LAPIN AMK
Lapland University of Applied Sciences

VERKKOINFRASTRUKTUURIN MUUTOSTYÖT

Markkanen Onni

Opinnäytetyö

Tieto- ja viestintätekniikka
Insinööri (AMK)

2025

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tieto- ja viestintätekniikka
Insinööri (AMK)

Tekijä	Onni Markkanen	**Vuosi**	2025
Ohjaaja	Kenneth Karlsson		
Toimeksiantaja	Istekki Oy		
Työn nimi	Verkkoinfrastruktuurin muutostyöt		
Sivumäärä	37		

Tämä opinnäytetyö toimii projektisuunnitelmana keskikokoisen yrityksen verkkoinfrastruktuurin uudistamiselle. Työssä kartoitettiin nykyisen verkon rakenne, laitteisto, ohjelmistot ja tietoturvatilanne. Kartoituksen pohjalta tunnistettiin useita kehityskohteita, kuten hajautettu IP-osoitteiden hallinta, puutteellinen segmentointi ja riittämätön etäyhteyksien hallinta.

Tietoperustassa esitellään keskeiset verkkosuunnittelun osa-alueet, kuten OSI-malli, IP-osoitteet ja aliverkko, verkkotopologiat, kytkimet, reitittimet, palomuurit, verkkoprotokollat ja nykyaikaiset tietoturvakäytännöt. Näitä hyödynnettiin uuden verkkomallin suunnittelussa.

Suunniteltu ratkaisu sisältää tekniset toimenpiteet, kuten VLAN-segmentoinnin, 802.1X-autentikoinnin, VPN-etäyhteydet, roolipohjaisen pääsynhallinnan ja verkon valvontatyökalujen käyttöönoton. Työssä kuvataan myös käyttöönottoprosessi, pilottivaihe, takaisinpalautussuunnitelma sekä ylläpito ja jatkokehitys.

Tuloksena syntyi vaiheittain etenevä ja nykyaikaisiin käytäntöihin perustuva suunnitelma, jonka avulla verkon uudistaminen voidaan toteuttaa käytännössä. Työ on hyödynnettävissä muissakin vastaavan kokoisissa organisaatioissa ja toimii esimerkkinä siitä, miten tietoturva ja hallittavuus voidaan toteuttaa kustannustehokkaasti.

Avainsanat 802.1X-autentikointi, DHCP, IP-osoitteet, OSI-malli, segmentointi, verkkoinfrastruktuuri

LAPIN AMK
Lapland University of Applied Sciences

Abstract of thesis

Study Programme in Information
and Communication Technology
Bachelor of Engineering

Author Onni Markkanen **Year** 2025
Supervisor Kenneth Karlsson
Commissioned by Istekki Oy
Title Network Infrastructure Modifications
Number of pages 37

The aim of this thesis project was to present a practical plan for designing and building a modern and secure network infrastructure for a medium-sized company.

The study started with the mapping of the current network, focusing on its structure, devices, software and security features. Several improvement areas were identified such as scattered IP address management, missing network segmentation and weak control of remote access. The theoretical part of the thesis covered key concepts such as the OSI model, IP addressing and subnetting, different types of network topologies, switches and routers, firewalls, common network protocols and current cybersecurity practices. These concepts supported the design of a new, more efficient network.

The proposed network solution includes steps like creating VLANs, enabling 802.1X authentication, setting up secure VPN access for external users and applying role-based access control. Monitoring tools and configuration backups were also included to help manage and maintain the network in the future. This thesis provides a clear and step-by-step network plan that can be used in real life implementation. It also works as a general example for similar organizations that want to modernize their network without large financial investments.

Keywords 802.1x authentication, DHCP, IP-addressing, OSI-model, segmentation, network infrastructure

SISÄLLYS

1 JOHDANTO

Verkkoinfrastruktuuri muodostaa olennaisen osan jokaisen organisaation teknisestä perusrakenteesta. Yritysten arki perustuu yhä enemmän digitaalisiin palveluihin, pilvipohjaisiin ratkaisuihin ja etätyöhön, minkä vuoksi toimivan ja tietoturvallisen verkkoympäristön merkitys korostuu. Nykyaikainen verkko ei ole vain yhteyksien joukko, vaan strateginen osa yrityksen toimintakykyä ja liiketoiminnan jatkuvuutta.

Tämä opinnäytetyö toimii käytännönläheisenä projektisuunnitelmana, jonka tavoitteena on luoda selkeä ja toteuttamiskelpoinen malli keskikokoisen yrityksen verkkoinfrastruktuurin uudistamiselle. Työn lähtökohtana oli nykyverkon kartoitus, jonka pohjalta tunnistettiin keskeiset kehityskohteet. Näiden havaintojen perusteella laadittiin vaiheittainen suunnitelma, jossa otetaan huomioon suorituskyky, tietoturva, hallittavuus ja skaalautuvuus.

Työn keskeinen tutkimuskysymys on: Kuinka suunnitellaan ja toteutetaan nykyaikainen, turvallinen ja tehokas verkkoinfrastruktuuri, joka vastaa organisaatio nykyisiä ja tulevia tarpeita?

Opinnäytetyö toteutettiin kehittämistehtävänä. Työ perustuu sekä olemassa olevan verkon analyysiin että ajankohtaiseen teoriaan ja teknisiin käytäntöihin. Lähdeaineistona hyödynnettiin alan kirjallisuutta, verkkostandardeja, ajantasaisia verkkolähteitä sekä omia käytännön havaintoja.

Opinnäytetyö sisältää sekä teoreettisen viitekehyksen että käytännönläheisen suunnittelun ja toteutuksen kuvauksen. Teoriaosuudessa käydään läpi verkon suunnitteluun liittyviä keskeisiä käsitteitä, kuten OSI-malli, IP-osoitteet, verkkotopologiat, tietoturva ja verkon hallinta. Käytännön osuus sisältää vaiheistetun mallin nykyverkon arviointiin, uuden verkon suunnitteluun, käyttöönottoon, ylläpitoon ja jatkokehitykseen.

Tämän työn tarkoituksena on tarjota selkeä toimintamalli yritykselle, joka haluaa kehittää verkkoinfrastruktuuriaan ajanmukaisilla ratkaisuilla ilman tarpeettomia kustannuksia. Samalla työ tukee myös omaa ammatillista kehittymistäni verkkosuunnittelun ja tietoturvan osa-alueilla.

2 VERKKOINFRASTRUKTUURIN PERUSTEET

2.1 OSI-malli ja sen vaikutus verkkorakenteeseen

OSI-malli on viitekehys, joka kuvastaa tietoliikennejärjestelmien toimintaa sen erillissä kerroksissa. Se rakentuu seitsemästä eri loogisesta kerroksesta. (GeeksforGeeks 2025b.)
Tässä on OSI-mallin kerrokset selitettynä ylhäältä alaspäin:

- **Sovelluskerros** tarjoaa loppukäyttäjälle palveluita mitä sovellukset käyttävät tiedonsiirroissa. Esimerkiksi verkkoselaimet ja sähköpostiohjelmat toimivat tämän kerroksen kautta. (GeeksforGeeks 2025b.)

- **Esittelykerros** vastaa tietojen esittämisestä ja tietojen muuntamisesta oikeanlaiseksi, jotta sovellukset ymmärtävät ne (GeeksforGeeks 2025b).

- **Istuntokerros** hallinnoi sovellusten väliset yhteydet, esimerkiksi istuntojen luominen, ylläpito ja lopetus (GeeksforGeeks 2025b).

- **Kuljetuskerros** varmistaa tiedon luotettavasta siirtymisestä lähettäjän ja vastaanottajan välillä. Tällä kerroksella toimivat esimerkiksi TCP- ja UPD-protokollat. (GeeksforGeeks 2025b.)

- **Verkkokerros** on vastuussa tietojen reitittämisestä eri verkkojen välillä. Se käyttää vain loogisia IP-osoitteita määrittääkseen polun tiedonsiirrossa. (GeeksforGeeks 2025b.)

- **Linkkikerros** vastaa luotettavasta tiedon siirtymästä kahden fyysisen laitteen välillä. Tässä käytetään MAC-osoitteita laitteiden yksilöimiseksi. (GeeksforGeeks 2025b.)

- Fyysinen kerros vastaa tietojen välittämisestä fyysisen siirtovälineen kautta, kuten kaapelien, signaalien ja liitinten kautta (GeeksforGeeks 2025b).

OSI-malli auttaa ymmärtämään ja suunnittelemaan verkkorakenteita jakamalla monimutkaiset tietoliikenneprosessit pienempiin hallittaviin osiin. Tämä kerrosten

kautta tapahtuva lähestymistapa mahdollistaa eri valmistajien laitteiden ja ohjelmistojen yhteensopivuutta sekä helpottaa vianmääritystä ja verkon hallitsemista. (Informatec Digital 2024.)

2.2 IP-osoitteet

IP-osoite on tunniste, joka annetaan jokaiselle verkkoon liitetylle laitteelle. Sen avulla laitteet pystyvät kommunikoimaan keskenään internetissä tai paikallisverkossa. IP-osoitteita on monenlaisia ja niiden luokittelu riippuu käyttötarkoituksesta ja osoitteen luonteesta. Nykyisin käytetään kahta eri IP-osoiteversiota. IPv4 on yleisin osoitemuoto. Se koostuu neljästä pistein erotetusta numerosta esimerkiksi 127.0.0.1 ja käyttää 32 bittistä osoiterakennetta. IPv4 tarjoaa noin 4.3 miljardia osoitetta. IPv6 on uudempi muoto, joka käyttää 128 bittistä rakennetta ja se eroaa paljon aikaisemmasta versiostaan. IPv6 tarjoaa käytännössä rajattoman määrän osoitteita. (Einoryte, A. 2023.)

IP-osoitteet voidaan jakaa eri luokkiin niiden käyttötarkoituksen mukaan:

- Tämä osoite näkyy internettiin. Jokaisella internettiin yhdistetyllä laitteella on oltava **julkinen IP-osoite**, jotta se voi olla yhteydessä muihin laitteisiin internetissä. Julkinen IP-osoite voi olla dynaaminen tai staattinen. (Einoryte, A. 2023.)

- **Yksityisiä IP-osoitteita** käytetään paikallisverkoissa esimerkiksi kotona tai yrityksissä. Näillä osoitteilla ei ole suoraa pääsyä internetiin, vaan ne kulkevat ensin reitittimen tai muun verkkolaitteen kautta. Esimerkkejä yksityisistä IP-osoitteista ovat 192.168.x.x ja 10.x.x.x. (Einoryte, A. 2023.)

- **Staattinen IP-osoite** pysyy aina samana. Sitä käytetään usein palvelimissa tai verkkolaitteissa, joiden täytyy olla aina tavoitettavissa samalla osoitteella. (Einoryte, A. 2023.)

- **Dynaamiset IP-osoitteet** muuttuvat ajoittain ja ne jaetaan automaattisesti, esimerkiksi kun laite yhdistetään verkkoon. Useimmat kuluttajayhteydet käyttävät dynaamista IP-osoitetta. (Einoryte, A. 2023.)

- **Jaettu IP-osoite** tarkoittaa sitä, että uset käyttäjät tai verkkosivustot voivat jakaa saman IP-osoitteen. Tätä käytetään usein jaetuissa hosting palveluissa. (Einoryte, A. 2023.)

- **Dedikoidussa IP-osoitteessa** käyttäjä tai palvelu saa yksilöllisen IP-osoitteen, jota ei jaeta muiden kanssa. Tämä voi parantaa suorituskykyä ja tietoturvaa esimerkiksi VPN-palveluissa. (Einoryte, A. 2023.)

2.3 Aliverkoitus

Aliverkotus tarkoittaa IP-verkon jakamista pienempiin osiin. Tavoitteena on parantaa verkon hallintaa, tietoturvaa ja resurssien jakamista. (Bryce Leo. 2024b)

Aliverkko määritellään aliverkon peitteen avulla. Tämä peite kertoo, mikä osa IP-osoitteesta viittaa itse verkkoon ja mikä osa yksittäiseen laitteeseen eli isäntään. (Bryce Leo. 2024b)

Tässä aliverkkoesimerkissä IP-osoite on 192.168.1.0 ja aliverkon peite on 255.255.255.0. Peitteen perusteella kolme ensimmäistä osaa 192.168.1 määrittelevät verkon osoitteen, kun taas viimeinen osa eli arvot 0–255, käytetään yksittäisten laitteiden osoittamiseen kyseisessä verkossa. Koska kaksi osoitetta varataan erityistarkoituksiin, yksi verkko-osoitteeksi ja toinen lähetysosoitteeksi, voidaan tällä aliverkolla yksilöidä yhteensä 254 laitetta. (Bryce Leo. 2024b)

Aliverkotuksen etuja ovat

- verkon kuormituksen pienentäminen

- laitteiden looginen erottaminen eli segmentointi

- parantunut turvallisuus esimerkiksi liikenteen rajoitus eri segmenttien välillä. (Bryce Leo. 2024b.)

2.4 Verkkotopologiat ja niiden vaikutukset suorituskykyyn

Verkkotopologia tarkoittaa tapaa, jolla verkkolaitteet, kuten tietokoneet, reitittimet ja kytkimet on järjestetty ja yhdistetty toisiinsa. Topologian valinta vaikuttaa ratkaisevasti verkon suorituskykyyn, laajennettavuuteen ja vikasietoisuuteen. (GeeksforGeeks 2025a.)

Verkkoa suunniteltaessa oikean topologian valinta voi helpottaa hallintaa, parantaa turvallisuutta ja varmistaa tasaisen tiedonsiirron kaikille käyttäjille (GeeksforGeeks 2025a).

Verkkotopologia malleja on monia ja niistä pitää osata valita verkkoa suunnitellessa se oikea. Seuraavaksi kerron tarkemmin yleisimmistä topologioista ja niiden vaikutuksista.

Kaikki laitteet on liitetty samaan tiedonsiirtoväylään eli kaapeliin. Tieto kulkee väylää pitkin ja kaikki laitteet vastaanottavat sen. Vain oikea kohde reagoi. **Väylätopologia** on yksinkertainen ja edullinen, mutta sen heikkoutena on, että yksi kaapelivika voi katkaista koko verkon toiminnan. Lisäksi useiden laitteiden yhtäaikainen käyttö voi aiheuttaa törmäyksiä ja hidastaa liikennettä. (GeeksforGeeks 2025a.)

Laitteet yhdistetään kehämäisesti, ja tieto liikkuu rengasta pitkin vain yhteen suuntaan. Jokainen laite toimii "toistimena" siirtäen tietoa seuraavalle. **Rengastopologian** etu on ennustettava liikenteen kulkusuunta, mutta yhden laitteen vika tai yhteyskatkos voi estää koko verkon toiminnan, ellei vikasietoisuutta ole erikseen toteutettu. (GeeksforGeeks 2025a.)

Kaikki laitteet on yhdistetty keskuskytkimeen tai reitittimeen. Tämä on yleisin topologia nykyisissä lähiverkoissa**. Tähtitopologia** on helppo hallita ja vikasietoinen yksittäisten laitteiden osalta, kuin yhden laitteen vika ei vaikuta muihin. Keskuslaitteen vika kuitenkin pysäyttää koko verkon. (GeeksforGeeks 2025a.)

Jokainen laite on yhdistetty suoraan useisiin muihin laitteisiin. Tämä mahdollistaa useita vaihtoehtoisia tiedonsiirtoreittejä ja lisää vikasietoisuutta. **Verkkomuotoinen topologia** on erittäin tehokas, mutta samalla kallis ja monimutkainen toteuttaa suurissa verkoissa. (GeeksforGeeks 2025a.)

Puutopologia yhdistää tähtimäisen ja väylätopologian piirteet. Se rakentuu kerroksittain, alkaen yhdestä keskuslaitteesta, josta haarautuu useita aliverkkoja. Puutopologia on hyvin skaalautuva ja sopii suuriin organisaatioihin, mutta keskusrunko voi olla haavoittuva. (GeeksforGeeks 2025a.)

Hybridi-topologia muodostuu yhdistämällä kaksi tai useampia topologioita samaan verkkoon. Esimerkiksi suurissa yritysverkoissa voi olla useita tähtitopologioita yhdistettynä puutopologiaan tai mesh elementteihin. Tämä mahdollistaa verkon muokkaamisen tarpeiden mukaan ja siitä saadaan käyttöön eri topologioiden parhaat puolet. Haittapuolena on toteutuksen monimutkaisuus ja ylläpidon vaativuus. (GeeksforGeeks 2025a.)

2.5 Kytkimet

Kytkimet ovat keskeisiä komponentteja nykyaikaisissa tietoverkoissa, erityisesti lähiverkoissa. Ne yhdistävät useita laitteita samaan verkkoon ja mahdollistavat tehokkaan tiedonsiirron laitteiden välillä. Kytkimet toimivat OSI-mallin toisella kerroksella eli siirtoyhteyskerroksella, jossa ne käsittelevät MAC-osoitteita ohjatakseen tietoliikennettä oikeaan kohteeseen. Joissakin edistyneemmissä kytkimissä on kolmannen verkkokerroksen toimintoja, kuten IP-osoitteiden käsittely ja reititys. (Bryce, L. 2024a)

Kytkimen toiminta, kun laite lähettää tietoa verkossa, tieto paketoidaan kehyksiksi, jotka sisältävät sekä lähettäjän että vastaanottajan MAC-osoitteet. Kytkin vastaanottaa nämä kehykset ja tallentaa lähettäjän MAC-osoitteen omaan osoitetauluunsa. Tämän jälkeen kytkin vertaa paketissa olevaa vastaanottajan MAC-osoitetta osoitetauluun ja lähettää paketin eteenpäin oikeaan porttiin. Jos vastaanottajan osoitetta ei löydy taulusta, kytkin lähettää paketin kaikkiin portteihin paitsi siihen, josta se saapui. (Patchbox 2022.)

Kytkimiä on useita eri tyyppejä, jotka on suunniteltu erilaisiin käyttötarkoituksiin. Kerron tarkemmin alapuolella yleisimmistä laitemalleista.

Hallitsemattomat kytkimet ovat yksinkertaisia laitteita, jotka eivät vaadi konfigurointia. Ne tarjoavat perustoiminnot laitteiden yhdistämiseen ja ovat usein käytössä pienissä verkoissa tai kotikäytössä. (Patchbox 2022.)

Hallittavat kytkimet tarjoavat laajat konfigurointi ja hallintamahdollisuudet, kuten VLAN:ien luomisen, liikenteen priorisoinnin ja tietoturva-asetusten määrittelyn. Ne soveltuvat erityisesti suurempiin ja monimutkaisempiin verkkoihin, joissa tarvitaan tarkempaa hallintaa. (Patchbox 2022.)

PoE-kytkimet voivat välittää sähkövirtaa Ethernet kaapeleiden kautta liitetyille laitteille, kuten puhelimille, kameroille tai langattomille tukiasemille. Tämä vähentää tarvetta erillisille virtalähteille ja yksinkertaistaa asennusta. (Patchbox 2022.)

Kytkin mahdollistaa tehokkaan tiedonsiirron ohjaamalla tiedon suoraan oikealle laitteelle, mikä vähentää verkon kuormitusta ja parantaa sen suorituskykyä. Verrattuna esimerkiksi keskittimiin, jotka lähettävät tiedon kaikille verkon laitteille. Lisäksi kytkin tukee verkon segmentointia, jolloin verkko voidaan jakaa pienempiin osiin. Tämä parantaa sekä verkon tietoturvaa että hallittavuutta, sillä esimerkiksi VLAN-teknologian avulla eri osastojen liikenne voidaan erottaa toisistaan. Kytkimien avulla verkko on myös helposti laajennettavissa, sillä uusia laitteita voidaan lisätä verkkoon ilman merkittäviä muutoksia olemassa olevaan infrastruktuuriin.

2.6 Reitittimet

Reititin on verkkolaite, jonka tehtävänä on yhdistää eri verkkoja toisiinsa ja ohjata tietoliikennettä verkkojen välillä. Reitittimet mahdollistavat esimerkiksi paikallisverkon liittämisen internetiin. Ne toimivat OSI-mallin kolmannella kerroksella eli verkkokerroksessa, jossa käytetään IP-osoitteita tiedon reitittämiseen. (Cisco Systems, Inc. 2025.)

Toimintaperiaate reitittimellä on, kun tietoa lähetetään verkon ulkopuoliselle laitteelle, reititin tarkistaa vastaanottajan IP-osoitteen ja selvittää parhaan mahdollisen reitin kohteeseen. Reititin käyttää tähän reititystaulua, joka sisältää tietoa siitä, mihin suuntaan eri verkkojen liikenne tulee ohjata. (Yasar, K., Irei, A. & Scarpati, J. 2025.) Reititin osaa ohjata liikennettä dynaamisesti muuttuvien olosuhteiden mukaan ja se voi päättää esimerkiksi liikenteen siirtämisestä toista reittiä pitkin, jos ensisijainen yhteys on alhaalla tai ruuhkautunut. (Cisco Systems, Inc. 2025)

Reitittimiä on useita eri tyyppejä, jotka on suunniteltu erilaisiin käyttötarkoituksiin. Alla yleisimmät reititintyypit.

Langaton reititin tarjoaa langattoman yhteyden käyttäjille. Ne yhdistävät lähiverkon laitteet toisiinsa ja internettiin. Yleensä käytetään kotiverkoissa ja pienissä toimistoissa. (Yasar ym. 2025.)

3G-, 4G- ja 5G-reitittimet käyttävät mobiilidatayhteyttä internettiin pääsemiseksi. Sopivat erityisesti tilanteisiin, joissa kiinteää laajakaistaa ei ole saatavilla esimerkiksi mökeillä tai työmaakäytössä. (Yasar ym. 2025.)

LAN- ja VPN-reitittimet on suunniteltu yhdistämään useita lähiverkkoja ja tarjoamaan suojattuja yhteyksiä. VPN-reitittimissä on sisäänrakennettu tuki salatuille yhteyksille, mikä parantaa tietoturvaa. (Cisco Systems, Inc. 2025.)

Mesh-reitittimien järjestelmä koostuu useista toisiinsa yhteydessä olevista reitittimistä, jotka muodostavat kattavan langattoman verkon. Tietoliikenne siirtyy solmusta toiseen, mikä takaa tasaisen signaalin koko alueella. Sopii hyvin suuriin koteihin ja rakennuksiin. (GeeksforGeeks 2024b.)

Yritysreitittimet on suuremmille organisaatioille tarkoitettuja tehokkaampia reitittimiä, joissa on laajat hallintaominaisuudet, varayhteydet, QoS tuki ja usein myös palomuuri tai IDS/IPS toiminnot. Näitä käytetään datakeskuksissa ja verkoissa, joiden on toimittava 24/7. (Cisco Systems, Inc. 2025)

Reitittimet ovat myös keskeinen osa tietoturvaa. Niissä voi olla sisäänrakennettu palomuuri, NAT ja mahdollisuus suodattaa liikennettä. Yritysympäristöissä käytetään usein myös reitinvarmistusprotokollia, kuten OSPF tai BGP, jotka mahdollistavat turvallisen ja tehokkaan reitityksen laajoissa verkoissa. (Yasar ym. 2025.)

2.7 Palomuurit

Palomuuri on verkkoturvallisuuden tärkeimpiä työkaluja. Sen tehtävänä on valvoa ja suodattaa verkkoliikennettä määriteltyjen sääntöjen perusteella. Palomuuri toimii eräänlaisena portinvartijana, joka päättää mikä liikenne saa tulla sisään tai lähteä verkosta ulos. (F-Secure 2022.)

Palomuuri analysoi saapuvan ja lähtevän liikenteen paketteja ja vertaa niitä käytäntöihin tai sääntöihin, jotka verkon ylläpitäjä on määrittänyt. Esimerkiksi voidaan sallia vain tietyistä IP-osoitteista tuleva liikenne tai estää tietyiltä porteilta lähtevä liikenne**.** Palomuuri voi olla asetettu suojaamaan yksittäsitä laitetta taikka sitten kokonaista verkkoa**.** (GeeksforGeeks 2025c.)

Palomuurit voidaan jakaa kahteen päätyyppiin käyttötarkoituksen ja toteutustavan mukaan. Ohjelmistopalomuurit asennetaan suoraan yksittäiseen laitteeseen, kuten tietokoneeseen, ja ne suojaavat kyseistä laitetta valvomalla kaikkea sen verkkoliikennettä. Useissa käyttöjärjestelmissä, kuten Windowsissa, on sisäänrakennettu ohjelmistopalomuuri, joka toimii perustason suojana. Laitteistopalomuuri puolestaan on erillinen fyysinen laite, joka sijoitetaan koko verkon ja ulkoisen verkkoyhteyden väliin. Se suojaa koko verkkoa keskitetysti yhdestä pisteestä. Yritykset suosivat usein laitteistopalomuureja, koska ne tarjoavat laajemmat suojausominaisuudet sekä mahdollisuuden hallita useita verkkoja samanaikaisesti (F-Secure 2022).

2.8 Protokollat

Protokollat mahdollistavat tietokoneiden, palvelimien ja muiden verkkoon liitettyjen laitteiden välisen viestinnän. Ne määrittelevät, miten tiedot muotoillaan, lähetetään, vastaanotetaan ja puretaan ymmärrettäväksi muodoksi verkossa. (GeeksforGeeks 2023.)

Seuraavaksi käsitellään yleisimpiä verkkoprotokollia ja avaan syvemmin niiden käyttötarkoitusta.

TCP on luotettava protokolla, joka varmistaa, että tiedot siirtyvät oikein ja oikeassa järjestyksessä lähettäjältä vastaanottajalle. Se luo yhteyden ennen tiedonsiirtoa ja lähettää paketit yksi kerrallaan, odottaen kuittauksen ennen seuraavaa. TCP:tä käytetään esimerkiksi sähköpostin, verkkosivujen ja tiedostonsiirron yhteydessä. (Klusaite, L. 2022.)

IP vastaa pakettien reitityksestä lähteestä määränpäähän. Se määrittelee osoitteet, joilla laitteet tunnistetaan verkossa. IPv4 on yleisin, mutta IPv6 yleistyy jatkuvasti. IP toimii yhdessä TCP:n tai UDP:n kanssa muodostaen TCP/IP- tai UDP/IP-yhdistelmiä. (Klusaite, L. 2022.)

UDP on nopeampi mutta epäluotettavampi kuin TCP. Se ei muodosta yhteyksiä eikä saa kuittauksia vaan se lähettää paketteja suoraan vastaanottajalle. Käytetään reaaliaikaisissa sovelluksissa, kuten suoratoistossa ja verkkopuheluissa, joissa nopeus on tärkeämpää kuin täydellinen eheys. (Zieniute, U. 2022.)

HTTP on verkkoprotokolla, jota käytetään web-selaimen ja palvelimen väliseen viestintään. Sen avulla selaimet pyytävät ja vastaanottavat verkkosivuja palvelimilta selattavaksi. (GeeksforGeeks 2024a.)

SMTP mahdollistaa sähköpostien lähettämisen palvelimelta toiselle. Kun käyttäjä lähettää sähköpostin, se kulkee SMTP:n avulla määränpäähän. Se toimii yleensä yhdessä POP3:n tai IMAPin kanssa, joilla sähköpostit haetaan vastaanottajalle. (Cloudflare, Inc. 2025.)

DNS muuntaa helpot verkkotunnukset esimerkiksi www.esimerkki.fi niiden vastaaviksi IP-osoitteiksi. Ilman DNS:ää käyttäjien pitäisi muistaa IP-osoitteita verkkosivujen sijaan. (Mills, M. 2021.)

3 NYKYISEN VERKON KARTOITUS JA OPTIMOINTI

3.1 Verkkolaitteet

Verkkojen fyysinen rakenne muodostuu erilaisista verkkolaitteista, jotka mahdollistavat tiedonsiirron ja verkon toiminnan. Jotta nykyverkkoa voidaan kehittää tai optimoida, on tärkeää kartoittaa käytössä olevat laitteet tarkasti. Kartoituksessa keskitytään siihen, missä laitteita sijaitsee, miten ne on konfiguroitu ja minkälaista roolia ne verkossa hoitavat.

Kartoitusprosessi etenee systemaattisesti useiden käytäntöjen avulla, jotta kaikki verkkoon liitetyt laitteet tunnistetaan ja dokumentoidaan luotettavasti. Ensimmäiseksi suoritetaan fyysinen tarkistus, jossa verkkoon kytketyt laitteet käydään läpi tiloittain. Erityisesti huomio kiinnitetään keskeisiin verkkolaitteisiin, kuten reitittimiin, kytkimiin, palomuureihin ja langattomiin tukiasemiin. Tarkistus voidaan tehdä paikan päällä tai olemassa olevien verkkokaavioiden avulla. Lisäksi tehdään yksityiskohtainen inventointi verkkojakamoista.

Mikäli aiempia verkkotopologiakuvauksia on saatavilla, ne otetaan tarkasteluun ja niitä verrataan nykytilanteeseen. Tarvittaessa kaaviot päivitetään vastaamaan todellista verkon rakennetta. Apuna käytetään myös erilaisia verkonhallintatyökaluja, kuten PRTG Network Monitor, SolarWinds ja Angry IP Scanner, joiden avulla voidaan automaattisesti havaita verkkoon liitetyt laitteet IP-osoitteiden perusteella. Nämä työkalut tarjoavat myös lisätietoa laitteista, kuten verkkokortin valmistajan tai tarjolla olevat palvelut.

MAC-osoitteiden ja IP-osoitteiden kartoitus toteutetaan analysoimalla reitittimien ja kytkinten porttitiedot. Tämän avulla saadaan selville laitteiden fyysinen sijainti ja niiden liittymät verkkoon. Samalla tarkastetaan verkkolaitteiden konfiguraatiotiedostot, kuten reitittimien, palomuurien ja hallittavien kytkinten asetukset. Näistä selviävät esimerkiksi VLAN-määritykset, reitityssäännöt ja pääsynhallinta-asetukset.

Kaikki löydetyt laitteet dokumentoidaan kattavasti. Dokumentointiin käytetään taulukkomuotoa, johon merkitään vähintään laitteen nimi, tyyppi, sijainti, IP- ja

MAC-osoitteet, hallintatapa sekä käytössä oleva käyttöjärjestelmä tai laiteohjelmiston versio. Näin muodostuu ajantasainen ja hyödyllinen kokonaiskuva verkon nykytilasta.

Kartoitettavat verkkolaitteet tunnistetaan ja analysoidaan niiden tyypin ja toiminnan mukaan osana verkon kokonaisvaltaista suunnittelua. Reitittimien osalta selvitetään niiden tarkka malli, IP-osoite sekä rooli verkossa. On tärkeää määrittää, toimivatko ne yhteytenä sisäverkon ja internetin välillä vai pelkästään sisäverkon reitityspisteinä. Kytkimet tarkastetaan porttikonfiguraatioiden, VLAN-jakojen sekä mahdollisen PoE-tuen osalta. Tämä auttaa ymmärtämään, miten liikenne kulkee eri segmenttien välillä.

Palomuureissa selvitetään käytetyt säännöt ja politiikat, jotka säätelevät verkkoliikennettä. Erityisesti tarkastellaan, miten liikenne on rajattu tai sallittu eri verkon segmenttien välillä. Langattomien tukiasemien osalta tarkistetaan niiden fyysinen sijainti, signaalin kattavuus eri tiloissa sekä niiden yhteys mahdolliseen keskitettyyn hallintajärjestelmään.

Palvelimista ja työasemista selvitetään erityisesti palvelinten roolit, kuten toimivatko ne Active Directoryn, DNS:n tai DHCP:n palvelualustoina. Lisäksi kartoitetaan, kuinka laajasti työasemat ovat liitettyinä verkkoon ja miten ne on hallinnollisesti keskitetty. IoT-laitteet ja muut älylaitteet tunnistetaan usein automaattisten verkkoskannerien tai manuaalisen inventoinnin avulla. Ne dokumentoidaan erityisen huolellisesti tietoturvan näkökulmasta, sillä niiden suojaaminen on usein puutteellisempaa kuin perinteisten IT-laitteiden.

3.2 Ohjelmistot

Ohjelmistot ovat isossa osassa verkkoympäristössä, sillä ne vastaavat verkon valvonnasta, suojaamisesta ja eri palveluiden tarjoamisesta. Kartoituksen tavoitteena on saada kokonaiskuva kaikista verkkoon liittyvistä ohjelmistoista, mitä ohjelmistoja käytetään, missä ne sijaitsevat ja mikä on niiden nykytila. Tämä tieto tukee verkon optimointia, tietoturvan parantamista sekä mahdollisten päivitystarpeiden tunnistamista.

Ohjelmistokartoitus voidaan suorittaa useilla menetelmillä, jotka täydentävät toisiaan ja tarjoavat kattavan kuvan organisaation ohjelmistoympäristöstä. Yksi tehokkaimmista tavoista on hyödyntää automaattisia skannereita. Skanneri työkalut mahdollistavat ohjelmistojen automaattisen inventoinnin, ja ne keräävät tietoa muun muassa asennetuista sovelluksista, ohjelmistoversioista sekä viimeisimmistä päivityksistä.

Jos organisaatiolla on käytössä keskitetty verkonhallintaratkaisu, voidaan ohjelmistojen tilaa ja asennuksia seurata sen kautta. Tällainen ratkaisu tarjoaa reaaliaikaisen näkymän ohjelmistoihin, mikä helpottaa ylläpitoa ja auttaa havaitsemaan mahdolliset tietoturvariskit, kuten vanhentuneet ohjelmistot.

Palvelinten osalta tietoa voidaan kerätä myös lokitiedoista ja konfiguraatiotiedostoista. Näiden avulla on mahdollista selvittää, mitä palveluita kuten DHCP, DNS, Active Directory tai tiedostopalvelut, on aktiivisena ja millä asetuksilla ne toimivat.

Mikäli automaattisia työkaluja ei ole käytettävissä, ohjelmistokartoitus voidaan suorittaa myös manuaalisesti. Tämä edellyttää työasemien ja palvelimien hallintaliittymien käyttöä, joiden kautta voidaan tarkistaa yksittäisten laitteiden ohjelmistotiedot. Tämä menetelmä on aikaa vievä, mutta tarpeen erityisesti pienemmissä ympäristöissä tai silloin, kun tarkkuus on erityisen tärkeää.

Kartoituksen aikana kiinnitetään huomiota erityisesti neljään keskeiseen ohjelmistokategoriaan. Ensimmäiseksi tarkastellaan verkonhallinta- ja valvontaohjelmistoja. Tavoitteena on selvittää, mitä työkaluja käytetään verkon tilan seurantaan ja automaattisiin hälytyksiin. Samalla varmistetaan, että ohjelmistot on konfiguroitu oikein ja että kaikki verkon osat on liitetty järjestelmiin asianmukaisesti.

Toiseksi kartoitetaan tietoturvaohjelmistot, kuten palomuurit, virustorjuntaohjelmistot, tunkeutumisen havaitsemis- ja estojärjestelmät sekä VPN-ratkaisut. Arvioinnissa keskitytään ohjelmistojen kattavuuteen, versioihin ja päivitysten ajantasaisuuteen. Erityishuomio kohdistetaan myös siihen, onko järjestelmänhallinnassa käytössä monivaiheinen tunnistautuminen.

Kolmantena kokonaisuutena selvitetään palvelinohjelmistot. Näihin kuuluvat muun muassa DHCP-, DNS- ja Active Directory -palvelut sekä tiedosto- ja sovelluspalvelimet. Jokaisen palvelun osalta dokumentoidaan sen rooli verkossa sekä käytössä oleva ohjelmistoversio.

Viimeisenä tutkitaan työasemien ja mobiililaitteiden hallintaan liittyvät ratkaisut. Tarkastellaan, onko käytössä mobiililaitteiden hallintaratkaisuja tai muita laitehallintajärjestelmiä. Lisäksi kartoitetaan, miten ohjelmistojen jakelu, päivitykset ja suojaustoimenpiteet on toteutettu loppukäyttäjien laitteissa. Tämä kokonaisuus on keskeinen, jotta koko verkon tietoturva ja hallittavuus voidaan varmistaa kattavasti.

Kaikista kartoitetuista ohjelmistoista kirjataan vähintään seuraavat tiedot:

- ohjelmiston nimi ja versio
- käyttötarkoitus ja asennusympäristö esimerkiksi onko se työasemalla, palvelimella taikka verkonvalvontalaitteissa
- päivitys ja tukitilanne
- mahdolliset lisenssitiedot
- havaitut puutteet tai kehityskohteet.

Tarkasti dokumentoitu ohjelmistokartoitus auttaa varmistamaan, että verkon ylläpito ja suojaus perustuvat ajantasaiseen ja luotettavaan tietoon. Lisäksi se tukee tulevien päivitysten ja ohjelmistoinvestointien suunnittelua.

3.3 IP-osoitteiden hallinta

IP-osoitteiden hallinnan kartoituksessa selvitetään, miten osoitteet on jaettu, millaisia osoitealueita käytetään ja miten osoitteiden jakaminen on toteutettu käytännössä. Hyvin hallittu osoitejärjestelmä parantaa verkon toimivuutta, turvallisuutta ja vianmääritystä.

Kartoituksen tavoitteena on muodostaa kokonaiskuva IP-osoitteiden jakautumisesta verkossa ja tunnistaa mahdolliset ongelmat, kuten

- osoitteiden päällekkäisyydet
- tarpeettoman laajat tai huonosti suunnitellut aliverkot
- manuaalisesti jaetut osoitteet, jotka vaikeuttavat hallintaa
- puutteet DHCP-palveluiden tai DNS-nimipalveluiden toiminnassa.

Kartoituksen yhteydessä tarkastellaan erityisesti IP-osoitteiden jakotapaa. Selvitetään, käytetäänkö verkossa staattista osoitteiden määrittelyä, dynaamista jakelua vai molempia rinnakkain. DHCP-palvelimen asetukset tarkistetaan huolellisesti, mukaan lukien vuokra-aikojen pituus, osoitealueiden rajaukset sekä mahdolliset varaukset tärkeille laitteille. Mikäli osoitteet on määritelty käsin, kartoitetaan käytössä olevat IP-listaukset ja arvioidaan dokumentaation ajantasaisuus.

Verkon aliverkotus ja osoitealueet ovat toinen keskeinen osa-alue. Selvitetään, kuinka verkko on jaettu eri aliverkkoihin ja mitkä aliverkon peitteet ovat käytössä. Tarkastellaan, onko luotu erilliset verkot esimerkiksi osastoille, palvelimille, vierailijoille tai IoT-laitteille. Käytettyjen IP-alueiden koko analysoidaan suhteessa todelliseen laitemäärään, jotta voidaan tunnistaa mahdollinen osoiteavaruuden tuhlaus tai ruuhkautumisriskit.

Nimipalveluiden ja dynaamisen osoitteiden jaon toiminta arvioidaan kolmantena kokonaisuutena. Tarkastellaan, mitä palvelimia käytetään DNS-toimintoihin ja kuinka nimien kääntäminen IP-osoitteiksi tapahtuu. Lisäksi arvioidaan palveluiden päivitysten ajantasaisuus, järjestelmien redundanssi sekä käytössä oleva hallintamalli. Erityistä huomiota kiinnitetään siihen, kirjautuvatko DHCP-varaukset ja osoitehistoria lokitietoihin, sillä tämä parantaa verkon jäljitettävyyttä.

Lopuksi tarkistetaan osoitteiden dokumentointi ja hallintakäytännöt. Selvitetään, onko organisaatiolla käytössään IPAM-järjestelmä, taulukkolaskentaohjelma tai muu seurantatyökalu osoitteiden hallintaan. Tarkastellaan osoitteiden nimeämisen selkeyttä sekä mahdollisten osoitealueiden sääntöjen käyttöä. Kartoituksessa kirjataan ylös myös mahdolliset ongelmat, kuten päällekkäiset osoitteet tai puutteet dokumentaatiossa, jotta ne voidaan huomioida jatkokehityksessä.

IP-osoitteiden hallinnan kartoitus auttaa varmistamaan, että osoitteet ovat tehokkaasti käytössä ja helposti hallittavissa. Se myös parantaa verkon luotettavuutta ja nopeuttaa ongelmatilanteiden ratkaisemista. Lisäksi kartoitus voi paljastaa tarpeen siirtyä IPv6-osoitteisiin tai ottaa käyttöön kehittyneempi osoitteiden hallintaratkaisu.

3.4 Tietoturvakartoitus

Tietoturvakartoituksen tarkoituksena on arvioida nykyisen verkkoinfrastruktuurin suojaustasoa ja tunnistaa mahdolliset haavoittuvuudet, väärinkonfiguroinnit tai puutteet, jotka voivat altistaa verkkoa uhilta. Kartoitus on olennainen osa verkon kehittämistä, sillä sen avulla voidaan tehdä perusteltuja päätöksiä korjaavista toimenpiteistä ja resurssien kohdentamisesta.

Kartoituksen tavoitteena on selvittää

- onko verkossa toteutettu riittävä segmentointi
- kuinka etäyhteyksiä hallitaan ja valvotaan
- ovatko laitteet ja ohjelmistot ajantasaisia
- miten käyttäjien ja toimittajien pääsy verkkoon on rajoitettu
- onko verkossa käytössä järjestelmät, jotka mahdollistavat uhkien havaitsemisen ja reagoinnin.

Yksi tärkeimmistä tarkasteltavista osa-alueista tietoturvan osalta on verkon segmentointi. Tällöin selvitetään, onko verkko jaettu loogisiin osiin esimerkiksi eri käyttäjäryhmien, palvelimien ja IoT-laitteiden välillä. Erityistä huomiota kiinnitetään siihen, mitä VLANeja on määritelty ja miten niiden välinen liikenne on rajattu palomuureilla tai reitityssäännöillä. Lisäksi tarkastetaan, onko vierailijaverkko asianmukaisesti eristetty sisäverkosta.

Etäyhteyksien hallinta on keskeinen tietoturvariski, jonka vuoksi dokumentoidaan kaikki käytössä olevat VPN-ratkaisut sekä muut etäkäyttöä mahdollistavat palvelut. Samalla arvioidaan, käyttääkö organisaatio monivaiheista tunnistautumista ja

hyppypalvelimia etäyhteyksien suojaamiseen. Etäyhteyksien hallinnassa tarkastellaan myös käyttöoikeuksien rajauksia ja mahdollisia aikarajoituksia.

Päivitysten ja haavoittuvuuksien hallinta liittyy laitteiden ja ohjelmistojen ajantasaisuuteen. Tarkistetaan, onko käyttöjärjestelmät, verkkolaitteiden ohjelmistot ja tietoturvaohjelmistot päivitetty säännöllisesti. Selvitetään myös, hyödynnetäänkö automaattisia päivitysjärjestelmiä tai keskitettyä hallintaa, sekä kuinka usein haavoittuvuusskannauksia suoritetaan.

Pääsynhallinnan osalta tarkastellaan, miten käyttäjien oikeudet on määritelty eri järjestelmissä. Arvioidaan, onko oikeuksia rajattu vain tarvittaviin palveluihin ja käytetäänkö järjestelmänhallintaan erillisiä hallintatunnuksia. Lisäksi selvitetään, kirjautuvatko sisäänkirjautumiset ja epäonnistuneet yritykset lokitiedostoihin.

Fyysinen turvallisuus on olennainen osa kokonaisvaltaista tietoturvaa. Tarkistetaan, sijaitsevatko verkkolaitteet lukituissa kaapeissa tai muissa rajoitetuissa tiloissa. Samalla selvitetään, onko palvelinsaleihin ja laitehuoneisiin pääsy rajoitettu vain luvan omaaville henkilöille.

Tapahtumien valvonta ja lokitus varmistavat, että poikkeavuudet havaitaan ajoissa. Tarkastellaan käytössä olevia järjestelmiä, joiden avulla tapahtumia seurataan, ja arvioidaan, miten lokitiedot kerätään, säilytetään ja analysoidaan. Lisäksi varmistetaan, onko käytössä hälytysjärjestelmiä ja kuka organisaatiossa vastaa lokien valvonnasta.

Tietoturvakartoituksen tulokset dokumentoidaan järjestelmällisesti. Jokaisesta osa-alueesta kirjataan

- tarkastetut kohteet ja menetelmät
- havaitut puutteet tai riskit
- kehitysehdotukset ja mahdolliset kiireelliset toimenpiteet.

Hyvin toteutettu tietoturvakartoitus auttaa tunnistamaan verkon suojauksen vahvuudet ja heikkoudet sekä toimii pohjana tietoturvan kehittämissuunnitelmalle.

3.5 Yhteenveto kartoituksesta

Kun edellä mainitut analyysit on suoritettu, seuraava vaihe on laatia selkeä ja kattava yhteenveto löydöksistä ja suosituksista. Ensimmäiseksi kaikki kartoituksessa kerätyt tiedot kootaan yhteen dokumenttiin, joka toimii perustana jatkotoimenpiteille. Tämä dokumentaatio sisältää tarkat tiedot nykytilasta, havaituista puutteista sekä jo olemassa olevista vahvuuksista.

Seuraavaksi laaditaan verkon optimointisuunnitelma, jossa määritellään tarvittavat parannukset. Näihin voi kuulua esimerkiksi laitteistopäivityksiä, verkkokonfiguraatioiden muutoksia tai tietoturvakorjauksia. Parannustoimenpiteet priorisoidaan kriittisyyden mukaan, ja niiden toteutukselle määritetään realistinen aikataulu.

Lopuksi varmistetaan verkon jatkuva toimivuus ja turvallisuus säännöllisillä auditoinneilla sekä automaattisilla valvontaratkaisuilla. Tämä jatkuvan kehityksen malli takaa, että infrastruktuuri pysyy ajan tasalla myös tulevaisuuden tarpeiden osalta. Kokonaisuudessaan kartoitus antaa yritykselle selkeän näkemyksen nykyisestä verkkoympäristöstään ja tukee päätöksentekoa sen kehittämiseksi.

4 UUDEN VERKON SUUNNITTELU

4.1 Uuden verkon suunnitteluperiaatteet ja tavoitteet

Uuden yritysverkon suunnittelu perustuu tarpeeseen rakentaa nykyaikainen, tehokas ja tietoturvallinen verkkoympäristö, joka vastaa organisaation nykyisiin ja tuleviin vaatimuksiin. Kartoitusvaiheessa havaittavat kehityskohteet osoittavat yleensä selkeästi, että verkon uudistaminen on välttämätöntä suorituskyvyn, hallittavuuden ja tietoturvan näkökulmista. Suunnittelun keskiössä on järjestelmän kokonaisvaltainen uudelleenrakentaminen, joka mahdollistaa paremman käytettävyyden ja turvallisuuden kaikille käyttäjäryhmille.

Verkkosuunnittelussa on tärkeää noudattaa selkeitä periaatteita, jotka tukevat verkon tehokkuutta, hallittavuutta ja tietoturvaa. Ensinnäkin verkon rakenteen tulee olla helposti ymmärrettävä ja loogisesti jäsennelty. Tämä tarkoittaa, että verkko voidaan jakaa eri kokonaisuuksiin esimerkiksi toimipisteiden, palvelinten ja käyttäjäryhmien perusteella, mikä helpottaa ylläpitoa ja kehittämistä.

Verkon hallintaa ja valvontaa varten otetaan käyttöön keskitetty ratkaisu. Tällainen järjestelmä mahdollistaa konfiguraatioiden hallinnan ja valvonnan yhdestä käyttöliittymästä, mikä tehostaa ylläpitotyötä ja vähentää virhemahdollisuuksia. Lisäksi keskitetty valvonta mahdollistaa automaattisten hälytysten ja raporttien avulla nopean reagoinnin mahdollisiin ongelmiin.

Tietoturva ei ole verkon erillinen osa-alue, vaan se tulee sisällyttää jokaiseen osaan verkon suunnittelun alusta lähtien. Tämä tarkoittaa, että jokainen ratkaisu ja komponentti suunnitellaan siten, että tietoturva on huomioitu jo suunnitteluvaiheessa, ei vasta myöhemmin lisättävänä ominaisuutena. Tämä lähestymistapa varmistaa kokonaisvaltaisen ja kestävän tietoturvan verkon kaikilla tasoilla.

Uuden verkon suunnittelutavoitteet on luotu kartoituksessa havaituista puutteista sekä organisaation nykyisistä ja tulevista toiminnallisista vaatimuksista. Verkon luotettavuus varmistetaan käyttämällä kahdennettuja reitittimiä ja redundantteja yhteyksiä tärkeimpiin solmupisteisiin. Kriittiset laitteet liitetään UPS-virtalähteisiin, ja niiden toimintaa seurataan jatkuvasti. Tietoturvaa vahvistetaan muun muassa käyttöoikeuksien hallinnalla, verkon segmentoinnilla, 802.1X-autentikoinnilla ja

salatuilla hallintayhteyksillä. Lisäksi otetaan käyttöön palomuurit ja tunkeutumisen estojärjestelmät. Verkon skaalautuvuus taataan valitsemalla laitteita, jotka tukevat suurempia IP-osoitealueita ja mahdollistavat laajennukset ilman merkittäviä fyysisiä muutoksia. Hallittavuuden parantamiseksi otetaan käyttöön keskitetty verkkohallintatyökalu, joka tukee reaaliaikaista valvontaa, laitehallintaa ja automaattista varmuuskopiointia. Verkko suunnitellaan tukemaan nykyaikaisia työtapoja, kuten etätyötä, pilvipalveluiden käyttöä ja mobiililaitteiden liittämistä. VPN-yhteyksille määritellään turvallisuuspolitiikat ja langattomat verkot eriytetään sisäverkosta SSID- ja VLAN-järjestelyin.

4.2 Verkkotopologia

Hierarkkinen verkkotopologia on paras ratkaisu, koska se jakaa verkon kolmeen eri tasoon, mikä parantaa liikenteen hallintaa ja tietoturvaa. Tämä malli takaa, että verkkoliikenne kulkee mahdollisimman sujuvasti ja vikatilanteissa voidaan rajata ongelmat nopeasti ilman, että koko yrityksen verkkoyhteydet häiriintyvät.

Tämän lisäksi hierarkkinen rakenne mahdollistaa verkon helpon laajentamisen, mikä on tärkeää yrityksen kasvaessa. Kun verkon rakenne on selkeä ja modulaarinen, uusia käyttäjiä, laitteita ja palveluita voidaan lisätä ilman suuria muutoksia koko infrastruktuuriin. Tämä säästää pitkällä aikavälillä sekä aikaa että kustannuksia.

Verkkotopologian valinnassa ei siis keskitytä vain nykyisiin tarpeisiin, vaan myös siihen, että verkko on pitkällä aikavälillä tehokas, hallittava ja turvallinen. Tämä mahdollistaa yrityksen liiketoiminnan jatkuvuuden ja teknologian kehityksen tukemisen ilman merkittäviä rakenteellisia muutoksia tulevaisuudessa.

4.3 Verkkotekniset ratkaisut ja verkkojen segmentointi

Uuden verkon tekninen toteutus rakentuu nykyaikaisten ja tietoturvallisten ratkaisujen varaan. Tavoitteena on kehittää kokonaisuus, joka on tehokas, skaalautuva ja helposti hallittava myös tulevaisuuden tarpeisiin. Tekninen suunnittelu perustuu aiemmin suoritetun kartoituksen havaintoihin, joiden perusteella verkkoa lähdetään suunnittelemaan nykyaikaisin menetelmin.

Erityistä huomiota kiinnitetään verkon segmentointiin, jonka avulla voidaan erottaa eri käyttäjäryhmien, laitteiden ja palveluiden liikenne toisistaan. Segmentointi vähentää riskejä, parantaa suorituskykyä ja mahdollistaa paremman hallinnan. Lisäksi liikennettä voidaan tarvittaessa rajoittaa tai valvoa VLAN- ja palomuurisäännöillä.

Verkon tekninen toteutus voidaan jakaa selkeisiin vaiheisiin, joista ensimmäinen on VLAN-rakenteen suunnittelu. Tässä vaiheessa verkko jaetaan loogisiin osiin eri osastojen, toimintojen ja laitekokonaisuuksien mukaan. Jokaiselle VLAN-alueelle määritetään oma IP-osoitealue, ja verkon hallinnan kannalta kriittiset laitteet, kuten palvelimet ja hallintalaitteet, erotellaan omiin VLANeihinsa työasemien, vierailijaverkon ja IoT-laitteiden ohella. Seuraavaksi konfiguroidaan kytkimet ja reititys siten, että määritellään pääsynvalvontasäännöt, joiden avulla voidaan tarkasti sallia tai estää liikennettä eri verkkojen välillä. Esimerkiksi vierailijaverkosta ei sallita liikennettä palvelinverkkoon, ja hallintaverkkoon pääsy rajoitetaan vain valtuutettuihin IP-osoitteisiin. Lisäksi palomuurisäännöillä ohjataan eri segmenttien välistä liikennettä estäen tarpeettomat yhteydet. Lopuksi otetaan käyttöön nykyaikaiset tietoturva- ja valvontaratkaisut, kuten SIEM-järjestelmät, tunkeutumisen estojärjestelmät sekä Zero Trust -mallin mukainen pääsynhallinta, joka perustuu jatkuvaan todennukseen ja vähimpien oikeuksien periaatteeseen.

4.4 Toimittajien etäyhteyden arviointi ja yhtenäistäminen

Useilla yrityksillä on ulkopuolisia toimittajia ja yhteistyökumppaneita, jotka tarvitsevat etäyhteyden organisaation verkkoon esimerkiksi järjestelmien ylläpitoa, ohjelmistopäivityksiä tai laitteistojen huoltoa varten. Nämä etäyhteydet ovat kriittisiä palveluiden jatkuvuuden kannalta, mutta ne voivat samalla muodostaa merkittävän tietoturvariskin, jos niitä ei hallita asianmukaisesti.

Kartoitusvaiheessa yleensä havaitaan, että toimittajien etäyhteyksiä ei ollut yhtenäistetty ja käytännöt vaihtelivat toimittajakohtaisesti. Yhteyksien tarkempi hallinta ja standardointi nousevat monesti keskeisiksi kehityskohteiksi uuden verkkoratkaisun suunnittelussa.

Etäyhteyksien standardointi ja turvallisuusperiaatteet ovat keskeisiä, kun halutaan varmistaa toimittajien hallittu ja suojattu pääsy yrityksen järjestelmiin. Jokaiselle ulkopuoliselle toimittajalle tarjotaan ennalta määritellyt VPN-yhteydet, jotka hyödyntävät turvallisia protokollia ja kuuluvat järjestelmän valvonnan piiriin. Spontaanit tai yksittäisille käyttäjille räätälöidyt etäyhteydet kielletään kokonaan. Etäyhteyden muodostaminen edellyttää aina monivaiheista tunnistautumista, joka voidaan toteuttaa esimerkiksi yhdistämällä salasana ja kertakäyttökoodi.

Kaikki yhteydet reititetään valvottujen hyppypalvelimien kautta, jolloin kaikki liikenne kirjataan lokitiedostoihin. Näin voidaan tarkasti jäljittää, kuka on muodostanut yhteyden, milloin se on tapahtunut ja mihin järjestelmiin on otettu yhteyttä. Toimittajilta estetään suora pääsy yrityksen kriittisiin järjestelmiin, kuten palvelinverkkoon tai hallintaverkkoon. Mikäli yhteys on tarpeellinen, se sallitaan vain väliaikaisesti ja rajoitetusti hyppypalvelimen kautta.

Pääsynhallinnan ja käyttöoikeuksien rajoittamisen osalta jokaiselle toimittajalle määritellään tarkasti heidän roolinsa sekä käyttöoikeudet perustuen siihen, mitä palveluita he tarvitsevat työnsä suorittamiseksi. Oletusarvoisesti pääsy muihin järjestelmiin estetään, ellei sitä ole erikseen hyväksytty. Toimittajille annetaan ainoastaan ne oikeudet, jotka ovat ehdottoman välttämättömiä sovittujen tehtävien hoitamiseksi. Esimerkiksi järjestelmävalvojan oikeuksia ei missään tilanteessa myönnetä ulkopuolisille ilman painavaa ja dokumentoitua perustetta.

Aikaperusteiset käyttöoikeudet lisäävät turvallisuutta rajaamalla toimittajien etäyhteydet tarkasti määriteltyyn ajanjaksoon. Esimerkiksi huoltotöiden yhteydessä toimittajalle voidaan myöntää oikeudet vain tietylle päivälle tai kellonajalle, jolloin yhteys on tarpeellinen. Lisäksi käyttöön otetaan automaattiset istunnon aikarajat, jotka katkaisevat yhteyden automaattisesti, mikäli sitä ei enää käytetä. Tämä vähentää merkittävästi riskiä siitä, että avoimeksi jäänyt yhteys jäisi huomaamatta ja voisi muodostaa tietoturvauhan.

Toimittajien etäyhteyksien valvonta ja raportointi ovat keskeinen osa verkkoinfrastruktuurin tietoturvaa. Kaikki etäyhteydet kirjataan automaattisesti järjestelmien lokitiedostoihin, joita analysoidaan säännöllisesti esimerkiksi SIEM-järjestelmän avulla. Tämä mahdollistaa poikkeavuuksien tunnistamisen ja reagoinnin ajoissa. Mikäli toimittaja yrittää päästä järjestelmään, johon hänellä ei ole käyttöoikeuksia,

järjestelmä laukaisee automaattisen hälytyksen. Näin mahdollisiin väärinkäytöksiin tai tietoturvapoikkeamiin voidaan puuttua välittömästi ja tehokkaasti.

5 TOTEUTUS JA KÄYTTÖÖNOTTO

5.1 Laitteiden asennus ja konfigurointi

Kun uusi verkkoinfrastruktuuri otetaan käyttöön, on tärkeää suorittaa laitteiden asennus ja konfigurointi systemaattisesti ja huolellisesti. Tämän vaiheen onnistuminen vaikuttaa suoraan verkon toimivuuteen, suorituskykyyn ja tietoturvaan.

Laitteiden fyysinen asennus aloitetaan sijoittamalla ne ennalta määriteltyihin paikkoihin, jotka on valittu verkkorakenteen, kattavuuden ja ylläpidettävyyden perusteella. Kytkimet, reitittimet, palomuurit ja langattomat tukiasemat asennetaan standardin mukaisesti 19 tuuman räkkikaappeihin. Laitteet kiinnitetään huolellisesti, jotta ne pysyvät turvallisesti paikoillaan ja ovat helposti huollettavissa. Ethernet-kaapelointi toteutetaan strukturoituna, mikä tarkoittaa, että kaapelit vedetään mahdollisimman lyhyttä ja selkeää reittiä pitkin. Kaapelit merkitään selkeästi ja suojataan sähkömagneettisilta häiriöiltä, jotta tiedonsiirto säilyy luotettavana.

Laitteiden peruskonfigurointi aloitetaan määrittämällä kytkimiin VLAN-konfiguraatiot, jotka tukevat suunniteltua verkkosegmentointia. Reitittimille luodaan sekä staattisia että dynaamisia reitityssääntöjä, joiden avulla verkkoliikenne ohjataan tehokkaasti eri segmenttien välillä. Palomuureihin asetetaan turvapolitiikat ja Access Control List -säännöt, jotka estävät ei toivotun liikenteen ja mahdollistavat vain sallittujen yhteyksien kulun. DHCP- ja DNS-palvelimet konfiguroidaan siten, että verkon laitteet saavat automaattisesti IP-osoitteet ja nimipalveluresurssit oikeista ja luotettavista lähteistä.

Langattoman verkon käyttöönotto toteutetaan asentamalla WLAN-tukiasemat suunnitelluille paikoille siten, että langaton signaali kattaa koko toimitilan tasaisesti ja ilman katvealueita. Verkon SSID:t jaetaan vähintään kahteen verkkoon, sisäverkkoon ja vierailijaverkkoon, jotka eristetään toisistaan esimerkiksi VLAN-konfiguraatioiden avulla. Langattoman verkon suojaus varmistetaan käyttämällä WPA3-salausta sekä 802.1X-autentikointia, jotka yhdessä tarjoavat vahvan suojan luvattomalta käytöltä ja takaavat turvallisen yhteyden verkon käyttäjille.

Hallintayhteyksien varmistamiseksi kaikki verkon laitteet liitetään valittuun keskitettyyn hallintaratkaisuun, joka mahdollistaa tehokkaan laitehallinnan ja etävalvonnan. Lisäksi käyttöön otetaan SNMP-protokolla, jonka avulla verkon tilaa voidaan seurata ja hallita reaaliaikaisesti. Tämä mahdollistaa nopean reagoinnin mahdollisiin häiriöihin ja tukee verkon ennakoivaa ylläpitoa.

Tietoturva-asetusten tarkistuksen yhteydessä varmistetaan, että kaikkiin verkkolaitteisiin on asennettu uusimmat ohjelmisto päivitykset, jotta tunnetut haavoittuvuudet on korjattu. Hallintayhteyksille luodaan yksilölliset hallintatunnukset, ja pääsy järjestelmiin sallitaan ainoastaan monivaiheisen tunnistautumisen kautta. Tämä parantaa merkittävästi järjestelmän suojausta luvattomalta käytöltä. Lisäksi kaikki laitteiden konfiguraatiot varmuuskopioidaan ennen tuotantovaiheen aloitusta, jotta mahdollisissa ongelmatilanteissa voidaan nopeasti palauttaa toimiva tilanne.

5.2 Pilottivaihe ennen tuotantoon siirtymistä

Ennen kuin uusi verkkoinfrastruktuuri otetaan käyttöön koko organisaation laajuisesti, suoritetaan pilottivaihe. Tämän vaiheen tarkoituksena on testata verkon toimivuutta, suorituskykyä ja tietoturvaa rajatulla käyttäjäryhmällä. Pilotti mahdollistaa mahdollisten ongelmien havaitsemisen ja korjaamisen ennen lopullista tuotantoon siirtymistä, mikä vähentää käyttöönottoon liittyviä riskejä.

Pilotointi sisältää monta eri vaihetta. Käydään tässä läpi, miten saadaan onnistunut pilotointi suoritettua.

Pilotointia varten valitaan testikäyttäjäryhmä, johon kuuluu työntekijöitä eri osastoilta. Valinnassa painotetaan monipuolista verkkokäyttöä, jotta saadaan kattava käsitys verkon toiminnasta erilaisissa tilanteissa. Mukaan otetaan sekä toimistolla työskenteleviä käyttäjiä että etäkäyttäjiä ja mobiililaitteiden hyödyntäjiä.

Verkon toimivuutta arvioidaan mittaamalla kaistanleveys ja viive, jotta varmistetaan sujuva tiedonsiirto. Langattoman verkon kattavuus ja signaalin laatu tarkistetaan koko toimitilan alueella. Lisäksi suoritetaan kuormitustestaus simuloimalla suurta liikennemäärää, minkä avulla arvioidaan verkon suorituskyky ruuhkatilanteissa.

Tietoturvatestauksen aikana varmistetaan, että VLAN-segmentointi toimii oikein eikä liikenne pääse vuotamaan verkkoalueiden välillä. Palomuurien ja pääsynhallintasääntöjen tehokkuutta testataan tunkeutumistestauksella. VPN-yhteyksien ja monivaiheisen tunnistautumisen toimivuus tarkistetaan käytännön testien avulla.

Palveluiden ja järjestelmien toiminnassa varmistetaan, että DHCP- ja DNS-palvelut jakavat IP-osoitteet ja nimipalvelut oikein. Yhteydet pilvipalveluihin, sisäverkkoon ja internetiin testataan huolellisesti. Valvontajärjestelmien toiminta tarkistetaan ja arvioidaan, tuottavatko ne luotettavaa ja ajankohtaista hälytystietoa poikkeustilanteista.

Pilottikäyttäjiltä kerätään palautetta muun muassa verkon nopeudesta, vakaudesta, käyttöönoton sujuvuudesta sekä mahdollisista ongelmista tai puutteista. Saatu palaute dokumentoidaan ja käsitellään yhdessä projektitiimin asiantuntijoiden kanssa, jotta tunnistetut kehityskohteet voidaan huomioida jatkosuunnittelussa.

Pilottivaiheessa havaittuihin ongelmatilanteisiin reagoidaan välittömästi ja ne korjataan ennen verkon laajempaa käyttöönottoa. Mikäli tarpeen, yksittäisten laitteiden tai verkon osa-alueiden konfiguraatio palautetaan aikaisempaan tilaan. Verkon suorituskykyä viimeistellään optimoimalla QoS-asetukset siten, että liikenteessä tärkeimmät sovellukset saavat etusijan.

5.3 Takaisinpalautussuunnitelma ongelmatilanteissa

Vaikka uuden verkkoinfrastruktuurin suunnittelu ja käyttöönotto tehdään huolellisesti, on aina olemassa riski siitä, että käyttöönoton aikana ilmenee odottamattomia ongelmia. Tämän vuoksi on olennaista laatia ennakoiva ja selkeä takaisinpalautussuunnitelma, joka mahdollistaa nopean siirtymisen aiempaan toimivaan järjestelmään ilman merkittäviä katkoksia yrityksen toimintaan.

Ennen kuin verkkoon tehdään muutoksia, kaikista verkkolaitteista otetaan varmuuskopiot niiden nykyisistä konfiguraatioista. Palvelimien tiedot varmuuskopioidaan sekä paikallisesti että pilvipalveluihin, jotta tarvittaessa on käytettävissä useita vaihtoehtoja tietojen palauttamiseen. IP-osoitteet, VLAN-konfiguraatiot ja

reititystaulukot dokumentoidaan selkeästi ja tallennetaan siten, että ne ovat helposti saatavilla kaikille henkilöille, jotka vastaavat järjestelmän ylläpidosta tai palautuksesta.

Jos verkon jokin VLAN tai segmentti ei toimi suunnitellulla tavalla, palautetaan kyseisen kytkimen tai reitittimen edellinen toimiva konfiguraatio. Mikäli palomuurisäännöissä tai pääsynhallinnassa havaitaan virheitä, otetaan käyttöön ennalta määritellyt varasäännöt tai palautetaan aikaisemmat asetukset. Langattoman verkon häiriötilanteissa voidaan palata aiempiin WLAN-asetuksiin tai ottaa väliaikaisesti käyttöön kaapeliyhteydet vakaan yhteyden varmistamiseksi. Mikäli uusi kokoonpano aiheuttaa verkon ylikuormittumista, palautetaan QoS-asetukset entiselleen ja niitä säädetään vaiheittain optimaalisemman suorituskyvyn saavuttamiseksi.

Vaiheittainen käyttöönotto mahdollistaa sen, että muutokset voidaan perua laitekohtaisesti ilman, että koko verkkoa tarvitsee palauttaa. Käytössä oleva konfiguraatioiden versiohallinta mahdollistaa aiempien, toimiviksi todettujen asetusten nopean käyttöönoton. Mikäli ilmennyttä vikaa ei saada nopeasti korjattua, otetaan käyttöön varasuunnitelma, jossa käyttäjät ohjataan takaisin aiempaan verkkoarkkitehtuuriin tai väliaikaisiin langattomiin tukiasemiin, jotta toiminta voi jatkua keskeytyksettä.

Tietohallinnolla on etukäteen määritelty vastuuhenkilöt, jotka on nimetty vastaamaan palautustoimenpiteistä eri järjestelmissä mahdollisen vikatilanteen sattuessa. Kaikista verkon muutoksista pidetään systemaattista kirjaa, jotta virheiden syyt voidaan jälkikäteen analysoida ja samankaltaiset tilanteet voidaan ehkäistä tulevaisuudessa. Lisäksi viestintäsuunnitelma takaa sen, että käyttäjille tiedotetaan viivytyksettä mahdollisista häiriöistä, niiden arvioidusta kestosta sekä suunnitelluista palautustoimenpiteistä.

5.4 Dokumentaatio

Verkkoinfrastruktuurin laadukas dokumentointi on olennainen osa verkon toimivuutta sillä se varmistaa verkon selkeän hallinnan ja vianmäärityksen. Hyvin ylläpidetty dokumentaatio vähentää käyttökatkojen riskiä ja nopeuttaa ongelmatilanteiden ratkaisemista.

Dokumentaatioon sisällytetään verkon topologia, laiteluettelo, IP-osoitteet, VLAN-määritykset, palomuurisäännöt ja pääsynhallintakäytännöt. Kaikki verkkolaitteiden konfiguraatiot tallennetaan järjestelmällisesti ja niihin tehdyt muutokset kirjataan ylös, jotta aikaisempiin asetuksiin voidaan tarvittaessa palata.

Verkonvalvontaan liittyvät lokitiedot ja hälytykset dokumentoidaan analysointia varten, jotta tietoturvapoikkeamat voidaan havaita ja korjata ajoissa. Lisäksi ohjelmistojen ja laitteistojen päivityshistoria tallennetaan, jotta järjestelmän ajantasaisuus voidaan varmistaa.

Dokumentaatio päivitetään säännöllisesti, ja sitä säilytetään sekä paikallisesti että pilvipalvelussa tietoturvallisesti. Kaikilla verkon ylläpidosta vastaavilla henkilöillä tulee olla pääsy dokumentaatioon, jotta he voivat toimia nopeasti ja tehokkaasti eri tilanteissa. Hyvin hoidettu dokumentaatio tukee verkon ylläpitoa, parantaa tietoturvaa ja mahdollistaa tehokkaan vianmäärityksen sekä verkon laajennukset ilman tarpeettomia viiveitä.

5.5 Ylläpito ja jatkokehitys

Verkkoinfrastruktuurin ylläpito on jatkuva prosessi, jonka tavoitteena on varmistaa verkon toimintavarmuus, tietoturva ja suorituskyky. Pelkkä suunnittelu ja käyttöönotto eivät tule riittämään, vaan verkko vaatii säännöllistä seurantaa, huoltoa ja kehittämistä, jotta se vastaa yrityksen tarpeisiin myös tulevaisuudessa.

Verkon toimintaa seurataan verkonhallintatyökaluilla, jotka mittaavat reaaliaikaisesti muun muassa kaistanleveyden käyttöä, latenssia ja verkkolaitteiden kuormitusta. Työkalut kuten PRTG tai SolarWinds tuottavat automaattisia hälytyksiä, joiden avulla voidaan reagoida ongelmatilanteisiin ennen kuin ne vaikuttavat liiketoimintaan.

Tietoturvan ylläpitäminen vaatii säännöllisiä ohjelmistopäivityksiä ja tietoturvakorjauksia. Palomuureihin, reitittimiin ja kytkimiin asennetaan uusimmat tietoturva päivitykset, jotta tunnetut haavoittuvuudet saadaan korjattua. Verkon pääsynhallintaa kehitetään varmistamalla, että vain tarvittavilla henkilöillä on oikeudet kriittisiin järjestelmiin ja monivaiheinen tunnistautuminen pidetään pakollisena hallintayhteyksissä.

Verkon suorituskykyä optimoidaan analysoimalla tietoliikennemalleja ja muokkaamalla QoS-asetuksia, jotka takaavat tärkeimpien palveluiden sujuvan toiminnan. Tarvittaessa lisätään uusia verkkolaitteita tai päivitetään kapasiteettia, jotta verkko skaalautuu yrityksen kasvaessa. Jatkokehityksen osalta verkkoa voidaan laajentaa ja modernisoida uusia teknologioita hyödyntämällä. Tulevaisuudessa voidaan siirtyä IPv6-osoitteisiin ja ottaa käyttöön SDWAN-teknologia, joka parantaa etätoimipisteiden verkkoyhteyksiä, sekä hyödyntää pilvipohjaisia verkonhallintaratkaisuja. Automaatio ja tekoälypohjaiset analyysityökalut mahdollistavat verkon proaktiivisen hallinnan, jossa järjestelmät ennakoivat ja ehkäisevät mahdollisia vikatilanteita ennen niiden toteutumista. Ylläpidon ja kehityksen jatkuva seuranta varmistaa, että verkkoinfrastruktuuri pysyy turvallisena, tehokkaana ja yrityksen liiketoimintaa tukevana pitkällä aikavälillä.

6 POHDINTA

Tämä opinnäytetyö toimii kokonaisvaltaisena projektisuunnitelmana keskikokoisen yrityksen verkkoinfrastruktuurin uudistamiseksi. Työn tavoitteena ei ollut pelkästään teoreettinen tarkastelu tai nykytilan analyysi, vaan selkeän ja toteutuskelpoisen mallin laatiminen, jonka avulla verkon kehitys voidaan käynnistää vaiheittain ja hallitusti. Suunnitelma sisältää kaikki keskeiset osa-alueet, nykyverkon kartoituksen, kehityskohteiden tunnistamisen, uuden verkon teknisen suunnittelun, käyttöönoton, ylläpidon ja jatkokehityksen.

Opinnäytetyössä esitetyt ratkaisut perustuvat nykyaikaisiin ja vakiintuneisiin käytäntöihin, joita voidaan hyödyntää konkreettisessa toteutuksessa. OSI-mallia hyödynnettiin verkkorakenteen hahmottamisessa ja eri komponenttien sijoittamisessa oikeille tasoille. Segmentoinnin, pääsynhallinnan, Zero Trust-mallin, 802.1X-autentikoinnin ja VPN-yhteyksien avulla muodostetaan tietoturvallinen ja selkeästi hallittava kokonaisuus. Työssä kuvattiin tarkasti myös käyttöönoton eteneminen sekä toimintasuunnitelmat mahdollisten ongelmatilanteiden varalle.

Tämän projektisuunnitelman avulla voidaan käynnistää todellinen verkkouudistus vaiheittain. Pilottivaiheen toteutus, laitteiden määrittely ja konfigurointi sekä dokumentoinnin mallipohjat antavat käytännön valmiudet aloittaa tekninen toteutus ilman, että jokainen vaihe täytyy suunnitella uudelleen. Suunnitelma on skaalautuva ja laajennettavissa myös tulevaisuuden tarpeisiin, kuten IPv6:een siirtyminen, SDWAN-teknologian käyttöönotto ja tekoälypohjainen verkonvalvonta.

Opinnäytetyön eettisyys ja luotettavuus toteutuivat hyvin, sillä kaikki ratkaisut perustuvat ajankohtaisiin lähteisiin ja vakiintuneisiin käytäntöihin. Henkilötietoja ei käsitelty, ja lähteet on viitattu asianmukaisesti. Lisäksi suunnitelma nojaa oman oppimisen ja työkokemuksen kautta tehtyyn käytännön analyysiin, mikä tekee siitä realistisen ja käytännönläheisen.

Tätä projektia ei ole vielä toteutettu käytännössä, mutta sen sisältämät vaiheet ja ratkaisuehdotukset tarjoavat selkeän etenemispolun toteutukselle. Työ toimii siis lähtökohtana yrityksen IT-osaston toteutettavalle verkkouudistukselle ja samalla mallina myös muille organisaatioille, jotka haluavat kehittää infrastruktuuriaan kustannustehokkaasti ja nykyaikaisia tietoturvaperiaatteita noudattaen.

Työ on ollut minulle arvokas oppimisprosessi, jossa olen päässyt yhdistämään teoriaa, käytännön osaamista ja projektinhallinnan näkökulmaa. Se on vahvistanut teknistä ymmärrystäni sekä kykyäni suunnitella ja perustella tietoverkkoratkaisuja osana laajempaa liiketoimintaympäristöä.

LÄHTEET

Bryce, L. 2024a. Router vs Switch - Difference Between Them. Guru99. 27.4.2024. Viitattu 28.2.2025. https://www.guru99.com/fi/router-vs-switch-difference.html

Bryce, L. 2024b. Subnetting and Subnet Mask Explained. Guru99. 21.11.2024. Viitattu 15.2.2025. https://www.guru99.com/fi/subnetting-subnet-mask.html

Cisco Systems, Inc. 2025. What is a Router? Viitattu 10.4.2025. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html

Cloudflare, Inc. 2025. What is the Simple Mail Transfer Protocol (SMTP)? Viitattu 28.3.2025. https://www.cloudflare.com/learning/email-security/what-is-smtp/

Einoryte, A. 2023. Types of IP Addresses: All you need to know. Nordvpn 18.7.2023. Viitattu 1.3.2025. https://nordvpn.com/fi/blog/types-of-ip-addresses/

F-Secure 2022. Mikä on palomuuri? Viitattu 14.3.2025. https://www.f-secure.com/fi/articles/firewall

GeegsforGeeks 2023. Network protcols. Viitattu 1.4.2025. https://www.geeksforgeeks.org/network-protocols/

GeeksforGeeks 2024a. What is HTTP? Viitattu 12.2.2025. https://www.geeksforgeeks.org/what-is-http/

GeeksforGeeks 2024b. Difference Between Router and Switch. Viitattu 28.2.2025. https://www.geeksforgeeks.org/difference-between-router-and-switch/

GeeksforGeeks 2025a. Types of Network Topology. Viitattu 4.4.2025. https://www.geeksforgeeks.org/types-of-network-topology/

GeeksforGeeks 2025b. Open Systems Interconnection Model (OSI). Viitattu 15.2.2025. https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/

GeeksforGeeks 2025c. Introduction of firewall in computer network. Viitattu 1.4.2025. https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

Informatec Digital 2024. Mitä tietokoneverkot ovat ja miten ne muuttavat digitaalista maailmaa. Viitattu 10.2.2025. https://informatecdigital.com/fi/Mit%C3%A4-ovat-tietokoneverkot%3F/

Klusaite, L. 2022. TCP IP Mikä se on, mihin sitä tarvitaan ja mitä se tekee? Nordvpn 9.3.2022. Viitattu 14.3.2025. https://nordvpn.com/fi/blog/tcp-ip-protokolla/

Mills, M. 2021. Mikä on DNS-protokolla ja miksi se on niin tärkeä? Itigic 13.10.2021. Viitattu 10.3.2025. https://itigic.com/fi/what-is-dns-protocol-and-why-is-it-so-important/

Patchbox 2022. What is a Network Switch. 4.7.2022 Viitattu 10.3.2025. https://patchbox.com/fi/blog/what-is-a-network-switch/

Yasar, K. Irei, A. Scarpati, J. 2025. What is a router? TechTarget, Inc. Viitattu 12.3.2025. https://www.techtarget.com/searchnetworking/definition/router

Zieniute, U. 2022. Mitä TCP ja UPD ovat? Nordvpn 6.3.2022. Viitattu 10.3.2025. https://nordvpn.com/fi/blog/tcp-udp-protokolla/