LAHDEN AMMATTIKORKEAKOULU
*Lahti University of Applied Sciences*

# PALOMUURIN JA INTERNET-YHTEYDEN KAHDENNUS

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2015
Janne Koistinen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

KOISTINEN, JANNE:

Palomuurin ja internet-yhteyden kahdennus

Tietoliikennetekniikan opinnäytetyö, 43 sivua, 4 liitesivua

Kevät 2015

TIIVISTELMÄ

---

Tämän opinnäytetyön tavoitteena oli suunnitella ja toteuttaa Lahti Energia Oy:lle kahdennettu palomuuri ja internetyhteys. Kahdennusprojekti tuo yrityksen IT-palveluille varmuutta ja vikasietoisuutta sekä antaa IT-henkilöstölle aikaa reagoida vikatilanteisiin paremmin.

Palomuuri tuo yrityksen verkolle turvaa ulkopuolisia hyökkääjiä vastaan suodattamalla pakettien kulkua internetin ja yrityksen sisäverkon välillä. Useampi palomuuri luo verkkoon vikasietoisuutta ja lisää palvelujen saatavuutta, koska järjestelmä toimii hyvin, vaikka yksi laite rikkoutuisikin. Useammalla palomuurilla voidaan myös saavuttaa tehostettua suojausta verkon kriittisille osille.

Kahdennus tuo verkkoihin vikasietoisuutta ja on hyvä tapa lisätä verkon ja verkon palveluiden saatavuutta. BGP-protokolla mahdollistaa useamman internet-palveluntarjoajan käytön, jolloin yhteydet toimivat, vaikka toisella internet-palveluntarjoajalla olisi vikaa verkossa.

Kahdennettavaksi palomuuriksi valittiin Palo Alton PA-5020. Se täyttää kaikki yrityksen vaatimat kriteerit, joista tärkeimpiä olivat virtuaalijärjestelmien määrä, riittävä verkonsiirtokapasiteetin ja suorituskyvyn omaaminen tulevaisuudessa. Tämän lisäksi yrityksellä on aikaisemmin ollut hyviä kokemuksia Palo Alton palomuureista.

Palo Alton laitteilla asetetaan oikein turvallisuusalueet ja porttikohtaiset asetukset, jotta myöhemmin voidaan ottaa käyttöön HA palomuureilla. Tämän lisäksi luodaan kahdennettu internetyhteys Ciscon reitittimillä.

Kahdennetun palomuurin HA-asetukset testattiin ja havaittiin HA-asetusten toimivuus pienin puuttein, mikä johtuu preemptive-ominaisuudesta palomuurissa. Preemptive uudelleenaktivoi aktiivisen palomuurin yliheiton jälkeen, mikäli virheen havaitaan poistuvan. Yritykselle kahdennettu palomuuri ja internetyhteys tuovat vikasietoisuutta verkkoon ja antaa henkilökunnalle aikaa korvata vikaantuneet laitteet ilman, että loppukäyttäjät huomaavat minkään olleen hajonnut.

Asiasanat: BGP, kahdennus, palomuuri

Lahti University of Applied Sciences
Degree Programme in Information Technology

KOISTINEN, JANNE: Configuring redundancy with a dual firewall and internet connection

Bachelor's Thesis in telecommunications, 43 pages, 4 pages of appendices

Spring 2015

ABSTRACT

---

The objective of this Bachelor's thesis was to plan and execute redundancy in the firewall and internet connection of Lahti Energia Oy. Redundancy gives security and fault tolerance for the company's services and gives the IT staff time to react in problem situations.

A firewall gives security to the company's network against hostile attackers by filtering packets between the internet and the company's local area network. Redundancy through dual firewalls brings fault tolerance to the network and increases the availability of the services, because the system works even if one device breaks down. Dual firewalls can also provide better protection to critical parts of the network.

Redundancy gives networks fault tolerance and it is a good way to increase the availability of the networks and the network services. The BGP protocol provides the means for using multiple internet service providers, which enables the connection to work even if the other internet service provider had defects in their network.

The firewall that was made redundant was a Palo Alto PA-5020. It fills all the criteria that the company presented, the most important of which were base virtual systems and sufficient throughput and performance in the future. In addition, the company has had good experiences from Palo Alto firewalls.

With Palo Alto devices, the correct options for security zones and interface options were set so that later on high availability can be deployed. In addition, a redundant internet connection was made with Cisco routers.

The HA configuration of a redundant firewall was successfully tested with a slight shortcoming due to the preemptive property in the firewall. The preemptive property reactivates the active firewall after a failover in case the cause of the error disappears. To the company a redundant firewall and internet connection provide fault tolerance in the network and give the staff time to replace the faulty devices without the end-users ever noticing that there was something broken.

Key words: BGP, redundancy, firewall

SISÄLLYS


1 JOHDANTO 1

2 TIETOTURVA YRITYKSESSÄ 2
2.1 Palomuuri yrityksen tietoturvana 2
2.2 Useamman palomuurin käyttö verkossa 3
2.3 Tietoturvauhat 4

3 KAHDENTAMINEN 6
3.1 Palomuurin kahdentaminen 6
3.2 High availability palomuureissa 7
3.3 Verkkolaitteiden ja -yhteyksien kahdentaminen 8
3.4 Kahdentamisen hyödyt ja haitat 11

4 BGP 13
4.1 Autonomous System 13
4.2 BGP-yhteyksien luominen 15
4.3 BGP-viestityypit 17
4.3.1 Open-viesti 18
4.3.2 Update-viesti 18
4.3.3 KeepAlive-viesti 20
4.3.4 Notification-viesti 20
4.3.5 Route-Refresh-viesti 20
4.4 RIB 21

5 PALOMUURIN VALINTA 22
5.1 Palomuurin kriteerit 22
5.2 Palomuurin vertailu ja valinta 22

6 VERKKOTOPOLOGIA 26
6.1 Työn toteutustavat ja toteutustavan valinta 27
6.1.1 Aktiivi/aktiivi 27
6.1.2 Aktiivi/passiivi 28
6.2 Vertailu toteutustavoista ja toteutustavan valinta 28

7 PALOMUURIN KÄYTTÖÖNOTTO 30
7.1 Palomuurin hallintapaneeliin pääsy 30
7.2 Palomuurin turvallisuusalueiden konfiguraatiot 31
7.3 Palomuurin porttien konfiguraatiot 32

7.4 Palomuurin HA-asetusten konfigurointi 33
7.4.1 HA-asetukset 34
7.4.2 Link and Path Monitoring -asetukset 36
7.5 BGP-asetukset 37
7.6 Testaussuunnitelma 39
7.7 Verkon vikasietoiseksi tekeminen 40
8 YHTEENVETO 42
LÄHTEET 44
LIITTEET 47

LYHENNELUETTELO

| | |
|---|---|
| AFI | Address Family Identifier, kenttätieto, joka on Route-Refresh -viestissä lähetetty 16 bitin tunniste, jolla tunnistetaan puhuja. |
| ARP | Address Resolution Protocol, protokolla, jolla selvitetään IP-osoitetta vastaava MAC-osoite. |
| AS | Autonomous System, järjestelmä, joka on yhden yrityksen tai tahon alla internetissä. |
| ASN | Autonomous System Number, numero, joka on yhden yrityksen tai tahon alla, jonka perusteella ne voidaan tunnistaa. |
| BGP | Border Gateway Protocol, protokolla, jota käytetään internetissä. |
| eBGP | external Border Gateway Protocol, BGP-protokolla, jonka avulla mainostetaan eri autonomisia järjestelmiä. |
| HA | High Availability, termi, jolla pyritään tarkoittamaan sitä, että järjestelmä on aina saatavilla. |
| HTTP | Hypertext Transfer Protocol, protokolla, jota käytetään internetin web-sivujen pohjana |
| IP | Internet Protocol, internetprotokolla, joka vastaa pakettien siirrosta kolmannen tason verkoissa. |
| ISP | Internet Service Provider, internet-palveluntarjoaja on organisaatio, joka tarjoaa yhdyskäytävän internetiin. |
| IT | Information Technology, tietotekniikka, yleisesti kaikki tietokoneisiin ja tietoteknisiin asioihin liittyvät asiat. |
| iBGP | internal Border Gateway Protocol, BGP-protokolla, jonka avulla mainostetaan verkon sisäisiä autonomisia järjestelmiä. |
| IETF | Internet Engineering Task Force, organisaatio, joka kehittää internetin standardeja. |

| | |
|---|---|
| LACP | Link Aggregation Control Protocol, protokolla, jonka avulla on mahdollista yhdistää useampi verkkolaitteen portti yhdeksi. |
| MAC | Media Access Control address, verkkosovittimen yksilöivä osoite, joka sisältää kuusi kaksinumeroista heksadesimaliarvoa. |
| MD5 | Message-Digest 5, algoritmi, jota käytetään salauksessa. |
| NAT | Network Address Translation, tekniikka, jonka avulla IP-osoitteet muunnetaan toiseksi. |
| PDF | Portable Document Format, tiedostomuoto, jota käytetään usein lähettäessä ja vastaanottaessa dokumentteja. |
| RIB | Routing Information Base, reititystieto, jota käytetään BGP-yhteyksissä. |
| RR | Route Reflector, verkkolaite, joka tarjoaa vaihtoehtoisen tavan toteuttaa internal borded gateway protocol toimien yhdyspisteenä muille laitteille. |
| SAFI | Subsequent Address Family Identifier, kenttätieto, jota käytetään Route-Refresh viestissä tunnistamaan puhuja. |
| SLA | Service Level Agreement, sopimuskohta, jossa määritellään sopimuksen laatu. |
| SPOF | Single Point Of Failure, järjestelmäosa, joka vikaantuessaan lamaannuttaa koko järjestelmän toimivuuden |
| SSH | Secure Shell, protokolla, jonka avulla on mahdollista salata tietoliikenne |
| STP | Spanning Tree Protocol, verkkoprotokolla, joka estää reitityssilmukoiden syntymistä |
| TCP | Transmission Control Protocol, protokolla, jonka avulla verkossa siirretään dataa varmistaen paketin perillepääsyn |

| | |
|---|---|
| UDP | User Datagram Protocol, protokolla, jonka avulla verkossa voi siirtää dataa varmistamatta sen perillepääsyä |
| VPN | Virtual Private Network, virtuaalinen verkko, jonka avulla on mahdollista yhdistää verkkoja näennäisesti yhteen suojatulla yhteydellä. |
| VLAN | Virtual Local Area Network, virtuaalinen verkko, joka toimii omana verkkona toisten virtuaalisten verkkojen rinnalla. |

# 1 JOHDANTO

Tämän opinnäytetyön tavoitteena on suunnitella ja toteuttaa Lahti Energia Oy:lle toimiva kahdennettu palomuuri kahden eri internet-palveluntarjoajan verkkoon. Työssä tutustutaan myös yleisesti yrityksen tietoturvaan, palomuureihin, kahdentamiseen ja BGP-protokollaan, jonka avulla kyseinen verkkototeutus on toteutettavissa. Työssä tutkitaan myös palomuurin valintaan liittyviä kysymyksiä ja siltä vaadittuja ominaisuuksia.

Yrityksen palveluiden saatavuutta ja internet-yhteyden toimivuutta pidetään nykyään yrityksissä suuressa arvossa. Palveluiden varmistamiseksi pyritään vähintään kahdentamaan verkkojen ja laitteiden kriittiset osat, jolloin yhden rikkoutuessa laite ei mene toimintakyvyttömäksi. Tämä antaa yrityksen IT (Information Technology) -henkilöstölle enemmän aikaa reagoida laitteen rikkoutumiseen.

Ongelmia tulee etenkin silloin, kun vika ei ole omissa laitteissa, vaan palveluntarjoajan laitteissa. Tällöin palvelut eivät ole internetin kautta saatavissa eikä IT-henkilöstö voi tehdä asialle mitään. Tässä tapauksessa toinen internet-palveluntarjoaja pystyy tarjoamaan toisen yhdyskäytävän internetiin, jolloin palvelut toimivat.

Lahti Energia Oy on energia-alan yritys, joka tuottaa sekä sähköä että kaukolämpöä. Yrityksellä on kaksi voimalaitosta Lahdessa ja yksi Heinolassa. Kaukolämpöä yritys toimittaa Lahdessa, Hollolassa, Nastolassa ja Asikkalassa ja sähkönsiirtoverkko ulottuu Lahden lisäksi Hollolan ja Nastolan kuntiin kokonaisvaltaisesti. Osin sähkönsiirtoverkko kattaa Iitin, Hämeenkosken ja Asikkalan kunnat. Henkilöstöä yrityksellä on 254, joiden keskimääräinen työskentelyikä on 19 vuotta ja keski-ikä 49 vuotta. (Lahti Energia 2014.)

# 2 TIETOTURVA YRITYKSESSÄ

Yrityksen tietoturvana pidetään usein palvelujen, järjestelmien, tietoliikenteen ja erityisesti tietojen suojaamista. Näiden kaikkien turvaamiseen palomuuri soveltuu. (Cisco 2015b.)

Yleisenä tietoturvallisuuden ohjeena on CIA-kolmikko, joka muodostuu kolmesta englanninkielisestä sanasta: confidentiality, integrity ja availability. Confidentiality, eli luottamuksellisuus, tarkoittaa, että tietoa näkevät ja käsittelevät vain henkilöt, joilla on siihen oikeus. Integrity, eli eheys, tarkoittaa, että tieto ei muutu vahingossa tai hyökkäyksen johdosta; ja tärkeintä on ainakin se, että muutos havaitaan. Availability, eli saatavuus, tarkoittaa sitä, että tieto on saatavilla tarvittaessa. (WhatIs.com 2015.)

## 2.1 Palomuuri yrityksen tietoturvana

Palomuurin päätehtävänä on hallita pakettien kulkua ulkoverkosta yrityksen verkkoon ja toisin päin. Pakettien kulkua voidaan hallita luomalla palomuuriin sääntöjä, joissa tietyt portit tai protokollat ovat sallittuja ja näin ollen palomuuri päästää paketit suojan läpi. Tämänlaisia palomuureja kutsutaan pakettisuodatin-palomuureiksi. (TechTarget 2015.)

Pakettisuodatin-palomuureja on kahdenlaisia: Tilattomat palomuurit seuraavat vain listassa olevia sääntöjä, ja mikäli paketti ei kuulu mihinkään sallittuun listaan, niin se pudotetaan. Tilalliset palomuurit muistavat käytetyt TCP (Transmission Control Protocol) -yhteydet ja viralliset UDP-yhteydet (User Datagram Protocol) sallien niiden yhteyteen kuuluvat paketit. Tällöin ei erikseen tarvitse määritellä sisään tulevia sallittuja portteja. Ongelma tilattomissa palomuureissa on myöskin siinä, että aina ei tiedetä, mistä portista vastaanotettava paketti saapuu luoden ongelmia tietynlaisten ohjelmien kanssa. (TechTarget 2015.)

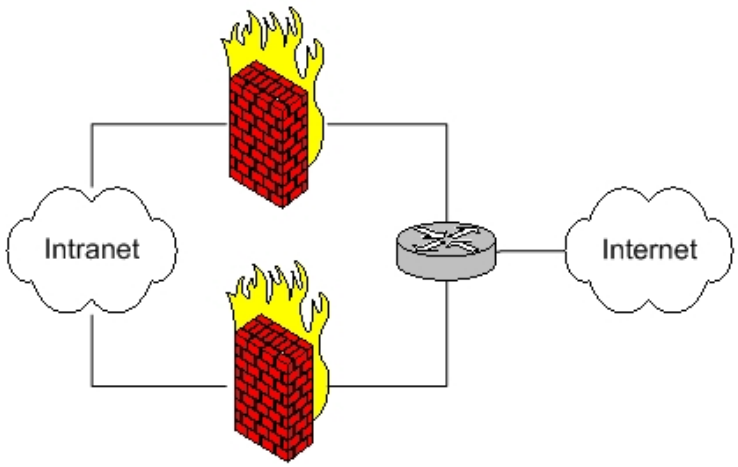
Sovelluspalomuurit toimivat korkeammalla tasolla kuin pakettisuodatin-palomuurit. Sovelluspalomuuri tarkistaa paketin sisältämää dataa ja vertailee, sisältääkö se laitonta dataa tai komentoja. Sovelluspalomuurit voivat myös suodattaa HTTP-liikennettä sisällön perusteella estäen tunnettuja tietoturva-aukkoja hyödyntäviä murtoyrityksiä. (TechTarget 2015.)

Yleisiä ongelmia palomuureille ovat salaukset, jotka salaavat paketin sisällön, jolloin niitä ei voida tarkistaa. Palomuuri ei myöskään pysty estämään liikennettä, joka tapahtuu vain sisäverkossa, eikä pysty estämään ihmisiä fyysisesti tunkeutumasta tiloihin. (Wikipedia 2014d.)

Mikäli joku onnistuu tunkeutumaan järjestelmään, on myös tärkeää, että järjestelmä ottaa talteen lokeja hyökkääjästä. Tällöin hyökkääjä voidaan saada kiinni ja myöhemmin tarkastella tämän toimia. (Viestintävirasto 2013.)

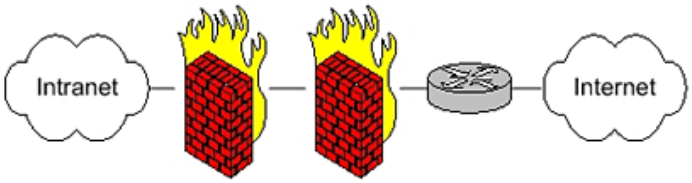
## 2.2 Useamman palomuurin käyttö verkossa

Useampaa palomuuria voi hyödyntää verkossa monella eri tapaa. Ensimmäinen toteutustapa on vikasietoinen verkko. Vikasietoisessa verkossa kaksi palomuuria laitetaan rinnakkain, jolloin toinen voi vikaantua käyttäjien huomaamatta. Toinen palomuuri ottaa tällöin itselleen koko verkon tuottaman kuorman. Tästä toteutustavasta kuva (KUVIO 1) seuraavaksi. (SearchFinancialSecurity 2015.)



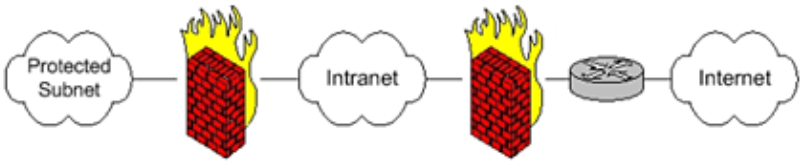

KUVIO 1. Rinnakkain asetetut palomuurit parantavat internetin saatavuutta (SearchFinancialSecurity 2015)

Toinen toteutustapa on lisättyä suojausta kaipaava verkko. Tällöin kaksi erimerkkistä palomuuria laitetaan peräkkäin verkkoon, jolloin voidaan välttää palomuurikohtaisia haavoittuvuuksia. Tällaista toteutustapaa käytetään joskus korkean turvallisuuden vaativissa verkoissa. Tästä toteutustavasta kuva (KUVIO 2) seuraavaksi. (SearchFinancialSecurity 2015.)




KUVIO 2. Erimerkkiset palomuurit internetin ja intranetin välillä luovat tehokkaan suojan palomuurikohtaisille haavoittuvuuksille (SearchFinancialSecurity 2015)

Kolmas toteutustapa on suojatut aliverkot. Tässä toteutustavassa aliverkkojen väliin sijoitetaan palomuuri, jolloin suojattuun aliverkkoon pääsy vaatii kahden palomuurin läpäisyn, mutta normaaliin intra-verkkoon pääsy vaatii vain yhden palomuurin läpäisyn. Tästä toteutustavasta kuva (KUVIO 3) seuraavaksi. (SearchFinancialSecurity 2015.)




KUVIO 3. Protected Subnet -aliverkkoon pääsy vaatii kahden palomuurin läpäisyn (SearchFinancialSecurity 2015)

## 2.3 Tietoturvauhat

Internetissä yrityksiin kohdistuu paljon erilaisia tietoturvariskejä. Palomuurilla voi parhaiten torjua kohdistetut hyökkäykset. Kohdistetussa hyökkäyksessä jokin taho yrittää päästä yrityksen tietoihin käsiksi, jolloin tietoja on mahdollista varastaa, muuttaa tai tuhota kokonaan. (Viestintävirasto 2013.)

Yleisiä sisällepääsemistapoja ovat myrkytetyt tiedostot, www-sivustot, jotka jakelevat haittaohjelmia, haittaohjelmien linkkien ja liitetiedostojen lähetys sähköpostissa ja 0-päivähaavoittuvuudet. Myrkytetyt tiedostot ovat tiedostoja, jotka näyttävät tavallisilta Office- tai PDF-tiedostoilta (Portable Document Format), mutta ovatkin oikeasti haittaohjelmia. Haittaohjelmia jakelevat www-sivustot näyttävät

jakavan tavanomaisia tiedostoja, mutta jakavatkin viruksia tai muita haittaohjelmia. Sähköpostin välityksellä voi myös lähettää linkkejä tai liitetiedostoina erilaisia haittaohjelmia. 0-päivähaavoittuvuudella tarkoitetaan vasta löydettyä haavoittuvuutta, jota ei vielä ole ehditty päivittämään. (Viestintävirasto 2013.)

Hyökkäystyyppejä on kolmea erilaista. Näistä ensimmäinen on edistyksellinen. Edistyksellinen viittaa siihen, että tunkeutuja on käyttänyt paljon aikaa hyökkäyksen tekoon räätälöidyillä järjestelmillä, he omaavat kyvyn piiloutua ja poistua jälkiä jättämättä. Toinen hyökkäystyyppi on jatkuva. Tällöin tavoitteena on säilyä piilossa ja kerätä tietoja pitkällä aikavälillä. Tavoitteena on juurruttaa pääsy haluttuihin järjestelmiin varastaen pääkäyttäjäoikeudet. Kolmas hyökkäystyyppi on kohdistettu. Tällöin kohteena ovat erityiset yritykset, kuten valtionhallinto, puolustusteollisuus ja korkean teknologian yritykset. Kohteita yrityksessä ovat johtajat, neuvottelijat ja tekninen ylläpito. (Viestintävirasto 2013.)

# 3 KAHDENTAMINEN

Kahdentamisella tarkoitetaan jonkin laitteen, palvelun tai kriittisen osan tuplaamista verkossa, laitteessa tai järjestelmässä. Tämän avulla pyritään estämään SPOF-pisteiden (Single Point Of Failure) syntyä. SPOF-piste muodostaa järjestelmässä kriittisen pisteen, jonka johdosta koko järjestelmä voi vikaantuessaan olla saavuttamattomissa, vaikka järjestelmä muuten toimisi oikein. (Belden 2015.)

Kahdentamisella pyritään maksimoimaan aika, jolloin palvelu on käyttäjän käytettävissä. Usein palveluntarjoajat käyttävät SLA:ta (Service Level Agreement) kuvaamaan palvelun saatavuutta yhdeksikköjen määrällä, eli ”viiden yhdeksikön” palvelu on saatavilla 99,999 % ajasta, jolloin palvelu saa vuodessa olla enintään 5 minuuttia ja 26 sekuntia käyttämättömissä. (Wikipedia 2014c.)

## 3.1 Palomuurin kahdentaminen

Palomuurien kahdennus voidaan toteuttaa kahdella eri tapaa. Käytetyt tavat ovat aktiivi/passiivi ja aktiivi/aktiivi. (Palo Alto Networks 2014e.)

Aktiivi/passiivi-tilassa toinen laitteista on aktiivinen ja toinen passiivinen, eli passiivi-laite odottaa aktiivi-laitteen vikaantumista. Laitteiden välissä oleva heartbeat-yhteys havaitsee saman tien, mikäli aktiivi-laite vikaantuu, ja tämän jälkeen passiivi-laite aloittaa toimintansa. Laitteet synkronoivat keskenään asetukset, jotta yliheitto (failover), eli tilanne, jossa passiivi-laite aloittaa toimintansa, toimii. (Palo Alto Networks 2014e.)

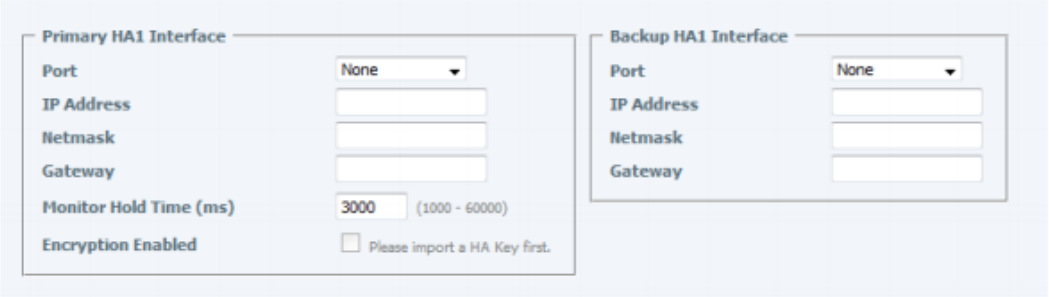
Aktiivi/aktiivi-tilassa laitteet synkronoivat jatkuvasti asetuksia ja istuntoja keskenään. Näiden välillä on myös heartbeat-yhteys, jossa tarkkaillaan jatkuvasti toisen laitteen tilaa. Mikäli yhteydessä on vikaa, ottaa toimiva laite itselleen kaikki toiminnot. Tässä tilassa laitteet tukevat myös kuormantasausta. (Palo Alto Networks 2014e.)

## 3.2 High availability palomuureissa

HA (High Availability) tarkoittaa laitteita, joista yksi tai useampi voi kaatua vaikuttamatta järjestelmän käytettävyyteen. Tekniikan avulla estetään SPOF-pisteiden syntyä. (Wikipedia 2014c.)

Palo Alton palomuureissa on kolme eri HA-linjaa. Linjat ovat Control Link, Data link ja HA3-link. Näiden kolmen lisäksi on mahdollista luoda Backup HA -linkkejä, minkä ansiosta jokaisen linkin voi vielä kahdentaa. (Palo Alto Networks 2014a.)

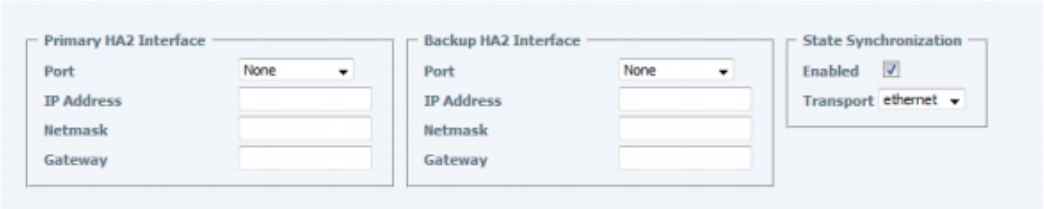
Control Link tunnetaan myös nimellä HA1-linkki. Sen tehtävänä on keskustella toisten samaan HA:n kuuluvien HA1-linkkien kanssa. Keskusteluun käytetään TCP-protokollan porttia 28769 tiedon ollessa salaamatonta, tai porttia 49969 tiedon ollessa salattua SSH:n (Secure Shell) avulla. Yhteyttä käytetään lähettämään ja vastaanottamaan hello-viestejä sekä HA-tilan, reititystietojen ja käyttäjien tietojen lähettämiseen. Linkkiin on mahdollista asettaa haluttu Monitor Hold Time, johon asetetun ajan palomuuri odottaa, että vastapuolen palomuuri on saavuttamattomissa. Tämän jälkeen vara-palomuuri aloittaa toimintansa. Kuva konfiguraatioiden tekemisestä kuviossa 4. (Palo Alto Networks 2014a.)




KUVIO 4. Control linkin asetukset laitetaan näin (Palo Alto Networks 2014a)

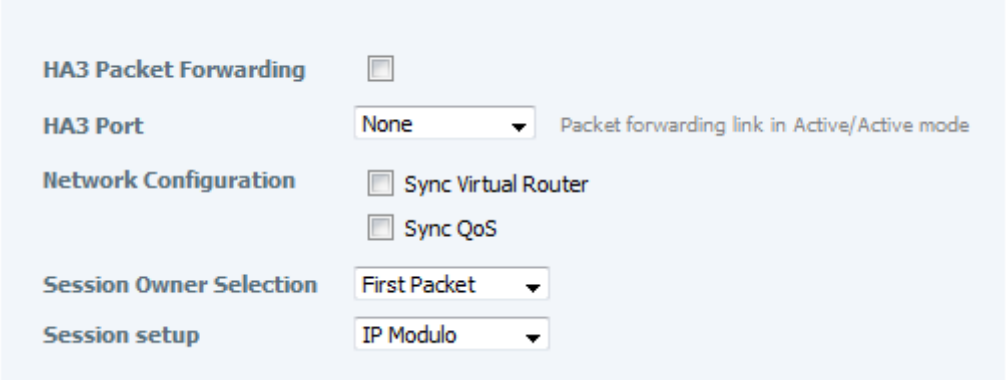
Data Link tunnetaan myös nimellä HA2-linkki. HA2-linkkiä käytetään tilojen, sessioiden, reititystaulujen, IPSec security associationsien ja ARP-taulujen (Address Resolution Protocol) synkronoimiseen. HA2-linkin voi asettaa toimimaan IP:n tai UDP:n kanssa, mutta oletuksena tieto lähetetään layer 2:lla. UDP:tä käytettäessä on huomattava hyöty, koska silloin checksum muodostetaan koko paketista, eikä vain headerista, kuten IP:tä käytettäessä. IP-protokolla käyttää siirtotie-

nä porttia 99 ja UDP porttia 29281. Data Linkin konfigurointi tapahtuu kuvion 5 lailla. (Palo Alto Networks 2014a.)




KUVIO 5. Data Linkin konfigurointi eroaa huomattavasti Control Linkin konfiguroinnista (Palo Alto Networks 2014a)

HA3-linkkiä käytetään vain aktiivi-aktiivi-toteutuksessa. Linkkiä käytetään pakettien edelleenlähettämiseen. HA3-linkki on layer2-linkki, ja se käyttää MAC-in-MAC-kotelointia (Media Access Control), eikä sille voi tehdä perinteistä varalinkkiä. Mikäli halutaan tehdä varalinkki HA3-linkille, on luotava yhdistetty linkki, ja asettaa se HA3:lle. HA3-linkkien konfigurointi voidaan tehdä seuraavanlaisella sivustolla (KUVIO 6). (Palo Alto Networks 2014a.)

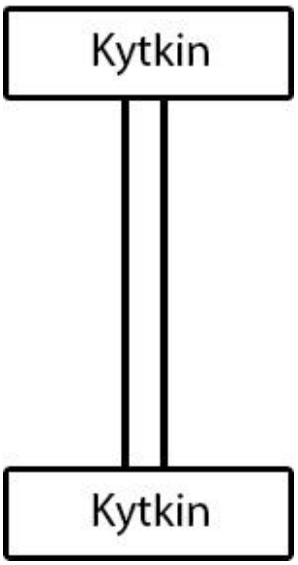



KUVIO 6. HA3-linkin konfigurointi (Palo Alto Networks 2014a)

## 3.3 Verkkolaitteiden ja -yhteyksien kahdentaminen

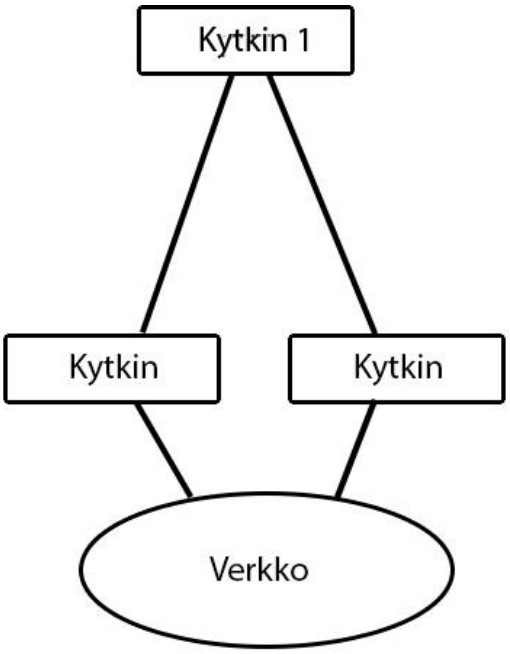
Verkkolaitteiden ja -yhteyksien kahdentamisen voi toteuttaa monella eri tapaa. Eri tavat eroavat toisistaan paljon, ja jokaisella on omat hyvät ja huonot puolensa. Yksinkertaisin tapa varmistaa yhteys kahden kytkimen välillä on käyttää LACP-protokollaa (Link Aggregation Control Protocol). Tällöin lisätään ylimääräinen verkkokaapeli laitteiden väliin, jolloin toinen linkeistä voi katketa ja verkko jatkaa toimintaansa. Tämä on helppo ja halpa tapa tuoda varmistuslinjoja verkkoon.

LACP tukee myös useampaa varmistuslinjaa. Kuvassa (KUVIO 7) esitellään useamman linkin tuoma etu. (WindowsITPro 2014.)



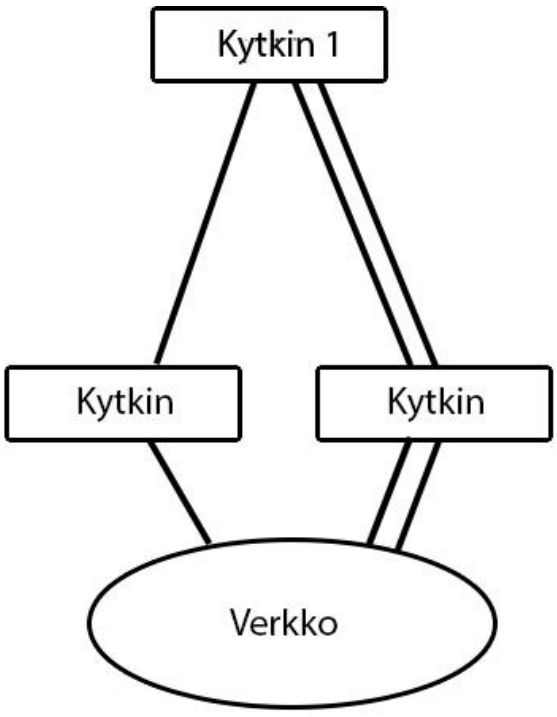

KUVIO 7. Monet verkkolaitteet tukevat useampia yhteyksiä toistensa välillä

Toinen tapa kahdentaa verkkolaitteet on asettamalla useampi polku määränpäiden välillä. Kuvassa (KUVIO 8) nähdään verkko, jossa kytkin on kahdennettu Kytkin1:n ja verkon välillä. Tällöin toinen kytkimistä voi vikaantua ja verkko jatkaa toimintaansa normaalisti. Tämä on huomattavasti kalliimpi toteutustapa kuin vain linkin kahdennus, mutta sallii yhden Kytkin-kytkimen vikaantumisen. (WindowsITPro 2014.)



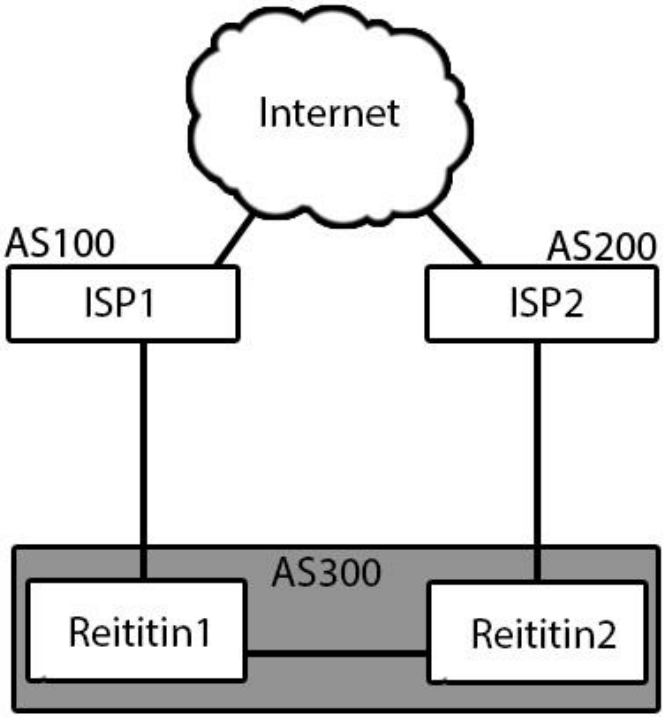

KUVIO 8. Kahden kytkimen avulla toinen voi vikaantua verkon jatkaessa toimintaansa normaalisti

Edellä mainittuja kahta tapaa voi myös yhdistää. Kuvassa (KUVIO 9) edellisen verkon oikeanpuoleisen kytkimen linkit on kahdennettu.




KUVIO 9. Oikean puolen kytkimen linkit ovat kahdennettu

Kolmas tapa on käyttää BGP:tä (Border Gateway Protocol) hyödyksi. Tämän avulla on mahdollista käyttää useampaa ISP:tä (Internet Service Provider), eli internet-palveluntarjoajaa. Tällöin toisen ISP:n toimimattomuus ei häiritse internetin toimivuutta. BGP vaatii kuitenkin yritykselle oman ASN:n (Autonomous System Number). Kuvassa (KUVIO 10) on esitelty BGP-verkon toimivuutta. (WindowsITPro 2014.)




KUVIO 10. BGP-verkko, jossa kaksi ISP:tä, joiden ASN:t ovat 100 ja 200 ja kohdeverkon ASN on 300

### 3.4 Kahdentamisen hyödyt ja haitat

Kahdentaminen on nykypäivänä tärkeä tapa yrityksille lisätä järjestelmän saatavuutta. Mikäli laitteella ei ole varajärjestelmää ja se menee rikki, on järjestelmä toimintakyvytön. Tämän takia on tärkeätä kahdentaa kriittiset osat niin verkossa kuin fyysisestikin. (WindowsNetworking.com 2014.)

Kahdennuksessa on muutamia yleisiä heikkouksia: varmistetut laitteet ovat monimutkaisempia, jolloin vikatilanteet ovat yleisempiä ja kahdentamisen johdosta työntekijöiden vastuu vähenee. Varmistaminen voi myös luoda tuottavuuspainei-

ta, jolloin järjestelmä toimii liian korkeilla nopeuksilla turvattomammin. Kahdentaminen lisää myös käyttöönottokustannuksia. (Wikipedia 2014e.)

# 4 BGP

BGP on reititysprotokolla, joka on käytössä ylemmän tason internet-palveluntarjoajien välisessä liikenteessä ja joissakin suuryrityksissä. Reititystietoja vaihdetaan eri AS:ien (Autonomous System) välillä. Jokaisella yrityksellä, internet-palveluntarjoajalla tai suuryrityksen toimipisteellä tulee olla oma ASN, mikäli haluaa hyödyntää BGP:tä. (Orbit-Computer Solutions 2014.)

BGP-laitteet konfiguroidaan manuaalisesti naapureiksi (englanniksi peer), jotka vaihtavat tietoja keskenään TCP:n portilla 179. Kun BGP toimii saman AS:n alaisena, kutsutaan sitä iBGP:ksi (Interior Border Gateway Protocol), ja kun se toimii eri AS:ien välillä, kutsutaan sitä eBGP:ksi (Exterior Border Gateway Protocol). Ero näiden välillä on se, että yleensä eBGP:ssä opitut reitit jaetaan eteenpäin iBGP:ssä ja eBGP:ssä oleville reitittimille, kun taas iBGP:stä opitut reitit opetetaan vain eBGP-reitittimille. (RFC4271 2006.)

iBGP-laitteet toimivat full-mesh-periaatteella, jolloin jokaisella laitteella tulee olla yhteys jokaiseen toiseen iBGP-laitteeseen. Tämä luo ongelmia suurempiin verkkoihin, koska jokainen uusi laite nostaa tarvittavia yhteyksiä exponentiaalisesti. Ongelman ratkaisemiseksi on kehitetty RR (Route Reflector) ja BGP Confederationsit. (Wikipedia 2014b.)

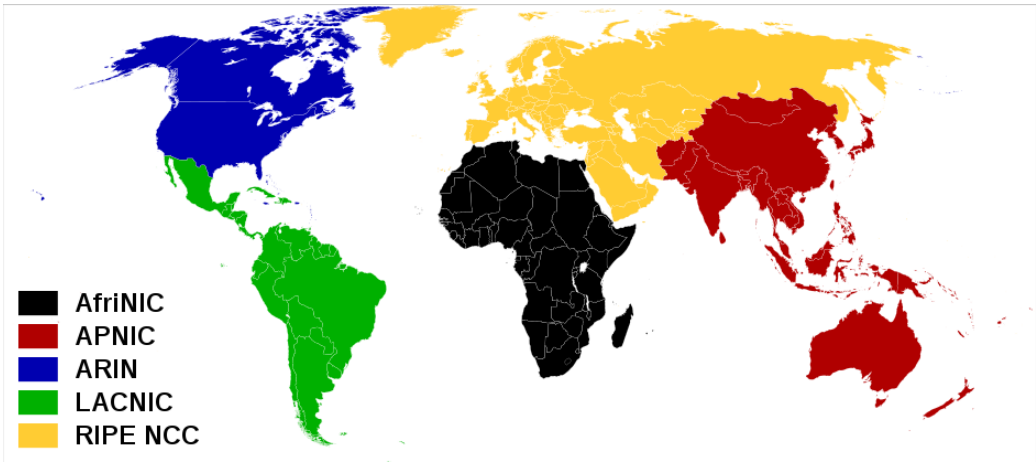
Route Reflectorit toimivat yhdyskäytävänä iBGP-yhteyksille; jokainen BGP-reititin yhdistää RR:ään sen sijaan, että yhdistäisi jokaiseen toiseen reitittimeen. Tämän avulla yhteyksiä tarvitsee vain luoda kaksi, mikäli uusi laite lisätään verkkoon. (RFC4456 2006.)

BGP Confederation avulla AS pilkotaan useampiin pienempiin AS:iin, mutta mainostaen sitä suurena AS:nä. Tarkoituksena on pienentää iBGP-yhteyksien määrää luomalla eBGP-yhteyksiä verkon sisälle. (Cisco 2014.)

## 4.1 Autonomous System

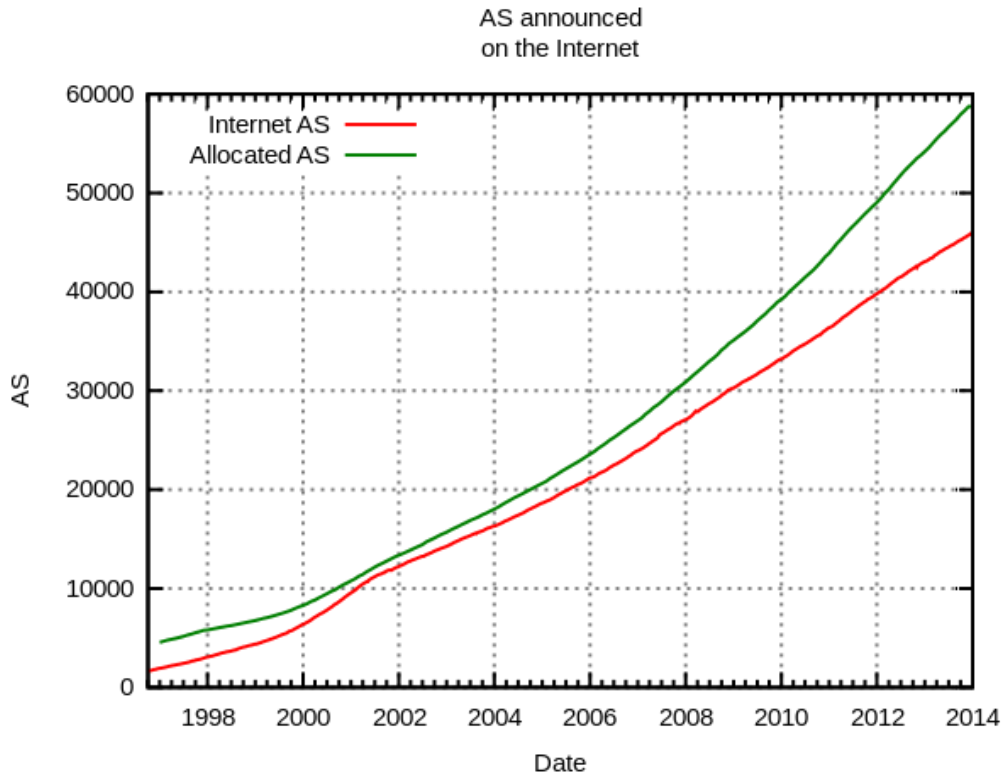
AS-numerot ovat IANA:n (Internet Assigned Numbers Authority) määrittelemiä lohkoja, jotka on jaettu RIR:eihin (Regional Internet Registries) (Wikipedia 2014a). RIR on organisaatio, joka vastaa IANA:n lohkon AS-numeroiden jakami-

sesta omalle alueelleen. RIR-organisaatioita on viisi kappaletta, joista kartta on kuviossa 11. (Wikipedia 2014a.)




KUVIO 11. RIR-organisaatiot kartalla (Wikipedia 2014f)

Vuoteen 2007 asti AS-numerot määriteltiin 16-bittisellä integerillä, jolloin saatavilla oli 65536 eri numeroa. Silloin IANA julkaisi 32-bittiset AS-numerot, jolloin saatavilla on yli neljä miljardia numeroa. Kuvaajassa (KUVIO 12) nähdään AS:ien rekisteröitymismäärä. (Wikipedia 2014a.)




KUVIO 12. Rekisteröityjen AS:ien määrä (Wikipedia 2014b)

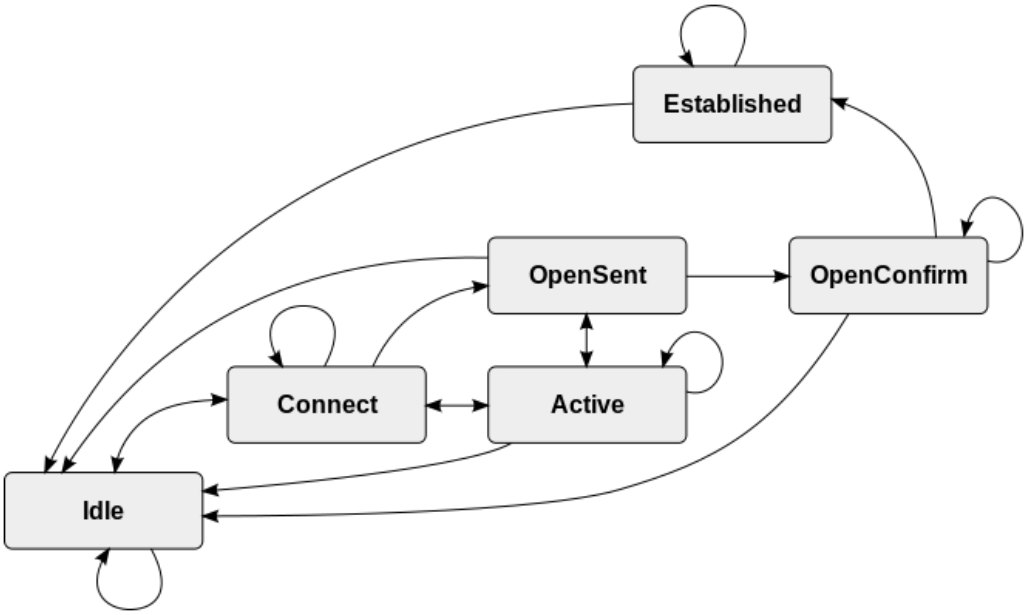
Yksityiseen käyttöön on varattu alkuperäisestä 16 bitin lohkosta numerot 64512–65534 ja 32-bitin lohkosta väli 4.200.000.000–4.294.967.294 tarkoittaen sitä, että näitä voidaan käyttää yrityksen sisäisessä AS-topologiassa, mutta niitä ei tule mainostaa internetiin. (Wikipedia 2014a.)

AS-ryhmiä on kolmea erilaista riippuen niiden käyttötarkoituksesta. Multihomed autonomous system on AS, joka ylläpitää yhteyttä useampaan kuin yhteen AS:ään. Tämä mahdollistaa AS:n internetin toimivuuden, vaikka yksi yhteys katkeaisikin kokonaan. Stub autonomous system on AS, joka on yhteydessä toiseen AS:ään. Transit autonomous system on AS, joka tarjoaa yhteyksiä omasta AS:stä toisiin verkkoihin. (Wikipedia 2014a.)

## 4.2 BGP-yhteyksien luominen

BGP-yhteyden luominen tapahtuu kuuden eri vaiheen aikana (KUVIO 13). Nämä vaiheet tunnetaan nimellä Idle, Connect, Active, OpenSent, OpenConfirm sekä Established. Mikäli jotain virheitä esiintyy yhteydenluonnin aikana, palaa yhteys

joko tilaan Idle tai Active riippuen siitä, missä vaiheessa virhe esiintyi. (Wikipedia 2014b.)




KUVIO 13. BGP-yhteyden luonti (Wikipedia 2014b)

Idle-tilassa hylätään kaikki BGP-yhteydet, mutta kuunnellaan porttia 179, mikäli BGP-peer yrittää ottaa yhteyttä. Samalla aloitetaan TCP-yhteyden luonti naapuriin ja vaihdetaan tila Connectiin. (RFC4271 2006.)

Connect-tilassa odotetaan onnistunutta TCP-neuvottelua. Tässä tilassa yhteys ei ole kauan, mikäli yhteydenluonti on onnistunut naapurin kanssa. Tämän jälkeen lähetetään Open-viesti ja vaihdetaan tila OpenSentiin. Mikäli jokin virhe tapahtuu tässä vaiheessa, siirtyy laite Active-tilaan. (RFC4271 2006.)

Active-tilassa TCP-yhteyden luonnissa on tapahtunut jokin virhe. Tällöin yritetään aloittaa uusi TCP-yhteys naapurin kanssa, ja mikäli se onnistuu, niin siirrytään OpenSent-tilaan. Tosin mikäli yhteys epäonnistuu uudelleen, siirrytään takaisin Idle-tilaan. (RFC4271 2006.)

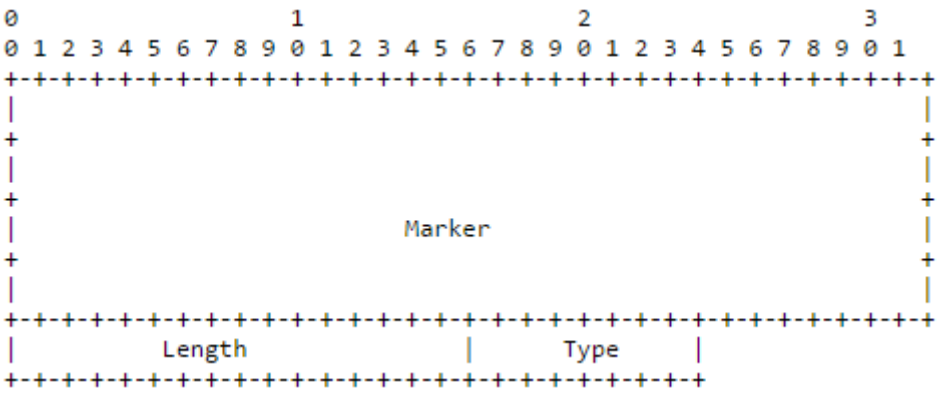
OpenSent-tilassa yhteys odottaa naapurilta sen Open-viestiä. Viestin saatuaan se tarkistetaan, ja mikäli jokin virhe esiintyy viestin kentissä, lähetetään ilmoitus virheestä ja virheen aiheuttajasta naapurille. Virhe voi johtua siitä, että viestin kentässä on eri BGP-versiot, MD5-salasanat/MD5 tai AS-numerot. Mikäli virheitä ei esiinny, siirrytään OpenConfirm-vaiheeseen. (RFC4271 2006.)

OpenConfirm-tilassa laite odottaa Keepalive-viestiä naapurilta. Mikäli viesti vastaanotetaan, ennen kuin mikään ajastin on umpeutunut, siirrytään Established-tilaan. Tosin mikäli jokin ajastin umpeutuu, siirtyy yhteys takaisin Idle-tilaan. (RFC4271 2006.)

Established-tilassa naapurit lähettävät keskenään Update-viestejä vaihtaen tietoa jokaisesta mainostetusta BGP-naapurista. Mikäli virheitä esiintyy tässä vaiheessa tai Keepalive-ajastin umpeutuu, lähetetään naapurille viesti ja siirrytään takaisin Idle-tilaan. (RFC4271 2006.)

## 4.3 BGP-viestityypit

BGP-4-viestityyppejä on viisi kappaletta. Viestin otsake-kenttä määritellään kuvion 14 mukaisesti. Otsake-kenttä lähetetään jokaisessa BGP-paketissa ja kenttä määrittelee tulevan viestin tyypin. Viestistä 0–127 bitit (Marker-alue) ovat kaikki ykkösiä, 128–143 bitit (Length-alue) määrittelevät viestin pituuden okteteissa ja 144–151 bitit (Type) määrittelee paketin tyypin. Eri tyypit ovat Open, Update, Notification, KeepAlive ja Route-Refresh. Route-Refresh lisättiin IETF:n (Internet Engineering Task Force) RFC2918-standardoinnissa. (RFC4271 2006.)

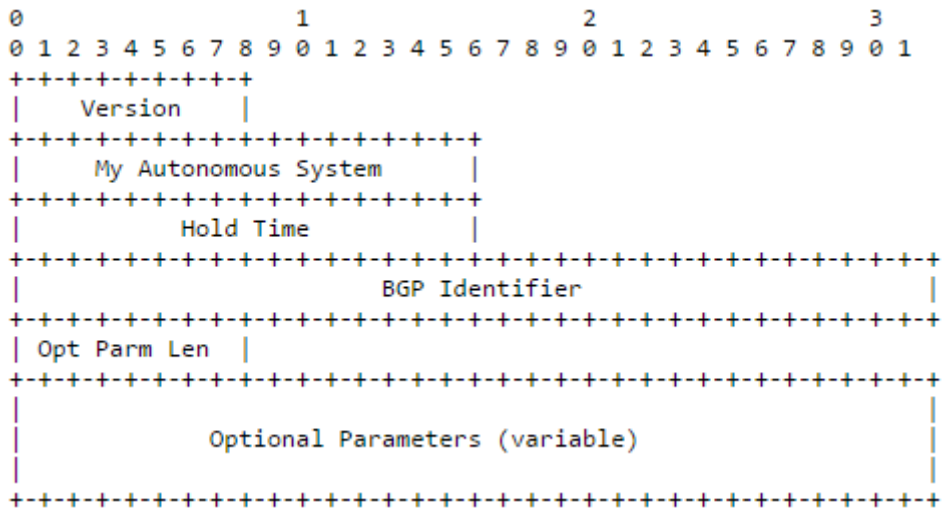



KUVIO 14. BGP-paketin otsake (RFC4271 2006)

TCP-yhteydenluonnin jälkeen ensimmäinen viesti, jonka molemmat BGP-yhteyden osapuolet lähettävät, on Open-viesti. Mikäli viesti on hyväksyttävä, lähetetään Keepalive-viesti seuraavaksi. (RFC4271 2006.)

### 4.3.1 Open-viesti

Molemmat BGP-yhteyden osapuolet lähettävät ensimmäisenä viestinä yhteydenluonnin aikana Open-viestin. Viesti sisältää seuraavan kuvan (KUVIO 15) kentät. (RFC4271 2006.)

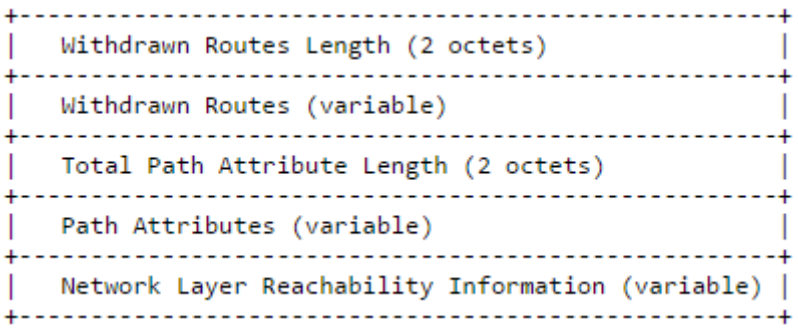



KUVIO 15. Open-paketin kentät (RFC4271 2006)

Versio-kenttä kertoo käytettävän BGP-version, joka on tällä hetkellä 4. My Autonomous System -kenttä, kertoo lähettävät osapuolet AS-numeron. Hold Time -kenttä kertoo ehdotettavan ajan sekunneissa, jolloin yhteyttä voi ylläpitää. Ajan täyttyessä oletetaan, että yhteys on katkennut. Hold Timen tulee olla joko nolla tai suurempi kuin kolme. BGP Identifier -kenttä määrittelee lähettäjän BGP identifier -arvon. Opt Parm Len -kenttä kertoo Optional Parameters -kentän pituuden, mikäli tämä arvo on nolla, ei Optional Parametereita ole. Viimeinen kenttä määrittelee Optional Parameterit yhteydelle. (RFC4271 2006.)

### 4.3.2 Update-viesti

Update-viestien avulla siirretään reititystietoja BGP-peerien välillä. Tiedon avulla voidaan rakentaa kaavio, joka kuvaa suhdetta eri AS:ien välillä. Näiden pakettien avulla voidaan myös havaita reitityssilmukat ja muut poikkeamat sekä poistaa ne jakelusta. Update-paketit sisältävät seuraavan kuvan (KUVIO 16) kentät. (RFC4271 2006.)




KUVIO 16. Update-viestin kentät (RFC4271 2006)

Withdrawn Routes Length -kenttä määrittelee sen jälkeen tulevan kentän pituuden. Arvon ollessa nolla ei seuraavassa kentässä ole lainkaan arvoja. Withdrawn Routes -kenttä sisältää listan poistettavista IP-osoitteista. Total Path Attribute Length -kenttä määrittelee Path Attribute-s ja Network Layer Reachability Information -kenttien pituuden. Tämän ollessa nolla, ei viesti sisällä kumpaakaan sen jälkeisistä kentistä. (RFC4271 2006.)

Path Attributes -kentällä voidaan lisätä erilaisia määritelmiä yhteydelle. Kentän avulla voidaan määrittää pakollisia ja valinnaisia määritelmiä. Pakolliset määritelmät sekä eBGP:ssä että iBGP:ssä ovat ORIGIN, AS_PATH ja NEXT_HOP. Valinnaisia ovat MULTI_EXIT_DISC, ATOMIC_AGGREGATE ja AGGREGATOR. iBGP:ssä vaaditaan lisäksi LOCAL_PREF. (RFC4271 2006.)

ORIGIN-määritelmän avulla kerrotaan kyseisen reititystiedon alkuperäisen lähettäjän tiedot; tätä kenttää ei tulisi muuttaa missään tapauksessa. AS_PATH kertoo, mitä reittiä pitkin viesti on liikkunut vastaanottajalle; tätä kenttää tulisi muokata, mikäli viesti menee muualle kuin omaan AS:ään, ja tämän kentän avulla on myös mahdollista havaita reitityssilmukat. NEXT_HOP määrittelee seuraavaksi käytettävän reitittimen IP-osoitteen, mitä tulisi käyttää seuraavana osoitteena UPDATE-viestissä määritellyille osoitteille; tätä kenttää ei tulisi muuttaa, ellei laitetta ole erikseen määritelty tekemään sitä. (RFC4271 2006.)

Valinnaisella määritelmällä MULTI_EXIT_DISC voidaan määritellä useampi ulos- tai sisääntulo samalle AS-naapurille. ATOMIC_AGGREGATE:n avulla voidaan yhdistää useampi reitti mainostettavaksi tietylle naapurille. AGGREGATOR:n avulla voidaan mainostaa, että päivityksissä on käytetty yhdistettyjä reittejä. LOCAL_PREF on määritelmä, jonka jokainen iBGP-puhuja

lähettää. Arvossa lasketaan jokaisen ulkoisen reitin arvo, joka jaetaan saman AS:n naapureille. (RFC4271 2006.)

### 4.3.3 KeepAlive-viesti

KeepAlive-viestejä lähetetään yhteyden ylläpitämistä varten. Erikseen määritelty Hold Time -arvo määrittää KeepAlive-viestien lähetystiheyden. Hyvänä perusarvona pidetään KeepAlive-viestin lähettämistiheydeksi kolmasosan Hold Time -arvosta. Viestiä ei tulisi kuitenkaan lähettää useammin kuin kerran sekunnissa. (RFC4271 2006.)

Mikäli Hold Time -arvo on 0, ei KeepAlive-viestejä lähetetä. KeepAlive-viesti muodostuu vain viestin otsakkeesta. (RFC4271 2006.)

### 4.3.4 Notification-viesti

Notification-viesti lähetetään, mikäli jokin virhe on huomattu. BGP-yhteys suljetaan välittömästi viestin lähettämisen jälkeen. Viestissä kerrotaan, mikä aiheutti virheen. (RFC4271 2006.)

Virheet on jaoteltu kuuteen eri päähaaraan, jotka ovat Message Header Error, OPEN Message Error, Update Message Error, Hold Timer Expired, Finite State Machine Error ja Cease. Päähaaroilla on myös alahaaroja, joilla on omat koodinsa. Virheilmoituksessa on myös Data-kenttä, jossa määritellään tarkemmin virheen syy, ja se on riippuvainen käytetyistä päähaaroista ja sivuhaaroista. (RFC4271 2006.)

### 4.3.5 Route-Refresh-viesti

Route-Refresh-viestityypin avulla on mahdollista kysyä BGP-naapurin reitityspäivityksien uudelleenlähetystä. Ennen standardin tuloa tämänlaiseen prosessiin vaadittiin ylimääräistä muistia ja prosessointitehoa, mikä johtui ”soft-reconfiguration”-ominaisuudesta, jonka johdosta jouduttiin säilömään kaikki BGP-naapurin reitit. (RFC4271 2006.)

Viesti itsessään sisältää kolme kenttää, jotka ovat AFI (Address Family Identifier), Res. ja SAFI (Subsequent Address Family Identifier). AFI- ja SAFI-kentät tulevat BGP-naapurilta yhteydenmuodostamisen aikana. (RFC2918 2000.)

## 4.4 RIB

RIB-tyyppejä (Routing Information Base) on kolmea erilaista. Niissä säilytetään opittuja ja prosessoituja reititystietoja. (RFC4271 2006.)

Adj-RIBs-In tallentaa reititystiedot, jotka on opittu sisääntulevalta UPDATE-viestiltä. Niiden sisältö esittää reittejä, jotka on mahdollista sisällyttää päätäntäprosessiin. (RFC4271 2006.)

Loc-RIB sisältää paikallisen reititystiedon perustuen sen omiin säädöksiin ja tietoon, joka saadaan Adj-RIBs-In:istä. Näitä reittejä käyttää paikallinen BGP-puhuja, jonka reititystaulusta on myös pystyttävä selvittämään jokaiselle reitille seuraavan hypyn osoite. (RFC4271 2006.)

Adj-Ribs-Out sisältää tiedon, jonka paikallinen BGP-puhuja päättää mainostaa sen naapureille. Reititystiedot lähetetään puhujan UPDATE-viesteissä sen naapureille. (RFC4271 2006.)

# 5 PALOMUURIN VALINTA

## 5.1 Palomuurin kriteerit

Palomuurilta vaaditaan tehoa sen verran, että palomuuri voi yksin ottaa haltuun koko sisä- ja ulkoverkon välisen kuorman. Sisäverkossa on useita satoja laitteita tuottamassa kuormaa verkolle. Lisäksi kohdeyritys vaatii palomuurilta 10 Base Virtual Systemsiä, eli mahdollisuutta luoda 10 virtuaalista palomuuria palomuurin sisälle, joita voi hallita erillään.

Tämän lisäksi palomuurin tulisi myös toimia useita vuosia ilman fyysistä päivitystä. Tulevaisuutta on myöskin ajateltava.

## 5.2 Palomuurin vertailu ja valinta

Palomuurin valitsemisessa on otettava huomioon monta eri osa-aluetta. Tällä hetkellä kohdeyrityksellä on käytössä useampi Palo Alto -merkkinen palomuuri. Tämä rajoittaa palomuurin valinnan kyseiseen merkkiin.

Palo Altolla on kuitenkin tarjottavana useampaa eri mallia, joista kaikilla on erilaiset ominaisuudet. Palo Alto tarjoaa kuutta erilaista fyysistä palomuurisarjaa, joiden tehot yltävät muutaman hengen yritysten tarpeista aina suurien yritysten palvelinsalien tarpeisiin. Tarjolla on myös virtuaalinen palomuurisarja, jota pyydettiin tarkastelemaan kohdeyrityksestä.

Vertailtaviksi laitteiksi otetaan PA-5020, PA-3050 ja VM-1000-HV. PA-5020-laite on käytössä tällä hetkellä yrityksen pääpalomuurina ja palomuuri on havaittu hyväksi laitteeksi yrityksessä. PA-3050 -laite tarjoaa paljon tehoa kilpailukykyisellä hinnalla. Virtuaalitoteutuksen arviointiin otetaan VM-1000-HV, koska se on tehokkain virtuaalipalomuuri, mitä Palo Alto tarjoaa.

TAULUKKO 1. Palomuurien ominaisuuksia (Palo Alto Networks 2015)

| Ominaisuudet | PA-5020 | PA-3050 | VM-1000HV |
|---|---|---|---|
| Uhkien torjuntateho (Threat prevention throughput) | 2 Gbps | 2 Gbps | 600 Mbps |
| Yhteyksiä sekunnissa (Connections per second) | 120.000 | 50.000 | 8.000 |
| Suurin mahdollinen istuntojen määrä (Max sessions (IPv4 or IPv6)) | 1.000.000 | 500.000 | 250.000 |
| Turvallisuusalueita (Max security zones) | 80 | 40 | 40 |
| Turvallisuusprofiileja (Security profiles) | 500 | 250 | 250 |
| Virtuaalireitittimiä (Virtual routers) | 20 | 10 | 3 |
| Virtuaalijärjestelmiä (Base virtual systems) | 10 | 1 | 1 |
| Enimmäismäärä virtuaalijärjestelmiä (Max virtual systems) | 20 | 6 | - |
| DHCP-palvelimia (DHCP servers) | 20 | 10 | 3 |
| Globalprotectin enimmäismäärä samanaikaisia käyttäjiä (Max tunnels (SSL and IPSec)) | 5.000 | 2.000 | 500 |

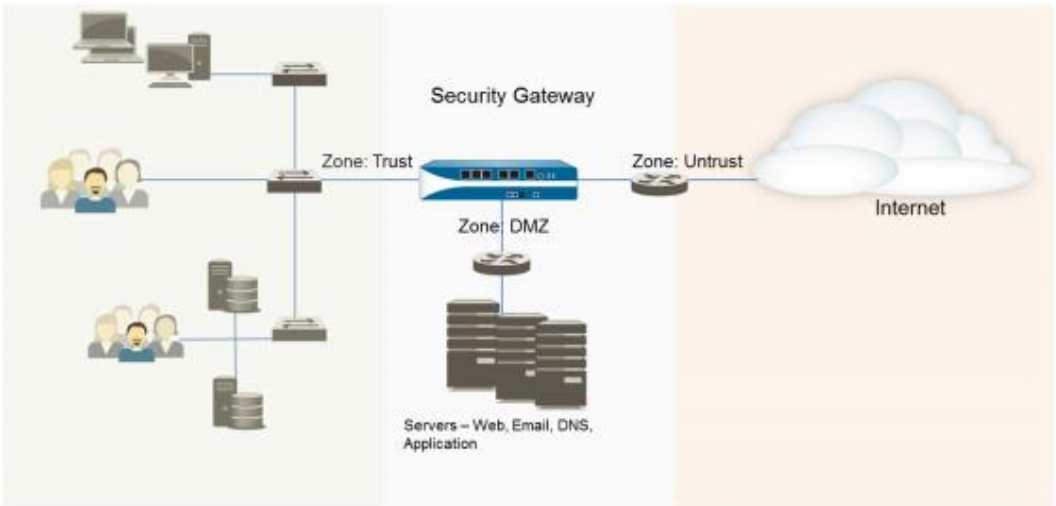
Yllä näkyvästä taulukosta (TAULUKKO 1) voidaan tarkastella eri laitteiden ominaisuuksia. Arvot on otettu Palo Alto Networksin laitteiden vertailusivulta. Arvot on valittu suuremmasta joukosta arvoja, jotka ovat tärkeitä ja eriäväisiä keskenään

tämän projektin sekä tulevaisuuden kannalta. Näin saadaan tarkempi käsitys laitteiden eroista.

”Uhkien torjuntateho”- ja ”yhteyksiä sekunnissa” -kentillä on otettava huomioon, että ne ovat mitattuja ihanneympäristössä, joten niiden todelliset arvot eivät välttämättä vastaa taulukossa olevia arvoja. Oletuksena on kuitenkin, että tämänhetkisellä käytöllä tehot ovat riittävät sekä PA-5020- ja PA-3050-palomuureille. Virtuaalipalomuurillakin on tällä hetkellä tarpeeksi toimintatehoa, mutta tulevaisuutta ajatellen se ei ole paras mahdollinen vaihtoehto.

Istuntojen määrät ovat riittävät kaikissa laitteissa. Virtuaalipalomuurilla jokaisella työntekijällä voisi olla 1000 istuntoa samanaikaisesti, joka sekin on jo epärealistisen suuri. Yrityksen internetsivut saattavat tosin kaivata samanaikaisia yhteyksiä, mutta oletuksena kuitenkin, että nämä istuntomäärät riittävät.

Turvallisuusalueet ovat verkon eri alueita. Alue on yhdistelmä fyysisiä ja virtuaalisia liittimiä, jotka kuvaavat eri verkon alueita. Oletuksena liikenne sallitaan saman alueen sisällä ja estetään eri alueiden välillä. Kuviossa 17 esitellään alueiden toimintatavat. Turvallisuusprofiilien avulla voidaan määritellä, sallitaanko vai estetäänkö liikenne eri alueiden, IP-osoitteiden (Internet Protocol), ohjelmien, käyttäjien tai palvelujen välillä. (Palo Alto Networks 2014d.)




KUVIO 17. Kuvassa esitellään kolme turvallisuusaluetta, jotka ovat Trust, DMZ ja Untrust (Palo Alto Networks 2014d)

Turvallisuusalueita ja -profiileja on jokaisessa laitteissa tarpeeksi. 5020-laitteessa on kuitenkin kaksinkertainen määrä molempia, minkä ansiosta tulevaisuuden tarpeet on myös varmistettu.

Virtuaalireitittimien avulla voi luoda virtuaalisia reitittimiä palomuurin sisälle. Näitä yritys voi mahdollisesti tarvita tulevaisuudessa.

Virtuaalijärjestelmän avulla voidaan luoda kokonaan uusi virtuaalinen palomuuri palomuurin sisälle. Virtuaalisella palomuurilla on itsenäinen hallintapaneeli, ja se toimii kuin se olisi fyysinen palomuuri. Näitä kohdeyritys tarvitsee kymmenen kappaletta. Tämän ehdon täyttää vain PA-5020-palomuuri. PA-3050-palomuuriin on mahdollista ostaa lisenssien avulla kuusi virtuaalipalomuuria, mutta sekään ei olisi optimaalinen yritykselle. VM-1000HV-virtuaalipalomuurille ei ole mahdollista ostaa lisenssien avulla virtuaalipalomuureja, joten sitä ei voi valita kahdennettavaksi palomuuriksi.

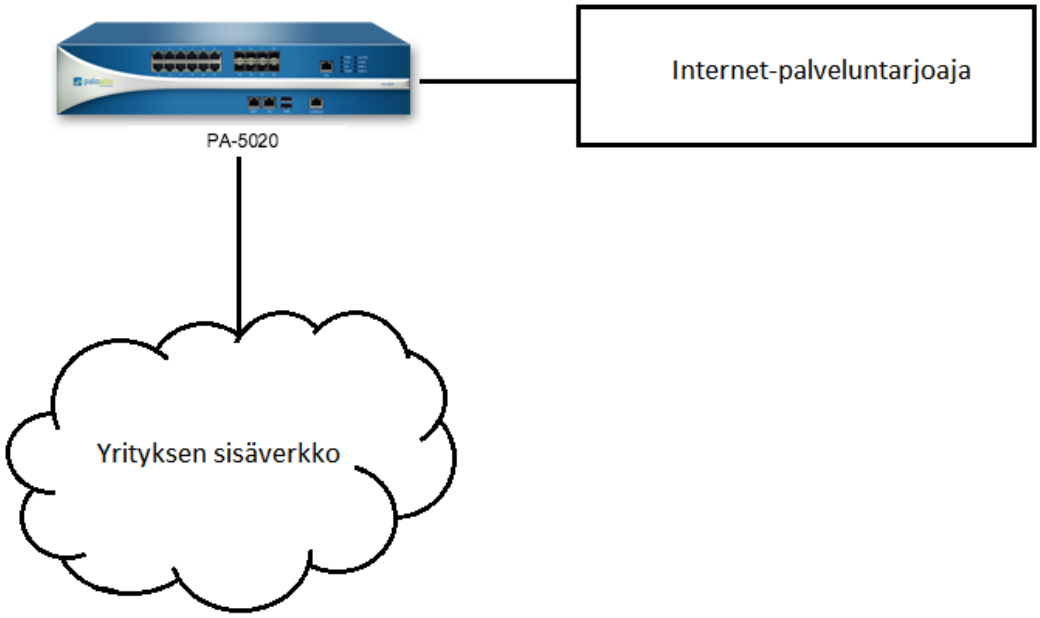
DHCP-palvelimia fyysisissä palomuureissa on tarpeeksi, mutta virtuaalipalomuurilla vain kolme kappaletta. Tästä saattaa koitua ongelmia yritykselle, mikäli jossain vaiheessa halutaan siirtyä palomuurin tarjoamaan DHCP-palvelimeen.

Globalprotect on Palo Alton VPN (Virtual Private Network) -toimintoalusta. Globalprotectin avulla on mahdollista ottaa yhteyttä yrityksen verkkoon internetistä. Olettaen, että yrityksen henkilöstömäärät eivät nouse paljon ja että suurin osa työskentelee sisäverkon kautta, niin kaikissa laitteissa on tarpeeksi tehoa hoitamaan yrityksen tarpeet tässä luokassa.

Taulukosta 1 voidaan havaita, että ainoa laite, joka täyttää yrityksen kaikki kriteerit, on PA-5020-laite. Tämän johdosta valitaan tämä kahdennettavaksi palomuuriksi. Palomuuri täyttää kaikki tämänhetkiset vaatimukset ja on tulevaisuutta ajatellen myös hyvä valinta. Siinä riittää suorituskykyä tämänhetkiseen tarpeeseen moninkertaisesti, joten voidaan olettaa laitteella olevan suhteellisen pitkä käyttöikä. Yritys omistaa myös jo valmiiksi yhden PA-5020-laitteen, jolloin riittää, että hankitaan samanlainen laite edellisen rinnalle.

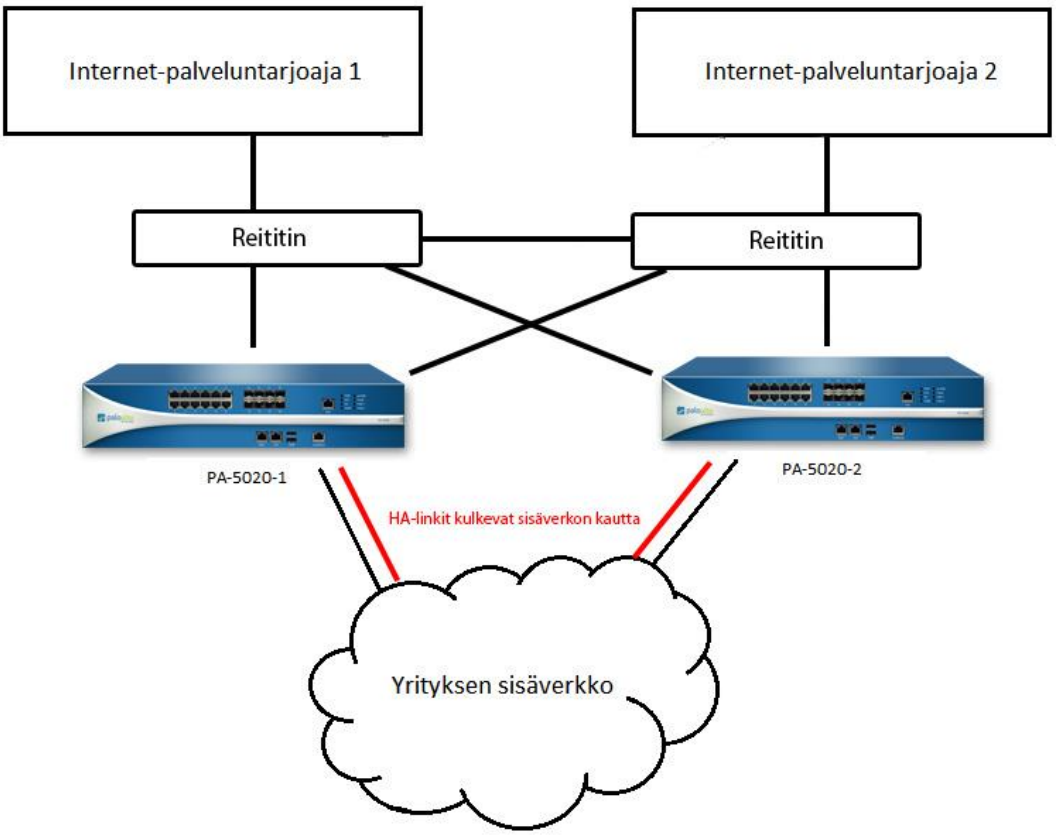
# 6 VERKKOTOPOLOGIA

Tämän työn tavoitteena on kahdentaa yrityksen pääpalomuuri ja varmistaa yrityksen internet-yhteys toisella internet-palveluntarjoajalla. Kuviossa 18 nähdään yrityksen alkuperäinen verkkotopologia, johon tullaan tekemään muutoksia.




KUVIO 18. Yrityksen alkuperäinen verkkotopologia

Kuten kuvasta (KUVIO18) huomataan, on tämänhetkinen verkko hyvin yksinkertainen. Internetin ja sisäverkon välillä toimii vain yrityksen pääpalomuuri. Kuvaan on lisättävä toinen ISP, HA-linkit, toinen pääpalomuuri ja ylimääräiset reitittimet BGP:tä varten, jotta toteutettava verkko (KUVIO19) saadaan aikaiseksi. Yritys on päättänyt sijoittaa toisen palomuurinsa eri datakeskukseen kuin toisen, jolloin on myös varauduttu siihen, että toinen datakeskus on jostain syystä saavuttamattomissa.




KUVIO 19. Toteutettavan verkon verkkotopologia.

## 6.1 Työn toteutustavat ja toteutustavan valinta

### 6.1.1 Aktiivi/aktiivi

Aktiivi/aktiivi-tilan voi toteuttaa useammalla eri tavalla. Ensimmäinen tapa on käyttää Virtual Wire -toteutustapaa. Tässä tilassa kaksi porttia yhdistetään loogisesti kaiken liikenteen kulkiessa portista toiseen niin, että sisältö tarkastetaan hallitusti (Palo Alto Networkin 2014b). Virtual Wire voidaan asentaa Layer 3 tason laitteiden väliin, jolloin käytetään dynaamista reititysprotokollaa, minkä avulla liikenne ohjataan toiselle HA-klusterin jäsenelle, mikäli tarvetta on. (Palo Alto Networks 2014a).

Toinen tapa toteuttaa HA on Floating IP. Tässä toteutustavassa jokaiselle linkille annetaan ylimääräinen IP-osoite (Floating IP) ja virtuaalinen MAC-osoite. Vian ilmetessä Floating IP ja virtuaalinen MAC-osoite siirretään toiselle HA-klusterin jäsenelle. Laitteita kutsutaan sisäverkosta Floating IP:n avulla. Tämä toteutustapa tukee myös ulkoisia kuormantasaajia, NAT-asetuksia (Network Address Transla-

tion) sekä VPN-toteutuksia (Virtual Private Network). (Palo Alto Networks 2014a.)

Kolmas toteutustapa on ARP load sharing. Tässä toteutustavassa HA-parille asetetaan jaettu IP-osoite, jota voi käyttää gateway-osoitteena. Vian ilmetessä toimiva laite ottaa haltuunsa Floating IP:n ja virtuaalisen MAC-osoitteen. Tässä toteutustavassa on oltava Layer 2 -erotus palomuurin ja sisäverkon välissä. (Palo Alto Networks 2014a.)

Neljäs toteutustapa on yhdistelmä Floating IP:tä ja ARP load sharingia. On mahdollista asettaa tietyt portit käyttämään Floating IP:tä ja toiset taas ARP load sharingia. (Palo Alto Networks 2014a.)

### 6.1.2 Aktiivi/passiivi

Aktiivi/passiivi-toteutus on huomattavasti yksinkertaisempi kuin aktiivi/aktiivi. Tässä toteutustavassa passiivi-tilassa oleva palomuuri odottaa aktiivi-palomuurin vikaantumista. Tilaa tarkastellaan jatkuvasti HA-linkin avulla. Tässä toteutustavassa ei myöskään tarvitse suunnitella sisäverkosta tulevan liikenteen ohjautumista palomuureille, NAT-asetusten toteutustapaa tai erikseen asennettavia load balancereita.

Huonoa toteutuksessa on se, että toinen palomuureista on täysin passiivisessa tilassa, jolloin sen tehot eivät ole käytettävissä. On myös mahdollista, että passiivisena toimiva laite ei sen koko käyttöikänä ole aktiivisessa toiminnassa, jolloin laite on ollut hyödytön.

## 6.2 Vertailu toteutustavoista ja toteutustavan valinta

Seuraavalla taulukolla (TAULUKKO 2) pyritään antamaan kuva eri toteutustavoista ja niiden tarjoamista hyödyistä ja haitoista. Ominaisuuksiksi on valittu tärkeitä huomioitavia asioita molemmista toteutustavoista.

TAULUKKO 2. Vertailua aktiivi/aktiivi ja aktiivi/passiivi -toteutustavoista.

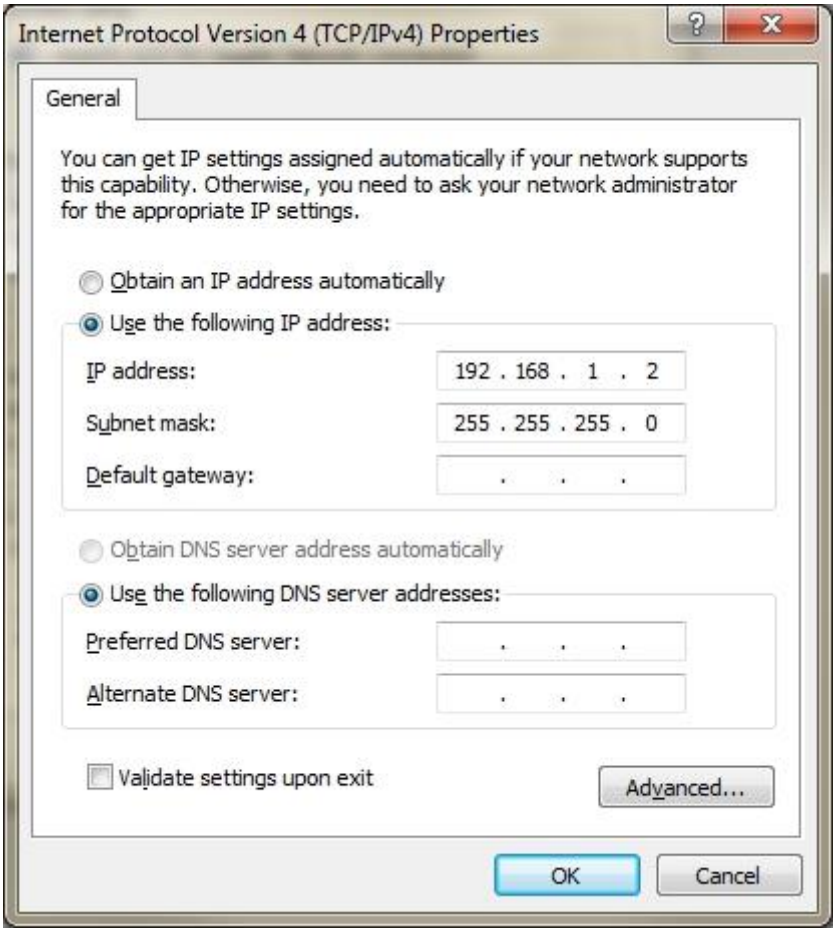
| Ominaisuus | Aktiivi/Aktiivi | Aktiivi/Passiivi |
|---|---|---|
| Molempien laitteiden aktiivinen hyödyntäminen | Kyllä | Ei |
| Yhteys ulkoverkkoon toimii, mikäli toinen laitteista vioittuu | Kyllä | Kyllä |
| HA-linkkien määrä | 3 | 2 |
| Verkon monimutkaistuminen | Monimutkaistuu selkeästi (vaatii enemmän IP-osoitteita ja suunnittelua) | Monimutkaistuu lievästi (ylimääräinen laite ympäristössä) |
| Ulkoverkon suunnittelu | Lievästi monimutkaisempi | Ei olennaisia muutoksia |
| Sisäverkon suunnittelu | Vaikeutuu lievästi (on määritettävä käytetäänkö Floating IP:tä, ARP load sharingia tai muuta vastaavaa) | Sisäverkon suunnittelu ei muutu olennaisesti |

Yrityksen kanssa päädyimme valitsemaan aktiivi/passiivi-toteutustavan. Tämä siksi, että se on taatusti toimiva ja aktiivi/aktiivi-toteutustapaa käytetään useimmiten asymmetrisesti reititetyssä ympäristössä, jota ei kohdeyrityksessä ole.

# 7 PALOMUURIN KÄYTTÖÖNOTTO

## 7.1 Palomuurin hallintapaneeliin pääsy

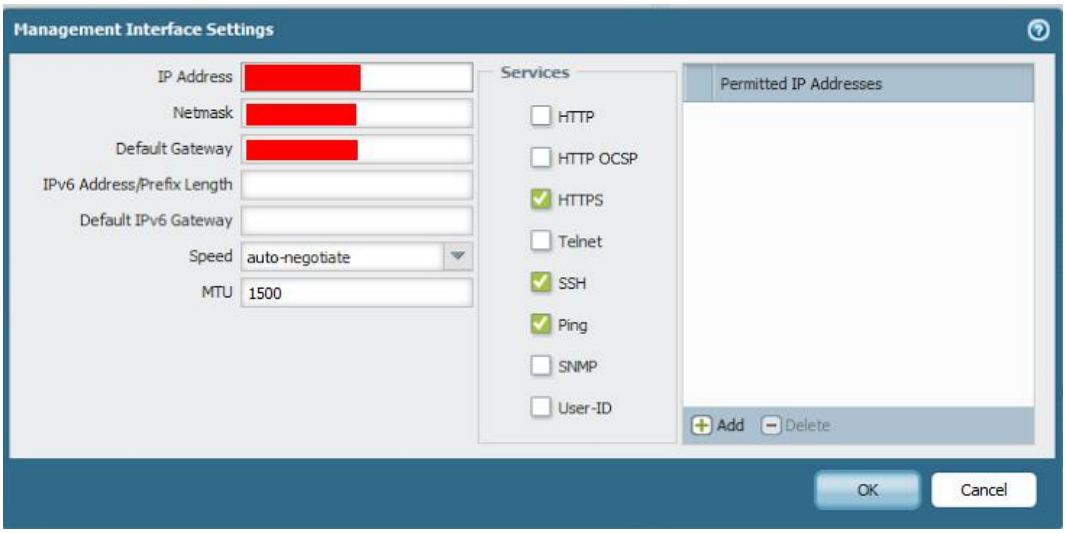
Perusasetukset, kuten IP-osoitteen asettaminen, VLANien (Virtual Local Area Network) määrittely ja muut vastaavat asetukset on hyvä laittaa heti aluksi kuntoon. Tämä onnistuu liittämällä tietokone Palo Alto -palomuurin mgmt-porttiin ja asettamalla tietokoneelle IP-osoite 192.168.1.0 -verkosta. IP-osoitteen vaihtaminen onnistuu Verkko- ja jakamiskeskuksesta Windows 7 -käyttöjärjestelmälliseltä koneelta kuvion 20 tavalla.




KUVIO 20. IP-osoitteen asettaminen tietokoneelle

Tämän jälkeen selaimen avulla voidaan ottaa yhteyttä Palo Alto -palomuuriin hallintasivustoon menemällä sivustolle https://192.168.1.1. Tämän jälkeen on mahdollista kirjautua sisään ja muokata laitteen mgmt-porttia verkkoon sopivaksi. Mgmt-portin asetuksia voi säätää siirtymällä Device->Management-

>Management Interface Settings ja klikkaamalla tämän oikealla puolella sijaitsevaa palloa. Tämän jälkeen aukeaa kuvan (KUVIO 21) mukainen ruutu, jonne on mahdollista asettaa mgmt-portin asetukset. On huomioitava, että näiden muutoksien jälkeen on valittava commit, jonka jälkeen mgmt-portin IP-asetukset astuvat voimaan, jolloin myös hallintapaneelin IP-osoite muuttuu.

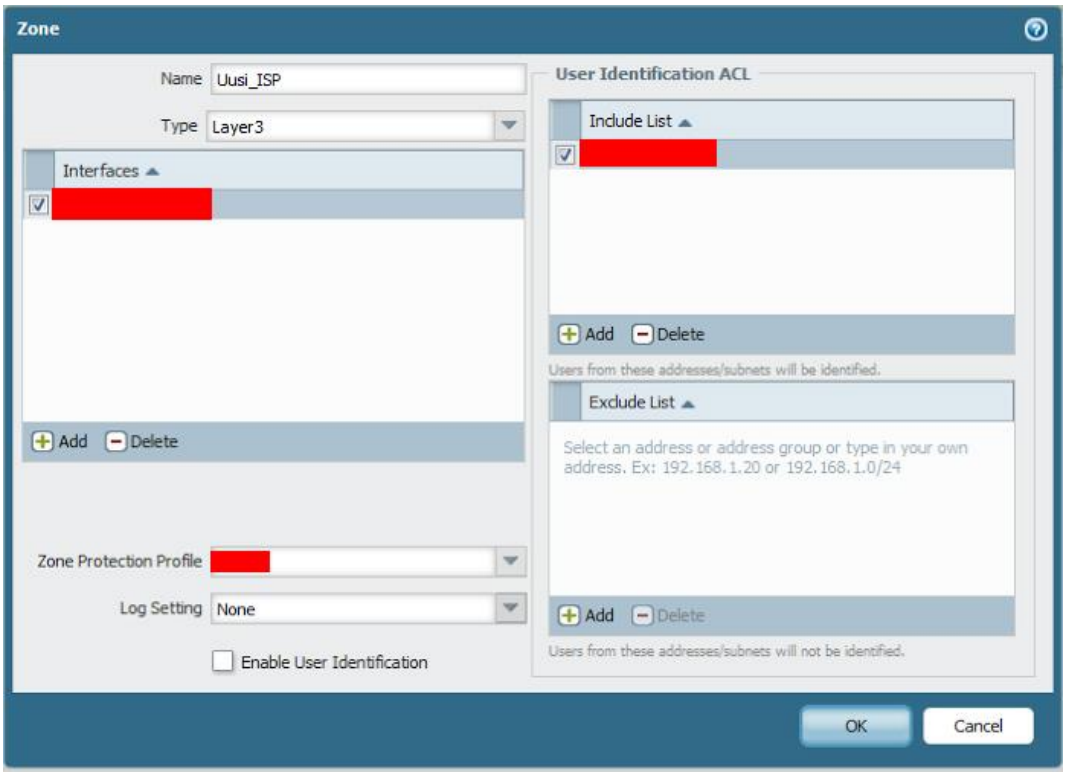



KUVIO 21. Mgmt-portin asetukset tehdään tässä ruudussa. Valittavana ovat yleiset verkkoasetukset ja käytettävät palvelut.

## 7.2 Palomuurin turvallisuusalueiden konfiguraatiot

Siirtymällä hallintapaneelissa Network -> Zones -ruudulle voidaan luoda erilaisia alueita palomuurille. Eri alueille voidaan luoda sääntöjä, jotka sallivat tai estävät liikenteen toisille alueille.

Uusi ISP (Internet Service Provider) asetetaan vanhan ISP:n kanssa samalle alueelle. Myöhemmin asennettavassa HA:ssa muut alueet tulevat automaattisesti passiivi-palomuurille. Alueiden luonti onnistuu seuraavanlaisesta ruudukosta (KUVIO 22).

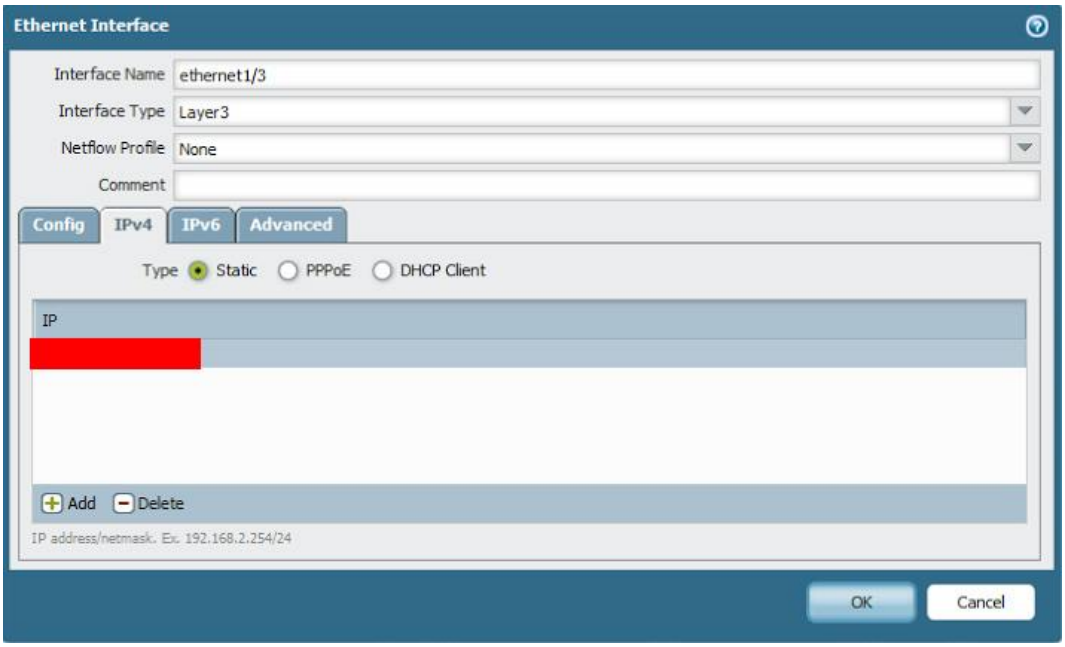



KUVIO 22. Alueiden luonti-ikkuna.

## 7.3 Palomuurin porttien konfiguraatiot

Siirtymällä hallintapaneelissa Network -> Interfaces -ruudulle voidaan asettaa laitteen eri portteihin asetuksia. Klikkaamalla haluttua porttia voidaan sille asettaa halutut asetukset.

Täällä asetetaan uudelle ISP-portille ISP:ltä saatu IP-osoite ja lisätään portti aikaisemmin konfiguroituun turvallisuusalueeseen (Security Zone). Esimerkki seuraavassa kuvassa (KUVIO 23).

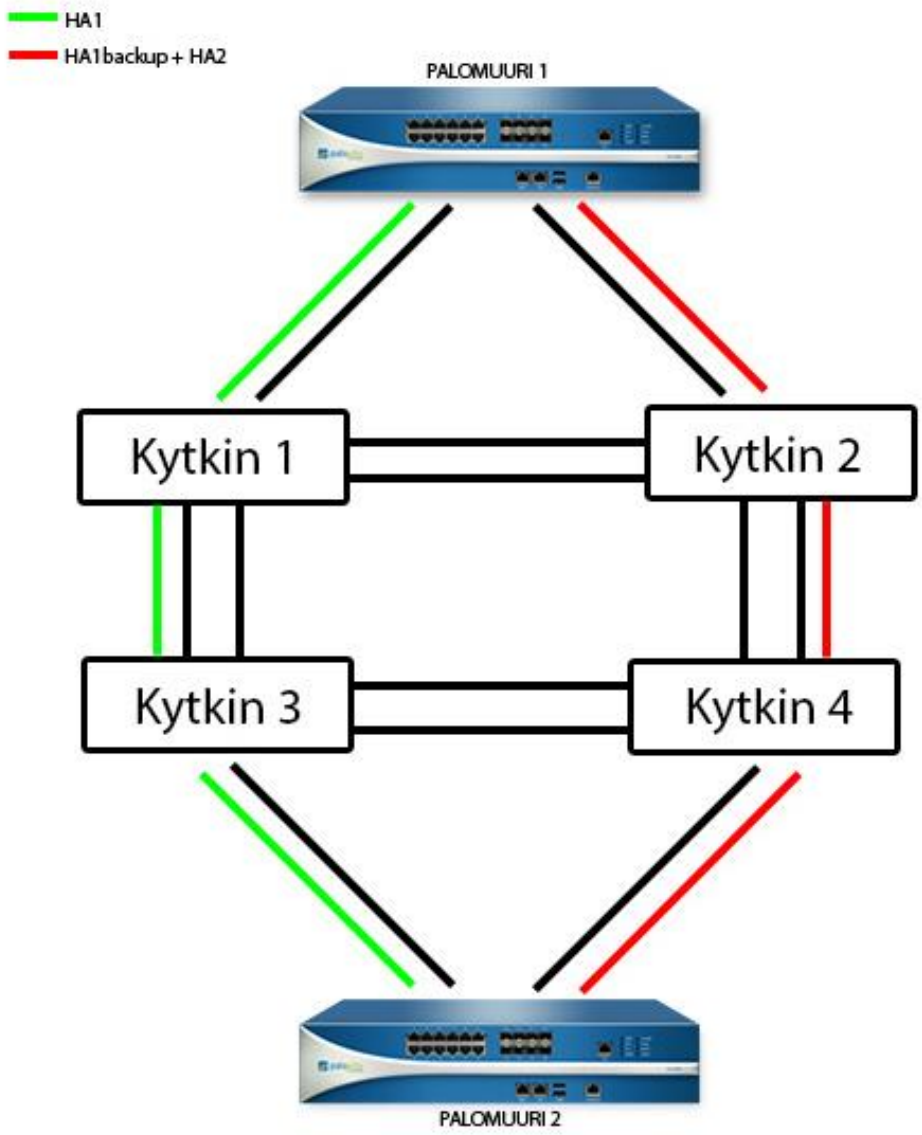



KUVIO 23. Porttien konfiguraatiot tehdään tämänlaisesta ruudusta

## 7.4 Palomuurin HA-asetusten konfigurointi

HA-asetukset asetetaan Device -> High Availability -> General -ruudussa. Molemmille palomuureille konfiguroidaan erilaiset asetukset, joten on varmistettava, kumpaan palomuuriin tehdään muutoksia.

On myös mietittävä HA-linkkien kuljetus verkon lävitse, mikäli ei ole mahdollisuutta liittää HA-linkkejä suoraan fyysisesti toisiinsa. Tätä varten luodaan yritykseen oma VLAN kytkimille ja asetetaan HA1- ja HA2-linkkiportit niihin. Toteutus on nähtävissä seuraavassa kuvassa (KUVIO 24). HA1:lle päätettiin asettaa varalinkki, mikäli yhteys ei jostain syystä toimi, jolloin PALOMUURI 2 käynnistyy automaattisesti. Tällöin verkossa alkaa ilmetä ongelmia, koska vain yhden palomuurin tulee olla käynnissä kerrallaan. HA1:n varalinkki sijoitettiin mgmt-portin taakse.

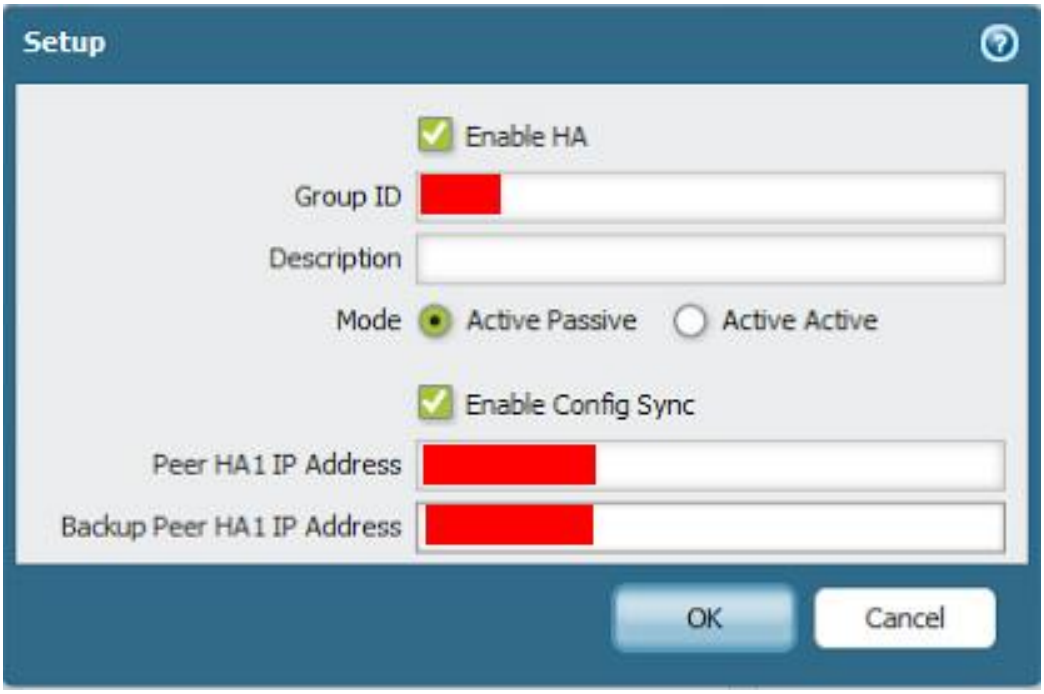



KUVIO 24. Yrityksen sisäverkko. Päätimme sijoittaa HA1:n kulkemaan kytkimien 1 ja 3 kautta, kun taas HA2:n ja HA1:n varalinkki (mgmt-portti) kulkee kytkimien 2 ja 4 kautta.

### 7.4.1 HA-asetukset

HA-asetukset asetetaan molemmille laitteille, minkä jälkeen ne voidaan synkronoida. Tämän jälkeen HA on käytössä. Laitteiden konfigurointi on hyvin samankaltaista, minkä takia näytetään vain toisen laitteen konfigurointi. Asetuksissa ainoat erot ovat IP-osoitteet ja Device Priority Election Settingsissä. Device Priority määrittelee sen, kumpi laite on aktiivinen ja kumpi passiivinen. Aktiivinen laite on se, jolla on pienempi Device Priority -arvo (Palo Alto Networks 2014c).

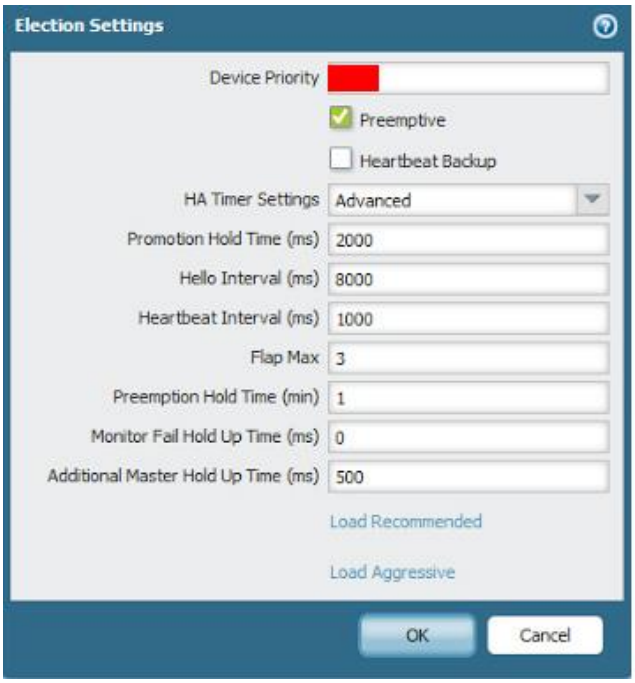
HA-asetukset otetaan käyttöön menemällä Device -> High Availability -> General -välilehdelle. Täältä klikataan Setup-ikkunan oikealla puolella olevaa palloa. Tämän jälkeen avautuu kuvan (KUVIO 25) mukainen ruutu, johon on mahdollista asettaa käytetty Group ID, HA-tapa ja HA1:n IP-osoite. Group ID pitää olla sama molemmissa palomuureissa.




KUVIO 25. HA:n konfigurointi-ikkuna

Tämän jälkeen asetetaan HA1-, HA1-backup ja HA2-porteille vastakkaisen puolen IP-asetukset. Kaikille löytyvät omat ikkunat General-välilehden alta.

Seuraavaksi asetetaan Election Settingsit (KUVIO 26). Täällä asetetaan aktiivi-palomuurille alhaisempi Device Priority -arvo kuin passiivi-palomuurille sekä otetaan käyttöön Preemtive-ominaisuus molemmilla palomuureilla. Tämä ominaisuus käynnistää aktiivi-palomuurin yliheiton jälkeen, mikäli yliheiton syy korjaantuu. Muut arvot pidetään oletusarvoisina.

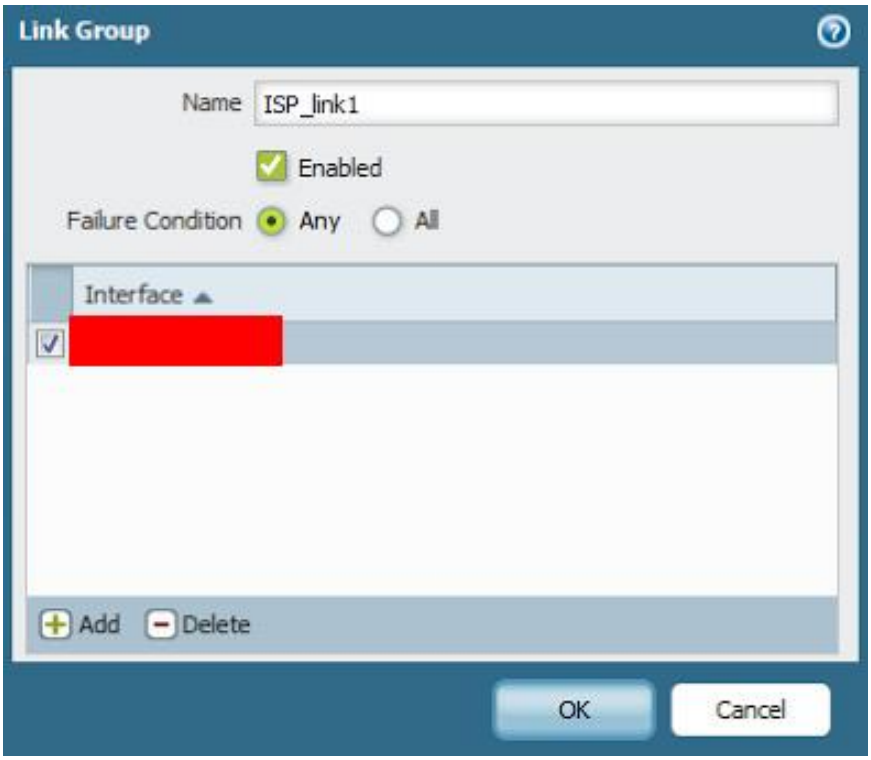



KUVIO 26. Passiivi-palomuurin asetukset. Election Settingsit asetetaan tämänlaisesta ikkunasta.

Tämän jälkeen asetetaan passiivi-palomuurille samankaltaiset asetukset, jonka jälkeen HA voidaan ottaa käyttöön menemällä Dashboard-välilehdelle aktiivi-palomuurilla ja klikataan ”sync to peer” -tekstiä. Synkronoinnin valmistuttua HA on käytössä.

### 7.4.2 Link and Path Monitoring -asetukset

Link and Path Monitoring asetuksia voi säätää menemällä Device -> High Availability -> Link and Path Monitorin -välilehdelle. Täällä voi asettaa sääntöjä, jolloin yliheitto tapahtuu. Link Monitoring -ominaisuudella voi tarkistaa, mikäli tietty linkki on alhaalla (KUVIO 27). Path Monitoring -ominaisuudella voi tarkistaa, jos tietty IP-osoite ei vastaa ping-paketteihin. Sääntöjä voi myös ryhmittää muuttaen Failure Condition -arvoa, jolloin yliheitto tapahtuu siihen määritetyn arvon täyttyessä. Arvo voidaan määrittää kaikkien ehtojen täyttyessä tai minkä tahansa ehdon täyttyessä.




KUVIO 27. Linkkiryhmän teko onnistuu tämänlaisen ruudukon takaa

Yliheittosuunnitelma muodostui seuraavanlaiseksi:

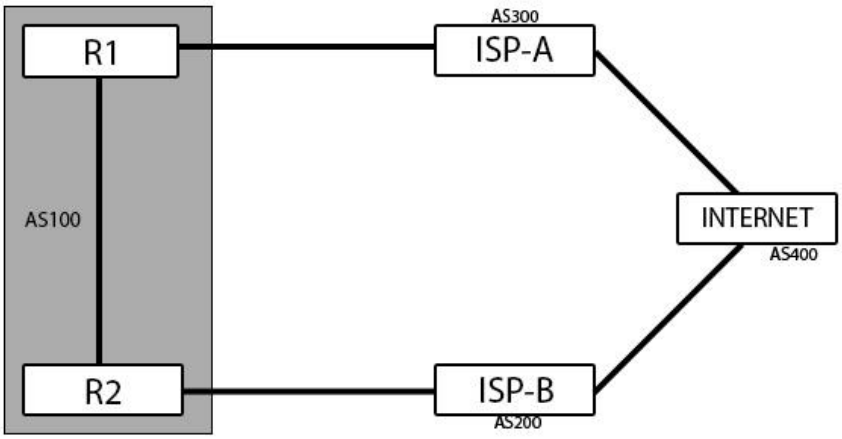
- Yrityksen Link Aggregate -linkit laitettiin omiksi ryhmikseen ja asetettiin niin, että molempien linkkien kuului olla alhaalla, jotta yliheitto tapahtuu. Link Aggregatet ovat kahdennettuja linkkejä.

- ISP:lle menevät linkit asetettiin ryhmäksi, ja molempien linkkien kuuluu olla alhaalla, jotta yliheitto tapahtuu.

- Molempien ISP:iden ja Googlen DNS-palvelimet asetettiin Path Monitoringiin.

## 7.5 BGP-asetukset

Palo Alton laitteet eivät pysty ylläpitämään BGP-naapurisuhdetta ollessaan passiivi-tilassa. Palomuureja ei siis kannata käyttää reunakytkiminä, vaan ISP:n ja palomuurien väliin on lisättävä reitittimet, jotka hoitavat BGP-asetukset. Kuviossa 28 nähdään esimerkkiin käytettyä verkkokuvaa.




KUVIO 28. BGP-asetusten esimerkkiverkko

Aluksi konfiguroidaan verkon laitteille IP-asetukset niin, että jokaisen laitteen välillä on oma verkkonsa. Tämän jälkeen asetetaan R1- ja R2-laitteiden välille iBGP-verkko. Tämä onnistuu liitteen (LIITE 1) komennoilla.

R2-laitteelle asetetaan muutoin samat komennot (LIITE 1), mutta neighbor-komentojen IP-osoitteeksi laitetaan R1:n IP-osoite. Network-komennolla mainostetaan oman AS:n verkkoja ja neighbor-komennolla määritellään naapurit. Kun molemmille laitteille on asetettu asetukset oikein, tulee viesti BGP-naapurisuhteen onnistuneesta luonnista. Tämän jälkeen määritellään eBGP-yhteydet R1:n ja ISP-A:n sekä R2:n ja ISP-B:n kanssa. Tämä onnistuu liitteen (LIITE 2) komennoilla.

Vastaavat komennot (LIITE 2) annetaan R2-laitteelle. Route-mapin avulla voidaan määritellä tarkemmin mistä AS:stä otetaan vastaan reititystietoja ja mitä mainostetaan ulospäin. Seuraavaksi luodaan route-mapit (LIITE 3).

Access-list komennolla (LIITE 3) luodaan aluksi lista numero 10, joka sallii 20.20.20.0-verkon ja käyttää wildcard maskia /8, joka tarkoittaa verkkoa 20.20.20.0-20.20.20.255. Route-map (LIITE 3) luo AS-300-IN -nimisen säännön, joka sallii access-listan numero 10 ja tarkistaa, että se vastaa as-path 1:n sallimia arvoja. Set local-preference (LIITE 3) asettaa preference-arvon, jonka avulla reititin määrittelee useamman mahdollisen reitin väliltä sen, jolla on korkein arvo

(Cisco 2015a). Luodaan as-path AS-300-IN-route-mapille liitteen (LIITE 4) komennolla.

Komennossa (LIITE 4) ^ tarkoittaa, että AS-numeron alku vastaa seuraavia numeroita ja $ lopettaa numeron. Tämä komento sallii AS-numerolta 300 tulevat tiedot ja siihen yhdistetyt linkit.

## 7.6 Testaussuunnitelma

Kun kaikki asetukset on laitettu kohdalleen, on tärkeää testata järjestelmän toimivuus. Kohdeyritykselle luotiin testaussuunnitelma, jonka avulla testataan verkon toimivuutta luomalla vikoja verkkoon. Testaussuunnitelma tehtiin pohtimalla mahdollisia vikatilanteita verkossa. Tämän jälkeen niitä simuloidaan sammuttamalla laitteita ja irrottamalla kaapeleita verkosta. Testaussuunnitelmaan sisältyy seuraavat vaiheet:

- Vaihe 1: Tarkistetaan, että yliheitto toimii. Tämä onnistuu katkaisemalla internet-yhteys pääpalomuurista. Tämän jälkeen passiivi-palomuurin tulee käynnistyä ja verkon toimia.

- Vaihe 2: Tarkistetaan, että HA2-linkin toimimattomuus ei käynnistä passiivi-palomuuria.

- Vaihe 3: Irrotetaan aktiivi-palomuuri ISP-verkoista, jolloin passiivi-palomuurin tulee käynnistyä.

- Vaihe 4: Testataan sisäverkkoa sulkemalla sisäverkon kytkimiä yksi kerrallaan niin, että yhteys katkeaa passiivi-palomuuriin.

- Vaihe 5: Testataan verkkoa irrottamalla kaapeleita ja tarkistetaan, että SPOF-pisteitä ei verkossa ole.

Testaussuunnitelma suoritettiin vajavaisesti, koska kohdeyrityksen muiden projektien johdosta ei ole voitu vielä hankkia toista internet-operaattoria tai projektiin tarvittavia kytkimiä. Testaus suoritettiin kuitenkin HA-asetusten osalta ja havaittiin muutamia tärkeitä seikkoja:

- Preemptive-ominaisuudessa havaittiin asioiden toimivan epävarmasti.
    - Yliheiton tapahtuessa havaittiin, että path monitoringin ollessa käytössä preemptive-ominaisuus käynnistää alkuperäisen aktiivi-palomuurin itsestään, koska laitteella on yhteys ulkoverkkoon toisen palomuurin kautta (tämä onnistuu siksi, että laite pystyy mgmt-portin kautta suorittamaan ping-komentoa ja mgmt-portin kautta on pääsy internetiin).
    - Siirtämällä fyysisesti kaikki johdot aktiivi-palomuurilta passiivi-palomuurille johti siihen, että passiivi-palomuuri aktivoitui. Tämä onnistui hyvin, mutta tämän jälkeen, kun johdot siirrettiin takaisin alkuperäiselle aktiivi-palomuurille, ei laite automaattisesti käynnistynyt. Tämän syynä voi olla erilaiset asetukset Link Monitoring -välilehdellä.
- Muutoin HA-asetusten käyttöönotto toimi odotusten mukaisesti.

### 7.7 Verkon vikasietoiseksi tekeminen

Palomuurin ja internetyhteyden kahdennusprojekti ei ole pieni asia yrityksessä, vaan projektiin on valmistauduttava hyvin ja projektin eri vaiheet tulee miettiä tarkkaan. Yrityksen pääpalomuuri saatiin kahdennettua, ja internetyhteyden kahdennus on kesken, johtuen yrityksen muista projekteista. Operaattoreille on esitetty tarjouspyyntö varainternetyhteydelle. Projektin pääkohtiin kuuluvat seuraavat vaiheet:

- kahdennettavan palomuurin valitseminen
    - valittavan palomuurin tulee yksin pystyä käsittelemään koko yrityksen tuottama kuorma, jotta yliheiton tapahtuessa ei ilmene suorituskykyongelmia
- kahdennuksen toteutustavan valinta (aktiivi/aktiivi vai aktiivi/passiivi)
- suunnitella, milloin yliheitto tapahtuu käyttäen hyödyksi Link and Path Monitorin -asetuksia

- järjestelmän laajamittainen testaus, jonka avulla varmistetaan järjestelmän toimivan odotetulla tavalla
- varaoperaattorin linkin asennus verkkoon ja yhteyden toimivuuden varmistaminen.

# 8 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli suunnitella ja toteuttaa Lahti Energia Oy:lle toimiva kahdennettu palomuuri kahden eri internet-palveluntarjoajan verkkoon. Tavoitteena oli myös tutustua yleisesti tietoturvaan, palomuureihin, kahdentamiseen ja BGP-protokollaan. Tämän lisäksi opinnäytetyössä tarkasteltiin palomuurin valintaan liittyviä kysymyksiä, siltä vaadittuja ominaisuuksia ja luotiin yleinen asennusohje kahdennettavalle palomuurille ja BGP-asetuksille.

Palomuurin avulla on mahdollista suojautua internetistä kohdistetuilta hyökkäyksiltä ja haitallisilta tiedostoilta. Tänä päivänä sovellustason palomuurit voivat tutkia verkosta tulevia paketteja ja sisällön perusteella määritellä, onko kyseessä haitallista liikennettä.

Kahdentamisen avulla on mahdollista parantaa verkon ja laitteiden toimivuutta. Yhden laitteen vikaantuminen ei saa kaataa koko yrityksen verkkoa. SPOF-pisteiden syntyä tulee välttää ja pohtia ratkaisuja, joissa niitä ei ilmene.

BGP:tä käytetään ylemmän tason palveluntarjoajien verkoissa ja isoissa yrityksissä. BGP antaa mahdollisuuden multihoming-toteutukseen, jonka avulla voidaan hyödyntää useampaa internet-palveluntarjoajaa, mikä taas parantaa yrityksen verkon saatavuutta huomattavasti. BGP käyttää reitityksessä hyödykseen AS-numeroita.

Palomuurin valitsemisessa on tämän hetken tarpeiden lisäksi huomioitava tulevaisuuden tarpeet. Verkossa oleva käyttäjämäärä ja verkon nopeustarve voivat kasvaa. Hyvä palomuuri on investointi yrityksen tulevaisuuteen. Edellä mainitut kriteerit täytti valittu palomuuri, joka oli Palo Alton PA-5020.

Järjestelmä tulee valmistuttuaan testata laajamittaisesti. Testaaminen kannattaa suorittaa ajan kanssa tarkasti laaditun suunnitelman avulla. Mikäli virheitä huomataan, on ne hyvä kirjata ylös ja selvittää ongelmien syy. Tarkasti testatun järjestelmän avulla IT-henkilökunta voi luottaa verkon toimivuuteen.

Testaus suoritettiin Palo Alton HA-asetuksille, joissa havaittiin pieniä ongelmia liittyen preemptive-ominaisuuteen. Ominaisuus uudelleenkäynnisti alkuperäisen aktiivi-palomuurin, vaikka siinä ei internetyhteys toiminut. Toisessa testissä sen

sijaan huomattiin, että aktiivi-palomuurin olisi pitänyt uudelleenkäynnistyä virheiden korjattua, mutta näin ei tapahtunut. Link and Path Monitoring -asetuksia on tarkasteltava uudestaan koko järjestelmän ollessa käytössä.

Nykyään tietoverkoilta vaaditaan paljon. Laitteiden ja palveluiden tulee olla jatkuvasti saatavilla; mikäli ne eivät ole, yritys saa huonoa mainetta huonosti hoidetuista web-sivuista tai palveluista. Kahdennus lisää palveluiden saatavuutta ja helpottaa verkon ylläpitäjien työtaakkaa antamalla heille enemmän aikaa reagoida rikkinäisiin laitteisiin.

LÄHTEET

Belden. 2015. Redundancy. Avoid Single Points of Failure [viitattu 29.3.2015]. Saatavissa: http://www.belden.com/products/industrialnetworking/redundancy/

Cisco. 2014. Introducing BGP Confederations [viitattu 12.11.2014]. Saatavissa: http://www.cisco.com/web/learning/le31/le46/cln/qlm/CCIP/bgp/introducing-bgp-confederations-2/player.html

Cisco. 2015a. BGP Case Studies - Cisco [viitattu 19.3.2015]. Saatavissa: http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

Cisco. 2015b. What Is Network Security? [viitattu 29.3.2015]. Saatavissa: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html

Lahti Energia. 2014. Lahti Energia [viitattu 12.11.2014]. Saatavissa: http://www.lahtienergia.fi/lahti-energia

Orbit-Computer Solutions. 2014. BGP: Border Gateway Protocol Explained [viitattu 12.11.2014]. Saatavissa: http://www.orbit-computer-solutions.com/BGP.php

Palo Alto Networks. 2014a. Configuring Active/Active HA [viitattu 1.12.2014]. Saatavissa: https://live.paloaltonetworks.com/servlet/JiveServlet/previewBody/2541-102-4-25153/HA-Active-Active-Tech-Note.pdf

Palo Alto Networks. 2014b. Computer Networking and Security - Networking Architecture [viitattu 1.12.2014]. Saatavissa: https://www.paloaltonetworks.com/products/features/networking.html

Palo Alto Networks. 2014c. How to Configure High Availability on PAN-OS [viitattu 1.12.2014]. Saatavissa: https://live.paloaltonetworks.com/docs/DOC-2926

Palo Alto Networks. 2014d. PAN-OS® Getting Started Guide [viitattu 1.12.2014]. Saatavissa:

https://live.paloaltonetworks.com/servlet/JiveServlet/previewBody/6604-102-10-31001/PAN-OS-6.0-GSG.pdf

Palo Alto Networks. 2014e. Redundancy and Resiliency Features for Your Firewall [viitattu 12.11.2014]. Saatavissa: https://www.paloaltonetworks.com/products/features/redundancy.html

Palo Alto Networks. 2015. Compare Firewalls [viitattu 15.4.2015]. Saatavissa: https://www.paloaltonetworks.com/products/product-selection.html

RFC2918. 2000. Route Refresh Capability for BGP-4 [viitattu 1.12.2014]. Saatavissa: http://tools.ietf.org/html/rfc2918

RFC4271. 2006. A Border Gateway Protocol 4 (BGP-4) [viitattu 1.12.2014]. Saatavissa: http://tools.ietf.org/html/rfc4271

RFC4456. 2006. BGP Route Reflection - An alternative to Full Mesh Internal BGP [viitattu 29.3.2015]. Saatavissa: http://tools.ietf.org/html/rfc4456

SearchFinancialSecurity. 2015. Firewall redundancy: Deployment and benefits [viitattu 22.1.2015]. Saatavissa: http://searchfinancialsecurity.techtarget.com/tip/Firewall-redundancy-Deployment-scenarios-and-benefits

TechTarget. 2015. What is firewall [viitattu 29.3.2015]. Saatavissa: http://searchsecurity.techtarget.com/definition/firewall

Viestintävirasto. 2013. Kohdistetut hyökkäykset [viitattu 1.12.2014]. Saatavissa: https://www.viestintavirasto.fi/attachments/esitykset/Kohdistetut_hyokkaykset.pdf

WhatIs.com. 2015. Confidentiality, integrity, and availability (CIA triad) [viitattu 29.3.2015]. Saatavissa: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

WindowsITPro. 2014. Build Redundancy into Your LAN/WAN [viitattu 18.12.2014]. Saatavissa: http://windowsitpro.com/networking/build-redundancy-your-lanwan

WindowsNetworking.com. 2014. The importance of Network Redundancy [viitattu 12.11.2014]. Saatavissa: http://www.windowsnetworking.com/articles-tutorials/netgeneral/Importance-Network-Redundancy.html

Wikipedia. 2014a. Autonomous System (Internet) [viitattu 12.11.2014]. Saatavissa: http://en.wikipedia.org/wiki/Autonomous_System_(Internet)

Wikipedia. 2014b. Border Gateway Protocol [viitattu 12.11.2014]. Saatavissa: http://en.wikipedia.org/wiki/Border_Gateway_Protocol

Wikipedia. 2014c. High availability [viitattu 12.11.2014]. Saatavissa: http://en.wikipedia.org/wiki/High_availability

Wikipedia. 2014d. Palomuuri [viitattu 12.11.2014]. Saatavissa: http://fi.wikipedia.org/wiki/Palomuuri

Wikipedia. 2014e. Redundancy (engineering) [viitattu 13.12.2014]. Saatavissa: http://en.wikipedia.org/wiki/Redundancy_(engineering)

Wikipedia. 2014f. Regional Internet registry [viitattu 12.11.2014]. Saatavissa: http://en.wikipedia.org/wiki/Regional_Internet_registry

# LIITTEET

## LIITE 1

```
R1(config)#router bgp 100
R1(config-router)#bgp log-neighbor-changes
R1(config-router)#network 10.10.10.0 mask 255.255.255.0
R1(config-router)#network 20.20.20.0 mask 255.255.255.0
R1(config-router)#neighbor 192.168.1.2 remote-as 100
R1(config-router)#neighbor 192.168.1.2 next-hop-self
```

LIITE 2

```
R1(config-router)#neighbor 192.168.30.2 remote-as 300
R1(config-router)#neighbor 192.168.30.2 route-map AS-300-IN in
R1(config-router)#neighbor 192.168.30.2 route-map AS-300-OUT out
```

LIITE 3

```
R1(config)#access-list 10 permit 20.20.20.0 0.0.0.255
R1(config)#access-list 20 permit 10.10.10.0 0.0.0.255
R1(config)#route-map AS-300-IN permit 10
R1(config-route-map)#match as-path 1
R1(config-route-map)#set local-preference 200
R1(config)#route-map AS-300-OUT permit 10
R1(config-route-map)#match ip address 10
R1(config-route-map)#set as-path prepend 100
R1(config)#route-map AS-300-OUT permit 20
R1(config-route-map)#match ip address 20
```

LIITE 4

R1(config)#ip as-path access-list 1 permit ^300$