



SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Joakim Haga

VPN-palvelin Raspberry Pi -tietokoneella

Seinäjoen ammattikorkeakoulu

Opinnäytetyö

Kevät 2022

SeAMK

Insinööri (AMK), tietotekniikka



SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Tutkinto-ohjelma: Insinööri (AMK), tietotekniikka

Suuntautumisvaihtoehto: Tietoliikenne

Tekijä: Joakim Haga

Työn nimi: VPN-palvelin Raspberry Pi -tietokoneella

Ohjaaja: Alpo Anttonen

Vuosi: 2022

Sivumäärä: 36

Opinnäytetyön tavoitteena oli asentaa VPN-palvelin Raspberry Pi -tietokoneelle. Tutustua VPN toimintaan ja yleisimpiin käyttötarkoituksiin. Työssä tutustaan myös Linux-käyttöjärjestelmiin ja Raspberry Pi -tietokoneeseen. Lopuksi työssä asennetaan ja konfiguroidaan VPN-palvelin ja tarvittavat ohjelmat sekä palvelut Raspberry Pi -tietokoneelle.

Työn lopputuloksena saatiin toimiva VPN-palvelin johon voidaan yhdistää Windows, Linux Android ja iOS-käyttöjärjestelmiä käyttävät laitteet. VPN-palvelimen tarkoituksena on suojata lähiverkon laitteet ulkopuolisilta tahoilta ja tietoturvariskeiltä ja saada yhteys lähiverkon laitteisiin ulkopuolisesta verkosta.

¹ Asiasanat: VPN, Linux, Raspberry Pi, Raspberry Pi OS

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Degree programme: Information Technology

Specialisation: Networking

Author: Joakim Haga

Title of thesis: VPN-server on Raspberry Pi Computer

Supervisor: Alpo Anttonen

Year: 2022

Number of pages: 36

The goal of the thesis was to install a VPN-server on a Raspberry Pi computer and to learn about the operations and common uses of VPN. The thesis also studied information on Linux operating systems and Raspberry Pi computers. Finally, the VPN server and the programs and services necessary for the Raspberry Pi computer were installed and configured.

As the result of the thesis there was a working VPN-server to which devices running Windows, Linux, iOS or Android operating systems can be connected. The purpose of a VPN server is to protect local area network devices from third parties and security risks and to connect to local area network devices from an external network.

¹ Keywords: VPN, Linux, Raspberry Pi, Raspberry Pi OS

SISÄLTÖ

Opinnäytetyön tiivistelmä	2
Thesis abstract	3
SISÄLTÖ	4
Kuvaluettelo.....	6
Käytetyt termit ja lyhenteet.....	7
1 JOHDANTO	8
1.1 Työn tausta	8
1.2 Työn tavoite.....	8
1.3 Työn rakenne	8
2 VPN.....	9
2.1 VPN-verkon alkuperäinen käyttötarkoitus	9
2.2 Yleisimmät VPN-verkon käyttötarkoitukset.....	10
3 LINUX-KÄYTTÖJÄRJESTELMÄ	11
3.1 Linux lyhyesti.....	11
3.2 Miten jakelut eroavat toisistaan	11
3.3 Linuxin edut verrattuna Windowsiin.....	12
4 RASPBERRY PI.....	13
4.1 Raspberry Pi, yleistietoa.....	13
4.2 Raspberry Pi 3 B laitteen tekniset tiedot.....	13
4.3 Raspberry Pi OS	14
5 RASPBERRY PI:N KÄYTTÖÖNOTTO JA OHEISLAITTEET	15
5.1 Käyttöönotto	15
5.2 Raspberry Pi OS -käyttöjärjestelmän asennus ja konfigurointi.....	17
5.3 Samba-tiedostopalvelin	18
6 VPN PALVELIMEN ASENNUS JA MÄÄRITTÄMINEN	23
6.1 DDNS:n ja aliverkon määrittäminen	23
6.2 DDClient-asennus ja määrittäminen.....	24
6.3 Portin edelleenlähetys	25
6.4 Wireguard-VPN-palvelimen asennus	28

6.4.1	Wireguard-sovelluksen asentaminen älypuhelimelle	28
6.4.2	Wireguard-sovelluksen asentaminen tietokoneelle	30
7	Yhteenveto	34
LÄHTEET	35

Kuvaluettelo

Kuva 1. Raspberry Pi, virallinen aloituspaketti (Upton, 2016).	15
Kuva 2. Raspberry Pi2 GPIO taulu. (ThePiHut, 2014).	16
Kuva 3. Raspberry Pi Imager -käyttöliittymä	17
Kuva 4. Raspberry Pi -asetukset	18
Kuva 5. Samba-palvelimen konfiguraatiotiedoston sisältö.	20
Kuva 6. smbд ja nmbd palveluiden uudelleen käynnistys.	20
Kuva 7. Verkkoaseman luonti Windowsissa.	21
Kuva 8. Verkkoasema Windows-työympäristössä.	22
Kuva 9. Uuden aliverkkotunnuksen luominen.	23
Kuva 10. DDClient-määrittelyt.....	25
Kuva 11. Reitittimen portin edelleenlähetysasetukset.....	27
Kuva 12. Wireguard-VPN-palvelimen asennus.....	28
Kuva 13. QR-koodi Windows PowerShell -sovelluksessa.....	29
Kuva 14. VPN-asetusten tuominen älypuhelimeen QR-koodilla.	30
Kuva 15. Asetustiedostot verkkoasemalla. Raspberry Pi -laitteella asema esiintyy normaalina kansiona.....	31
Kuva 16. Windows PowerShell -komentorivi-ikkunan avaaminen kansioista.....	32
Kuva 17. Wireguard ohjelma on yhdistänyt VPN-palvelimeen.	33

Käytetyt termit ja lyhenteet

DDCLIENT	Havaitsee IP-osoitteen muutokset ja päivittää ne DDNS-verkkopalveluntarjoajalle.
DNS	Domain name system on internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi. DNS antaa käyttäjälle mahdollisuuden muodostaa yhteyden verkkosivustoihin käyttämällä internet-verkkotunnuksia ja haettavissa olevia URL-osoitteita numeristen IP-osoitteiden sijasta.
GPIO	General Purpose I/O on monikäyttöinen sisään ja ulostulo.
IP-osoite	Internet Protocol address on yksilöivä osoite, jonka perusteella laite tunnistetaan Internetissä tai paikallisessa verkossa.
NTFS	New technology file system on Microsoftin kehittämä tiedostojärjestelmä joka on käytössä kaikissa Windows NT -pohjaisissa käyttöjärjestelmissä.
Raspberry Pi	Raspberry Pi on luottokortin kokoinen tietokone, jota käytetään esimerkiksi koodauksen opettelemiseen ja elektroniikka projektien rakentamiseen.
SSH	Secure Shell on salattuun tietoliikenteeseen tarkoitettu protokolla.
UDP	User Datagram Protocol on yhteydetön tietoliikenneprotokolla, joka ei vaadi yhteyttä laitteiden välille, mutta mahdollistaa tiedon siirron.
VNC	Virtual network computing on protokolla tietokoneen graafisen käyttöliittymän etäkäyttöön.
VPN	Virtuaalinen erillisverkko, jolla kaksi tai useampia verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon.

1 JOHDANTO

1.1 Työn tausta

Internetin käyttäminen on nykyään turvatonta. VPN-verkon avulla pystytään suojaamaan laitteet ulkopuolisilta ja selata internetiä turvallisesti. VPN-yhteyden avulla voidaan käyttää internetiä ilman, että jokin taho kerää tietoja tai seuraa käyttöä. VPN-yhteys piilottaa laitteen IP-osoitteen, VPN-palveluntarjoajia on lukuisia, mutta kaikilla on ominaista kuukausimaksut. Rakentamalla itse palvelimen ja käyttämällä sitä kotiverkosta maksetaan vain laitteen hinta. Raspberry Pi on tehokas ja vähän virtaa käyttävä, edullinen yhden mikropiirin tietokone, jolla on mahdollista tehdä erilaisia projekteja. Tästä syystä opinnäytetyön aiheeksi valikoitui Raspberry Pi VPN -palvelin joka toteutetaan tee se itse-projektityyllillä.

1.2 Työn tavoite

Tavoitteena työssä on tuoda tietoa tietoturvariskeistä, sekä esitellä Raspberry Pi -laitetta, jolla voidaan tehdä edullisesti tietoteknisiä projekteja. Työssä tämä tehdään rakentamalla toimiva VPN-palvelin Raspberry Pi -tietokoneelle käyttäen Linux-pohjaista Raspberry Pi OS -käyttöjärjestelmää, järjestelmä toimii Windows-työympäristössä.

1.3 Työn rakenne

Työn alussa kerrotaan VPN-verkon toiminnasta ja sen käyttötarkoituksesta. Lisäksi kerrotaan Linuxista lyhyesti ja verrataan Linux-jakeluita keskenään ja Windows-käyttöjärjestelmään. Lopuksi tutustutaan Raspberry Pi -laitteeseen ja Raspberry Pi OS -käyttöjärjestelmään ja asennetaan laitteelle VPN-palvelin tee se itse-projektina.

2 VPN

VPN eli Virtual Private Network on virtuaalinen erillisverkko (VPN-yhteydet.fi, 2021). VPN on salattu yhteys, joka suojaa tietoliikennettä ja peittää identiteetit verkossa. VPN on kuin suojattu tunneli verkossa toimivien laitteiden välillä, jolloin palveluntarjoajat, hakkerit tai muut tahot eivät näe identiteettiäsi, IP-osoitettasi tai sijaintiasi.

Kun laite yhdistetään internetiin ilman VPN-verkkoa yhdistetään laite ensimmäiseksi internetpalveluntarjoajaan, joka yhdistää laitteen käyttäjän haluamille verkkosivuille. Kaikki verkkoliikenne kulkee internetpalveluntarjoajan kautta. Tämä tarkoittaa, että internetpalveluntarjoaja pystyy seuraamaan verkkoliikennettä. Kun yhdistetään internetiin VPN:n kautta, tietoliikenne kulkee VPN-palveluntarjoajan palvelimien kautta salatulla yhteydellä. Näin kaikki laitteen ja VPN-palvelimen välillä kulkeva verkkoliikenne on piilotettu kolmansilta osapuolilta.

Sen sijaan että laite yhdistetään internetpalveluntarjoajalle, yhteys kulkee ensin VPN-palvelimen kautta (F-secure, i.a.). Verkkopalvelut näkevät, että liikenne tulee VPN-palvelimen IP-osoitteesta eikä käyttäjän laitteen julkisesta IP-osoitteesta. Näin todellinen IP-osoite ja käyttäjän identiteetti pysyy salassa, eikä internetpalveluntarjoaja tai verkkosivut voi seurata internetin käyttöä.

Liikenteen ohjaaminen ulkoisen palvelimen kautta tarjoaa kuitenkin monia etuja myös yksityiselle käyttäjälle (VPN-yhteydet.fi, 2021). Tämä johtuu siitä, että liikenteen ohjaaminen ulkoisen palvelimen kautta piilottaa ja vaihtaa laitteen todellisen IP-osoitteen ja sijainnin. IP-osoitteen piilottaminen parantaa yksityisyyttäsi ja mahdollistaa erilaisten estojen kuten suoratoistopalvelujen maarajoitusten kiertämisen. Kun laitteesi on yhdistetty internetiin VPN:n kautta, internetpalveluntarjoaja ei voi nähdä mitä käyttäjä tekee verkossa. Internetpalveluntarjoaja näkee vain, että laite on yhdistetty internetiin VPN-yhteyden kautta.

2.1 VPN-verkon alkuperäinen käyttötarkoitus

VPN-teknologiaa kehitettiin suurten yritysten ja organisaatioiden omiin tarkoituksiin (Mocan, T). Yritykset tarvitsivat turvallisen ja yksityisen menetelmän mahdollistaakseen viestinnän ja tiedostojen jakamisen eri toimistojen välillä ja mahdollistaakseen työntekijöiden pääsyn tärkeisiin tiedostoihin etäyhteyden kautta ilman että luvattomat käyttäjät varastavat

arkaluonteisia tietoja. VPN:n avulla käyttäjät pääsivät yksityisiin yritysten ja organisaatioiden verkkoihin ja tiedostoihin sekä dataan.

2.2 Yleisimmät VPN-verkon käyttötarkoitukset

Yleisimmin VPN yhteyttä käytetään, kun

- tarvitaan pääsy verkkoon turvallisesti, kun ei olla samassa tilassa (esim. yrityksen verkko)
- halutaan käyttää avointa, suojaamatonta tai julkista verkkoa turvallisesti
- suojellaan laitteita jäljittämislta tai hakkeroinnilta
- on tarve kiertää geoaitoja ja saada pääsy maantieteellisesti rajoitettuun sisältöön
- halutaan välttää sensuuri ja verkkosivustojen estoja (McCann, M. & Hardy, A).

3 LINUX-KÄYTTÖJÄRJESTELMÄ

3.1 Linux lyhyesti

GNU/Linux on UNIX-järjestelmään pohjautuva käyttöjärjestelmä, joka on luotu vaihtoehdoksi aiemmin kalliille UNIX-käyttöjärjestelmälle (Linux, i.a.). Nimi "Linux" tulee Linus Torvaldsin vuonna 1991 kehittämästä Linux-ytimeistä. Linux-käyttöjärjestelmiä on useita erilaisia jakeluita, jotka koostuvat Linux-ytimeistä, järjestelmälle oleellisista ohjelmista, työpöytäjärjestelmistä sekä sovelluksista (petrit.net, i.a.).

Suurin osa maailman palvelimista käyttää Linux-pohjaista käyttöjärjestelmää ja mm. puhelimet, kulkuneuvot, sekä sulautetut järjestelmät ovat lähes poikkeuksetta Linux-pohjaisia (Linux, i.a.). Linux-käyttöjärjestelmät ovat vapaata lähdekoodia, jonka vuoksi yhteisöt kehittävät jatkuvasti uusia versioita eli jakeluita. Käyttäjä valitsee jakelun eri kriteereillä esimerkiksi kuinka kokenut käyttäjä on, minkälainen käyttöliittymä halutaan ja tarvitaanko käyttöjärjestelmä palvelin tai työpöytäkäyttöön. Yleensä palvelimiin ei asenneta graafista käyttöliittymää ollenkaan.

3.2 Miten jakelut eroavat toisistaan

Linux-jakelut eroavat toisistaan oletusasennukseen sisällettyjen ohjelmien ja työpöytäympäristön suhteen (Kainulainen, S). Ohjelmien asentamiseen tarvittava pakettinhallintaohjelma vaihtelee eri Linux-jakeluiden mukaan ja vaikuttaa siihen kuinka helppoa tai vaikeaa on uusien ohjelmien asentaminen.

Jakelut käyttävät myös erilaisia pakettinhallintaohjelmia, konfigurointiapuohjelmia ja muita ohjelmistoja (Hoffman, C. 2016). Esimerkiksi Ubuntu ja Red Hat on suunniteltu vakaiksi jakeluiksi, joita tuetaan tietoturvapäivityksillä ja virheenkorjauksilla useita vuosia eteenpäin, kun tietyt jakelut eivät saa tukea kovin pitkään, vaan ovat käyttäjän osaamisen varassa. Osa Linux-jakeluista on tarkoitettu palvelimille ilman graafista käyttöliittymää, osa työpöytäkäyttöön ja osa erikoiskäyttöön, kuten kotiteatteriksi, ajoneuvon tietokoneeksi tai lot-laitteen hallintaan.

3.3 Linuxin edut verrattuna Windowsiin

Linuxin suurin etu Windowsiin verrattuna on sen tietoturva. Windowsille on kymmeniätuhansia eri haittaohjelmia ja viruksia, Linuxille vain pieni osa tästä, eikä yksikään erityisesti haitallinen (Zinoune, M). Linuxin markkinaosuus yksityisille käyttöjärjestelmille on historiansa aikana ollut pieni. Verrattuna Windowsiin, se ei ole iso ja helppo kohde, jotta haittaohjelmia kannattaisi tehdä Linuxille (Hoffman, C. 2017).

Linux on avointa lähdekoodia ja käyttöjärjestelmät ovat ilmaisia. Linux käyttöjärjestelmissä on alhaisemmat laitteistovaatimukset Windowsiin verrattuna (Mills, M). Linux käyttöjärjestelmät sopivat hyvin vanhempiin tietokoneisiin, joissa on vähemmän muistia ja prosessoritehoa. Linuxilla on useita käyttöjärjestelmiä, jotka ovat tarkoitettu vanhemmille ja vähätehoisimmille tietokoneille (Delony, D).

4 RASPBERRY PI

4.1 Raspberry Pi, yleistietoa

Raspberry Pi on luottokortin kokoinen yhden piirilevyn tietokone, joka on tarkoitettu koulutukseen ja pieniin projekteihin (Peda.net). Raspberry Pin alkuperäisenä ideana on olla halpa pienoistietokone, jolla voi harjoitella ja tutustua Linux pohjaisiin käyttöjärjestelmiin ja oppia ohjelmoimaan. Linux-käyttöjärjestelmällä toimivaksi suunnitellusta tietokoneesta löytyy käytännössä kaikki oleellinen mitä nykyaikaiselta tietokoneelta voi odottaa. Koneeseen on helppo liittää esimerkiksi näppäimistö, hiiri ja ulkoinen kovalevy USB-porttien kautta, ja prosessori on riittävän tehokas esimerkiksi pyörittämään HDMI-liitännän kautta täydellä HD-resoluutiolla kuvattuja videotiedostoja.

4.2 Raspberry Pi 3 B laitteen tekniset tiedot

- Neliytiminen 1.2GHz Broadcom BCM2837 64bit prosessori
- 1GB RAM-muistia
- 40 pinninen GPIO
- Bluetooth
- Wlan
- 100/10Mb Ethernet -portti
- 4 kappaletta USB 2 -porttia
- HDMI-portti
- CSI kamera -portti Raspberry Pi kameralle
- DSI näyttö -portti Raspberry Pi kosketusnäytölle

- Micro SD -muistikorttipaikka
- Micro USB -virtalähdeportti (Raspberry Pi a, i.a).

4.3 Raspberry Pi OS

Raspberry Pi OS (aikaisemmin tunnettu nimellä Raspbian) on ilmainen Debian-Linuxiin perustuva käyttöjärjestelmä joka, on erityisesti optimoitu Raspberry Pi -laitteita varten (Raspberry Pi, i.a.-b). Käyttöjärjestelmä sisältää joukon perusohjelmia ja apuohjelmia. Raspberry Pi OS tarjoaa enemmän kuin pelkän käyttöjärjestelmän, sillä mukana tulee yli 35000 pakettia valmiiksi käännettyjä ohjelmistoja. Käyttöjärjestelmää kehitetään aktiivisesti, tarkoituksena parantaa suorituskykyä ja vakautta. Raspberry Pi OS -käyttöjärjestelmä sopii hyvin aloittelijalle ja on helposti asennettavissa toimintakuntoon.

laitteeseen syötetään väärä jännite, voi se vahingoittaa laitetta. Suositeltu jännite on 5 voltia ja syöttövirta 2 ampeeria. Laitteessa on tähän tarkoitettu micro USB portti, jonka kautta on tarkoitettu syöttää virta virtalähteen avulla. Tähän sopii esimerkiksi puhelimen laturi. Kun Raspberry Pi -piirilevyyn halutaan syöttää virta GPIO-porttien kautta, tulisi virta liittää portteihin 4 (DC Power 5v) ja 6 (Ground) kuten kuvassa (2). Vaihtoehtoisesti laite saadaan pysymään toiminnassa vaikka virtalähde irroitetaan laitteesta. Tämä onnistuu, jos virtaa syötetään USB-porttien kautta, laitteessa on näitä 4 kappaletta. Laitetta ei kuitenkaan voi käynnistää syöttämällä virtaa tätä kautta.

Raspberry Pi2 GPIO Header

Pin#	NAME		NAME	Pin#
01	3.3v DC Power		DC Power 5v	02
03	GPIO02 (SDA1 , I ² C)		DC Power 5v	04
05	GPIO03 (SCL1 , I ² C)		Ground	06
07	GPIO04 (GPIO_GCLK)		(TXD0) GPIO14	08
09	Ground		(RXD0) GPIO15	10
11	GPIO17 (GPIO_GEN0)		(GPIO_GEN1) GPIO18	12
13	GPIO27 (GPIO_GEN2)		Ground	14
15	GPIO22 (GPIO_GEN3)		(GPIO_GEN4) GPIO23	16
17	3.3v DC Power		(GPIO_GEN5) GPIO24	18
19	GPIO10 (SPI_MOSI)		Ground	20
21	GPIO09 (SPI_MISO)		(GPIO_GEN6) GPIO25	22
23	GPIO11 (SPI_CLK)		(SPI_CE0_N) GPIO08	24
25	Ground		(SPI_CE1_N) GPIO07	26
27	ID_SD (I ² C ID EEPROM)		(I ² C ID EEPROM) ID_SC	28
29	GPIO05		Ground	30
31	GPIO06		GPIO12	32
33	GPIO13		Ground	34
35	GPIO19		GPIO16	36
37	GPIO26		GPIO20	38
39	Ground		GPIO21	40

Rev. 1
26/01/2014

<http://www.element14.com>

Kuva 2. Raspberry Pi2 GPIO taulu. (ThePiHut, 2014).

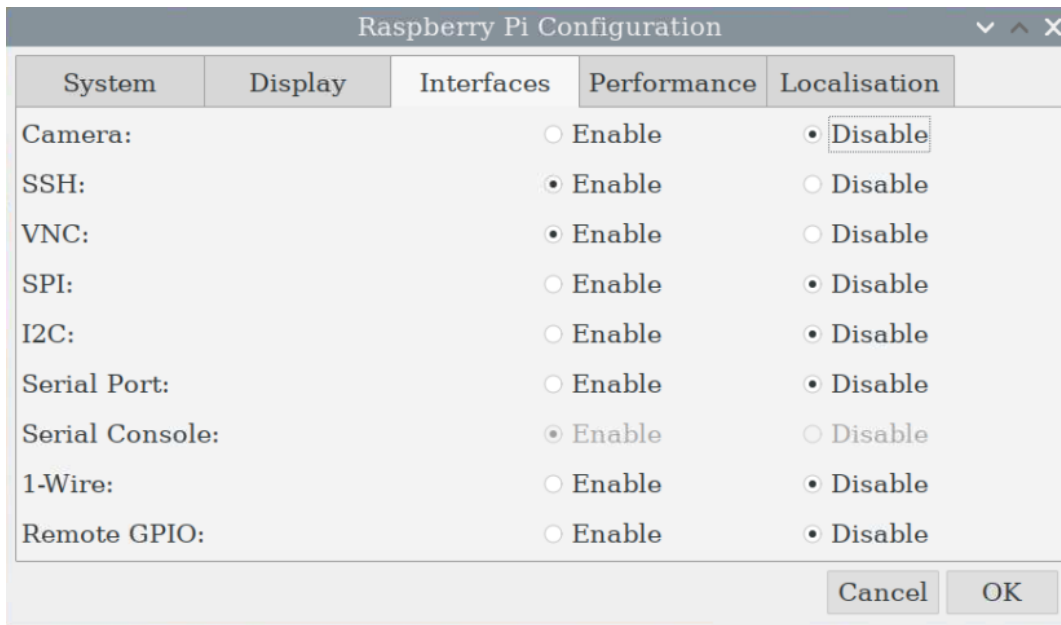
5.2 Raspberry Pi OS -käyttöjärjestelmän asennus ja konfigurointi

Raspberry Pi OS -käyttöjärjestelmä ei tule esiasennettuna laitteeseen, joten käyttöjärjestelmä täytyy asentaa erikseen (Howchoo. i.a.). Käyttöjärjestelmän asennukseen käytetään apuna toista tietokonetta. Raspberry Pi Imager -ohjelmalla ladataan käyttöjärjestelmän asennustiedostoista tehty image-tiedosto MicroSD-muistikortille. MicroSD-muistikortin pitää olla liitettynä apuna käytettävään tietokoneeseen ohjelman käytön aikana. Ohjelman voi ladata Raspberry Pin kotisivuilta. Ohjelma on helppokäyttöinen ja muutamalla klikkauksella käyttöjärjestelmän image-tiedosto on siirretty muistikortille. Tämän jälkeen MicroSD-kortti asetetaan Raspberry Pi -laitteeseen. Laite käynnistetään liittämällä virtalähde, jolloin käyttöjärjestelmä asentuu itsestään ensimmäisellä käynnistyskerralla. Laitteeseen kiinnitetään näyttö, näppäimistö, hiiri ja verkkojohto. Se on valmis käytettäväksi kuin normaali tietokone. Vaihtoehtoisesti laite voidaan yhdistää lähiverkkoon ja sitä käytetään etätyöpöytä-ohjelmalla tai ilman graafista käyttöliittymää SSH-yhteyden avulla.



Kuva 3. Raspberry Pi Imager -käyttöliittymä

Koska laite toimii palvelimena ja laitteeseen halutaan saada yhteys vaikka käyttäjä on eri verkossa, sallitaan SSH- ja VNC-etyhteys. Tämä onnistuu käyttöjärjestelmän asetuksia muokkaamalla.



Kuva 4. Raspberry Pi -asetukset

5.3 Samba-tiedostopalvelin

Samba-palvelin asennettiin Raspberry Pi -laitteelle ja ylimääräisestä kovalevytilasta tehtiin verkkolevy, johon jokaisella lähiverkon laitteella käyttöjärjestelmästä riippumatta on pääsy ja johon voi ladata ja jakaa tiedostoja.

Samban kehitystyö alkoi tarpeesta saada käyttöön UNIX-palvelimien jaetut resurssit Windows-työasemilla (Hertel, C. 2001). Samba toimii UNIX-alustalla, mutta Windows-työasemat saavat siihen yhteyden, kuin se olisi Windows-tietokone. Samban toimimisen Windows-ympäristössä mahdollistaa protokollapaketti CIFS "Common Internet File System", jonka ytimenä toimii SMB "Server Message Block" -protokolla.

Samba yhdistää Windows-, Linux- ja UNIX-koneet käyttämään samoja resursseja (Hertel, C. 2001). Sambassa on kaksi pääohjelmaa eli demonia, smbd ja nmbd, sekä asiakas- ja

apuohjelmia esim. Smbclient ja smbprint. Nämä kaksi pääohjelmaa tarjoavat Samban neljä peruspalvelua: tiedosto- ja tulostuspalvelu, autentikointi, nimipalvelu ja palveluiden listaus.

Samba-palvelimen asennus ja konfigurointi suorituu seuraavilla komentorivin komennolla.

Pakettilista eli tieto pakettilähteiden sisällöstä päivitetään komennolla "sudo apt-get update".

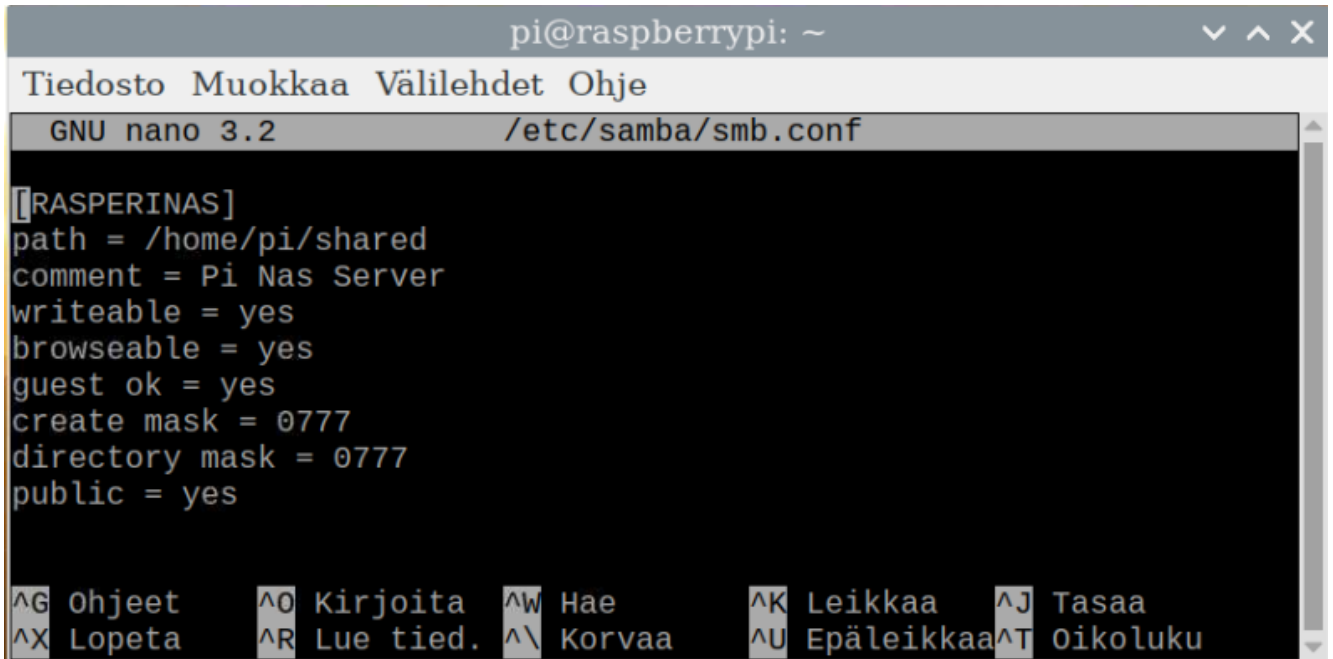
Samba-palvelin asennus suoritetaan komennolla "sudo apt-get install samba samba common-bin"

Seuraavaksi luodaan kansio joka jaetaan lähiverkossa komennolla "sudo chmod 777 /home/pi/shared"

Sitten syötetään komento "sudo apt-get install ntfs-3g", joka asentaa NTFS-järjestelmäpaketin. NTFS (New Technology File System) on Microsoftin kehittämä tiedostojärjestelmä, joka on käytössä kaikissa Microsoft Windows NT -pohjaisissa käyttöjärjestelmissä (Wikipedia). Järjestelmäpaketin avulla Linuxin ja Windowsin tiedostojärjestelmät tunnistavat eri järjestelmien tiedostot palvelimella.

Samba-palvelimen konfiguraatitiedosto varmuuskopioidaan muuttamalla alkuperäisen tiedoston nimi komennolla "sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.old"

Uusi konfiguraatitiedosto luodaan komennolla "nano /etc/samba/smb.conf". Komento luo smb.conf-tiedosto /etc/samba-kansioon ja avaa sen nano-tekstinkäsittelyohjelmalla. Kuvan rivit lisätään tekstinkäsittelyohjelmalla tiedostoon. Tämän jälkeen painetaan ctrl + x, jolloin tekstinkäsittelyohjelma nano sulkeutuu. Nano kysyy sulkeutuessaan, haluatko tallentaa? Tähän vastataan kyllä "k" ja enter.



```

pi@raspberrypi: ~
Tiedosto Muokkaa Välilehdet Ohje
GNU nano 3.2 /etc/samba/smb.conf

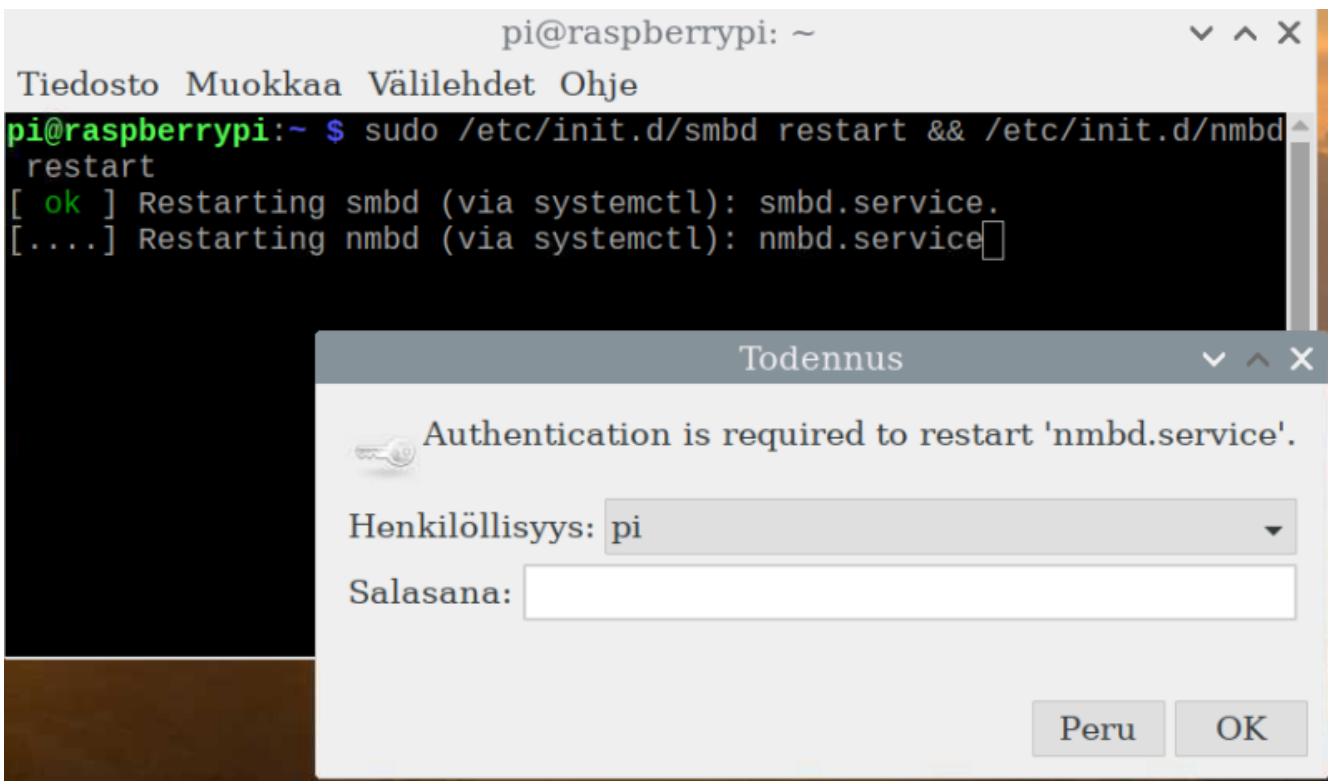
[[RASPERINAS]
path = /home/pi/shared
comment = Pi Nas Server
writeable = yes
browseable = yes
guest ok = yes
create mask = 0777
directory mask = 0777
public = yes

^G Ohjeet      ^O Kirjoita    ^W Hae         ^K Leikkaa    ^J Tasaa
^X Lopeta     ^R Lue tied.  ^\ Korvaa     ^U Epäleikkaa ^T Oikoluku

```

Kuva 5. Samba-palvelimen konfiguraatitiedoston sisältö.

Samba-palvelimen palvelut käynnistetään uudelleen komennolla “sudo /etc/init.d/smbd restart && sudo /etc/init.d/nmbd restart”. Kuvassa (6) järjestelmä pyytää salasana tunnistusta, jotta voi suorittaa palveluiden uudelleen käynnistysen.



```

pi@raspberrypi: ~
Tiedosto Muokkaa Välilehdet Ohje

pi@raspberrypi:~ $ sudo /etc/init.d/smbd restart && /etc/init.d/nmbd
restart
[ ok ] Restarting smbd (via systemctl): smbd.service.
[....] Restarting nmbd (via systemctl): nmbd.service

Todennus
Authentication is required to restart 'nmbd.service'.
Henkilöllisyys: pi
Salasana:
Peru OK

```

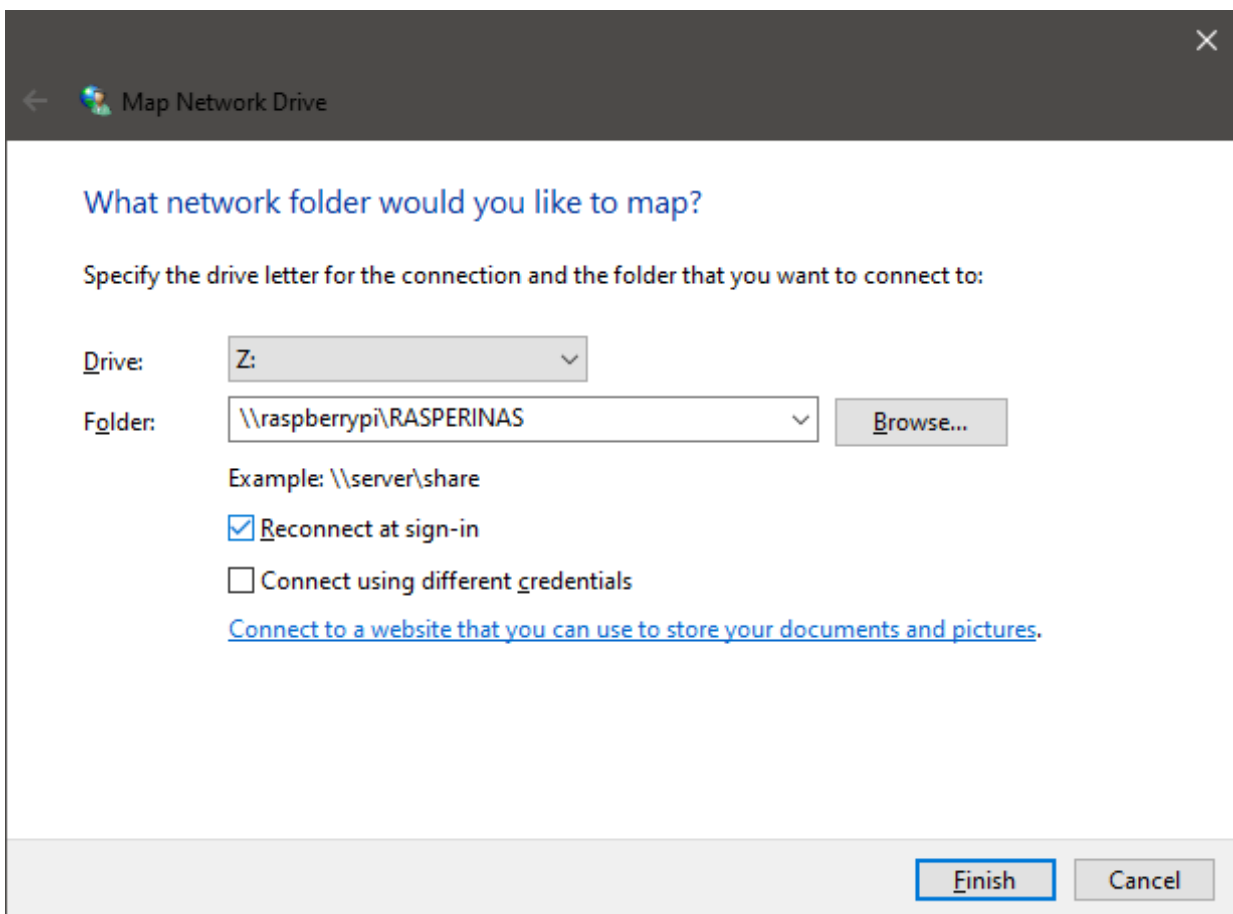
Kuva 6. smbd ja nmbd palveluiden uudelleen käynnistys.

Kuvassa (7) luodaan verkkoasema Windows-työympäristössä.

Drive-kohdasta valitaan verkkolevylle haluttu kirjaintunnus

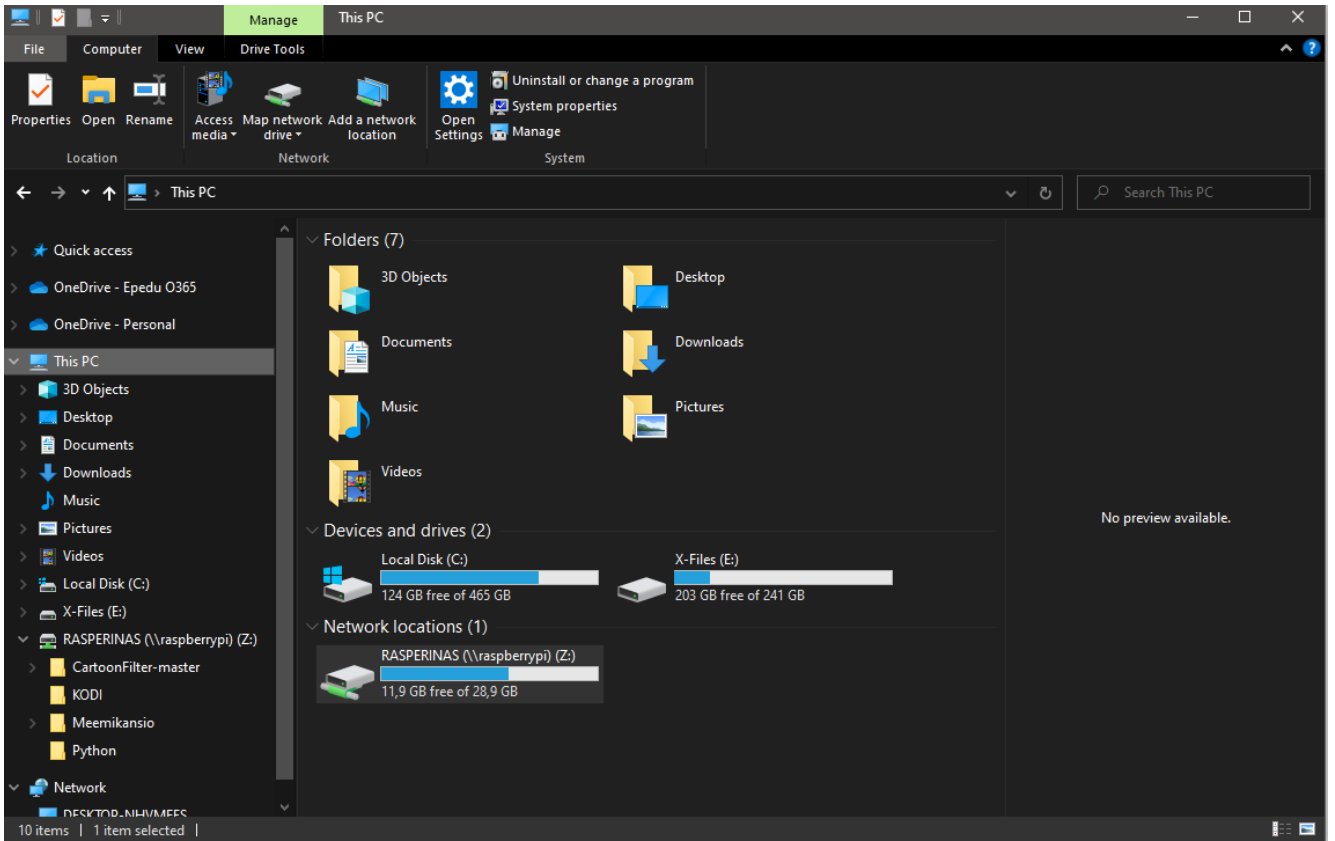
Folder-kohtaan lisätään polku, joka määritettiin aikaisemmin samba-palvelimen smb.conf konfiguraatitiedostoon kuvassa (5). \\raspberrypi\RASPERINAS

Kohtaan Reconnect at sign-in merkitään ruksi, jolloin Windows yhdistää automaattisesti asemaan käynnistyessään. Lopuksi painetaan Finish ja kirjaudutaan levyille Raspberry Piin tunnuksilla.



Kuva 7. Verkkoaseman luonti Windowsissa.

Nyt verkkoasemalle lisätyt tiedostot näkyvät kaikilla lähiverkon tietokoneilla. Raspberry Pi -laitteella tiedostot näkyvät kansiossa /home/pi/shared. Kuvassa (8) näkyy verkkoasema johon Windows on yhdistänyt.



Kuva 8. Verkkoasema Windows-työympäristössä.

6 VPN PALVELIMEN ASENNUS JA MÄÄRITTÄMINEN

6.1 DDNS:n ja aliverkon määrittäminen

DDNS eli dynaaminen DNS on dynaaminen verkkotunnusjärjestelmä (Mitchell, B. i.a.). Se on palvelu, joka kartoittaa internet-verkkotunnuksia IP-osoitteisiin. Toisin kuin DNS, joka toimii pelkästään staattisten IP-osoitteiden kanssa, DDNS on suunniteltu tukemaan dynaamisia eli muuttuvia IP-osoitteita. Yksityinen käyttäjä saa yleensä dynaamisen julkisen IP-osoitteen internet-palveluntarjoajaltaan. Koska VPN-palvelin rakennetaan verkkoon, jossa ei ole staattista IP-osoitetta, tarvitaan ulkoinen DDNS-palvelu, joka ohjaa liikenteen VPN-palvelimelle, vaikka IP-osoite olisi muuttunut. DDNS-palvelu on hyödytön mikäli käytössä on staattinen IP-osoite.

Työssä käytetään freedns.afraid.org tarjoamaa ilmaisversiota DDNS-palvelusta.

The image shows a web form titled "Add a new subdomain". The form has the following fields and values:

- Type: A (dropdown menu)
- Subdomain: rasperivpn (text input)
- Domain: ignorelist.com (public) (dropdown menu)
- Destination: 0.0.0.0 (text input)
- TTL: For our premium supporter seconds (optional) (text input)
- Wildcard: Enabled for all subscribers (more info)

Below the Wildcard field is a CAPTCHA image with a "Different Image" link. At the bottom right of the form is a "Save!" button.

Kuva 9. Uuden aliverkkotunnuksen luominen.

Kuvan (9) kentät ovat seuraavat:

- Subdomain: haluttu nimi aliverkkotunnukselle
- Domain: valikosta valitaan haluttu julkinen verkkotunnus

- Destination: Tähän tulee automaattisesti nykyinen julkinen IP-osoite, mutta se muutetaan 0.0.0.0 näin voidaan testata toimiiko dynaaminen IP-osoitteen määrittämisohjelmisto myöhemmässä vaiheessa.

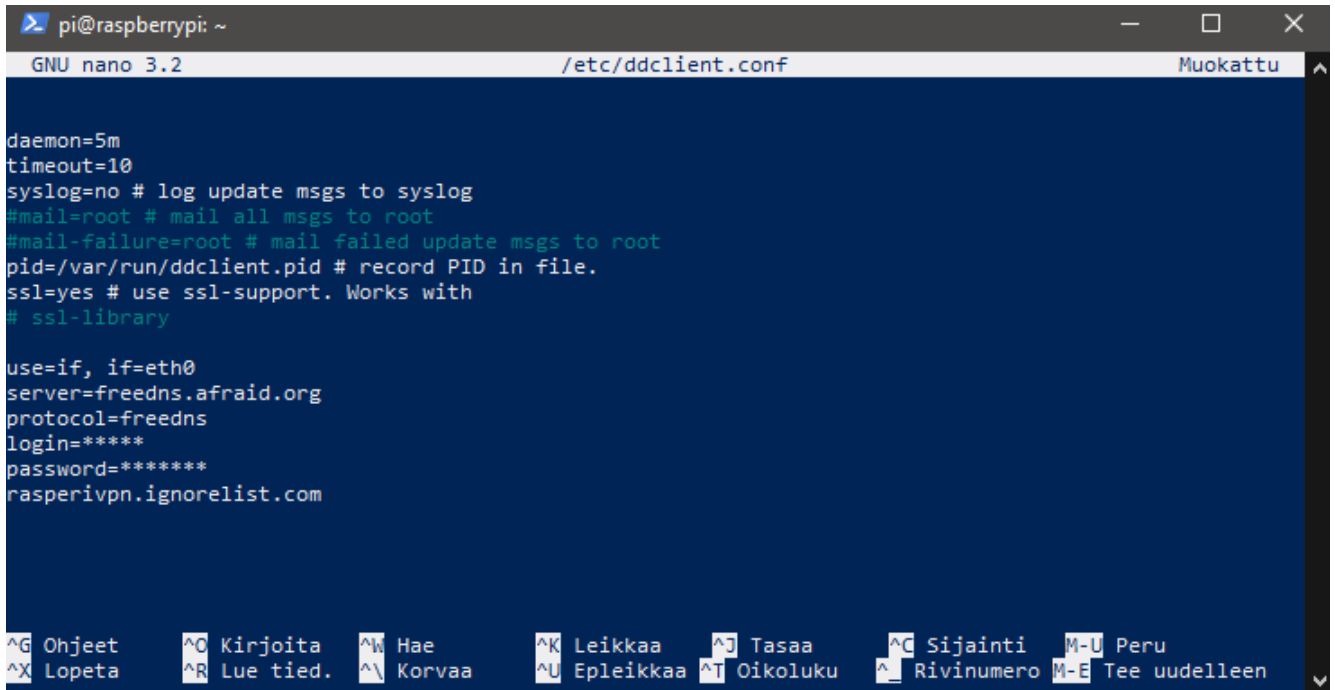
6.2 DDClient-asennus ja määrittäminen

DDClient-asennus tehdään Windows PowerShell -ohjelmalla ssh-yhteyttä käyttäen, sillä myöhemmässä vaiheessa Raspberry Piin natiivi komentorivi ei pysty luomaan QR-koodia. Sitä tarvitaan, kun älypuhelin yhdistetään VPN-palvelimeen Wireguard-sovellusta käyttäen.

SSH-yhteys luodaan Windows PowerShell-ohjelmassa komennolla "ssh pi@[laitteen ip-osoite]".

DDClient asennetaan komennolla "sudo apt install ddclient". Asennusohjelma kysyy tietoja. Painamalla Enter ohitetaan kaikki kysymykset. Asetukset määritetään itse .conf-tiedostoon.

Asennuksen jälkeen määritetään DDClientin asetukset .conf-tiedostoon. Tiedosto avataan nano-tekstinmuokkausohjelmalla komennolla "sudo nano /etc/ddclient.conf" ja korvataan sisältö kuvassa (10) näkyvillä määrittäyksillä.



```

pi@raspberrypi: ~
GNU nano 3.2 /etc/ddclient.conf Muokattu
daemon=5m
timeout=10
syslog=no # log update msgs to syslog
#mail=root # mail all msgs to root
#mail-failure=root # mail failed update msgs to root
pid=/var/run/ddclient.pid # record PID in file.
ssl=yes # use ssl-support. Works with
# ssl-library

use=if, if=eth0
server=freedns.afraid.org
protocol=freedns
login=****
password=*****
rasperivpn.ignorelist.com

^G Ohjeet      ^O Kirjoita   ^W Hae         ^K Leikkaa    ^J Tasaa     ^C Sijainti   M-U Peru
^X Lopeta     ^R Lue tied.  ^_ Korvaa     ^U Epleikkaa  ^T Oikoluku  ^_ Rivinumero M-E Tee uudelleen

```

Kuva 10. DDClient-määrittelyt

Näppäinyhdistelmä ctrl + o tallentaa, ja ctrl + x poistuu ohjelmasta.

Lopuksi käynnistetään DDClient uudelleen komennolla “sudo systemctl restart ddclient” ja varmistetaan, että DDClient käynnistyy automaattisesti, kun Raspberry Pi:iin kytketään virta komennolla “sudo systemctl enable ddclient”. Kun palvelu on käynnistynyt uudelleen DDClient päivittää julkisen IP-osoitteen DDNS-palvelulle. Kuvassa (9) verkkosivulla freedns.afraid.org kohtaan Destination ei määritetty IP-osoitetta. DDClient on nyt päivittänyt tiedon DDNS-palvelulle, ja siihen on tullut Raspberry Pi -laitteen julkinen IP-osoite.

6.3 Portin edelleenlähetys

Portin edelleenlähetys pitää ei-toivotun liikenteen pois paikallisverkoista. Portin edelleenlähetys sallii paikallisverkon ulkopuoliset yhteydet tietokoneeseen tai reitittimeen ja sieppaa IP- tai porttityhdistelmään saapuvan dataliikenteen uudelleen ohjaten eri IP:hen tai porttiin.

Portti vastaanottaa tietoa, se sallii datan kulun laitteella olevasta ohjelmasta ulospäin, tai vastaavasti internetistä tai lähiverkosta sisäänpäin.

Portin edelleenlähetys uudelleenohjaa dataa paikallisverkossa olevan tietokoneen ja ulkoisessa verkossa olevien laitteiden välillä (Andreas, K). Käytännössä tämä on prosessi,

jossa siepataan tietyn laitteen IP-osoitteeseen matkalla oleva data ja ohjataan se eri sijaintiin. Portin edelleenohjauksen suurimpia hyötyjä on, että se piilottaa laitteiden julkisen IP-osoitteen paikallisverkon ulkopuolisilta laitteilta ja siksi se on oleellinen osa VPN-palvelua.

Portin edelleenlähetyks tapahtuu reitittimen Port Forwarding -asetuksissa, tämä löytyy jokaisesta nykyisestä reitittimestä. Tarvitavat asetukset riippuvat reitittimestä, mutta pääsääntöisesti ne ovat kaikki samoja vaikka eri reitittimillä eri nimillä. Raspberry Pi VPN -palvelin tarvitsee seuraavat portin edelleenlähetyksasetukset.

- Laitteen nimi tai IP-osoite
- Protokolla UDP
- Internetyhteyden salliminen
- Avattava portti tai portit

Kuvassa (11) näkyy reitittimen portin edelleenlähetyksasetukset.

← Portin edelleenlähetys VALMIS

Palvelutyypit
MUKAUTETTU

Palvelun nimi
Wireguard ×

Ulkoinen portti
51820

Sisäinen IP
192.168.68.104

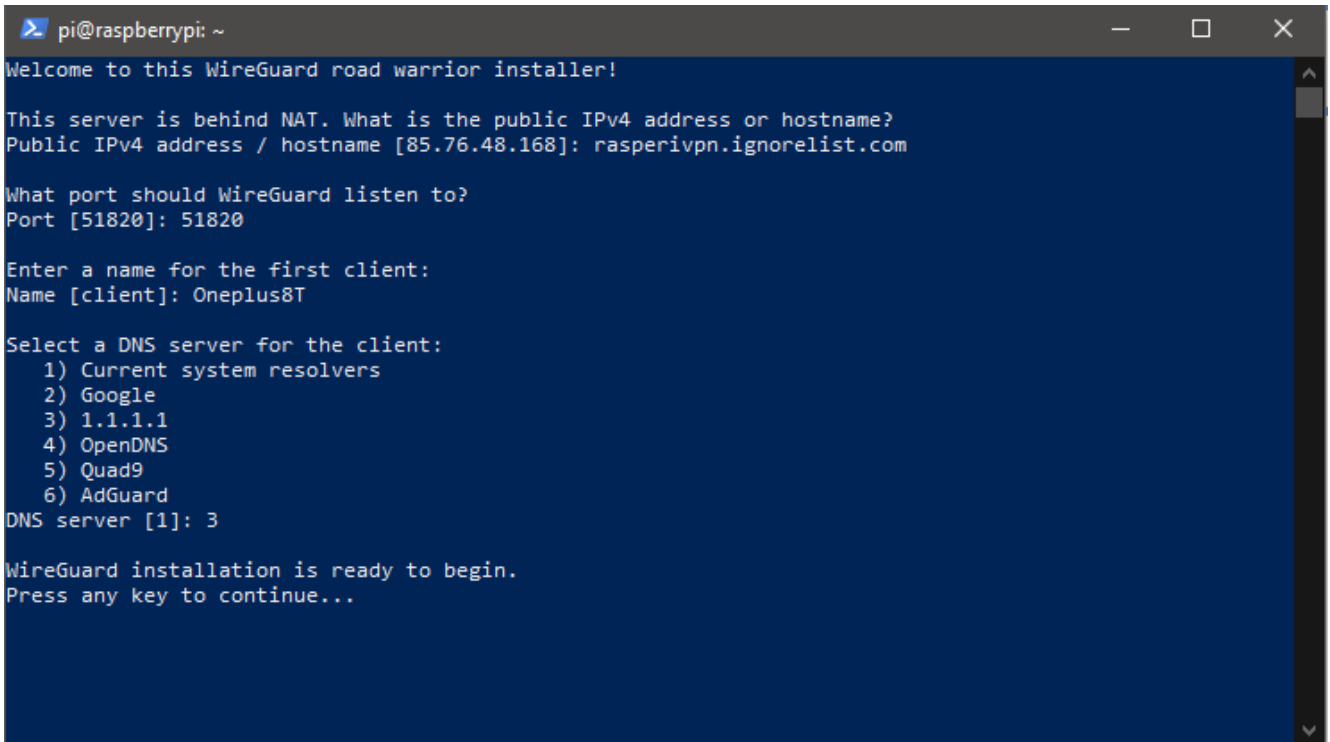
Sisäinen portti (valinnainen)
51820

Protokolla
UDP

Kuva 11. Reitittimen portin edelleenlähetysasetukset.

6.4 Wireguard-VPN-palvelimen asennus

Wireguard-VPN-palvelimen asentaminen Raspberry Pi -laitteelle onnistuu helposti seuraavalla skriptillä jonka github-käyttäjä Nyr on tehnyt: “wget https://git.io/wireguard -O wireguard-install.sh && bash wireguard-install.sh” (<https://github.com/Nyr/wireguard-install>).



```
pi@raspberrypi: ~
Welcome to this WireGuard road warrior installer!

This server is behind NAT. What is the public IPv4 address or hostname?
Public IPv4 address / hostname [85.76.48.168]: rasperivpn.ignorelist.com

What port should WireGuard listen to?
Port [51820]: 51820

Enter a name for the first client:
Name [client]: Oneplus8T

Select a DNS server for the client:
 1) Current system resolvers
 2) Google
 3) 1.1.1.1
 4) OpenDNS
 5) Quad9
 6) AdGuard
DNS server [1]: 3

WireGuard installation is ready to begin.
Press any key to continue...
```

Kuva 12. Wireguard-VPN-palvelimen asennus.

Skripti kysyy julkista IP-osoitetta tai isäntänimeä, tähän tulee DDNS-verkkotunnus joka luotiin aikaisemmassa vaiheessa. Seuraavaksi kysytään laitteen nimeä, jolla VPN-verkkoa käytetään. Viimeiseksi tulee kertoa, mitä DNS-palvelinta halutaan käyttää. Näihin kysymyksiin vastaamisen jälkeen skripti asentaa Wireguard-VPN-palvelimen Raspberry Pi -laitteelle.

6.4.1 Wireguard-sovelluksen asentaminen älypuhelimelle

Wireguard-VPN-palvelin tarvitsee toimiakseen ohjelmiston, joka yhdistää palvelimelle. Wireguardin sovelluksen voi ladata ilmaiseksi Android laitteelle Google playsta ja iPhone älypuhelimelle App storesta.

Wireguard (App Store): <https://apps.apple.com/us/app/wireguard/id1441195209>

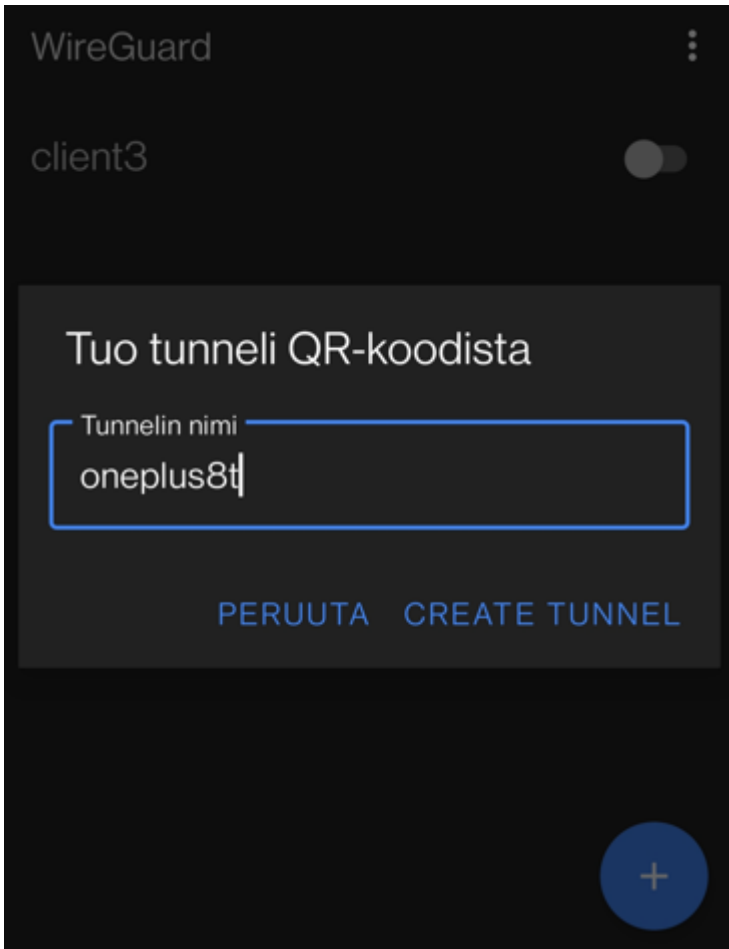
Wireguard (Google Play): <https://play.google.com/store/apps/details?id=com.wireguard.android>

Laite yhdistetään VPN-palvelimeen klikkaamalla sovelluksen oikeassa alanurkassa olevaa sinistä plusmerkkiä. Sovellus pyytää lukemaan QR-koodin, joka tulee komentorivin ikkunaan asennuksen päätyttyä.



Kuva 13. QR-koodi Windows PowerShell -sovelluksessa.

Älypuhelimien kameralla luetaan QR-koodi. Se tuo VPN-sovellukseen asetukset, joilla yhdistetään VPN-palvelimelle.



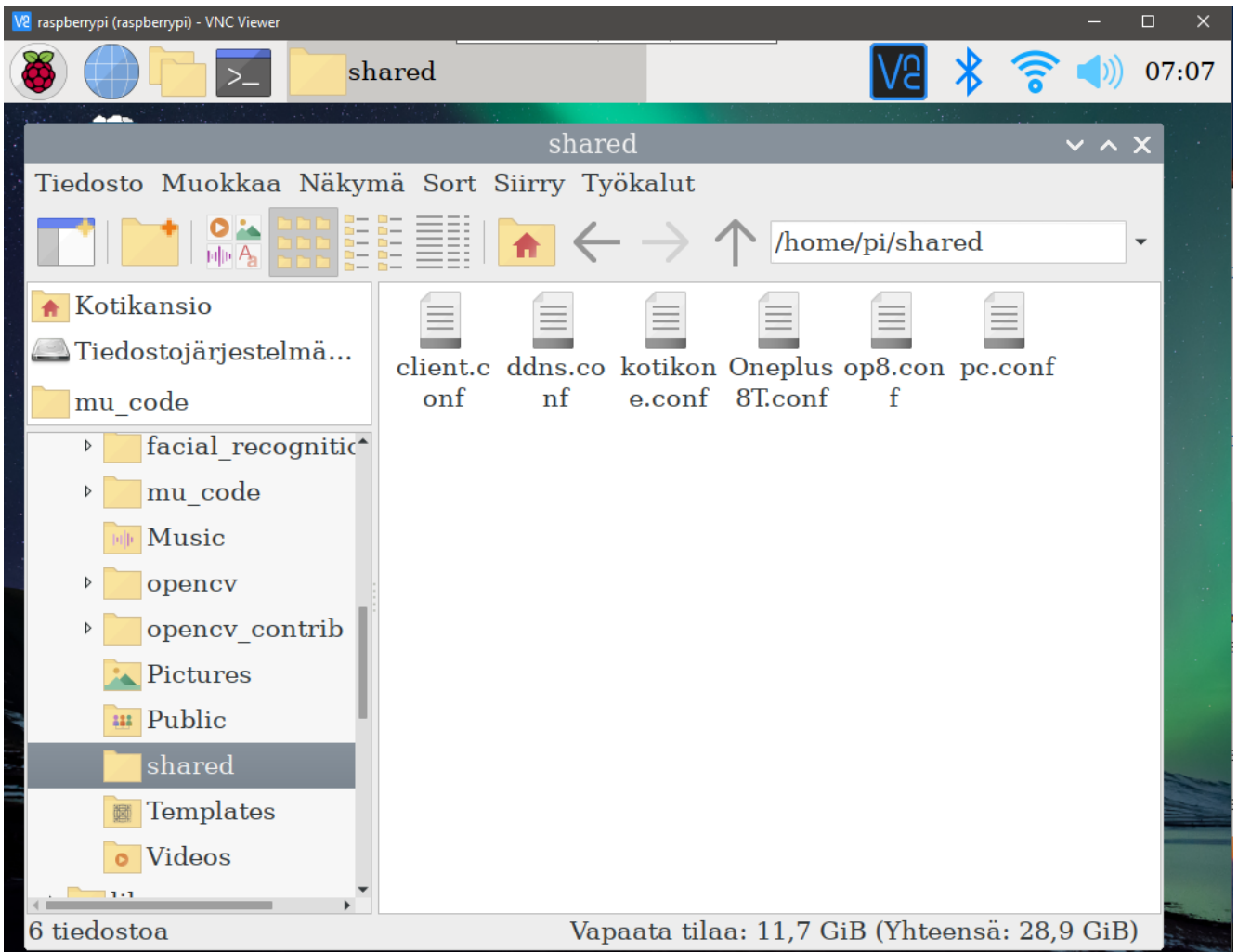
Kuva 14. VPN-asetusten tuominen älypuhelimeen QR-koodilla.

6.4.2 Wireguard-sovelluksen asentaminen tietokoneelle

Tietokoneen yhdistäminen Wireguard VPN -palvelimelle onnistuu tuomalla asetustiedostot Raspberry Pi -laitteelta tietokoneelle käyttäen verkko-asemaa, joka luotiin aikaisemmassa vaiheessa. Asetustiedostot siirretään shared-kansioon, jolloin ne tulevat näkyviin verkko-asemalla. Koska asetustiedostot menevät juurihakemistoon, Raspberry Pi -laitteella tarvitaan root-käyttäjän oikeudet tiedostojen siirtoon.

Root on Unix/Linux-järjestelmien pääkäyttäjä. Root-käyttäjällä on oikeudet tehdä järjestelmässä käytännössä mitä vain.

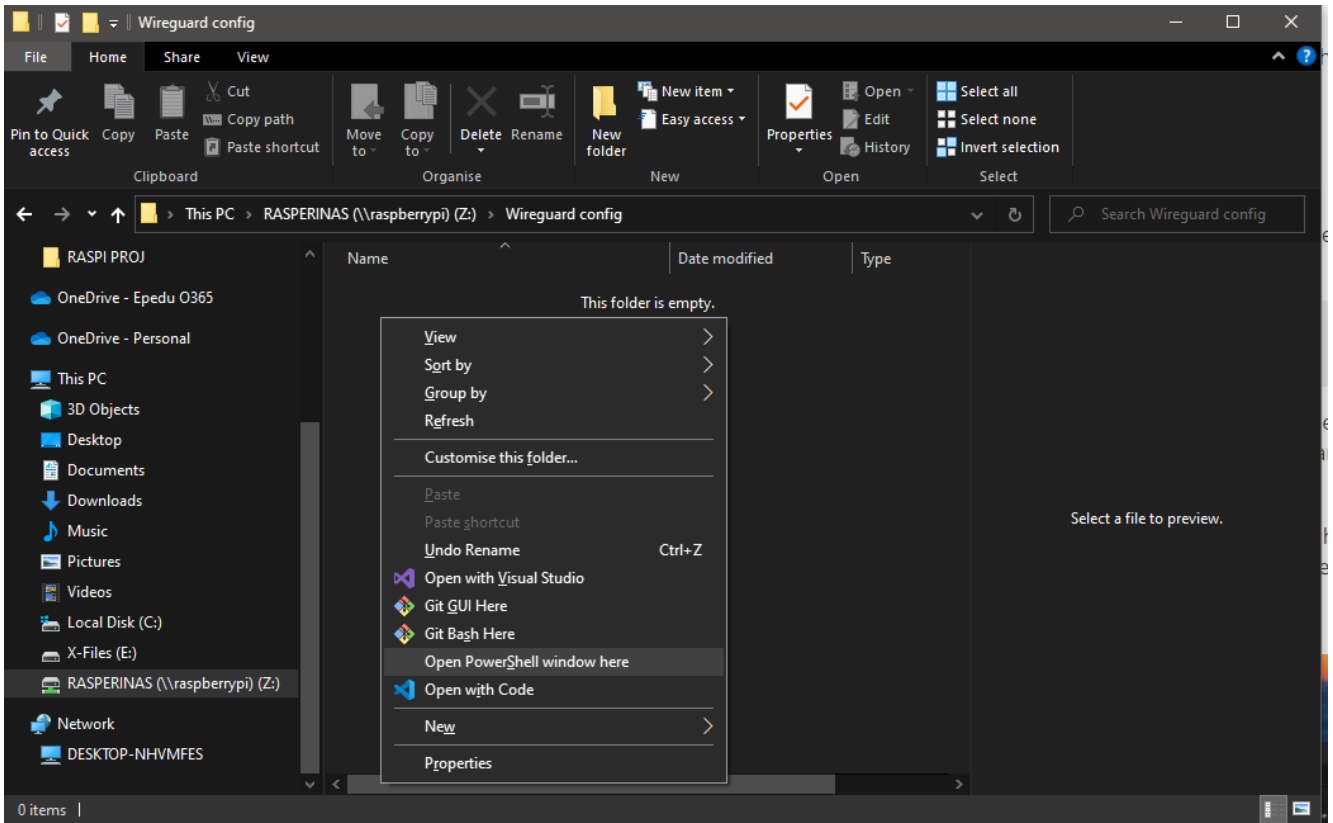
Root-käyttäjäksi kirjaudutaan komennolla “sudo su” ja kopioidaan asetustiedostot juurihakemistosta komennolla “cp /root/*.conf /home/pi/shared”. Komento siirtää kaikki .conf-päätteiset tiedostot root-hakemistosta polun hakemistoon.



Kuva 15. Asetustiedostot verkkoasemalla. Raspberry Pi -laitteella asema esiintyy normaalina kansiona.

Tiedostot voidaan siirtää tietokoneelle myös SFTP-yhteyttä käyttäen luomalla uusi kansio asetustiedostoille haluttuun paikkaan. Luodaan kansio “Wireguard config” verkkoasemalle. Avataan Windows PowerShell -sovellus suoraan kansiota klikkaamalla tyhjää tilaa kansion

sisällä hiiren oikealla näppäimellä ja Avaa PowerShell ikkuna tähän, kuten kuvassa (16). Komentorivi-ikkuna saa automaattisesti oikean polun hakemistoon.

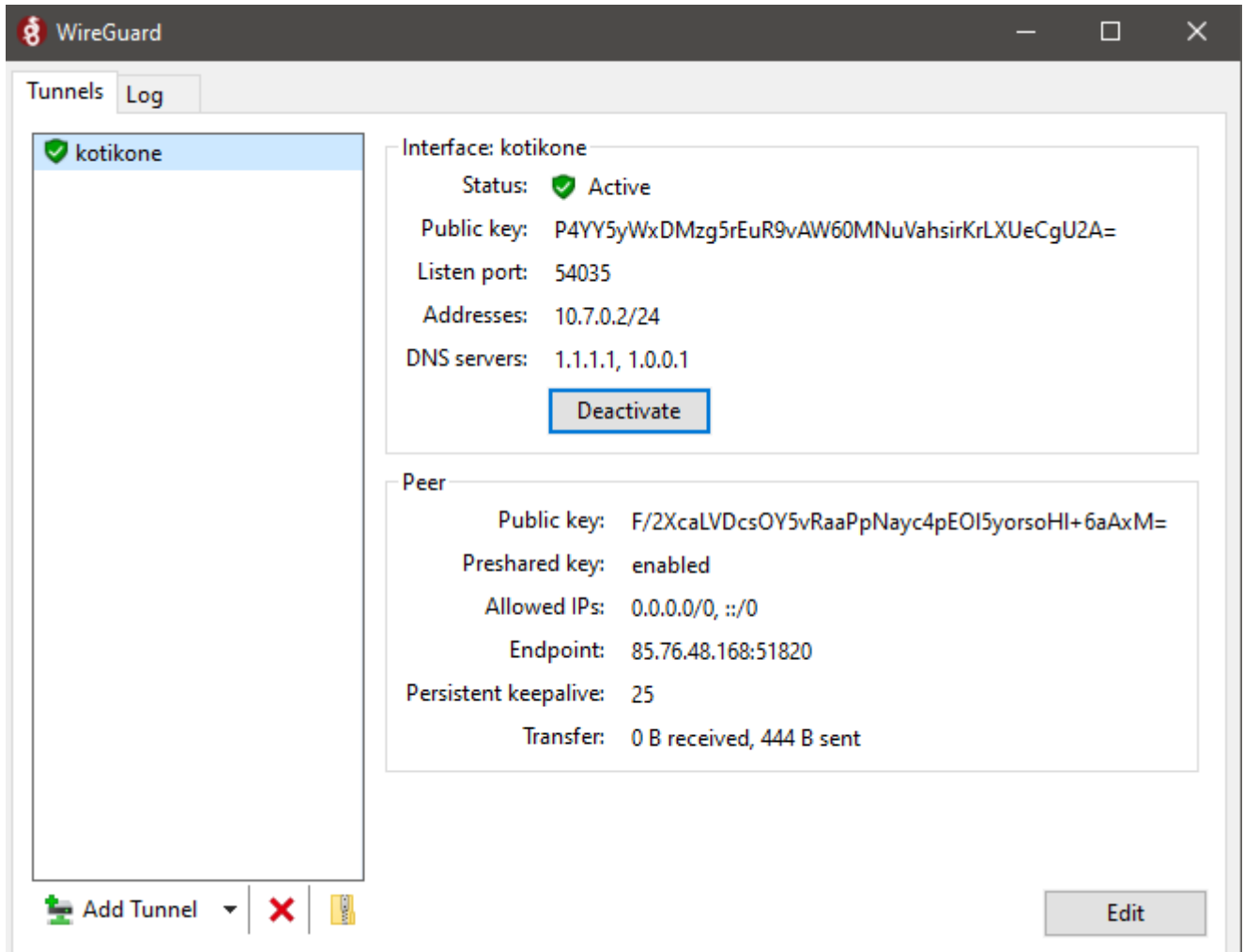


Kuva 16. Windows PowerShell -komentorivi-ikkunan avaaminen kansioista.

Yhdistetään Windows PowerShell Raspberry Piin SFTP-yhteyttä käyttäen komennolla “sftp pi@[laitteen ip-osoite]”. Nyt voidaan siirtää tiedostot kansioon käyttämällä komentoa “get *.conf”, joka siirtää kaikki .conf-päätteiset tiedostot hakemistoon, missä Windows PowerShell avattiin. Käyttäjätavallisempi tapa siirtää tiedostoja SFTP-yhteyden kautta on siihen tarkoitetuilla ohjelmilla esimerkiksi FileZilla.

Tietokoneelle asennetaan Wireguard-sovellus. Sovelluksen voi ladata ilmaiseksi osoitteesta: <https://www.wireguard.com/install/>

Wireguard sovelluksessa painetaan Add tunnel -painiketta ja valitaan luotu asetustiedosto. Tämän jälkeen painetaan painiketta Activate jolloin ohjelma yhdistää tietokoneen VPN-palvelimeen.



Kuva 17. Wireguard ohjelma on yhdistänyt VPN-palvelimeen.

7 Yhteenveto

Tässä opinnäytetyössä tutkittiin Linux-pohjaisia käyttöjärjestelmiä ja niiden eroja, lisäksi selvitettiin mihin tarkoitukseen eri käyttöjärjestelmiä on kehitetty, vertailtiin Linuxia Windowsiin sekä tehtiin toimiva VPN-palvelin lähiverkon laitteille. VPN-palvelin asennettiin Raspberry Pi -tietokoneelle joka käyttää Linux-Debian pohjaista Raspberry Pi OS -käyttöjärjestelmää. Raspberry Pi -laitteesta tehtiin myös verkkoasema, jonka avulla lähiverkon laitteet voivat jakaa tiedostoja käyttöjärjestelmästä riippumatta. VPN suojaa laitteiden IP-osoitteet ja kaikki dataliikenne tapahtuu VPN-palvelimen kautta. Lähiverkkoon voidaan yhdistää ulkoisesta verkosta esimerkiksi älypuhelimien mobiiliverkosta, jolloin on pääsy lähiverkon muihin laitteisiin ja tiedostoihin. Internetin selaaminen tapahtuu kuin lähiverkosta suojatulla yhteydellä.

Koska tämä VPN-palvelin toimii kotiverkossa, ei sillä voida kiertää maakohtaisia rajoituksia, mitä esimerkiksi suoratoistopalveluissa voi esiintyä.

LÄHTEET

Andreas, K. Port Forwarding – *What is it & How Can it Help You in 2022?* WizCase. <https://www.wizcase.com/blog/everything-you-need-to-know-about-port-forwarding/>

Delony, D. (7.2.2022). *5 Reasons to Install Linux on Old Computer*. MakeUseOf (MUO). <https://www.makeuseof.com/why-install-linux-old-computer/>

Fromaget, P. (i.a.). *What's the best micro sd card for raspberry pi? (benchmark)*. Raspberry-Tips. <https://raspberrytips.com/best-sd-card-raspberry-pi/>

F-secure. (i.a.). *Mikä on VPN?*. <https://www.f-secure.com/fi/home/articles/what-is-a-vpn>

Hoffman, C. (23.9.2016). *What is a Linux Distro, and how are they different from one another?* How-to Geek. <https://www.howtogeek.com/132624/htg-explains-whats-a-linux-distro-and-how-are-they-different/>

Hoffman, C. (11.7.2017). *Why You Don't Need an Antivirus On Linux (Usually)*. How-To Geek. <https://www.howtogeek.com/135392/htg-explains-why-you-dont-need-an-antivirus-on-linux-and-when-you-do/>

Howchoo. (i.a.). *How to Use Raspberry Pi Imager*. <https://howchoo.com/pi/raspberry-pi-imager>

Kainulainen, S. (i.a.). *Linux – Jakelut*. Emute. <https://emute.edu.fi/kayttojarjestelmat/linux-jakelut>

Linux.com. (i.a.). *What is Linux?* <https://www.linux.com/what-is-linux/>

McCann, M. & Hardy, A. (25.1.2022). *9 Reasons Why Everyone Should Use A VPN. Yes, Even Non-Techies*. Forbes Advisor. <https://www.forbes.com/advisor/business/software/why-use-a-vpn/>

Mills, Matt. (17.5.2021). *Programmin in Linux: Advantages Over Windows and macOS*. <https://itigic.com/programming-in-linux-advantages-over-windows-and-macos/>

Mitchell, B. (22.6.2021). *What Does Dynamic DNS Mean?* Lifewire.
<https://www.lifewire.com/definition-of-dynamic-dns-816294>

Mocan, T. (3.9.2018). *VPN History & The Future of VPN Technology.* CactusVPN.
<https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-history/>

Peda.net (i.a.) *Raspikoulu. Mikä Raspberry Pi?* <https://peda.net/jyu/it/koulutusteknologia/opintojaksot/TIES461/ah/harjoitusty%C3%B6t/oaahjv/materiaali/mik%C3%A4-raspberry-pi>

Petrit.net (i,a). *Linux-jakelut.* <https://petrit.net/Linux-kurssi/johdanto/jakelut/>

Raspberry Pi, (i.a.-a). *Raspberry Pi 3 Model B.* <https://www.raspberrypi.com/products/raspberry-pi-3-model-b/>

Raspberry Pi b. (i.a.-b). *Raspberry Pi Documentation.* Raspberry Pi OS. <https://www.raspberrypi.com/documentation/computers/os.html>

Hertel, C. (27.11.2001). *Samba: An Introduction.* <https://www.samba.org/samba/docs/SambaIntro.html>

ThePiHut. (2014). *How do I power my Raspberry Pi?* <https://thepihut.com/blogs/raspberry-pi-tutorials/how-do-i-power-my-raspberry-pi>

Upton, E. (8.9.2016). *Raspberrypi. Ten Millionth Raspberry Pi, And a New Kit.*
<https://www.raspberrypi.org/blog/ten-millionth-raspberry-pi-new-kit/>.

VPN-yhteydet.fi. (9.5.2021). *Mikä on VPN ja miten saan sen käyttöön?.* <https://www.vpn-yhteydet.fi/mika-on-vpn/>

Wikipedia. *NTFS.* <https://fi.wikipedia.org/wiki/NTFS>

Zinoune, M. (i.a.). *Meet Linux Viruses.* *Unixmen.* <https://www.unixmen.com/meet-linux-viruses/>

