LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Kahden WAN-liitännän hyödyntäminen palomuurissa

Case: Hiihdon MM-kisat 2017 mediakeskus

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2017
Kimmo Piirainen

Lahden ammattikorkeakoulu
Tietotekniikka

PIIRAINEN, KIMMO:

Kahden WAN-liitännän hyödyntäminen palomuurissa
Case: Hiihdon MM-kisat 2017 mediakeskus

Tietoliikennetekniikan opinnäytetyö, 39 sivua

Kevät 2017

TIIVISTELMÄ

Tutkimuksen tavoitteena oli selvittää kahden eri palomuurin soveltuvuus hiihdon MM-kisojen tietoverkkojen tarpeisiin. Opinnäytetyö tehtiin Lahden ammattikorkeakoulun tekniikan alalle.

Palomuuri sijaitsee yrityksen tietoverkon ja julkisen verkon, kuten Internetin, välissä suodattaen ja valvoen pakettien kulkua verkkojen välillä. Palomuurien tarkoituksena on parantaa yrityksen tietoturvaa estämällä ei-toivottua liikennettä pääsemästä yrityksen sisäverkkoon.

Tutkimuksessa keskityttiin palomuurien yleisiin ominaisuuksiin, jotka ovat merkittäviä Lahden ammattikorkeakoulun toteuttamien tietoverkkojen kannalta hiihdon MM-kisoissa. Tutkimukseen valittiin kaksi palomuuria, joiden ominaisuuksia vertailtiin laitteista saatavilla olevien tietojen perusteella. Opinnäytetyöhön valitut palomuurit olivat pfSense ja Cisco RV320.

Valituista palomuureista testattiin eroja, joita löytyy toimivuudessa ja käytettävyydessä. Konfiguraatioiden ja yleisen toimivuuden testauksen lisäksi laitteilla suoritettiin verkon nopeuden mittaukset. Testauksen ympäristönä toimi koulun tietoliikennelaboratorio. Testien perusteella palomuurit eivät eronneet toisistaan merkittävästi. Suurimmaksi eroavaisuudeksi nousi laitteiston kahdennuksen mahdollisuus.

Tehdyn tutkimuksen tulosten perusteella pystyttiin suosittelemaan pfSensen palomuuria tuotantoympärisössä käyttöönotettavaksi. Sen merkittävimpänä etuna oli laajempi vikasietoisuus kuin Cisco RV320:llä. Vikasietoisuus ja jatkuva yhteys Internetiin olivat tärkeitä ominaisuuksia palomuurin valinnassa tuotantoympäristöön.

Asiasanat: palomuuri, tietoturva, tietoverkot, pfSense, Cisco

Lahti University of Applied Sciences
Degree Programme in Information Technology

PIIRAINEN, KIMMO:

Utilization of Dual-WAN in firewalls
Case: Nordic World Ski
Championships 2017 Media Centre

Bachelor's Thesis in Telecommunications, 39 pages

Spring 2017

ABSTRACT

The aim of this thesis was to study the basic elements of firewalls and to examine the suitability of two different firewalls for the networks of the Nordic World Ski Championships. The thesis was executed for Lahti University of Applied Sciences, Faculty of Technology.

A firewall filters packets and stands between a corporate network and a public network like the Internet. Firewalls are focused on enhancing information security by preventing unwanted network traffic from entering corporate local area networks.

In this thesis the focus was on general attributes of firewalls which were crucial to the networks implemented by Lahti University of Applied Sciences at the Nordic World Ski Championships. Two firewalls were chosen for comparision, based on the available information. The chosen firewalls were pfSense and Cisco RV320.

Differences in functionality and usability of the two firewalls were examined. In addition to testing configurations and general operation, network speed measurements were made on both firewalls. The testing and measurements took place in the telecommunications laboratory at the campus. The firewalls did not differ significantly, according to test results. The most noticeable difference between the firewalls was the ability to perform firewall redundancy.

Based on the results of the study, it was possible to recommend the deployment of the pfSense firewall in the work environment. The major benefit of pfSense was a broader range of options to perform failover. The failover ability and continuous connection to the Internet were significant features when selecting a suitable firewall for the work environment.

Key words: firewall, information security, data networks, pfSense, Cisco

SISÄLLYS

LYHENNELUETTELO

BGP	Border Gateway Protocol. Reititysprotokolla.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, joka jakaa automaattisesti verkkoasetukset päätelaitteille.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka muuntaa verkkotunnukset IP-osoitteiksi.
HA	High Availability. Laitteiden jatkuvaan toimintaan tähtäävä vikasietoinen ratkaisu.
HTTP	Hypertext Transfer Protocol. Protokolla, jota käytetään tiedonsiirtoon www-ympäristössä.
HTTPS	Hypertext Transfer Protocol Secure. Salattu tiedonsiirtoprotokolla.
ICMP	Internet Control Message Protocol. Kontrolliprotokolla, jota käytetään viestien lähetykseen koneiden välillä.
IP	Internet Protocol. Internetin ydinprotokolla, jota käytetään IP-pakettien toimittamiseen pakettikytkentäisessä verkossa.
IPsec	IP Security Architecture. Turvattu Internet-yhteyksien protokolla.
LACP	Link Aggregation Control Protocol. Protokolla, jolla voidaan yhdistää useita Ethernet-liitäntöjä yhdeksi loogiseksi linkiksi.
LAN	Local Area Network. Rajatulla alueella sijaitseva lähiverkko, jota hallinnoidaan paikallisesti.
NAT	Network Address Translation. Tekniikka, jossa lähiverkon osoitteet muunnetaan julkisiksi IP-osoitteiksi.
OSPF	Open Shortest Path First. Standardoitu TCP/IP-reititysprotokolla.

PPTP	Point-to-Point Tunneling Protocol. VPN-tunnelointiprotokolla Windows-työaseman ja Windows-palvelimen välillä.
RAID	Redundant Array of Independent Disks. Tekniikka, jolla yhdistetään useampi kiintolevy yhdeksi loogiseksi levyksi.
RIP	Routing Information Protocol. Etäisyysvektoriin pohjautuva standardoitu reititysprotokolla.
SNMP	Simple Network Management Protocol. Standardoitu TCP/IP-tietoverkkojen hallinnassa käytettävä protokolla.
SSH	Secure Shell. Tietoturvallinen salatun tietoliikenteen protokolla.
SSL	Secure Sockets Layer. Salausprotokolla, jolla suojataan Internet-sovellusten tietoliikenne IP-verkoissa.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla luotettavaan tiedonsiirtoon.
TCP/IP	Transmission Control Protocol / Internet Protocol. Tietoverkkoprotokollien yhdistelmä, jossa tietoliikenne tapahtuu pääasiassa TCP-yhteyksinä IP-protokollan päällä.
UDP	User Datagram Protocol. Tietoliikenneprotokolla ilman pakettien vastaanoton varmistusta.
VLAN	Virtual LAN. Teknikka, joka mahdollistaa fyysisen tietoverkon jakamisen loogisiin lähiverkkoihin.
VPN	Virtual Private Network. Tekniikka, jolla laite tai kokonainen verkko voidaan yhdistää yrityksen yksityiseen verkkoon julkisen verkon yli.
WAN	Wide Area Network. Maantieteellisesti laajojen alueiden tietoverkkoja, jotka yhdistävät pienempiä verkkoja toisiinsa.
WWW	World Wide Web. Internetissä toimiva hypertekstijärjestelmä.

1 JOHDANTO

Tämän opinnäytetyön tavoitteena on vertailla kahta palomuuria ja sen perusteella antaa suositus, kumpaa laitteista käytetään Lahden ammattikorkeakoulun tekniikan alan toteuttamissa tietoverkoissa hiihdon MM-kisoissa Lahdessa helmi-maaliskuussa 2017. Lahden ammattikorkeakoulun vastuulla on toteuttaa mediakeskuksen tietoverkot toimittajien käyttöön. Opinnäytetyö tehdään Lahden ammattikorkeakoulun (LAMK) tekniikan alan toimeksiannosta ja ympäristönä käytetään oppilaitoksen tietoverkkolaboratoriota. Toimeksianto oli hyvin avoin ja annettu vain pääpiirteittäin, joten toimeksianto mahdollisti laajat vapaudet työn toteutukseen.

Lahden ammattikorkeakoulu on osakeyhtiömuotoinen monialainen korkeakoulu. LAMK:n koulutusaloja ovat liiketalous, matkailu, muotoilu ja viestintä, musiikki, kuvataide, sosiaali- ja terveysala sekä tekniikka. Lahden ammattikorkeakoulussa henkilöstöä on yli 400 ja tutkinto-opiskelijoita vuosittain noin 5 000. (Lahden ammattikorkeakoulu 2016.)

Tässä opinnäytetyössä selvitetään aluksi yleisellä tasolla palomuureja ja niiden ominaisuuksista. Tämän jälkeen tutustutaan palomuurin kannalta oleellisiin lähiverkon ominaisuuksiin. Tarkasteltaviksi kohteiksi valittiin sellaisia asioita, jotka vaikuttavat ja ovat oleellisia palomuurien mahdollisessa tuotantoympäristössä MM-kisoissa.

Valittujen palomuurilaitteiden vertailu tapahtuu ensin teoriapohjalta niiden ominaisuuksien ja teknisten tietojen perusteella. Käytännön testauksessa selvitetään muun muassa palomuurien käyttöönoton helppoutta, vikasietoisuutta, läpäisynopeutta sekä muiden ominaisuuksien toimivuutta käytännön tasolla. Testiympäristönä koulun tietoverkkolaboratoriosta löytyy riittävästi laitteita ja muita resursseja työn toteutukseen.

2 PALOMUURIT

2.1 Palomuurien käyttötarkoitus

Palomuureja käytetään ulkopuolisia hyökkäyksiä vastaan suojautumiseen. Palomuuri sijoitetaan yleensä yrityksen sisäisen lähiverkon ja julkisen tietoverkon väliin valvomaan läpi kulkevaa tietoliikennettä. Niiden avulla voidaan estää pääsy verkosta toiseen ei-halutulle liikenteelle. Palomuuri on mahdollista toteuttaa ohjelmistopohjaisesti tietokoneessa, erillisellä palomuurilaitteella tai reitittimellä. (Elers 2016.)

Liikennettä valvotaan palomuurin reititysominaisuuden avulla. Jokainen palomuurin kautta kulkeva IP-paketti (Internet Protocol) tarkistetaan ja analysoidaan annettujen sääntöjen mukaisesti. Säännöillä voidaan määritellä IP-paketin otsikkokentän perusteella, päästetäänkö paketti läpi vai hylätäänkö paketti. Sääntöjen perusteena voidaan käyttää protokollaa ja kohteen sekä lähteen IP-osoitetta. Pääsääntöisesti sisäverkosta ulkoverkkoon lähtevän liikenteen osoite muutetaan osoitteenmuunnoksella (NAT) näyttämään siltä, että liikenne on lähtöisin palomuurista, jotta sisäverkon osoitteet eivät ole näkyvillä ulkoverkkoon. (Suomen Internetopas 2016.)

Palomuureilla voidaan suojautua suoraan verkosta tulevilta tietoturvauhilta. Ajantasalla oleva suojautuminen vaatii myös palomuurin ylläpitoa sekä käyttäjien vastuullista ja huolellista toimintaa. Käyttäjät voivat aiheuttaa tietämättään tai huolimattomuudellaan palomuurin tuoman tietoturvan pettämisen. Esimerkiksi huijaussivuistoille tai -sähköposteihin luovutettu salasana tai avokonttorille jäänyt lukitsematon päätelaite tarjoavat mahdollisuuksia päästä yrityksen sisäverkkoon palomuurin ohi. (Elers 2016.)

2.2 Tilaton palomuuri

Tilaton palomuuri eli pakettisuodatin (Stateless Firewall tai Packet Filter) tarkistaa yksinkertaisuudessaan vain pakettien IP- tai TCP/UDP-tiedot, joiden perusteella palomuuri päättää, sallitaanko datan kulkeminen. Tämä voidaan toteuttaa asettamalla reitittimelle Access Control List (ACL) -sääntöjä. (Shimonski, Shinder, Shinder & Carasik-Henmi 2003, 56.)

Tilattoman palomuurin heikkous on juuri siinä, että palomuuri ei tutki ovatko paketit osa avoinna olevaa yhteyttä. Sille riittää, että paketin lähde tai kohde IP-osoite, lähde- tai kohdeportti tai protokollan tyyppi, kuten TCP, UDP tai ICMP, täsmäävät asetettuihin ACL-listan konfiguraatioihin. Pakettisuodatus aiheuttaa vain vähän viivettä liikenteelle, koska paketit ainoastaan reititetään eteenpäin. (Shimonski ym. 2003, 56.)

2.3 Tilallinen palomuuri

Tilallinen palomuuri (Statefull Firewall) on kehittyneempi versio tilattomasta palomuurista. Tilallisen palomuurin tarkoituksena on mahdollistaa hyvä yhteysnopeus, mutta parantaa tilattoman palomuurin tietoturvaa. Tilalliset palomuurit pitävät listaa avoinna olevista yhteyksistä ja niiden tiloista. Saapuvan paluupaketin tiedot voidaan verrata tilataulussa oleviin tietoihin ja todentaa näillä tiedoilla paketin alkuperäisyys ja oikeellisuus. Tilatauluun luodaan tieto ensimmäisestä TCP-session yhteydenavauspaketista alkaen ja taulua päivitetään yhteyden jatkuessa. Tietyn ajan kuluttua yhteystiedot vanhenevat automaattisesti tilataulusta. (Shimonski ym. 2003, 56.)

UDP-protokollan yhteyksissä voidaan käyttää myös tilallista palomuuria. Tilatauluun muodostuu merkintä, kun ensimmäinen UDP-paketti lähtetään. Paluupaketti sallitaan vain siinä tapauksessa, että sille löytyy sopiva merkintä tilataulusta. Tilallainen palomuuri mahdollistaa myös monimutkaisempien protokollien, kuten FTP (File Transfer Protocol), käytön. Esimerkiksi FTP-protokollan tiedonsiirrossa yhteys avataan porttiin 21, mutta paluupaketit tulevat takaisin porttiin 20. Tilallinen palomuuri

pystyy pitämään kirjaa näistä yhteyksistä ja yhdistämään saman yhteyden paketit eri portteihin. (Shimonski ym. 2003, 56.)

2.4 Sovelluspalomuuri

Sovellustason palomuurit (Application Proxy Firewall) toimivat niin sanottuina välikäsinä verkkoliikenteelle. Käyttäjän yhdistäminen ulkoverkkoon tapahtuu normaalisti palomuurin välityksellä, mutta kahtena eri istuntona. Näistä ensimmäinen on päätelaitteen ja palomuurin välinen yhteys, jota ei suoraan välitetä kohteeseen. Sovelluspalomuuri avaa uuden yhteyden itsensä ja kohteen välille päätelaitteelta saatujen tietojen perusteella. Tällöin avattuja yhteyksiä ja niiden sallimista voidaan analysoida aina sovellustasolla asti. (Shimonski ym. 2003, 57.)

Tarkempi liikenteen analysointi mahdollistaa laajemman tietoturvan tason kuin tilallinen tai tilaton palomuuri, mutta samalla pakettien syvempi tarkastelu vaatii enemmän resursseja ja vaikuttaa näin ollen myös hitaampaan suorituskykyyn. Sovellustason palomuurissa voi olla lisäksi ongelmana uusien tekniikoiden ja protokollien käyttöönotto. Jokaiselle protokollalle täytyy olla kehitettynä yhteensopiva välityspalvelin (proxy), joten uusien protokollien käyttämiseen saattaa joutua odottamaan palomuurin valmistajalta sopivaa päivitystä. (Shimonski ym. 2003, 57.)

2.5 Osoitteenmuunnos ja Port Forwarding

Osoitteenmuunnos eli NAT (Network Address Translation) määritellään RFC 1631 -standardissa. Palomuuri huolehtii yleensä lähiverkon osoitteiden muuntamisesta ulkoverkkoon soveltuvaksi IP-osoitteeksi. Osoittenmuunnosta käytetään tuomaan lähiverkon laitteille lisää tietoturvaa estämällä lähiverkon osoitteen näkyminen ulkoverkkoon. Tällä tavalla on pystytty myös vähentämään tarvetta julkisille IP-osoitteille tietoverkkojen kasvaessa maailmanlaajuisesti. Osoitteenmuunnoksessa palomuuri muokkaa paketin lähde- tai kohdeosoitteet IP-otsikossa, jolloin

liikenne näyttäisi lähteävän palomuurista sen omalla osoitteella. (Shimonski ym. 2003, 62.)

Vaihtoehtoina on tehdä osoitteenmuunnos staattisesti tai dynaamisesti. Staattisessa osoitteenmuunnoksessa yksi sisäverkon osoite vastaa yhtä ulkoverkon osoitetta. Näin ollen julkisia IP-osoitteita täytyy olla yhtä monta kuin sisäverkossa Internet-yhteyden tarvitsevia laitteita. Dynaaminen NAT eroaa staattisesta sillä, että siinä käytetään julkisten IP-osoitteiden ryhmää, josta otetaan osoitteita käyttöön sitä mukaan kun yhteyksiä avataan ulkoverkkoon. Myös tässä tapauksessa yksi sisäverkon osoite vastaa yhtä ulkoverkon osoitetta, mutta osoitteita ei ole sidottu toisiinsa kuin tilapäisesti. Näin jokainen sisäverkon laite voi muodostaa yhteyden ulkoverkkoon aina kun osoitteita on vapaana. (Shimonski ym. 2003, 63.)

Osoitteenmuunnos tehdään palomuurissa useimmiten käyttämällä *NAT overloadingia*, jossa yhdelle ulkoverkon osoitteelle voidaan osoittaa monia sisäverkosta tulevia yhteyksiä. Tästä osoitteenmuunnoksen muodosta käytetään nimitystä PAT (Port Address Translation). Palomuuri erottelee avoimet yhteydet käyttämällä eri TCP/UDP-lähdeportteja eri yhteyksille ja ylläpitämällä niistä listaa, jonka perusteella se pystyy ohjaamaan paluuliikenteen oikeille sisäverkoin laitteille. TCP/UDP-protokollia käytettäessä voi olla samanaikaisesti aktiivisena 65 536 porttia eli eri yhteyttä. (Shimonski ym. 2003, 64.)

Port Forwarding on osa NAT:a ja mahdollistaa ulkoverkosta pääsyn tietylle sisäverkon laitteelle, jolla ei ole itsessään julkista ulkoverkon IP-osoitetta. Palomuurin ulkoverkon IP-osoite sekä tietyn portin yhdistelmä asetetaan ohjaamaan tuleva liikenne määritellylle sisäverkon laitteelle, kuten palvelimelle.

2.6 Palomuuriklusteri

Vikasietoisuutta voidaan lisätä merkittävästi ottamalla käyttöön palomuuriklusteri, joka koostuu kahdesta tai useammasta palomuurilaitteesta. Tätä nimitetään myös High Availability- tai HA-

klusteriksi. Klusterien tarkoituksena on palomuuritoiminnan jatkuminen niin kauan kuin yksikin palomuureista on toiminnassa. Tämä tuo etuna myös helpomman hallinnan muun muassa päivityksien asennuksille, koska data jatkaa kulkemista yhden laitteen poissaolosta huolimatta. (Shimonski ym. 2003, 714.)

HA-klusterissa yksi jäsenistä on aktiivinen ja reitittää tietoliikennettä. Muut laitteista ovat varalla toissijaisina palomuureina niin kauan kuin ensisijainen laite asetetaan hallitusti pois käytöstä tai laite vikaantuu. On kuitenkin huomioitava, etteivät kaikki palomuurit tue HA-klustereita. (Shimonski ym. 2003, 715.)

2.7 Kuormantasaus ja liitäntöjen vikasietoisuus

Osa palomuureista mahdollistaa kuorman jakamisen (Load Sharing) klusterissa kahden tai useamman palomuurin välillä. Tämä mahdollistaa vikasietoisuuden lisäksi myös suuremman tiedonsiirtokapasiteetin. Kuorman jakaminen tasaisesti (Load Balancing) eri klusterin jäsenien kesken on joillakin laitteilla mahdollista. (Shimonski, Shinder, Shinder & Carasik-Henmi 2003, 715.)

Usea palomuuri tarjoaa mahdollisuuden kuormantasaamiseen laitteen omien liitäntöjen välillä. Oletuksena on useimmiten tasajako liitäntöjen välillä eli joka toinen yhteys ohjataan eri WAN-liitäntään. Monilla laitteilla voidaan säätää liitäntöjen käyttöastetta esimerkiksi yhteyksien nopeuksien suhteessa, jolloin on mahdollista asettaa liikenne käyttämään pääasiassa nopeampaa yhteyttä, mutta osa paketeista ohjataan hitaamman yhteyden kautta.

Kahden WAN-yhteyden ollessa käytettävissä voidaan toinen asettaa ensisijaiseksi yhteydeksi ja toinen varayhteydeksi. Ensisijaisen yhteyden vikaantuessa varayhteys otetaan käyttöön. Tätä voidaan käyttää esimerkiksi tilanteissa, joissa toinen yhteys on merkittävästi hitaampi tai varayhteyden kustannukset perustuvat siirretyn datan määrään.

3 LAN JA WAN

3.1 Lähiverkko

Lähiverkko eli LAN on tietoverkko, joka toimii rajatulla alueella ja jota hallinnoidaan paikallisesti. Yritysten ja kotitalouksien sisäverkot ovat esimerkkejä lähiverkoista. Lähiverkko muodostuu laitteista, jotka ovat yhteydessä toisiinsa Layer 2-tasolla. Yleensä laitteet kytketään samaan verkkoon Ethernet-kytkimillä. Lähiverkoista toisiin lähiverkkoihin paketit kulkevat reitittimien kautta Layer 3-tason IP-protokollaa käyttäen. (Burke 2015.)

RFC 1918 -standardissa määritellään IP-avaruudet, joita ei reititetä Internetissä vaan ne ovat tarkoitettuja yksityisiin sisäverkkoihin käytettäviksi. Nämä osoiteavaruudet eivät ole uniikkeja vaan niitä käytetään ympäri maailmaa yritysten ja kotitalouksien sisäverkoissa. Sisäverkkoihin varattuja osoitteita ovat seuraavat:

- 10.0.0.0 – 10.255.255.255 eli 10/8 merkintä
- 172.16.0.0 – 172.31.255.255 eli 172.16/12 merkintä
- 192.168.0.0 – 192.168.255.255 eli 192.168/16 merkintä.

(Shimonski ym. 2003, 62.)

3.2 DHCP ja DNS

Dynamic Host Configuration Protocol eli DHCP on protokolla, jonka avulla päätelaitteet saavat IP-osoitteen sekä muut tarvittavat verkon asetukset. Verkkoon liittyvä päätelaite lähettää UDP broadcast -kyselyn, jossa laite pyytää verkon asetuksia. Kun päätelaite saa paluuviestinä vastauksen DHCP-palvelimelta, laite konfiguroi asetuksensa saatujen tietojen mukaisesti. Yleensä palomuurit voivat toimia sekä DHCP-palvelimena että asiakaslaitteena. DHCP-palvelin jakaa konfiguraation mukaisten verkkojen IP-osoitteita ja pitää kirjaa lainatuista osoitteista sekä niitä käyttävistä

laitteista. Palvelimella voidaa valita mitkä liitännät jakavat DHCP-palvelimen osoitteita. (Shimonski ym. 2003, 341.)

Domain Name System eli DNS on protokolla, jota käytetään domain-nimien muuntamiseen IP-osoitteiksi ja päinvastoin. Tämä ominaisuus on erittäin tärkeä esimerkiksi www-sivujen käytössä sekä sähköpostin lähettämisen ja vastaanottamisen yhteydessä. (Shimonski ym. 2003, 663.)

3.3 VLAN

VLAN on lyhenne virtuaalisesta lähiverkosta (Virtual LAN) ja se määritellään IEEE 802.1Q-standardissa. Virtuaalisten LAN:ien avulla voidaan samassa kytkimessä ja liitännöissä siirtää dataa toisistaan erillisissä virtuaalisissa lähiverkoissa. Perusasetuksilla virtuaaliset lähiverkot eivät näe toistensa liikennettä tai tiedä toistensa olemassaolosta. (Burke 2015.)

Samaan kytkinporttiin voidaan konfiguroida yksi tai useampi VLAN. Tämä mahdollistaa verkon ylläpitäjälle eri tapoja toteuttaa verkon osioimista fyysisiin kytkentöihin koskematta. Virtuaalisten lähiverkkojen avulla on mahdollista yhdistää fyysisesti eri sijainneissa olevia lähiverkkoa samaksi loogiseksi lähiverkoksi. (Burke 2015.)

3.4 VPN

Virtuaalinen yksityinen verkko eli VPN (Virtual Private Network) on teknologia, jolla salataan liikenne tietoturvattomassa verkossa, kuten Internetissä. VPN on tietoturvallinen ratkaisu ympäristössä, jossa verkkoinfrastruktuuri on turvaton. Yleisimpiä tapoja toteuttaa VPN on remote-access VPN ja site-to-site VPN. (Burke 2016.)

Remote-access VPN on nimensä mukaisesti tietoturvallisen etäyhteyden muodostamisen tapa yrityksen sisäverkkoon julkisen verkon, kuten Internetin, ylitse. VPN asiakaslaite (client) yhdistää yrityksen VPN-reitittimeen ja reititin pyytää asiakaslaitetta autentikoitumaan. Kun laite on

tunnistettu ja VPN-tunneli luotu, voi asiakaslaite käyttää yrityksen sisäverkon resursseja samalla tavalla kuin ollessaan kytkettynä lähiverkkoon. Käytettävinä VPN-yhteyden salaustekniikoina ovat yleensä IPsec sekä SSL VPN. SSL VPN:ää käytetään tosin yleensä tietyn sovelluksen tai sovelluksien salattuun yhteyteen eikä niinkään koko verkkoliikenteen salaamiseen. (Burke 2016.)

Site-to-site VPN on tekniikka, jota käytetään kokonaisten verkkojen yhdistämiseen toisiinsa sijainnista riippumatta. Palomuuri avaa VPN yhteyden toiseen palomuuriin ja liikenne kulkee salattuna näiden välillä. Päätelaitteille tämä ei näy käytännössä, eikä niiden tarvitse yhdistää erikseen VPN-reitittimeen sillä palomuurit käsittelevät keskenään liikenteen salaamisen sekä VPN-yhteyden avaamisen ja ylläpidon. Tällä tavalla voidaan yhdistää esimerkiksi yrityksen pää- ja sivukonttorien tietoverkot turvallisesti toisiinsa. Internetin välityksellä tapahtuva site-to-site VPN käyttää yleensä IPsec-protokollaa yhteyden salaamiseen. Muita vaihtoehtoja ovat esimerkiksi palveluntarjoajan MPLS pilvessä käytettävä MPLS IP VPN. (Burke 2016.)

4 PALOMUURIEN VERTAILU

4.1 Vertailuun valitut palomuurit

Tässä opinnäytetyössä keskitytään vertailemaan kahta erityyppistä palomuuriratkaisua. Vertailussa käytetyt palomuurit ovat yhdysvaltalaisen verkkolaitevalmistaja Ciscon RV320 VPN -reititin (”Cisco”) sekä avoimen lähdekoodin ohjelmisto pfSense, joka voidaan asentaa lähes mille tahansa tämän päivän PC:lle sekä virtuaali- tai fyysiselle palvelimelle. Palomuurien vertailuun laitteet valitsi ja toimitti kisaorganisaatio (Cisco) sekä Lahden ammattikorkekoulu (pfSense). Cisco RV320:n ja pfSensen vertailussa keskitytään palomuurien tärkeimpiin osa-alueisiin, jotka vaikuttavat palomuurilaitteiden mahdolliseen käyttöönottoon hiihdon MM 2017 -kisojen mediakeskuksissa Lahdessa.

Cisco on vuodesta 1984 asti toiminut yhdysvaltalainen tietoliikenne- ja elektroniikkateollisuusyritys, joka suunnittelee, valmistaa ja markkinoi verkkolaitteita. Yritys on maailman suurin toimialallaan ja laajalti arvostettu. Verkkolaitteita, kuten kytkimiä ja reitittimiä, Ciscolla on tarjota aina kuluttajien ja PK-yritysten tarpeista tietoliikenneoperaattoreiden vaatimuksiin asti.

pfSense on avoimen lähdekoodin reititys- ja palomuuriohjelma, joka perustuu FreeBSD käyttöjärjestelmään. pfSensen kehitys aloitettiin vuonna 2004. Palomuuriohjelman perusasennus on laajennettavissa lukuisilla lisäominaisuuksilla erilaisten modulien avulla. pfSense on laajentanut viime vuosina toimintaansa myös verkkolaitteiden pariin ja pfSensen tarjontaan kuuluu nykyisin myös yrityskäyttöön tarkoitettuja palomuurireitittimiä, jotka toimivat pfSensen käyttöjärjestelmällä.

4.2 Palomuurin tyyppi

Cisco RV320 on tilallisen palomuuri. Web-käyttöliittymällä voidaan asettaa sääntöjä protokollien, porttien ja IP-osoitteiden perusteella. Palomuurilla

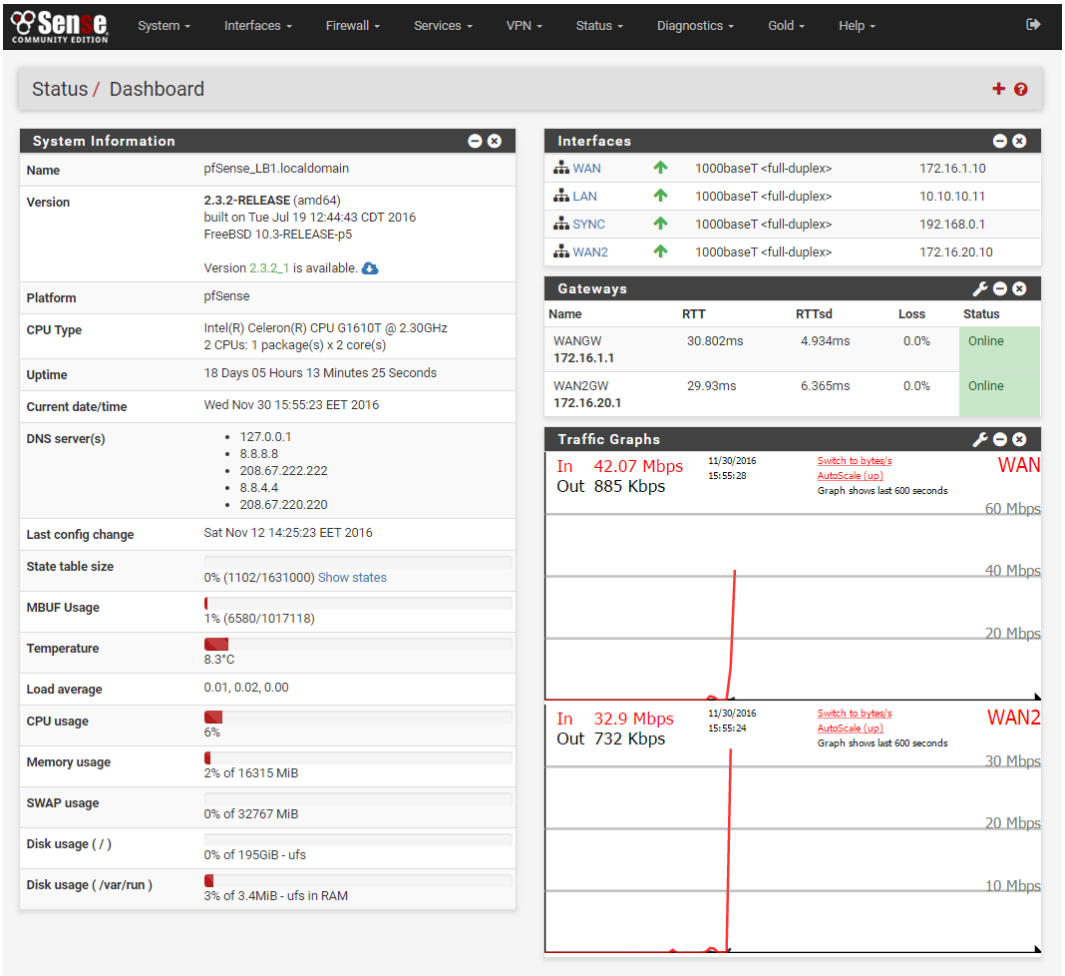
on myös mahdollista estää haluttuja verkko-osoitteita tai vaihtoehtoisesti estää oletuksena kaikki ja sallia vain nimetyt verkko-osoitteet. Osassa Cisco RV320 reitittimissä on ominaisuutena myös sisällön suodatus (Content Filter), mutta tässä opinnäytetyössä käytettävässä mallissa sitä ei ole. Suodatus onnistuu asettamalla valmiita suodatusparametrejä, joilla voidaan estää tietynlaisia www-sivujen sisältöjä. Pakettien sisällön suodatusta toteutetaan Ciscon ylläpitämien avainsanalistojen perusteella sekä asettamalla suoraan halutut verkko-osoitteet estettyjen tai hyväksyttyjen domainien listalle. (Cisco 2014.)

pfSense on tilallinen palomuuri, johon on saatavilla erikseen asennettavana lisämoduulina mahdollisuus pakettien suodatukseen. squidGuard-lisäosalla voidaan suodattaa web-liikennettä muun muassa sallimalla vain tietyt sivustot, käyttämällä avoimen lähteen mustia listoja sekä estämällä sivustoja domain-nimen tai avainsanojen perusteella. (pfSense 2015d.)

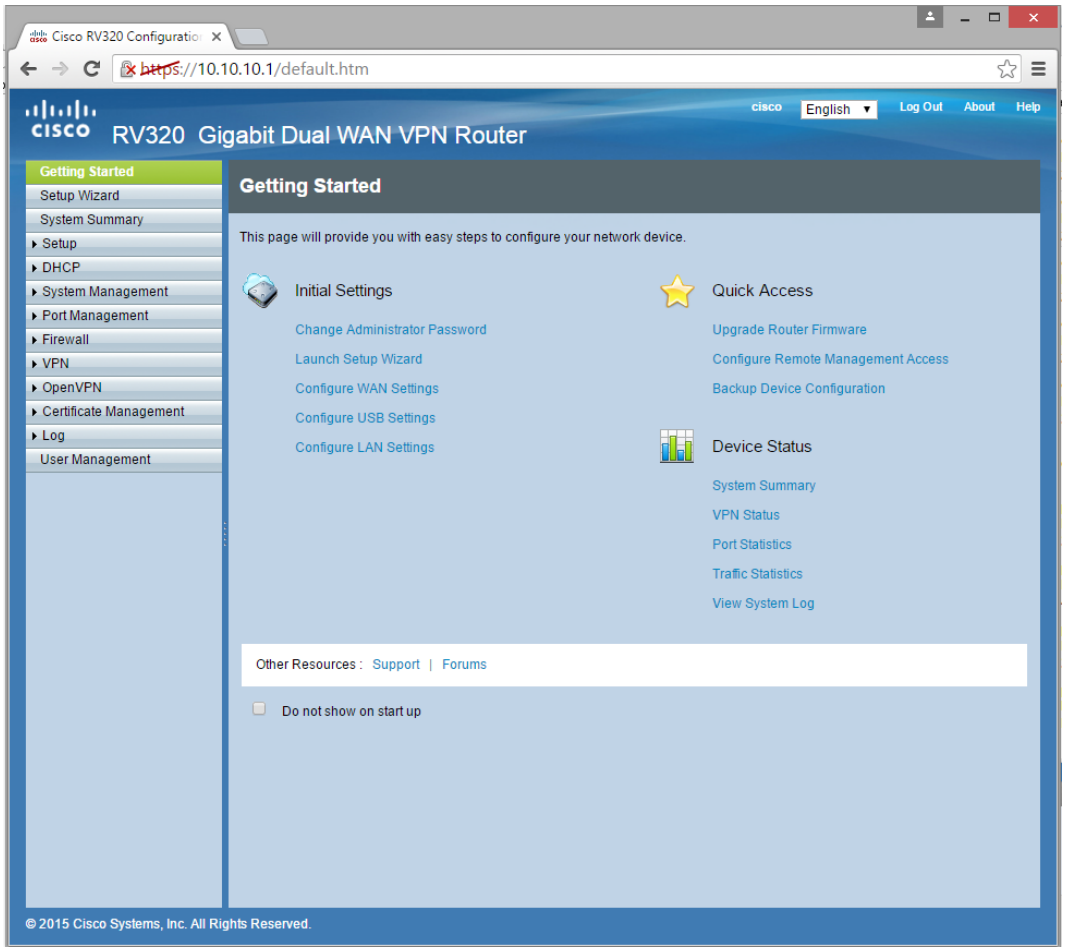
4.3 Käyttöliittymä

Molemmissa palomuureissa on graafinen web-käyttöliittymä, jonka avulla voi tehdä kaikki konfiguraatiot. Poikkeuksena tässä on pfSensen asennus, joka täytyy suorittaa konsolin kautta ennen palomuurin graafiseen käyttöliittymään kirjautumista. pfSensellä sekä Ciscolla voi valita käyttöliittymän protokollaksi http tai https.

Etähallinnan voi avata kummassakin palomuurissa WAN-liitynnälle, mutta se ei ole tietoturvasyistä suotavaa. Etähallinta suositellaan toteutettavan VPN:n avulla. pfSensen konsolinäkymään on mahdollista aktivoida SSH etäyhteyttä varten. Seuraavilla sivuilla olevissa kuvioissa on kuvakaappaukset molempien palomuurien aloitusnäkymistä (kuviot 1 ja 2).



KUVIO 1. pfSense aloitusnäkymä, johon on lisätty liikennegraafit ja yhdyskäytävien monitorointi



KUVIO 2. Cisco RV320 aloitusnäkymä

4.4 Liitännät ja läpäisynopeus

Cisco RV320-reitittimessä on neljä LAN-liitäntää, yksi WAN-liitäntä sekä yksi WAN/DMZ-liitäntä, jota voidaan käyttää toisena WAN-liitäntänä tai eteisverkkoliitäntänä. Kaikki liitännät ovat nopeudeltaan 1Gbps. Laitteessa on lisäksi kaksi USB 2.0-liitäntää, joihin voi liittää mobiililaajakaistasovittimen tai USB-massamuistin. (Cisco 2016.)

pfSensessä ei ole ohjelmiston puolelta rajoittavaa tekijää liitäntöjen määrälle. Fyysisten liitäntöjen määrän rajoittaa vain käytettävän laitteen verkkokorttien kapasiteetti. (pfSense 2015b.)

Tässä opinnäytetyössä käytetyissä HPE:n mikropalvelimissa oli kaksi RJ-45 liitäntää vakiona sekä sen lisäksi yksi neliporttinen Intelin verkkokortti. Palvelimessa on lisäksi kaksi USB 3.0 ja neljä USB 2.0 -porttia sekä VGA-liitäntä.

Cisco (2016) lupaa IPSecillä nopeudeksi 100 Mbps ja SSL VPN:llä 20 Mbps sekä yhteensä 20 000 samanaikaista yhteyttä. Reid (2014) mainitsee Ciscon luvanneen NATin kautta kulkevalle liikenteelle 900 Mbps nopeuden. pfSense ei lupaa palomuurilleen mitään nopeuksia, koska toteutuva nopeus riippuu merkittävästi käytetyistä laitteista ja komponenteista.

4.5 VPN

Cisco RV320:llä on mahdollista olla 100 VPN-tunnelia. Reititin tukee PPTP-, IPsec- ja SSL VPN-protokollia. VPN tekniikoista Ciscolla on mahdollista käyttää sekä Remote Access VPN että Site-To-Site VPN tekniikkaa. (Cisco 2016.)

pfSense tukee IPsec-, OpenVPN- ja PPTP-protokollia. Myös pfSensen palomuuriohjelma mahdollista sekä Site-To-Site VPN- että Remote Access VPN-tekniikoita. (pfSense 2016c.)

4.6 VLAN, IPv4 ja IPv6

Molemmat palomuurit tukevat sekä IPv4- että IPv6-protokollia. IPv4-protokolla on ainoastaan käytössä kummankin laitteen perusasetuksilla. (Cisco 2016; pfSense 2016a.)

Cisco (2016) ilmoittaa RV320:n tukevan maksimissaan seitsemää virtuaalista LAN-liitäntää. pfSensellä ei ole määriteltyä maksimimäärää VLAN-liitännöille. Laitteiston suorityskyky voi olla rajoittavana tekijänä erittäin suurilla VLANien määrillä. pfSensen palomuureja on käytössä tunnetusti yli 50 VLANin toimintaympäristöissä. (pfSense 2015b.)

4.7 Kuormantasaus (Load balancing)

Cisco RV320 mahdollistaa kahden WAN-liitännän samanaikaisen käytön ja liikenteen kuormantasauksen. LAN-verkosta tuleva liikenne ohjataan vuorotellen molempiin WAN-liitäntöihin. Reitittimen voi myös konfiguroida käyttämään vain toista WAN-liitäntää tietyn protokollan, lähde- tai kohdeosoitteen perusteella. (Cisco 2016.)

pfSensen palomuurilla voidaan asettaa kaksi tai useampi WAN-liitäntää samanarvoisiksi, jolloin LAN-verkon liikenne ohjataan vuorotellen näihin liitäntöihin. WAN-liitännät toimivat tällöin samalla vikasietoisesti keskenään toisen vikaantuessa. (pfSense 2016b.)

4.8 Vikasietoisuus (Failover)

Ciscon reitittimessä on kaksi vaihtoehtoa vikasietoisuuden toteuttamiseen. Toinen on kahden WAN-liitännän asettaminen Smart Link Backup -tilaan. Tällöin ensisijaiseksi asetetun WAN:n vikaantuessa reititin siirtyy käyttämään varaliitännäksi asetettua WAN:ia. Ethernet WAN-liitäntöjen vikaantuessa liikenne voidaan siirtää käyttämään USB-porttiin liitettyä 3G/4G-mobiiliyhteyttä. USB Failover asetuksista voidaan asettaa reititin toimimaan myös pelkästään mobiiliyhteyden kautta. Kahden kuormaa tasaavan WAN-liitännän vikasietoisuus toimii automaattisesti ja toisen linkin vikaantuessa palomuuri käyttää vain toimivaa linkkiä. (Cisco 2016.)

pfSensellä vikasietoisuutta voidaan toteuttaa eri menetelmillä, kuten kahdentamalla palomuuri (High Availability), kahdentamalla laitteen kiintolevy (RAID 1) sekä käyttämällä kahta tai useampaa WAN-liitäntää (Multi-WAN). CARP-menetelmästä kerrotaan tarkemmin seuraavassa alaluvussa 4.9. Näiden lisäksi pfSensellä on mahdollista lisätä vikasietoisuutta käyttämällä LAGG:ia yhdistämään kaksi tai useampi liitäntä yhdeksi loogiseksi linkiksi toiselle aktiivilaitteelle. LAGG:stä lisää alaluvussa 4.11.

Kiintolevyn kahdennusta pfSense tukee ohjelma-RAID 1:nä (GEOM Mirror) asennusvaiheessa, mikäli asennusohjelma tunnistaa useamman kiintolevyn. Suoraan BIOS:in kautta tehtyä kiintolevyn kahdennusta pfSense ei tue. Asennusvaiheessa valitaan mitä levyä käytetään ensisijaisena levynä sekä mitä levyä toissijaisena peilauskopiona. Asennuksen jälkeen Web-käyttöliittymästä on mahdollista tarkkailla peilauksen tilaa. Kumman tahansa levyistä voi ottaa pois tai vaihtaa milloin tahansa ja palomuuri säilyy toiminnassa. Tilalle voi vaihtaa uuden levyn ja määrittää pfSensen käyttämään sitä nykyisessä kahdennuksessa. (pfSense 2014a.)

Useamman WAN-liitännällä vikasietoisuus voidaan toteuttaa pfSensen palomuuriohjelmalla kahdella tavalla. Toinen näistä on käyttää edellisessä alaluvussa esiteltyä Load balancing -ominaisuutta, jolloin käytetään molempia yhteyksiä samanaikaisesti ja toisen vikaantuessa siirrytään käyttämään ainoaa toimivaa yhteyttä. Toinen vaihtoehto on merkitä esimerkiksi kahden WAN-liitännän tapauksessa toinen liitännöistä ensisijaiseksi yhteydeksi ja toinen sen varayhteydeksi. Käytettävien liitäntöjen järjestys määritetään asettamalle ne halutun tasoisiksi (tier). pfSense tukee myös näiden ominaisuuksien yhdistämistä esimerkiksi tapauksessa, jossa käytössä on yksi nopea WAN-yhteys ja kaksi hitaampaa. Tällöin voidaan asettaa nopea yhteys ensisijaiseksi yhteydeksi ja ensisijaisen yhteyden vikaantuessa siirrytään käyttämään kahden hitaamman yhteyden samanaikaista kuormantasausta. (pfSense 2016b.)

4.9 Palomuurilaitteiston kahdennus (High Availability)

Cisco ei tue palomuurin kahdennusominaisuutta RV320-palomuurissaan. pfSense (2015) mahdollistaa usean palomuurilaitteen käytön korkean saatavuuden (High Availability) klusterissa. Tällöin palomuurit asetetaan vikasietoiseen klusteriin, jossa yksi laitteista toimii ensisijaisesti käytettynä palomuurina (Master) ja loput toissijaisina (Backup). Tässä opinnäytetyössä toteutettiin HA-klusteri kahdella pfSense-palomuurilla.

HA-klusterin osa-alueet ovat pfSensellä CARP (Common Address Redundancy Protocol), tilasynkronointi sekä konfiguroinnin synkronointi. CARP:ia käytetään virtuaalisten IP-osoitteiden (VIP) luomiseen ja hyödyntämiseen palomuurilaitteiden välillä. Virtuaalista IP-osoitetta varten tarvitaan kolme staattista IP-osoitetta samasta aliverkosta. Näistä osoitteista yksi on VIP:lle, toinen Masterille ja kolmas Backupille. Tämä sama vaatimus on sekä WAN, että LAN puolelle. Virtuaalisen IP-osoitteen avulla kaikki pfSenseille tuleva liikenne kohdistuu VIP-osoitteeseen, joten toisen palomuurin vikaantuessa liikenne siirtyy katkoitta uudelle Masterille. Tilasynkronointia ylläpitää pfsync-protokolla, joka lähettää ensisijaisen palomuurin päivitettyjä tilatietoja toissijaisille palomuureille. Näin avatut yhteydet eivät katkea vaikka liikenne siirtyisi kulkemaan varalla olleen palomuurin kautta. Konfiguroinnin synkronointi tapahtuu XMLRPC-protokollan kautta. Tämä toimii samalla periaatteella kuin pfsync eli XMLRPC ylläpitää ja tiedottaa ajankohtaiset muutokset konfiguraatioon toissijaisille pfSense-palomuureille. pfSense suosittelee HA-klusterin synkroinointiliikenteelle omaa aliverkkoa sekä verkkoliitäntää, jottei siirrettävä data turhaan häiritse tuotantoverkon liikennettä. (pfSense 2015a.)

4.10 SNMP

RV320 reitittimessä on tuki SNMP:lle. Palomuuri tukee SNMP v1/v2c sekä v3 versioita ja laite toimiii SNMP agenttina, joka vastaa SNMP-kyselyihin. Reititin voidaan myös asettaa lähettämään trap-ilmoituksia. (Cisco 2016.)

pfSense tukee SNMP-kyselyitä sekä SNMP trap-ilmoituksia. Palomuurille on saatavilla lisämoduleita erilaisia SNMP-informaatioita varten. (pfSense 2014b). pfSense ei tue SNMP v3 versiota.

4.11 Tietoliikenneprotokollat

Cisco (2016) tukee IPv4 RIP v1 ja v2 -reititysprotokollia sekä IPv6 RIPng-reititiysprotokollaa. Reititysprotokollia pfSense ei tue suoraan

perusversiossa. Erikseen asennettavilla lisämoduleilla voidaan kuitenkin reititysprotokollia ottaa käyttöön. Näiden moduleiden avulla palomuuri tukee OSPF, RIP v1 ja v2, OLSR sekä BGP reititysprotokollia. (pfSense 2016a.)

pfSensellä on mahdollista yhdistää liitäntöjä luomalla virtuaalinen LAGG-liitäntä. LAGG-liitäntä luodaan valitsemalla isäntäliitännät sekä protokolla, jota yhdistelmäliitäntä käyttää. Käytettäviä protokollia ovat esimerkiksi kansainvälisen IEEE 802.3ad -standardin LACP sekä Ciscon FEC. LAGG-linkki pysyy ylhäällä niin pitkään kuin vähintään yksi fyysinen linkki säilyy toimivana kokoonpanossa. LAGG mahdollistaa vikasietoisuuden lisäksi kaistannopeuden kasvattamisen käytettyjen liitäntöjen määrän mukaisesti. (pfSense 2015c). Esimerkiksi LACP-protokollalla maksimimäärä käytettyjä liitäntöjä on kahdeksan. (Wikipedia 2016.)

4.12 Palomuurien vertailutaulukko

Cisco RV320 ja pfSense palomuurien ominaisuuksista tehdyn vertailun havainnolistamiseksi luotiin yhteenvetotaulukko. Taulukosta voidaan helposti tarkastella laitteiden ominaisuuksien eroavaisuuksia eri osa-alueilla.

Alla olevassa taulukossa 1 esitetään taulukkomuodossa Cisoc RV320 ja pfSense palomuurien vertailu. Taulukossa on esitetty tiivistettynä laitteiden tekniset tiedot ja ominaisuudet, joita on vertailtu tarkemmin aiemmin tässä luvussa.

TAULUKKO 1. Palomuurivertailun yhteenvetotaulukko

Ominaisuudet	**Cisco RV320**	**pfSense**
Palomuurityyppi	Tilallinen palomuuri	Tilallinen palomuuri

(jatkuu)

TAULUKKO 1. (jatkuu)

Käyttöliittymä	Web GUI	Web GUI, shell
Liitännät (Verkkoliitännät ovat 1 Gpbs, jos ei muuta mainittu)	1 WAN, 1 DMZ/WAN, 4 LAN ja 2 USB 2.0	Laitteistokohtainen. Tässä toteutuksessa: 6 Ethernet, 2 USB 3.0, 4 USB 2.0 ja VGA.
Läpäisynopeus	900 Mbps	Laitteistokohtainen
VPN	Site-to-site VPN ja Remote Access VPN. IPsec, SSL VPN ja PPTP.	Site-to-site VPN ja Remote Access VPN. IPsec, OpenVPN ja PPTP.
IPv4/IPv6	Molemmat	Molemmat
VLAN	Kyllä, maksimimäärä on 7.	Kyllä, ei ole maksimimäärää.
Kuormantasaus (Load Balancing)	Kyllä. Yhteys käyttää vain yhtä liitäntää kerralla. Kuormantasausta voidaan totetuttaa painotetusti.	Kyllä. Yhteys käyttää kaikkia WAN-liitäntöjä kerralla. Kuormantasausta voidaan totetuttaa painotetusti.
Vikasietoisuus	Load Balancing tai Smart Link Backup WAN-liitännöissä.	Load Balancing tai haluttu järjestys WAN-liitännöissä, RAID 1, HA-klusteri ja LAGG.
Palomuurilaitteiston kahdennus (HA-klusteri)	Ei	Kyllä
SNMP	v1, v2c ja v3	v1 ja v2c

(jatkuu)

TAULUKKO 1. (jatkuu)

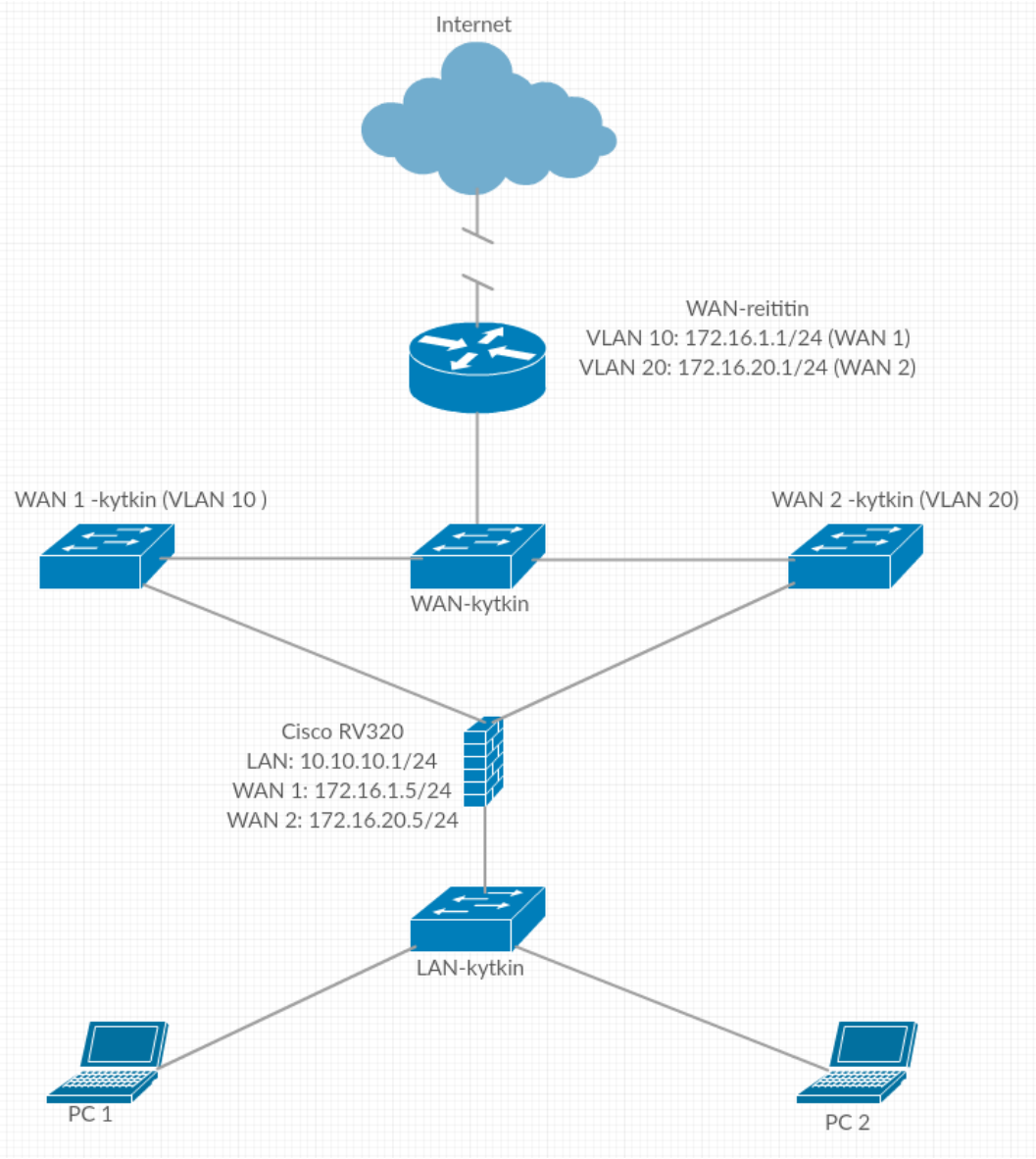
Tietoliikenneprotokollat	IPv4 RIP v1 ja v2 sekä IPv6 RIPng	LAGG (LACP ja FEC). OSPF, RIP v1 ja v2, OLSR sekä BGP saatavissa lisämoduleilla.

5 PALOMUURIEN TESTAUS

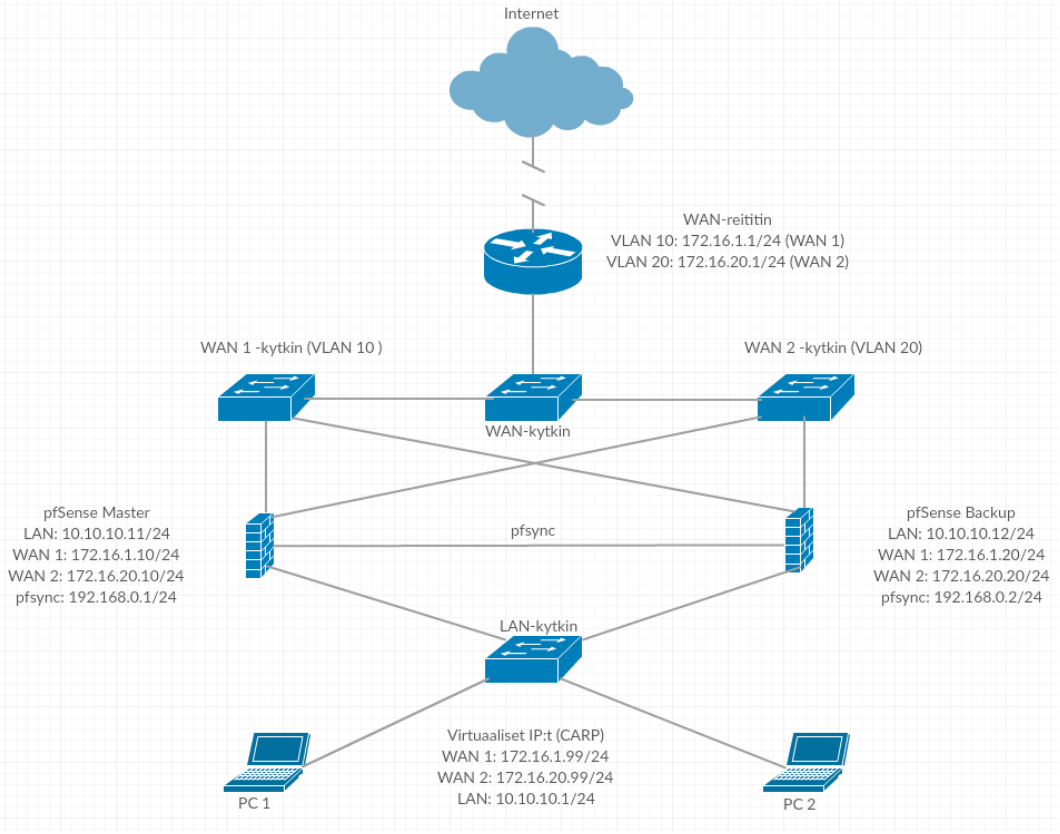
5.1 Testiverkon topologia

Palomuurien testiympäristönä toimi Lahden ammattikorkeakoulun tietoverkkolaboratorio. Testausta varten käytössäni oli yksi kappale Cisco RV320 -reititintä (”Cisco”) sekä kaksi kappaletta HPE ProLiant MicroServer Gen8 -palvelimia (”HP” tai ”pfSense”), joihin pfSense asennettiin. HP:n palvelimissa oli lisätty 8GB muistia (yhteensä 12GB) sekä asennettu 4-porttinen Intelin 1Gbps verkkokortti, mutta muuten ne olivat vakiomallisia.

Testiverkon topologia oli samankaltainen molemmilla palomuureilla. Kummassakin testiverkossa tietoverkkolaboratoriosta tuotiin Internet-yhteys Ciscon 2800-sarjan reitittimelle, jotta pystyttiin käyttämään staattisia IP-osoitteita kahdesta eri verkosta. Kahta WAN-yhteyttä simuloitiin tässä opinnäytetyössä kahdella VLAN-verkolla. WAN-reitittimen ja -kytkimen välille konfiguroitiin trunk-linkki siirtämään molempien VLAN-tagien paketteja. WAN-kytkimeen, joka oli Cisco 2960-sarjaa, asetettiin lisäksi access-portit molempia VLAN:eja varten. Näihin access-portteihin kytkettiin WAN 1- ja WAN 2 -kytkimet, jotka molemmat olivat HP Procurve 1400-sarjaa. Näistä kytkimistä oli linkit jokaiselle palomuurille. Käytettyjen topologioiden havaitsemisen helpoittamiseksi on seuraavilla sivuilla kuviot (3 ja 4) molemmista testiverkoista.



KUVIO 3. Cisco RV320 -testiverkon topologia



KUVIO 4. pfSense-testiverkon topologia

5.2 Asennus

5.2.1 Cisco RV320

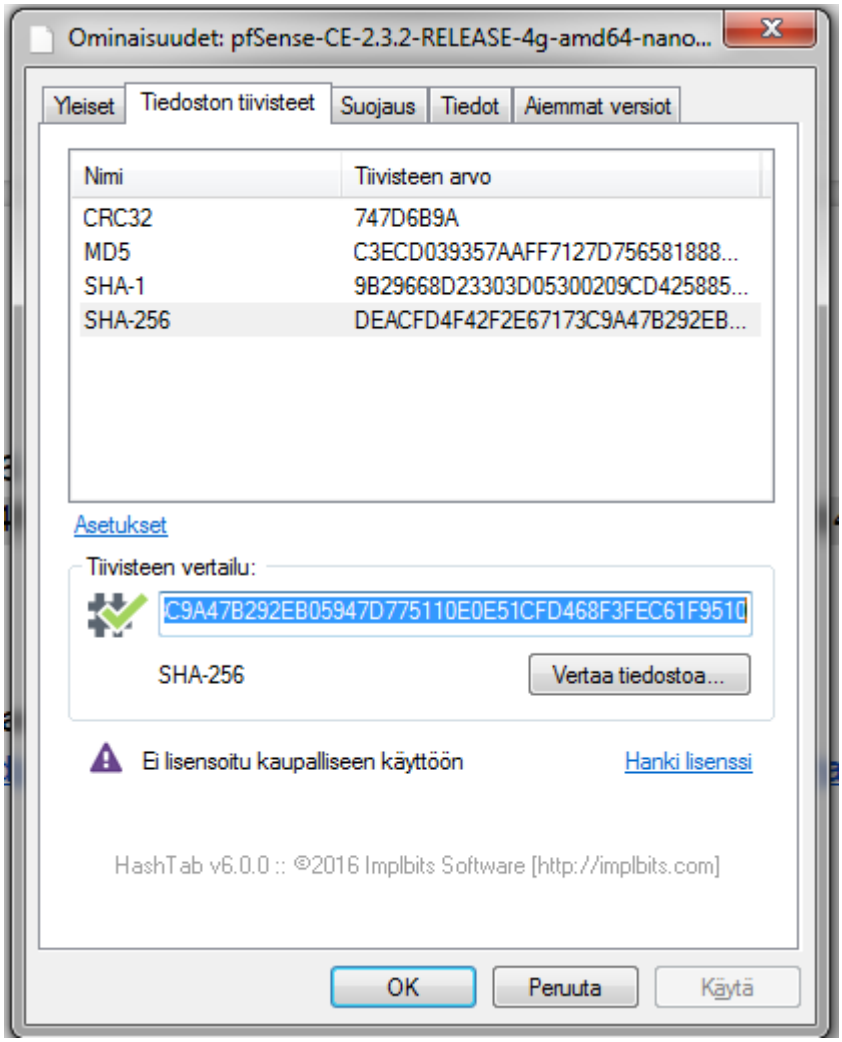
Ciscon reititin ei vaadi erillistä asennusta vaan laitteen voi ottaa heti käyttöön ja alkaa valitsemaan haluttuja asetuksia. Käytössäni olleessa reitittimessä oli kuitenkin jo aiempi konfiguraatio sisässä, joten se täytyi nollata. Tämä onnistuu helposti painamalla reset-nappia pohjassa 30 sekuntia virran ollessa päällä ja sen jälkeen sammuttamalla laite muutamaksi sekunniksi. Tämän jälkeen reitittimeen voi kytkeä virran ja laitteen käynnistyttyä voidaan kirjautua web-käyttöliittymään osoitteessa 192.168.1.1 käyttäjätunnuksella cisco ja salasanalla cisco. Ensikirjautumisen yhteydessä laite pakottaa vaihtamaan salasanan. Web-käyttöliittymässä voi suorittaa ohjatun asetusvelhon, jossa on mahdollista valita laitteen perusasetuksia. Vaihtoehtoisesti konfiguraatiot voi tehdä

käyttöliittymän sivuvalikoiden kautta. Tässä opinnäytetyössä konfiguroinnit tehtiin sivupalkin yksityiskohtaisten valikoiden kautta.

Ciscossa oli perusasetuksena molemmat WAN-portit ylhäällä ja käyttövalmiina. IP-osoitteen liitynnät hakevat DHCP-palvelimelta. LAN-portit ovat myös ylhäällä ja käyttövalmiita. Kaikkien liitäntöjen IP-asetukset löytyvät valikosta Setup->Network. Ciscolla oli tehdasasetuksissa valmiina VLAN-verkot 1, 25 ja 100. Reititin toimii DHCP-palvelimena LAN-verkon laitteille. DHCP-palvelimen asetuksissa valikossa DHCP->DHCP Setup voidaan määrittää VLAN:eille IP-aliverkot. Aliverkon peitteeksi voidaan asettaa valikon esiasetuksista /24 tai sitä kapeammat peitteet. Näin ollen esimerkiksi /23 tai laajempia aliverkkoja ei ole mahdollista käyttää ja tämä voi olla joissain toteutuksissa hyvinkin merkittävä asia. On kuitenkin muistettava, että laite on suunnattu PK-yrityksille ja ongelmaa voidaan kiertää tiettyyn pisteeseen asti VLAN-verkkojen avulla.

5.2.2 pfSense HPE-mikropalvelimella

pfSensen asennuksen voi tehdä CD-levyllä tai USB-muistitikulla. Palomuuriohjelma ladataan pfsense.org -sivustolta. pfSensen verkkosivuilla on valittavissa versiot eri alustoille sekä asennustavoille. Verkkosivut tarjoavat myös SHA256-tarkistussumman, jolla ladattu tiedosto voidaan varmistaa oikeaksi. Tiedoston oikeellisuus tarkistettiin pfSensen asennusohjeessa suositellulla HashTab-sovelluksella, josta on seuraavalla sivulla kuvakaappaus (kuvio 5). USB-asennustikun luomiseen käytin Rufus nimistä sovellusta, koska pelkkä levykuvan siirtäminen ei riitä asennuksessa.



KUVIO 5. SHA256 tarkistussumman vertaaminen HashTab-sovelluksella

pfSensen asennuksessa asetettiin ensin GEOM Mirrorin ensi- ja toissijaiset kiintolevyt ja sen jälkeen valittiin Quick/Easy Install, jossa palomuurin asennus tapahtuu lähes automaattisesti. Käyttäjän oli vain hyväksyttävä levyjen alustus sekä valita haluaako käyttää VGA-konsolia. Tämän jälkeen asennusvelho pyytää käynnistämään laitteen uudelleen ja laitteen käynnistyttyä on web-käyttöliittymä käytettävissä LAN-liitännässä osoitteessa 192.168.1.1. Liitäntöjen järjestyksen ja käyttötarkoituksen voi vaihtaa sekä konsolin että web-käyttöliittymän kautta.

pfSensestä on myös saatavilla NanoBSD-versio, joka toimii suoraan USB-muistitikulta tai muilta sulautetuilta järjestelmiltä, kuten SD-muistikorteilta.

Tällöin käytössä on samat toiminnot, mutta Flash-muistin käyttöä minimoidaan esimerkiksi vähentämällä tallennusten määrää. pfSenseä testattiin ensin NanoBSD-versiolla, mutta kyseisellä versiolla kohdattiin selittämättömiä bugeja, joita ei enää myöhemmin HDD:lle asennetulla versiolla esiintynyt. Edellä mainituin perustein voidaan suositella suhtautumaan NanoBSD-versioon varauksella sekä käyttämään täysasennusta laitteiden sen salliessa.

5.3 Kuormantasaus

Ciscossa on tehdasasetuksena kuormantasaus päällä. Valikon kohdasta System Management -> Dual Wan voidaan asetuksia muuttaa. Kuormantasauksen toimivuuden eli verkkoliikenteen vuorottelun WAN-liitäntöjen välillä testattiin ensin pingaamalla Googlen palvelinta komennolla *ping –f –l 1024 8.8.8.8 –t* ja seuraamalla web-käyttöliittymän Traffic Statistics taulukkoa. Edellä mainitulla komennolla saadaan pingattua 1024 tavun kokoisilla paketeilla, joten liikenne on helpompi havaita statistiikasta. Taulukko näyttää WAN-liitäntäkohtaisen liikenteen lähetettyjen (Tx = Transmit) ja vastaanotettujen (Rx = Receive) tavujen mukaan. LAN-verkon kytkimessä oli kaksi PC:tä, joista pingattiin yksitellen sekä samanaikaisesti 8.8.8.8 IP-osoitetta. Taulukosta oli selvästi havaittavissa, kumpaa WAN-liitännöistä ping-paketit käyttivät. Molempien laitteiden pingatessa samanaikaisesti, oli taulukosta nähtävissä kummankin WAN-liitännän olevan käytössä. Lopuksi testattiin vielä kuormantasausta Internetin speedtest.net -palvelulla ja sama tulos oli havaittavissa Traffic Statistics -taulukkoa seuraamalla.

pfSense vaati Ciscoon verrattuna enemmän konfigurointia kuormantasaamista varten. WAN-liitännöistä täytyy ensiksi luoda yhdyskäytäväryhmä (gateway group) valikosta System -> Routing. Groups-välilehdellä käytetyistä WAN-liitynnöistä luodaan ryhmä halutuilla arvoilla. Arvoja muuttamalla voidaan tehdä kuormaa tasaava tai vikasietoinen ryhmä. Samalle tasolle (tier) asetetut yhdyskäytävät toimivat kuormaa tasaavasti kun taas eri tasoille asetetut yhdyskäytävät

vikaisietoisina vaihtoehtoina. pfSensellä on mahdollista myös asettaa yhdyskäytävän tilaa tarkkailevia arvoja. Esimerkiksi monitorointi IP-osoite ja aikaraja, joidenka perusteella liitäntä voidaan todeta olevan pois käytöstä, mikäli yhteyttä IP-osoitteeseen ei saada aikarajan sisässä.

Etuna pfSensellä on kuitenkin molempien WAN-liitäntöjen samanaikainen käyttö, mikäli avattu yhteys mahdollistaa suuremman nopeuden kuin yksittäisellä WAN-liitynnällä on käytettävissä. Tämä ominaisuus varmistettiin kytkemällä WAN-liitynnät kahteen eri tietoverkkolaboratorion kytkimeen, joista on eri yhteydet ulkoverkkoon, ja testaamalla nopeutta speedtest.net -palvelulla. pfSensen Traffic Grapheja tarkkailemalla oli nähtävissä yhteyden käyttävän molempia liitäntöjä samanaikaisesti. Myös nopeustestin tulos oli parempi kuin yksittäistä WAN-liitäntää käyttäen. pfSense ohjaa yhteydet, kuten Ciscokin, käyttämään vuorotellen eri WAN-liitäntöjä primäreinä liikenteelle.

5.4 Vikasietoisuus

Kummallakaan laitteella yhden WAN-liitynnän vikaantuminen ei haittaa LAN-verkon Internet-yhteyttä merkittävästi. Molemmissa palomuureissa oli havaittavissa hetkellinen Internet-yhteyden katkeaminen, joka näkyi esimerkiksi pingin tai verkkosivun latauksen pysähdyksenä. Laitteet kyllä siirtyvät käyttämään toimivaa WAN-liitäntäänsä, mutta avoinna olleet yhteydet täytyy avata uudelleen, koska ne eivät automaattisesti siirry WAN-liitynnältä toiselle. Käytännössä tämä tarkoittaa esimerkiksi pingin lopettamista ja uudelleenaloittamista tai verkkosivun uudelleenlataamista. Poikkeuksena edelliseen on tapaus, jossa Ciscolla data kulkee käytössä pysyvän WAN-liitynnän kautta. Tällöin toisen WAN-yhteyden vikaantuminen ei haittaa kyseistä liikennettä. WAN-liitännän vikaantumista testattiin myös Youtube-videostreamilla, koska videon lataus tapahtuu puskuroimalla dataa purskeisesti tietyin aikavälein. Tämän tyyppisessä yhteydessä ei ole havaittavissa minkäänlaista katkosta vaan uusi purske ohjautuu suoraan käytössä olevaan WAN-liitäntään. Opinnäytetyössä

käytettiin WAN-yhteyden vikaantumisen simulointina verkkokaapelin irroittamista kytkimestä.

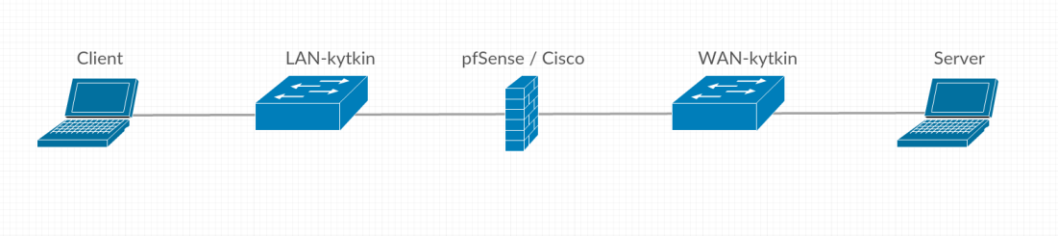
pfSensellä on WAN-liitäntöjen vikasietoisuuden lisäksi merkittävänä etuna mahdollisuus kahdentaa koko palomuurilaite asetuksineen. Laitteiden välille on vain konfiguroitava High Availability -klusteri. Tällöin Internet-yhteys säilyy käytössä jos esimerkiksi palomuurilaite vikaantuu, tarvitsee päivityksen tai jonkin muun syyn vuoksi joudutaan käynnistämään uudelleen. Aktiivisen pfSensen vaihto Masterilta Backupille tapahtuu erittäin sujuvasti ja yhteys siirtyy heti. Tämä ominaisuus testattiin pingaamalla jatkuvasti lähiverkon PC:llä komentokehoitteen komennolla *ping 8.8.8.8 -t* Googlen palvelinta. Pingin jatkuessa katkaistiin Masterina toimivan pfSensen yhteys lähiverkkoon ottamalla verkkokaapeli irti. Pingissä ei tullut katkosta ja yhteys oli siirynyt Backup palomuurille, jonka liikenteen graafeissa näkyi kulkevan dataa. pfSense siirtää palomuurivastuun Backupille vain kun Masteriin ei saada yhteyttä lähiverkosta. Esimerkiksi vain Masterin WAN-liitännän vikaantuminen ei siirrä vastuuta Backupille.

Tietoverkkolaboratoriossa testattiin myös pfSensen kiintolevyn kahdennusta eli GEOM Mirroria. HPE:n mikropalvelimessa oli kaksi 250GB kiintolevyä, joille pfSense oli asennettu käyttämällä RAID 1:tä. Toiminnassa olevasta laitteesta otettiin ensisijaiseksi valittu kiintolevy irti ja palomuuri jatkoi toimintaansa ilman ongelmia tai katkosta. Kun levy asennettiin takaisin paikalleen, pfSense alkoi synkronoimaan takaisin asetettua kiintolevyä nykyisen mukaiseksi.

5.5 Läpäisykyky

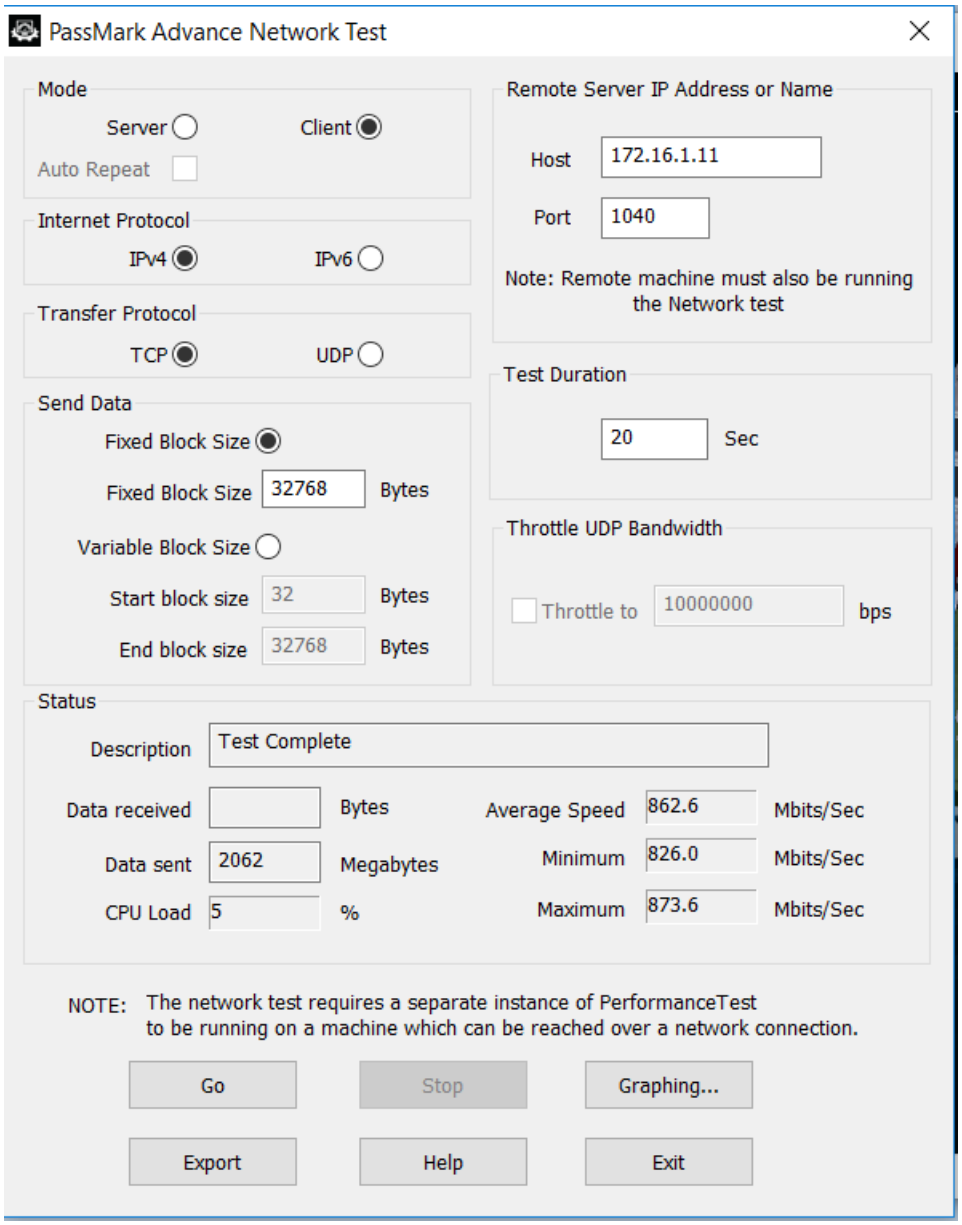
Palomuurien dataliikenteen läpäisykyvyn mittaamiseen käytin PassMark PerformanceTest -ohjelman Advance Network Test ominaisuutta. Ohjelmaa ei tarvitse asentaa päätelaitteelle eikä se tallenna testauksessa mitään kiintolevylle, joten ohjelmalla saa tarkan mittauksen juuri verkkokortin liikenteestä. Jotta testi voidaan suorittaa, ohjelma täytyy olla

käytössä kahdella eri PC:llä, joista toinen toimii testin palvelimena ja toinen asiakkaana. Palvelin-PC:lle annettiin kiinteä IP-osoite 172.16.1.11/24 ja palvelin yhdistettiin palomuurin ensimmäiseen WAN-liitäntään. Asiakaskone oli LAN-verkossa normaalisti. HP:n 1Gbps-nopeuden kytkimet olivat palomuurin ja PC:eiden välissä. Palomuurin WAN-liitynnälle annettiin IP-osoitteeksi 172.16.1.1/24. Molemmilla palomuureilla oli käytössä sama verkon topologia, josta on alla havainnekuvio (kuvio 6).



KUVIO 6. Verkon nopeuden testauksessa käytetty topologia

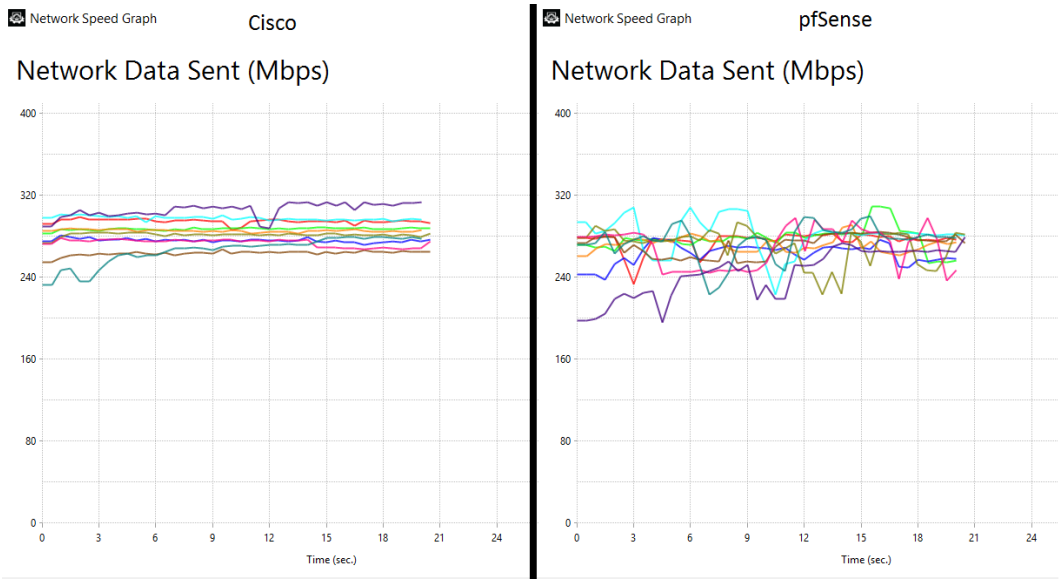
Testi suoritettiin kolmella eri tavalla: minimikokoisilla (32 tavua), vaihtelevan kokoisilla (32–32768 tavua) sekä maksimikokoisilla TCP-paketeilla (32768 tavua). Mittauksen näytteitä oli kymmenen kullakin pakettikoolla molemmilla palomuurilaitteilla. Testit suoritettiin kahtena eri päivänä ja näytteet mitattiin peräjälkeen ilman erityisiä taukoja. Mittauksissa käytettiin 20 sekunnin pituista jaksoa. Pienestä näytekoosta ja olosuhteiden vähäisestä muutoksesta johtuen nämä tulokset ovat käsiteltävä suuntaa antavasti. Molemmat laitteet toimivat todella samanlaisella tavalla, eikä suuria eroja syntynyt. Seuraavalla sivulla on kuvakaappaus mittauksissa käytetystä PassMark Advance Network Testistä (kuvio 7).



KUVIO 7. PassMark Advance Network Testin näkymä asiakaslaitteella

32 tavun kokoisilla paketeilla molempien laitteiden verkkoliitäntöjen nopeudet jäivät vaatimattoman pieniksi verrattuna verkon nimellisnopeuteen. Ciscolla vaihteluväli oli noin 235–315 Mbps kun taas pfSensellä väli oli hieman suurempi vaihdellen noin 200 Mbps ja 315 Mbps välillä. pfSensellä verkon nopeus saattoi vaihdella yhdenkin mittauksen aikana lähes koko vaihteluvälillä, mutta Ciscolla nopeus pysyi tasaisempana yksittäisten mittausten aikana. Seuraavalla sivulla olevassa

kuviossa 8 on esitetty lähetetyn datan määrän perusteella laskettu verkon nopeus 32 tavun kokoisilla paketeilla. Kuvaajat on otettu kuvakaappauksina PassMarkin sovelluksesta. Yksi kuvaaja esittää yhtä testitapausta. Pystyakselilla on verkon nopeus megabitteinä sekunnissa ja vaaka-akselilla on aika sekunneissa.

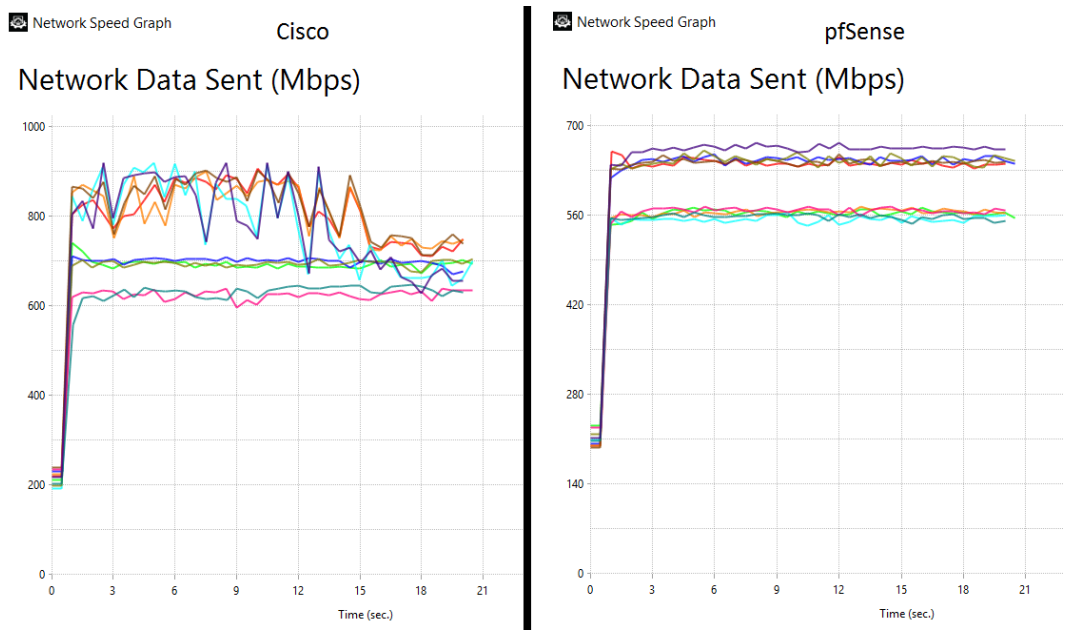


KUVIO 8. Verkon nopeuden kuvaajat 32 tavun paketeilla

Toinen testi tehtiin vaihtelevan kokoisilla paketeilla. Tämän testin perusteella laitteissa oli nähtävissä enemmän eroavaisuuksia kuin tasaisella pakettikoolla. Molemmilla laitteilla verkon nopeus nousi nopeasti paketin koon noustessa. Alkunopeus oli kummallakin palomuurilla noin 200 Mbps, mutta pakettien koon muuttuessa nopeuksissa tuli huomattavia eroavaisuuksia. Ciscolla nopeus nousi viidessä näytteessä parhaimmillaan hieman yli 900 megabittiin sekunnissa, mutta näissä näytteissä nopeuden vaihtelu oli suurta. Loppujen viiden näytteen maksiminopeudet vaihtelivat 600–700 Mbps välillä ja pysyivät huomattavasti tasaisempina.

pfSensen nopeudet jäivät tässä mittaustavassa alle 700 megabittiin sekunnissa. Lähetetyn datan nopeus vaihteli maksimissaan noin 560 ja

670 Mbps välillä sekä yhtesnopeus pysyi kohtuullisen tasaisena. Alla olevassa kuviossa 9 on kuvakaappaus mittausohjelman kuvaajista kummallakin palomuurilla vaihtelevan kokoisilla paketeilla. Huomioi, että näiden mittausten kuvaajien pystyakseleissa on eri skaala.

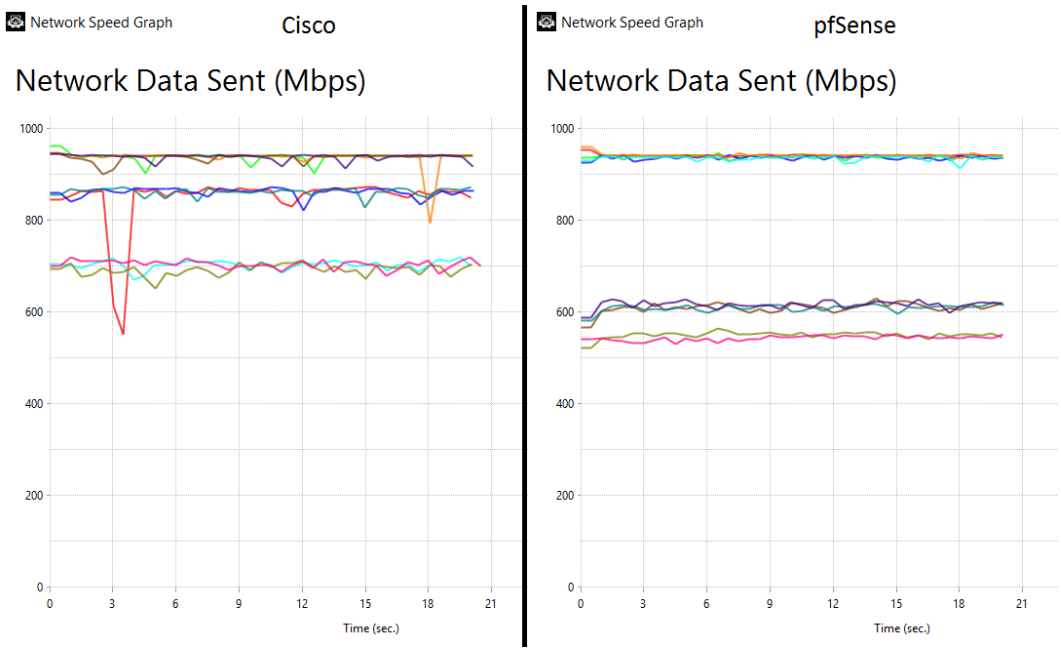


KUVIO 9. Verkon nopeuden kuvaajat vaihtelevan kokoisilla paketeilla

Suurimmalla pakettikoolla tehdyissä mittauksissa molemmat palomuurit saivat hyviä nopeuksia, mutta vaihtelua oli silti kohtuullisen runsaasti. Sekä Cisco että pfSense saivat parhaimmillaan noin 950 Mbps nopeudet lähetetyn datan mittauksella. Ciscon laitteen kuvaajista on haivaittavissa suurempaa hajaumaa yksittäisten mittausten sisällä kuin pfSensellä. Ciscon näytteet jakautuivat kolmelle eri tasolle. Heikoimmat kolme saavuttivat noin 700 Mbps nopeuden. Seuraavalla tasolla oli myös kolme näytettä noin 850 megabitillä sekunnissa. Neljä näytettä olivat selvästi nopeampia siirtäessään noin 950 megabittiä sekunnissa.

pfSensellä kuvaajien minimi- ja maksimiarvot vaihtelivat laajemmin ollen noin 525 Mbps ja 950 Mbps. pfSensen näytteet olivat jaettavissa kahteen

tasoon. Heikommalla tasolla oli puolet näytteistä. Näiden nopeudet olivat noin 550–650 Mbps. Toiset viisi näytteistä taas ylsi 950 megabittiin sekunnissa ja niiden hajauma yksittäisten näytteiden sisällä oli vähäinen. Alla esitetyssä kuviossa 10 havainnollistetaan Ciscon ja pfSensen läpäisynopeuksia maksimikokoisilla paketeilla PassMark Network Testin kuvaajilla.



KUVIO 10. Verkon nopeuden kuvaajat 32768 tavun paketeilla

Näiden nopeustestien perusteella on vaikea arvioda, kumpi laitteista olisi nopeampi tai toimisi luotettavammin parhailla nopeuksilla. Nopeudet olivat hyvin samankaltaisia kaikilla mittaustavoilla. Cisco tosin saavutti paremmat nopeudet vaihtelevan kokoisilla paketeilla kymmenen näytteen sarjassa, mutta kuten kuvaajista on huomattavissa, nopeudet saattavat vaihdella suuresti näytteiden välillä samalla mittaustekniikallakin. Osa mittauksista oli selvästä heikompia kuin seuraava tai sitä edeltänyt näyte. Tästä syystä ei kannata suoraan tehdä johtopäätöstä, että pfSense ei pystyisi mitattua parempiin nopeuksiin vaihtelevalla paketin koolla. Jotta laitteet voisi

asettaa nopeusjärjestykseen, vaadittaisiin huomattavasti suurempi määrä näytteitä, joista tehdä tilastoja. Tämän testin perusteella voidaan kuitenkin todeta, että Ciscon lupaama 900 Mbps nopeus RV320-palomuurireitittimelle on täysin mahdollista saavuttaa.

6 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli selvittää Cisco RV320 ja pfSense palomuurien soveltuvuus Lahden ammattikorkeakoulun tekniikan laitoksen toteuttamiin tietoverkkoihin hiihdon MM-kisoissa Lahdessa talvella 2017. Näitä palomuureja vertailtiin ensin teoriassa ja vertailun jälkeen testattiin niiden ominaisuuksia. Laitteista löytyi eroavaisuuksia, mutta kumpikaan ei osoittautunut ylivertaiseksi toiseen nähden.

Cisco RV320 toimi pääasiassa luotettavammin, sillä se ei missään vaiheessa testauksia osoittanut ongelmia yleisessä toiminnassa tai vaatinut uudelleenkäynnistämistä esimerkiksi konfiguraation käyttöönottamiseksi. Ciscon palomuuri vaati myös huomattavasti vähemmän konfigurointia ja oli heti tehdasasetuksillaan valmis käyttöönotettavaksi. Laitteen heikompina puolina voidaan toisaalta pitää konfiguraatiomahdollisuuksien rajallisuutta paikoittain, kuten VLAN:ien maksimin määrittäminen seitsemään sekä aliverkkojen koon rajaaminen laajimmillaan /24-aliverkonpeitteellä.

pfSensen palomuuri tarjoaa huomattavasti monipuolisemmat mahdollisuudet kuin RV320. Näistä esimerkkeinä vikasietoisuus (HA-klusteri ja RAID), rajaton VLAN:ien määrä sekä vapaasti valittavat LAN-puolen aliverkkojen koot ovat asioita, joita Cisco ei palomuurissaan tarjoa. pfSense vaati kuitenkin enemmän konfigurointia ja joskus asetukset astuivat voimaan vasta laitteen uudelleenkäynnistämisen jälkeen, vaikka ohjelmisto ei sitä erikseen pyytänyt. Tästä syystä järjestelmä tuntui ajoittain myös hieman epäluotettavalta, vaikkakaan palomuurin toiminnassa ei tullut ilmi ongelmia sen jälkeen kun kaikki konfiguraatiot olivat suoritettu ja palomuuri valmiina tuotantoympäristöön. pfSenseen on saatavilla lisäosilla lukuisia lisäominaisuuksia erilaisiin tarpeisiin. Näihin ei tässä opinnäytetyössä perehdytty, mutta lisäosien tarjoamat mahdollisuudet on syytä pitää mielessä.

Suoritetuissa nopeustesteissä ei ilmaantunut merkittäviä eroja palomuurien välillä. Molemmilla laitteilla esiintyi mittauksissa hajontaa niin

mittausten välillä kuin yksittäisten mittausten sisällä. Tulokset olivat hyvät, sillä kumpikin palomuuri saavutti parhaimmillaan yli 900 Mbps nopeuksia. Saadut tulokset ovat suuntaa antavia, ja läpäisynopeuksien tarkempi vertailu pfSensen ja Ciso RV320:n välillä vaatisi laajempaa tutkimista ja useampia mittauksia kaikilla pakettiko'oilla.

Tässä opinnäytetyössä tehtyjen omainaisuuksien selvittämisen ja testaamisen perusteella molempia laitteita voidaan suositella PK-yrityksille palomuuriksi tai muuhun vastaavaan käyttöön. Tarkoituksena oli kuitenkin selvittää, kumpi laite tulisi valita Lahden ammattikorkeakoulun tekniikan laitoksen toteuttamiin tietoverkkoihin hiihdon MM-kisoissa 2017. Tehdyn selvitystyön perusteella pfSensen palomuuria suositellaan otettavaksi käyttöön tuotantoympäristössä. Näissä tietoverkoissa on tarkoitus taata lähiverkon laitteille jatkuva ja laadukas yhteys Internetiin. pfSensen oleellisina etuina ovat laajempi vikasietoisuus, kuten palomuuripalvelun kahdennus, sekä laajemmat konfigurointimahdollisuudet. Näistä esimerkiksi LAN ja VLAN koon määrittely /23 tai laajemmalla aliverkon peitteellä ovat oleellisia ominaisuuksia, koska tuotantoon tulevien tietoverkkojen täytyy mahdollistaa verkkoon pääsy suurelle määrälle päätelaitteita. Edellä mainittujen syiden lisäksi halutaan nostaa esiin pfSensen mahdollisuuden yhdistää liitäntöjä esimerkiksi LACP-protokollaa käyttämällä sekä kahden WAN-liitännän samanaikaisen käytön, joista molemmat tavat nostavat verkon maksiminopeutta Internetiin.

Kahden tai useamman WAN-yhteyden käyttö yrityksissä on suositeltavaa, jotta voidaan taata jatkuva saatavuus ja tavoitettavuus nykypäivän usein vahvasti tietoverkkoihin tukeutuvassa liiketoiminnassa. Useaa WAN-yhteyttä hyödyntämällä voidaan aikaansaada myös suurempi tiedonsiirtokapasiteetti. Tulevaisuudessa esimerkiksi laitteiden Internet tulee vaatimaan lisää vikasietoisia ratkaisuja sekä kasvattamaan tietoliikenteen määrää. PK-yrityksillä on kaikki edellytykset edellä mainittujen ominaisuuksien hyödyntämiseen, sillä esimerkiksi varteenotettavien palomuurilaitteiden hankinta ei vaadi välttämättä suuria investointeja.

LÄHTEET

Burke. 2015. Virtual LAN (VLAN) [viitattu 28.12.2016]. SearchNetworking. Saatavissa: http://searchnetworking.techtarget.com/definition/virtual-LAN

Cisco 2014. Cisco RV320/RV325 Gigabit Dual WAN VPN Router ADMINISTRATION GUIDE [viitattu 27.10.2016]. Cisco. Saatavissa: https://cdn.cnetcontent.com/7a/ee/7aeec5a7-95e4-48b3-9a00-99856dca89fc.pdf

Cisco 2016. Cisco RV320 Dual Gigabit WAN VPN Router Data Sheet [viitattu 27.10.2016]. Cisco. Saatavissa: http://www.cisco.com/c/en/us/products/collateral/routers/rv320-dual-gigabit-wan-vpn-router/datasheet-c78-726132.html

Elers. 2016. Palomuuri [viitattu 17.12.2016]. Ficom ry. Saatavissa: http://www.ficom.fi/tietoa/tietoa_4_1.html?Id=1057649869.html

Lahden ammattikorkeakoulu 2016. Organisaatio [viitattu 31.12.2016]. Saatavissa: http://www.lamk.fi/lamk-oy/organisaatio/Sivut/default.aspx

pfSense 2014a. Create a Software RAID1 (gmirror) [viitattu 4.12.2016]. pfSense. Saatavissa: https://doc.pfsense.org/index.php/Create_a_Software_RAID1_(gmirror)

pfSense 2014b. SNMP Daemon [viitattu 4.12.2016]. pfSense. Saatavissa: https://doc.pfsense.org/index.php/SNMP_Daemon

pfSense 2015a. High Availability [viitattu 4.12.2016]. pfSense. Saatavissa: https://doc.pfsense.org/index.php/High_Availability

pfSense 2015b. How many interfaces does pfSense support [viitattu 23.11.2016]. pfSense. Saatavissa: https://doc.pfsense.org/index.php/How_many_interfaces_does_pfSense_support

pfSense 2015c. LAGG Interfaces [viitattu 4.12.2016]. pfSense. Saatavissa: https://doc.pfsense.org/index.php/LAGG_Interfaces

pfSense 2015d. SquidGuard package [viitattu 27.10.2016]. pfSense. Saatavissa: https://doc.pfsense.org/index.php/SquidGuard_package

pfSense 2016a. Features List [viitattu 27.11.2016]. pfSense. Saatavissa: https://doc.pfsense.org/index.php/Features_List

pfSense 2016b. Multi-WAN [viitattu 27.11.2016]. pfSense. Saatavissa: https://doc.pfsense.org/index.php/Multi-WAN

pfSense 2016c. VPN Capability Overview [viitattu 6.12.2016]. pfSense. Saatavissa: https://doc.pfsense.org/index.php/VPN_Capability_Overview

Reid. 2014. Cisco RV320 Dual Gigabit WAN VPN Router Reviewed [viitattu 6.12.2016]. SmallNetBuilder. Saatavissa: http://www.smallnetbuilder.com/lanwan/lanwan-reviews/32317-cisco-rv320-dual-gigabit-wan-vpn-router-reviewed

Shimonski, Shinder, Shinder & Carasik-Henmi. 2003. Best Damn Firewall Book Period [viitattu 17.12.2016]. Saatavissa: https://docstore.mik.ua/cisco/pdf/security/Syngress%20-%20Best%20Damn%20Firewall%20Book%20Period.pdf

Suomen Internetopas 2016. Tekninen suojaus [viitattu 17.12.2016]. Saatavissa: http://www.internetopas.com/yleistietoa/tietoturva/tekninensuojaus/

Wikipedia 2014. Link aggregation [viitattu 4.12.2016]. Wikipedia. Saatavissa: https://en.wikipedia.org/wiki/Link_aggregation