OULUN AMMATTIKORKEAKOULU

Yrjänä Vesala

TOIMISTOVERKON SEGMENTOINNIN JA PÄÄSYNHALLINNAN TOTEUTUKSEN SUUNNITELMA

TOIMISTOVERKON SEGMENTOINNIN JA PÄÄSYNHALLINNAN TOTEUTUKSEN SUUNNITTELMA

Yrjänä Vesala
Opinnäytetyö
Syksy 2023
Tietotekniikan tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma, laite- ja tuotesuunnittelun suuntautumisvaihtoehto

---

Tekijä(t): Yrjänä Vesala
Opinnäytetyön nimi: Toimistoverkon segmentoinnin ja pääsynhallinta ratkaisun suunnittelu.
Työn ohjaaja(t): Teemu Korpela
Työn valmistumislukukausi ja -vuosi: Syksy 2023 Sivumäärä: 51

Opinnäytetyön tarkoituksena oli alun perin suunnitella ja toteuttaa projektin kohteen toimiston verkon segmentointi, sekä ottaa käyttöön pääsynhallinta kohteen verkkoon. Työn tilaaja oli kiinteistöautomaatioratkaisuja tuottava suomalainen konserni. Projekti toteutettiin yrityksen erääseen toimipisteeseen. Projektin edetessä huomattiin, että aika ei riitä segmentoinnin toteuttamiseen käytännössä, sillä palomuurisäännöstön luominen palomuurille on paljon aikaa vievä osuus. Päätettiin, että työn tarkoitus on esittää ratkaisuvaihtoehtoja pääsynhallintamallille sekä verkon segmentoinnille ja suunnitella verkkosegmentit valmiiksi.

Opinnäytetyön aiheen valintaan vaikutti aikaisempi kokemus lähiverkoista sekä yrityksen konkreettinen tarve verkon segmentoinnille ja pääsynhallinnan käyttöönotolle lähiverkon tietoturvan parantamiseksi.

Tässä työssä käsitellään teoriatasolla lähiverkkoja, erilaisia VLAN-verkkoja, verkkotopologioita, verkkoarkkitehtuureja, pääsynhallintaa, tietoturvamalleja ja verkon segmentointimenetelmiä. Työssä esitetään myös pintapuolisesti yritysverkossa tapahtuneet muutokset.

Työn tuloksena syntyi suunnitelma verkon segmentoinnin ja pääsynhallinnan toteuttamisesta. Segmentoinnin ja pääsynhallinnan ratkaisut tullaan toteuttamaan tämän suunnitelman pohjalta. Yrityksen verkkoon tullaan luomaan uusia VLAN-verkkoja sekä tullaan ottamaan käyttöön lähiverkon pääsynhallinta.

Johtopäätöksenä todettiin, että verkkojen segmentointi on yksi verkon tietoturvan perusasioita. Sillä voidaan pienentää hyökkäyspinta-alaa ja ennaltaehkäistä koko verkon saastumista murtotilanteessa. Pääsynhallinta on tietoturvallisuuden kannalta myös oleellinen asia. Sen avulla voidaan estää ulkopuolisten laitteiden pääsy sisäverkkoon.

Asiasanat: toimistoverkko, tietoliikenneverkko, pääsynhallinta, VLAN-segmentointi, tietoturva

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Information Techonogy, Option of Device and Product Design

---

Author(s): Yrjänä Vesala
Title of thesis: Office network segmentation and access control planning
Supervisor(s): Teemu Korpela
Term and year when the thesis was submitted: 2023
Number of pages: 51

The original plan was plan and impellent network segmentation and network access control to the office network. The client of the work was the Finnish building automation concern, and the project was implemented to one of the offices in Finland. As the project progressed, we noticed that we there wasn't enough time to fully implement access control and network segmentation. Making the firewall rules between networks was too time-consuming section of the project.

We decided that the idea of this project was to plan the segmentation and network access control. We decided to implement segmentation and network access control later. I introduced access control and segmentation methods in this work.

I decided to take this job because I have experience of network maintenance jobs, and the company has a need for network segmentation and access control to improve network security. This job was a good project for thesis work.

In this work local area networks, different VLAN networks, network topologies, network architectures, access control and network segmentation methods are introduced at a theoretical level. Also changes in the WAN-network are introduced in this work.

As a conclusion, we stated that network segmentation is one of the basic security methods to improve organization information security. Network segmentation can be used to reduce the attack surface area in the network. Also access control is an important security feature in networks. Using access control in network is possible to prevent external devices from accessing to the network.

Keywords: network, office network, access control, VLAN-segmentation, security

SISÄLLYSLUETTELO

SANASTO

Access-portti tai untagged-portti	Verkkokytkimissä käytetty protokolla, jolla voidaan merkata tietty portti haluttuun virtuaalilähiverkkoon.
Aliverkonpeite	Määrittää verkon osoitealueen.
DHCP	Protokolla, jonka tehtävä on asettaa dynaamisesti IP-osoitteita uusille laitteille.
IP-osoite	IP-verkossa olevan laitteen yksilöivä tunnus.
Kytkin	Siirtoyhteyskerroksessa toimiva verkkolaite, joka liikuttaa dataa verkkojen välillä. Kytkimen avulla laitteet liitetään lähiverkkoon, jossa laitteet voivat kommunikoida keskenään.
LAN	Paikallinen lähiverkko. Esimerkiksi yrityksen toimipisteen sisäinen tietoliikenneverkko.
Pääsynhallinta	Määrittelee verkkoon liitetyn laitteen oikeudet.
Reititin	Tietoliikenneverkkojen välisiä yhteyksiä reitittävä laite.
Segmentti	Verkkosegmentti on lähiverkon yksittäinen osa. Esimerkiksi toimistoverkon tulostimet voivat olla omassa verkkosegmentissään.
Tietoliikenneverkkoarkkitehtuuri	Arkkitehtuurilla tarkoitetaan verkon rakennetta ja toimintalogiikkaa.

Tietoliikenneverkkotopologia	Topologialla tarkoitetaan sitä, miten verkkolaitteet ovat liitetty toisiinsa.
Trunk-portti tai tagged-portti	Verkkokytkimissä käytetty protokolla, joka mahdollistaa useamman virtuaalilähiverkon merkkaamisen yhteen porttiin. Portti päästää läpi liikennettä kaikista virtuaalilähiverkoista, jotka ovat merkattu kyseiseen trunk-porttiin.
VLAN	VLAN eli virtuaalilähiverkko. Sen avulla voidaan jakaa verkkoa pienempiin virtuaalisiin osiin.
WAN-verkko	Maantieteellisesti laaja verkko, joka muodostuu yksittäisistä pienemmistä verkoista.
Zero trust-malli	Tietoturvamalli, jossa jokainen käyttäjä ja laite on lähtökohtaisesti epäluotettava.

1 JOHDANTO

Opinnäytetyön tarkoituksena oli valmistella yrityksen erään toimipisteen toimistoverkkoon pääsynhallinnan ratkaisu ja suunnitella valmiiksi lähiverkon segmentointi. Verkko on jo valmiiksi VLAN-segmentoitu muutamaan osaan, mutta tietoturvasyistä oli aiheellista jakaa verkkoa vielä pienempiin osiin. Verkon jako pienempiin osiin eli segmentteihin tehostaa verkon suorituskykyä, tietoturvaa ja hallittavuutta. Tässä opinnäyteyössä perehdytään virtuaaliverkkosegmentointiin eli VLAN-segmentointiin sekä aliverkottamiseen.

Yrityksen toimistoverkkoon oli aiheellista muodostaa myös pääsynhallinta. Lähtötilanteessa yrityksen toimistoverkossa ei ollut pääsynhallintaa ja ulkopuoliset laitteet pääsivät yhdistämään suoraan lähiverkkoon ja toimistoverkkoon. Silloisessa toimistoverkossa oli laitteita, joissa oli arkaluonteista tietoa tai joiden kaatamisella tai saastuttamisella voitaisiin lamaannuttaa yrityksen toimintaa. Pääsynhallinnan tehtävä on tunnistaa laite ja ohjata se oikeaan verkkoon. Ulkopuoliset laitteet ohjattaisiin vierasverkkoon, josta ei ole pääsyä yrityksen sisäisiin palveluihin.

Lisäksi opinnäytetyössä kuvataan projektin kohteen verkon sekä yritysverkon tilaa ja näihin tulleita muutoksia. Yrityksen yritysverkko muuttui SD WAN -ratkaisuun ja sen muutoksen dokumentointi oli myös yksi osa opinnäytetyötä. Projektin kohteen verkon segmentointi on pilottiprojekti, joka tullaan tarpeen mukaan myös toteuttamaan muihinkin toimipisteisiin.

2 PROJEKTIN KOHTEEN LÄHIVERKKO

Tässä luvussa kerrotaan projektin kohteen lähiverkosta lähtötilanteessa ja uudistustarpeista. Lisäksi myös teoriaa verkkotopologioista ja verkkoarkkitehtuureista. Projektin kohteen verkkoarkkitehtuurimallia ei muutettu projektin aikana. Verkkotopologia sen sijaan oli tarpeellista muuttaa vikasietoisemmaksi alkuperäisestä mallista.

2.1 Kohteen verkon lähtötilanteen kuvaus

Kohteen verkko on tavanomainen toimistoverkko, jonka neljästä laitetilasta on kaapeloitu verkkokytkimet suoraan pääjakamoon, missä sijaitsee operaattorin ylläpitämä reititin. Toimistoverkon pääasiallinen jako on kehitysverkko, toimistoverkko ja vierasverkko. Yhteydet kulkevat ulkoverkkoon operaattorin hallinnoiman reitittimen kautta. Toimiston laitteisto on pääasiassa työasemia, tulostimia, tukiasemia ja palvelimia. Kehitysverkossa on kehityksen ja testauksen alla olevia yrityksen laitteita sekä muita laitteita, jotka eivät ole yrityksen laitehallinnassa. Toimistoverkossa on kaikki henkilökunnan työasemat, tulostimet ja palvelimet. Vierasverkossa on laitteet, joilla ei ole sertifikaattia toimistoverkkoon tai laitteet, joilla ei ole tarpeellista päästä sisäverkon palveluihin. Osa opinnäytetyötä on suunnitella osittain uusiksi verkon osia eli segmenttejä. Lisäksi haluttiin luoda tulevien verkkojen välille palomuurisäännöstö, jolla rajoitettaisiin verkkojen välistä liikennettä. Lähtötilanteessa kaikki sisäiset palvelut olivat samassa toimistoverkossa, joten sisäverkon palomuurisäännöstöä ei ollut olemassa lainkaan.

Langattomia verkkoja on tuotannon tiloissa ja toimistossa. Tuotanto on samassa verkossa toimistoverkon kanssa. Sitten on langaton vierasverkko, joka on tarkoitettu vieraiden käytettäväksi. Tukiasemat kaiuttavat kaikkia kolmea verkkoa. Tällä hetkellä yritysverkossa on yksi keskitetty palomuuri, jonka kautta kaikki yrityksen tietoliikenne kulkee. Kuva 2 esittää lähtötilanteen toimistoverkon topologian. Yhteydet menevät reitittimille ja siitä keskitetylle palomuurille. Taulukko 1 esittää lähtötilanteen verkot.

Yritys on siirtymässä SD WAN -ratkaisuun, jossa jokaiselle yrityksen toimipisteelle tulee oma operaattorin ylläpitämä palomuurilaite. Verkossa ei ole pääsynhallintaa tällä hetkellä eli verkko ei osaa

dynaamisesti tunnistaa verkkoon kytkettyä laitetta ja ohjata niitä oikeaan verkkoon. Pääsynhallinnan tarkoitus on ohjata tunnistamaton laite vierasverkkoon, mikäli laite on tunnistettu luotettavaksi, se saa oikeudet yrityksen sisäiseen verkkoon.

Lähtötilanteessa toimistoverkon DHCP-osoiteavaruus on määritetty palvelimilla ja muiden verkkojen DHCP-osoiteavaruudet on määritelty reitittimellä.

IPv6-osoitteita ole ollenkaan käytössä sisäverkossa. Sisäverkossa on niin vähän laitteita, joten IPv4-verkkojen osoitemäärillä pärjää hyvin. Julkisia verkkojakin on hyvin vähän, joten ei ole ollut tarvetta IPv6-verkoille.

2.2 Tarpeiden kartoitus

Kohteen toimiston verkko on jaettu kolmeen osaan. Toimistoverkko, kehitysverkko ja vierasverkko. Toimistoverkossa on laitteita, joiden olisi syytä olla erillisissä verkoissa. Lähtötilanteessa palvelimet sekä tuotannon työasemat olivat toimistoverkossa. On järkevää segmentoida tuotannon työasemat ja palvelimet erillisiin verkkoihin. Palvelimilla on arkaluontoista tietoa ja niiden lamaannuttamisella tai saastuttamisella voitaisiin haitata merkittävästi yrityksen toimintaa. Verkkotulostimet myös on syytä segmentoida omaan verkkoonsa, vaikka niitä ei ole määrällisesti kovin paljoa.

Tilanteessa, jossa segmentoitu verkko saastuu hyökkääjällä tai haittaohjelmalla ei ole suoraa pääsyä muihin verkkoihin, kun verkko on segmentoitu oikealla tavalla. Tällaisessa tilanteessa verkon saastuminen rajoittuu vain sen verkkosegmentin sisälle. Verkon segmentointi aliverkottamalla tai virtuaalisia lähiverkkoja käyttämällä tehostaa ja tekee tietoliikenneverkosta luotettavamman.

Esimerkiksi Cybernews -niminen yritys oli tehnyt vuonna 2022 testin, missä se skannasi avoimia tulostimia maailmanlaajuisesti. He tavoittivat noin 800 000 tulostinta, joista 447 000 oli suojaamattomia. On tapauksia, joissa verkkotulostimien heikkouksia hyödyntäen on murtauduttu verkkoihin, joten nekin on syytä siirtää omaan verkkoonsa. (1.)

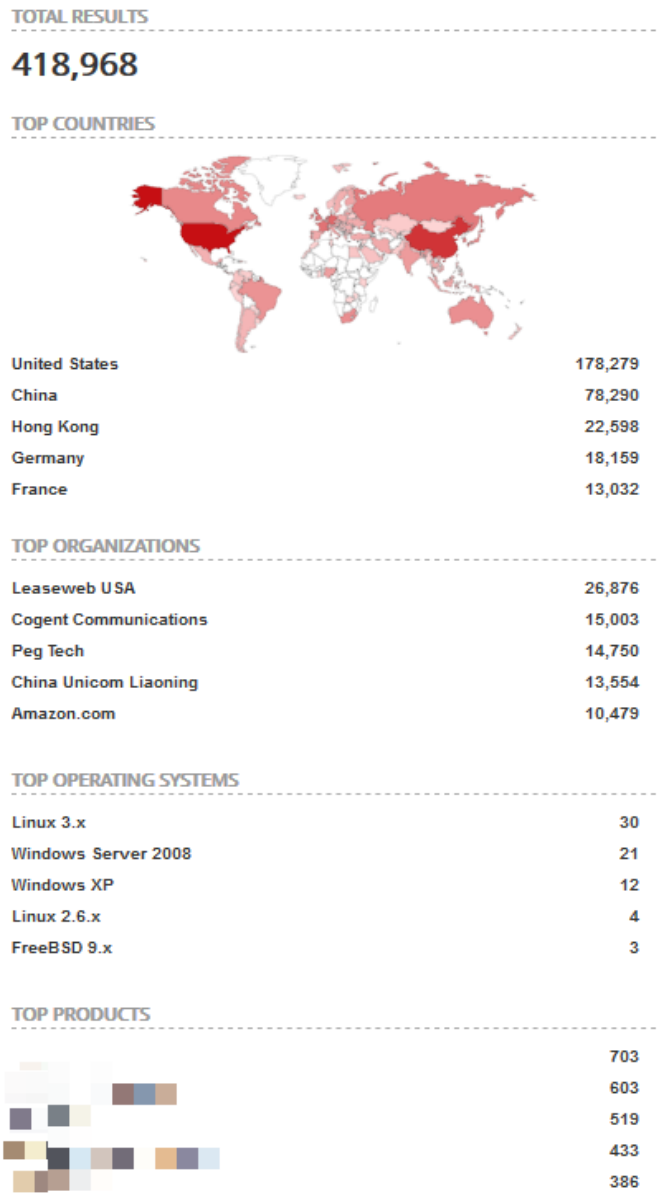
Kuvassa 1 esitetään tilastot edellä mainitusta avoimien verkkotulostimien skannauksesta. Tulostinten ollessa vanhaa laitekantaa niissä voi olla vanhanaikaisia protokollia käytössä, mikä voi olla helppo väylä murtautua verkkoon. Esimerkiksi NTLM-protokolla voi olla vielä käytössä monissa

uusissakin verkkotulostimissa. NTLM-protokolla on helppo murtaa esimerkiksi väsytyshyökkäyksellä heikon salasanaominaisuutensa vuoksi. (2.)

Tuotanto on oleellinen osa organisaation toimintaa. Tuotantoverkon olisi hyvä toimia omana verkkonaan kriittisyytensä kannalta. Muiden verkkojen ongelmat ei vaikuttaisi tuotannon toimintaan, kun tuotantoverkko on erillään muista verkoista. Tuotannon verkosta on myös ruuhkaa suhteessa enemmän kuin muista verkoista.

Palvelimilla on arkaluonteista tietoa sekä ne ovat aktiivisessa käytössä päivittäin. Palvelimien mahdollinen saastuminen tai kaatuminen aiheuttaisi mittavia ongelmia yrityksen toiminnassa. Palvelimet olivat samassa verkossa kuin muutkin toimiston työasemat, tämä oli aukko toimistoverkon tietoturvassa. Toimistoverkon saastuessa haittaohjelma tai murtautuja pääsisi käsiksi palvelimiin ja tästä syystä palvelimet oli syytä segmentoida omaan verkkoonsa. Lisäksi ongelmana on, että niitä hallinnoitiin toimistoverkosta. Olisi fiksua luoda oma hallintaverkko palvelimille, jonne on oikeudet vain IT-tiimillä. Hallintaverkossa olisi työasemia vain silloin yhdistettynä, kun hallintayhteyttä tarvittaisiin palvelimille. Tämä takaisi sen, että hallintaverkko pysyy eristettynä.

Lisäksi kohteen verkkoon halutaan pääsynhallinta. Pääsynhallinnalla tarkoitetaan sitä, että verkkoon kytketty laite tunnistetaan automaattisesti ja se ohjataan oikeaan verkkoon. Esimerkiksi tuntemattomat laitteet ohjataan vierasverkkoon ja yrityksen laitekannan omat laitteet päästetään sisäverkkoon kiinni. Tämä estää tuntemattomien laitteiden pääsyn yrityksen verkkoon. Tällä hetkellä, kun pääsynhallintaa ei ole, verkkoon kytketty laite pääsee suoraan kiinni siihen verkkoon mikä ethernet-rasiaan on kytketty. Avoimia langattomia verkkoja toimistossa ei ole tällä hetkellä. Lisäksi toive oli luoda palomuurisäännöstö projektin kohteen verkkoon, jotta ylimääräinen liikenne aliverkkojen välillä saataisiin kitkettyä pois. Lähtötilanteessa kaikki laitteet olivat samassa verkossa, joten ei ollut tarvetta palomuurisäännöille. Kun verkko segmentoidaan palomuurille, täytyy luoda säännöstö, jossa määritellään tarpeelliset verkkojen väliset yhteydet.



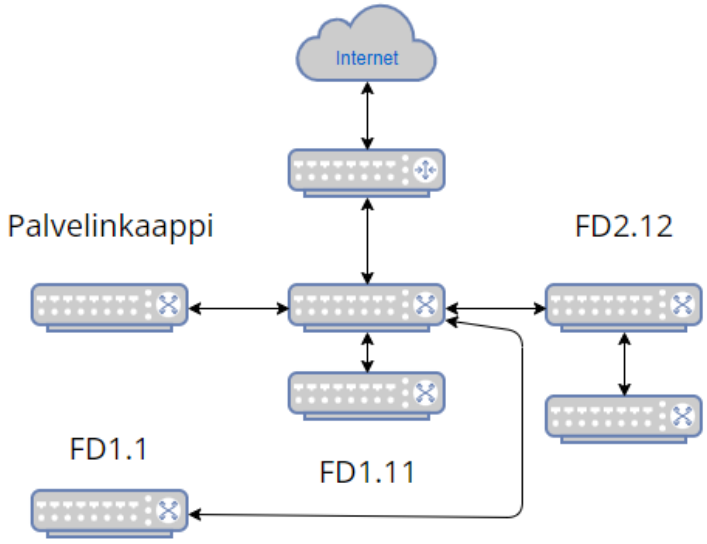
KUVA 1. Cybernewsin vuonna 2022 tuottama avoimien tulostimien skannaus maailmanlaajuisesti. (1.)

3 PROJEKTIN KOHTEEN VERKKOARKKITEHTUURI SEKÄ TOPOLOGIA

Tässä luvussa esitellään projektin kohteen verkkoarkkitehtuurimalli ja verkkotopologiamalli sekä lähtö- että lopputilanteessa. Kappaleessa käsitellään myös teoriaa erilaisista verkkotopologiamalleista.

3.1 Projektin kohteen verkon lähtötilanteen topologia

Verkko oli rakennettu ethernet-kaapeleilla ja verkon topologia oli ketjutettu tähtitopologia. Yksi kytkin oli ketjutettuna toiseen kytkimeen, mutta muuten verkko toteutti tähtitopologiaa. Tähtitopologian heikkoutena on kuormittuva keskuslaite, joka on kuvassa keskellä FD1.11 -laitetilassa, johon suurin osa yhteyksistä kytkeytyy. Kuvassa 2 näkyy kohteen verkon lähtötilanteen tietoliikenneverkkotopologia, joka oli ethernet-kaapeliverkko. Taulukossa 1 esitellään lähtötilanteen verkot, joita olivat toimistoverkko, kehitysverkko ja vierasverkko.



KUVA 2. Lähtötilanteen verkon fyysinen topologiakuva.

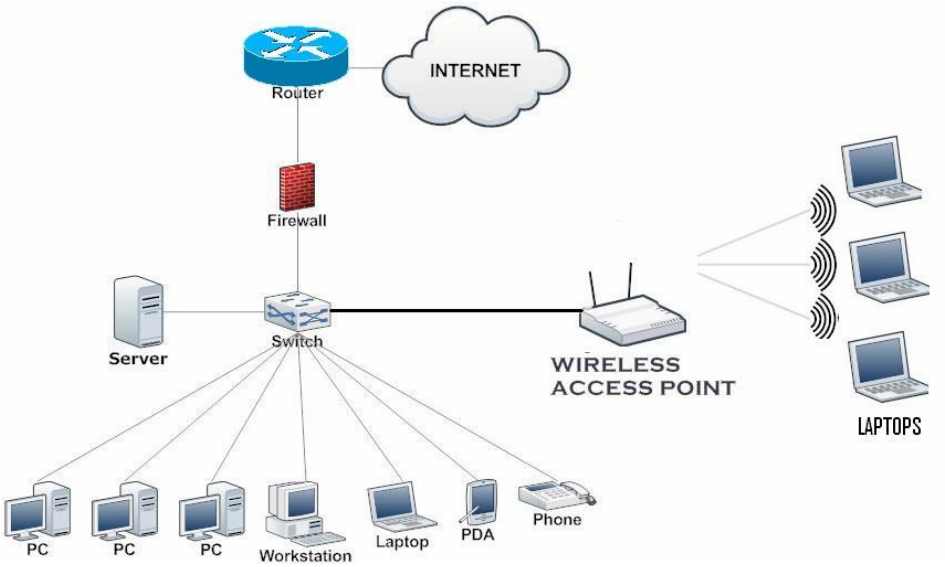
TAULUKKO 1. Lähtötilanteen virtuaaliverkot ja aliverkot.

Virtuaaliverkko	Verkon nimi	aliverkko	Osoitemäärä
VLAN 10	Toimistoverkko	10.6.74.0/24	256
VLAN 20	Kehitysverkko	10.3.74.0/24	256
VLAN 150	Vierasverkko	192.168.10.0/24	256

3.2 Projektin kohteen verkkoarkkitehtuuri

Kuva 3 esittää yksinkertaisen mallin SOHO-arkkitehtuurista. Oikeanlaisen tietoliikenneverkkoarkkitehtuurin valitseminen on oleellinen osa verkon perustamista. Verkkoarkkitehtuuri esittää kuvauksen tietoliikenneverkon tasoista ja runkoyhteyksistä. Tietoliikenneverkko arkkitehtuurin valitseminen helpottaa verkon ylläpitoa ja verkon kehittämistä, kun tunnetaan verkon topologia sekä miten laitteet ovat yhteydessä toisiinsa ja kuinka tietoliikenne kulkee julkiseen internettiin. Pienissä toimistoissa paras tietoliikennearkkitehtuuri on SOHO-arkkitehtuuri eli Small Office Home Office -arkkitehtuuri. Se kattaa tarpeelliset verkkolaitteet tietoturvan ylläpitämiseen sekä toimivien lähiverkkojen muodostamiseen. SOHO-arkkitehtuuri on myös kustannustehokas ja se ei vaadi mittavia investointeja. Lisäksi SOHO-arkkitehtuurin verkkoa on helppo soveltaa itse sen yksinkertaisen rakenteen vuoksi esimerkiksi topologioiden osalta. Lisäksi se on helppo rakentaa ja ylläpitää. (3.) (18.)

Kuvassa on yksinkertainen esimerkki SOHO-arkkitehtuurista. Projektin kohteeseen, jonne toteutin verkon muutokset, oli useampi kytkin kuin tässä esimerkkikuvassa, mutta arkkitehtuuriltaan kohteen verkko on samanlainen.



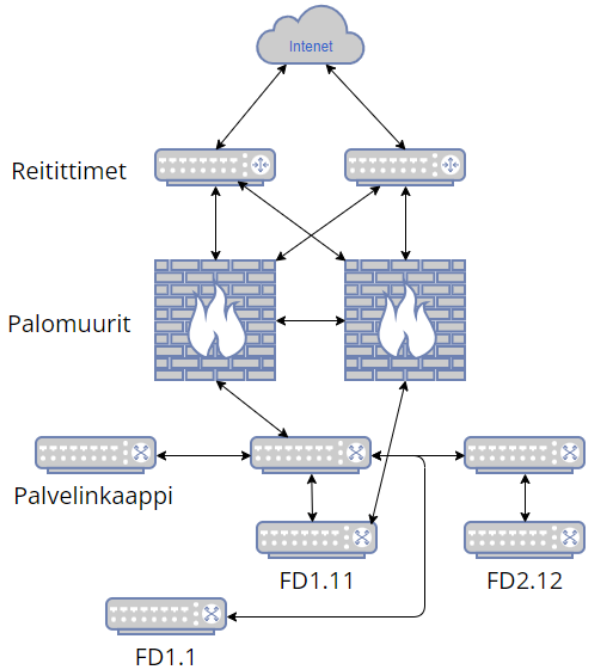
KUVA 3. Tyypillinen SOHO-verkkotopoliga ja sen jäsenet. (4.)

3.3 Projektin kohteeseen valittu verkkotopologia

Verkkotopologia on arkkitehtuurin osa, joka esittää fyysisen kerroksen, johon kuuluu verkkolinkit sekä verkon jäsenet. Se esittää verkkoyhteyksien rakenteen ja verkon yhteyksien muodostumisen. Verkkotopologioita on muutamia erilaisia, joista valitsin kohteen verkkoon tähtitopologian. Valitsin sen topologian, koska se on helppo toteuttaa kohteen ympäristössä ja se on tehokas ja helposti hallittava verkkotopologia. Parhaat vaihtoehdot mielestäni olivat tähtitopologia tai sitten rengastopologia. Rengastopologia on vikasietoisempi perusrakenteeltaan, mutta siihen uusien laitteiden lisääminen häiritsee aina verkkoa. Myös liikenne on hitaampaa, kun liikenne kulkee kerrallaan vain yhteen suuntaan. Lisäksi rengastopologia on vaikea konfiguroida verrattuna tähtitopologiaan, sillä se vaatii takaa konfigurointia, että se toimii oikealla tavalla. En kokenut ympyrätopologiassa olevan sen vaatimaan työmäärään nähden tarpeeksi etua.

Konfiguroin valmiiksi varalaitteen, mikäli tähtitopologian keskuslaite hajoaa. Kuvassa 4 on projektin kohteeseen toteutettu uusi topologia, joka on nyt toteutettu valokuidulla. Keskuskytkimeen yhdistyy valokuidulla muut kytkimet ja pääyhteys tulee ethernet-kaapelilla palomuurien kautta kahdennettuna kahteen FD1.11 -tilan kytkimiin. Keskuskytkimen rikkouduttua verkon saa nopeasti korjattua

siirtämällä linkit keskuskytkimestä alempaan FD1.11 tilan kytkimeen, johon tulee toinen runkoyhteyden ethernet-kaapelilinkki palomuurilta.



KUVA 4. Projektin kohteen uudistettu verkkotopologia. Topologiamallit ja niiden ominaisuudet

Tässä luvussa on esitettynä erilaisia verkon topologiamalleja ja niiden etuja sekä haittapuolia. (5.)

- Tähtitopologia

  Edut:

  - Yksinkertainen rakenne.
  - Helppo ylläpitää.
  - Helppo lisätä uusia laitteita.
  - Nopea.

  Haittapuolet:

  - Ei ole vikasietoinen kun, kaikki liikenne kulkee yhden solmun kautta.

- Rengastopologia

  Edut:

  - Vikasietoinen kun, liikenne voi kulkea kahteen suuntaan.
  - Ei tarvitse keskuslaitetta.

Haittapuolet:

- Liikenne on hitaampaa, kun liikenne voi kulkea vain yhteen suuntaa renkaassa.
- Laitteen hajoaminen vaikuttaa koko verkkoon, kun laitteen hajotessa spanning tree luo varayhteyden.
- Uusien laitteiden lisäämien vaikuttaa koko verkkoon, kun spanning tree joutuu luomaan varayhteyden.
- Haastava konfiguroida.
- Vaikea etsiä vikaa vikojen ilmentyessä.

- Väylätopologia

Edut:

- Kustannustehokas.
- Tehokas pienissä verkoissa.
- Helppo lisätä uusia laitteita ja poistaa laitteita.

Haittapuolet:

- Ei ole toteutuskelpoinen nykyaikaisessa toimistoympäristössä.
- Ei ole vikasietoinen, kun kaikki yhteydet ovat yhden kaapelin varassa.
- Hidas isommissa verkoissa, kun kaikki liikenne menee yhtä väylää pitkin.

- Silmukkatopologia

Edut:

- Hyvin vikasietoinen kun kaikki yhteydet ovat kahdennettu.

Haittapuolet:

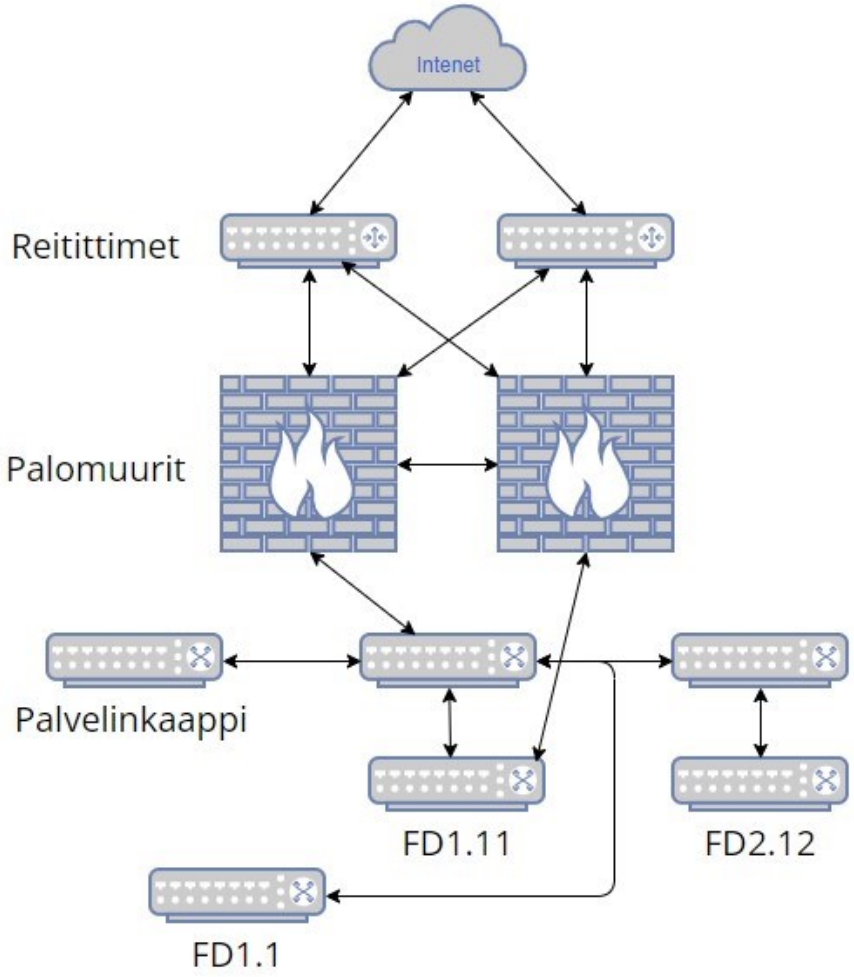
- Haasteellinen konfiguroida.
- Vaikea hallittava.
- Vaatii paljon kaapelointia.

Table -1: ANALYSIS OF DIFFERENT TOPOLOGIES

Parameters	BUS	STAR	RING	MESH	TREE
Installation	easy	easy	difficult	difficult	easy
Cost	inexpensive	expensive	moderate	expensive	less
Flexible	yes	yes	no	no	yes
Reliability	moderate	high	high	high	moderate
Extension	easy	easy	easy	poor	easy
Robust	no	yes	no	yes	no

TAULUKKO 2. Eri verkkotopologioiden ominaisuudet. (5.)

Tähtitopologia oli helppo toteuttaa kyseiseen verkkoon. Se vaati trunk-porttien konfiguroinnin kaikkiin kytkimiin. Trunk-portteihin kytkettiin valokuitumoduulit ja valokuitulinkit kytkettiin keskuskytkimen valokuituportteihin. Laitetiloista oli suorat valokuituyhteydet keskuskytkimeen, joka toimii solmukohtana. Kuva 5 esittää verkon uudistetun topologiamallin.



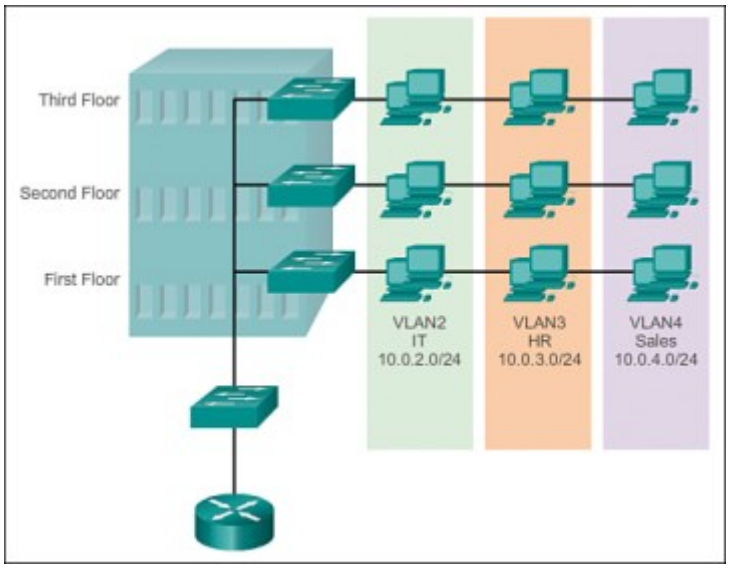
KUVA 5. Uudistettu verkkotopologia projektin kohteen toimistoverkossa.

4 VIRTUAALILÄHIVERKOT

Tässä luvussa kerrotaan teoriaa virtuaalilähiverkoista ja niiden käyttötarkoituksista. Projektin kohteeseen oli tarpeellista luoda uusia verkkosegmenttejä ja ne toteutettiin VLAN-verkoilla ja aliverkoilla. Luvussa on myös esitelty erilaisia VLAN-teknologioita. VLAN-verkoilla voidaan parantaa tietoliikenneverkon tietoturvaa oikealla tavalla hyödynnettynä, mutta VLAN-verkot voivat kuitenkin monimutkaistaa verkon ylläpitoa. Tässä luvussa käsitellään myös VLAN-verkkojen hyötyjä sekä mahdollisia haittapuolia.

Virtuaalilähiverkon auki kertomiseen paras tapa lienee se, että vertaa asiaa analogiseen versioon virtuaalisesta lähiverkosta. Virtuaalinen lähiverkko on verkon osa, jonka päätelaitteet kommunikoivat keskenään ikään kuin ne olisivat liitettyinä samaan kaapeliin. Esimerkiksi voidaan kuvitella tilanne, jossa toimiston käytävän kaikki viisi tietokonetta olisivat kytkettynä samaan kaapeliin. Tässä tapauksessa ei muista verkoista ole pääsyä tähän verkkoon, ellei sitä erikseen kytketä kiinni tähän verkkoon. Tällä tavalla käytävä muodostaa oman lähiverkkonsa. Tämä olisi vanhanaikainen väylätopologia missä kaikki laitteet ovat kytkettyinä samaan kaapeliin. Sen sijaan VLAN-verkko perustuu loogisiin yhteyksiin fyysisten yhteyksien sijaan, jolloin laitteen sijainnilla ei ole merkitystä. Virtuaalilähiverkoilla voidaan muodostaa virtuaalisia verkkoja esimerkiksi verkossa olevien päätelaitteiden käyttötarkoituksen, organisaation tai tietoturvaprioriteetin mukaan.

Virtuaalilähiverkkojen määrittäminen mahdollistaa verkkojen jakamisen pienempiin osiin mikä tehostaa verkon toimintaa, vähentää muun muassa tietoliikenneruuhkia ja lisää tietoturvaa kyseisessä tietoliikenneverkossa. Kuva 6 esittää toimistorakennusta, jossa on kolme kerrosta ja työasemat ovat jaettu virtuaalisiin lähiverkkoihin. (6.)

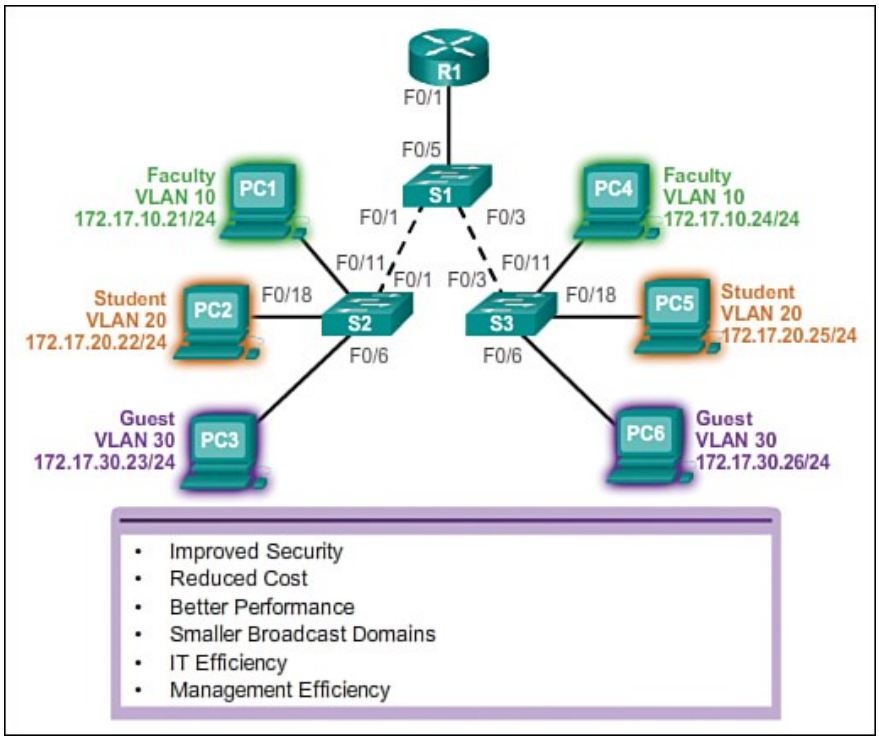


KUVA 6. Virtuaalilähiverkot (6.)

4.1 VLAN-segmentoinnin edut ja heikkoudet

Tässä kappaleessa käsitellään verkon VLAN-segmentointia ja käydään läpi mitä etuja sen avulla saavutetaan, kun verkko segmentoidaan. Kuva 7 esittää VLAN-verkkojen etuja.

- Segmentoinnin edut. (6.)
    - Verkon segmentointi vähentää tietoliikenneruuhkia ja lisää verkon suorituskykyä, kun broadcast liikenne vähenee. Kuten kuvassa 3 esitetään, on laitteita kuusi kappaletta, mutta liikenne tapahtuu silti vain kolmessa segmentissä.
    - Se lisää tietoturvallisuutta verkossa, kun eri palvelut ovat omissa verkoissaan. Esimerkiksi tilanteessa, jossa verkkolaite saastuu se ei pääse saastuttamaan kaikkia lähiverkon laitteita sillä saastuminen rajoittuu tähän virtuaalilähiverkkoon.
    - Helpottaa verkon ylläpitoa, kun tiedetään valmiiksi mihin verkkoon uudet laitteet kytketään. Samat vaatimukset omaavat laitteet jakavat saman VLAN: in.
    - Projektien hallinta helpottuu, kun projektit, tuotekehitys tai sovellusympäristöt voidaan laittaa omaan verkkoonsa.
    - VLAN-verkottaminen tuo joustavuutta aliverkkojen välisten yhteyksien luomiseen.



KUVA 7. VLAN segmentoinnin edut. (6.)

Virtuaalisia lähiverkkoja ei itsessään olla kehitetty parantamaan tietoliikenneverkon tietoturvaa, mutta oikein käytettynä ne lisäävät verkon luotettavuutta ja tietoturvallisuutta.

- VLAN:it lisäävät verkon monimutkaisuutta. Laajoissa tietoliikenneverkoissa VLAN-verkon ylläpito on vaikeaa ja vaatii tarkkaa suunnittelua ja jatkuvaa valvontaa sekä tarkkaa dokumentaatiota. Verkon monimutkaisuus lisää mahdollisuuksia virheellisille määrityksille. Tällaisessa tilanteessa dokumentaation laatu on ratkaisevaa. (7.)

- Kun verkko on monimutkainen VLAN-verkko virheelliset konfiguraatiot aiheuttavat herkästi tietoturva-aukkoja. (7.)

- VLAN:it rajoittavat kommunikaatiota. Mikäli toisesta vlan-verkosta halutaan kommunikoida toiseen vlan-verkkoon, joudutaan aina konfiguroimaan yhteys erikseen. (7.)

- Mikäli tietyssä vlan-verkossa on saastunut laite se saastuttaa kaikki samassa vlan-verkossa olevat laitteet. Tässä käy ilmi sekä vlan-verkkojen heikkous sekä vahvuus. (7.)

4.2 Aliverkottaminen ja VLAN-verkottaminen

On syytä ajatella aliverkot ja VLAN-verkot erillisinä asioina. Nämä eivät ole toisiaan pois sulkevia teknologioita. Internetin keskustelufoorumeilta kävi ilmi, että usein ajatellaan VLAN-verkottamisen olevan tarpeetonta, jos verkko on jo aliverkotettu tai toisinpäin. VLAN-verkkojen käyttäminen oli mielestäni paras ratkaisu sillä se vähentää kaapelointia ja niiden avulla tietoturvan lisääminen verkkojen välillä on yksinkertaista. Mikäli ei käytä VLAN-verkkoja ollenkaan jokainen aliverkko pitää kaapeloida erikseen reitittimelle sekä jokainen verkko vaatisi oman kytkimen, joten se ei ollut mahdollista toteuttaa tällä tavalla. Tämä ei ollut mahdollista rajallisten reitittimen porttien ja rajallisen kytkin kapasiteetin vuoksi. Kuva 10 esittää eroavaisuudet VLAN-segmentoinnin ja fyysisen segmentoinnin välillä. Molempia teknologioita voidaan käyttää liikenteen hallintaan, suorituskyvyn parantamiseen ja tietoturvan lisäämiseen. (7.)

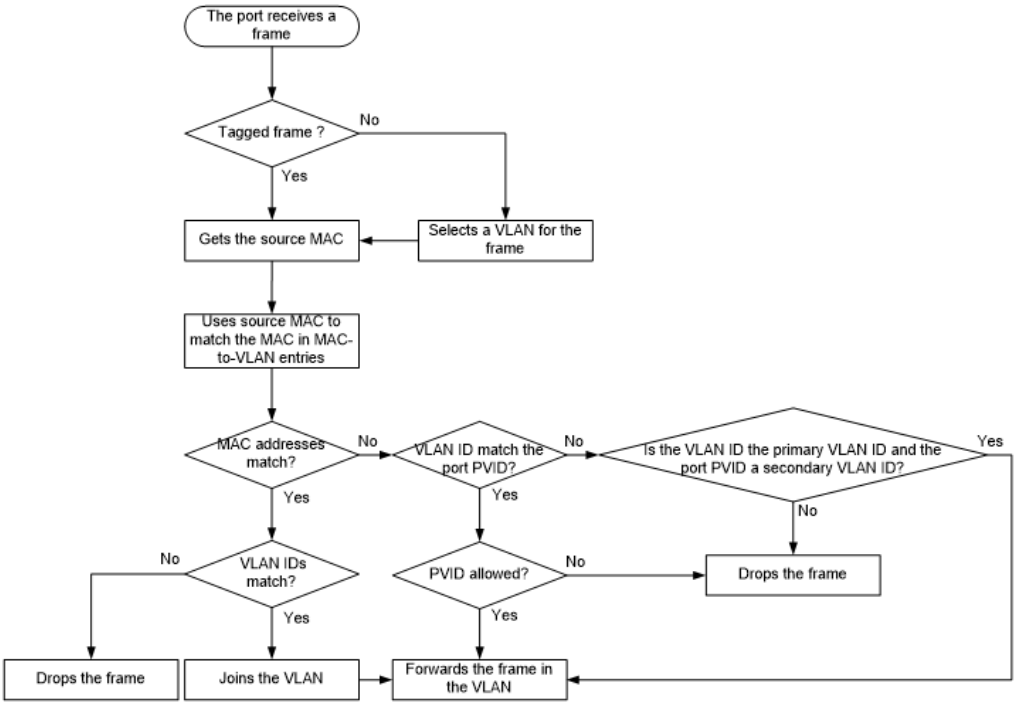
VLAN-verkottamien on oikein käytettynä enemmän tietoturvaa lisäävä elementti, jolla rajoitetaan verkkojen välistä liikennettä. VLAN-verkoilla on helppo lisätä tietoturvaa verkossa ja jakaa oikeuksia tiettyihin verkkosegmentteihin. VLAN-verkkoja käytettäessä joutuu konfiguroimaan yhteydet erikseen jokaisen verkon välille, mikäli niille on tarvetta. VLAN-verkot ja aliverkot toteuttavat samoja ominaisuuksia verkon suorituskykyyn, tietoturvaan ja liikenteenhallintaan liittyen.

4.3 MAC-osoitepohjainen VLAN-verkko

MAC-pohjainen VLAN-verkko on VLAN-verkko malli, jossa kytkin osaa laittaa portin oikeaan VLAN-verkkoon laitteen MAC-osoitteen perusteella. Tämä on dynaaminen malli, joka toimii hyvin muuttuvassa ympäristössä, jossa laitteet vaihtavat sijaintia usein. Tällä VLAN-verkko ratkaisulla vältetään siltä, että portti pitäisi joka kerta konfiguroida uudestaan, kun laitteen sijainti vaihtuu eri sijaintiin ja eri kytkimeen.

Tämä verkkomalli vaatii MAC-osoitteiden ylläpitoa. Suuressa verkossa, jossa on esimerkiksi paljon toimipisteitä ja toimipistekohtaisia lähiverkkoja on MAC-osoitteiden listausta työläs ylläpitää. Kuva 8 esittää toimintalogiikan MAC-osoitepohjaisesta VLAN-verkossa. Kytkin vertaa MAC-osoitetta listaan, jossa on mihin verkkoon mikäkin MAC-osoite kuuluu ja osaa sen avulla laittaa portin oikeaan virtuaalilähiverkkoon.

Projektin kohteen verkossa MAC-osoitepohjainen VLAN-verkko ei ole hyvä ratkaisu. Työasemat ja muut laitteet eivät liiku fyysisesti paikasta toiseen, joten staattinen VLAN-verkko on ylläpidon kannalta parempi ratkaisu. MAC-osoitepohjaisen VLAN-verkko olisi liian työläs ylläpitää ja konfiguroida käyttöön sen etuihin nähden. Verkkoon tulee pääsynhallinta, joten kyseisellä VLAN-verkkomallilla ei saavutettaisi hyötyjä.

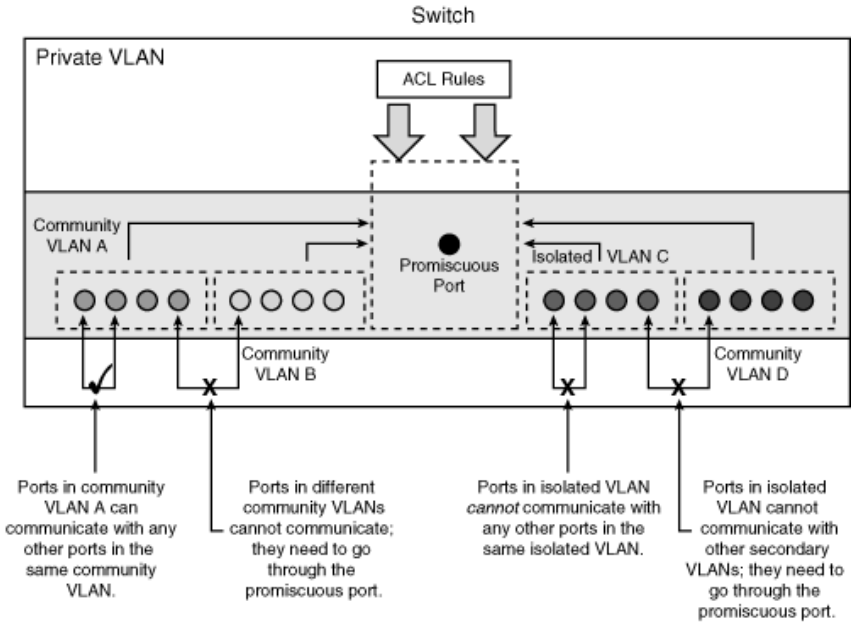


KUVA 8. MAC-osoitepohjaisen VLAN verkon toimintalogiikka. (8.)

4.4 Private VLAN

Privaatti VLAN on OSI-mallin siirtoyhteyskerroksen vlan teknologia, jolla voi estää päätelaitteiden välisen liikenteen tietyn VLAN-verkon sisällä, mikäli laitteet eivät tarvitse yhteyttä toisiinsa. Yksinkertaistettuna tällä teknologialla voi jakaa VLAN-verkkoja pienempiin osiin. Esimerkiksi tällä teknologialla voitaisiin eristää kerrostaloasuntojen verkot omiin privaattiverkkoihin, vaikka ne ovatkin saman VLAN:in alla. Privaatit VLAN-verkot lisäävät myös tietoturvaa, kun laitteiden välinen liikenne voidaan estää tällä teknologialla. Private VLAN teknologialla voidaan estää muun muassa ”ARP spoofing” hyökkäyksiä, sillä ARP-kyselyä ei voi tehdä privaatti VLAN:ssa, kun yhteyttä ei ole toisiin päätelaitteisiin.

Kuvassa 9 näkyy kuinka privaatti VLAN toimii. Privaatin VLAN-verkon alle voi määritellä VLAN-yhteisöjä, joissa on tietyt portit. On myös mahdollista käyttää eristettyä VLAN:ia VLAN-yhteisön sijaan. Tietyn VLAN-verkon sisällä päätelaitteilla, jotka ovat VLAN yhteisön sisällä on yhteys toisiinsa, mutta ei yhteyttä toisen yhteisön päätelaitteisiin. Eristetyt portit eivät voi kommunikoida keskenään vaikka olisivatkin samassa eristetyssä virtuaalilähiverkossa. Yhteisössä olevat portit eivät myöskään voi kommunikoida toisen yhteisön porttien kanssa tai eristettyjen porttien kanssa. (9.)



KUVA 9. Private VLAN toimintaperiaate. (9.)

5 PROJEKTIN KOHTEEN VERKON UUDISTUKSEN TOTEUTUS

Toimiston yleiseen laitekantaan kuului kytkimiä, reititin, palomuurit, työasemia, palvelimia, tulostimia ja erilaisia kehitysorganisaation testattavia laitteita ja tuotteita. On tärkeää selvittää millaisia laitteita oli yrityksen verkossa. Verkon segmentointia lähdettiin suunnittelemaan kohteen verkon laitekannan pohjalta, eri laitteet kuuluvat eri riskiryhmään ja niillä on eri käyttötarpeita.

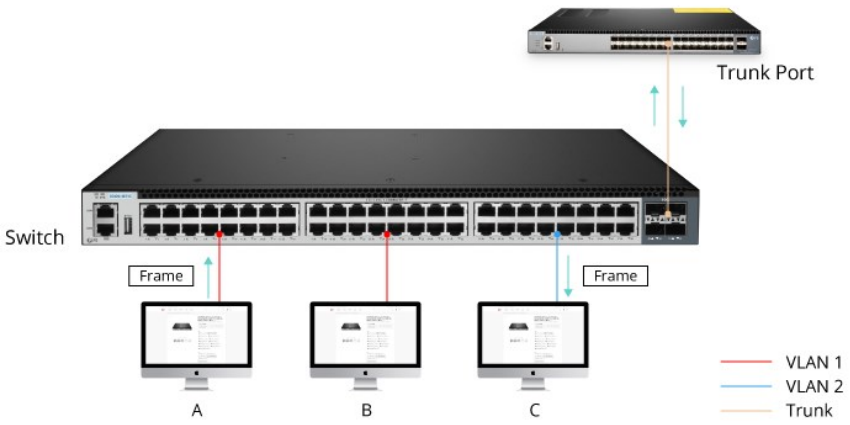
Verkon osalta liityntäkerroksessa toimii Aruban ja HPE:n kytkimiä. Käytössä on kolme kappaletta Aruba CX 6000 -sarjan kytkimiä sekä kaksi Aruba 2530 -sarjan kytkintä sekä yksi HPE OfficeConnect 1820 -sarjan kytkin. CX 6000 -sarjan kytkimissä on PoE eli power over ethernet -ominaisuus, joten langattoman verkon tukiasemat eivät tarvitse erillistä virtalähdettä. Tämä yksinkertaistaa verkon ylläpitoa ja vähentää kaapelointia.

6 SEGMENTOINTIIN TARVITTAVAT LAITTEET

Palomuuri on laite tai ohjelmisto, jolla voidaan rajoittaa liikennettä verkkojen välillä tai liikennettä julkisen verkon ja sisäverkon välillä. Sitä voidaan käyttää myös kirjaamaan liikennettä ja valvomaan liikennettä. Palomuurit ovat tietoliikenneverkkojen tietoturvan peruspilareita. (10.)

Reitittimet reitittävät liikennettä julkiseen internettiin ja paikallisten aliverkkojen välillä. Se toimii ikään kuin tienviittana, joka ohjaa liikennettä oikeaan paikkaan. Reitittimellä voidaan määrittää ali-verkkoja, vlan-verkkoja, aliverkon peitteitä sekä DHCP-osoitealueita verkoille.

Kytkin on verkkolaite, joka yhdistää kaapelilla kytkimeen yhdistetyt laitteet kuten esimerkiksi tieto-koneet, palvelimet, tukiasemat ja IOT-laitteet lähiverkkoon eli LAN-verkkoon. Kytkimiin voidaan konfiguroida VLAN-verkkoja porttikohtaisesti access-portteihin mikä erottelee laitteet omiin VLAN-verkkoihinsa. Kuvassa 10 esitetään yksinkertaistettu kuva access-porteista, trunk-porteista ja VLAN-verkoista. (11.)



KUVA 10. VLAN-verkot kytkimessä. (12.)

7 SUORITUSKYKY

Suorituskyky verkkolaitteissa on täysin riittävä. Kytkimien suorituskyky riittää mainiosti pienessä toimistoverkossa. Palomuurit pystyvät käsittelemään datamäärän hyvin, eikä yrityksessä olla havaittu sen aiheuttavan pullonkaulaa verkkoon. Tietoliikenteen määrää vähennettiin verkossa alkutilanteeseen nähden, joten ei ole huolta laitteiden ylikuormittumisesta. Yrityksen palveluja siirrettiin toimipisteiden välillä ja tällä tavalla saatiin vähennettyä liikenteen määrää projektin kohteen toimistoverkon palomuurilla.

Uudessa verkossa ei esiintynyt tarvetta ottaa käyttöön IPv6-verkkoja. Projektin kohteen uudistettu verkko säilyi IPv4-verkkona. IPv6-verkon käyttöönotolle ei olisi suuria esteitä. Verkkolaitteet tukevat IPV-6 osoitteita. IPV-6 verkkojen käyttöönotto vaatisi palomuurisääntöjen ja DHCP-asetusten muuttamista.

7.1 Segmentointimenetelmät

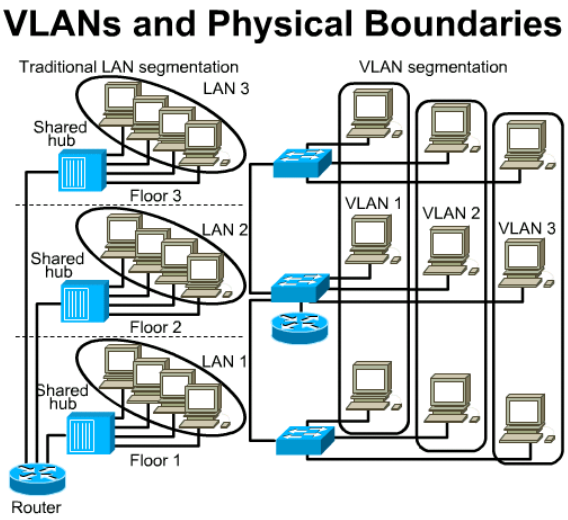
On olemassa muutamia menetelmiä, jotka soveltuvat toimistoverkon segmentointiin. Niihin lukeutuu fyysinen segmentointi ilman virtuaalilähiverkkoja, ohjelmistolla toteutettava mikrosegmentointi, portti eristäminen ja privaatit virtuaalilähiverkot. Kappaleessa 6.2 on esitetty tarkemmin privaatit virtuaalilähiverkot ja porttien eristäminen.

7.2 Toteutustavan valitseminen

Valitsin toteutusmenetelmäksi perinteisen VLAN-segmentoinnin ja aliverkottamisen. Perinteinen VLAN-segmentointi ja aliverkottaminen ei vaadi erillisiä kustannuksia, ja ne ovat molemmat tietoturvaa lisääviä elementtejä ja edelleen toimivia ratkaisuja toimistoverkossa. Uusia verkkoja tuli kohtuullinen määrä, joten hallittavuus pysyi selkeänä. Verkkoon harvoin halutaan uusia laitteita, joten ylläpitokaan ei vaadi resurssien lisäämistä.

7.3 Fyysinen segmentointi

Fyysisessä segmentoinnissa jokaisen kytkimen tai keskuksen täytyy olla erikseen kytkettynä reitittimelle. Fyysisesti segmentoidussa verkossa paikallisen verkon päätelaitteiden pitää olla samassa paikassa, jotta kaapelointi onnistuu. Tässä tilanteessa VLAN-verkkoja ei ole käytössä, joten laitteiden on pakko olla samassa keskuksessa tai kytkimessä kiinni, jotta ne saavat näkyvyyden toisiinsa. Tällainen ei ole mahdollista projektin kohteen toimistossa, joten VLAN-segmentointi on parempi. VLAN-segmentoinnissa riittää yksi linkki reitittimelle, jossa VLAN-verkot ovat konfiguroituna. Mikäli VLAN-verkkojen välisen liikenteen haluaa tehdä reitittimellä kuvan mukaisella tavalla, se onnistuu myös reitittävillä kytkimillä. VLAN-reititys kannattaa tehdä kytkimillä, jotta liikenne ei muodosta reitittimelle menevään linkkiin pullonkaulaa. VLAN-segmentoinnissa päätelaitteen sijainnilla ei ole väliä, joten sellainen sopii paremmin nykyaikaiseen toimistoympäristöön. Kuva 11 esittää topologiakuvan VLAN-verkosta ja fyysisesti segmentoidusta verkosta. (13.)

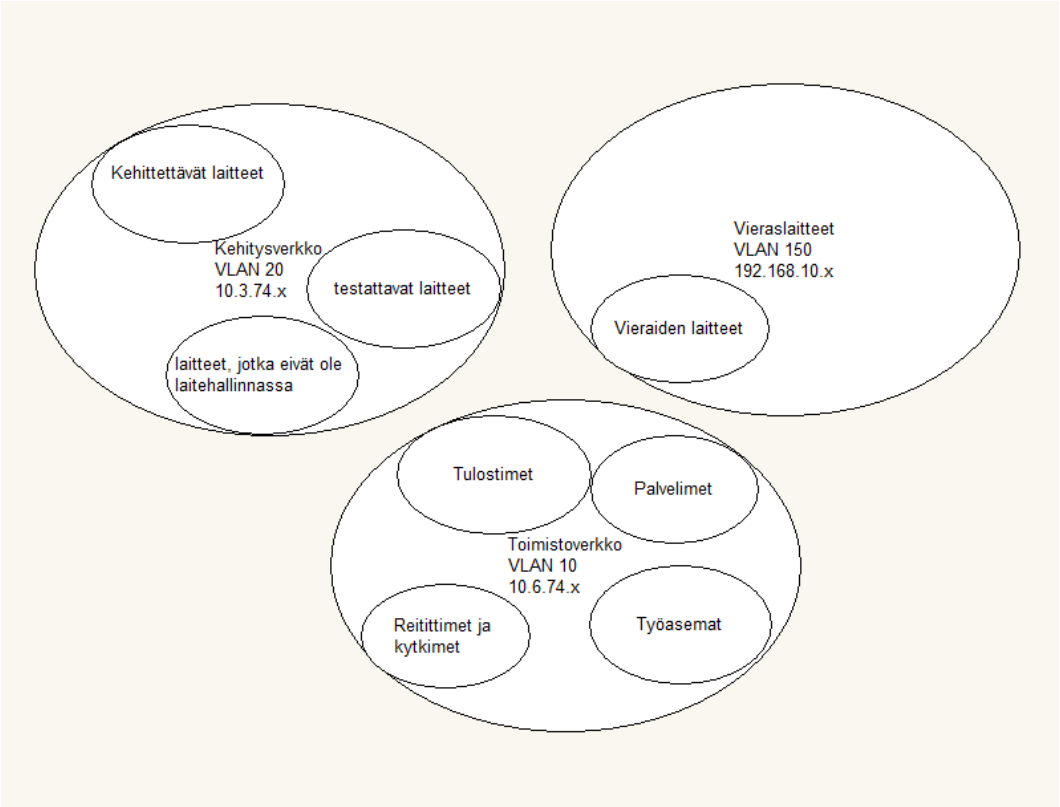


KUVA 11. VLAN-segmentoinnin ja fyysisen segmentoinnin eroavaisuudet. (13.)

7.4 Segmentoinnissa huomioitavat asiat

Ensimmäisenä selvitettiin minkä vuoksi segmentointi haluttiin toteuttaa ja mitkä segmentoinnin edut ovat. Syitä olivat tietoturva, hallittavuus ja tehokkuus. Suurimapa tarpeena koettiin tietoturvan lisääminen toimiston tietoliikenneverkossa. Toisena on varmistettava, että laitekanta on oikeanlaista, jotta verkon segmentointia voidaan toteuttaa. Toimistotta löytyi tarvittavat laitteet segmentointiin eli kytkimet, reitittimet ja palomuurit. Tärkein asia segmentoidun verkon toimivuuden kan-

nalta oli selvittää tarpeelliset verkkojen väliset yhteydet. Kun verkkoa segmentoidaan, täytyy palomuuriin konfiguroida sääntöjä, jotka mahdollistavat liikenteen rajoittamisen verkkojen välillä. Kuva 13 esittää yksinkertaistetun kuvan lähtötilanteen verkoista ja niissä olevista laitteista. Kuvasta voidaan huomata, että toimistoverkossa on tulostimia ja palvelimia, jotka olisi syytä olla omissa verkoissaan.



KUVA 13. Yksinkertaistettu verkkokuva lähtötilanteen verkoista.

7.5 Kohteen lähiverkon segmentoinnin suunnitelma

Palastelin verkon uudelleen rakentamisen pienempiin osiin. Sen pystyi jakamaan fyysiseen osaan ja virtuaaliseen osaan. Fyysinen osa kattaa laiteasennukset ja verkon fyysiset yliheitot, missä muutetaan verkkoa tai otetaan uusia laitteita käyttöön. Virtuaalinen osa on uusien verkkojen konfigurointi kytkimiin, reitittimiin ja palomuuriin. Ideana oli ensin rakentaa verkko fyysiseltä osalta valmiiksi ja sen jälkeen konfiguroida halutut ominaisuudet verkkoon.

1. Ensimmäisenä tein listausta laitteista mitä on kohteen verkossa ja sen pohjalta lähdin pohtimaan mitkä laitteet on syytä olla omissa verkoissaan. Selvitin myös perinpohjaisesti, miten lähtötilanteen verkko rakentui ja millainen oli sen topologia. Loin suunnitteluohjelmalla

verkon topologiasta dokumentteja, jotka helpottivat ymmärtämään verkon rakennetta ja toimintaa. Niitten avulla oli myös helppo suunnitella muutoksia ja dokumentoida muutoksia.

2. Seuraava vaihe oli ottaa käyttöön yrityksen ostamat uudet kytkimet ja asentaa ne paikalleen ja testata niiden toimivuus. Konfiguroin ne toimimaan samanlailla, kun vanhatkin kytkimet, joten tässä vaiheessa ei verkkoon tullut muutoksia.

3. Kolmannessa vaiheessa suunnittelin millaiselle segmentoinnille oli tarvetta. Jaottelin verkon järkeviin segmentteihin verkkolaitteiden käyttötarpeiden ja riskialttiuden perusteella. Tässä vaiheessa myös määriteltiin VLAN ID:t ja verkkojen osoitteet. Vaiheet 4 ja 5 toteutetaan käytännössä myöhemmin, niitä ei toteutettu tämän projektin aikana.

4. Neljäs vaihe on tilata operaattorilta työ, jossa konfiguroidaan uudet verkot reitittimille ja palomuureille.

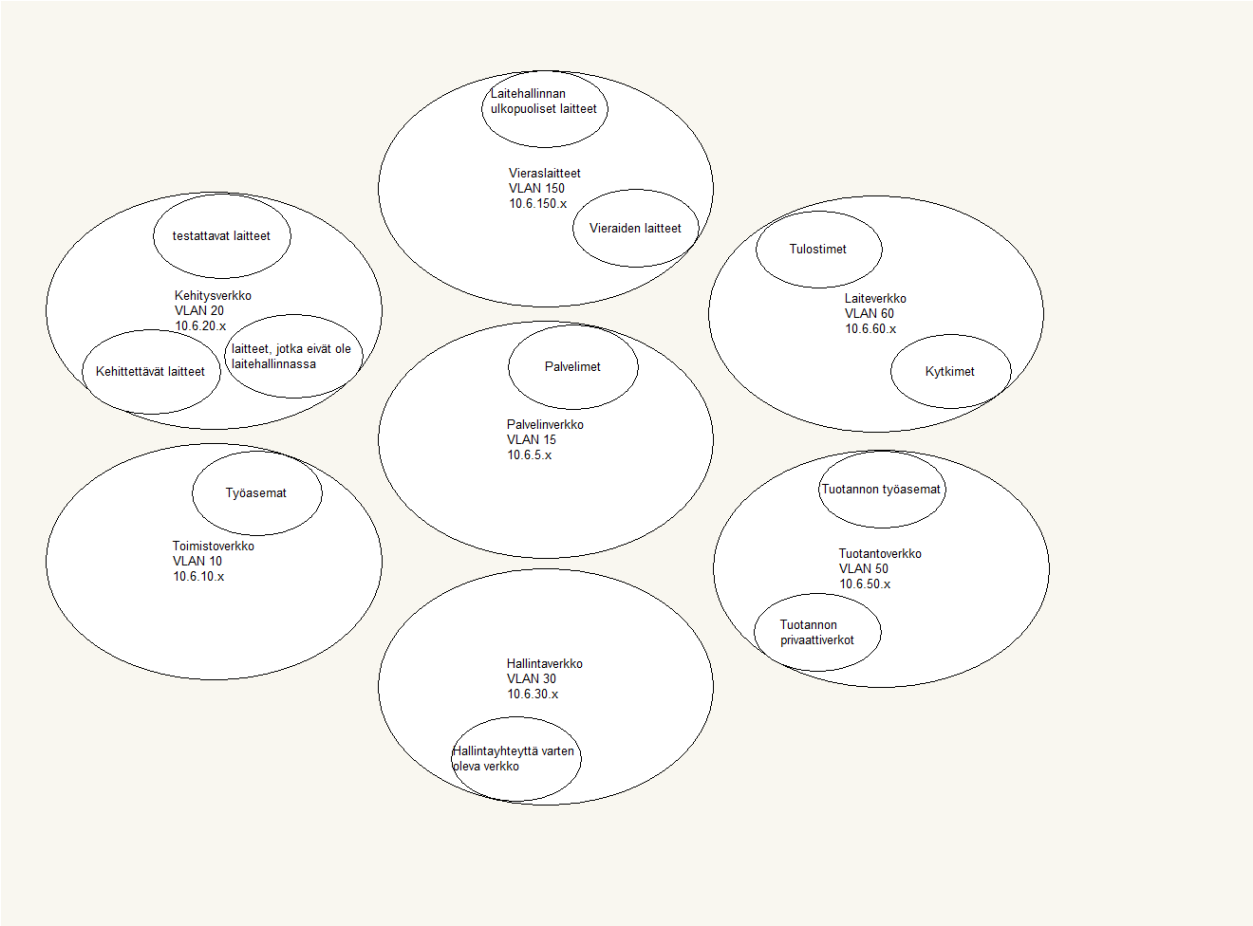
5. Viimeinen vaihe on tutkia ja analysoida verkkoliikennettä ja rakentaa palomuurisäännöstö sen pohjalta. Verkkojen välisitä yhteyksistä, protokollista ja porteista ei ollut dokumentaatiota, joiden pohjalta palomuurisäännöstö haluttiin luoda, joten se pitää toteuttaa tutkimalla verkkojen välistä liikennettä. Esimerkiksi WireShark pakettianalysointiohjelmalla voidaan tarkastella liikennettä ja palomuurin monitorointitilaa voidaan myös hyödyntää liikenteen analysoimiseen.

8 KOHTEEN LÄHIVERKON SEGMENTOINNIN TOTEUTUS

Tässä kohteessa verkon segmentointi tapahtuu OSI-mallin siirtoyhteyskerros-tasolla virtuaalisten lähiverkkojen avulla sekä myös jakamalla verkkoja aliverkkoihin. Lähtötilanteen VLAN-segmentointi rajoittui toimistoverkkoon, kehitysverkkoon ja vierasverkkoon. Segmentaatio toteutettiin pääasiassa tietoturvallisuutta katsoen. Oleellista on siirtää arkaluonteiset laitteet mukaan lukien kytkimet, palvelimet ja tulostimet pois toimistoverkosta, missä on eniten käyttäjiä. Kun käyttäjämäärä on suuri, silloin on myös suurin riski verkon saastumiseen.

Uusi segmentaatio tulee olemaan toimistoverkko, tulostinverkko, tuotantoverkko, kehitysverkko, palvelinverkko, laiteverkko, vierasverkko ja hallintaverkko. DHCP-verkkoprotokolla on käytössä toimistoverkossa, kehitysverkossa ja vierasverkossa. DHCP-verkkoprotokolla tulee myös käyttöön uudessa tuotantoverkossa. Palvelimille, tulostimille ja virtuaalikoneille tulee kiinteät IP-osoitteet. Taulukoissa 2 ja 3 on esitetty uudet verkot mitkä tulivat käyttöön kohteen verkossa. Verkkojen osoitteiden logiikka tulee VLAN ID:n mukaan. Osoitteen kolmas numero kertoo mikä verkko on kyseessä ja se on sama kuin VLAN ID.

Kuva 14 esittää yksinkertaistetun mallin uusista verkoista ja niissä olevista päätelaitteista. Verrattaessa kuvaan vanhasta segmentoinnista huomataan, että tulostimet, palvelimet ja tuotannon laitteet on laitettu omiin verkkoihinsa. Lisäksi on tehty hallintaverkko palvelimen hallintaa varten.



KUVA 14. Uudet verkot ja verkossa olevat päätelaitteet.

8.1 verkkojen väliset riippuvuudet

Nämä säännöstöt luodaan palomuurilla verkkojen välille. Verkkojen välille ei luoda reititystä vaan reititin ohjaa liikenteen palomuurille, jossa on säännöt konfiguroitu verkkojen väliseen liikenteeseen.

Toimistoverkko

- Pääsy palvelinverkon tiedostojakoihin, internettiin, tulostinpalvelimelle.
- Estää hallintayhteys palvelinverkkoon.
- Estää yhteys tuotantoverkkoon, kehitysverkkoon ja vierasverkkoon.

Kehitysverkko

- Pääsy julkiseen internettiin.

- Estää kaikki yhteydet palvelinverkkoon, laiteverkkoon, toimistoverkkoon, tuotantoverkkoon sekä vierasverkkoon sekä sisäänpäin, että ulospäin.

Palvelinverkko

- Hallintayhteys ainoastaan hallintaverkosta.
- Tarvittavat yhteydet toimistoverkkoon ja tuotantoverkkoon tiedostojakoja varten.
- Yhteys internettiin.
- Ei tarvitse yhteyttä kehitysverkkoon ja vierasverkkoon.

Tuotantoverkko

- Pääsy palvelinverkon tiedostojakoihin, tulostimiin, julkiseen internettiin.
- Ei hallintayhteyttä palvelinverkkoon.
- Ei pääsyä muihin verkkoihin.

Hallintaverkko

- Hallintayhteydet laiteverkkoon ja palvelinverkkoon VPN-yhteyden ylitse.
- Internetyhteys.
- Muista verkoista ei ole pääsyä hallintaverkkoon eikä hallintaverkosta ole pääsyä muihin verkkoihin.

Laiteverkko

- Verkkotulostimia ja kytkimiä varten luotu verkko. Tuotanto- ja toimistoverkosta tulostimien asentamiseen tarvittavat yhteydet tulostinpalvelimelle ja tulostamiseen tarvittavat yhteydet tulostimille laiteverkkoon.
- Yhteys palvelinverkkoon tulostinpalvelimelle.
- Hallintaverkosta yhteys kytkimille.
-

Vierasverkko

- Ainoastaan pääsy julkiseen internettiin. Vierasverkko on yrityksen tarjoama langaton verkko toimipisteillä. Ei tarvitse pääsyä muihin sisäverkkoihin tai sisäverkon palveluihin.

TAULUKKO 4. Uudet DHCP-verkot.

VLAN ID	Verkon nimi	Verkko	Maski	Osoitealueet	Kiinteät osoitteet
VLAN 10	Toimisto-verkko	10.6.10.0	255.255.255.0	10.6.10.50–250	
VLAN 20	Kehitys-verkko	10.6.20.0	255.255.255.0	10.6.20.50–250	
VLAN 30	Hallinta-verkko	10.6.30.0	255.255.255.0	10.6.30.50–100	
VLAN 50	Tuotanto-verkko	10.6.50.0	255.255.255.0	10.6.50.50–250	Osittain kiinteät ositteet.
VLAN 150	Vierasverkko	10.6.150.0	255.255.255.0	10.6.150.50–250	

TAULUKKO 5. Uudet staattiset verkot.

VLAN ID	Verkon nimi	Verkko	Maski	Osoitealueet	Kiinteät osoitteet
VLAN 5	Palvelin-verkko	10.6.5.0	255.255.255.0	10.6.5.x	x
VLAN 60	Laiteverkko	10.6.60.0	255.255.255.0	10.6.60.x	x

8.2 Haasteet ja ongelmat

Suurimpana haasteena oli selvittää mistä verkkojen väliset riippuvuudet. Se ei pelkästään riitä, että lisää uudet verkot kytkimiin ja palomuuriin. Verkkojen väliset riippuvuudet pitää selvittää ja verkkojen väliset mahdolliset yhteydet suunnitella ja konfiguroida myös.

8.3 Segmentoinnin lopputulos

Uudet verkot saatiin suunniteltua, mutta palomuurisääntöjä ja kaikkia verkkoja ei saatu konfiguroitua palomuurille ja reitittimille ajan puutteen vuoksi, sillä samaan aikaan oli menossa yritysverkon uudistus. Palomuurisääntöjen luominen oli odotettua haasteellisempi ja aikaa vievämpi projekti kuin aluksi ajattelin, koska verkkojen välisitä riippuvuuksista ei ollut valmista dokumentaatiota. Jokaisen verkon tarpeelliset yhteydet pitää selvittää liikennettä analysoimalla ja sen pohjalta estää kaikki ylimääräinen liikenne verkkojen välillä palomuurisäännöillä. Segmentointi saatiin suunniteltua valmiiksi, mutta toteutus jätettiin myöhemmälle.

9 PÄÄSYNHALLINTA JA ZERO TRUST

Tässä kappaleessa kerrotaan lähiverkon pääsynhallinnan sekä zero trust- mallin teoriaa ja niiden käyttötarkoituksia. Yritys halusi pääsynhallinnan yrityksen palveluihin ja resursseihin sekä myös pääsynhallinnan projektin kohteen sisäverkkoon.

9.1 Pääsynhallinnan määrittely

Pääsynhallinta tietoliikenneverkossa on prosessi, joka estää tuntemattomien laitteiden pääsyn sisäverkkoon ja tunnistaa luotetut laitteet ja kytkee ne oikeaan verkkoon. Verkko tunnistaa, että onko verkkoon pyrkivällä laitteella oikeutta verkkoon. Pääsynhallinta varmistaa, että ainoastaan käyttäjät, jolla on oikeus verkossa oleviin tietoihin, pääsee yhdistämään tarpeellisiin resursseihin ja verkkoon. (14.)

Pääsynhallinnan tarkoitus on lisätä tietoturvaa verkossa hallinnoimalla verkkoon liitettyjen laitteiden pääsyä tiettyihin resursseihin. Pääsynhallinta voi olla esimerkiksi roolipohjainen. Roolipohjaisuus tarkoittaa sitä, että tietyn roolin omistavilla työntekijöillä on pääsy tiettyihin resursseihin. Esimerkiksi toimistotyöntekijöillä ei ole hallintamahdollisuutta palvelimiin mikä on pelkästään organisaation IT-tiimillä.

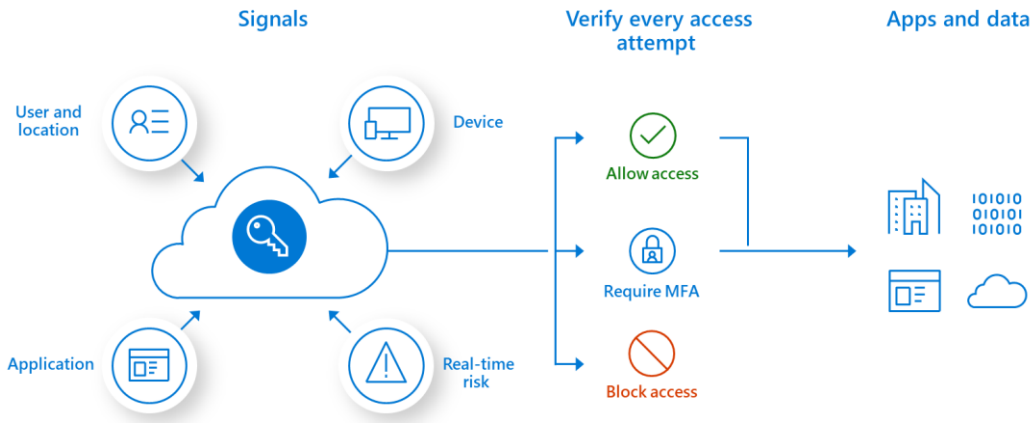
9.2 Zero trust -malli

Zero trust on eräänlainen tietoturvamalli, joka pohjautuu luottamattomuuteen. Zero trust -mallissa ei ole olemassa luotettua sisäverkkoa vaan yrityksen resursseihin tavoitteleva käyttäjä on lähtökohtaisesti aina epäluotettava. (15.)

Käyttäjä joutuu aina tunnistautumaan erilaisin menetelmin. Menetelmiä voi olla esimerkiksi biometriset menetelmät kuten kasvojen tunnistus tai sormenjälkitunnistus tai sitten laitteen sijainti tai laitteeseen kohdistetut vaatimusmäärittelyt. Esimerkiksi Microsoft Windows tarjoaa Windows Hello-ohjelmiston tarjoamia biometrisiä tunnistautumisvaihtoehtoja. Niitä ovat kasvojentunnistus, sormenjälkitunnistus ja PIN-koodi. Laitteen vaatimusmäärittelyt voivat olla esimerkiksi oikea Windows-versio, laitteen ikä, laitteen sijainti tai virustorjuntaohjelmistot.

”Yritysverkon sisältä tuleviin pyyntöihin ei luoteta sen enempää kuin ulkopuolelta tuleviin, vaan käyttäjien ja laitteiden täytyy aina todistaa olevansa oikeutettuja verkon palveluihin tai resursseihin” (16.)

Kuva 15 esittää yksinkertaistetun mallin Zero trust -mallin toimintaperiaatteesta, jossa jokainen yhteyskokeilu hyväksytään tai hylätään vahvan tunnistautumisen kautta. Mikäli laite ei täytä compliance-vaatimuksia tai käyttäjä ei läpäise tunnistautumista kirjautumisyritys hylätään.



KUVA 15. Zero trust- mallin toimintaperiaate. (17.)

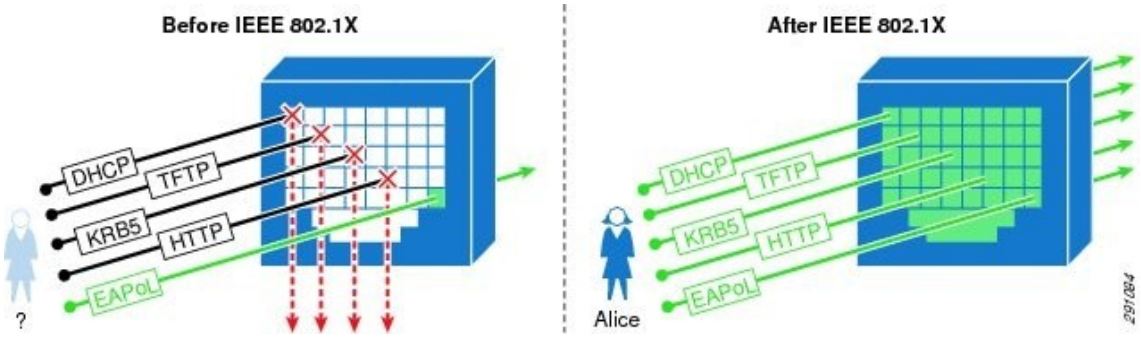
Projektin kohteen ympäristö on osittain pilvipohjainen ympäristö. Osittain pilvipohjainen ympäristö tunnetaan paremmin nimellä hybrid-ympäristö. Se tarkoittaa, että yrityksellä on sekä sisäverkossa toimivia palvelimia ja muita järjestelmiä. Esimerkiksi paikallinen Active Directory ja myös pilviympäristössä toimivia palveluita, kuten esimerkiksi Azure Active Directory. Toimistolla on palvelimia vielä paikallisessa sisäverkossa, joten sisäverkolle on edelleen tarvetta. Usein Zero trust -malli on yksinkertaisin ottaa käyttöön cloud only-ympäristössä, kun ei tarvitse ottaa huomioon paikallista sisäverkkoa. Mikäli hybrid-ympäristöön halutaan ottaa käyttöön Zero trust -mallin, täytyy sisäverkkoon rakentaa oma pääsynhallinta. Esimerkiksi IEEE 802.1x-pääsynhallintamalli on toimiva vielä nykypäivänäkin. Yrityksen sisäverkossa on siihen tarvittava Radius-palvelin. IEEE 802.1x-pääsynhallinta oli jo valmiiksi toteutettu langattomassa verkossa.

Kuva 16 esittää hybrid-ympäristön ja pilvipohjaisten ympäristöjen eroavaisuudet palveluittain. Projektin kohteen ympäristö mukailee hyvin pitkälti kuvassa näkyvää hybrid-ympäristöä.

Kuva 16. Hybrid- ympäristön ja pilvipohjaisten ympäristöjen erot. (18.)

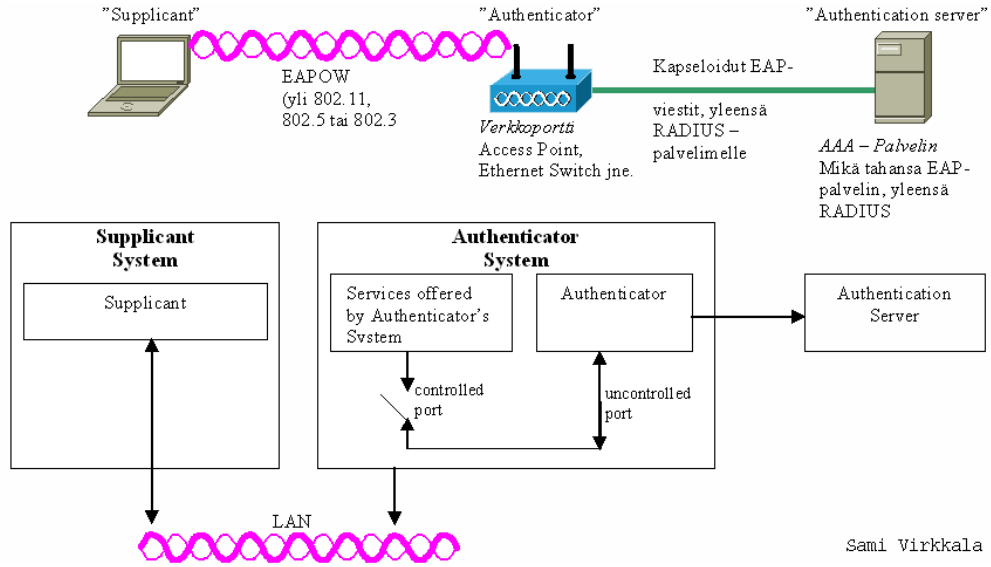
9.3 Lähiverkon pääsynhallinta

IEEE 802.1x-protokolla mahdollistaa porttikohtaisen pääsynhallinnan autentikoinnin avulla. IEEE 802.1x-protokollaa tukeva portti kykenee dynaamisesti sulkeutumaan ja avautumaan käyttäjän tai laitteen identiteetin perusteella. Kuva esittää IEEE 802.1x-protokollan toiminnan periaatteen. Se mahdollistaa laitteen autentikoinnin ensin ja sen onnistuttua se päästää laitteen yhdistämään verkkoon. IEEE 802.1x-protokolla osaa myös dynaamisesti asettaa porttiin oikean virtuaalilähiverkon käyttäjän perusteella. Esimerkiksi tuntemattoman identiteetin IEEE 802.1x-protokolla osaa automaattisesti siirtää vierasverkkoon, kun laite kytketään lähiverkkoon. (19.) (8.)



KUVA 17. 802.1x-protokollan toimintaperiaate portissa. (19.)

IEEE 802.1x-protokolla vaatii toimiakseen autentikaattorin ja autentikointipalvelimen. Autentikaattori on esimerkiksi kytkin tai langaton tukiasema. Autentikaattori toimii liityntäpisteenä päätelaitteelle. Liityntäpisteessä on fyysinen tai virtuaalinen portti joka päästää tai estää liikennettä kulkemasta. Autentikointipalvelin vastaanottaa yhteyspyynnöt ja vastaa niihin. Autentikointipalvelin voi olla esimerkiksi Radius- palvelin, joka tukee EAP- protokollaa. Autentikointipalvelin varmistaa onko laitteella oikea sertifikaatti ja estää hyväksymättömien laitteiden pääsyn verkkoon. Kuva 16 esittää IEEE 802.1x protokollan toiminnallisuuden ja siihen kuuluvat komponentit. (22.)



KUVA 18. IEEE 802.1x toiminnallisuuden komponentit. Sami Virkkala. 2005. (20.)

9.4 IEEE 802.1x protokolla projektin kohteen verkossa

Projektin kohteen verkon laitekannan osalta tämä olisi mahdollista toteuttaa. Toimiston sisäverkko on melko pieni, joten IEEE 802.1x protokollan käyttöönotto ja ylläpito on mahdollista. Toimiston sisäverkko tarvitsee oman pääsynhallintasa, sillä projektin kohteen lähiverkossa ei ole pääsynhallintaa lainkaan. Se on kustannustehokas, sillä IEEE 802.1x pääsynhallinnan käyttöönoton voi toteuttaa jo valmiiksi löytyvillä komponenteilla. Projektin kohteen verkossa pääsynhallinnan käyttöönotolla tavoitellaan sitä, että ulkopuoliset laitteet eli laitehallinnan ulkopuoliset laitteet eivät pääse sisäverkkoon ollenkaan.

IEEE 802.1x voi olla kankea joissakin tapauksissa. Esimerkiksi ulkopuolisilla vierasverkkoon liitetyillä laitteilla. (21.)

Tämän voi ratkaista vierasverkolla, josta ei ole pääsyä sisäverkon palveluihin ollenkaan. Myös haasteita ilmenee kehitysverkossa, jossa testattavat laitteet eivät tue IEEE 802.1x toiminnallisuuksia. Yksi ratkaisu on tehdä MAC-osoite autentikointia, mutta se ei ole toimiva ratkaisu projektin kohteen verkossa, sillä uusia testattavia laitteita on useita ja testattavat laitteet vaihtuvat usein. MAC-osoitteiden listan ylläpito olisi liian työlästä. Paras ratkaisu on sulkea kehitysverkko kokonaan pois pääsynhallinnasta.

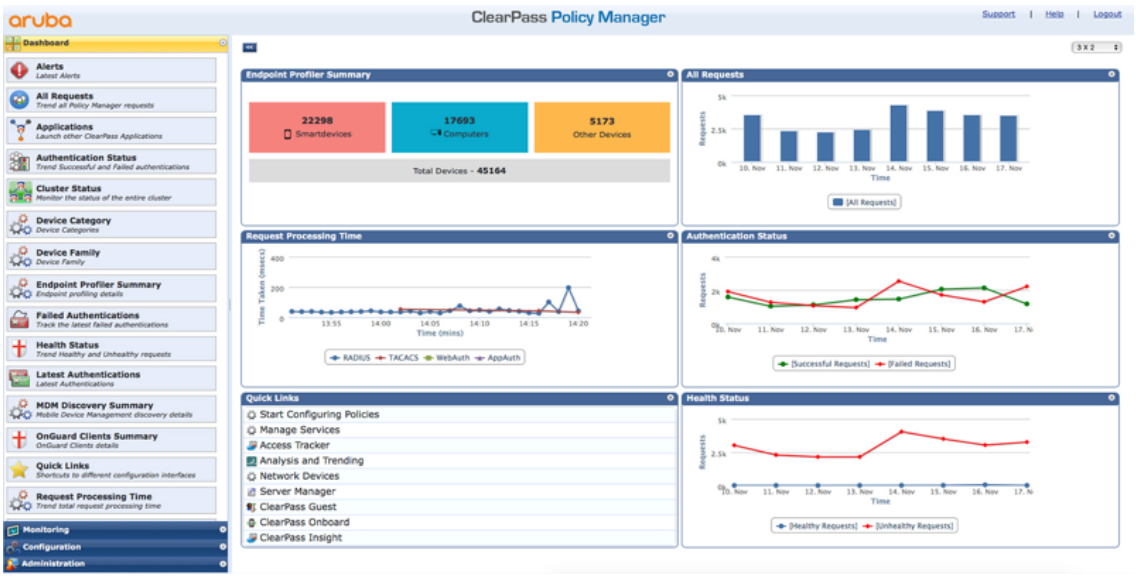
Ongelmia voi myös olla se, että mikäli verkossa on vanhempaa laitekantaa, täytyy niille rakentaa erilainen tunnistautumismenetelmä, jos ne eivät tue IEEE 802.1x protokollaa. Lisäksi verkossa tulee olemaan hieman viivettä, sillä verkkoon ei pääse ennen kuin tunnistautuminen on suoritettu. (22.)

IEEE 802.1x käyttöönotto voi olla monimutkaista sillä se ei itsessään tarjoa mitään käyttöliittymää. Lisäksi NPS-palvelimen konfigurointi on monimutkainen, mikäli asiaan ei ole ennen perehtynyt. Kaupalliset pääsynhallintaratkaisut tarjoavat käyttöliittymän ja usein niiden käyttöönotto on paljon käyttäjäystävällisempää.

10 KAUPALLISET PÄÄSYNHALLINTARATKAISUT

Kupallisia pääsynhallintaratkaisuja on useita. Muun muassa verkkolaitevalmistaja Aruba tarjoaa Aruba ClearPass Policy Manager-nimistä pääsynhallintapalvelua. Myös muilla verkkolaitevalmistajilla ja tietoturvayrityksillä on tarjolla erilaisia pääsynhallintaratkaisuja.

Kaupallisten pääsynhallintaratkaisujen etu on käyttäjäystävällisyys. Ne ovat usein rakennettu siten, että käyttäjällä on näkyvyys ja hallintaoikeudet verkon pääsynhallintaan käyttöliittymän avulla. Ne vaativat lisenssin ostamisen, joten se tuo kiinteitä lisäkuluja organisaatiolle. Kuvassa 17 näkyy Aruba ClearPass Policy manager-palvelun käyttöliittymä, josta on näkyvyys muun muassa verkkolaitteisiin ja laitetyyppeihin sekä pääsynhallinnan seurantaan.



KUVA 19. Aruba ClearPass Policy Manager-palvelun käyttöliittymä. (23.)

11 YRITYSVERKON UUDISTUKSET

Tässä kappaleessa kerrotaan yritysverkon uudistuksesta, joka toteutettiin koko yritysverkkoon projektin aikana. Projektin kohteen yritys siirtyi MPLS-verkosta SD WAN -verkkoratkaisuun.

11.1 Lähtötilanne

Lähtötilanteessa yrityksen WAN-verkko oli MPLS-yritysverkko. Uudessa verkkomallissa siirryttiin SD-WAN verkkoratkaisuun. MPLS-verkko on staattinen yritysverkko, joka yhdistää yrityksen lähiverkot yhdeksi suuremmaksi WAN-verkoksi. Verkossa oli yksi keskitetty palomuurilaite. Palomuurille ei ollut suoraa näkyvyyttä yrityksen IT-tiimillä. Jokainen raportti piti pyytää erikseen operaattorilta. Sen lisäksi myös muutokset verkossa täytyi tilata erikseen operaattorilta mikä oli melko hidas prosessi. Operaattori tarjosi uudistusta uudempaan SD WAN -ratkaisuun vedoten kustannustehokkuuteen.

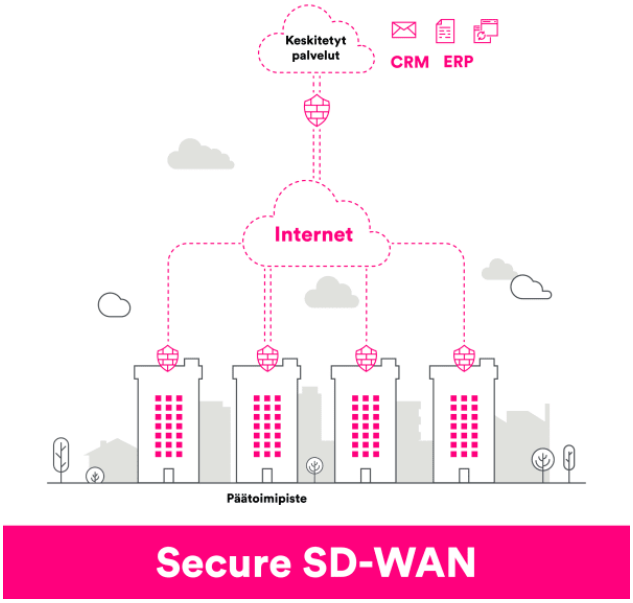
11.2 Uudistukset

Yritysverkko vaihtui vanhammasta MPLS-yritysverkkomallista SD WAN -pohjaiseen yritysverkkomalliin. Uusi SD-WAN verkkomalli on monella tapaa nykyaikaisempi yritysverkkoratkaisu. Se tarjoaa keskitetyn hallinnan, näkyvyyden ja älykkään tietoliikenteen ohjauksen. SD-WAN verkko voi hyödyntää yhteyksissä esimerkiksi internetliittymää, mobiiliverkkoa ja MPLS-verkkoa. (24.)

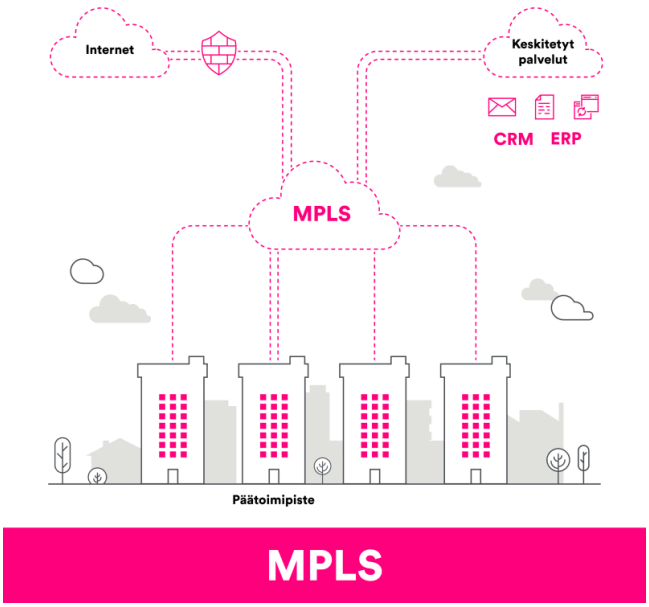
Kohteen toimistoverkon kannalta tilanne muuttui verkkotopologia otsalta siten, että verkot siirrettiin kulkemaan yhtä trunk-kaapelia pitkin reitittimiltä palomuurille ja siitä kytkimiin. Aikaisemmin verkot olivat omissa porteissaan reitittimellä sekä yritysverkossa oli yksi keskitetty palomuuri. Uudessa yritysverkkomallissa jokaiselle toimipisteelle tuli omat palomuurilaitteet sekä oma laajakaistaliittymä. Verkkojen konfigurointi yhteen porttiin helpottaa ja vähentää kaapelointia ja tekee verkkotopologiasta selkeämmän.

Yrityksen IT-tiimi halusi myös itselleen näkyvyyden uusille palomuureille ja reitittimille verkkoliikenteen seuraamista varten ja mahdollisia konfiguraatiomuutoksia varten. Kun IT-tiimillä on näkyvyys verkkoliikenteeseen ja tarpeen vaatiessa mahdollisuus laitteen konfigurointiin on haavoittuvuuksien

havaitseminen ja mahdollisten tietoturvaloukkauksien selvittäminen nopeampaa. Liikenteen seuraamisella voidaan nopeammin jäljittää murto ja tehdä korjaavia toimenpiteitä. Kuvassa 18 näkyy SD-WAN verkon toimintaperiaate. Kuvassa 19 näkyy MPLS-verkon toimintaperiaate.



KUVA 20. SD WAN verkon toimintaperiaate (25.)



KUVA 21. MPLS-verkon toimintaperiaate. (25.)

SD-WAN on helposti muunneltavissa tarpeen mukaan ja siksi sopii hyvin yrityksiin, joilla on useita toimipisteitä. SD-WAN on kustannustehokkaampi ratkaisu, kun aikaisemmin käytössä ollut MPLS-

yritysverkko, kun se pystyy hyödyntämään useita yhteystapoja MPLS-verkkoon nähden. SD-WAN on myös helposti skaalautuva yrityksen liiketoiminnan tarpeiden mukaan ja se tarjoaa myös näkyvyyden yrityksen tietoliikenteeseen. Myös näkyvyys tietoliikenteeseen ja keskitetty hallinta olivat tärkeitä parannuksia, sillä se helpottaa toimimista ongelmatilanteissa. (25.)

12 YHTEENVETO

Opinnäytetyön tuloksena saatiin toteutettua tavoitteissa olleet verkon muutokset verkon topologian osalta sekä suunniteltua verkon segmentointi. Tässä opinnäytetyössä esitellään myös vaihtoehtoja verkon pääsynhallintaratkaisuun sekä käytiin teoriatasolla läpi Zero trust -mallia ja yritysverkossa tapahtuneita muutoksia. Pääsynhallinta ja uudet verkkosegmentit konfiguroidaan käyttöön erillisessä projektissa ajan puutteen vuoksi.

Jatkotoimenpiteitä opinnäyteprojektin jälkeen tulee olemaan pääsynhallintaratkaisun käyttöönotto ja segmentoinnin loppuun vieminen. Segmentoinnin loppuun viemiseen kuuluu palomuurisäännöstön luominen palomuurille ja verkkojen konfigurointi sekä niiden testaaminen. Pääsynhallintaratkaisun käyttöönotto tullaan tekemään segmentoinnin käyttöönoton jälkeen.

Projektin suhteen joitakin asioita jäi suunnittelematta. Niitä oli ainakin porttieristäminen, verkon laitteista lokidataa keräävä toiminallisuus ja verkon redundanttisuuden hiominen vielä hieman paremmaksi. Porttieristämisellä voidaan eristää vielä tarkemmin kriittisiä laitteita. Tätä voi hyödyntää esimerkiksi palvelimilla. Porttieristämisellä voidaan pienentää hyökkäyspinta-alaa entisestään verkossa jakamalla esimerkiksi yksittäisiä palvelimia privaatteihin virtuaalisiin lähiverkkoihin. Privaateista virtuaalilähiverkoista ja porttieristämisestä on kerrottu tarkemmin kappaleessa virtuaalilähiverkot. Verkkoon olisi hyvä lisätä lokidataa keräävä toiminnallisuus. Projektin aikana en kerennyt perehtyä lokidataa kerääviin tekniikoihin. Näkyvyys lokidataan helpottaa ongelmatilanteissa vian selvittämistä. Verkon topologiaa voi parantaa laittamalla verkkokytkimiä renkaaseen. Ne ovat tällä hetkellä tähtitopologiassa, mutta niitä pystyisi kytkemään osittain mesh-topologiaan, joka on redundanttisempi kuin tähtitopologia.

Projektin aikana opin tuntemaan lähiverkon toimintaa sekä kuinka lähiverkkoja rakennetaan ja ylläpidetään käytännössä. Perehdyin myös siihen, miten verkkoja suunnitellaan sekä miten lähiverkkojen muutoksia toteutetaan käytännössä. Omaksuin projektin aikana paljon tietoa tietoturvasta ja siitä, miten organisaation tietoturvaa ylläpidetään ja kuinka se rakentuu monesta osasta mukaan lukien lähiverkkojen tietoturvallisuudesta. Opettelin myös käyttämään erilaisia IT-hallintajärjestelmiä kuten esimerkiksi Entra ID-palvelua ja Defender for endpoint-järjestelmää. Opin kattavasti lä-

hiverkkotekniikoista ja niiden ominaisuuksista sekä organisaation IT-järjestelmän ylläpidosta. Selvät kehityskohde omaa työskentelyä ajatellen on aikatauluttaminen. Minulla oli haasteita aikatauluttaa asioita ja arvioida projektin osuuksien ajallista kestoa mikä toi haasteita projektin aikana.

LÄHTEET

1. Cybernews 2022. We hacked 28000 unsecured printers to raise awarness of printer security issues. Hakupäivä 18.9.2023. https://cybernews.com/security/we-hacked-28000-unsecured-printers-to-raise-awareness-of-printer-security-issues/.

2. Naaym, Gilad David 2023. NTLM authentication security risks and how to avoid them. Haku-päivä 17.11.2023. https://www.networkdatapedia.com/post/ntlm-authentication-security-risks-and-how-to-avoid-them-gilad-david-maayan.

3. Geeksforgeeks 2022. What is a small office home office (SOHO) network? Hakupäivä 13.11.2023. https://www.geeksforgeeks.org/what-is-a-small-office-home-office-soho-network/.

4. A small office/Home office (SOHO) network topology. 2013. Computer Networking demystified. Hakupäivä 6.7.2023. https://computernetworkingsimplified.wordpress.com/2013/06/07/how-will-a-typical-small-officehome-office-soho-lan-look-like/comment-page-1/.

5. Bisht, Nicedita & Singh, Sapna 2015. Analytical study of different network topologies International Research Journal of Engineering and Technology (IRJET) 2 (1), 88-89. Hakupäivä 17.6.2023. https://www.irjet.net/archives/V2/i1/Irjet-v2i120.pdf.

6. Cisco 2014. Networking academy's introduction to VLANs. Hakupäivä 10.6.2023. https://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=4.

7. Chokshi, Rajul & Yu, Chansu 2007. Study on vlan in Wireless Network. Haku-päivä18.6.2023 https://engineering.csuohio.edu/sites/default/files/media/ece/documents/VLAN.pdf.

8. Cisco 2014. Introduction to MAC-based VLAN. Hakupäivä 9.11.2023. https://technhub.hpe.com/eginfolib/networking/docs/switches/5500hi/5998-5328_l2-lan_cg/content/377991805.htm#:~:text=The%20MAC-based%20VLAN%20feature,network%20access%20for%20terminal%20devices.

9. Cisco 2008. Security features of Switches. Hakupäivä 22.7.2023. https://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=13.

10. Cisco 2023. What Is a Firewall? Hakupäivä 17.6.2023. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-fire-wall.html#:~:text=They%20establish%20a%20barrier%20between,or%20private%20cloud%20(virtual).

11. Cisco 2023. What Is an Ethernet Switch? Hakupäivä 25.7.2023. https://www.cisco.com/c/en/us/products/switches/what-is-an-ethernet-switch.html.

12. Irving 2021. VLAN: How does it change your network management? Hakupäivä 27.09.2023. https://community.fs.com/blog/vlan-how-does-it-change-your-network-management.html.

13. VLANS 2013. Hakupäivä 9.10.2023. https://basantshrestha.wordpress.com/2013/02/04/vlan/.

14. Fortinet. 2023. What is network access control? Hakupäivä 22.10.2023. https://www.fortinet.com/resources/cyberglossary/what-is-network-access-cont-rol#:~:text=FortiNAC%20is%20the%20Fortinet%20NAC,%2C%20routers%2C%20and%20IoT%20devices.

15. Elisa 2021. Zero trust – nollaluottamus modernin turvallisen ict-ympäristön perustana. Haku-päivä 5.11.2023. https://yrityksille.elisa.fi/ideat/zero-trust-nollaluottamus-turvaa-ict-ymparistosi/.

16. Lintuala, Markus 2021. Luottamus hyvä, zero trust parempi. Elisa Hakupäivä 15.11.2023. https://yrityksille.elisa.fi/ideat/luottamus-hyva-zero-trust-parempi/.

17. Microsoft 2019. Zero-trust-model-1.png. Hakupäivä 18.11.2023. https://www.microsoft.com/fi-fi/microsoft-365/blog/2019/09/18/why-banks-adopt-modern-cybersecurity-zero-trust-model/attachment/2394/.

18. Tietokeskus 2023. Tietoturva all in one Zero trust defender. Sisäinen lähde.

19. Wikipedia 2023. IEEE 802.1x. Hakupäivä 20.6.2023. IEEE 802.1X - Wikipedia

20. Petryschu, Steve 2021. What is 802.1x. authentication? Hakupäivä 15.10.2023. https://www.auvik.com/franklyit/blog/802-1x-authentication/.

21. Cisco 2011. Wired 802.1X Deployment Guide. Hakupäivä 13.10.2023. https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html.

22. Aruba 2023. Aruba ClearPass OnGuard Software. Hakupäivä 09.11.2023. https://buy.hpe.com/fi/en/networking/aruba-software/aruba-software/aruba-wireless-software/aruba-clearpass-onguard-software/p/1009648564.

23. Arvery, Stanley 2023. Subnets vs VLAN. Orhan Ergun. Hakupäivä 13.7.2023.https://orhanergun.net/subnet-vs-vlan.

24. DNA 2023. Onko yritysverkollesi paras vaihtoehto SD-WAN vai MPLS? Vai molemmat? Hakupäivä 11.11.2023. https://www.dna.fi/yrityksille/blogi/-/blogs/onko-yritysverkollesi-paras-vaihtoehto-sd-wan-vai-mpls-vai-molemmat.

25. DNA 2023. Secure SD-WAN. Hakupäivä 15.11.2023. https://www.dna.fi/yrityksille/tietoliikenneyhteydet/secure-sd-wan?gclid=EAIaIQobChMI0svQspy7gQMVbQuiAx3xlgE7EAAYASAAEgLdAvD_BwE&adfcd=1695282788.MrhHn-xsREKu2PevPFZeXg.OTEwOTg4LDE1MDE2NDQ.