

Antti Pyhäluoto

VERKKOSALAUSTEKNIIKOIDEN VERTAILU

VERKKOSALAUSTEKNIKOIDEN VERTAILU

Antti Pyhäluoto
Opinnäytetyö
Syksy 2021
Tietotekniikan tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma, laite- ja tuotesuunnittelu

Tekijä: Antti Pyhäluoto

Opinnäytetyön nimi suomeksi: Verkkosalaustekniikoiden vertailu

Opinnäytetyön nimi englanniksi: Comparison of network encryption techniques

Työn ohjaajat: Teemu Korpela, Jyrki Kennilä

Työn valmistumislukukausi ja -vuosi: syksy 2021

Sivumäärä: 55 + 10 liitettä

Opinnäytetyön aiheena oli eri verkkosalaustekniikoiden vertaileminen. Tavoitteena oli selvittää, miten vertailut teknikat vertautuvat toisiinsa ja mikä testatuista tekniikoista olisi suorituskyvyltään paras vaihtoehto käyttöönotettavaksi.

Työssä vertaillaan IPseciä kolmella eri salauksella, MACseciä, OpenVPN:ää ja WireGuardia toisiinsa ja vertailukohteeseen, missä mikään näistä ei ole käytössä. Vertailu suoritetaan ideaalitulanteessa ja useilla eri häiriötyypeillä. Testaamiseen käytetään iPerf-, ping- ja scp-ohjelmia eri tilanteiden testaamiseen ja NetEm-ohjelmaa häiriöiden simuloimiseen. Testaus suoritetaan Raspberry Pi 4 -laitteilla ilman salauksen laitteistokiihdytystä. Käytännön testien suorittamisen, tulosten keräämisen ja tekniikoiden käyttöön ja pois käytöstä ottamisen automatisoimiseen käytetään itse tehtyä test_system.py-ohjelmaa.

Testatuista tekniikoista paras suorituskky on WireGuardilla ja toiseksi paras IPsecillä ChaCha-salausta käytettäessä. Näiden kahden suorituskky ei ole myöskään tulosten perusteella erityisen herkkä testatuille häiriötyypeille. Kaikilla muilla tekniikoilla käytössä on jokin AES-pohjainen salaus ja laitteistokiihdytyksen puute huonontaa näiden tekniikoiden suorituskkyä.

Asiasanat: salausalgoritmi, Raspberry Pi 4, suorituskkyvertailu, IPsec, MACsec, OpenVPN, WireGuard

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Information Technology, option of Device and Product Design

Author: Antti Pyhäluoto
Title of thesis: Comparison of network encryption techniques
Supervisors: Teemu Korpela, Jyrki Kennilä
Term and year when the thesis was submitted: Fall 2021
Pages: 55 + 10 appendices

The subject of this thesis is to compare different network encryption techniques. The aim is to study how techniques compare to each other and which of the studied techniques would have the best performance in the tested or similar hardware.

Compared network encryption techniques consist of IPsec with three different encryptions, MACsec, OpenVPN and WireGuard. Tests are also run without any of the previous enabled as a control group. Comparison is performed in an ideal network condition and with multiple different network interference types. iPerf, ping and scp are used to test different use cases. Testing is performed on Raspberry Pi 4 computers without hardware acceleration for encryption.

WireGuard has the best performance of the tested techniques and IPsec with ChaCha encryption has the second best. Also, neither techniques performance was especially sensitive to the tested interference types. All other techniques utilized AES-encryption in some form and thus their performance was weakened by the lack of hardware acceleration.

Keywords: cipher, Raspberry Pi 4, performance comparison, IPsec, MACsec, OpenVPN, WireGuard

SISÄLLYS

TIIVISTELMÄ	1
ABSTRACT	2
SISÄLLYS	3
1 JOHDANTO	5
2 POHJATIEDOT	6
2.1 VPN-tekniikoiden käyttökohteet	6
2.2 Vertailtavat toteutukset	6
2.2.1 IPsec ja IKEv2	7
2.2.2 IEEE 802.1AE - MACsec ja MKA	9
2.2.3 OpenVPN	10
2.2.4 WireGuard	10
3 TESTAAMINEN JA TULOSTEN KERÄÄMINEN	13
3.1 Testauslaitteisto	13
3.2 Testausympäristö	13
3.3 Testausmenetelmä	14
3.3.1 iperf	14
3.3.2 NetEm ja tc	15
3.3.3 test_system.py	16
3.4 Ajettavat testit	18
4 MITTAUSTULOKSET	22
4.1 Ideaaliverkko	22
4.1.1 Ping-testi ja MTU	22
4.1.2 TCP-testi	23
4.1.3 UDP-testit	26
4.1.4 SCP-testi	32
4.2 Häiriöinen verkko	34
4.2.1 Viiveen vaikutus	34
4.2.2 Jitterin vaikutus	36
4.2.3 Pakettien pudotuksen vaikutus	39
4.2.4 Viiveen, jitterin ja pakettien pudotuksen yhteisvaikutus	43
4.3 Johtopäätökset	47

5 YHTEENVETO	50
LÄHTEET	52
LIITTEET	55

1 JOHDANTO

Bittium on suomalainen tietoturvallesiin laitteisiin ja liitettävyyssratkaisuihin erikoistunut yritys. Bittiumin tuotteisiin kuuluu mm. viranomaiskäyttöön suunnattu Tough Mobile 2 -älypuhelin ja armeijakäyttöön suunnattu Tactical Wireless IP Network -verkkoratkaisu, joka sisältää kaiken runkoverkosta sitä hyödyntäviin päätelaitteisiin. Bittiumin pääkonttori sijaitsee Oulussa. (1.)

Työn tarkoituksena on selvittää, miten eri verkkosalaustekniikat vertautuvat kais-tanleveyden, prosessorin ja muistin käytön kannalta toisiinsa ja vertaillaan niitä tilanteeseen, missä mitään salaustekniikkaa ei ole käytössä. Verkkosalaustekniikoita testaus suoritetaan ideaalitalanteessa sekä usealla eri keinotekoisesti lisä-tyllä häiriöparametrilla ja niiden yhdistelmällä. Lisäksi jokaisesta testattavasta verkkosalaustekniikasta selvitetään pääpiirteittäin, miten salaus on niissä toteutettu ja mitä salaukseen liittyviä algoritmeja niissä on käytössä.

Tässä raportissa kerrotaan ensimmäisenä, mitkä ovat yleiset käyttökohteet salaustekniikoille ja käydään läpi vertailtavat toteutukset ja niiden tärkeimmät vertailtavat ominaisuudet. Itse testaamisesta käydään läpi testiympäristö, sen valintaperusteet, testaamisessa käytettävä laitteisto, ohjelmisto ja parametrit, mihin testaaminen keskittyy. Mittaustulokset käydään läpi ja niiden perusteella johdetaan perustelut, mikä tai mitkä toteutukset parhaiten suoriutuvat testatulla laitteistolla.

2 POHJATIEDOT

2.1 VPN-tekniikoiden käyttökohteet

Virtual Private Network (VPN) -tekniikoilla voidaan yhdistää sisäverkkoja julkisen internetin yli ja tätä varten on olemassa useita toteutuksia, joita tämän työn tarkoituksen on vertailla. VPN-tekniikoiden käyttökohteita ovat esimerkiksi mahdollistaa pääsy yrityksen sisäverkkoon julkisesta verkosta ja yrityksen kahden eri konttorin sisäverkkojen yhdistäminen. (2; 3.)

Näissä tapauksissa VPN:n läpi menevä liikenne on normaalia internetliikennettä. Se voi sisältää mm. tiedostojen lataamista ja lähettämistä, reaaliaikaista ääni- ja videoliikennettä ja kaikkea siltä väliltä.

Tietoturvan näkökulmasta VPN:n läpi menevä liikenne on yleensä salattu, jolloin ulkopuoliset eivät sitä voi lukea. VPN:n rakenteeseen myös yleensä kuuluu suojausta toistetun liikenteen varalta. Sen johdosta mikä tahansa yksittäinen VPN:n paketti hyväksytään vain kerran. Lisäksi VPN:nä käytettäessä voidaan olla varma vastapuolen identiteetistä. (2; 3.)

2.2 Vertailtavat toteutukset

Toteutuksia vertailussa keskitytään toteutusten Linux-versioihin. Vertailussa käytetyn Linux-ytimen ja toteutusten versiot on listattuna liitteessä 1. Taulukossa 1 on yhteenveto toteutusten ominaisuuksista.

TAULUKKO 1. Toteutusten ominaisuuksien yhteenveto.

	IPsec (4, s. 3, 18, 19)	MACsec (5, s. 4, 5, 23, 45)	OpenVPN (6)	WireGuard (7, s. 1,3,4)
IPv6-tuki	Kyllä	-	Kyllä	Kyllä
OSI-taso	Taso 3	Taso 2	Taso 3	Taso 3
Split-tunnelit	Tuettu	Virtual Inter- face	Virtual Inter- face	Virtual Inter- face
IP-verkon vaatimukset	UDP, ESP ja AH sallittu	-	UDP tai TCP sallittu	Yksi UDP portti sallittu
Laitteistokiihdytys mahdollista	Riippuu salauksesta	Kyllä	Riippuu salauksesta	Ei
Käyttäjä vai ydinavaruus	Ydin	Ydin	Käyttäjä	Ydin
Avoin lähdekoodi	Kyllä	Kyllä.	Kyllä.	Kyllä

2.2.1 IPsec ja IKEv2

IPsec on suunniteltu lisäämään tietoturvallinen salaaminen IP-liikenteeseen, sillä IP-protokollaan ei kuulu tietoturva ominaisuuksia. IPsec itsessään ei määrittele käytettäviä algoritmeja salaukseen ja tunnistukseen, vaan ne ovat määriteltä eri-
lisessä RFC-dokumentissa. (4, s. 4.)

RFC 8221 määrittelee vaatimukset, mitä salausalgoritmeja IPsec toteutusten täy-
tyy tukea ja RFC 8247 määrittelee, mitä algoritmeja IPsecin käyttämän IKEv2-
protokollan täytyy tukea, kun taas RFC 7296 määrittelee itse IKEv2-protokollan
(8, s. 1; 9, s. 1; 10, s. 1). IPsecin viimeisin määritelmä on RFC 4301:ssä (4, s. 1).

IPsecin Security Association (SA) kuvaa yksisuuntaista tietoliikenneyhteyttä ja koostuu yhteydelle käytettävästä protokollasta, Encapsulating Security Payload (ESP) tai Authentication Header (AH), ja näiden protokollien käyttämistä parametreista ja avaimista. Kun halutaan luoda kaksisuuntainen yhteys, tarvitaan yksi SA molempiin suuntiin. Jos halutaan käyttää ESP:tä ja AH:ta, molemmille määritellään yhteen suuntaan omat SA:t. (4, s. 12.)

SA:iden automaattista luomista varten on olemassa Internet Key Exchange version 2 (IKEv2) -protokolla. Sen tehtävänä on SA:iden neuvottelu ja SA:iden ylläpitäminen. IKEv2 hoitaa nämä asiat omille SA:ille ja IPsecin SA:ille. Neuvotteluun kuuluu käytettävän IPsec-protokollan, salausalgoritmin ja salausavainten valinta. Onnistuneen neuvottelun lopputuloksena molemmilla osapuolilla on tarvittavat tiedot tiedon suojaamiseksi IPsecin avulla. (10, s. 6.)

IPsec määrittelee kaksi protokollaa, joita voidaan käyttää yhdessä tai erikseen: Authentication Header (AH) ja Encapsulating Security Payload (ESP). AH:ta käytettäessä dataa ei ole salattu, alkuperäinen data lähetetään sellaisenaan, mutta datan eheys ja lähettäjän voidaan todentaa. ESP:tä käytettäessä data salataan ja datan eheys ja lähettäjän voidaan todentaa. Periaatteessa on mahdollista käyttää AH:ta ja ESP:tä yhtä aikaa, mutta RFC 4301 ei vaadi tätä toiminnallisuutta. (4, s. 9, 17.)

Testauksessa käytettiin StrongSwan-ohjelmaa yhteyden luomiseen. Linuxilla käytettäessä StrongSwan, LibreSwan tai OpenSwan huolehtivat IKEv2-protokollan toteuttamisesta eli SA:iden muodostamisesta ja itse tiedon salaamisesta ja purkamisesta huolehtii Linux-ytimen IPsec-toteutus.

Manuaalinen IPsecin käyttöön ottaminen koostuu konfiguraatitiedoston määrittelemisestä ja StrongSwan-ohjelman käynnistämisestä (11). Testaamista varten on tehty kolme konfiguraatitiedostoa, jotka ovat muuten samanlaisia mutta käyttävät eri salausalgoritmia tiedon salaamiseen. Tällöin saadaan IPsec käyttämään samaa salausalgoritmia kuin WireGuard (ChaCha20Poly130) ja MACsec (GCM-AES-128), jolloin saadaan parempi kuva itse toteutuksen suorituskyvystä ilman salausalgoritmin vaikutusta. Konfiguraatitiedostot ovat luettavissa liitteessä 2.

2.2.2 IEEE 802.1AE - MACsec ja MKA

IEEE 802.1AE MACsec on IEEE 802.1:n määrittelemä verkkostandardi Ethernet liikenteen yhteyksien suojaamiseksi. MACseciä käytettäessä läpi menevä dataa salataan, sen eheys varmistetaan ja sen lähettäjän identiteetti voidaan todentaa. (8, s. 4, 9)

MACsec on toteutettu virtuaalisena verkkoliitännänä (8, s. 23). Tämä mahdollistaa usean MACsec liitännän luomisen yhden fyysisen liitännän päälle. Myös liikenteen reititykseen voidaan käyttää käyttöjärjestelmän reititystauluja.

MACsec yhteys itsessään koostuu konsepteista Secure Channel (SC) ja Secure Association (SA). SC kuvastaa yksisuuntaista tietoliikenne yhteyttä. Eli kaksisuuntainen yhteys kahden laitteen välillä vaatii yhden SC:n lähettämiseen ja yhden SC:n vastaanottamiseen. Jokaisella MACsec verkkoliitännällä on yksi SC lähettämiseen ja voi olla useita SC:tä vastaanottamiseen. SC:n sisällä voi olla enintään neljä SA:ta. Jokaisella SA:lla on uniikit avaimet liikenteen salaamiseen. Usean SA:n ansiosta per SC käytettäviä salausavaimia voidaan vaihtaa lennosta ilman yhteyden katkeamista. (8, s. 6.)

MACsecin konfigurointi voidaan suorittaa luomalla manuaalisesti kaikki tarvittavat SC:t, niiden SA:t ja käytetyt avaimet halutuille laitteille tai voidaan hyödyntää MACsec Key Agreement (MKA) -protokollaa. MKA:ta käytettäessä protokolla huolehtii tarvittavien SC:iden ja SA:iden luomisesta laitteiden välille ja näiden käyttämien avaimien luomisesta. (8, s. 7; 12, s. 5–6.)

Testauksessa MACsec otetaan käyttöön hyödyntämällä wpa_supplicant-ohjelmaa. MACsec otetaan käyttöön komennolla:

- wpa_supplicant -c /home/pi/macsec/wpa_supplicant.conf -i eth0 -D macsec_linux

-c määrittelee käytettävän konfiguraatio tiedoston, -i määrittelee, mihin verkkolaitteeseen MACsec liitetään ja -D määrittelee käytettävän ajurin (13; 14). Käytetty wpa_supplicant.conf.mac tiedosto on luettavissa liitteessä 3.

2.2.3 OpenVPN

OpenVPN on alun perin James Yonan kehittämä avoimen lähdekoodin VPN ohjelmisto, jonka kehitys nykyisin tapahtuu OpenVPN-projektin toimesta.

OpenVPN hyödyntää tietojen salaamiseen kokonaan OpenSSL-kirjastoa, ja tukee näin samoja salaus ja todennus menetelmiä kuin OpenSSL. Tunnelin luomiseen ja vastapuolten autentikoimiseen OpenVPN käyttää SSL/TLS-protokollaa, ja itse tiedonsiirtoon OpenVPN käyttää IPsecin ESP-protokollaa. (6.)

OpenVPN on laajasti muokattavissa eri käyttökohteita varten. OpenVPN voi muodostaa tunnelin joko TCP tai UDP-yhteyden yli, voi luoda OSI-mallin 2- tai 3-tason tunnelin ja tukee tunnistautumista joko salasanojen avulla tai sertifikaattien avulla. (6.)

OpenVPN:n on toteutettu virtuaalisena verkkoliitännänä. Läpi menevä liikenne voidaan tällöin määritellä käyttämällä käyttöjärjestelmän yleistä reititystaulua. (6.)

OpenVPN:ää hallitaan `openvpn`-komennolla. Testauksessa OpenVPN otetaan käyttöön komennolla:

- `openvpn /home/pi/openvpn/server.conf`

Komennolle annetaan ainoastaan polku käytettävään konfiguraatiotiedostoon. Konfiguraatiotiedoston lisäksi OpenVPN:n toiminnallisuutta voidaan hallita `openvpn`-ohjelmalle annettavilla lisääargumenteilla.

Testauksessa käytetyt konfiguraatiotiedostot ovat luettavissa liitteessä 4.

2.2.4 WireGuard

WireGuard on Jason A. Donenfeldin kehittämä VPN-ohjelmisto. WireGuardin tavoitteina on ollut olla mahdollisimman yksinkertainen ottaa käyttöön ja ylläpitää, mutta olla kuitenkin mahdollisimman nopea ja tietoturvallinen. Aluksi se oli toteutettu Linuxin ytimeen mutta on nyt saatavissa mm. Windowsille, macOS:lle, BSD:lle, iOS:lle ja Androidille. (15.)

WireGuard on toteutettuna virtuaalisena verkkoliitännänä. WireGuardin läpi menevä liikenne voidaan tällöin määritellä käyttämällä käyttöjärjestelmän yleistä reititystaulua. (7, s. 3.)

WireGuardin virtuaalisen verkkoliitännän konfiguraatio koostuu normaalista liitännän IP-osoitteesta ja maskista, liitännän omasta yksityisestä avaimesta, portista, jota kuunnella ja listasta vertaisia eli laitteista, joiden kanssa halutaan kommunikoida WireGuardin läpi. Yksi listan merkintä koostuu vertaisen julkisesta avaimesta, vertaisen sallituista IP-osoitteista (lähettämistä ja vastaanottamista varten WireGuardin sisällä) ja vertaisen julkisesta IP-osoitteesta, joka on voitu asettaa etukäteen. Jos IP-osoitetta ei ole esiasetettu, vertaisen kanssa ei voi kommunikoida kuin vasta vertaisen yhteydenoton jälkeen. (7, s. 4; 16)

Avainten vaihtotapaan WireGuard ei ota kantaa eikä sillä ole mitään protokollaa sitä varten. Kunhan vertaiset vaihtavat julkisia avaimiaan, vertaisten välinen kommunikaatio voidaan salata. (7, s. 3.)

Vertainen voidaan konfiguroida esimerkiksi seuraavilla komennoilla (17; 18):

- ip link add wg0 type wireguard
- ip addr add 10.0.0.1/24 dev wg0
- wg set wg0 private-key ./private
- wg set wg0 listen-port 51820
- ip link set wg0 up
- wg set wg0 peer NZyYbm1yZ7/8q/7Vh33hDk22iT/Dowf45053s1z5lX8= allowed-ips 10.0.0.2/32 endpoint 169.254.16.161:51820

Selitykset komennoille (17; 18):

- Luodaan virtuaalinen verkkoliitäntä wg0.
- Annetaan wg0:lle IP-osoite 10.0.0.1 ja maski /24
- Asetetaan wg0-liitännälle yksityinen avain tiedostosta.
- Määritetään portti WireGuard-liikenteelle.
- Käynnistetään wg0-liitäntä.

- Määritellään vertainen wg0-liitännälle kertomalla vertaisen julkisen avain, WireGuardin läpi menevä IP-avaruus ja vertaisen IP WireGuardin ulkopuolella.

WireGuardin käyttöönotossa voi hyödyntää myös wg-quick-työkalua, joka lataa kaikki tarvittavat konfiguraatiot yhdestä tiedostosta (19). Yllä olevat konfiguraatiot saa käyttöön myös lataamalla liitteessä 5 olevat konfiguraatitiedoston wg0-raspi1.conf tai wg0-raspi2.conf komennolla:

- `wg-quick up /home/pi/wireguard/wg0-raspi1.conf`

3 TESTAAMINEN JA TULOSTEN KERÄÄMINEN

3.1 Testauslaitteisto

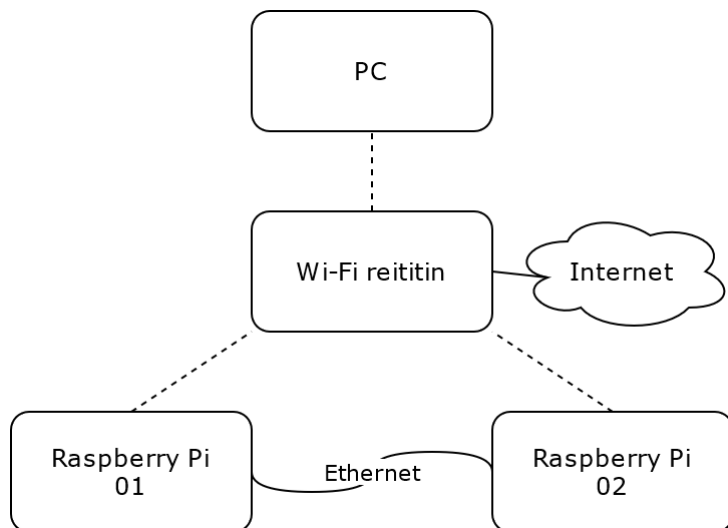
Testaus suoritettiin kahdella Raspberry Pi 4 Model B -tietokoneella. Muita harkittuja vaihtoehtoja olivat virtuaalikoneet ja tuotekehityksessä käytetyt kehitysalustat.

Raspberry Pi 4 -laitteet valittiin aiempien Raspberry Pi 3 -laitteiden sijasta, sillä vaikka Raspberry Pi 3 -laitteissakin on 1 Gbit Ethernet-liittimet, ne kulkevat USB 2:n läpi. Tästä johtuen Raspberry Pi 3 -laitteiden Ethernet-porttien kaistanleveys on 300 Mbit/s. (20; 21). Lisäksi Raspberry Pi -laitteita on helposti saatavilla, ovat edullisia ja Raspberry Pi -laitteita käytettäessä ei tarvitse huolehtia salassa pidettävistä asioista verrattuna tilanteeseen, jos käytettäisiin jotain Bittiumin tuotetta tai tuotteen kehitysalustaa testien tekemiseen.

Raspberry Pi 4 Model B -laitteissa ei ole AES-laitteistokiihdytystä.

3.2 Testausympäristö

Testausympäristö koostuu kahdesta Raspberry Pi -laitteesta ja Wi-Fi-reitittimestä. Raspberry Pit ovat liitettyinä toisiinsa Ethernet-kaapelilla ja ovat kiinni samassa Wi-Fi-verkossa. Testaus suoritetaan käyttämällä Ethernet-yhteyttä. Raspberry Pi -laitteita hallitaan etänä SSH-yhteyden avulla samassa Wi-Fi-verkossa olevalta tietokoneelta. Testausympäristö on kuvattuna myös kuvassa 1.



KUVA 1. Testausympäristö

3.3 Testausmenetelmä

Toteutuksen suorituskyvyn mittaaminen suoritetaan hyödyntämällä iperf-, ping- ja tc-ohjelmia ja itse kirjoitettua Python-ohjelmaa `test_system.py`. Alun perin oli tarkoitus toteuttaa kaikki testaus manuaalisesti, mutta testattavia konfiguraatioiden määrän ja jokaiselle suoritettavien testien määrän selvennettyä manuaalinen testaus ja testien tulosten kerääminen todettiin olevan huono lähestymistapa. Automaattinen testaus suoritetaan `test_system.py`-ohjelmalla.

Testaus suoritetaan käynnistämällä Raspberry Pit, yhdistämällä ne yhteiseen Wi-Fi-verkkoon, yhdistämällä ne Ethernet-kaapelilla, luomalla niihin SSH-yhteys ja käynnistämällä `test_system.py` molemmilla laitteilla sopivilla argumenteilla. Tulokset ovat luettavissa `test_system.py:n` luomista tiedostoista.

3.3.1 iperf

iperf on työkalu IP-verkkojen kaistanleveyden mittaamiseen. Oletuksena iperfin tuloksista selviää siirretyn datan määrä, mitattu kaistanleveys ja lisäksi UDP-yhteyksillä mitattu pakettien viivevaihtelu (jitter) sekä lähetettyjen ja kadonneiden pakettien määrä. Näistä tuloksista otetaan talteen kaikki paitsi siirretyn datan määrä. (22.)

Testauksessa iperf-työkalu käynnistetään palvelinlaitteella, joko UDP- tai TCP-tilassa ja UDP-tilassa halutulla paketin koolla. Palvelin-tila otetaan käyttöön -s lipulla, UDP-tila otetaan käyttöön -u lipulla, muutoin toimii TCP-tilassa ja UDP-tilassa paketin pituus määritellään -l lipulla (22). Asiakaslaitteella UDP/TCP valinta ja UDP-tilassa paketin koko valinta tehdään samalla tavalla. Näiden lisäksi asiakaslaitteella määritellään palvelimen IP-osoite -c lipulla, testin kesto määritellään -t lipulla ja UDP-tilassa tavoiteltu nopeus -b lipulla (22).

3.3.2 NetEm ja tc

tc (traffic control) -komento on NetEm (network emulator) -ohjelman hallinta työkalu. tc:n avulla voidaan simuloida erilaisia verkon ominaisuuksia mm. pakettien järjestystä, pakettien lähetysajoitusta ja pakettien monistumista. (23.)

Testaamisessa tc-komentoa on käytetty keinotekoisien viiveiden luomiseen ja pakettien satunnaiseen pudottamiseen. Tällä tavoin simuloidaan häiriöistä verkkoa ja saadaan selville, onko sillä erityistä vaikutusta toteutusten suorituskykyyn.

Testauksen aikana tc-komentoa käytetään seuraavasti (23):

- tc qdisc add dev eth0 root netem
 - o Otetaan NetEm käyttöön Ethernet-porttiin.
- tc qdisc change dev eth0 root netem loss 0,5% delay 10 ms 1 ms distribution normal
 - o Asetetaan haluttu paketinpudotus todennäköisyys ja viive. Esimerkki komennossa otetaan käyttöön 0,5 %:n paketinpudotus todennäköisyys, 10 ms:n viive ja 1 ms:n jitter.
- tc qdisc del dev eth0 root netem
 - o Poistetaan NetEm käytöstä.

Testauksen aikana NetEm otetaan käyttöön halutun toteutuksen käyttöönoton jälkeen mutta ennen testin aloittamista. Testin jälkeen NetEm otetaan pois käytöstä. Testauksen aikana NetEm on käytössä molemmilla Raspberry Pi -laitteilla eli liikennettä häiritään molempiin suuntiin.

Oletuksena NetEmiä käytetään lähtevän liikenteen hallintaan, mutta sitä voidaan myös tarvittaessa käyttää saapuvan liikenteen hallintaan. Tämä voi olla tarpeen, koska ohjesivujen mukaan NetEm raportoi pudottamansa paketit ylemmille kerroksille, mikä voi johtaa pakettien uudelleen lähettämiseen. (23.)

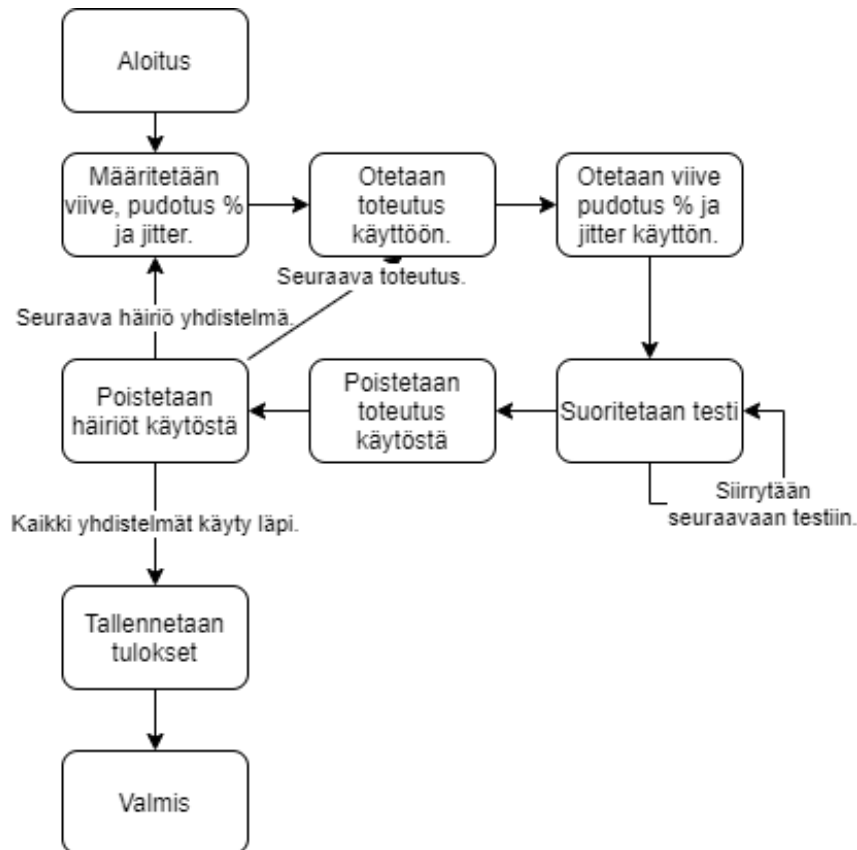
3.3.3 test_system.py

Testien suorittamisen ja tulosten keräämisen automatisoimiseksi kehitettiin test_system.py-ohjelma. Ohjelma käynnistetään molemmilla Raspberry Pi -laitteilla ja ohjelma testaa määritetyt toteutukset, määritetyillä testeillä, määritetyillä parametreilla, määritetyssä virheympäristössä. Testien tulokset tallennetaan Raspberry Pin muistiin tekstitiedostoihin, jotka voidaan avata Microsoft Excelillä tarkempaa analysointia varten. Lisäksi test_system.py kirjoittaa omasta toiminnastaan lokitiedostoa, josta voi myös lukea tarvittaessa iperf-, ping- ja scp-komentojen koko tulosteen.

test_system.py:lle voidaan antaa seuraavia argumentteja:

- ip: Määritellään palvelimen IP-osoite.
- impl: Määritellään lista testattavia toteutuksia.
- test: Määritellään lista toteutettavista testeistä.
- drop: Määritellään lista käytettävistä todennäköisyyksistä pudottaa paketti.
- delay: Määritellään lista käytettävistä viiveistä.
- jitter: Määritellään lista käytettävistä jitter arvoista.
- server: Käynnistetään test_system.py palvelintilassa. Kaikki muut argumentit jätetään tällöin huomiotta.
- pingCount: Määritellään, kuinka monella ping-paketilla ping-testi suoritetaan. Jätetään huomiotta, jos ping-testiä ei ajeta.
- iperfTime: Määritellään, kuinka pitkään iperf-testiä ajetaan. Jätetään huomiotta, jos iperf-testiä ei ajeta.
- remoteNetem: Toteutetaan viive, jitter ja pakettien pudottaminen sisään tulevaan liikenteeseen.
- cli: Käynnistetään komentokehote-tilassa.

impl-, test-, drop-, delay- ja jitter-argumenteilla voidaan antaa joko yksi arvo tai lista käytettävistä arvoista erotettuna "-"-merkillä. Jos argumenttina annetaan lista tai listoja, käydään kaikki mahdolliset kombinaatio läpi. Tämä toiminta on kuvattuna kuvassa 2 siirtymällä takaisin häiriöiden määritykseen tai toteutuksen käyttöönottoon.



KUVA 2. Lohkokaavio test_system.py:n toiminnasta.

Otetaan esimerkiksi alla oleva tapaus, jossa määritellään mitä toteutusta testataan, millä testeillä ja millä häiriöllä:

- Testattavat toteutukset:
 - o Vertailukohde, ei mitään toteutusta käytössä
 - o WireGuard
- Suoritettavat testit:
 - o Ping-testi
 - o UDP-testi 500 Mbit/s:n tavoitenopeudella ja 256 tavun pakettikoolla
- Käytettävät häiriöt:

- 2,5 %:n paketin pudotus todennäköisyys.

Yllä oleva tapaus voidaan toteuttaa komennolla:

- `test_system.py -ip 192.168.177.166 -impl ethernet-wireguard -test ping-udp_500m_256 -drop 2.5`

Toisella laitteella `test_system.py` käynnistetään palvelintilassa seuraavalla komennolla, jolloin laite toimii asiakaslaitteen käskyjen mukaan:

- `test_system.py -server`

Ensimmäisellä komennolla annettu IP-osoite on vastapuolen Raspberry Pin IP-osoite yhteisessä Wi-Fi-verkossa. Wi-Fi-yhteyden yli ohjelmat pystyvät kommunikoimaan huolimatta niiden välisestä Ethernet-yhteydestä, jonka yli testaus toteutetaan.

Testien aikana `test_system.py` seuraa lisäksi molempien Raspberry Pi -laitteiden suorittimen kuormaa, lämpötilaa ja kellotaajuutta ja käytössä olevan muistin määrää. Vertailemalla näitä muuttujia saman testin mutta eri toteutuksen aikana voidaan tehdä päätelmiä, kuinka vaativia eri toteutukset ovat. Näiden muuttujien kerääminen toteutetaan psutil-kirjastolla (24).

Testien aikana dataa lähetetään asiakaslaitteelta palvelinlaitteelle. Molempien testauksessa olevien laitteiden ollessa samanlaisia käytännössä ei ole väliä, mikä on datan kulkusuunta, kunhan kulkusuunta tiedetään tuloksia tulkitessa. Tällöin nähdään mahdolliset erot datan lähettämisen ja vastaanottamisen välillä.

3.4 Ajettavat testit

Seuraavat testit on toteutettu ja niiden tulokset tallennettu:

- iperf TCP:
 - Saavutettu kaistanleveys
- iperf UDP 400 Mbit/s ja 1300 tavun pakettikoko:
 - Saavutettu kaistanleveys
 - Lähetettyjen ja pudonneiden pakettien määrä

- iperf UDP 1 Mbit Mbit/s ja 256 tavun pakettikoko:
 - o Saavutettu kaistanleveys
 - o Lähetettyjen ja pudonneiden pakettien määrä
- Ping:
 - o Mitattu latenssi 500 ping-paketilla.
- SCP 256 MB tiedoston siirtäminen:
 - o Tiedonsiirtoon käytetty aika.

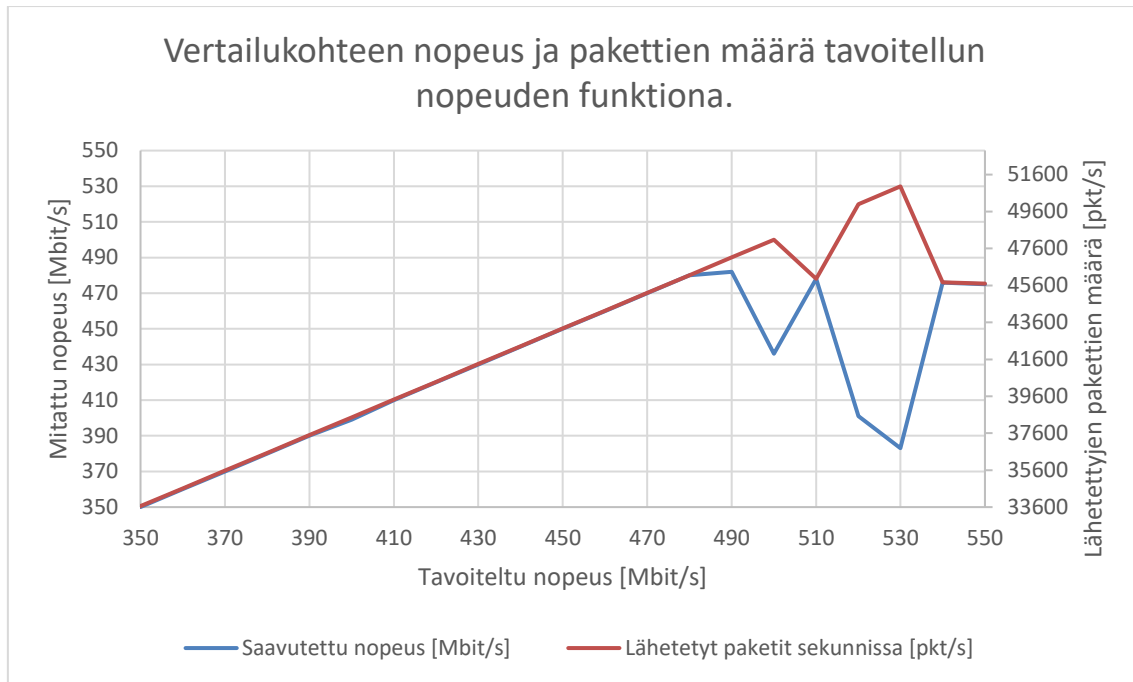
Yllä mainitut testit suoritettiin ilman häiriöitä ja useiden häiriöparametrien kanssa. Ilman häiriötä testit on ajettu viisi kertaa, pois lukien ping-testi. Näistä viidestä kerrasta on laskettu tulosten keskiarvot ja keskihajonta eri ajojen välillä. Ping raportoi nämä tiedot automaattisesti, joten sen ajaminen moneen kertaan ei ole tarpeen. Mainitut iperf-testit toteutetaan 5 minuutin kestolla.

Alla on kuvattu, millä häiriöparametriyhdistelmillä testit on suoritettu. Yksittäinen testi ajetaan kullakin häiriöparametriyhdistelmällä vain kerran. Parametrit kuvastavat yhteen suuntaan käytettäviä parametreja ja häiriöt otetaan käyttöön molempiin suuntiin.

- Viive 0–100 ms, jitter 0 ms, pudotus 0 %
 - o Viive toteutetaan 10 ms askelin, yhteensä 11 testikierrosta.
- Viive 20 ms, jitter 0–10 ms, pudotus 0 %
 - o Jitter toteutetaan 1 ms askelin, yhteensä 11 testikierrosta.
- Viive 0 ms, jitter 0 ms, pudotus 0–5 %
 - o Pudotus toteutetaan 0,5 % askelin, yhteensä 11 testikierrosta.
- Viive 40 ms, jitter 5 ms, pudotus 0,5 %
 - o Verkko 1. Toimeksiantajan määrittelemät parametrit.
- Viive 80 ms, jitter 10 ms, pudotus 1 %
 - o Verkko 2. Toimeksiantajan määrittelemät parametrit.
- Viive 120 ms, jitter 15 ms, pudotus 1,5 %
 - o Verkko 3. Toimeksiantajan määrittelemät parametrit.

Ensimmäisen UDP-testin tavoitteena on maksimoida lähetetyn datan määrä 1300 tavun paketti koko määräytyi WireGuardin ja vertailukohteen mukaan. Pa-

kettikoon ollessa 1400 tcpdump-tulosteesta selvisi, että paketit pirstaloituivat. Kuvassa 3 on kuvattu useiden testien tulokset 1300 tavun pakettikoolla ja eri tavoitenopeuksilla. Tavoiteltu ja saavutettu nopeus ovat samassa linjassa n. 480 Mbit/s nopeuteen asti. Tästä eteenpäin saavutettu nopeus on alhaisempi kuin tavoiteltu nopeus. Sama nähdään myös lähetettyjen pakettien määrässä hiukan myöhemmin n. 500 Mbit/s nopeuden kohdalla.



KUVA 3. Mitattu vertailukohteen UDP-nopeus ja lähetettyjen pakettien määrä tavoitellun nopeuden funktiona.

Toisen UDP testin tavoitteena on simuloida tyypillistä UDP-liikennettä. Microsoft Teamsin suositeltu verkon nopeus videopuhelulle on 1500 Kbit/s (25). Teamsin suositeltuun nopeuteen verrattuna 1 Mbit/s nopeus on alle suosituksen mutta toimii tyypillisen UDP-liikenteen simuloimiseen.

Testien tulosten perusteella on tehty myös alla mainittu tarkentava testi:

- iperf UDP 25–400 Mbit/s, 1300 tavun pakettikoko, ei häiriötä.

Tällä testillä saadaan tarkemmin selville, missä menee toteutuksen suorituskyvyn rajat saavutetun kaistanleveyden osalta. Toteutetaan 25 Mbit/s askelin yhteensä 16 mittausta. Testi ajetaan vain kerran.

Lisäksi jokaisesta toteutuksesta tutkitaan ja varmistetaan MTU (maximum transmission unit). Tutkiminen hoidetaan ifconfig ohjelmalla ja varmistaminen toteutetaan manuaalisesti lähettämällä ping-paketteja kasvattaen pakettien kokoa ja esittämällä pakettien pirstoutumisen. Kun ping raportoi virheestä, mikä johtuu liian suuresta paketista ja pirstoutumisen kiellosta, ping raportoi datan määrän mitä yritettiin lähettää ja sen hetkisen polun MTU:n.

Testit on suoritettu seuraavilla toteutuksilla ja salausalgoritmeilla:

- Ei toteutusta ja ei salausta, vertailukohde.
- IPsec, 128-bit AES-GCM
- IPsec, 256-bit AES-GCM
- IPsec, 256-bit ChaCha20/Poly1305
- WireGuard, ChaCha20/Poly1305
- MACsec, 128-bit AES-GCM
- OpenVPN, 256-bit AES-CBC

IPseciä tutkitaan usealla salauksella. IPsec tukee useita eri salauksia, joihin kuuluvat WireGuardin käyttämä ChaCha20/Poly1305 ja MACsecin käyttämä 128-bit AES-GCM. Tällöin vertailusta saadaan vähennettyä salausalgoritmin vaikutusta.

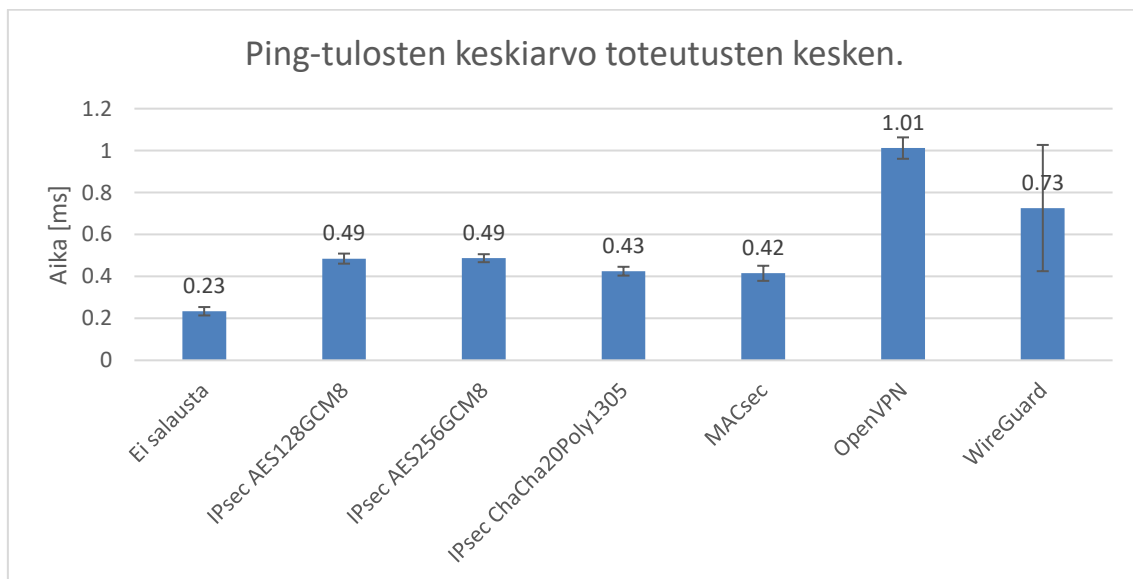
4 MITTAUSTULOKSET

Käydään mittaustulokset läpi. Ensimmäisenä perehdytään ideaaliverkon tuloksiin ja käydään tulokset läpi yksi testi kerrallaan. Käydään läpi, miten toteutukset ver-
tautuvat toisiinsa ideaalitilanteessa. Toisena perehdytään häiriöisen verkon tu-
loksiin käyden eri häiriötyypit läpi yksi kerrallaan ja lopuksi niiden yhteisvaikutus.
Häiriöisen verkon tuloksissa kerrotaan häiriön vaikuttaa vertailukohteeseen ja ku-
hunkin toteutukseen. Kaikki tutkitut mittaustulokset ovat luettavissa taulukkomuo-
dossa liitteistä 6–10.

4.1 Ideaaliverkko

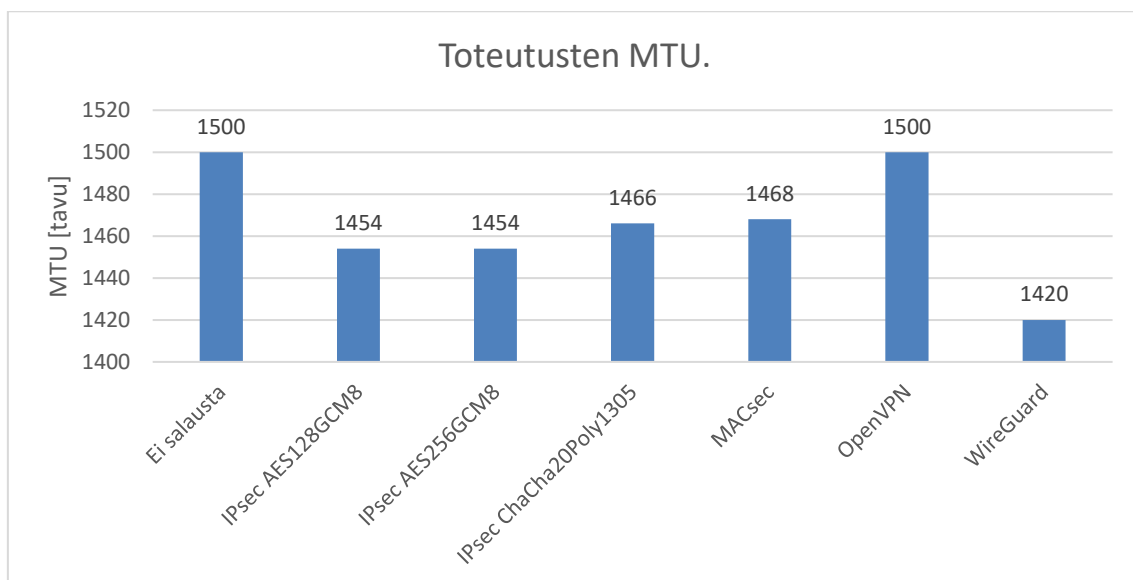
4.1.1 Ping-testi ja MTU

Ping-testin tulokset eri toteutusten kesken on kuvattu kuvassa 4. Kaikista toteu-
tuksista tulee jonkin verran viivettä. Eniten viivettä tulee OpenVPN:stä ja Wire-
Guardista. Lisäksi WireGuardin tuloksissa on muista huomattavasti suurempi ha-
jonta. Osittain tämä mahdollisesti selittyy WireGuardin yhteyden avainten vaih-
dosta, joka tapahtuu 2 minuutin välien (7, s 14). Ping-tulosteessa n. 120 tuloksen
välein tulos oli huomattavasti suurempi kuin muuten. Tulosteesta löytyy kuitenkin
myös satunnaiselta vaikuttavia ryppäitä, jotka huonontavat WireGuardin tulosta.



KUVA 4. Ping-tulosten keskiarvot ja hajonnat eri toteutusten.

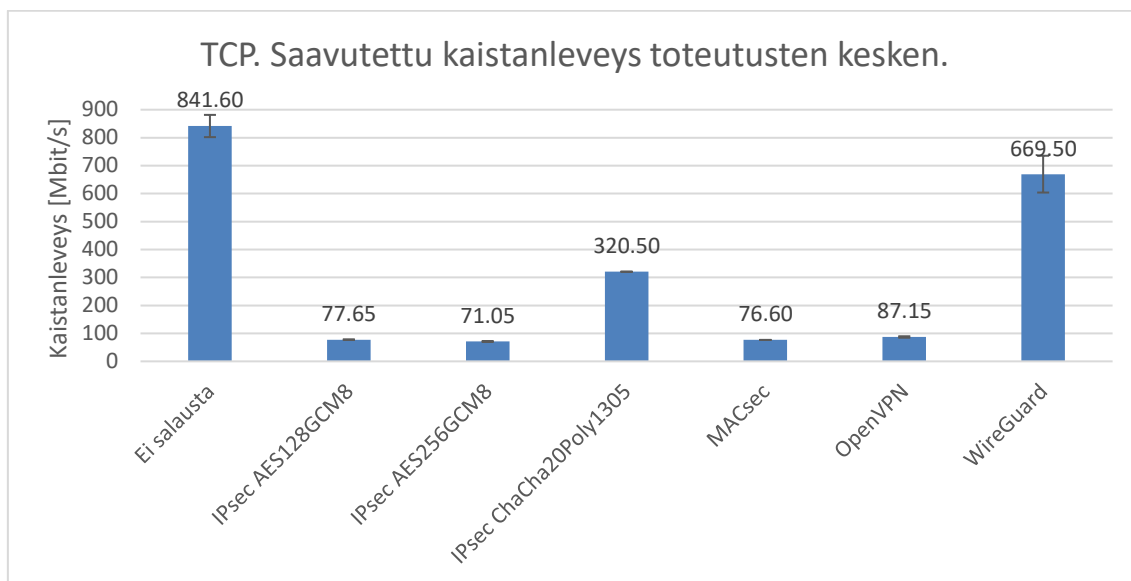
Kuvassa 5 on kuvattu toteutusten MTU (maximum transmission unit). OpenVPN on ainut toteutuksista, jonka MTU on sama kuin vertailukohteella. WireGuardin MTU on testattavista toteutuksista pienin. IPsec AES-toteutusten MTU on sama. IPsec ChaCha MTU on hiukan AES-toteutuksia suurempi eli ChaCha vaatii vähemmän dataa jokaiseen viestiin toimiakseen, jolloin hyötykuromalle jää enemmän tilaa. MACsecin MTU on hiukan suurempi kuin IPsec AES128:n, vaikka molemmissa on sama salaus.



KUVA 5. Toteutusten MTU.

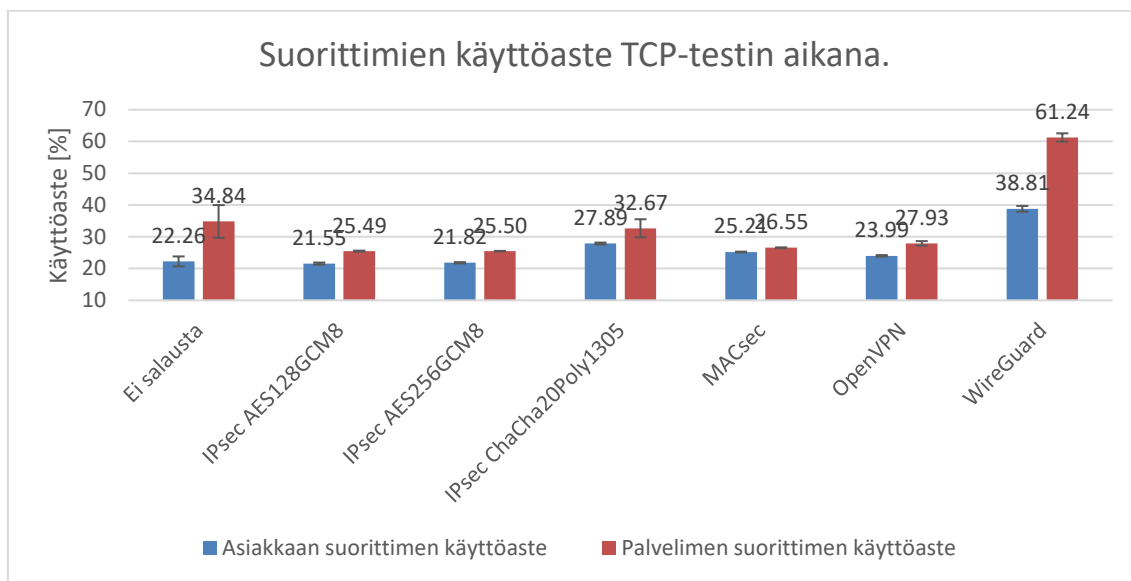
4.1.2 TCP-testi

TCP-testin tulokset ovat kuvattuna kuvassa 6. Vertailukohde pois lukien parhaiten suoriutuu WireGuard ja toiseksi parhaiten IPsec ChaCha-salauksella. IPsecin AES128- ja AES256-salauksilla ei ole suurta eroa mutta kun käytössä on ChaCha-salaus niin kaistanleveys moninkertaistuu. MACsecin ja OpenVPN:n tulokset ovat samaa luokkaa IPsec AES -tulosten kanssa. Lisäksi ainoat merkittävät hajonnat tuloksissa ovat vertailukohteen ja WireGuardin tuloksissa.



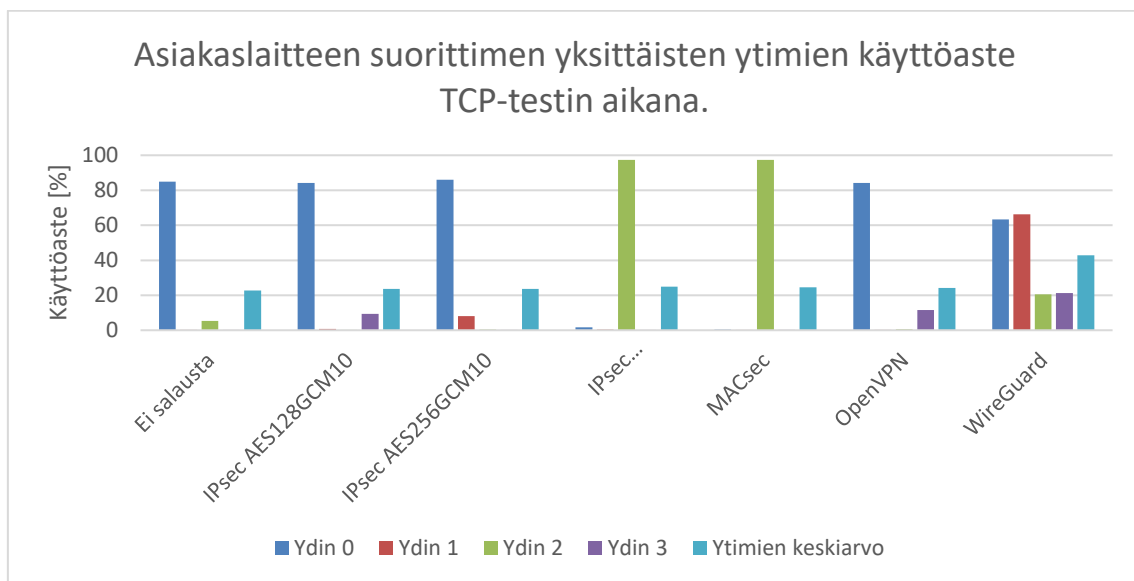
KUVA 6. TCP. Saavutettu kaistanleveys toteutusten kesken.

Molempien laitteiden suorittimen käyttöaste TCP-testin ajalta on kuvattuna kuvassa 7. Poikkeuksetta palvelimen suorittimen käyttöaste on suurempi kuin asiakkaan. Molemmat IPsec AES -toteutukset, MACsec ja OpenVPN ovat kaikki hyvin lähellä toisiaan samaan tapaan kuin itse testin tuloksissa. Näiden toteutusten tulosten ja suorittimen käyttöasteen läheisyys johtuu mahdollisesti toteutusten käyttämästä AES-salauksesta. AES-salaus vaikuttaa toimivan pullonkaulana laitteistokiihdytyksen puuttumisen takia. Selvästi aiemmista eroaa IPsec ChaCha ja erityisesti WireGuard, mitkä molemmat hyödyntävät ChaCha-salausta. Itse WireGuardin TCP-tulokset ovat hiukan yli kaksinkertaiset IPsec ChaChahan verrattuna ja WireGuardin suorittimen käyttöaste on hiukan alle kaksinkertaiset IPsec ChaChahan verrattuna. Vaikuttaa siltä, että WireGuard pystyy hyödyntämään suoritinta paremmin, mikä johtaa parempaan kaistanleveyteen. Jos IPsec ChaChan ja WireGuardin kaistaleveydet olisivat samat, niiden suorittimien käyttöaste olisi myös samaa luokkaa.

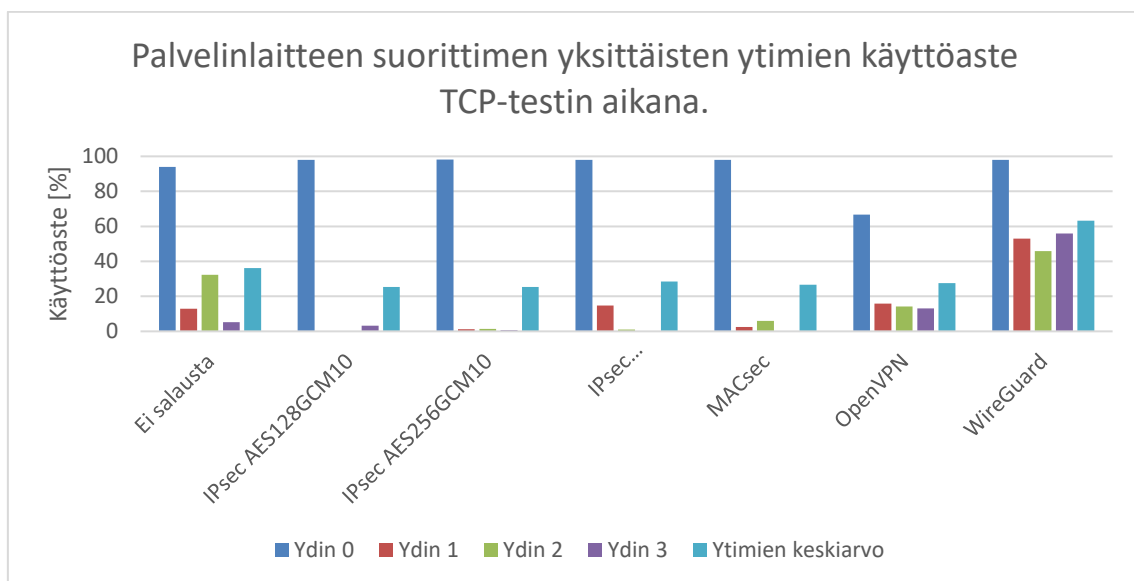


*KUVA 7. Molempien laitteiden suorittimen käyttöaste TCP-testin aikana eri totu-
tuksilla.*

TCP-testi ajettiin uudestaan, jotta saadaan tutkittua yksittäisten ytimien käyttöas-
tetta ja sitä, hyödyntääkö toteutus useampaa ydintä. Tämän testin tulokset näky-
vät kuvissa 8 ja 9. Tulokset ovat keskiarvoja koko testin ajalta. Yksittäisten yti-
mien käyttöasteiden perusteella asiakaslaitteella vain WireGuard käyttää useam-
paa kuin yhtä ydintä ja palvelinlaitteella WireGuard ja OpenVPN käyttää useam-
paa kuin yhtä ydintä.



KUVA 8. Asiakaslaitteen suorittimen yksittäisten ytimien käyttöaste TCP-testin aikana.



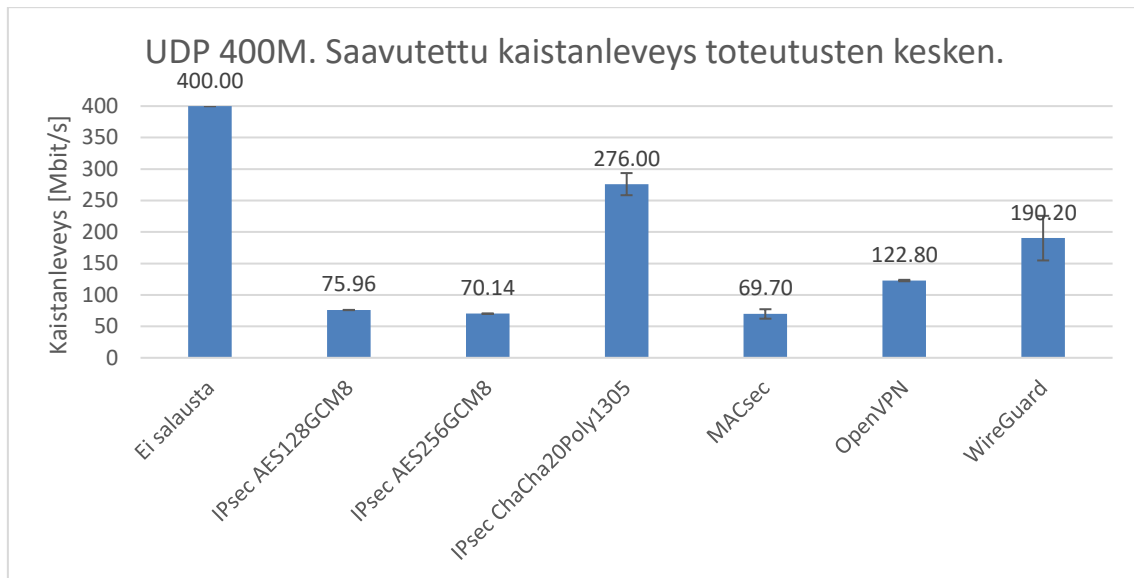
KUVA 9. Palvelinlaitteen suorittimen yksittäisten ytimien käyttöaste TCP-testin aikana.

4.1.3 UDP-testit

UDP 400 Mbit/s 1300 tavua

UDP 400 Mbit/s -testin tulokset ovat kuvattuna kuvassa 10. Ainoastaan vertailukohte saavuttaa tavoitellun 400 Mbit/s kaistanleveyden. Seuraavaksi parhaiten

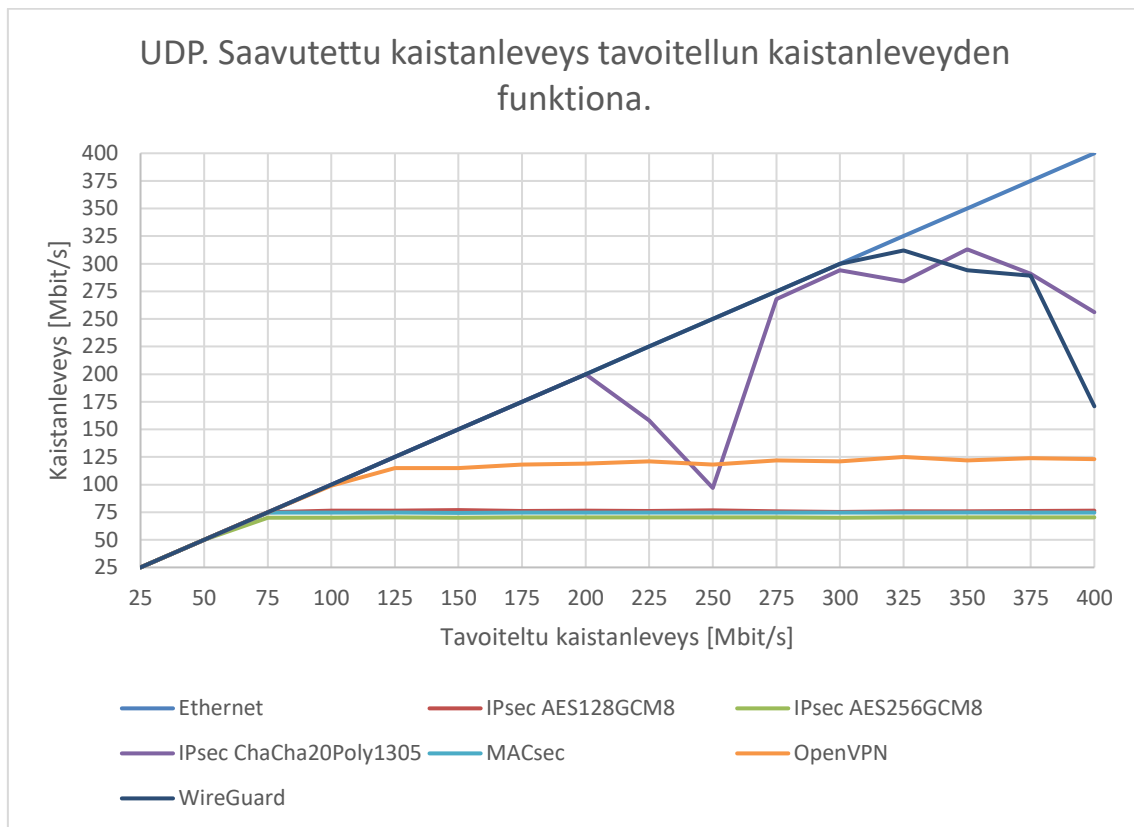
suoriutuu IPsec ChaCha-salauksella ja WireGuard. Lisäksi muihin toteutuksiin verrattuna WireGuardissa on huomattavaa keskihajontaa.



KUVA 10. UDP 400M. Saavutettu kaistanleveys toteutusten kesken.

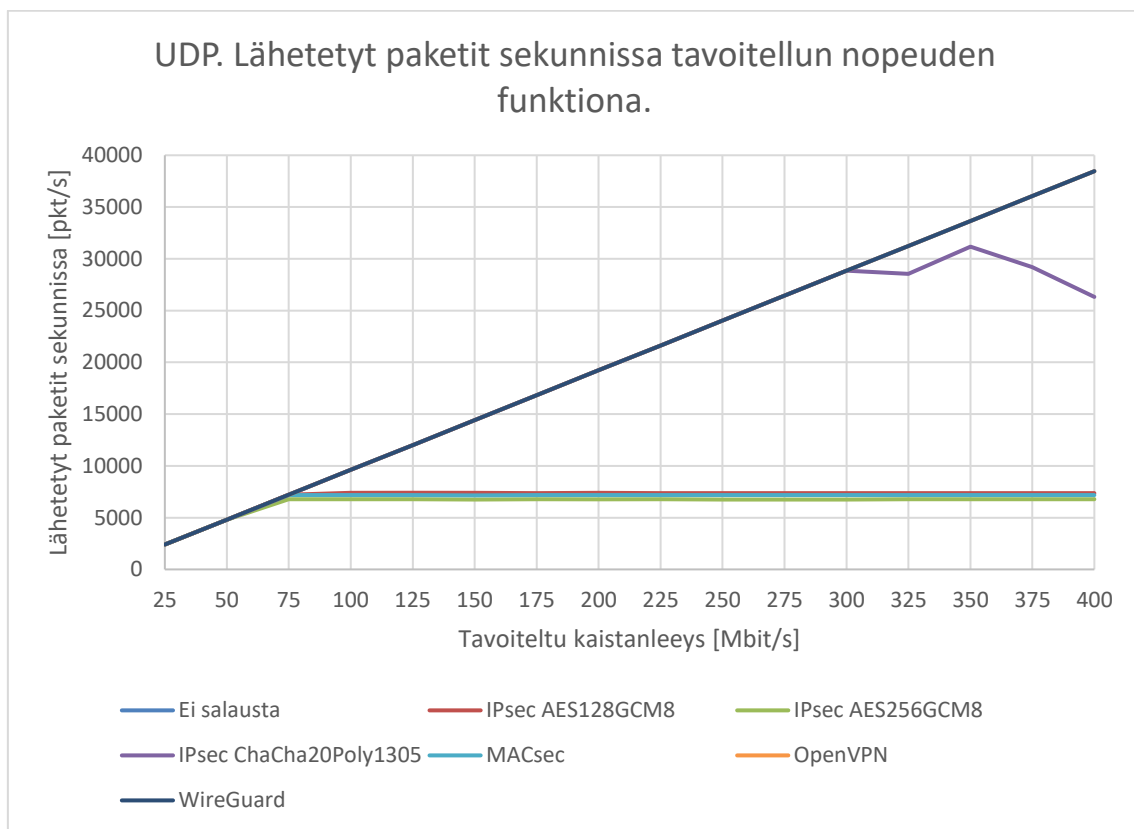
Jotta nähdään, miten eri toteutukset käyttäytyvät eri UDP tavoitenopeuksilla, toteutettiin UDP-testi nopeuksilla 25–400 Mbit/s 25 Mbit/s askelilla. Osa tämän testin tuloksista on kuvattuna kuvissa 11 ja 12.

Kuvassa 11 on kuvattu saavutettu kaistanleveys UDP-testissä eri toteutusten kesken. Vertailukohde on ainoa, mikä saavuttaa tavoitenopeuden koko testialueelta. WireGuard putoaa tavoitteesta 300 Mbit/s jälkeen. IPsec ChaCha-salauksella putoaa tavoitteesta 200 Mbit/s jälkeen mutta on lähellä tavoitetta 275 Mbit/s ja 300 Mbit/s tavoitenopeuksilla. Notkahdus toistuu, jos testi ajetaan uudelleen. OpenVPN putoaa tavoitteista 100 Mbit/s jälkeen. IPsec AES128, IPsec AES256 ja MACsec putoavat tavoitteista n. 75 Mbit/s kohdalla.



KUVA 11. Saavutettu kaistanleveys tavoitellun kaistanleveyden funktiona.

Kuvassa 12 on kuvattu lähetettyjen pakettien määrä UDP-testissä eri toteutusten kesken. Tämä tulos poikkeaa saavutetusta kaistanleveydestä. Toisin kuin kuvassa 11 WireGuard ja OpenVPN käyrät eivät putoa vaan pysyvät samalla tasalla vertailukohteen kanssa. Ne siis pystyvät lähettämään mutta eivät vastaanottamaan tavoitemäärän dataa. Sama näkyy myös IPsec ChaCha tuloksissa 300 Mbit/s asti, sillä kuvan 11 notkahdusta 225–250 Mbit/s kohdalla ei ole vaan jää 300 Mbit/s tavoitenopeuden tasolle. MACsec ja molemmat IPsec AES tulokset ovat samankaltaisia molemmissa kuvissa.

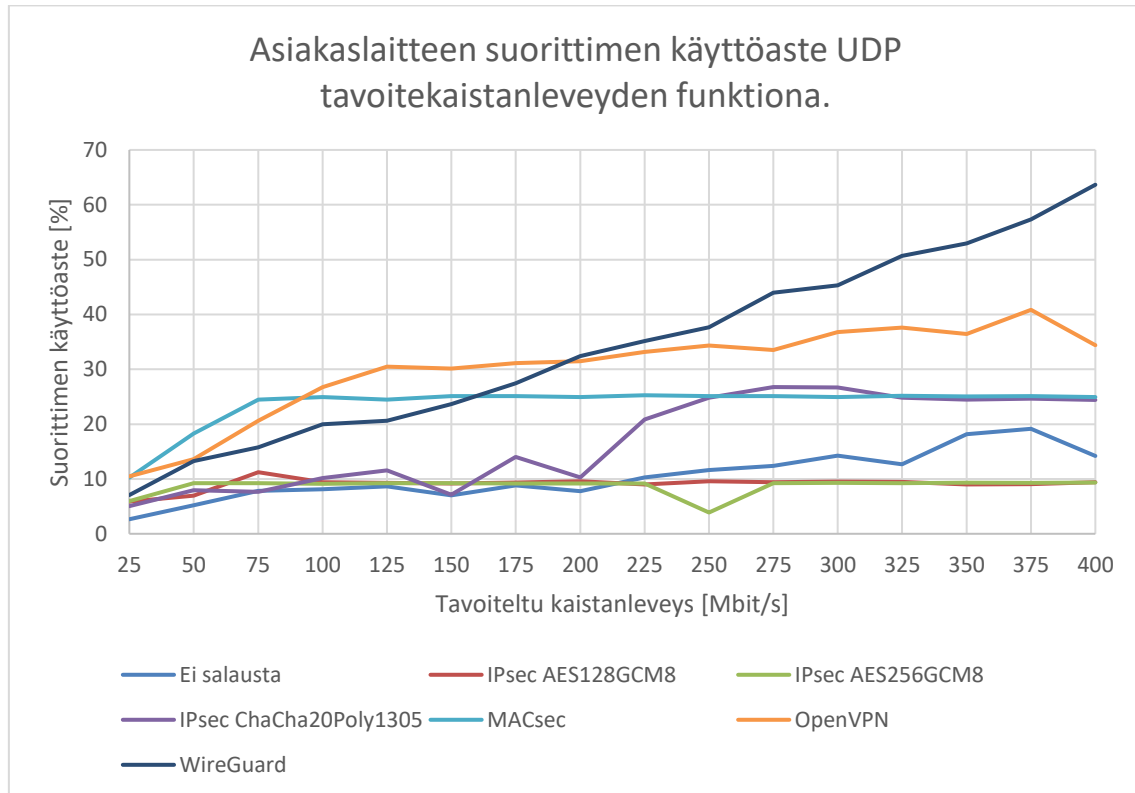


KUVA 12. Lähetetyt paketit sekunnissa tavoitellun nopeuden funktiona.

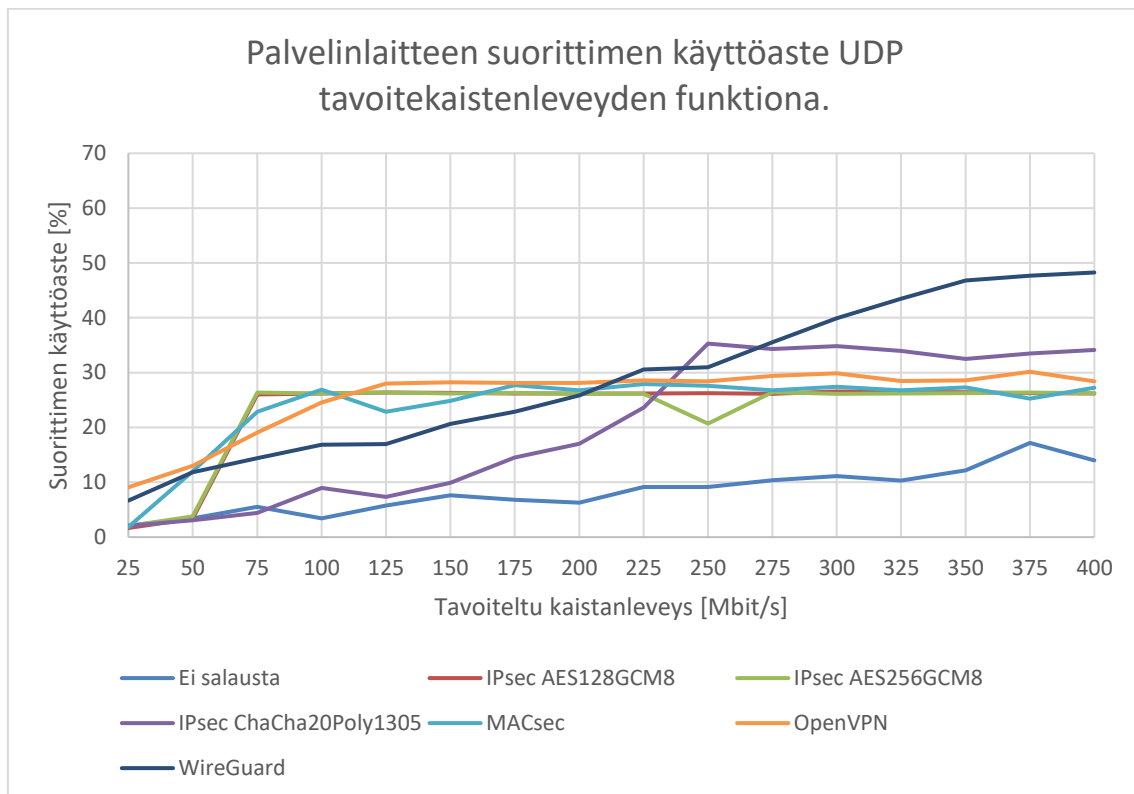
Tutkimalla kuvien 11 ja 12 tuloksia voi tutkia, onko toteutuksen raskaampaa lähettää vai vastaanottaa paketteja. Jos paketteja lähetetään koko ajan tasaisesti enemmän tavoitellun nopeuden kasvaessa ilman, että saavutettu kaistanleveys nousee samassa suhteessa, vaikuttaa siltä, että lähettäjän näkökulmasta dataa voisi siirtää enemmänkin. Tässä tilanteessa vastaanottava osapuoli ei ehdi käsitellä kaikkia saapuvia paketteja ja joutuu pudottamaan ne, jota ei pysty käsittelemään. Jos taas lähettäminen on yhtä raskasta tai raskaampaa, tällöin paketti määrät ja saavutettu nopeus eivät poikkea toisistaan. Vastaanottaja saa kaikki lähetetyt paketit vastaan, käsittelee ne ja odottaa lisää paketteja.

Samaa asiaa voi tutkia myös vertailemalla lähettävän ja vastaanottavan laitteen prosessorin käyttö-, kellotaajuus- ja lämpötiladataa testin ajalta. Kuva 13 ja 14 kuvaavat asiakkaan ja palvelimen suorittimen käyttöastetta eri tavoitekaistanleveyksillä. Käyrät mukailevat saavutetun kaistaleveyden käyriä. Varsinkin palvelimen suorittimen käyttöasteissa nousu lakkaa lähes kaikilla toteutuksilla samassa

kohtassa saavutetun kaistanleveyden kanssa. Poikkeuksena tähän on asiakaslaitteen suorittimen käyrät OpenVPN:llä ja WireGuardilla. Nämä käyrät nousevat koko ajan samalla tavalla kuin lähetettyjen pakettien määrän kanssa.



KUVA 13. Asiakaslaitteen suorittimen käyttöaste UDP tavoitekaistanleveyden funktiona.

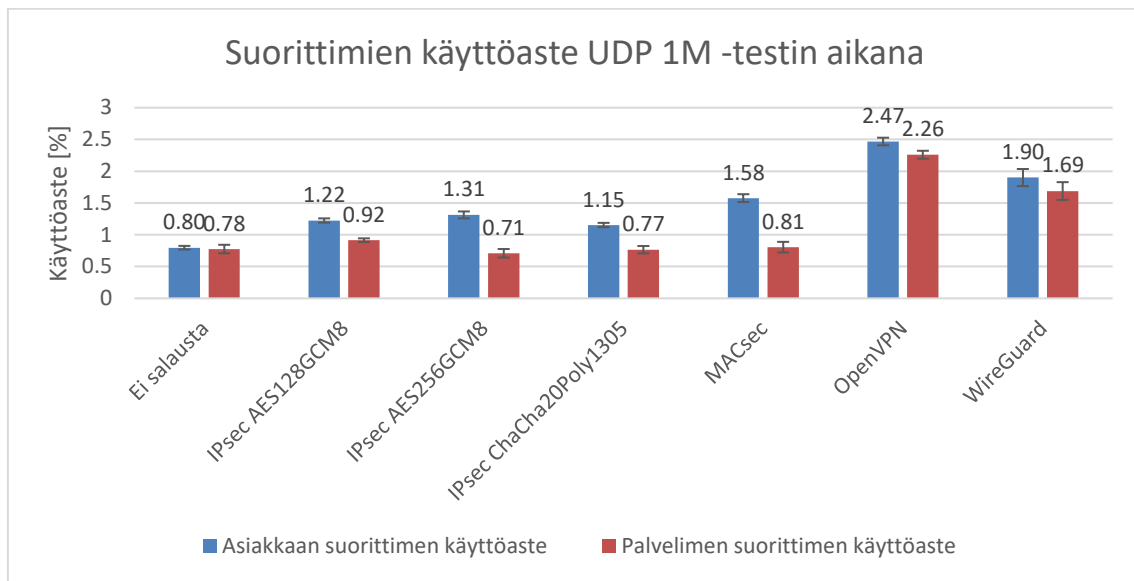


KUVA 14. *Palvelinlaitteen suorittimen käyttöaste UDP tavoitekaistanleveyden funktiona.*

UDP 1 Mbit/s 256 tavua

Kaikkien toteutusten tulokset UDP 1 Mbit/s 256 tavun -testissä ovat suurimmalta osin identtisiä. Kaikki toteutukset kykenevät 1 Mbit kaistanleveyteen. Ainoa poikkeama on iperfin raportoimissa jitter tuloksissa WireGuardin kohdalla. WireGuardin mitattu jitter on 0,0232 ms, kun muut toteutukset ja vertailukohde ovat 0,006–0,002 ms:n haarukassa.

Kuvassa 15 on esitettyä asiakas- ja palvelinlaitteen suorittimien käyttöaste UDP 1 Mbit/s testin aikana. IPsec-toteutukset ja MACsec nostavat käyttöastetta vain vähän verrattuna vertailukohteeseen varsinkin palvelimen osalta, kun taas OpenVPN ja WireGuard ainakin kaksinkertaistavat käyttöasteen.

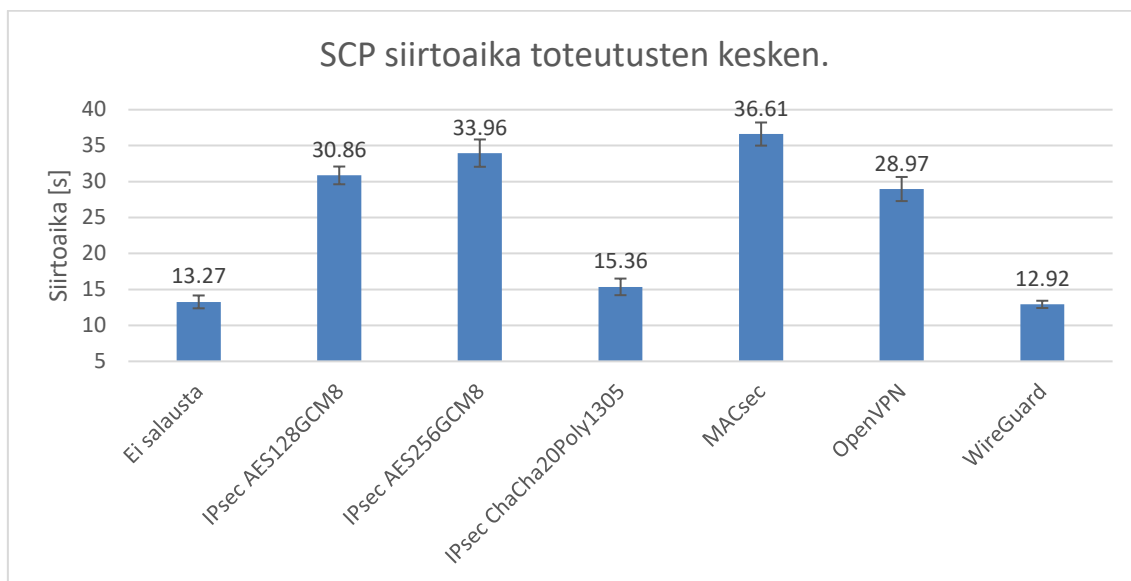


KUVA 15. Suorittimien käyttöaste UDP 1 Mbit/s -testin aikana.

4.1.4 SCP-testi

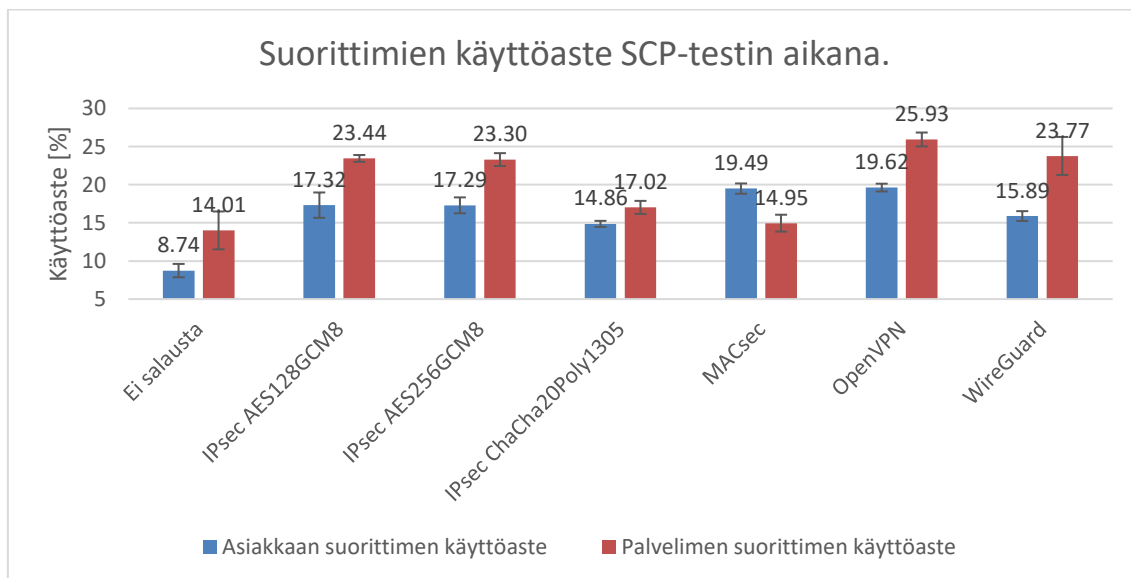
SCP käyttää tiedon siirtämiseen SSH-protokollaa, joka taas käyttää TCP-protokollaa, joten SCP- ja TCP- testien tulokset ovat samankaltaiset. Lisäksi täytyy pitää mielessä, että massamuistina toimivan SD-kortin suorituskyky vaikuttaa tuloksiin, sillä testitiedosto täytyy lukea levyltä lähetettäessä ja kirjoitettava levyille vastaanotettaessa, sekä SCP-protokolla myös itse salaa datan ennen sen lähettämistä. Kun testataan muuta kuin vertailukohdetta, niin data on salattu kahdesti.

SCP-testin tulokset on kuvattu kuvassa 16. TCP-testin tapaan parhaat tulokset ovat vertailukohteella, IPsec ChaChalla ja WireGuardilla. Hajonta mukaan lukien WireGuardin tulokset on käytännössä identtiset vertailukohteen kanssa. Vaikka SCP hyödyntää TCP:tä ja tulokset suurimmaksi osaksi mukailevat käänteisesti TCP:n tuloksia, MACsec poikkeaa näistä tuloksista. TCP-tuloksissa MACsecin tulokset osuvat IPsec AES128 ja IPsec AES256 tulosten väliin, kun taas nyt SCP-testissä MACsecin tulokset ovat huonoimmat.



KUVA 16. SCP-testin tulokset toteutusten kesken.

Kuvassa 17 on kuvattuna molempien suorittimien keskimääräinen käyttöaste SCP-testin aikana. Eniten suoritinta kuormittaa OpenVPN ja tämän jälkeen IPsec AES -toteutukset ja WireGuard. Kaikkein vähiten suoritinta kuormittaa IPsec ChaCha. MACsec kuormittaa vain vähän enemmän kuin IPsec ChaCha.



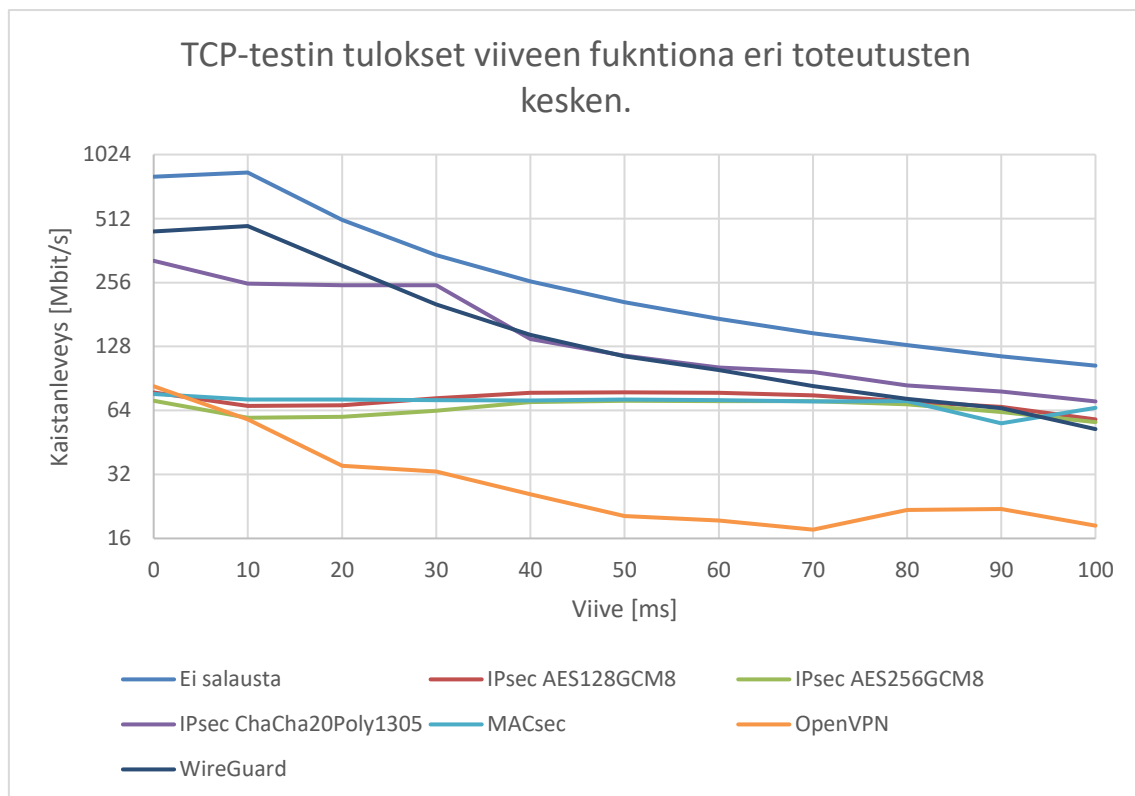
KUVA 17. Molempien laitteiden suorittimen käyttöaste SCP-testin aikana eri toteutuksilla.

MACsec poikkeaa muista toteutuksista suorittimien välisessä suhteessa. Asiakkaan suorittinta eli datan lähetyspuolella suorittinta kuormitetaan enemmän, kun taas kaikissa muissa tuloksissa palvelimen suoritin on enemmän kuormitettu.

4.2 Häiriöinen verkko

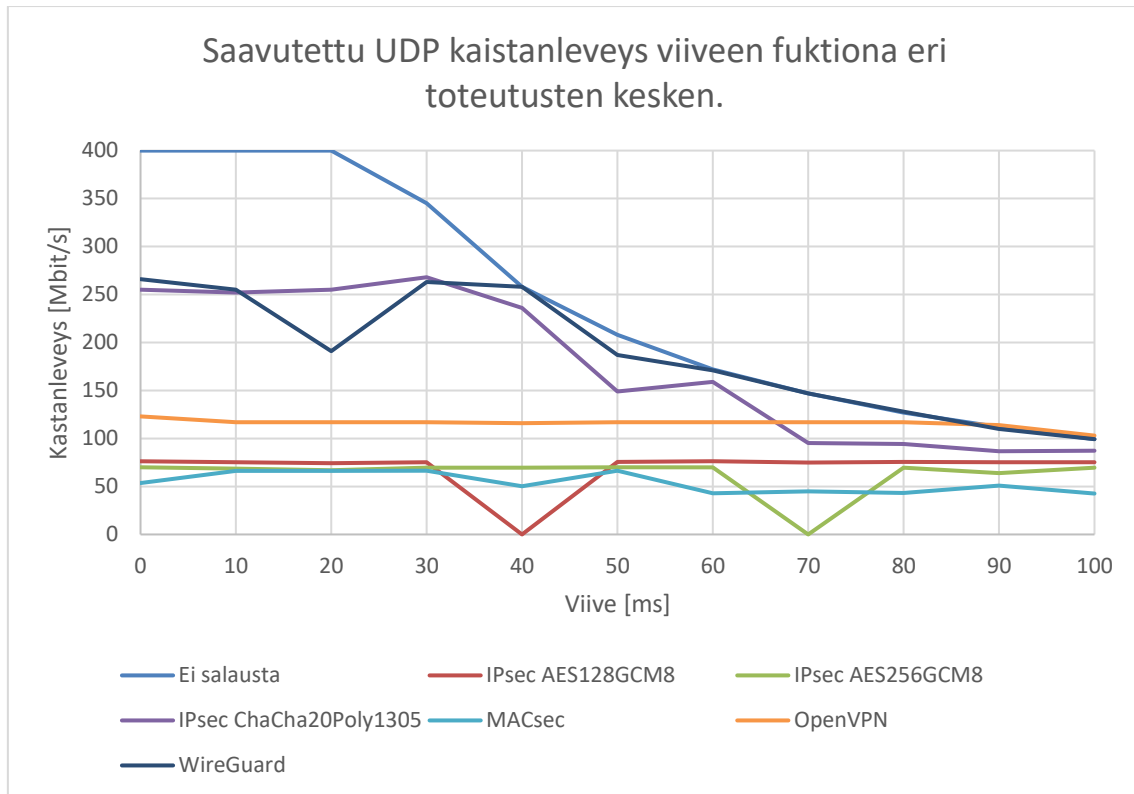
4.2.1 Viiveen vaikutus

Kuvassa 18 on kuvattu TCP-testin tulokset keinotekoisen viiveen funktiona logaritmisella y-akselilla. IPsec AES -toteutuksiin ja MACsec tuloksiin viiveellä ei juurikaan ole vaikutusta ja niiden tulokset ovat 55.7–77.9 Mbit/s haarukassa koko testin ajan. Näiden toteutusten ideaaliverkon TCP-tulokset kuitenkin olivat huonoimpia. WireGuardin ja IPsec ChaChan tulokset ovat samankaltaiset 40 ms ja sitä suuremmalla viiveellä. Molempien tulokset ovat noin 145 Mbit/s tässä kohdassa. Kuvaajassa vertailukohteen, WireGuardin, IPsec ChaChan ja OpenVPN:n käyrät ovat kaikki samanmuotoisia. 10 ms viiveen lisäys laskee näiden toteutusten suorituskyykyä noin viides osan. Lisäksi OpenVPN:n käyrässä on jonkin verran vaihtelua verrattuna muihin käyriin.



KUVA 18. TCP-testin tulokset viiveen funktiona eri toteutusten kesken.

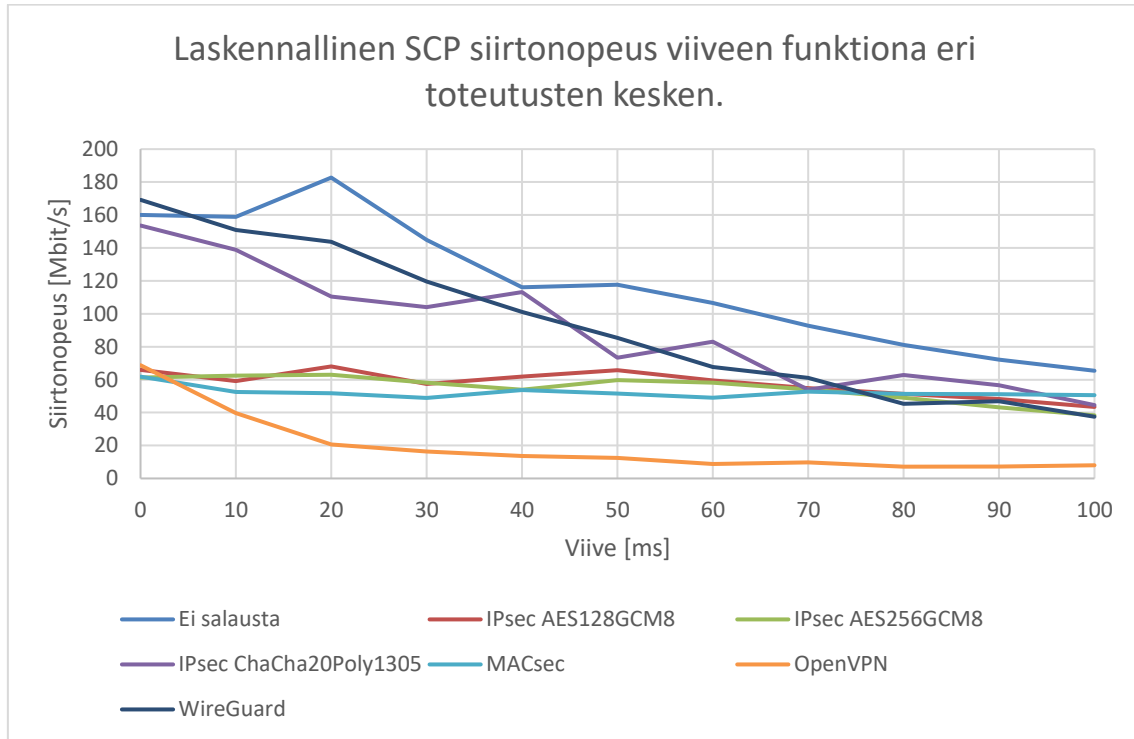
Kuvassa 19 on kuvattu viiveen vaikutus UDP 400 Mbit/s testiin. Minkään toteutuksen tulokset eivät ylitä vertailukohteen tuloksia. Lisäksi toteutukset, joiden tulokset laskevat viiveen kasvaessa, eli WireGuard, IPsec ChaCha ja OpenVPN, mukailevat laskussaan vertailukohdetta, kun saavuttavat vertailukohteen käyrän. Viiveellä ei ole ollenkaan vaikutusta IPsec AES -toteutusten, MACsecin ja OpenVPN:n tuloksiin. Eli toteutusten tulosten lasku ei johdu toteutuksista.



KUVA 19. UDP 400 Mbit/s -testin tulokset lisätyllä viiveellä. Testit epäonnistuivat 40 ms kohdalla IPsec AES128:lla ja 70 ms kohdalla IPsec AES256:lla.

Kuvassa 20 on kuvattu laskennallinen siirtonopeus SCP-testin aikana viiveen funktiona. Vertailukohteen siirtonopeus laskee tasaisesti viiveen kasvaessa. Samaa tahtia laskee myös WireGuardin ja IPsec ChaChan siirtonopeus. Lisäksi WireGuardin ja IPsec ChaChan tulokset ovat samaa luokkaa 40 ms ja sitä suuremmalla viiveellä. Ennen tätä WireGuardin siirtonopeus on jonkin verran parempi kuin IPsec ChaCha. IPsec AES -toteutusten ja MACsecin tulokset ovat samaa luokkaa toistensa kanssa mutta kuitenkin noin 100 Mbit/s huonompi kuin vertailukohde, WireGuard ja IPsec ChaCha. IPsec AES -toteutusten ja MACsecin siirto-

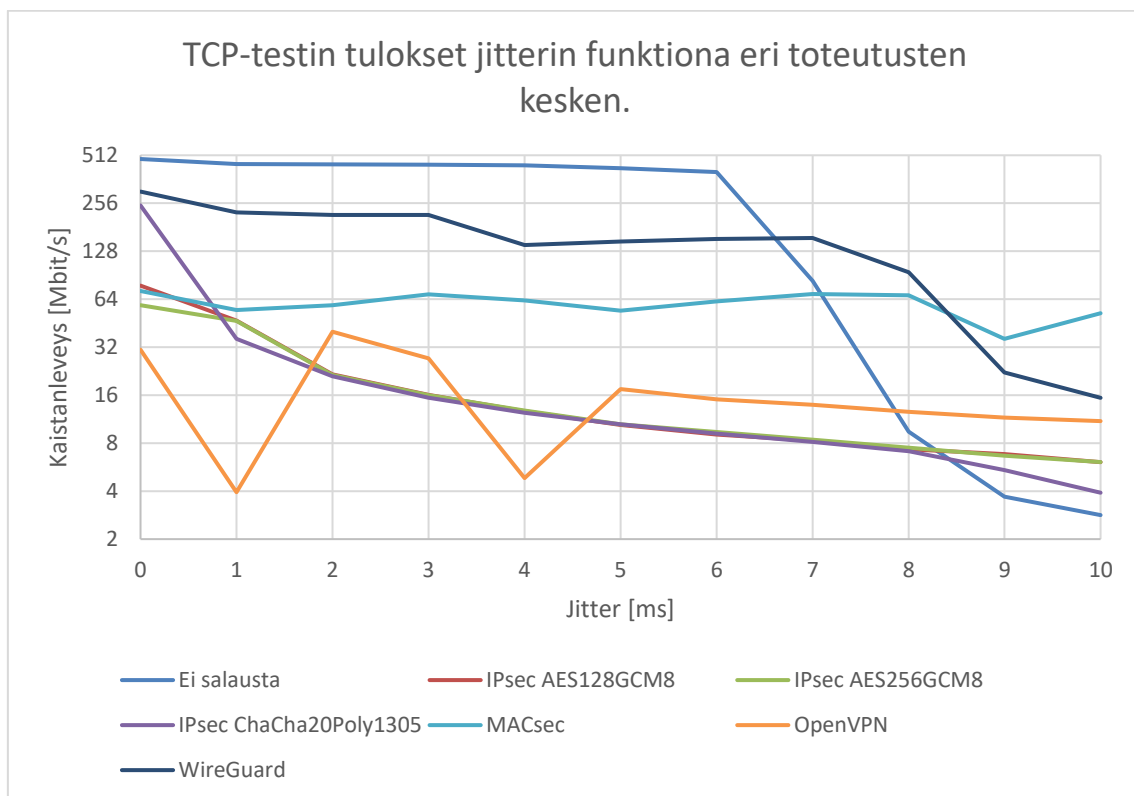
nopeus laskee vain vähän mitatulla viive alueella. OpenVPN:n siirtonopeus läh-
tee samoista lukemista IPsec AES -toteutusten ja MACsecin kanssa mutta laskee
samaa tahtiin vertailukohteen, WireGuardin ja IPsec ChaCha kanssa 20 ms
viiveeseen asti, mistä eteenpäin se jatkaa laskemistaan hitaammin.



KUVA 20. Laskennallinen SCP siirtonopeus viiveen funktiona eri toteutusten kes-
ken.

4.2.2 Jitterin vaikutus

Kuvassa 21 on kuvattu TCP-testin tulokset jitterin funktiona logaritmisella y-ak-
selilla. Vertailukohteen tulokset lähtevät 485 Mbit/s ja putoavat vain vähän 6 ms
jitteriin asti, minkä jälkeen tulokset putoavat rajusti. IPsec ChaCha lähtee 248
Mbit/s:sta ja IPsec AES -toteutukset n. 64 Mbit/s:sta mutta 1 ms jitterin jälkeen
kaikki kolme ovat n. 40 Mbit/s ja jatkavat laskua samoin tuloksin. MACsecin tu-
lokset pysyvät lähes koko jitter skaalalla samoissa lukemissa n. 64 Mbit/s. Tulok-
set putoavat ainoastaan 9 ja 10 ms jitter arvoilla jonkin verran. OpenVPN:n tulok-
set, pois lukien notkahdukset 0, 1 ja 4 ms jitterillä, ovat muodoltaan samanlaiset
kuin IPsec tulokset, ainoastaan IPsecin tulokset ovat noin puolet OpenVPN:n tu-
loksista.



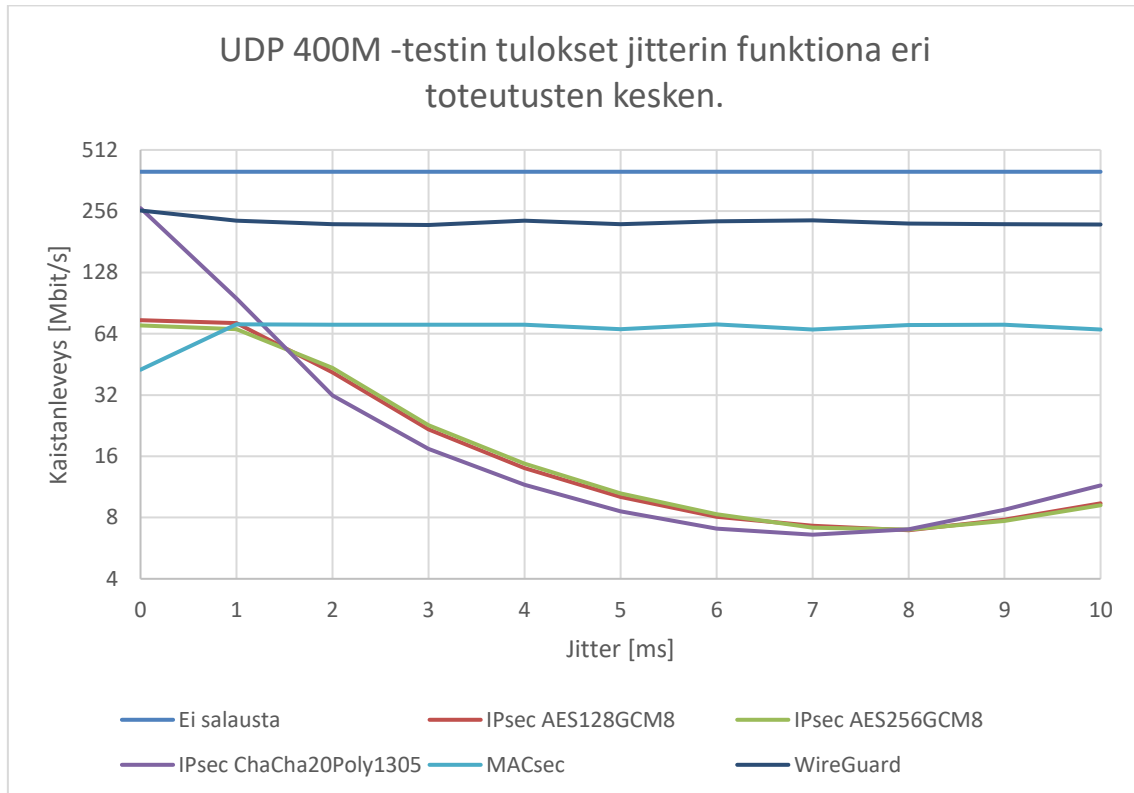
KUVA 21. TCP-testin tulokset lisätyllä jitterillä. Viive 20 ms.

8 ms jitterillä WireGuard ja MACsec suoriutuvat paremmin kuin vertailukohde ja 9 ms ja sitä suuremmalla jitterillä kaikki toteutukset suoriutuvat paremmin kuin vertailukohde.

OpenVPN:n notkahdukset kuvan 21 kuvaajassa toistuvat satunnaisesti. Uusinta-ajoissa notkahduksia voi tapahtua millä tahansa alle 5 ms:n jitterillä.

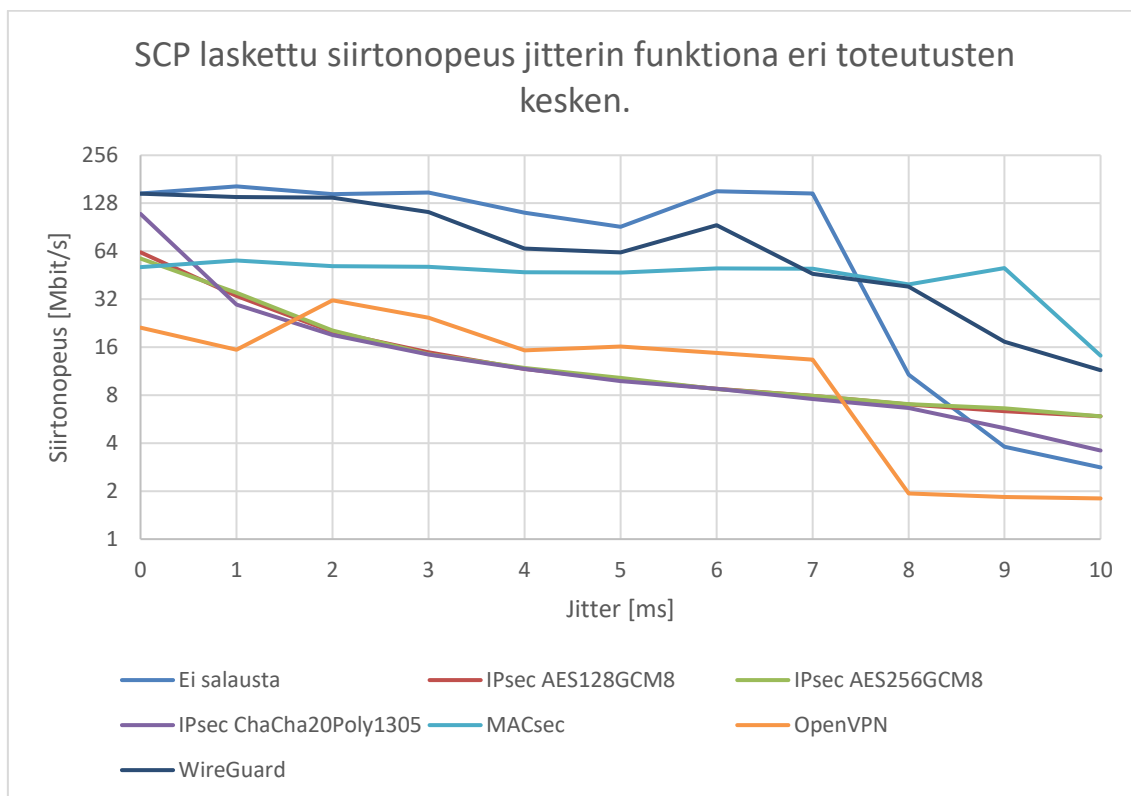
Kuvassa 22 on kuvattu UDP 400M:n testin tulokset jitterin funktiona logaritmisella y-akselilla. Jitterillä ei ole ollenkaan vaikutusta vertailukohteen tuloksiin ja vain pieni vaikutus WireGuardin ja MACsecin tuloksiin. Jitterin vaikutus IPsec toteutuksiin on samantapainen ChaChalla ja molemmilla AES-salauksilla. ChaChan ensimmäinen mittausta 265 Mbit/s ja AES-toteutusten 70 ja 74 Mbit/s. 1 ms:n jitteristä eteenpäin AES ja ChaCha tulokset ovat enimmillään 10 Mbit/s päässä toisistaan. Tulokset ovat huonoimmillaan jitter arvoilla 7 ja 8 ms, minkä jälkeen tulokset alkavat nousemaan. IPsec ChaCha suoriutuu IPsec AES -toteutuksia huonommin jitter välillä 2–7 ms, muuten IPsec ChaCha suoriutuu paremmin. OpenVPN:stä ei saa UDP 400M tuloksia 1 ms ja sitä suuremmalla jitter määrällä.

OpenVPN:n lokiin ilmestyy tällöin mainintoja toistosuojauksen (replay protection) aktivoitumisesta. Vaikuttaa, että OpenVPN tunnistaa testin luoman liikenteen toistohyökkäykseksi ja tästä syystä estää liikenteen.



KUVA 22. UDP 400M -testin tulokset lisätyllä jitterillä.

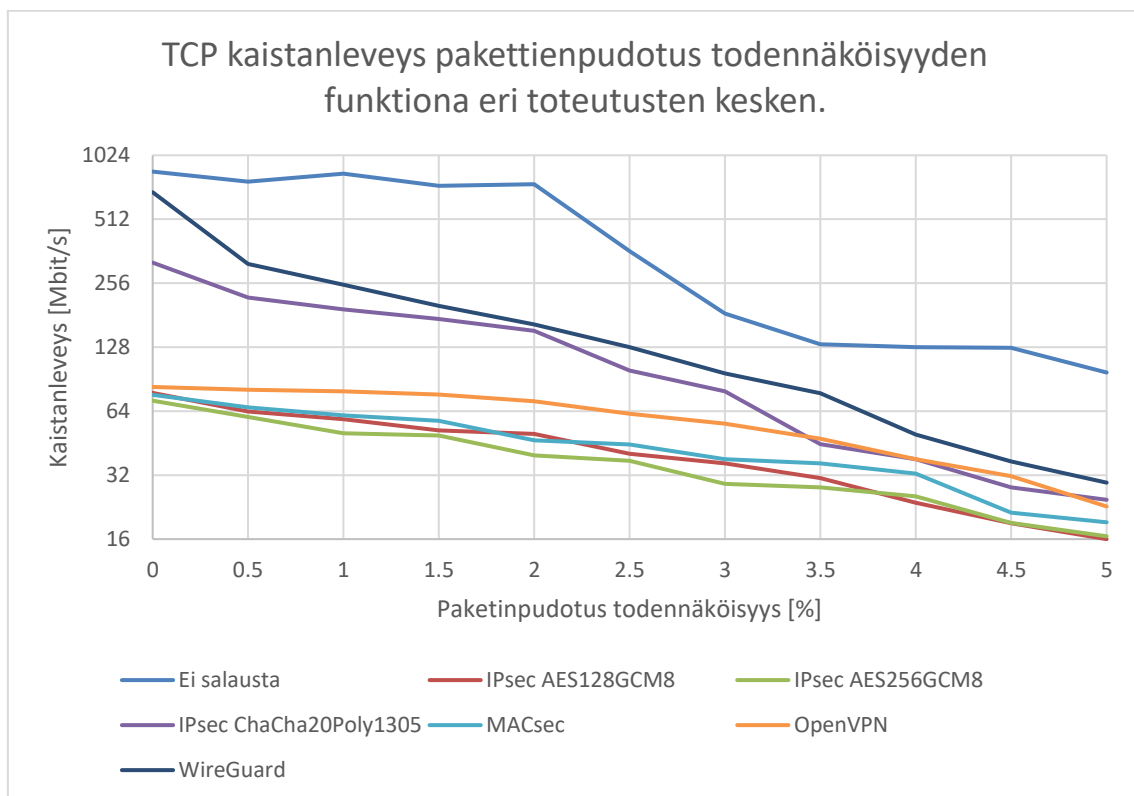
Kuvassa 23 on kuvattu SCP-testin laskennallinen siirtonopeus jitterin funktiona eri toteutusten kesken logaritmisella y-akselilla. Testin tulokset mukailevat TCP-testin tuloksia. Vertailukohteella tulokset käyttäytyvät samalla tavalla 0–7 ms jitter välillä, minkä jälkeen tulokset ovat käytännössä samat. Myös WireGuardilla käyttäytyminen on samanlaista molemmissa testeissä, mutta SCP-testin tulokset ovat koko jitter välillä huonommat kuin TCP-testissä. Pois lukien 0 ms jitter tilanne IPsec-toteutusten tulokset ovat lähes sama SCP- ja TCP-testissä. Myös MACsecin tulokset ovat hyvin lähellä toisiaan molemmissa testeissä. OpenVPN:n notkahdukset 0–1 ja 8–10 ms jitterillä ei toistu aina, mutta jokaisella uudelleen ajolla jollain kohdalla on ollut vastaavia notkahduksia. Notkahdukset pois lukien myös OpenVPN:n SCP-tulokset ovat hyvin lähellä TCP-tuloksia.



KUVA 23. SCP-testin laskennallinen siirtonopeus lisätyllä jitterillä.

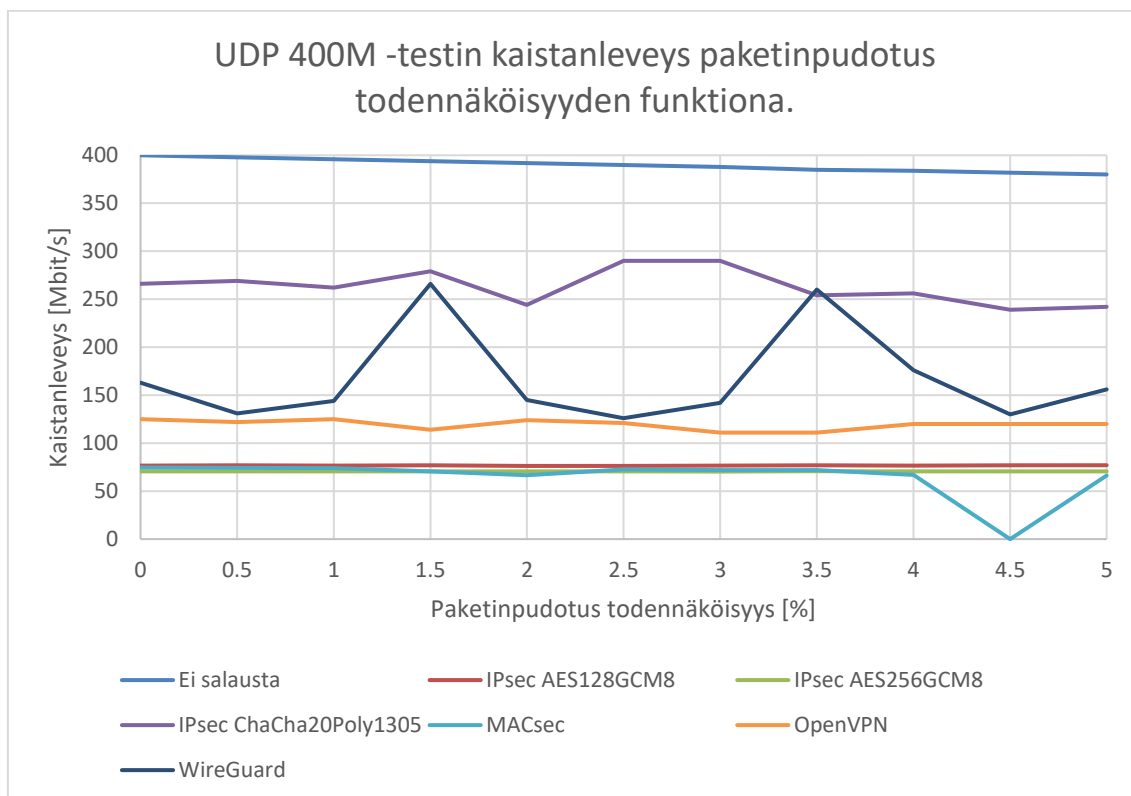
4.2.3 Pakettien pudotuksen vaikutus

Kuvassa 24 on kuvattu TCP-testin tulokset paketinpudotus todennäköisyyden logaritmisella y-akselilla. Vertailukohteen tulokset alkavat 858 Mbit/s ja pysyvät samoissa lukemissa 2 %:n asti, minkä jälkeen suorituskyky noin puolittuu 3.5 %:n asti. WireGuardin suorituskyky alkaa 686 Mbit/s:stä, putoaa puoleen 0,5 %:n kohdalla ja tästä eteenpäin laskee noin neljäsosan per 0,5 %. IPsec ChaChan suorituskyky on samankaltainen kuin WireGuardin vain lähtöpiste on noin puolet WireGuardin lähtöpisteestä. OpenVPN:n suorituskyky alkaa 83 Mbit/s:stä ja laskee vain hiukan 1,5–2 %:n asti, mistä eteenpäin paketinpudotuksen vaikutus nousee jonkin verran. IPsec AES -toteutukset ja MACsec käyttäytyvät kaikki samalla tavalla. Tulokset alkavat 72–78 Mbit/s ja laskee noin 5 Mbit/s per 0,5 %. IPsec AES128 ja MACsecin tulokset ovat erittäin lähellä toisiaan ja IPsec AES256 on samoissa lukemissa mutta hiukan huonommilla tuloksilla.



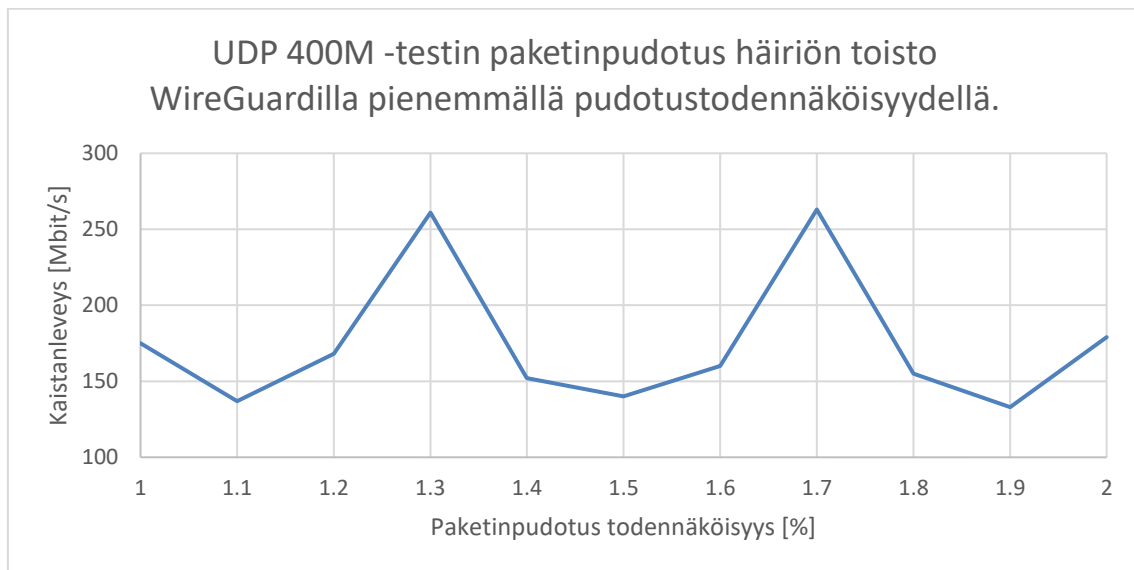
KUVA 24. TCP-testin tulokset lisättyllä pakettienpudotus todennäköisyydellä.

Kuvassa 25 on kuvattu UDP 400M:n testin tulokset pakettienpudotus todennäköisyyden funktiona. Pakettienpudotuksella on selvä vaikutus vain vertailukohteeseen, jonka kaistanleveys alkaa 400 Mbit/s:stä ja putoaa pakettienpudotus todennäköisyyden verran. Kaikkien muiden, pois lukien WireGuardin, kaistanleveydet pysyvät samoissa lukemissa koko pakettienpudotus todennäköisyyden välillä. WireGuardin tulokset ovat 130-176 Mbit/s paitsi pakettienpudotus todennäköisyyksillä 1,5 ja 3,5 %, jolloin tulokset ovat noin 260 Mbit/s.



KUVA 25. UDP 400M -testin tulokset lisätyllä paketinpudotus todennäköisyydellä. MACsecin 4,5 % testi epäonnistui.

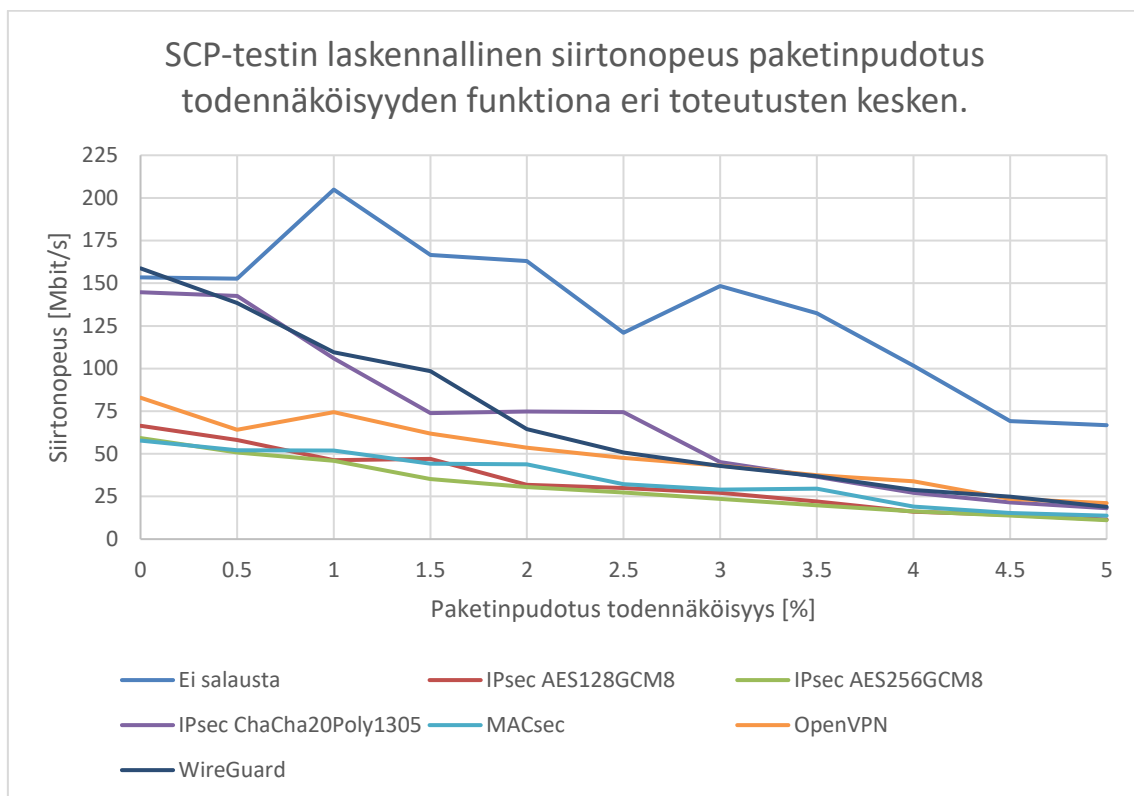
WireGuardin toiminta UDP 400M -testissä on erikoinen. Kyseinen testi ajettiin uudelleen WireGuardilla paketinpudotus todennäköisyys välillä 1–2 %, 0,1 %:n askelin. Tarkoituksena oli saada tarkempi kuva kyseisellä välillä tapahtuvasta piikkistä kaistanleveydessä. Tulokset on kuvattu kuvassa 26. WireGuardin käyrät kuvissa 25 ja 26 ovat muodoiltaan hyvin samanlaiset huolimatta käytetystä todennäköisyys haarukasta, eikä kuvan 26 käyrä vastaa kuvan 25 WireGuardin käyrää ollenkaan niiden yhteisellä paketinpudotus todennäköisyyden välillä. Molemissa kuvaajissa joka 4. mittaus poikkeaa muista huomattavasti. UDP 400M -testi toistettiin WireGuardilla vielä 1 %:n paketinpudotus todennäköisyydellä 11 kertaa putkeen. Tulosten käyrä pysyy saman muotoisena kuin kuvissa 25 ja 26. Joka 4. mittaus poikkeaa muista. Piikit eivät siis johdu tietystä paketinpudotus todennäköisyydestä vaan jostain muusta. Kaistanleveyden piikkien kohdalla lähetettyjen pakettien ja pudotettujen pakettien määrä on poikkeuksellisen matala.



KUVA 26. UDP 400M -testin uudelleen ajo WireGuardilla paketinpudotus todennäköisyyksillä 1–2 %.

UDP 1 Mbit/s testissä kaikkien tulos laskee pakettienpudotus todennäköisyyden verran. Vertailukohteen ja kaikkien toteutusten tulokset ovat käytännössä samat.

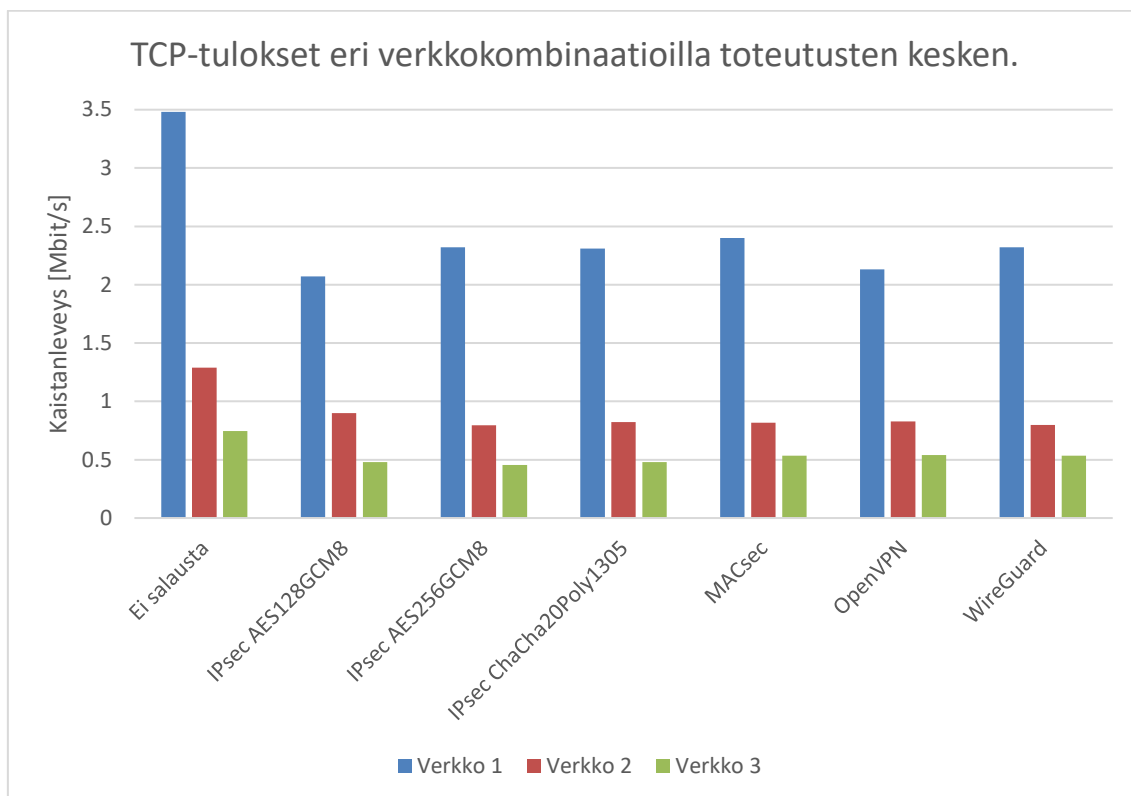
Kuvassa 27 on kuvattu SCP-testin laskennallinen siirtonopeus paketinpudotus todennäköisyyden funktiona. Testin tulokset ymmärrettävästi mukailevat TCP-testin tuloksia. Vertailukohteen tulosten käyttäytyminen on samalainen kuin TCP-testissä ainoastaan aloituspisteenä toimii 150 Mbit/s. Myös IPsec ChaChan ja WireGuardin käyttäytyminen on samalainen TCP-testissä mutta aloituspisteenä toimii 144 Mbit/s ja 158 Mbit/s. IPsec AES -totutusten, MACsecin ja OpenVPN:n TCP-testin tulokset ovat tasaisesti noin 10 Mbit/s korkeammat kuin SCP-testissä.



KUVA 27. SCP-testin laskennallinen siirtonopeus lisätyllä pakettin pudotus todennäköisyydellä.

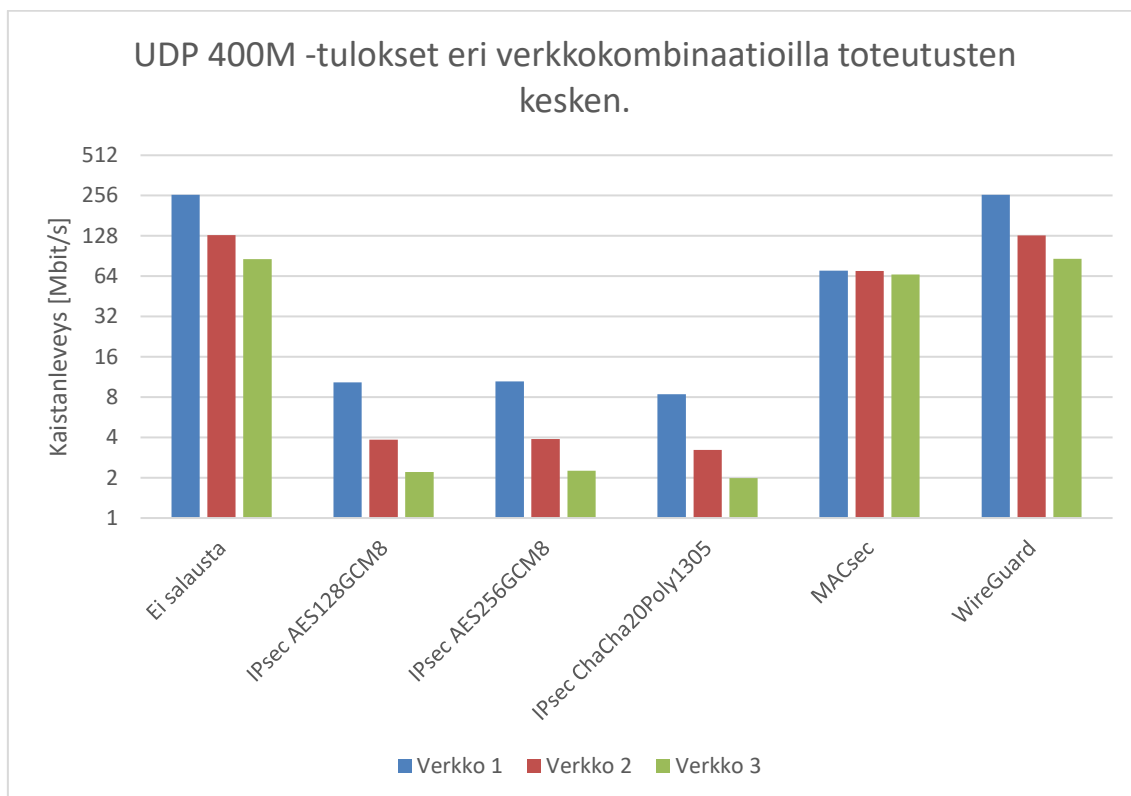
4.2.4 Viiveen, jitterin ja pakettien pudotuksen yhteisvaikutus

Kuvassa 28 on esitetty TCP-testin tulokset eri verkkokombinaatioilla. Ero vertailukohteen ja toteutusten välillä on selvä, mutta toteutusten kesken erot ovat pieniä.



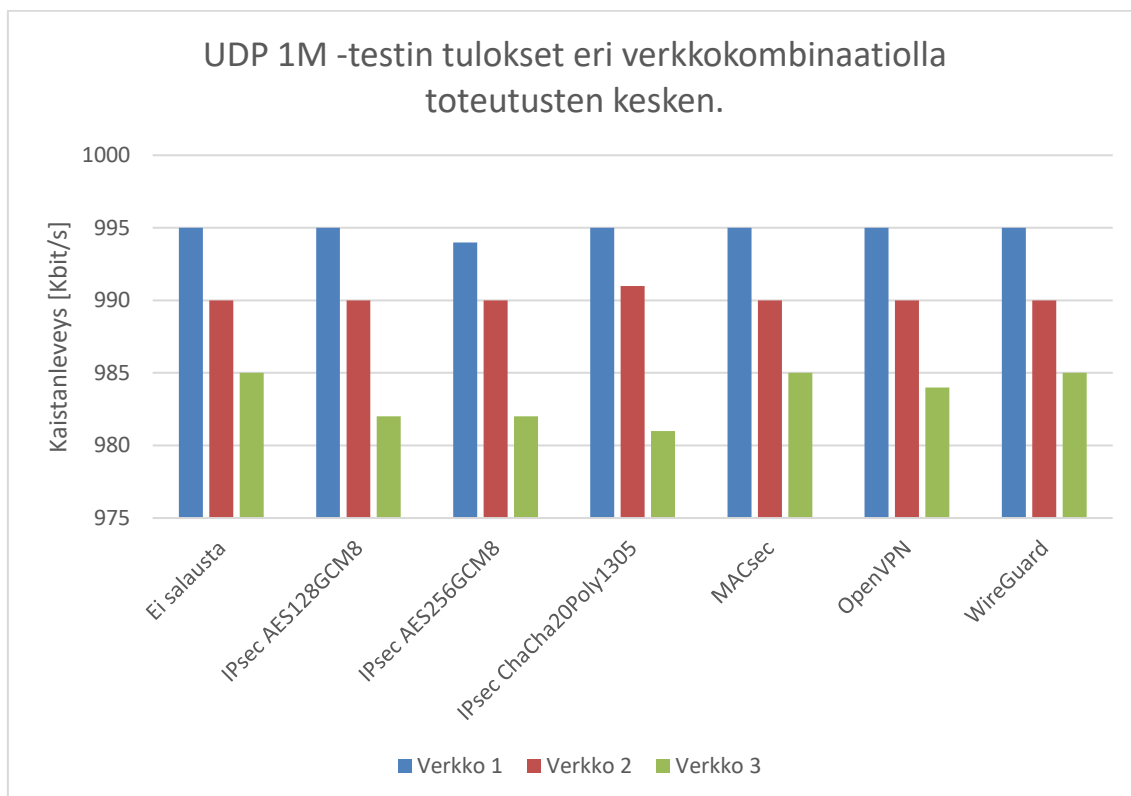
KUVA 28. TCP-testin tulokset eri verkkokombinaatioilla.

Kuvassa 29 on kuvattu UDP 400M testin tulokset eri verkkokombinaatiolla logaritmisella y-akselilla. IPsec toteutusten tulokset ovat kaikki hyvin lähellä toisiaan. Ainoastaan IPsec ChaChan tulokset ovat IPsec AES -toteutuksia huonommat. WireGuardin kaistanleveys on käytännössä sama kuin vertailukohteella. MACseciin eri verkkojen vaikutus vastaa verkossa olevan paketinpudotus todennäköisyyden vaikutusta. Jitter häirityn UDP 400M -testin tapaan OpenVPN ei toimi testin aikana ja OpenVPN:n lokiin ilmestyy samantapaisia viestijä toistosuojauksesta.



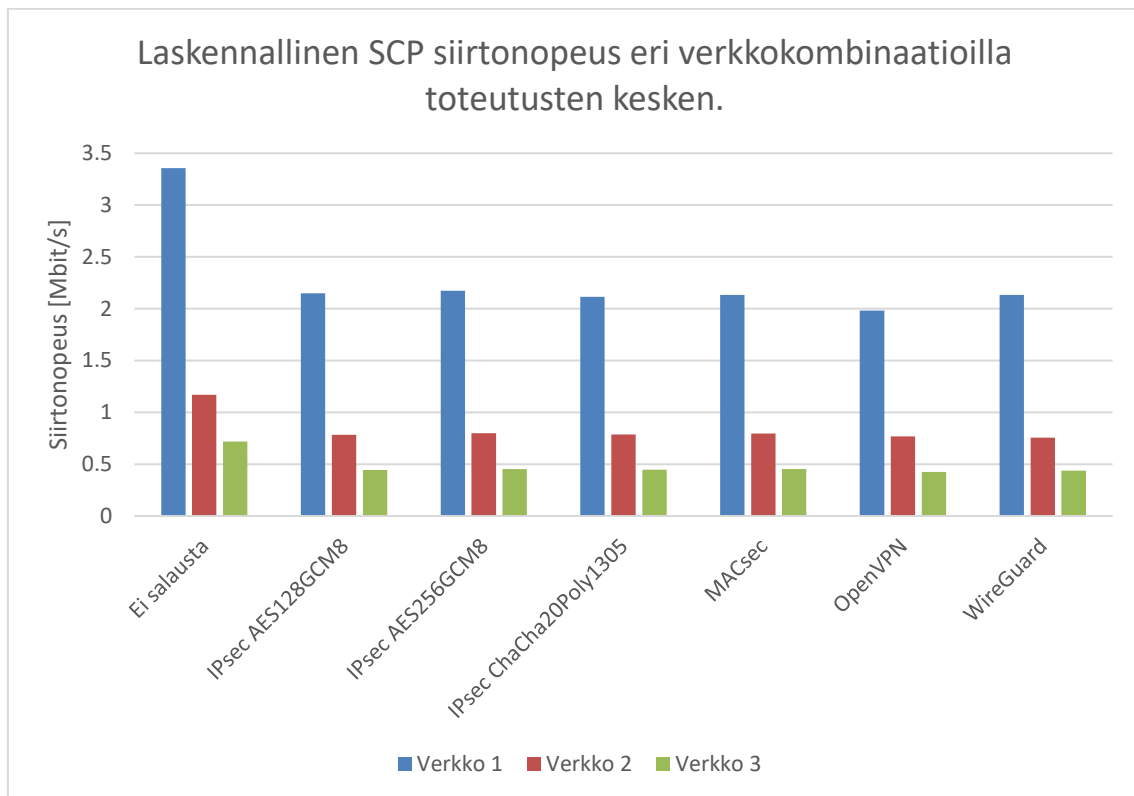
KUVA 29. UDP 400M -testin tulokset eri verkkokombinaatioilla.

Kuvassa 30 on kuvattu UDP 1M testin tulokset eri verkko kombinaatioilla. UDP 1M toteutusten tulosten erot ovat pieniä. Kaistanleveys putoaa yleensä pakettien-pudotus todennäköisyyden verran ja raportoitu jitter kasvaa verkon jitterin mu-kana. Poikkeuksena tähän on IPsec-toteutukset ja OpenVPN, mitkä putoavat ver-kon 3 tilanteessa muutaman kilotavun enemmän.



KUVA 30. UDP 1M -testin tulokset eri verkkokombinaatioilla.

Kuvassa 31 on kuvattu SCP-testin laskennallinen siirtonopeus eri verkko kombinaatioilla. Vertailukohteen ja toteutusten SCP-siirtonopeus on erittäin samansuuntainen TCP-tulosten kanssa. Ainoa ero TCP-tuloksiin on, että SCP-siirtonopeus on kaikissa tuloksissa hiukan TCP-tuloksia pienempi. Erot toteutusten välillä ovat hyvin pienet.



KUVA 31. SCP-testin laskennallinen siirtonopeus eri verkkokombinaatioilla.

4.3 Johtopäätökset

Kokonaisuudessaan IPsec AES128:n ja IPsec AES256:n tulokset poikkeuksetta hyvin lähellä toisiaan ja IPsec AES256:n tulokset hiukan huonompia kuin IPsec AES128:n tulokset. Ideaaliverkossa IPsec AES -toteutusten suorituskyky on myös poikkeuksetta huonoimpien joukossa. IPsec AES -toteutusten pullonkaulana toimii mitä todennäköisimmin laitteistokiihdytyksen puute AES-suvun salausalgoritmeille. Tämä on totta myös OpenVPN:n ja MACsecin kohdalla. Häiriöverkon testeissä testatulla viivehaarukalla ei vaikuta olevan vaikutusta IPsec AES -toteutusten tuloksiin. Jitterillä ja paketin pudotuksella taas on huomattava vaikutus tuloksiin. Näillä häiriöillä suurin vaikutus IPsec AES tuloksiin on ensimmäisillä häiriöarvoilla nollatilanteen jälkeen. Tästä eteenpäin häiriön vaikutus tuloksiin pienenee. Poikkeuksena tähän käyttäytymiseen on jitterhäiritetty UDP 400M -testi, jossa tulokset alkavat noustamaan tietyn pisteen jälkeen, ja paketinpudotus häiritetty SCP-testi, jossa siirtonopeus laskee tasaisesti koko paketinpudotus todennäköisyyskaalalla.

IPsec ChaChan suorituskyyky on ideaalitalanteessa toteutusten kesken yleensä toiseksi paras ja UDP 400M -testissä paras. Lisäksi IPsec ChaChan suorittimen kuormitus on samalla tasolla tai pienempi IPsec AES -toteutusten kanssa, vaikka se suoriutuu AES-toteutuksia paremmin. Häiriöisissä testeissä IPsec ChaChan suorituskyyky on hyvin lähellä WireGuardin suorituskyykyä. Poikkeuksena tähän on jitter häirityt testit, missä häiriöskaalan alkupään jälkeen IPsec ChaChan tulokset ovat huomattavasti huonommat ja ovat hyvin lähellä IPsec AES -toteutusten tuloksia.

MACsecin suorituskyyky ideaaliverkon testeissä on samaa luokkaa IPsec AES -toteutusten kanssa. Usein MACsecin tulokset ovat kahden IPsec AES -toteutuksen välissä. MACsecin suorituskyyvyn pullonkaulana on todennäköisesti IPsec AES -toteutusten tapaan laitteistokiihdytyksen puute AES-salausalgoritmile. Häiriöisissä testeissä MACsecin suorituskyyky pysyy usein koko häiriöskaalan matkalla samoissa lukemissa. Poikkeuksena tähän on paketinpu-dotus testit, jossa MACsecin suorituskyyky laskee koko skaalan matkalla.

MACsec ja IPsec AES128 käyttävät samaa salausalgoritmia, joten tämän ansiosta voidaan vertailla IPsecin ja MACsecin suorituskyykyä ilman salausalgoritmien vaikutusta. Ideaaliverkon testeissä MACsecin ja IPsec AES128:n tulokset ovat lähellä toisiaan mutta IPsec AES128 suoriutuu hieman MACseciä paremmin ja pienemmällä prosessorin kuormituksella. Poikkeukset tähän ovat:

- Ping-testi, MACsecin tuoma viive on hiukan pienempi kuin IPsec AES128:n
- toteutusten MTU, MACsecin kanssa jää enemmän tilaa hyötyliikenteelle

OpenVPN:n suorituskyyky ideaaliverkon testeissä on pääsääntöisesti kolmanneksi paras. Poikkeus tähän on ping-testi, missä OpenVPN:n tulokset ovat huonommat. Lisäksi ideaaliverkon UDP 1M -testissä, missä kaikkien testi tulokset ovat käytännössä samat, OpenVPN:n suorittimen käyttöaste on korkein. Eli OpenVPN joutuu tekemään eniten työtä saman lopputuloksen saavuttamiseksi. Häiriöverkon viivetestissä OpenVPN:n suorituskyyky on huonoin. Jitter-testeissä TCP- ja SCP-suorituskyyky on kolmanneksi paras, jos tuloksissa ovat notkahdukset eivät toistu. Paketinpu-dotus testeissä häiriöllä ei ole muista toteutuksista

poikkeavaa vaikutusta. Lisäksi OpenVPN on ainoa toteutus, mikä kokonaan lopettaa toimimisen UDP 400M -testissä jitterin kanssa. Tätä tilannetta voisi mahdollisesti yrittää korjata säätämällä OpenVPN toistosuojaus (replay protection) parametreja tai kokonaan poistamalla toistosuojauksen käytöstä.

WireGuardin suorituskyky ideaaliverkon testeissä on toteutusten kesken yleensä paras. Ainoat poikkeukset ovat UDP 400M, missä IPsec ChaCha suoriutuu paremmin ja Ping-testi, jossa WireGuard aiheuttaa suurimman lisäyksen viiveeseen. Monella tavoitenopeudella tehdyssä UDP 25–400M testissä kuitenkin WireGuard pysyy toteutuksista pisimpään tavoitenopeudessa. Häiriöisen verkon testeissä WireGuard suorituskyvyn muutokset mukailevat vertailukohteen muutoksia. Suhteellinen vaikutus molempiin on samaa luokkaa. Poikkeus tähän on paketinpudotus testit. TCP-tulokset puolittuvat jo 0,5 %:n paketinpudotus todennäköisyydellä ja UDP 400M -tulokset vaihtelevat suuresti, vaikka todennäköisyys pysyisi saman.

Sen ansiosta, että IPsec ChaCha ja WireGuard käyttävät salaamiseen samoja algoritmeja, voidaan vertailla toteutusten itsensä suorituskyky ilman salausalgoritmien vaikutusta. Ideaaliverkossa WireGuard suoriutuu IPsec ChaChata paremmin ja UDP 400M -testissä WireGuard pystyy suurempaan tavoite kaistanleveyteen. Häiriö-testeissä molempien tulokset ovat yleensä samoissa lukemissa. Ainoastaan pienimmillä häiriöarvoilla WireGuard suoriutuu paremmin. Poikkeuksena tähän on jitter testit, missä poikkeuksetta WireGuard suoriutuu paremmin.

Kokonaisuudessaan tulosten perusteella parhaiten Raspberry Pillä suoriutuu WireGuard ja tämän jälkeen IPsec ChaCha-salauksella. Näiden toteutusten suorituskyky on hyvä eivätkä ne ole poikkeuksellisen herkkiä häiriöille.

5 YHTEENVETO

Tämän työn tarkoituksena oli selvittää, miten eri verkkosalaustekniikat vertautuvat toisiinsa. Salaustekniikoiden suorituskykyä testattiin ideaaliverkossa ja häiriöisessä verkossa. Häiriöiden vaikutusta testattiin ottamalla käyttöön yksi häiriötyyppi kerrallaan ja ottamalla käyttöön toimeksiantajan määrittelemiä usean häiriön yhdistelmiä.

Vertailussa tutkittiin IPseciä kolmella eri salauksella, MACseciä, OpenVPN:ää ja WireGuardia ja vertailukohteena testit suoritettiin ilman mitään näistä. IPseciä tutkittiin useilla salauksilla, jotta voidaan vertailla toteutuksia ilman salausalgoritmin vaikutusta. IPseciä käytettiin AES128-, AES256- ja ChaCha-salauksilla. Tällä tavoin vertailtiin keskenään IPseciä ja MACseciä sekä IPseciä ja WireGuardia. Vertailu toteutettiin kahden Raspberry Pi 4 -laitteella, Ethernet-yhteyden yli.

Vertailussa parhaiten suoriutui WireGuard ja toiseksi parhaiten IPsec ChaCha salauksella. Molempien näiden toteutusten suorituskyky on hyvä ideaaliverkossa eivätkä ne ole erityisen herkkiä häiriöille. Suurimmat erot näiden toteutusten välillä ovat WireGuardin moniydin-tuki, joka mahdollistaa paremman suorituskyvyn, ja WireGuardin pienempi herkkyys jitterille.

Kuitenkin siirtonopeuksien ollessa pieniä, kuten UDP 1M -testissä, kaikkien toteutusten tulokset ovat hyvin samanlaiset. Toteutusten väliset erot ilmenevät vasta suuremmilla nopeuksilla.

Yksi suurimmista tuloksiin vaikuttavista asioista on Raspberry Pin AES-laitteistokiihdytyksen puute. Tämä laskee IPsec AES -toteutusten, OpenVPN:n ja MACsecin suorituskykyä huomattavasti. Ainoat toteutukset, mihin tämä puute ei vaikuta, ovat IPsec ChaCha -toteutus ja WireGuard.

Kattavampien tulosten saamiseksi työtä voisi jatkaa tutkimalla lisää verkkosalaustekniikoita, ottaen mukaan jo tietoturvan kannalta vanhentuneita tekniikoita ja tekniikoita, jotka huomattavasti poikkeavat jo tutkituista. Lisäksi häiriöiden osalta voitaisiin tutkia, miten epäsymmetrinen yhteys vaikuttaa tekniikan suori-

tuskykyyn ja miten pakettien uudelleen järjestäminen tai monistaminen vaikuttavat. Häiriöt myös olisi parempi toteuttaa kolmannella laitteella kahden Raspberry Pi -laitteen välissä. Myös pelkän IPsecin vaikutusta voisi tutkia ottamalla IPsecin käyttöön ilman mitään salausalgoritmia. Viimeisenä AES-laitteistokiihdytystä tukevan laitteiston käyttäminen mahdollistaisi huomattavasti paremman suorituskyvyn IPsec AES -toteutusten, MACsecin ja OpenVPN kohdalla.

LÄHTEET

1. Bittium. 2021. Bittium. Saatavissa: <https://www.bittium.com>. Hakupäivä 12.4.2021.
2. Microsoft. 2009. Virtual Private Networking: An Overview. Microsoft. Saatavissa: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742566\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742566(v=technet.10)). Hakupäivä 22.10.2021.
3. Cloudflare. What is IPsec? Cloudflare. <https://www.cloudflare.com/learning/network-layer/what-is-ipsec/>. Hakupäivä 14.4.2021.
4. Kent, Stephen - Seo, Karen 2005. Security Architecture for the Internet Protocol. The Internet Engineering Task Force. Saatavissa: <https://data-tracker.ietf.org/doc/html/rfc4301>. Hakupäivä 14.4.2021.
5. Dubroca, Sabrina 2016. MACsec - Encryption for wired LAN. Red Hat. Saatavissa: <https://netdevconf.info/1.1/proceedings/slides/dubroca-macsec-encryption-wire-lan.pdf>. Hakupäivä 16.4.2021.
6. OpenVPN. 2016. Overview of OpenVPN. OpenVPN. Saatavissa: <https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn>. Hakupäivä 5.10.2021.
7. Donenfeld, Jason A. 2020. WireGuard: Next Generation Kernel Network Tunnel. Saatavissa: <https://www.wireguard.com/papers/wireguard.pdf>. Hakupäivä 29.3.2021.
8. Wouters, Paul - Migault, Daniel - Mattsson, John - Nir, Yoav - Kivinen, Tero 2017. Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH). The Internet Engineering Task Force. Saatavissa: <https://data-tracker.ietf.org/doc/html/rfc8221>. Hakupäivä 26.11.2021.

9. Nir, Yoav - Kivinen, Tero - Wouters, Paul - Migault, Daniel 2017. Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2). The Internet Engineering Task Force. Saatavissa: <https://datatracker.ietf.org/doc/html/rfc8247>. Hakupäivä 26.11.2021.
10. Kaufman, Charlie - Hoffman, Paul - Nir, Yoav - Eronen, Pasi - Kivinen, Tero 2014. Internet Key Exchange Protocol Version 2 (IKEv2). The Internet Engineering Task Force. Saatavissa: <https://datatracker.ietf.org/doc/html/rfc7296>. Hakupäivä 5.5.2021.
11. Kili, Aaron 2020. How to Set Up IPsec-based VPN with Strongswan on Debian and Ubuntu. TecMint. Saatavissa: <https://www.tecmint.com/setup-ipsec-vpn-with-strongswan-on-debian-ubuntu/>. Hakupäivä 1.6.2021.
12. Weis, Brian 2009. Overview of IEEE 802.1X-REV - Dynamic Session Key Agreement. The Internet Engineering Task Force. Saatavissa: <https://www.ietf.org/proceedings/76/slides/msec-5.pdf>. Hakupäivä 17.9.2021.
13. Malinen, Jouni 2007. wpa_supplicant(8) - Linux man page. die.net Saatavissa: https://linux.die.net/man/8/wpa_supplicant. Hakupäivä 9.6.2021.
14. Dubroca, Sabrina 2017. What's new in MACsec: setting up MACsec using wpa_supplicant and (optionally) NetworkManager. RedHat. https://developers.redhat.com/blog/2017/06/28/whats-new-in-macsec-setting-up-macsec-using-wpa_supplicant-and-optional-networkmanager. Hakupäivä 9.6.2021.
15. Donenfeld, Jason A. 2020. Saatavissa: <https://www.wireguard.com/>. Hakupäivä 29.3.2021.
16. Ludwig, Justin 2020. Vastaus kysymykseen: What is the difference between Endpoint and AllowedIPs fields in Wireguard config file? stackoverflow. Saatavissa: <https://stackoverflow.com/a/65453146>. Hakupäivä 19.5.2021.
17. Donenfeld, Jason A. 2020. Quick Start. Saatavissa: <https://www.wireguard.com/quickstart/>. Hakupäivä 29.3.2021.

18. Donenfeld, Jason A. WG. Saatavissa: <https://git.zx2c4.com/wireguard-tools/about/src/man/wg.8>. Hakupäivä 29.3.2021.
19. Donenfeld, Jason A. WG-QUICK. Saatavissa: <https://git.zx2c4.com/wireguard-tools/about/src/man/wg-quick.8>. Hakupäivä 29.3.2021.
20. Raspberry Pi 3 Model B+. The Raspberry Pi Foundation. Saatavissa: <https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/>. Hakupäivä 4.5.2021.
21. Raspberry Pi 4 Tech Specs. The Raspberry Pi Foundation. Saatavissa: <https://www.raspberrypi.org/products/raspberry-pi-4-model-b/specifications/>. Hakupäivä 4.5.2021.
22. iPerf. iPerfs user docs. Iperfs.fr Saatavissa: <https://iperf.fr/iperf-doc.php>. Hakupäivä 17.2.2021.
23. netem. 2021. The Linux Foundation. Saatavissa: <https://wiki.linuxfoundation.org/networking/netem>. Hakupäivä 13.4.2021.
24. Rodola, Giampaolo 2020. psutil documentation. Saatavissa: <https://psutil.readthedocs.io/en/latest/>. Hakupäivä 21.5.2021.
25. Microsoft. 2021. Prepare your organization's network for Microsoft Teams. Microsoft. Saatavissa: <https://docs.microsoft.com/en-us/microsoftteams/prepare-network>. Hakupäivä 3.8.2021.

LIITTEET

Liite 1 Ohjelmistojen versiot

Liite 2 IPsec konfiguraatiotiedostot

Liite 3 MACsec konfiguraatiotiedosto

Liite 4 OpenVPN konfiguraatiotiedostot

Liite 5 WireGuard konfiguraatiotiedostot

Liite 6 Ideaaliverkon tulokset

Liite 7 Viivehäiriön tulokset

Liite 8 Paketinpudotushäiriön tulokset

Liite 9 Jitterhäiriön tulokset

Liite 10 Viiveen-, pakettienpudotus- ja jitterhäiriöiden yhteistulokset

Linux ytimen versio:

Linux raspberrypi-2 5.10.39-v7l-pyhaant-macsec-added+ #1 SMP Fri May 28 05:56:33
BST 2021 armv7l GNU/Linux

OpenVPN versio:

OpenVPN 2.5.3 armv7l-unknown-linux-gnueabi [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[MH/PKTINFO] [AEAD] built on Jul 6 2021
library versions: OpenSSL 1.1.1d 10 Sep 2019, LZO 2.10

IPsec versio:

Linux strongSwan U5.7.2/K5.10.39-v7l-pyhaant-macsec-added+

wpa_supplicant versio:

wpa_supplicant v2.8-devel

wireguard-tools versio:

wireguard-tools v1.0.20200827 - <https://git.zx2c4.com/wireguard-tools/>

MACsec ja WireGuard kuuluvat Linuxin ytimen lähdekoodiin.

ipsec.conf.aes128

```
config setup
    charondebug="all"
    uniqueids=yes
conn client2-to-server1
    type=tunnel
    auto=start
    keyexchange=ikev2
    authby=secret
    left=169.254.133.103
    leftsubnet=169.254.133.103/16
    right=169.254.16.161
    rightsubnet=169.254.16.161/16
    ike=aes128gcm8-prfsha256-modp1024!
    esp=aes128gcm8-prfsha256!
    aggressive=no
    keyingtries=%forever
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=30s
    dpdtimeout=120s
    dpdaction=restart
```

ipsec.conf.aes256

```
config setup
    charondebug="all"
    uniqueids=yes
conn client2-to-server1
    type=tunnel
    auto=start
    keyexchange=ikev2
    authby=secret
    left=169.254.133.103
    leftsubnet=169.254.133.103/16
    right=169.254.16.161
    rightsubnet=169.254.16.161/16
    ike=aes256gcm8-prfsha256-modp1024!
    esp=aes256gcm8-prfsha256!
    aggressive=no
    keyingtries=%forever
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=30s
    dpdtimeout=120s
    dpdaction=restart
```

ipsec.conf.chacha

```
config setup
    charondebug="all"
    uniqueids=yes
conn client2-to-server1
    type=tunnel
    auto=start
    keyexchange=ikev2
    authby=secret
    left=169.254.133.103
    leftsubnet=169.254.133.103/16
    right=169.254.16.161
    rightsubnet=169.254.16.161/16
    ike=chacha20poly1305-prfsha256-modp1024!
    esp=chacha20poly1305-prfsha256!
    aggressive=no
    keyingtries=%forever
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=30s
    dpdtimeout=120s
    dpdaction=restart
```

wpa_supplicant.conf.mac

ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev

update_config=1

country=FI

network={

key_mgmt=NONE

eapol_flags=0

macsec_policy=1

mka_cak=0123456789ABCDEF0123456789ABCDEF

37475767778797A303132333435

mka_cken=6162636465666768696A6B6C6D6E6F7071727

mka_priority=128

}

server.conf:

```
dev tun
ifconfig 10.8.0.1 10.8.0.2
secret /home/pi/openvpn/static.key
```

```
keepalive 10 120
ping-timer-rem
persist-tun
persist-key
```

```
cipher AES-256-CBC
```

client.conf:

```
remote 169.254.16.161
dev tun
ifconfig 10.8.0.2 10.8.0.1
secret /home/pi/openvpn/static.key
```

```
keepalive 10 120
ping-timer-rem
persist-tun
persist-key
```

```
cipher AES-256-CBC
```

wg0-raspi1.conf

[Interface]

Address = 10.0.0.1/24

PrivateKey = qPoq/PHnspqTe6SqJANclxKlyNzHcA0RqRh3rE33P1U=

ListenPort = 51820

[Peer]

Endpoint = 169.254.133.103:51820

PublicKey = TO0gZu62dnFI87EeNnxXvwIG91Pk4hzBAUJxvjX5Q3g=

AllowedIPs = 10.0.0.2/32

wg0-raspi2.conf

[Interface]

Address = 10.0.0.2/24

PrivateKey = iHDPxXAskIQ/wjA51qFXd4/bU1StV5gRG8XNm7Cb8Uo=

ListenPort = 51820

[Peer]

Endpoint = 169.254.16.161:51820

PublicKey = NZyYbm1yZ7/8q/7Vh33hDk22iT/Dowf45053s1z5IX8=

AllowedIPs = 10.0.0.1/32

IDEAALIVERKON TULOKSET

Liite 6

Mittauksen keskiarvot:

Name	Ping - min	Avg	Max	Mdev	Yksikkö	TCP - kaista	Yksikkö	SCP - kesto / s
Ei salausta	0.1998	0.2348	0.2584	0.017	ms	841.6	Mbits/sec	13.26944308
IPsec AES128GCM8	0.4482	0.49	0.5364	0.0244	ms	77.65	Mbits/sec	30.86078749
IPsec AES256GCM8	0.4564	0.5014	0.5508	0.023	ms	71.05	Mbits/sec	33.96057153
IPsec ChaCha20Poly1305	0.3762	0.4306	0.4738	0.0248	ms	320.5	Mbits/sec	15.359829
MACsec	0.338	0.4148	0.4634	0.0326	ms	76.6	Mbits/sec	36.60967126
OpenVPN	0.8654	1.0644	2.4806	0.2144	ms	87.15	Mbits/sec	28.96586337
WireGuard	0.6296	0.8006	1.2166	0.1912	ms	669.5	Mbits/sec	12.92455707

Name	UDP 400 M - kaista	Yksikkö	Jitter	Yksikkö	Pudotetut	Lähetetyt	UDP 1M - kaista	Yksikkö	Jitter	Yksikkö	Pudotetut	Lähetetyt
Ei salausta	400	Mbits/sec	0.0006	ms	2717.2	11538461	1	Mbits/sec	0.0028	ms	0	146485
IPsec AES128GCM8	75.96	Mbits/sec	0.5482	ms	18085.6	2209338	1	Mbits/sec	0.0056	ms	0	146485
IPsec AES256GCM8	70.14	Mbits/sec	0.5334	ms	2908.4	2026811.4	1	Mbits/sec	0.0022	ms	0	146485
IPsec ChaCha20Poly1305	276	Mbits/sec	0.0312	ms	969260	8931456	1	Mbits/sec	0.0024	ms	0	146485
MACsec	69.7	Mbits/sec	0.047	ms	108563.8	2119436.6	1	Mbits/sec	0.0024	ms	0	146485
OpenVPN	122.8	Mbits/sec	7.8548	ms	7994953.6	11538462.4	1	Mbits/sec	0.0052	ms	0	146485
WireGuard	190.2	Mbits/sec	9.4146	ms	5279704	10766943.8	1	Mbits/sec	0.0232	ms	0	146485

IDEAALIVERKON TULOKSET

Liite 6

Mittauksen keskihajonnat:

Name	Ping - min	Avg	Max	Mdev	Yksikkö	TCP - kaista	Yksikkö	SCP - kesto / s
Ei salausta	0.00304	0.00496	0.00752	0.0028	ms	39.76	Mbits/sec	0.894722
IPsec AES128GCM8	0.00696	0.0052	0.00712	0.00712	ms	0.144	Mbits/sec	1.233286
IPsec AES256GCM8	0.00688	0.00928	0.00496	0.0044	ms	0.144	Mbits/sec	1.899635
IPsec ChaCha20Poly1305	0.01264	0.00912	0.00416	0.00504	ms	0.64	Mbits/sec	1.152831
MACsec	0.002	0.00344	0.00648	0.00192	ms	0.104	Mbits/sec	1.608166
OpenVPN	0.01592	0.03824	2.07696	0.25424	ms	2.616	Mbits/sec	1.676957
WireGuard	0.03008	0.14216	0.58256	0.24512	ms	65.84	Mbits/sec	0.505375

Name	UDP 400 M - kaista	Yksikkö	Jitter	Yksikkö	Pudotetut	Lähetetyt	UDP 1M - kaista	Yksikkö	Jitter	Yksikkö	Pudotetut	Lähetetyt
Ei salausta	0	Mbits/sec	0.00048	ms	859.76	0.4	0	Mbits/sec	0.00128	ms	0	0
IPsec AES128GCM8	0.208	Mbits/sec	0.00424	ms	4751.68	2229.6	0	Mbits/sec	0.00272	ms	0	0
IPsec AES256GCM8	0.048	Mbits/sec	0.05992	ms	1198.88	815.84	0	Mbits/sec	0.00112	ms	0	0
IPsec ChaCha20Poly1305	17.6	Mbits/sec	0.00984	ms	474051.6	496137.2	0	Mbits/sec	0.00088	ms	0	0
MACsec	7.52	Mbits/sec	0.022	ms	173277.7	43879.84	0	Mbits/sec	0.00064	ms	0	0
OpenVPN	1.12	Mbits/sec	6.21024	ms	35592.16	0.48	0	Mbits/sec	0.00064	ms	0	0
WireGuard	35.44	Mbits/sec	7.49648	ms	2081630	1234430	0	Mbits/sec	0.01504	ms	0	0

IDEAALIVERKON TULOKSET

Liite 6

Asiakkaan CPU:

Toteutus	Testi	Keskiarvo			Hajonta		
		Käyttö / %	Taajuus / MHz	Lämpö / °C	Käyttö / %	Taajuus / MHz	Lämpö / °C
Ei salausta	Ping	0.098815	600	47.42748	0.005032	0	0.157036
Ei salausta	SCP	8.739381	935.4156	49.35422	0.875505	43.78701	0.094094
Ei salausta	TCP	22.25674	1476.547	55.94976	1.563075	0	0.236679
Ei salausta	UDP 1m	0.796863	604.0523	50.55665	0.028261	1.385621	0.152912
Ei salausta	UDP 400m	17.05132	1476.501	59.33574	2.978558	0.036789	0.363316
IPsec AES128GCM8	Ping	0.253483	600.2899	49.93125	0.236254	0.463768	0.247702
IPsec AES128GCM8	SCP	17.31738	1299.383	51.846	1.664077	10.27938	0.320723
IPsec AES128GCM8	TCP	21.55322	1476.547	56.7058	0.340821	0	0.315868
IPsec AES128GCM8	UDP 1m	1.22451	646.3399	49.96143	0.033725	9.72549	0.301876
IPsec AES128GCM8	UDP 400m	9.151347	1402.407	55.69092	0.121658	5.971003	0.301613
IPsec AES256GCM8	Ping	0.398576	600	48.84177	0.463178	0	0.351254
IPsec AES256GCM8	SCP	17.294	1317.791	52.00263	1.041756	8.079121	0.241023
IPsec AES256GCM8	TCP	21.82287	1476.678	56.41296	0.207088	0.156352	0.277289
IPsec AES256GCM8	UDP 1m	1.312614	657.1242	50.02318	0.054745	15.60784	0.230959
IPsec AES256GCM8	UDP 400m	9.268925	1405.993	55.66485	0.079583	2.058632	0.262187
IPsec ChaCha20Poly1305	Ping	0.102656	600	49.19899	0.005523	0	0.339098
IPsec ChaCha20Poly1305	SCP	14.86016	1109.644	50.93295	0.397774	34.10277	0.373727
IPsec ChaCha20Poly1305	TCP	27.88799	1476.647	59.29702	0.29806	0.180878	0.297106
IPsec ChaCha20Poly1305	UDP 1m	1.153529	624.7712	51.31707	0.034301	7.895425	0.237834
IPsec ChaCha20Poly1305	UDP 400m	24.57043	1478	60.79399	0.483517	1.704371	0.157746
MACsec	Ping	0.112511	600	49.11411	0.013291	0	0.380582
MACsec	SCP	19.48934	1285.993	53.15424	0.675263	15.48504	0.297164
MACsec	TCP	25.21485	1476.612	57.37681	0.116586	0.104235	0.217516
MACsec	UDP 1m	1.576928	697.3203	51.95749	0.061595	0.104575	0.228031
MACsec	UDP 400m	24.93492	1478.306	59.6481	0.213472	1.407166	0.316122

IDEAALIVERKON TULOKSET

Liite 6

OpenVPN	Ping	0.276364	600	49.23941	0.241576	0	0.206606
OpenVPN	SCP	19.62477	1232.156	53.37324	0.508609	24.70421	0.181237
OpenVPN	TCP	23.99111	1476.532	57.11052	0.243466	0.024526	0.272513
OpenVPN	UDP 1m	2.467908	698.1046	52.94009	0.059895	0.888889	0.200529
OpenVPN	UDP 400m	36.99375	1478.161	63.13618	0.665856	1.699687	0.238895
WireGuard	Ping	0.106151	600.8781	48.04229	0.006196	0.702472	0.11972
WireGuard	SCP	15.88829	993.9524	51.19985	0.643371	38.8381	0.484217
WireGuard	TCP	38.80954	1476.667	60.5096	0.899948	0.235294	0.55397
WireGuard	UDP 1m	1.900392	620.2614	53.4064	0.13498	6.143791	0.756919
WireGuard	UDP 400m	58.85996	1479.596	68.17436	8.974992	0.213834	2.210867

Palvelimen CPU:

Toteutus	Testi	Keskiarvo			Hajonta		
		Käyttö / %	Taajuus / MHz	Lämpö / °C	Käyttö / %	Taajuus / MHz	Lämpö / °C
Ei salausta	Ping	0.547304	600	46.40921	0.544581	0	0.178738
Ei salausta	SCP	14.00695	1010.351	48.66621	2.483888	51.7193	0.154815
Ei salausta	TCP	34.83829	1483.454	56.79246	5.141536	1.414064	0.548774
Ei salausta	UDP 1m	0.775869	601.377	49.25539	0.066859	1.652459	0.149964
Ei salausta	UDP 400m	16.5842	1480.156	57.77159	2.983576	1.111411	0.241892
IPsec AES128GCM8	Ping	0.280882	604.2379	48.97139	0.230071	4.488467	0.199848
IPsec AES128GCM8	SCP	23.44437	1336.779	51.71349	0.44783	12.24348	0.290465
IPsec AES128GCM8	TCP	25.48689	1483.475	55.28269	0.152656	1.416393	0.232866
IPsec AES128GCM8	UDP 1m	0.915148	695.0164	50.14572	0.028275	2.990164	0.27834
IPsec AES128GCM8	UDP 400m	26.42282	1484.656	56.99182	0.076433	0.944262	0.265311
IPsec AES256GCM8	Ping	0.127965	603.8851	48.64382	0.039021	5.610131	0.27872
IPsec AES256GCM8	SCP	23.29628	1359.036	51.94209	0.840281	23.1403	0.28022
IPsec AES256GCM8	TCP	25.4958	1482.885	55.22904	0.067069	0.944262	0.285111

IDEAALIVERKON TULOKSET

Liite 6

IPsec AES256GCM8	UDP 1m	0.708787	697.9672	50.14508	0.067462	0.104918	0.320111
IPsec AES256GCM8	UDP 400m	26.23351	1483.751	57.01587	0.0784	1.793635	0.311321
IPsec ChaCha20Poly1305	Ping	0.873324	603.0303	48.7069	0.613829	4.848485	0.292693
IPsec ChaCha20Poly1305	SCP	17.02421	1209.719	51.09481	0.854845	37.77483	0.318054
IPsec ChaCha20Poly1305	TCP	32.67089	1482.295	56.828	2.853036	0	0.708561
IPsec ChaCha20Poly1305	UDP 1m	0.765443	694.623	51.04468	0.057652	1.993443	0.348468
IPsec ChaCha20Poly1305	UDP 400m	31.89456	1483.672	59.39681	1.469272	1.259016	0.755569
MACsec	Ping	0.126888	600.6061	47.98004	0.024396	0.969697	0.227108
MACsec	SCP	14.95419	1321.075	52.09621	1.108133	19.32139	0.228249
MACsec	TCP	26.54767	1483.475	55.36892	0.121862	1.416393	0.192628
MACsec	UDP 1m	0.805508	695.082	50.68541	0.083462	1.57377	0.216899
MACsec	UDP 400m	25.84367	1484.066	57.93804	1.84501	1.416393	0.233249
OpenVPN	Ping	0.1375	605	48.83058	0.033125	3.625	0.359163
OpenVPN	SCP	25.93269	1283.676	52.45649	0.909125	25.3215	0.305878
OpenVPN	TCP	27.9314	1482.548	56.78014	0.705373	2.169284	0.235388
OpenVPN	UDP 1m	2.259541	697.7705	51.22	0.0624	0.209836	0.256753
OpenVPN	UDP 400m	28.83479	1480.513	59.90092	0.564568	1.975356	0.264986
WireGuard	Ping	0.424202	602.6866	47.15447	0.366618	4.298507	0.133162
WireGuard	SCP	23.76856	1038.665	50.17344	2.494039	42.04334	0.330537
WireGuard	TCP	61.24443	1483.63	62.20718	1.313824	1.25384	0.275313
WireGuard	UDP 1m	1.688455	603.8689	51.22938	0.139744	4.118033	0.404736
WireGuard	UDP 400m	45.64759	1482.332	64.30182	4.696414	1.182642	1.094667

VIIVE-HÄIRIÖN TULOKSET

Liite 7

Nimi	Viive / ms	Ping - min	Avg	Max	Mdev	Yksikkö	TCP - kaista	Yksikkö	SCP - kesto / s
Ei salausta	0	0.196	0.234	0.268	0.009	ms	807	Mbits/sec	12.80032
IPsec AES128GCM8	0	0.443	0.484	0.532	0.027	ms	77.7	Mbits/sec	31.04675
IPsec AES256GCM8	0	0.437	0.496	0.578	0.029	ms	71.1	Mbits/sec	33.3981
IPsec ChaCha20Poly1305	0	0.384	0.435	0.488	0.019	ms	324	Mbits/sec	13.33205
MACsec	0	0.347	0.424	0.463	0.035	ms	76.5	Mbits/sec	33.10953
OpenVPN	0	0.846	0.997	1.092	0.05	ms	83.2	Mbits/sec	29.77228
WireGuard	0	0.651	1.699	2.889	1.032	ms	445	Mbits/sec	12.10253
Ei salausta	10	20.242	20.269	20.338	0.114	ms	843	Mbits/sec	12.89014
IPsec AES128GCM8	10	20.492	20.514	20.584	0.123	ms	67.3	Mbits/sec	34.64952
IPsec AES256GCM8	10	20.479	20.515	20.568	0.095	ms	59.1	Mbits/sec	32.75042
IPsec ChaCha20Poly1305	10	20.415	20.441	20.498	0.169	ms	253	Mbits/sec	14.75558
MACsec	10	20.374	20.439	20.485	0.151	ms	72.1	Mbits/sec	39.03403
OpenVPN	10	20.867	21.033	21.181	0.149	ms	58.1	Mbits/sec	51.69922
WireGuard	10	20.709	20.77	21.142	0.167	ms	472	Mbits/sec	13.56893
Ei salausta	20	40.249	40.262	40.286	0.216	ms	505	Mbits/sec	11.20737
IPsec AES128GCM8	20	40.448	40.508	40.565	0.184	ms	67.8	Mbits/sec	30.10334
IPsec AES256GCM8	20	40.502	40.528	40.591	0.156	ms	59.8	Mbits/sec	32.5185
IPsec ChaCha20Poly1305	20	40.431	40.453	40.493	0.194	ms	249	Mbits/sec	18.53352
MACsec	20	40.387	40.441	40.518	0.042	ms	72	Mbits/sec	39.55596
OpenVPN	20	40.847	41.04	41.219	0.249	ms	35.2	Mbits/sec	99.64752
WireGuard	20	40.686	40.749	40.816	0.197	ms	307	Mbits/sec	14.25447
Ei salausta	30	60.253	60.278	60.31	0.269	ms	344	Mbits/sec	14.13934
IPsec AES128GCM8	30	60.482	60.504	60.564	0.19	ms	73.2	Mbits/sec	35.63882
IPsec AES256GCM8	30	60.483	60.535	60.572	0.333	ms	63.9	Mbits/sec	35.24961
IPsec ChaCha20Poly1305	30	60.414	60.45	60.497	0.277	ms	249	Mbits/sec	19.67768
MACsec	30	60.372	60.443	60.492	0.266	ms	71.5	Mbits/sec	41.88328
OpenVPN	30	60.932	61.087	61.217	0.313	ms	33	Mbits/sec	125.774
WireGuard	30	60.691	60.787	62.78	0.332	ms	202	Mbits/sec	17.13424

VIIVE-HÄIRIÖN TULOKSET

Liite 7

Ei salausta	40	80.241	80.26	80.283	0.327	ms	259	Mbits/sec	17.64848
IPsec AES128GCM8	40	80.478	80.502	80.565	0.37	ms	77.5	Mbits/sec	33.06473
IPsec AES256GCM8	40	80.495	80.522	80.564	0.323	ms	70	Mbits/sec	38.02898
IPsec ChaCha20Poly1305	40	80.421	80.442	80.468	0.116	ms	139	Mbits/sec	18.1024
MACsec	40	80.382	80.444	80.517	0.165	ms	71.3	Mbits/sec	38.11532
OpenVPN	40	80.925	81.081	81.231	0.293	ms	25.8	Mbits/sec	149.6447
WireGuard	40	80.691	80.765	81.41	0.297	ms	145	Mbits/sec	20.23639
Ei salausta	50	100.244	100.266	100.347	0.142	ms	207	Mbits/sec	17.40358
IPsec AES128GCM8	50	100.482	100.507	100.573	0.327	ms	77.9	Mbits/sec	31.18505
IPsec AES256GCM8	50	100.498	100.52	100.577	0.347	ms	71.1	Mbits/sec	34.24271
IPsec ChaCha20Poly1305	50	100.42	100.444	100.501	0.3	ms	116	Mbits/sec	27.89833
MACsec	50	100.376	100.444	100.487	0.405	ms	72	Mbits/sec	39.6542
OpenVPN	50	100.928	101.087	101.424	0.193	ms	20.4	Mbits/sec	164.075
WireGuard	50	100.676	100.747	100.824	0.415	ms	115	Mbits/sec	23.99361
Ei salausta	60	120.247	120.264	120.322	0.11	ms	173	Mbits/sec	19.23153
IPsec AES128GCM8	60	120.492	120.521	120.573	0.219	ms	77.4	Mbits/sec	34.41691
IPsec AES256GCM8	60	120.443	120.517	120.572	0.066	ms	70.8	Mbits/sec	35.15752
IPsec ChaCha20Poly1305	60	120.416	120.456	120.528	0.311	ms	102	Mbits/sec	24.63945
MACsec	60	120.355	120.44	120.52	0.396	ms	71.6	Mbits/sec	41.79271
OpenVPN	60	120.922	121.089	121.21	0.419	ms	19.4	Mbits/sec	234.3558
WireGuard	60	120.71	120.759	120.847	0.444	ms	99.2	Mbits/sec	30.25503
Ei salausta	70	140.247	140.272	140.295	0.226	ms	148	Mbits/sec	22.09354
IPsec AES128GCM8	70	140.478	140.504	140.542	0.512	ms	75.5	Mbits/sec	37.35678
IPsec AES256GCM8	70	140.491	140.517	140.581	0.216	ms	70.9	Mbits/sec	37.90017
IPsec ChaCha20Poly1305	70	140.434	140.459	140.503	0.097	ms	97.2	Mbits/sec	37.99022
MACsec	70	140.374	140.428	140.501	0.416	ms	70.5	Mbits/sec	38.89793
OpenVPN	70	140.91	141.052	141.173	0.396	ms	17.6	Mbits/sec	208.1038
WireGuard	70	140.67	140.755	140.845	0.37	ms	83.5	Mbits/sec	33.49251
Ei salausta	80	160.23	160.259	160.295	0.551	ms	130	Mbits/sec	25.24569

VIIVE-HÄIRIÖN TULOKSET

Liite 7

IPsec AES128GCM8	80	160.485	160.513	160.571	0.552	ms	70.5	Mbits/sec	39.9334
IPsec AES256GCM8	80	160.489	160.518	160.572	0.207	ms	68.4	Mbits/sec	41.83352
IPsec ChaCha20Poly1305	80	160.392	160.442	160.503	0.127	ms	84	Mbits/sec	32.62654
MACsec	80	160.393	160.439	160.52	0.491	ms	70.9	Mbits/sec	39.81529
OpenVPN	80	160.932	161.057	161.195	0.287	ms	21.8	Mbits/sec	285.6703
WireGuard	80	160.703	160.755	160.844	0.195	ms	72.5	Mbits/sec	45.23293
Ei salausta	90	180.244	180.263	180.286	0.337	ms	115	Mbits/sec	28.37024
IPsec AES128GCM8	90	180.474	180.506	180.552	0.537	ms	66.6	Mbits/sec	42.48732
IPsec AES256GCM8	90	180.456	180.511	180.568	0.269	ms	62.9	Mbits/sec	47.44805
IPsec ChaCha20Poly1305	90	180.442	180.462	180.514	0.403	ms	78.6	Mbits/sec	36.23677
MACsec	90	180.392	180.446	180.507	0.425	ms	55.7	Mbits/sec	39.95478
OpenVPN	90	180.982	181.05	181.14	0.433	ms	22	Mbits/sec	284.4871
WireGuard	90	180.683	180.761	181.042	0.238	ms	65.7	Mbits/sec	43.63562
Ei salausta	100	200.258	200.271	200.315	0.611	ms	104	Mbits/sec	31.31141
IPsec AES128GCM8	100	200.476	200.499	200.568	0.409	ms	58.1	Mbits/sec	47.1476
IPsec AES256GCM8	100	200.498	200.517	200.57	0.392	ms	56.4	Mbits/sec	53.43648
IPsec ChaCha20Poly1305	100	200.428	200.453	200.503	0.316	ms	70.6	Mbits/sec	45.97422
MACsec	100	200.381	200.436	200.517	0.366	ms	65.8	Mbits/sec	40.45668
OpenVPN	100	200.949	201.06	201.302	0.592	ms	18.4	Mbits/sec	255.2724
WireGuard	100	200.7	200.754	200.827	0.498	ms	52.3	Mbits/sec	54.62276

Nimi	Viive / ms	UDP 1M - kaista	Yksikkö	Jitter / ms	Pudote- tut	Lähetet- tyt	UDP 400M - kaista	Yksikkö	Jitter / ms	Pudote- tut	Lähetetyt
Ei salausta	0	1	Mbits/sec	0.002	0	146485	400	Mbits/sec	0.001	906	11538462
IPsec AES128GCM8	0	1000	Kbits/sec	0.01	0	146485	76.1	Mbits/sec	0.552	10173	2207127
IPsec AES256GCM8	0	1000	Kbits/sec	0.008	0	146485	70	Mbits/sec	0.598	7314	2025514

VIIVE-HÄIRIÖN TULOKSET

Liite 7

IPsec	0	1000	Kbits/sec	0.001	0	146485	255	Mbits/sec	0.024	441251	7796151
ChaCha20Poly1305											
MACsec	0	1000	Kbits/sec	0.002	0	146485	53.7	Mbits/sec	0.002	453517	2002846
OpenVPN	0	1000	Kbits/sec	0.006	0	146485	123	Mbits/sec	13.224	7998014	11538462
WireGuard	0	1000	Kbits/sec	0.035	0	146485	266	Mbits/sec	0.074	131401	7803297
Ei salausta	10	1000	Kbits/sec	0.001	0	146485	400	Mbits/sec	0.007	14381	11538461
IPsec AES128GCM8	10	1000	Kbits/sec	0.01	0	146485	75.1	Mbits/sec	0.252	4496576	6665333
IPsec AES256GCM8	10	1	Mbits/sec	0.002	0	146485	68.5	Mbits/sec	4.764	4301100	6279259
IPsec	10	1000	Kbits/sec	0.002	0	146485	252	Mbits/sec	0.025	687005	7947548
ChaCha20Poly1305											
MACsec	10	1000	Kbits/sec	0.002	0	146485	66.3	Mbits/sec	0.004	417	1911691
OpenVPN	10	1	Mbits/sec	0.008	0	146485	117	Mbits/sec	12.774	8146858	11538462
WireGuard	10	1000	Kbits/sec	0.01	0	146485	255	Mbits/sec	15.656	4187999	11538463
Ei salausta	20	1	Mbits/sec	0.004	0	146485	400	Mbits/sec	0.014	8922	11538463
IPsec AES128GCM8	20	1	Mbits/sec	0.002	0	146485	74.2	Mbits/sec	0.259	4724675	6865036
IPsec AES256GCM8	20	1	Mbits/sec	0.002	0	146485	67	Mbits/sec	5.389	4599772	6534759
IPsec	20	1	Mbits/sec	0.003	0	146485	255	Mbits/sec	0.031	655797	8014376
ChaCha20Poly1305											
MACsec	20	1000	Kbits/sec	0.003	0	146485	66.1	Mbits/sec	0.003	12178	1918919
OpenVPN	20	1	Mbits/sec	0.004	0	146485	117	Mbits/sec	13.059	8163860	11538461
WireGuard	20	1	Mbits/sec	0.012	0	146485	191	Mbits/sec	15.666	6020643	11538463
Ei salausta	30	1	Mbits/sec	0.003	0	146485	345	Mbits/sec	0.009	1585353	11538460
IPsec AES128GCM8	30	1000	Kbits/sec	0.005	0	146485	75.3	Mbits/sec	6.917	4483868	6657093
IPsec AES256GCM8	30	1	Mbits/sec	0.004	0	146485	69.5	Mbits/sec	6.042	4009855	6016704
IPsec	30	1	Mbits/sec	0.003	0	146485	268	Mbits/sec	0.026	388489	8108260
ChaCha20Poly1305											
MACsec	30	1000	Kbits/sec	0.003	0	146485	66.4	Mbits/sec	0.002	0	1914325
OpenVPN	30	1	Mbits/sec	0.004	0	146485	117	Mbits/sec	0.087	8167897	11538462
WireGuard	30	1000	Kbits/sec	0.017	0	146485	263	Mbits/sec	0.022	3956820	11538462
Ei salausta	40	1	Mbits/sec	0.002	0	146485	258	Mbits/sec	0.008	4085435	11538460

VIIVE-HÄIRIÖN TULOKSET

Liite 7

IPsec AES128GCM8	40	1000	Kbits/sec	0.004	0	146485	-	-	-	-	-
IPsec AES256GCM8	40	1	Mbits/sec	0.004	0	146485	69.7	Mbits/sec	0.29	3998235	6010840
IPsec	40	1000	Kbits/sec	0.004	0	146485	236	Mbits/sec	0.06	1558763	8355171
ChaCha20Poly1305											
MACsec	40	1000	Kbits/sec	0.003	0	146485	50.3	Mbits/sec	15.654	582646	2034476
OpenVPN	40	1000	Kbits/sec	0.007	0	146485	116	Mbits/sec	12.739	8181553	11538463
WireGuard	40	1	Mbits/sec	0.017	0	146485	258	Mbits/sec	15.665	4084512	11538463
Ei salausta	50	1000	Kbits/sec	0.003	0	146485	208	Mbits/sec	0.013	5549992	11538462
IPsec AES128GCM8	50	1000	Kbits/sec	0.003	0	146485	75.7	Mbits/sec	8.32	4487678	6673194
IPsec AES256GCM8	50	1	Mbits/sec	0.003	0	146485	70	Mbits/sec	7.297	3940924	5961709
IPsec	50	1	Mbits/sec	0.005	0	146485	149	Mbits/sec	0.015	4536778	8847182
ChaCha20Poly1305											
MACsec	50	1000	Kbits/sec	0.003	0	146485	66.4	Mbits/sec	0.003	0	1914187
OpenVPN	50	1	Mbits/sec	0.009	0	146485	117	Mbits/sec	12.797	8155131	11538462
WireGuard	50	1000	Kbits/sec	0.012	0	146485	187	Mbits/sec	0.013	6134739	11538461
Ei salausta	60	1	Mbits/sec	0.004	0	146485	172	Mbits/sec	0.008	6589248	11538463
IPsec AES128GCM8	60	1	Mbits/sec	0.009	0	146485	76.3	Mbits/sec	8.824	4494464	6696233
IPsec AES256GCM8	60	1000	Kbits/sec	0.003	0	146485	69.8	Mbits/sec	7.902	3885260	5900780
IPsec	60	1000	Kbits/sec	0.002	0	146485	159	Mbits/sec	0.009	4086277	8667032
ChaCha20Poly1305											
MACsec	60	1	Mbits/sec	0.003	0	146485	42.8	Mbits/sec	0.001	795872	2031165
OpenVPN	60	1	Mbits/sec	0.003	0	146485	117	Mbits/sec	13.058	8166929	11538463
WireGuard	60	1	Mbits/sec	0.017	0	146485	171	Mbits/sec	0.027	6600677	11538462
Ei salausta	70	1	Mbits/sec	0.005	0	146485	147	Mbits/sec	0.008	7294187	11538462
IPsec AES128GCM8	70	1000	Kbits/sec	0.003	0	146485	74.9	Mbits/sec	0.252	4478207	6639385
IPsec AES256GCM8	70	1	Mbits/sec	0.007	0	146485	-	-	-	-	-
IPsec	70	1	Mbits/sec	0.003	0	146485	95.2	Mbits/sec	15.66	7056471	9804993
ChaCha20Poly1305											
MACsec	70	1000	Kbits/sec	0.003	0	146485	45	Mbits/sec	15.655	731737	2032041
OpenVPN	70	1000	Kbits/sec	0.007	0	146485	117	Mbits/sec	13.075	8157532	11538462

VIIVE-HÄIRIÖN TULOKSET

Liite 7

WireGuard	70	1000	Kbits/sec	0.012	0	146485	147	Mbits/sec	0.024	7289161	11538461
Ei salausta	80	1000	Kbits/sec	0.006	0	146485	127	Mbits/sec	0.013	7867044	11538462
IPsec AES128GCM8	80	1000	Kbits/sec	0.003	0	146485	75.7	Mbits/sec	0.306	4443292	6626566
IPsec AES256GCM8	80	1	Mbits/sec	0.001	0	146485	69.6	Mbits/sec	0.238	4029587	6038210
IPsec	80	1000	Kbits/sec	0.004	0	146485	94.1	Mbits/sec	0.013	7435787	10150614
ChaCha20Poly1305											
MACsec	80	1000	Kbits/sec	0.003	0	146485	43.3	Mbits/sec	0.003	779018	2027514
OpenVPN	80	1	Mbits/sec	0.008	0	146485	117	Mbits/sec	13.077	8162321	11538462
WireGuard	80	1000	Kbits/sec	0.012	0	146485	128	Mbits/sec	15.676	7832538	11538463
Ei salausta	90	1	Mbits/sec	0.002	0	146485	112	Mbits/sec	15.659	8302574	11538464
IPsec AES128GCM8	90	1	Mbits/sec	0.005	0	146485	75.1	Mbits/sec	10.68	4460706	6627986
IPsec AES256GCM8	90	1	Mbits/sec	0.003	0	146485	63.8	Mbits/sec	9.716	6144314	7987194
IPsec	90	1000	Kbits/sec	0.009	0	146485	86.7	Mbits/sec	15.653	7794257	10297926
ChaCha20Poly1305											
MACsec	90	1	Mbits/sec	0.002	0	146485	51	Mbits/sec	0.002	560597	2031163
OpenVPN	90	1	Mbits/sec	0.008	0	146485	114	Mbits/sec	12.782	8233468	11538463
WireGuard	90	1	Mbits/sec	0.024	0	146485	110	Mbits/sec	15.672	8365395	11538463
Ei salausta	100	1	Mbits/sec	0.01	0	146485	99.3	Mbits/sec	0.011	8674402	11538459
IPsec AES128GCM8	100	1	Mbits/sec	0.01	0	146485	75.4	Mbits/sec	27.573	3343722	4959568
IPsec AES256GCM8	100	1	Mbits/sec	0.002	0	146485	69.5	Mbits/sec	10.401	4036511	6042646
IPsec	100	1	Mbits/sec	0.004	0	146485	87.4	Mbits/sec	15.689	7971776	10495591
ChaCha20Poly1305											
MACsec	100	1000	Kbits/sec	0.003	0	146485	42.6	Mbits/sec	0.005	799265	2029148
OpenVPN	100	1	Mbits/sec	0.011	0	146485	103	Mbits/sec	13.157	8555371	11538463
WireGuard	100	1000	Kbits/sec	0.012	0	146485	99.3	Mbits/sec	15.687	8673042	11538462

PAKETINPUDOTUS-HÄIRIÖN TULOKSET

Liite 8

Nimi	Pudotus %	Ping - min	Avg	Max	Mdev	Yksikkö	TCP - kaista	Yksikkö	SCP - kesto / s
Ei salausta	0	0.192	0.234	0.265	0.02	ms	858	Mbits/sec	13.34832
IPsec AES128GCM8	0	0.443	0.485	0.538	0.032	ms	78	Mbits/sec	30.82562
IPsec AES256GCM8	0	0.441	0.49	0.541	0.035	ms	71.7	Mbits/sec	34.56503
IPsec ChaCha20Poly1305	0	0.375	0.421	0.483	0.028	ms	320	Mbits/sec	14.15129
MACsec	0	0.329	0.402	0.46	0.036	ms	76.4	Mbits/sec	35.46036
OpenVPN	0	0.893	1.065	1.175	0.062	ms	83.2	Mbits/sec	24.70323
WireGuard	0	0.643	0.685	0.737	0.044	ms	686	Mbits/sec	12.9019
Ei salausta	0.5	0.195	0.235	0.28	0.018	ms	769	Mbits/sec	13.42172
IPsec AES128GCM8	0.5	0.457	0.502	0.551	0.02	ms	63.7	Mbits/sec	35.23041
IPsec AES256GCM8	0.5	0.454	0.493	0.545	0.033	ms	60.2	Mbits/sec	40.2548
IPsec ChaCha20Poly1305	0.5	0.371	0.417	0.464	0.021	ms	219	Mbits/sec	14.37171
MACsec	0.5	0.337	0.416	0.459	0.033	ms	66.6	Mbits/sec	39.28276
OpenVPN	0.5	0.829	1.013	1.136	0.053	ms	80.6	Mbits/sec	31.94671
WireGuard	0.5	0.615	0.71	0.872	0.04	ms	316	Mbits/sec	14.80269
Ei salausta	1	0.226	0.25	0.274	0.022	ms	838	Mbits/sec	9.995329
IPsec AES128GCM8	1	0.428	0.484	0.539	0.031	ms	58.7	Mbits/sec	44.24907
IPsec AES256GCM8	1	0.44	0.491	0.551	0.027	ms	50.4	Mbits/sec	44.61229
IPsec ChaCha20Poly1305	1	0.383	0.43	0.477	0.029	ms	193	Mbits/sec	19.3135
MACsec	1	0.326	0.424	0.464	0.025	ms	61.2	Mbits/sec	39.50481
OpenVPN	1	0.915	1.02	1.155	0.044	ms	79.4	Mbits/sec	27.50989
WireGuard	1	0.603	1.196	2.745	0.864	ms	252	Mbits/sec	18.69175
Ei salausta	1.5	0.203	0.243	0.275	0.013	ms	735	Mbits/sec	12.30103
IPsec AES128GCM8	1.5	0.436	0.486	0.539	0.035	ms	51.9	Mbits/sec	43.61862
IPsec AES256GCM8	1.5	0.452	0.504	0.532	0.018	ms	49.2	Mbits/sec	58.28178
IPsec ChaCha20Poly1305	1.5	0.366	0.421	0.491	0.025	ms	174	Mbits/sec	27.71176
MACsec	1.5	0.346	0.433	0.482	0.028	ms	57.6	Mbits/sec	46.27438
OpenVPN	1.5	0.86	1.013	1.094	0.056	ms	76.7	Mbits/sec	33.1317
WireGuard	1.5	0.666	0.725	0.857	0.034	ms	200	Mbits/sec	20.8184

PAKETINPUDOTUS-HÄIRIÖN TULOKSET

Liite 8

Ei salausta	2	0.201	0.25	0.321	0.021	ms	749	Mbits/sec	12.5654
IPsec AES128GCM8	2	0.439	0.497	0.525	0.017	ms	50	Mbits/sec	64.20328
IPsec AES256GCM8	2	0.457	0.515	0.561	0.02	ms	39.6	Mbits/sec	66.92474
IPsec ChaCha20Poly1305	2	0.378	0.421	0.468	0.017	ms	153	Mbits/sec	27.40248
MACsec	2	0.347	0.436	0.488	0.032	ms	46.6	Mbits/sec	46.67543
OpenVPN	2	0.838	1.005	1.155	0.062	ms	71.3	Mbits/sec	38.24006
WireGuard	2	0.655	0.716	0.94	0.049	ms	164	Mbits/sec	31.72286
Ei salausta	2.5	0.2	0.241	0.268	0.023	ms	362	Mbits/sec	16.93124
IPsec AES128GCM8	2.5	0.439	0.481	0.553	0.034	ms	40.3	Mbits/sec	68.55086
IPsec AES256GCM8	2.5	0.444	0.492	0.543	0.021	ms	37.4	Mbits/sec	74.99574
IPsec ChaCha20Poly1305	2.5	0.37	0.424	0.492	0.025	ms	99.5	Mbits/sec	27.49687
MACsec	2.5	0.339	0.426	0.462	0.027	ms	44.6	Mbits/sec	63.46513
OpenVPN	2.5	0.841	1.009	1.155	0.062	ms	62.3	Mbits/sec	42.94564
WireGuard	2.5	0.66	0.72	0.798	0.037	ms	128	Mbits/sec	40.27526
Ei salausta	3	0.204	0.234	0.282	0.013	ms	184	Mbits/sec	13.79863
IPsec AES128GCM8	3	0.453	0.494	0.553	0.028	ms	36.3	Mbits/sec	75.20523
IPsec AES256GCM8	3	0.458	0.503	0.553	0.031	ms	29.1	Mbits/sec	87.03132
IPsec ChaCha20Poly1305	3	0.394	0.426	0.472	0.025	ms	79.4	Mbits/sec	45.28515
MACsec	3	0.345	0.421	0.463	0.032	ms	38	Mbits/sec	70.72906
OpenVPN	3	0.876	1.031	1.149	0.062	ms	55.9	Mbits/sec	47.53634
WireGuard	3	0.624	0.719	0.796	0.034	ms	96.3	Mbits/sec	47.73608
Ei salausta	3.5	0.208	0.255	0.283	0.024	ms	132	Mbits/sec	15.46221
IPsec AES128GCM8	3.5	0.455	0.499	0.543	0.021	ms	31	Mbits/sec	92.97054
IPsec AES256GCM8	3.5	0.442	0.49	0.564	0.029	ms	28	Mbits/sec	103.1422
IPsec ChaCha20Poly1305	3.5	0.37	0.421	0.464	0.025	ms	44.8	Mbits/sec	55.9365
MACsec	3.5	0.344	0.421	0.464	0.027	ms	36.4	Mbits/sec	69.37639
OpenVPN	3.5	0.853	1.014	1.133	0.054	ms	47.5	Mbits/sec	54.63126
WireGuard	3.5	0.65	0.788	2.761	0.38	ms	77.7	Mbits/sec	55.39578
Ei salausta	4	0.185	0.232	0.274	0.021	ms	128	Mbits/sec	20.16113

PAKETINPUDOTUS-HÄIRIÖN TULOKSET

Liite 8

IPsec AES128GCM8	4	0.44	0.489	0.552	0.033	ms	23.7	Mbits/sec	127.6448
IPsec AES256GCM8	4	0.434	0.496	0.551	0.033	ms	25.4	Mbits/sec	125.4434
IPsec ChaCha20Poly1305	4	0.412	0.454	0.491	0.016	ms	38.1	Mbits/sec	75.36623
MACsec	4	0.335	0.415	0.462	0.031	ms	32.5	Mbits/sec	107.4662
OpenVPN	4	0.828	1.008	1.108	0.043	ms	38	Mbits/sec	60.57152
WireGuard	4	0.637	0.913	2.816	0.591	ms	49.7	Mbits/sec	70.97549
Ei salausta	4.5	0.197	0.235	0.282	0.019	ms	127	Mbits/sec	29.63221
IPsec AES128GCM8	4.5	0.436	0.488	0.534	0.019	ms	19	Mbits/sec	144.3456
IPsec AES256GCM8	4.5	0.449	0.5	0.536	0.031	ms	19.1	Mbits/sec	148.356
IPsec ChaCha20Poly1305	4.5	0.386	0.433	0.48	0.026	ms	28	Mbits/sec	95.35153
MACsec	4.5	0.341	0.427	0.484	0.033	ms	21.3	Mbits/sec	134.3734
OpenVPN	4.5	0.831	0.989	1.137	0.059	ms	31.7	Mbits/sec	87.13409
WireGuard	4.5	0.65	1.312	2.77	0.891	ms	37.1	Mbits/sec	82.0422
Ei salausta	5	0.197	0.243	0.276	0.014	ms	97.3	Mbits/sec	30.66401
IPsec AES128GCM8	5	0.451	0.495	0.547	0.025	ms	16	Mbits/sec	178.0303
IPsec AES256GCM8	5	0.47	0.518	0.553	0.021	ms	16.5	Mbits/sec	184.3734
IPsec ChaCha20Poly1305	5	0.367	0.42	0.471	0.024	ms	24.5	Mbits/sec	112.9757
MACsec	5	0.348	0.422	0.454	0.033	ms	19.2	Mbits/sec	149.0186
OpenVPN	5	0.837	1.002	1.109	0.056	ms	22.8	Mbits/sec	96.98525
WireGuard	5	0.609	0.716	0.812	0.053	ms	29.5	Mbits/sec	108.2741

Nimi	Pudotus %	UDP 1M - kaista	Yksikkö	Jitter / ms	Pudote- tut	Lähetet- tyt	UDP 400M - kaista	Yksikkö	Jitter / ms	Pudote- tut	Lähetetyt
Ei salausta	0	1	Mbits/sec	0.004	0	146485	400	Mbits/sec	0.001	69	11538462
IPsec AES128GCM8	0	1	Mbits/sec	0.003	0	146485	76.6	Mbits/sec	0.234	12482	2221825
IPsec AES256GCM8	0	1	Mbits/sec	0.001	0	146485	70.6	Mbits/sec	0.599	4327	2041812

PAKETINPUDOTUS-HÄIRIÖN TULOKSET

Liite 8

IPsec	0	1	Mbits/sec	0.004	0	146485	266	Mbits/sec	0.024	145559	7827479
ChaCha20Poly1305											
MACsec	0	1	Mbits/sec	0.002	0	146485	74.6	Mbits/sec	0.052	184	2151658
OpenVPN	0	1	Mbits/sec	0.005	0	146485	125	Mbits/sec	13.273	7934521	11538462
WireGuard	0	1000	Kbits/sec	0.014	0	146485	163	Mbits/sec	0.016	6842217	11538462
Ei salausta	0.5	995	Kbits/sec	62.507	665	146485	398	Mbits/sec	0.001	57698	11538462
IPsec AES128GCM8	0.5	995	Kbits/sec	0.006	782	146485	76.8	Mbits/sec	0.184	20443	2237290
IPsec AES256GCM8	0.5	995	Kbits/sec	0.002	720	146485	70.5	Mbits/sec	0.188	15678	2049725
IPsec	0.5	995	Kbits/sec	0.002	740	146485	269	Mbits/sec	0.024	462640	8225056
ChaCha20Poly1305											
MACsec	0.5	995	Kbits/sec	0.002	743	146485	74.2	Mbits/sec	0.043	11075	2150958
OpenVPN	0.5	995	Kbits/sec	0.004	770	146485	122	Mbits/sec	12.971	8029059	11538463
WireGuard	0.5	995	Kbits/sec	0.173	742	146485	131	Mbits/sec	15.661	7754752	11538463
Ei salausta	1	990	Kbits/sec	0.001	1458	146485	396	Mbits/sec	0.001	115950	11538462
IPsec AES128GCM8	1	990	Kbits/sec	0.004	1461	146485	76.5	Mbits/sec	0.496	34867	2242968
IPsec AES256GCM8	1	990	Kbits/sec	0.002	1453	146485	70.6	Mbits/sec	0.577	21643	2059298
IPsec	1	990	Kbits/sec	0.002	1497	146485	262	Mbits/sec	0.028	486786	8034736
ChaCha20Poly1305											
MACsec	1	990	Kbits/sec	0.002	1444	146485	73.8	Mbits/sec	0.003	22480	2150273
OpenVPN	1	991	Kbits/sec	0.006	1342	146485	125	Mbits/sec	13.263	7940352	11538462
WireGuard	1	990	Kbits/sec	0.012	1400	146485	144	Mbits/sec	0.016	7373623	11538462
Ei salausta	1.5	985	Kbits/sec	0.002	2219	146485	394	Mbits/sec	0.002	177352	11538462
IPsec AES128GCM8	1.5	985	Kbits/sec	0.002	2181	146485	76.8	Mbits/sec	0.539	42876	2258754
IPsec AES256GCM8	1.5	985	Kbits/sec	0.001	2222	146485	70.5	Mbits/sec	0.267	33235	2068105
IPsec	1.5	985	Kbits/sec	0.002	2176	146485	279	Mbits/sec	0.051	348339	8391521
ChaCha20Poly1305											
MACsec	1.5	985	Kbits/sec	0.002	2141	146485	70.6	Mbits/sec	0.004	72000	2108018
OpenVPN	1.5	985	Kbits/sec	0.005	2143	146485	114	Mbits/sec	12.986	8244229	11538464
WireGuard	1.5	985	Kbits/sec	0.013	2203	146485	266	Mbits/sec	0.034	194985	7857257
Ei salausta	2	980	Kbits/sec	0.003	2873	146485	392	Mbits/sec	0.001	233506	11538462

PAKETINPUDOTUS-HÄIRIÖN TULOKSET

Liite 8

IPsec AES128GCM8	2	981	Kbits/sec	0.002	2809	146485	76.4	Mbits/sec	0.55	57839	2262164
IPsec AES256GCM8	2	980	Kbits/sec	0.002	2920	146485	70.7	Mbits/sec	0.312	43653	2083590
IPsec	2	979	Kbits/sec	0.002	3052	146485	244	Mbits/sec	0.019	772142	7818297
ChaCha20Poly1305											
MACsec	2	979	Kbits/sec	0.003	3058	146485	66.6	Mbits/sec	0.001	93170	2015654
OpenVPN	2	980	Kbits/sec	0.005	2873	146485	124	Mbits/sec	0.075	7957010	11538461
WireGuard	2	980	Kbits/sec	0.01	2931	146485	145	Mbits/sec	15.665	7352445	11538463
Ei salausta	2.5	975	Kbits/sec	0.002	3612	146485	390	Mbits/sec	0.003	293060	11538461
IPsec AES128GCM8	2.5	976	Kbits/sec	0.003	3588	146485	76.3	Mbits/sec	0.542	71742	2274098
IPsec AES256GCM8	2.5	975	Kbits/sec	0.004	3605	146485	70.7	Mbits/sec	0.2	53723	2094964
IPsec	2.5	975	Kbits/sec	0.002	3644	146485	290	Mbits/sec	0.068	433918	8796726
ChaCha20Poly1305											
MACsec	2.5	974	Kbits/sec	0.001	3743	146485	72.5	Mbits/sec	0.016	54545	2146022
OpenVPN	2.5	975	Kbits/sec	0.005	3725	146485	121	Mbits/sec	13.246	8057531	11538463
WireGuard	2.5	976	Kbits/sec	0.009	3545	146485	126	Mbits/sec	0.01	7893697	11538462
Ei salausta	3	971	Kbits/sec	0.001	4264	146485	388	Mbits/sec	0.001	346005	11538461
IPsec AES128GCM8	3	970	Kbits/sec	0.007	4367	146485	76.6	Mbits/sec	0.528	81679	2292021
IPsec AES256GCM8	3	970	Kbits/sec	0.005	4394	146485	70.4	Mbits/sec	0.582	68149	2100068
IPsec	3	970	Kbits/sec	0.006	4412	146485	290	Mbits/sec	0.012	626516	9004350
ChaCha20Poly1305											
MACsec	3	970	Kbits/sec	0.002	4446	146485	72.1	Mbits/sec	0.018	64329	2145037
OpenVPN	3	970	Kbits/sec	0.004	4366	146485	111	Mbits/sec	0.091	8334083	11538462
WireGuard	3	970	Kbits/sec	0.013	4374	146485	142	Mbits/sec	15.654	7431341	11538463
Ei salausta	3.5	966	Kbits/sec	0.002	5045	146485	385	Mbits/sec	0.001	407039	11538461
IPsec AES128GCM8	3.5	966	Kbits/sec	0.003	5047	146485	76.8	Mbits/sec	0.537	86163	2303143
IPsec AES256GCM8	3.5	965	Kbits/sec	0.006	5051	146485	70.8	Mbits/sec	0.583	75449	2117786
IPsec	3.5	966	Kbits/sec	0.005	5017	146485	254	Mbits/sec	0.016	676505	8006449
ChaCha20Poly1305											
MACsec	3.5	965	Kbits/sec	0.002	5060	146485	71.9	Mbits/sec	0.007	75528	2148982
OpenVPN	3.5	965	Kbits/sec	0.007	5168	146485	111	Mbits/sec	13.006	8320553	11538462

PAKETINPUDOTUS-HÄIRIÖN TULOKSET

Liite 8

WireGuard	3.5	965	Kbits/sec	0.02	5195	146485	260	Mbits/sec	0.083	493164	8003440
Ei salausta	4	960	Kbits/sec	0.003	5859	146485	384	Mbits/sec	15.647	462631	11538462
IPsec AES128GCM8	4	960	Kbits/sec	0.008	5803	146485	76.7	Mbits/sec	13.194	98582	2313439
IPsec AES256GCM8	4	960	Kbits/sec	15.656	5792	146486	70.7	Mbits/sec	0.166	85869	2124504
IPsec	4	960	Kbits/sec	0.002	5861	146485	256	Mbits/sec	0.019	557042	7948568
ChaCha20Poly1305											
MACsec	4	961	Kbits/sec	0.002	5778	146485	67	Mbits/sec	0.001	81160	2014674
OpenVPN	4	960	Kbits/sec	0.006	5916	146485	120	Mbits/sec	13.256	8074635	11538463
WireGuard	4	959	Kbits/sec	0.013	5940	146485	176	Mbits/sec	0.01	6472115	11536771
Ei salausta	4.5	955	Kbits/sec	0.002	6553	146485	382	Mbits/sec	0.004	521425	11538462
IPsec AES128GCM8	4.5	956	Kbits/sec	0.001	6485	146485	76.8	Mbits/sec	0.538	112482	2327590
IPsec AES256GCM8	4.5	955	Kbits/sec	0.002	6582	146485	70.6	Mbits/sec	62.33	99310	2136507
IPsec	4.5	955	Kbits/sec	0.004	6595	146485	239	Mbits/sec	15.692	991082	7898844
ChaCha20Poly1305											
MACsec	4.5	859	Kbits/sec	0.002	5869	133008	-	-	-	-	-
OpenVPN	4.5	955	Kbits/sec	0.008	6617	146485	120	Mbits/sec	13.004	8074954	11538463
WireGuard	4.5	955	Kbits/sec	0.013	6617	146485	130	Mbits/sec	15.663	7794492	11538463
Ei salausta	5	951	Kbits/sec	0.002	7177	146485	380	Mbits/sec	0.001	578584	11538462
IPsec AES128GCM8	5	950	Kbits/sec	0.002	7310	146485	77	Mbits/sec	0.542	123024	2343967
IPsec AES256GCM8	5	950	Kbits/sec	0.011	7323	146485	70.6	Mbits/sec	0.585	109816	2147042
IPsec	5	950	Kbits/sec	0.004	7390	146485	242	Mbits/sec	15.655	1023107	8020256
ChaCha20Poly1305											
MACsec	5	948	Kbits/sec	15.652	7439	146486	66.4	Mbits/sec	0.001	100710	2016675
OpenVPN	5	950	Kbits/sec	0.008	7347	146485	120	Mbits/sec	0.088	8069441	11538462
WireGuard	5	950	Kbits/sec	0.011	7274	146485	156	Mbits/sec	0.025	7023910	11538461

UDP 400M -testin uudelleen ajo WireGuardilla:

Name	Pudotus %	UDP 400M - kaista	Yksikkö	Jitter / ms	Pudotetut	Lähetetyt
WireGuard 1	175		Mbits/sec	0.021	6495203	11538461
WireGuard 1.1	137		Mbits/sec	0.019	7587513	11538462
WireGuard 1.2	168		Mbits/sec	15.668	6693529	11538462
WireGuard 1.3	261		Mbits/sec	0.044	276117	7813290
WireGuard 1.4	152		Mbits/sec	15.667	7158886	11538463
WireGuard 1.5	140		Mbits/sec	0.024	7512590	11538461
WireGuard 1.6	160		Mbits/sec	15.668	6931508	11538463
WireGuard 1.7	263		Mbits/sec	0.042	361895	7944140
WireGuard 1.8	155		Mbits/sec	0.018	7069978	11538461
WireGuard 1.9	133		Mbits/sec	0.02	7704947	11538462
WireGuard 2	179		Mbits/sec	15.665	6356822	11538463

JITTER-HÄIRIÖN TULOKSET

Liite 9

Jitter mittauksissa viive 20 ms.

Nimi	Jitter / ms	Ping - min	Avg	Max	Mdev	Yksikkö	TCP - kaista	Yksikkö	SCP - kesto / s
Ei salausta	0	40.232	40.255	40.278	0.137	ms	485	Mbits/sec	13.89767933
IPsec AES128GCM8	0	40.474	40.507	40.597	0.177	ms	77.9	Mbits/sec	32.49139643
IPsec AES256GCM8	0	40.505	40.524	40.571	0.201	ms	58.7	Mbits/sec	35.5465548
IPsec ChaCha20Poly1305	0	40.413	40.448	40.505	0.267	ms	248	Mbits/sec	18.65735054
MACsec	0	40.369	40.432	40.468	0.249	ms	72.1	Mbits/sec	40.26135278
OpenVPN	0	40.882	41.057	41.206	0.169	ms	30.9	Mbits/sec	96.26778269
WireGuard	0	40.666	40.771	42.71	0.373	ms	303	Mbits/sec	13.93210268
Ei salausta	1	36.433	40.29	42.781	1.48	ms	451	Mbits/sec	12.5392065
IPsec AES128GCM8	1	37.891	40.865	44.81	1.222	ms	46.9	Mbits/sec	60.96329379
IPsec AES256GCM8	1	35.037	40.496	43.926	1.606	ms	46.8	Mbits/sec	58.17630458
IPsec ChaCha20Poly1305	1	37.046	40.315	45	1.485	ms	36.1	Mbits/sec	69.03008914
MACsec	1	36.604	40.636	44.323	1.698	ms	54.7	Mbits/sec	36.5817709
OpenVPN	1	37.608	40.913	44.336	1.502	ms	3.94	Mbits/sec	132.7995
WireGuard	1	35.965	40.952	45.009	1.484	ms	224	Mbits/sec	14.63974571
Ei salausta	2	32.588	39.892	44.743	2.789	ms	448	Mbits/sec	14.00227833
IPsec AES128GCM8	2	36.043	40.585	46.293	2.603	ms	21.6	Mbits/sec	102.2792628
IPsec AES256GCM8	2	31.449	39.796	44.105	2.466	ms	21.4	Mbits/sec	100.801331
IPsec ChaCha20Poly1305	2	33.533	39.972	46.116	3.164	ms	21	Mbits/sec	107.2901344
MACsec	2	33.6	39.913	45.922	3.175	ms	58.6	Mbits/sec	39.72135019
OpenVPN	2	34.883	41.304	48.202	2.739	ms	40	Mbits/sec	65.03244829
WireGuard	2	31.979	40.753	47.102	2.855	ms	216	Mbits/sec	14.79025936
Ei salausta	3	29.704	39.284	45.868	3.466	ms	447	Mbits/sec	13.72728801
IPsec AES128GCM8	3	31.416	40.2	50.835	4.405	ms	16.1	Mbits/sec	137.5934818
IPsec AES256GCM8	3	30.687	40.531	49.03	4.436	ms	16	Mbits/sec	141.9373789
IPsec ChaCha20Poly1305	3	31.339	40.335	51.061	4.088	ms	15.4	Mbits/sec	142.5520687
MACsec	3	29.188	40.18	49.814	4.565	ms	68.7	Mbits/sec	40.08783388

JITTER-HÄIRIÖN TULOKSET

Liite 9

OpenVPN	3	29.918	41.497	55.497	4.179	ms	27.2	Mbits/sec	83.44369102
WireGuard	3	30.744	40.477	48.643	4.133	ms	216	Mbits/sec	18.2150805
Ei salausta	4	18.749	40.015	49.937	5.625	ms	443	Mbits/sec	18.301368
IPsec AES128GCM8	4	29.842	40.561	51.822	6.121	ms	12.7	Mbits/sec	175.1894879
IPsec AES256GCM8	4	27.645	40.464	55.978	5.449	ms	12.8	Mbits/sec	172.7254224
IPsec ChaCha20Poly1305	4	29.964	39.898	50.86	4.922	ms	12.4	Mbits/sec	175.2198665
MACsec	4	22.761	39.269	54.48	7.225	ms	62.8	Mbits/sec	43.30706191
OpenVPN	4	28.832	41.373	54.137	4.42	ms	4.82	Mbits/sec	133.7329202
WireGuard	4	31.317	40.447	54.339	5.31	ms	140	Mbits/sec	30.73604774
Ei salausta	5	20.225	40.308	63.566	7.542	ms	424	Mbits/sec	22.49133134
IPsec AES128GCM8	5	24.092	38.504	53.928	6.924	ms	10.4	Mbits/sec	204.7457538
IPsec AES256GCM8	5	28.548	41.93	56.972	6.364	ms	10.5	Mbits/sec	199.7765992
IPsec ChaCha20Poly1305	5	18.713	39.693	57.215	7.011	ms	10.5	Mbits/sec	208.6854045
MACsec	5	26.2	40.185	64.363	7.165	ms	54.2	Mbits/sec	43.46559215
OpenVPN	5	28.332	41.317	56.045	6.65	ms	17.5	Mbits/sec	126.5363078
WireGuard	5	25.57	40.967	59.291	8.323	ms	147	Mbits/sec	32.56511354
Ei salausta	6	22.692	41.201	61.189	8.757	ms	402	Mbits/sec	13.48622155
IPsec AES128GCM8	6	27.655	41.369	61.271	7.587	ms	9.07	Mbits/sec	233.5345895
IPsec AES256GCM8	6	22.533	39.629	57.398	7.848	ms	9.39	Mbits/sec	234.1911948
IPsec ChaCha20Poly1305	6	23.724	41.695	64.225	9.359	ms	9.18	Mbits/sec	233.1280131
MACsec	6	21.617	40.675	61.062	8.547	ms	62	Mbits/sec	41.01175833
OpenVPN	6	21.49	40.228	54.548	7.95	ms	15.1	Mbits/sec	138.8394723
WireGuard	6	22.529	41.06	62.198	7.766	ms	153	Mbits/sec	21.91983318
Ei salausta	7	21.85	40.055	59.192	9.385	ms	83.3	Mbits/sec	13.90642047
IPsec AES128GCM8	7	17.832	41.315	68.534	11.178	ms	8.28	Mbits/sec	258.5716271
IPsec AES256GCM8	7	23.182	41.024	69.104	9.123	ms	8.4	Mbits/sec	258.6497507
IPsec ChaCha20Poly1305	7	18.984	40.15	60.02	10.557	ms	8.13	Mbits/sec	270.7462761
MACsec	7	15.583	41.515	65.169	10.62	ms	68.9	Mbits/sec	41.19140816
OpenVPN	7	13.695	41.219	61.6	10.048	ms	13.9	Mbits/sec	152.9998646

JITTER-HÄIRIÖN TULOKSET

Liite 9

WireGuard	7	18.075	42.879	69.3	9.882	ms	155	Mbits/sec	44.32385564
Ei salausta	8	8.28	41.751	62.655	11.478	ms	9.46	Mbits/sec	190.6279082
IPsec AES128GCM8	8	8.476	39.689	64.761	12.386	ms	7.33	Mbits/sec	292.5056813
IPsec AES256GCM8	8	21.736	42.524	81.089	11.51	ms	7.5	Mbits/sec	290.8091128
IPsec ChaCha20Poly1305	8	18.096	42.492	61.673	9.912	ms	7.11	Mbits/sec	307.900697
MACsec	8	12.533	43.725	69.811	12.532	ms	67.8	Mbits/sec	51.7852664
OpenVPN	8	14.363	42.882	66.728	12.543	ms	12.6	Mbits/sec	1059.900166
WireGuard	8	17.126	40.369	64.613	12.012	ms	94.4	Mbits/sec	53.4393611
Ei salausta	9	10.116	39.845	68.176	11.637	ms	3.69	Mbits/sec	538.8849468
IPsec AES128GCM8	9	12.556	41.79	76.211	12.902	ms	6.82	Mbits/sec	322.2637126
IPsec AES256GCM8	9	15.869	41.608	66.397	11.948	ms	6.69	Mbits/sec	310.0932076
IPsec ChaCha20Poly1305	9	13.588	40.979	64.188	11.354	ms	5.42	Mbits/sec	412.2947519
MACsec	9	8.889	40.088	66.187	12.464	ms	36.1	Mbits/sec	40.73276114
OpenVPN	9	9.483	41.843	64.95	12.301	ms	11.6	Mbits/sec	1114.612236
WireGuard	9	16.255	39.813	66.65	10.88	ms	22.2	Mbits/sec	118.2463238
Ei salausta	10	17.645	41.85	67.499	10.555	ms	2.83	Mbits/sec	726.5176606
IPsec AES128GCM8	10	14.798	40.795	69.612	13.141	ms	6.08	Mbits/sec	347.3760343
IPsec AES256GCM8	10	12.308	40.254	71.576	13.61	ms	6.09	Mbits/sec	347.3896358
IPsec ChaCha20Poly1305	10	10.234	41.937	71.083	14.094	ms	3.91	Mbits/sec	569.4810169
MACsec	10	6.031	43.15	72.529	14.64	ms	52.2	Mbits/sec	144.5805011
OpenVPN	10	14.88	44.8	79.072	13.705	ms	11	Mbits/sec	1137.421761
WireGuard	10	2.147	39.594	66.856	13.775	ms	15.4	Mbits/sec	178.4805763

Name	Jit- ter / ms	UDP 400M - kaista	Yksikkö	Jitter / ms	Pudote- tut	Lähetet- tyt	UDP 1M - kaista	Yksikkö	Jitter / ms	Pudote- tut	Lähetet- tyt
Ei salausta	0	400	Mbits/sec	0.006	6796	1E+07	1	Mbits/sec	0.006	0	146485
IPsec AES128GCM8	0	74.6	Mbits/sec	6.334	5E+06	7E+06	1000	Kbits/sec	0.005	0	146485

JITTER-HÄIRIÖN TULOKSET

Liite 9

IPsec AES256GCM8	0	70.3	Mbits/sec	0.275	4E+06	6E+06	1	Mbits/sec	0.007	0	146485
IPsec ChaCha20Poly1305	0	265	Mbits/sec	0.033	448715	8E+06	1	Mbits/sec	0.002	0	146485
MACsec	0	42.6	Mbits/sec	0.002	807223	2E+06	1	Mbits/sec	0.002	0	146485
OpenVPN	0	117	Mbits/sec	13.051	8E+06	1E+07	1	Mbits/sec	0.007	0	146485
WireGuard	0	258	Mbits/sec	0.017	4E+06	1E+07	1	Mbits/sec	0.01	0	146485
Ei salausta	1	400	Mbits/sec	1.437	12866	1E+07	1000	Kbits/sec	1.212	0	146485
IPsec AES128GCM8	1	72.1	Mbits/sec	0.66	5E+06	7E+06	1000	Kbits/sec	1.2	0	146485
IPsec AES256GCM8	1	67.4	Mbits/sec	0.735	4E+06	6E+06	1000	Kbits/sec	1.367	0	146485
IPsec ChaCha20Poly1305	1	95.3	Mbits/sec	0.517	6E+06	8E+06	1000	Kbits/sec	1.226	0	146485
MACsec	1	71.2	Mbits/sec	1.008	3443	2E+06	1	Mbits/sec	1.036	0	146485
OpenVPN	1	-	-	-	-	-	-	-	-	-	-
WireGuard	1	230	Mbits/sec	1.01	5E+06	1E+07	1	Mbits/sec	1.379	0	146485
Ei salausta	2	400	Mbits/sec	1.083	6753	1E+07	1000	Kbits/sec	2.888	0	146485
IPsec AES128GCM8	2	41.3	Mbits/sec	0.74	4E+06	5E+06	1000	Kbits/sec	2.318	1	146485
IPsec AES256GCM8	2	43.4	Mbits/sec	0.634	4E+06	5E+06	1000	Kbits/sec	2.085	0	146485
IPsec ChaCha20Poly1305	2	31.8	Mbits/sec	1.017	7E+06	8E+06	1	Mbits/sec	2.57	0	146485
MACsec	2	71	Mbits/sec	1.901	13723	2E+06	1	Mbits/sec	1.874	0	146485
OpenVPN	2	-	-	-	-	-	1	Mbits/sec	2.195	0	146485
WireGuard	2	221	Mbits/sec	1.428	5E+06	1E+07	1000	Kbits/sec	2.201	1	146485
Ei salausta	3	400	Mbits/sec	2.123	2987	1E+07	1	Mbits/sec	3.195	0	146485
IPsec AES128GCM8	3	21.7	Mbits/sec	1.166	5E+06	5E+06	1000	Kbits/sec	3.726	0	146485
IPsec AES256GCM8	3	22.7	Mbits/sec	0.92	4E+06	5E+06	1	Mbits/sec	3.99	0	146485
IPsec ChaCha20Poly1305	3	17.4	Mbits/sec	0.756	8E+06	8E+06	1	Mbits/sec	2.506	1	146485
MACsec	3	70.9	Mbits/sec	2.095	17117	2E+06	1000	Kbits/sec	3.885	0	146485
OpenVPN	3	-	-	-	-	-	1	Mbits/sec	3.584	0	146485
WireGuard	3	219	Mbits/sec	2.84	2E+06	8E+06	1000	Kbits/sec	3.533	0	146485
Ei salausta	4	400	Mbits/sec	2.336	4147	1E+07	1000	Kbits/sec	5.088	0	146485
IPsec AES128GCM8	4	14	Mbits/sec	1.536	5E+06	5E+06	1000	Kbits/sec	4.258	0	146485
IPsec AES256GCM8	4	14.7	Mbits/sec	0.954	4E+06	5E+06	1	Mbits/sec	4.557	4	146485

JITTER-HÄIRIÖN TULOKSET

Liite 9

IPsec ChaCha20Poly1305	4	11.6	Mbits/sec	0.665	8E+06	8E+06	1000	Kbits/sec	6.286	2	146485
MACsec	4	70.8	Mbits/sec	4.388	17547	2E+06	1000	Kbits/sec	4.436	0	146485
OpenVPN	4	-	-	-	-	-	-	-	-	-	-
WireGuard	4	230	Mbits/sec	2.623	5E+06	1E+07	1000	Kbits/sec	4.961	2	146485
Ei salausta	5	400	Mbits/sec	3.841	2031	1E+07	1	Mbits/sec	5.582	1	146485
IPsec AES128GCM8	5	10.1	Mbits/sec	1.536	5E+06	5E+06	1000	Kbits/sec	6.208	0	146485
IPsec AES256GCM8	5	10.5	Mbits/sec	0.912	5E+06	5E+06	1000	Kbits/sec	5.091	1	146485
IPsec ChaCha20Poly1305	5	8.59	Mbits/sec	0.754	8E+06	8E+06	1000	Kbits/sec	5.828	0	146485
MACsec	5	67.3	Mbits/sec	3.819	7592	2E+06	1000	Kbits/sec	5.474	0	146485
OpenVPN	5	-	-	-	-	-	1000	Kbits/sec	5.162	0	146485
WireGuard	5	221	Mbits/sec	2.952	5E+06	1E+07	1	Mbits/sec	5.554	3	146485
Ei salausta	6	400	Mbits/sec	2.658	2461	1E+07	1	Mbits/sec	6.754	0	146485
IPsec AES128GCM8	6	8.06	Mbits/sec	1.469	5E+06	5E+06	1	Mbits/sec	6.695	0	146485
IPsec AES256GCM8	6	8.31	Mbits/sec	1.314	5E+06	5E+06	1000	Kbits/sec	7.427	4	146485
IPsec ChaCha20Poly1305	6	7.06	Mbits/sec	1.014	8E+06	8E+06	1000	Kbits/sec	6.649	0	146485
MACsec	6	71.1	Mbits/sec	5.089	14504	2E+06	1	Mbits/sec	8.359	3	146485
OpenVPN	6	-	-	-	-	-	1000	Kbits/sec	6.184	2	146485
WireGuard	6	228	Mbits/sec	2.875	5E+06	1E+07	1	Mbits/sec	6.539	2	146485
Ei salausta	7	400	Mbits/sec	9.642	6615	1E+07	1000	Kbits/sec	10.263	0	146485
IPsec AES128GCM8	7	7.28	Mbits/sec	1.225	4E+06	5E+06	1	Mbits/sec	7.849	1	146485
IPsec AES256GCM8	7	7.14	Mbits/sec	1.188	5E+06	5E+06	1000	Kbits/sec	5.848	0	146485
IPsec ChaCha20Poly1305	7	6.59	Mbits/sec	1.455	7E+06	7E+06	1	Mbits/sec	4.662	1	146485
MACsec	7	67.1	Mbits/sec	5.102	8618	2E+06	1000	Kbits/sec	9.759	1	146485
OpenVPN	7	-	-	-	-	-	1000	Kbits/sec	7.642	0	146485
WireGuard	7	231	Mbits/sec	3.634	2E+06	8E+06	1000	Kbits/sec	9.379	4	146485
Ei salausta	8	400	Mbits/sec	4.406	1155	1E+07	1000	Kbits/sec	8.058	0	146485
IPsec AES128GCM8	8	6.93	Mbits/sec	1.633	5E+06	5E+06	1000	Kbits/sec	8.862	0	146485
IPsec AES256GCM8	8	6.98	Mbits/sec	1.496	5E+06	5E+06	1000	Kbits/sec	7.068	1	146485
IPsec ChaCha20Poly1305	8	7	Mbits/sec	1.154	8E+06	8E+06	1000	Kbits/sec	11.008	2	146485

JITTER-HÄIRIÖN TULOKSET

Liite 9

MACsec	8	70.7	Mbits/sec	7.367	17945	2E+06	1000	Kbits/sec	6.09	0	146485
OpenVPN	8	-	-	-	-	-	1000	Kbits/sec	7.845	0	146485
WireGuard	8	223	Mbits/sec	5.49	5E+06	1E+07	1	Mbits/sec	10.808	7	146485
Ei salausta	9	400	Mbits/sec	3.904	460	1E+07	1000	Kbits/sec	10.412	3	146485
IPsec AES128GCM8	9	7.8	Mbits/sec	1.135	5E+06	5E+06	1000	Kbits/sec	8.552	4	146485
IPsec AES256GCM8	9	7.7	Mbits/sec	1.485	5E+06	5E+06	1000	Kbits/sec	8.765	1	146485
IPsec ChaCha20Poly1305	9	8.75	Mbits/sec	1.066	8E+06	8E+06	1000	Kbits/sec	9.85	3	146485
MACsec	9	70.9	Mbits/sec	6.725	14211	2E+06	1	Mbits/sec	13.366	3	146485
OpenVPN	9	-	-	-	-	-	1000	Kbits/sec	9.998	3	146485
WireGuard	9	221	Mbits/sec	4.375	5E+06	1E+07	1000	Kbits/sec	8.253	0	146485
Ei salausta	10	400	Mbits/sec	4.175	4048	1E+07	1	Mbits/sec	9.887	0	146485
IPsec AES128GCM8	10	9.38	Mbits/sec	1.214	5E+06	5E+06	1000	Kbits/sec	13.513	0	146485
IPsec AES256GCM8	10	9.18	Mbits/sec	1.346	5E+06	5E+06	1000	Kbits/sec	8.308	0	146485
IPsec ChaCha20Poly1305	10	11.5	Mbits/sec	0.92	8E+06	8E+06	1000	Kbits/sec	9.808	3	146485
MACsec	10	67.2	Mbits/sec	7.898	10271	2E+06	1000	Kbits/sec	11.144	0	146485
OpenVPN	10	-	-	-	-	-	1	Mbits/sec	14.271	3	146485
WireGuard	10	220	Mbits/sec	3.746	5E+06	1E+07	1000	Kbits/sec	10.949	1	146485

VIIVEEN-, PAKETTIENPUDOTUS- JA JITTER-HÄIRIÖIDEN YHTEISTULOKSET

Liite 10

Nimi	Pudotus / %	Viive / ms	Jitter / ms	Ping - min	Avg	Max	Mdev	Yksikkö	TCP - kaista	Yksikkö	SCP - kesto / s
Ei salausta	0.5	40	5	70.119	80.919	94.157	5.287	ms	3.48	Mbits/sec	609.9089
IPsec AES128GCM8	0.5	40	5	70.276	82.944	98.472	6.49	ms	2.07	Mbits/sec	953.214
IPsec AES256GCM8	0.5	40	5	60.302	79.821	96.029	6.976	ms	2.32	Mbits/sec	941.7815
IPsec ChaCha20Poly1305	0.5	40	5	61.516	79.815	98.101	7.648	ms	2.31	Mbits/sec	967.6638
MACsec	0.5	40	5	59.889	80.108	97.256	7.462	ms	2.4	Mbits/sec	959.4993
OpenVPN	0.5	40	5	63.341	79.784	93.151	6.994	ms	2.13	Mbits/sec	1032.498
WireGuard	0.5	40	5	65.978	80.874	101.259	7.607	ms	2.32	Mbits/sec	960.5241
Ei salausta	1	80	10	137.56	159.367	199.154	11.663	ms	1.29	Mbits/sec	1749.076
IPsec AES128GCM8	1	80	10	119.098	162.508	195.509	14.232	ms	899	Kbits/sec	2610.856
IPsec AES256GCM8	1	80	10	116.402	160.142	188.827	15.535	ms	796	Kbits/sec	2561.101
IPsec ChaCha20Poly1305	1	80	10	128.957	161.288	198.64	14.018	ms	823	Kbits/sec	2602.758
MACsec	1	80	10	135.109	162.059	193.761	13.959	ms	818	Kbits/sec	2575.631
OpenVPN	1	80	10	120.079	158.249	190.53	13.428	ms	828	Kbits/sec	2660.625
WireGuard	1	80	10	126.026	159.265	183.686	11.933	ms	799	Kbits/sec	2705.191
Ei salausta	1.5	120	15	177.548	238.412	280.813	21.224	ms	745	Kbits/sec	2849.885
IPsec AES128GCM8	1.5	120	15	196.19	236.293	276.071	19.748	ms	480	Kbits/sec	4623.946
IPsec AES256GCM8	1.5	120	15	176.356	242.711	289.489	21.798	ms	456	Kbits/sec	4529.818
IPsec ChaCha20Poly1305	1.5	120	15	199.045	237.457	291.954	21.39	ms	480	Kbits/sec	4595.618
MACsec	1.5	120	15	200.253	243.527	297.561	20.187	ms	533	Kbits/sec	4524.501
OpenVPN	1.5	120	15	169.509	239.249	285.045	21.599	ms	540	Kbits/sec	4802.417
WireGuard	1.5	120	15	164.649	244.751	298.734	22.822	ms	533	Kbits/sec	4669.939

VIIVEEN-, PAKETTIENPUDOTUS- JA JITTER-HÄIRIÖIDEN YHTEISTULOKSET

Liite 10

Nimi	Pudotus / %	Viive / ms	Jitter / ms	UDP 1M kaista	Yksikkö	Jitter / ms	Pudotetut	Lähetetyt
Ei salausta	0.5	40	5	995	Kbits/sec	5.06	743	146485
IPsec AES128GCM8	0.5	40	5	995	Kbits/sec	6.193	754	146485
IPsec AES256GCM8	0.5	40	5	994	Kbits/sec	18.754	781	146486
IPsec ChaCha20Poly1305	0.5	40	5	995	Kbits/sec	5.755	702	146485
MACsec	0.5	40	5	995	Kbits/sec	6.591	745	146485
OpenVPN	0.5	40	5	995	Kbits/sec	8.157	676	146485
WireGuard	0.5	40	5	995	Kbits/sec	4.095	703	146485
Ei salausta	1	80	10	990	Kbits/sec	10.694	1445	146485
IPsec AES128GCM8	1	80	10	990	Kbits/sec	11.029	1449	146485
IPsec AES256GCM8	1	80	10	990	Kbits/sec	14.316	1429	146485
IPsec ChaCha20Poly1305	1	80	10	991	Kbits/sec	12.929	1401	146485
MACsec	1	80	10	990	Kbits/sec	14.419	1474	146485
OpenVPN	1	80	10	990	Kbits/sec	11.183	1448	146485
WireGuard	1	80	10	990	Kbits/sec	11.105	1486	146485
Ei salausta	1.5	120	15	985	Kbits/sec	16.715	2156	146485
IPsec AES128GCM8	1.5	120	15	982	Kbits/sec	14.858	2687	146485
IPsec AES256GCM8	1.5	120	15	982	Kbits/sec	16.907	2607	146485
IPsec ChaCha20Poly1305	1.5	120	15	981	Kbits/sec	21.735	2745	146485
MACsec	1.5	120	15	985	Kbits/sec	12.217	2162	146485
OpenVPN	1.5	120	15	984	Kbits/sec	17.682	2287	146485
WireGuard	1.5	120	15	985	Kbits/sec	16.462	2133	146485

VIIVEEN-, PAKETTIENPUDOTUS- JA JITTER-HÄIRIÖIDEN YHTEISTULOKSET

Liite 10

Nimi	Pudotus / %	Viive / ms	Jitter / ms	UDP 400M - kaista	Yksikkö	Jitter	Yksikkö	Pudotetut	Lähetetyt
Ei salausta	0.5	40	5	260	Mbits/sec	3.706	ms	4049825	11538461
IPsec AES128GCM8	0.5	40	5	10.3	Mbits/sec	0.998	ms	4893302	5189436
IPsec AES256GCM8	0.5	40	5	10.5	Mbits/sec	0.917	ms	4621041	4923958
IPsec ChaCha20Poly1305	0.5	40	5	8.41	Mbits/sec	1.448	ms	8317126	8559771
MACsec	0.5	40	5	70.4	Mbits/sec	3.13	ms	22655	2052862
OpenVPN	0.5	40	5	-	-	-	-	-	-
WireGuard	0.5	40	5	259	Mbits/sec	18.293	ms	4056998	11538463
Ei salausta	1	80	10	130	Mbits/sec	9.231	ms	7797967	11538462
IPsec AES128GCM8	1	80	10	3.85	Mbits/sec	2.158	ms	5352927	5464013
IPsec AES256GCM8	1	80	10	3.9	Mbits/sec	1.653	ms	4993103	5105737
IPsec ChaCha20Poly1305	1	80	10	3.23	Mbits/sec	2.286	ms	9811868	9904980
MACsec	1	80	10	70.1	Mbits/sec	5.349	ms	34522	2057136
OpenVPN	1	80	10	-	-	-	-	-	-
WireGuard	1	80	10	129	Mbits/sec	20.02	ms	7821314	11538463
Ei salausta	1.5	120	15	85.8	Mbits/sec	20.178	ms	9061904	11538462
IPsec AES128GCM8	1.5	120	15	2.21	Mbits/sec	2.572	ms	5815175	5878852
IPsec AES256GCM8	1.5	120	15	2.26	Mbits/sec	3.563	ms	5280028	5345287
IPsec ChaCha20Poly1305	1.5	120	15	1.99	Mbits/sec	4.07	ms	10343286	10400599
MACsec	1.5	120	15	65.9	Mbits/sec	11.03	ms	40511	1940816
OpenVPN	1.5	120	15	-	-	-	-	-	-
WireGuard	1.5	120	15	86.2	Mbits/sec	13.31	ms	9052859	11538462