Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Jere Vepsä

WireGuard-yhteyden käyttöönotto hajautetuissa valvontakohteissa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikka

Insinöörityö

9.4.2021

Tekijä Otsikko Sivumäärä Aika	Jere Vepsä WireGuard-yhteyden käyttöönotto hajautetuissa valvontakohteissa 30 sivua 9.4.2021
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	Sähkö- ja automaatiotekniikan tutkinto-ohjelma
Ammatillinen pääaine	Automaatiotekniikka
Ohjaajat	Lehtori Timo Kasurinen

Virtuaalinen erillisverkko (VPN) on tunneloitu yhteys, jonka tarkoitus on mahdollistaa kahden tai useamman lähiverkon yhdistäminen toisiinsa turvallisesti internetin tai jaetun verkon yli. Tyypillisesti VPN-yhteyksiä käytetään yrityksen toimistorakennuksien verkkojen yhdistämiseen keskenään, etäyhteyden ottamiseen tai etätyöskentelyyn.

Tämän yrityslähtöisen opinnäytetyön tavoitteena oli korvata käytössä oleva maksullinen VPN-yhteys ja käyttöönottaa oma WireGuard-pohjainen ratkaisu. Omalla ratkaisulla yritys voi säästää palvelumaksuissa, ja yhteys on paremmin yrityksen hallittavissa. Parempi hallittavuus nopeuttaa mahdollisia muutoksia tulevaisuudessa ja helpottaa järjestelmän laajennettavuutta.

Työssä tutkittiin yrityksen tarpeisiin vastaavia VPN-yhteystyyppejä ja niihin soveltuvia laiteratkaisuja. Laitevalinnassa pyrittiin edulliseen mutta luotettavaan ja ammattimaiseen ratkaisuun. Tutkimustyön lisäksi työhön kuului myös testauksen ja laitevalinnan jälkeen laitteiden konfigurointi ja asennus sekä VPN-verkon käyttöönotto yli 40 kohteessa.

Työn lopputuloksena syntyi yrityksen käyttöön oma VPN-ratkaisu, joka mahdollistaa salatun yhteyden yrityksen valvomiin kohteisiin. Uusi VPN-yhteys korvasi maksullisena palveluna ostetun yhteyden, mikä toi yritykselle säästöjä ja mahdollisti yhteyden täysivaltaisen hallinnan yrityksellä. Työn tuloksena syntyi myös dokumentaatio yhteyden käyttöönotosta, jota voidaan hyödyntää tulevaisuudessa ohjeena vastaavan verkon rakentamisessa.

Avainsanat	VPN, WireGuard, Etäyhteydet

Author Title Number of Pages Date	Jere Vepsä Implementing WireGuard Connection to Scattered Surveillance Sites 30 pages 9 April 2021
Degree	Bachelor of Engineering
Degree Programme	Electrical and Automation Engineering
Professional Major	Automation Engineering
Instructors	Timo Kasurinen, Senior Lecturer

A Virtual Private Network (VPN) is a tunneled connection designed to allow two or more Local Area Networks (LAN) to be connected to each other securely over the Internet or a shared network. Typically, VPN connections are used to connect networks in a company's office buildings, to establish a remote connection, or work remotely.

The aim of this company-oriented thesis work was to replace the existing paid VPN connection and to introduce company's own WireGuard-based solution. With its own solution, the company can save on service fees and the connection can be better managed by the company. Better manageability will speed up possible changes of the network in the future and facilitate system scalability.

The study examined the types of VPN connections that meet the company's needs and the device solutions suitable for them. The choice of equipment was aimed at an affordable but reliable and professional solution. In addition to the research work, the work also included the configuration and installation of equipment after testing and device selection, as well as the implementation of a VPN network in more than 40 locations.

The result of the work is the company's own VPN solution, which enables an encrypted connection to the sites maintained by the company. The new VPN connection replaced the connection purchased as a paid service, which brought savings to the company and enabled the company to fully manage the connection. The work also resulted in documentation on the implementation of the connection, which can be used in the future as a guide in building a similar network.

Keywords	VPN, WireGuard, Remote Connections

Sisällys

Lyhenteet

AES	Advanced Encryption Standard. Tietotekniikassa käytetty lohkosalausmenetelmä.
BSD	Berkeley Software Distribution on UNIX-pohjainen käyttöliittymä.
CLI	Command Line Interface. Tietotekniikassa käytettävä tekstipohjainen komentoliittymä.
IP	Internet Protocol on TCP/IP-viitemallin verkkokerroksen protokolla.
LAN	Local Area Network. Rajatulla alueella oleva tietoverkko.
RSA	Rivestin, Shamirin ja Adlemanin kehittämä julkisen avaimen salausmetodi.
SSH	Secure Shell. Tietotekniikassa käytettävä salatun tietoliikenteen protokolla.
SSL	Secure Socket Layer on internetsovellusten tietoliikenteen suojaukseen käytetty protokolla.
UDP	User Datagram Protocol on tietotekniikassa käytettävä tiedonsiirtoprotokolla.
VPN	Virtual Private Network. Julkisen verkon yli muodostettu virtuaalinen erillisverkko.

1 Johdanto

Nykyinen teollisuus- ja yritysmaailma luottaa yhä enemmän etäyhteyksien käyttöön ja tiedonsaantiin sijainnista riippumatta. Monille yrityksille tämä realisoitui 2020 keväällä, kun merkittävä osa työntekijöistä siirtyi etätöihin vallitsevan pandemiatilanteen takia.

Etäyhteyksien arvo yrityksille näkyy myös tilanteissa, joissa työntekijän valvonta- tai huoltokohteet ovat hajautetusti sijoittuneet eri maantieteellisiin paikkoihin. Näissä tilanteissa siirtymäajasta kohteiden välillä tulee merkittävä kulu, jos työtehtävää ei voida toteuttaa etäyhteyden avulla.

Tämä insinöörityö on työelämälähtöinen, ja sen kohdeyrityksenä on turvallisuus- ja telemetria-alan yritys Noatek Oy. Työn tavoitteena on kartoittaa kohdeyritykselle vaihtoehtoisia tietoliikenneratkaisuja käytössä olevan, maksullisena palveluna hankitun VPN-yhteyden korvaamiseksi. Tarkoituksena on luoda ja käyttöönottaa oma, itsehallittava VPN-verkko useaan hajautettuun kohteeseen, jotka sijaitsevat Etelä-Suomen alueella.

Tuotoksena insinöörityössä toteutetaan yritykselle oma VPN-yhteys ja luodaan suunnitelma kohteissa käytettävistä IP-osoitteista sekä dokumentaatio laitteiden konfiguroinnista yhteyttä varten. Työn kirjallisessa osiossa perehdytään yrityksen tarpeisiin, salatun yhteyden teoriaan, VPN-yhteystyyppeihin ja -protokoliin sekä eri laitevaihtoehtoihin yhteyden toteuttamiseksi. Lisäksi käydään yksityiskohtaisesti läpi valitun VPN-ratkaisun konfigurointi yhteyden muodostamiseksi.

2 Projektin tausta ja yrityksen tarpeet

Projekti toteutetaan turvallisuus- ja telemetria-alan yritykselle Noatek Oy:lle, joka tuottaa valvontaan ja turvallisuuteen liittyviä ratkaisuja ja palveluja. Yrityksellä on erilaisia valvontakohteita hajautetusti ympäri maata. Kohteiden valvonta vaatii tarkistuksia, ylläpitoa ja huoltoa. Etäyhteys on taloudellisesti järkevin ja tietoturvallinen vaihtoehto toteuttaa tämä. Tähän asti yritys on käyttänyt tarpeisiinsa maksullisena palveluna hankittua OpenVPN-pohjaista ratkaisua. Ratkaisussa salattu yhteys on ollut laitekohtainen, ja se on ollut sidottuna suoraan 3G/4G-modeemiin, joka on toiminut samalla yhteyden päätelaitteena. Yhteyden salaamisen lisäksi VPN mahdollistaa dynaamisen IP-osoitteen käyttämisen kohteessa. OpenVPN:n vuoksi kohteella on kiinteä, VPN-sidonnainen IP-osoite, jota käytetään yhteyden muodostamiseen.

Yrityksen tavoitteena on ollut korvata maksullinen etäyhteysjärjestelmä omalla VPN-yhteydellä, joka on edullisempi ratkaisu, ja mahdollistaa laajemman hallittavuuden ja laajennettavuuden. Ostettuna palveluna etäyhteyskokonaisuus on kankeampi hallita, ja muutokset, kuten uuden kohteen lisääminen, ovat hitaampia.

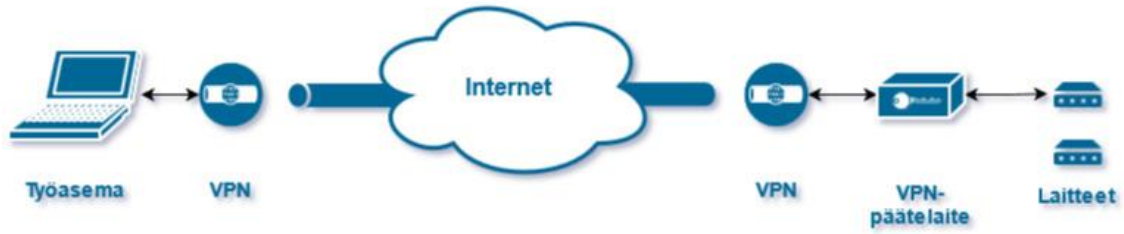
Omalla VPN-yhteydellä yritys voi hallita etäyhteyksiään joustavammin ja paremmin omien tarpeidensa mukaan. Uusien kohteiden lisääminen järjestelmään on nopeampaa, ja mahdolliset muutokset esimerkiksi IP-osoitteiden suhteen tapahtuvat nopeasti. Järjestelmän osoittauduttua hyväksi voi yritys tarjota sitä myös omana maksullisena palveluna tulevaisuudessa.

Yrityksen tarve suojatuille etäyhteyksille on vaihteleva niin laitteiston kuin sijainninkin osalta. Etäyhteys on kyettävä ottamaan usealla eri laitteella, niin Linux- kuin Windows-pohjaisestikin. Yhteys on kyettävä muodostamaan sekä yrityksen toimistoverkosta että yksittäisen työntekijän verkosta riippumatta siitä, onko hänellä käytössään kiinteä internetyhteys kotona vai mobiiliverkkoyhteys puhelimen avulla, ja kaiken tämän on tapahduttava turvallisesti.

3 VPN-yhteys

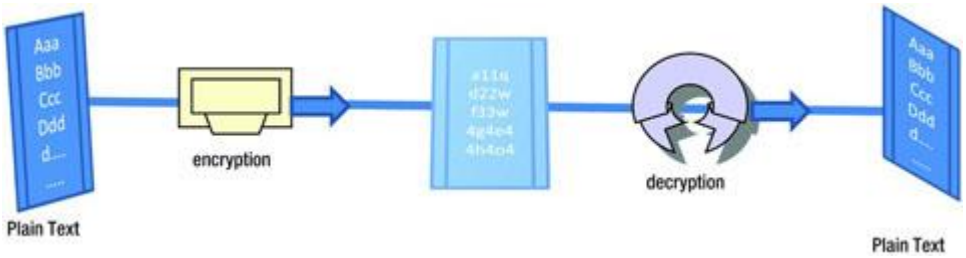
3.1 Virtual Private Network

Virtuaalinen erillisverkko eli VPN (Virtual Private Network) on yhteys, joka muodostetaan kahden lähiverkon eli LAN:in (Local Area Network) välille julkisen tai jaetun verkon yli. VPN-yhteydellä yhdistetyt laitteet toimivat, kuin ne olisivat samassa lähiverkossa todellisesta verkkorakenteesta tai maantieteellisestä sijainnista riippumatta. [1.] Kuvassa 1 havainnollistetaan VPN-yhteyden tunnelointia internetin yli.



Kuva 1. VPN-yhteyden perusperiaate.

VPN-yhteyden perusperiaate on salata lähetettävä data niin, että sitä ei voida lukea tai muokata ilman oikeaa salausavainta. Tämä vahvistaa tietoturvaa tilanteissa, joissa VPN-yhteys kulkee jaetun tai julkisen verkon yli. [2.] Datan salaaminen, eli kryptaus, toteutetaan erilaisia matemaattisia algoritmeja ja salausavainta käyttäen. Data muutetaan muotoon, jossa sen lukeminen ja muokkaaminen ilman salausavainta on mahdotonta tai vähintäänkin runsaasti aikaa vievää. Data avataan taas luettavaan muotoon salauksen purkumetodilla, johon hyödynnetään salaustavasta riippuen samaa tai eroavaa salausavainta. [3.] Salauksen perusperiaatetta visualisoidaan kuvassa 2.



Kuva 2. Visualisointi tiedon salaamisesta. [4]

Tyypillinen perustarve VPN-yhteydelle syntyy, kun yrityksellä on useita konttoreita eri sijainneissa tai yksittäisellä käyttäjällä on tarve päästä muualta käsiksi yrityksen lähiverkossa olevaan tietokantaan [5]. Yhteys voidaan toteuttaa myös erikseen rakennetulla verkkoyhteydellä, mutta tämä on kalliimpi ja merkittävästi työläämpi vaihtoehto. [4.]

Hyvän VPN-järjestelmän tulisi tukea seuraavia tekijöitä:

- tunnelointi
- osapuolten todennus ja tietojen eheys
- uusinnan estävät palvelut (Anti-Replay Services)
- tietojen salaus.

Tunneloinnilla tarkoitetaan varsinaisen datan pakkausta toisen eri protokolan datapaketin sisälle tiedonsiirtoa varten. Osapuolten todennuksella tarkoitetaan sitä, että molemmat kommunikoivat osapuolet todennetaan ja sillä taataan, että vain autentikoidut osapuolet lähettävät ja vastaanottavat dataa. Tietojen eheydellä tarkoitetaan metodia, jolla voidaan todentaa, ettei tietoa ole muokattu siirron aikana. [4.]

Uusinnan estävät palvelut tarkoittavat järjestelmää, joka tunnistaa ja hylkää kaksoiskappaleet sekä myöhästyneet datapaketit. Tämän tarkoitus on suojata järjestelmää uusintahyökkäyksiltä. Tietojen salaus on mekanismi, jolla suojataan tietojen luottamuksellisuus ja yksityisyys julkisessa verkossa. [4.]

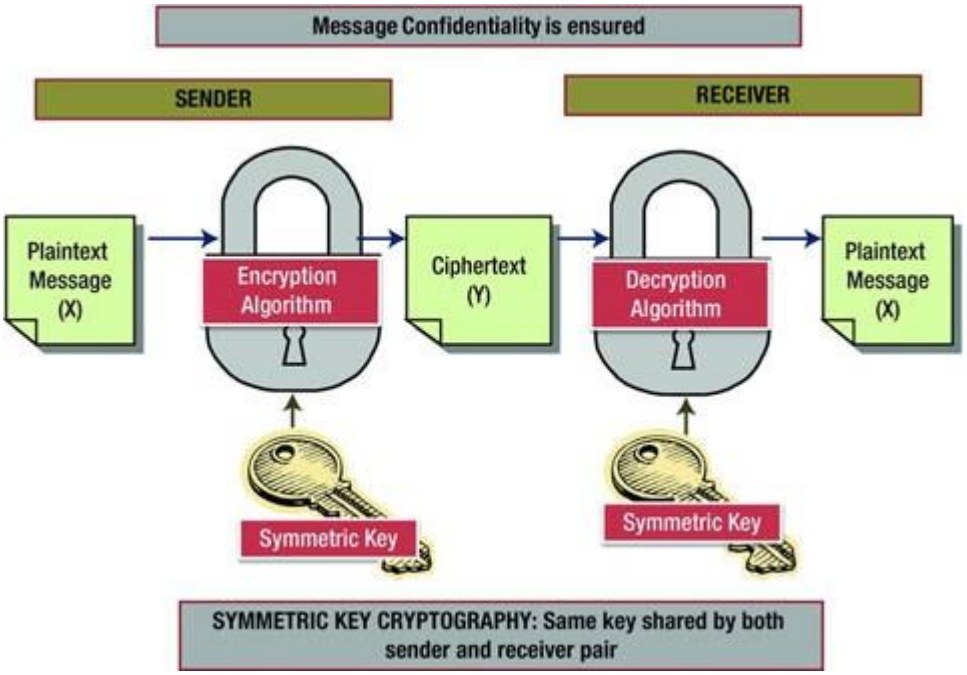
3.2 Symmetrinen ja epäsymmetrinen salaus

Salausmetodit voidaan jakaa kahteen ryhmään: symmetrisiin ja epäsymmetrisiin salausmenetelmiin. Näiden salausmenetelmien ratkaisevana erona on salausavaimien lukumäärä ja käyttö.

3.2.1 Symmetrinen salaus

Symmetrinen salaus tarkoittaa salausmetodeja, joissa viestin salaamiseen ja purkamiseen käytetään samaa salausavainta. Symmetrinen salaus on yksinkertainen tapa salata viesti, mutta sen ongelmaksi muodostuu avaimen jakaminen vastaanottajalle. Koska

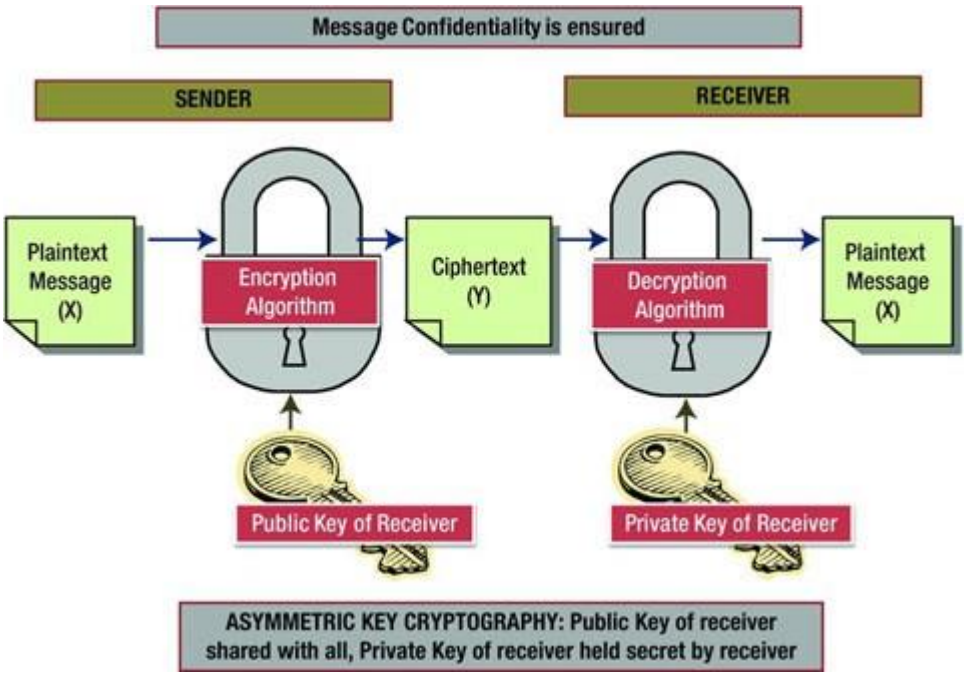
samaa salausavainta käytetään salaamiseen ja purkamiseen, on se kyettävä jakamaan turvallisesti niin, että avain ei joudu ulkopuolisten haltuun. Kuvassa 3 näkyy yksinkertaistetusti symmetrisen salauksen idea. [4.]



Kuva 3. Symmetrisen salauksen visualisointi. [4]

3.2.2 Epäsymmetrinen salaus

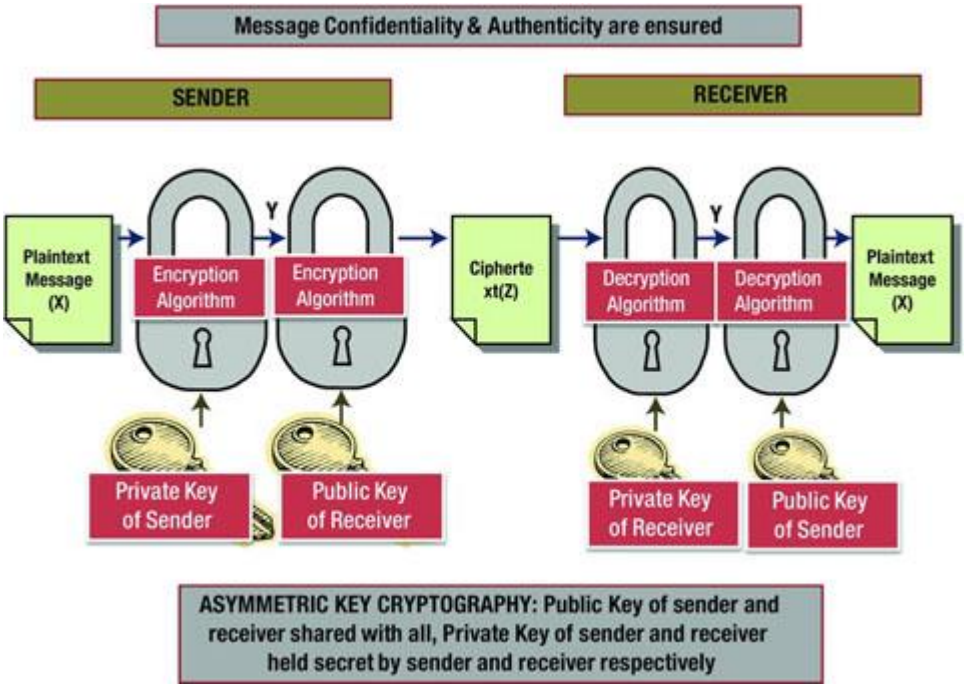
Epäsymmetrisessä salauksessa käytetään kahta salausavainta: julkista ja yksityistä. Julkinen salausavain on nimensä mukaan julkinen eli lähettäjän tiedossa ja sillä salataan lähtevä viesti. Julkista salausavainta ei voida käyttää salauksen purkamiseen. Yksityinen salausavain on vain vastaanottajan tiedossa, ja sillä puretaan vastaanotettu viesti. Julkinen ja yksityinen avain muodostetaan matemaattisesti niin, että julkisella salausavaimella salattua viestiä ei voida purkaa samalla salausavaimella, eikä yksityistä salausavainta voida laskea sen perusteella. Kuva 4 havainnollistaa käytettyjen avaimien roolia epäsymmetrisessä salauksessa. [4.]



Kuva 4. Epäsymmetrisen salauksen visualisointi. [4]

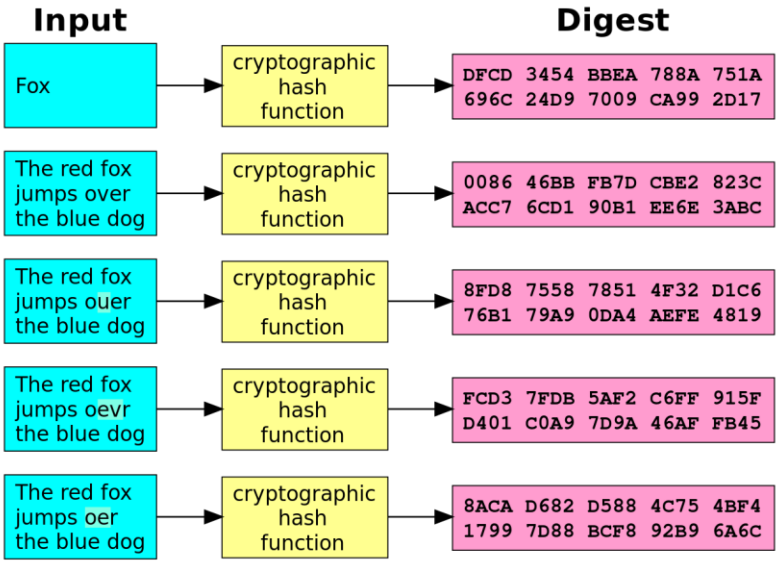
3.3 Autentikointi ja tiiviste

Salaustekniikkoja voidaan hyödyntää myös muihin tarkoituksiin. Epäsymmetrisen salauksen tekniikkaa voidaan käyttää osapuolien autentikointiin. [6.] Yhdistämällä salaukseen lähettäjän yksityisen avaimen salauksen ja vastaanottajan julkisen avaimen salauksen, voidaan muodostaa yhteys, jossa tarvitsee jakaa vain julkinen avain. Näin sekä lähettäjä että vastaanottaja voidaan autentikoida. Tätä kutsutaan julkisen avaimen salaukseksi (PKC), joista tunnetuimpia metodeja ovat Diffie Hellman, RSA (Rivest, Shamir, Adleman) ja Digital Signature Algorithm. Kuvassa 5 havainnollistetaan salausavaimien roolia osapuolten autentikoinnissa. [4.]



Kuva 5. Kuvaus julkisen avaimen salauksesta, jolla lähettäjä voidaan autentikoida. [4]

Tiivisteellä (englanniksi hash) voidaan todentaa datan eheys eli muuttumattomuus [6]. Tiiviste on yksisuuntainen matemaattinen funktio, jolla tiedosta muodostetaan tietyn mittainen merkkijono eli tiiviste. Tiivisteen perusteella ei voida palauttaa alkuperäistä dataa, mutta vertaamalla saatua tietoa sen tiivisteeseen, voidaan todentaa sen muuttumattomuus. Tiivisteen toimintaa kuvataan esimerkein kuvassa 6. [4.]



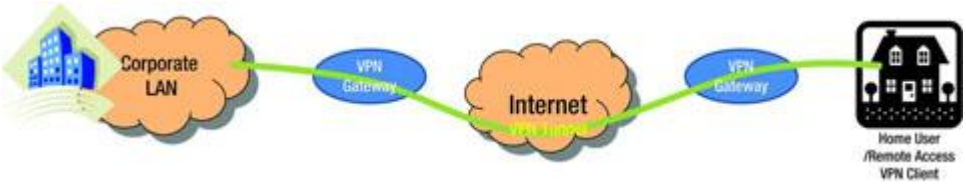
Kuva 6. Tiivistefunktion visualisointi, jossa ”Digest” kuvaa tiivistettä. [7]

3.4 VPN-yhteystyypit

VPN-yhteyden yhteystyypit voidaan jakaa eri luokkiin sen perusteella, minkä laitteen tai lähiverkon osan välille yhteys kulloinkin muodostetaan. Eri yhteystavat mahdollistavat VPN-yhteyden erilaisen käytön. [4.]

3.4.1 Host-to-Site-yhteys

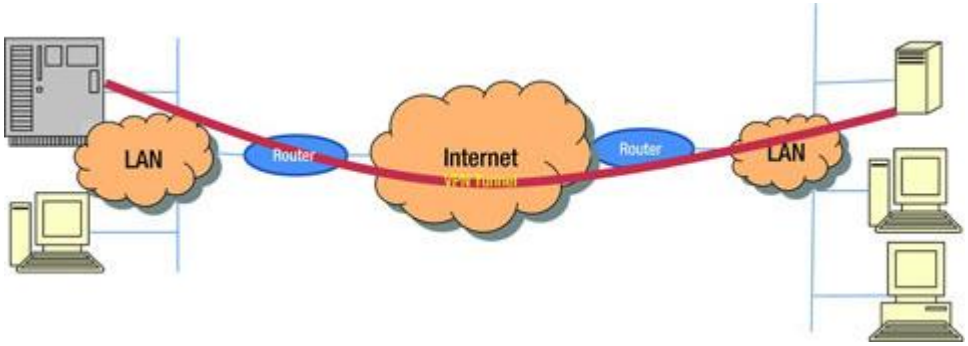
Host-to-Site tai toiselta nimeltään etäyhteys (Remote Access VPN) on yhteys yksittäisen käyttäjän laitteen ja toisen LAN-verkon välillä, joka on muodostettu virtuaalista tunnelia käyttäen. Tyypillisesti tämä tilanne esiintyy, kun yrityksen työntekijän pitää ottaa yhteyttä yrityksen lähiverkkoon internetin yli. [4.] Tämän tyyppistä tilannetta esitetään kuvassa 7.



Kuva 7. Visualisointi Host-to-Site VPN-yhteydestä. [4]

3.4.2 Host-to-Host-yhteys

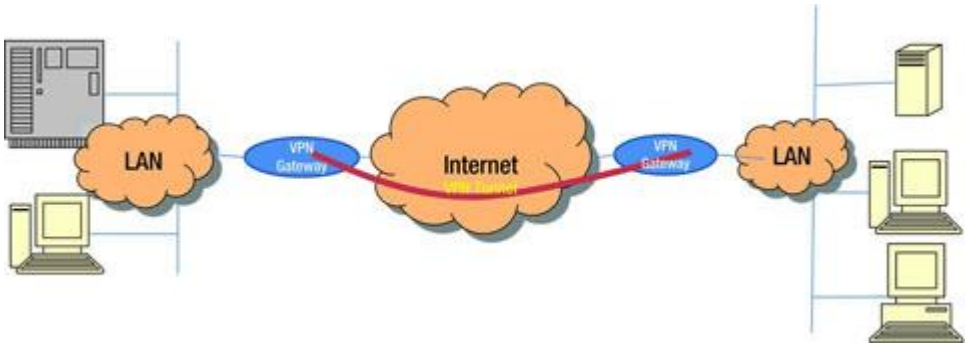
Host-to-Host VPN tarkoittaa suojattua yhteyttä kahden päätelaitteen välillä. Tässä tilanteessa muut lähiverkossa olevat laitteet eivät ole suoraan yhdistettynä VPN-yhteyteen. VPN-verkossa olevilla laitteilla on käytännössä oma VPN-sovellus. [4.] Tilannetta visualisoidaan kuvassa 8.



Kuva 8. Host-to-Host-yhteyden visualisointi kahden laitteen välillä. [4]

3.4.3 Site-to-Site-yhteys

Site-to-Site-yhteys tarkoittaa VPN-yhteyttä kahden LAN-verkon välillä. Käytännössä tämä yhteys luodaan siten, että molemmissa lähiverkoissa on oma VPN-yhteensopiva yhdyskäytävä kuten VPN-modeemi. Tämän tyyppinen yhteystapa mahdollistaa laitteiden kommunikaation keskenään lähiverkosta toiseen. [4.] Kuva 9 esittää tämän tyyppistä topologista ratkaisua.



Kuva 9. Site-to-Site VPN-yhteyden visualisointi kahden LAN-verkon välillä. [4]

3.5 Yleisimmät VPN-protokollat

VPN-toteutuksille on olemassa useita eri teknisiä vaihtoehtoja eli VPN-protokolia, joilla yhteyden muodostaminen ja salaus toteutetaan. Jotta yhteys voidaan muodostaa, pitää molempien tiedonsiirtopäiden tukea samaa protokolaa. [5.] Seuraavaksi käsitellään nykyään tyypillisimpiä käytössä olevia VPN-protokollia.

3.5.1 PPTP (Point to Point Tunneling Protocol) -protokolla

Point to Point Tunneling Protocol (PPTP) on yksi vanhimmista yhä käytössä olevista VPN-tunnelointiprotokollista. PPTP pohjautuu vanhempaan PPP-protokollaan ja sen on kehittänyt Microsoft Windos 95 -käyttöjärjestelmälle. PPTP on yksi helpommista VPN-tyypeistä konfiguraation kannalta. Se vaatii ainoastaan käyttäjätunnuksen, salasanan ja serverin IP-osoitteen muodostaakseen yhteyden palvelimelle. Vanhana protokollana PPTP:n salaus ei ole enää kovin luotettava, eikä sitä yleisesti pidetä enää turvallisena standardina. [8.]

3.5.2 L2TP/IPsec -tunnelointiprotokolla

L2TP:tä (Layer 2 Tunneling Protocol) käytetään yhdessä Internet Protocol Securityn (IPSec) kanssa PPTP:tä turvallisemman etäyhteyden luomiseksi. Data salataan ensin L2TP-standardilla ja kapsuloidaan sitten uudelleen IPSec-protokolla. L2TP/IPSec tarjoaa AES-256-bittisen salauksen, joka on turvallisuudeltaan yksi parhaista. [8.]

3.5.3 SSTP (Secure Socket Tunneling Protocol) -protokolla

Secure Socket Tunneling Protocol (SSTP) käyttää Secure Socket Layeria (SSL) tiedon siirtoon. SSTP on osa Microsoftin Windows-käyttöjärjestelmiä, mutta se on saatavilla myös Linuxille ja BSD:lle. [8.]

3.5.4 OpenVPN-protokolla

Yksi yleisimmistä VPN-protokollista on OpenVPN, joka on avoimen lähdekoodin tunnelointiprotokolla. Se käyttää AES-256-bittistä salausta datapakettien suojaamiseen. [8.] OpenVPN on saatavilla useimmille käyttöjärjestelmille, kuten Android, macOS, Linux, Windows ja iOS [9].

3.5.5 WireGuard

WireGuard on Jason A. Donenfeldin luoma avoimen lähdekoodin VPN-ratkaisu. Se kehitettiin alun perin Linux-pohjaiseksi, mutta on nykyään monialustainen ja siitä on saatavilla versiot myös Androidille, iOS:lle, BSD:hen, macOS:lle ja Windowsille. Se on yksinkertainen ja moderni VPN-ohjelmisto ja pyrkii korvaamaan yleisesti käytössä olevat IPsec- ja OpenVPN-protokollat. WireGuardin tavoitteena on olla turvallinen, kevyt ja helppo korvaava ratkaisu olemassa oleville vaihtoehdoille. [10.]

WireGuard perustuu Cryptokey routing -ratkaisuun, jonka perustana on julkinen salausavain ja sallittujen IP-osoitteiden lista, joiden perusteella sallitaan tunnelin liikenne. Autentikointiin käytetään ennalta jaettuja salausavaimia Curve25519-protokollalla. WireGuardin tunnelointiin käytetään salattuja UDP-paketteja ja data kapseloidaan ChaCha20Poly130-salauksella. Tämä mahdollistaa turvallisen ja nopean datansiirron. [10.]

Kilpailijoihinsa nähden WireGuard on erittäin kevyt ohjelmisto. Se on toteutettu Linuxille alle 4000 koodirivillä, mikä on alle prosentti IPseciin ja OpenVPN:ään koodeihin verrattuna. Tämä tekee ohjelmasta kevyen suorittaa sekä helpon tarkistaa ja todentaa, minkä vuoksi se on helpompi ylläpitää. Vähemmän koodia tarkoittaa myös vähemmän potentiaalista hyökkäyspintaa muihin protokoliin verrattuna. [10.]

Yksi WireGuardin merkittävistä suunnitteluedeista on se, ettei järjestelmä vastaa mitään tunnistamattomille saapuville paketeille. Tämä tarkoittaa sitä, että WireGuard on järjestelmänä näkymätön verkkoskannauksille ja ulkopuolisille yhteydenmuodostuksille. [10.]

WireGuard lisättiin osaksi virallista Linux-kerneliä 5.6-versiossa maaliskuussa 2020, ja se on tästä eteenpäin osa kaikkia Linux-julkaisuja. Vanhemmille Linux-versioille se on ladattavissa erikseen. [10.]

WireGuardin katsottiin vastaavan hyvin yrityksen tarpeita: se on kevyt eikä vaadi kovin suurta laskentatehoa, turvallinen, yksinkertainen käyttää ja avoimen lähdekoodin vaihtoehto. WireGuard itsessään on myös hyvin dokumentoitu, joten sen käyttöönoton oletettiin olevan melko yksinkertainen ja helposti hallittava prosessi. Myös WireGuardin liittäminen osaksi tulevia Linux-julkaisuja todettiin olevan positiivinen piirre ja todennäköisesti pidentävän ratkaisun elinkaarta. Tulevaisuudessa järjestelmää laajennettaessa saatetaan valita eri Linux-pohjaiset komponentin VPN-verkon päätelaitteiksi, mikä tarkoittaa, että WireGuard-tuki tulee olemaan niissä natiivi.

4 Yhteyden muodostamiseen käytettävät laitteet

Tämä luku esittelee projektissa käytettyjä laitteita. Käytettävä laitteisto pohjautuu enimmäkseen olemassa oleviin laitteisiin, joiden rinnalle hankittiin etäyhteyden päätelaitteiksi valikoituneita reitittimiä. Suunnittelussa pyrittiin hyödyntämään olemassa olevaa laitteistoa mahdollisimman tehokkaasti välttäen turhia hankintakuluja.

4.1 Etäyhteyden päätelaite

Etäyhteyden päätelaitteena kohteissa käytetään Ubiquitin EdgeRouterX-5-porttista reititintä. Reititin on Linux-pohjainen ja käytettävissä on sekä Secure Shell eli SSH-yhteys, että komentorivikäyttöliittymä (CLI), joten WireGuardin asentaminen sille on vaivatonta. SSH-yhteys mahdollistaa myös etäkirjautumisen reitittimeen, jolloin tietyt huoltotoimenpiteet voidaan suorittaa helpommin etänä. Reitittimen pieni koko, huomaamaton olemus ja metallinen rakenne tekee siitä helposti sijoitettavan kohteeseen. Lisäksi laite vaatii vähän virtaa ja on passiivijäähdytetty eli käytännössä äänetön. Laitteessa on Dual-Core 880 MHz:n prosessori ja 256 megatavua DDR3 RAM -muistia ja saman verran tallennustilaa. Nämä ominaisuudet riittävät hyvin WireGuardin tarpeisiin.

4.2 Modeemi kohteissa

Laitteiston verkkoyhteys toteutetaan olemassa olevilla Conelin 3G- ja 4G-modeemeilla, joihin aiempi OpenVPN-yhteys oli konfiguroitu. Osassa kohteita käytetään myös Teltonikan RUT240-4G-modeemia. Modeemeja varten on hankittu erillinen dataliittymä jokaiseen kohteeseen. Dataliittymien valinnassa on huomioitu erot paikallisessa kuuluvuudessa eri operaattoreiden välillä.

4.3 WireGuard-palvelin

WireGuard-yhteyden serverinä toimii yrityksen olemassa oleva Linux-pohjainen palvelin. Palvelimen käyttöjärjestelmänä on Ubuntu Server 18.04. Koska palvelinta käytetään aktiivisesti myös muihin tarkoituksiin, ei sen käyttöjärjestelmää lähdetty projektin myötä

päivittämään, jotta muut toiminnot eivät vaarannu. Koska käyttöjärjestelmä on vanhempaa kerneliä kuin 5.6-versio, ei WireGuard ole osa kokoonpanoa vaan se on asennettava erikseen.

4.4 Windows-laitteet

Yhteyden muodostus valvottaviin verkkoihin tapahtuu yrityksen käyttämiltä Windows-pohjaisilta työpisteiltä ja kannettavilta tietokoneilta WireGuardin Windows Client -sovellusta käyttäen. Jokaiselle työasemalle on luotu yksilölliset salausavaimet.

4.5 Linux-laitteet

Osaa kohteista valvotaan myös automaattisesti käyttäen Linux-järjestelmiä, esimerkiksi Zabbixia hyödyntäen. Näille laitteille on konfiguroitu WireGuard-yhteys hyvin samaan tapaan kuin päätelaitteille.

4.6 Muihin käyttöjärjestelmiin pohjautuvat laitteet

WireGuard tukee myös muita käyttöjärjestelmiä kuten Androidia ja macOS:ää. Näille käyttöjärjestelmille löytyy Windows Clientin kaltainen sovellus, jolla yhteyden muodostus onnistuu helposti. Yrityksen käytössä ei toistaiseksi ole tämän tyyppisiä laitteita, joilla olisi tarvetta ottaa yhteyttä kohteisiin, mutta tulevaisuutta ajatellen tämä mahdollisuus on myös merkittävä etu.

5 WireGuardin käyttöönotto

5.1 WireGuard-verkon rakenne

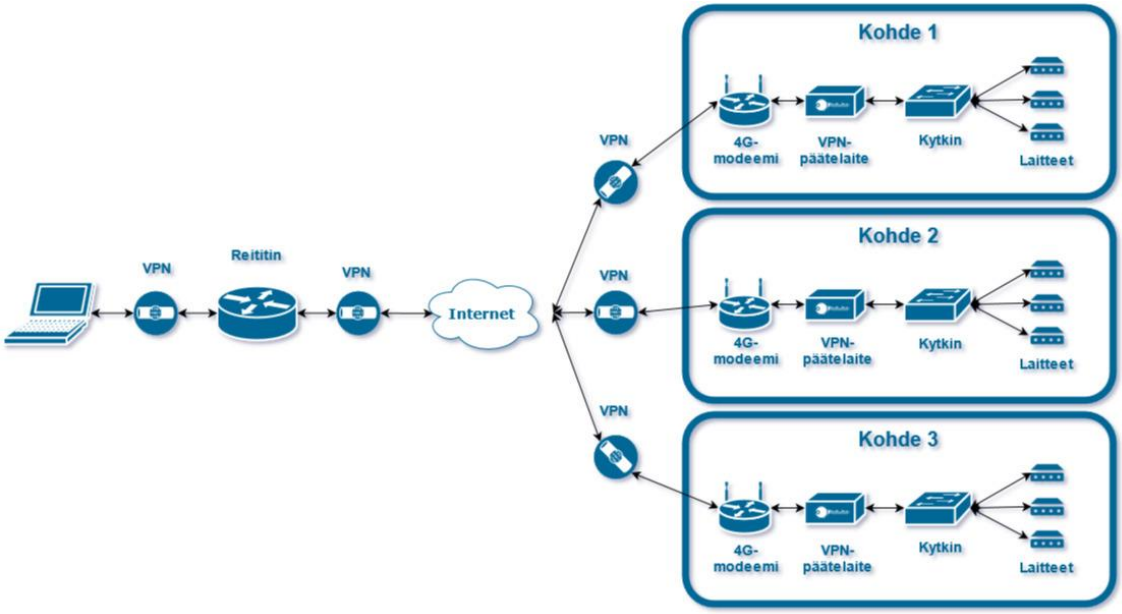
Tyypillisesti kohde, johon halutaan yhteys, on omassa lähiverkossaan. Tämä vaatii yhdyskäytävän julkisen verkon yli, mikä suoraan toteutettuna ei olisi turvallista. Tämän vuoksi yhteys muodostetaan salatun VPN-tunnelin yli.

Käytännössä kohteen sisäiseen lähiverkkoon tuodaan liittymäkohta julkiseen verkkoon. Tämä on usein 3G/4G/5G-modeemi. Modeemi tarjoaa yhteyden julkiseen verkkoon, mutta ongelmaksi muodostuu usein, sopimuksesta riippuen, vaihtuva eli dynaaminen IP-osoite, jolloin yhteyden saaminen kohteeseen menee monimutkaiseksi.

Lisäämällä verkkoon laitteen, joka toimii myös VPN:n päätepisteenä, voidaan muodostaa yhteys turvallisesti toimistoverkosta julkisenverkon yli kohteen lähiverkkoon. Oman VPN:n määrittäminen helpottaa myös dynaamisen IP-osoitteen ongelmaa, sillä tähän ratkaisuun tarvitaan vain yksi kiinteä IP-osoite VPN-verkon palvelinta varten. Kohteen päätelaitteella on oma VPN-pohjainen osoitteensa.

WireGuard-verkossa on VPN-palvelin, joka ylläpitää salattuja yhteyksiä ja ohjaa liikennettä. Jokainen VPN-pääte ottaa yhteyttä palvelimeen julkisen verkon yli palvelimen tunnetun IP-osoitteen perusteella. Palvelin ja päätelaite suorittavat kättelyn eli vaihtavat salausavaimia ja muodostavat välilleen salatun yhteyden. Näin palvelin saa tietoonsa myös päätelaitteen sen hetkisen IP-osoitteen. Sekä VPN-päätelaitteella että palvelimella on lista sallituista laitteiden IP-osoitteista, joiden välillä kommunikointi on mahdollista.

Ottaessa yhteyttä toimistoverkosta kohteen verkkoon, yhdistää toimiston tietokone liikenteen ensin palvelimeen, joka ohjaa liikenteen eteenpäin kohteen VPN-päätelaitteelle. Rakennettu verkko muistuttaa rakenteeltaan Host-to-Site-verkkoa sillä erotuksella, että yhteys muodostetaan yhdeltä laitteelta useamman kohteen lähiverkkoon samanaikaisesti. Teknisesti verkkorakenne on siis useampaan LAN-verkkoon haarautuva VPN-yhteys. Kuvassa 10 havainnollistaa tämän tyyppistä verkonrakennetta.



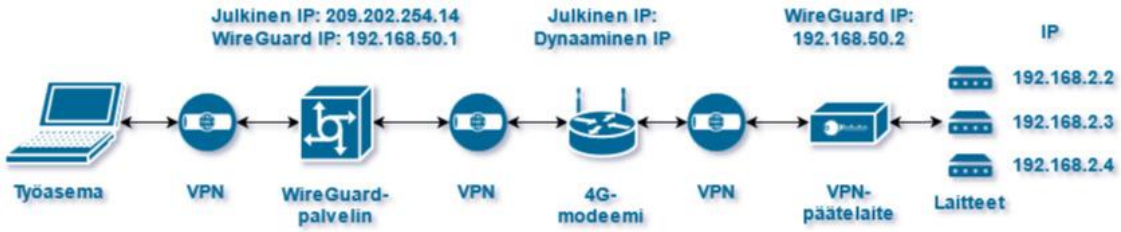
Kuva 10. Kaaviokuvaus haaroittuvasta WireGuard-verkon rakenteesta.

5.2 Kohteiden IP-osoitteet

Jokaiselle kohteelle on määritetty omat IP-osoitteet siten, että osoitteen alku on sama ja kolmas oktetti yksilöi kohteen LAN-verkon, ja se on kyseisessä WireGuard-verkossa uniikki. Tämä mahdollistaa yksilöllisen IP-osoitteen jokaiselle laitteelle samassa WireGuard-verkossa. Yksilölliset IP-osoitteet poistavat päällekkäisyyden riskiä, mikä helpottaa verkkoliikenteen reititystä ja ylläpitoa.

Tässä esimerkkiverkossamme WireGuard-palvelimen todellinen IP-osoite on 209.202.254.14 ja WireGuardin IP-osoite on 192.168.50.1. Kohteen 1 IP-osoite on dynaaminen eli muuttuva ja WireGuardin IP-osoite on 192.168.50.2. Kohteen 1 LAN-verkossa laitteiden IP-osoitteet määräytyvät WireGuardin kolmannen oktetin mukaan ja ovat esimerkiksi muotoa 192.168.2.2…192.168.2.20. IP-osoitteita havainnollistetaan tarkemmin kuvassa 11.

Kohteen 2 IP-osoitteet määräytyisivät samalla logiikalla: WireGuardin IP-osoite 192.168.50.3 ja laitteiden IP-osoitteet LAN-verkossa 192.168.3.2.…192.168.3.20. WireGuardin IP-osoitteen viimeinen oktetti on siis sama kuin kyseisen kohteen LAN-verkon IP-osoitteen kolmas oktetti.



Kuva 11. Esimerkki laitteiden IP-osoitteista kohteessa 1.

Esimerkki listaus IP-osoitteesta verkkorakenteessa:

- Palvelimen IP: 209.202.254.14
- Palvelimen WireGuard IP: 192.168.50.1
- Kohteen 1 WireGuard IP: 192.168.50.2
- Kohteen 2 WireGuard IP: 192.168.50.3
- Kohteen 3 WireGuard IP: 192.168.50.4
- Kohteen 1 LAN-verkon IP:t: 192.168.2.2…192.168.2.20
- Kohteen 2 LAN-verkon IP:t: 192.168.3.2…192.168.3.20
- Kohteen 3 LAN-verkon IP:t: 192.168.4.2…192.168.4.20.

5.3 WireGuardin testaus

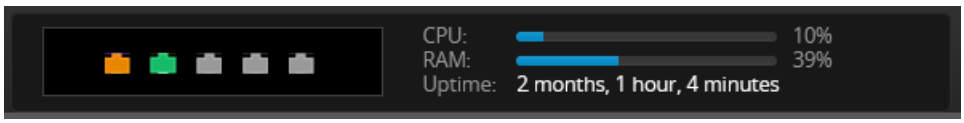
Ennen uuden VPN-yhteyden käyttöönottoa WireGuard-protokolla haluttiin testata, jotta voitiin varmistua sen soveltuvuudesta yrityksen käyttöön. Testaus aloitettiin asentamalla WireGuard yrityksen käytössä olleelle palvelimelle ja yksittäiselle laitteelle, joiden välille muodostettiin testiyhteys. Samalla tutustuttiin WireGuardin konfigurointiin ja käyttöönottoon.

5.3.1 Raspberry Pi 3 yhden piirilevyn tietokone

Ensimmäinen WireGuardin testaus suoritettiin Raspberry Pi 3 yhden piirilevyn tietokoneella, jonka käyttöjärjestelmänä toimi Linux-pohjainen Raspbian-käyttöjärjestelmä. Yhteys muodostettiin toimiston Ubuntu-palvelimen ja Raspberryn välille ensin samassa lähiverkossa, sitten 4G-modeemin avulla internetin yli. Kun VPN-yhteys oli toimisto-olosuhteissa todettu toimivaksi, siirrettiin Raspberry oikeaan kohteeseen testikäyttöön olemassa olevan OpenVPN-yhteyden rinnalle. Raspberry Pi -tietokoneita olisi voinut käyttää hyvin yhteyden toteuttamiseen, mutta tilalle haluttiin yksinkertaisempi ja mahdollisesti edullisempi laite.

5.3.2 Ubiquiti EdgeRouter X -reititin

WireGuard-järjestelmän osoittauduttua yrityksen käyttöön soveltuvaksi, selvitettiin sen asennusmahdollisuutta muille laitteille. Ubiquitin EdgeRouter X valikoitui käyttöön pääasiassa hinnan, pienen koon ja soveltuvan käyttöliittymän sekä WireGuard-yhteensopivuuden pohjalta. Tälle laitteelle suoritettiin samat testit kuin Raspberrylle. Testauksen aikana kokeiltiin laitteen luotettavuutta, ohjelmiston automaattista käynnistymistä laitteen uudelleen käynnistyksen ja mahdollisten virtakatkosten jälkeen, WireGuard-yhteyden palautumista verkkoyhteys katkoksen jälkeen sekä laitteen prosessorin rasitusta WireGuard-yhteyttä käytettäessä. WireGuard-yhteyden ollessa käytössä käyttää EdgeRouter X:n prosessorin laskentatehosta keskimäärin 10 % ja ram-muistista noin 40 %, kuten kuvasta 12 näkyy, minkä perusteella laitteen tekninen suorituskyky voitiin todeta riittäväksi tähän käyttötarkoitukseen. Aluksi luotiin kohdetta vastaava lähiverkko toimistolle, johon otettiin yhteyttä 4G-modeemin yli. Kun yhteys todettiin toimivaksi, testattiin tätä myös kohteessa OpenVPN:n rinnalla. Yhteensopivuuden varmistuttua ratkaisua alettiin monistamaan myös muihin kohteisiin.



Kuva 12. EdgeRouter X:n resurssien käyttö WireGuard-yhteyden ollessa käytössä.

5.4 WireGuardin asennus

Tässä luvussa kuvataan esimerkkimuotoinen asennus WireGuardista, jossa IP:t ja salausavaimet on turvallisuuden vuoksi muutettu. IP-osoitteina käytetään edellä kuvattuja IP-osoitteita vastaavalla tavalla. Tarkoituksena on demonstroida käytäntöä mahdollisimman tarkassa ja ymmärrettävässä muodossa. Kuvaus toimii myös dokumentaationa laitteiden konfiguroinnille WireGuard-yhteyttä varten.

5.4.1 WireGuardin asentaminen Ubuntu-palvelimelle

Asennus aloitetaan kirjautumalla palvelimelle joko root-tunnuksin tai suorittamalla komennot sudo-kehoitteella, kuten tässä esimerkissä. Koska käytetty Linux-versio on vanhempi eikä sisällä suoraan WireGuardia, aloitetaan asennus päivittämällä asennustietokanta ja asentamalla WireGuard komennoilla:

```
sudo apt update
sudo apt install wireguard
```

Luodaan palvelimen yksityinen ja julkinen salausavain komennolla:

```
wg genkey | sudo tee /etc/wireguard/privatekey | wg pubkey | sudo tee
/etc/wireguard/publickey
```

Saadut avaimet ovat alla. Ensimmäinen on yksityinen avain ja seuraava julkinen. Saadut avaimet otetaan talteen myöhempää käyttöä varten.

```
eBqc+wSftjb7i4HdjaPCk40yuYXkDWPJFuPCmix5I3k=
9OriDsmtswKUvOBPpH/gl/AWclkXBNTalbfXxvkJGg0=
```

Luodaan WireGuard-rajapinta verkkosovittimelle ja määritetään palvelimen WireGuard IP-osoite ja yksityinen salaus avain alla olevilla komennoilla. Lopuksi käynnistetään WireGuard-rajapinta:

```
ip link add wg0 type wireguard
ip addr add 192.168.4.1/24 dev wg0
wg set wg0 private-key eBqc+wSftjb7i4HdjaPCk40yuYXkDWPJFuPCmix5I3k=
ip link set wg0 up
```

Avataan konfigurointitiedosto asetusten määrittämistä varten käyttäen nano-tiedostoeditoria:

```
sudo nano /etc/wireguard/wg0.conf
```

Konfigurointitiedosto on mallia:

```
[Interface]
PrivateKey = eBqc+wSftjb7i4HdjaPCk40yuYXkDWPJFuPCmix5I3k=
Address = 192.168.50.1
ListenPort =8172
Table = auto
MTU = 1300

[Peer]
PublicKey =
Allowed IPs =
```

Konfiguraatiotiedostossa määritetään palvelimen yksityinen salausavain (PrivateKey), wireguard-osoite (192.168.50.1), käytettävä UDP-portti (8172) sekä ensimmäinen päätelaite (Peer). Päätelaitteesta on määritetty tämän julkinen salausavain (PublicKey) ja sallittujen IP-osoitteiden lista. Tässä tapauksessa sallittuja osoitteita ovat päätelaitteen WireGuard-IP (192.168.50.2), jonka perässä oleva /32-merkintä viittaa käytettävään verkkomaskiin. Tämän lisäksi sallituiksi IP-osoitteiksi on määritelty kohteen lähiverkon IP-osoitteet, jotta yhdistäminen suoraan yksittäiseen laitteeseen onnistuisi.

5.4.2 WireGuardin asentaminen Edgerouter X:lle

EdgeRouter X:n asennus aloitetaan kytkeytymällä kiinni laitteeseen ja kirjautumalla laitteen graafiseen käyttöliittymään verkkoselainta käyttäen. Käyttöliittymässä määritetään laitteelle uudet käyttäjät, salasanat ja kiinteät IP-osoitteet.

Tämän jälkeen asennusta jatketaan komentorivikäyttöliittymässä, johon päästään ottamalla SSH-yhteys esimerkiksi Puttyä käyttäen. Sisäänkirjautumisen jälkeen vaihdetaan root-käyttäjän salasana komennolla:

```
sudo passwd
```

Tämän jälkeen kirjaudutaan sisään root:ina ja siirrytään väliaikaiskansioon tmp:

```
su -
cd /tmp
```

Ladataan WireGuard-ohjelmisto komennolla:

```
curl -qLs https://github.com/Lochnair/vyatta-wireguard/releases/down-
load/0.0.20180802-1/wireguard-e50-0.0.20180802-1.deb -o wireguard.deb
```

Komento lataa WireGuardin asennuspaketin. Se on olennaista, koska Edgerouter X:n käyttämä ohjelmistoversio ei vielä sisällä WireGuard-ohjelmistoa. Tämän jälkeen ohjelmisto puretaan ja asennetaan komennolla:

```
dpkg -i wireguard.deb
```

Ohjelmiston asentaminen vie noin minuutin, jonka jälkeen luodaan päätelaitteelle sen omat yksityinen ja julkinen salausavain komennolla:

```
wg genkey | tee /dev/tty | wg pubkey
```

Saadut avaimet ovat esimerkiksi muotoa:

```
4OgcIKIE1fNFijdS+VW8o7Oo9du/bYygcrBBkHWAX1c=
WlToJEYK3iZVCshiPhCFOnT2TWebwmteKvYIE+A00FY=
```

Jossa ylempi on yksityinen avain ja alempi julkinen avain.

Kun avaimet on luotu, ne kopioidaan talteen myöhempää käyttöä varten ja siirrytään konfiguroimaan päätteen WireGuard-asetuksia. Rajapinnan asetuksiin pääsee komennolla:

```
configure
```

Päätelaitteen WireGuard-osoite määritellään komennolla:

```
set interfaces wireguard wg0 address 192.168.50.2/24
```

Tämä määrittää laitteen WireGuard-osoitteeksi 192.168.50.2, jonka verkkomaski on ”/24”, eli 255.255.255.0. Osoitteen tulee olla yksilöllinen kyseisessä WireGuard-verkossa. Tämän jälkeen määritellään kyseisen rajapinnan yksityinen salausavain komennolla, jossa käytetään edellä luotua salausavainta:

```
set interfaces wireguard wg0 private-key 4Og-
cIKIE1fNFijdS+VW8o7Oo9du/bYygcrBBkHWAX1c=
```

Määritetään päätelaitteelle WireGuard-palvelimen todellinen IP-osoite ja UDP-portti, jota käytetään. Näin päätelaite osaa ottaa yhteyden oikeaan IP-osoitteeseen yhteyttä muodostaessa. Tässä Ip-osoite on muodossa 209.202.254.14 ja UDP-portti 8172. Salausavaimena käytetään palvelimen julkista salausavainta:

```
set interfaces wireguard wg0 peer 9OriDsmtswKUvOBPpH/gl/AWclkXBNTalbfXxvkJGg0=
endpoint 209.202.254.14:8172
```

Lisätään allowed-IPs-listalle ne osoitteet, joista liikenne sallitaan tämän tunnelin läpi:

```
set interfaces wireguard wg0 peer 9OriDsmtswKUvOBPpH/gl/AWclkXBNTalbfXxvkJGg0=
allowed-ips 192.168.2.0/24
```

Lisätään komento, joka pitää yhteyden aktiivisena, vaikka liikennettä ei olisikaan:

```
set interfaces wireguard wg0 peer 9OriDsmtswKUvOBPpH/gl/AWclkXBNTalbfXxvkJGg0=
persistent-keepalive 25
```

Hyväksytään sekä otetaan käyttöön rajapinnalle tehdyt muutokset ja tallennetaan ne. Tämän jälkeen poistutaan configure-tilasta komennoilla:

```
commit
save
exit
```

5.4.3 Uuden Peerin lisääminen palvelimelle

Kirjaudutaan palvelimelle ja avataan WireGuardin konfiguraatiotiedosto komennolla:

```
sudo nano /etc/wireguard/wg0.conf
```

Lisätään uusi päätelaite (Peer) konfiguraatiotiedostoon muodossa:

```
[Peer]
PublicKey = WlToJEYK3iZVCshiPhCFOnT2TWebwmteKvYIE+A00FY=
AllowedIPs = 192.168.50.2/32, 192.168.2.0/24
```

Tallennetaan ja suljetaan tiedosto ja käynnistetään WireGuard-rajapinta palvelimella uudelleen komennolla:

```
systemctl restart wg-quick@wg0
```

Yhteyksien muodostuminen vie uudelleen käynnistyksen jälkeen noin minuutin. Yhteyden voi testata lähettämällä ping-pyynnön WireGuard-päätteeltä palvelimelle.

```
ping 192.168.50.1
```

5.4.4 WireGuard-clientin asennus Windows-koneelle

WireGuardin sovellus Windowsille on ladattavissa osoitteesta https://www.wireguard.com/install/. WireGuard asennetaan suorittamalla wireguard-installer.exe. Käyttöliittymä on itsessään hyvin yksinkertainen eikä vaadi paljon asetuksia. Ainoa varsinainen vaadittava asetus on tunnelin konfiguraatio, joka ei juurikaan eroa palvelimen konfiguroinnista ja on muotoa:

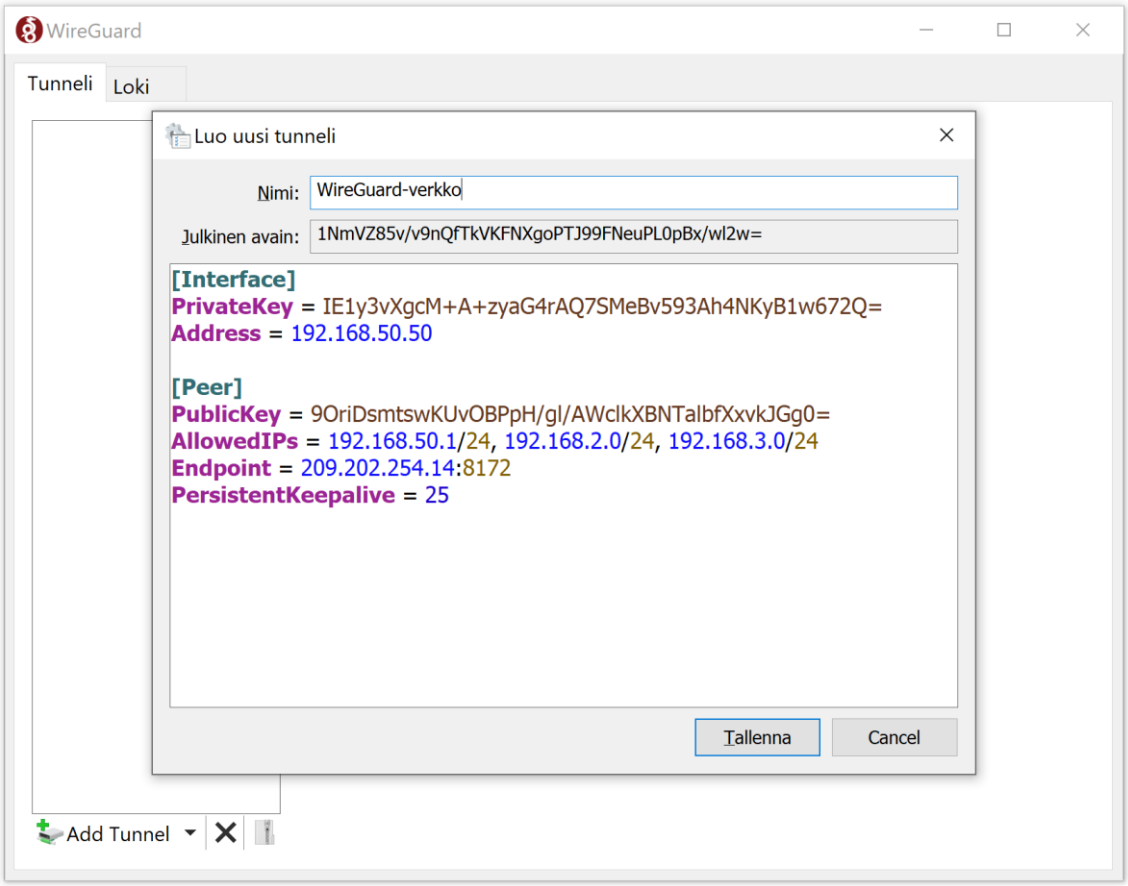
```
[Interface]
PrivateKey = IE1y3vXgcM+A+zyaG4rAQ7SMeBv593Ah4NKyB1w672Q=
Address = 192.168.50.50

[Peer]
PublicKey = 9OriDsmtswKUvOBPpH/gl/AWclkXBNTalbfXxvkJGg0=
AllowedIPs = 192.168.50.1/24, 192.168.2.0/24, 192.168.3.0/24
Endpoint = 209.202.254.14:8172
PersistentKeepalive = 25
```

Windows-client on hyvin pelkistetty ja selkeä käyttää. Kuvassa 13 näkyy tarkemmin tunnelin konfigurointi kyseistä ohjelmaa käyttäen.

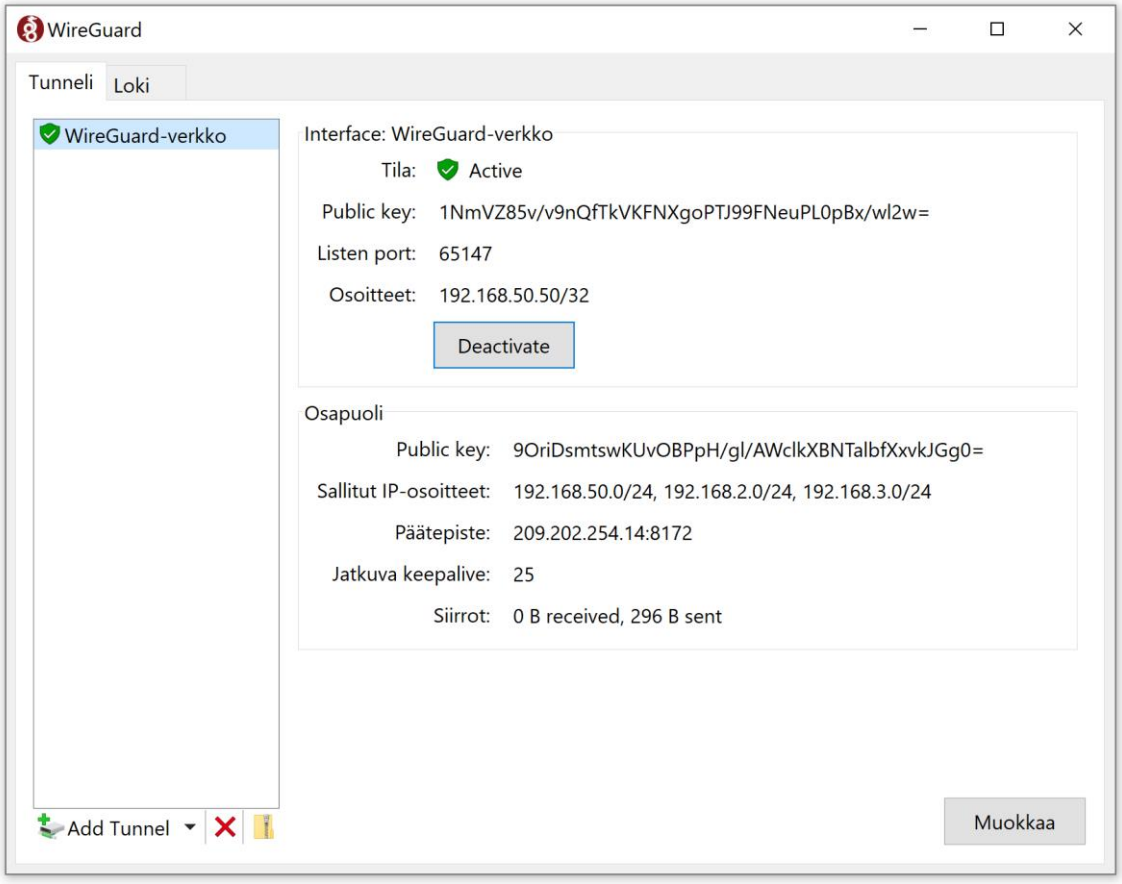
Syöttämällä yksityisen avaimen ohjelma laskee automaattisesti julkisen avaimen yhteydelle. Tämän muotoinen konfiguraatio ohjaa sallittujen IP-osoitteiden liikenteen tunnelin läpi. Muu liikenne tietokoneelta kulkee sen standardireittiä. Jos kaikki liikenne halutaan ohjata tunnelin läpi, on se mahdollista lisäämällä AllowedIPs listalle ”0.0.0.0/1” ja muu liikenne voidaan estää tämän jälkeen valitsemalla ”Block untunneled traffic (kill-switch)”.

Huomioitavaa on, että AllowedIPs-listaan tulee listata kaikkien niiden lähiverkkojen IP-osoitteet, joihin työpäätteeltä halutaan olla yhteydessä.



Kuva 13. WireGuardin Windows-client ja tunnelin konfiguraatio.

Varsinainen yhteyden muodostus on helppoa ja nopeaa. Valitaan sovelluksesta tunneli eli VPN-verkko, johon halutaan olla yhteydessä. Valitaan yhdistä, ja sovellus luo suojatun yhteyden muutamissa sekunneissa ja ohjaa AlloweIPs-listan osoitteet tunnelin läpi. Aktivoitu tunneli näkyy kuvassa 14.



Kuva 14. Aktivoivu WireGuard-tunneli

5.5 Yhteyden testaus kohteissa

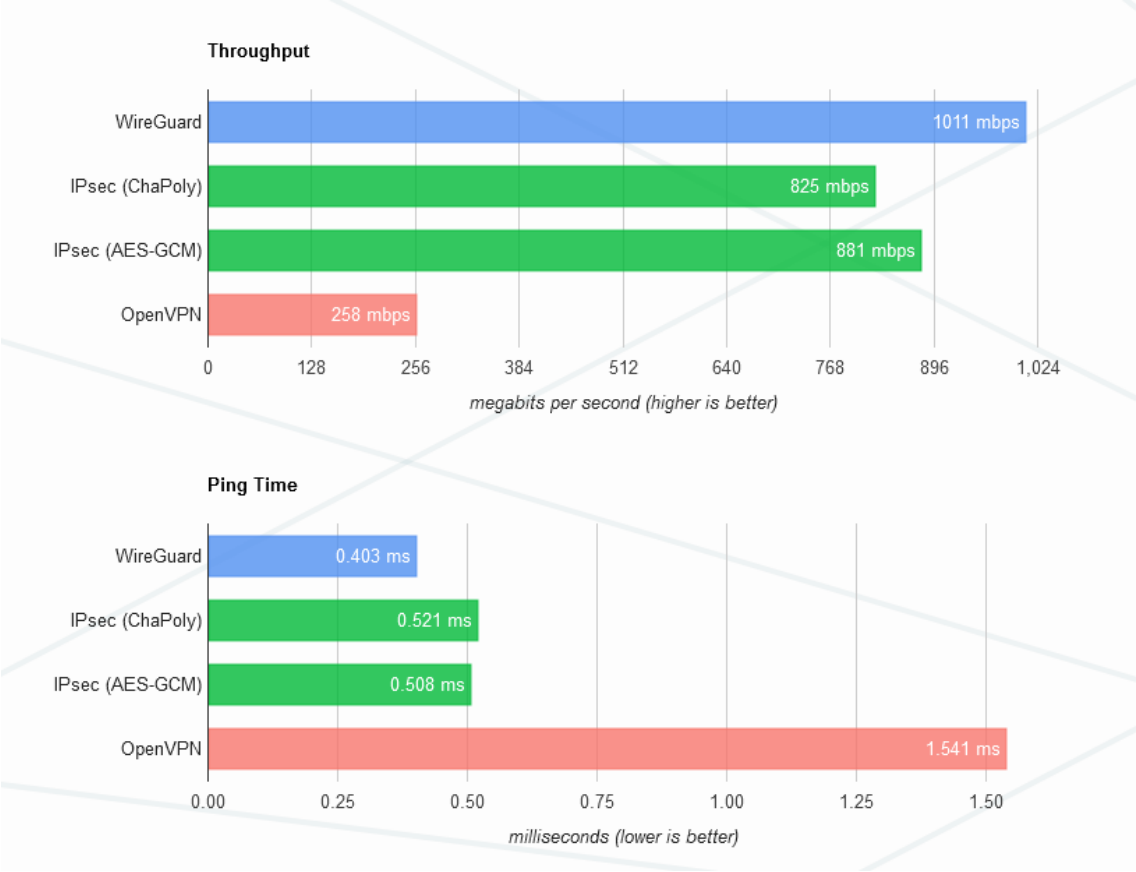
Yhteyden toimivuus voidaan nopeasti todentaa ensin ping-kyselyllä kohteeseen. Ensin kysely lähetetään WireGuardin päätelaitteelle, ja kun tältä saadaan vastaus, voidaan kysely lähettää myös kohteen lähiverkossa olevalle laitteelle. Yhteyden toimivuutta voidaan todentaa myös ottamalla etäyhteys kohteen lähiverkossa olevaan laitteeseen.

5.5.1 WireGuard-verkon nopeus

Valmistajan omien testausten mukaan WireGuard on IPsec- ja OpenVPN-yhteyksiä nopeampi ja sen viive on lyhyempi. Testitulokset ovat luettavissa kuvasta 15. Testaus suoritettiin seuraavalla laitteistolla.

- Intel Core i7-3820QM ja Intel Core i7-5200U
- Intel 82579LM ja Intel I218LM gigabit -verkkokortit
- Linux 4.6.1 -käyttöjärjestelmä.

Valmistajan oman lausunnon mukaan testi on kohtalaisen vanha ja WireGuardin nykyinen versio on suoritustasoltaan mittauksia parempi. [11.]



Kuva 15. Nopeusvertailu WireGuardin omien testien mukaan. [11]

Nopeusero oli havaittavissa myös konkreettisesti yrityksen käytössä. Etäyhteydet ovat nopeammat WireGuardin kuin OpenVPN:n yli, ja se näkyy käytännössä sujuvampana etäkäyttönä ja nopeampina latausaikoina. Kohteiden tiedot saadaan luettua nopeammin ja tehokkaammin, ja parhaimmillaan latausajat lähes puolittuivat käytössä.

5.5.2 WireGuard-verkon luotettavuus

Testikäytön aikana uudet yhteydet ovat toimineet hyvin, eikä merkittäviä häiriöitä ole ilmennyt. Kohdatut ongelmat ovat olleet yksittäisiä laiteongelmia, eivätkä niinkään WireGuardista johtuvia virhetiloja. Uutena piirteenä on mainittava yrityksen VPN-verkkojen riippuvuus palvelimen internetyhteydestä, siinä missä edeltävä OpenVPN-verkko oli riippuvainen palveluntarjoajasta. Tämä saattaa nykyisessä muodossaan aiheuttaa käyttökatkoksia tulevaisuudessa, mikäli WireGuard-palvelimen verkkoyhteys katkeaa. Tämän tyyppiset katkokset ovat harvinaisia mutta mahdollisia. Tämä on asia, joka kannattaa selvittää, ja pyrkiä kehittämään ratkaisu tilanteen välttämiseksi tulevaisuudessa.

5.5.3 Käyttöönoton yhteydessä ilmenneet ongelmat

WireGuard-verkkoa rakennettaessa vastaan tulleet ongelmat eivät liittyneet suoranaisesti itse VPN-yhteyden käyttöön tai ominaisuuksiin. Merkittävimpiä haasteita useasta verkosta ja kohteiden määrästä johtuen oli päällekkäisten IP-osoitteiden välttäminen ja liikenteen reitittäminen. Tässä työssä IP-osoitteet suunniteltiin huolellisesti etukäteen, joten päällekkäisyysongelmia ei ilmennyt tarkkaan harkituista valmistelutöistä johtuen. Sen sijaa reitityksen kanssa ilmeni useammin ongelmia. Tyypillisessä ongelmatilanteessa yhteys saatiin toimimaan palvelimen ja päätelaitteen välillä heti, mutta etäyhteyttä varsinaisille laitteille kohteessa ei kyetty muodostamaan. Tämä ongelma liittyi tyypillisesti paluuliikenteeseen ja tietoliikenteen reititysvirheisiin kohteen päässä. Asia ratkaistiin testaamalla yhteyksien toimintaa vaihe vaiheelta ping-pyynnöillä. Tarpeen vaatiessa voitiin käyttää myös traceroute-komentoa, jonka avulla saatettiin joissain tilanteissa määrittää ongelmakohtia. Kun potentiaalinen ongelmakohta oli kartoitettu, alettiin selvittää reititystä. Yleisimpiä virheitä oli väärä tai puuttuva yhdyskäytävä laitteella tai jossain verkon solmukohdassa.

6 Projektin tuotos ja saavutetut hyödyt yritykselle

Projektin tuloksena uudistettiin yrityksen VPN-järjestelmät ja korvattiin olemassa oleva OpenVPN-yhteys omalla WireGuard-pohjaisella ratkaisulla. Projektin myötä otettiin käyttöön neljä toisistaan erillistä WireGuard-verkkoa, joissa on yhteensä yli 40 VPN-päätelaitetta ja yhtä monta valvottavaa kohdetta. Lisäksi luotiin dokumentaatio käytettävien laitteiden konfiguroinnista ja yhteyden muodostamisesta. Projektin lopuksi testattiin järjestelmän toimivuutta ja luovuttiin aiemmasta VPN-ratkaisusta. Tämän lisäksi projektin yhteydessä opinnäytetyön ulkopuolella luotiin kaikkiin kohteisiin myös toiseen teknologiaan perustuva varayhteys, mikä mahdollistaa huoltoyhteyden WireGuard-verkon rinnalla ja turvaa verkkokokonaisuuden toimintaa myös häiriötilanteissa.

Yritys kykeni projektin myötä korvaamaan käytössään olleen maksullisen VPN-palvelun täysin omalla WireGuard-pohjaisella VPN-ratkaisulla. Oman VPN-yhteyden käyttöönoton hyödyt ovat yritykselle taloudellisia ja lisäävät kokonaisuuden hallittavuutta ja tehokkuutta.

Yritys säästää taloudellisesti voidessaan luopua kuukausimaksullisesta palvelusta. Lisäksi ostetussa palvelussa kuluja syntyi myös muun muassa uusien kohteiden lisäämisestä ja mahdollisista IP-muutoksista. Oman VPN-yhteyden myötä ainoat kulut näissä tilanteissa ovat edulliset laitekulut, kun uusia kohteita lisätään verkkoon, sekä työtunnit muutosten osalta.

Yrityksen kannalta merkittäviin etuihin kuuluu myös etäyhteyden hallinnoinnin siirtyminen omaan kontrolliin. Käytännössä tämä merkitsee nopeampia reaktio- ja muutosaikoja yhteyden suhteen uusia kohteita lisättäessä, muutoksia tehdessä tai vikoja korjatessa. Mahdollisesti hajonneen yhteyspäätteen korvaaminen uudella tai salausavaimien vaihtaminen voidaan toteuttaa itse eikä tähän tarvita ulkopuolista tekijää.

7 Yhteenveto

Tämän insinöörityön tavoitteena oli kartoittaa kohdeyritykselle vaihtoehtoisia tietoliikenneratkaisuja käytössä olevan, maksullisena palveluna hankitun VPN-yhteyden korvaamiseksi. Tuotoksena insinöörityössä toteutettiin yritykselle oma VPN-yhteys ja luotiin suunnitelma kohteissa käytettävistä IP-osoitteista. Korvaavaksi vaihtoehdoksi valikoitui oman WireGuard-verkon käyttöönotto, joka on edullinen, kevyt ja helposti muokattava ja siksi loistava vaihtoehto yrityksen käyttöön.

Opinnäytetyössä toteutetut WireGuard-verkot mahdollistivat yrityksen siirtymisen maksullisesta VPN-palvelusta itse hallittavaan ratkaisuun. Omat WireGuard-pohjaiset VPN-yhteydet ovat sekä nopeampi kuin edeltäjänsä että paremmin hallittavissa. Luotua dokumentaatiota WireGuardin käyttöönotosta voidaan hyödyntää tulevaisuudessa yrityksessä verkkoja laajennettaessa. Myös yrityksen ulkopuoliset voivat hyödyntää dokumentaatiota esimerkkinä salatun verkkoyhteyden luomiseksi.

Tulevaisuuden kehittämisprojektiksi voitaisiin toteuttaa WireGuard-palvelimen varmentaminen. Tällä hetkellä WireGuard-verkko on yhden palvelimen toiminnan varassa ja palvelimen kaatuessa tai menettäessä internetyhteyden koko WireGuard-verkko lakkaa toimimasta. Tähän ratkaisuksi olisi esimerkiksi palvelimen kahdentaminen kahdelle fyysisesti eri laitteelle käyttäen virtuaalista IP-osoitetta kahden eri verkkoyhteyden yli.

Lähteet

1 Virtual Private Networking: An Overview. Verkkoaineisto. Microsoft Co. < https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742566(v=technet.10)>. 9.12.2009. Luettu: 10.2.2021.

2 What Is a VPN? - Virtual Private Network. Verkkoaineisto. Cisco Systems. < https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>. Luettu: 12.2.2021.

3 Casad, Joe. 2017. Sams Teach Yourself TCP/IP in 24 Hours. Sams.

4 Rao, Umesh Hodeghatta & Nayak, Umesha. 2014. The InfoSec Handbook. New York: Apress Media LLC.

5 Kerrigan Saoirse. 2018. Virtual Private Networks: How They Work And Why You Might Need One. Verkkoaineisto. <https://interestingengineering.com/virtual-private-networks-how-they-work-and-why-you-might-need-one>. Luettu: 1.3.2021.

6 Cisco Networking Academy. 2020. Enterprise Networking, Security, and Automation Companion Guide (CCNAv7). Cisco Press.

7 Cryptographic_Hash_Function. Verkkoaineisto. https://en.wikipedia.org/wiki/Cryptographic_hash_function. Luettu: 2.3.2021.

8 Athow, Desire. 2020. VPN Tunnels explained: what are they and how can they keep your internet data secure. Verkkoaineisto. Techradar. < https://www.techradar.com/vpn/vpn-tunnels-explained-how-to-keep-your-internet-data-secure>. Luettu: 15.3.2021.

9 OpenVPN. Verkkoaineisto. <https://openvpn.net/>. Luettu: 7.4.2021

10 Donenfeld, Jason. 2020. WireGuard: Next Generation Kernel Network Tunnel. Verkkoaineisto. < https://www.wireguard.com/papers/wireguard.pdf>. 1.6.2020. Luettu: 11.2.2021.

11 Performance. Verkkoaineisto. <https://www.wireguard.com/performance/>. Luettu: 2.3.2021.