AVOIMEN LÄHDEKOODIN VPN-RATKAISU PIENYRITYKSEN TARPEISIIN

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tieto- ja viestintätekniikka, insinööri (AMK)

Kevät 2022

Jukka Kuri

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka Tiivistelmä
Tekijä Jukka Kuri Vuosi 2022
Työn nimi Avoimen lähdekoodin VPN-ratkaisu pienyrityksen tarpeisiin
Ohjaaja Teemu Järvenpää

Opinnäytetyön tavoitteena oli valita opinnäytetyön tilaajalle soveltuva avoimen lähdekoodin VPN-protokolla ja havainnollistaa sen käyttöönotto remote access -moodia hyödyntäen. Tilaajana toimi viestintäalan pienyritys, jonka tehokas toiminta vaatii mahdollisimman suurella tiedonsiirtokyvyllä varustetun VPN-ratkaisun.

Opinnäytetyön teoriaosuudessa tarkasteltiin avoimella lähdekoodilla levitettyjä VPN-tekniikoita sekä avoimen lähdekoodin OpenVPN- ja Wireguard-protokollia. Opinnäytetyön tilaajalle paremmin soveltuvan protokollan valitsemiseksi, suoritettiin protokollien välillä laadullinen analyysi, hyödyntäen painotettua päätöksentekomatriisia. Tilaajalle paremmin soveltuvaksi protokollaksi osoittautui Wireguard-protokolla. Opinnäytetyön toiminnallisessa osuudessa suoritettiin Wireguard-protokollaa hyödyntäen, havainnollistava VPN-ratkaisun käyttöönotto, tilaajan verkkoinfrastruktuuria toiminnallisuuksiltaan vastanneessa koeympäristössä. Käyttöönotto sisälsi VPN-palvelimen sekä Windows- ja Linux-käyttöjärjestelmien remote client -toiminnallisuuksien käyttöönoton.

Toiminnallisessa osuudessa suoritettu VPN-ratkaisun käyttöönotto, kyettiin suorittamaan onnistuneesti ja käyttöönotto läpäisi sille laaditun testiohjelman. Toiminnan kehittämisen kannalta Wireguard-protokollan avoin lähdekoodi mahdollistaa erilaisten avoimen lähdekoodin lisäosien asentamisen, esimerkiksi VPN-yhteyksien ylläpitoa ja hallintaa helpottamiseksi.

Avainsanat Wireguard, avoin lähdekoodi, VPN-tekniikka, tietoverkkotekniikka
Sivut 35 sivua ja liitteitä 6 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and communication technology
Author Jukka Kuri
Subject Open source VPN solution for small business
Supervisor Teemu Järvenpää

Abstract
Year 2022

The aim of this thesis was to choose an open source VPN protocol which complies best with the client's requirements, and demonstrate the implementation of that VPN protocol in remote access mode. The client of this thesis is a small business that operates in the communication technology industry.

The theoretical section of this thesis covered different open source VPN technologies and two different open source VPN protocols, which were OpenVPN and Wireguard. These two protocols were compared together and analysized using a weighted decision matrix, with the aim to find a better protocol for the client. The better protocol for the client was Wireguard. In the practical section of this thesis, implementation of Wireguard was demonstrated, using a test enviroment which expressed the main functions of the client's network. Implementation was performed with the VPN server and two different remote clients, which were laptops running with Windows and Linux operating systems.

Wireguard was implemented successfully and it passed the test program – which was made particularly for this thesis. Wireguard is an open source protocol which offers a possibility to develope the VPN system in the future, with different open source extensions, such as management interface.

Keywords Wireguard, open source, VPN technique, datanetworks
Pages 35 pages and appendices 6 pages

Sisällys

Lyhenteet

1 Johdanto 1
2 Virtual private network 2
2.1 VPN-tekniikat 3
2.1.1 Site-to-site 4
2.1.2 Remote access 6
2.2 VPN-protokollat 7
2.2.1 OpenVPN 8
2.2.2 Wireguard 10
3 Tilaaja 14
3.1 Tilaajan verkko 14
3.2 Tilaajan vaatimukset 15
4 Vertailu 17
4.1 Analysoitavat ominaisuudet ja painotukset 17
4.2 Matriisianalyysi 18
5 Toteutus 20
5.1 Koeympäristö ja testitavoitteet 21
5.2 Asennukset ja VPN:n konfigurointi 23
5.2.1 Wireguard-palvelin 23
5.2.2 Remote access -client Linux 24
5.2.3 Remote access -client Windows 25
5.2.4 Verkon muut laitteet 26
5.3 Asennusten todentaminen 27
5.4 Havainnot 29
6 Yhteenveto 30
Lähteet 32

Kuvat ja taulukot

Kuva 1. Site-to-site -tekniikalla toteutettu VPN-yhteys. 5
Kuva 2. Remote access -tekniikalla toteutettu VPN-yhteys. 7
Kuva 3. Wireguard-palvelimen salausavainreititystaulu (Donenfeld, s. 5, 2020a). 13
Kuva 4. Tilaajan verkkoinfrastruktuuri ja tavoiteltu loppuasetelma. 15
Kuva 5. Koeympäristön verkkokuva. 22
Kuva 6. VPN-palvelimen konfiguraatiotiedosto wg0.conf. 23
Kuva 7. Linux-työaseman konfiguraatiotiedosto wg0.conf. 24
Kuva 8. Window-työaseman VPN-asetukset tunnelille wg0. 26
Kuva 9. Linux-työaseman suorittamat testit 1–3. 27
Kuva 10. Windows-työaseman suorittamat testit 1–3. 28
Kuva 11. VPN-palvelimen ylläpitonäkymä voimassaolevista VPN-yhteyksistä. 28

Taulukko 1. Painotettu päätöksentekomatriisi. 20

Liitteet

Liite 1 VPN-palvelimen asetukset
Liite 2 Linux-työaseman VPN-asetukset
Liite 3 Windows-työaseman VPN-asetukset

Lyhenteet

AD	Active Directory
AES	Advanced Encryption Standard
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IPSec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation
SASE	Secure Access Service Edge
SSH	Secure Shell protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TSL	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

1 Johdanto

Etätyö yleistyi voimakkaasti koronapandemiasta johtuen vuonna 2020 ja eniten etätyötä tehdään tieto- ja viestintätekniikan alalla (Leskinen, 2021). Etätyö asettaa lisävaatimuksia tietoturvallisuudelle, korostaa tiedon ja datan eheyttä, luottamuksellisuutta sekä käytettävyyttä, osana toimivaa työskentelyä. Työn vaatimat tiedot ja välineet tulee olla työntekijän käytettävissä oikea aikaisesti sekä turvallisesti. Yksi tätä vaatimusta tukeva ratkaisu on yksityisen virtuaaliverkon yhteys, eli VPN-yhteys ja sen mahdollistama, salauksella suojattu pääsy etäältä yrityksen sisäverkkoon ja sisäverkon palveluihin. (Markkola, 2020, ss. 12, 48)

Opinnäytetyön tilaaja on viestintäalan pienyritys, joka haluaa suosituksia ja esimerkkiratkaisun heille sopivasta VPN-yhteydestä. Opinnäytetyön teoreettisessa osuudessa tutustutaan VPN-tekniikkaan sekä kahteen erilaiseen avoimen lähdekoodin VPN-protokollaan. Käsiteltävät protokollat ovat OpenVPN sekä Wireguard. OpenVPN on ollut vuosien ajan suosituin avoimen lähdekoodin VPN-protokolla, jolle vaihtoehtoiseksi ratkaisuksi on noussut Wireguard-protokolla (Long, 2022). Näiden kahden protokollan – suositun ja uuden – välillä suoritetaan laadullinen analyysi, tilaajan tarpeita parhaiten vastaavan protokollan löytämiseksi. Analyysin perusteella valitusta protokollasta toteutetaan opinnäytetyön toiminnallisessa osuudessa havainnollistava VPN-ratkaisu, joka mallintaa ratkaisun asentamista ja käyttöönottoa tilaajan yksinkertaistetussa verkkoinfrastruktuurissa.

Tilaajan toiveesta opinnäytetyössä käsiteltävät tilaajan verkkoinfrastruktuuri sekä toiminnan erityispiirteet, ovat rajattu sisältämään ainoastaan VPN-ratkaisuun vaikuttavat tekijät. Tästä syystä opinnäytetyössä ei käsitellä yksityiskohtaisesti yrityksen käyttämiä verkkolaitteita, IP-osoitteita tai kuvata tarkasti VPN-yhteyden avulla tapahtuvaa työskentelyä. Yrityksen käyttämistä ratkaisuista, kuten verkkoinfrastruktuurista, on luotu opinnäytetyötä varten yleismalliset versiot, joilla opinnäytetyön toiminnallinen osuus toteutetaan.

Opinnäytetyössä pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

1. Millaisia avoimeen lähdekoodiin perustuvia VPN-tekniikoita on olemassa?

2. Miten OpenVPN- ja Wireguard-protokollat toimivat?
3. Millaisia vaatimuksia tilaajan verkkoinfrastruktuuri ja toiveet asettavat tulevalle VPN-ratkaisulle?
4. Kumpi avoimen lähdekoodin VPN-protokolla – OpenVPN vai Wireguard – on laadullisesti parempi valinta tilaajan tarpeisiin?
5. Miten tilaajalle sopiva VPN-ratkaisu otetaan käyttöön sisäverkon palvelimella ja etätyöskentelyyn tarkoitetuilla päätelaitteilla?

2 Virtual private network

Julkisen verkkoinfrastruktuurin välityksellä jaettua, yksityiseen käyttöön tarkoitettua tietoverkkoa, kuten etäyhteyttä tai yrityksen toimipaikkojen välistä yhteyttä, kutsutaan virtuaaliseksi yksityisverkoksi eli VPN-verkoksi (Perlmutter & Zarkower 2000/2001, s. 10). VPN-tekniikan avulla, yksityiseksi tarkoitettu tietoliikenne salataan ennen julkiseen verkkoon siirtämistä ja vastaanottajalle saavuttuaan, salattu tietoliikenne avataan selkokieliseksi. Tällöin tietoliikenteen yksityisyys kyetään säilyttämään liikennöitäessä julkisessa verkossa, kuten internetissä. VPN-tekniikan hyödyntäminen kuluttajapuolella liittyy hyvin vahvasti anonymiteetin ja yksityisyyden vahvistamiseen, kun taas yritysmaailmassa käytetyt VPN-yhteydet on rakennettu pääosin sujuvamman ja tietoturvallisemman etätyöskentelyn mahdollistamiseksi. (Hoffman, 2021)

VPN-tekniikka on yleinen kuvaus käytetystä yhteystyypistä, jonka tarkka tekninen toiminta määrittyy käytetyn VPN-protokollan ja sen ominaisuuksien mukaan (Williams, 2022). Tässä luvussa käsitellään ainoastaan toimeksiannon kannalta relevantteja VPN-tekniikoita, eli yritysmaailmaan suunniteltuja ratkaisuja, sekä niihin sopivia itse ylläpidettäviä avoimen lähdekoodin VPN-protokollia. Näin ollen kuluttajille suunnitellut ratkaisut ja niiden käyttöperiaatteet ovat rajattu käsittelyn ulkopuolelle. Tässä luvussa vastataan tutkimuskysymyksiin*: Millaisia avoimeen lähdekoodiin perustuvia VPN-tekniikoita on olemassa* sekä *miten OpenVPN- ja Wireguard-protokollat toimivat*?

2.1 VPN-tekniikat

VPN-tekniikka käsittää yleisellä tasolla kahden päätelaitteen välille muodostettavaa päästä päähän salattua tiedonsiirtoyhteyttä. Salattu yhteys voidaan muodostaa esimerkiksi tietokoneesta tai älypuhelimesta palvelimeen, palvelimesta palvelimeen tai tietokoneesta toiseen. Käytettävät päätelaitteet vaihtelevat käyttötapauksen mukaisesti. Esimerkiksi toimistojen väliset yhteydet toteutetaan yleensä palvelimesta palvelimeen, jolloin kyseessä on site-to-site yhteys, kun taas etänä työskenneltäessä yhteys toteutetaan yleensä tietokoneesta palvelimeen, jolloin kyseessä on remote access -yhteys. (Tyson, Pollette & Crawford, 2021)

Molemmissa VPN-tekniikoissa – remote access ja site-to-site – on mahdollista määrittää tietoliikenteen tunnelointi joko full tunnel- tai split tunnel -moodeihin. Full tunnel -moodissa kaikki käyttäjän tietoliikenne ohjataan VPN-tunneliin ja sitä kautta esimerkiksi yrityksen lähiverkkoon, josta se reitittyy julkiseen internetiin ja sen palveluihin. Tällaisessa tapauksessa etätyössä olevan työntekijän tarkastaessa säätiedot internetistä, hänen tietoliikenteensä sääsivulle kulkee ensin salattuna hänen tietokoneeltaan yrityksen verkkoon, josta se reitittyy internetissä olevaan sääpalveluun ja sieltä takaisin. Full tunnel -tekniikassa kaikki tiedonsiirto vaikuttaa VPN-yhteyteen ja tästä johtuen mahdollisesti kuormittaa yhteyttä. Vaihtoehtoinen ratkaisu full tunnel -tekniikalle on split tunnel. Split tunnel -tekniikassa on mahdollista määrittää salattava – VPN-tunnelin kautta välitettävä – tietoliikenne erikseen muusta tietoliikenteestä, kuten julkisten internetpalveluiden käytöstä. Split tunnel -tekniikassa yleensä vain yrityksen sisäverkkoon tarkoitettu liikenne tunneloidaan ja kaikki muu liikenne jätetään tunneloinnin ulkopuolelle. Tällaisessa tapauksessa etätyössä olevan henkilön tarkastaessa säätietoja, tietoliikenne reitittyisi suoraan hänen päätelaitteeltaan internetiin ja sääpalveluun sekä sieltä takaisin. Samaan aikaan kuitenkin työntekijän suorittamat työasiat kulkisivat päätelaitteelta tunneloituina yrityksen lähiverkkoon. (Chapple & Seidl, 2018, ss. 370-371)

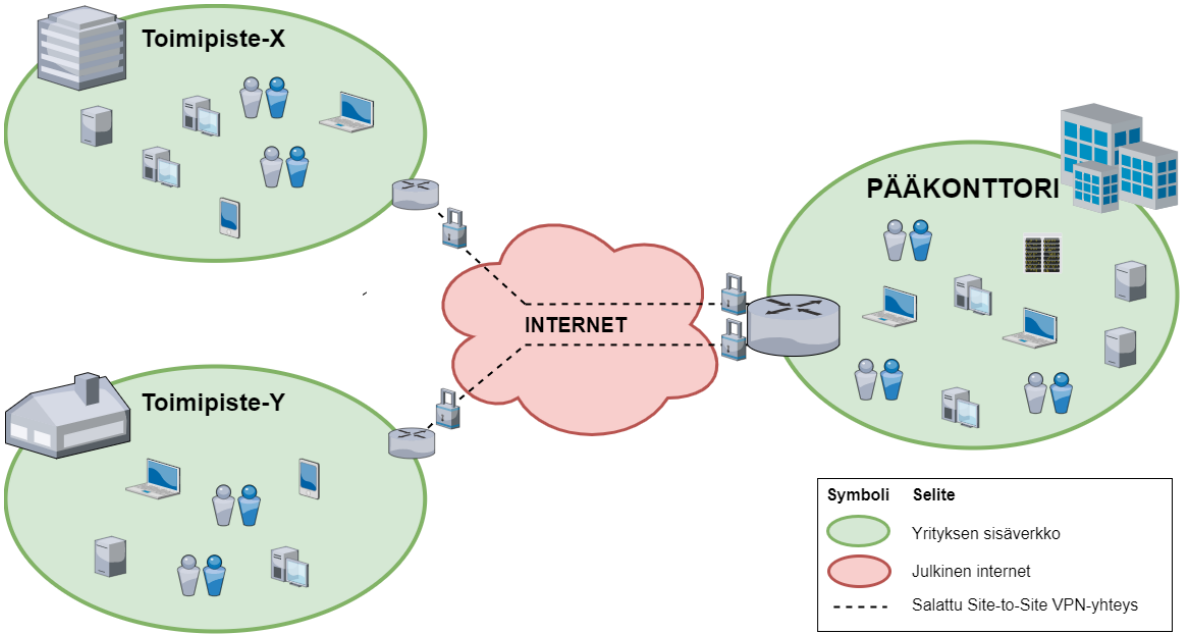
Koronapandemian aiheuttama etätyöskentelyn nopea kasvu, aiheutti useille yrityksille ongelmia VPN-yhteyksien tiedonsiirtokapasiteettien osalta, mikäli heillä oli käytössään full tunnel -tekniikka. Kasvanut etätyöskentelyn määrä hidastutti yritysten verkkoja

huomattavasti. Yksi suositus hidastumisen korjaamiseksi oli split tunnel -tekniikan käyttöönotto yrityksissä. Split tunnel -tekniikan käyttöönotto vaatii tarkat määrittelyt tekniikan toteuttamiselle, sillä väärin konfiguroituna kyseinen tekniikka saattaa mahdollistaa hyökkääjälle pääsyn ulkoverkosta yrityksen sisäverkkoon (Jeffery, 2020). Suuresta hyökkäysvektorista johtuen, yritysten tulisi tehdä riskiarvio aina tapauskohtaisesti split tunnel -tekniikan käyttöönotosta ja harkita tarkkaan, mikä tietoliikenne jätettäisiin tunneloinnin ulkopuolelle. (Kyberturvallisuuskeskus, 2020)

2.1.1 Site-to-site

Site-to-site -yhteyttä käytetään, kun halutaan yhdistää kaksi tai useampia eri lähiverkkoja toisiinsa, julkisen internetin yli VPN-tekniikan avulla. Tällainen käyttötapaus on esimerkiksi yrityksen kahden eri toimipisteen sisäverkkojen liittäminen toisiinsa. Tällöin toimipisteiden lähiverkkoihin perustetaan VPN-palvelimet, jotka määritetään muodostamaan niiden välille jatkuvasti päällä oleva salattu VPN-tunneli. Toimipisteestä toiseen tapahtuva liikenne ohjataan palvelimien väliseen VPN-tunneliin, jolloin tietoliikenne kulkee toimisteiden välillä salattuna. Tietoliikenteen salauksesta ja salauksen purkamisesta vastaavat toimipisteiden verkkotopologioiden reunamilla sijaitsevat VPN-palvelimet, jolloin käyttäjä ei edes välttämättä huomaa liikennöivänsä VPN:n avulla toimipisteestä toiseen. Kuvassa 1 on esitetty esimerkkikuva site-to-site verkosta, jossa kaksi erillistä toimipistettä on yhdistetty päätoimipisteeseen VPN-yhteyden avulla. (Paloalto, n.d.b)

Kuva 1. Site-to-site -tekniikalla toteutettu VPN-yhteys.



Site-to-site -yhteyksien määrä on nykyaikana vähenemään päin, sillä pilvipalveluiden laajeneminen ja palveluiden kehittyminen ovat mahdollistaneet myös VPN-ratkaisun siirtämisen pilveen. Pilvipohjaisissa VPN-palveluissa oletuksena on, että yrityksellä ei ole enää itsenäisesti hallittua datakeskusta tai suurta ylläpidettävää verkkoa, vaan yrityksen omat palvelut ovat myös pilvessä. Pilveen siirretyt palvelut tarkoittavat sitä, että toimipisteiden välillä ei tarvitse tiedonsiirtoon salattua VPN-tunnelia, vaan toimipiste tai jokainen työntekijä muodostaa oman VPN-yhteyden pilvipalveluun ja täten yrityksen pilviverkkoon. Tällaista palvelua kutsutaan termillä SASE (secure access service edge) ja palveluja on ostettavissa ainakin suurimmilta pilvipalveluiden tarjoajilta. (Korolov, 7.4.2022)

Pilvipohjainen SASE-palvelun periaate muistuttaa hyvin paljon remote access -VPN-yhteyttä, jossa käyttäjät muodostavat yksittäisiä VPN-tunneleita oman päätelaitteen ja yrityksen VPN-palvelimen välille. Vaikka pilvipalveluiden käyttö on lisääntynyt ja todennäköisesti lisääntyy jatkossa, ei site-to-site -yhteyksien tarve poistu todennäköisesti kokonaan. Tämä johtuu siitä, että kaikki toimijat eivät halua tai kykene siirtymään pilvipalveluiden pariin. Esimerkiksi tämän opinnäytetyön tilaaja on panostanut omaan verkkoinfrastruktuuriinsa niin paljon, että he haluavat kehittää ja ylläpitää sitä itsenäisesti myös jatkossa, eivätkä tästä syystä pidä pilvipalvelua heille sopivana vaihtoehtona.

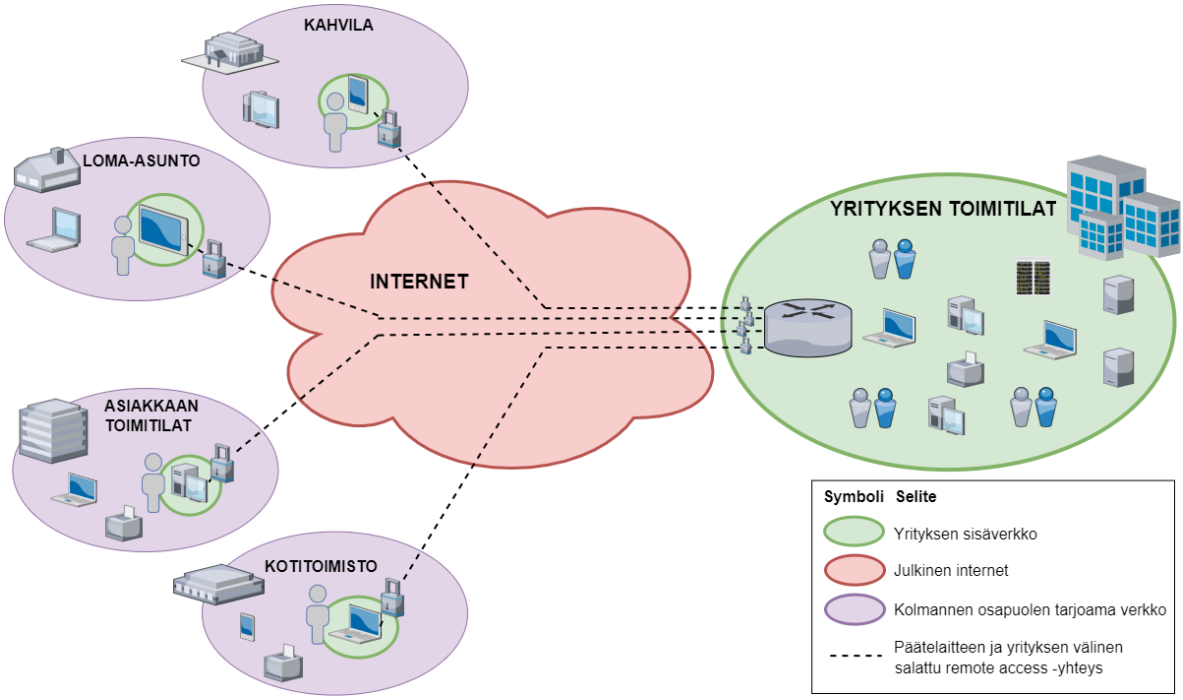
2.1.2 Remote access

Remote access -yhteys on salattu VPN-yhteys, josta käytetään joissain yhteyksissä myös termiä host-to-site. Remote access -yhteydessä työntekijöiden käytössä olevat erilaiset päätelaitteet, kuten kannettavat tietokoneet tai mobiililaitteet, muodostavat niihin asennetun asiakasohjelmiston avulla salatun point-to-point -VPN-tunnelin yrityksen sisäverkossa sijaitsevaan VPN-palvelimeen. Salatun VPN-tunnelin mahdollistamana työntekijän päätelaite käyttäytyy kuin fyysisesti yrityksen toimitiloissa oleva sisäverkkoon kytketty laite. Remote access -yhteyttä varten yrityksen sisäverkossa sijaitsevaan VPN-palvelimeen tulee asettaa ja hallita, jokaista etäyhteyttä laite- tai käyttäjäkohtaisesti – käyttöön valitun VPN-protokollan vaatimalla tavalla. Toimivaa remote access -yhteyttä varten päätelaitteille tulee asentaa ja konfiguroida asiakasohjelmisto, joka vastaa päätelaitteella salatun VPN-tunnelin muodostamisesta, ylläpidosta sekä liikennöinnistä. Osa VPN-protokollista vaatii remote access -toiminnossa protokollan oman asiakasohjelmiston käyttöä, mutta osa protokollista hyväksyy myös käyttöjärjestelmien kuten Microsoft Windows:n sisäänrakennetun asiakasohjelmiston käytön. (Tyson ym., 2021)

Remote access -yhteyden käytössä on monia työskentelyä tukevia puolia; salattu yhteys mahdollistaa pääsyn etäältä yrityksen tiedostoihin ja tietoihin, jolloin päätelaitteella ei ole tarpeen säilyttää kaikkea tietoa tai tiedostoja, vaan niitä käytetään salatun VPN-tunnelin välityksellä yrityksen sisäverkossa. Tällä tavoin toimimalla on mahdollista pienentää mahdollisia haittavaikutuksia ja riskejä, mikäli päätelaite esimerkiksi häviäisi tai varastettaisiin työntekijältä. (Gargiulo, 2018)

Remote access -yhteys on mahdollista muodostaa hyödyntäen mitä tahansa verkkoa, joka on yhteydessä internetiin ja sitä kautta yrityksen verkkoon. Tällaisia niin kutsuttuja kolmannen osapuolen verkkoja voivat olla esimerkiksi kahviloiden tarjoamat maksuttomat WLAN-verkot, työntekijän kotona tai mökillä oleva internetyhteys tai asiakkaan yritysverkko. Toisin sanoen remote access -yhteys mahdollistaa sijainnista riippumattoman työskentelyn, kunhan päätelaite on kytkettynä johonkin internetiin yhteydessä olevaan verkkoon. Remote access -yhteyden mahdollistama laitekohtainen tunnelointi useammasta eri sijainnista yrityksen sisäverkkoon on esitetty kuvassa 2. (Peek, 2021)

Kuva 2. Remote access -tekniikalla toteutettu VPN-yhteys.



Pilvipohjainen SASE-palvelu on vähentänyt myös remote access -yhteyksien määrää ja erityisesti isoissa yrityksissä, joissa työskennellään paljon etänä, on tehokkaampaa hyödyntää pilvipalveluiden tarjoamaa VPN-toiminnallisuutta (Paloalto, n.d.a). Pilvipalveluiden kasvusta huolimatta remote access -toiminnallisuus on erittäin käyttökelpoinen ja kustannustehokas ratkaisu pienemmissä yrityksissä, joissa osaaminen ja resurssit mahdollistavat oman VPN-palvelun ylläpitämisen. On myös yrityksiä, jotka eivät halua luovuttaa omistamaansa dataa ulkopuoliselle pilvipalvelun tarjoajalle, joten tällaisille yrityksille remote access -toiminnallisuus on edelleen käyttökelpoinen. (Gargiulo, 2018)

2.2 VPN-protokollat

VPN-protokolla käsittää tarkan teknisen kuvauksen ja tekniset ratkaisut VPN-yhteyden muodostamisesta, ylläpidosta sekä esimerkiksi salauksesta. Keskeisimmät eroavaisuudet ja tekniset ominaisuudet eri protokollien välillä ovat tietoliikenteen salaus, yhteyden autentikointi, datan kuljetuksessa käytettävät tietoliikenneprotokolla ja tietoliikenneportti, turvallisuus, yhteensopivuudet eri käyttöjärjestelmien kanssa sekä laajennettavuus kolmannen osapuolen laitteiden ja sovellusten kanssa. (Mazūra, 2022)

2.2.1 OpenVPN

OpenVPN on James Yonan kehittämä avoimen lähdekoodin VPN-protokolla, jonka ensimmäinen versio julkaistiin vuonna 2001. Protokollan kehittämisestä vastaa OpenVPN projekti jonka viimeisin, 16.maaliskuuta 2022 julkaistu versio on numeroltaan 2.5.6 (OpenVPN, n.d.b). OpenVPN perustuu SSL/TLS-salausprotokollien (Secure Sockets Layer / Transport Layer Security) hyödyntämiseen. OpenVPN on saatavilla Linux-, Mac OS X-, Windows-, Solaris-, OpenBSD- ja FreeBSD-käyttöjärjestelmille. (OpenVPN, n.d.i)

OpenVPN-protokollasta on saatavilla ilmainen Community-versio sekä maksullinen, suuremmille käyttäjämäärille soveltuva Access Server. Palvelun ylläpito on mahdollista myös ulkoistaa ja sitä varten on olemassa maksullinen OpenVPN Cloud -palvelu. (OpenVPN, n.d.a)

OpenVPN sisältää kaksi eri autentikointimenetelmää, jotka ovat staattisen avaimen periaate sekä TLS. Staattisen avaimen menetelmässä VPN-yhteyden muodostaviin laitteisiin, kuten sisäverkon VPN-palvelimeen ja etäkäytettävään päätelaitteeseen, luodaan asennusvaiheessa staattiset avaimet, joiden avulla salaus toteutetaan. Staattinen avain sisältää yhteensä neljä itsenäistä avainta, joista jokaista käytetään eri yhteydessä. Itsenäiset avaimet ovat HMAC-lähetysavain (Hash-based message authentication code), HMAC-vastaanottoavain, salausavain ja salauksen purkuavain. Oletusasetuksilla liikennöitäessä palvelin sekä päätelaite käyttävät liikennöintiin kuitenkin samaa HMAC-avainta sekä samaa salaus- ja purkuavainta. Kaikkia neljää avainta on mahdollista hyödyntää ottamalla käyttöön niin kutsuttu kovennettu toiminnallisuus, tarkentamalla yhteydenmuodostuksen parametreja lisäkomennolla "--secret". (OpenVPN, n.d.c)

TLS-autentikointimenetelmässä muodostetaan kaksisuuntaisella autentikoinnilla varmennettu SSL-istunto, jossa molemmat yhteyden osapuolet, palvelin ja päätelaite, omistavat autentikointia varten itsenäiset sertifikaatit. Tässä autentikointimenetelmässä ei käytetä kaksisuuntaisia avaimia, vaan kaikki avaimet ovat itsenäisiä ja uniikkeja. Varmennetun yhteyden muodostuttua palvelimen ja päätelaitteen välille, luodaan VPN-yhteyden vaatimat muut avaimet hyödyntäen OpenSSL-salauskirjaston RAND_bytes -funktiota. Satunnaisnumeroinnin avulla luotujen avainten turvallinen vaihto

palvelimen ja päätelaitteen välillä suoritetaan olemassa olevan SSL-istunnon avulla. Avainten vaihdon jälkeen VPN-yhteyden molemmat osapuolet omistavat neljä itsenäistä avainta: HMAC-lähetysavain, HMAC-vastaanottoavain, salausavain ja salauksen purkuavain. SSL-istunnon turvallisuutta ylläpidetään uusimalla SSL-istunnon autentikointi aika ajoin, jolloin palvelimen ja päätelaitteen sertifikaatit vaihtuvat uusiksi. SSL-istunnon päivittyessä on myös salausavaimet päivitettävä ja tämän vuoksi OpenVPN-protokolla hyväksyy salausavainten päällekkäisyyden uuden SSL-istunnon muodostamisen ajan. (OpenVPN, n.d.c)

OpenVPN-protokollaa käyttöönottaessa on mahdollista valita avaintenmuodostuksessa käytettävä salakirjoitusmenetelmä. Oletuksena käytettävä salakirjoitusmenetelmä on BlowFish-tekniikka (OpenVPN, n.d.c). Muita mahdollisia salakirjoitusmenetelmiä ovat muun muassa AES, Camellia, ChaCha20, DES, 3DES, Poly1305 ja GOST 28147-89 (Long, 2022).

OpenVPN-protokolla on mahdollista asettaa käyttämään UDP- tai TCP-tietoliikenneprotkollaa. UDP on yhteydetön ja nopeampi kuin yhteydellinen ja virhekorjattu TCP-protokolla. UDP-liikenne on linkitetty tietoliikenneporttiin 1194 ja TCP-liikenne tietoliikenneporttiin 443. Portti 443 on yleisesti käytetty HTTPS-liikennöintiin, joten TCP-protokollalla muodostettu VPN-yhteys naamioituu suojatun verkkoselainliikenteen sekaan ja vähentää liikenteen tunnistamismahdollisuuksia (OpenVPN, n.d.d). OpenVPN tukee IPv4- sekä IPv6-verkko-osoitteita. (OpenVPN, n.d.i)

OpenVPN-yhteyksien ylläpito ja hallinta on mahdollista toteuttaa eri tavoin, riippuen miten yhteys on asennettu. Mikäli kyseessä on palvelin-päätelaite –yhteys, tapahtuu ylläpito pääosin tekstipohjaisen komentorivin avulla. Windows-käyttöjärjestelmälle on luotu myös graafinen käyttöliittymä (OpenVPN, n.d.e). Lisäksi maksullisessa Access server -palvelussa on sisäänrakennettu graafinen käyttöliittymä, jonka avulla yhteyksien ylläpitoa toteutetaan. Asennettaessa OpenVPN esimerkiksi palomuurin tai reitittimen yhteyteen, on yhteyksiä mahdollista hallita kyseisen verkkolaitteen käyttöliittymän avulla. OpenVPN-protokollan hallinta- ja ylläpitorajapintana toimii TCP-yhteys tietoliikenneporttiin 7505. (OpenVPN, n.d.f)

OpenVPN-protokollaa pidetään kyberturvallisena VPN-protokollana ja sen avoin lähdekoodi mahdollistaa protokollan auditoinnin kenen tahansa toimesta. Lähdekoodi sisältää kuitenkin

satoja tuhansia rivejä koodia, joten sen tarkastaminen ja läpikäynti eivät ole yksittäiselle henkilölle tarkoituksenmukaisia toteuttaa (Long, 2022). QuarksLab ja Cryptography Engineering suorittivat virallisen auditoinnin protokollalle joulukuun 2016 ja huhtikuun 2017 välisenä aikana. Auditoinnin yhteydessä protokollasta löytyi haavoittuvuuksia, jotka oli paikattu toukokuussa 2017 julkaistussa versiossa. (OpenVPN, n.d.g)

Avoimen lähdekoodin ansiosta laajennettavuudet ovat hyvällä tasolla. Maksullinen *OpenVPN Access Server* -palvelu mahdollistaa virallisten *OpenVPN Connect* -mobiilisovellusten avulla VPN-yhteyden käytön Android- ja iOS-mobiililaitteissa (OpenVPN, n.d.h). Ilmaiselle *Community*-versiolle on kehitetty Android-mobiililaitteisiin Arne Schwaben toimesta *OpenVPN for Android* -sovellus, jolla on Google Play -kaupassa yli 10 miljoonaa latauskertaa (Google Play, n.d.). Ilmaisen Community-version tuki löytyy myös useista verkkolaitteista, kuten OPNsense-palomuureista (OPNsense, n.d.).

Käyttäjähallintaan tarkoitettujen AD- tai LDAP-palvelimien hyödyntäminen VPN-yhteyden muodostamisessa ja käyttäjän todentamisessa on mahdollista tietyin rajoituksin. Community-versio ei sisällä käyttäjänhallintaa, mutta eri laitevalmistajat, kuten OPNsense, ovat liittäneet omaan hallintasovellukseensa rajapinnan tai toiminnon käyttäjien hallintaa ja tunnistamista varten (OPNsense, n.d.). Maksullinen Access Server -palvelu sitältää AD- ja LDAP-liitännän (OpenVPN, n.d.a).

OpenVPN on toimiva ja turvallinen VPN-protokolla, joka on asennettavissa usealle eri alustalle ja käyttöjärjestelmälle. Lähes kaikista käyttöä ja ylläpitoa helpottavista toiminnoista aiheutuu kustannuksia, joko lisenssien (Access Server tai OpenVPN Cloud -palvelu) tai laitehankintojen (OPNsense-palomuuri) muodossa. Ilmainen Community-versio taipuu kuitenkin myös moneen käyttötarkoitukseen ja on toimiva ratkaisu asiantuntevien henkilöiden käytössä.

2.2.2 Wireguard

Wireguard on avoimen lähdekoodin VPN-protokolla, joka julkaistiin vuonna 2018 ja sen on kehittänyt tietoturva-asiantuntija Jason Donenfeld. Wireguard on saatavilla useille eri

käyttöjärjestelmille kuten Windows, macOS, eri Linux-jakelut, Android sekä iOS. VPN-yhteyden muodostuminen perustuu Wireguard-protokollassa julkisen avaimen periaatteeseen. (Wireguard, n.d.a)

Tietoturva-asiantuntija Tim Mocanin (2020) mukaan, yhteyden muodostaminen julkisen avaimen periaatteella on poikkeuksellinen ratkaisu VPN-alalla. Wireguard-protokolla käyttää 32-bittisiä Curve25519-salattuja julkisia avaimia, joiden avulla yhteydet muodostetaan. Yhteyttä muodostettaessa vastapäät, kuten palvelin ja päätelaite, omistavat tiedon toistensa julkisista avaimista sekä sallituista IP-osoitteista. Näiden lisäksi palvelimelle asetettu virtuaalinen Wireguard-rajapinta, omistaa yksityisen salausavaimen, yksityisen IP-osoitteen sekä tiedon kuunteluun asetetusta UDP-portista. Kyseisestä mallista Wireguard käyttää termiä ”*Cryptokey Routing*”, eli vapaasti suomennettuna salausavainreititystä. Päätelaitteen ottaessa yhteyttä palvelimeen, tunnistautuu päätelaite omalla julkisella avaimella, jonka lisäksi palvelin tarkastaa, että liikenne on lähtöisin sallitusta, virtuaaliselle Wireguard-rajapinnalle asetetusta, yksityisestä IP-osoitteesta. Mikäli julkinen avain tai IP-osoite on virheellinen, ei palvelin vastaanota lähetettyä dataa. Palvelimen lähettäessä päätelaitteelle dataa, tarkastaa palvelin vastapään tiedoista tämän julkisen avaimen ja salaa lähetettävän datan sen avulla. VPN-yhteys perustuu siis vastaanottajan julkisen avaimen hyödyntämiseen, jota tukee lähettäjille sallittujen yksityisten IP-osoitteiden listaus. (Donenfeld, ss. 4-5, 2020a)

Yhteyden muodostamisessa on myös mahdollista käyttää ennalta jaettuja symmetrisia salausavaimia. Julkisia avaimia käyttäessä, yhteyden turvallisuus perustuu Curve25519-salaustekniikkaan ja sen murtamattomuuteen. Tulevaisuudessa kvanttitietokoneiden uskotaan kykenevän murtamaan erilaisia – tänä päivänä murtamattomia – salaustekniikoita, jolloin julkisen avaimen avulla muodostettava yhteys ei olisi todennäköisesti enää turvallinen. Tätä vaihtoehtoista tulevaisuuden näkymää varten Wireguard-protokolla on mahdollista määrittää toimimaan ennalta jaettujen avainten periaatteella. (Donenfeld, ss. 7-8, 2020a)

Kokonaisuudessaan turvallinen tiedonsiirto päätelaitteelta palvelimelle tapahtuu Wireguard-protokollaa hyödyntäen seuraavasti:

1. Selkokielinen datapaketti siirretään päätelaitteeseen luodulle virtuaaliselle Wireguard-rajapinnalle wg0.
2. Vastaanottajan (palvelimen) IP-osoitetta verrataan vastaanottajan julkiseen avaimeen ja vastaavuuden löytyessä datapaketti siirtyy salaukseen. Mikäli vastaavuutta ei löydy, hylätään datapaketti ja siitä ilmoitetaan käyttäjälle.
3. Datapaketti salataan symmetrisella lähetysavaimella sekä suojatun yhteyden tunnistusnumerolla, käyttäen ChaCha20Poly1305-salakirjoitusmenetelmää.
4. Tähän kokonaisuuteen lisätään otsikko ja lähetetään UDP-pakettina julkisen tiedonsiirtoverkon yli vastaanottajan IP-osoitteen ennalta määritettyyn UDP-porttiin.

Päätelaitteen lähettämä salattu datapaketti vastaanotetaan palvelimessa seuraavasti:

1. UDP-paketti saapuu vastaanottajalle ennalta määritettyyn UDP-porttiin.
2. Datapaketista tarkastetaan, että lähettäjän julkinen avain on sallittujen yhteyksien listassa ja suojatun yhteyden tunnistusnumero on oikea. Mikäli tarkastukset ovat onnistuneita, pyritään salattu datapaketti purkamaan käyttäen suojatun yhteyden avulla vastaanotettua symmetrista avainta.
3. Mikäli vastaanotettu paketti on onnistuneesti tunnistettu ja avattu, päivitetään paketin lähettäneen päätelaitteen julkinen IP-osoite Wireguardin reititystauluun.
4. Selkokieliseksi puretusta datapaketista tarkastetaan lähettäjän yksityinen IP-osoite, jonka tulee vastata virtuaaliselle wireguard-rajapinnalle määritettyä lähettäjän IP-osoitetta. Mikäli IP-osoite ei ole sallittujen osoitteiden listassa, datapaketti hylätään.
5. Tarkistuksen läpäissyt selkokielinen datapaketti siirretään virtuaalisesta rajapinnasta palvelimelle ja täten salattu tiedonsiirto on onnistunut päätelaitteelta palvelimelle. (Donenfeld, ss. 5-6, 2020a)

Wireguard-protokollassa kaikki tiedonsiirto tapahtuu UDP-tiedonsiirtoprotokollaa hyödyntäen. Oletusasetuksena käytetään UDP-tietoliikenneporttia 51820, mutta käytettävä portti on yhteyden ylläpitäjän määritettävissä. Käytettävien tiedonsiirtoprotokollan ja salaustekniikan ansiosta Wireguard-protokollaa pidetään erittäin nopeana VPN-tekniikkana. (Mocan, 2020)

Wireguard-yhteyksiä ylläpidetään kuvassa 3 esitetyn salausavainreititystaulun avulla, jossa on määritetty oman virtuaalisen rajapinnan yksityinen ja julkinen salausavain, kuunneltava UDP-portti, vastapään julkinen salausavain, vastapään yksityinen IP-osoite sekä vastapään julkinen IP-osoite. Ylläpito on suunniteltu toteutettavaksi SSH-yhteyden avulla käyttäen komentoriviä. Wireguard mainostaa omissa materiaaleissaan ylläpidon olevan helppoa, eikä sen vuoksi erillistä graafista käyttöliittymää ole tehty. Myöskään suoraa käyttäjähallintaan perustuvaa tunnistautumista tai yhteyttä ei VPN-yhteyksillä ole, koska tunnistautuminen tapahtuu julkisten avainten periaatteella. (Wireguard, n.d.a)

Kuva 3. Wireguard-palvelimen salausavainreititystaulu (Donenfeld, s. 5, 2020a).

Configuration 1a

Interface Public Key	**Interface Private Key**	**Listening UDP Port**
HIgo...8ykw	yAnz..fBmk	41414
Peer Public Key	**Allowed Source IPs**	
xTIB...p8Dg	10.192.122.3/32, 10.192.124.0/24	
TrMv...WXX0	10.192.122.4/32, 192.168.0.0/16	
gN65..z6EA	10.10.10.230/32	

Wireguard-protokollan avoin lähdekoodi mahdollistaa kolmansien osapuolien kehittää omia sovelluksia ja toimintoja protokollan ympärille. Näin on tehty esimerkiksi käyttäjähallinnan ja yhteyksien ylläpidon osalta. Christoph Haasin tekemä Wireguard Portal -niminen työkalu on avoimen lähdekoodin projekti, joka muun muassa mahdollistaa käyttäjätunnistuksen LDAP-protokollaa (Lightweight Directory Access Protocol) käyttäen. Wireguard Portal sisältää myös graafisen selainpohjaisen käyttöliittymän, joka on mahdollisesti joillekin ylläpitäjille mieluisampi vaihtoehto ylläpidon suorittamiseen, kuin komentorivi. Wireguard Portalin ensimmäinen versio julkaistiin marraskuussa 2020 ja tämän hetken uusin versio 1.0.14 on julkaistu maaliskuussa 2022. (Haas, n.d.)

Wireguard on suunniteltu kevyeksi ja turvalliseksi VPN-protokollaksi. Wireguardin lähdekoodi koostuu hieman yli 4 000 rivistä koodia, mikä on VPN-protokollalle merkittävän pieni määrä. Lähdekoodin avoimuus ja keveys mahdollistavat protokollaan tutustumisen ja auditoinnin kaikille halukkaille. 4 000 riviä koodia on määrä, joka yksittäisen ihmisen on mahdollista tutkia säädyllisessä ajassa. (Wireguard, n.d.a)

Wireguard-protokollassa on myös sisäisesti rakennettuja turvallisuustoimintoja. Yksi tällainen on palvelunestohyökkäyksiä vastaan kehitetty evästeen lisääminen yhteyden kättelyvaiheeseen. Mikäli aktiivisena olevaan päätelaite-palvelin -yhteyteen pyrkii jokin toinen taho muodostamaan yhteyttä samanaikaisesti, ei yhteyden avauksen muodostuvaa kättelyä suoriteta onnistuneesti loppuun. Tällöin ulkopuolelta tulevaan kättelyn avaukseen vastataan evästeellä, jonka johdosta evästeen saanut taho ei kykene kyllästämään virheellisillä kättelypyynnöillä päätelaitetta tai palvelinta. (Donenfeld, ss. 8-10, 2020a)

Wireguard-protokolla on laajennettavuudeltaan hyvällä tasolla. Wireguard on niin sanotusti konttiyhteensopiva, eli se on mahdollista ottaa käyttöön Docker-konttisovellusyksikössä. Wireguard-tuki on olemassa myös fyysisissä verkkolaitteissa, kuten OPNsensen valmistamissa palomuureissa (OPNsense, n.d.). Kaikkein merkittävin toteamus Wireguard-protokollaa ja sen laajennettavuutta kohtaan oli Linux 5.6 -käyttöjärjestelmän päivitys, jonka yhteydessä Wireguard hyväksyttiin sisäänrakennetuksi osaksi Linux-ydintä (Donenfeld, 2020b). Mobiililaitteiden osalta Wireguard on käytettävissä Android- ja iOS-laitteissa. (Wireguard, n.d.a)

3 Tilaaja

Tämän opinnäytetyön tilaaja on viestintäalan pienyritys, joka haluaa esimerkkiratkaisun heille sopivasta avoimen lähdekoodin VPN-palvelusta. Tilaajan oma henkilöstö hallitsee ja ylläpitää heidän IT-toimintojaan, joten myös tuleva VPN-ratkaisu jää tilaajan itsensä ylläpidettäväksi. Tilaajan toiminnan sisältö ja sen erityispiirteet, sekä verkkoinfrastruktuuri määrittävät vaatimukset tulevalle VPN-ratkaisulle. Tässä luvussa vastataan tutkimuskysymykseen: *Millaisia vaatimuksia tilaajan verkkoinfrastruktuuri ja toiveet asettavat tulevalle VPN-ratkaisulle?*

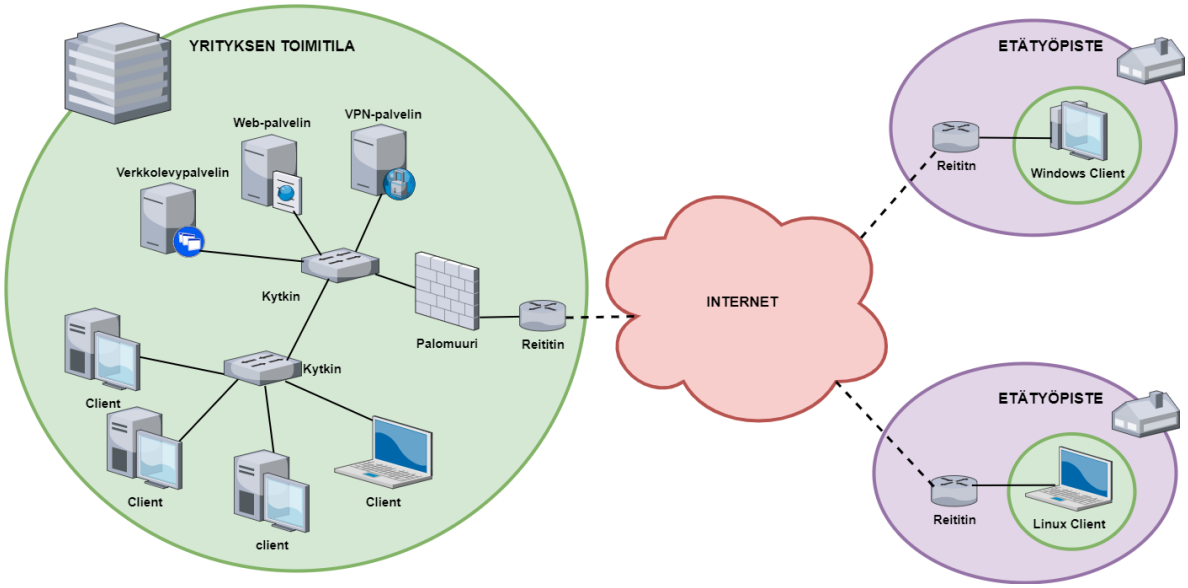
3.1 Tilaajan verkko

Tilaajan verkkoinfrastruktuuri koostuu tällä hetkellä erilaisista työntekijöiden päätelaitteista, palvelimista sekä verkon aktiivilaitteista. Työntekijöiden päätelaitteet ovat pääosin kannettavia tietokoneita, joissa käyttöjärjestelminä toimii Microsoft Windows 10 ja -11, sekä

erilaisia Linux-jakeluita. Verkossa toimivista palvelimista tämän työn kannalta ainoat merkitykselliset ovat verkkolevy- ja web-palvelin, joilla ylläpidetään tilaajan sisäisiä työkaluja sekä selainpohjaisia palveluja. Muut palvelimet eivät ole merkityksellisiä VPN-ratkaisua valittaessa tai asentaessa, joten siitä syystä niitä ei esitellä. Verkon muita aktiivilaitteita ovat kytkimet, palomuuri sekä reititin.

Tilaajan sisäverkko on rakennettu kytkimien avulla niin sanotusti kaksiosaiseksi, jossa työntekijöiden päätelaitteet on erotettu verkon muista laitteista kytkimien avulla omaksi segmentikseen. Verkon muut laitteet sijaitsevat fyysisesti erillisessä tilassa, jolloin verkon segmentointi päätelaitteet – muut laitteet, on erittäin perusteltua. Tilaajan verkkoinfrastruktuuria yleisellä tasolla kuvaava verkkokuva, sisältäen opinnäytetyön tavoiteltavan loppuasetelman – eli VPN-palvelimen sekä etäkäyttömahdollisuuden – on esitetty kuvassa 4.

Kuva 4. Tilaajan verkkoinfrastruktuuri ja tavoiteltu loppuasetelma.



3.2 Tilaajan vaatimukset

Tilaaja tuottaa audiovisuaalisia ja graafisia julkaisuja, joiden työstäminen ja valmistelu tapahtuvat pääosin työntekijöiden päätelaitteilla. Merkittävänä osana työskentelyä ovat ostettujen ohjelmistojen lisäksi tilaajan itse kehittämät selainpohjaiset sovellukset ja

palvelut, joita ylläpidetään web-palvelimella. Tilaajaa sitoo tiukat vaitiolosopimukset julkaisemattomissa asiakasprojekteissa ja tästä syystä he haluavat pitää kaiken materiaalin sisäverkkonsa verkkolevypalvelimilla.

Tällainen tiukka toimintakulttuuri sekä itse ylläpidettyjen palveluiden hyödyntäminen, vaativat verkolta ja tiedonsiirrolta mahdollisimman suurta kapasiteettia ja nopeutta. Tästä syystä tilaaja on määritellyt tulevan VPN-ratkaisun ensimmäiseksi prioriteetiksi toiminnallisuuden osalta mahdollisimman suuren tiedonsiirtonopeuden. Tätä vaatimusta tukee myös tilaajan suosima tapa työskennellä pienissä tiimeissä, jolloin kommunikaatio sekä palaverit toteutettaisiin tulevaisuudessa VPN-ratkaisun mahdollistamana virtuaalisesti videoneuvotteluiden avulla.

Toinen vaatimus koskee ratkaisun kompleksisuutta ja sen minimoimista. Tilaajan edustaja kuvailee IT-henkilöstöään perusteelliseksi ja äärimmäisen kiinnostuneeksi tietotekniikasta, jonka vuoksi he ylläpitävät ja kehittävät omia palvelujaan. Tämän vuoksi tilaajan toiveena on VPN-ratkaisu, joka olisi rakennettu mahdollisimman yksinkertaisesti, mutta turvallisesti ja nykyaikaisesti. VPN-ratkaisun ymmärrettävyyttä voi mitata eri tavoin, mutta tilaajan toiveena on ymmärrettävä salaustekniikka, yhteyden muodostus sekä valitun protokollan lähdekoodin luettavuus.

Kolmas vaatimus on kohtuullinen ylläpitokuorma ja valvonta. Ylläpidolla tarkoitetaan uusien päätelaitteiden käyttöönottoa ja vanhojen poistamista sekä ylläpidollisten päivitysten asentamista. Valvonnan osalta tilaaja toivoo mahdollisimman yksinkertaista tapaa seurata aktiviisia VPN-yhteyksiä ja mahdollisuutta eristää tai poistaa yhteyden voimassaolo poikkeavissa tapauksissa, kuten laitteen katoamisen tai anastamisen yhteydessä.

Neljäs vaatimus ratkaisulle on kustannusten minimointi. Mahdollisia kustannuksia tilaajalle voisi tulla uusien laitteiden hankinnoista tai maksullisten käyttösovellusten lisensoimisesta. Tämän vuoksi ratkaisun tulisi sisältää vain avoimen lähdekoodin protokolla sekä mahdollisia avoimen lähdekoodin sovelluksia, eikä esimerkiksi lisensoitua ylläpitosovellusta. Laitehankintoja voi mahdollisesti syntyä uuden palvelimen hankinnasta, johon VPN-palvelin

asennettaisiin. On kuitenkin mahdollista, että tilaaja hyödyntää lopullisessa ratkaisussaan jo olemassa olevia laitteita, jolloin hankintoja ei olisi tarpeen tehdä.

Tilaajan vaatimukset tämän työn toiminnalliseen osuuteen ja sen toimivuuden todentamiseen ovat yksinkertaiset, jotka vastaavat tilaajan kannalta riittävällä tasolla ratkaisun todellistä käyttöä ja ylläpitoa. Toiminnalliset vaatimukset ovat:

1. VPN-ratkaisun tulee toimia Windows- ja Linux-käyttöjärjestelmien päätelaitteilla sekä Linux-palvelimella.
2. VPN-yhteyden muodostuttua päätelaite kykenee käyttämään selainpohjaisia sovelluksia, joita ylläpidetään sisäverkon palvelimilla.
3. VPN-yhteyden muodostuttua päätelaite kykenee käyttämään verkkolevyjä ja siirtämään kaksisuuntaisesti materiaalia päätelaitteen ja verkkolevyn välillä.
4. Ylläpitohenkilöstö kykenee näkemään listauksen aktiivisista VPN-yhteyksistä.
5. Palomuuriin asetettavat säännöt mahdollistavat VPN-yhteydellä ulkoverkosta liikennöinnin sisäverkon palveluihin, mutta mikään muu ulkoverkosta tuleva liikenne ei pääse sisäverkon palveluihin.

4 Vertailu

Tässä luvussa suoritetaan vertailu, aiemmin esitettyjen VPN-protokollien välillä. Vertailussa hyödynnetään päätöksentekomatriisia (Pherson & Heuer, ss. 329-332, 2021), jonka kriteerit pohjautuvat tilaajan – luvussa 3 – esittämiin vaatimuksiin ja toiminnan erityispiirteisiin. Esitettyjen vaatimusten ja toiminnan erityispiirteiden perusteella kirjoittaja on muodostanut omaan asiantuntijuuteen peilaten painotukset eri kriteereille. Tässä luvussa vastataan tutkimuskysymykseen: *Kumpi avoimen lähdekoodin VPN-protokolla – OpenVPN vai Wireguard – on laadullisesti parempi valinta tilaajan tarpeisiin?*

4.1 Analysoitavat ominaisuudet ja painotukset

Painotettu päätöksentekomatriisii toimii yleensä parhaiten silloin, kun arvioitavia kriteerejä on neljästä kuuteen kappaletta (Pherson & Heuer, s. 331, 2021). Tilaajan esittämiä kriteerejä

oli neljä, joista kirjoittaja muodosti viisi arvioitavaa kriteeriä. Muodostettavat kriteerit ovat nopeus, turvallisuus, ylläpito & valvonta, kustannukset sekä laajennukset. Turvallisuus käsittää muun muassa lähdekoodin ymmärrettävyyden ja protokollan yleisen turvallisuuden, kuten auditoinnit. Ylläpito ja valvonta kuvaavat kuinka helposti VPN-yhteyksiä on mahdollista tarkastella ja tarvittaessa poistaa käytöstä. Kustannusten osalta analyysissa on huomioitu ainoastaa ilmaisten toiminnallisuuksien hyödyntämistä. Viides analysoitava kriteeri on laajennukset, joka kuvaa protokollan käytettävyyttä esimerkiksi kolmannen osapuolen laitteissa. Laajennukset on kirjoittajan lisäämä kriteeri, sillä ne vaikuttavat välillisesti kaikkiin muihin analysoitaviin kriteereihin sekä suorasti protokollan käytettävyyteen ja on tästä syystä huomioon otettava ominaisuus.

Jokaiselle arvioitavalle kriteerille annetaan oma prosentuaalinen painoarvonsa siten, että kaikkien kriteerien painoarvot yhteenlaskettuna muodostavat 100 %. Mikäli arvioitavat kriteerit olisivat yhtä tärkeitä ja arvokkaita keskenään, tulisi jokaiselle kriteerille tässä analyysissä painotukseksi 20 %. Tilaaja kuitenkin esitti tärkeimmäksi ominaisuudeksi nopeuden, joten tästä syystä nopeuden painotus on muita korkeampi eli 30 %. Muille kriteereille ei tilaaja esittänyt priorisointia tai painotusta. Käytettäessä avoimen lähdekoodin protkollia, ei tilaajalle aiheudu juurikaan kustannuksia, joten kustannusten painotus pudotettiin vähäisimmäksi – arvoon 10 %. Loput kolme kriteeriä painotettiin keskenään vertaisiksi, antaen jokaiselle kriteerille painoarvo 20 %. (Pherson & Heuer, ss. 329-332, 2021)

Arviointiasteikko kriteereittäin on 0–5 siten, että asteikosta on käytössä arvot 0, 1, 3 ja 5. Tiivistetyt kuvaukset kyseisille arvoille ovat: 0 – ei toteudu, 1 – toteutuu rajoituksin, 3 – toteutuu ja 5 – toteutuu erinomaisesti.

4.2 Matriisianalyysi

Tiedonsiirtonopeutta mitattaessa, esiin nousevat mitattavina ominaisuuksina itse siirtonopeus sekä viive (Mills, 2020). Vertailtavien VPN-protokollien nopeuksia ovat tutkineet mm. Long (2020), Wireguard (n.d.c) sekä Pyhäluoto opinnäytetyössään *verkkosalaustekniikoiden vertailu* (2021). Kaikissa näissä testeissä Wireguard on ollut vertailluista protokollista siirtonopeudeltaan ja viiveeltään nopein. OpenVPN on sijoittunut

vastaavissa testeissä selvästi heikoimmaksi protokollaksi ja esimerkiksi IPsec-protokolla eri salakirjoitusmenetelmillä on todettu nopeammaksi kuin OpenVPN. Edellämainituin perustein Wireguard saa arvon 5 (erinomainen) ja OpenVPN 1 (toteutuu rajoituksin).

Turvallisuuden osalta molemmat protokollat selviytyvät puhtain paperein. OpenVPN sisälsi pieniä haavoittuvuuksia, jotka havaittiin ulkopuolisen auditoinnin yhteydessä 2016-2017, mutta paikattiin nopeasti löytymisen jälkeen 2017 (OpenVPN, n.d.g). Selkein ero protokollien välillä on tilaajan arvostama lähdekoodin luettavuus ja ymmärrettävyys. Wireguard sisältää vain noin sadasosan verran koodirivejä OpenVPN:ään verrattuna (Long, 2020). Täten turvallisuudesta pisteitä Wireguard 5 ja OpenVPN 3.

Ylläpito ja valvonta toteutuu molemmissa protokollissa hyvin. Olemassa olevien yhteyksien hallinta tapahtuu natiivisti komentorivin avulla. Aktiiviset yhteydet on mahdollista listata ylläpitäjän näkyville ja tarpeettomien yhteyksien poistaminen on mahdollista. Lisäksi molemmat protokollat ovat liitettävissä ylläpidollisesti, esimerksiksi avoimen lähdekoodin analyysi- ja monitorointipalveluun nimeltä Grafana (Grafana, n.d.a; Grafana, n.d.b). Grafana mahdollistaa graafisen yhteyksien valvonnan ja mikäli Grafana on käytössä muihin verkonvalvonnan toimiin, on VPN-yhteyksien valvonta mahdollista liittää samalle Grafana-alustalle. Ylläpidosta ja valvonnasta täten molemmille arvo 5.

Analyysi on toteutettu oletuksella, että protokollista käytetään ainoastaan ilmaisia avoimen lähdekoodin versioita. Maksulliset ominaisuudet saattaisivat vaikuttaa muihin tämän analyysin arvioitaviin kohtiin, joten tästä syystä niitä ei huomioida kustannusten yhteydessä; esimerkiksi OpenVPN:än olisi mahdollista ostaa graafinen käyttöliittymä, joka vaikuttaisi mahdollisesti tukevasti myös *ylläpito ja valvonta* -kriteerin arvioihin. Ilmaisten versioiden johdosta kumpikaan protokolla ei aiheuta kustannuksia, joten molemmat saavat arvon 5.

Laajennukset ovat molemmissa protokollissa hyvällä tasolla. Kuten luvussa 2 todettiin, protokollat ovat yhteensopivia eri käyttöjärjestelmien kanssa ja niihin löytyy kolmansien osapuolien kehittämiä lisäosia. OpenVPN on kuitenkin ollut vuosia markkinoiden johtava VPN-protokolla, jolle on kehitetty huomattava määrä yhteensopivia laitteita kuten reitittimiä

ja palomuureja (OPNsense, n.d.; Long, 2022). Laajennusten osalta pisteitä Wireguard 3 ja OpenVPN 5.

Arvioiduista ominaisuuksista, painotuksista ja arvosanoista lasketaan ominaisuuksittain painotetut arvosanat. Nämä painotetut arvosanat lasketaan tämän jälkeen protokollittain yhteen, jolloin niistä muodostuu kokonaisarvosana. Tämän analyysin maksimiarvosana on 500. Painotettu matriisianalyysi on esitetty taulukossa 1. (Pherson & Heuer, ss. 329-332, 2021)

Taulukko 1. Painotettu päätöksentekomatriisi.

Ominaisuus	**Painotus**	**OpenVPN**	**Wireguard**
Nopeus	**30 %**	1 x 30 = 30	5 x 30 = 150
Turvallisuus	**20 %**	3 x 20 = 60	5 x 20 = 100
Ylläpito & valvonta	**20 %**	5 x 20 = 100	5 x 20 = 100
Kustannukset	**10 %**	5 x 10 = 50	5 x 10 = 50
Laajennukset	**20 %**	5 x 20 = 100	3 x 20 = 60
Yhteensä	**100 %**	**340**	**460**

Vertailun tuloksena voidaan todeta, että eroavaisuuksia protokollien välillä on nopeudessa, turvallisuudessa sekä laajennuksissa, joista nopeus ja turvallisuus kääntyivät Wireguardin eduksi ja laajennukset OpenVPN:n puolelle. Ylläpidon ja valvonnan osalta tai kustannuksista ei merkittäviä eroja protokollien välille syntynyt. Painotetun päätöksentekomatriisin ja laadullisen analyysin lopputuloksena voidaan todeta, että Wireguard-protokolla on näistä kahdesta vaihtoehdosta tilaajalle paremmin soveltuva VPN-protokolla.

5 Toteutus

Tässä luvussa suoritetaan opinnäytetyön toiminnallinen osuus, jossa toteutetaan esimerkin omaisesti, valitun VPN-protokollan asennus ja käyttöönotto. Asennus alkaa koeympäristön sekä testitavoitteiden määrittelyllä ja päättyy asennusten jälkeiseen pohdintaan. Tässä

luvussa vastataan tutkimuskysymykseen: *Miten tilaajalle sopiva VPN-ratkaisu otetaan käyttöön sisäverkon palvelimella ja etätyöskentelyyn tarkoitetuilla päätelaitteilla?*

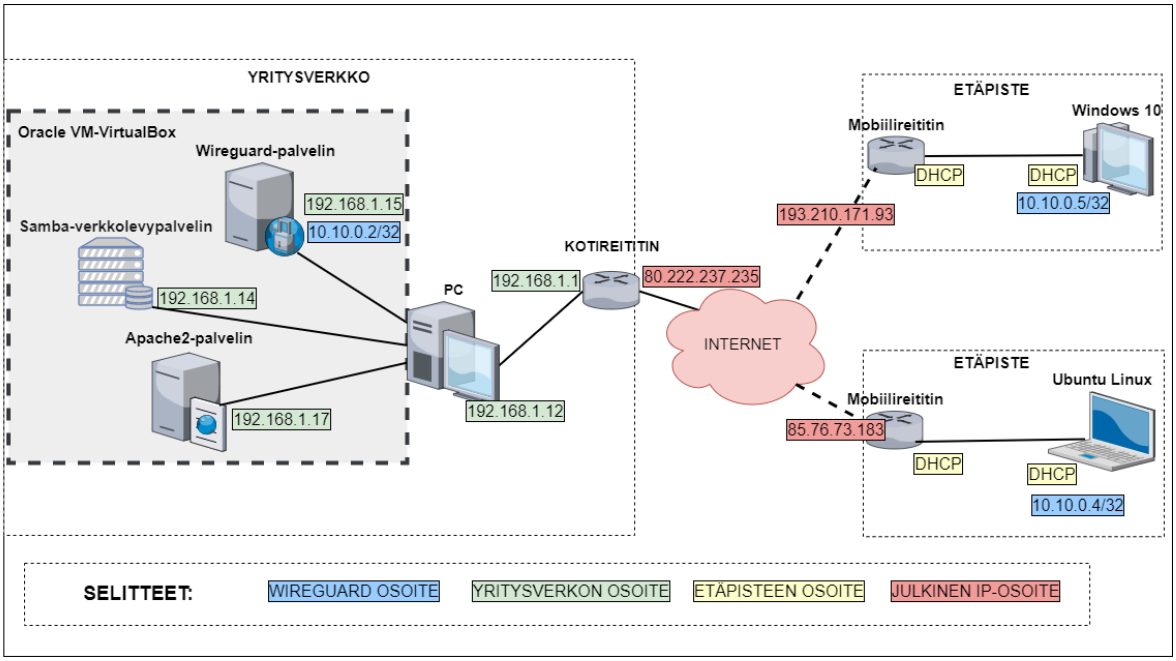
5.1 Koeympäristö ja testitavoitteet

Koeympäristön suunnittelussa alkuperäinen tavoite oli, että asennukset olisi kyetty suorittamaan oppimiskokemuksen kasvattamiseksi autenttisessa ympäristössä, oikeilla fyysisillä laitteilla. Tilaajan kanssa käydyn keskustelun pohjalta päädyttiin kuitenkin siihen, että koeympäristö rakennetaan virtuaalisesti, koska tilaaja ei kyennyt tarjoamaan koeympäristöä kirjoittajan käyttöön. Virtuaalisina koeympäristöinä vaihtoehdoiksi nousi eri palveluntarjoajien pilvipalvelut – kuten Microsoft Azure ja Google Cloud (Chai & Bigelow, 2021) – sekä paikallisesti ylläpidettävä virtuaaliympäristö Oracle Virtualbox (VirtualBox, n.d.).

Pilvipalveluihin on mahdollista luoda normaalia kuluttajatiliä edullisempi opiskelijatili, jolloin koeympäristön rakentaminen ei olisi aiheuttanut suuria kustannuksia kirjoittajalle. Pilvipalvelut olisivat lisäksi nykyaikainen ja joustava ratkaisu koeympäristöksi. Kirjoittaja on kuitenkin kiinnostunut perehtymään paikalliseen virtualisointiin ja avoimen lähdekoodin verkkolaitteisiin, joilla koeympäristö on mahdollista rakentaa. Tästä syystä koeympäristöksi valikoitui avoimen lähdekoodin Oracle VirtualBox. Koeympäristö ja siinä käytetyt IP-osoitteet on esitetty kuvassa 5 . Koeympäristöön perustettavat laitteet ovat Apache2 -web-palvelin, Samba-verkkolevypalvelin sekä Wireguard-palvelin. Kaikki kolme palvelinta asennetaan 64-bittisten Ubuntu-käyttöjärjestelmien päälle.

Oracle VirtualBox -virtualisointiympäristö ja sen virtualisoidut palvelut asennetaan kirjoittajan Windows 10 -tietokoneelle. Etäkäyttöön tarkoitettuina työasemina toimivat kirjoittajan omistamat Windows 10- ja Linux-käyttöjärjestelmän kannettavat tietokoneet. Toimivat internetyhteydet muodostetaan tässä toteutuksessa siten, että virtualisoitu palvelinympäristö hyödyntää kirjoittajan kotiverkkoa sekä kotiverkon reititintä ja kannettavat tietokoneet käyttävät erillisiä mobiilitukiasemia. Tällöin jokainen laite toimii erillisessä verkossa, omalla internetyhteydellään.

Kuva 5. Koeympäristön verkkokuva.



Asennusten onnistuminen ja palvelun toimivuus todennetaan käyttöönoton jälkeisillä testeillä. Testit pohjautuvat luvussa 3 esitettyihin tilaajan toiminnallisen osuuden vaatimuksiin, joista on luotu yksinkertaistettu testiohjelma. Testiohjelma on seuraava:

1. Yhteyden muodostuminen
    a. Linux-päätelaite muodostaa VPN-yhteyden Linux-palvelimeen
    b. Windows-päätelaite muodostaa VPN-yhteyden Linux-palvelimeen
2. Selainpohjaisten sovellusten käyttö
    a. Linux-päätelaite pääsee Apache2-palvelimella ylläpidetylle verkkosivulle
    b. Windows-päätelaite pääsee Apache2-palvelimella ylläpidetylle verkkosivulle
3. Verkkolevyjen käyttö
    a. Linux-päätelaite toteuttaa kaksisuuntaista tiedostojen siirtoa Ubuntu-palvelimen verkkolevyltä
    b. Windows-päätelaite toteuttaa kaksisuuntaista tiedostojen siirtoa Ubuntu-palvelimen verkkolevyltä
4. Ylläpito ja valvonta
    a. VPN-palvelimelta näkee voimassaolevat Wireguard-yhteydet
5. Palomuurin toiminta

a. Reitittimen palomuurisäännöt estävät virtuaaliympäristöön tulevan liikenteen poislukien Wireguard-liikenteen.

5.2 Asennukset ja VPN:n konfigurointi

Onnistuneiden asennusten perusta on toimivat ja ajantasaiset käyttöjärjestelmät. Ennen asennusten aloittamista tulee käyttöjärjestelmien päivitykset tarkastaa ja mahdolliset päivityspaketit asentaa.

5.2.1 Wireguard-palvelin

Wireguard-palvelimen asennus aloitetaan lataamalla ja asentamalla Wireguard-protokollan virallinen ohjelmistopaketti. Asennuksen yhteydesssä ohjelmistolle luodaan oma hakemisto polkuun */etc/wireguard*. Kyseiseen hakemistoon tulee luoda VPN-yhteyksissä käytettävät julkinen ja yksityinen salausavain. On suositeltavaa rajoittaa salausavainten luku- ja kirjoitusoikeuksia, koska ylläpitäjä on ainoa jonka tarvitsee kyseisiä tiedostoja käyttää.

Asennuksen ja salausavainten luonnin jälkeen tulee Wireguard-palvelimen asetukset määritellä tiedostoon */etc/wireguard/wg0.conf.* Koeympäristöön asennetun Wireguard-palvelimen konfiguraatiotiedoston määritykset on esitetty kuvassa 6, ja asetettujen määritysten merkitykset on avattu liitteessä 1.

Kuva 6. VPN-palvelimen konfiguraatiotiedosto wg0.conf.

Konfiguraatiotiedoston luonnin jälkeen, tulee palvelimelta ottaa käyttöön pakettien välityksestä vastaava *net.ipv4.ip_forward* -ominaisuus. Tavoiteltava tilanne on, että VPN-palvelimen käynnistymisen yhteydessä, myös VPN-palvelu käynnistyy automaattisesti. Oletusasetuksilla näin ei ole, vaan käynnistymisen yhteydessä tapahtuva palvelu tulee erikseen määritellä aktiiviseksi asennuksen yhteydessä.

5.2.2 Remote access -client Linux

Wireguard-palvelun asennus etäkäyttöön tarkoitetulla työasemalla on samankaltainen prosessi, kuin wireguard-palvelimen asennus. Eroavaisuuksia on ainoastaan konfiguraatiotiedoston sisällössä sekä pakettien välityksestä vastaavan asetuksen jättämistä pois käytöstä.

Wireguard-palvelun käyttöönotto tapahtuu lataamalla ja asentamalla Wireguard-protokollan virallinen ohjelmistopaketti. Asennuksen yhteydessä ohjelmistolle luodaan oma hakemisto polkuun */etc/wireguard.* Kyseiseen hakemistoon tulee luoda VPN-yhteydessä käytettävät julkinen ja yksityinen salausavain. Salausavainten jälkeen VPN-yhteyden asetukset tulee määritellä tiedostoon */etc/wireguard/wg0.conf.* Koeympäristöön asennetun Linux-työaseman Wireguard-ohjelmiston konfiguraatiotiedosto on esitetty kuvassa 7, ja siinä käytettyjen asetusten selitykset on esitetty liitteessä 2.

Kuva 7. Linux-työaseman konfiguraatiotiedosto wg0.conf.

```
[Interface]
Address = 10.10.0.5/32
SaveConfig = true
ListenPort = 40922
FwMark = 0xca6c
PrivateKey = (

[Peer]
PublicKey = bEbjYt4zE/4ECt2WOy7yxfY9YqU3DywbIGirIbmEzyo=
AllowedIPs = 0.0.0.0/0
Endpoint = 80.222.237.235:49222
PersistentKeepalive = 25
```

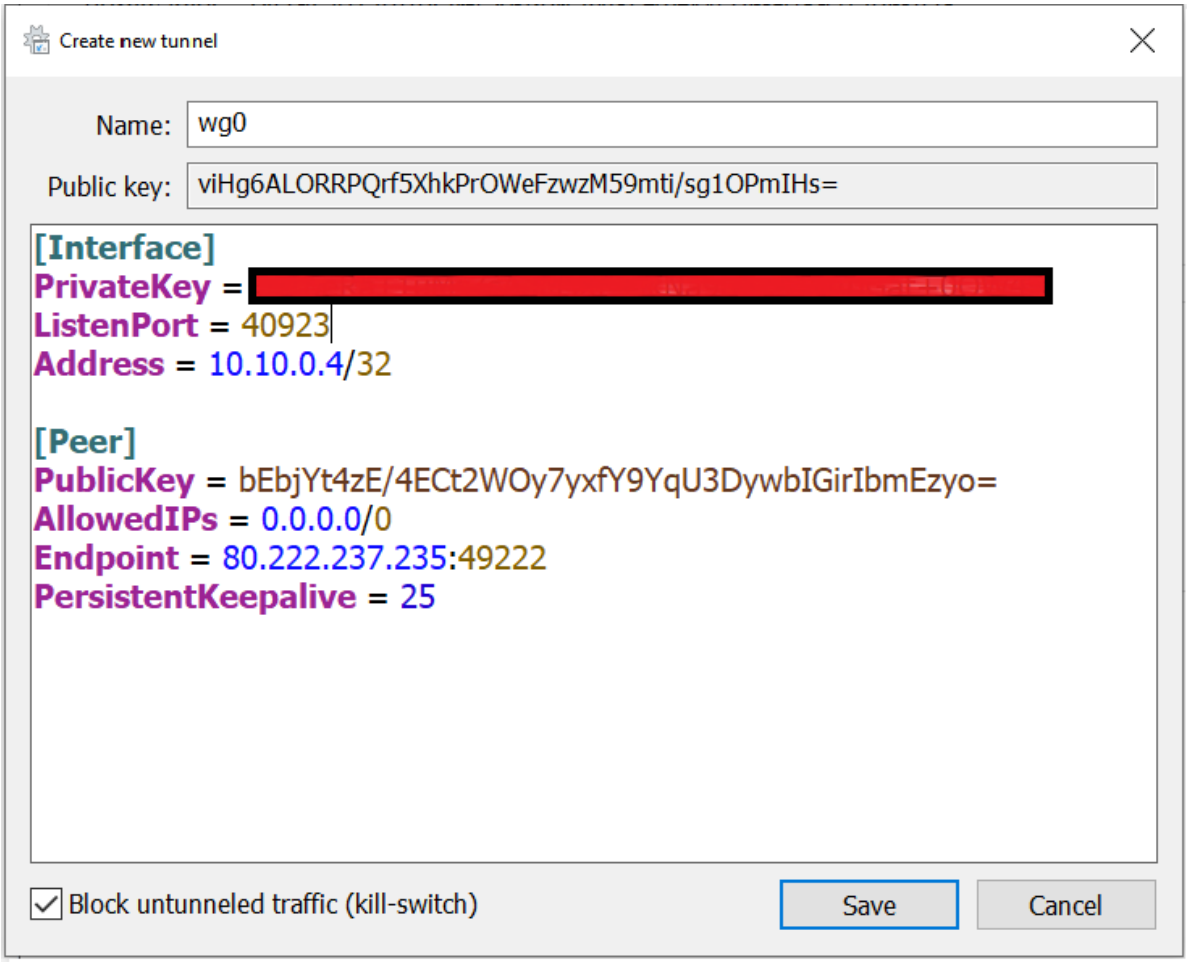
Asetusten määrittämisen jälkeen VPN-yhteys on käyttöönotettavissa. Mikäli VPN-yhteyden tulee käynnistyä automaattisesti työaseman käynnistyksen yhteydessä, tulee se määritellä erikseen hyväksytyksi prosessiksi käynnistymisen yhteyteen.

5.2.3 Remote access -client Windows

Windows-käyttöjärjestelmälle on luotu oma asennuspaketti, joka on ladattavissa Wireguard:n viralliselta lataussivulta (Wireguard, n.d.b). Asennuspaketin lataamisen jälkeen suoritetaan asentaminen Windows:n asennustyökalua hyödyntäen.

Wireguard-ohjelman käyttämät asetukset voi määritellä manuaalisesti tai vaihtoehtoisesti asetukset on mahdollista asettaa ulkoisen konfiguraatiotiedoston mukaisiksi. Asetusten manuaalinen määrittäminen Windows-sovelluksessa, on helpompaa kuin Linux-työasemalla, sillä sovellus luo käytettävät salausavaimet automaattisesti konfiguraatiotiedoston avaamisen yhteydessä. Koeympäristöön perustetun Windows-työaseman konfiguraatiotiedosto on esitetty kuvassa 8 ja siinä käytettyjen asetusten selitykset on esitetty liitteessä 3.

Kuva 8. Window-työaseman VPN-asetukset tunnelille wg0.



5.2.4 Verkon muut laitteet

Koeympäristöön perustettiin Oracle VirtualBox:n sisään virtuaalisen VPN-palvelimen lisäksi kaksi virtuaalista Ubuntu-palvelinta, joihin toiseen asennettiin Apache2 -web-palvelin ja toiseen Samba-verkkolevypalvelin. Apache2 -web-palvelimen etusivu muokattiin sisältämään itse tehty yksinkertainen html-verkkosivu, jossa lukee ”Tämä on sisäverkon web-palvelin”. Samba-verkkolevypalvelin asetettiin jakamaan kansiota */share/vpn_files.*

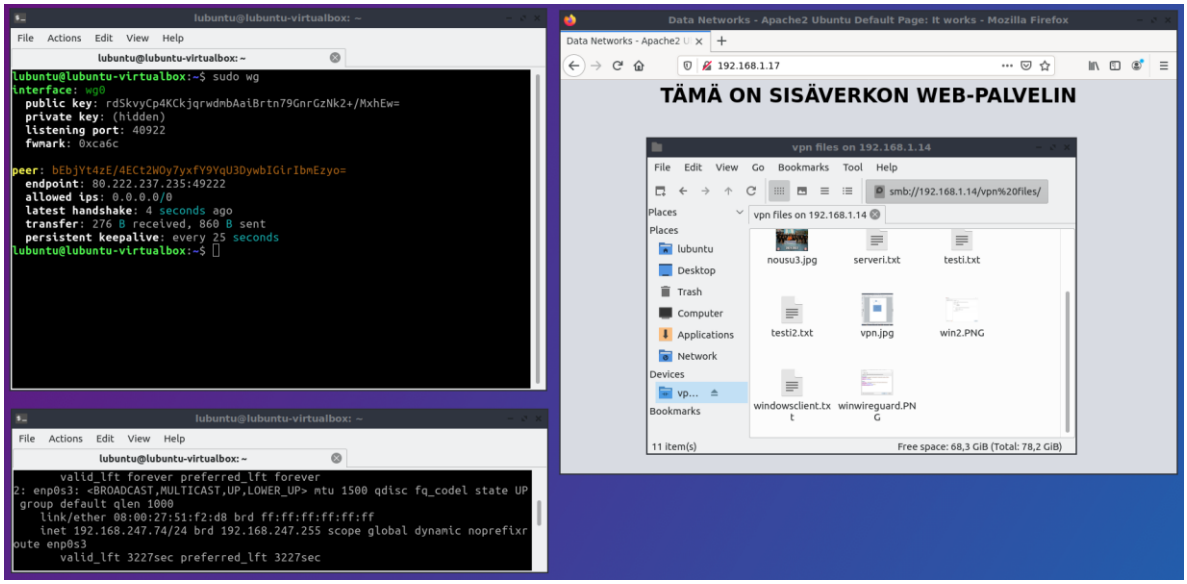
Koeympäristön Oracle Virtualbox ja sen sisään virtualisoidut palvelimet ovat yhteydessä internetiin kirjoittajan kotiverkon reitittimen välityksellä. Kotireitittimessä on sisäänrakennettuja turvallisuusominaisuuksia, joista yksi on *Access Control* ja sen sisältämä *Port forwarding* -toiminnallisuus. Reitittimelle tulee kertoa Wireguard-protokollan

käyttämästä UDP-liikenteestä ja määritellä se edelleen lähetettäväksi sisäverkon VPN-palvelimelle. Koeympäristön kotireitittimeen asetettiin ulkoverkosta saapuva UDP-tietoliikenne portista 49220 sallituksi, kun sisäverkon kohdeosoite on VPN-palvelimen enp0s8-verkkokortille liitetty osoite 192.168.1.15.

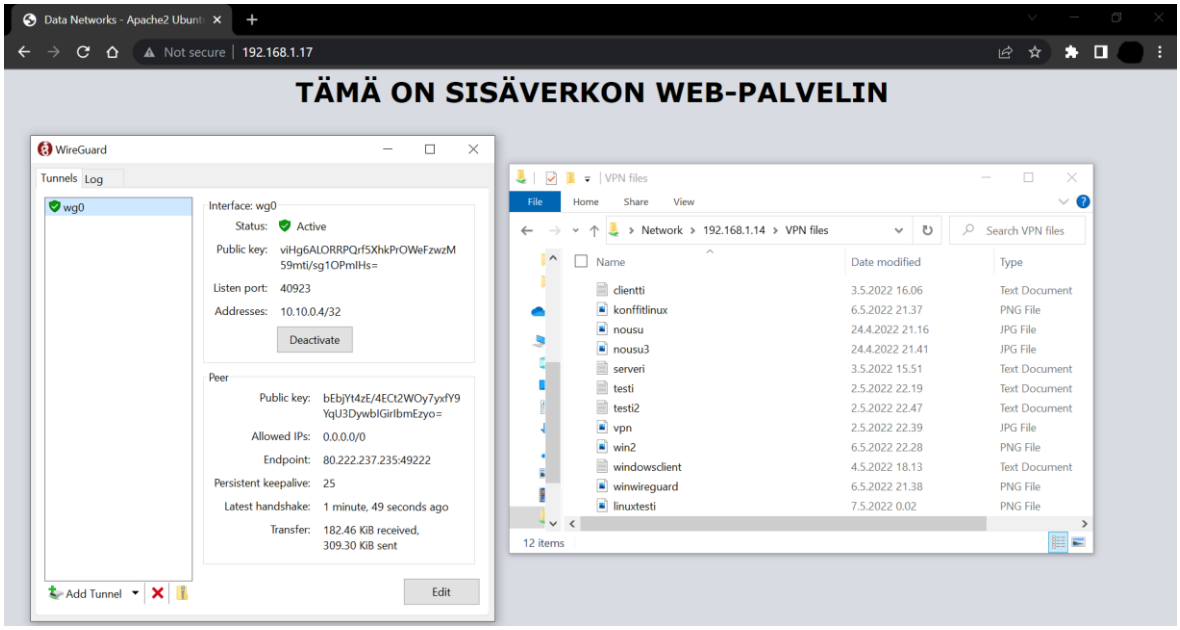
5.3 Asennusten todentaminen

Asennusten ja VPN-palvelun käyttöönoton onnistuminen todennetaan luvussa 5.1 esitetyn testiohjelman mukaisesti. Testiohjelman kohdat 1–3 suoritettiin onnistuneesti Linux- ja Windows-työasemilla, eli molemmat työasemat muodostivat onnistuneen yhteyden VPN-palvelimeen, jonka jälkeen työasemat pystyivät käyttämään Apache2-palvelinta ja suorittamaan kaksisuuntaista tiedonsiirtoa Samba-verkkolevypalvelimen kanssa. Onnistuneet Linux-työaseman testit on esitetty kuvassa 9 ja onnistuneet Windows-työaseman testit on esitetty kuvassa 10.

Kuva 9. Linux-työaseman suorittamat testit 1–3.

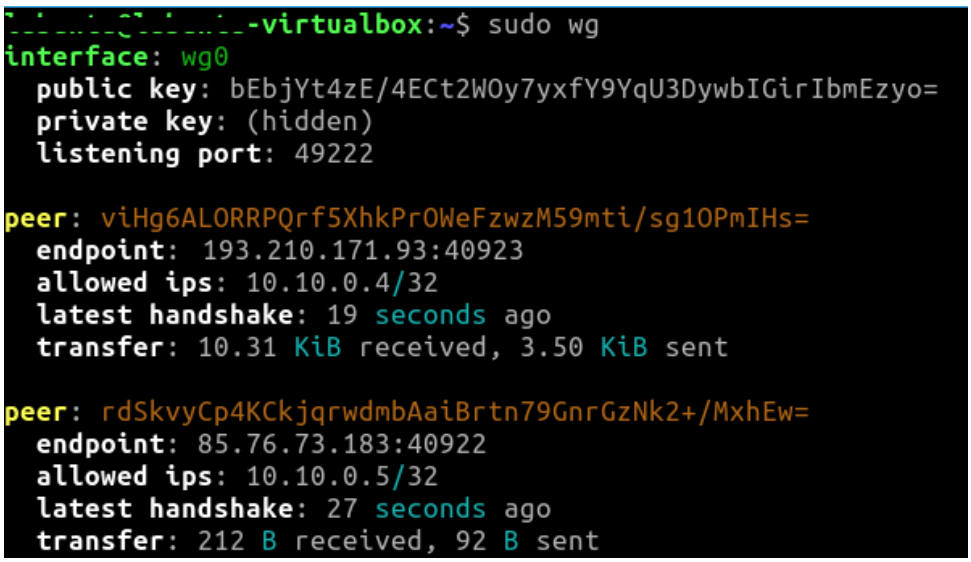


Kuva 10. Windows-työaseman suorittamat testit 1–3.



Testiohjelman kohta 4 liittyi VPN-palvelimen ylläpitoon ja valvontaan. VPN-palvelimelta näkee voimassaolevat VPN-yhteydet komennolla *sudo wg*, joten testin kohta 4 suoritettiin onnistuneesti. Kuvassa 11 on esitetty VPN-palvelimen näkymä voimassaolevista VPN-yhteyksistä – eli Windows- ja Linux-työasemien yhteyksistä.

Kuva 11. VPN-palvelimen ylläpitonäkymä voimassaolevista VPN-yhteyksistä.



Testiohjelman viides kohta koski palomuurisääntöjä, joiden toimiessa VPN-yhteyden avulla sisäverkon palvelut ovat käytettävissä, mutta ilman toimivaa VPN-yhteyttä ei sisäverkkoon ole pääsyä. Tässä koeympäristössä ei käytössä ollut varsinaisesti erillistä palomuuria, johon olisi määritelty sääntöjä VPN-yhteydelle. Käytössä olleisiin laitteisiin kuitenkin tehtiin muutoksia, jotka vaikuttivat liikenteen sallimiseen tai estämiseen. Kotireitittimen oletusasetuksissa palomuuriin oli asetettu sääntö *WAN -> LAN | BLOCK ALL*, jonka tarkoituksena on estää ulkoverkosta sisäverkkoon pääsy. VPN-yhteyden sallimiseksi kotireitittimestä otettiin käyttöön *port forward* -toiminto, jossa määritettiin VPN-palvelimen käyttämään UDP-porttiin kohdistuneen liikenteen salliminen. Palomuurisääntöjen voidaan todeta toimineen riittävän havainnollistavasti tässä testissä, sillä ilman VPN-yhteyttä sisäverkon palveluihin ei ollut pääsyä etäkäytetyiltä työasemilta, eikä ilman *port forward* -toimintoa edes VPN-yhteyttä ollut mahdollista muodostaa.

5.4 Havainnot

Tilaajalle soveltuvan VPN-ratkaisun havainnollistava käyttöönotto ja testaus onnistui koeympäristössä hyvin. Ohjelmistojen asennukset sekä asetusten määrittäminen onnistuivat Wireguard-verkkosivuston (wireguard, n.d.a) ja sieltä löytyneen materiaalin avulla hyvin. Erilaisia asennus- ja konfiguraatio-ohjeita on tarjolla avoimissa lähteissä, mutta kaikkein varmin tapa palvelun käyttöönotossa on seurata valmistajan virallista dokumentaatiota ja suosituksia. Suurimmat oivallukset ja haasteet palvelun käyttöönoton yhteydessä, liittyivät Wireguard:n sisäisten reititys- ja nimenmuutossääntöjen (iptables) määrittämiseen sekä kotireitittimen port forward -säännön asettamiseen.

Palvelun käyttöönotto ja asentaminen on suoritettava aina tapauskohtaisesti, sillä eroavaisuuksia aiheuttaa esimerkiksi käytettävä laitteisto ja osoitteisto. Käyttöönoton realistinen havainnollistaminen ja asetusten määrittäminen vaati jokaiselle VPN-laitteelle oman julkisen IP-osoitteen. Valitun koeympäristön kohdalla tämä tarkoitti kolmea eri julkista IP-osoitetta, jotka oli mahdollista saada käyttämällä kolmea eri internetliittymää. Vastaavaa haastetta ei olisi tullut, mikäli koeympäristö olisi tehty pilvipalveluita hyödyntäen, sillä pilvipalvelut tarjoavat kätevästi julkisia IP-osoitteita tarpeen mukaan.

Käyttöönotto herätti ajatuksia ylläpidosta ja palvelun käytettävyydestä. Ylläpitotoimet, kuten yhden yksittäisen yhteyden poistaminen sallituista yhteyksistä, vaatii palvelimen konfiguraatiotiedoston muokkaamisen ja täten myös palvelun uudelleen käynnistämisen. Tämä tarkoittaa sitä, että kaikki VPN-yhteydet katkeavat toimenpiteestä johtuen. Tämä ongelma on mahdollista ratkaista ottamalla käyttöön jokin Wireguard:lle kehitetty avoimen lähdekoodin ylläpitosovellus, johon tällainen ominaisuus on rakennettu (Haas, n.d.). Toinen ylläpidollinen havainto liittyy VPN-palvelimien määrään, kun palvelua otetaan yrityksissä käyttöön. Yhden palvelimen ratkaisussa VPN-yhteydet ovat pois käytöstä aina, kun kyseistä palvelinta huolletaan tai käynnistetään päivitysten yhteydessä uudelleen. Tämä ongelma olisi ratkaistavissa ottamalla käyttöön varapalvelin, jolloin toisen palvelimen ollessa pois käytöstä, olisi VPN-pavelu edelleen käytettävissä.

6 Yhteenveto

Tämän opinnäytetyön tavoitteena oli valita tilaajalle soveltuva avoimen lähdekoodin VPN-protokolla ja suorittaa havainnollistava VPN-ratkaisun käyttöönotto. Opinnäytetyön teoriaosuudessa perehdyttiin avoimella lähdekoodilla levitettyihin VPN-tekniikoihin sekä OpenVPN- ja Wireguard-protokolliin, joiden välillä suoritettiin laadullinen matriisianalyysi. Analyysin perusteella Wireguard oli tilaajana toimineelle viestintäalan pienyritykselle paremmin soveltuva VPN-protokolla, joten opinnäytetyön toiminnallisessa osuudessa havainnollistettiin Wireguard-protokollan käyttöönotto. Käyttöönottoa varten rakennettiin koeympäristö, joka vastasi toiminnallisuuksiltaan yksinkertaistettua tilaajan verkkorakennetta. Käyttöönotto onnistui tavoitteiden mukaisesti ja käyttöönotolle suunniteltu testiohjelma suoritettiin onnistuneesti läpi. VPN-ratkaisun käyttöönotto on aina tapauskohtaista, joten on suositeltavaa, että käyttöönotosta luodaan aina erillinen suunnitelma, joka pohjautuu riitävään tietotaitoon olemassa olevasta verkkoinfrastruktuurista ja sen erityispiirteistä.

Tässä opinnäytetyössä suoritettu havainnollistava käyttöönotto sisälsi vain Wireguard-protokollan sisäisten ominaisuuksien hyödyntämistä. VPN-ratkaisun käytettävyyttä ja ylläpitoa olisi mahdollista parantaa, integroimalla siihen erillinen graafinen hallintasovellus tai -rajapinta. Valmiita integroitavia avoimen lähdekoodin lisäosia on

löydettävissä esimerkiksi GitHub-palvelusta. Mahdollisen lisäosan asentamisesta tulee kuitenkin tehdä riskiarvo ja tutustua lisäosan toiminnallisuuksiin riittävän tarkasti, jotta VPN-ratkaisun turvallisuus ei vaarannu.

Opinnäytetyön kirjoittajan osaaminen ja ymmärrys VPN-tekniikoista – ja erityisesti Wireguard-protokollasta – kasvoi opinnäytetyöprosessin aikana merkittävästi. Opinnäytetyöprosessi eteni suunnitellusti ja yhteydenpito tilaajan sekä ohjaajan kanssa oli aktiivista ja onnistunutta. Opinnäytetyössä suoritettu matriisianalyysi sekä VPN-ratkaisun havainnollistava käyttöönotto esiteltiin tilaajan edustajalle. Tilaajan edustaja oli tyytyväinen opinnäytetyön tuloksiin ja malliratkaisun havainnollistamiseen.

Lähteet

Chapple, M. & Seidl, D. (2018) *Comptia security+ study guide.* Indianapolis, Indiana: Sybex inc. U.S.

Chai, W. & Bigelow, S. (16.12.2021) *Cloud computing.* Haettu 23.4.2022 osoitteesta https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing

Donenfeld, J. (1.6.2020) *Wireguard: Next Generation Kernel Network Tunnel.* [Julkaisun yksilöllinen versionumero: 4846ada1492f5d92198df154f48c3d54205657bc]. Haettu 27.4.2022 osoitteesta https://www.wireguard.com/papers/wireguard.pdf

Gargiulo, M. (15.11.2018) *What Is A Business VPN, And How Can It Secure Your Company?* https://www.forbes.com/sites/forbestechcouncil/2018/11/15/what-is-a-business-vpn-and-how-can-it-secure-your-company/

Google Play. (n.d.) *OpenVPN for Android.* Haettu 26.4.2022 osoitteesta https://play.google.com/store/apps/details?id=de.blinkt.openvpn&hl=fi&gl=US

Grafana. (n.d.a) *1 OpenVPN Server - Dashboard.* Haettu 6.5.2022 osoitteesta https://grafana.com/grafana/dashboards/10562

Grafana. (n.d.b) *Wireguard - Dashboard.* Haettu 6.5.2022 osoitteesta https://grafana.com/grafana/dashboards/12177

Haas, C. (n.d) *Wireguard Portal – GitHub repository.* Haettu 27.4.2022 osoitteesta https://github.com/h44z/wg-portal

Harkness, A. (15.5.2019) *5 Common VPN protocols explained.* Haettu 21.4.2022 osoitteesta https://www.netmotionsoftware.com/blog/connectivity/vpn-protocols

Hoffman, C. (11.08.2021) *What Is a VPN, and Why Would I Need One?* Haettu 21.4.2022 osoitteesta https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

Jeffery, E. (19.6.2020) *VPN Split-Tunneling – To Enable or Not To Enable.* https://www.infosecurity-magazine.com/opinions/vpn-split-tunneling/

Korolov, M. (7.4.2022) *Who's selling SASE and what do you get?* https://www.networkworld.com/article/3586127/who-s-selling-sase-and-what-do-you-get.html

Kyberturvallisuuskeskus. (20.4.2020) *VPN-yhteyksien kapasiteetin varmistaminen.* https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vpn-yhteyksien-kapasiteetin-varmistaminen

Leskinen, T. (29.3.2021). *Etätyö yleistyi eniten aloilla ja alueilla, joilla sitä ennen tehtiin vähiten*. Tilastokeskus. https://www.tilastokeskus.fi/tietotrendit/artikkelit/2021/etatyo-yleistyi-eniten-aloilla-ja-alueilla-joilla-sita-ennen-tehtiin-vahiten/

Long, H. (2022). *Wireguard vs OpenVPN in 2022: 7 big differences.* Päivitetty 21.4.2022. Haettu 25.4.2022 osoitteesta https://restoreprivacy.com/vpn/wireguard-vs-openvpn/

Markkola, L. (2020). *Tietoturva työmatkoilla* [opinnäytetyö, Jyväskylän ammattikorkeakoulu]. https://urn.fi/URN:NBN:fi:amk-2020052915320

Mazūra, J. (18.3.2022). *VPN protocols explained.* https://cybernews.com/what-is-vpn/vpn-protocols/

Mills, M. (2.1.2020) *Internet speed and latency.* https://itigic.com/fi/internet-speed-and-latency/

Mocan, T. (7.11.2020). *What is WireGuard?* https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-wireguard/

MTI College. (25.6.2021) *What Are the Different Types of Cloud Services?* https://mticollege.edu/blog/technology/aws-cloud-administration/cloud-services-types/

OpenVPN. (n.d.a) *OpenVPN.* Haettu 26.4.2022 osoitteesta https://openvpn.net

OpenVPN. (n.d.b) *Community downloads.* Haettu 26.4.2022 osoitteesta https://openvpn.net/community-downloads/

OpenVPN. (n.d.c) *Community resources: OpenVPN cryptographic layer.* Haettu 26.4.2022 osoitteesta https://openvpn.net/community-resources/openvpn-cryptographic-layer/

OpenVPN. (n.d.d) *Advanced option settings on the command line.* Haettu 26.4.2022 osoitteesta https://openvpn.net/vpn-server-resources/advanced-option-settings-on-the-command-line/

OpenVPN. (n.d.e) *How to install the OpenVPN GUI on Windows.* Haettu 26.4 osoitteesta https://openvpn.net/community-resources/how-to-install-the-openvpn-gui-on-windows/

OpenVPN. (n.d.f) *Controlling a running OpenVPN process.* Haettu 26.4.2022 osoitteesta https://openvpn.net/community-resources/controlling-a-running-openvpn-process/

OpenVPN. (n.d.g) *Security audit vulnerabilities resolved.* Haettu 26.4.2022 osoitteesta https://openvpn.net/community-resources/controlling-a-running-openvpn-process/

OpenVPN. (n.d.h) *VPN-Client: OpenVPN Connect.* Haettu 26.4.2022 osoitteesta https://openvpn.net/vpn-client/

OpenVPN. (n.d.i) *Wiki: Overview of OpenVPN.* Haettu 26.4.2022 osoitteesta https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn

OPNsense. (n.d.) *Virtual Private Networking.* Haettu 26.4.2022 osoitteesta https://docs.opnsense.org/manual/vpnet.html#

Paloalto networks. (n.d.a) *What Is a Remote Access VPN?* Haettu 20.4.2022 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn

Paloalto networks. (n.d.b) *What is a Site-to-Site VPN?* Haettu 18.4.2020 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn

Peek, S. (5.5.2021) *What Is Remote Access VPN?* https://www.business.com/vpn/remote-access/

Pehrson, R. & Heuer, R. (2021). *Structured Analytic Techniques for Intelligence Analysis – Third edition.* California: SAGE, CQ Press.

Perlmutter, B. & Zarkower, J. (2001). *VPN – Virtuaaliset yksityisverkot.* (T. Kokkonen, käänt.). Edita Oyj. (alkuperäisteos julkaistu 2000)

Pyhäluoto, A. (2021). *Verkkosalaustekniikoiden vertailu* [opinnäytetyö, Oulun ammattikorkeakoulu]. https://urn.fi/URN:NBN:fi:amk-2021121890012

Tyson, J., Pollette, C. & Crawford, S. (9.4.2022) *How a VPN (Virtual Private Network) works.* Haettu 20.4.2022 osoitteesta https://computer.howstuffworks.com/vpn.htm

VirtualBox. (n.d.) *About VirtualBox.* Haettu 24.4.2022 osoitteestsa https://virtualbox.org/wiki/VirtualBox

Williams, M. (10.1.2022) *What is a VPN protocol?* https://www.techradar.com/vpn/what-is-a-vpn-protocol

Wireguard. (n.d.a) *Wireguard.* Haettu 27.4.2022 osoitteesta https://www.wireguard.com/

Wireguard. (n.d.b) *Installation.* Haettu 6.5.2022 osoitteesta https://www.wireguard.com/install/

Wireguard. (n.d.c) *Performance.* Haettu 27.4.2022 osoitteesta https://www.wireguard.com/performance/

Liite 1: VPN-palvelimen asetukset

rajapinta	Asetus	Asetuksen arvo	Selite
Interface			Palvelimelle luotavan rajapinnan vakioitu nimi.
	Address	10.10.0.2/32	Palvelimen VPN-yhteyteen käyttämä yksityinen IP-osoite.
	SaveConfig	True	Konfiguraatiotiedosto tallennetaan ja sitä on mahdollista käyttää pikakomentojen yhteydessä.
	PostUp	iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE;	Skripti, joka suoritetaan VPN-yhteyden käynnistämisen yhteydessä. VPN-pakettien suodatus ja osoitteenmuutos: ketjuun FORWARD lisätään sallittu suodatus rajapinnalle wg0 säännöllä ACCEPT; NAT-tauluun lisätään POSTROUTING sääntö ulos menevään rajapintaan enp0s8, jolloin sisäverkon osoitteet muutetaan one-to-many -periaatteella yhdeksi samaksi osoitteeksi.
	PostDown	iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o enp0s8 -j MASQUERADE;	Skripti, joka toteutetaan VPN-yhteyden sammuttamisen yhteydessä. VPN-pakettien suodatus ja osoitteenmuutos: poistetaan edellisessä kohdassa luodut säännöt suodatuksen ja osoitteenmuutosten osalta.
	ListenPort	49222	UDP-tietoliikenneportti, josta otetaan vastaan VPN-yhteyden tietoliikennepaketit. Ylläpitäjän määrittämä.
	PrivateKey	<sensuroitu merkkjono>	Palvelimen yksityinen salausavain tiedostosta /etc/wireguard/privatekey.

Peer			Etäkäyttöpisteen rajapinnan vakioitu nimi.
	PublicKey	<merkkijono>	Etäkäytettävän työaseman asennuksen yhteydessä luotu työaseman julkinen salausavain.
	AllowedIPs	10.10.0.5/32	Sallittu yksityinen IP-osoite, joka on asetettu etäkäytettävän työaseman virtuaaliselle rajapinnalle wg0. Mahdollista laajentaa käytettyä maskia tai lisätä osoite-maski -yhdistelmiä pilkulla erotettuina.
	Endpoint	85.76.73.183:40922	Etäkäytettävän työaseman julkinen IP-osoite ja työaseman kuunteluun asettama UDP-tietoliikenneportti.
Peer			Etäkäyttöpisteen rajapinnan vakioitu nimi.
	PublicKey	<merkkijono>	Etäkäytettävän työaseman asennuksen yhteydessä luotu työaseman julkinen salausavain.
	AllowedIPs	10.10.0.4/32	Sallittu yksityinen IP-osoite, joka on asetettu etäkäytettävän työaseman virtuaaliselle rajapinnalle wg0. Mahdollista laajentaa käytettyä maskia tai lisätä osoite-maski -yhdistelmiä pilkulla erotettuina.
	Endpoint	193.210.171.93:40923	Etäkäytettävän työaseman julkinen IP-osoite ja työaseman kuunteluun asettama UDP-tietoliikenneportti.

Liite 2: Linux-työaseman VPN-asetukset

Rajapinta	Asetus	Asetuksen arvo	Selite
Interface			Työasemalle luotavan rajapinnan vakioitu nimi.
	Address	10.10.0.5/32	Työaseman VPN-yhteyden yksityinen IP-osoite, joka on asetettuna palvelimelle sallituksi yhteydeksi.
	SaveConfig	true	Konfiguraatiotiedosto tallennetaan ja sitä on mahdollista käyttää pikakomentojen yhteydessä.
	ListenPort	40922	UDP-tietoliikenneportti, josta otetaan vastaan VPN-yhteyden tietoliikennepaketit. Ylläpitäjän määrittämä.
	FwMark	<merkkijono>	Merkintä datapaketissa, joka mahdollistaa palvelimen uudelleen reitittää liikenne palvelimelta eteenpäin sisäverkkossa.
	PrivateKey	<sensuroitu merkkijono>	Työaseman yksityinen salausavain tiedostosta /etc/wireguard/privatekey.
Peer			VPN-palvelimen rajapinnan vakioitu nimi.
	PublicKey	<merkkijono>	VPN-palvelimen julkinen salausavain.
	AllowedIPs	0.0.0.0/0	Tämä kuvaa VPN-yhteyden välityksellä siirrettävää työaseman tietoliikennettä. Asettamalla arvon 0.0.0.0/0 reititetään kaikki työaseman tietoliikenne virtuaalisen wg0 rajapinnan välityksellä eteenpäin, eli pakotetaan VPN-tunneliin full tunnel -moodilla.
	Endpoint	80.222.237.235:49222	VPN-palvelimen julkinen IP-osoite ja kuunteluun asettama UDP-tietoliikenneportti, johon VPN-liikennöinti suoritetaan.

	PersistentKeepalive	25	Yhteyden ylläpitoon tarkoitettujen pienien datapakettien lähetysintervalli sekunneissa. Eli mikäli liikennöintiä ei työaseman ja palvelimen välillä ole, niin työasema lähettää 25 sekunnin välein ylläpitopaketin palvelimelle ja näin yhteys pysyy auki.

Liite 3: Windows-työaseman VPN-asetukset

Rajapinta	Asetus	Asetuksen arvo	Selite
	Name	Wg0	Tunnelin nimi
	Public key	<merkkijono>	VPN-yhteydessä käytettävä Windows-työaseman julkinen salausavain, jonka sovellus on automaattisesti luonut.
Interface			Työasemalle luotavan rajapinnan vakioitu nimi.
	PrivateKey	<sensuroitu merkkijono>	VPN-yhteydessä käytettävä Windows-työaseman yksityinen salausavain. Salausavain on sovelluksen automaattisesti luoma.
	ListenPort	40923	UDP-tietoliikenneportti, josta otetaan vastaan VPN-yhteyden tietoliikennepaketit. Ylläpitäjän määrittämä.
	Address	10.10.0.4/32	Windows-työaseman VPN-yhteyden yksityinen IP-osoite, joka on asetettuna palvelimelle sallituksi yhteydeksi.
Peer			VPN-palvelimen rajapinnan vakioitu nimi.
	PublicKey	<merkkijono>	VPN-palvelimen julkinen salausavain.
	AllowedIPs	0.0.0.0/0	Tämä kuvaa VPN-yhteyden välityksellä siirrettävää työaseman tietoliikennettä. Asettamalla arvon 0.0.0.0/0 reititetään kaikki työaseman tietoliikenne virtuaalisen wg0 rajapinnan välityksellä eteenpäin, eli pakotetaan VPN-tunneliin full tunnel -moodilla.
	Endpoint	80.222.237.235:49222	VPN-palvelimen julkinen IP-osoite ja kuunteluun asettama

			UDP-tietoliikenneportti, johon VPN-liikennöinti suoritetaan.
	PersistentKeepalive	25	Yhteyden ylläpitoon tarkoitettujen pienien datapakettien lähetysintervalli sekunneissa. Eli mikäli liikennöintiä ei työaseman ja palvelimen välillä ole, niin työasema lähettää 25 sekunnin välein ylläpitopaketin palvelimelle ja näin yhteys pysyy auki.
	Block untunneled traffic (kill-switch)	Yes	Asetus estää tunneloimattomat tietoliikenneyhteydet, eli mikäli VPN-palvelu menee pois päältä käyttäjän tietämättä, suojelee asetus käyttäjää estämällä liikennöinnin ilman toimivaa VPN-yhteyttä.