LAB University of Applied Sciences

SD-WAN ja sen osa nykypäivän laajaverkkoa

LAB-ammattikorkeakoulu
Insinööri (AMK), Tieto- ja viestintätekniikka
2021
Samuli Lampimäki

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Lampimäki, Samuli	Opinnäytetyö, AMK	2021
	Sivumäärä	
	34	

Työn nimi

SD-WAN ja sen osa nykypäivän laajaverkkoa

Tutkinto

Insinööri (AMK), tieto- ja viestintätekniikka

Ohjaavan opettajan nimi, titteli ja organisaatio

Marianne Matilainen, vastuuopettaja, Tekniikan ala, LAB

Toimeksiantajan nimi, titteli ja organisaatio

Saku Määttä, Ryhmäpäällikkö, DNA Oyj

Tiivistelmä

Opinnäytetyön tavoitteena oli toteuttaa DNA Oyj:lle asiakirja, jossa käytiin läpi laajaverkon teknologioita, protokollia ja SD-WAN:in toimintaa ja SD-WAN-toimittajia. DNA Oyj on yksi Suomen suurimmista tietoliikennekonserneista ja osa Telenor-konsernia.

Opinnäytetyö toteutettiin laadullisella tutkimusmenetelmällä. Tutkimus pohjautui asiantuntijakirjoituksiin ja teknologiayritysten tuottamiin dokumentteihin. Tuloksena tuotettiin asiakirja, josta selviää laajaverkon teknologioiden ja protokollien pääpiirteet, ohjelmallisen määrittelyn periaatteet, palomuurien toiminnan periaatteet ja SD-WAN:in toimintaperiaate.

Asiasanat

palomuuri, fortinet, cisco, SD-WAN, wan

Abstract

Author(s)	Type of Publication	Published
Lampimäki, Samuli	Thesis, UAS	2021
	Number of Pages	
	34	

Title of Publication

SD-WAN and its part in today's wide area network

Name of Degree

Bachelor of Engineering, Information and Communication Technology

Name, title, and organization of the supervising teacher

Marianne Matilainen, Senior Lecturer, Technical field, LAB

Name, title, and organization of the client

Saku Määttä, Technical manager, DNA Oyj

Abstract

The goal of this thesis was to produce a document for DNA Oyj. DNA Oyj is one of the largest telecommunication groups in Finland. DNA Oyj is also part of the Telenor group.

The purpose of this document was to serve as an aid for DNA´s corporate business division and its sales department, to help with sales regarding the SD-WAN products.

The thesis was conducted with the use of a qualitative research method. This thesis analyzed expert writings and documentations from technology companies. The result was a document that outlines the protocols and technologies for wide area networking, the concept of software defined and it´s parts, the functionality of firewalls and the concept of SD-WAN.

Keywords

firewall, cisco, fortinet SD-WAN, wan

Sisällys

Lyhenneluettelo

AAC	(eng. Application Awerness and Controll) sovellus tietoisuus ja kontrollointi
ATM	(eng. Asynchronous Transfer Mode) asynkroninen tiedonsiirtotapa
DOCSIS	(eng. Data Over Cable Service Interface Specification) antennikaapelissa käytetty tiedonsiirtotapa
DPI	(eng. Deep Packet Inspection) pakettien syvällinen sisällön tarkistelu
DSL	(eng. Digital Subscriber Line) digitaalinen tilaajayhteys, datan siirto lankapuhelinkaapelissa
IPSec	(eng. Internet Protocol Security) IP-pakettien suojausmenetelmä
LAN	(eng. Local Area Network) lähiverkko
MPLS	(eng. Multi Protcol Label Switching) IP-pakettien kuljetusmenetelmä
NAT	(eng. Network Address Translation) verkko-osoitteen kääntäminen
NGFW	(eng. Next Generation Firewall) uuden sukupuolen palomuuri, monipuoleisimmat ominaisuudet
Palomuuri	Tietoliikenne komponentti, jota käytetään tietoverkon suojaamiseen
pilvi	(eng. cloud) tietoteknillinen palvelualusta internetissä
SD	(eng. Software Defined) ohjelmallisesti määritelty
SDN	(eng. Software Defined Networking) ohjelmallisesti määritelty verkko
SD-WAN	(eng. Software Defined Wide Area Networking) ohjelmallisesti määritelty laajaverkko
SSH	(eng. Secure Shell) tietoverkkosalausprotokolla
SSL	(eng. Secure Socets Layer) tietoverkkosalausprotokolla
TCP/IP	(eng. Transmission Control Protocol / Internet Protocol) tietoliikenneprotokollapino
VPN	(eng. Virtual Private Network) virtuaalinen erillisverkko
WAN	(eng. Wide Area Network) laajaverkko

1 Johdanto

1.1 Työn aiheen esittely

DNA Oyj on suomalainen tietoliikenneyritys, joka tuottaa puhe-, data-, ja tv-palveluita. DNA on yksi Suomen suurimmista tietoliikennekonserneista ja osa Telenor-konsernia. Telenor on yksi maailman suurimmista televiestintäalan yrityksistä. Yrityksen yritysliiketoiminnan yksikössä tiedostettiin tarve asiakirjalle, jossa käydään läpi mitä tarkoitetaan termillä SD-WAN. Opinnäytetyön tavoitteena on toimia kyseisenä asiakirjana sellaisenaan. Asiakirjan tavoite on toimia yritysliiketoiminnan myyjien tukena SD-WAN-tuotteiden myynnissä.

Asiakirjan tavoitteena on tuoda esille eri tekniikan osa-alueet, jotka vaikuttavat SD-WAN:iin ja sen toimintaan. Tavoite on myös kasvattaa mahdollisten yritysasiakkaiden tietämystä SD-WAN:nista. Työn aihetta ja rajoja mietittäessä tuli selväksi, että asiakirjassa olisi hyvä käydä läpi myös perinteisen laajaverkon tekniikkaa, jotta voidaan muodostaa erot normaalissa laajaverkon toiminnassa ja SD-WAN:in toiminnassa.

1.2 Tutkimusmenetelmä, tutkimuskysymykset ja tutkimusongelmat

Opinnäytetyö on toteutustavaltaan kvalitatiivinen eli laadullinen tutkimus. Tutkimus perustuu asiantuntijakirjoituksien ja dokumentaatioiden analysointiin.

Tutkimusongelmaksi muodostui kysymys, kuinka teknisesti käydään laajaverkon ja SD-WAN:in toimintaa lävitse. Koska työn kohteena on yritysliiketoiminnan myynti ja yritysasiakkaat, opinnäytetyössä keskitytään käymään aiheet pintapuolisesti ja suoraviivaisesti läpi.

Tutkimuskysymyksiä työn aiheen miettimisen yhteydessä ilmeni kolme. Kuinka periteinen laajaverkko toimii. Miten perinteinen laajaverkko määritellään. Kolmanneksi tutkimuskysymykseksi muodostui miten SD-WAN eroaa perinteisestä laajaverkosta.

1.3 Opinnäytetyön rakenne

Ensiksi käydään läpi mitä tarkoitetaan laajaverkolla. Laajaverkon määrittelyn jälkeen käydään läpi ja esitellään laajaverkon teknologioita ja protokollia.

Laajaverkon jälkeen käydään läpi ohjelmallisesti määrittelemisen eri käsitteet ja sen osa-alueet. Ohjelmallisesti määrittelemisen läpikäyminen on tärkeää, sillä SD-WAN:in toiminta perustuu sen käsitteisiin ja tekniikoihin.

Kolmantena aihealueena on palomuurit. Palomuurit ja niiden toiminta luovat pohjan sille, miten SD-WAN toimii ja miten SD-WAN toimii laajaverkon teknologiana. Palomuurit ovat suosittuja laitepohjia SD-WAN-ratkaisulle.

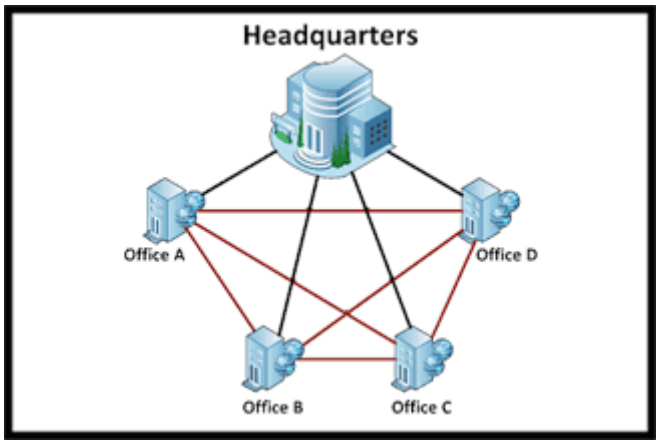
Neljäntenä opinnäytetyön kohtana on SD-WAN, sen toiminta, erot muihin laajaverkon toteutusmenetelmiin, SD-WAN-toimittajien esittely ja SD-WAN-toimittajien vertailu. Toimittajia käydään läpi, jotta saadaan tuotua eri näkemyksiä SD-WAN:in toteutustavoista. Toimittajien vertailulla tuodaan tarkemmin erot esille. Toimittajat on valittu mielivaltaisesti. Viimeisenä kiteytetään pääkohdat yhteenvedossa.

2 Laajaverkko

2.1 WAN

Laajaverkko, englanniksi Wide Area Network (WAN), tarkoittaa tiedonsiirtoverkkoa, joka linkittää yhteen eri lähiverkkoja, englanniksi Local Area Network (LAN). Tämän verkon laajuus voi olla maantieteellisesti todella suuri, se voi jopa kattaa useita maita. Laajaverkko voi olla yksityisistä tietoverkoista koostuva tai se voi myös yhdistää pienempiä julkisia tietoverkkoja. Internetiä voidaan pitää maailman suuripana laajaverkkona. (Bradley 2020.)

Pienemmässä mittakaavassa yrityksillä voi olla laajaverkko, joka koostuu useammasta tietoverkosta. Esimerkiksi, pääkonttori, sivukonttorit, datakeskus ja pilvipalvelut. Nämä kaikki voidaan yhdistää yhdeksi yrityksen kattavaksi laajaverkoksi (Kuvio 1). Laajaverkko mahdollistaa pienempien tietoverkkojen yhdistämisen toisiinsa riippumatta siitä, kuinka kaukana ne ovat toisistaan. (Bradley 2020.)

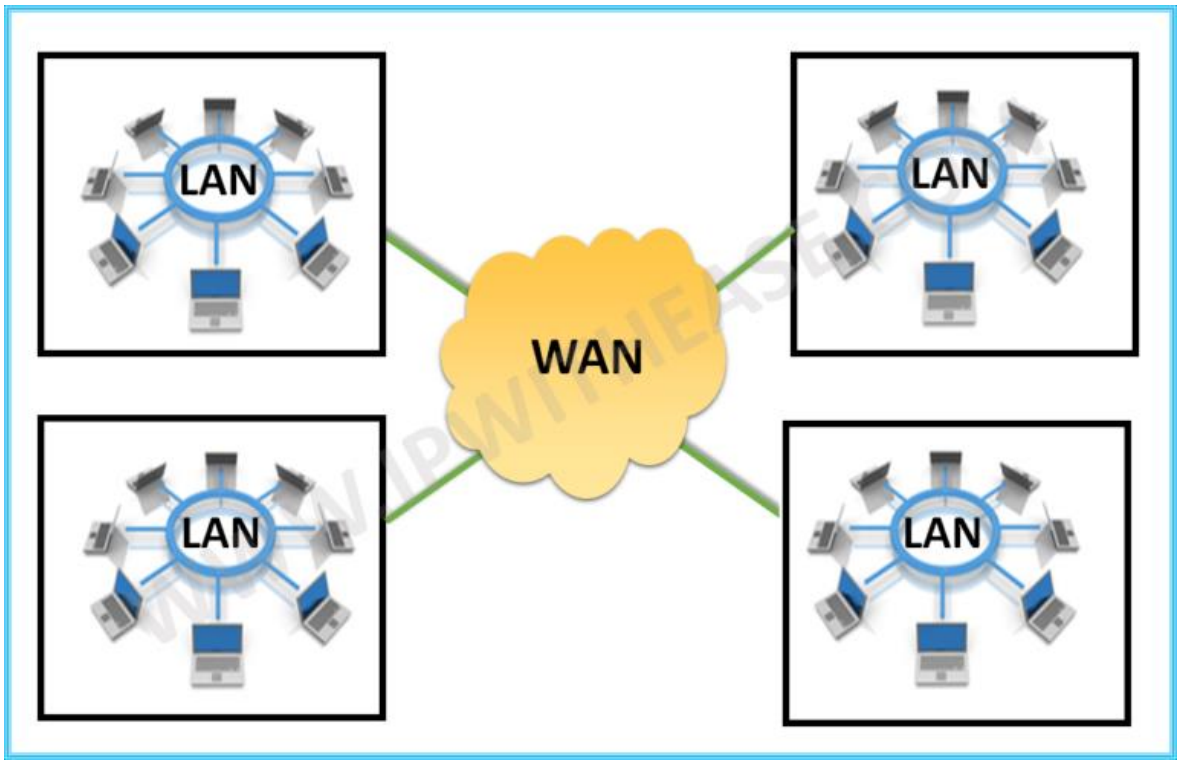


Kuvio 1. Esimerkki mahdollisesta yrityksen laajaverkosta. (Network Encyclopedia)

2.2 WAN vastaan LAN

Laajaverkon (WAN) vastakohta on lähiverkko (LAN). Lähiverkot rajoittuvat yleensä suurimmillaan yhteen kampukseen, yhteen rakennukseen tai joissain tapauksissa yhteen kerrokseen rakennuksen sisällä (Kuvio 2.). Lähiverkossa käytettävät teknologiat ja protokollat ovat helppoja käyttää ja rakentaa, mutta kyseiset teknologiat ja protokollat eivät tue todella pitkiä välimatkoja tai todella suuria määriä käyttäjiä tai verkkolaitteita. Sitä varten laajaverkolla on omat teknologiat ja protokollat. (Fruhlinger 2020.)

Ylläpidollisesti laajaverkko on yleensä ostettu tietoliikenneoperaattorilta maksullisena palveluna ja sen operointivastuu on tietoliikenneoperaattorilla. Lähiverkko on taas yleensä yrityksen omassa ylläpidossa ja hallinnassa. (Fruhlinger 2020.)



Kuvio 2. Laajaverkko vs lähiverkko (IP With Ease)

2.3 Laajaverkon protokollat

Laajaverkon pitää siirtää tietoa ja dataa suuria välimatkoja ja suurissa määrissä. Tähän tiedonsiirtoon eivät lähiverkon protokollat ole sopivia. Sitä varten laajaverkolla on käytössä omat protokollat. (Fruhlinger 2020.)

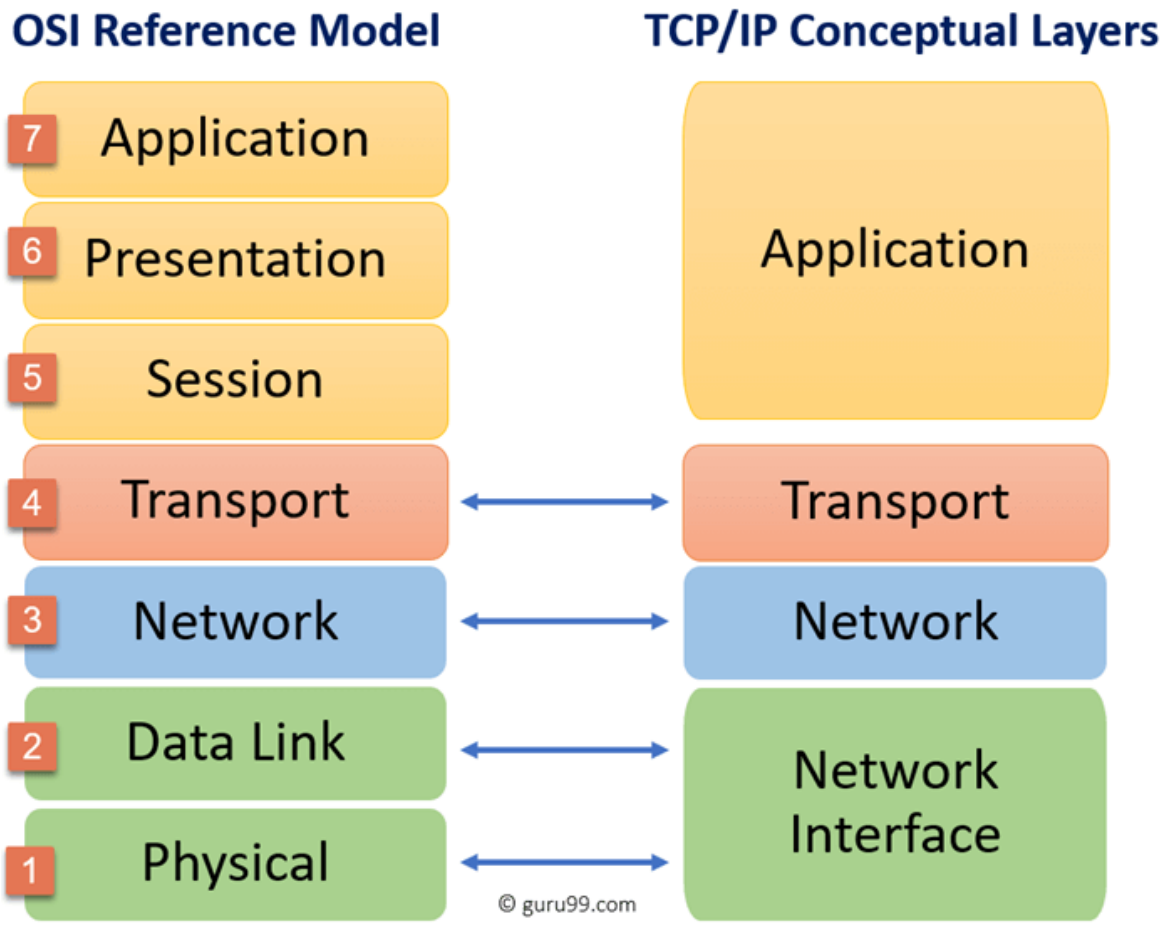
Tutkimushetkellä käytetyimpiä laajaverkon protokollia ovat TCP/IP, MPLS ja IPSec VPN. Seuraavaksi käydään läpi nämä protokollat pintapuoleisesti. (Fruhlinger 2020.)

2.3.1 TCP/IP

TCP/IP on internet-liikennöinnissä käytetty protokollapino (englanniksi protocol stack). Pinossa yhdistetään protokollat IP (internet protokolla) ja TCP (englanniksi Transmission Control Protocol). (IBMRedbooks 2006)

Alemmalla tasolla IP-protokolla hoitaa päätelaitteiden välisen kommunikoinnin hyväksikäyttäen IP-osoitteita. IP-osoitejako samalla hoitaa minne ja miten paketit voivat liikkua verkossa. Päällimmäisenä protokollana on useimmiten TCP, vaikka muitakin protokollia on käytössä. Valtaosa tietoliikenteestä on TCP-pohjaista, joten koko protokollapinoa nimitetään yleisesti TCP/IP. TCP-protokolla kuljettaa varsinaisen datan tietoverkossa. TCP-

protokollan tarkistussumma, ajastimet ja tunnistimet mahdollistavat tiedon siirtämisen onnistuneesti. Tarkistussummalla varmistetaan, että paketin sisältö ei ole muuttunut. Ajastimet pitävät huolen paketin uudelleen lähetyksestä, jos se hukkuu tai saapuu myöhässä. Jokaisesta paketista lähetetään kuittaus takaisin lähettäjälle. Lähettäjä lähettää paketin uudestaan, jos kuittausta ei saada. Tämä tekee TCP-yhteydestä vikasietoisen tavan siirtää datapaketteja. TCP/IP liikennöinti pääsääntöisesti tapahtuu internetin yli (Kuvio 3). (IBMRedbooks 2006)

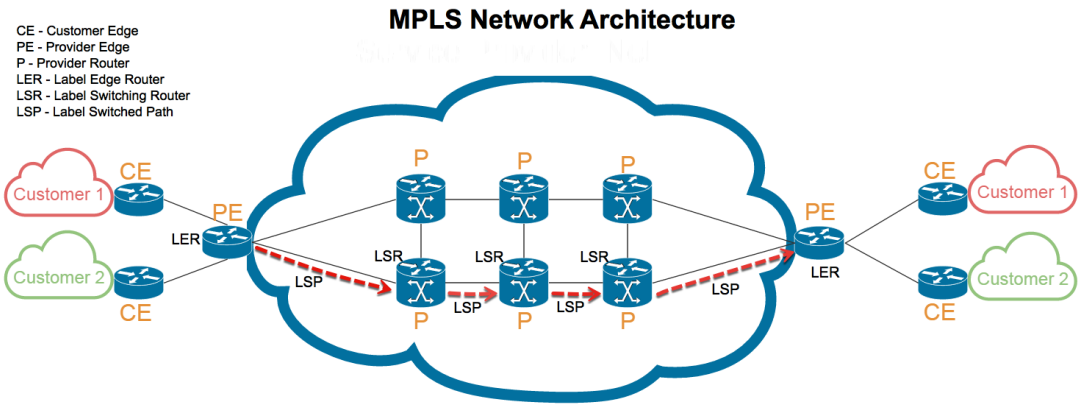


Kuvio 3. OSI-malli vs TCP/IP-malli (Guru 99)

2.3.2 MPLS

Multi Protocol Label Switching eli MPLS, on IP-pakettien kuljetusmenetelmä. MPLS-protokollassa paketit ”leimataan” ja kuljetetaan ilman itse verkossa tapahtuvaa reititystä. Esimerkiksi: Yrityksellä on konttorit Helsingissä ja Turussa. Molempien konttorien verkot ovat samassa IP-osoiteavaruudessa. Konttoreita yhdistää MPLS-verkko. MPLS-verkon toimii siten, että Helsingin konttorista verkkoon saapuvat paketit ”leimataan” kuuluvaksi yrityksen MPLS verkkoon. Leimauksen perusteella MPLS-verkko osaa määrittää pakettien kohteeksi

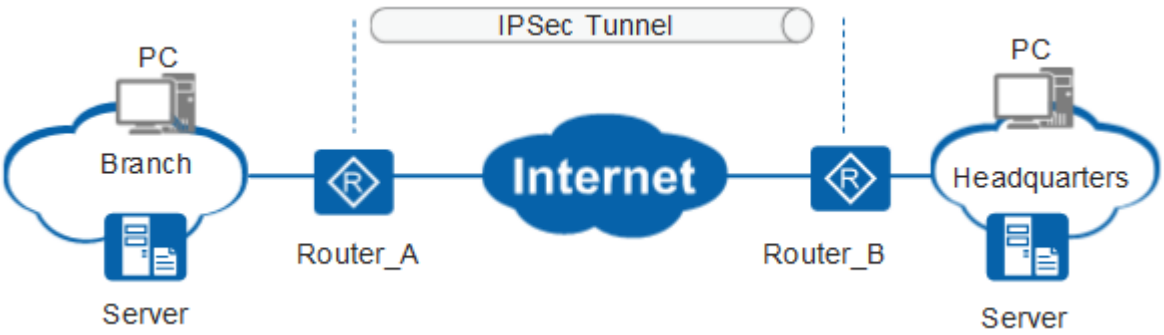
yrityksen konttorin Turussa. Tätä havainnollistetaan kuviossa neljä (Kuvio 4.). MPLS-protokolla toimii OSI-mallin neljännellä tasolla. (De Ghein 2007.)



Kuvio 4. MPLS verkkoarkkitehtuuri (Medium)

2.3.3 IPSec VPN

IPSec (englanniksi IP-Security Architecture) kuuluu aikaisemmin jo mainittuun TCP/IP protokollapinoon. IPSec tuo tiedonsiirtoon mukaan salauksen ja osapuolten todentamisen, kasvattaen siten tietoturvaa. VPN (englanniksi Virtual Private Network) on tapa yhdistää verkkoja toisiinsa hyväksikäyttäen julkisia verkkoja. IPSec VPN muodostaa tunnelit kahden tai useamman kohteen välillä hyväksikäyttäen julkisia verkkoja eli internettiä. Kuviossa viisi mallinnetaan tunnelin muodostamista (Kuvio 5). IPSec VPN on tietoturvallisempi vaihtoehto pelkälle TCP/IP:lle, sillä yhteyden muodostaminen vaati molempien kohteiden olevan tietoinen toisen salausasetuksista (osapuolten todentaminen). Jos salaukset eivät täsmää, tunneli ei muodostu. Kun tunneli on muodostettu, tunneliin kohdistuva liikenne salataan ja salaus puretaan tunnelin toisessa päässä. Ulkopuolinen taho, esimerkiksi operaattori, näkee vain kahden kohteen välisen tunnelin, eikä millaista liikennettä tunnelin sisällä liikkuu. IPSec VPN toimii OSI-mallin kolmannella tasolla. (Kerrigan 2018, Juniper 2021.)



Kuvio 5. IPSec tunnelointi (Huawei)

2.4 Laajaverkon teknologiat

Laajaverkon pitkät etäisyydet, suuret laitemäärät ja isot käyttäjämäärät vaativat myös omat tiedonsiirtoteknologiat. Teknologioista käytössä voi olla aina antennikaapelista valokuituun. Esimerkkejä käytettävistä teknologioista:

DOCSIS, (englanniksi Data Over Cable Service Interface Specification) käytetään kaapeliverkossa. Kaapeliverkossa keskimääräiset nopeudet kirjoitushetkellä ovat noin 350/20Mbit/s. Maksiminopeudet ovat DOCSIS 4.0 avulla jopa 10/1Gbs (Cable Labs.)

DSL (englanniksi Digital Subscriber Line) eli digitaalinen tilaajayhteys, jossa tieto ja data siirretään perinteisen lankapuhelimen kaapelissa. DSL-standardeja ovat mm. ADSL, VDSL ja SHDSL, näistä yleisin on ASDL. DSL-tekniikan maksiminopeus on standardista riippuvainen ja yleensä maksiminopeus on yhdellä kaapeliparilla noin 100/10Mbit/s (Franklin 2008)

Valokuitu. Valokuidussa tieto siirretään laitteiden välillä eri valon aallonpituuksia hyväksikäyttäen. Valokuidulla voidaan saavuttaa yli 10/10Gbit/s nopeudet. (FOA 2002)

Ethernet. Ethernet on pakettipohjainen tiedonsiirtotapa lähiverkossa. Ethernet toimii OSI-mallin kerroksilla 1 ja 2, eli fyysinen- ja siirtoyhteyskerros, nämä on havainnollistettu kuviossa kuusi (Kuvio 6). Ethernet-tekniikan yleisimmät nopeudet kirjoitushetkellä ovat 100/100Mbit/s ja 1Gbit/s. (Balchaunas 2012)

Kuvio 6. OSI-malli (Puomo)

ATM (englanniksi Asynchronous Transfer Mode) eli asynkroninen tiedonsiirtotapa. ATM on toinen pakettipohjaan liittyvä tiedonsiirtotapa. ATM pilkkoo lähetettävän datan pieniksi vakiomittaisiksi 53 tavun soluiksi. ATM:n tiedostosiirtotekniikalla on mahdollista saavuttaa nopeuksia väliltä 1.544Mbit/s – 622Mbit/s. (Cisco Systems Inc. 2000.)

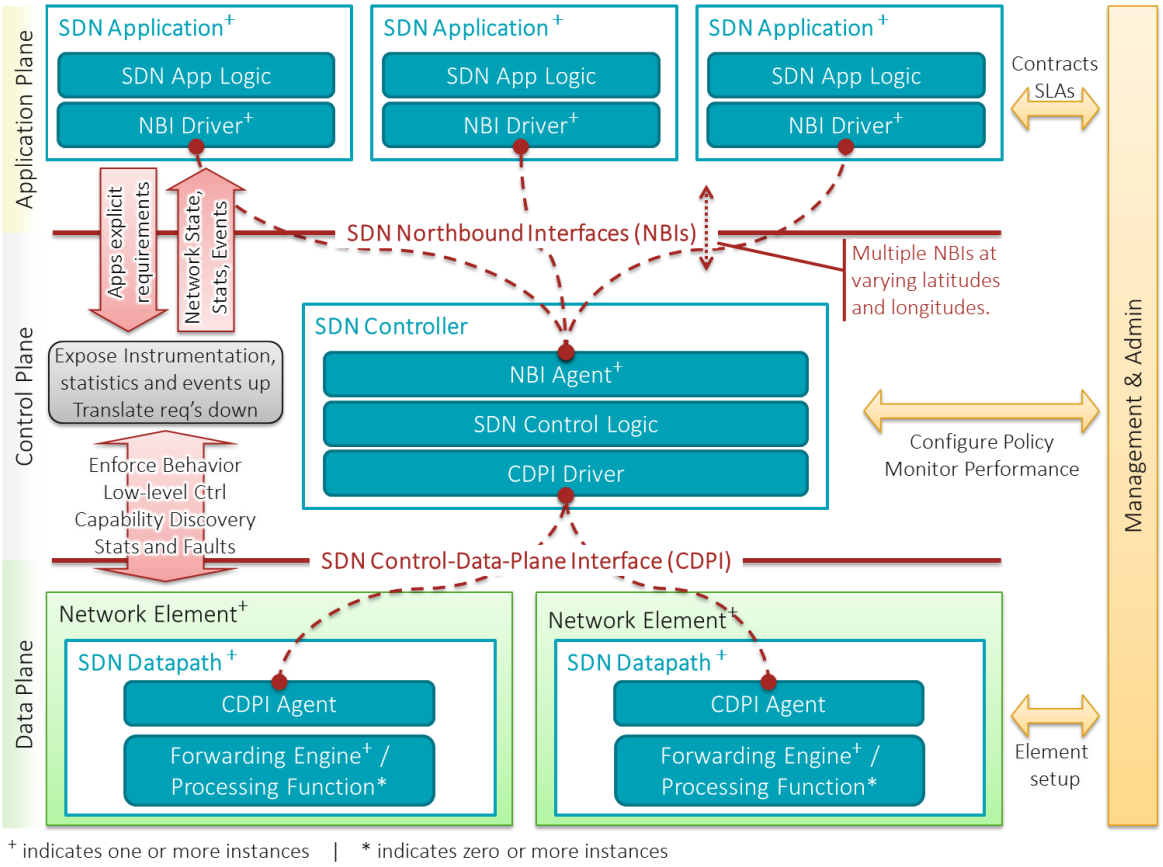
3 Ohjelmallisesti määritelty verkko

3.1 Ohjelmallisesti määritelty verkko ja sen määritelmä

Software Defined Networking (SDN) eli ohjelmallisesti määritelty verkko. Ohjelmallisesti määritetty verkko tarjoaa dynaamisemman ja ohjelmallisesti tehokkaamman tavan hallita verkkoa. Parantamalla samalla verkon suorituskykyä ja valvontaa. (Benzekki ym. 2016)

Ohjelmallisesti määritelty verkko tuo verkon ylläpidon lähemmäksi pilvipohjaista ratkaisua, verrattuna perinteisempään tapaan ylläpitää verkkoa. SD-WAN:in älykkyys ja ohjelmallisesti hallittavuus pohjautuu vahvasti SDN-konseptiin. (Benzekki ym. 2016)

3.2 Ohjelmallisesti määritelty verkko ja sen komponentit



Kuvio 7. SDN Arkkitehtuuri (Open Networking)

3.2.1 SDN Application

Software Defined Network Application eli ohjelmallisesti määritellyn verkon sovellus. SDN-sovellukset ovat ohjelmia, jotka kertovat suoraan verkon vaatimukset ja halutun verkon

käyttäytymisen SDN-kontrollerille NBI:n välityksellä. NBI eli North Bound Iterface on tiedonsiirtoväylä, jonka avulla SDN-applikaatiot kommunikoivat SDN Controllerille. Kuviossa seitsemän on havainnollistettu kyseinen tiedonsiirtoväylä (Kuvio 7.). (Open Networking)

SDN-sovellus voi käyttää abstraktia kokonaiskuvaa verkosta sisäisissä päätöksentekoprosesseissaan. SDN-sovellus koostuu yhdestä SDN-sovellus logiikasta ja yhdestä, tai useammasta, NBI Driver:ista. NBI Driver on SDN-sovelluksen rajapinta NBI-tiedonsiirtoväylään. (Open Networking)

3.2.2 SDN Controller

Software Defined Network Controller eli ohjelmallisesti määritellyn verkon kontrolleri. SDN-kontrolleri on loogisesti keskitetty kokonaisuus, jonka tehtävä on kääntää SDN-sovelluksen vaatimukset SDN-sovelluksen kerrokselta, yhden kerroksen alemmaksi SDN-datapolulle (SDN Datapath) ja toimittaa SDN-sovellukselle abstrakti kuva verkosta. Tähän voi kuulua mm. statistiikkaa ja tietoa verkon tapahtumista. (Open Networking)

SDN-kontrolleri koostuu yhdestä tai useammasta NBI-agentista, SDN-kontrolleri logiikasta ja CDPI Driver:ista. NBI-agentti toimii kontrollin rajapinta NBI-väylään ja CDPI Driver on kontrollerin datapolun rajapinta. SDN-kontrollerin määritelmä ei sisällä määrityksiä sen toteutustavasta, kontrollerien määrästä, niiden hierarkkisesta toteutuksesta tai sen mahdollisesta virtualisoinnista. (Open Networking)

3.2.3 SDN Datapath

Software Defined Network Datapath eli ohjelmallisesti määritellyn verkon datapolku. SDN-datapolku on looginen verkon laite, joka antaa näkyvyyttä ja kilpailematonta hallittavuutta sen mainostamista reitittämisen ja datan prosessointikyvyistä. (Open Networking)

SDN-datapolku koostuu CDPI-agentista, yhdestä tai useammasta liikenteen reitittävästä tahosta (forwarding engine) ja mahdollisesta liikenteen prosessointifunktiosta. Liikenteen prosessointifunktio ei ole pakollinen SDN-datapolun määrityksen mukaan. SDN-datapolkuja voi olla useampia yhdessä verkon fyysisessä elementissä. SDN-datapolun määritelmä ei myöskään ota kantaa sen implementointiin, loogiseen tai fyysiseen kartoitukseen tai fyysisten resurssien hallintaan. (Open Networking)

3.2.4 SDN Control to Data-Plane Interface

Software Defined Network Control to Data-Plane Interface eli ohjelmallisesti määritelty verkon kontrollerin ja datapolun Liittymä. SDN CDPI toimii liittymänä SDN-kontrollerin ja SDN-datapolun välillä. (Open Networking)

SDN CDPI tarjoaa ohjelmallisen hallittavuuden kaikkiin reitittäviin operaatioihin, kyvykkyyksien mainostamisen, statistiikan raportoinnin ja tapahtumien ilmoitukset. CDPI:n implementointi on avoin sekä toimittajasta riippumaton ja yhteen toimiva. (Open Networking)

3.2.5 SDN Northbound Interfaces

Software Defined Network Northbound Interfaces eli ohjelmallisesti määritelty verkon pohjoissuuntainen liittymä. SDN NBI toimii liittymänä SDN-kontrollerin ja SDN-applikaation välissä. (Open Networking)

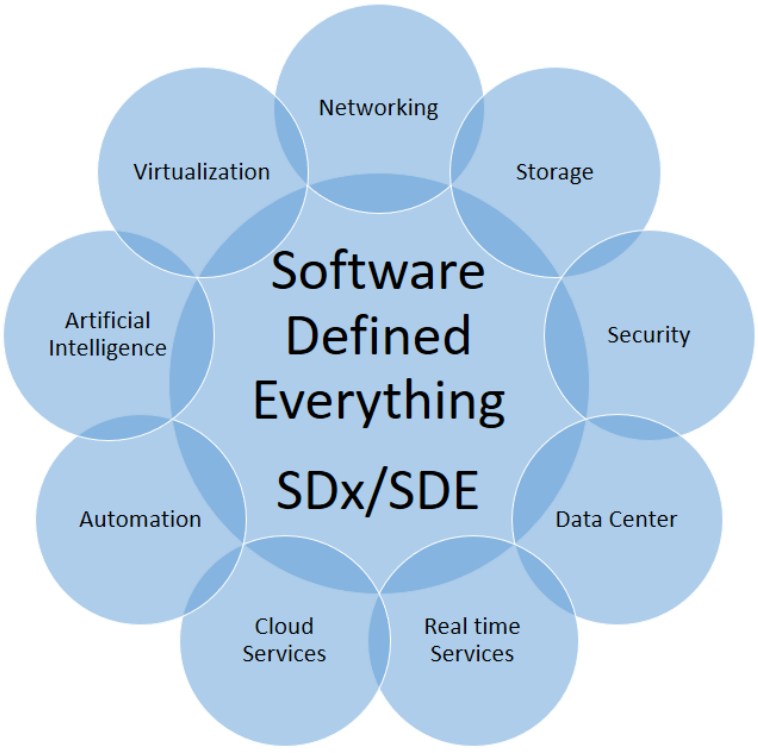
SDN NBI tyypillisesti tarjoaa abstraktin kuvan verkosta ja mahdollistaa suoran tiedon saamisen verkon käyttäytymisestä ja vaatimuksista. NBI tuo SDN:n toimintaa lisäarvoa, kun se on toteutettu avoimesti, toimittajasta riippumattomalla ja yhteensopivalla tavalla. (Open Networking)

4 SDx, Ohjelmallisesti määritelty kaikki

SDx, Softaware defined everything eli Ohjelmallisesti määritelty kaikki. Tällä tarkoitetaan, että ohjelmallisesti määritellään kaikkea mahdollista ja tätä on myös pyritty havainnollistamaan kuviossa kahdeksan (Kuvio 8.). SdxCentral määrittellee SDX:n seuraavasti:

*Määritämme "SDx":ksi minkä tahansa fyysisen kohteen tai toiminnon, joka voidaan suorittaa ohjelmistona tai automatisoida. Tietotekniikan ulkopuolella tämä sisältää sovelluksia, kuten Uber ja Airbnb, mobiililaitteiden sovelluksia ja IOT-laitteita, kuten GoPro-kameroita, Nest-termostaatteja, Phantom-droneja ja itse ajavia autoja. Ohjelmistomäärätty infrastruktuuri (SDxI) on seuraavan sukupolven infrastruktuuri, joka tarvitaan kaikkien näiden ohjelmistomääriteltyjen laitteiden ja sovellusten liittämiseen verkkoonsa, lopulta loppukäyttäjiin. (*SDxCentral Studios 2016, kirjoittajan suomennos*)*

SDx-infrastruktuuri auttaa yhdistämään ja tukemaan biljoonia käyttäjiä ja laitteita, miljooniin erilaisiin palveluihin. Tämä tarkoittaa sitä, että nykyään tietoverkkojen ongelmat ovat eksponentiaalisesti suurempia ja haastavampia, verrattuna tietoverkkoihin kymmen vuotta sitten. (SDxCentral Studios 2016 pt. 5)



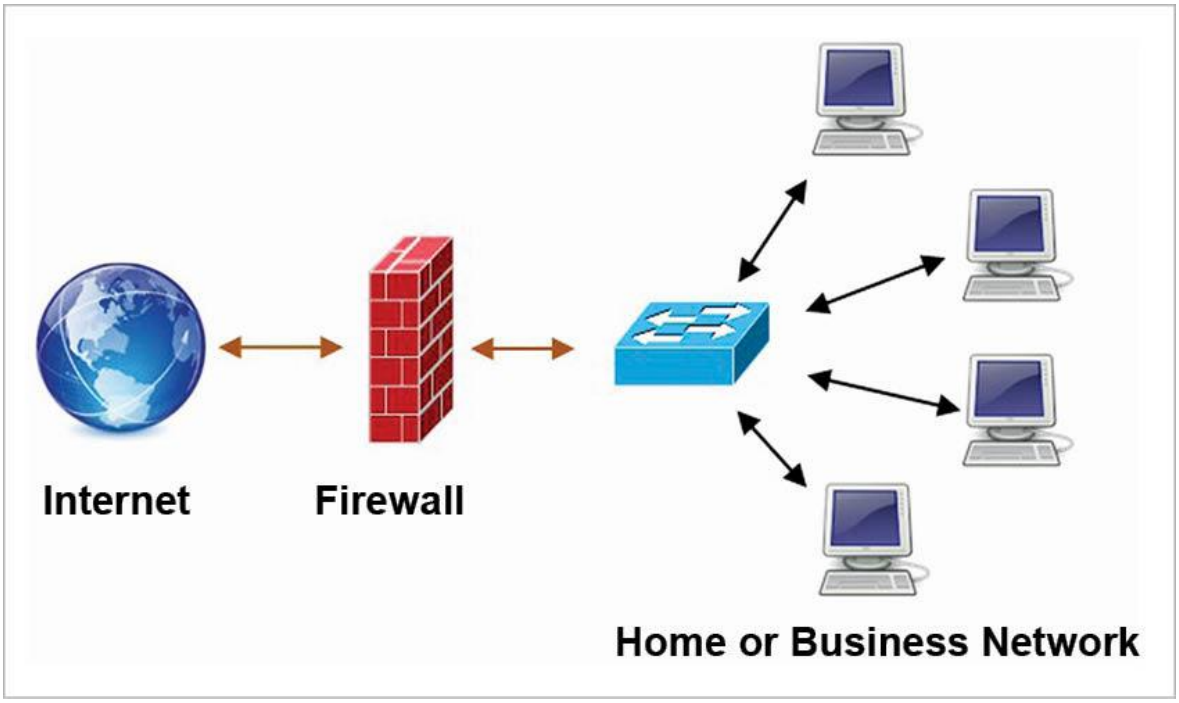
Kuvio 8. SDx Ympäristö (HCLTech)

5 Palomuuri

5.1 Palomuurin määritelmä

Käsitteenä palomuuri tulee fyysisestä muurista, joita rakennettiin rakennusten väliin. Näin yritettiin estää tulipalon leviäminen rakennusten välillä. (Oppliger 1997)

Tietotekniikassa palomuuri (englanniksi firewall), tarkoittaa tietoverkon komponenttia, jolla hallitaan ja rajataan tietoverkon liikennettä. Palomuurilla erotellaan verkot ulkoverkkoon ja sisäverkkoon, kuten kuviossa yhdeksän havainnollistetaan (Kuvio 9.). Palomuurin tehtävä on suojella sisäverkkoa ulkoverkolta. Ulkoverkolla tarkoitetaan yleensä internetiä ja sisäverkolla esimerkiksi yrityksen sisäverkkoa. (Oppliger 1997)



Kuvio 9. Palomuuri (Com-4t)

5.2 Palomuurin toimintaperiaate ja tekniikka

Palomuuri voi olla joko fyysinen, erillinen tietoverkon laite, tai ohjelmistopohjainen ratkaisu. Esimerkkinä ohjelmistopohjaisesta ratkaisusta on esimerkiksi Windowsin oma palomuuriratkaisu tai F-Securen palomuuri- ja virustorjuntaohjelmistot. (CISA 2009, 2019)

Sisäverkkoa voidaan suojata palomuurilla estämällä liikennettä kokonaan tietyistä verkko-osoitteista, rajoittaa applikaatioiden liikennettä tai hyväksymällä liikenne vain tietyistä tcp/ip porteista. Esimerkiksi yritys voi haluta rajoittaa liikennettä siten, että palvelimelle sallitaan

ulkoverkosta ainoastaan FTP-liikenne, silloin sallittaisiin vain portit 20 ja 21.(CISA 2009, 2019)

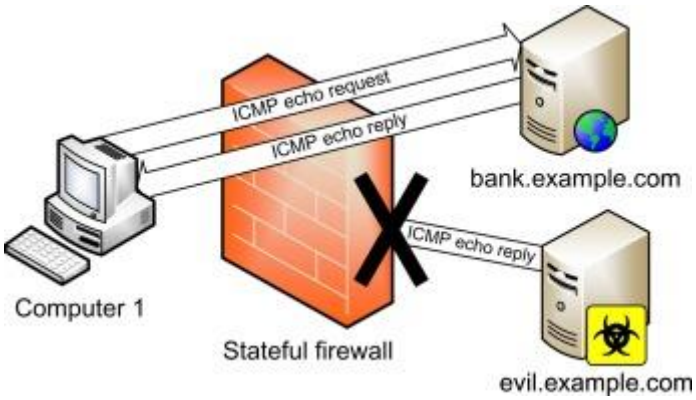
Palomuurien toimintaperiaatteen standardiksi on muodostunut policy-pohjainen, hierarkkinen toimintamalli. Policy:llä tarkoitetaan sääntöä ja hierarkkisessa toimintamallissa sääntöjä luetaan järjestyksessä, esimerkiksi ylhäältä alaspäin. Kun liikenteelle löytyy siihen sopiva sääntö, muita mahdollisia sääntöjä ei lueta. Perinteisesti viimeisimpänä on implicit deny -sääntö, eli ehdoton kielto; jos liikenteelle ei ole löytynyt sopivaa sääntöä, se kielletään kokonaan. (Caldeira & Monteiro 2002.)

5.2.1 Perinteinen palomuuri

Perinteisellä palomuurilla on kaksi eri tyyppiä. Nämä tyypit ovat tilatiedoton (englanniksi stateless) ja tilatietoinen (englanniksi statefull). Perinteiset palomuurit tarkkailevat liikennettä vain OSI-mallin tasoilla 2–4, eli siirto- ja verkkokerroksilla. Liikennettä myös rajoitetaan lähde- ja kohdeosoitteiden, tilatiedon ja protokollan perusteella. (Njoroge 2017.)

Tilatiedoton palomuuri ei tunnista tiedon kulkua, vaan se tarkistaa jokaisen paketin yksitellen. Tämä voi siis vaatia palomuuriavaukset molempiin suuntiin. Esimerkiksi avataan yhteys ulkoverkossa sijaitsevaan palvelimeen, jotta yhteys onnistuu pitää ensin sallia liikenne palvelimen suuntaan sisäverkosta ja pitää myös erikseen sallia paluuliikenne palvelimen suunnasta sisäverkkoon. (Njoroge 2017.)

Tilatietoinen palomuuri vuorostaan tarkkailee liikenteen kulkua tarkemmin. Esimerkiksi halutaan sallia FTP-yhteys ulkoverkon palvelimelle sisäverkosta. Tilatietoisella palomuurilla riittää vain yksi avaus sisäverkosta ulkoverkkoon. Kun yhteys avataan sisäverkosta, ulkoverkosta tulevat paluupaketit ovat automaattisesti sallittuja. Sama koskee yhteyttä toisin päin. Jos FTP-yhteys on sallittu ulkoverkosta sisäverkkoon riittää, että yhteys avataan sallitusta osoitteesta, ja sisäverkosta tulevat paluupaketit sallitaan. Kuviossa kymmenen näytetään tämä käytännössä (Kuvio 10.). (Njoroge 2017.)



Kuvio 10. Tilatietoinen palomuuri (Science direct)

5.2.2 Uuden sukupolven palomuuri

Uuden sukupolven palomuuri eli Next Generation Firewall tuo mukanaan useita eri tapoja suojata tehokkaasti verkkoa. Kuviossa yksitoista listataan uuden sukupolven palomuurin pääpiirteitä (Kuvio 11.). Lähtökohtaisesti kaikki uudet palomuurit ovat jo uutta sukupolvea. Uuden sukupuolen palomuurit ovat yleensä aina tilatietoisia. Yleisimpiä uuden sukupolven palomuurin ominaisuuksia ovat:

Deep Packet Inspection, DPI, eli pakettien syvällinen tarkastelu. DPI ottaa vastaan tulevan paketin ja purkaa sen osiin. DPI tarkistaa datan ja vertaa sitä ennalta asetettuihin ehtoihin ja kasaa paketin uudestaan. DPI on sekä nopeatoiminen ja tehokas. Siitä ei aiheudu haittaa verkon suorituskykyyn. (Njoroge 2017.)

Application Awarness and Control, AAC, eli sovellustietoisuus ja hallinta. AAC tuo mahdollisuuden asettaa rajoituksia sovellustasolla. Tällä voidaan tarkoittaa esimerkiksi sosiaalisen median palveluiden liikenteen rajoittamista kieltämällä vaikka videoiden toistamisen. Sosiaalisen median sivu voi aueta, mutta kyseiseltä sivulta ei anneta toistaa videoita. (Njoroge 2017.)

Integrated Intrusion Protection System, IPS, eli integroitu tunkeutumisen suojausjärjestelmä. Tunkeutumissuojausjärjestelmä on vastuussa mahdollisten tunkeutumisyritysten tai hyökkäysten havaitsemisesta. Tekniikoita tunkeutumisen havaitsemiseksi ovat mm. integroitujen uhka-allekirjoitusten käyttö, tunnetut hyökkäykset, poikkeava toiminta ja liikenteen käyttäytymisanalyysi. Perinteisen palomuurin yhteydessä on voinut olla erillinen komponentti, joka on hoitanut IPS:n tehtävää. Kun se on integroituna suoraan palomuuriin, saadaan verkon suorituskykyä parannettua huomattavasti. (Njoroge 2017.)

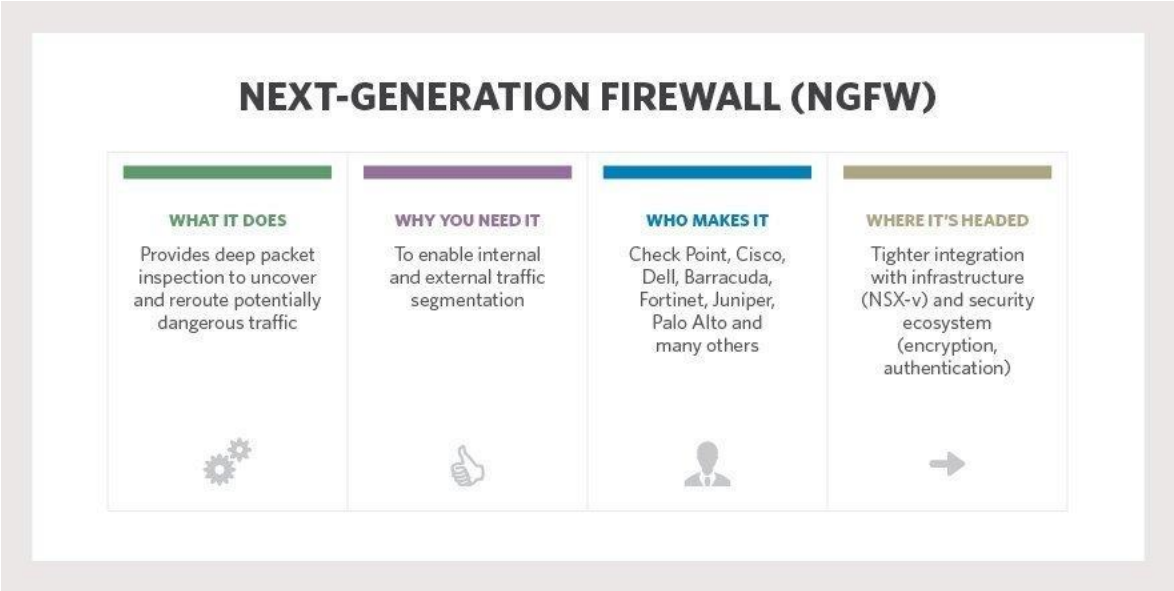
Secure Sockets Layer (SSL) Inspection and Secure Shell (SSH) Control, eli SSL-tarkistus ja SSH-hallinta. Uuden sukupolven palomuurille on tärkeää, että se voi tunnistaa ja purkaa SSL- ja SSH-liikennettä missä tahansa saapuvassa tai lähtevässä portissa. Tämä tulee palomuurin myös pystyä tekemään samanaikaisesti kymmenien tuhansien SSL- ja SSH-yhteyksien kohdalla ja ennalta arvattavissa olevalla suorituskyvyllä. (Njoroge 2017.)

Sandbox integration, eli hiekkalaatikkointegraatio. Kehittyneet verkkohyökkäykset voivat käyttää tuntemattomia haittaohjelmia välttääkseen perinteisen suojauksen. Nämä uhat käyttävät kohdennettuja hyökkäyksiä päästäkseen verkkoon ja pyrkivät pysymään havaitsemattomina pitkään. Hyökkäyksen menestyminen riippuu siitä, kuinka kauan tutkan pysytään. Yksi tällainen uhka, joka on viime aikoina saanut julkisuutta, on ransomware.

Ransomware salaa käyttäjien tiedostoja ja vaati rahallista korvausta salauksen purkamisesta. Hiekkalaatikko on yksi tekniikka, joka on nykyään käytettävissä näiden uusien ja muiden tuntemattomien uhkien torjumiseksi. Hiekkalaatikko on eristetty, turvallinen ympäristö, joka jäljittelee kokonaista verkkoa. Hiekkalaatikossa epäilyttävät ohjelmat voidaan suorittaa, seurata niiden käyttäytymistä ja ymmärtämään niiden tarkoitusta, vaarantamatta organisaation verkkoa. (Njoroge 2017.)

Network Address Translation (NAT) Firewalls, eli verkko-osoitekäännös (NAT) palomuuri. NAT-palomuuri supistaa liikenteen yhden yhdyskäytävän kautta Internetiin. NAT-palomuuri ei yleensä tarjoa liikennetarkastuksia, vaan yksinkertaisesti pyrkii piilottamaan sisäisen verkon ulkoisilta laitteilta ja käyttää yhtä IP-osoitetta ulkoisiin yhteyksiin. NAT-palomuurin avulla voidaan piilottaa useita sisäverkkoja yhden julkisen NAT-yhdyskäytävän taakse. NAT-yhdyskäytäviä käytetään usein VPN-palveluiden kanssa, kuten VPN-tunneleissa lähteenä tai kohteena. (Njoroge 2017.)

Web-kontrollointi ja URL-suodatus. Eri verkkosivuilla vierailun rajoittaminen voidaan toteuttaa joko URL-pohjaisesti tai olemassa olevien kirjastojen pohjalta. Kirjastoihin on kasattu eri verkkosivuja ja verkkosivujen tyypin perusteella voidaan tehdä rajoituksia. Esimerkiksi sivut, jotka tunnistetaan sosiaalisen median sivustoiksi, voidaan kieltää kokonaan, siten jokaista sosiaalimedian sivua ei tarvitse erikseen estää. (Njoroge 2017.)



Kuvio 11. Uuden sukupolven palomuuri (McLaughlin)

5.3 Palomuurien valmistajia

Tunnetuimpia palomuuriratkaisujen toimittajia ovat Fortigate, Cisco, Checkpoint ja Palo Alto. Muita palomuuritoimittajia ovat Sophos, pfSense ja Juniper. (It Central Station 2021.)

Ohjelmistopohjaisia palomuureja toimittavat esimerkiksi Avast, AVG ja Azure. Myös tunnetuimmilla fyysisillä palomuuriratkaisujen toimittajilla on ohjelmistopohjaisia ratkaisuja. (It Central Station 2021.)

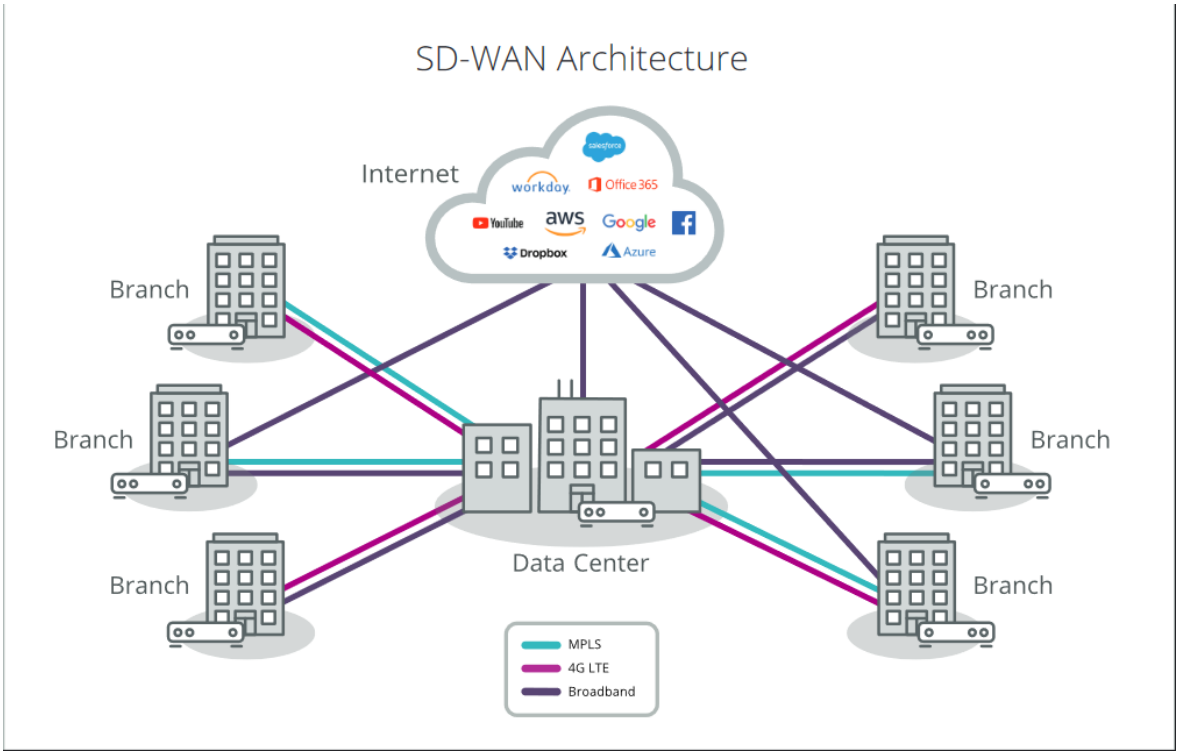
6 SD-WAN

6.1 Mitä on SD-WAN

Software Defined Wide Area Networking eli ohjelmallisesti määritelty laajaverkko. SD-WAN on tapa virtualisoida laajaverkon infrastruktuuri. Ohjelmallisesti määritteleminen tekee SD-WAN:ista älykkään tavan toteuttaa laajaverkkoja ja SD-WAN on sovellustietoinen. Sovellustietoisuus tarkoittaa, että se pystyy ohjaamaan verkkoa jopa yksittäisen sovelluksen tasolla. (Silver-Peak.)

SD-WAN tarjoaa mahdollisuuden käyttää hyväksi monia eri laajaverkon tekniikoita ja protokollia. Hyväksikäyttämällä SD-WAN:ia yritys ei ole riippuvainen yhdestä laajaverkon tyypistä, yhdistäessään verkkonsa eri osia toisiinsa. Tämä näkyy kuviossa kaksitoista (Kuvio 12.). (Silver-Peak.)

SD-WAN ohjelmallisesti ja älykkäästi ohjaa liikennettä oikeaan suuntaan. Esimerkiksi pilvessä olevan palvelun liikenne voidaan ohjata suoraan pilvipalveluun, vaikka laajakaistayhteyden kautta ja yrityksen omassa datakeskuksessa sijaitsevaan palveluun kohdistuva liikenne voidaan ohjata suoraan jo olemassa olevaa MPLS-linkkiä pitkin. (Silver-Peak.)



Kuvio 12. SD-WAN arkkitehtuuri (Silver-Peak)

6.2 SD-WAN arkkitehtuuri

SD-WAN ottaa oppia SDN-arkkitehtuurista siten, että SD-WAN-arkkitehtuuri voidaan jakaa kolmen komponentin sijasta neljään komponenttiin. Nämä neljä komponenttia ovat sovellustaso, hallintataso, kontrollitaso ja datataso. Kuviosta kolmetoista selviää tiivistettynä SD-WAN:in arkkitehtuurin päätasot (Kuvio 13.). (Silver-Peak.)

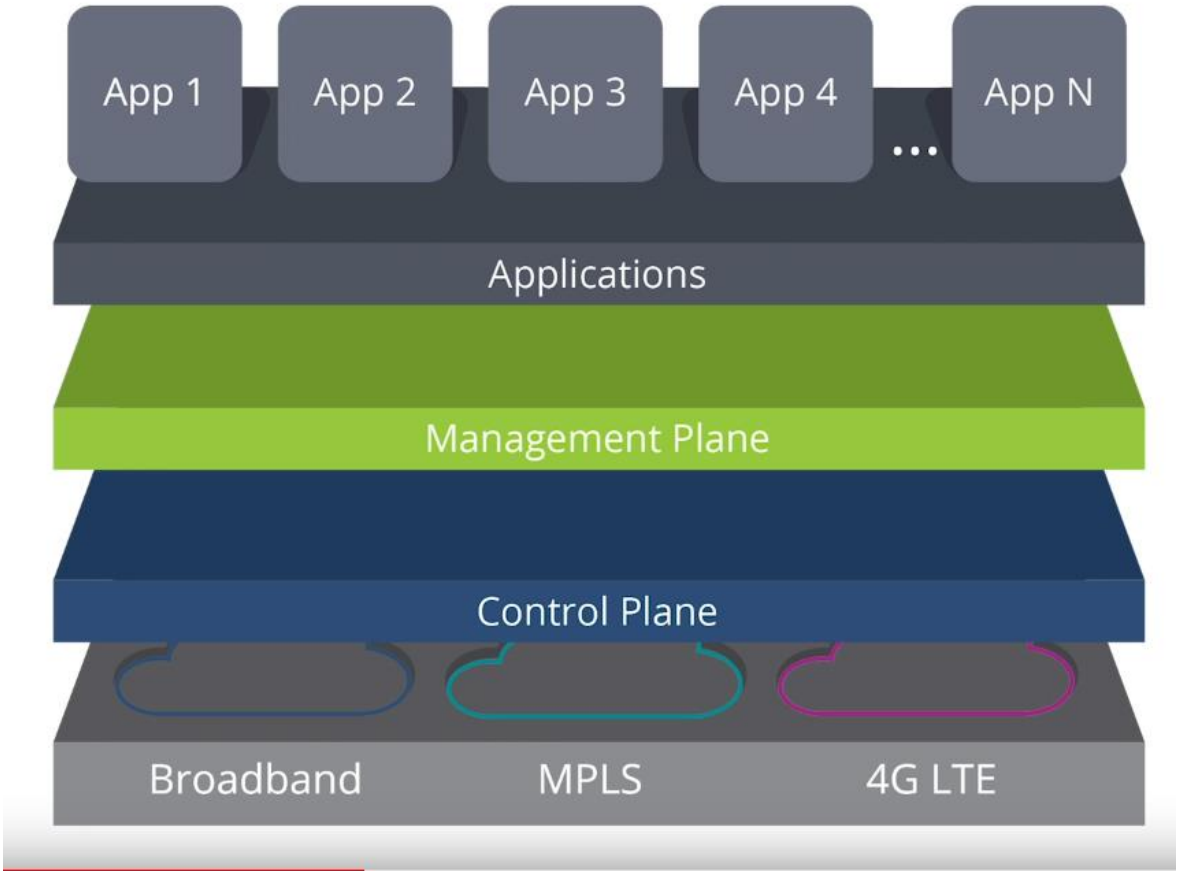
SD-WAN eroaa SDN arkkitehtuurista siten, että hallintataso ja kontrollitaso irrotetaan loogisesti datatasosta. Tällä tarkoitetaan sitä, että kaikki reitityksiin liittyvät päätökset otetaan pois laitteelta, vapauttaen siten laitteen fyysisiä resursseja reitittämisestä. Näitä resursseja ovat esimerkiksi prosessorin tehoa ja muistin määrää. Resurssien vapauttaminen reitittämisestä johtaa parempaan laatuun dataliikenteessä. (Silver-Peak.)

Arkkitehtuuriltaan SD-WAN on jaettu kolmeen eri tyyppiin. Nämä tyypit ovat omassa toimitiloissa pyörivä (On-premises), puhtaasti pilvipohjainen (Cloud enabled) ja pilvipohjainen ratkaisu, johon on liitetty runkoverkko (Cloud enabled plus backbone). (Apcela.)

On-premises, eli omissa toimitiloissa toimiva ratkaisu. Ratkaisu sisältää ”plug ’n play” SD-WAN-laitteen, joka yhdistää vain yrityksen konttorit. Tämä arkkitehtuurityyppi sopii parhaiten yrityksille, jotka ylläpitävät kaikkia applikaatioitaan omassa ympäristössään, ilman julkisia pilvipalvelualustoja. (Apcela.)

Cloud enabled, eli pilvipohjainen ratkaisu. Tämä toteutus sisältää sekä laitteiston että ohjelmiston, joka käyttää paikan päällä olevaa virtuaaliseen yhdyskäytävään liitettyä SD-WAN-laitetta. Pilvipohjainen lähestymistapa tarjoaa sekä yrityksen oman verkon, että pilvipohjaisten arkkitehtuurien edut, reaaliaikaisen liikenteen muotoilun ja useamman yhteyden vikaisietoisuuden sekä paremman suorituskyvyn. Yritykset, jotka käyttävät suuria pilvisovelluksia, sopivat parhaiten tähän arkkitehtuurin malliin. Varsinkin jos ne edelleen ylläpitävät yrityksen sisäisiä sovelluksia pienessä MPLS-verkossa ja käyttävät kaikkia muita pilvisovelluksia julkisen internetin kautta. (Apcela.)

Cloud enabled plus backbone, eli pilvipohjainen ratkaisu, johon on liitetty runkoverkko. Pilvipohjaisen ratkaisun lisäksi yrityksen konttori liitetään SD-WAN:in toimittajan omaan runkoverkkoon. Runkoverkolla voidaan korvata esimerkiksi MPLS-verkko kokonaan. Pilvipohjaiseen yhdistettyä runkoverkkoarkkitehtuuria toimittaa vain harvat valmistajat ja se on erittäin yksilöllinen ja räätälöity ratkaisu. (Apcela.)



Kuvio 13. SD-WAN:in komponentit (Silver-peak)

6.3 SD-WAN:in Komponentit ja toiminta

6.3.1 Sovellustaso

Sovellustaso koostuu käyttäjien käyttämistä sovelluksista. Näitä sovelluksia voivat olla yrityksen yksityisessä pilvessä pyörivät palvelut, julkisessa pilvessä olevat palvelut tai yrityksen omassa konesalissa olevat palvelut. Esimerkiksi käytettäviä palveluita voi olla Microsoftin Office, inventaariojärjestelmä tai tiedostopalvelin. (Cisco SD-WAN, Silver-Peak.)

Yksi SD-WAN:in voimakkaimmista ominaisuuksista on sen sovellustietoisuus. SD-WAN pystyy älykkäästi tarkkailemaan verkon ”terveyttä” ja tekemään päätöksiä, että mikä on jokaisen sovelluksen kohdalla paras yhteys. Esimerkiksi pilvipalvelussa oleva palvelu voi toimia yhtä hyvin langattoman yhteyden kautta tai kiinteän yhteyden kautta. Puhepalvelu ei välttämättä toimi kunnolla langattoman yhteyden kautta. Tässä tapauksessa SD-WAN pystyy älykkäästi tasapainoittamaan liikenteen siten, että puhepalvelu kulkee kiinteän yhteyden kautta ja pilvipalvelun yhteys kulkee langattoman yhteyden läpi. (Cisco SD-WAN, Silver-Peak.)

6.3.2 Hallintataso

Hallintatasolla tarkoitetaan tahoa, miten laitteita hallintaan. Aikaisemmin reitittimien tai palomuurien hallinta on tapahtunut laitetasolla, yksi laite kerrallaan. Hallintaa on voinut joutua toteuttamaan komentokehotteen tai graafisen käyttöliittymän kautta. (Cisco SD-WAN, Silver-Peak.)

SD-WAN-toteutuksessa hallinta tapahtuu laitteesta irrallisena. Esimerkiksi pilvipohjaisessa ratkaisussa, missä tehdään konfiguraatiot valmiiksi ja kyseinen konfiguraatio voidaan ”puskea” useammalle laitteelle samaan aikaan. Yksilölliset konfiguraation osapuolet otetaan tässä jo huomioon, esimerkiksi eri konttorien omat IP-osoiteavaruudet. Tämä ei kuitenkaan poista yksittäisen laitteen konfiguroinnin mahdollisuutta tai sen tarvetta. (Cisco SD-WAN, Silver-Peak.)

6.3.3 Kontrollitaso

Kontrollitaso vastaa siitä, miten liikenne oikeasti liikkuu. Kontrollitason käytössä on samat työkalut liikenteen kontrollointiin, kuin perinteisillä reitittimillä tai palomuurilla. (Cisco SD-WAN, Silver-Peak.)

Kontrollitaso voi käyttää liikenteen ohjaamiseen palomuurille tyypillisiä sääntöjä tai reitittimelle tyypillisiä reititysohjauksia. Päätelaite saa nämä määritykset ja säännöt SD-WAN:in keskitetystä hallinnasta. Keskitetty hallinta voi olla pilvessä tai yrityksen omassa verkossa olevalla hallintapalvelimella. (Cisco SD-WAN, Silver-Peak.)

6.3.4 Datataso

Datataso vastaa itse tiedonsiirrosta. Tiedonsiirtotapoja voi olla esimerkiksi MPLS, laajakaista ja langattomat yhteydet, kuten 4G tai 5G. (Cisco SD-WAN, Silver-Peak.)

Käytössä voi olla yksi tai useampi tiedonsiirtotapa. SD-WAN:ista saadaan eniten irti hyötyä, kun käytössä on useampi eri tiedonsiirtotapa. Tällöin liikenteen optimointiin on parhaimmat mahdollisuudet. SD-WAN:in toteuttamisessa suositellaan, että käytössä olisi vähintään kaksi eri yhteyttä. (Cisco SD-WAN, Silver-Peak.)

SD-WAN:in toiminta perustuu siihen, että laajaverkon hallinta ja ohjaus keskitetään. Yksittäisen laitteen hallinta on silti mahdollista. Ohjeistuksena on, että hallinta olisi keskitettyä. Keskittämisellä pyritään helpottamaan verkon hallintaa ja samalla parantamaan suorituskykyä ja tietoturvaa. Hallittavuus parantuu siten, että jokaista laitetta ei tarvitse hallinnoida

erikseen, vaan hallinta tapahtuu yhdestä paikasta. Konfiguraatiomuutokset ”ajetaan” vain laitteille verkon yli. Laitteelle yleensä tehdään peruskonfiguraatio valmiiksi. Siten laite saa yhteyden keskitettyyn hallintaan, kun se lopuksi viedään toimipaikkaan. Suorituskyky paranee, koska yksittäisten laitteiden ei tarvitse ylläpitää reititystauluja tai muita verkon hallintaprosesseja. Nämä kaikki on ulkoistettu keskitettyyn hallintaan. Tietoturva paranee, kun konfiguraatio tapahtuu yhdessä paikassa ja se vain räätälöidään jokaiselle eri toimipaikalle sopivaksi. Tämä toimintamalli vähentää virheiden mahdollisuuksia, koska jokaista laitetta ei tarvitse erikseen konfiguroida. Mahdolliset konfiguraatiovirheet voidaan korjata yhdestä paikasta ja levittää korjaukset kaikkiin toimipaikkoihin. (Silver-Peak, Cisco SD-WAN, Multapplied)

SD-WAN:in voimakkaimpia ominaisuuksia on sen applikaatiotietoisuus. Tämä usein on se mikä näkyy heti loppukäyttäjälle, jos yhteys on heikko tai huono. Jos esimerkiksi toimipaikan MPLS tai muu pääyhteys on ruuhkautunut ja laadun määrityksen asetukset (englanniksi Quality Of Service eli QoS) eivät ole kunnossa, saattaa kaista tukkiutua raskaasta TCP-liikenteestä. Silloin UDP-pohjainen liikenne, kuten video tai puhe voi kärsiä. Normaalissa kahdennetussa laajaverkon yhteyksissä liikenne ei käänny varayhteydelle, ellei pääyhteys katkea kokonaan, tai ole jotenkin kokonaan käyttökelvoton. SD-WAN:in applikaatiotietoisuus ja sen älykäs laajaverkon monitorointikyky pystyy älykkäästi ohjaamaan raskaamman TCP-liikenteen vaikkapa langattomalle 4G-varayhteydelle, jolloin kiinteää pääyhteyttä voidaan käyttää UDP-liikenteelle, joka kärsii herkemmin langattoman yhteyden mahdollisista heilahduksista. (Silver-Peak, Cisco SD-WAN, Multapplied)

Perinteinen tapa toteuttaa SD-WAN:ia on jakaa se kolmeen osaan. Osa yksi on datatason liittymät, eli laajaverkon toteutus teknologiat yms. Nämä niputetaan yhdeksi resurssiryhmäksi. Toinen osa on jonkin sortin mittarit tai mittaus tapa, jolla mitataan ja tarkkaillaan verkon laatua. Mittarina voi olla virtualisoitu käyttäjä tai agentti, joka vahtii reaaliajassa verkkoa. Kolmas osa on SD-WAN säännöt. Nämä säännöt käyttävät mittareiden tuottamaa dataa perustana siihen, miten liikennettä ohjataan. Jokaisella SD-WAN toimittajalla on oma toteutustapansa, mutta tämä kolmen osan rakenne on hyvin standardisoitunut toteutustapa. (Silver-Peak)

6.4 MPLS vastaan SD-WAN

MPLS on pitkään ollut yksi käytetyimmistä laajaverkon toteutustavoista sen luotettavuuden takia. MPLS-verkon luotettavuus johtuu sen käyttämistä ”tageistä” liikenteen reitityksessä. Nämä ”tägit” virtuaalisesti eristävät paketit ja MPLS:än palvelutuottajat voivat priorisoida tiettyä liikennettä. Nämä osapuolet luovat ennalta arvattavan liikenteen verkossa. MPLS-verkon heikkoja puolia ovat sen kallis kapasiteetin hinta, ja MPLS-verkossa ei ole

sisäänrakennettua tietoturvaa datalle. Virheet MPLS-verkon määrityksissä voivat jättää verkon haavoittuvaksi. MPLS-verkossa myös tulevat vastaan maantieteelliset rajoitteet. (SDxCentral.)

SD-WAN puolestaan on riippumaton maantieteellisestä sijainnista. SD-WAN skaalautuu paremmin kuin MPLS, koska SD-WAN ei vaadi erillisiä perustamisia tai ylimääräisä konfiguraatioita. Riittää, että laitteella on julkinen IP-osoite. SD-WAN on myös tehokkaampi ja sen hallinta on helpompaa. SD-WAN-ratkaisussa verkon päivittäminen on myös helpompaa ja halvempaa. SD-WAN-ratkaisuun voidaan vain lisätä uusia linkkejä ja nämä voivat olla joko laajakaistayhteyksiä tai langattomia 4G- tai 5G-yhteyksiä. SD-WAN hoitaa itse liikenteen jakamisen ja laadun seuraamisen. Tietoturvakin paranee SD-WAN:in myötä, sillä sen liikenne on valmiiksi jo salattua ja hallittavuus ja konfigurointi on keskitettyä. Haittapuolena on, että SD-WAN-ratkaisussa ei tule MPLS:lle tyypillistä takuuta sen toimivuudesta, kuten palvelutasosopimusta (englanniksi Service Level Agreement eli SLA), joka takaa tietyn saatavuuden MPLS-verkolle. (SDxCentral.)

SD-WAN:in ja MPLS:än välillä on neljä tärkeätä eroa. Nämä erot ovat:

- MPLS on fyysinen ratkaisu ja SD-WAN on virtualisoitu ratkaisu.
- MPLS-linja on vuokrattu ainoastaan yrityksen omaan käyttöön.
- MPLS-yhteydet ovat pakettihävikiltään pienempiä, mutta kalliimpia kapasiteetiltaan.
- SD-WAN tarjoaa useita vaihtoehtoja laajaverkon toteutustavoista, mukaan lukien MPLS. (SDxCentral.)

7 Vertailuku

Tämä vertailu tulee perustumaan jo valmiiksi saatavilla oleviin materiaaleihin tai tehtyihin vertailuihin. Perusteena tälle on se, että tutkimuksen tekemisen aikana ei ollut mahdollisuutta saada molemmilta toimittajilta fyysisiä laitteita testejä varten. Jo saatavilla olevan materiaalin pohjalta tullaan tekemään omat johtopäätökset.

Ensin esitellään kaksi SD-WAN-ratkaisun toimittajaa. Valitut toimittajat ovat Cisco ja Fortinet. Valinta on tehty mielivaltaisesti. Esittelyn jälkeen vuorossa on itse vertailu. Vertailun tavoitteena ei ole selvittää parempaa ratkaisua tai toimittaa, vaan tuoda eroja esille, miten SD-WAN:ia voidaan toteuttaa.

7.1 Cisco SD-WAN

Cisco on amerikkalainen teknologiayritys, joka perustettiin vuonna 1984. Cisco on tunnettu sen verkkolaitteista, ohjelmistoista ja telekommunikaatio ratkaisuista. Arvioilta 80 % koko maailman tietoliikenteestä kulkee Ciscon reitittimien läpi. Ciscon tuotteisiin kuuluu mm. kytkimiä, reitittimiä ja palomuureja. (Cisco about)

Vuonna 2017 Cisco osti toisen amerikkalaisen yrityksen, Viptelan. Viptela on tunnettu sen SD-WAN-ratkaisuista. Tämä yrityskauppa nosti Ciscon SD-WAN-ratkaisun markkinan kärkeen, markkinaosuuden perusteella. Ciscon SD-WAN-ratkaisun pohjalla on vSmart, vManage, vBond, vEdge ja vAnalytics. Ciscon SD-WAN-ratkaisun arkkitehtuuria on avattu kuviossa neljätoista (Kuvio 14.) (Cisco Viptela.)

Ciscon vSmart on virtuaalinen kontrolleri, joka hoitaa laitteiden hallinnan ja SD-WAN:ille tyypilliset ominaisuudet. Näitä ominaisuuksia ovat esimerkiksi käytettävien datayhteyksien tarkkailu ja mittareiden rankentaminen. Mittareiden pohjalta tehdään reitityspäätökset. vSmart:in avulla tehdään SD-WAN:in policy-paketit valmiiksi. Virtuaalisen kontrollerin etu on se, että jos hallittavia laitteita tulee lisää, esimerkiksi yrityskaupan tai yrityksen laajenemisen myötä, kontrollerille on helppo lisätä resursseja. Tarvitsee ainoastaan perustaa yksi tai useampi vSmart-instanssi ja vSmart osaa itse tasapainottaa kuorman. (Cisco SD-WAN, Kerr 2020.)

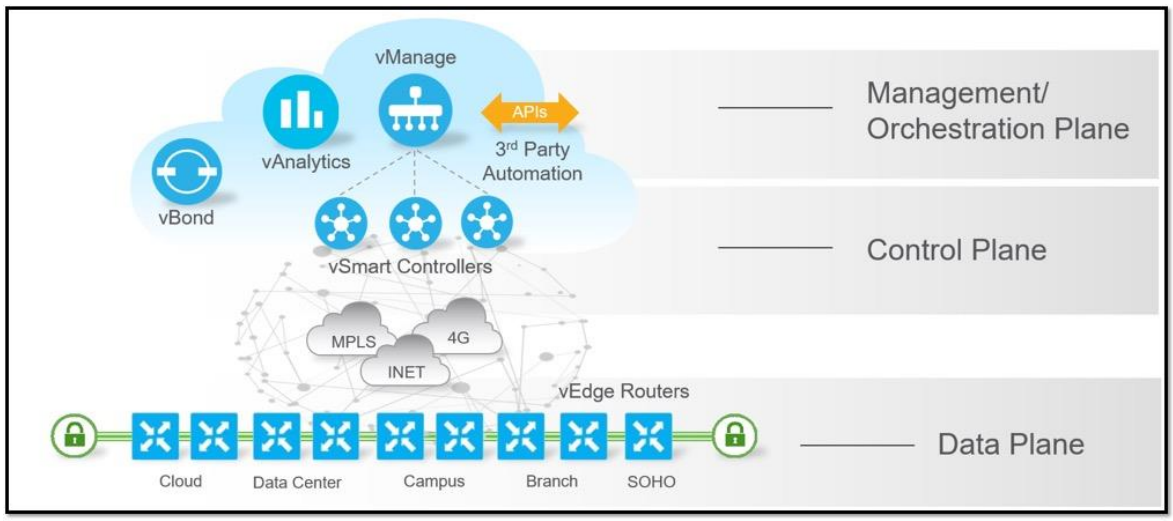
vManage on Ciscon hallinta konsoli, jonka kautta käyttäjät tekevät muutoksia SD-WAN-ympäristöönsä. vManage:n kautta voidaan tehdä keskitetysti muutokset, joko koko SD-WAN-ympäristöön tai yksittäisille laitteille. (Cisco SD-WAN, Kerr 2020.)

vBond yhdistää uudet laitteet verkkoon. vBond käyttää hyväkseen ilman kosketusta tapahtuvaa provisiointia (englanniksi Zero Toutch Provisioning eli ZTP). Tämä tarkoittaa, että laitteita ei tarvitse erikseen konfiguroida käyttöönoton yhteydessä. vBond on Ciscon tarjoama

pilvipalvelu, jonka kautta laitteet ohjataan, joko Ciscon isännöimään pilvipalveluun, jossa pyörii vSmart ja vManage tai laite ohjataan yrityksen omaan vSmart ja vManage palveluihin. vBond:in ainoat vaatimukset toimiakseen ovat, julkinen IP-osoite ja toimiva DNS-palvelu. Ciscon SD-WAN laitteet ovat konfiguroitu siten, että ne yhdistävät ensin suoraan Ciscon vBond-palveluun ilman erillistä konfiguraatiota. (Cisco SD-WAN, Kerr 2020.)

vEdge on Ciscon nimitys sen datatason toteutustavalle. vEdge sisältää Ciscon SD-WAN-laitesarjat kuten ISR-, ASR- ja ENCS-tuotteet. Tähän kuuluu myös jokaisen kohteen käyttämä tiedonsiirto tapa, esimerkiksi mahdollinen MPLS-yhteys tai vaikkapa perus laajakaistayhteys. (Cisco SD-WAN, Kerr 2020.)

vAnalytics on Ciscon SD-WAN:in analysointi- ja tiedonkeruutyökalu. vAnalytics:in avulla voidaan kerätä dataa verkon käytöstä, tiedonsiirron trendeistä ja tehdä siten tarkempia ja laadukkaampia päätöksiä. vAnalytics pystyy myös ennustamaan verkon tulevaisuutta ja tekemään omia ehdotuksia liikenteen hallintaan. (Cisco SD-WAN, Kerr 2020.)



Kuvio 14. Ciscon SD-WAN arkkitehtuuri. (Cisco)

7.2 Fortinet SD-WAN

Fortinet on yhdysvaltalainen kyberturvallisuuden yritys. Fortinet on perustettu vuonna 2000 ja sen pääkonttori sijaitsee Sunnyvalessa, Kaliforniassa. Fortinetin tuoteperheeseen kuuluu mm. heidän lippulaivanansa oleva palomuurilinjasto, Fortigate, antivirus ja tunkeilijan havaitsemisjärjestelmä Fortinet Security Fabric, www-suodatus FortiWeb ja tietoturvan tiedon keruu työkalu FortiAnalyzer. (Fortinet About.)

Fortinetin SD-WAN-arkkitehtuurin keskiössä on FortiManager-tuote. FortiManager:in kautta voidaan hoitaa kaikki SD-WAN:in toimivuuden kannalta olevat tärkeät prosessit ja

toimenpiteet. Kuvio viisitoista avaa lisää Fortinetin SD-WAN-arkkitehtuuria (Kuvio 15.). (Fortinet Secure SD-WAN Reference Architecture.)

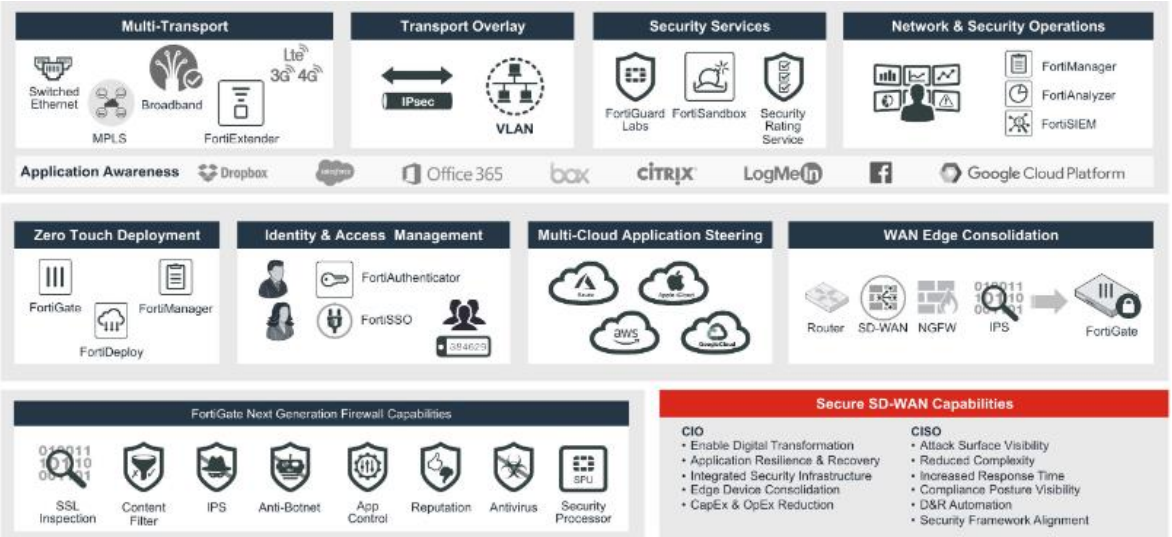
SD-WAN:ille tyypilliseen tapaan, Fortinetin SD-WAN-arkkitehtuuri on neliosainen. Arkkitehtuuri koostuu kolmesta pääpiirteestä, jotka ovat SD-WAN Interface, Performance SLA ja SD-WAN rule. Neljäs osa on hallintatyökalu FortiManager. (Fortinet Secure SD-WAN Reference Architecture.)

Ensimmäinen pääpiirre on SD-WAN Interface, näillä määritetään datatasolla, mitkä rajapinnat osallistuvat SD-WAN:in toimintaan. Fortinetin toiminnassa ylärajaksi on määritelty 255 rajapintaa. Rajapinnat voivat olla fyysisiä, kuten MPLS-yhteyksiä tai laajakaistayhteyksiä tai virtuaalisia, kuten VPN-tunneleita. (Fortinet Secure SD-WANSolution Overview and Architecture Guide.)

Toinen pääpiirre on Performance SLA. Fortinetillä tämä toimii mittarina, miten SD-WAN:in reititykset tapahtuvat. Performance SLA:n määritykset voidaan tehdä käsin, muuttamalla parametreja kuten ping-kutsun vasteaika tai pakettihävikin määrä. Vaihtoehtoisesti voidaan myös Performance SLA:na käyttää suoraan Fortinetin tarjoamia mittareita. (Fortinet Secure SD-WAN Solution Overview and Architecture Guide.)

Kolmas pääpiirre on SD-WAN rule, eli SD-WAN-sääntö. SD-WAN-säännöt määrittelevät miten liikenteen ohjaus tapahtuu. SD-WAN-säännöt käyttävät SD-WAN-rajapintoja ja Performance SLA-mittareita liikenteen ohjauksessa. (Fortinet Secure SD-WAN Solution Overview and Architecture Guide.)

Näiden kolmen edellä mainitun pääpiirteiden ohjaaminen ja hallinta tapahtuu FortiManager:in keskitetyn hallinnan kautta. Laitekohtainen hallinta on silti mahdollista. FortiManagerissa, Fortinet on yhdistänyt SD-WAN:in toiminannasta hallintatason ja kontrollitason. FortiManager:in virtuaalista versiota voi päivittää suorituskyvyllisesti vain lisäämällä resursseja virtuaalikoneelle. FortiManager:ista on myös saatavilla Fortinteiltä fyysisiä versioita. Osa Fortinetin FortiManager:ia on SD-WAN Orchestrator, eli organisaattori. Organisaattori mahdollistaa keskitetyn käyttöönoton organisaation tasolla. FortiManager mahdollistaa myös automaation, vapauttaen henkilöstöresursseja muihin tehtäviin. Automatisaatioon kuuluu provisiointi ilman erillistä manuaalista konfigurointityötä. FortiAnalyzer on Fortinetin tiedonkeruutyökalu. FortiAnalyzer:illä voidaan kerätä ja analysoida verkon dataa ja verkon käyttäytymistrendejä. (Fortinet FortiManager data sheet.)



Kuvio 15. Fortinet SD-WAN arkkitehtuuri. (Fortinet Secure SD-WAN Reference Architecture.)

7.3 Fortinet ja Cisco SD-WAN vertailu

Vertailussa käydään läpi avainkohtia SD-WAN toimittajien laitteistoista, käyttöönotosta, konfiguraatiosta ja arkkitehtuurista. Hintoja ja kuluja ei pystytä tässä työssä suoraan vertailemaan, koska nämä tiedot saa vain toimittajilta.

Laitteistoltaan toimittajien välillä ei ole suuria eroja. Molempien toimittajien laitteet ovat pääsääntöisesti palomuuriin pohjautuvia. Fortinet tarjoaa ainoastaan NGFW-tyyppisiä laitteitaan SD-WAN:in toteuttamiseksi. Ciscolta löytyy myös muutama SD-WAN-toimintaan kykenevä reititin, mutta Cisconkin tuotteet ovat pääsääntöisesti NGFW-tyyppisiä. Suorituskyvyn puolesta Fortinetin laitteilla on pieni etu Ciscon laitteisiin. Etu johtuu Fortinetin käyttämistä ASIC-mikropiireistä. ASIC (englanniksi Application Specific Integrated Circuit) tarkoittaa mikropiiriä, joka on suunniteltu tiettyyn käyttötarkoitukseen. Tutkimuksen aikana Cisco ei ole vielä ottanut ASIC-mikropiirejä käyttöön SD-WAN-tuotteissaan.

Käyttöönotto on molemmilla toimittajilla hyvin samanlainen. Uuden SD-WAN-ympäristön pystyttäminen vaatii enemmän konfiguraatiota ja se ei ole samalla tavalla ”plug and play”, kuin jo olemassa olevan ympäristön kasvattaminen. Molemmilla toimittajilla on vahva ”zero touch provisioning” -politiikka, eli uusille laitteille voidaan suorittaa käyttöönotto ilman erillistä laitekohtaista konfiguraatiota.

Konfiguraatio on Fortinetin ja Ciscon tapauksessa hyvin yksinkertaisesti tehtävissä. Konfiguraatiot voidaan hoitaa suoraan SD-WAN:in keskitetystä hallinasta. Fortinetillä keskitettynä hallintana on FortiManage-työkalu ja Ciscolla vManage-työkalu. Molemmissa SD-WAN-ympäristöissä konfiguraatiota voidaan myös tehdä laitekohtaisesti tarvittaessa.

Arkkitehtuurissa suurin ero tulee siitä, että Ciscon arkkitehtuurissa hallintataso ja kontrollitaso on hajautettu vManage- ja vSmart-alustoille. Nämä pyörivät omina virtuaalisina koneinaan ja vaativat omat lisenssit. Fortinetin FortiManage-työkalussa hallintataso ja kontrollitaso ovat yhdistetty.

Taulukossa yksi tuodaan visuaalisesti eroja vertailusta. Vihreä väri merkitsee vahvempaa suoriutujaa kyseisessä aiheessa. Punainen väri merkitsee heikompaa suoriutujaa.

Suorituskyky	Fortinet	Cisco
Käyttöönotto	Fortinet	Cisco
Arkkitehtuuri	Fortinet	Cisco
Hallinta	Fortinet	Cisco

Taulukko 1. SD-WAN-toimittajien vertailu.

8 Yhteenveto

Opinnäytetyön tavoite oli tuottaa asiakirja, jota DNA Oyj:n yritysmyynnin myyntihenkilökunta voisi käyttää apuna yrityksen SD-WAN-tuotteiden myynnissä. Asiakirjan avulla myyntihenkilöt voivat kasvattaa omaa tietämystään SD-WAN:in toiminnasta ja siten nostaa arvoa SD-WAN-tuotteiden myynnissä.

Koska SD-WAN on uusi laajaverkon toteutustapa, tunnistettiin tarve, että asiakirja sisältää myös osiot nykyisistä laajaverkon toteutustavoista, tekniikoista, protokollista, ohjelmallisesti määrittelemisen perusteista, palomuurin toimintaperiaatteet ja SD-WAN:in toiminnan. Mukaan lisättiin myös kaksi eri SD-WAN-toimittajaa auttamaan eri toteutusmenetelmien ja tapojen hahmottamisessa.

Opinnäytetyö toteutettiin kvalitatiivisena, eli laadullisena, tutkimuksena. Opinnäytetyö toimii suoraan tarvittavan asiakirjana ja toimitetaan DNA Oyj:lle sellaisenaan.

Opinnäytetyön tuloksena tuotettiin onnistuneesti asiakirja, joka tuo esille eri laajaverkon osat ja esittelee SD-WAN:ia onnistuneesti. Vielä kymmenen vuotta sitten SD-WAN oli käsitteenä olematon ja tuntematon. Nyt SD-WAN:ista on nopeasti tulossa johtava tapa yrityksille toteuttaa laadukas, nopea ja tehokas laajaverkko. SD-WAN tulee varmasti tulevaisuudessa olemaan yksi laajaverkon johtavista standardeista.

Lähteet

Apcela. What is SD-WAN Architecture. Viitattu 12.5.2021.

Saatavissa https://www.apcela.com/blog/what-is-sdwan-architecture/

Balchunas 2012. Ethernet Technologies Viitattu 25.4.2021.

Saatavissa https://www.routeralley.com/guides/ethernet.pdf

Benzekki ym. 2016. Software-defined networking (SDN): A survey. Viitattu 30.4.2021.

Saatavissa https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737

Bradley, M 2020. What Is a Wide Area Network (WAN)? Viitattu 1.4.2021.

Saatavissa https://www.lifewire.com/wide-area-network-816383

Cable Labs. DOCSIS 4.0 Technology. Viitattu 25.4.2021.

Saatavissa https://www.cablelabs.com/technologies/docsis-4-0-technology

Caldeira & Monteiro 2002. A policy-based approach to firewall management. Viitattu 6.5.2021.

Saatavissa https://www.researchgate.net/publication/221493150_A_policy-based_approach_to_firewall_management

CISA 2019. Security Tip. Viitattu 5.5.2021.

Saatavissa https://us-cert.cisa.gov/ncas/tips/ST04-004

Cisco about. Viitattu 14.5.2021.

Saatavissa https://www.cisco.com/c/en/us/about.html

Cisco. Getting to know Cisco SD-WAN. Viitattu 15.5.2021.

Saatavissa https://blog.cdw.com/networking/getting-to-know-cisco-sd-wan-vendor-overview-series

Cisco. SD-WAN. Viitattu 12.5.2021.

Saatavissa https://www.cisco.com/c/en/us/solutions/enterprise-networks/SD-WAN/index.html?ccid=cc000954&dtid=esoytb000259&oid=voren010717#~benefits

Cisco Systems Inc. 2000. Guide to ATM Technology Viitattu 25.4.2021.

Saatavissa https://indigothemes.com/wikipedia-contribution/techgd.pdf

Cisco Viptela. Viitattu 14.5.2021.

Saatavissa https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/viptela.html

Com-4t. Protection and Inspection of traffic flow. Viitattu 3.5.2021.

Saatavissa https://www.com-4t.rs/en/solutions/security/protection-and-inspection-traffic-flow-0

De Ghein 2007. MPLS Fundamentals. Viitattu 10.4.2021.

Saatavissa https://doc.lagout.org/network/Cisco/CCIE/CCIE%20SP/CiscoPress%20-%20MPLS%20Fundamentals.pdf

Fortinet About. Viitattu 15.5.2021.

Saatavissa https://www.fortinet.com/corporate/about-us/about-us

Fortinet. FortiManager data sheet. Viitattu 15.5.2021.

Saatavissa https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf

Fortinet. Secure SD-WAN Solution Overview and Architecture Guide. Viitattu 15.5.2021.

Saatavissa https://www.fortinet.com/content/dam/fortinet/assets/deployment-guides/dg-secure-sd-wan-architecture-guide.pdf

Fortinet. Secure SD-WAN Reference Architecture. Viitattu 15.5.2021.

Saatavissa https://www.fortinet.com/content/dam/fortinet/assets/document-library/ra-sd-wan-reference-architecture.pdf

FOA 2002. Wavelength. Viitattu 25.4.2021.

Saatavissa https://www.thefoa.org/tech/wavelength.html

Fruhlinger, J 2020. What is a WAN? Wide-area network definition and examples. Viitattu 1.4.2021.

Saatavissa https://www.networkworld.com/article/3248989/what-is-a-wan-wide-area-network-definition-and-examples.html

Franklin, C 2008. How DSL Works. Viitattu 25.4.2021.

Saatavissa https://computer.howstuffworks.com/dsl.htm#pt1

Guru 99. Viitattu 1.4.2021.

Saatavissa https://www.guru99.com/difference-tcp-ip-vs-osi-model.html

HCLTech How to Realize the Full Value of Software-Defined Everything? Viitattu 3.5.2021.

Saatavissa https://www.hcltech.com/blogs/how-realize-full-value-software-defined-everything

Huawei. Viitattu 20.4.2021.

Saatavissa https://support.huawei.com/enterprise/en/doc/EDOC1100041799/f2298f86/using-ipsec-vpn-to-implement-secure-interconnection-between-lans

IBM Redbooks 2006. TCP/IP Tutorial and Technical Overview. Viitattu 1.4.2021.

Saatavissa http://www.redbooks.ibm.com/abstracts/gg243376.html?Open

IP With Ease. LAN vs WAN. Viitattu 1.4.2021.

Saatavissa https://ipwithease.com/lan-vs-wan/

It Central Station 2021. Viitattu 10.5.2021.

Saatavissa https://www.itcentralstation.com/categories/firewalls

Juniper 2021. Viitattu 20.4.2021.

Saatavissa https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-ipsec-vpn-overview.html#id-comparing-policybased-and-routebased-vpns

Kerr. 2020. Getting to Know Cisco SD-WAN: Vendor Overview Series. Viitattu. 15.5.2021.

Saatavissa https://blog.cdw.com/networking/getting-to-know-cisco-sd-wan-vendor-overview-series

McLaughlin 2016. Viitattu 12.5.2021.

Saatavissa https://searchcio.techtarget.com/photostory/450294510/Enterprise-security-architecture-Technology-overview/3/Next-gen-firewalls-What-why-who

Medium. What is Multiprotocol Label Switching (MPLS)? Viitattu 20.4.2021.

Saatavissa https://medium.com/@blogstevej327stuff/what-is-multiprotocol-label-switching-mpls-f9e9cc7fe43b

Multapplied. How SD-WAN Improves Network Application Performance. Viitattu 13.5.2021.

Saatavissa https://www.multapplied.net/how-SD-WAN-improves-network-application-performance/

Network Encyclopedia. Wide Area Network (WAN). Viitattu 1.4.2021.

Saatavissa https://networkencyclopedia.com/wide-area-network-wan/

Njoroge, J. 2017. When a Traditional Firewall Doesn't Go Far Enough. Viitattu 9.5.2021.

Saatavissa https://gtb.net/why-gtb/blog/when-traditional-firewall-doesn%E2%80%99t-go-far-enough

Oppliger, R. 1997. Internet security: fire walls and beyond. Viitattu 4.5.2021.

Saatavissa https://www.thefreelibrary.com/Internet+security%3A+fire+walls+and+beyond-a019569217

Open Networking. SDN Architecture Overview. Viitattu 30.4.2021.

Saatavissa https://opennetworking.org/wp-content/uploads/2013/02/SDN-architecture-overview-1.0.pdf

Puomo. Viitattu 30.4.2021.

Saatavissa https://punomo.fi/kasityotekniikat/elektroniikka-tvt-ict/tvt-ict-tekniikka/miten-web-toimii-tcp-ip-pino/

Kerrigan, S. 2018. Virtual Private Networks: How They Work and Why You Might Need One. Viitattu 10.4.2021.

Saatavissa https://interestingengineering.com/virtual-private-networks-how-they-work-and-why-you-might-need-one

Science direct. Viitattu 10.5.2021.

Saatavissa https://www.sciencedirect.com/topics/computer-science/stateful-firewall

Silver-Peak. SD-WAN explained. Viitattu 12.5.2021.

Saatavissa https://www.silver-peak.com/SD-WAN/SD-WAN-explained

Silver-peak What is SD-WAN. Viitattu 12.5.2021.

Saatavissa https://www.silver-peak.com/sites/default/files/images/what-is-sdwan/what-is-SD-WAN-panel-2-diagram-expanded.pdf

Silver-peak. Viitattu 13.5.2021.

Saatavissa https://www.silver-peak.com/SD-WAN/SD-WAN-explained#item2

SDxCentral. SD-wan vs MPLS.Viitattu 13.5.2021.

Saatavissa https://www.sdxcentral.com/networking/sd-wan/definitions/sd-wan-vs-mpls-pros-cons-technologies/

SDxCentral Studios 2016. What Is Software Defined Everything - Part 1: Definition of SDx. Viitattu 3.5.2021.

Saatavissa https://www.sdxcentral.com/cloud/definitions/software-defined-everything-sdx-part-1-definition/

SDxCentral Studios 2016. Software Defined Everything Pt 5: SDx Use Cases. Viitattu 3.5.2021.

Saatavissa https://www.sdxcentral.com/cloud/definitions/software-defined-everything-part-5-sdx-use-cases/