SD-WAN -järjestelmän rakentaminen verkkoon

Mikko Tukia

2019 Laurea

Laurea-ammattikorkeakoulu

SD-WAN -järjestelmän rakentaminen verkkoon

Mikko Tukia
Tietojenkäsittelyn koulutus
Opinnäytetyö
Maaliskuu, 2019

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutus
Tradenomi (AMK)

Mikko Tukia

SD-WAN -järjestelmän rakentaminen verkkoon

Vuosi 2019 Sivumäärä 32

Opinnäytetyön tavoitteena oli perehtyä SD-WAN -tekniikkaan ja sen ominaisuuksiin. Työ suoritettiin yrityksen toimeksiantona, joka halusi tietosuojan vuoksi pysyä nimettömänä. Tekniikasta haluttiin saada yleiskatsaus sen käyttötarkoituksista ja analysoida myös sen taloudellisia vaikutuksia, jotta siitä voitaisiin kehittää yritykselle myytävää tuotetta.

Työhön sisältyi myös SD-WAN -järjestelmän rakentaminen ja konseptitestaus. Testaus tapahtui yrityksen verkossa, ja siinä kokeiltiin osaa SD-WAN:in ominaisuuksista. Tämän tavoitteena oli tuottaa yritykselle toistettava ja kehitettävä läpikatsaus järjestelmän konfiguroinnista.

Toimeksiantoon kuului myös eri valmistajien SD-WAN -toteutusten tutkiminen ja niiden ominaisuuksien erittely. Tämän tarkoituksena oli selvittää tilannepohjaisia käyttötarkoituksia erilaisille verkkoratkaisuille.

Tutkimuksen lopputuloksena saatiin yleikatsaus SD-WAN:in toiminnasta verrattuna MPLS- ja VPN-tekniikoihin, sekä läpikäynti tietyn SD-WAN -tuotteen toiminnasta.

Asiasanat: SD-WAN, software-defined wide-area network, laajaverkko

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Mikko Tukia

Building an SD-WAN System into a Network

Year 2019 Page count 32

The purpose of this thesis was to investigate the SD-WAN technology and its properties. The work was commissioned by a company, who wished to remain anonymous for information security. An overview of the technology as well as a view on its economic effects was requested so that SD-WAN could be developed as a product for the company.

The thesis also included constructing SD-WAN system as a proof of concept. The test took place in the company's network, and some of the advertised properties of SD-WAN were given a trial run. The purpose of this was to give the company a repeatable walkthrough of configuring the system to improve upon.

The commission also included a comparison of SD-WAN products by different vendors and a breakdown between their properties. The reasoning behind this was to find situational uses for different network solutions.

The final result of this study was an overview of how SD-WAN functions compared to MPLS and VPN -technologies, as well as a detailing of a certain SD-WAN product's function.

Keywords: SD-WAN, software-defined wide-area network

Sisällys

1 Johdanto 8
2 Yritysten laajaverkkoihin liittyviä ongelmia 8
2.1 Kaistan tarpeen kasvu 8
2.2 Verkkojen lisääntyminen 10
3 SD-WAN 11
3.1 Määritelmä 11
3.2 SD-WAN ominaisuudet 11
3.2.1 Keskitetty hallinta 11
3.2.2 Kuljetusagnostisuus 12
3.2.3 Multipath-tekniikka 12
3.2.4 VPN-verkko 12
3.2.5 Kuormituksen tasapainotus 13
3.3 SD-WAN -toteutusten väliset erot 13
3.4 SD-WAN:in suhde MPLS- ja VPN-tekniikoihin 15
3.4.1 MPLS 15
3.4.2 VPN 17
3.5 Taloudelliset vaikutukset 17
4 Tutkimus 18
4.1 Tutkimuksen toteutus 19
4.1.1 Kuljetusagnostisuuden testaus 19
4.1.2 Multipath-tekniikan testaus 20
4.1.3 Keskitetyn hallinan testaus 20
4.1.4 VPN:n testaus 23
4.1.5 Kuormituksen tasapainotuksen testaus 24
5 Johtopäätökset 26
6 Pohdinta 27
Lähteet 28
Kuvat 32

Lyhenteet

4G	Yhteisnimitys neljännen sukupolven mobiiliverkkotekniikoille.
FEC	Forwarding *Equivalence Class*. MPLS-tekniikassa käytetty termi tietoliikennepaketeista, jotka reititetään niihin liitetyillä lyhyillä etiketeillä.
HTTP	*Hypertext Transfer Protocol*. Yleinen selainten käyttämä protokolla.
QoE	*Quality of Experience*. IT-palvelun laadusta käytetty termi. Koskee useimmiten esimerkiksi videon- ja äänenlaatua.
QoS	*Quality of Service*. IT-palvelun laadusta käytetty termi. Yleensä liitetty tietoliikenteen kulkuun, jossa priorisoidaan tiettyjen ohjelmien liikennettä.
IP	*Internet Protocol*. Yleisin nykyaikaisen tietoliikenneverkon tiedonsiirtoprotokolla.
LAN	*Local Area Network*. Lähiverkko tai sisäverkko. Esimerkiksi yhden toimiston tai huoneiston oma, pienempi verkko.
LTE	*Long-Term Evolution*. Yksi 4G-tyypin mobiiliverkkotekniikoista.
Mbps	Megabittiä sekunnissa. Tiedonsiirtonopeuden yksikkö.
MPLS	*Multiprotocol Label Switching*. Tekniikka, jolla viesti ohjataan verkon laitteelta nopeasti toiselle etikettien avulla, eikä käytä IP-verkkoa reititykseen.
MPLS VPN	*Multiprotocol Label Switching Virtual Private Network*. MPLS-verkon läpi kulkeva VPN-tunneli. Ei välttämättä salattu.
SDN	*Software-Defined Network*. Lähiverkon teknologia, joka keskittää verkkolaitteiden käytön.
SD-WAN	*Software-Defined Wide Area Network*. Laajaverkkojen hallintaan erikoistunut teknologia.
UDP	*User Datagram Protocol*. IP-verkossa käytetty tiedonsiirtoprotokolla, joka ei luo yhteyttä reitittimien välille.

VMDK	*Virtual Machine Disk*. Virtuaalikoneiden käyttämä tiedostotyyppi virtuaalikovalevyille.
VoIP	*Voice over Internet Protocol*. Reaaliaikainen äänensiirto IP-verkossa.
VPN	*Virtual Private Network*. Salattu yhteys kahden tai useamman kohteen välillä.
WAN	*Wide Area Network*. Laajaverkko, pitää sisällään useamman lähiverkon.

1 Johdanto

Tämä opinnäytetyö toteutettiin yritykselle X, joka päätettiin pitää nimettömänä tietosuojan vuoksi. Työssä tutustutaan yritysten laajaverkkojen ongelmiin, SD-WAN–teknologian ominaisuuksiin ja käyttötarkoituksiin, sekä eri valmistajien SD-WAN–toteutusten eroihin. Ohessa on myös konseptitestaus, jossa kokeillaan SD-WAN -järjestelmän rakentamista verkkoon Fortinetin SD-WAN -toteutuksella ja sen ominaisuuksien testausta (Fortinet 2019).

SD-WAN tiivistettynä on laajaverkonhallintatyökalu ohjelmamuodossa, joka pohjautuu SDN-verkkotekniikkaan. SD-WAN itse on tekniikkana varsin tuore, joten opinnäytetyö pyrkii olemaan siihen liittyen mahdollisimman selkeä. Työn tavoitteena on antaa yritykselle yleiskatsaus SD-WAN:in käytöstä ja toiminnasta, jotta palvelusta voitaisiin mahdollisesti kehittää yritykselle myytävää tuotetta.

Uutena teknologiana SD-WAN:ista oli työn kirjoituksen aikana vähän painettua, kirjallista tietoa, joten valtaosa tekstistä perustuu internet-artikkeleihin sekä valmistajien kuvauksiin omista SD-WAN –toteutuksistaan.

2 Yritysten laajaverkkoihin liittyviä ongelmia

Jotta saisimme SD-WAN -tekniikasta ja sen hyödyistä paremman ymmärryksen, perehdymme ensiksi suurten yritysten kasvavien laajaverkkojen yleisimpiin ongelmiin.

2.1 Kaistan tarpeen kasvu

Yksi haasteista nykypäivän yrityksissä on kasvava kaistan tarve (Huntley 2017). Yhä useampi yrityksen funktio, joka ennen saattoi toimia kirjoituskoneilla, paperilla ja postilla on nykyään verkossa. Prosessien vaiheita seurataan reaaliaikaisesti verkossa, ja dataliikenteen määrä yrityksessä kasvaa. (IBM Software 2012.)

Monet yritysten käyttämät palvelut toimivat myös nykyään pilvessä. Sekä laitteiston että ohjelmiston puolella siirrytään nykyaikana useasti virtualisoidun ratkaisun puoleen. Pilvipalvelualustoja voidaan myös vaihdella esimerkiksi tietyn ohjelman kohdalla riippuen sen tarpeista. Otetaan esimerkiksi kuvitteellinen ohjelma, jota yritys käyttää kuukausittaiseen taloustilanteen raportointiin suurelle määrälle asiakkaita. Palvelu on käyttämättömänä valtaosan kuukaudesta, paitsi päivänä, kun raportit lähetetään, jolloin se halutaan suorittaa mahdollisimman tehokkaasti. Tämä palvelu voitaisiin siis siirtää suorituskykyiselle pilvipalvelualustalle raportoinnin ajaksi kerran kuukaudessa, ja loput ajasta ohjelma viettäisi tallessa jollain paikallisella levyllä. Tämä voisi olla hyvä ratkaisu esimerkiksi pilvipalvelun ylläpitokulujen kannalta, kun ohjelmaa pitää isännöidä vain hetken ajan kuukaudessa. Tällainen menetelmä kuitenkin nostaa VMDK:n (Virtual Machine Disk) työn painoa kaistalla, kun ohjelmaa pitää sen kautta kuljettaa. (Kerravala 2010.) Kun samankaltaisia elementtejä

verkossa aletaan laskea yhteen muiden tekijöiden kanssa, voi kaistan kuormittuminen olla aivan eri tasolla kuin ennen pilvipalvelujen käyttöä.

Suurimmat kaistanviejät julkisessa internetissä ovat videonsuoratoistopalvelut, kuten YouTube ja Netflix. Pohjoisamerikkalaisen tilaston mukaan, videopalvelut vastasivat noin 70 %:a internetin kaistan käytöstä. Kolmanneksi eniten kaistaa vei HTTP-selaus (Hypertext Transfer Protocol). (Rosoff 2015.)

Suurenevat tarpeet kaistoilta ilmenevät esimerkiksi nykyisessä videolaadussa. Esimerkiksi, videopalvelu YouTube tuki alun perin vuonna 2005 vain 320x240 videoresoluutiota (Adobe Systems Incorporated 2010). Tähän aikaan YouTube käytti vielä Adobe Flash Playeriä videoiden toistamiseen (Fildes 2009). 2015-luvulla, eli vain 10 vuotta myöhemmin, YouTube ilmoitti tukevansa jo 8K-laatua, eli 7680x4320 videoresoluutiota. 8K-videonkatselu on toki vielä harvinaista 2018-luvulla, mutta on odotettavissa, että 8K-näyttöjen käyttö tulee myös kasvamaan. (Schroeder 2015.) Kymmenessä vuodessa videon pikseleiden määrä on siis potentiaalisesti 432-kertaistunut. Videoiden laadun kasvaessa vaaditaan luonnollisesti huomattavasti enemmän kaistaa niiden toistoon, varsinkin jos halutaan välttää latailutaukoja videoita katsellessa.

Kysymys voi tulla mieleen, että mitä tekemistä videoiden katselulla on yritysten toiminnassa. Työnantaja saattaa kyseenalaistaa työntekijöiden tarpeen katsoa videoita tai ylipäätään selata internetiä viihdemielessä työajalla. Tästä huolimatta tutkimukset osoittavat, että keskiverto työntekijä kuluttaa päivittäin noin 1-3 tuntia aikaa henkilökohtaiseen internetin selailuun (Heathfield 2018). On myös todettu, että vapaa selailu voi edistää työntekijöiden henkistä hyvinvointia ja työtehoa (Gain 2011). On siis fakta, että työntekijät katsovat videoita työajalla, eikä tästä pitäisi koko toimiston kärsiä niukan kaistan takia. Videoiden katselu ei myöskään ole aina pelkkää henkilökohtaista viihdettä, vaan monet opetus- ja ohjemateriaalit ovat tarjolla videoina julkisessa internetissä.

Täysin yrityksensisäiset toimet, kuten videokonferenssit, havittelevat parempaa videon- ja äänenlaatua käyttäjäkokemusta parantaakseen. Tämä ei vaadi linjalta pelkästään hyvää nopeutta, vaan myös alhaista latenssia, että keskustelu olisi mahdollisimman luontevaa. Tällaisesta käyttäjäkokemuksen toteutumisesta käytetään termiä QoS (Quality of Service), jolla usein viitataan dataliikenteen priorisoituun kulkuun tärkeiden ohjelmien kohdalla, kuten kommunikaatiovälineissä. Tämä koskee muun muassa VoIP-käyttöä (Voice over Internet Protocol), eli internetin läpi kulkevaa puhelua. Mikä tahansa korkeakapasiteettinen kaista ei välttämättä riitä yrityksen tarpeisiin, mikäli QoS-laatu koetaan huonoksi. QoS:n kannalta korkealaatuisemmasta liittymästä saadaan todennäköisesti myös maksaa enemmän kuin tavanomaisesta yhteydestä.

2.2 Verkkojen lisääntyminen

Siirrymme ongelmiin kasvavien verkkojen puolelle. Suurilla yrityksillä voi olla kymmeniä, satoja tai jopa tuhansia toimipisteitä. Samoja yrityksen yksityisiä resursseja halutaan käsitellä monessa eri toimipisteessä. Yksi tapa tuoda nämä resurssit kaikille toimipisteille on yhdistää toimipisteiden sisäverkot eli LAN:it. Kun yrityksen toimipisteiden LAN-verkkoja on yhdistetty, voidaan tätä nimittää WAN:ksi, eli laajaverkoksi (Rouse 2016). Jos muutama yhdistetty toimipiste ei yritykselle riitä, vaan toimintaa halutaan laajentaa vielä pidemmälle, aletaan kasvavan verkkojen määrän ja niiden vaatimusten kanssa kohtaamaan uusia vaikeuksia.

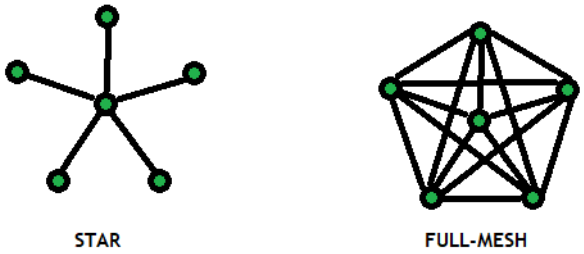
Valtaosa normaalista internetin käytöstä on julkista ja jättää jälkensä, mutta yritykset luonnollisesti haluavat pitää haavoittuvaiset tietonsa yksityisenä. Tässä tapauksessa vaihtoehtoja ovat esimerkiksi MPLS-tekniikka (Multiprotocol Label Switching) ja VPN-tunnelit (Virtual Private Network).

Yksi tapa yhdistää toimipisteitä on MPLS:n avulla. Perehdymme tekniikkaan tarkemmin seuraavassa luvussa verrataksemme sitä SD-WAN–tekniikkaan. Tässä vaiheessa voidaan tiivistää MPLS-tekniikka suhteellisen kalliiksi ja vaikeaksi toimittaa verrattuna normaaliin laajakaistaan, mutta tästä huolimatta se on QoS:n kannalta vaihtoehtona luotettava. Ongelma MPLS-yhteyksissä on yleensä niiden hinta, varsinkin, kun kaistaa on tarkoitus kasvattaa tukemaan useamman toimipisteen työntekijöitä. Syrjäiset kohteet voi jo olla hankalaa yhdistää MPLS:llä yrityksen verkkoon, mutta etenkin, jos ulkomailla sijaitsevat toimipisteet halutaan yhdistää saman verkon alle, on palvelusta odotettavissa huomattavat kulut (Sevounts 2017).

VPN on puolestaan edullisempi verrattuna MPLS-tekniikkaan liikenteen kulkiessa julkisen internetin kautta. VPN voi siis vaihtoehtona MPLS:lle olla edullisempi ja nopeampi pystyttää, mutta QoS voi toteutua odotettavasti huonommin julkisen internetin ongelmista johtuen. VPN:kin vaatii silti konfigurointia jokaisen toimipisteen verkkolaitteilta uuden toimipisteen syntyessä ja verkkojen määrän kasvaessa.

Kuvitellaan, että yritys on päättänyt käyttää verkossaan edullisia VPN-tunneleita, jotka yhdistävät yrityksen 10 toimipistettä. Yritys on päättänyt yhdistää kaikki toimipisteet toisiinsa, eli käyttää full-mesh-verkkotopologiaa. Tässä tapauksessa point-to-point tunneleita toimipisteiden välillä olisi 45, perustuen yhtälöön (n * (n - 1) / 2), jossa muuttuja n on toimipisteiden määrä (CiscoNET 2010). Toimipiste #11 perustetaan, ja nyt jokaisen toimipisteen konfiguraatioon on tehtävä muutoksia. Perinteisessä järjestelmässä nämä muutokset on tehtävä erikseen jokaiselle laitteelle. Työn määrä vain kasvaa toimipisteiden lisääntyessä; suuremmissa yrityksissä voi toimipisteiden määrä olla useissa kymmenissä tai jopa sadoissa. Samankaltaiseen implementointiongelmaan törmätään, kun yritys haluaa esimerkiksi muuttaa palomuuriensa konfiguraatiota, ja uudet säännöt on määriteltävä

jokaiselle toimipisteen palomuurille erikseen. On kuitenkin huomioitava, että yrityksissä jotka käyttävät star-verkkotopologiaa, uuden toimipisteen konfigurointi ei olisi lainkaan yhtä työlästä. Tällaisessa toteutuksessa sivutoimipisteet yhdistetään yhteen pisteeseen, esimerkiksi pääkonttoriin, jolloin kaikki liikenne toimipisteiden välillä kulkee sen kautta. Vaikka tämä voikin liikennettä keskipisteen kohdalla ruuhkauttaa, voi tämä olla suotavampi vaihtoehto kuin full-mesh-verkon konfigurointi ja ylläpito.



Kuva 1: Star- ja full-mesh -verkkotopologiat.

3 SD-WAN

Tässä luvussa tutustutaan SD-WAN:iin käsitteenä sekä SD-WAN -tekniikan käyttöön. Käymme myös läpi ominaisuudet joita järjestelmän tulee pitää sisällään, että se voidaan määritellä SD-WAN:iksi.

3.1 Määritelmä

SD-WAN, eli software-defined wide-area network, tarkoittaa karkeasti suomennettuna ohjelmistolla määritettyä laajaverkkoa (Butler 2017). Tästä uudesta verkotusteknologiasta alettiin käyttää verkotusjulkaisuissa SD-WAN -termiä ensimmäistä kertaa vuonna 2014 (Banks 2014). Tiivistettynä SD-WAN -tekniikan tarkoituksena on yksinkertaistaa WAN:in eli laajaverkon hallintaa, vähentää kuluja sekä olla joustava (Banks 2014).

3.2 SD-WAN ominaisuudet

3.2.1 Keskitetty hallinta

SD-WAN yksinkertaistaa laajaverkon toimintaa tiivistämällä verkkolaitteiden hallinnan yhden käyttöliittymän perään. Tätä kutsutaan myös linkkiaggregaatioksi. SD-WAN:illa voi ottaa haltuun WAN-laitteiden hallinnan ja eriyttää ne yhden käyttöliittymän alle. Eriytyksestä käytetään englannissa termiä decouple. Keskitetyn hallinnan tarkoituksena on helpottaa verkkolaitteiden konfigurointia sekä hallintaa. Tämä on suoraan verrattavissa SDN-verkkoarkkitehtuuriin (Software-Defined Network), jota käytetään lähinnä tietoliikennekeskuksissa, kuten konesaleissa, kouluissa tai yritysten pääkonttoreissa, joissa

toimitaan laajempien sisäverkkojen kanssa. SD-WAN toimii SDN:n tapaisesti, erottamalla hallintatason tietoliikennetason toiminnasta ja siirtäen sen yhden käyttöliittymän taakse verkossa, näin yksinkertaistaen muutosten tekoa, kun hallinnassa on useampia laitteita. (Butler 2017.)

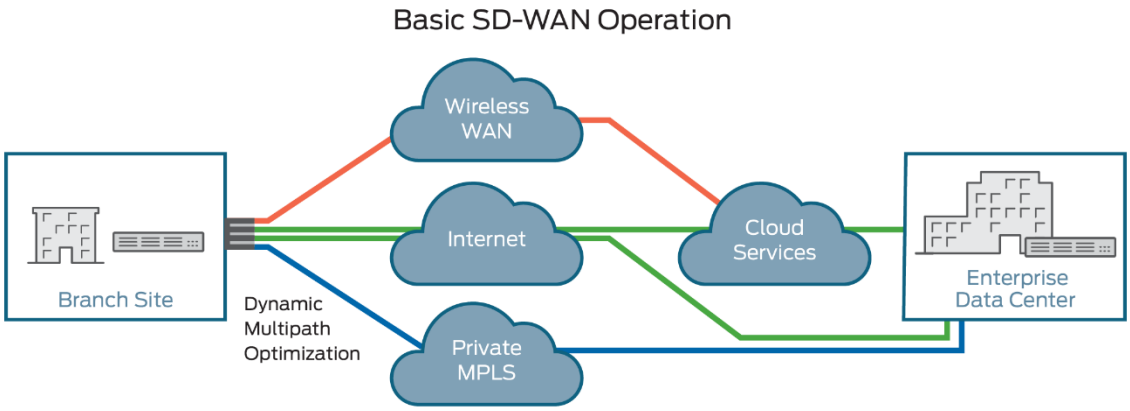
SD-WAN:in tulee myös tukea verkon lisälaitteita. Näihin kuuluvat esimerkiksi palomuurit ja WAN-optimointilaitteet (Lerner 2015).

3.2.2 Kuljetusagnostisuus

Toinen SD-WAN:in pääpiirteistä on sen kyky hyödyntää erityyppisiä yhteyksiä liikenteen siirtämiseen. Tuettuihin yhteystyyppeihin kuuluvat muun muassa peruslaajakaistaliittymät, 4G ja MPLS-tekniikalla toimivat yhteydet. (Butler 2017.) Tästä ominaisuudesta käytetään myös hienostunutta termiä kuljetusagnostisuus (Khan 2016).

3.2.3 Multipath-tekniikka

Multipath-tekniikka viittaa siihen, että SD-WAN kykenee käyttämään useaa yhteyttä samaan aikaan (Gintert 2018). Kohteen käytössä voisi siis olla esimerkiksi sekä laajakaista- että 4G-liittymä, jolloin liikenne voi kulkea molempien läpi halutulla tavalla.



Kuva 2: Diagrammi SD-WAN verkkoarkkitehtuurista (SDxCentral 2018)

3.2.4 VPN-verkko

SD-WAN:in tulee kyetä luoda turvallinen VPN-verkko (Lerner 2015). SD-WAN:in tulee pystyä konfiguroimaan käytössä olevien yhteyksien päälle VPN-tunnelit, jolloin yhdistettyjen verkkojen kokonaisuus muistuttaa esimerkiksi full-mesh VPN-verkkoa (Khan 2016). Testissä käyttämämme Fortinetin SD-WAN tukee myös star-verkkotopologiaa.

3.2.5 Kuormituksen tasapainotus

SD-WAN:in ominaisuuksiin kuuluu myös kuormituksen tasapainottamiskyky, josta käytetään englanniksi termiä load balancing. Käytännössä tämä tarkoittaa sitä, että yhteydessä kulkevaa dataliikennettä voidaan siirrellä eri linjojen välillä, välttäen yksittäisen linjan saturointia. Liikennettä voi myös priorisoida esimerkiksi ohjelmalle määritellyn tärkeyden perusteella. Jos käytössä on useampia liittymiä, voidaan liikenteen kaistoja myös vaihdella niiden ruuhkan perusteella ohjelmakohtaisesti. (Garson 2016.)

Kuvitellaan esimerkiksi, että VoIP-liikenteen oletuksena käyttämällä kaistalla on poikkeuksellisen korkea latenssi. SD-WAN:lle voi olla määritettynä sääntö ohjata VoIP-ohjelman liikenne toiselle kaistalle, jos oletuskaistan latenssi nousee yli 100 ms. Säännön ollessa voimassa SD-WAN voi dynaamisesti ohjata liikenteen parhaalle mahdolliselle reitille tarkkailemalla verkon linkkien tiloja, ja siirtää sen takaisin oletuskaistalle sen latenssin normalisoituessa.

3.3 SD-WAN -toteutusten väliset erot

Tässä luvussa käymme läpi eri tarjoajien SD-WAN -tuotteiden eroja. Eri toteutuksia ei voi suoranaisesti luokitella paremmiksi tai huonommiksi, vaan hyödyt riippuvat lähinnä ostajan tarpeista. Objektiivisempia QoS-eroja toteutusten toiminnassa tutkitaan luvun lopussa.

Yksi mainostetuimmista eroista SD-WAN -toteutusten välillä on käyttöönoton helppous. Esille nousee etenkin termi ZTP, eli zero touch provisioning (English 2017). Tästä käytetään myös termiä zero touch deployment. ZTP viittaa laitteiden automaattiseen konfigurointiin, kun ne lisätään verkkoon. Ominaisuuden tarkoituksena on vähentää työn määrää ja johtaa järjestelmän nopeampaan pystyttämiseen. (Rouse 2016.)

SD-WAN -tuotteesta kiinnostuneen kannattaa myös ottaa huomioon tuotteen tukemat reititystekniikat ja -protokollat. Ostajan kannattaa esimerkiksi varmistaa, mitä reititysprotokollia SD-WAN -tuote tukee, kuten BGP:tä (Border Gateway Protocol) tai OSPF:ää (Open Shortest Path First) ennen lopullista valintaa. (English 2017.) Muun muassa Ciscon SD-WAN tukee myös omaa prokollaansa OMP:tä (Viptela Overlay Management Protocol) (Cisco 2016). Näiden lisäksi on huomioitava, että esimerkiksi IPv6-kommunikaatioprotokolla (Internet Protocol version 6) ei ole kaikkien SD-WAN -toteutusten tukema (English 2017).

SD-WAN:ista pilvipalveluna kiinnostuneiden tulee myös ottaa huomioon tuotteiden tukemat pilvipalvelualustat. Valtaosa SD-WAN–toteutuksista tukee pilvipalvelualustoinaan AWS:ää (Amazon Web Services), Google Cloudia ja Azurea. (English 2017.)

Jotkut SD-WAN -toteutukset on saatavilla fyysisinä laitteina, jotkut taas virtuaalisina (English 2017). Esimerkiksi SD-WAN voi toimia fyysisenä lisälaitteena yrityksen sisäverkossa, kuten

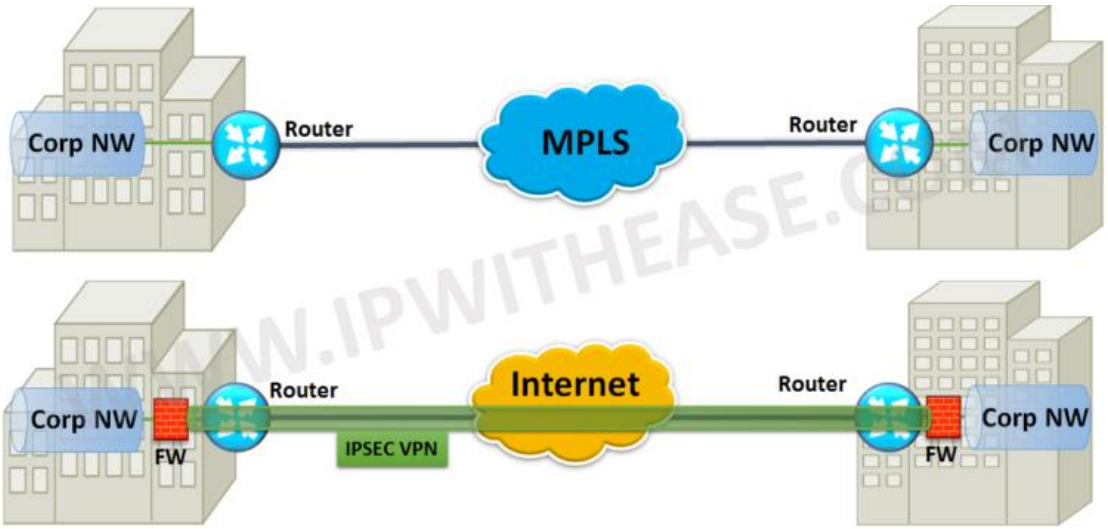
Fortinetin FortiManager, tai virtuaalilaitteena (Fortinet 2018). Jotkin nykyiset SD-WAN -toteutukset, kuten Riverbedin SteelConnect, ovat saatavilla pilvipalveluna (Riverbed 2016).

SD-WAN -teknologiassa löytyy myös tuotekohtaista liikenteen seurantaa ja hallintaa. Joistakin toteutuksista löytyy hallintajärjestelmä itsessään, kun taas jotkut toteutukset käyttävät kolmannen osapuolen ohjelmia työkaluinaan (English 2017). Tarkemman hallinnan ja liikenteenseurannan tarve liittyy lähinnä ostajan toiveisiin, ja ei ole välttämätön, jos esimerkiksi käyttäjä haluaa pitää SD-WAN:in käytön mahdollisimman yksinkertaisena ja automatisoituna.

SD-WAN:in tarjotessa näkymän omaan toimintaansa, kuten kaistojen käyttöön ja ohjelmakohtaiseen kuormitukseen, voi tämä ominaisuus olla hyödyllinen myös palvelun loppukäyttäjälle. Valmiin SD-WAN -tuotteen hallintanäkymä voidaan esimerkiksi tarjota pääteasiakkaalle vain-luku muodossa, jossa verkon sääntöjä ja liikennettä voidaan seurata. Mikäli tällainen näkyvyys on pääteasiakkaan tarpeissa, voi SD-WAN olla asiakkaalle esimerkiksi MPLS:ää mieleisempi vaihtoehto, jonka liikennöintiin ja statistiikkaan ei ole mitään suoraa näkymää loppuasiakkaan puolelta.

NSS Labsin suorittamassa tutkimuksessa verrattiin SD-WAN -toteutusten eroja, joissa arvioinnin kohteet olivat VoIP:in QoS ja videoiden QoE (Quality of Experience), eli kokemuksen laatu. Tutkimuksessa selvitettiin, kuinka hyvin sovellusten toiminta säilyy tarkoitettuna SD-WAN -toteutusta hyödyntävässä verkossa. Esimerkiksi, jos priorisoidun VoIP-liikenteen laatu kärsi ruuhkauttaessa linjaa, aiheuttaen soitoissa pätkintää ja huonoa äänenlaatua, sai SD-WAN -tekniikka vähemmän pisteitä. (Skybakmoen 2018). Fortinetin SD-WAN sai kyseisestä tutkimuksesta hyvät arvosanat, joka on yksi syistä miksi se valittiin testattavaksi tässä työssä.

3.4 SD-WAN:in suhde MPLS- ja VPN-tekniikoihin



Kuva 3: MPLS- ja VPN-arkkitehtuurit. (IP With Ease 2017)

3.4.1 MPLS

On yleistä nähdä SD-WAN asetettuna vastakkain sitä vanhemman MPLS-tekniikan kanssa (SDxCentral 2018). MPLS:ää käytetään monissa yritysverkoissa ja tutustumme siihen lyhyesti verrataksemme sitä SD-WAN:in toimintaan.

MPLS-tekniikan tarkoituksena on luoda kohteiden välille yksityinen, mahdollisimman korkean QoS:n reitti. Datapakettien ensimmäisiin bitteihin liitetään lyhyt etiketti jota kutsutaan FEC:ksi (Forwarding Equivalence Class), jonka perusteella MPLS-reitittimet ohjaavat paketit eteenpäin. Tällaista reititystä nopeuttaa se, ettei reitittimen tarvitse analysoida koko pakettia ja selvittää sille reittiä, vaan lukea läpi lyhyt FEC-tunnus, jonka avulla selviää paketin seuraava määränpää jo valmiiksi määritettynä. (Weinberg & Johnson 2018.)

MPLS-liikenne ei lähtökohtaisesti ole salattua niin kuin VPN:issä, mutta se luokitellaan turvalliseksi kuljetukseksi, sillä se ei kulje julkisen IP-verkon kautta ollenkaan, vaan pakettien etikettien määrittelemän reitin mukaisesti. Tämä myös tarkoittaa sitä, ettei MPLS ole haavoittuvainen esimerkiksi palvelunestohyökkäyksille. Näistä hyökkäyksistä käytetään termiä DDoS. MPLS:n suoja DDoS:lta johtuu siitä, että hyökkääjällä ei ole julkista IP-osoitetta, johon voisi kohdistaa hyökkäyksensä. (Weinberg & Johnson 2018.) MPLS-yhteyksiä on saatavilla myös salaksella, kuten IPsecillä, MPLS VPN:n muodossa. MPLS VPN ei itsessään tarkoita, että yhteys olisi salattu, vaan että VPN-putki on luotu olemassaolevan MPLS-verkon ylle. (Brandenburg 2010.)

Keskivertohintaa on vaikeaa MPLS:stä arvioida, sillä palvelun hinta riippuu laajalti palvelun tarjoajasta, yhteyden nopeudesta, toimitussijainnista sekä lisäominaisuuksista. Erittäin

suurena vaikuttajana on myös, mikäli yhteys ylittää valtioiden rajoja ulkomaille. (Garson 2017.) Odotettavissa kuitenkin on, että MPLS-yhteydestä saa maksaa moninkertaisen määrän verrattuna tavanomaiseen laajakaistayhteyteen (Gottlieb 2012).

Vaikka MPLS-tekniikka on myös käytettävissä SD-WAN:in rinnalla, SD-WAN:illa voi käyttää julkista internettiä kulkuvälineenä, eli esimerkiksi laajakaista- tai 4G-yhteyttä. Vaikka hyvä syy MPLS:n kokonaiseen korvaamiseen on sen hinta, on kuitenkin huomioitava, että reititys julkisen internetin kautta on korkeista ja suhteellisen edullisista nopeuksista huolimatta altis latenssille, jitterille ja pakettihukalle eri tasolla kuin MPLS-tekniikka. Latenssilla viitataan viivettä paketin kulussa paikasta toiseen, jitterillä pakettien saapumisvälien eroon ja pakettihukalla datapakettien hukkumista matkalla määränpäähänsä. Yhdysvaltalaisen arvion mukaan, julkisessa internet-yhteydessä linjan luotettavuus oli vuonna 2012 noin 99%. Luotettavuudella tarkoitetaan keskivertoa todennäköisyyttä, että paketti saavuttaa määränpäänsä onnistuneesti. MPLS-yhteyden kohdalla luotettavuuden todettiin olevan noin 99,99% luokkaa. (Gottlieb 2012.) Mikäli QoS:n ehdoton toteutuminen on tärkeää liittymän hakijalle, on MPLS-tekniikka yhä nykyaikana merkityksellinen.

Linjan ongelmat, kuten aiemmin mainitut latenssi, jitter ja pakettihukka vaikuttavat huomattavimmin reaaliaikaisesta liikenteestä riippuviin sovelluksiin, kuten VoIP-puheluihin, suoratoistoon sekä tietokoneiden etähallintaan. Tämä tarkoittaa pääosin UDP-pohjaista (User Datagram Protocol) liikennettä, jossa ei seurata eikä korjata virheellisiä tai saapumattomia paketteja (Rouse 2014). Esimerkiksi VoIP-käytössä, pakettihukka aiheuttaa puhelun pätkimistä, jitter vaikuttaa äänenlaatuun ja korkea latenssi saa soittajat helposti puhumaan päällekkäin (Vouzis 2016). Myös videoiden suoratoistosta voi tulla näiden ongelmien ilmetessä vaikeasti katseltavaa puuroa. MPLS voi siis reaaliaikaisten sovellusten kohdalla olla itsessään hieman luotettavampi vaihtoehto kuin julkisen internetin kautta kulkevat yhteydet, mikäli sovellusten virheetön toimivuus on yrityksen käytössä kriittistä. On kuitenkin huomioitava, että suuri osa yritysten internet-toiminnasta ei välttämättä vaadi reaaliaikaista dataliikennettä. Tällaiseen toimintaan sisältyvät muun muassa tiedostojen siirto, sekä sähköposti- ja selainkäyttö.

Verkon ongelmia, kuten latenssia ja pakettien putoilua voidaan siis SD-WAN:in avulla vältellä ilman MPLS-yhteyttä. Ylimääräisellä yhteydellä, kuten esimerkiksi toisen operaattorin laajakaistalla, joka käyttää toista kaapelireittiä, voi SD-WAN siirtää herkemmät prosessit paremmin toimivalle kaistalle. Vaikka tämä ei julkisen verkon ongelmia kokonaan korjaisi, voisi kuitenkin olettaa tämän ehkäisevän niistä aiheutunutta haittaa.

Toisin kuin SD-WAN:in markkinointi voi antaa ymmärtää, MPLS-tekniikalla on vielä sijansa verkotuksessa, eikä SD-WAN voi sen QoS:n tasoa kokonaan korvata. SD-WAN voi hyvinkin johtaa edullisempiin verkkoratkaisuihin vähentämällä MPLS-kaistan kapasiteetin tarvetta,

esimerkiksi oheisella laajakaista- tai 4G-liittymällä, jonka kautta ei-reaaliaikainen liikenne voidaan ohjata. Valtaosan liikenteestä voisi ohjata esimerkiksi laajakaistayhteyttä pitkin MPLS:n toimiessa eräänlaisena prioriteettilinjana.

3.4.2 VPN

Seuraavaksi tarkastelemme hieman VPN:ien toimintaa. VPN-yhteydessä lähtevä liikenne salataan, ja tämän salauksen ihanteellisesti pystyy purkamaan vain sen tarkoitettu vastaanottaja. Paketit, jotka eivät ole peräisin varmennetusta kohteesta, pudotetaan (Sturt 2018). VPN-tekniikka voi kuitenkin olla vahingoittuvainen julkisen internetin ongelmille, kuten odottamattomille tukoksille ja DDoS:lle (Distributed Denial of Service), eli palvelunestohyökkäyksille. Nykyajan merkityksellisimpiä VPN-teknologioita ovat muun muassa OpenVPN, L2TP/IPsec, IKEv2 ja SSTP. (Bischoff 2016.)

Yksi käytetyimmistä VPN-tekniikoista on OpenVPN. Se toimii monien VPN-palveluiden oletusprotokollana. OpenVPN:n on hyvin konfiguroitavissa. Se tukee useita salaustekniikoita, kuten AES:ää sekä eri porttien käyttöä, joka auttaa piilottamaan VPN-liikennettä, tehden siitä palomuureille vaikeamman torjua. (Hoffman 2015.)

SD-WAN:in muodostaman laajaverkon arkkitehtuuri on samanlainen kuin full-mesh VPN –verkkotopologia. Tämä tarkoittaa sitä, että kaikki lähiverkot laajaverkossa on yhdistetty toisiinsa. Käytännössä SD-WAN:in ero full-mesh VPN:ään ovat SD-WAN:in sisältämät muut lisäominaisuudet. (Khan 2016.)

VPN voi olla hyvä vaihtoehto käyttäjille, jotka haluavat edullisen tavan suojata verkkoliikenteensä julkisuudelta. Verrattuna SD-WAN:iin, pelkkä VPN-palvelu voi olla kustannustehokkaampi riippuen loppukäyttäjän tarpeista. Esimerkiksi jos linjan ohjelmakohtainen suorituskyky ei kuulu ostajan tarpeisiin, ja ostajalla ei ole aikeita käyttää useampaa kuin yhtä liittymää kohteessaan, voi SD-WAN:illa toteutettu verkko olla tarpeeton.

VPN:t eivät kuitenkaan tarjoa keinoja hallita WAN:ia tai ohjata liikennettä älykkäästi, johon SD-WAN kykenee. SD-WAN -tekniikka on laajalti tarkoitettu käyttäjille, joille tyypillinen VPN-palvelu ei riitä.

3.5 Taloudelliset vaikutukset

SD-WAN -tekniikka syntyi isojen yritysten tarpeesta kasvattaa, hallita ja käyttää laajaverkkoja sekä edullisemmin että tehokkaammin. ICT-alan tutkimusyritys Gartner arvioi Yhdysvalloissa, että perinteisellä järjestelmällä 250-haaraisen laajaverkon kustannukset olisivat noin 1 285 000 dollarin tasolla kolmessa vuodessa, kun taas SD-WAN –toteutuksella kustannusten arvioitiin olevan vain 452 500 dollaria samanlaisessa laajaverkossa. (Butler 2017.) IDC:

mukaan SD-WAN:in käyttöönotto tulee yhä suurempaan kasvuun, ja arvioi, että teknologia tulee ylittämään 6 miljardia dollaria tuloissa maailmalla vuonna 2020 (Cato Networks, 2017).

Costs for SD-WAN

Example: Three-Year Costs for 250-Branch WAN		
Item	Traditional	SD-WAN
Router Capex	$1,000,000	$250,000
Router Maint/Support	$180,000	$150,000
Staffing Opex	$105,000	$52,500
Total	$1,285,000	$452,500

Kuva 4: Arvio laajaverkkokuluista (Gartner 2017)

On kuitenkin huomioitava, kehen SD-WAN:in taloudelliset hyödyt todella kohdistuvat. SD-WAN voi vähentää loppukäyttäjän kuluja verrattuna MPLS-yhteyteen, mutta hyötyykö tästä internetpalveluntarjoaja? Internetpalveluntarjoaja voi SD-WAN -tekniikalla laajentaa tuotevalikoimaansa, mutta on vaikeaa arvioida, tulisiko tästä juurikaan enempää voittoa kuin MPLS-yhteyden toteutuksesta. Tietenkin, jos jokin loppuasiakkaan toimipisteen sijainti on hyvinkin syrjäinen, voi MPLS-yhteyden tuottaminen järkevään hintaan olla lähes mahdotonta. Tällöin SD-WAN voi olla hyödyllinen vaihtoehto myös internetpalveluntarjoajalle, joka voi tässä tapauksessa saada asiakkaan, jota ei pelkillä MPLS-tuotteilla saisi.

4 Tutkimus

SD-WAN -testi tehtiin yrityksen verkossa. Kokeessa päätettiin käyttää Fortinetin laitteita, sillä yrityksellä oli niitä hallussa ja niiden käytöstä oli työntekijöillä aiempaa kokemusta.

Kokeen tarkoituksena oli testata osaa SD-WAN:in ominaisuuksista. Kokeessa simuloitiin laajaverkkoa, johon sisältyivät kuvitteellisen yrityksen näennäinen pääkonttori ja etäkonttori. Konttorit oli tarkoitus yhdistää FortiGate-palomuureilla käyttäen SD-WAN -tekniikkaa niiden hallinnoimiseen. Pääkonttorin verkossa käytettiin kuitu- sekä 4G-yhteyttä, ja etäkonttorissa käytettiin kuituyhteyttä. FortiManager-hallintalaite asennettiin virtuaalipalvelimelle.

Kokeessa käytettiin kolmea Fortinetin laitetta SD-WAN -ympäristön rakentamiseen.

— FortiManager-VM64-KVM, virtuaalinen hallintalaite

- FortiGate-60E, palomuuri
- FortiGate-30E, palomuuri

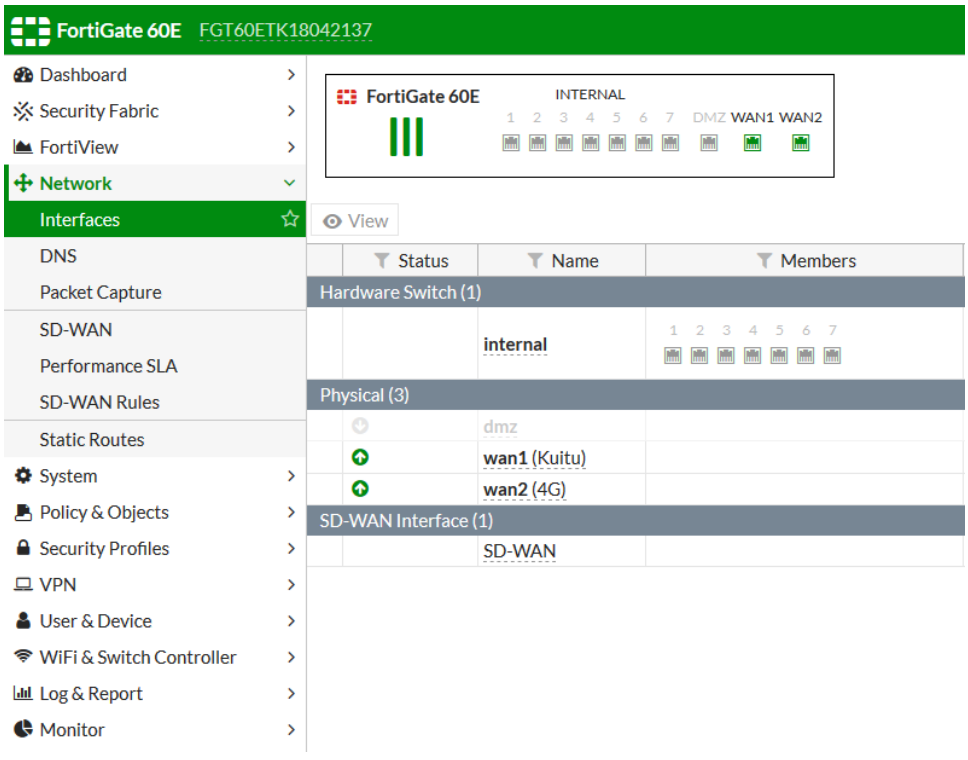
Tutkimuksen tavoitteina oli pystyttää palomuurit sekä hallintalaite onnistuneesti, testata hallintalaitteen käyttöliittymän toimintaa sekä lisätä palomuurit hallintakokonaisuuteen, käytännössä testaten SD-WAN:in keskitetyn hallinnan ominaisuutta. Tarkoituksena oli myös ohessa kokeilla kuormituksen tasapainotusta, multipath-tekniikkaa, erityyppisten liittymien tukea, sekä hallintalaitteen tarjoamia VPN-ominaisuuksia.

4.1 Tutkimuksen toteutus

Aloitimme Fortigate-palomuurien valmistelulla SD-WAN:ia varten. Palomuureissa oli oma konfiguraatio jo ennalta, joten ne oli ensiksi resetoitava tehdasasetuksille. Kirjauduimme muurien käyttöliittymiin sisäverkon kautta. Palomuureissa laitettiin käyttöön “SD-WAN interface”, ne liitettiin verkkoon ja ne saivat DHCP:n kautta julkiset IP-osoitteet. Tämän jälkeen konfigurointia jatkettiin etähallinnan puolelta julkisten IP:iden kautta.

4.1.1 Kuljetusagnostisuuden testaus

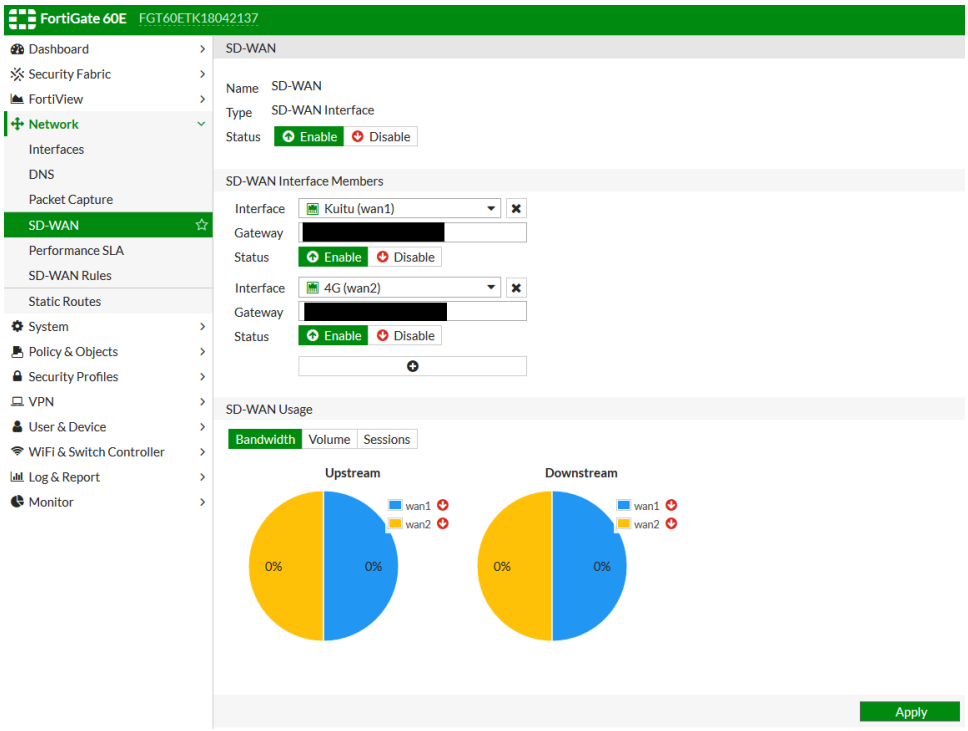
Erityyppisten liittymien toimivuus testattiin pääkonttorin laitteella. WAN-linkit seuraavassa kuvassa osoittavat sekä 4G- että kuituyhteyden toimineen.



Kuva 5: Kuvakaappaus fyysisistä liittymistä.

4.1.2 Multipath-tekniikan testaus

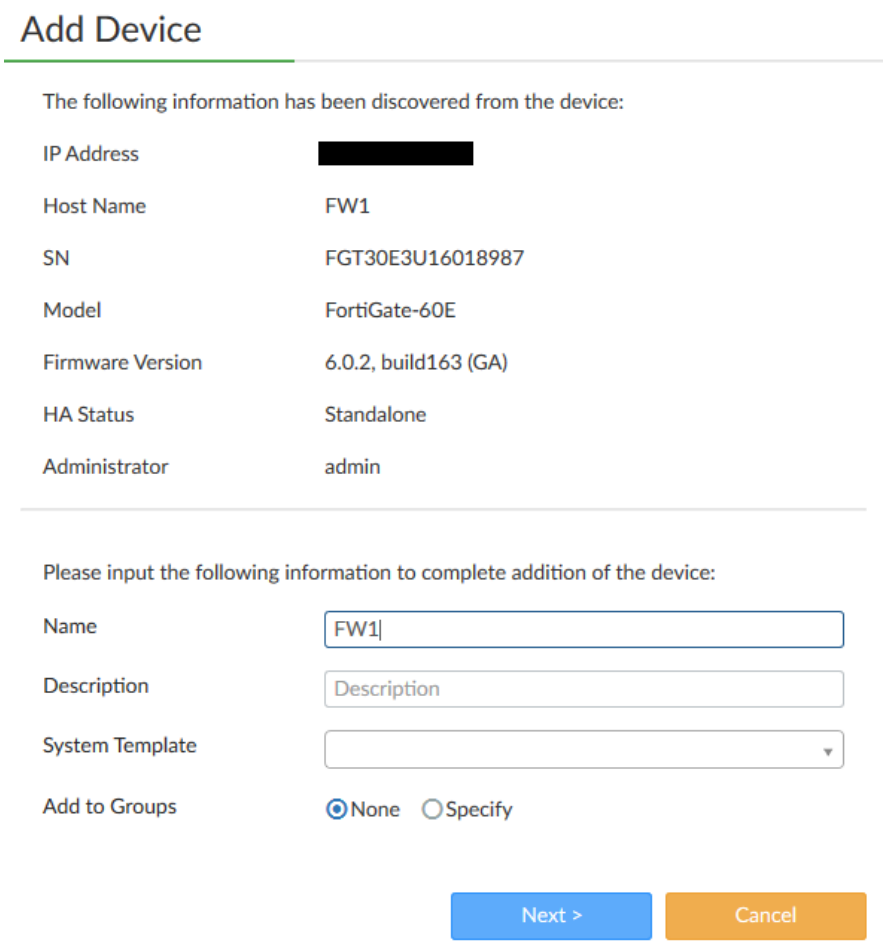
Saatuamme WAN-linkit pystyyn, lisäsimme pääkonttorin palomuurin 4G- ja kuituliittymän SD-WAN -kokonaisuuteen. Liittymien liikennettä voi monitoroida nopeuden, kuljetetun datan määrän tai hetkellisten sessioiden määrän perusteella. Asetuksia ei vielä ole viimeistelty, jonka vuoksi liikennettä ei vielä kulje.



Kuva 6: Kuvakaappaus liittymän läpi kulkevasta liikenteestä.

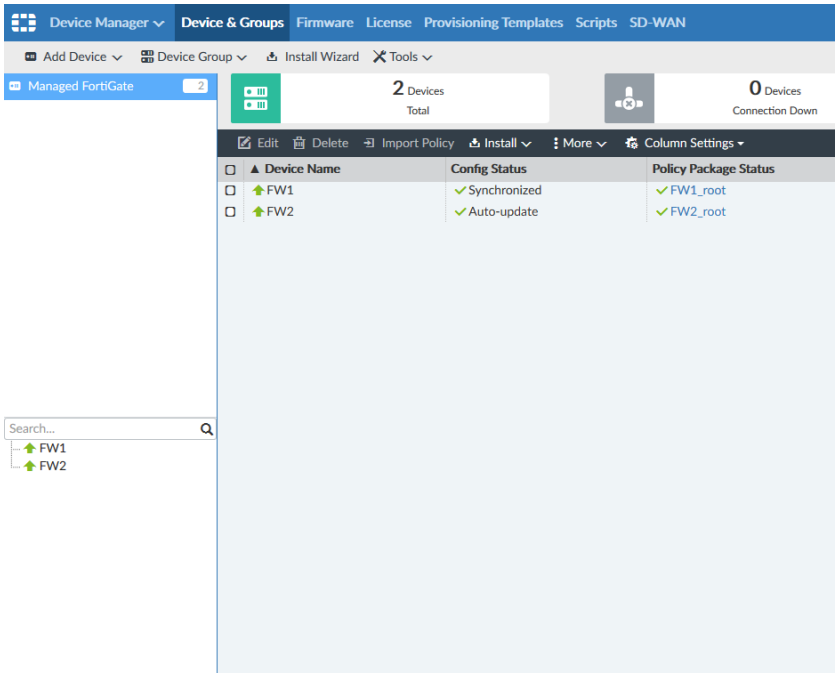
4.1.3 Keskitetyn hallinan testaus

Seuraavaksi kirjauduimme FortiManageriin, SD-WAN:in hallintalaitteeseen, ja aloitimme hakemalla FortiGaten palomuureja Device Manager -käyttöliittymästä. Laitteiden julkiset osoitteet syötettiin Device Managerille ja niille määritettiin nimet FW1 ja FW2, joissa FW1 vastasi pääkonttorin ja FW2 etäkonttorin palomuuria.



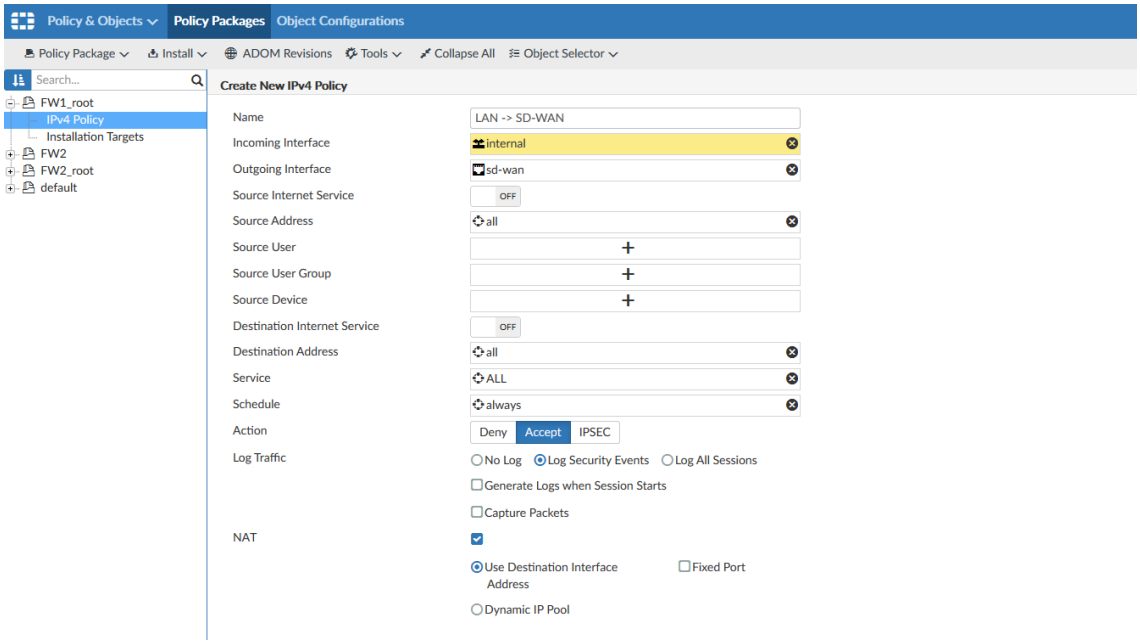
Kuva 7: Kuvakaappaus palomuurin lisäyksestä FortiManageriin.

Hallintalaite löysi palomuurit verkosta ja ne lisättiin hallintaan. Palomuurien konfiguraatiota pystyi nyt muuttamaan suoraan hallintalaitteesta käsin.



Kuva 8: Kuvakaappaus onnistuneesti lisätyistä laitteista.

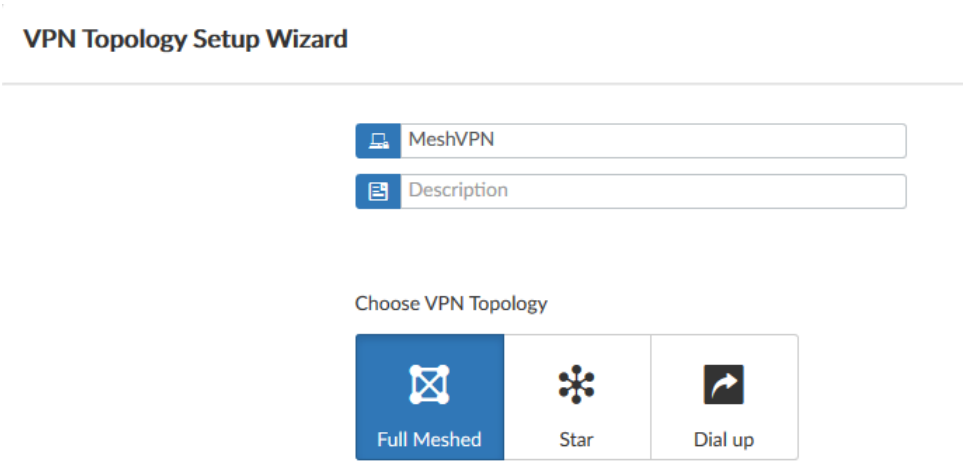
Nyt kun keskitetty hallinta oli toiminnassa, Policy & Objects -käyttöliittymän kautta pystyi luomaan palomuureille sääntöpaketteja ja kohdistamaan niitä halutuille laitteille Import Policy -painikkeella. Loimme esimerkiksi säännön, joka sallii kaiken liikenteen sisäverkosta SD-WAN:iin päin.



Kuva 9: Kuvakaappaus palomuurisännön luomisesta.

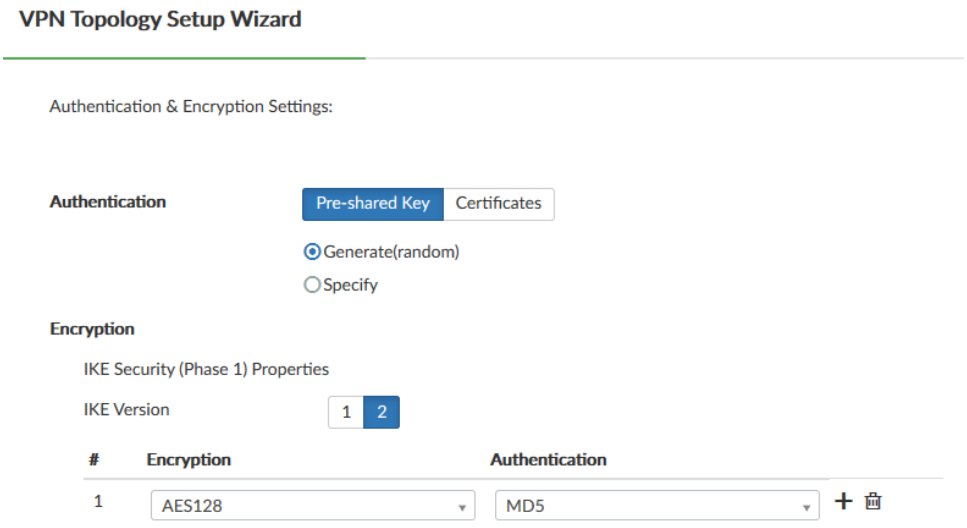
4.1.4 VPN:n testaus

Tässä vaiheessa vilkaisimme myös hallintalaitteen VPN-ratkaisuja. Tähän FortiManager tarjoaa VPN Manageria. VPN:n luonti aloitettiin topologian konfiguroimisella, luoden niin sanottu VPN-yhteisö.



Kuva 10: Kuvakaappaus VPN-topologian valinnasta.

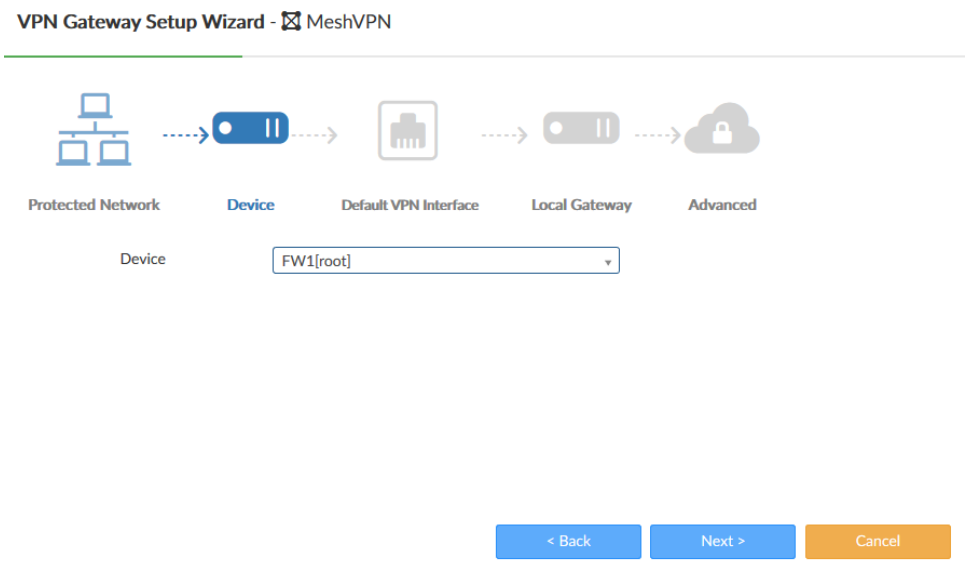
VPN Manageriin syötettiin myös yhteisön haluttu autentikointi- ja salausmuoto.



Kuva 11: Kuvakaappaus VPN-salauksen valinnasta.

Kun VPN-yhteisö oli pystyssä, voitiin siihen lisätä halutut verkot. Tämäkin onnistui VPN Managerin kautta, VPN Gateway Setup Wizardista. Keskitettyyn hallintaan lisätyt FW1 ja FW2

löytyivät täältä. Ohessa ohjelmaan syötettiin myös suojatun verkon tiedot sekä oletus VPN-liittymä, johon laitettiin tässä tapauksessa SD-WAN.

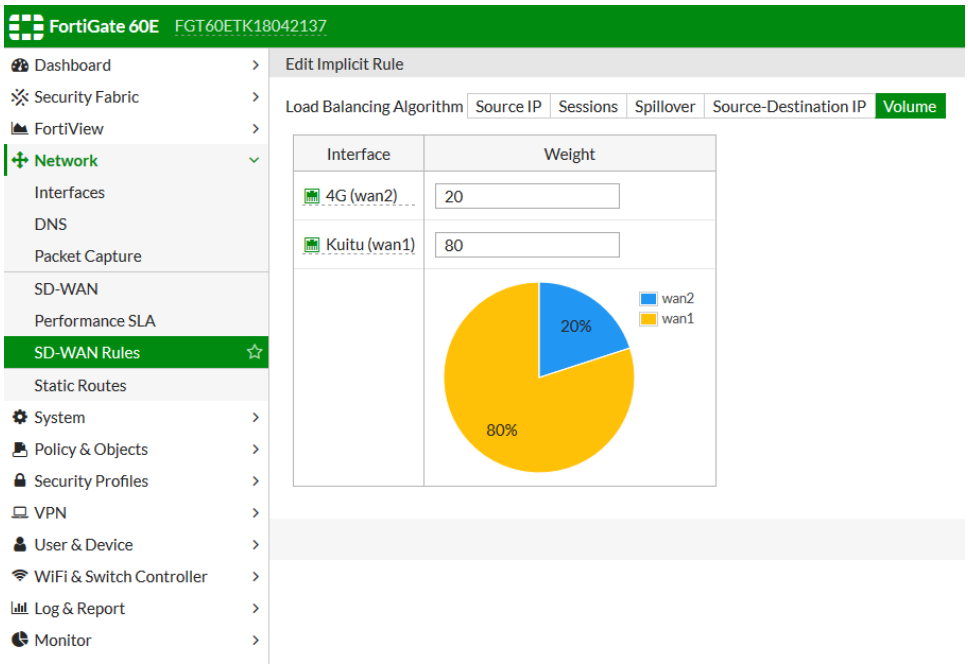


Kuva 12: Kuvakaappaus palomuurin lisäämisestä VPN-yhteisöön.

VPN-konfiguraation luotuamme se voitiin asentaa FW1:lle ja FW2:lle keskitetyn hallinnan kautta. Tässä vaiheessa luodun VPN:n käyttöön tuli vaikeuksia, eikä sitä saatu toimimaan. Tarkoituksena ei kuitenkaan siihen ollut VPN:iin syvemmin perehtyä, vaan tämä jätettiin avoimeksi myöhempää jatkotutkintaa varten.

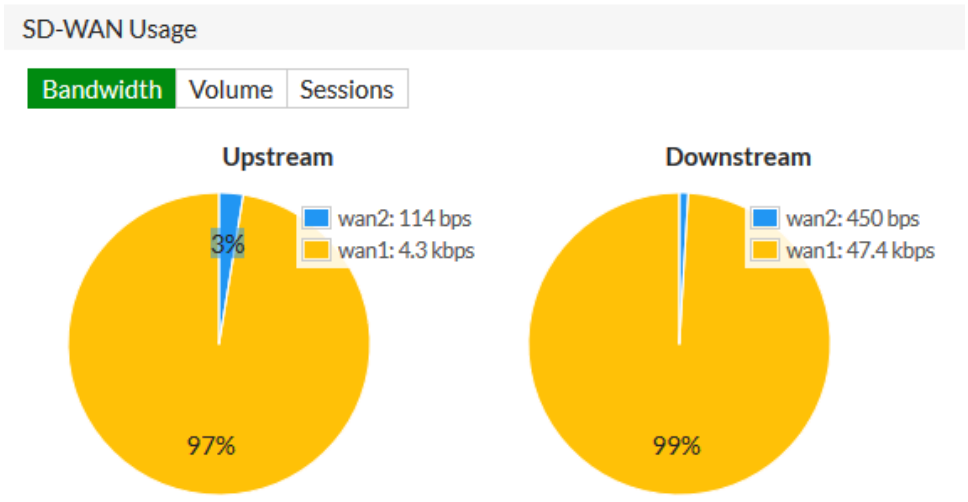
4.1.5 Kuormituksen tasapainotuksen testaus

Lopuksi testaamme vielä SD-WAN:in kuormituksen tasapainotusta. Fortinetin SD-WAN kykenee jakamaan kaistan käytön halutun kokoisiin osiin, kuten esimerkiksi jos liittymien nopeudet olisivat 40 Mbps ja 10 Mbps, olisi jako tasainen liittymien osuuksien ollessa 75%/25%. Jaon voi myös tehdä useamman kuin kahden liittymän välillä. Päätimme tässä tapauksessa jakaa kaistan käytön kuitu- ja 4G-liittymien välillä 80%/20%, sillä kuidun nopeus oli testatessa noin 400 Mbps ja 4G:n noin 100 Mbps.



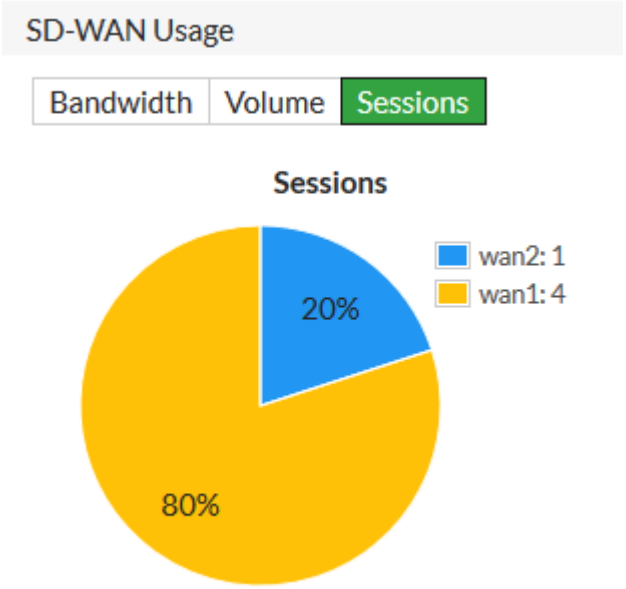
Kuva 13: Kuvakaappaus liittymien osuuksista kuormituksen tasapainotuksessa.

Huomasimme, että jaosta huolimatta kaistojen osuudet olivat epätasaiset, 97%/3%. Tämä johtui siitä, että palomuurin käsittelemien sessioiden määrä oli pieni.



Kuva 14: Kuvakaappaus liittymien läpi kulkevasta liikenteestä.

Kuten kuvasta voi huomata, liikenteen hetkellinen määrä oli minimaalinen. Sessioiden graafi puolestaan näyttää enemmän halutunlaiselta.



Kuva 15: Kuvakaappaus liittymien ylläpitämien sessioiden määrästä.

SD-WAN pyrkii pyöristämään liittymien käytön mahdollisimman tarkasti, mutta pienellä liikenteellä voivat erot määriteltyyn jakoon olla huomattavia. Esimerkiksi jos sessioita olisi vain kolme, jakaisi SD-WAN niistä kaksi kuidulle ja yhden 4G:lle kokeessa käytetyllä konfiguraatiolla. Liikenteen ja sessioiden määrän kasvaessa graafit pystyisivät kuitenkin noudattamaan haluttua jakoa tarkemmin.

5 Johtopäätökset

Monet tutkimuksessa testatut SD-WAN:in ominaisuudet toimivat onnistuneesti. Näihin sisältyivät tässä kokeessa keskitetty hallinta, multipath-tekniikka, erityyppisten liittymien tuki ja kuormituksen tasapainotus. Avoimeksi jäi VPN-verkon generoiminen, jota ei saatu saman tien toimimaan.

Tutkimuksessa ei törmätty erityisempiin ongelmiin SD-WAN:in käytön kanssa. Vaikeuksia järjestelmän rakentamisessa oli odotettua vähemmän, lukuun ottamatta sitä, kun omassa huolimattomuudessa konfiguroin itseni pois palomuurin etähallinnasta. Tämän korjaus tehtiin kuitenkin pikaisesti LAN:in kautta.

Jatkotutkimuksessa voisi testata esimerkiksi SD-WAN:in liittymän laadun monitorointia. Kokeessa SD-WAN voitaisiin ohjelmoida seuraamaan kahden liittymän pakettihukkaa ja latenssia ja vaihtelemaan käytettyä VoIP-ohjelmaa paremman välillä. SD-WAN:in VPN-toiminnan tutkiminen oli niukkaa. Tästä saisi myös helposti aiheen kattavampaa jatkotestiä varten.

Liittymien dynaamisen ohjelmakohtaisen vaihtelun testaus ei myöskään sisältynyt kokeeseen. Tätä voisi kokeilla manuaalisesti kuormittamalla liittymiä, ja katsoa mikäli SD-WAN onnistuu todellakin vaihtelemaan käytettyjä linkkejä halutulla tavalla.

6 Pohdinta

Kaiken kaikkiaan tutkimuksessa käsitellyt materiaalit osoittavat, ettei SD-WAN kaikissa tapauksissa ole täydellinen korvike MPLS-yhteyksille. Odotettavissa on, että MPLS:n käyttö tulee kuitenkin vähentymään SD-WAN:in käytön kasvaessa. MPLS-yhteyksistä on kuitenkin vielä hyötyä niiden korkean QoS:n vuoksi, eikä SD-WAN tätä kykene korvaamaan. SD-WAN:in avulla kuluja voitaisiin kuitenkin säästää myös käyttämällä pienempikapasiteettista MPLS:ää.

Perinteinen manuaalinen VPN:n konfigurointi voi yhä olla pienyrityksille järkevämpi vaihtoehto SD-WAN:in sijaan. SD-WAN -palvelun tarjoamat ominaisuudet eivät välttämättä ole tarpeellisia tai tehokkaita pienemmän verkon hallinnoimiseen, kun SD-WAN:in lisäkulut otetaan huomioon. SD-WAN on kuitenkin hyvä lisäys internet-palveluntarjoajan tuotevalikoimaan, sillä se voi saavuttaa asiakkaita, joita ei muuten tavoitettaisi.

SD-WAN -teknologialle löytyy siis sijaa markkinoilta, missä MPLS:n toteutus on vaikeaa, tai kun pelkkä perus-VPN ei riitä. Odotettavissa on, että lähitulevaisuudessa lähes kaikilta internetin operaattoreilta löytyy jonkinlainen SD-WAN -palvelu.

Lähteet

Sähköiset

Fortinet. 2019. FortiGate Secure SD-WAN. Viitattu 1.2.2019. https://www.fortinet.com/products/sd-wan.html

Rosoff, M. 2015. Which services use the most bandwidth? Viitattu 28.11.2018. https://www.businessinsider.com/which-services-use-the-most-bandwidth-2015-12?r=US&IR=T&IR=T

Kerravala, Z. 2010. How does cloud computing affect WAN bandwidth? Viitattu 29.11.2018. https://searchenterprisewan.techtarget.com/podcast/How-does-cloud-computing-affect-WAN-bandwidth

Rouse, M. 2016. WAN (wide area network). Viitattu 16.11.2018. https://searchenterprisewan.techtarget.com/definition/WAN

CiscoNET. 2010. How to calculate full mesh WAN links. Viitattu 29.11.2018. http://www.cisconet.com/wan/wan-general/443-how-to-calculate-wan-links.html

Butler, B. 2017. SD-WAN: What is it and why you'll use it one day. Viitattu 15.11.2018. https://www.networkworld.com/article/3031279/sd-wan/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html

Banks, E. 2014. Software-Defined WAN: A Primer. Viitattu 15.11.2018. https://www.networkcomputing.com/networking/software-defined-wan-primer/2018665838

Skybakmoen, T. 2018. SD-WAN Comparative Report. Viitattu 15.11.2018. https://www.fortinet.co.jp/doc/NSS-Labs-SD-WAN-Comparative-Report-Performance.pdf

SDxCentral. 2018. SD-WAN vs. MPLS: The Pros and Cons of Both Technologies. Viitattu 15.11.2018. https://www.sdxcentral.com/sd-wan/definitions/sd-wan-vs-mpls-pros-cons-technologies/

Garson, S. 2016. How Does SD-WAN Work? Viitattu 15.11.2018. https://www.sd-wan-experts.com/blog/how-does-sd-wan-work/

Gottlieb, A. 2012. Why does MPLS cost so much more than Internet connectivity? Viitattu 15.11.2018. https://www.networkworld.com/article/2222196/cisco-subnet/why-does-mpls-cost-so-much-more-than-internet-connectivity-.html

Dickle, B. 2018. Client-Side SD-WAN with IPsec VPN Deployment Scenario (Expert). Viitattu 15.11.2018. https://cookbook.fortinet.com/client-side-sd-wan-ipsec-vpn-deployment-example-expert/

Kerravala, Z. 2018. Understanding Virtual Private Networks [and why VPNs are important to SD-WAN]. Viitattu 15.11.2018. https://www.networkworld.com/article/3268744/internet-of-things/understanding-virtual-private-networks-and-why-vpns-are-important-to-sd-wan.html

Weinberg, N. & Johnson, J. 2018. MPLS explained. Viitattu 19.11.2018. https://www.networkworld.com/article/2297171/sd-wan/network-security-mpls-explained.html

Garson, S. 2017. MPLS Pricing: What's the Difference Between the Pricing Models. Viitattu 20.11.2018. https://www.sd-wan-experts.com/blog/mpls-pricing-whats-difference-pricing-models/

Sevounts, G. 2017. 5 Questions MPLS Providers Hope You Won't Ask. Viitattu 11.3.2019. https://www.aryaka.com/blog/5-questions-mpls-providers-hope-you-wont-ask/

Cato Networks. 2017. From VPN Internet Access to SD-WAN: An Evolution of Enterprise Networking. Viitattu 30.11.2018. https://www.catonetworks.com/blog/from-vpn-internet-access-to-sd-wan-an-evolution-of-enterprise-networking/

Rouse, M. 2014. UDP (User Datagram Protocol). Viitattu 20.11.2018. https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol

Vouzis, P. 2016. Impact of Packet Loss, Jitter, and Latency on VoIP. Viitattu 20.11.2018. https://netbeez.net/blog/impact-of-packet-loss-jitter-and-latency-on-voip/

English, J. 2017. Infographic: Compare the leading SD-WAN vendors before you buy. Viitattu 22.11.2018. https://searchsdn.techtarget.com/tip/Infographic-Compare-the-leading-SD-WAN-vendors-before-you-buy

Rouse, M. 2016. zero touch provisioning. Viitattu 22.11.2018. https://searchitoperations.techtarget.com/definition/zero-touch-provisioning-ZTP

Huntley, M. 2017. Business and bandwidth how much do you actually need. Viitattu 22.11.2018. https://www.mdsiinc.com/company/news/business-and-bandwidth-how-much-do-you-actually-need/

IBM Software. 2012. Managing the growing pains in today's expanding networks. Viitattu 22.11.2018. https://www-

935.ibm.com/services/multimedia/Managing_the_growing_pains_in_today_s_expanding_networks.pdf

Adobe Systems Incorporated. 2010. Adobe Flash Video File Format Specification Version 10.1. Viitattu 22.11.2018.
http://download.macromedia.com/f4v/video_file_format_spec_v10_1.pdf

Fildes, J. 2009. Flash moves on to smartphones. Viitattu 22.11.2018.
http://news.bbc.co.uk/2/hi/8287239.stm

Schroeder, S. 2015. You can watch an 8K video on YouTube — in theory. Viitattu 22.11.2018.
https://mashable.com/2015/06/10/youtube-8k-video/?europe=true#gnQNwhv5z8q2

Heathfield, S. 2018. Surfing the Web at Work. Viitattu 22.11.2018.
https://www.thebalancecareers.com/surfing-the-web-at-work-1919261

Gain, B. 2011. Why Employees Should Surf the Web at Work. Viitattu 22.11.2018.
https://www.pcworld.com/article/239054/why_employees_should_surf_the_web_at_work.html

Cisco. 2016. View OMP Information. Viitattu 4.12.2018. https://sdwan-docs.cisco.com/Product_Documentation/vManage_How-Tos/Operation/View_OMP_Information

Riverbed. 2016. STEELCONNECT: Application-Defined SD-WAN for the Cloud Era. Viitattu 4.12.2018. https://www.riverbed.com/fi/products/steelconnect.html

Fortinet. 2018. FortiManager. Viitattu 4.12.2018. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiManager.pdf

Khan, F. 2016. The Top 4 SD-WAN Myths. Viitattu 4.12.2018.
https://www.networkcomputing.com/networking/top-4-sd-wan-myths/1072744350

Gintert, J. 2018. How Software Defined Wide Area Networking (SD-WAN) Provides Reliable Voice and Video Services Over the Internet. Viitattu 4.12.2018.
https://sdn.ieee.org/newsletter/march-2018/how-software-defined-wide-area-networking-sd-wan-provides-reliable-voice-and-video-services-over-the-internet

Bischoff, P. 2016. VPN comparison cheat sheet. Viitattu 7.12.2018.
https://www.comparitech.com/vpn/protocols/

IP With Ease. 2017. MPLS VS INTERNET. Viitattu 1.2.2019.
https://ipwithease.com/mpls-vs-internet/

Lerner, A. 2015. I hate my WAN…SD-WAN to the rescue. Viitattu 7.12.2018. https://blogs.gartner.com/andrew-lerner/2015/07/07/sdwan/

Hoffman, C. 2015. Which is the Best VPN Protocol? PPTP vs. OpenVPN vs. L2TP/IPsec vs. SSTP. Viitattu 7.12.2018. https://www.howtogeek.com/211329/which-is-the-best-vpn-protocol-pptp-vs.-openvpn-vs.-l2tpipsec-vs.-sstp/

Sturt, R. 2018. SD-WAN vs. VPN: How do they compare? Viitattu 7.12.2018. https://searchnetworking.techtarget.com/tip/SD-WAN-vs-VPN-How-do-they-compare

Skybakmoen, T. 2018. SD-WAN COMPARATIVE REPORT. Viitattu 7.12.2018. https://www.fortinet.co.jp/doc/NSS-Labs-SD-WAN-Comparative-Report-Performance.pdf

Brandenburg, M. 2010. MPLS VPN basics. Viitattu 1.2.2019. https://searchnetworking.techtarget.com/tutorial/MPLS-VPN-basics

Kuvat

Kuva 1: Star- ja full-mesh -verkkotopologiat. 11

Kuva 2: Diagrammi SD-WAN verkkoarkkitehtuurista (SDxCentral 2018) 12

Kuva 3: MPLS- ja VPN-arkkitehtuurit. (IP With Ease 2017) 15

Kuva 4: Arvio laajaverkkokuluista (Gartner 2017) 18

Kuva 5: Kuvakaappaus fyysisistä liittymistä. 19

Kuva 6: Kuvakaappaus liittymän läpi kulkevasta liikenteestä. 20

Kuva 7: Kuvakaappaus palomuurin lisäyksestä FortiManageriin. 21

Kuva 8: Kuvakaappaus onnistuneesti lisätyistä laitteista. 22

Kuva 9: Kuvakaappaus palomuurisännön luomisesta. 22

Kuva 10: Kuvakaappaus VPN-topologian valinnasta. 23

Kuva 11: Kuvakaappaus VPN-salauksen valinnasta. 23

Kuva 12: Kuvakaappaus palomuurin lisäämisestä VPN-yhteisöön. 24

Kuva 13: Kuvakaappaus liittymien osuuksista kuormituksen tasapainotuksessa. 25

Kuva 14: Kuvakaappaus liittymien läpi kulkevasta liikenteestä. 25

Kuva 15: Kuvakaappaus liittymien ylläpitämien sessioiden määrästä. 26