

Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2021

Janne Salmi

SD-WAN-RATKAISUN TESTAUS JA ARVIOINTI

Janne Salmi

SD-WAN-RATKAISUN TESTAUS JA ARVIOINTI

Ohjelmisto-ohjatut laajaverkko- eli SD-WAN-palvelut ovat yleistyneet paljon viime vuosina, ja niitä tarjoavien yritysten määrä on kasvussa. Tässä opinnäytetyössä testattiin yhden laitevalmistajan SD-WAN-ratkaisun soveltuvuutta yritysasiakkaille tarjottavan verkkopalvelun pohjaksi. Ratkaisuun sisältyi fyysiset verkkolaitteet sekä niitä yhdistävä pilvihallintaohjelmisto, joille molemmille suoritettiin testejä niiden toiminnallisuuden testaamiseksi. Työn tavoitteena oli testaustulosten perusteella muodostaa kokonaisarvio ratkaisusta sekä palvelua käyttävän yritysasiakkaan, että palvelua tarjoavan yrityksen näkökulmasta.

Työ tehtiin suunnittelemalla ja rakentamalla testiverkko SD-WAN-ratkaisun ympärille toimeksiantajan runkoverkkoon. Testeissä tutkittiin ratkaisun eri osien toiminnallisuutta, määritysmahdollisuuksia ja soveltuvuutta täyttämään toimeksiantajan sille asettamat vaatimukset.

Testauksessa ratkaisu todettiin ominaisuuksiltaan pääosin toimivaksi, mutta sen hetkisen pilvihallintaohjelmistoversion ongelmat tekivät siitä toistaiseksi kelpaamattoman käytettäväksi osana palvelua. Ratkaisun sisältämiä laitteita voidaan kuitenkin lähteä käyttämään palvelussa manuaalisesti määritettyinä ilman pilvihallintaohjelmistoa, kunnes ongelmat korjataan.

Työn tuloksena sekä toimeksiantajalle että työn tekijälle jäi paremmat tiedot SD-WANin toiminnasta ja yritysverkkojen toteuttamisesta sen avulla. SD-WAN-palvelun kehityksessä päästiin testaustulosten avulla siirtymään eteenpäin ensimmäisiin käytännön testeihin asiakaskohteissa.

ASIASANAT:

SD-WAN, ohjelmisto-ohjattu laajaverkko, laajaverkko, yritysverkko

Janne Salmi

TESTING AND EVALUATION OF SD-WAN SOLUTION

Software-driven wide area network (SD-WAN) services have become more widespread in recent years, and amount of companies that offer them is growing. The purpose of this thesis was to test the suitability of one manufacturer's SD-WAN-solution as a basis for a service offered to business customers. The solution included physical network equipment as well as its cloud management software, and different tests were conducted to test the functionality of them both. The purpose of the work was to evaluate the solution based on the test results from the point of view of both the corporate customer using the service and the company providing the service.

The work was carried out by designing and building a test network in the company's backbone network that is based on the hardware and software of the SD-WAN solution. The tests examined the solution's functionality, configuration possibilities and suitability to meet the requirements set by the company.

In testing, most of the solution's features were found to be functional, but the problems of the current cloud management software version made it unusable as part of the service in its current state. However, the devices included in the solution can be manually configured without cloud management software and used in the development until the problems are fixed.

As a result of the work, both the client and the writer of the thesis were left with better information about the operation of SD-WAN and the implementation of corporate networks with it. With the test results, the SD-WAN-service project was able to move forward to practical testing in real life corporate networks.

KEYWORDS:

SD-WAN, software-defined wide-area networks, wide area networks, corporate networks

SISÄLTÖ

KÄYTETYT LYHENTEET	6
1 JOHDANTO	1
2 SD-WAN VERRATTUNA PERINTEISIIN LAAJAVERKKOTOTEUTUKSIIN	3
2.1 SD-WAN	3
2.2 Keskitetty hallinta	3
2.3 Käyttöönotto	4
2.4 Yhteysriippumattomuus	4
2.5 Tunneloidut yhteydet	5
2.6 Liikenteen ohjaus	5
2.7 Tietoturva	6
3 TESTIVERKKO	7
3.1 Testattava ohjelmisto ja laitteisto	7
3.2 Testiverkon suunnitelma	8
3.3 Testiverkon rakennus ja määrittäminen	12
4 TESTIT JA TULOKSET	14
4.1 Testattavat asiat ja ominaisuudet	14
4.2 Käyttöönotto	15
4.3 IPSec-tunnelit	18
4.4 IPSec-tunneleiden läpisyöttöteho	23
4.5 Tunneloidun yhteyden viive	29
4.6 Varayhteys	33
4.7 Ohjelmistopäivitys	35
4.8 Laitteenvaihto	37
5 ARVIOT JA JOHTOPÄÄTÖS	39
LÄHTEET	42

KUVAT

Kuva 1. Testiverkon looginen topologia.	9
Kuva 2. IPSec-tunneleiden hub and spoke -topologia.	10
Kuva 3. Esimerkki HQ-reitittimen ja palomuurin CreaNODE-mittauslaitteiden välisestä yhteydestä. Muiden reitittimien ja palomuurin väliset yhteydet ovat toteutettu samalla periaatteella.	11
Kuva 4. Pilvihallinnan Inter-site VPN -määrittys yleisten asetusten ja hub-laitteen osalta.	18
Kuva 5. Pilvihallinnan Inter-site VPN -määrittys spoke-laitteiden ja IPSec-asetusten osalta.	19
Kuva 6. Pilvihallinnan kautta palomuurille automaattisesti määritetty pääsynvalvontalista 3999.	20
Kuva 7. Liikenteen kulku HQ-reitittimeltä Internetiin palomuurin kautta.	21
Kuva 8. Palomuurin NAT-määrittymään tehty muutos, joka estää osoitteenmuunnoksen liikenteeltä, jonka määränpää on jokin laitteiden lähiverkoista.	22
Kuva 9. Esimerkki TrueTCP-testin asetusikkunasta palomuurin ja HQ-reitittimen välisessä mittauksessa.	24
Kuva 10. Esimerkki Palomuurin ja BR-2-reitittimen 200 yhteyden TrueTCP-mittauksen tuloksista.	25
Kuva 11. Palomuurin ja BR-1-reitittimen välisen tunneloidun yhteyden keskimääräinen kahdensuuntainen viive CreaNODE-mittalaitteilla mitattuna.	30
Kuva 12. BR-2-reitittimen lähiverkossa olevalla tietokoneella tehty nopeustesti IPSec-tunneloidulla yhteydellä VDSL-liittymää käyttäen.	32
Kuva 13. BR-1-reitittimen komentorivi käynnistäessä jatkuvan ping-komennon ja irroittaessa Ethernet-kaapelin.	34
Kuva 14. Ohjelmistopäivitysaikataulun luonti kahdelle laitteelle pilvihallinnan kautta.	36
Kuva 15. Pilvihallintapalvelimen korvausvalikko vaihtaessa HQ-reitittimen toiseen samanmalliseen laitteeseen.	37

TAULUKOT

Taulukko 1. Mittaustulokset mittausliikenteen kulkiessa palomuurin mittalaitteelta reitittimien mittalaitteille.	26
Taulukko 2. Mittaustulokset mittausliikenteen kulkiessa reitittimien mittalaitteilta palomuurin mittalaitteelle.	27
Taulukko 3. Maksimikaistanleveyden mittaustulokset.	28

KÄYTETYT LYHENTEET

AES	Lohkosalausmenetelmä (Advanced Encryption Standard)
APN	Mobiililiittymän yhteysosoite (Access Point Name)
DHCP	Verkkoprotokolla IP-osoitteiden jakamiseen (Dynamic Host Configuration Protocol)
DNS	Internetin nimipalvelujärjestelmä (Domain Name System)
Epipe VLL	Virtuaalinen kahden pisteen välinen yhteys (Ethernet Pipe Virtual Leased Line)
Gb/s	Gigabittiä sekunnissa
GE	Gigabit Ethernet
GRE	Tunnelointiprotokolla (Generic Routing Encapsulation)
ICMP	Verkkoprotokolla viestien lähettämiseen (Internet Control Message Protocol)
IPSec	Tunnelointiprotokolla (Internet Protocol Security)
LAN	Lähiverkko (Local Area Network)
MAC	Verkkosovittimen yksilöivä osoite (Media Access Control)
Mb/s	Megabittiä sekunnissa
MD5	Salausalgoritmi (Message Digest 5)
MPLS	IP-liikenteen kuljetusmenetelmä, jossa ei tarvita reititystä (Multiprotocol Label Switching)
MSS	Suurin mahdollinen paketin datan määrä (Maximum Segment Size)
MTU	Suurin mahdollinen pakettikoko (Maximum Transmission Unit)
NAT	Osoitteenmuunnos (Network Address Translation)

NETCONF	Verkonhallintaprotokolla (Network Configuration Protocol)
PAT	Osoitteenmuunnosmenetelmä (Port Address Translation)
SAS	Nokian kytkinten tuotesarja (Service Access Switch)
SD-WAN	Ohjelmisto-ohjattu laajaverkko (Software-defined Wide Area Network)
SFP	Verkkoliitäntätyyppi (Small Form-factor Pluggable)
SHA	Kryptograafinen tiivistefunktio (Secure Hash Algorithm)
SSH	Salatun tietoliikenteen verkkoprotokolla (Secure Shell)
TCP	Luotettava, yhteyspohjainen tietoliikenneprotokolla (Transmission Control Protocol)
UDP	Nopea, yhteydetön tietoliikenneprotokolla (User Datagram Protocol)
VDSL	Nopea, kuparikaapeliyhteyksiin perustuva yhteystyyppi (Very High-speed Digital Subscriber Line)
VLAN	Virtuaalinen lähiverkko (Virtual Local Area Network)
VPN	Julkisen verkon läpi kulkeva tunnettu virtuaalinen lähiverkko (Virtual Private Network)
WAN	Laajaverkko (Wide Area Network)
ZTP	Verkkolaitteiden automaattinen määrittäminen verkkoon yhdistäessä (Zero Touch Provisioning)

1 JOHDANTO

SD-WAN- eli ohjelmisto-ohjattu laajaverkko on teknologia, joka helpottaa laajaverkkojen määrittystä, ylläpitoa ja vianratkaisua laitteiden keskitetyn etähallinnan avulla. Se on nykyään nopeasti kasvava osa verkkoinfrastruktuurimarkkinoita, jonka avulla verkkojen toimintaa saadaan parannettua ja tehostettua.

Tämä opinnäytetyö tehtiin toimeksiantona yritykselle, joka on kehittämässä omaa palveluaan yhden laitevalmistajan SD-WAN-ratkaisun pohjalta. Ratkaisu sisältää laitteiston sekä niiden hallintaan tarkoitetun ohjelmiston. Yritysasiakkaille tarjottavaan SD-WAN-palveluun sisältyisi SD-WAN-ratkaisun lisäksi keskitetty palomuuuri- ja verkon ylläpitopalvelu. Palvelu mahdollistaisi laajaverkkopalvelujen tarjoamisen asiakasyrityksille toimeksiantajayrityksen oman runkoverkkoalueen ulkopuolelle sekä helpottaisi huomattavasti yritysverkkojen asennusta, määrittystä, hallintaa ja vianselvitystä. Sen avulla toimeksiantajayritys saisi kasvatettua asiakasmääräänsä sekä toimialuettaan ja samalla yksinkertaistettua asiakasverkkojen parissa työskentelyä.

Toimeksiantajalla on omat yksilölliset tarpeet, jotka suunnitellun palvelun tulee täyttää. Ensinnäkin kaiken yritysasiakkaiden liikenteen tulee kulkea palveluntarjoajan keskitetyn palomuurin läpi tunneloidulla yhteydellä ilman että yhteys eroaa asiakkaan näkökulmasta perinteisestä yritysytymisestä. Ratkaisun sisältämien laitteiden tulee tukea korkeita nopeuksia tunneloidulla yhteydellä ja olla yksinkertaisia ottaa käyttöön. Lisäksi yritysverkkojen ylläpidon ja vianselvityksen pitää olla suoraviivaista mahdollisimman korkean käytettävyyden takaamiseksi.

Työssä rakennetaan testiverkko SD-WAN-ratkaisun ohjelmiston ja laitteiston ympärille ja sen avulla testataan sekä varmistetaan ratkaisun toimivuus. Tavoitteena on testeissä saatujen tuloksien avulla arvioida ratkaisun soveltuvuutta osaksi yritysasiakkaille tarjottavaa palvelua. Tarkoituksena on selvittää, miten hyvin ratkaisu toimii ja mahdollisesti myös mitä puutteita siinä on.

Työ koostuu teoriaosuudesta, testauksesta ja arvioinnista. Teoriaosuudessa käydään läpi lyhyesti SD-WAN-teknologiaa ja sen tuomia etuja verrattuna tavanomaisiin laajaverkkoratkaisuihin. Testausosuudessa kerrotaan ensin työtä varten kehitetystä testiverkosta ja testattavista ominaisuuksista ja sitten esitellään jokainen testi ja niistä saadut tulokset. Testien jälkeen arvioidaan kerättyjen tietojen perusteella SD-WAN-ratkaisun

tekniisiä ja taloudellisia ominaisuuksia sekä asiakasyrityksen että palveluntarjoajan eli toimeksiantajayrityksen näkökulmasta. Lopuksi esitetään johtopäätökset ratkaisun käytökelpoisuudesta ja palvelun kehityksen jatkosta.

2 SD-WAN VERRATTUNA PERINTEISIIN LAAJAVERKKOTOTEUTUKSIIN

2.1 SD-WAN

Laajaverkot ovat maailman merkittävimpiä tietoliikenneverkkoja, jotka kuljettavat tietoa paikasta toiseen pitkien matkojen yli ja siten luovat perustan maailmanlaajuiselle Internetille. Ohjelmistopohjainen laajaverkko eli SD-WAN (software-defined wide area network) on virtuaalitekniikka, jossa laajaverkkoa hallitaan ohjelmiston avulla. Sen pääperiaate on erottaa verkon hallinta- ja tietoliikennetasot toisistaan ja siirtää hallintataso keskitettyyn ohjelmistoportaaliin, joka useimmiten toimii joko palveluntarjoajan tai asiakkaan pilvessä. SD-WAN-toteutus voi koostua erilaisista fyysisistä laitteista, kuten reitittimistä ja kytkimistä tai virtuaalilaitteista kuten virtuaalipalomuureista. Merkittävin osa on laitteita niitä yhdistävä ohjelmisto, jolla koko laajaverkkoa hallitaan. (Cooney 2019.) Eri palveluntarjoajien ratkaisuissa on eroja, mutta niiden kaikkien perusideana on helpottaa laajaverkkojen rakentamista, ylläpitoa ja vianmäärittystä.

Yhä useampi laitevalmistaja ja palveluntarjoaja on kiinnostunut SD-WANista, sillä se on nykyään nopeitten kasvavimpia verkkoinfrastruktuurimarkkinoiden osa-alueita. Futuuriomien vuonna 2020 julkaiseman tutkimuksen mukaan SD-WAN-ratkaisujen kysyntä tulee jatkamaan kasvuaan COVID-19-pandemiasta huolimatta ainakin 2023 asti ja todennäköisesti vielä pidempään. Myös potentiaalisten asiakkaiden tietoisuus eri ratkaisuista on kasvanut markkinoiden kasvaessa ja tutkimuksessa haastatelluista yrityksistä 92% on jo harkinnut niiden käyttöönottoa. (Raynovich 2020.)

2.2 Keskitetty hallinta

Nykyään yritykset kasvavat nopeasti ja levittäytyvät maantieteellisesti laajoille alueille perustaen uusia toimipisteitä. Yritysten verkot laajenevat myös luonnollisesti yritysten laajentuessa, ja verkon muutokset suoritetaan yleensä määrittelemällä jokainen verkko-laite manuaalisesti laitevalmistajan tavan mukaisesti, joka on hidasta ja virhealtista työtä. (Yang ym. 2019, 1.) SD-WANin avulla koko verkon hallinta tapahtuu keskitetysti, joten kaikki tarvittavat määrytykset voidaan tehdä laitteille etänä. Tehdyt muutokset päivittyvät kaikille niitä koskeville laitteille automaattisesti, mikä helpottaa huomattavasti etenkin

suurten ja monimutkaisten verkkojen hallintaa. IT-henkilökuntaa ei myöskään välttämättä tarvitse paikan päällä, koska kaiken tarvittavan saa hoidettua etänä. (Riverbed 2021.) Kun verkon hallinta muuttuu yksinkertaisemmaksi, myös yrityksen toiminta voi tehostua. Aikaa kuluu vähemmän sen ylläpitoon ja yrityksen laajentuessa myös verkko laajenee ketterämmin sen mukana.

2.3 Käyttöönotto

Verkkojen laajentaminen helpottuu SD-WAN-teknologian avulla huomattavasti, sillä uudet laitteet voidaan ottaa käyttöön ZTP eli zero touch provisioning -ominaisuuden avulla. ZTP:tä tukevat laitteet tulee käyttöön ottamiseksi yhdistää vain virtoihin ja Internetiin, jolloin ne yhdistävät automaattisesti SD-WAN-hallintaan ja voidaan määritellä sieltä käsin käyttökuntoon etänä. Laitteille voidaan myös määritellä oikeat asetukset etukäteen valmiiksi ja sitten lähettää ne uuteen toimipisteeseen kytkettäväksi paikoilleen. ZTP:n avulla kuka tahansa työntekijä voi kytkeä uuden verkkolaitteen, vaikka heillä ei olisi IT-taitoja. Perinteiset laajaverkkojen laitteet eivät tue tätä ominaisuutta ja vaativat aina ammattilaisen tekemän manuaalisen määrittelyn käyttöönottilanteessa. (Riverbed 2021.)

2.4 Yhteysriippumattomuus

Perinteiset laajaverkkototeutukset ja toimipisteiden väliset yritysverkko-yhteydet vaativat paljon suunnittelua ja resursseja sekä yritykseltä että palveluntarjoajalta. Palveluntarjoajien runkoverkkojen rajat ylittävät yhteydet vaativat yhteistyötä ja koordinaatiota myös kaikilta, joiden runkoverkon läpi yhteys kulkee. Yritysverkko-yhteydet ja -laitteet ovat aina sidottuja tiettyyn sijaintiin ja muutosten tekeminen on hidasta.

SD-WANin merkittävimpiä ominaisuuksia on se, että se voidaan toteuttaa lähes mitä tahansa internetyhteyttä käyttäen. Tämä mahdollistaa kustannustehokkaiden laajakaistaja mobiiliyhteyksien käytön osana verkkoa, eikä yritys välttämättä tarvitse kalliimpia yritysverkko-yhteyksiä, kuten MPLS-yhteyksiä ollenkaan. (Craven 2017.) Samalla myös operaattori-riippumattomuus on mahdollista ja yritys voi hyödyntää parasta tarjottua yhteyttä tietyn toimipisteen sijainnin mukaan. Jos toimipiste muuttaa, SD-WAN mukautuu muutokseen automaattisesti, eikä ole siten sidottu fyysiseen sijaintiin.

SD-WAN on kuitenkin aina vaan niin hyvä kuin sen heikoin yhteys, joten se ei ole kokonaan korvaamassa kiinteitä yritysverkkoyhteyksiä. Koko yritysverkkoa ei esimerkiksi kannata rakentaa pelkästään mobiiliyhteyksien varaan. Monien yritysten kannattaakin tarpeen mukaan yhdistää yritysverkkoyhteytensä SD-WAN-toteutukseen, jolloin ne saavat sekä luotettavimman mahdollisen yhteyden, että SD-WANin tuomat ominaisuudet ja edut.

2.5 Tunneloidut yhteydet

Koska SD-WAN perustuu virtualisoituun verkkoon, käytännössä kaikissa nykyisissä toteutuksissa yhteydet kulkevat automaattisesti luoduissa virtuaalisissa tunneleissa. Yleisimpiä käytettyjä tunnelointitekniikoita ovat GRE ja IPSec, joiden avulla kahden pisteen välinen liikenne kulkee kapseloituna julkisen Internetin läpi. IPSecin avulla liikenne saadaan myös salattua tietoturvan parantamiseksi. (Mota 2020, 5.) Tunneleiden avulla yrityksen toimipisteet saadaan yhdistettyä turvallisesti toisiinsa riippumatta yhteystyypistä ja reitin varrella olevasta infrastruktuurista.

Tunneloitujen yhteyksien käytöllä on kuitenkin myös haittoja. Merkittävimpänä näistä on liikenteen kapseloinnista ja salauksesta johtuen kasvava pakettikoko, jonka vuoksi kaistanleveyttä tarvitaan tunneloimatonta yhteyttä enemmän. Koska tunneloidut yhteydet kulkevat julkisen Internetin läpi, fyysiset linkit voivat jossain tapauksissa ruuhkautua huonontuen yhteyden suorituskykyä. (Mota 2020, 6.) Nykyään on kehitteillä myös SD-WAN-ratkaisuja, jotka pyrkivät näiden haittojen ehkäisemiseksi muodostamaan yhteydet ilman tunneleita.

2.6 Liikenteen ohjaus

Tiedonsiirto perinteisten laajaverkkojen läpi toteutetaan perinteisesti ilman minkäänlaista liikenteen priorisointia, best effort -periaatteella, jolloin liikenteen perille pääsyä tai sovel-luskohtaisten vaatimusten täyttymistä ei pystytä takaamaan. Monet uudet sovellukset nostavat verkkoyhteyksien vaatimuksia, eivätkä ole enää yhteensopivia perinteisellä tavalla toteutettujen laajaverkkojen kanssa. Tästä esimerkkinä on reaaliaikaiset sovellukset, kuten etänä suoritettavat terveydenhuollon toimenpiteet, jotka vaativat onnistuakseen verkolta tasaista ja alhaista viivettä. Tätä best effort -tiedonsiirtoperiaatteella ei pystytä takaamaan. (Yang ym. 2019, 2.)

SD-WANin avulla liikennettä voidaan ohjata sovellustietoisesti ja siten priorisoida eri tarpeiden mukaan. Esimerkiksi reaaliaikainen ja alhaisesta viiveestä riippuvainen liikenne, kuten ääni- ja videoliikenne voidaan määritellä kulkemaan aina nopeinta mahdollista yhteyttä pitkin. Vähemmän tärkeän liikenteen prioriteettia voidaan samalla laskea esimerkiksi rajoittamalla sille käytettävissä olevaa kaistanleveyttä, tai ohjaamalla se kulkemaan hitaamman yhteyden kautta. (Davies 2021.) Perinteisissä laajaverkossa eri palvelut lähettävät liikennettä halutessaan ajankohdasta tai lähetettävän tiedon määrästä riippumatta. Tämä aiheuttaa hetkittäisiä piikkejä yhteyden käyttöasteessa, jonka vuoksi yhteyskapasiteettia on usein varattu tarvittua enemmän ruuhkautumisen ja pakettihäviön välttämiseksi. (Yang ym. 2019, 3.) SD-WANin avulla eri sovellusten keskinäistä toimintaa voidaan koordinoita, jolloin yhteyden käytön hetkittaiset vaihtelut vähenevät ja kaistanleveyttä saadaan hyödynnettyä tehokkaammin.

Vikatilanteissa SD-WAN voi ohjata liikennettä dynaamisesti varmistaen korkean käytettävyyden. Jos jokin fyysinen linkki äkillisesti katkeaa tai jokin käytettävistä yhteyksistä hetkellisesti ruuhkautuu, liikenne käännettään automaattisesti kulkemaan paremman tai korvaavan yhteyden kautta. Liikennettä voi myös jakaa useammalle käytettävälle yhteydelle samanaikaisesti verkon kuormituksen tasaamiseksi tai käytettävyyden parantamiseksi. (Riverbed 2021.)

2.7 Tietoturva

Tietoturva on aina merkittävä osa kaikissa verkkoratkaisuissa ja niin se on myös SD-WANissa. Perinteisistä laajaverkoista poiketen koko verkkoa saa hallittua ja monitoroitua keskitetysti etänä, joten mahdollisen verkkohyökkäyksen sattuessa IT-henkilökunta voi havaita tilanteen ja reagoida siihen nopeasti. Kaikkiin verkon laitteisiin saa tarvittaessa tehtyä nopeasti muutoksia kerralla, ja niiden ohjelmistot saa pidettyä ajan tasalla helposti. (Riverbed 2021.) Hyökkäyspinta-alan minimoimiseksi verkkoa voi sovellustasolla virtuaalisesti rajata pieniin osioihin, ja laitteiden välistä tarpeetonta kommunikaatiota saa rajoitettua. Siten verkkohyökkäys ei tapahtuessaan pääse vaikuttamaan koko verkkoon. Monien SD-WAN-ratkaisujen laitteet sisältävät myös silicon root of trust -sirun tai -komponentin, jotka aina laitteiden käynnistyessä varmistavat suoritettavan ohjelmiston aitouden. Siten esimerkiksi kesken toimituksen kaapattua ja muokatulla laiteohjelmistolla varustettua laitetta ei saa otettua käyttöön verkossa. (Wiesner 2020.)

3 TESTIVERKKO

3.1 Testattava ohjelmisto ja laitteisto

Testattavaan SD-WAN ratkaisuun sisältyy pilvihallintaohjelmisto, joka on suunniteltu laajaverkkoja pienempien campus-verkkojen keskitettyyn hallintaan ja ylläpitoon, mutta se sopii laitevalmistajan tarjoamista vaihtoehtoista parhaiten yrityksen tarpeisiin. Sen avulla eri asiakasyrityksille voi luoda omat käyttäjänsä, joiden avulla toimeksiantajayritys saa hallittua niiden eri toimipisteiden verkkoja etänä keskitetyn verkkokäyttöliittymän kautta. Laitteet saadaan yhdistettyä palvelimeen maantieteellisestä sijainnista tai Internet-palveluntarjoajasta riippumatta ja niiden väliset yhteydet toteutetaan IPSec-tunneleilla. Pilvihallintaohjelmisto oli asennettu valmiiksi yrityksen omaan lähipilveen virtuaalikoneelle, sillä sitä käytettiin opinnäytetyön testiverkon lisäksi samanaikaisesti jo toisessa projektissa.

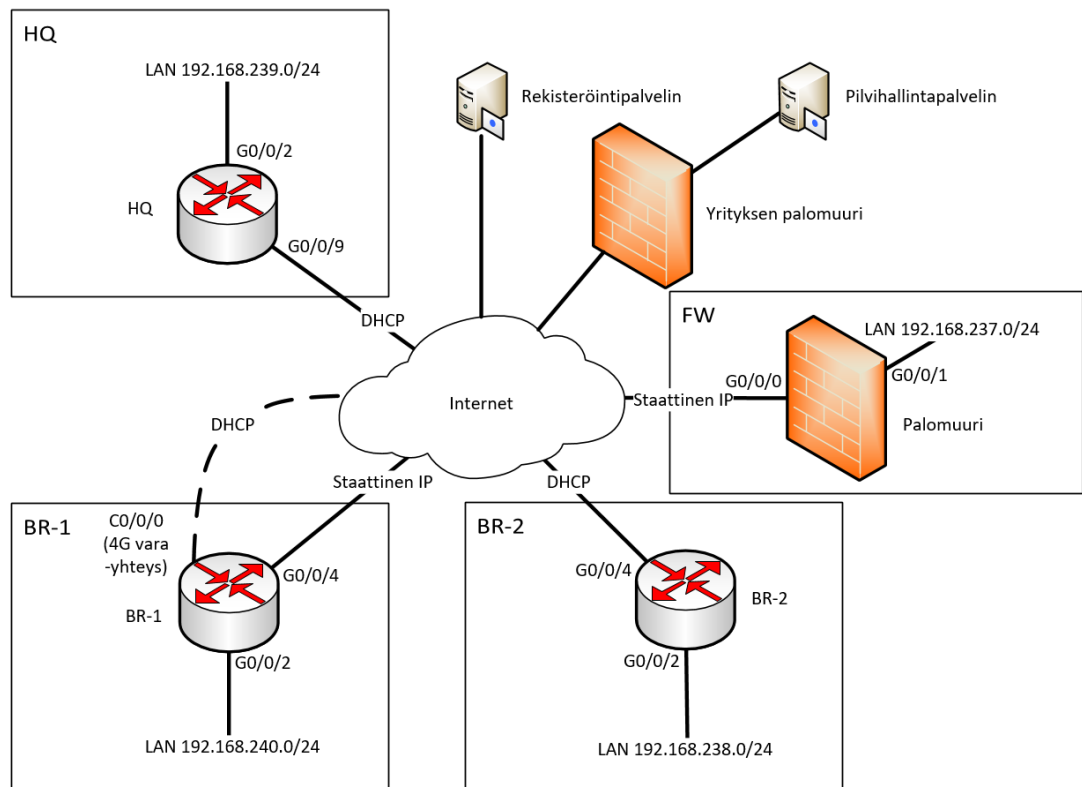
Testiverkossa käytettiin kolmea eri reititintä, joista kaikki olivat laitevalmistajan mukaan ominaisuuksiltaan suunniteltu pienille tai keskisuurille yrityksille. Kaikki testattavat reitittimet sekä myös yhteensopivat saman laitevalmistajan kytkimet ja langattomat tukiasemat voidaan lisätä pilvihallintaan. Siten lähes koko yrityksen sisäistä verkkoinfrastruktuuria voidaan hallita etänä. Käytettävät reitittimiä ovat kahdesta eri sarjasta, kalliimmasta ja edullisemmasta. Kalliimmasta sarjasta testattavana on yksi reititin, joka ominaisuuksiltaan soveltuu isoimmille asiakasyrityksille. Se sisältää 8 GE RJ45-liitintä LAN-yhteyksille ja 2 GE RJ45-liitintä WAN-yhteyksille. Sen suurin mahdollinen läpisyöttöteho on 2Gb/s, myös IPSec-tunnelin kautta, joka kuitenkin rajoittuu oletuskonfiguraatiossa yhdellä tunnelilla testatessa laitteen liitäntöjen vuoksi 1Gb/s. Tähän reitittimeen viitataan jatkossa lyhenteellä HQ, sillä tulevaisuudessa se asiakasyrityksen päätoimipistettä (engl. headquarters).

Edullisemmasta sarjasta testattavana oli kaksi reititintä, joista toinen sisältää tuen myös 4G-yhteydelle. Muilta ominaisuuksiltaan laitteet ovat lähes samanlaisia, molemmat sisältävät 4 GE RJ45-liitintä LAN-yhteyksille, 1 GE RJ45-liittimen WAN-yhteyksille sekä Wi-Fi-yhteyden. Suurin mahdollinen läpisyöttöteho on molemmissa 300Mb/s, ja IPSec-tunnelien maksimiläpisyöttötehoksi on ilmoitettu 200Mb/s. Nämä reitittimet simuloivat teisteissä asiakasyrityksen pienempiä haaratoimipisteitä, joten niihin viitataan jatkossa nimillä BR-1 ja BR-2 (engl. branch), joista BR-1 sisältää 4G-yhteyden.

Testiverkon palomuurina toimi saman laitevalmistajan palomuuuri, jonka tärkein ominaisuus testauksen kannalta on 2Gb/s suurin mahdollinen liikenne- ja IPSec- läpisyöttöteho. Tätä laitetta ei olla reitittimien tavoin myymässä asiakasyrityksille, vaan laite simuloi yrityksen keskitettyä palomuuria tai virtuaalipalomuuria, jonka kautta asiakasyrityksen liikenne kulkee. Koska pilvihallintaohjelmisto tukee myös kolmannen osapuolen laitteita osana verkkokonfiguraatioita, lopulliseen palveluun käytettävän palomuurin merkkiä tai mallia ei ollut opinnäytetyötä tehdessä vielä päätetty.

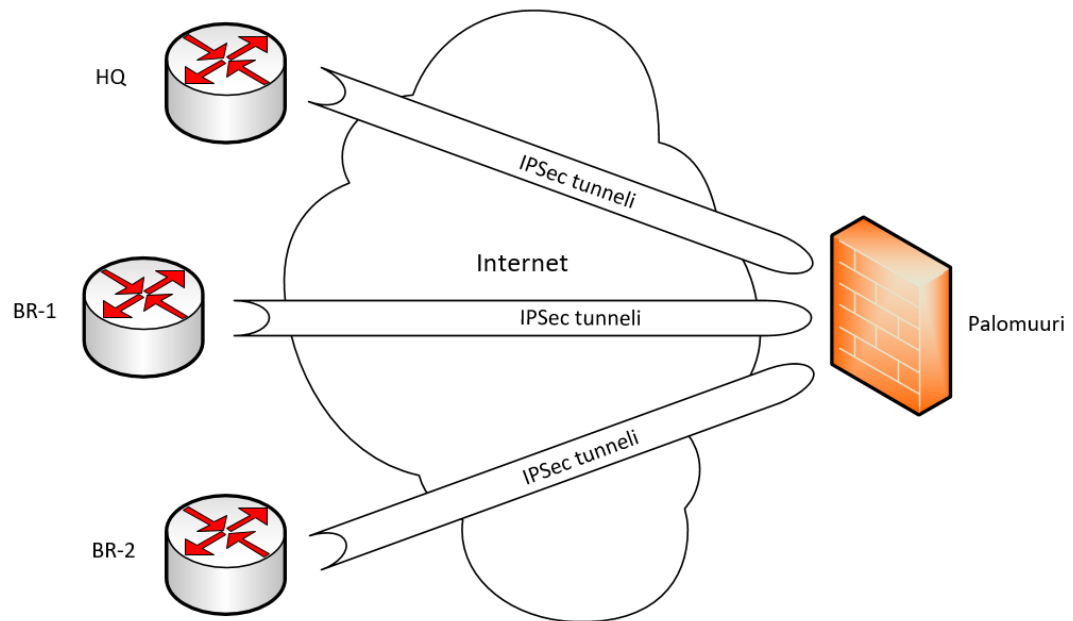
3.2 Testiverkon suunnitelma

Testiverkko suunniteltiin kuvan 1 topologian mukaisesti mallintamaan esimerkkiyritystä, jolla on kolme eri toimipistettä. Kaksi toimipisteistä esittää pienempiä haarapisteitä, ja ne sisältävät reitittimet BR-1 ja BR-2. Kolmas toimipiste esittää yrityksen isompaa päätoimipistettä, ja se sisältää reitittimen HQ. Jokainen reititin sijaitsee fyysisesti yrityksen testilaboratoriossa, on yhteydessä Internetiin ja jokaisella on oma lähiverkkonsa. Lisäksi BR-1:llä on käytössä myös 4G-varayhteys SIM-kortin avulla. Testiverkon viimeinen fyysisesti laboratoriossa sijaitseva laite on palomuuuri, jolla on reitittimien tavoin yhteys Internetiin sekä oma lähiverkkonsa. Palomuuuri mallintaa suunnitellun palvelun keskitettyä palomuuria, jonka läpi kaikki yrityksen verkkoliikenne kulkee. Se kuuluu omaan toimipisteeseensä FW (engl. firewall), joka suunnitellussa palvelussa ei ole asiakasyrityksen toimipiste, vaan toimeksiantajayrityksen oma laitetila.



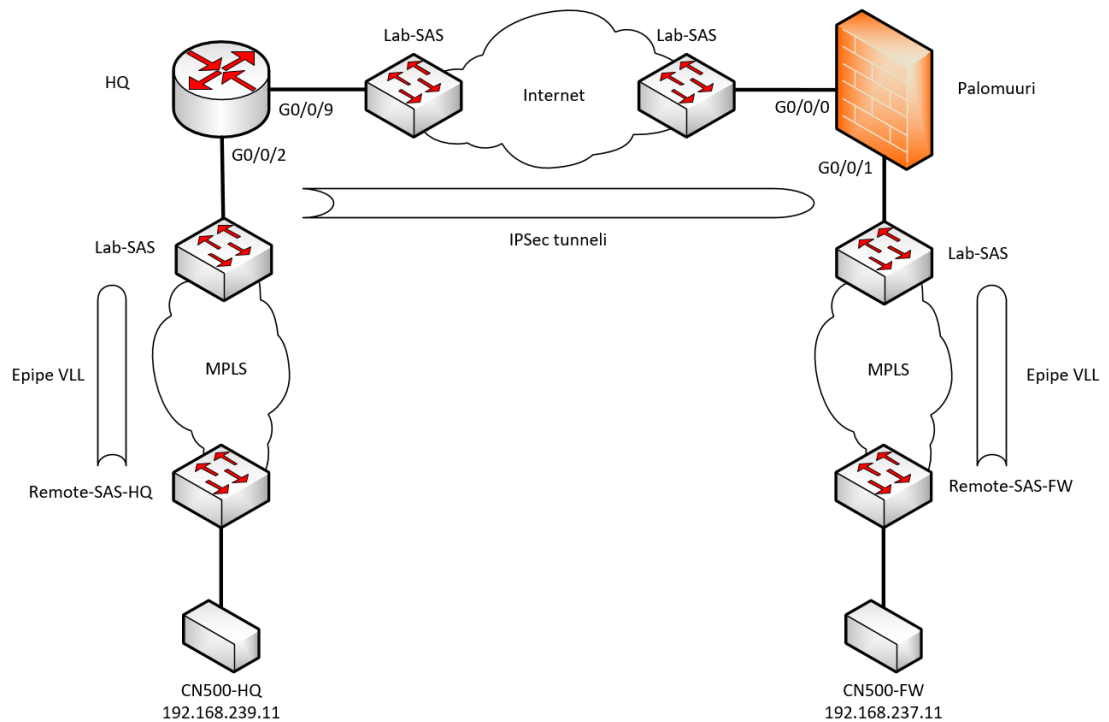
Kuva 1. Testiverkon looginen topologia.

Yhteydet reitittimien ja palomuurin välillä toteutetaan IPSec-tunneleilla, jotka toimivat kuvan 2 hub and spoke -topologian mukaisesti reitittimien toimiessa spoke-laitteina ja palomuurin toimiessa hub-laitteena.



Kuva 2. IPsec-tunneleiden hub and spoke -topologia.

Kaikki laitteet ovat yhteydessä yrityksen pilvihallintapalvelimeen, jonka kautta niitä hallitaan. Liikenne palvelimen ja ulkoverkon välillä kulkee yrityksen palomuurin läpi, johon on tehty tarvittavat avaukset sen sallimiseksi. Kaukaisimpana osana verkkoa on kuvassa 1 näkyvä laitevalmistajan rekisteröintipalvelin, johon uudet laitteet automaattisesti yhdistävät asennusvaiheessa ja saavat osoitetiedot siitä pilvihallintapalvelimesta, johon niiden sarjanumerot on lisätty. Siten laitteet osaavat yhdistää oikean palveluntarjoajan palvelimeen.



Kuva 3. Esimerkki HQ-reitittimen ja palomuurin CreaNODE-mittauslaitteiden välisestä yhteydestä. Muiden reitittimien ja palomuurin väliset yhteydet ovat toteutettu samalla periaatteella.

Toimipisteiden lähiverkkojen laitteita testiverkossa on mallintamassa neljä CreaNordin CreaNODE 500-verkkomittauslaitetta, jotka sijaitsevat yrityksen eri toimipisteissä noin 40-100 kilometrin etäisyydellä toisistaan. Normaalitilanteessa laitteet valvovat yrityksen runkoverkon eri pisteiden tilaa ja toimivuutta. Tässä opinnäytetyössä tehtävissä testeissä verkkomittauslaitteiden avulla saadaan mitattua eri laitteiden välisten IPsec-tunnelien läpisyöttötehoa ja viivettä. Jokaisesta laboratorion laitteesta on luotu yhteys omaan CreaNODE-laitteeseensa kuvan 3 esimerkin mukaisesti käyttäen Nokian SAS-kytkinten Epipe VLL-palvelua. Yhdessä Epipe VLL:n ja IPsec:n kanssa verkkomittauslaitteet saavat yhteyden toisiinsa laboratorion laitteiden kautta.

3.3 Testiverkon rakennus ja määrittäminen

Testiverkon rakennus aloitettiin kytkemällä reitittimiin ja palomuurin tarvittavat virta- ja Ethernet-johdot. Kaikki laitteet yhdistettiin samaan laboratorion Internetiin yhteydessä olevaan Nokian SAS-kytkimeen kahdella Ethernet-kaapelilla. Ensimmäiset kaapelit yhdistettiin kytkimestä laitteiden WAN-liitäntöihin internetyhteyden luomiseksi. Palomuurille ja BR-1-reitittimelle määriteltiin manuaalisesti staattinen julkinen IP-osoite ja oletusreitti, muut reitittimet saivat julkiset osoitteet ja määrittäykset automaattisesti DHCP:n avulla.

Toiset kaapelit yhdistettiin saman kytkimen toisista liitännöistä laitteiden LAN-liitäntöihin. Nämä laboratorion kytkimen liitännät yhdistettiin Epipe VLL -palvelun avulla niiden laite-tilojen SAS-kytkimiin, joissa kullekin laitteelle määritetty CreaNODE-laite oli yhdistettynä. Jokaisen verkkomittauslaitteen GE-liitäntöihin luotiin uudet aliliitännät VLAN tunnuksella 105 ja niille määriteltiin yksityiset IP-osoitteet jokaisen laboratoriolaitteen lähiverkon mukaan. Aliliitännät käytettiin, koska jokaisella verkkomittauslaitteella oli valmiiksi luotuna jo muita aliliitännät toisia mittauksia varten. Laboratoriokytken liitännät olivat määritetty poistamaan VLAN-tunnukset reitittimille ja palomuurille menevästä liikenteestä. CreaNODE-laitteille määriteltiin reitit kaikkien muiden verkkomittauslaitteiden lähiverkoihin, jotka kulkivat jokaisen verkkomittauslaitteen oletusyhdyskäytävän, eli oman laboratorion laitteen VLAN 1 -liitännän osoitteen kautta.

Viimeiseksi palomuurin toimintatila vaihdettiin normaalista pilvihallittuun, joka mahdollistaa pilvihallintapalvelimeen yhdistämisen. Reitittimiä ei tarvitse erikseen vaihtaa pilvihallittuun tilaan, vaan ne tukevat sitä suoraan. Palomuuuri käynnistyi uudelleen, jonka jälkeen sen liitännät määriteltiin sallimaan ICMP-liikenne yhteyksien toimivuuden testaamiseksi ping-komennon avulla.

Testiverkon fyysisen rakentamisen jälkeen siirryttiin ottamaan pilvihallintaa käyttöön. Pilvihallintapalvelimelle kirjauduttiin yrityksen pääkäyttäjällä selaimen käyttöliittymän kautta, ja testiverkkoa varten luotiin uusi yläkäyttäjä. Tällä käyttäjällä ei ole pääkäyttäjän tavoin käyttöoikeuksia itse palvelimen asetuksien, kuten lisenssien ja yhteyksien muokkaamiseen, vaan sitä käytetään itsenäisten alakäyttäjien eli tenantien hallitsemiseen. Yläkäyttäjä on tässä hierarkiassa toimeksiantajayritys ja jokainen sen hallinnassa oleva tenant-käyttäjä on oma asiakasyrityksensä tai itsenäinen yritysverkkonsa. Testiverkolle luotiin oma tenantinsa ja sen alle määriteltiin vielä yksittäisten laitteiden hallintasalasana.

Tämä salasana korvaa jokaisen pilvihallintaan yhdistetyn laitteen paikallisen konsolisalasanan.

Seuraavaksi kirjauduttiin tenantin hallintaan ja ryhdyttiin luomaan testiverkon topologiaa. Aluksi jokaiselle neljälle laitteelle luotiin oma virtuaalinen sijaintinsa, jotka simuloivat asiakas- tai toimeksiantajayrityksen toimipisteitä. Jokaiselle sijainnille pystyi antamaan tarvittavia tietoja, kuten osoitteen, vastuuhenkilön ja yhteystiedot. Myös käytettävä laitteisto valittiin luontivaiheessa jokaiselle sijainnille, testiverkon tapauksessa kolmelle sijainnille valittiin reitittimet ja yhdelle palomuuuri.

Ennen kuin laitteet sai yhdistettyä pilvihallintapalvelimeen, yrityksen omaan keskitettyyn palomuuriin piti tehdä tarvittavat portinavaukset. Liikenne sallittiin kulkemaan reitittimien käyttämistä IP-osoitelohkoista palvelimen osoitteeseen. Reitittimet lisättiin pilvihallintapalvelimelle syöttämällä niiden sarjanumerot, nimeämällä ne ja valitsemalla niille oikea sijainti. Sen jälkeen laitteille syötettiin konsoliyhteydellä komentorivin kautta komento, joka määrittelee pilvihallintapalvelimen osoitteen ja portin. Laitteet aloittivat yhdistämisprosessin ja siirtyivät online-tilaan palvelimella noin minuutin kuluessa. Yhdistämisprosessin jälkeen laitteet saivat automaattisesti niille aiemmin määritellyt asetukset, kuten laitenimen NETCONF-protokollaa käyttäen. Laitteiden yhdistämisen jälkeen niille määriteltiin loput testiverkon asetukset pilvihallinnan kautta. Ensisijaiseksi Internet-liitännäksi valittiin jokaisen laitteen WAN-Ethernet liitäntä ja jokaiselle laitteelle luotiin omat lähiverkot, joiden oletusyhdyksikäytäviksi määriteltiin laitteiden VLAN 1 -liitännät. Palomuurille määriteltiin näiden lisäksi myös tarvittavat säännöt, jotka sallivat muiden laitteiden lähiverkkojen, sekä julkisten IP-osoitteiden liikenteen kulun sen lävitse.

Jokaiselta laitteelta varmistettiin yhteyksien toimivuus toisten laitteiden, pilvihallintapalvelimen ja rekisteröintipalvelimen julkisiin IP-osoitteisiin ping-komennolla. Myös yhteys laboratoriolaitteiden omiin verkkomittauslaitteisiin varmistettiin ping-komennolla käyttäen lähdeosoitteena VLAN 1 -liitännän osoitetta. Kaikki yhteydet toimivat kuten pitikin, joten testiverkko oli määritelty onnistuneesti ja seuraavaksi päästiin siirtymään testaukseen.

4 TESTIT JA TULOKSET

4.1 Testattavat asiat ja ominaisuudet

Käytettävän ohjelmiston ja laitteiston tulee täyttää tietyt kriteerit, jotta niistä voidaan lähteä kehittämään asiakasyrityksille tarjottava palvelua. Ensimmäinen testattava asia on laitteiden asennus ja käyttöönottoprosessi. Pilvihallinnan tarkoituksena on tehdä laitteen käyttöönotosta paikan päällä mahdollisimman yksinkertaista ja jättää kaikki verkon määrittäminen tehtäväksi etänä. Laitteet tulisi saada yhdistettyä pilvihallintapalvelimeen ja otettua käyttöön sijainnista, Internet-palveluntarjoajasta ja yhteystyypistä riippumatta. Käyttöönoton jälkeen laitteen maantieteellistä sijaintia ja käytettävää internetyhteyttä pitäisi pysyä myös muuttamaan niin että yhteys palvelimeen säilyy. Tarkoituksena on testata ja varmistaa, että toimiiko laitteiden automaattinen rekisteröityminen ja säilyykö yhteys pilvihallintapalvelimeen myös muutosten jälkeen.

Laitteiden käyttöönoton jälkeen testataan palveluntarjoajan eli toimeksiantajayrityksen näkökulmasta itse pilvihallintaa. Tavoitteena olisi saada tehtyä kaikki tai ainakin suurin osa yritysverkkojen määrittämisestä pilvihallintapalvelimen käyttöliittymän kautta. Testatessa tutustutaan pilvihallinnan ominaisuuksiin ja tutkitaan saako sen kautta tehtyä kaikki tarvittavat määrittäykset laitteisiin.

Yrityksen suunnitelmana on toteuttaa palvelu siten, että asiakasyrityksen eri toimipisteiden reitittimet saavat yhteyden toisiinsa sekä Internetiin keskitetyn virtuaalipalomuurin kautta. Verkkoyhteydet toimipisteiden ja palomuurin välillä kulkevat salattuina IPSec-tunneleissa, joten on tärkeää, että tunnelit saadaan määritettyä toimimaan pilvihallintapalvelimen avulla. Tunneleita luodessa testataan, että kulkeeko liikenne halutulla tavalla, miten yksinkertaista määrittäminen on ja minkälaiset asetukset laitteet saavat automaattisesti.

Suunnitellussa palvelussa on myös tärkeää, että IPSec-tunnelien läpisyöttötehot ovat tarpeeksi suuret, sillä ne määrittelevät kuinka suuren yhteysnopeuden asiakasyritykselle voi tarjota, tai kuinka suuren nopeuden se voi hankkia toiselta operaattorilta yrityksen runkoverkon ulkopuolelta. Laittevalmistaja on ilmoittanut jokaiselle laitteelle maksimiläpisyöttötehon IPSec-tunneleille, ja näiden arvojen paikkansapitävyys tulee testata ja varmistaa. Lisäksi tulee tutkia, että minkälainen vaikutus tunneloidun yhteyden käytöllä on verrattuna tavanomaiseen yhteyteen. Asiakasyrityksen näkökulmasta näillä eri toteutuksilla ei tulisi olla käytössä merkittävää eroa.

Laitteet tulisi tietoturvan ja toiminnallisuuden parantamiseksi pitää aina päivitettynä. Normaalisti laiteohjelmistot pitää päivittää joko konsoliyhteydellä paikan päällä tai etänä SSH-yhteydellä yksi kerrallaan, joka on työlästä etenkin suuria laitemääriä sisältävissä yritysverkoissa. Pilvihallintapalvelin sisältää ominaisuuden, jolla yhdistetyt laitteet saadaan päivitettyä etänä automatisoidusti, joten sen toimivuutta on tarkoitus testata laboratorion laitteilla.

Yritysten verkkoyhteyksien tulee toimia luotettavasti keskeytyksettä, joten yhteydet tulee varmentaa ja mahdollisten vikatilanteiden kesto tulee minimoida. Testiverkon laitteista BR-1 sisältää tuen 4G-yhteydelle, jota voidaan käyttää varayhteytenä kiinteän laajakaistayhteyden rinnalla. Tarkoituksena on testata, miten yhteys käyttäytyy, kun toinen jostain syystä katkeaa ja kuinka pitkä katkos tästä aiheutuu. Parhaassa tilanteessa yhteys vaihtuisi nopeasti toiseen, ilman että käyttäjä huomaa merkittävää eroa. Toinen testattava asia on mahdollinen laitevikatilanne, jossa laite pitää vaihtaa toiseen. Laitemäärän ollessa suuri, myös riski laitevialle kasvaa, joten vaihdon tulisi olla mahdollisimman yksinkertainen toimenpide pilvihallinnan kautta. Pilvihallitussa tilassa laitteiden määitykset ovat tallennettuina pilvihallintapalvelimelle, joten on testattava, että siirtyvätkö ne automaattisesti vanhasta laitteesta uuteen.

4.2 Käyttöönotto

Ensimmäinen testattava ominaisuus oli ZTP, eli laitteiden automaattinen käyttöönotto ilman määrittystä paikan päällä. Laitevalmistajan dokumentaation mukaan prosessi etenee seuraavanlaisesti: Ensin uuden laitteen sarjanumero otetaan ylös ja pilvihallintapalvelimelle luodaan uusi sijainti ja laite kyseisellä sarjanumerolla. Laite ilmestyy sijainnille ja ilmoittaa tilaksi "unregistered" eli ei-rekisteröity. Seuraavaksi laite kytketään virtoihin ja yhdistetään Internetiin. Kun laite on yhdistetty Internetiin joko WAN Ethernet -liitännän tai SFP-moduulin kautta, se pystyy hakemaan IP-osoitteen DHCP:n avulla automaattisesti. Laitteelle voi myös tarvittaessa määritellä IP-osoitteen ja oletusreitit manuaalisesti. Kun laite saa internetyhteyden, se yhdistää automaattisesti laitevalmistajan lähimpään rekisteröintipalvelimeen. Rekisteröintipalvelimella on yhteys jokaisen samaa ratkaisua käyttävän palveluntarjoajan pilvihallintapalvelimeen ja se tietää siten mikä laite kuuluu millekin palvelimelle. Jos uuden laitteen sarjanumero vastaa jollekin pilvihallintapalvelimelle syötettyä sarjanumeroa, rekisteröintipalvelin lähettää laitteelle sen palvelimen

osoitteen. Siten laite osaa yhdistää automaattisesti oikean palveluntarjoajan pilvihallintapalvelimeen, ja laite ilmestyy siellä online-tilaan. Laitevalmistaja loi rekisteröintipalvelimen käyttöä varten yritykselle omat tunnukset, jotka lisättiin pilvihallintapalvelimelle yhdessä vaadittavan sertifikaatin kanssa. Tällä tapaa rekisteröintipalvelin sai tiedon yrityksen palvelimesta ja testaus voitiin aloittaa.

Ensimmäiseksi testattiin ZTP:tä parhaiten varustelluimmalla ja kalleimmalla reitittimellä, HQ:lla. Laite palautettiin ensin tehdasasetuksille konsoliyhteyden kautta, jotta mitkään aiemmat määrytykset eivät vaikuttaisi testiin. Ethernet-kaapeli kytkettiin laboratorion kytimestä laitteen WAN-liitäntään GE9, ja toimeksiantajayrityksen DHCP-palvelin määritettiin jakamaan osoite laitteelle. Laitevalmistajan dokumentaation mukaan normaali tehdasasetusten palautus tapahtuu, kun laitteen reset-painiketta painetaan yli 5 s, mutta alle 10 s. Rekisteröintiprosessin aloittamiseksi laitteen takaa löytyvää reset-painiketta tulee painaa yli 10 sekuntia pohjassa, kunnes laitteen etupuoella sijaitseva CTRL-valo alkoi vilkkua. Kun näin tehtiin, laite aloitti rekisteröintiprosessin onnistuneesti ja noin minuutin kuluttua se siirtyi online-tilaan yrityksen pilvihallintapalvelimelle. Laitteeseen latautui kaikki sille aiemmin määritellyt asetukset, kuten laitenumero ja lähiverkon asetukset.

Edullisemmilla reitittimillä kokeiltaessa testi ei tuottanut odotettuja tuloksia, eivätkä laitteet yhdistyneet pilvihallintapalvelimeen. Testissä molemmat laitteet olivat HQ:n tavoin tehdasasetuksilla, internetyhteys oli kytketty Ethernet-kaapelilla laitteiden WAN-liitäntöihin, ja ne saivat IP-osoitteen DHCP:n avulla. Reset-painiketta painettaessa yli 10 sekuntia laitteiden toiminta tai merkkivalot eivät kuitenkaan eronneet tavanomaisesta tehdasasetusten palautuksesta, vastoin dokumentaation tietoja. Molemmat laitteet käynnistyivät uudelleen noin 5 minuutin kuluttua ja saivat IP-osoitteen, mutta yhteys pilvihallintapalvelimeen jäi muodostumatta. Ping-komento laitteilta rekisteröintipalvelimen osoitteeseen kuitenkin onnistui. Testi suoritettiin molemmilla laitteilla kaksi kertaa alkuperäisellä ohjelmistoversiolla, sekä BR-2:lla toiset kaksi kertaa uudemmalla ohjelmistoversiolla, mutta ilman muutosta asiaan.

ZTP:n toimimattomuuden lisäksi edullisemmilla reitittimillä ilmeni myös toinen ongelma, sillä kun ne oli komentorivin kautta yhdistetty pilvihallintaan, ne eivät enää uudelleenkäynnistytksen jälkeen yhdistäneet sinne uudelleen. Tämä oli erityisen kriittinen puute, sillä laitteiden pilvihallinta on koko yrityksen suunnitteleman palvelun perusidea. Testatessa huomattiin myös, että melkein kaikki komentorivin kautta tehdyt määrytykset olivat laitteiden uudelleenkäynnistytksen jälkeen kadonneet, mutta kaikki komennot, jotka olivat syötetty ennen laitteiden yhdistämistä pilvihallintapalvelimeen, olivat edelleen tallella.

Tämä ongelma koski kaikkia reitittimiä, myös HQ-laitetta. Laitevalmistajalta kysyttäessä selvisi, että senhetkinen pilvihallintapalvelimen ohjelmistoversio ei tukenut reitittimien komentorivin kautta syötettyjen komentojen tallentamista laitteen ollessa pilvihallitussa tilassa. Pilvihallinnan uudempi ohjelmistoversio korjaisi tämän ongelman, mutta sen aikataulusta opinnäytetyötä tehdessä ei ollut vielä tietoa.

Pilvihallintapalvelimen rajoitusten vuoksi ryhdyttiin kehittämään vaihtoehtoista tapaa yhdistää reitittimet pilvihallintaan, pitää ne yhdistettynä myös uudelleenkäynnistyksen jälkeen ja säilyttää niille komentorivin kautta määritetyt asetukset. Kun laitteen yhdistää pilvihallintaan, mahdollisuus tallentaa määrittelyt paikalliseen asetustiedostoon ei ole enää sen jälkeen käytössä. Sen sijaan määrittelyt tallentuvat erilliseen ja erityyppiseen asetustiedostoon, jota ei pysty manuaalisesti avaamaan tai muokkaamaan, jos sen siirtää laitteelta tietokoneelle. Tämä tiedosto sisältää kaikki pilvihallintapalvelimen käyttöliittymän kautta tehdyt muutokset, ja se päivittyy automaattisesti kahden tunnin välein tai kun sen tallentaa manuaalisesti. Laitevalmistaja ehdotti ratkaisuksi lisätä laitteelle pilvihallintapalvelimen osoite ja tallentaa määrittelyt ennen laitteen yhdistämistä Internetiin. Näin tieto palvelimen osoitteesta säilyisi laitteella myös uudelleenkäynnistyksen jälkeen. Koska laitteet kuitenkin Internetiin yhdistettynä alkavat yhdistää palvelimeen heti komennon syöttämisen jälkeen, suljimme laitteille internetyhteyden tarjoavat liitännät laboratoriokytkimeltä komennon syöttämisen ja määrittelytallentamisen ajaksi. BR-1-laitteelle määriteltiin tässä kohtaa myös staattinen IP-osoite ja oletusreitti. Näin saimme tallennettua määrittelyt, jolla laitteet tietävät palvelimen osoitteen myös uudelleenkäynnistyksen jälkeen.

Kun laboratoriokytkimen liitännät taas avasi, laitteet yhdistivät palvelimeen ja hakivat niille määritellyt asetukset. Kun pilvihallinnasta tallensi laitteiden määrittelyt, se loi laitteille toiset määrittelytiedostot, jotka sisälsivät sen kautta tehdyt muutokset. Nyt kun laitteet käynnistettiin uudelleen, joko konsolin tai pilvihallinnan kautta, ne yhdistivät automaattisesti uudelleen pilvihallintapalvelimeen. Laboratoriokytkimen liitännät kokeiltiin myös sulkea ja sitten käynnistää reitittimet uudelleen. Koska määrittelyt olivat tallennettu pilvihallinnan kautta, laitteet säilyttivät sen kautta tehdyt asetukset. Ja koska palvelimen osoite oli käyttöönottoaiheessa asetettu paikalliseen asetustiedostoon, laitteet osasivat laboratoriokytkimen liitännät avattaessa yhdistää siihen uudelleen.

4.3 IPSec-tunnelit

Pilvihallinnan kautta määriteltävät IPSec-tunnelit ovat suunnitellussa palvelussa merkittävin osa asiakasyrityksen verkon määrittystä, sillä niiden avulla eri toimipisteiden verkot saavat kommunikoida keskenään. Palvelussa laitteet muodostaisivat hub and spoke -mallisen topologian, jossa asiakasyrityksen eri toimipisteiden reitittimet toimisivat spoke-laitteina, ja olisivat kaikki yhteydessä hub-laitteena toimivaan toimeksiantajayrityksen palomuruuriin. Siten kaikki asiakasyrityksen liikenne Internetiin sekä toimipisteestä toiseen kulkisi saman palomuurin kautta, joka valvoo koko yritysverkkoa keskitetysti.

IPSec-tunnelit sai luotua automaattisesti pilvihallinnan Inter-site VPN -asetuksen avulla, kun kaikki laitteet olivat yhteydessä pilvihallintapalvelimeen ja niille oli määritetty omat lähiverkot sen kautta. Määrittelyyn sai lisättyä saman asetuksen avulla myös laitevalmistajan laitteita, joita ei oltu yhdistetty pilvihallintaan tai toisen valmistajan manuaalisesti määriteltäviä laitteita. Näiden laitteiden lisäämiseksi pilvihallintapalvelimelle tarvitsi syöttää niiden julkinen IP-osoite sekä lähiverkon osoite.

The screenshot displays the 'Inter-site VPN' configuration page. At the top, the 'Modify Inter-site VPN' section is active. The 'Name' field is set to 'Hub-and-spoke-TEST1'. Under 'Topology mode', the 'Hub-Spoke' option is selected, showing a diagram of a central hub connected to multiple spokes. The 'Mesh' option is also visible. Below this, the 'IPsec intelligent traffic steering' toggle is turned off, with a note stating it cannot be changed during configuration. The 'Route injection' toggle is turned on, with a note advising its use in multi-uplink scenarios. The 'Hub' section at the bottom includes fields for 'Hub node' (set to 'Cloud managed de...'), 'Device' (set to 'FW'), 'Outbound Interface' (set to 'Default outbound int...'), and 'Subnet' (set to '192.168.237.1/24').

Kuva 4. Pilvihallinnan Inter-site VPN -määrittäminen yleisten asetusten ja hub-laitteen osalta.

Ensimmäisessä Inter-site VPN -testissä topologimalliksi valittiin kuvan 4 mukaisesti Hub-spoke, hub-noden tyypiksi valittiin cloud managed device, ja palomuuuri valittiin hub-nodeksi palvelimen laitelistalta. Lisäasetukset IPsec intelligent traffic steering ja Route injection pystyi kytkemään joko päälle tai pois. IPsec intelligent traffic steering-asetuksen

avulla pilvihallinta pystyy yhteyden laadusta riippuen dynaamisesti päättämään mitä fyysistä linkkiä pitkin liikenne kulkee spoke-laitteista hub-laitteeseen. Tämä asetus oli oletuksena pois päältä, ja koska kaikissa testiverkon laitteissa on samanaikaisesti käytössä vain yksi yhteys ulkoverkkoon, ei tähän asetukseen tehty muutoksia. Route injection -asetuksen avulla hub-laite saa luotua automaattisesti staattiset reitit spoke-laitteiden lähiverkkoihin IPSec-tunneleissa kulkevan liikenteen päämääräosoitteiden avulla. Tämä asetus oli oletuksena päällä ja siihen ei myöskään tehty muutoksia. Palomuurin lähiverkon osoite syötettiin subnet-kohtaan ja hub-laitteen osalta konfiguraatio oli valmis.

Spoke-laitteet lisättiin valitsemalla ne palvelimeen yhdistetyistä laitteista, jonka jälkeen ne tulivat näkyviin Spoke-laitteiden listalle kuvan 5 mukaisesti. Jokaiselle laitteelle valittiin oikea lähiverkon osoite ja kytkettiin Spoke mutual access -asetus päälle, joka mahdollisti laitteiden lähiverkkojen välisen kommunikoinnin hub-laitteen kautta. Spoke-laitteiden yhteyksien nopeutta pystyi tarvittaessa myös rajoittamaan tiettyyn maksiminopeuteen rate limit -asetuksella, mutta tässä testiverkossa sitä ei koettu merkitykselliseksi.

Spoke

* Device selection:

<input type="checkbox"/>	Device Name	ESN	Site Name	Outbound Interface	Local Subnet	Rate Limit (KB/s)	Spoke Mutual Access	Operation
<input type="checkbox"/>	BR-2	21500104812SL3604275	BR-2	GigabitEthernet0/0/4	192.168.238.1/24	0	Disable	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	HQ	21500104832SL8500110	HQ	GigabitEthernet0/0/9	192.168.239.1/24	0	Disable	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	BR-1	21500104792SL4600691	BR-1	GigabitEthernet0/0/4 Cellular0/0/0	192.168.240.1/24	0	Disable	<input type="button" value="edit"/> <input type="button" value="delete"/>

Total records: 3

Connect to third-party devices:

<input type="checkbox"/>	Device Name	IP	Local Subnet	Spoke Mutual Access	Operation
No records found.					

Security

* IPsec policy template:

* Key:

Authentication type: ☒ IP ☐ ESN ☐ FQDN

Kuva 5. Pilvihallinnan Inter-site VPN -määrittäminen spoke-laitteiden ja IPSec-asetusten osalta.

IPsec-tunnelien luonnin viimeisenä vaiheena määritettiin varsinaiset IPSec-asetukset. Asetuksissa oli valittavana useita parametrejä, kuten IKE:n versio, IKE:n käyttämät salaus- ja todennusalgoritmit sekä IPSec:in käyttämät salaus- ja todennusalgoritmit. Oletuksena käytössä oleva salausalgoritmi AES-256 ja todennusalgoritmi SHA-2-256 olivat turvallisuudeltaan riittävät. Asetusikkunasta pystyi halutessaan valitsemaan myös turvatomiksi todettuja algoritmeja, kuten MD5 tai SHA-1, joita käyttäliittymä kuitenkin selkeästi

varoitti olemaan käyttämättä. Oletusparametrit olivat kaikin puolin käyttöön sopivat, eikä niihin tehty muutoksia.

Yhteyksien todennukseen määritettiin salasana ja todennus valittiin suoritettavaksi IP-osoitteen perusteella. Tässä tapauksessa spoke-laitteet tunnistavat hub-laitteen sen julkisen staattisen IP-osoitteen perusteella, ja muodostavat tunneloidun yhteyden sen kanssa. Todennuksen voi vaihtoehtoisesti valita suoritettavaksi myös laitteiden sarjanumeron tai täysin määritellyn verkkotunnuksen avulla. Inter-site VPN -määrittely oli nyt valmis ja pilvihallinta loi määrittelyt laitteisiin automaattisesti.

Komentorivin kautta katsottuna jokainen reititin muodosti tunneloidun yhteyden palomuriin ja yhteyksien toimivuus testattiin suorittamalla ping-komento jokaisen laitteen VLAN 1 -liitännän IP-osoitteesta toisen laitteen lähiverkossa olevan CreaNODE-laitteen osoitteeseen. Yhteydet toimivat kuten pitikin ja traceroute-komennon avulla varmistettiin, että reitittimien väliset yhteydet kulkivat palomuurin kautta. Pilvihallinta oli automaattisesti luonut jokaiseen laitteeseen numeroidun pääsynvalvontalistan 3999, joka määritteli IPSec-tunnelissa sallitun liikenteen. Reitittimissä oli kolme erillistä sääntöä, joista jokainen sallii laitteen omasta lähiverkosta peräisin olevan liikenteen kulun tiettyyn toisen laitteen lähiverkkoon. Palomuurissa oli sama pääsynvalvontalista 3999, mutta hieman eri säännöillä. Kuvan 6 mukaisesti sen ensimmäinen sääntö määritteli palomuurin omasta lähiverkosta lähtöisin olevan liikenteen pääsyn mihin tahansa osoitteeseen. Muut kuusi sääntöä määrittivät jokaisen toisen reitittimen lähiverkon liikenteen pääsyn kahden muun reitittimen lähiverkkoon.

```
#
acl number 3999
rule 1 permit ip source 192.168.237.0 0.0.0.255
rule 2 permit ip source 192.168.238.0 0.0.0.255 destination 192.168.239.0 0.0.0.255
rule 3 permit ip source 192.168.238.0 0.0.0.255 destination 192.168.240.0 0.0.0.255
rule 4 permit ip source 192.168.239.0 0.0.0.255 destination 192.168.238.0 0.0.0.255
rule 5 permit ip source 192.168.239.0 0.0.0.255 destination 192.168.240.0 0.0.0.255
rule 6 permit ip source 192.168.240.0 0.0.0.255 destination 192.168.238.0 0.0.0.255
rule 7 permit ip source 192.168.240.0 0.0.0.255 destination 192.168.239.0 0.0.0.255
#
```

Kuva 6. Pilvihallinnan kautta palomuurille automaattisesti määritetty pääsynvalvontalista 3999.

Tässä kohtaa kaikki vaikutti toimivan kuten pitääkin, mutta tunneloidun yhteyden toiminnallisuudessa ilmeni ongelma, kun palomuurille määriteltiin osoitteenmuunnos lähiverkon laitteiden internetyhteyttä varten. Palomuri määritettiin muuntamaan kaikkien lait-

teiden lähiverkkojen osoitteet palomuurin Internetiin yhteydessä olevan liitännän osoitteeksi käyttäen PAT-osoitteenmuunnosmenetelmää. Siten kaikkien reitittimien lähiverkkojen pitäisi saada yhteys Internetiin lähettämällä liikenne ensin IPSec-tunnelilla palomuurille, joka ohjaa sen eteenpäin. Lähiverkkojen välinen liikenne kulki halutusti reitittimeltä reitittimelle palomuurin kautta, mutta Internetiin tai muihin ulko-verkon osoitteisiin tarkoitettu liikenne ei kulkenut ollenkaan. Kun jollekin reitittimistä määriteltiin testiksi oma osoitteenmuunnos, ulko-verkon liikenne kulki normaalisti, mutta laitteen oman Internetiin yhteydessä olevan liitännän kautta. Ulko-verkkoon kulkeva liikenne ei siis koskaan päässyt IPSec-tunneliin.

Ongelman syyksi ilmeni nopeasti aiemmin mainitut pilvihallinnan automaattisesti luomat pääsynvalvontalistan säännöt, jotka sallivat vain liikenteen, jonka päämäärä on toisen laitteen lähiverkko. Sääntöjä muutettiin laitteiden komentorivien kautta siten, että jokainen reititin sallii kaiken omasta lähiverkostaan peräisin olevan liikenteen mihin tahansa päämäärään, ja palomuri sallii kaiken liikenteen, jonka päämääränä on jokin reitittimien lähiverkoista. Näin sekä reitittimillä että palomuurilla oli vain yksi sääntö ja Internet-liikenne saatiin kulkemaan IPSec-tunneleissa palomuurin kautta. Kuvan 7 mukaisesti suorittaessa traceroute-komennon reitittimen lähiverkosta Cloudflaren DNS-palvelimen osoitteeseen 1.1.1.1, reitti kulki ensin palomuurin julkisen osoitteen ja edelleen palomuurin oletusyhdykäytävän kautta eteenpäin päämääräänsä asti.

```
<HQ>tracert -a 192.168.239.1 1.1.1.1
tracert to 1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C to break
 1 Palomuri 1 ms 10 ms 1 ms
 2 Oletusyhdykäytävä 1 ms 1 ms 1 ms
 3 87.236.154.168 10 ms 1 ms 1 ms
 4 87.236.154.212 10 ms 1 ms 1 ms
 5 193.110.224.29 10 ms 1 ms 10 ms
 6 1.1.1.1 10 ms 1 ms 10 ms
<HQ>
```

Kuva 7. Liikenteen kulku HQ-reitittimeltä Internetiin palomuurin kautta.

Tässä kohtaa testiä huomattiin kuitenkin, että lähiverkkojen välinen liikenne ei enää toiminut. Traceroute-komennolla kahden reitittimen lähiverkon välistä yhteyttä testatessa ilmeni, että palomuri yrittää ohjata liikenteen perille toiselle reitittimelle käyttäen sen julkista IP-osoitetta. Koska pääsynvalvontalistoissa oli määriteltä ainoastaan lähiverkkojen osoitteet, tämä liikenne ei mennyt tunnelien kautta, eikä siten päässyt perille, koska reitittimillä ei ollut määriteltynä osoitteenmuunnoksia.

Komentorivin NAT-asetuksista selvisi, että osoitteenmuunnoksen voi tarvittaessa estää liikenteelle, jolla on tietty päämäärä. Tämä vaikutti ratkaisulta senhetkiseen ongelmaan,

mutta kyseistä asetusta ei ollut saatavilla pilvihallintapalvelimen käyttöliittymässä, eikä sitä saanut suoritettua palomuurin komentorivin kautta, koska pilvihallitussa tilassa laitemäärittäsmahdollisuudet olivat rajoitettuja. Tässä vaiheessa palomuuuri päädyttiin poistamaan pilvihallitusta tilasta, ja asetukset määriteltäisiin jatkossa manuaalisesti. Senhetkistä pilvihallinnan kautta laitteelle määritellyistä asetuksista otettiin varmuuskopio ja palomuuuri palautettiin tehdasasetuksille, jonka jälkeen komentorivin kautta saatiin muokattua kaikkea toiminnallisuutta. Pilvihallintapalvelimelle tehtiin uudelleen sama Inter-site VPN -konfiguraatio määrittäen nyt ei-pilvihallittu palomuuuri sen julkisen IP-osoitteen avulla hub-laitteeksi. Kun kaikki aiemmat asetukset oli palautettu, testattiin aiemmin mainittua muokkausta osoitteenmuunnokseen ping- ja traceroute -komennoilla. Nyt kun osoitteenmuunnos oli estetty palomuurilta lähiverkkoihin päätyvälle liikenteelle käyttäen kuvassa 8 näkyvää destination-address-exclude range -komentoa, liikenne ohjautui oikein ja kaikki toimi kuten pitikin.

```
nat-policy
rule name LAN-to-internet
destination-zone untrust
source-address range 192.168.237.1 192.168.240.254
destination-address-exclude range 192.168.237.1 192.168.240.254
action source-nat easy-ip
#
```

Kuva 8. Palomuurin NAT-määrittäykseen tehty muutos, joka estää osoitteenmuunnoksen liikenteeltä, jonka määränpää on jokin laitteiden lähiverkoista.

Viimeisenä ongelmana kuitenkin oli se, että koska pilvihallintapalvelimen laitteisiin automaattisesti luomiin pääsynvalvontalistoihin oli tehty komentorivin kautta muutoksia, määrittäykset eivät säilyneet laitteiden uudelleenkäynnistyksen jälkeen. Ei-pilvihallitun palomuurin kanssa tämä ei ollut ongelma, mutta asiakasyrityksen tiloihin tulevissa reitittimissä tunnelien määrittäyksen pitää onnistua täysin etänä pilvihallinnan kautta. Ongelma oli yritykselle kriittinen SD-WAN-ratkaisun käyttökelpoisuuden kannalta, joten asiasta oltiin laitevalmistajaan yhteydessä. Aikaisemmin mainitussa pilvihallinnan seuraavassa ohjelmistopäivityksessä oli tulossa toiminnallisuus, joka mahdollistaisi tunnelien halutunlaisen määrittäyksen reitittimille kokonaan ilman komentorivikomentoja. Päivityksen aikataulusta ei ollut kuitenkaan varmuutta, joten laitevalmistaja kehitti pienen korjauspäivityksen pilvihallintapalvelimeen, jonka avulla reitittimiin saatiin tehtyä oikeat määrittäykset pilvihallinnan kautta.

Nyt inter-site VPN -määrittelyssä hub-laitteen aliverkon kohdalle sai määriteltyä verkon 0.0.0.0/0, joka käytännössä tarkoittaa, että hub-laite toimii spoke-laitteiden oletusreitien kohteena. Spoke-laitteet saivat nyt automaattisesti samat pääsynvalvontalistojen säännöt, mitkä oli testissä aiemmin muokattu komentorivin kautta. Yhdessä manuaalisesti määritellyn palomuurin kanssa kaikki toimi nyt niin kuin pitikin ja laitteet säilyttivät oikeat asetukset myös uudelleenkäynnistyksen jälkeen.

4.4 IPSec-tunneleiden läpisyöttöteho

Laitteiden IPSec-tunnelien läpisyöttötehot määrittelevät mitä yhteysnopeuksia asiakasyrityksille voidaan tarjota tai kuinka nopeita yhteyksiä yrityksen runkoverkon ulkopuolella oleva asiakasyritys voi hankkia toiselta operaattorilta. Jokaiselle laitteelle on valmistajan lupaamat IPSec-tunnelien liikenteen maksimiläpisyöttötehot. palomuurille ja HQ-reitittimelle luvattu läpisyöttöteho on suurin, 2 Gb/s, ja edullisempien BR-1- ja BR-2-reitittimien ilmoitetaan pystyvän maksimissaan 200 Mb:n/s läpisyöttötehoon.

Läpisyöttötehomittauksissa käytettiin aiemmassa testissä reitittimien ja palomuurin välille määritettyjä IPSec-tunneleita. Koko reitin kaistanleveys CreaNODE-mittalaitteelta toiselle reitittimien ja palomuurin kautta on laitteiden Ethernet-liitännöistä johtuen 1Gb/s. Koska on kyse TCP-protokollasta, joka luo kaksisuuntaisia yhteyksiä osoitteiden välille sekä varmistaa pakettien pääsyn perille, osa käytettävissä olevasta kaistanleveydestä menee yhteyden ylläpitoon tarvittaviin toimintoihin. (Cook 2017) Tämä tarkoittaa, että 1Gb/s läpisyöttötehoon käytännön testeissä ei tulla pääsemään, mutta sitä huomattavasti alempi tulos tarkoittaa, että IPSec-tunnelit rajoittavat yhteyttä. HQ-reitittimen pitäisi pystyä käytännössä lähes 1Gb/s läpisyöttötehoon ja molempien edullisempien reitittimien lähes 200Mb:n/s läpisyöttötehoihin.

Mittaukset suoritettiin CreaNODE-mittalaitteiden WWW-hallinnan EchoVaultin kautta käyttäen TrueTPC-mittausominaisuutta. TrueTCP-mittaus perustuu RFC 6349 -menetelmään, joka on suunniteltu kahden IP-verkon laitteen välisen TCP-liikenteen läpisyöttötehon luotettavaan mittaamiseen ja todentamiseen (CreaNord 2020). Testejä varten jokaiseen CreaNODE-laitteeseen kytkettiin hallinnan kautta TrueTCP-ominaisuus ensin päälle. Sitten luotiin uusi TrueTCP RFC 6349 -mittaus, jossa valittiin lähettävä ja vastaanottava laite, sekä kummastakin lähettävät ja vastaanottavat liitännät.

Add a New TrueTCP RFC 6349

Test Name: fw-ipsec-100-2
Test Description:
Executed: 1.4.2021 11:27:57
Scheduled: Immediately

Nodes

Sender: CN500 Port: eth1
Receiver: P1-CN500 Port: eth1

Test to Run

☒ MTU Discovery ☒ Bottleneck Bandwidth (BB)
TCP Test Duration: 1 Minutes
CIR Distribution: Automatic (symmetric)

TCP Configuration

Server TCP Port: 80 Max. Number of Retransmission: 15
TCP Timeout (seconds): 180 Maximum Number of Retransmitted SYN: 6
TCP Timewait (seconds): 0 Max. Backoff: 4
☐ Fast connection ramp-up TCP Initial Retransmission Timeout (milliseconds): 500
Minimum total ramp-up time (seconds): 30

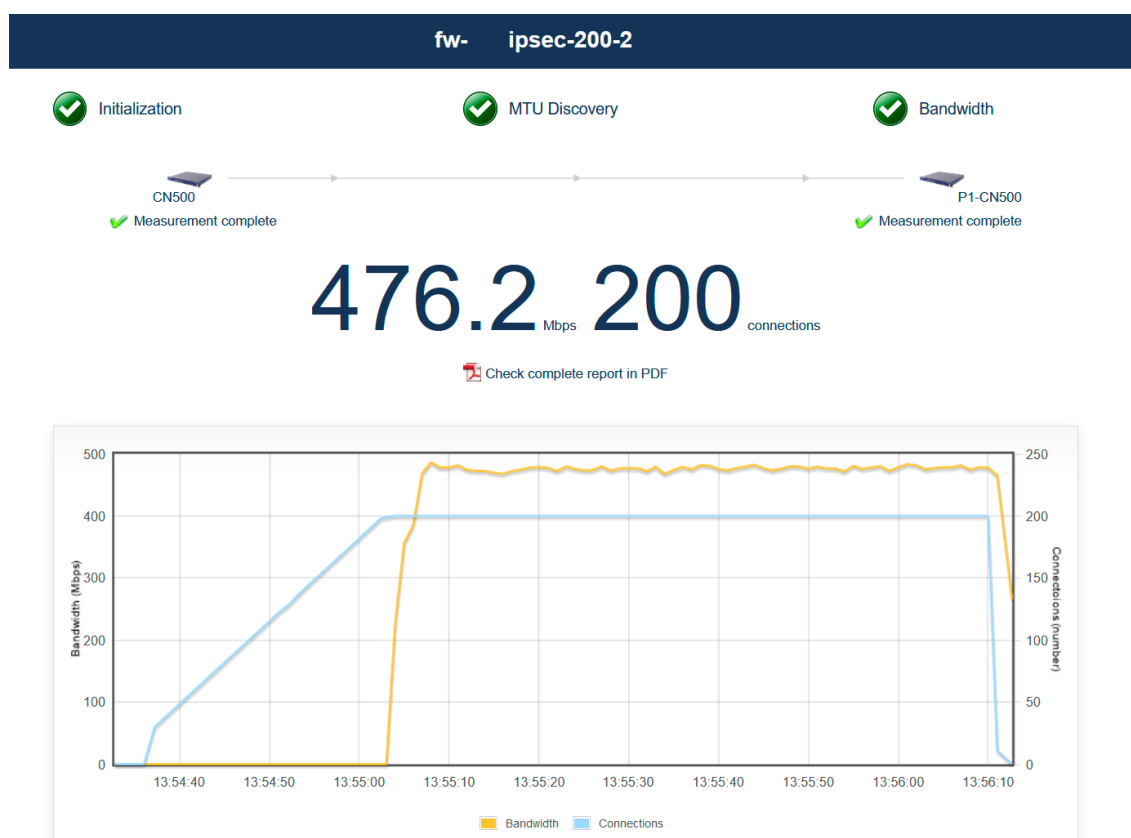
Services

Number of TCP Connections: 100

Kuva 9. Esimerkki TrueTCP-testin asetussivustosta palomuurin ja HQ-reitittimen välisessä mittauksessa.

Kuvan 9 mukaisesta asetussivustosta valittiin läpisyöttötehon lisäksi ajettaviksi testeiksi MTU Discovery, joka testaa kahden pisteen välillä olevan reitin suurimman mahdollisen pakettikoon sekä Bottleneck Bandwidth (BB), joka mittaa reitin suurimman mahdollisen kaistanleveyden (CreaNord 2020). Mittauksen merkittävintä muuttujaa, eli TCP-yhteyksien määrää muutettiin testien välillä, jotta selviäisi miten yhteys käyttäytyy eritasoisen rasiuksen alaisena. TCP-yhteyksien määrää sai vaihdeltua yhden ja 10 miljoonan välillä. Mittauksen ajaksi valittiin oletuksena oleva 1 minuutti. Seuraavassa ikkunassa testattavalle palvelulle annettiin nimi ”LAN-to-LAN” ja sekä lähettävälle että vastaanottavalle päälle määriteltiin oikea virtuaalilähiverkon tunnus 105. Molemmille laitteille määritettiin

myös mittausliitännöiden osoitteet ja yhdyskäytävän osoitteet, jotka tässä tapauksessa ovat reitittimen tai palomuurin VLAN 1 -liitännät. Mittausliitännöiden MAC-osoitteet hallinta löysi ja lisäsi automaattisesti. Mittausasetusten määrittämisen jälkeen mittauksen sai suoritettua sivun alareunassa olevalla painikkeella. Mittauksen valmistuttua tulokset tulivat näkyviin ja niitä pystyi tarkastelemaan joko kuvan 10 mukaisesti selaimella tai tarkemmin lataamalla erillisen raporttiedoston.



Kuva 10. Esimerkki Palomuurin ja BR-2-reitittimen 200 yhteyden TrueTCP-mittauksen tuloksista.

Tyypillisestä yhteyksien määrästä yhtä laitetta tai yhtä yrityksen toimipistettä kohden löytyi hyvin vähän tarkkaa tietoa, joten tutkimme toimeksiantajayrityksen yhden oman palomuurin lokeja normaalissa käyttötilanteessa ja päädyimme sen perusteella keskimääräiseen arvoon 10 yhteyttä yhtä laitetta kohden. Tämä keskiarvo ei ole kovin tarkka, sillä yhteyksien määrä vaihtelee eri laitetyyppien ja sovellusten välillä, mutta se määrittää tarpeeksi tarkan laitekohtaisen arvion tämän testauksen tarkoituksiin.

Jokaisesta reitittimestä palomuriin kulkevan IPSec-tunnelin läpi kulkevaa liikennettä testattiin kolmella eri TCP-yhteyksien määrällä. Jokaiselle TCP-yhteyksien määrälle samoja testejä tehtiin kaksi tai tarvittaessa enemmän, jotta mahdolliset hetkittäiset vaihtelut verkossa eivät vaikuttaisi tuloksiin. Samat testit toistettiin jokaiselle reitittimelle lähettämällä liikennettä palomuurin päästä. Käytännössä testit, joissa reitittimen verkkomittauslaitteelta lähetettiin liikennettä, simuloivat yhteyttä asiakasyrityksen toimipisteestä ulko verkkoon tai muihin toimipisteisiin. Testit, joissa palomuurin verkkomittauslaitteelta lähetettiin liikennettä, simuloivat yhteyttä ulkoverkosta asiakasyrityksen toimipisteeseen. Kalliimmalle HQ-reitittimelle suoritetuissa testeissä käytetyt yhteysmäärät olivat 100, 500 ja 1000, jotka simuloivat noin kymmentä, viittäkymmentä ja sataa laitetta. Edullisempien BR-1- ja BR-2-reitittimien testien yhteysmäärät olivat 50, 200 ja 500, jotka puolestaan simuloivat noin viittä, kahtakymmentä ja viittäkymmentä laitetta.

Taulukko 1. Mittaustulokset mittausliikenteen kulkiessa palomuurin mittalaitteelta reitittimien mittalaitteille.

TCP-yhteyksien määrä	IPSec-tunnelin keskimääräinen maksimiläpisyöteho, hub to spoke (Mb/s)		
	HQ	BR-1	BR-2
50	-	443,7	401,2
100	890,9	-	-
200	-	485,1	483,9
500	895,3	484,5	484,9
1000	895,5	-	-

Taulukko 2. Mittaustulokset mittausliikenteen kulkiessa reitittimien mittalaitteilta palomuurin mittalaitteelle.

TCP-yhteyksien määrä	IPSec-tunnelin keskimääräinen maksimiläpisyöttöteho, spoke to hub (Mb/s)		
	HQ	BR-1	BR-2
50	-	392,9	354,6
100	779,8	-	-
200	-	403,7	376,0
500	710,9	297,7	339,5
1000	835,9	-	-

Taulukon 1 mukaisesti lähettäessä liikennettä palomuurilta HQ:lle, testit antoivat hyviä tuloksia ja jokaisella yhteysmäärällä keskimääräiseksi IPSec-tunnelien maksimiläpisyöttötehoksi saatiin lähes 900Mb/s, joka vastaa TCP-liikenteeltä odotettua arvoa. Toisin päin testatessa arvot olivat matalampia ja vaihtelivat suuresti eri yhteysmäärien välillä, kuten taulukosta 2 selviää. Reitittimen suunnasta lähetetyn liikenteen läpisyöttöteho tunnelin läpi oli selvästi matalin keskimmaisella viidensadan yhteyden määrällä ja selvästi suurin suurimmalla tuhannen yhteyden määrällä.

Edullisempien reitittimien tulokset yllättivät, sillä taulukon 1 tulosten mukaan niiden IPSec-tunnelien maksimiläpisyöttöteho oli keskimäärin yli kaksi kertaa laitevalmistajan lupaamaa arvoa korkeampi lähettäessä liikennettä palomuurilta. Toisinpäin testatessa ne saavuttivat taulukon 2 mukaan myös tasaisesti yli 300-400Mb:n/s tuloksia, BR-2 jääden hieman jälkeen tuloksissa. HQ-reitittimen testien tavoin keskimääräiset tulokset vaihtelivat eri yhteysmäärien välillä. Reitittimeltä palomuurille menevälle liikenteelle suurin yhteysmäärä aiheutti odotetusti eniten hidastusta, mutta toisinpäin testatessa pienimmät arvot antoivat pienimmällä yhteysmäärällä tehdyt testit.

Testien toistaminen ei tuonut merkittävää muutosta mitattuihin arvoihin, eikä syytä ajoittain odottamattomille tulosten vaihteluille eri yhteysmäärien välillä selvinnyt laitevalmistajan dokumentaatiosta. Todennäköisemmäksi aiheuttajaksi tälle kuitenkin arveltiin joko itse verkkomittauslaitteita tai niiden ohjelmistoa. HQ:n yhteydellä mitatut arvot alimmillaankin sisältyvät 1000Mb:n/s liittymän normaaliin vaihteluväliin ja edullisemmilla reitittimillä mitatut arvot puolestaan olivat alimmillaankin laitevalmistajan lupaamia maksimilä-

pisyöttötehoja parempia, joten laitteiden voitiin todeta pystyvän ainakin luvattuihin läpisyöttötehoihin. Käytännön arvot selviäisivät luultavasti paremmin myöhemmässä vaiheessa, jossa yhteyttä käytettäisiin ja mitattaisiin usealla tietokoneella samanaikaisesti. Opinnäytetyötä tehdessä tähän ei vielä ollut mahdollisuutta.

Taulukko 3. Maksimikaistanleveyden mittaustulokset.

Liikenteen suunta	IPSec-tunnelin keskimääräinen maksimikaistanleveys (Mb/s)		
	HQ	BR-1	BR-2
Spoke-to-hub	961,1	274,5	277,1
Hub-to-spoke	959,4	249,9	240,4

TrueTCP-testissä suoritettiin läpisyöttötehon mittauksen lisäksi myös aiemmin mainitut MTU Discovery ja Bottleneck Bandwidth (BB) -testit. MTU Discovery antoi jokaisessa testissä tulokseksi 1438, joka tarkoittaa, että MTU on oletusarvoa 1500 pienempi tunneloitua yhteyttä käyttäessä. Laitteiden väliseen yhteyteen tällä ei näyttänyt olevan testeissä vaikutusta. BB-testin tarkoituksena oli mitata kahden verkkomittauslaitteen välisen reitin suurin mahdollinen kaistanleveys. HQ-reitittimen ja palomuurin välisissä testeissä BB:n arvoksi tuli taulukon 3 mukaisesti liikenteen suunnasta tai yhteyksien määrästä riippumatta aina noin 960Mb/s, joka vastasi hyvin odotettua arvoa.

Edullisempien reitittimien testeissä ilmeni kuitenkin ristiriitaisia tuloksia BB:n arvon ja mitatun läpisyöttötehon kesken, sillä molempien laitteiden kaikissa testeissä BB:n arvoksi saatiin taulukon 3 mukaisesti noin 240–280Mb/s, vaikka mitattu maksimiläpisyöttöteho oli joka kerta suurempi. Tässä kohtaa testausta heräsi epäily mittaustulosten paikkansapitävyydestä, sillä molemmat mittausravot olivat myös ristiriidassa laitevalmistajan ilmoittamien maksimiläpisyöttötehojen kanssa. Seuraavaksi oli selvítettävä, että kumpaan mitatuista arvoista voi luottaa vai voiko niistä luottaa kumpaankaan.

RFC 6349 -menetelmästä ei löytynyt kovin yksityiskohtaista dokumentaatiota mittalaitteiden valmistajalta CreaNordilta, joten asiasta kysyttiin heiltä suoraan sähköpostitse. CreaNordin mukaan BB-testi suoritetaan lähettämällä UDP-liikennettä laitteiden välillä nopeina purskeina ja ilmoittamalla BB:n arvo perille päässeeseen liikenteen mukaan. Koska UDP-liikenne ei varmista datan perille pääsyä, se käyttää kaistanleveyttä TCP-liikennettä tehokkaammin ja soveltuu paremmin juuri tähän testiin (Cook 2017).

Mittalaittevalmistaja suositteli kokeilemaan UDP-liikenteen lähetysnopeuden rajoittamista testin asetuksista edullisemman sarjan reitittimien mittauksissa, koska oletuksena oleva 1000Mb:n/s lähetysnopeus saattoi huonontaa joko mittalaitteiden tai niiden välisen verkon suorituskykyä. Suoritimme uudet testit BR-1-reitittimen ja palomuurin väliselle yhteydelle reitittimien päästä 50 yhteydellä asettaen BB-testin lähetysnopeudeksi 500Mb/s, jolloin BB:n arvoksi saatiin hieman aiempaa korkeampi 316Mb/s. Saman mittauksen maksimiläpisyöttöteho oli kuitenkin huomattavasti korkeampi 395Mb/s ja suunnilleen sama arvo oli tullut myös alkuperäisessä mittauksessa 1000Mb:n/s lähetysnopeudella. Sama testi toistettiin useampaan kertaan laskien aina lähetysnopeutta, kunnes vasta arvolla 300Mb/s BB:n arvo saatiin vastaamaan sitä. Tässä kohtaa mitattu arvo oli kuitenkin merkityksetön, koska lähetysnopeus oli asetettu alle tulokseksi saadun maksimiläpisyöttötehon. Bottleneck Bandwidth -mittaus todettiin siten epäluotettavaksi edullisemmilla reitittimillä, eikä sen tuloksiin perehdytty enää tarkemmin. Läpisyöttötehon mittauksissa saadut arvot todettiin kuitenkin lopullisesti luotettaviksi, sillä myös CreaNordilta todettiin, etteivät he löydä syytä epäillä virhettä testauksessa.

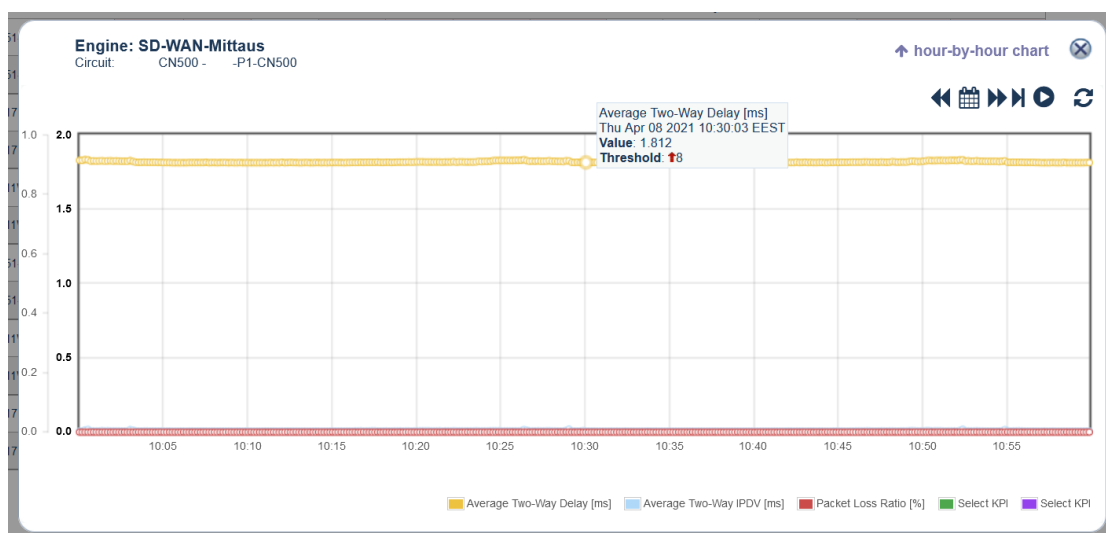
Testeissä selvisi, että jokainen laite pystyy käytännössä luvattuun IPSec-tunneloidun yhteyden läpisyöttötehoon, ja edullisemmilla reitittimillä se on huomattavasti luvattua korkeampi. Testeissä laitteiden välinen liikenne kulki kokonaan yrityksen runkoverkossa, jonka kaistanleveys testiverkon laitteiden liitäntöjä lukuun ottamatta oli aina vähintään 10Gb/s. Asiakasympäristöissä on huomattava, että läpisyöttötehot saattavat vaihdella paljonkin riippuen lähettävän ja vastaanottavan laitteen yhteystyypeistä ja niiden välisestä verkkoinfrastruktuurista. Pääasia kuitenkin oli, että saatiin käsitys millaisten liittymänopeuksien kanssa laitteet ovat yhteensopivia. HQ tukee testien perusteella suurimpia 1000Mb:n/s liittymänopeuksia ja edullisemmat reitittimet tukevat ainakin 200Mb:n/s sekä ehkä jopa 400Mb:n/s nopeuksia.

4.5 Tunneloidun yhteyden viive

Viive on läpisyöttötehon lisäksi toinen tärkeä asia IPSec-tunneleiden avulla luodussa yhteydessä. On tärkeää, että tunneloitu yhteys käyttäytyy asiakasyrityksen näkökulmasta samalla tavalla kuin mikä tahansa muukin yhteys, eikä viive kasva liian suureksi. Viiveen mittausta varten Echovaultiin luotiin uusi SLA-mittaus, joka mittaa jatkuvasti 10 sekunnin välein tietoa eri CreaNODE-laitteiden välisestä yhteydestä. Jokaisesta verkkomittauslaitteesta määritettiin mittaus kolmeen toiseen laitteeseen, joista selviäisi laitteiden välisen

yhteyden keskimääräinen viive eri ajankohtina. Kaikkien laitteiden välillä oli jo valmiiksi luotuna omat tunneloimattomat mittaukset verkonvalvontaa varten. Niitä voitaisiin siten käyttää vertauskohtana IPSec-tunneloidun yhteyden mittauksille.

Palomuurin ja BR-1-reitittimen verkkomittauslaitteen maantieteellinen etäisyys oli testiverkon suurin, noin 100km. Kuvan 11 mittauksen perusteella IPSec-tunneloidun yhteyden keskimääräinen kahdensuuntainen viive oli noin 1,8 ms. Ei-tunneloidun yhteyden viive samalla välillä oli puolestaan keskimäärin noin 1,4 ms. Kummankaan yhteyden viiveessä ei ollut havaittavaa vaihtelua koko mittausaikana. IPSec-tunneloitu yhteys vaikutti siis tässä testissä lisänneen yhteyden viivettä 0,4 ms, joka on niin pieni ero, ettei sitä yrityskäytössä käytännössä huomaisi.



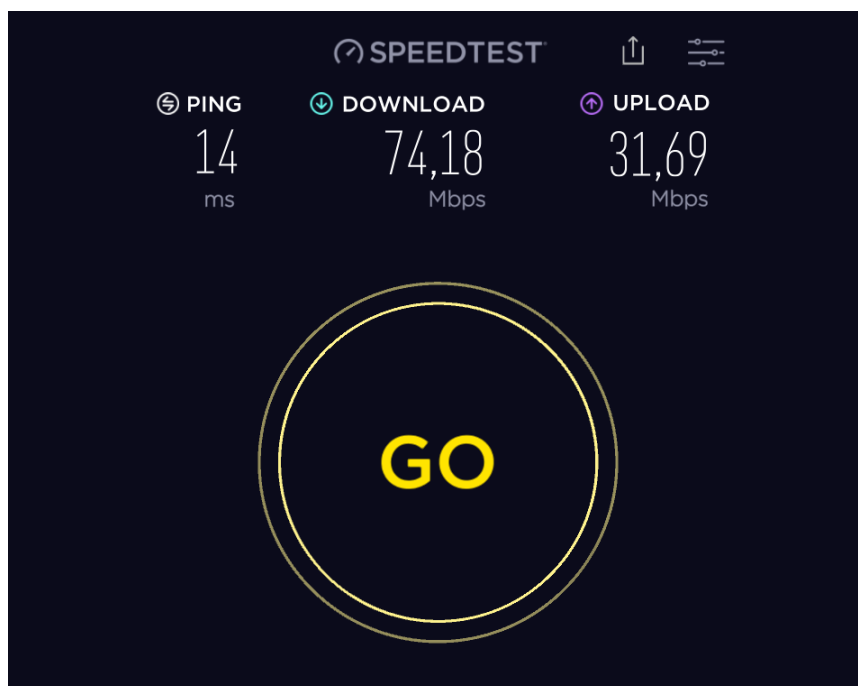
Kuva 11. Palomuurin ja BR-1-reitittimen välisen tunneloidun yhteyden keskimääräinen kahdensuuntainen viive CreaNODE-mittalaitteilla mitattuna.

Mittauksessa oli kuitenkin monta tekijää, jotka tekivät siitä jälkeenpäin ajateltuna epäluotettavan. Ensinnäkin verkkomittauslaitteiden ja testiverkon laitteiden väliset Epipe VLL -yhteydet kulkivat runkoverkon kautta molemmissa testeissä, joten erot pystyivät muodostumaan ainoastaan testiverkon laitteiden väliseen IP-verkon yhteyteen. Testiverkon Internetin kautta kulkeva liikenne kulki myös ainoastaan yhden runkoverkon reitittimen kautta laitteesta toiseen. Tämä ei vastaa hyvin tilannetta jossa IPSec-tunneloitua yhteyttä tulisi käyttää, sillä käytännössä kahden laitteen välisen yhteys kulkee aina useamman, ellei useamman kymmenen reitittävän laitteen kautta, varsinkin jos kommunikoivat laitteet käyttävät eri operaattorien yhteyksiä.

Jotta IPSec-tunneleiden vaikutusta yhteyden viiveeseen saisi testattua paremmin ja käytännönläheisemmin, BR-1 yhdistettiin Internetiin toisen operaattorin 100/50 Mb:n/s VDSL-kuluttajaliittymän kautta noin 50km päässä testiverkon sijainnista. Yrityksen palomuurilta sallittiin yhteys pilvihallintapalvelimeen tämän liittymän julkisesta IP-osoitteesta. Yhteys laitteelle tuotiin VDSL-mediamuuntimelta Ethernet-kaapelilla. Kun laitteen yhdisti virtoihin ja Internetiin, se loi automaattisesti IPSec-tunnelin sen ja palomuurin välille, sillä tunnelin toisen pään, eli palomuurin IP-osoite oli määritetty sille aiemmin.

Viiveen testaamiseksi ja vertailemiseksi VDSL-yhteyttä testattiin ensin yhdistämällä tietokone Ethernet-kaapelilla kuluttajareitittimeen ja lataamalla koneelle Speedtest-sovel-lus. Sen jälkeen suoritettiin nopeustesti, joka antoi vertailuarvot yhteyden viiveelle sekä nopeudelle. Tämän jälkeen BR-1 kytkettiin samaan liittymään ja sama tietokone kytket-tiin siihen Ethernet-kaapelilla. Nyt nettiyhteys toimi testiverkon palomuurin kautta, ja tie-tokoneen julkisena IP-osoitteena näkyi palomuurin IP-osoite. Traceroute-komennolla rei-tittimen julkisen osoitteen ja palomuurin julkisen osoitteen välillä näkyi kahdeksan run-koverkon reititintä, joiden kautta liikenne kulki oikeaan osoitteeseen. Nyt kun nopeustes-tin suoritti tietokoneelta, kaikki muu vaikutti toimivan normaalisti, mutta upload-nopeus jäi erittäin alhaiseksi eikä noussut suuremmaksi kuin 1 Mb/s.

Vianselvityksen jälkeen kävi ilmi, että aiemmin tunneloidun yhteyden mittauksissa ilmen-nyt normaalia pienempi MTU:n arvo 1438 oli ongelman taustalla. Ping-komennon suorit-taessa ilman fragmentaatiota reitittimen lähiverkosta palomuurin lähiverkkoon, suurin läpi menevä datatavujen määrä oli 1410. Tämä vastaa mitattua MTU:n arvoa, josta on vähennetty 20 tavun IP- ja 8 tavun ICMP-kentät (Citrix 2018). Laitevalmistajan avulla vika ratkaistiin muuttamalla palomuurin päästä TCP MSS -asetusta pienemmäksi, koska IPSec-tunneloinnin lisäämät kentät vähentävät pakettiin mahtuvien datatavujen määrää. Oikean MSS:n arvon sai määritettyä vähentämällä MTU:n arvosta IP- ja TCP-kentät, jotka molemmat olivat kooltaan 20 tavua (Cloudflare 2021). Siten MSS:n arvoksi saatiin 1398, ja kun se syötettiin palomuurille, myös upload-nopeus testissä alkoi antaa odotet-tuja tuloksia.



Kuva 12. BR-2-reitittimen lähiverkossa olevalla tietokoneella tehty nopeustesti IPSec-tunneloidulla yhteydellä VDSL-liittymää käyttäen.

Nyt yhteys toimi tietokoneella kuten pitikin, ja myös upload-nopeuden sai mitattua. Viive oli kuvan 12 nopeustestissä 14 ms, yhden millisekunnin korkeampi kuin ilman IPSec-tunnelia testatessa, joten ero on käyttäjälle käytännössä huomaamaton. Sekä download-että upload-nopeudet olivat keskimäärin 2-3 Mb/s alhaisempia kuin ilman IPSec-tunnelia testatessa, mutta nämäkään muutokset eivät normaalikäytössä ole merkittäviä. Molemmat testit suoritettiin hetkellisten vaihteluiden vaikutusten minimoimiseksi kolme kertaa, mutta tulokset niiden välillä eivät vaihdelleet merkittävästi.

Testissä todettiin, että IPSec-tunnelointi aiheuttaa yhteyteen viivettä sekä nopeuden laskemista, mutta niin vähän, ettei kumpaakaan normaalikäytössä huomaa. Samalla saatiin varmistettua, että tunneloitu yhteys toimii toisen operaattorin liittymällä laboratorion testiverkon ulkopuolella ja että laitteen sijaintia tai sen käyttämää liittymää voi vaihtaa säilyttäen yhteyden pilvihallintapalvelimeen. Ratkaisu on siis näiltä osin käyttökelpoinen ja sitä on mahdollista asiakasverkoissa niiden sijainnista riippumatta.

4.6 Varayhteys

Yritysverkoissa olisi aina hyvä olla varmentava varayhteys mahdollisten vikatilanteiden varalle. Testiverkon laitteista BR-1-reititin sisältää paikan SIM-kortille, joten sille voidaan määritellä 4G-mobiiliyhteys langallisen laajakaistayhteyden lisäksi. Pilvihallinnan kautta reitittimelle voidaan määritellä ensi- ja toissijainen liitانتä internetyhteyttä varten, jolloin ensisijaisen yhteyden katketessa liikenteen pitäisi automaattisesti siirtyä kulkemaan toissijaisen liitännän kautta. Testin tapauksessa liitännät olivat GE 0/0/4, johon yhteys tuli Ethernet-kaapelilla testilaboratorion kytkimeltä, sekä Cellular 0/0/0, eli laitteen mobiiliyhteyksiliitانتä.

Pilvihallintapalvelimen käyttöliittymän kautta ei saanut määriteltyä asetuksia mobiiliyhteyksiliitännälle, joten oikeat asetukset, kuten mobiiliyhteyksiliittymän APN, SIM-kortin PIN-koodi ja oletusreitti tuli syöttää komentorivin kautta ennen palvelimeen yhdistämistä. Ongelmia tuli vastaan kuitenkin jo alkuvaiheessa, sillä pilvihallinnan kautta ensi- ja toissijaista liitانتää valittaessa käyttöliittymä ei hyväksynyt asetusta, vaan ilmoitti jommankumman Internet-liitännän määrittelyjen olevan puutteellinen. Tämä asetus vaikuttaa varayhteyden lisäksi ainakin automaattiseen kuormantasaukseen, joka vaatii myös kaksi liitانتää määritettäväksi käyttöliittymän kautta. Laite ja sen liitännät kokeiltiin määrittää uudelleen kahteen kertaan, mutta ongelma ei selvinnyt. Kaikilla kerroilla laitteen molemmat liitännät saivat julkisen IP-osoitteen DHCP:n kautta ja onnistuivat vuorollaan yhdistämään ulkonverkon osoitteisiin, kun toisen liitännän yhteyden katkaisi. Tästä huolimatta reitittimen Internet-liitännän valinta ei onnistunut, joten kyseessä oli mitä ilmeisimmin ohjelmistovika. Laitevalmistajalta ei saatu asiaan ratkaisua opinnäytetyön tekemisen aikana.

Inter-site VPN -määrittelyssä pystyi edellä mainitusta huolimatta valitsemaan laitteen molemmat liitännät Internet-liitännöiksi Spoke-laitteiden asetusten kohdalla. Tällöin pilvihallintapalvelin loi reitittimelle kaksi ipsec policy -määrittelyä, ja liitti yhden kumpaankin liitانتää. Määrittelyt olivat nimeä lukuun ottamatta identtiset, ja ohjeistivat laitteen luomaan tunnelin palomuurin osoitteeseen, kun liikennettä alettiin lähettää jostain reitittimen lähiverkon osoitteesta. Määrittelyksiä piti olla kaksi, sillä ne voidaan liittää vain yhteen liitانتään kerrallaan. Laitteelle manuaalisesti ennen pilvihallintaan yhdistämistä määritetyt oletusreitit sisälsivät korkeamman prioriteetin langalliselle yhteydelle, joten laite loi tunnelin palomuurille käyttäen Ethernet-liitانتää. Samalla mobiiliyhteyksiliitانتä pysyi aktiivisessa tilassa, mutta ei luonut tunnelia. Yhteyden toimivuus ja liikenteen oikea kulku ulkonverkkoon varmistettiin traceroute-komennolla.


```

[BR-1]ping -c 1000 -a 192.168.240.1 1.1.1.1
PING 1.1.1.1: 56 data bytes, press CTRL_C to break
  Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=59 time=19 ms
  Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=59 time=18 ms
  Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=59 time=18 ms
  Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=59 time=18 ms
Apr 19 2021 08:23:10+02:00 BR-1 IFNET/1/IF_LINKDOWN:OID 1.3.6.1.6.3.1.1.5.3 Interface 7 turned into DOWN state.(Admin
Status=1, OperStatus=2, InterfaceName=GigabitEthernet0/0/4)
[BR-1]
Apr 19 2021 08:23:10+02:00 BR-1 IPV6/2/IF_IPV6CHANGE:OID 1.3.6.1.2.1.55.2.0.1 The status of the IPv6 Interface change
d. (IfIndex=7, IfDescr=
[BR-1]
Apr 19 2021 08:23:10+02:00 BR-1 %%01IFPDT/4/IF_STATE(1)[98]:Interface GigabitEthernet0/0/4 has turned into DOWN state
[BR-1]
Apr 19 2021 08:23:10+02:00 BR-1 %%01IFNET/4/LINK_STATE(1)[99]:The line protocol IP on the interface GigabitEthernet0/
0/4 has entered the DOWN state.
[BR-1]
Apr 19 2021 08:23:10+02:00 BR-1 %%01IFNET/4/LINK_STATE(1)[100]:The line protocol IPv6 on the interface GigabitEtherne
t0/0/4 has entered the DOWN state.
[BR-1]
Apr 19 2021 08:23:11+02:00 BR-1 IPSEC/4/IKESAPHASE1ESTABLISHED:OID 1.3.6.1.4.1.2011.6.122.26.6.13 IKE phase1 sa estab
lished. (PeerAddress=, PeerPort=500, LocalAddress=, AuthMethod=pre-shared-key, AuthID=
, IDType=IP, VsysName=, Role=Initiator)
[BR-1]
Apr 19 2021 08:23:11+02:00 BR-1 IPSEC/4/IPSECTUNNELSTART:OID 1.3.6.1.4.1.2011.6.122.26.6.1 The IPsec tunnel is establi
shed. (Ifindex=12, SeqNum=1, TunnelIndex=4026531857, RuleNum=1, DstIP=, InsideIP=, RemotePort=500, CpuID=0, SrcIP=
, FlowInfo=Source: 192.168.240.0/255.255.255.0:0-65535 Destination: 0.0.0.0/0.0.0.0:0-65535 Protocol: 0 DSCP:
255, LifeSize=1843200, Lifetime=3600, VsysName=, InterfaceName=Cellular0/0/0, SlotID=0, Role=Initiator)
[BR-1]
Request time out
  Reply from 1.1.1.1: bytes=56 Sequence=6 ttl=59 time=24 ms
  Reply from 1.1.1.1: bytes=56 Sequence=7 ttl=59 time=16 ms
  Reply from 1.1.1.1: bytes=56 Sequence=8 ttl=59 time=25 ms
  Reply from 1.1.1.1: bytes=56 Sequence=9 ttl=59 time=18 ms
  Reply from 1.1.1.1: bytes=56 Sequence=10 ttl=59 time=24 ms
  Reply from 1.1.1.1: bytes=56 Sequence=11 ttl=59 time=23 ms
Apr 19 2021 08:23:14+02:00 BR-1 IPSEC/4/IPSECTUNNELSTOP:OID 1.3.6.1.4.1.2011.6.122.26.6.2 The IPsec tunnel is deleted
. (Ifindex=7, SeqNum=1, TunnelIndex=4026531856, RuleNum=1, DstIP=, InsideIP=, RemotePort=500, CpuID=0, SrcIP=
, FlowInfo=Source: 192.168.240.0/255.255.255.0:0-65535 Destination: 0.0.0.0/0.0.0.0:0-65535 Protocol: 0 DSCP:
255, LifeSize=1843200, Lifetime=3600, VsysName=, InterfaceName=GigabitEthernet0/0/4, SlotID=0)
fflineReason=Config modify or manual offline, VsysName=, InterfaceName=GigabitEthernet0/0/4, SlotID=0)
[BR-1]
  Reply from 1.1.1.1: bytes=56 Sequence=12 ttl=59 time=21 ms
  Reply from 1.1.1.1: bytes=56 Sequence=13 ttl=59 time=21 ms
  Reply from 1.1.1.1: bytes=56 Sequence=14 ttl=59 time=20 ms
  Reply from 1.1.1.1: bytes=56 Sequence=15 ttl=59 time=23 ms
  Reply from 1.1.1.1: bytes=56 Sequence=16 ttl=59 time=26 ms
  Reply from 1.1.1.1: bytes=56 Sequence=17 ttl=59 time=22 ms

--- 1.1.1.1 ping statistics ---
  17 packet(s) transmitted
  16 packet(s) received
  5.88% packet loss
  round-trip min/avg/max = 16/21/26 ms

```

Kuva 13. BR-1-reitittimen komentorivi käynnistäessä jatkuvan ping-komennon ja irroitta-
essa Ethernet-kaapelin.

Yhteyden kulun ja IPsec-tunnelin vaihtumista liitännästä toiseen testattiin käynnistä-
mällä jatkuva ping-komento reitittimen VLAN 1-liitännän osoitteesta ulkoverkkoon
Cloudflaren DNS-palvelimen osoitteeseen 1.1.1.1. Lähetettävien pakettien maksimimää-
räksi valittiin tuhat ja pakettien lähetysväli oli oletusarvon mukaisesti puoli sekuntia. Pian
testin aloittamisen jälkeen Ethernet-yhteys katkaistiin irrottamalla kaapeli laitteesta,
jonka jälkeen laite muodosti kuvan 13 mukaisesti uuden tunnelin käyttäen mobiiliyhtey-
den liitännää kadottaen vain yhden paketin katkoksen aikana. Tämä vastaa noin puolen
sekunnin katkosta, jonka jälkeen yhteys jatkoi toimimista toisen liitännän kautta. Yhteys
vaihtui siis erittäin nopeasti kulkemaan toista reittiä, ja katkos oli niin lyhyt, ettei sitä to-
dennäköisesti käyttäjä huomaisi. Ethernet-kaapelin kytkiessä takaisin laite teki samat
toimenpiteet, vain käänteisessä järjestyksessä. Uusi tunneli muodostui, vanha poistui ja
yhteys siirtyi kulkemaan toista reittiä kadottaen tällä kertaa kaksi pakettia muutoksen ai-
kana. Tämä vastaa noin sekunnin katkosta, mutta on silti hyvin pieni katkos normaali-
käytössä.

Pilvihallintapalvelimen käyttöliittymän ohjelmistovioista huolimatta tunneloidun yhteyden vaihtuminen toimi halutulla tavalla, ja liikenne vaihtui kulkemaan vikatilanteessa liitännöjen välillä ilman merkittävää viivettä. Samat viat kuitenkin estävät ainakin liitännöjen välisen kuormantasauksen sekä mahdollisesti monen muun ominaisuuden käytön osittain tai kokonaan. Myös mobiiliyhteyshäiriön määrittäminen voi aiheuttaa ongelmia, sillä jos asiakasyritys esimerkiksi vaihtaa 4G-liittymänsä operaattoria niin laite tulee poistaa pilvihallintapalvelimelta ja liitäntä tulee määritellä uudelleen manuaalisesti. Vaikka varayhteys toimiikin halutulla tavalla, testaushetken tilassa pilvihallinta ei näiden ominaisuuksien osalta todennäköisesti sovellu vielä tuotantokäyttöön.

4.7 Ohjelmistopäivitys

Laitteet tulisi aina pitää päivitettyinä, jotta ne saisivat uusimmat ominaisuudet ja tietoturvapäivitykset. Pilvihallinta sisältää device upgrade -toiminnon, jonka avulla yhdistetyille laitteille saa asennettua uuden ohjelmistoversion tai pienemmän päivityksen sen nykyiseen ohjelmistoversioon. Toiminnon testaamiseksi laitevalmistajalta hankittiin uusi ohjelmistoversiotiedosto edullisemmille reitittimille, jotka käyttivät HQ-reititintä vanhempaa ohjelmistoa. Tiedosto ladattiin pilvihallinnan omaan tiedostosäilöön verkkoliittymän kautta ja sille määriteltiin tiedosto- ja laitetyyppi, testin tapauksessa ”software package” eli ohjelmistoversiotiedosto ja reititin.

Kun päivitystiedosto oli ladattu pilvihallintapalvelimelle, käyttöliittymä ilmoitti automaattisesti, että kahden toimipisteen laitteisiin oli saatavilla päivitetty ohjelmisto. Päivitettävät laitteet sai valittua toimipisteiden listalta, jonka jälkeen niille sai luotua päivitysaikataulun. Päivityksen ajastaminen verkon aktiivisen ajan ulkopuolelle katkosten minimoimiseksi on tärkeää, ja käyttöliittymä sisälsi siihen hyvät ominaisuudet. Pilvihallinnan kautta sai määriteltä ajan, milloin päivitystiedostot ladataan laitteille, sekä milloin laitteet käynnistyvät uudelleen ja aloittavat päivitysprosessin. Laitteille sai valittua halutun uuden ohjelmistoversion tai päivityksen ja tarvittaessa sai asennettua myös vanhemman ohjelmistoversion tai poistettua aiemman päivityksen.

The device discovery protocol is NETCONF. Click [here](#) to switch to another protocol.

Update Schedule

Configure an Upgrade Time

Time mode: **Device Time** Client Time

Time to Download Upgrade Files: **Immediately** Specific Date and Time Specific Time Every Week Network local time (UTC +02:00)

Software Update Restart Time: **Immediately** Specific Time Every Week

Tuesday 11:00:00

Configure an Upgrade Method

File server: **Built-in file server**

Configure the Target Version

Enter a keyword:

Device Model	Device Type	Site	Current Software Version	Current Patch Version	Upgrade Software Version	Upgrade Patch Version	Uninstall Patch
AR1117M-1T1E-A	AR	BR-1	V300R019C10SPC300	ARV300R019SPH016	V300R019C11SPC200/AR110 V...	Not upgrade	Do not uninstall
AR1117M-1T1E-A	AR	BR-2	V300R019C11SPC200		V300R019C11SPC200/AR110 V...	Not upgrade	Do not uninstall

Total records: 2

20

Cancel OK

Kuva 14. Ohjelmistopäivitysaikataulun luonti kahdelle laitteelle pilvihallinnan kautta.

Päivitysominaisuuksien testaamiseksi BR-1 ja BR-2 valittiin päivitettäväksi uudempaan ohjelmistoversioon, päivitystiedosto määriteltiin ladattavaksi laitteille heti ja laitteet määritettiin kuvan 14 mukaisesti käynnistymään uudelleen sekä asentamaan päivitys joka tiistai klo 11.00. Testissä kaikki toimi kuten odotettiin ja uusi ohjelmistoversiotiedosto siirtyi sekä asentui laitteille määritellyn aikataulun mukaisesti. Uudelleenkäynnistymisen jälkeen laitteet palasivat normaalisti takaisin yhteyteen pilvihallintaan. Onnistuneen päivityksen jälkeen käyttöliittymä antoi rollback-vaihtoehdon aiempaan versioon palaamiseksi, siltä varalta, että päivitys aiheutti ongelmia. Tämä ei kuitenkaan toiminut, sillä reitittimet ei senhetkisessä pilvihallinnan ohjelmistoversiossa tukeneet tätä ominaisuutta.

Päivitysprosessi toimi testissä halutulla tavalla ja kaksi laitetta saatiin päivitettyä uudempaan ohjelmistoversioon ilman, että laitteisiin piti yhdistää manuaalisesti SSH:n tai konsoliyhteyden kautta. Tämä voi helpottaa huomattavasti verkkolaitteiden päivitystä vähentämällä vaadittavan työn määrää sekä käyttökatkojen kestoja. Testauksen aikaan tieto uusista saatavilla olevista laitepäivityksistä piti saada laitevalmistajalta ja päivitystiedostot tuli ladata manuaalisesti pilvihallintapalvelimelle, mutta muuten automatisoitu päivitysprosessi toimi suoraviivaisesti. Ongelmatilanteissa aiempaan päivitykseen tuli kuitenkin palata manuaalisesti, sillä pilvihallinta ei tukenut automaattista palaamista reitittimillä. Tämä saattaa aiheuttaa merkittäviä ongelmia ja lisätyötä, jos uuden päivityksen kanssa ilmenee ongelmia, jotka koskevat useita reitittimiä.

4.8 Laitevaihto

Yritysverkoissa jatkuvasti käytössä olevat laitteet saattavat joskus rikkoutua, jolloin ne joudutaan vaihtamaan uuteen. Korkean käytettävyyden ylläpitämiseksi laitevaihdon tulee olla suoraviivainen ja nopea prosessi suorittaa pilvihallinnan osalta. Laitevaihdon testaamiseksi testiverkkoon ja pilvihallinnan samaan toimipisteeseen lisättiin toinen HQ-reititin, jonka tarkoituksena on korvata alkuperäinen samanmallinen reititin. Laitteen korvaaminen ei onnistu, jos laitteet eivät ole samaa mallia. Laiterikon simuloimiseksi alkuperäisestä HQ-reitittimestä katkaistiin virta, jolloin laite siirtyi offline-tilaan pilvihallintapalvelimella noin kahden minuutin kuluttua.

Device Management | Management Settings

Replacement List

Old device:

Name	ESN	Status	Description	Site	Device Model	Public IP address	Device Software Version	Registration Time
HQ	21500104832SL8500110	Alarm		HQ	JPM3T	10.42.191.274	V300R019C10SPC300	2021-03-30 13:32:54 DST

New device:

Name	ESN	Status	Description	Site	Device Model	Public IP address	Device Software Version	Registration Time
HQ_2	21500104812SL3604275	Norm...		HQ	JPM3T	10.42.191.272	V300R019C10SPC300	2021-04-07 11:03:46 DST

Cancel OK

Kuva 15. Pilvihallintapalvelimen korvausvalikko vaihtaessa HQ-reitittimen toiseen samanmalliseen laitteeseen.

Laitelistalta valittiin sen nimen kohdalta "replace", joka avasi laitteen korvausvalikon ja korvaavaksi laitteeksi ehdotettiin automaattisesti toista samanmallista laitetta. Alkuperäinen laite valittiin kuvan 15 mukaisesti korvattavaksi uudella, jolloin laitteiden nimet tiedot vaihtuivat pilvihallinnassa keskenään ja alkuperäinen laite poistettiin automaattisesti sen toimipisteestä. Pilvihallintapalvelin tallentaa laitteille tehdyt määrityksen kahden tunnin välein, joten uusi laite sai kaikki määritykset vanhalta laitteelta, ja jatkoi sen toimintaa ilman uudelleenkäynnistystä. Vanha laite oli nyt turha ja sen pystyi poistamaan turvallisesti pilvihallinnasta.

Suurin viive tosimaailmaan laiterikkotilanteissa tulee ajasta laitteen rikkoutumisen ja korvaavan laitteen asennuksen välissä. Koska vanhan laitteen määritykset säilyvät pilvihal-

linnassa ja korvaavan laitteen sarjanumero voidaan lisätä sinne jo etukäteen, asennustilanteessa uutta laitetta ei tarvitse määritellä vaan ainoastaan kytkeä paikalleen vanhan tilalle. Tämä nopeuttaa laitevaihtoprosessia sekä estää laitemääritysten menetyksen viikatilanteissa. Laitevaihdon osalta pilvihallinta siis toimii halutulla tavalla.

5 ARVIOT JA JOHTOPÄÄTÖS

Laboratoriossa suoritettujen testien perusteella voidaan todeta, että testattu SD-WAN-ratkaisu soveltuu monelta osin toimeksiantajayrityksen asiakasyrityksille tarjottavan palvelun pohjaksi. Ratkaisun sisältämät reitittimet ovat hintatasoltaan samankaltaisia kuin muut toimeksiantajayrityksen tällä hetkellä yritysverkkoysteysien mukana tarjoamat laitteet ja sisältävät hintaansa nähden paljon ominaisuuksia. ZTP toimi testaushetkellä ainostaan HQ-reitittimellä, joten edullisempia laitteita asiakasyritys ei voi ottaa itse käyttöön ilman asentajaa. Normaalisti asentaja kuitenkin käy aina asentamassa asiakasyrityksen laitteet käyttökuntoon paikan päällä, joten ongelma ei ole palvelun kannalta kriittinen.

IPSec-tunneloinnilla ei ollut testeissä merkittävää vaikutusta yhteyden viiveeseen tai nopeuteen, joten asiakasyrityksen ei pitäisi käytössä huomata eroa tunneloimattomaan yhteyteen. Laitteiden IPSec-tunneleiden mitatut läpisyöttötehot olivat myös korkeat, joten asiakasyritykset voivat vapaammin valita liittymänopeuksia jopa 1000Mb: iin/s asti. Mahdolliset liitännästyypit internetyhteydelle rajoittuvat pilvihallinnan vuoksi joko Ethernetiin tai mobiiliyhteyteen. Esimerkiksi VDSL-liitännää ei pysty käyttämään pilvihallitun tilan määrittämissä, vaikka laite sillä yhteyden saisikin. Tämä ongelma voidaan kiertää asentamalla reitittimen ja seinäpistokkeen väliin asennettavalla VDSL-Ethernet-mediamuuntimella. Tunneloitu yhteys osaa automaattisesti reagoida liittymän IP-osoitteen tai tyypin vaihtumiseen. Normaalisti langallisella yhteydellä yhdistetyn laitteen voi esimerkiksi siirtää väliaikaiseen sijaintiin ja käyttää sitä siellä mobiiliyhteydellä.

asiakasyrityksestä riippuen pilvihallintapalvelimen tarjoama keskitetty ja ulkoistettu hallinta voi olla erittäin hyvä peruste SD-WAN-palvelun hankkimiseksi. Opinnäytetyön tekemisen kanssa samaan aikaan tehdyssä asiakaspilottiprojektissa käytettiin onnistuneesti pilvihallinnan kautta hallittuja saman laitevalmistajan kytkimiä ja langattomia yhteyspisteitä asiakasyrityksen verkossa. Siten myös asiakasyrityksen lähiverkon hallitseminen on mahdollista yhteensopivia laitteita käyttäessä. Lisäksi keskitetty palomuuriratkaisu tarkoittaa, että jokaiseen toimipisteeseen ei tarvitse hankkia erillistä palomuuria vaan reititin riittää yhdyskäytäväksi ulko verkkoon. Käytännössä lähes koko asiakasyrityksen verkko voidaan saattaa toimeksiantajayrityksen hallintaan, joka voi vähentää asiakasyrityksen omaa työmäärää ja nopeuttaa ongelmatilanteiden ratkaisua merkittävästi.

Suurimmat ongelmat asiakasyritysten kannalta ovat mahdolliset yhteensopivuusongelmat reitittimien ja pilvihallinnan kanssa, joita voi ilmetä integroitaessa asiakasyrityksen nykyistä verkkoinfrastruktuuria SD-WAN-palveluun. Näitä ei vielä yksinkertaisen testiverkon testeissä voinut paremmin todeta, joten ongelmat pitää ratkaista tapauskohtaisesti niiden ilmetessä.

Toimeksiantajayritykselle SD-WAN-palvelun kehittäminen on kannattavaa ja tavoiteltavaa, sillä SD-WAN on nopeasti kasvava verkkoteknologiamarkkinoiden osa-alue sekä maailmanlaajuisesti että Suomessa. Sen tarjoama mahdollisuus laajentaa toimialuetta ja hankkia asiakkaita fyysisen runkoverkon alueen ulkopuolelta on merkittävin yksittäinen tekijä palvelun kehityksen taustalla. Tarjolla olevista ratkaisuista opinnäytetyössä testattu laitteiston ja ohjelmiston yhdistelmä on selvästi hinnaltaan ja ominaisuuksiltaan yrityksen käyttötarkoitukseen parhaiten soveltuva, joten tahto luoda sen pohjalta asiakasyrityksille tarjottava palvelu on suuri. Erityisesti reitittimien IPsec-läpisyöttöteho oli merkittävässä asemassa laitevalmistajaa valittaessa, sillä saman tason läpisyöttötehoja tarjoavat muiden valmistajien laitteet olivat hinnaltaan reilusti suurempia, jopa yli kymmenkertaisia. Lisäksi myös saman laitevalmistajan palomuurien, kytkinten ja langattomien yhteyspisteiden yhteensopivuus pilvihallinnan kanssa mahdollistaa teoriassa melkein koko verkkoinfrastruktuurin myymisen asiakkaalle.

Laitteiden asennuksen testaus laboratoriossa aiheutti yrityksen kannalta pettymyksen, sillä laitevalmistajan lupaama ZTP-ominaisuus ei toiminut testauksen aikaan muilla kuin HQ-reitittimellä. Laitteet saatiin pilvihallittuun tilaan vain manuaalisella määrittelyllä, joka tarkoittaa, että asiakasyritys ei itse voi ottaa niitä käyttöön. Myös mahdollinen mobiiliyhteys piti määritellä aina asennusvaiheessa, eikä sitä voinut myöhemmin muokata tai ottaa käyttöön ilman laitteen uudelleenasetusta. Vaikka olisi toivottavaa, että ZTP toimisi luvatusi ja mobiiliyhteyden pystyisi määrittelemään pilvihallinnan kautta, niiden puuttuminen ei kuitenkaan estä palvelun kehitystä. Ellei pilvihallintaan tai reitittimiin tule palvelun kehityksen aikana näitä asioita korjaavaa päivitystä, laitteita varten voidaan luoda halutut määrittelyt sisältävä pohjakonfiguraatio. Asentaja voi tietenkin myös asettaa oikeat asetukset komentorivin kautta paikan päällä. Laitteet tukivat IPsec-tunneleiden puolesta liittymänopeuksia 1000Mb: iin/s asti, joten asiakasyritysten ei tarvitse tyytyä normaalia alhaisempaan nopeuteen SD-WAN-palvelun käytön vuoksi. Asiakasyrityksille ei myöskään tarvitse välttämättä määritellä operaattoriverkkojen rajat ylittäviä yritysverkko-yhteyksiä, mikä helpottaa toimeksiantajayrityksen työtä.

Pilvihallinnan avulla sai määriteltä valtaosan halutuista verkon ominaisuuksista, mutta yleisesti ottaen sen reitittimien määrittymismahdollisuudet olivat rajoittuneita. Suurimman ongelma määrittymiseen toi reitittimien komentorivin asetusten tallentumattomuus pilvihallituksessa tilassa. Vertailun vuoksi toisessa projektissa käytetyt saman laitevalmistajan kytkimet sekä langattomat yhteyspisteet säilyttivät komentorivin kautta tehdyt määrittymiset onnistuneesti uudelleenkäynnistyksen jälkeen. Näille laitteille oli myös enemmän määrittymismahdollisuuksia saatavilla pilvihallinnan kautta. Esimerkki testattujen reitittimien rajoittuneista ominaisuuksista on laiteohjelmiston päivitys, joka onnistui pilvihallinnan kautta, mutta ilman mahdollisuutta vikatilanteessa palata aiempaan versioon. Myös puute kaikkien laitteissa fyysisesti olevien liitännöiden määrittymiselle osoitti pilvihallintaohjelmiston keskeneräisen tilan.

Yhdessä manuaalisesti määritellyn palomuurin kanssa tunneloidut yhteydet kuitenkin saatiin toimimaan halutulla tavalla, siten että kaikki tarvittavat määrittymiset tehtiin reitittimille pilvihallinnan kautta. IPSec-asetuksiin ei pitäisi joutua tekemään alkumäärittymisen jälkeen muokkauksia, koska tunnelit toimivat sillä periaatteella, että reitittimet tietävät aina palomuurin osoitteen. Siten reitittimien liittymätyyppi tai IP-osoite voi vaihdella häiritsemättä tunneloidun yhteyden muodostamista. Uusia laitteita pystyi lisäämään valmiiseen tunnelimäärittymiseen helposti, ja vikatilanteessa rikkiäisen laitteen sai korvattua uudella yksinkertaisesti. Reitittimien määrittymisen jäivät pilvihallituksessa tilassa yksinkertaisiksi, joten tarkemmat verkon määrittymiset, kuten lähiverkkojen välistä liikennettä säätelevät säännöt tai pakettikoon asetukset pitää määrittellä manuaalisesti palomuurilta.

Opinnäytetyötä tehdessä aikataulu palvelun kehitykselle oli ennalta määriteltä, joten asian kanssa piti tehdä tilanteeseen nähden sopiva ratkaisu. Melkein kaikki kohdatut ongelmat ja rajoitukset johtuivat pilvihallintaohjelmistosta, ei niinkään reitittimistä, jotka toimivat odotetusti ja hyvin. Vaikka testien lopussa kaikki toimi suurimmalta osin niin kuin pitikin, oli kuitenkin kyse hyvin yksinkertaistetusta testiverkosta. Oikeissa asiakasympäristöissä valmiina olevat verkot, tai uusilta verkoilta vaadittavat ominaisuudet ovat usein paljon monimutkaisemmat, ja ongelmia todennäköisesti tulee vastaan niiden kanssa.

Tehtyjen testien perusteella testatun SD-WAN-ratkaisun pohjalta on vaikea tämänhetkessä tilanteessa lähteä luomaan asiakasyrityksille tarjottavaa palvelua. Tämä tarkoittaa, että palvelun kehityksen aikataulua pitää luultavasti pidentää. Reitittimiä voidaan kuitenkin alkaa jo käyttää manuaalisesti määriteltynä tietyissä pilottiverkoissa siihen asti, että pilvihallintaan saadaan päivitys joka parantaa reitittimien toiminnallisuutta ja korjaa nykyisiä ongelmia.

LÄHTEET

Citrix, 2018. "How to Find Maximum Size of IP Data Payload that can Traverse WAN Environment Without Fragmentation." Luettu 19.4.2021.
<https://support.citrix.com/article/CTX115434>

Cloudflare. 2021. "What is MSS (maximum segment size)?" Luettu 19.4.2021.
<https://www.cloudflare.com/learning/network-layer/what-is-mss/>

Cook, Matt 2017. "TCP vs. UDP: What's the Difference?" Luettu 19.4.2021. <https://www.lifefsize.com/en/blog/tcp-vs-udp/>

Cooney, Michael 2019. "What is SD-WAN, and what does it mean for networking, security, cloud?" Luettu 26.1.2021.
<https://www.networkworld.com/article/3031279/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html>

Craven, Connor 2017. "The Primary Benefits of SD-WAN Technology." Luettu 25.1.2021.
<https://www.sdxcentral.com/networking/sd-wan/definitions/sd-wan-technology/>

CreaNord. 2020. "EchoVault R8.7.0 USER GUIDE." Ei saatavilla julkisesti.

Davies, Nahla 2021. "Benefits of SD-WAN." Luettu 20.4.2021.
<https://www.enterprisestorageforum.com/networking/benefits-of-sd-wan/>

Mota, Ray. 2020. "Tunnel-Based versus Tunnel-Free SD-WAN." ACG Research.
<https://www.acgcc.com/reports/tunnel-based-versus-tunnel-free-sd-wan/>

Raynovich, R. Scott 2020. "2020 SD-WAN Growth Report: Market Poised to Accelerate." Luettu 23.4.2021.
<https://www.futuriom.com/articles/news/2020-sd-wan-growth-report-sd-wan-market-likely-to-accelerate/2020/06>

Riverbed. 2021. "What is SD-WAN?" Luettu 21.4.2021.
<https://www.riverbed.com/faq/what-is-sd-wan.html>

Wiesner, Ashley 2020. "What is Software-Defined Security? — Definition." Luettu 26.1.2021.
<https://www.sdxcentral.com/security/definitions/what-is-software-defined-security>

Yang, Cui, Li, Liu ja Yi Xu. 2019. "Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities." 2019 28th International Conference on Computer Communication and Networks. doi:10.1109/ICCCN.2019.8847124