kuorma jaetaan resursseille, jolloin yksittäinen resurssi ei ylikuormitu. Kuormantasausta voidaan kuvata käyttämällä käytännön esimerkkiä postin palvelupisteestä. Kuviossa 2 postiin saapuu asiakkaita (inbound traffic), jotka ottavat yksikerrallaan vuoronumeron koneesta (load balancing). Oman vuoron tullessa valonäyttöön, siirrytään kyseiselle palvelutiskille (server) saamaan palvelua. Jos välissä ei olisi vuoronumeroja jakavaa konetta, asiakkaat jonottaisivat pahimmassa tapauksessa yhteen ainoaan palvelutiskiin, vaikka muitakin olisi vapaana.



Kuvio 2. Kuormantasaus (Broadwell 2016)

Samanlainen logiikka toimii myös verkkoliikenteen kuormantasauksessa. Liikenneryöpyn saapuessa kuormantasaajaan, se jakaa liikenteen eteenpäin määriteltyä tapaa käyttäen. Kuviossa 3 on esitetty hyvin yksinkertainen tapa verkkoliikenteen kuormantasauksesta. Liikennettä tulee kahdesta eri lähteestä, joka jaetaan kuormantasaajalta

kahdelle eri laitteelle.

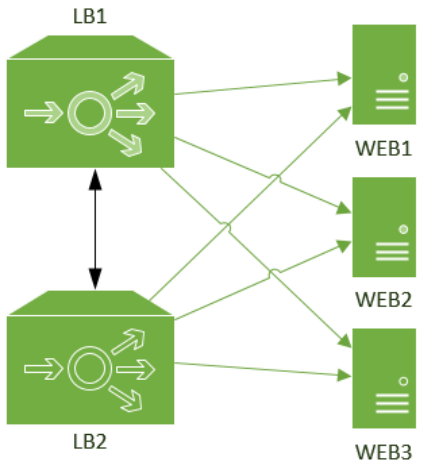


Kuvio 3. Verkkoliikenteen kuormantasaus (Load Balancing 2016)

2.1 Kuormantasaus ja klusterointi

Kuormantasaus ja klusterointi sekoitetaan usein, joten niitä on termeinä hyvä avata. Yleisenä terminä klusterilla tarkoitetaan joukkoa asioita, jotka käyttävät toistensa resursseja saavuttamaan yhteinen tavoite. Laitteet pitävät toisensa ajan tasalla omasta tilastaan, jotta vikatilanteissa liikenne voidaan ohjata toimivalle laitteelle. Klusterointia käytetään esimerkiksi web-palvelimissa, jotta verkkosivujen käytettävyys ei laske yhden palvelimen vikaantuessa. Klusterointia käytetään myös paljon datan säilyttämisessä sekä tietokoneiden yhdistämisessä.

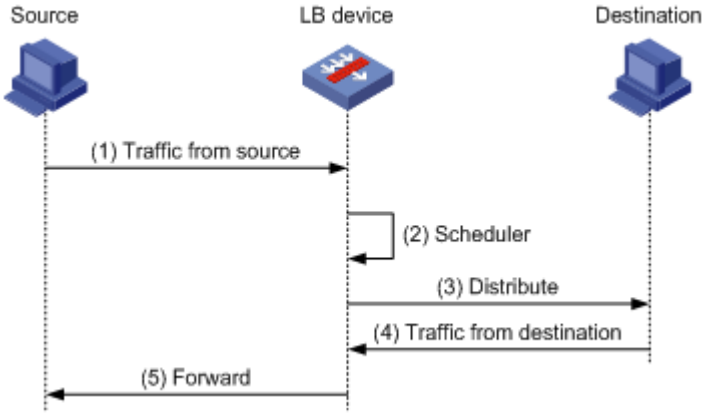
Kuormantasauksen tarkoituksena on tasata kuormaa eri laitteiden/linkkien välillä. Kuviossa 4 kuormantasaus on esitetty vihreillä nuolilla ja klusterointi mustalla. Kuormantasaajat ovat klusteroituna keskenään. Eli kyseisessä tapauksessa toisen kuormantasaajan (LB1) vikaantuessa, toinen kuormantasaaja (LB2) ottaa kuormantasauksen hoitaakseen. Kuormantasausta voidaan tehdä myös ilman klusterointia, mutta se ei ole järkevää. Tällöin kuormantasaajat eivät keskustele toistensa kanssa ja molemmat pyrkivät ohjaamaan liikennettä eteenpäin. (Clustering vs. Load Balancing – What is the difference? 2009.)



Kuvio 4. Kuormantasaus ja klusterointi

2.2 Toiminta

Osa kuormantasaajan toiminnasta voidaan selittää käyttämällä esimerkkikuviota 5. Kuvion ensimmäisessä vaiheessa, lähteestä (source) tulee liikennettä kuormantasaajaan (LB device). Seuraavassa vaiheessa kuormantasaaja valitsee käytettävän linkin algoritmien perusteella. Algoritmeja käsitellään luvussa 2.2.1. Seuraavassa vaiheessa kuormantasaaja työntää liikenteen kyseiseen linkkiin vastaanottajalle. Seuraavaksi liikenne tulee takaisin vastaanottajalta kuormantasaajalle, ja se ohjaa liikenteen lähteelle.



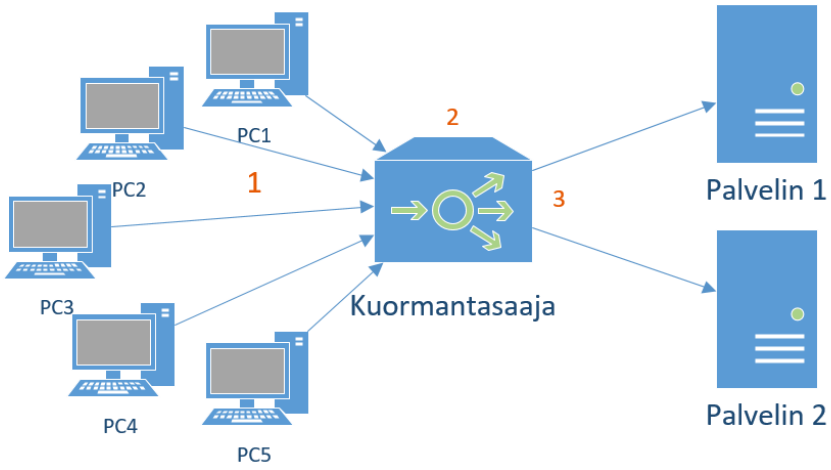
Kuvio 5. Kuormantasauksen toimintaperiaate (Load Balancing Technology White Paper n.d.)

2.2.1 Algoritmit

Kuormantasaaja tekee algoritmien perusteella päätökset, minne liikenne lähetetään. Algoritmeja on olemassa monia, mutta valitaan vertailuun kaikkien kolmen järjestelmän tukemat Round Robin ja Least Connections.

Round Robin

Round Robin on algoritmeista yksinkertaisin ja suosituin. Algoritmi jakaa yhteydet puoliksi, jolloin palvelimelle 1 tulee parittomat yhteydet (1,3,5 jne.) ja palvelimelle 2 parilliset. Esimerkiksi kuviossa 6, viisi eri tietokonetta yrittää ottaa yhteyden klusteroidulle palvelimelle, joka sijaitsee kuormantasaajan takana. Ensimmäisessä vaiheessa (punaiset numerot) tietokone pyytää yhteyttä palvelimelle. Toisessa vaiheessa kuormantasaaja tarkistaa algoritmia käyttäen, kumpaan palvelimeen yhteys välitetään. Kolmannessa vaiheessa kuormantasaaja välittää liikenteen valitulle palvelimelle. Seuraavan yhteyden saapuessa kuormantasaaja valitsee toisen palvelimen. Kolmas yhteys yhdistetään taas palvelimelle 1. Loppujen lopuksi Palvelin 1 hoitaa yhteyden PC1:lle, PC3:lle ja PC5:lle. Palvelin 2 hoitaa PC2:n ja PC4:n.



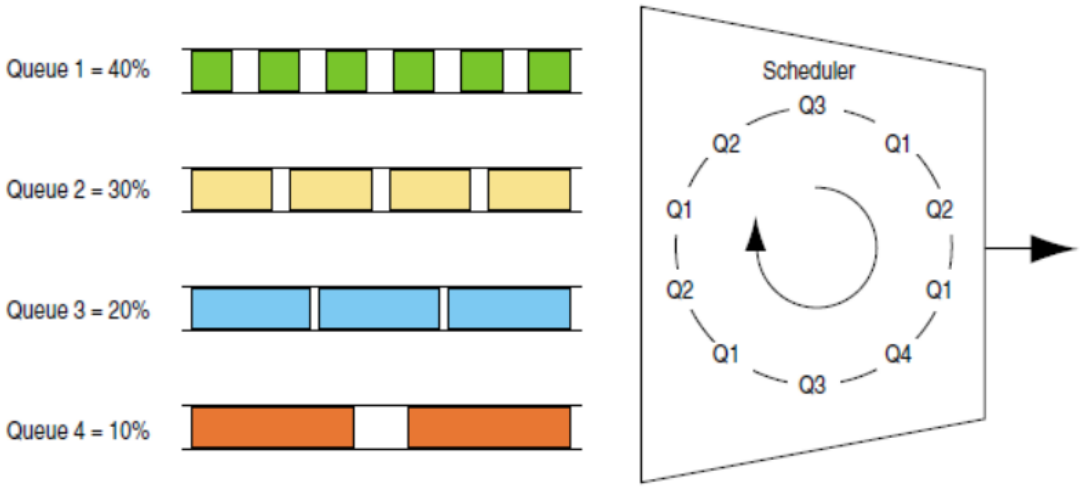
Kuvio 6. Round Robin (Managed File Transfer and Network Solutions 2015)

Nopeasti ajateltuna Round Robin on tehokas algoritmi, mutta liikenteen ollessa vaihtelevaa, ei algoritmi toimi toivotulla tavalla. Jos parittomat tietokoneet lataavat suuria tiedostoja palvelimelle ja parittomat tietokoneet käyvät pyörähtämässä verkkosivuilla. Esimerkkitapauksessa palvelimella 1 on kolme yhteyttä kuormittamassa palvelinta pitkän aikaa, kun taas palvelin 2 saa olla rauhassa ilman kuormaa. Algoritmin ongelma huomataan myös, jos palvelimet ovat eri tehoisia. Algoritmin jakaessa kuormaa tasaisisesti tehottomampi palvelin saattaa kaatua raskaassa kuormassa.

Edellisessä kappaleessa kuvattuun eri tasoisia palvelimia koskevaan ongelmaan on kehitetty parempi versio Round Robinista. Painotetussa Round Robinissa (Weighted Round Robin) palvelimille määritellään painoarvo. Esimerkiksi aikaisempaa kuviota 5 käyttäen palvelimelle 1 annetaan painoarvo 4, jolloin kuormantasajaa ohjaa ensimmäiset 4 yhteyttä palvelimelle 1 ja viimeisen yhteyden palvelimelle 2. (Managed File Transfer and Network Solutions 2015.)

Painotetun Round Robin ongelma on edelleen liikenteen vaihtelevuus. Kuvion 7 vasemmassa reunassa näkyy linkkien painotus. Pakettikoko Q1:ssä 100 tavua, Q2:ssa 200 tavua, Q3:ssa 300 tavua ja Q4:ssa 400 tavua. Painoarvon vuoksi Q1 lähettää kymmenestä paketista neljä. Näin ollen kierroksen aikana Q1 käyttää 4*100 tavua = 400 tavua, Q2 3*200 tavua = 600 tavua, Q3 käyttää 2*300 = 600 tavua ja Q4 käyttää 1*400 = 400 tavua. Kokonaismääräksi tulee 2000 tavua. Tästä saadaan laskettua, että

Q1 kautta kulkee ainoastaan 20 % (400/2000) liikenteestä vaikka sen painotettu arvo on suurin. Vastaavat arvot muille: Q2 30 %, Q3 30 % ja Q4 20 %. (Saharinen 2014.)



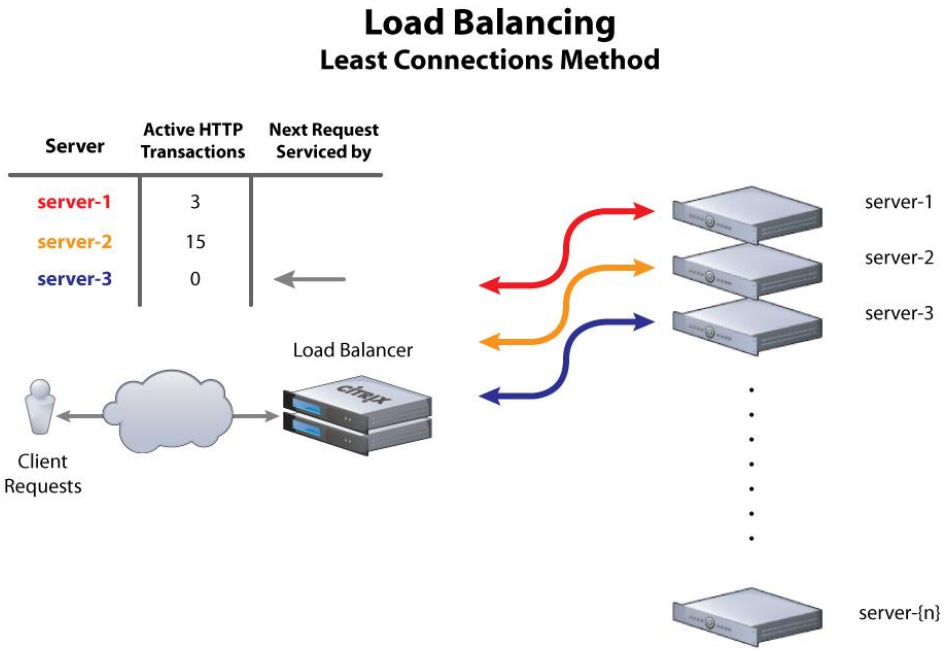
Kuvio 7. Weighted Round Robin (Saharinen 2014)

Round Robinista on kehitetty vielä kolmas algoritmi, dynaaminen Round Robin (Dynamic Round Robin). Dynaaminen Round Robin toimii painotetun Round Robinin tavoin, mutta siinä on jatkuva monitorointi päällä, joka vaihtelee painotusta reaaliaikaisesti. Painotukseen vaikuttavia asioita ovat mm. käynnissä olevat yhteydet ja palvelimen nopein vasteaika. (MacVittie 2009; What is Round-Robin load balancing? n.d.)

Least Connections

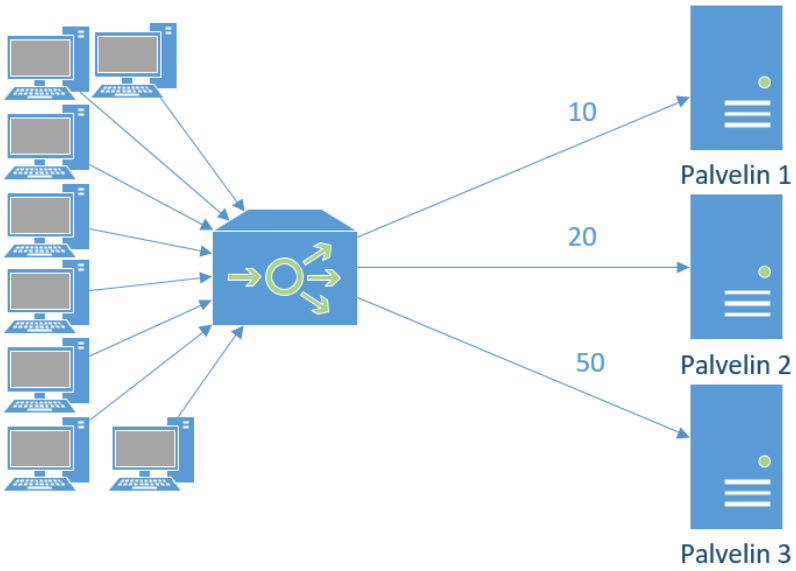
Least Connections (suom. vähiten yhteyksiä) algoritmi valitsee käytettävän yhteyden, nimensä mukaisesti, yhteyksien määrän perusteella. Se palvelin, jolla on vähiten aktiivisia yhteyksiä, saa uusimman yhteyden. Esimerkki kuviossa 8 on tilanne, jossa palvelin 1:llä on 3 aktiivista yhteyttä, palvelin 2:lla 15 ja palvelin 3:lla 0. Algoritmin mukaan seuraava muodostettava yhteys ohjataan palvelin 3:lle, koska siellä on vähiten yhteyksiä. Myös seuraavat kaksi yhteyttä muodostuvat palvelin 3:lle, jolloin palvelin 1:llä ja palvelin 3:lla on yhtä monta aktiivista yhteyttä. Seuraavat yhteydet muodoste-

taan vuorotellen palvelimien 1 ja 3 välillä. (Ellrod 2010.)



Kuvio 8. Least Connections (Ellrod 2010)

Tästäkin algoritmista on tehty painotettu versio (Weighted Least Connections). Palvelimille määritetään maksimi yhteysmäärät, joista lasketaan palvelimen käytössä oleva kapasiteetti. Kuviossa 9 kolmelle palvelimelle on annettu maksimi yhteysmäärät 10, 20 ja 50.



Kuvio 9. Weighted Least Connections

Taulukossa 1 näkyy punaisella merkattu kunkin yhteyden valittu palvelin. Ruudukon numero kertoo palvelimen käytössä olevan kapasiteetin. Kapasiteetti lasketaan jakamalla aktiiviset yhteydet maksimi yhteysmäärällä. Eli esimerkiksi neljännen yhteyden jälkeen palvelin 3:lla on 2 aktiivista yhteyttä ja maksimimäärä on 50. Laskukaavaa noudattaen tulokseksi saadaan 0,04 eli 4 prosenttia. Yhdennentoista yhteyden jälkeen palvelin 1:llä on 2 aktiivista yhteyttä ja kapasiteetista on käytössä 2/10=20 %. Palvelin 2:lla on 3 yhteyttä ja 15 % prosenttia kapasiteetin käyttö. Palvelin 3:lla, jolla oli suurin kapasiteetti, vastaavat luvut ovat 6 yhteyttä ja 12 %. (Configuring Load Balancing Pools 2004.)

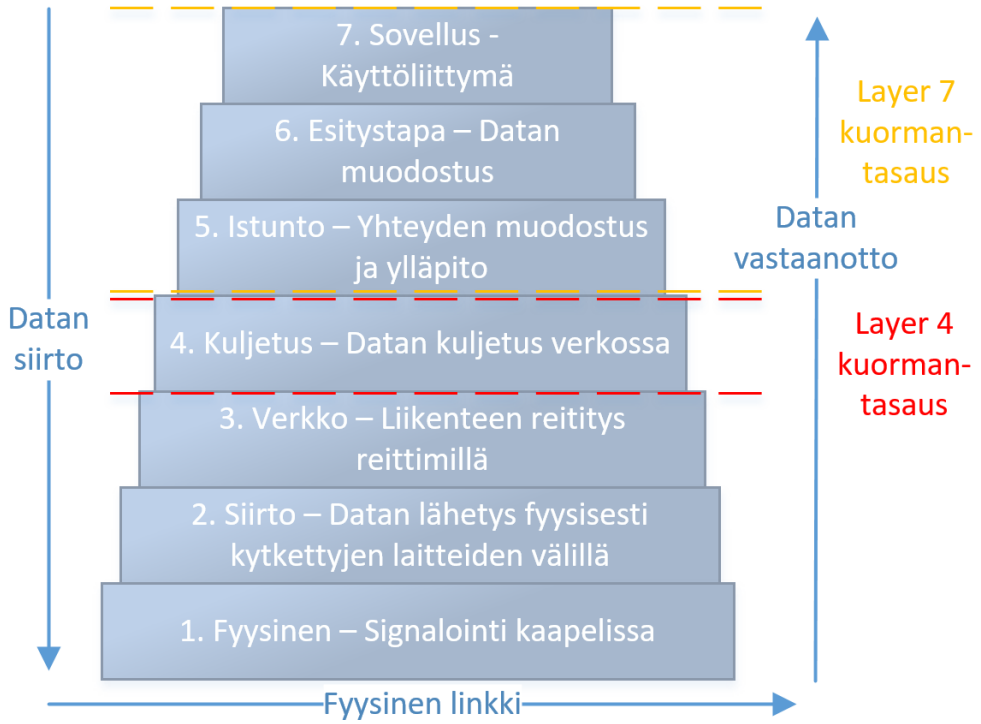
Taulukko 1. Weighted Least Connections esimerkki

Yhteydet	1	2	3	4	5	6	7	8	9	10	11
Palvelin 1	0%	0%	10%	10%	10%	10%	10%	10%	10%	10%	20%
Palvelin 2	0%	5%	5%	5%	5%	10%	10%	10%	10%	15%	15%
Palvelin 3	2%	2%	2%	4%	6%	6%	8%	10%	12%	12%	12%

Least Connections algoritmin ongelma on sama kuin Round Robinissa. Vaikka yhteydet jakautuisivatkin tasaisesti tai halutun mukaisesti, eivät liikennemäärät välttämättä ole siltikään tasaiset. (MacVittie 2013.)

2.2.2 Kuormantasaus eri OSI-mallin kerroksissa

OSI-malli on kansainvälisen standardijärjestön (ISO, International Organization for Standardization) kehittämä malli, jolla kuvataan tietokoneiden välistä kommunikaatiota. Mallissa on 7 kerrosta, joista kuormantasaukseen käytetään kahta kerrosta. OSI-malli ja kerrosten tehtävät on esitetty kuviossa 10.



Kuvio 10. Kuormantasaus OSI-mallin kerroksissa (Miller 2013; Load Balancing Layer 4 and Layer 7 n.d.)

Kuljetuskerroksessa tapahtuvaa kuormantasausta kutsutaan layer 4 kuormantasaukseksi. Layer 4 kuormantasaus on yleisempi ja yksinkertaisempi vaihtoehto kahdesta mahdollisesta. Kyseisessä tapauksessa kuormaa tasataan IP-osoitteiden ja tietoliikenneprotokolla (TCP/UDP) porttien perusteella ja liikenne käsitellään paketti paketilta. Layer 4 kuormantasaus ei tarkista paketin sisältöä, jonka vuoksi kuorman-

tasaus hoituu nopeasti. (What Is Layer 4 Load Balancing? n.d.; Load balancing Frequently Asked Questions n.d.)

Kuormantasausta voidaan tehdä myös sovellustasolla. Layer 7 kuormantasaus käyttää istunto-, esitystapa ja sovelluskerrosta. Layer 7 kuormantasaus tekee kuormantasauspäätökset käyttäen tietoa IP-osoitteista, tietoliikenneprotokollaporteista ja sovelluksista. Kun layer 4 kuormantasauksessa kuorma käydään läpi paketti paketilta, layer 7 kuormantasaus ylläpitää yhteyttä clientin ja palvelimen välillä, eli se toimii ikään kuin välityspalvelimena (proxy). Koko yhteyden ajan, client asioi saman palvelimen kanssa. (What Is Layer 7 Load Balancing? n.d.; Load balancing Frequently Asked Questions n.d.)

2.3 Hyödyt

Kuormantasaajasta on paljon hyötyä yritykselle. Kolme isointa kuormantasaajan tuomaa etua ovat skaalautuvuus, korkea saatavuus ja hallittavuus.

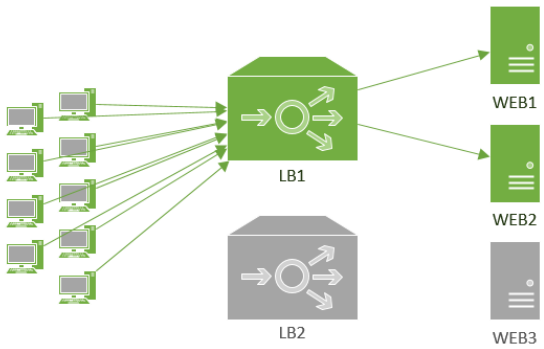
2.3.1 Skaalautuvuus

Kuormantasaaja tuo skaalautuvuutta koko järjestelmälle. Jos esimerkiksi virtuaaliseen web-palvelimeen tarvitsee lisää suorituskykyä, voidaan nykyinen palvelin kloonata toiseksi virtuaalipalvelimeksi. Tässä tapauksessa kuormantasaajalle määritettäisiin pooli (eli kokoelma palvelimia), johon molemmat virtuaalipalvelimet tulisivat. Kuormantasaajan avulla yhdellä virtuaalipalvelimella ollut liikenne voidaan jakaa kahdelle (tai useammalle) virtuaalipalvelimelle. Sama onnistuu myös fyysisellä web-palvelimella, tosin siinä tapauksessa joutuisi hankkimaan toisen fyysisen palvelimen. (Pronickin 2011; Sales 2014.)

2.3.2 Korkea saatavuus

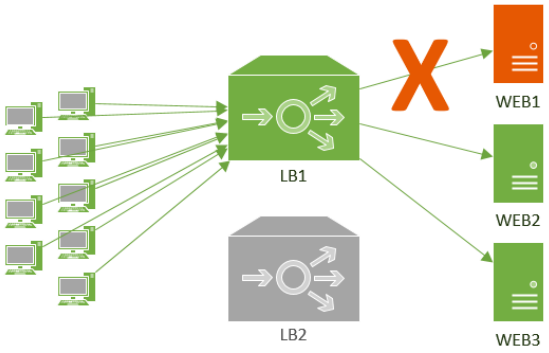
Kuormantasaajan avulla voidaan saavuttaa korkea saatavuus, varsinkin jos käytössä on useampi kuormantasaaja mahdollisten vikatilanteiden vuoksi. Kuviossa 11 on kuvattu kuormantasaajan toimintaa normaali tilanteessa. Yleensä kaksi kuormantasaajaa toimii aktiivinen(active)/valmiustila(standby) menetelmällä. Eli ainoastaan toinen laite hoitaa kuormaa eteenpäin palvelimille ja toinen on valmiustilassa. Kuorman

ollessa vähäistä kaikki takana olevat palvelimetkaan eivät ole käytössä. (Pronickin 2011; Sales 2014.)



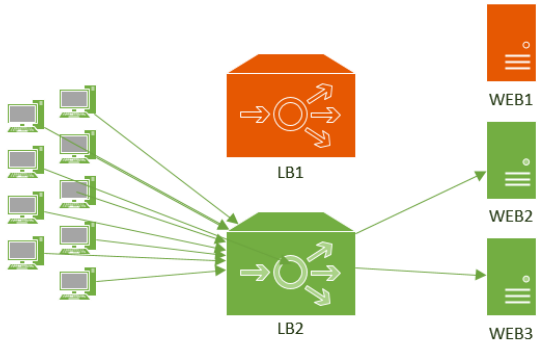
Kuvio 11. Kuormantasaajan normaali tilanne

Kuviossa 12 WEB1-palvelimessa ilmenee vikatilanne, jolloin kuormantasaaja välittömästi lakkaa välittämästä liikennettä kyseiselle palvelimelle. Liikenne siirretään muille toiminnassa oleville palvelimille.



Kuvio 12. WEB1-palvelimessa vikatilanne

Kuviossa 13 sekä kuormantasaajassa että WEB1-palvelimessa ilmenee vikatilanne. Tässä tapauksessa valmiustilassa ollut kuormantasaaja LB2 ottaa aktiivisen kuormantasaajan roolin. Kuormantasaaja pystyy vaihtamaan nopeasti aktiiviseen tilaan, jolloin tavallisessa käytössä katkoa ei huomaa laisinkaan. Kyseinen verkko kestäisi yhden kuormantasaajan ja kahden WEB-palvelimen hajoamisen ilman merkittävää asiakasvaikutusta.



Kuvio 13. Kuormantasaajassa LB1 ja WEB1-palvelimessa vikatilanne

2.3.3 Hallittavuus

Kahden kuormantasaajan ratkaisussa hallittavuus on omaa luokkaansa. Esimerkiksi laitteita huollettaessa tai päivitettäessä valmiustilassa olevalle kuormantasaajalle tehdään tarvittavat toimenpiteet ja varmistetaan laitteen toiminta. Tämän jälkeen vaihdetaan kyseinen laite aktiiviseksi, minkä jälkeen aiemmin aktiivisena olleelle laitteelle voidaan tehdä samat toimenpiteet. Tällöin laitteiden takana ollut palvelu on koko ajan käytössä ilman palvelukatkoksia. (Pronickin 2011; Sales 2014.)

3 Ominaisuudet

Kuormantasausta pystytään tekemään esimerkiksi reitittimellä, mutta kuormantasaukseen dedikoitu laite pystyy paljon muuhunkin kuin pelkästään kuormantasaukseen. Seuraavissa luvuissa paneudutaan kuormantasaajan tärkeimpiin lisäominaisuuksiin.

3.1 DoS

Nykypäivänä sovellussuojaus on todella tärkeää kasvavien hyökkäysmäärien vuoksi. DoS-hyökkäys (Denial of Service) tarkoittaa palvelunestohyökkäystä. Dos-hyökkäyksessä käytetään yksittäistä tietokonetta ja tarkoituksena on kaataa tietty palvelu/palvelin. DoS-hyökkäyksessä pyritään hyödyntämään sovelluksien haavoittu-

vuuksia tai aiheuttamalla ”tulvaa” (flood) palvelimelle, jolloin palvelimen resurssit loppuvat kesken. DoS-hyökkäyksestä kehittyneempi versio on DDoS (Distributed Denial of Service), joka tarkoittaa hajautettua palvelunestohyökkäystä. Hajautetussa palvelunestohyökkäyksessä hyökkääjät käyttävät monia eri uniikkeja IP-osoitteita (kaapattuja laitteita), joista luodaan liikennettä palvelun kaatamiseksi. Voimakkaimmissa DDoS-hyökkäyksissä liikennemäärät ovat olleet yli 1 Tbps ja kaapattuja laitteita on ollut 150 000 kpl. Kyseisellä liikennemäärällä saadaan kaadettua mikä tahansa palvelin. (Goncharov 2012; Khandelwal 2016; Woolf 2016.)

3.1.1 Layer 3 ja 4

Sovellussuojausta voidaan tehdä kolmella eri OSI-mallin kerroksella: 3 verkko-, 4 kuljetus- ja 7 sovelluskerros. Hyökkäykset kohdistuvat yleensä verkko- ja kuljetuskerrokseen. Kyseisellä hyökkäyksellä pyritään tukkimaan verkon kapasiteetti tai ylikuormittamaan laitetta.

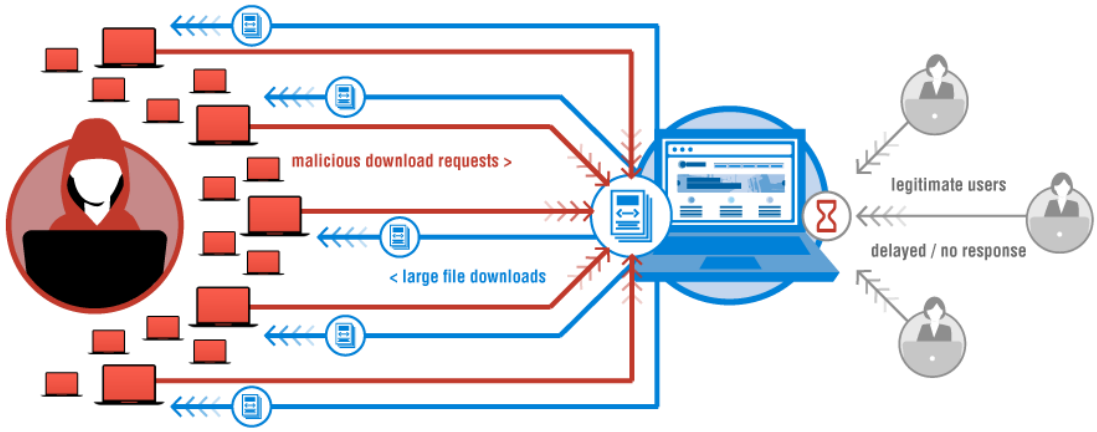
Layer 3 ja 4 hyökkäyksiä ovat mm. SYN- ja ICMP-tulva. SYN-tulvassa hyödynnetään TCP-yhteyden muodostuksessa käytettävää kolmen viestin sarjaa. TCP-yhteys muodostuu niin, että client lähettää SYN-paketin palvelimelle, johon palvelin vastaa SYN ACK. Client lähettää vielä ACK-kuittauksen palvelimelle, minkä jälkeen yhteys on muodostettu. SYN-tulvassa client lähettää ainoastaan SYN-paketteja palvelimelle eikä välitä palvelimen vastauksista. Tällöin palvelin jää odottamaan clientiltä tulevaa ACK-kuittausta. Yhteyksiä on rajoitettu määrä palvelimella, eli kun yhteysmäärä on täynnä, ei palvelin käsittele uusia yhteyspyyntöjä laisinkaan. (MacVittie 2008.)

3.1.2 Layer 7

Sovelluskerroksen DDoS-hyökkäyksiä on vaikeampi huomata, koska hyökkäys voidaan tehdä esimerkiksi yrityksen verkkosivuilla olevaan elementtiin. Elementtiin piilotetun koodin avulla verkkoa/palvelinta kuormitetaan käyttäjän huomaamatta. Hyökkäystä ei välttämättä myöskään erota piikkinä liikennemäärissä, mikä myös vaikeuttaa hyökkäyksen huomaamista. (Kaczmarek 2016; Kostadinov 2013; Miller 2013.)

Hyökkäyksen havaitsemisesta tekee vaikean myös se, että siinä yleensä käytetään HTTP GET -pyyntöä, joka taas vaatii muodostetun TCP-yhteyden. Muodostettu/hyväksytty TCP-yhteys tarkoittaa sitä, että hyökkääjän liikenne vaikuttaa normaa-

lilta liikenteeltä palvelimelle. Kun hyökkääjä rupeaa pyytämän suuria tiedostoja, palvelimen resurssit kuluvat siihen, eivätkä oikeat käyttäjät pysty käyttämään palvelua. HTTP GET -hyökkäys on esitetty kuviossa 14. (MacVittie 2008.)

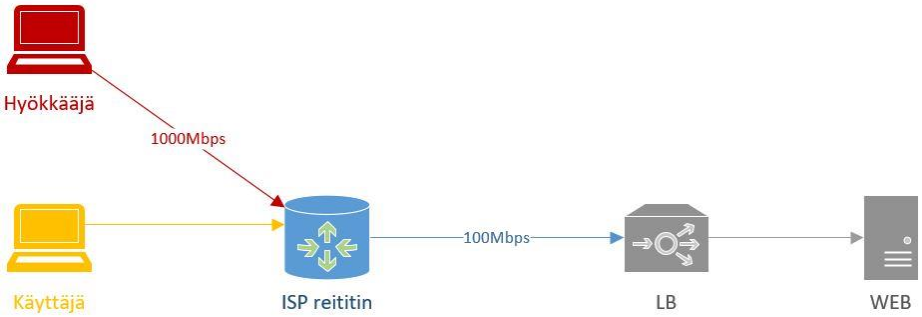


Kuvio 14. HTTP GET -hyökkäys (HTTP Flood Attack n.d.)

3.1.3 Suojautuminen

Layer 4-hyökkäyksien havaitseminen on helppoa kasvavien yhteysmäärien vuoksi. SYN-tulvahyökkäykset voidaan estää käyttämällä SYN-evästeitä (cookie). Laite lähettää evästeen kaikille TCP-yhteyttä muodostaville, mutta ei jätä kyseisiä yhteyksiä auki. Tässä tapauksessa palvelimelle jää resursseja, mutta se ei kuitenkaan estä verkkoyhteyden tukkimista. (Layer 3-4 SYN Denial-of-Service Protection 2012.) Layer 7-hyökkäyksiltä on paljon vaikeampi suojautua. Liikennettä on osattava tulkita ja tehtävä johtopäätös, johtuuko suuri liikennemäärä suosiosta vai DDoS-hyökkäyksestä. Hyökkäyksiltä voidaan suojautua osittain rajoittamalla mm. TCP-, UDP- ja ICMP-pakettien määrää. Jos hyökkääjä lähettää liikennettä yli kapasiteetin verran, menee verkko tukkoon rajoituksista huolimatta. (DDoS Protection n.d.; The Top 10 DDoS Attack Trends 2015.)

Kuviossa 15 on esitetty tilanne, jossa yrityksellä on käytössä 100 Mbps yhteys operaattorilta ja hyökkääjä luo liikennettä 10-kertaisen määrän. Normaaleille käyttäjillä (keltaisella merkitty) hyökkäys ilmenee hitaana tai estyneenä palveluna.



Kuvio 15. DDoS-hyökkäys

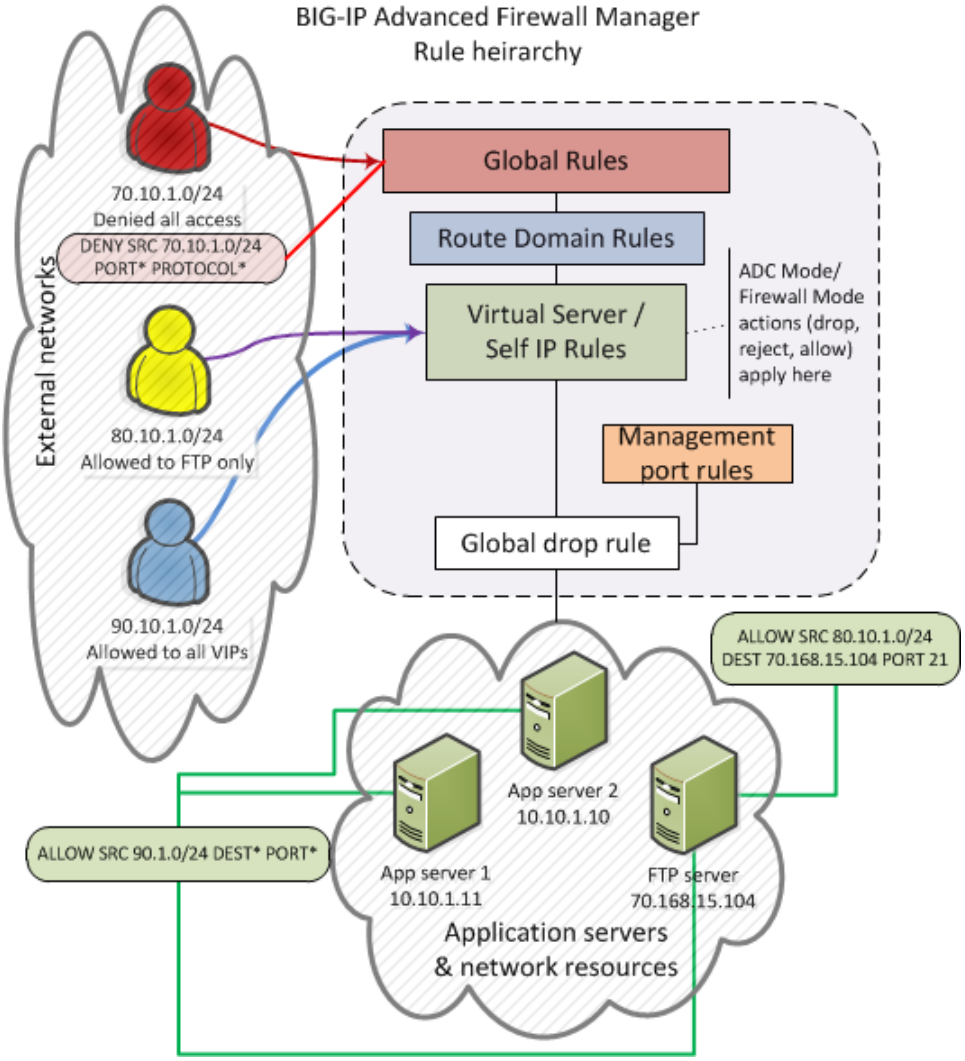
Jos suojautumista ei halua tehdä itse, onnistuu sen ostaminen operaattorilta tai yritykseltä. Suojatumista voidaan myös tehdä peilaamalla liikenne operaattorin tai jonkin yrityksen palveluun, joka tarkistaa kaiken liikenteen ennen sen ohjautumista yrityksen verkkoon. Palvelua tarjoavat mm. F5 Silverline DDoS Protection, Arbor ja Sonera Verkkosuoja.

3.2 Palomuuri

DDoS-suojauksen lisäksi kuormantasaajalla voidaan tehdä palomuurausta. Palomuuri sijoitetaan ”best practicen” mukaan verkon reunalle, josta se voi kontrolloida liikennettä molempiin suuntiin luontevasti. Palomuurille määriteltyjen sääntöjen perusteella se pudottaa kaiken ylimääräisen liikenteen pois ja merkitsee lokeihin pudotettujen pakettien tiedot. Palomuurin avulla saadaan myös estettyä päätelaitteiden ja sovellusten näkyvyys ulkoverkkoon. (Saharinen 2013.)

Jotta palomuurisäännöistä olisi eniten hyötyä, kannattaa säännöstö suunnitella hyvin. Paras keino on sallia kaikki tarvittava liikenne ja palvelut, minkä jälkeen estetään kaikki muut. Tässä tapauksessa verkkoon ei pääse mikään muu kuin haluttu liikenne. (Saharinen 2013.)

Kuviossa 16 on esitetty palomuurisääntöjen toimintaa. Vasemmassa ylänurkassa näkyy sääntö ”DENY SRC 70.10.1.0/24 PORT* PROTOCOL*”, joka estää kaiken liikenteen osoiteavaruudesta 70.10.1.0/24. Oikealla vihreässä laatikossa on sääntö ”ALLOW SRC 80.10.1.0/24 DEST 70.168.15.104 PORT 21”, joka sallii FTP liikenteen (portti 21) osoiteavaruudesta 80.10.1.0/24 IP-osoitteeseen 70.168.15.104.



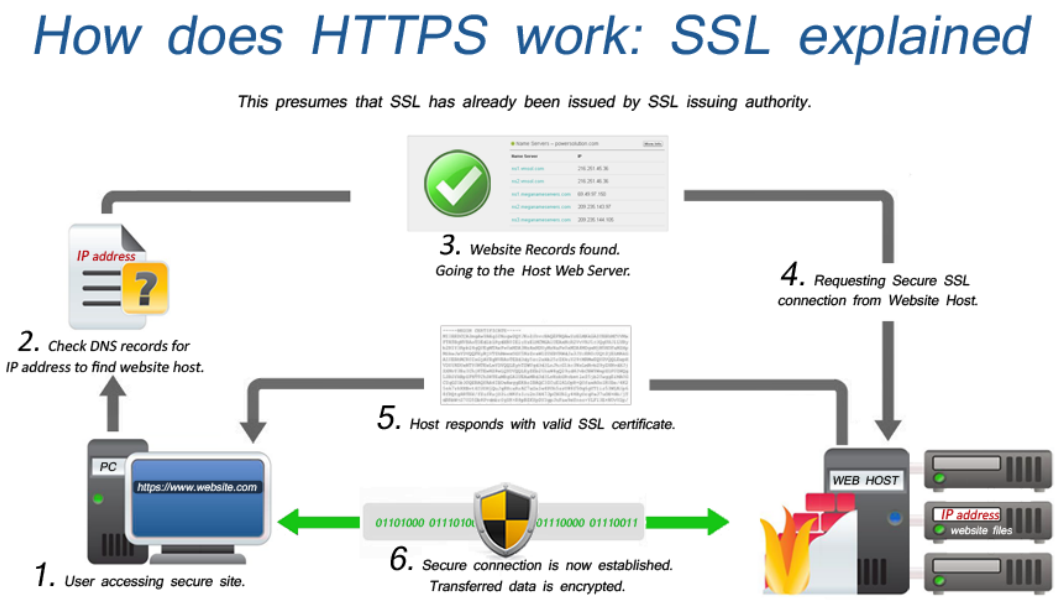
Kuvio 16. Palomuurisääntöjen toiminta (About firewall rules n.d.)

Palomuurilla voidaan estää/sallia liikenne myös maantieteellisen sijainnin perusteella. Toiminto vaatii GeoIP-tietokannan, joka sisältää tiedot IP-osoitteiden maantieteellisistä sijainneista. Ominaisuus on nykypäivänä hyödyllinen, koska esimerkiksi Lähi-idän hyökkäysmäärät ovat nousussa. Toiminnon avulla voidaan tarvittaessa estää liikenne koko Lähi-idästä. (Cyber threat in Middle East higher than global average: report 2016.)

3.3 SSL

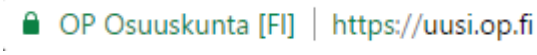
SSL:n (Secure Sockets Layer) avulla luodaan salattu yhteys clientin ja palvelin välillä, jotta tietoja voidaan siirtää turvallisesti. Ilman salausta kaikki tiedot siirtyvät selaimen

(client) ja verkkosivun (palvelin) välillä selkokielellä. Kuviosta 17 selviää, kuinka SSL toimii. Ensimmäisenä käyttäjä ottaa yhteyden jollekin sivustolle, joka käyttää SSL-suojausta. Toisessa vaiheessa tarkistetaan DNS-tietokannasta (Domain Name System) IP-osoite, jolla pyritään löytämään verkkosivun palvelin. Kolmannessa vaiheessa palvelin löytyy tietokannasta, jolta neljännessä vaiheessa pyydetään SSL-yhteyttä. Viidennessä vaiheessa palvelin lähettää SSL-sertifikaatin käyttäjälle. Käyttäjän saadessa SSL-sertifikaatin muodostetaan käyttäjän ja palvelimen välille TLS-tunneli (Transport Layer Security), jossa salattu data liikkuu. (How SSL works tutorial with HTTPS example? 2015; What is SSL n.d.)



Kuvio 17. SSL:n toiminta (How SSL works tutorial with HTTPS example? 2015.)

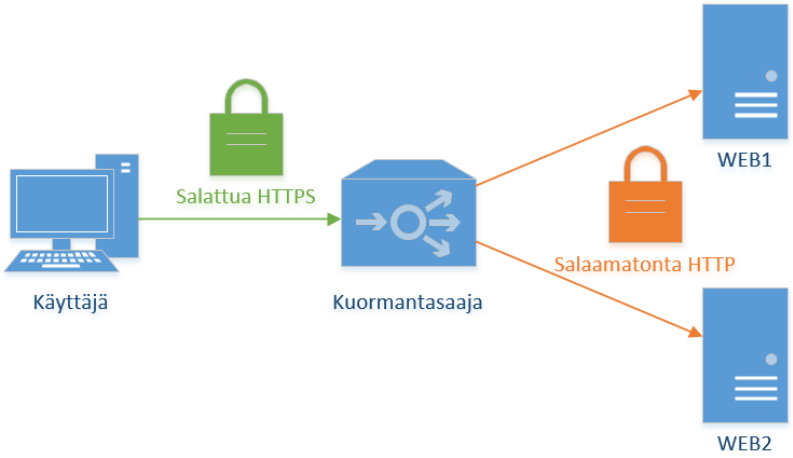
Verkkosivuilla käytössä olevan SSL-salauksen tunnistaa yleensä osoiterivillä olevasta vihreästä lukosta ja HTTPS-osoitteesta (ks. kuvio 18).



Kuvio 18. SSL-salaus käytössä

3.3.1 SSL offloading

Kun yhteyksiä on runsaasti, voi liikenteen salaaminen ja salauksen purkaminen kuormittaa web-palvelinta. Sen vuoksi on kehitetty SSL offloading, jonka avulla liikenteen salaaminen ja salauksen purkaminen voidaan suorittaa toisella laitteella. Kuviossa 19 kuormantasaaja terminoi https-liikenteen eteenpäin http-liikenteenä.



Kuvio 19. SSL offloading

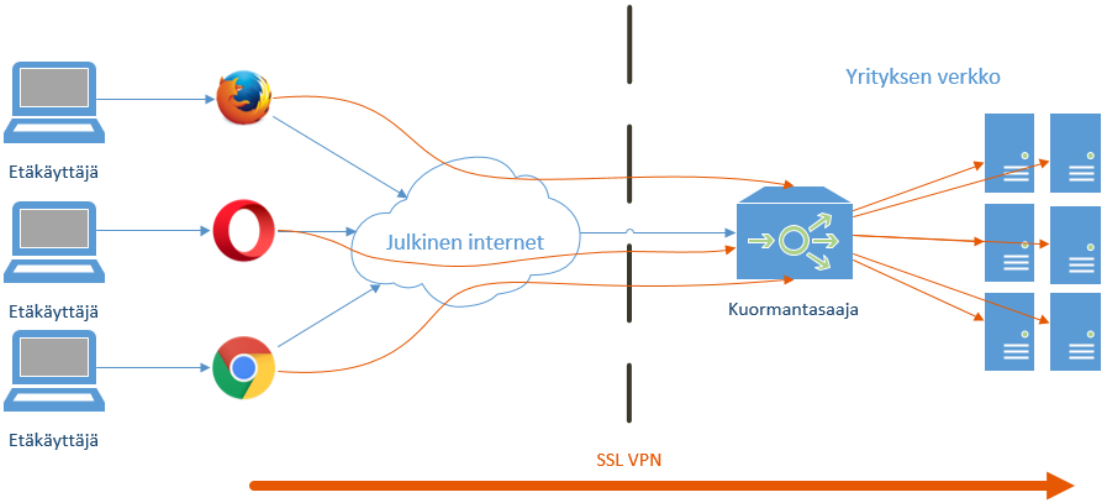
Liikennettä voidaan myös uudelleen salata palvelimille. Siinä tapauksessa liikennettä voidaan tarkastella suojaamattomassa kohdassa ja tarvittaessa uudelleenkirjoittaa otsikoita (headers).

SSL offloadingin hyödyt tulevat erillisen laitteen suorituskyvystä, joka näkyy käyttäjille mm. verkkosivujen nopeudella. Ylläpitäjälle SSL offloading voi tuoda säästöjä mm. sertifikaattien yksinkertaisella hallinnalla, kun sertifikaatit voidaan hoitaa yhdellä laitteella. (Dadighat 2015; Nelson 2014; SSL Offloading n.d.)

3.3.2 SSL VPN

SSL VPN:n (Virtual Private Network) avulla luodaan turvallinen etäyhteys julkisen verkon ylitse ilman erillisen sovelluksen asentamista koneelle. SSL VPN on hyvin yksinkertainen loppukäyttäjälle. Siihen tarvitaan vain verkkoselain ja internetyhteys. Se on ylläpitäjälle yksinkertaista, kun kaikki tarvittavat konfiguraatiot tehdään yhdelle laitteelle. Kuviossa 20 on esimerkkikuva SSL VPN:n toiminnasta. Julkisen verkon puolella

olevat käyttäjät (etäkäyttäjät) voivat esimerkiksi olla työmatkalla tai työskennellä eri paikkakunnalla. He pääsevät yrityksen verkkoon SSL VPN:n avulla, joka on terminoitu yrityksen kuormantasaajaan. Näin ollen he pystyvät käyttämään suojatun yhteyden avulla julkisen verkon puolelta yrityksen sisäisiä palveluita tms. (Kilpatrick 2007; SSL VPN n.d.; SSL VPN Security n.d.)



Kuvio 20. SSL VPN:n toiminta

SSL VPN voidaan käyttää myös koneelle asennettavan ohjelman avulla, jonka avulla saadaan yhteys entistä turvallisemmaksi. VPN clientiin voidaan keskitetysti määritellä vaatimuksia, jotka yhdistettävän koneen on läpäistävä ennen yhteyden muodostumista. Määrityksiä voivat olla esimerkiksi: käynnissä oleva viruksentorjuntaohjelma ja Windows päivitykset. (Scarfone n.d.)

4 Kuormantasausjärjestelmät

4.1 F5 Networks

F5 Networks on amerikkalainen yritys, joka on perustettu vuonna 1996. F5 hallitsee järeän luokan kuormantasaus markkinoita BIG-IP tuoteperheellään. Ylivoimasta kertoo se, että Amerikan 20 suurinta pankkia ja maailman 10 suurinta vakuutusyhtiötä luottavat F5 palveluihin. (Leadership n.d.)

4.1.1 BIG-IP tuoteperhe

F5 pystyy tarjoamaan todella laajan paketin kuormantasauksen lisäksi. BIG-IP tuoteperheen avulla ei ole enää tarvetta erillisille palomuureille, SSL VPN ratkaisuille ja sovellussuojauksille. Kaikki tämä voidaan tehdä yhdellä laitteella.

LTM Local Traffic Manager on koko järjestelmän aivot. LTM on kuormantasausjärjestelmä, johon moduulit tuovat lisäarvoa. LTM sisältää mm. SSL offloadingin ja monitoroinnin, joka tunnistaa ja estää ”pahan” liikenteen ja päästää ”hyvän” liikenteen lävitse. Järjestelmä on saatavilla laitteena, sovelluksena tai pilvipalveluna.

APM Access Policy Manager avulla käyttäjän pääsy ohjelmiin ja dataan on yksinkertaista ja turvallista. Moduuli sisältää SSO:n (single sing-on), eli ns. kertakirjautumisen, jolloin käyttäjän autentikointi tehdään vain kerran, vaikka käyttäjä käyttäisikin eri sovelluksia. Moduulissa on myös VDI-tuki (Virtual Desktop Infrastructure) Citrixille, Microsoftille ja VMwarelle.

Secure Web Gateway Services kerää tietoa verkkosivuilta ja sovelluksista, minkä jälkeen tiedot tarkistetaan haittaohjelmien varalta. Moduuli on myös yhteydessä pilvipohjaiseen järjestelmään, joka kerää tietoa havaituista haittaohjelmista ja pyrkii estämään haitat etukäteen.

ASM Application Security Manager eli WAF:n (web application firewall) avulla suojataan sovellukset ja tiedostot erilaisilta uhkilta, kuten layer 7 DDoS-hyökkäyksiltä.

AFM Advanced Firewall Manager moduuli on palomuuri, jolla suojaudutaan layer 3-4 DoS-hyökkäyksiltä.

AAM Application Acceleration Manager avulla palvelimen kapasiteettia saadaan kasvatettua n.20 % pakkaamalla lähetettävää dataa ja poistamalla TCP uudelleenlähetys.

DNS moduuli lisää entisestään suorituskykyä, turvallisuutta ja saatavuutta. DNS pystyy hoitamaan 100 miljoonaa vastausta sekunnissa. Samalla saadaan käyttöön DNSSEC (Domain Name System Security Extensions), jonka avulla voidaan varmistaa nimipalvelun (DNS) tietojen oikeellisuus.

Link Controller avulla voidaan monitoroida ja hallinnoida linkkien välejä. Järjestelmä osaa automaattisesti vaihtaa yhteyden kulkemaan toista kautta, jos järjestelmä löytää paremman reitin.

PEM Policy Enforcement Manager avulla voidaan määritellä oikeudet kullekin laitteelle. Sen tarkoituksena on helpottaa oikeuksien hallintaa kasvavien laitemäärien vuoksi.

CGNAT Carrier-Grade NAT moduuli on tehty helpottamaan siirtymistä IPv4-osoitteista IPv6-osoitteisiin. Se mahdollistaa kommunikaation IPv6-osoitteilla, mutta on myös yhteensopiva IPv4-osoitteiden kanssa. (BIG-IP Platform n.d.)

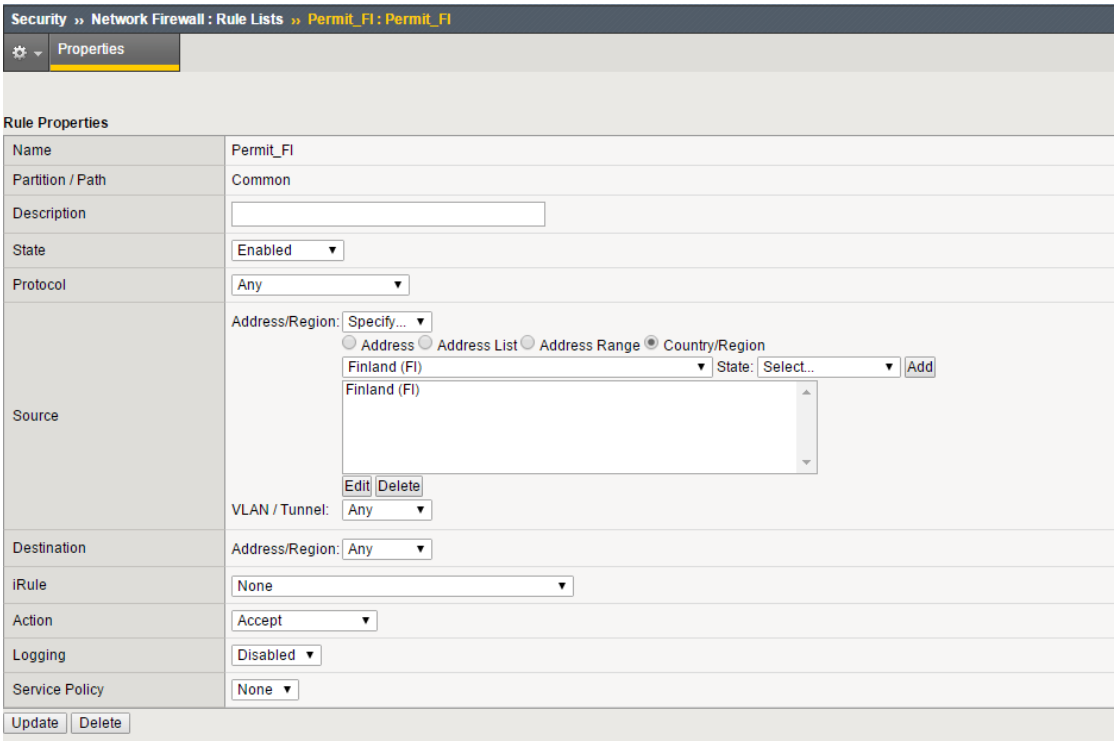
4.1.2 Muita palveluita

BIG-IP tuoteperheen lisäksi F5 tarjoaa yksittäisiä palveluita ja pienempiä kokonaisuuksia. Niistä käytetyimmät ovat BIG-IQ, joka on keskistetty laitehallinta F5-laittelle ja Herculon, joka sisältää kaksi tietoturva moduulia.

4.1.3 Asennus

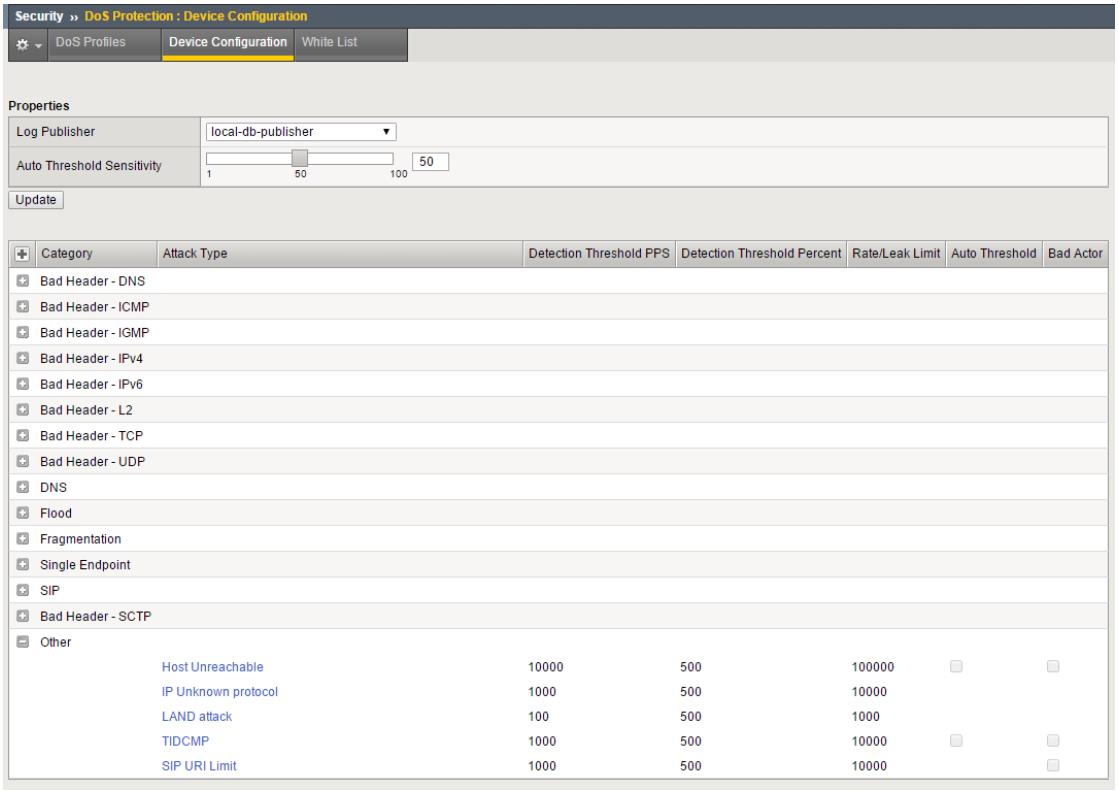
Järjestelmän asentaminen on helppoa. Liitteessä 1 on kuormantasauksen konfiguraatio. Konfiguraatiossa ollaan määritelty ”Healt Monitors” eli kuinka palvelinten toimintaa valvotaan. Kuormantasaus algoritmiksi on määritelty Round Robin. Pooliin kuuluu kolme palvelinta, joiden IP-osoitteet ovat: 1.2.3.4, 2.3.4.5 ja 3.4.5.6.

Myös erilaisten palomuurisääntöjen tekeminen on helppoa. Kuviossa 21 on määritelty sääntö ”Permit_FI”, jolla sallitaan liikenne Suomesta mihin tahansa.



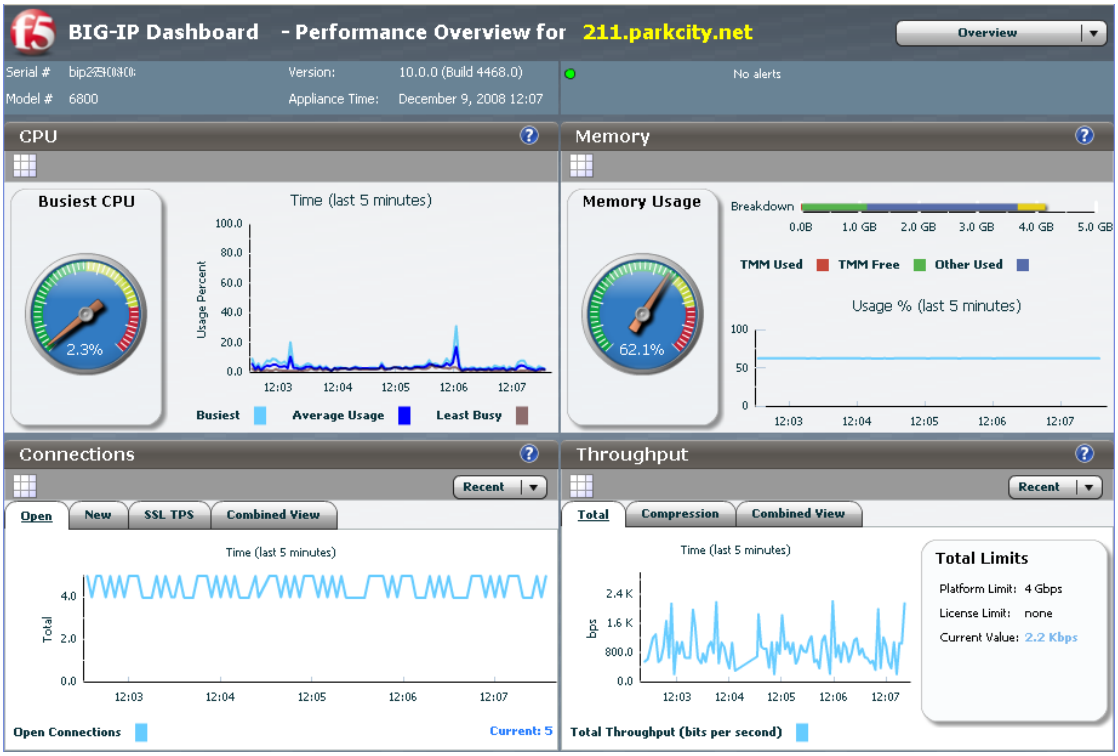
Kuvio 21. F5 IP ja maantieteellinen blacklist

Kuviossa 22 määritetään DoS-suojauksen raja-arvoja. Laitteeseen voidaan määrittää mm. TCP, UDP ja tulvan pakettimäärien raja-arvot



Kuvio 22. F5 DoS -profiilit

Laitteiden suorituskykyä ja liikenteen määrää pystyy seuraamaan suoraan yhdestä näkymästä. Näkymä on esitetty kuviossa 23.



Kuvio 23. F5 monitorointi (Monitoring the BIG-IP System n.d.)

4.2 Citrix

Citrix on kaikkien tuntema amerikkalainen IT-alan yritys, joka on perustettu jo vuonna 1989. Citrix on erikoistunut kuormantasausjärjestelmien lisäksi virtualisointiin, josta heiltä löytyvät kaikkien tuntemat järjestelmät XenApp ja XenDesktop.

4.2.1 NetScaler

Citrix NetScaler kuuluu F5:n kanssa järeämpiin kuormantasausjärjestelmiin. Molemmat tarjoavat laajan paketin kuormantasaukseen lisäksi.

NetScaler ADC (Application Delivery Controller) on NetScalerin aivot. Se hoitaa kuormantasauksen, jonka lisäksi se hoitaa CGNAT:n (vastaava kuin F5 CGNAT), DoS-suojauksen ja monitoroinnin. Se on F5:n tavoin saatavilla laitteena, sovelluksena tai pilvipalveluna.

NetScaler Unified Gateway on etäkäytön moduuli, joka on optimoitu Citrixin sovelluksille XenApp, XenDesktop ja XenMobile.

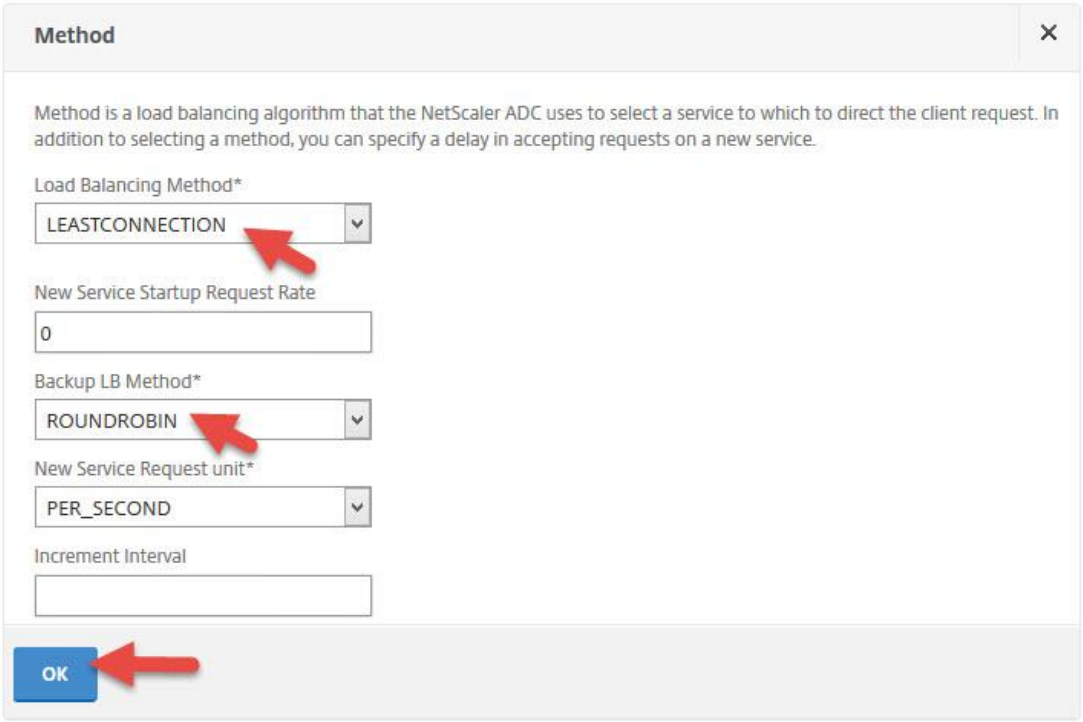
NetScaler AppFirewall (WAF) on sovellussuojain, joka puolustaa DDoS-, SSL-hyökkäyksiltä ja SQL-injektiolta.

NetScaler SD-WAN (Software Defined Wide Area Network) avulla yrityksen kallis MPLS-verkko (Multiprotocol Label Switching) voidaan korvata halvemmalla sovellus-pohjaisella ratkaisulla.

NetScaler MAS (Management and Analytics System) on hallintaan ja monitorointiin tarkoitettu keskitetty sovellus. (Networking n.d.)

4.2.2 Asennus

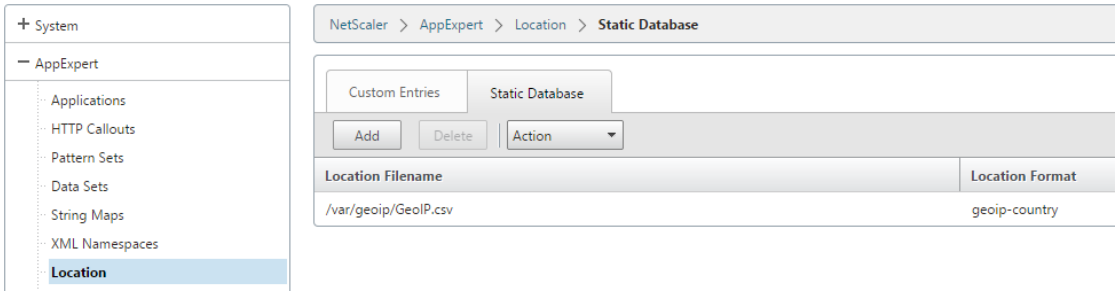
Valitettavasti NetScalerin VirtualBox asennuksessa aiheutui ongelmia, jonka vuoksi asennusta en päässyt kokeilemaan. Alla kuitenkin verkosta löytyneitä kuvia NetScalerin asennuksesta. Kuviossa 24 on esitetty algoritmin valinta.



Kuvio 24. NetScaler algoritmit (Samuel 2016)

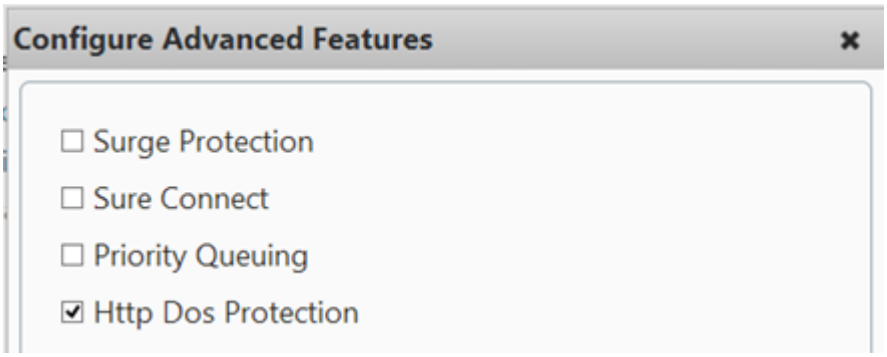
Maantieteellinen blokkaus toimii samalla tavalla kuin F5:lla. Ensin ladataan GeoIP tietokanta, joka lisätään NetScalerin tietoihin. Sen jälkeen määritetään estetyt maat.

Tietokannan lisäämisestä on esitetty kuviossa 25.



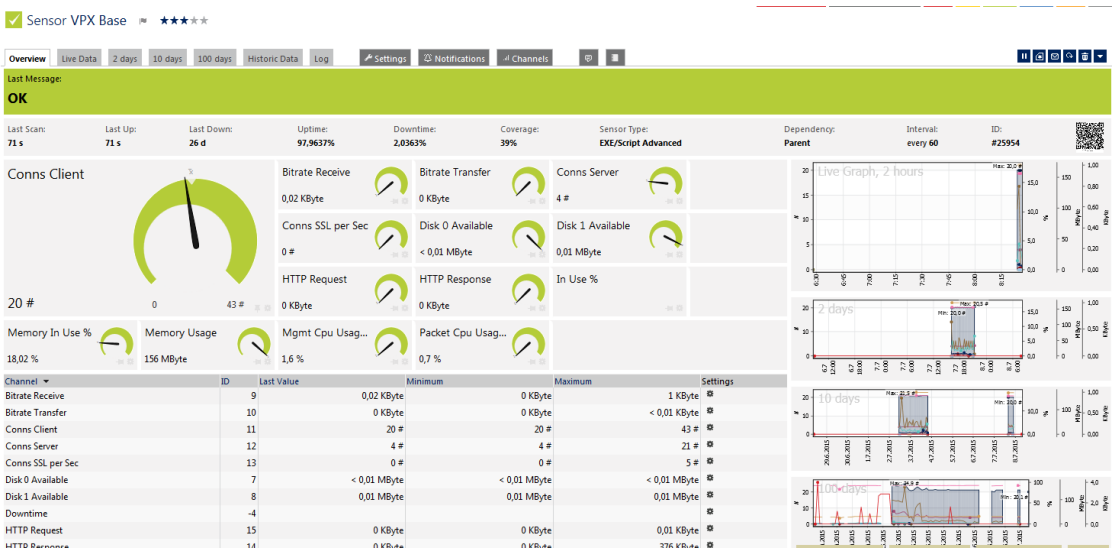
Kuvio 25. NetScaler maantieteellinen blokkaus (Smali 2014)

Myös DoS-suojaukset onnistuvat NetScalerilla. Suojaus asetukset ovat esitetty kuviossa 26.



Kuvio 26. NetScaler Dos-suojaus (Sandbu 2013)

NetScalerin monitorointi näkymä on hyvin samanlainen kuin F5:ssakin. Näkymä on esitetty kuviossa 27.



Kuvio 27. NetScaler monitorointi (Citrix NetScaler Monitoring with PRTG Plugins 2016)

4.3 HAProxy

HAProxy (High Availability Proxy) on Willy Tarreaun kehittämä sovellus vuodelta 2001, joka pystyy kuormantasauksen lisäksi toimimaan välityspalvelimena. HAProxy tukee seuraavia alustoja: Linux, Solaris, FreeBSD, OpenBSD ja AIX. (HaProxy 2017.) HAProxya käyttävät mm. Airbnb, Imgur, Instragram, Reddit, Twitter ja Vimeo. (They use it ! n.d.)

4.3.1 Asennus

HAProxya ajettiin VirtualBox:sta. Alustana järjestelmälle asennettiin Ubuntun versio 16.10. HAProxyn konfiguraatiotiedosto on esitetty liitteessä 3. HAProxyn monitorointi oli hyvin pelkistetty verkkosivu. Monitorointi on esitetty kuvioissa 28 ja 29. Kuviosta 28 nähdään, että HAProxyyn on konfiguroitu 3 palvelinta: mint1, mint2 ja mint3. Vihreä taustaväri kertoo palvelimen mint1 olevan ylhäällä. Punainen väri kertoo palvelimien olevan alhaalla.

http-back																
	Queue			Session rate			Sessions						Bytes		Denied	
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp
mint1	0	0	-	0	2		0	1	-	8	8	1m17s	2 542	9 873		0
mint2	0	0	-	0	0		0	0	-	0	0	?	0	0		0
mint3	0	0	-	0	0		0	0	-	0	0	?	0	0		0
Backend	0	0		0	2		0	1	20	8	8	1m17s	2 542	9 873	0	0

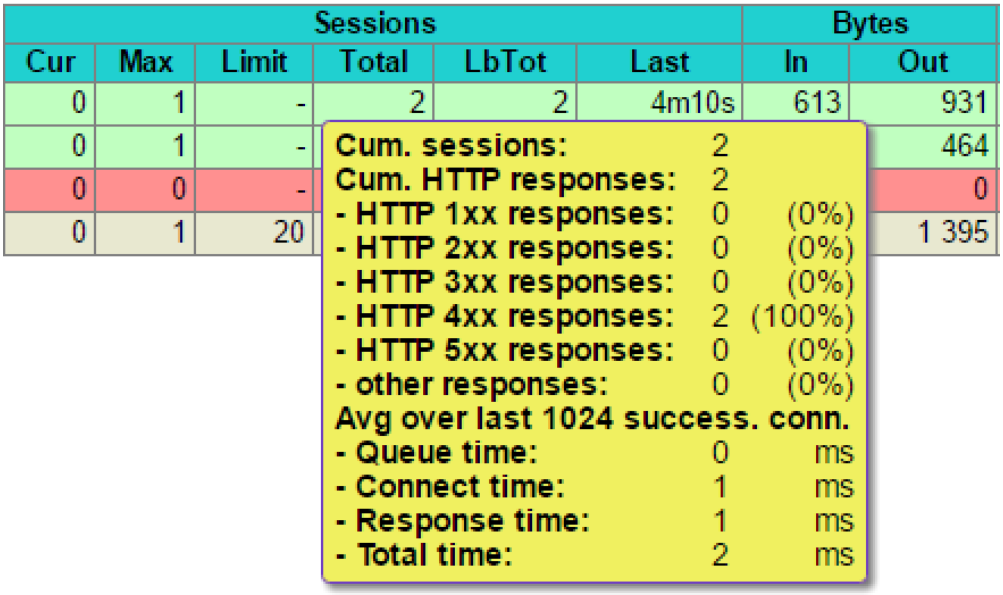
Kuvio 28. HAProxy statistiikka 1/2

Kuviosta 29 nähdään palvelinten status ja kuinka kauan laite on ollut ylhäällä/alhaalla.

Denied		Errors			Warnings		Server								
Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
	0		0	0	0	0	3m3s UP	L4OK in 1ms	1	Y	-	0	0	0s	-
	0		0	0	0	0	3m DOWN	* L4TOUT in 2001ms	1	Y	-	1	1	3m	-
	0		0	0	0	0	3m DOWN	* L4CON in 1070ms	1	Y	-	1	1	3m	-
0	0		0	0	0	0	3m3s UP		1	1	0		0	0s	

Kuvio 29. HAProxy statistiikka 2/2

Näkymästä saadaan lisätietoa, viemällä osoitin halutun kohdan päälle. Kuviossa 30 nähdään lisätietoa istunnosta.



Kuvio 30. HAProxy istuntojen tiedot

5 Yhteenveto

F5 BIG-IP ja Citrix NetScaler sisältävät samantapaisia tuotteita erilaisilla nimillä. Molemmat pystyvät tekemään toimeksiantajalle tarpeelliset palomuuraukset, sovellussuojaukset ja SSL-salaukset. Kuormantasauksen lisäksi HAProxy ei sisällä mitään vaadituista ominaisuuksista, mutta alusta, jolle sovellus asennetaan voi sisältää ominaisuudet.

5.1 F5 BIG-IP hyvät ja huonot puolet

F5 vahvuudet molemmissa käyttötapauksissa ovat ehdottomasti monipuolisuus ja tehokkuus. Järjestelmällä pystyy hoitamaan monen laitteen tehtävät. Ja kun verkosta saadaan poistettua ylimääräisiä laitteita, saadaan myös yrityksen kustannukset laskemaan. Hankintakustannusten ollessa hyvin korkeat, ei muiden kustannusten laskusta varmasti haittaa ole. Virtuaaliversioiden hinnat lähtevät liikkeelle n.7 000€/v. Kalleimmat fyysiset ratkaisut kustantavat n. 140 000€ kertamaksuna, jonka päälle tulevat vielä ylläpitokulut. Hinta tiedot on otettu AWS-palvelusta (Amazon Web Services) ja NGINX blogista (Memon 2016).

Muita kustannuksia säästäviä ominaisuuksia ovat iControls, iApps, EAVs ja viimeisimpänä iRules, jonka avulla pystytään manipuloimaan ja tutkimaan IP sovelluksien liikennettä. iRulesin avulla pystytään tekemään mm. oma tunnistautumis menetelmä SecurID tms. tilalle.

F5 ominaisuudet ovat markkinoiden parhaat, mutta se voi olla kustannuksellisesti ylimitoitettu yrityksen tarpeisiin. Ensimmäisen käyttötapauksen ollessa tavallinen web-palvelin, ei laitteen ominaisuuksista saataisi kaikkea mahdollista irti ja tällöin maksettaisiin täysin turhasta.

5.2 Citrix NetScaler hyvät ja huonot puolet

Monilla yrityksillä on ennestään käytössä muita Citrixin sovelluksia (kts. liite2). NetScalerin paras puoli on ehdottomasti Citrix sovellusten loistava tuki. NetScalerin avulla sovellusten käyttö nopeutuu huomattavasti. NetScaler on myös hieman halvempi vaihtoehto kuin F5. Netscalerin virtuaalisen platina version hinnat vaihtelevat n.9 000€ ja n.41 400€ välillä. Ainoana erona versioiden välillä on suorituskyky (throughput). Halvimassa versiossa suorituskykyä on 10 Mbps ja kalleimmassa jopa 3 000 Mbps (Citrix Store n.d.). Lähteistä riippuen järeimmät fyysiset versiot vaihtelevat 70 000€ ja 140 000€ välillä.

Jos yrityksellä ei ole käytössä Citrix sovelluksia, on NetScalerin käyttö minimaalista. NetScaler on suunniteltu käytettäväksi Citrix sovelluksia varten. Järjestelmän hankintakustannukset ovat hyvin korkeat, jonka lisäksi järjestelmä on monimutkainen asentaa ja käyttää.

5.3 HAProxy hyvät ja huonot puolet

HAProxyn hyvinä puolina ovat avoin lähdekoodi ja ilmaisuus. Järjestelmä on myös hyvin tietoturvallinen ja varmatoiminen, josta kertoo se, että vakaasta versiosta ei ole löydetty bugia 13 vuoteen. HAProxy pystyy käsittelemään istuntoja 100 000/s (prosessorina Xeon E5). Liikennemääränä samainen laite pystyy välittämään 40 Gbps. (HaProxy 2017.)

Ulkoisille palveluille HAProxy sopii todella hyvin. Jos alustan tietoturva ominaisuudet eivät riitä, voi rinnalle hankkia palomuurin tms. järjestelmän/laitteen.

HAProxyn käyttömahdollisuudet ovat rajatut vähäisten ominaisuuksien takia, jonka vuoksi se ei sovi toiseen käyttötapaukseen. Varsinkin jos käytössä olisi Citrixin sovelluksia.

6 Pohdinta

Jokaisella kuormantasausjärjestelmällä oma käyttötarkoituksena, jonka vuoksi ei ole yhtä oikeaa ratkaisua parhaan kuormantasaajan valintaan. Jos tarkoituksena on pystyttää tavallinen web-sivusto ja siihen riittävät Linuxin (tai muun alustan) tietoturva ominaisuudet, niin kannattaa mielummin valita HAProxy, kuin 100 000€ kalliimpi vaihtoehto. Jos yrityksellä on käytössä paljon Citrix sovelluksia, niin kannattaa valita kuormantasaajaksi sellainen, joka varmasti tukee kyseisiä sovelluksia. Jos yritys haluaa tietoturvallisen kokonaisuuden käyttöönsä, kannattaa valita F5.

Opinnäytetyön aihe vaikutti mielenkiintoiselta itselleni. Teoria osuuksiin aikaa käytin mielestäni sopivasti, mutta testaamiseen olisi voinut panostaa ajallisesti paljon enemmän. Sen vuoksi järjestelmien testaaminen jäi hyvin pitkälti puolitiehen. Toimeksiantajan tavoitteet kuitenkin täyttyi, joten työhön täytyy olla tyytyväinen.

Lähteet

About firewall rules. N.d. Viitattu 27.1.2017. https://support.f5.com/kb/en-us/products/big-ip-afm/manuals/product/network-firewall-policies-implementations-11-3-0/2.html

Amazon Web Services. N.d. Viitattu 12.3.2017. https://aws.amazon.com/marketplace/seller-profile?id=74d946f0-fa54-4d9f-99e8-ff3bd8eb2745

BIG-IP Platform. N.d. Viitattu 5.3.2017. https://f5.com/products/big-ip

Broadwell, T. 2016. Viitattu 16.11.2016. https://www.ctl.io/blog/post/cloud-load-balancing/

Citrix NetScaler Monitoring with PRTG Plugins. 2016. Viitattu 12.3.2017. http://www.prtgplugins.com/list-of-plugins/citrixplugins/citrix-netscaler-monitoring

Citrix Store. N.d. Viitattu 12.3.2017. http://store.citrix.com/store/citrix/en_US/pd/productID.315172500/ThemeID.37713000

Clustering vs. Load Balancing – What is the difference? 2009. Viitattu 17.11.2016. http://standardwisdom.com/softwarejournal/2009/09/clustering-vs-load-balancing-what-is-the-difference/

Configuring Load Balancing Pools. 2004. Viitattu 2.12.2016. https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm_configuration_guide_10_0_0/ltm_pools.html

Cyber threat in Middle East higher than global average: report. 2016. Viitattu 17.3.2017. http://www.deccanchronicle.com/technology/in-other-news/181016/cyber-threat-in-middle-east-higher-than-global-average-report.html

Dadighat, U. 2015. What Is SSL Offloading? Viitattu 19.1.2017. https://www.techwalla.com/articles/what-is-ssl-offloading

DDoS Protection. N.d. Viitattu 31.12.2016. https://www.cloudflare.com/ddos/

Ellrod, C. 2010. Load Balancing – Least Connections. Viitattu 1.12.2016 https://www.citrix.com/blogs/2010/09/02/load-balancing-least-connections/

Erillisverkot. N.d. Viitattu 8.11.2016. http://www.erillisverkot.fi/erillisverkot

Goncharov, M. 2012. Russian Underground 101. Viitattu 15.12.2015. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

HAProxy. 2017. Viitattu 12.3.2017. http://www.haproxy.org/

How SSL works tutorial with HTTPS example? 2015. Viitattu 19.1.2017. http://www.privatesslcertificate.com/how-ssl-works-tutorial-with-https-example/

HTTP Flood Attack. N.d. Viitattu 21.2.2017. https://www.verisign.com/en_US/security-services/ddos-protection/ddos-attack/index.xhtml

Kaczmarek, M. 2016. Defending Against Layer 7 DDoS Attacks. Viitattu 5.1.2017. https://blog.verisign.com/security/defending-against-layer-7-ddos-attacks/

Khandelwal, S. 2016. World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices. Viitattu 15.12.2016. http://thehackernews.com/2016/09/ddos-attack-iot.html

Kilpatrick, I. 2007. Benefits and disadvantages of SSL VPNs. Viitattu 19.1.2017. http://www.itproportal.com/2007/05/18/benefits-and-disadvantages-of-ssl-vpns/

Kostadinov, D. 2013. Layer 7 DDoS Attacks: Detection & Mitigation. Viitattu 16.1.2017. http://resources.infosecinstitute.com/layer-7-ddos-attacks-detection-mitigation/

Layer 3-4 SYN Denial-of-Service Protection. 2012. Viitattu 21.2.2017. https://docs.citrix.com/en-us/netscaler/11/security/ns-httpdosp-wrapper-con-10/ns-syn-dos-protection-con.html

Leadership. N.D. Viitattu 11.3.2017. https://f5.com/about-us/leadership

Load Balancing. 2016. Viitattu 16.11.2016. https://www.keycdn.com/support/load-balancing/

Load Balancing Layer 4 and Layer 7. N.d. Viitattu 15.1.2017. https://freeloadbalancer.com/load-balancing-layer-4-and-layer-7/

Load balancing Frequently Asked Questions. N.d. Viitattu 15.1.2017. http://blog.haproxy.com/loadbalancing-faq/

Load Balancing Technology White Paper. N.d. Viitattu 17.11.2016. http://www.h3c.com.hk/products___technology/products/security_products/h3c_secblade_module/h3c_secblade_lb/white_paper/200907/641567_57_0.htm

MacVittie, L. 2008. Layer 4 vs Layer 7 DoS Attack. Viitattu 21.2.2017. https://devcentral.f5.com/articles/layer-4-vs-layer-7-dos-attack

MacVittie, L. 2009. Intro to Load Balancing for Developers – The Algorithms. Viitattu 13.12.2016. https://devcentral.f5.com/articles/intro-to-load-balancing-for-developers-ndash-the-algorithms

MacVittie, L. 2013. Back to Basics: Least Connections is Not Least Loaded. Viitattu 2.12.2016. https://devcentral.f5.com/articles/back-to-basics-least-connections-is-not-least-loaded

Managed File Transfer and Network Solutions. 2015. Viitattu 27.11.2016. http://www.jscape.com/blog/load-balancing-algorithms

Memon, F. 2016. NGINX Plus vs. F5 BIG-IP: A Price-Performance Comparison. Viitattu 12.3.2017. https://www.nginx.com/blog/nginx-plus-vs-f5-big-ip-a-price-performance-comparison/

Miller, A. 2013. What Is A Layer 7 DDoS Attack? Viitattu 5.1.2017. http://ddosattackprotection.org/blog/layer-7-ddos-attack/

Monitoring the BIG-IP System. N.d. Viitattu 12.3.2017. https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip_getting_started_guide_10_1_0/bip_gs_app_dshbd.html#1011668

Nelson, R. 2014. SSL/TLS Offloading, Encryption, and Certificates with NGINX and NGINX Plus. Viitattu 19.1.2017. https://www.nginx.com/blog/nginx-ssl/

Networking. N.d. Viitattu 11.3.2017. https://www.citrix.com/networking/

Pronickin, A. 2011. Overview of Network Load Balancing. Viitattu 20.12.2016. https://technet.microsoft.com/en-us/library/cc725691(v=ws.11).aspx

Saharinen, K. 2013. Palomuuraus IDS/IPS. Jyväskylän ammattikorkeakoulun kurssimateriaali.

Saharinen, K. 2014. Jonotus ja ruuhkanhallinta. Jyväskylän ammattikorkeakoulun kurssimateriaali.

Sales, D. 2014. What Advantages Does Load Balancing Provide for Web Servers? Viitattu 20.12.2016. http://blog.wsol.com/what-advantages-does-load-balancing-provide-for-web-servers

Samuel, J. 2016. How to use Citrix NetScaler with CensorNet MFA (SMS PASSCODE) multi-factor authentication. Viitattu 12.3.2017. http://www.jasonsamuel.com/2016/12/07/how-to-use-citrix-netscaler-with-censornet-mfa-sms-passcode-multi-factor-authentication/

Sandbu, M. 2013. Managing DDoS with Citrix NetScaler. Viitattu 12.3.2017. https://msandbu.wordpress.com/2013/05/28/managing-ddos-with-citrix-netscaler/

Scarfone, K. N.d. Comparing the top SSL VPN products. Viitattu 8.2.2017. http://searchsecurity.techtarget.com/feature/Comparing-the-top-SSL-VPN-products

Smali, P. 2014. Deny Access to your Access gateway VIP By Using Location Database (GeoIP) Based on User's Country. Viitattu 12.3.2017. https://www.smali.net/deny-access-to-your-access-gateway-vip-by-using-location-database-geoip-based-on-users-country/

SSL VPN. N.d. Viitattu 19.1.2017. https://f5.com/glossary/ssl-vpn

SSL VPN Security. N.d. Viitattu 19.1.2017. http://www.cisco.com/c/en/us/about/security-center/ssl-vpn-security.html

The Top 10 DDoS Attack Trends. 2015. Viitattu 5.1.2017. https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf

They use it ! N.d. Viitattu 11.3.2017. http://www.haproxy.org/they-use-it.html

What Is Layer 4 Load Balancing? N.d. Viitattu 15.1.2017. https://www.nginx.com/resources/glossary/layer-4-load-balancing/

What Is Layer 7 Load Balancing? N.d. Viitattu 15.1.2017. https://www.nginx.com/resources/glossary/layer-7-load-balancing/

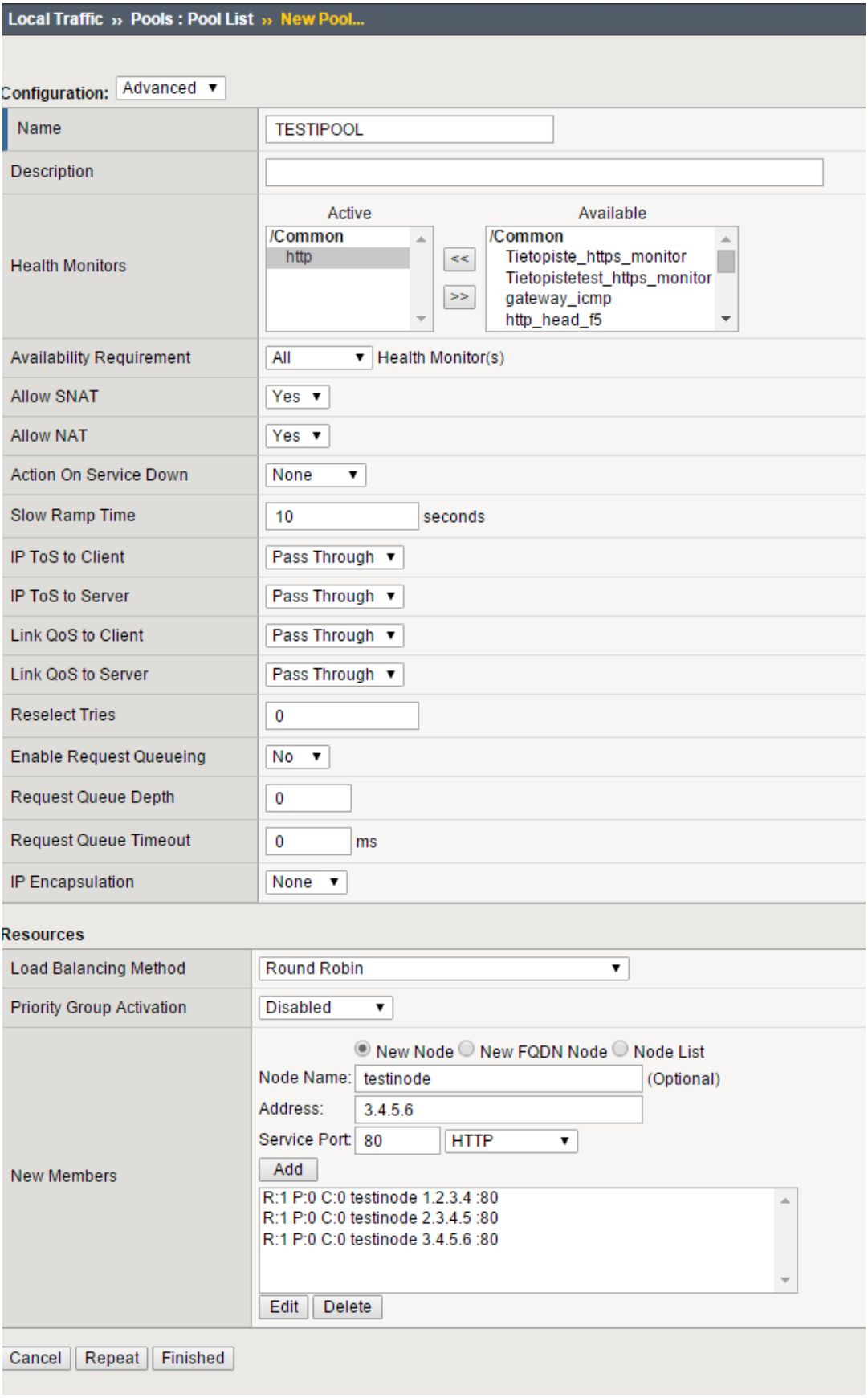
What is Round-Robin load balancing? N.d. Viitattu 13.12.2016. https://www.nginx.com/resources/glossary/round-robin-load-balancing/

What is SSL. N.d. Viitattu 19.1.2017. https://ssl.comodo.com/ssl.php

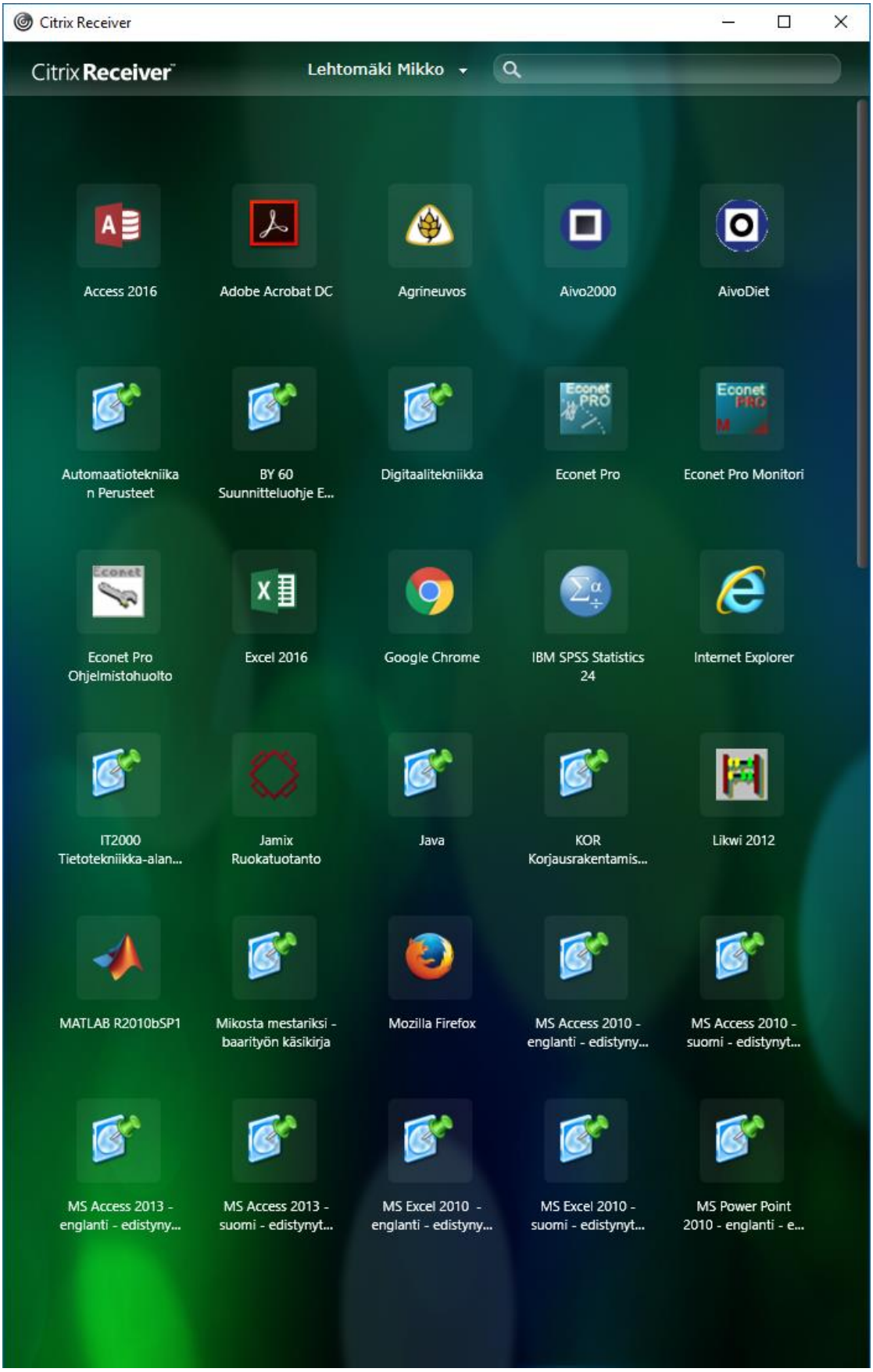
Woolf, N. 2016. DDoS attack that disrupted internet was largest of its kind in history, experts say. Viitattu 15.12.2016. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Liitteet

Liite 1. F5 kuormantasaus konfiguraatio



Liite 2. Citrix Receiver



Liite 3. HAProxy asetukset

```
global
        log /dev/log    local0
        log /dev/log    local1 notice
        chroot /var/lib/haproxy
        stats socket /run/haproxy/admin.sock mode 660 level admin
        stats timeout 30s
        user haproxy
        group haproxy
        daemon
        maxconn 100

        # Default SSL material locations
        ca-base /etc/ssl/certs
        crt-base /etc/ssl/private

        # Default ciphers to use on SSL-enabled listening sockets.
        # For more information, see ciphers(1SSL). This list is from:
        #  https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/
        ssl-default-bind-ciphers ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:I
        ssl-default-bind-options no-sslv3

defaults
        log     global
        mode    http
        option  httplog
        option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
        errorfile 400 /etc/haproxy/errors/400.http
        errorfile 403 /etc/haproxy/errors/403.http
        errorfile 408 /etc/haproxy/errors/408.http
        errorfile 500 /etc/haproxy/errors/500.http
        errorfile 502 /etc/haproxy/errors/502.http
        errorfile 503 /etc/haproxy/errors/503.http
        errorfile 504 /etc/haproxy/errors/504.http
        option forwardfor
        option http-server-close

frontend http-front
        bind *:80
        stats uri /haproxy?stats
        reqadd X-Forwarded-Proto:\ http
        default_backend http-back
        maxconn 200

backend http-back
        server mint1 192.168.1.33:80 check
        server mint2 192.168.1.56:80 check
        server mint3 192.168.1.58:80 check
        balance roundrobin
```