SAVONIA

OPINNÄYTETYÖ - AMMATTIKORKEAKOULUTUTKINTO
TEKNIIKAN JA LIIKENTEEN ALA

MIKROYRITYKSEN KÄYTTÖÖN SOVELTUVA VPN-RATKAISU

TEKIJÄ/T: Eeli Pirinen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma	
Työn tekijä(t) Eeli Pirinen	
Työn nimi Mikroyrityksen käyttöön soveltuva VPN-ratkaisu	
Päiväys 11.6.2021	Sivumäärä/Liitteet 24
Toimeksiantaja/Yhteistyökumppani(t) Tietotekniikka Pirinen	

Tiivistelmä

Opinnäytetyön tavoitteena oli toteuttaa VPN-ratkaisu, joka soveltuu mikroyrityksen käyttöön. Oleellisena osana toteutuksessa oli helppokäyttöisyys, turvallisuus sekä kustannustehokkuus. VPN-yhteyden avulla saadaan käytettyä yrityksen sisäverkossa sijaitsevia resursseja myös ulkoverkosta käsin sekä suojattua oma tietoliikenne.

Teoriaosiossa tutustutaan VPN-tekniikkaan, yleisimpiin tunnelointi- ja salausprotokolliin sekä avoimen lähdekoodin ohjelmapohjaisiin toteutuksiin. Toteutus osiossa käydään läpi WireGuard palvelinohjelmiston asennuksen vaiheet, päätelaitteen ohjelmiston toiminta, sekä muut tarvittavat vaiheet tietoliikenteen reitittämiseksi ulkoverkkoon. Lopuksi valmista toteutusta testattiin nopeustestillä sekä tutkittiin tietoliikennettä tietoturvan näkökulmasta.

Opinnäytetyön tuloksena saatiin toimiva VPN-ratkaisu. Nopeustestissä huomattiin lataus- ja lähetysnopeuden puolittuvan sekä verkon viive kaksinkertaistui. Vaikka yhteys heikentyi, oli käytettävyys edelleen kohtuullisella tasolla. Testauksessa tutkittiin myös tietoturvan näkökulmaa ja siinä ilmeni, että VPN-tunnelin sisällä kulkevat IP-paketit ovat salattuja ja niitä ei saa purettua kuin siihen tarkoitetulla salausavaimella.

Avainsanat

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Information Technology	
Author(s) Eeli Pirinen	
Title of Thesis VPN Solution Suitable for Use by Micro-Enterprise	
Date 11 June 2021	Pages/Appendices 24
Client Organisation /Partners Tietotekniikka Pirinen	

Abstract

The purpose of this thesis was to implement VPN solution that is suitable for a micro-enterprise. Ease of use and cost efficiency were an essential part of the implementation. With a VPN connection user get an access the company's resources located in the internal network from public network and VPN protects communication.

For the theory section VPN technology, the most common tunneling and encryption protocols and open-source program-based implementations were studied. In the implementation section server software installation steps, operation on the device to which the connection is made and other steps required to route communications to the public network are taken. The finished implementation was tested with a speed test and communication was studied from the security perspective.

The result of the thesis was a working VPN solution. In the speed test, it was found that the download and upload speed halved, and network latency doubled. Although the connection deteriorated, usability was still at a reasonable level. The testing also examined the security aspect and revealed that inside the VPN tunnel passing IP packets are encrypted and may only be decrypted with the encryption key provided.

Keywords

SISÄLTÖ

KUVALUETTELO

1 JOHDANTO

Tämän opinnäytetyön tavoitteena on luoda mikroyrityksen käyttöön soveltuva VPN-ratkaisu. VPN-yhteyden avulla päästään yrityksen sisäverkon resursseihin myös muista verkoista, sekä saadaan suojattua oma tietoliikenne julkisia verkkoja käytettäessä. Palvelun tavoitteena on olla helppokäyttöinen, turvallinen sekä kustannustehokas. Työn tarkoituksena on tutustua VPN-tekniikkaan, mitä VPN on ja mihin sitä käytetään. Työssä tutustutaan erilaisiin tunnelointi- ja salausprotokolliin, joita VPN-yhteyksissä käytetään, sekä avoimen lähdekoodin VPN-ohjelmistoihin. Työssä käydään läpi myös toteutuksessa käytettävä laite, sekä sen toimintaa ja muita malleja yleisellä tasolla.

Opinnäytetyössä toteutetaan WireGuard VPN-palvelin Raspberry Pi tietokoneelle. Raspberri Pi:lle on asennettuna Raspberry Pi OS käyttöjärjestelmä. Työssä näytetään asennuksen vaiheet ja työkalut, jotta VPN-ohjelmisto saadaan toimimaan palvelimena sekä päätelaitteelle asennettava ohjelma, jonka avulla VPN-yhteys saadaan muodostettua päätelaitteen ja palvelimen välille. Valmista toteutusta testataan nopeustestillä sekä tutkitaan VPN-yhteyden tietoturvaa. Nopeustesti suoritetaan viidesti, josta lasketaan keskiarvo lataus- ja lähetysnopeudelle sekä viiveelle. Tietoturvaa tutkitaan Wireshark pakettianalysaattorilla, jossa verrataan kirjautumistietojen näkyvyyttä suojaamattomassa http-yhteydessä sekä WireGuard VPN-yhteydessä.

2 VPN

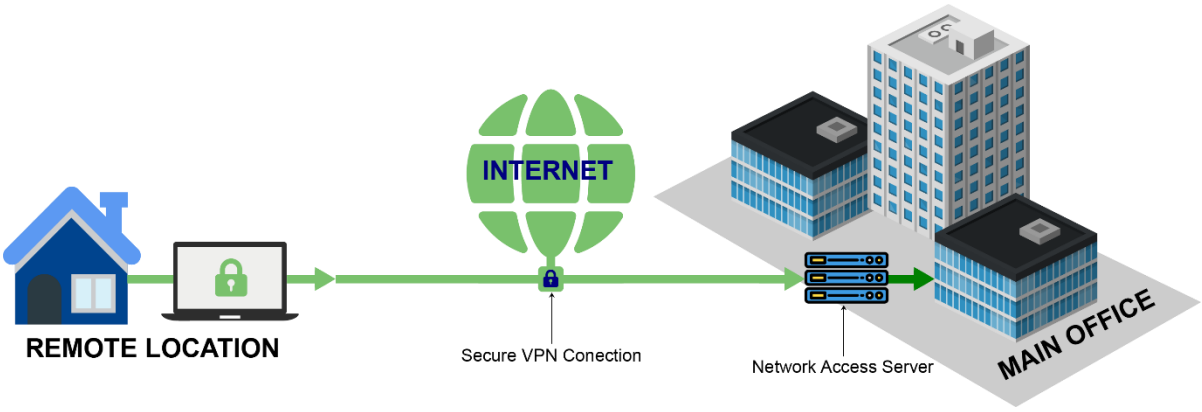
2.1 VPN-tekniikka

VPN eli virtuaalinen erillisverkko mahdollistaa salatun verkkoyhteyden muodostamisen julkisen verkon kautta kahden yksityisen verkon välille. VPN salaa laitteiden välisen verkkoliikenteen reaaliaikaisesti. VPN piilottaa IP-osoitteen ja käyttäjän tiedot ohjaamalla laitteelta tulevan tietoliikenteen suoraan VPN-palvelimeen ja sieltä ulkoverkkoon. Tämä tarkoittaa sitä, että verkkoa käyttäessä tietojen lähde on päätelaitteen sijaan VPN-palvelin. Tiedon salaus mahdollistaa sen, että internet palveluntarjoaja sekä muut kolmannen osapuolen palvelut eivät voi tarkkailla tietoliikennettä ja nähdä siellä kulkevaa tietoa.

2.2 VPN-tyypit

2.2.1 Remote Access

Remote Access VPN antaa käyttäjälle mahdollisuuden päästä käyttämään yrityksen sisäisessä verkossa olevia sovelluksia ja dataa samalla tavalla kuin loppukäyttäjä työskentelisi normaalisti toimistolla. Remote Access VPN luo virtuaalisen tunnelin yrityksen verkon network access (NAS) palvelimen ja loppukäyttäjän päätelaitteelle asennetun VPN clientin välille, jolloin tietoliikenne on salattua, vaikka käyttäjä itse olisi julkisessa verkossa. Useat käyttäjän ovat sallittuja Remote Access yhteydessä (Spadafora 2020).

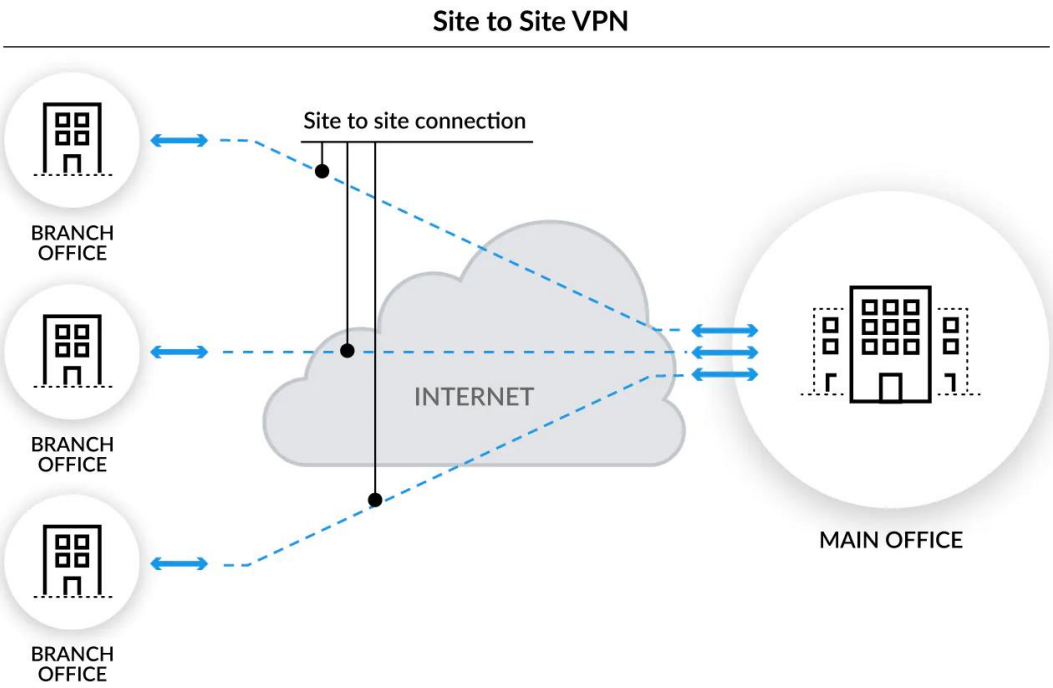


Kuva 1. Remote Access VPN esimerkki (Greyson Technologies 2020)

2.2.2 Site-to-site

Site-to-site VPN tunnetaan myös nimellä Router-to-router VPN. Site-to-site VPN on suosittu erityisesti yrityskäytössä. Useilla yrityksillä on pääkonttorin lisäksi useita sivutoimipisteitä eri paikkakunnilla tai ulkomailla. Site-to-site VPN-yhteyden avulla pääkonttorin verkko saadaan yhdistettyä sivutoimipisteisiin. Site-to-site VPN yhdistää eri sijaintien verkot internettiin ja salaa verkkojen välisen tietoliikenteen IPsec protokollalla. VPN-yhteys muodostetaan yleensä kahden verkkolaitteen välille. Useat käyttäjät Site-to-site VPN-yhteydessä ei ole sallittu (vpnMentor 2021).

Vaikka Site-to-site VPN yhteys on edelleen varsin yleinen, ei se välttämättä ole enää riittävä sellaisenaan. Site-to-site yhteys toimii erittäin hyvin silloin kun yrityksellä on oma palvelinkeskus, erittäin arkaluontoista dataa tai vähäinen kaistanleveysvaatimus. Nykyään useat yritykset siirtävät sovelluksia sekä dataa pilveen. Ei ole välttämättä järkevää, että loppukäyttäjän on ensin otettava VPN-yhteys yrityksen sisäiseen datakeskukseen päästäkseen pilveen, kun käyttäjä voisi mennä sen sijaan suoraan pilveen (Palo Alto Networks julkaisuaika tuntematon).



Kuva 2. Site-to-site VPN esimerkki (Palo Alto Networks)

2.3 VPN-protokollia

VPN-protokollat määrittävät, kuinka data kulkee yhteyden läpi. Protokollilla on usein erilaiset määritykset toivottujen hyötyjen ja käyttökohteen mukaan. Jotkin protokollat ovat keskittyneet tehokkaaseen tiedonsiirtoon, kun toiset keskittyvät enemmän datan suojaukseen, jolloin tiedonsiirtonopeus yleensä kärsii. Usein VPN yhteydessä on käytössä useampi protokolla, joista toinen hoitaa tiedon siirron ja toinen tiedon suojauksen. On myös protokollia, jotka käsittelevät molemmat osa-alueet samassa protokollassa (Harkness 2019).

2.3.1 Point-to-point tunneling protocol (PPTP)

PPTP on Microsoftin kehittämä VPN-tunnelointiprotokolla, joka pohjautuu aikaisempaan PPP (Point-to-point) tiedonsiirtoprotokollaan. PPTP on PPP protokollan laajennus, joka mahdollistaa tiedonsiirron TCP/IP verkossa GRE protokollaa hyödyntäen (Bennet 2020).

PPTP on yksi vanhimpia VPN-tunnelointiprotokollia ja sen kehitys on jo pysähtynyt. PPTP:n kovaajaksi on tullut L2TP sekä IPsec protokollat. PPTP käyttää 128-bittistä salausta ja siitä on havaittu useita tietoturvaongelmia liittyen PPTP:n kanssa käytettävään CHAP todennusprotokollaan. Alhainen salaustaso tekee PPTP:stä erittäin nopean, mutta sitä ei suositella enää käytettäväksi lukuisten tietoturvaongelmien takia (Scott 2019).

2.3.2 Layer 2 Tunneling Protocol (L2TP)

L2TP on kehitetty kahden vanhemman, PPP ja L2F (Layer 2 Frowarding) protokollien pohjalta. L2TP:tä käytetään kuljettamaan PPP kehyksiä. L2TP ei itsessään sisällä vahvaa tiedon salausta, joten sen kanssa on käytettävä myös toista salausprotokollaa. Yleensä L2TP:n kanssa käytettävä protokolla on IPsec. Tämä yhdistelmä on huomattavasti turvallisempi kuin PPTP ja se tunnetaan nimellä L2TP/IPsec (IETF).

2.3.3 Internet Protocol Security (IPsec)

IPsec on kokoelma TCP/IP tietoliikenneprotokollia, jotka tarjoavat tietoliikenteen salauksen, molempien osapuolten todennuksen sekä tiedon eheyden varmistuksen IP-tasolla. IPsec protokollaa voidaan käyttää VPN-tunnelin muodostukseen sekä myös yhdessä toisen tunnelointiprotokollan kanssa tietoliikenteen salaukseen. IPsec toimii verkkokerroksen tasolla OSI-mallissa, joten se sopii myös muihin kuin TCP pohjaisten protokollien suojaamiseen. Yleisesti tämä tarkoittaa sitä, että IPsec sopii myös UDP ja IP pohjaisien sovelluksien suojaukseen (Juniper Networks 2020).

2.3.4 Internet Key Exchange v2 (IKEv2)

IKEv2 on avaintenvaihtoprotokolla, joka käsittelee pyyntö- ja vastaustoimintoja. Protokolla perustuu Diffie-Helman avaintenvaihtoalgoritmiin. Protokolla suorittaa keskinäisen todennuksen kahden osapuolen välille ja perustaa IKEv2-yhteyden, jota kutsutaan nimellä SA (Security Association). Yhteys sisältää salaista jaettua tietoa, jota käytettään CHILD_SA luomiseen ESP-protokollalle (Encapsulating Security Payload) tai AH-todennusotsikolle (Authentication Header) ja salausalgoritmien määritykseen, joita SA-yhteydet käyttävät suojatakseen siellä kulkevan tietoliikenteen. Yleensä IKEv2 protokollan kanssa käytetään IPSec protokollaa, jossa IKEv2:n avulla jaetaan ja tarkistetaan suojausavaimet ja IPSec:n avulla luodaan turvallinen VPN-tunneli laitteiden välille (IETF 2010).

2.3.5 Secure Socket Tunneling Protocol (SSTP)

SSTP on Microsoftin kehittämä ja omistama protokolla. Windows Vista ja sitä uudemmat versiot tukevat kyseistä VPN protokollaa. SSTP toimii muodostamalla suojatun yhteyden VPN palvelimen ja clientin välille ja kaikki yhteydessä kulkeva liikenne on salattua. SSTP kuljettaa PPP-kehyksiä SSL/TSL protokollaa käyttäen TCP 443 portin kautta. Käyttäessään TCP porttia se pääsee läpi suurimmasta osasta palomuureja, sillä HTTPS liikenne käyttää yleisesti samaa porttia. Mikäli ulkopuolinen taho yrittää tarkkailla tietoliikennettä, sen on vaikeaa erottaa VPN tunnelissa kulkevaa liikennettä normaalista HTTPS liikenteestä, kun käytössä on sama portti. Varmentaakseen uuden yhteyden avaamisen, vaaditaan käyttäjäntodennusta. Todennus tehdään yleensä clientin päässä (Mocan 2019).

2.3.6 Datagram Transport Layer Security (DTLS)

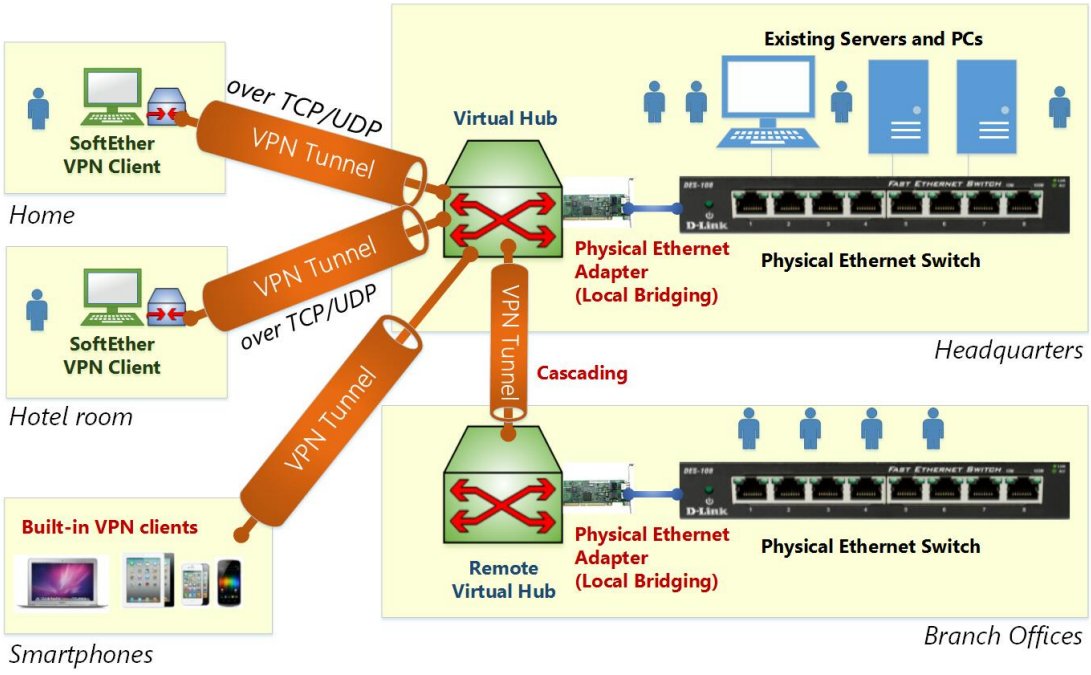
DTSL on tietoliikenneprotokolla, joka on suunniteltu suojaamaan dataa ja estämään tiedon urkintaa tai datan muokkausta. DTSL on hyvin samantapainen TSL (Transport Layer Security) protokollan kanssa. TSL on laajasti käytössä oleva tietoliikenneprotokolla, joka tarjoaa yhteyspainotteisen kanavan tietoliikenteen siirtoon. TLS:n heikkous on, että sen täytyy kulkea luotettavan kanavan kautta, joka on tyypillisesti TCP ja tästä syystä TSL:n avulla ei voida suojata epäluotettavaa datagrammiliikennettä. DTLS on suunniteltu hyvin samanlaiseksi kuin TSL, pääeroavaisuutena on, että DTSL käyttä UDP protokollaa TCP:n sijaan. DTSL on tarkoitettu toimittamaan sovelluksen data luotettavasti ja todennetulla salauksella sovellusten välillä mahdollisimman pienellä viiveellä. Tästä syystä DTSL:ää käytetään esimerkiksi median suoratoiston, online pelaamisen tai VoIP yhteyden suojaamiseen, jossa mahdollisimman pieni viive on tärkeämmässä asemassa kuin pakettien häviö (IETF 2012).

2.4 Avoimen lähdekoodin VPN vaihtoehtoja

2.4.1 SoftEther VPN

SoftEther on japanilaisen Daiyuu Noborin kehittämä VPN toteutus, jonka 1.0 versio julkaistiin talvella 2003. SoftEther VPN on julkaistu avoimen lähdekoodin projektina vuonna 2014.

SoftEther on suunniteltu tehokkaaksi ja helppokäyttöiseksi VPN ohjelmistoksi, joka tukee useaa eri protokollaa. Se on yhteesopiva OpenVPN-, L2TP-, IPsec-, EtherIP-, L2TPv3-, Cisco VPN-retittimien ja MS SSTP VPN-ohjelmistojen kanssa. SofEther virtualisoi ethernet-laitteet, jotta virtuaalisen erillisverkon toteutus onnistuu sekä remote access sekä site-to-site VPN-yhteyksillä. VPN-tunneli toteutetaan TCP/IP- tai TCP/UDP-yhteyden kautta kahden laitteen välille. Remote Access toteutuksessa palvelintietokoneelle luodaan yksi tai useampi Virtual Hub, joka käsittelee asiakastietokoneilta tulevia yhteyspyyntöjä ja asiakastietokoneille (client) luodaan yksi tai useampi virtuaalinen verkkosovitin, jonka avulla muodostetaan yhteys palvelinkoneella sijaitsevaan Virtual Hubiin. SSL salaa VPN-tunnelin läpi tulevan tietoliikenteen. Site-to-site toteutuksessa luodaan yhteys kahden tai useamman Virtual Hubin välille. Yhteydellä saadaan integroitua useita erillisiä ethernet segmenttejä yhteen ethernet segmenttiin. Esimerkiksi, jos yhteys luodaan pisteiden A, B ja C välille, pisteessä A sijaitsevat koneet voivat kommunikoida myös pisteiden B ja C koneiden kanssa (SoftEther julkaisuaika tuntematon).



Kuva 3. SoftEther VPN arkkitehtuuri esimerkki (SoftEther)

2.4.2 OpenVPN

James Yonan aloitti OpenVPN avoimen lähdekoodin projektina vuonna 2001 ja ensimmäinen versio siitä julkaistiin vuonna 2002 GNU GPL -lisenssin alaisena.

OpenVPN on protokolla, jonka avulla saadaan luotua turvallinen tunneli asiakkaan ja vpn-palvelimen välille. Se käsittelee sekä tiedon salauksen, että osapuolten todennuksen käyttämällä OpenSSL kirjastoa. OpenSSL on avoimen lähdekoodin toteutus SSL/TLS salausprotokollista. Salaukseen voidaan käyttää myös muita protokollia lisäämään salauksen tasoa. Tiedonsiirrossa voidaan käyttää joko UDP tai TCP protokollaa. OpenVPN ei sisällä tukea perinteisiin L2TP, IPsec tai PPTP protokolliin, vaan se käyttää omaa kustomoitua protokollaa, joka pohjautuu SSL ja TLS protokolliin (Tim Mocan 2019).

Protokollalle on tehty kaksi tietoturva auditointia joulukuun 2016 ja huhtikuun 2017 välisenä aikana. Auditoinneissa löydettiin kaksi haavoittuvuutta palvelunestohyökkäyksiin liittyen. Löydetyt haavoittuvuudet eivät vaarantaneet käyttäjätietoja eivätkä ne olleet kriittisiä ja ne korjattiin nopeasti kehittäjien toimesta. Lisäksi OpenVPN tarjoaa sivuillaan paljon tietoa, kuinka salauksen ja todennuksen käsittelyä saadaan vahvistettua. Auditoinnissa kävi myös ilmi, että protokollalle on saatavilla lukuisia erilaisia kokoonpanoja, joista kaikki kokoonpanot eivät ole täysin turvallisia. Tästä syystä palvelimen ylläpitäjällä on myös vastuu riittävästä suojauksen tasosta (Quarkslab 2017).

2.4.3 WireGuard

WireGuard on avoimen lähdekoodin palvelimelle asennettava VPN-ohjelmisto. Alun perin Linuxille suunnatusta ohjelmistosta on myös tehty versioita muille käyttöjärjestelmille. Maaliskuussa 2020 WireGuardista julkaistiin ensimmäinen vakaa 1.0 versio ja samoihin aikoihin julkaistuun Linux kernel versioon 5.6 sisällytettiin WireGuard tuki (Salter 2020).

Wireguardin virtuaalisen verkkotunnelin toiminta perustuu julkisen avaimen salaukseen sekä tunnelin sisällä sallittuihin IP-osoitteisiin, tästä käytetetään termiä Cryptokey Routing. Jokaisella verkkoliitännällä on yksityinen avain ja lista sallituista kohteista.

Tunnelissa ennen IP-paketin lähettämistä kohde IP-osoite tunnistetaan julkisella avaimella. Mikäli vastaavuutta ei löydy, paketti tiputetaan pois. Tunnistuksen jälkeen lähetettävä paketti salataan ChaCha20Poly1305 algoritmia käyttäen. Salattu paketti lähetetään kohteesen UDP-pakettina. Paketti sisältää tietyn otsikon ja salatun kuorman. Paketti saapuu kohdeporttiin, jota kohdekone kuuntelee. Saapunut paketti tunnistetaan oikeaksi otsikon avulla ja kuorman salaus puretaan. Lopuksi kohteessa on purettu IP paketti, josta tarkistetaan vielä lähde IP-osoitteen vastaavuus sallittujen IP-osoitteiden listaan (Donenfeld 2020).

Kaikki paketit, jotka lähetään WireGuard verkkoliitännän kautta ovat salattuja ja todennettuja. Verkkotunnelin päiden identiteetin tunnistuksella ja sallittujen IP-osoitteiden välillä on tiukka yhteys, joten yhteyden ylläpitäjän ei tarvitse toteuttaa ylimääräisiä palomuurilaajennuksia. Tämä malli tarjoaa yksinkertaisen ja helposti hallinnoitavan kokoonpanon (WireGuard julkaisuaika tuntematon).

3 RASPBERRY PI

3.1 Yleistä

Raspberry Pi on brittiläisen Raspberry Pi Foundation kehittämä yhden piirilevyn kokoinen tietokone. Tämä pienikokoinen ja edullinen tietokone sopii hyvin pieniin projekteihin sekä koulutukseen. Kehittäjillä oli tavoitteena tehdä helposti lähestyttävä sekä kustannustehokas laite, jonka avulla saadaan tehtyä kaikki mihin normaali pöytätietokonekin pystyy. Halvan hintansa sekä kompaktin kokonsa ansiosta se on erittäin suosittu ja käytössä useissa erilaisissa projekteissa niin yrityksissä kuin yksityisillä elektroniikkaharrastajillakin. Laitteessa olevat GPIO-pinnit mahdollistavat lisäosien ja erilaisten anturien kytkennän Raspberry Pi:hin (Raspberry Pi julkaisuaika tuntematon).

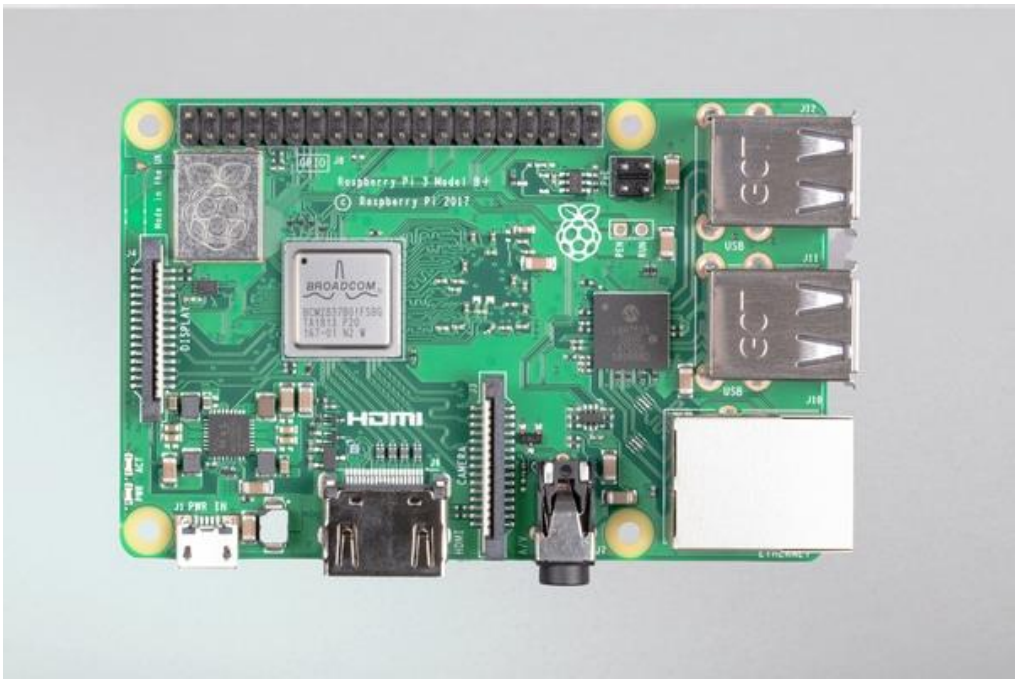
3.2 Mallit

Raspberry Pi tietokoneita on ollut useampaa sukupolvea, Raspberry Pi 1, 2, 3 ja 4 sekä kaksi aiemmista eroavaa mallia: Raspberry Pi Zero sekä Raspberry Pi 400. Zero malli on riisuttu versio perinteisestä mallista. Karsitut ominaisuudet, kuten ethernet liitännän puuttuminen sekä USB liitäntöjen määrän vähennys tekevät Zero mallista erittäin halvan sekä pienikokoisen. 400 malli on Raspberry Pi:n uusin julkaisu. Vuonna 2020 julkaistu 400 malli on tähänastisista versioista tehokkain sekä se on integroitu näppäimistön sisään. Myös jokaisesta Raspberry Pi perinteisestä mallista on tehty useampia versioita (Raspberry Pi julkaisuaika tuntematon).

Product	SoC	Speed	RAM	USB Ports	Ethernet	Wireless	Bluetooth
Raspberry Pi Model A+	BCM2835	700MHz	512MB	1	No	No	No
Raspberry Pi Model B+	BCM2835	700MHz	512MB	4	100Base-T	No	No
Raspberry Pi 2 Model B	BCM2836/7	900MHz	1GB	4	100Base-T	No	No
Raspberry Pi 3 Model B	BCM2837A0/B0	1200MHz	1GB	4	100Base-T	802.11n	4.1
Raspberry Pi 3 Model A+	BCM2837B0	1400MHz	512MB	1	No	802.11ac/n	4.2
Raspberry Pi 3 Model B+	BCM2837B0	1400MHz	1GB	4	1000Base-T	802.11ac/n	4.2
Raspberry Pi 4 Model B	BCM2711	1500MHz	2GB	2xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0
Raspberry Pi 4 Model B	BCM2711	1500MHz	4GB	2xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0
Raspberry Pi 4 Model B	BCM2711	1500MHz	8GB	2xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0
Raspberry Pi Zero	BCM2835	1000MHz	512MB	1	No	No	No
Raspberry Pi Zero W	BCM2835	1000MHz	512MB	1	No	802.11n	4.1
Raspberry Pi Zero WH	BCM2835	1000MHz	512MB	1	No	802.11n	4.1
Raspberry Pi 400	BCM2711	1800MHz	4GB	1xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0

Kuva 4. RaspBerry Pi mallit (Raspberry Pi)

3.3 Raspberry Pi 3 Model B+ laitetiedot



Kuva 5. Raspberry Pi 3 model B+ (Raspberry Pi)

Pi 3 Model B+ on vuonna 2018 julkaistu, kolmannen sukupolven viimeinen Raspberri Pi malli. Edeltäjiinsä nähden tähän malliin on lisätty prosessorin sekä tiedonsiirron suoritusnopeutta sekä langattomia tiedonsiirto-ominaisuuksia. Laitteessa on 1,4 GHz 64-bittinen Broadcom BCM2837B0 neliydinprosessori, joka näkyy piirilevyn keskiosassa. Kuvassa piirilevyn ylälaidassa näkyvät GPIO-pinnit, joita laitteessa on yhteensä 40. Mitä tahansa pinniä voidaan käyttää ohjelmistoissa sisään -tai ulostulona. Virtaa tietokone saa erillisestä virtalähteestä, joka yhdistetään micro-USB liitännällä. Sopiva virtalähde laitteelle on 5V/2,5A. Pi:ssä on myös 4 kappaletta USB-portteja, 3,5 mm audioliitäntä sekä HDMI-portti. Verkkoyhteyden laitteeseen saa Ethernet kaapelilla tai langattomasti WiFi-yhteydellä. Piirilevyn takapuolelta löytyy paikka SD-kortille, joka toimii laitteen tallennustilana käyttöjärjestelmälle, ohjelmille sekä muille tiedostoille. Laitteeseen voi myös liittää ulkoisia tallennustiloja (Upton & Halfacree 2016).

3.4 Mahdolliset käyttöjärjestelmät toteutukseen

Raspberry Pi:ssa ei ole oletuksena asennettuna käyttöjärjestelmää, mutta sille on tarjolla lukuisia linux-pohjaisia jakeluita, joista käyttäjä voi valita käyttötarkoituksen mukaan haluamansa jakelun. Linux jakeluiden lisäksi laitteessa on myös tuki Windows 10 IoT Core käyttöjärjestelmälle, joka on myös optimoitu ARM-prosessoriarkkitehtuurille.

3.4.1 Raspberry Pi OS

Raspberry Pi OS (kutsutaan myös nimellä Raspbian) on ensisijaisesti suositeltu ja alun perin suunniteltu käytettäväksi Raspberry Pi laitteille. Käyttöjärjestelmä on ilmainen ja se perustuu Linuxin Debian jakeluun. Sen asentamisen yhteydessä tulee paljon ohjelmia ja työkaluja tietokoneen normaaliin käyttöön, kuten graafinen käyttöliittymä, internet selain, LibreOffice-paketti sekä ohjelmointityökaluja. Lisäohjelmistojen asennus onnistuu apt paketinhallinnan avulla (Upton & Halfacree 2016).

Raspberry Pi OS käyttää perinteisen BIOS:in (Basic Input-Output System) sijaan erillistä konfiguraatio tiedostoa. Tämä tiedosto sisältää tarvittavat käyttöjärjestelmän kokoonpanoparametrit, joita voidaan muokata millä tahansa tekstieditorilla tai sisäänrakennetulla raspi-config ohjelmalla, joka tarjoaa asetuksien muuttamiseen graafisen käyttöliittymän. Asetetut parametrit ladataan tiedostosta laitteen käynnistyessä.

Raspberry Pi OS on aktiivisen kehityksen alla oleva yhteisöprojekti. Käyttöjärjestelmän toiminnassa painotetaan mahdollisimman monen Debian-paketin suorituskyvyn ja vakauden parantamista (Raspberry Pi julkaisuaika tuntematon).

3.4.2 Ubuntu

Ubuntu on GNU/Linux tuoteperheeseen kuuluva käyttöjärjestelmä, joka pohjautuu Debian-jakeluun. Ubuntu on avoimen lähdekoodin projekti, jota rahoittaa ja ylläpitää Canonical-yhtiö. Ubuntu tarjoaa käyttäjälleen kaikki normaaliin tietokoneen käyttöön tarvittavat perusohjelmistot kuten, tekstinkäsittely, verkkoselain sekä käyttöliittymä. Kehittäjien mukaan projektin tavoitteena on ollut tarjota yhtenäinen ja ajantasainen käyttöjärjestelmä, joka sopii työpöytä ja palvelinkäyttöön. Ubuntu tarjoaa järjestelmäversioita sekä työpöytä-, että palvelinkäyttöön. Ubuntusta julkaistaan uusi versio kuuden kuukauden välein ja joka neljäs kahden vuoden välein julkaistu versio sisältää pitkäaikaisen tuen, joka merkitään versioon termillä LTS. Ubuntu on yksi eniten käytetyistä käyttöjärjestelmistä työpöytä- sekä palvelinkäytössä ympäri maailman (Ubuntu julkaisuaika tuntematon).

3.4.3 Debian

Debian GNU/Linux on Linux-kerneliin eli ytimeen perustuva jakelupaketti, jonka kehityksen Ian Murdock aloitetti vuonna 1993. Debian on edelleen jatkuvan kehityksen alla ja siitä pidetään yllä aina vähintään kolme julkaisua. Nämä julkaisut ovat vakaa, testattava sekä epävakaa. Vakaa (stable) jakelu on viimeisin ja virallisesti käytössä oleva Debianin tuotantojulkaisu, jota Debian suosittelee ensisijaisesti käyttämään. Testattava (testing) jakelu sisältää paketteja, joita ei ole vielä hyväksytty viralliseen tuotantojulkaisuun. Epävakaata (unstable) jakelua käytettään Debianin kehitykseen ja yleensä kyseinen jakelu on käytössä enimmäkseen Debianin kehittäjillä. Debianista julkaistaan säännöllisesti uusi vakaa versio, johon voidaan odottaa kolmen vuoden täysi tuki sekä vielä kahden vuoden ylimäärinen LTS-tuki uuden vakaan julkaisun jälkeen. Debian on erittäin suosittu ja yleisesti käytössä oleva jakelu. Se on tunnettu monipuolisuudestaan, sillä Debianin mukana tulee yli 58000 pakettia ja se tukee kymmentä eri arkkitehtuuria. Debianin pohjalta on tehty useita uusia Linux-jakeluita (Debian julkaisuaika tuntematon).

4 TOTEUTUS

4.1.1 Teknologiset valinnat toteutuksessa

Laitteeksi valikoitui Raspberry Pi 3 Model B+. Kyseisen laitteen lisäksi harkinnassa oli myös vanhempia työasemia sekä läppäreitä. Kaikki laitteet löytyivät itseltä jo valmiiksi, joten hankintoja ei tarvinnut tehdä. Raspberry Pi valikoitui käyttöön sen kompaktin koon sekä vähäisen virrankulutuksen takia. Raspberry Pi on myös halpa ja vaikka se menisi rikki, olisi koko laite halvempi korvata kuin yksittäinen komponentti perinteisessä tietokoneessa. Laitteeseen asennettiin Raspberry Pi Os NOOBS (New Out Of Box Software) asennuksenhallintaohjelmistoa käyttäen. Kyseinen käyttöjärjestelmä valittiin, koska se on optimoitu erityisesti Raspberry Pi laitteilla ja se on itselle tuttu jo aikaisemmista projekteista.

VPN toteutuksena oli tarkoituksena käyttää jotain avoimen lähdekoodin toteutusta. Näistä vaihtoehtoina olivat OpenVPN ja WireGuard. WireGuardin hyvinä puolina ovat, että se on uusin markkinoilla oleva VPN toteutus, se on nopeampi kuin OpenVPN, se kuluttaa vähemmän akkua mobiililaitteissa sekä sille on tuki uusimmassa Linux kernel versiossa, joka nopeuttaa käyttöönottoa. OpenVPN on sen sijaan jo vanhempi ja vakiintunut protokolla, se on hyväksytty usean tarkastajan toimesta sekä se tukee sekä TCP- että UDP-protokollaa. Kummassakaan protokollassa ei ole tunnettuja tietoturva-aukkoja (Hayat 2021). Protokollaksi valittiin WireGuard, sillä se on tällä hetkellä uusin vaihtoehto sekä useiden lähteiden perusteella nopeampi kuin OpenVPN.

Verkkolaitteen IP-osoite saattaa muuttua tietyn ajan välein. Koska käytettävissä ei ole staattista IP-osoitetta, käytetään No-Ip Dynamic DNS (DDNS) palvelua. DDNS-palvelulla saadaan seurattua dynaamista IP-osoitetta ja sen muutoksia. DDNS-palvelun avulla dynaaminen IP-osoite saadaan sidottua sille määritettyyn verkkotunnukseen, vaikka laitteen oma IP-osoite muuttuu (Pramatarov 2018).

4.1.2 Asennus

Ennen varsinaista asennusta otettiin reitittimessä käyttöön DDNS asetukset, johon syötetään käytössä olevan DDNS palvelun käyttäjätiedot sekä verkkotunnus. Reitittimeen täytyi myös luoda uusi port forwarding sääntö, jolla määritetään oikeanlainen yhteys reitittimen ja Raspberry Pi:n välille. Sääntöön määritetään Raspberry Pi:n IP-osoite sekä haluttu portti sekä tiedonsiirtoprotokolla. Protokollaksi asetettiin UDP, sillä WireGuard tukee vain sitä.

WireGuardin asennukseen käytetään sille kehitettyä PIVPN asennus skriptiä. Skriptillä saadaan nopeutettua käyttöönottoa sekä se tarjoaa asennukseen graafisen käyttöliittymän. Ennen lataamista on syytä tarkastella skriptiä, ettei sinne ole lisätty mitään ylimääräisiä haitallisia komentoja. Skripti saadaan ladattua komennolla

curl -L https://install.pivpn.io | bash

Latauksen jälkeen skripti lähtee pyörimään automaattisesti. Ennen asennuksen aloitusta se tarkistaa APT-hakemistojen päivitykset ja päivittää ne, mikäli päivitettävää löytyy, levytilan määrän, jotta tila riittää tulevalle asennukselle sekä laitteelle asennetun Linux-jakelun, jotta se on yhteensopiva. Tarkistuksien jälkeen graafinen käyttöliittymä aukeaa asennusta varten. Asennuksen alussa näkyy ilmoitus, jossa kehotetaan asettamaan palvelimelle staattinen IP-osoite.

Siirryttäessä seuraavaan vaiheeseen, saadaan asetettua nykyinen paikallinen IP-osoite Raspberry Pi:n staattiseksi osoitteeksi. Skripti tarkistaa onko staattisia asetuksia jo luotu, jos ei ole, se lisää dhcpcd.conf tiedostoon nykyisen IP-osoitteen, sekä verkon palveluntarjoajan nimipalvelimien osoitteet. Staattiset asetukset osoitetaan eth0 verkkosovittimelle, mikä on kyseisen laitteen ainoa fyysinen verkkosovitin.

Verkkoasetusten asettamisen jälkeen tulee varoitus mahdollisesta IP-konfliktista, jossa reititin voisi yrittää asettaa tätä samaa staattista paikallista osoitetta toiseen reitittimeen yhdistettyyn laitteeseen. Tämän voi estää tapahtumasta varaamalla kyseinen IP-osoite, mutta yleensä reitittimet ovat itsessään tarpeeksi viisaita estämään tallaista tapahtumasta.

Seuraavaksi näytetään lista paikallisista käyttäjistä, joista määritetään yksi käyttäjä tallentamaan WireGuard konfiguraatiotiedostot laitteelle.

Valitaan haluttu protokolla, vaihtoehtoina on WireGuard tai OpenVPN. Valitaan WireGuard ja asetetaan sille haluttu portti. Skripti luo /etc/pivpn hakemiston ja luo sinne setupVars.conf konfiguraatiotiedoston WireGuardille ja asettaa sinne oletusarvot käytettävästä tiedonsiirtoprotokollasta, verkkoadpterin nimestä sekä sallituista IP-osoitteista. Oletuksena kaikki IP-osoitteet ovat sallittuja. Asennuksen edetessä skripti päivittää syötetyt tiedot setupVars.conf tiedostoon. Tässä vaiheessa skripti tarkistaa laitteesta Linux-kernel version ja päivittää sen tarvittaessa, sillä uusimmasta kernel-versiosta löytyy WireGuard tuki. Asennuksessa pyydetään antamaan DNS-palvelimen osoite, koska omaa DNS palvelinta ei ole, käytetään Googlen osoitteita 8.8.8.8 ja 8.8.4.4. Seuraavaksi määritetään, miten päätelaitteelle asennettu ohjelma yhdistää WireGuard palvelimeen. Tähän asetetaan aiemmin määritetty DDNS-osoite, joka ohjaa tiedon reitittimen IP-osoitteeseen.

DDNS-osoitteen asettamisen jälkeen skripti luo palvelimen salausavaimet, jotka WireGuard vaatii ja käynnistää WireGuard palvelun uudelleen. WireGuardin vaatii julkisen ja yksityisen Base64 koodatut avaimet. Salausavaimet luodaan hakemistoon /etc/wireguard/keys/ komennolla

wg genkey | tee privatekey | wg pubkey > publickey

Avaimet kopioidaan myös sijaintiin /etc/wireguard/, jota WireGuardin virtuaalinen wg0 verkkoadapteri käyttää. Salausavainten lisäksi tiedostossa on myös palvelimen IP osoite sekä kuunneltava portti. Palvelun uudellenkäynnistys tapahtuu komennolla

systemctl restart wg-quick@wg0.service

Palvelun uudelleenkäynnistyksen jälkeen wg0 verkkoadapteri on valmis käyttöön.

```
interface: wg0
  public key: vkB2/bTknAc5VN6KNr0ZS7Ealm8IRxlQfHj6idCdVlg=
  private key: (hidden)
  listening port: 51820
```

Kuva 6. WireGuard wg0 verkkoadapteri

WireGuardin konfiguroinnin jälkeen skripti muokkaa RaspBerry Pi:n järjestelmäasetuksia, jotka löytyvät sijainnista /etc/sysctl.conf. Otetaan käyttöön IPv4-liikenteen edelleenlähetys ottamalla kommentti pois kohdasta *net.ipv4.ip_forward=1*.

```
  GNU nano 3.2                    /etc/sysctl.conf


# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Kuva 7. sysctl.conf tiedoston muutokset

Liikenteen edelleenlähetystä varten skripti luo sille säännöt sijaintiin /etc/iptables/rules.v4.

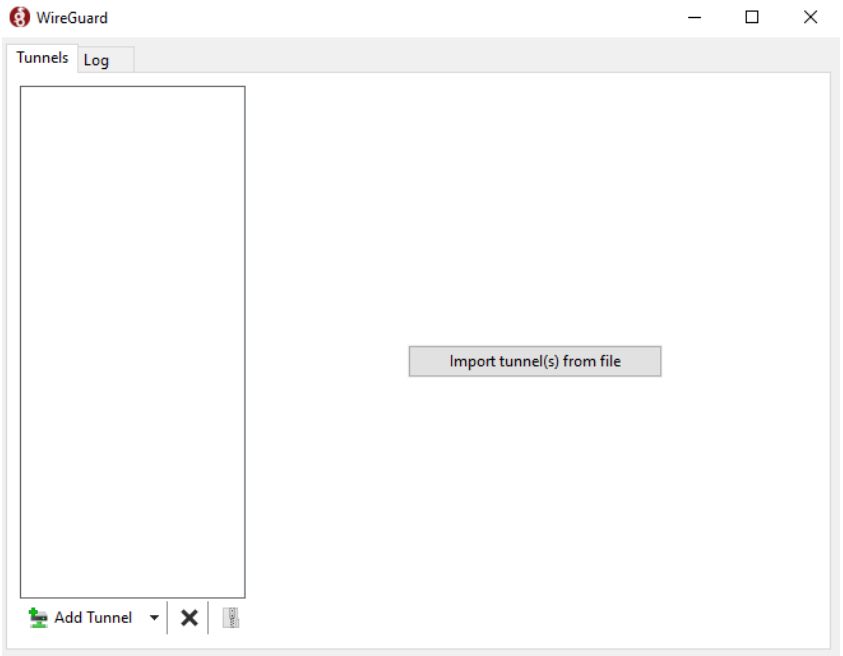
```
*filter
:INPUT ACCEPT [101883:21488217]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [127530:27955436]
COMMIT


*nat
:PREROUTING ACCEPT [34:2787]
:INPUT ACCEPT [34:2787]
:POSTROUTING ACCEPT [32:2563]
:OUTPUT ACCEPT [32:2563]
-A POSTROUTING -s 10.6.0.0/24 -o eth0 -m comment --comment wireguard-nat-rule -j MASQUERADE
COMMIT
```

Säännöt tulevat käyttöön, kun WireGuard palvelu käynnistetään uudelleen. Skripti pyytää asentamaan unattented-upgrades paketin (valvomattomat sovelluspäivitykset). Paketin tarkoitus on pitää

laite ajan tasalla automaattisten tietoturvapäivityksien avulla. Asennetaan paketti, mutta ei vielä toistaiseksi oteta sitä käyttöön, jotta saadaan itse hallittua haluttujen päivitysten asennus. Viimeisenä sijaintiin /opt/pivpn ladataan skripti, jonka avulla saadaan hallinnoitua palvelinta *pivpn*- komennolla.

4.1.3 Päätelaitteen ohjelmisto

Päätelaitteelle pitää asentaa WireGuard client ohjelma, jotta VPN-yhteys saadaan muodostettua palvelimeen. Ohjelman asennusmedian saa ladattua WireGuardin omalta nettisivulta, jossa voidaan valita media käyttöjärjestelmän mukaan. Käytössä olevat tietokoneet käyttävät Windows 10 käyttöjärjestelmää, joten valitaan sille sopiva asennustiedosto. Ohjelman asennus on erittäin yksinkertainen, suoritetaan asennustiedosto ja asennus suoritetaan oletusasetuksilla. WireGuardista on myös omat versiot mobiililaitteille, jonka saa ladattua Android-laitteille Google Play-kaupasta sekä IOS laitteille App Storesta.



Kuva 8. WireGuard graafinen käyttöliittymä päätelaitteella

VPN-yhteyden muodostamiseksi tarvitaan myös päätelaitteelle oma konfiguraatiotiedosto, joka saadaan luotua palvelimella PiVPN skriptin avulla, komennolla

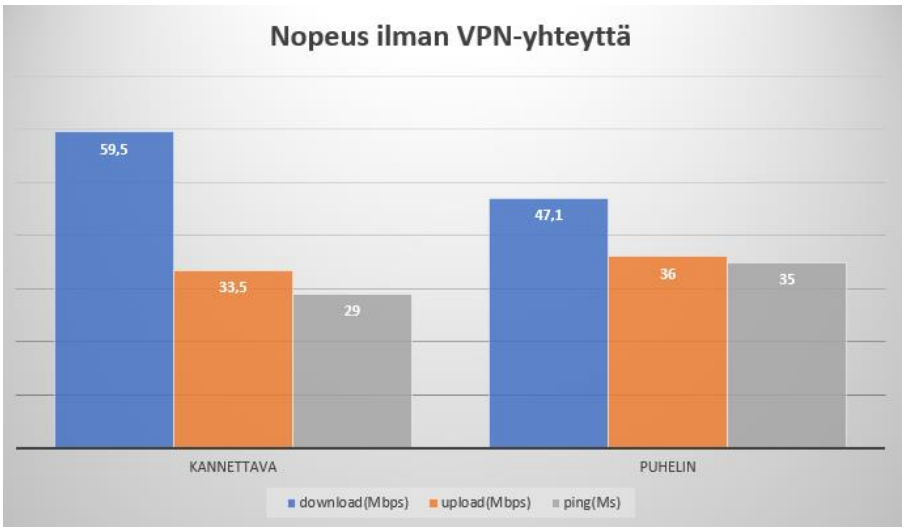
pivpn -a

Skripti pyytää nimeämään uuden konfiguraatiotiedoston ja luo tämän jälkeen salausavaimet uudelle tiedostolle sekä päivittää palvelimen wg0 konfiguraatiotiedostoon tiedot uudesta päätelaitteen tiedostosta. Luotu tiedosto kopioidaan palvelimen käyttäjän kotihakemistoon, josta se on helppo kopioida päätelaitteeseen. Jakelun voi suorittaa vaikkapa USB-tikun avulla. Toteutuksen aikana sekä palvelin, että päätelaitteet sijaitsivat samassa verkossa, joten jakelu onnistui Python SimpleHTTPServer-palvelimen avulla. Palvelimen avulla saadaan luotua verkkopalvelin, joka näyttää halutun hakemiston sisällön ja sieltä saa ladattua tiedostoja päätelaitteille. Palvelinta pidettiin päällä sen aikaa, että konfiguraatiotiedosto saatiin ladattua sekä tietokoneelle, että mobiililaitteille. Kun tiedosto on

ladattu laitteeseen, se saadaan liitettyä ohjelmaan ”import tunnel from file” ominaisuuden avulla. Konfiguraatiotiedoston liittämisen jälkeen voidaan muodostaa VPN-yhteys client-ohjelman ja palvelimen välille.

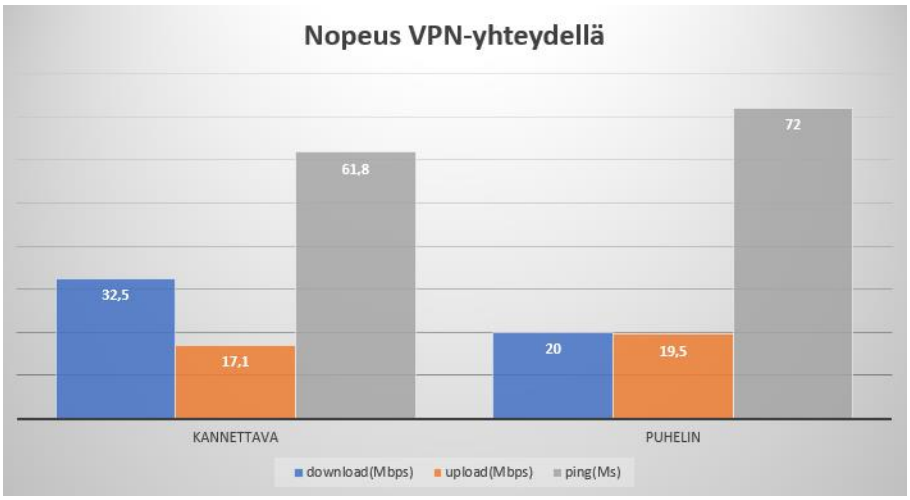
4.1.4 Testaus

Aluksi testattiin Internet-yhteyden nopeus (latausnopeus, lähetysnopeus ja viive) ilman VPN-yhteyttä ja tämän jälkeen VPN-yhteyden kanssa. Testaus suoritettiin kannettavalla tietokoneella sekä puhelimella samalla langattomalla verkkoyhteydellä. Nopeuden testaamiseen käytettiin speedtest.net (https://www.speedtest.net/) verkkosivun palvelua. Testi suoritettiin kummallakin laitteella viisi kertaa ja saaduista tuloksista laskettiin keskiarvo.



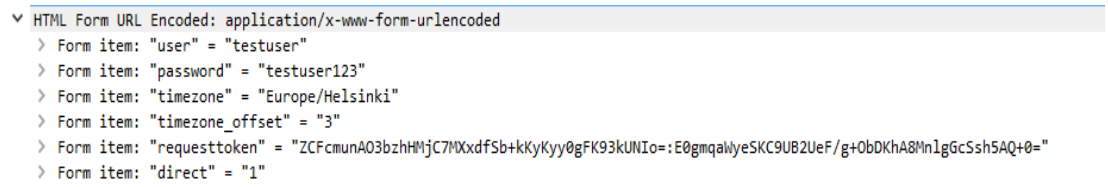
Kuva 9. Nopeus ilman VPN-yhteyttä

Testin tuloksista nähdään, että VPN-yhteys hidastaa verkkoyhteyden nopeutta huomattavasti kummallakin testissä käytetyllä laitteella. Lataus- sekä lähetysnopeus laskee noin puoleen sekä viive (ping) nousee noin kaksinkertaiseksi. Havaitut muutokset olivat täysin odotettavissa, sillä kaikki tietoliikenne kulkee VPN-palvelimena toimivan Raspberry Pi:n kautta. Vaikka yhteyden nopeus hidastuu, pysyy käytettävyys vielä aivan kohtuullisena.



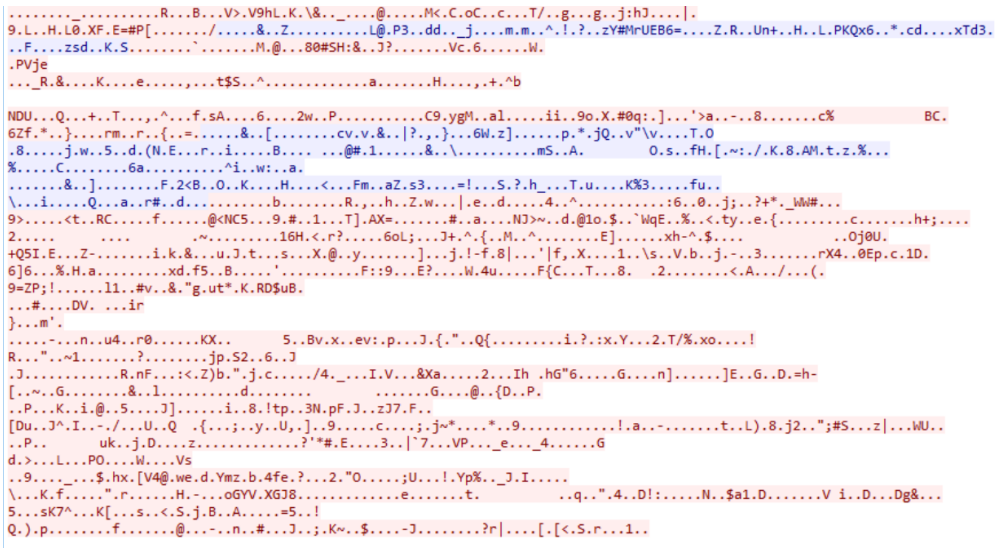
Kuva 10. Nopeus VPN-yhteydellä

Samalle laitteelle on myös asennettu Nextcloud palvelinohjelmisto, joka toimii tiedostopalveluna. Palveluun kirjautumista testattiin suojaamattomalla http-yhteydellä sekä sen jälkeen VPN-yhteydellä ja siinä tapahtuvaa tietoliikennettä tarkkailtiin samalla Wireshark ohjelmalla. Wiresharkilla saadaan kaapattua, tallennettua ja analysoitua tietoliikennettä paketti kerrallaan. Kun käytössä on pelkkä suojaamaton http-yhteys, kirjautumistiedot ovat IP-paketissa selkokielisenä tekstinä. Mikäli ulkopuolinen taho tarkkailisi tietoliikennettä samaan ajankohtaan, hän saisi urkittua käytettävät tunnukset erittäin helposti. Tästä syystä tiedostopalvelulle ei avata omia portteja ulkoverkkoon, vaan palvelua käytetään VPN-yhteyden avulla, jolloin tietoliikenne on suojattua.



Kuva 11. Kirjautumistiedot IP-paketissa suojaamattomassa yhteydessä

VPN-yhteydessä tietoliikenne kulkee erillisessä tunnelissa ja paketit ovat salattuja. Kun tietoliikennettä monitoroidaan Wiresharkilla, huomataan että VPN-tunnelissa kulkevat paketit vaikuttavat hyvin samanlaisilta ja niistä on mahdotonta erottaa kirjautumistapahtumaa. Myös paketin sisällöstä ei saa selvää, koska se on salattu ja mitään tietoja ei näy selkokielisenä tekstinä.



Kuva 12. Salatun IP-paketin sisältö

5 YHTEENVETO

Opinnäytetyön tavoitteena oli tuottaa mikroyrityksen käyttöön soveltuva VPN-ratkaisu. Työssä tutkittiin yleisesti käytössä olevia tunnelointi- ja salausprotokollia, sekä avoimen lähdekoodin VPN-ohjelmistoja. Toteutuksen suunnittelussa mentiin vahvasti kustannustehokkuus edellä ja tästä syystä toteutus tehtiin Raspberry Pi tietokoneelle, johon asennettiin ilmainen WireGuard VPN-palvelin ohjelmisto.

Opinnäytetyössä tuotettu VPN-toteutus mahdollistaa pääsyn ulkoverkosta yrityksen sisäverkon resursseihin suojatun yhteyden yli, joten kaikille palveluille ei tarvitse erikseen avata portteja ja tehdä tarvittavia reitityksiä ulkoverkosta käsin työskentelyä ajatellen. VPN-yhteys muodostuu palvelimen ja päätelaitteelle asennetun WireGuard GUI ohjelmiston välille siihen määritetyn konfiguraatiotiedoston avulla. Julkisia verkkoja käytettäessä ulkopuolinen taho voi yrittää seurata laitteiden välistä tietoliikennettä ja käyttää sitä hyväkseen esimerkiksi kirjautumistietojen saamiseksi. VPN-yhteydellä saadaan suojauduttua tällaiselta man-in-the-middle hyökkäykseltä ja testauksessa toteutus osoittautui toimivaksi. VPN-tunnelissa kulkevat IP-paketit ovat salattuja, joten niiden sisällöstä ei saa selvää ilman salauksen purkamista.

WireGuard osoittautui toimivaksi ja halvaksi sekä tietoturvalliseksi ratkaisuksi VPN-yhteyden luomiseksi. Käyttö ei itsessään maksa mitään ja palvelinohjelmisto sekä päätelaitteelle asennettava ohjelma ovat ilmaisia. Ainoaksi kustannukseksi jää laite ja sille tarvittavat oheistarvikkeet.

LÄHTEET

Adam Harkness 2019. Common VPN protocols explained. Verkkojulkaisu. https://www.netmotion-software.com/blog/connectivity/vpn-protocols. Viitattu 8.4.2021.

Anthony Spadafora 2020. Remote access VPN: what are they, how do they work and which are the best. Verkkojulkaisu. https://www.techradar.com/vpn/remote-access-vpn. Viitattu 26.3.2021.

AO Kapersky lab julkaisuaika tuntematon. What is VPN. Verkkojulkaisu. https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn. Viitattu 23.3.2021.

Eben Upton and Gareth Halfacree 2016. Raspberry Pi User Guide. Verkkojulkaisu. https://dn.odroid.com/IoT/other_doc.pdf#page=33&zoom=100,0,0. Viitattu 28.4.2021.

Debian julkaisuaika tuntematon. Definitions and overview. Verkkojulkaisu. https://www.debian.org/doc/manuals/debian-faq/basic-defs.en.html. Viitattu 3.5.2021.

Internet Engineering Task Force (IETF) 1999. Layer Two Tunneling Protocol "L2TP". Verkkojulkaisu. https://tools.ietf.org/html/rfc2661#page-9/. Viitattu 6.4.2021.

Internet Engineering Task Force (IETF) 2010. Internet Key Exchange Protocol Version 2 (IKEv2). Verkkojulkaisu. https://tools.ietf.org/html/rfc5996/. Viitattu 6.4.2021.

Internet Engineering Task Force (IETF) 2012. Datagram Transport Layer Security Version 1.2. Verkkojulkaisu. https://tools.ietf.org/html/rfc6347#page-4. Viitattu 8.4.2021

Jason A. Donenfeld 2020. WireGuard: Next Generation Kernel Network Tunnel. Verkkojulkaisu. https://www.wireguard.com/papers/wireguard.pdf/. Viitattu 22.4.2021

Jim Salter 2020. WireGuard VPN makes it to 1.0.0—and into the next Linux kernel. Verkkojulkaisu. https://arstechnica.com/gadgets/2020/03/wireguard-vpn-makes-it-to-1-0-0-and-into-the-next-linux-kernel/. Viitattu 22.4.2021.

John Bennet 2021. VPN-turvallisuusprotokollat selitettynä: Näin toimii PPTP. Verkkojulkaisu. Päivitetty 24.3.2020. https://fi.wizcase.com/blog/vpn-turvallisuusprotokollat-selitettyna-nain-toimii-pptp/. Viitattu 26.3.2021.

Juniper Networks 2020. IPsec VPN overview. Verkkojulkaisu. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-ipsec-vpn-overview.html. Viitattu 26.3.2021.

Martin Pramatarov. What is DDNS. Verkkojulkaisu. https://www.cloudns.net/blog/what-is-dynamic-dns/. Viitattu 6.5.2021.

Olivia Scott 2019. The PPTP VPN protocol: Is it safe? Verkkojulkaisu. https://resources.infosecinstitute.com/topic/the-pptp-vpn-protocol-is-it-safe/. Viitattu 26.3.2021.

Palo Alto Networks julkaisuaika tuntematon. What is Site-to-site VPN? Verkkojulkaisu. https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn. Viitattu 23.3.2021.

Quarkslab 2017. OpenVPN 2.4.0 Security Assessment Technical Report. Verkkojulkaisu. https://ostif.org/wp-content/uploads/2017/05/OpenVPN1.2final.pdf/. Viitattu 20.4.2021.

Ran Greenberg 2021. Different Types of VPNs and When to Use Them. Verkkojulkaisu. https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/. Viitattu 26.3.2021.

Raspberry Pi julkaisuaika tuntematon. Raspberry Pi OS. Verkkojulkaisu. https://www.raspberrypi.org/documentation/raspbian/. Viitattu 29.4.2021.

Raspberry Pi julkaisuaika tuntematon. What is Raspberry Pi. Verkkojulkaisu. https://www.raspberrypi.org/help/what-%20is-a-raspberry-pi/. Viitattu 28.4.2021.

SoftEther julkaisuaika tuntematon. SoftEther VPN Project. Verkkojulkaisu. https://www.softether.org/. Viitattu 20.4.2021.

Tim Mocan 2019. What Is OpenVPN. Verkkojulkaisu. https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-openvpn/. Viitattu 20.4.2021.

Tim Mocan 2019. What is SSTP. Verkkojulkaisu. https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-sstp/#definition/. Viitattu 6.4.2021.

Ubuntu julkaisuaika tuntematon. The Story of ubuntu. Verkkojulkaisu. https://ubuntu.com/about. Viitattu 3.5.2021.

Usman Hayat 2021. WireGuard vs OpenVPN – Which is Better? Let's Find Out. Verkkojulkaisu. https://www.vpnranks.com/blog/wireguard-vs-openvpn/. Viitattu 3.5.2021.

VpnMentor 2021. Eri VPN-tyypit ja niiden käyttö. Verkkojulkaisu. https://fi.vpnmentor.com/blog/eri-vpn-tyypit-ja-niiden-kaeyttoe/. Viitattu 26.3.2021.

WireGuard julkaisuaika tuntematon. WireGuard Conceptual Overview. Verkkojulkaisu. https://www.wireguard.com/. Viitattu 22.4.2021

Kuvat:

Greyson Tecnologies 2020. Remote Access esimerkki. Valokuva. https://www.greyson.com/wp-content/uploads/2020/03/remote-access-vpn-1.png/. Viitattu 23.3.2021.

Palo Alto Networks julkaisuaika tuntematon. Site-to-site VPN esimerkki. Valokuva. https://www.paloaltonetworks.com/content/dam/pan/en_US/images/cyberpedia/site-to-site-vpn.png/. Viitattu 23.3.2021.

Raspberry Pi julkaisuaika tuntematon. Raspberry Pi 3 model B+. Valokuva. https://www.raspberrypi.org/homepage-9df4b/static/2379729c131cf7a8afe312734e1b1ae1/ae23f/4a84795d-bc61-4c77-9f48-4d217c439a23_3B%252B%2BTOP%2BDOWN%2BREFRESH_.jpg. Viitattu 28.4.2021.

Raspberry Pi julkaisuaika tuntematon. Raspberry Pi mallit. Valokuva. https://www.raspberrypi.org/documentation/faqs/#hardware-compare. Viitattu 28.4.2021.

SoftEther julkaisuaika tuntematon. SoftEther VPN arkkitehtuuri esimerkki. Valokuva. http://www.softether.org/@api/deki/files/683/=1.0.2.jpg?size=webview/. Viitattu 20.4.2021.