LAPIN AMK
Lapland University of Applied Sciences

VPN-PROTOKOLLIEN VERTAILU

Suorituskyky site-to-site-konfiguraatiossa mobiiliyhteydellä

Räisänen Juha

Opinnäytetyö

Tieto- ja viestintätekniikka
Insinööri (AMK)

2024

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tieto- ja viestintätekniikka
Insinööri (AMK)

Tekijä	Juha Räisänen	**Vuosi**	2024
Ohjaaja	Ari Karjalainen		
Toimeksiantaja	Rajavartiolaitos		
Työn nimi	VPN-protokollien vertailu. Suorituskyky site-to-site-konfiguraatiossa mobiiliyhteydellä.		
Sivumäärä	47		

Tässä opinnäytetyössä luodaan katsaus VPN-teknologian historiaan ja käydään läpi erilaisia tunnelointiprotokollia ja niiden eroavaisuuksia. Varsinaisena tutkimuskysymyksenä oli selvittää kolmen suositun VPN-protokollan suorituskykyä välittää salattua IP-kameran kuvaa pienitehoisilla reititinlaitteillä mobiiliyhteyden yli. Työn tavoitteena oli saada esiin eroja protokollien suorituskyvyssä ja käytettävyydessä sekä selvittää protokollien käyttökelpoisuutta erilaisiin toimintaympäristöihin. Tutkittavina protokollina olivat IKEv2/IPsec, OpenVPN sekä WireGuard.

Opinnäytetyö suoritettiin toiminnallisena, ja työtä varten rakennettiin pienimuotoinen testiympäristö, joka koostui perinteisestä reitittimestä, 5G-mobiilireitittimestä, nopeusmittauspalvelimesta, IP-kamerasta sekä konfigurointiin ja mittaukseen käytettävästä tietokoneesta. Reitittimien välille luotiin tunnelit kaikilla tutkittavilla protokollilla, ja niiden läpi suoritettiin samat testit mittauspalvelinta sekä IP-kameraa hyödyntäen.

Työn edetessä korostui hyvän testaussuunnitelman laadinta sekä konfiguraatioiden toimivuuden järjestelmällinen testaaminen. Erilaisten haasteiden vuoksi VPN-tunneleiden konfiguraatiota jouduttiin tekemään uudestaan useampaan otteeseen, joten niiden kanssa työskentelyyn ja reitittimien konfigurointiin tuli samalla hyvää rutiinia.

Työn tuloksena saatiin selville, että protokollista erityisesti WireGuard suoriutuu hyvin salatun videokuvan välittämisestä pienemmissä verkkoympäristöissä. Alan standardina pitkään ollut IPsec on myös edelleen hyvin toimiva protokolla, jota voi käyttää myös yhdessä uudempien salausalgoritmien kanssa. Työn tulokset otetaan huomioon toimeksiantajan tulevissa kehitysprojekteissa.

Avainsanat matkaviestinverkot, reitittimet, salaus, tietoliikenne

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

Study Programme in Information
and Communication Technology
Bachelor of Engineering

Author	Juha Räisänen	**Year**	2024
Supervisor	Ari Karjalainen		
Commissioned by	The Finnish Border Guard		
Title	Comparison of VPN Protocols - Performance in Site-to-Site Configuration over a Mobile Connection		
Number of pages	47		

The aim of this thesis was to examine the history of VPN technology and to go through some common tunneling protocols and their differences. The goal of the study was to find out differences in the performance and the ease of use of the protocols and to assess the usability of the protocols in different operating environments.

The actual research question was to examine the performance of three popular VPN protocols in transmitting an encrypted IP camera image with low-power router devices over a mobile connection. The investigated protocols were IKEv2/IPsec, OpenVPN and WireGuard. The research method was functional and a small-scale test environment was built for the study. The environment consisted of a traditional router, a 5G mobile router, a speed measurement server, an IP camera and a laptop that was used for configuration and measurement. Tunnels were created between the routers with all examined protocols and they were tested with consistent routines using the measurement server and an IP camera. The study focused on creating and following a proper test plan and systematically testing the functionality of the configurations as the research progressed. Due to a few and various challenges, the VPN tunnels and routers had to be reconfigured several times. This led to getting more routine in configuring network devices and generally working with them.

As a result of the study it was found out that the WireGuard protocol performs particularly well in transmitting encrypted video in smaller network environments. IPsec, which has long been the de facto industry standard, still is a very well-functioning protocol that can also be made to work with more modern encryption algorithms. The results of this study will be considered in the client's future development projects

Keywords data communications, encryption, mobile communications networks, routers

SISÄLLYS

1 JOHDANTO 7

2 YLEISTÄ VPN-TEKNOLOGIASTA 8

2.1 Mikä on VPN-tunneli? 8
2.2 Historiaa 9
2.3 Erilaisia tunnelointiprotokollia 9
2.3.1 GRE 9
2.3.2 PPTP 10
2.3.3 L2TP 11
2.3.4 SSTP 11

3 TYÖSSÄ KÄYTETYT TEKNOLOGIAT 12

3.1 Virve 2 12
3.2 IKEv2/IPsec 12
3.2.1 Turvallisuusprotokollat 12
3.2.2 Turvallisuusassosiaatiot 14
3.2.3 Avaintenhallinta 14
3.2.4 Kryptografiset algoritmit 15
3.3 OpenVPN 16
3.4 WireGuard 18
3.5 VPN-protokollien ominaisuuksien vertailu 20

4 TESTAUSSUUNNITELMA 22

4.1 Testauksen pääperiaatteet 22
4.2 Tekninen testaus 22
4.3 Käyttötapaustesti 23

5 TESTIYMPÄRISTÖN RAKENTAMINEN 24

5.1 Testipalvelin 24
5.1.1 Iperf3 24
5.1.2 OpenSpeedTest 26
5.2 Reititin 27
5.3 Mobiilireititin 28
5.4 IKEv2/IPsec-konfiguraatio 28
5.5 OpenVPN-konfiguraatio 29

5.6 WireGuard-konfiguraatio 30
5.7 IP-kamera 32
5.8 Yhteenveto 33
6 TESTAUS 34
6.1 Tekninen testi 34
6.1.1 IKEv2/IPsec 34
6.1.2 OpenVPN 35
6.1.3 WireGuard 37
6.2 Käyttötapaustesti 38
6.2.1 IKEv2/IPsec 39
6.2.2 OpenVPN 39
6.2.3 WireGuard 40
6.3 Yhteenveto 41
7 POHDINTA 42
LÄHTEET 44

KÄYTETYT LYHENTEET

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Algorithm
AH	Authentication Header
CBC	Cipher Block Chaining
CNSA	Commercial National Security Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ESP	Encapsulating Security Payload
GCM	Galois/Counter Mode
GRE	Generic Routing Encapsulation
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPsec	Internet Protocol security
ISAKMP	Internet Security Association and Key Management Protocol
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
MPPE	Microsoft Point to Point Encryption
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
SSTP	Secure Socket Tunneling Protocol
SwIPe	Software IP Encryption Protocol
TLS	Transport Layer Security
VMS	Video Management System
VPN	Virtual Private Network

1 JOHDANTO

Verkkoyhteyksien tunneloinnin, virtuaalisten erillisverkkojen ja kaupallisen IP-tietoliikenteen salauksen historia alkaa 1990-luvun puolivälistä. Silloin Columbian yliopiston ja AT&T Bell Labsin tutkijat loivat SwIPe-protokollan, joka tunnetaan ensimmäisenä VPN-teknologian ilmentymänä. Sittemmin yleisesti käytetyimmäksi menetelmäksi turvallisten tietoliikenneyhteyksien muodostamiseen asemansa vahvisti IPsec, joka on IETF:n standardoima protokollapaketti IP-yhteyksien salaamiseen ja autentikointiin. IPsec-protokollaa käyttävien yhteyksien dynaamista muodostamista varten luotiin IKE-protokolla, jonka uusin versio IKEv2 näki päivänvalonsa vuonna 2014. Näillä menetelmillä luotua VPN-yhteyttä kutsutaankin yleisesti nimellä IKEv2/IPsec-tunneli. (Zahorski 2022.)

James Yonan loi 2000-luvun alussa ensimmäisen avoimen lähdekoodin VPN-protokollan, OpenVPN:n, josta on tullut yleisesti melko suosittu helppokäyttöisyytensä ja vapaan käytettävyytensä vuoksi (Palo Alto Networks 2024). 2010-luvun lopulla Jason A. Donenfeld julkaisi oman avoimen lähdekoodin VPN-protokollansa, WireGuardin, jonka tavoitteena oli olla kaikkia aiempia protokollia turvallisempi, nopeampi ja helppokäyttöisempi (Donenfeld 2020, 1). Yritysten ja suurten verkkolaitevalmistajien keskuudessa, varsinkin kahden eri verkkolaitteen välillä käytettävissä tapauksissa, IKEv2/IPsec on kuitenkin edelleen de facto -standardi salattujen tietoliikenneyhteyksien muodostamiseen (McClure 2021).

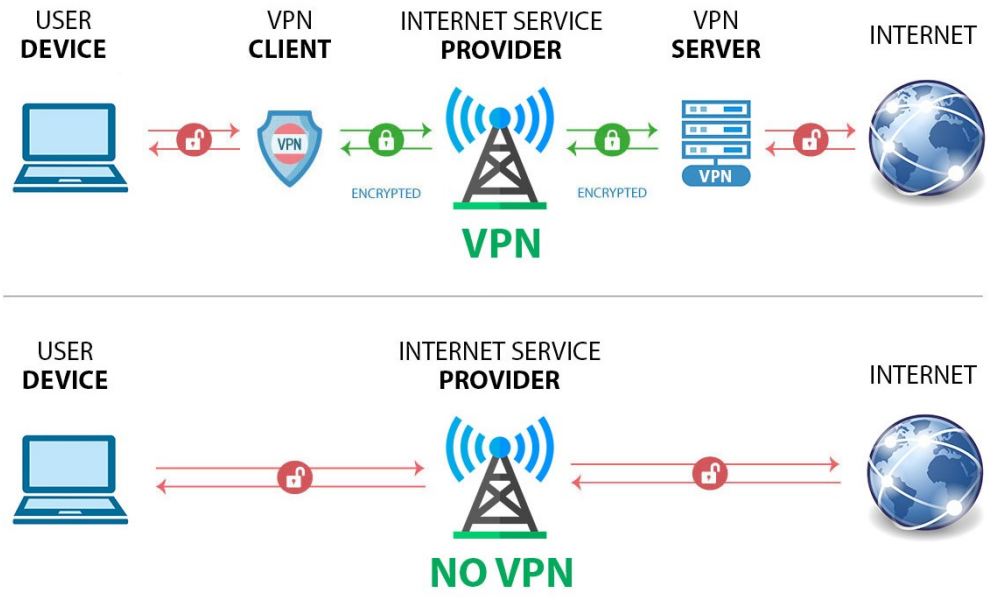
Tässä opinnäytetyössä käydään läpi VPN-teknologian historiaa ja esitellään nykyisin käytössä olevia protokollia. Opinnäytetyön pääasiallisena tavoitteena on vertailla työhön valittujen VPN-protokollien suorituskykyä pienimuotoisessa testiympäristössä. Teknisessä testissä mitataan tutkittavien VPN-protokollien absoluuttista suorituskykyä, ja käytännön testissä tutkitaan käyttäjälle välittyvää suorituskykyä käyttötapauksessa, jossa IP-kameran lähettämään kuvaa siirretään mobiiliyhteydellä kahden reitittimen välillä VPN-tunnelin läpi. Lopputuloksena pyritään saamaan käsitys siitä, minkä protokollan VPN-tunnelia käyttämällä saadaan mahdollisimman nopea salattu tietoliikenneyhteys muodostettua mobiilireitittimestä, jonka suorituskyky salaustoimenpiteisiin ei ole samaa tasoa järeiden konesalireitittimien kanssa.

2 YLEISTÄ VPN-TEKNOLOGIASTA

2.1 Mikä on VPN-tunneli?

Virtuaaliset yksityisverkot eli VPN:t ovat keino luoda salattuja ja autentikoituja tietoliikenneyhteyksiä ja jatkaa yksityisiä verkkoja julkisten verkkojen, kuten internetin yli. VPN-yhteyksille on olemassa erilaisia topologioita ja käyttötapauksia. Site-to-site-VPN-yhteyksillä voidaan esimerkiksi turvallisesti yhdistää yritysten eri toimipisteitä toisiinsa osaksi samaa lähiverkkoa. Remote access -tyyppisellä VPN-ratkaisulla sen sijaan yrityksen työntekijä voi esimerkiksi ottaa päätelaitteellaan yhteyden työnantajan palveluihin salattua yhteyttä käyttäen. Vaihtoehtoisesti yksityishenkilöt voivat VPN-yhteyksiä hyödyntäen salata omaa tietoliikennettään ja kiertää esimerkiksi maantieteellisiä käyttörajoituksia. Yksityishenkilöt käyttävät tähän yleensä jotain kaupallista VPN-palveluntarjoajaa, joita on nykyään markkinoilla erittäin paljon. (Gillis 2021.)

VPN-yhteyden muodostamista kutsutaan yleisesti myös tunneloinniksi. Tällä tarkoitetaan sitä, että verkkoliikenne pystyy siirtymään verkosta toiseen virtuaalista tunnelia pitkin. (Mendenhall 2022.) VPN-tunnelin toiminta havainnollistetaan kuviossa 1.



Kuvio 1. VPN-tunnelin havainnollistaminen (Mendenhall 2022)

2.2 Historiaa

Kun internetin tietoliikenteen määrä lisääntyi 1990-luvulla, alkoi esiin nousta myös huolia sen turvallisuudesta. Vuonna 1993 ensimmäisenä IP-tietoliikenteen salausprotokollana AT&T Bell Labsissa kehitettiin SwIPE, jolla pystyttiin suorittamaan IP-paketin salaus tietoliikenneyhteyden päästä päähän. Trusted Information Systemsin tutkija Xu Wei jatkoi tätä työtä, ja vuotta myöhemmin julkaisi ensimmäisen version IPsec-protokollasta. Vuonna 1995 IETF aloitti IPsec-työryhmän ja IPsecistä tuli IETF:n standardoima protokolla, jota ylläpidetään edelleen. Ensimmäisenä varsinaisena VPN-protokollana pidetään Microsoftin vuonna 1996 julkaisemaa PPTP-protokollaa. Tämän protokollan avulla voitiin luoda virtuaalisia yksityisverkkoja, mutta sen salausominaisuudet ovat nykymittapuulla varsin heikot. (Zahorski 2022.)

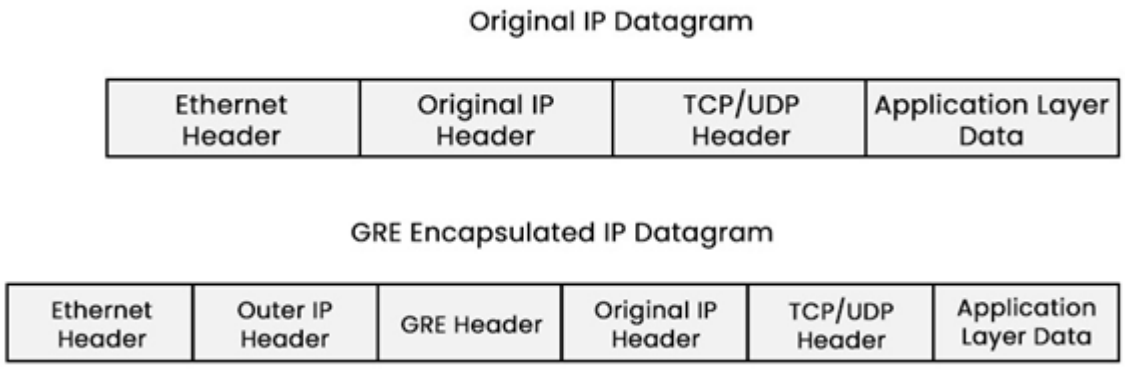
2.3 Erilaisia tunnelointiprotokollia

Tässä tutkimuksessa käsiteltävien protokollien lisäksi on olemassa useita muita edelleen yleisessä käytössä olevia tunnelointiprotokollia. Jotkin protokollista ovat avoimia, toiset suljettuja ja jotkut ovat jo nykymittapuun mukaan vanhentuneita, eikä niiden käyttöä suositella. Maailmalla on kuitenkin paljon tietoliikenneverkkoja, joissa käytetään edelleen myös hyvin vanhaa tekniikkaa, eli kaikki protokollat ovat varmasti edelleen käytössä jossain päin maailmaa, muodossa tai toisessa. Seuraavaksi esitellään näistä yleisimmät, jotka ovat GRE, PPTP, L2TP ja SSTP. (Traefik Labs 2024.)

2.3.1 GRE

GRE on Ciscon kehittämä tunnelointiprotokolla, joka on määritelty RFC-dokumenteissa 2784 ja 2890. GRE toimii yhdessä useimpien verkkoprotokollien kanssa, ja sitä usein käytetäänkin paketoimaan ei tuettua verkkoliikennettä sellaiseen muotoon, jota verkko tukee. GRE:llä voidaan myös esimerkiksi välittää IPv6-liikennettä IPv4-verkon läpi paketoimalla se välillä IPv4-paketiksi. GRE-tunneleita käytetäänkin yleisesti silloin, kun halutaan helpottaa verkkoliikenteen kulkua erilaisten verkkoliikennekäytäntöjen ohi. GRE:ssä ei itsessään ole salausominaisuuksia, joten sitä käytetäänkin usein yhdessä IPsec-protokollan kanssa,

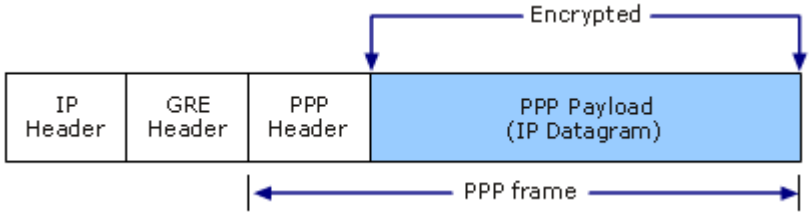
jolloin tunneli saadaan myös salattua. GRE ei ole avoin protokolla, joten kaikki, etenkin kuluttajille suunnatut verkkolaitteet, eivät välttämättä tue GRE-protokollaa. (PyNetLabs 2024.) GRE-kapseloitu IP-paketti on esitettynä kuviossa 2.



Kuvio 2. GRE-kapseloitu IP-paketti (PyNetLabs 2024)

2.3.2 PPTP

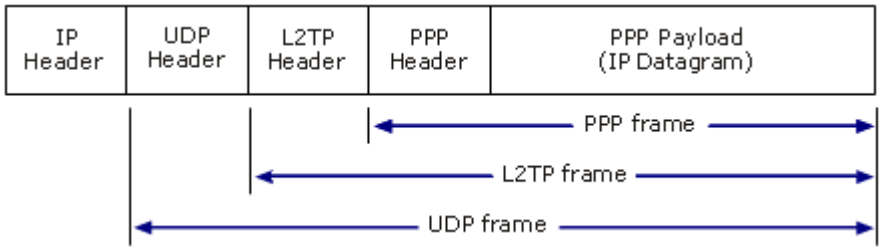
PPTP:tä pidetään vanhimpana varsinaisena VPN-protokollana, ja se onkin kehitetty jo 1990-luvulla Microsoftin johtaman konsortion toimesta. PPTP on määritelty RFC 2637:ssä. Protokolla tehtiin parantamaan vanhempaa PPP-protokollaa ja on määritelty RFC 1661:ssä. PPTP käyttää GRE paketointia tunnelin muodostamiseen, ja MPPE standardin mukaista tietoliikenteen salausta. PPTP:tä pidetään nopeana ja helppokäyttöisenä, mutta se ei nykymittapuulla ole enää tietoturvallinen, eikä sen käyttöä suositella. (Mash 2022a.) PPTP kapseloitu IP-paketti on esitettynä kuviossa 3.



Kuvio 3. PPTP-kapseloitu IP-paketti (Microsoft 2012)

2.3.3 L2TP

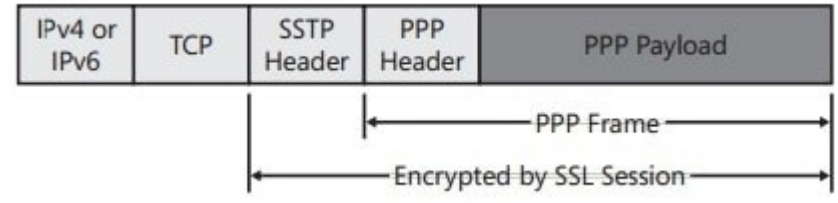
L2TP on tunnelointiprotokolla, jolla voidaan L2-kytkinverkkoja yhdistää IP-verkon yli. L2TP-protokollassa yhdistettiin parhaat ominaisuudet L2F- ja PPTP-protokollista, ja se on määritelty alun perin dokumentissa RFC 2661. L2TP ei itsessään sisällä salausta, ja sitä käytetäänkin usein yhdessä IPsec-protokollan kanssa tietoturvan parantamiseksi. L2TP/IPsec onkin yleisesti käytetty tunnelointiprotokolla edelleen. (Mash 2022b.) L2TP-kapseloitu IP-paketti on esitettynä kuviossa 4.



Kuvio 4. L2TP-kapseloitu IP-paketti (Microsoft 2012)

2.3.4 SSTP

SSTP on Microsoftin kehittämä tunnelointiprotokolla erityisesti Windowsin etäkäyttöyhteyksiä varten. Protokollaa ei voikaan käyttää varsinaisesti site-to-site-yhteyksien luomiseen. SSTP-protokollassa hyödynnetään PPP- tai L2TP-kapseloitua pakettia, joka kapseloidaan uudestaan SSTP-paketiksi. SSTP käyttää SSL/TLS-salausta, jonka turvallisuus koetaan tänäkin päivänä vielä hyväksi. SSTP käyttää yhteyden muodostamiseen TCP-porttia 443, joten liikenne sekoittuu muun HTTPS-liikenteen sekaan, joten sillä pääsee yleensä helpommin palomuurien läpi. SSTP on edelleen suosittu protokolla Windows-ympäristöissä. (Mash 2022c.) SSTP-kapseloitu IP-paketti on esitettynä kuviossa 5.



Kuvio 5. SSTP-kapseloitu IP-paketti (Davis 2023)

3 TYÖSSÄ KÄYTETYT TEKNOLOGIAT

3.1 Virve 2

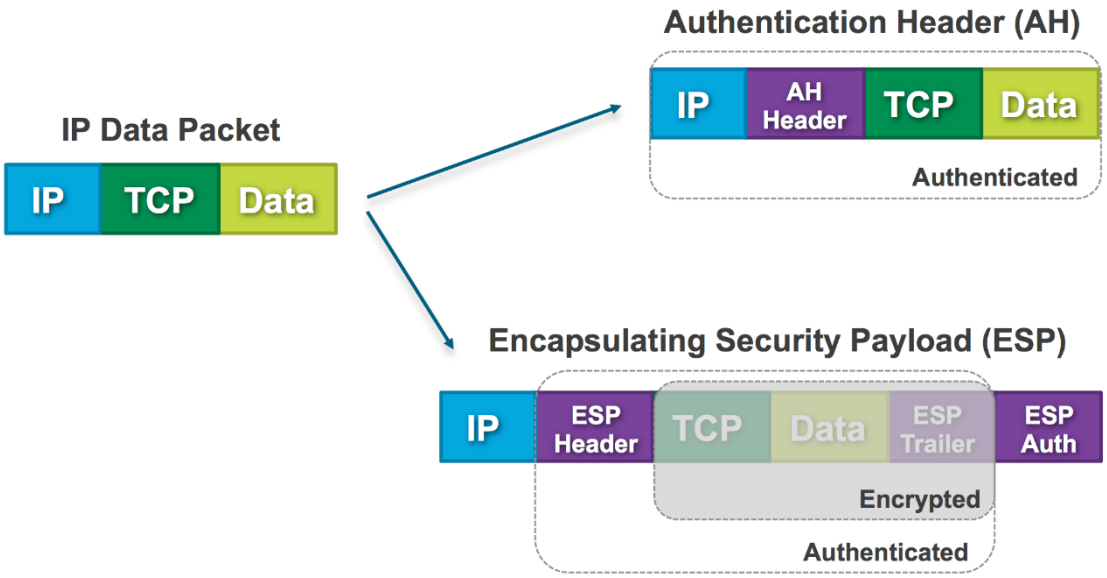
Virve 2 on laajakaistainen mobiiliverkkopalvelu, joka korvaa elinkaarensa päähän tulleen TETRA-teknologiaan pohjautuvan viranomaisverkko Virven. Uuden verkon on tarkoitus mahdollistaa käyttäjilleen nykyaikaiset ja turvalliset viestintä- ja tiedonsiirtopalvelut, kun langattomasti siirrettävän datan määrän tarve kasvaa viranomaiskentässä. Virve 2 -palvelu hyödyntää Elisan 4G- ja 5G-radioverkkoa sekä Erillisverkkojen operoimaa ja Ericssonin toimittamaa 5G Core-runkoverkkoa. (Suomen Erillisverkot Oy 2024.) Tässä tutkimuksessa on tavoitteena käyttää tiedonsiirtoyhteytenä Virve 2 Data -mobiililiittymää.

3.2 IKEv2/IPsec

IPsec on IETF:n standardoima joukko menetelmiä turvallisten tietoliikenneyhteyksien luomiseen. Ensimmäinen IPsec-versio määriteltiin vuonna 1995 IETF:n dokumentissa RFC 1825. Tämä dokumentti on kuitenkin jo uudistettu kahteen otteeseen, ja uusin versio on vuonna 2005 julkaistu RFC 4301. IPsec koostuu neljästä perustavanlaatuisesta osakokonaisuudesta, jotka ovat turvallisuusprotokollat, turvallisuusassosiaatiot, avaintenhallinta ja kryptografiset algoritmit. (Kent & Seo 2005.)

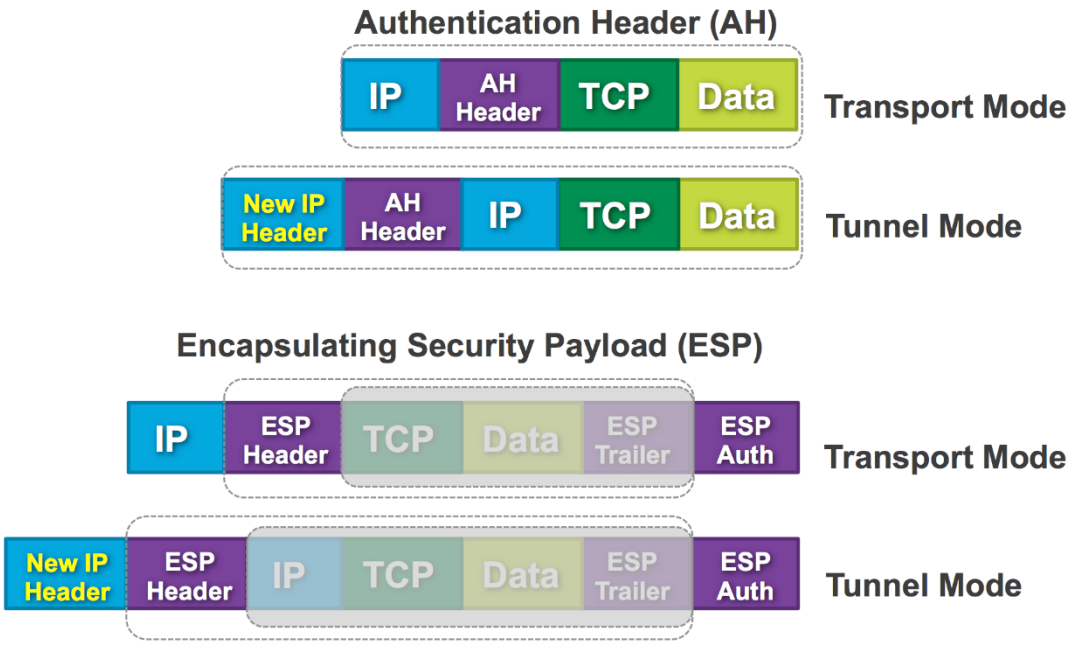
3.2.1 Turvallisuusprotokollat

IPsecin turvallisuusprotokollia ovat AH ja ESP. AH on IPsec-yhteyden todentamiseen sekä tiedon eheyden varmistamiseen käytettävä protokolla. ESP on protokolla, jolla voidaan myös tehdä todennus ja eheyden tarkistus, mutta sillä voidaan tehdä myös yhteyden salaus. AH:ta ja ESP:tä voidaan myös käyttää yhdessä IPsec-yhteyden luomisessa. (Kent & Seo 2005.) AH:n ja ESP:n rakenne IPsec-paketin yhteydessä on esitetty kuviossa 6.



Kuvio 6. AH- ja ESP-protokollien rakenne (Farag 2017)

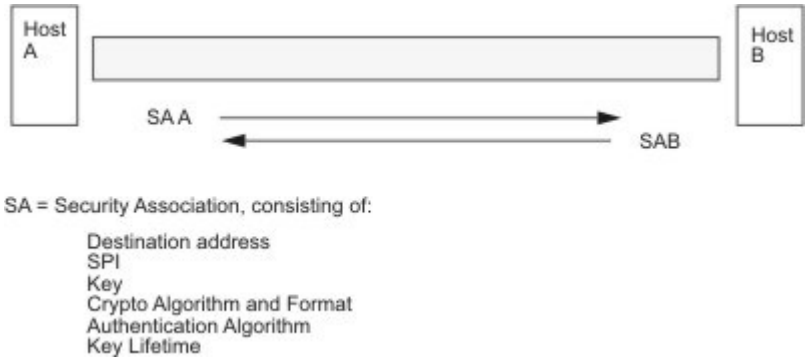
IPsec voi myös toimia kahdessa eri moodissa. Transport-moodia käytetään yleensä kahden päätteen välisen yhteyden muodostamiseen, tai silloin kun IPsec-protokollaa käytetään yhdessä jonkin toisen tunnelointiprotokollan kanssa. Tunnel-moodi on yleisempi, ja tavallisesti sitä käytetään tunneloiduissa IPsec-yhteyksissä. (Kent & Seo 2005.) AH:n ja ESP:n käyttö molemmissa toimintamoodeissa on esitetty kuviossa 7.



Kuvio 7. IPsec-toimintamoodit (Farag 2017)

3.2.2 Turvallisuusassosiaatiot

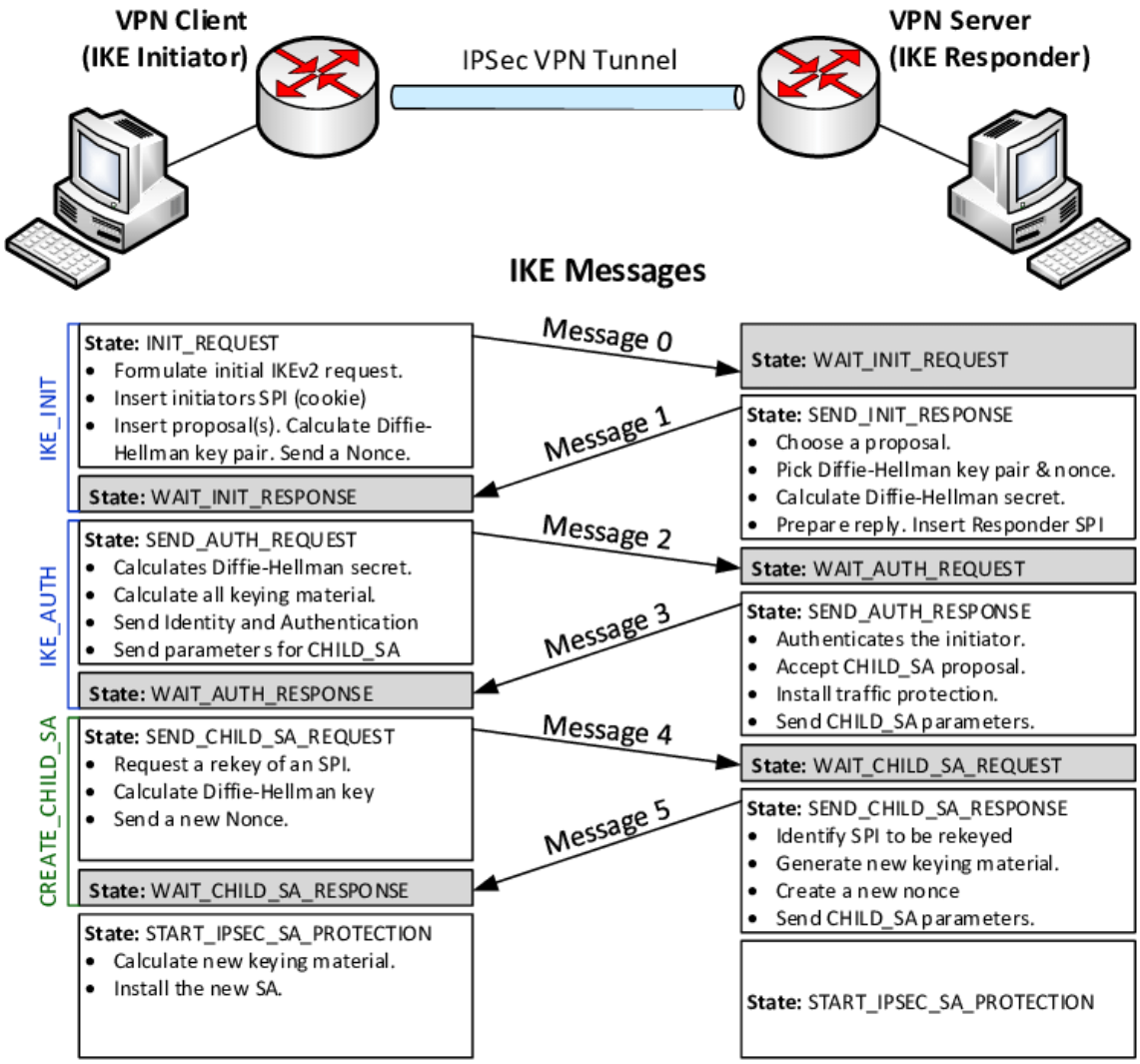
Turvallisuusassosiaatiot eli SA:t ovat IPsec-yhteyden muodostuksessa käytettäviä, yhteyden osapuolten osoitetietoja, tunnisteita, algoritmeja ja parametreja. Yhteyden osapuolet sopivat turvallisuusassosiaatioista kättelyn yhteydessä. (IBM 2023.) Yhteenveto IPsec-protokollan turvallisuusassosiaatioista on esitettynä kuviossa 8.



Kuvio 8. IPsec-turvallisuusassosiaatiot (IBM 2023)

3.2.3 Avaintenhallinta

IETF julkaisi ISAKMP-protokollan dokumentissa RFC 2408. Se antoi raamit sille, kuinka edellä mainittujen turvallisuusassosiaatioiden määritys tulisi tapahtua turvallisen tietoliikenneyhteyden muodostuksessa. Tähän raamin sopivaksi protokollaksi luotiin IKE, jonka uusin versio IKEv2 on määritelty vuonna 2014 dokumentissa RFC 7296. (Kaufman, Hoffman, Nir, Eronen, & Kivinen 2014.) IKEv2/IPsec-yhteyden muodostukseen käytetään IKEv2-protokollan kättelyä. IKEv2-kättelyn kulku on kuvattu kuviossa 9.



Kuvio 9. IKEv2-kättely (Naby, Arslan & Kim 2017)

3.2.4 Kryptografiset algoritmit

IPsec tukee huomattavan suurta määrää erilaisia kryptografisia algoritmeja autentikaatioon ja salaukseen. Kansallisen turvallisuuden tasolla käytettävä suositus turvallisten algoritmien valintaan on CNSA, joka on Yhdysvaltain kansallisen turvallisuusvirasto NSA:n luoma, ja sen IPsecissä käytettävien salaussarjojen määrittely löytyy dokumentista RFC 9206. (Corcoran & Jenkins 2022.) CNSA:ssa riittävän turvallisiksi hyväksytyt algoritmit on esitetty taulukossa 1. Vuonna 2022 CNSA:sta julkaistiin versio 2.0, joka listaa myös suositukset kvanttisietoiseen tietoturvaan (National Security Agency 2022). Kvanttisietoisia algoritmeja ei kuitenkaan käsitellä tämän työn yhteydessä, vaan oheisesta taulukosta löytyvät vain vanhemmat suositukset.

Taulukko 1. CNSA-turvallisuusalgoritmit (National Security Agency 2022)

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm for key establishment	NIST SP 800-56A	Use Curve P-384 for all classification levels.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm for digital signatures	FIPS PUB 186-4	Use Curve P-384 for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 for all classification levels.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm for key establishment	IETF RFC 3526	Minimum 3072-bit modulus for all classification levels
RSA	Asymmetric algorithm for key establishment	FIPS SP 800-56B	Minimum 3072-bit modulus for all classification levels
RSA	Asymmetric algorithm for digital signatures	FIPS PUB 186-4	Minimum 3072-bit modulus for all classification levels.

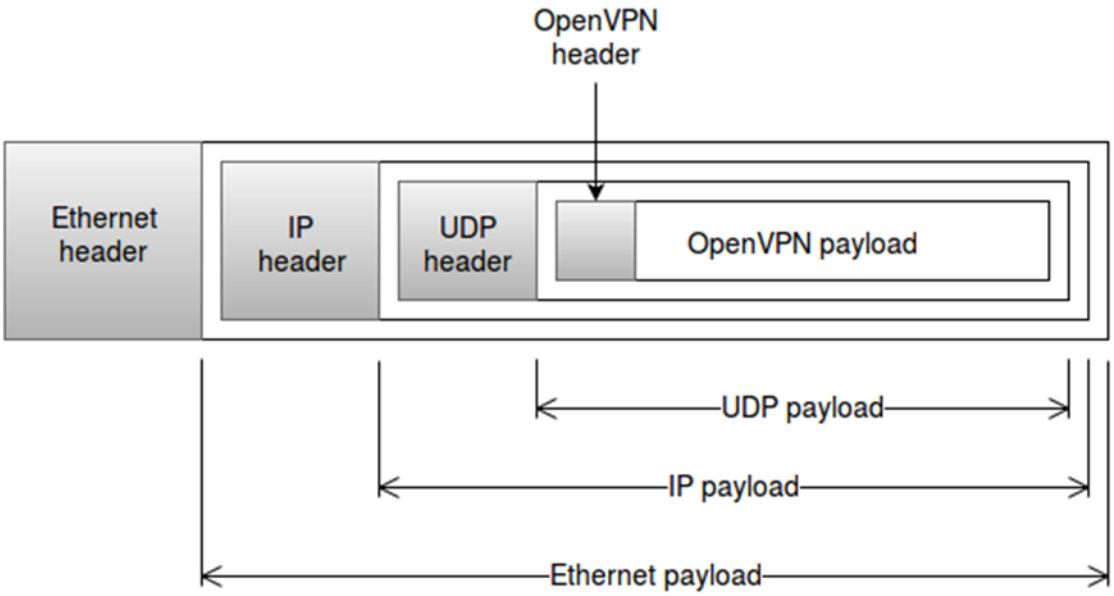
3.3 OpenVPN

OpenVPN on samaa nimeä kantavan yrityksen perustajan, James Yonanin luoma avoimen lähdekoodin VPN-protokolla. Sen ensimmäinen julkinen versio julkaistiin vuonna 2002, ja sittemmin yritys on laajentanut portfoliotaan ja tarjoaa ilmaisen protokollan lisäksi muun muassa suuryrityksille skaalautuvia ja pilvipohjaisia VPN-ratkaisuja. OpenVPN tukee lukuisia eri turvallisuusprotokollia ja algoritmeja. (OpenVPN 2024b.) Esimerkkinä OpenVPN-salaussarjasta on VPN-palveluntarjoaja VyprVPN:n omassa palvelussaan käyttämät algoritmit esitettynä kuviossa 10.

- **Authentication:** SHA256 (also known as SHA2)
- **Control channel:** AES-256-GCM cipher and SHA384 HMAC are the defaults. We can also use AES-256-CBC cipher/SHA256 HMAC, or AES-256-CBC cipher/SHA1 HMAC in the case that the client or network has compatibility issues with the default levels of encryption.
- **RSA Encryption:** TLS-ECDHE-RSA-2048. The ECDHE means we provide the "Elliptic curve Diffie-Hellman" key exchange, which provides Perfect Forward Secrecy.

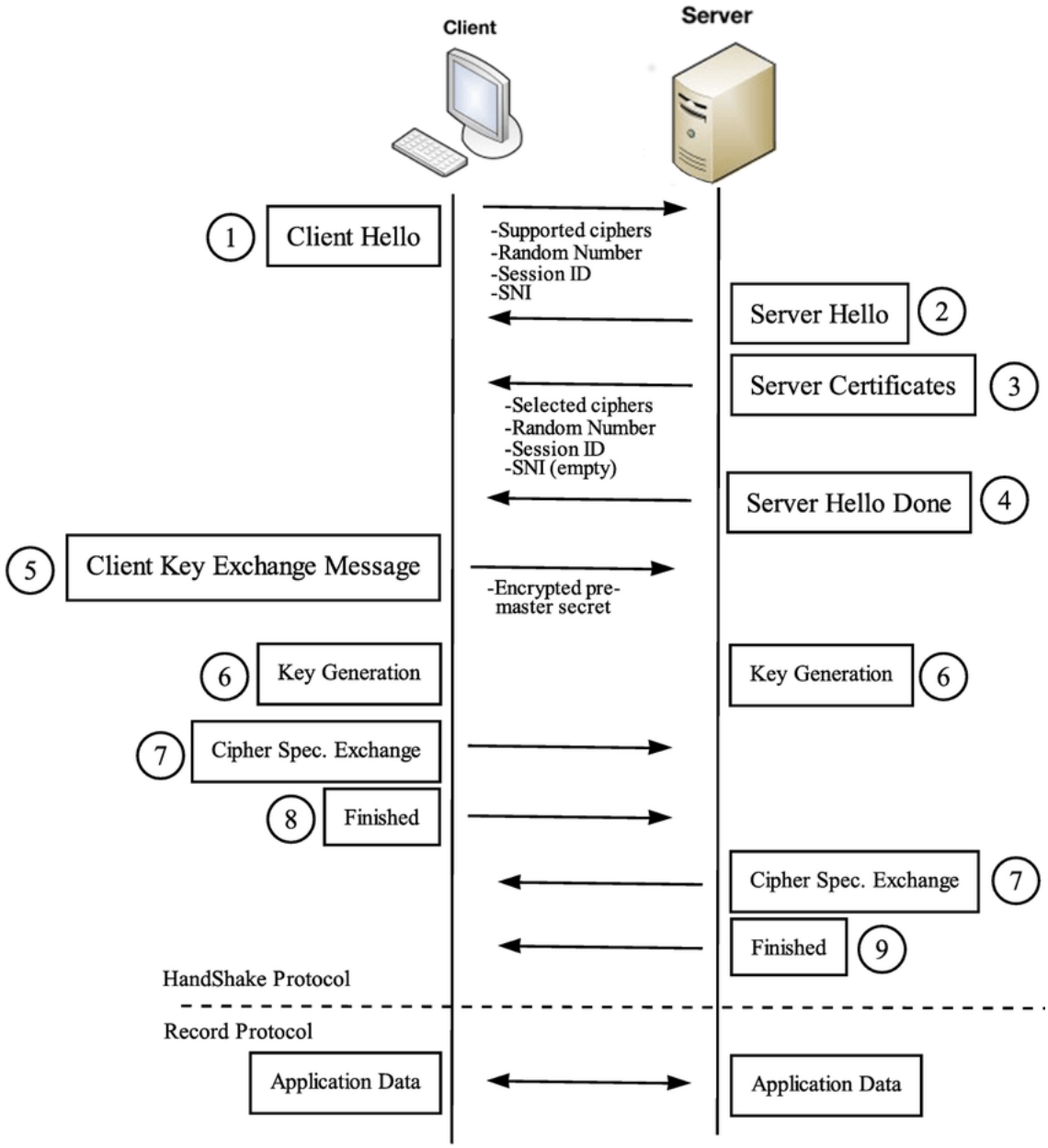
Kuvio 10. OpenVPN-turvallisuusalgoritmit (VyprVPN 2024)

OpenVPN voi käyttää tietoliikenteessä joko TCP- tai UDP-protokollaa. Yhteyden muodostukseen voidaan käyttää joko SSL/TLS-kättelyä tai staattisia avaimia. (OpenVPN 2024c.) OpenVPN:n IP-paketin kapselointi on esitetty kuviossa 11.



Kuvio 11. IP-paketin kapselointi OpenVPN-protokollassa (Novickis 2016)

OpenVPN-protokollan käyttämä SSL/TLS kättely on hyvin yleinen tapa autentikoida yhteyksiä. Sitä käytetään esimerkiksi verkkosivujen autentikointiin HTTPS-protokollalla internetiä selatessa. (SSL.com 2023.) SSL/TLS-kättelyn kulku on esitetty kuviossa 12.

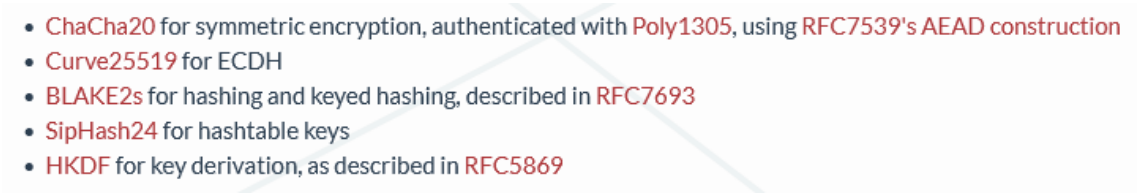


Kuvio 12. TLS-kättely (Shbair, Cholez, Francois & Chrisment 2016)

3.4 WireGuard

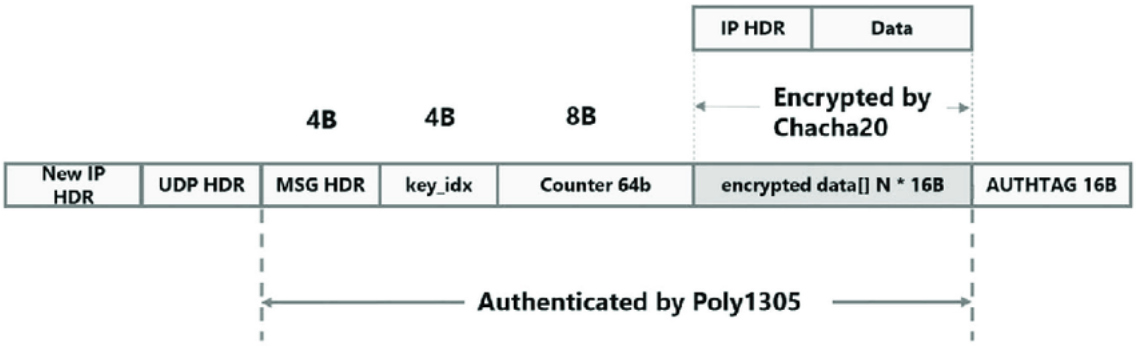
WireGuard on Jason A. Donenfeldin luoma avoimen lähteen VPN-protokolla, joka julkaistiin ensimmäisen kerran vuonna 2016. WireGuardin tavoitteena oli olla turvallisempi, nopeampi ja helpompi käyttää kuin IPsec- ja OpenVPN-protokollat, jotka kehittäjä itsekin mainitsee julkaisussaan vuodelta 2020. (Donenfeld 2020, 1.) WireGuard käyttää hyvin moderneja algoritmeja salaukseen ja avaintenhallintaan ja luo niiden avulla virtuaalisen rajapinnan, joka käyttäjän on helppo ottaa käyttöön. WireGuardissa nähtiin niin paljon potentiaalia jopa itse Linus Torvaldsin

suunnalta, että se lisättiin Linux kernelin version 5.6 julkaisuun vuonna 2020. (Vaughan-Nichols 2021.) WireGuard käyttää salaussarjassaan ChaCha20-Poly1305-algoritmia, joka on tyypiltään AEAD-algoritmi (Nir & Langley 2018). WireGuardin käyttämä salaussarja on kokonaisuudessaan kuvattuna kuviossa 13.



Kuvio 13. WireGuard-turvallisuusprotokollat (WireGuard 2024)

WireGuard käyttää tietoliikenteessä UDP-protokollaa. Yhteyden muodostukseen käytetään Noise protokollan IK-tyypin kättelyä. (Donenfeld 2020, 7.) WireGuardin IP-paketin kapselointi on esitetty kuviossa 14.



Kuvio 14. IP-paketin kapselointi WireGuard-protokollassa (Cho, Sergeev & Zou 2020)

Noise IK tyypin -kättely tarkoittaa, että kättelyn aloittaja lähettää oman julkisen avaimensa heti vastaanottajalle ja että vastaanottajan julkinen avain on kättelyn aloittajan tiedossa (Perrin 2018). Noise IK -kättelyn eteneminen on esitetty kaavassa 1.

$$
\begin{aligned}
&IK: \\
&\quad \leftarrow s \\
&\quad \ldots \\
&\quad \rightarrow e, es, s, ss \\
&\quad \leftarrow e, ee, se
\end{aligned}
\tag{1}
$$

missä

→	on	aloittajalta vastaanottajan suuntaan kulkeva tieto
←	on	vastaanottajalta aloittajan suuntaan kulkeva tieto
...	on	raja, jonka yläpuolinen tieto välitetään ennen ensimmäistä protokollaviestiä
e	on	tilapäinen avain
s	on	staattinen avain
nn	on	DH algoritmi; ensimmäinen kirjain kertoo aloittajan, ja toinen kirjain vastaanottajan avaimen tyypin

(Kobeissi, Nicolas & Bhargavan 2019)

3.5 VPN-protokollien ominaisuuksien vertailu

Yhteenvetona tutkimukseen valittujen protokollien vertailemiseksi ChatGPT-tekoälysovellusta pyydettiin laatimaan vertailutaulukko näiden protokollien tärkeimmistä ominaisuuksista. Tuotos vaati pari korjaavaa syötettä tekoälylle, mutta lopputuloksena syntyi asiallinen taulukko tekoälyn syötteeseen annettujen protokollien ominaisuuksista. Taulukon tiedot tarkastettiin vielä muista lähteistä ChatGPT:n antamien tietojen varmistamiseksi ja ovat esitettyinä taulukossa 2.

Taulukko 2. Tutkittavien protokollien ominaisuudet

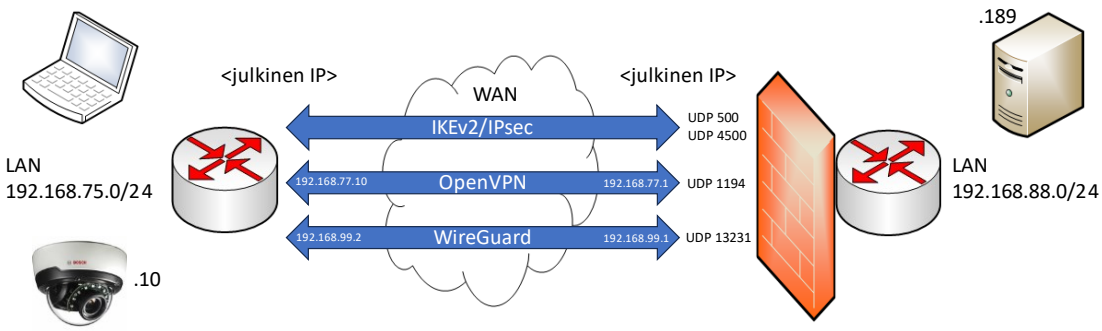
Ominaisuus	IKEv2/IPSec	OpenVPN	WireGuard
Suorituskyky	Hyvä	Hyvä	Erinomainen
Turvallisuus	Erinomainen	Hyvä	Erinomainen
Salausalgoritmit	AES, 3DES, SHA-2	AES, Blowfish, SHA-1/2	ChaCha20, Poly1305
Kättelyprotokollat	IKEv2	TLS (SSL)	Noise
Transport layerin protokollat	UDP, TCP	UDP, TCP	UDP
Tunnistautumismenetelmät	Sertifikaatit, EAP, PSK	Käyttäjätunnus/salasana, sertifikaatit, PSK	Julkinen avain
Yhteysnopeus	Nopea	Hyvä	Erinomainen
Tuki	Laajasti tuettu	Laajasti tuettu	Vähemmän tukea, kasvaa
Toteutettavuus	Monipuolinen	Monipuolinen	Yksinkertainen, helppo
Yhteensopivuus	Windows, macOS, iOS, Android, Linux	Lähes kaikki	Rajoitetumpi
Suorituskyvyn vaikutus	Kohtuullinen	Kohtuullinen	Hyvin vähäinen
Asennuksen monimutkaisuus	Kohtalainen	Korkea	Matala
Käytettävyys	Hyvä	Hyvä	Erinomainen
Julkinen tunnettuus	Kyllä	Kyllä	Ei

4 TESTAUSSUUNNITELMA

4.1 Testauksen pääperiaatteet

Tutkimuksen käytännön testaus suoritettiin kahdessa eri vaiheessa. Ensimmäisessä vaiheessa kahden reitittimen välistä yhteysnopeutta eri VPN-protokollia käyttäen mitattiin kahdella eri tietoliikenneyhteyden nopeutta mittaavalla työkalulla. Testauksen ensimmäisen vaiheen tarkoituksena oli löytää eri protokollien teknisen suorituskyvyn maksimiarvot.

Testauksen toisessa vaiheessa reitittimien välistä VPN-yhteyttä käytettiin välittämään kuvaa IP-kameralta taustajärjestelmään. Testauksen toisen vaiheen tarkoituksena oli tutkia, onko eri VPN-protokollien välillä näkyvää vaikutusta kameravalvonnan suorituskykyyn. Muutoksia suorituskykyyn arvioitiin aistinvaraisesti sekä mahdollisuuksien mukaan absoluuttisia mittausarvoja käyttäen. Testiympäristön verkkotopologia on kuvattuna kuviossa 15.



Kuvio 15. Testiympäristön topologia

4.2 Tekninen testaus

Teknistä suorituskykytestausta varten testaukseen käytettäviin kahteen reitittimeen luotiin virtuaaliset liitännät jokaiselle kolmelle testattavalle VPN-menetelmälle. Kunkin VPN-yhteyden toimivuus testattiin ennen varsinaista testin suoritusta. Teknisen suorituskyvyn testausta varten yhdelle palvelimelle asennettiin OpenSpeedTest- sekä iperf3-ohjelmistot, joita vasten yhteyden nopeutta voitiin testata. Palvelin kytkettiin kiinteän verkon reitittimeen, ja nopeustestit suoritettiin toisella työasemalla mobiiliyhteyttä käyttävän reitittimen läpi.

Molemmista menetelmistä dokumentoitiin testausasetelma sekä reitittimien ja VPN-tunneleiden konfiguraatio. Mittaussuoritteista dokumentoitiin selkeään muotoon kaikki relevantit tulokset, jotta eri VPN-protokollien suorituskyvyn erot saatiin esitettyä.

4.3 Käyttötapaustesti

Käytännön testissä mobiilireitittimeen kytkettiin IP-kamera, joka liitettiin kiinteän verkon reitittimen takana olevaan VMS-järjestelmään VPN-yhteyden läpi. IP-kamera asetettiin kuvaamaan paljon erisuuntaista liikettä sisältävää Youtube-videota. VMS-järjestelmään välitetyn videokuvan laatua arvioitiin pysäytyskuvalla testimateriaalina käytetyn videon samasta kohdasta. Kameran käyttökokemusta eri VPN-yhteyksillä verrattiin toisiinsa.

Käyttökokemuksen arviointiin käytettiin aistinvaraista arviointia sekä tietoliikenteessä havaittavia ilmiöitä, kuten pakettien häviämistä, välitettyä kuvatiheyttä ja bitrate-arvoa. Videokuvan laatua ja kaistantarvetta oli mahdollista kasvattaa erojen esiin saamiseksi, ja tarvittaessa voitiin käyttää mobiilireitittimen perässä useampaa IP-kameraa.

5 TESTIYMPÄRISTÖN RAKENTAMINEN

5.1 Testipalvelin

Nopeustestaukseen käytettävänä testipalvelimena käytettiin Raspberry Pi 4B -pienoistietokonetta. Tässä mallissa on gigabitin nopeuteen kykenevä verkkokortti, joten se ei muodosta pullonkaulaa nopeustestaukseen.

Palvelimelle asennettiin nopeuden mittaamista varten OpenSpeedTest-, sekä iperf3-ohjelmistot. Käyttöjärjestelmäksi palvelimeen asennettiin uusin 64-bittinen Raspberry Pi OS Lite. Lite-versiossa ei ole lainkaan työpöytäympäristöä, eli sitä käytetään ainoastaan terminaalin komentorivin kautta. Nopeusmittaustyökalujen asennusta varten palvelimella oli käytössä SSH- sekä Docker-palvelut.

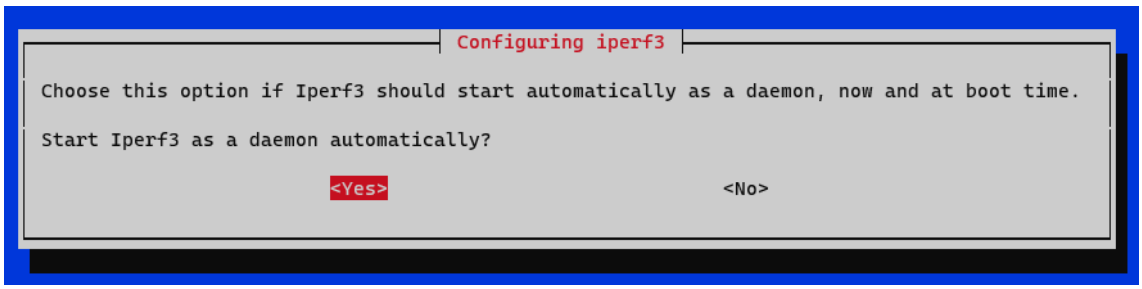
5.1.1 Iperf3

Nopeusmittausohjelmisto iperf3 toimii server–client-periaatteella, eli mittaustapahtumassa toisen pään pitää toimia palvelimena ja toinen pää toimii clientina. Iperf3 asennettiin Linuxiin suoraan apt-pakettikirjastosta. Iperf3:n asentaminen apt-pakettikirjastosta on esitettynä kuviossa 16.

```
admin@testserver:~ $ sudo apt install iperf3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libcamera0.1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libiperf0 libsctp1
Suggested packages:
  lksctp-tools
The following NEW packages will be installed:
  iperf3 libiperf0 libsctp1
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 148 kB of archives.
After this operation, 509 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

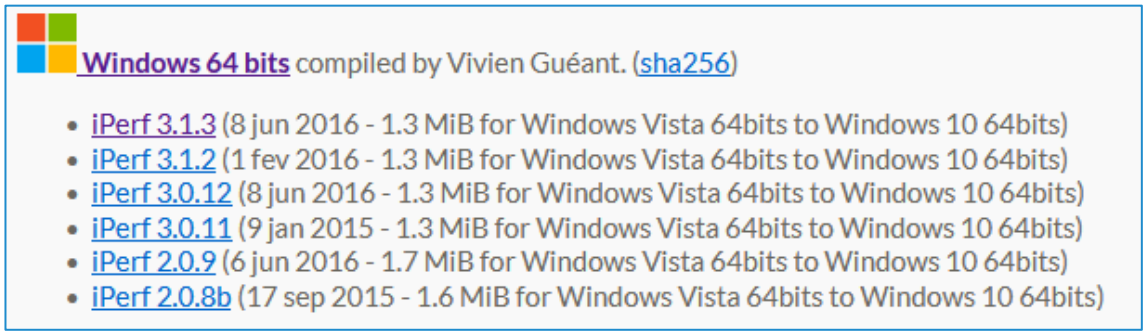
Kuvio 16. Iperf3:n asennus apt-pakettikirjastosta

Iperf3 voitiin asennuksen yhteydessä asettaa järjestelmäpalveluksi, joka käynnistyy automaattisesti järjestelmän käynnistyessä. Sovelluksen automaattinen käynnistyminen on suositeltavaa ottaa käyttöön palvelinasennuksissa. Kuvankaappaus asetuksesta on esitettynä kuvioissa 17.



Kuvio 17. Iperf3:n asettaminen järjestelmäpalveluksi

Mobiilireitittimen päässä tapahtuvaa testausta varten iperf3 asennettiin myös kannettavaan tietokoneeseen, jossa on Windows 11 käyttöjärjestelmä. Iperf3 asennuspaketin saa ladattua internetistä osoitteesta https://iperf.fr/. Kuviossa 18 on esitettynä valikoima verkkosivulla tarjolla olevista iperf-asennuspaketeista Windowsille.



Kuvio 16. Windowsille tarjolla olevat iperf-versiot (Guéant 2024)

Lopuksi iperf3-ohjelmiston toiminta testattiin. Tässä tapauksessa molemmat työasemat olivat kaapeliyhteydellä samassa lähiverkossa yhden gigabitin verkkoliitäntöjen takana, joten nopeustestissä saatiin tulokseksi lähes gigabitin siirtonopeus, kuten kuviosta 19 voidaan nähdä.

```
C:\iperf>iperf3 -c 192.168.88.253
Connecting to host 192.168.88.253, port 5201
[  4] local 192.168.88.254 port 59566 connected to 192.168.88.253 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec   112 MBytes   935 Mbits/sec
[  4]   1.00-2.00   sec   111 MBytes   931 Mbits/sec
[  4]   2.00-3.00   sec   111 MBytes   933 Mbits/sec
[  4]   3.00-4.00   sec   112 MBytes   937 Mbits/sec
[  4]   4.00-5.00   sec   112 MBytes   938 Mbits/sec
[  4]   5.00-6.00   sec   112 MBytes   939 Mbits/sec
[  4]   6.00-7.00   sec   112 MBytes   938 Mbits/sec
[  4]   7.00-8.00   sec   112 MBytes   942 Mbits/sec
[  4]   8.00-9.00   sec   112 MBytes   940 Mbits/sec
[  4]   9.00-10.00  sec   112 MBytes   940 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec  1.09 GBytes   937 Mbits/sec                  sender
[  4]   0.00-10.00  sec  1.09 GBytes   937 Mbits/sec                  receiver

iperf Done.
```

Kuvio 17. Iperf-testaus kaapeliyhteydellä

5.1.2 OpenSpeedTest

OpenSpeedTest on verkkoyhteyden mittaukseen käytettävä sovellus, joka asennetaan vain palvelimelle. Sovellus luo asennuksen yhteydessä käyttöliittymäkseen palvelimelle web-sivun, jolla vierailemalla voidaan yhteysnopeutta mitata ilman client-sovelluksen asennuksia. OpenSpeedTest-sovelluksen asennusohjeet löytyvät verkkosivulta https://openspeedtest.com/. Asennustavalle on tarjolla useita eri vaihtoehtoja, ja tässä tapauksessa helpoin ja toimivin vaihtoehto oli asentaa se Docker-konttina. Kuviossa 20 voidaan nähdä, että Docker-asennukselle löytyy verkkosivulta valmis komento, jonka voi kopioida palvelimen komentoriville.

A) Quick and Easy Deployment using Docker.

This is docker implementation using nginxinc/nginx-unprivileged:stable-alpine. uses significantly fewer resources. OpenSpeedTest contains Only "STATIC" Files like HTML,CSS & JS. So you don't need to worry about Security Updates or Hidden Exploits that may compromise your secure environments.

Install Docker and run the following command! [Official Docker Image]

```
docker run --restart=unless-stopped --name openspeedtest -d -p 3000:3000 -p 3001:3001 openspeedt
```

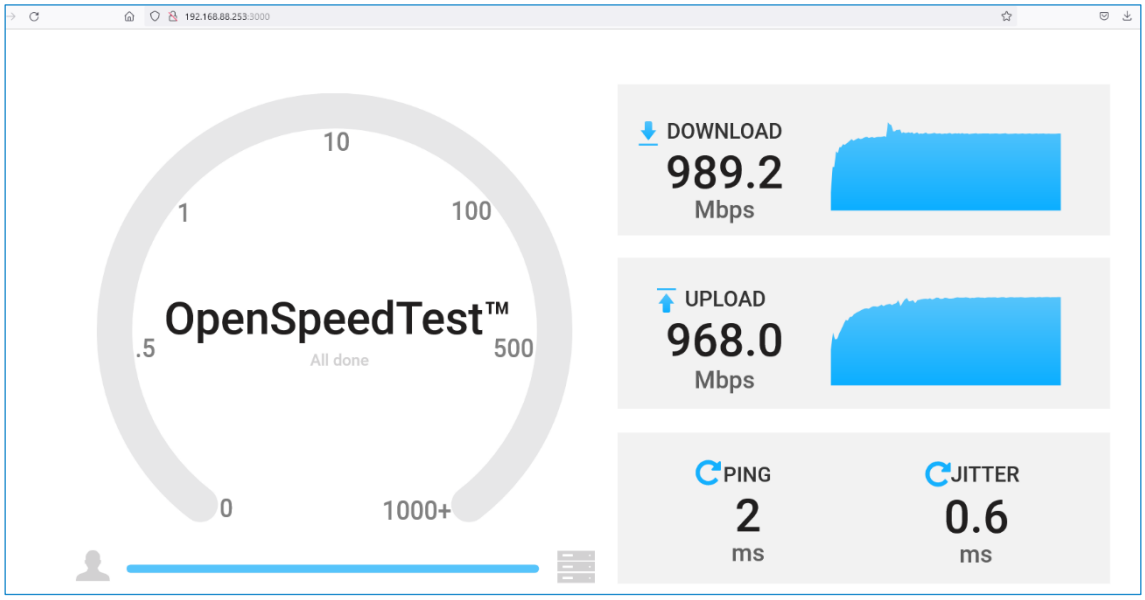
Kuvio 18. OpenSpeedTest-palvelimen asennusohje (OpenSpeedTest 2024)

Asennuksen suorittamisen jälkeen varmistettiin, että ohjelmisto pyörii Docker-kontissa kuten pitääkin. Docker-kontin statuksen tarkastaminen on esitettynä kuviossa 21.

```
admin@testserver:~ $ sudo docker ps
CONTAINER ID   IMAGE                  COMMAND                  CREATED          STATUS          PORTS
                                                       NAMES
6ce387bf2363   openspeedtest/latest   "/docker-entrypoint.…"   44 minutes ago   Up 44 minutes   0.0.0.0:3000-3001->
3000-3001/tcp, :::3000-3001->3000-3001/tcp, 8080/tcp   openspeedtest
admin@testserver:~ $
```

Kuvio 19. OpenSpeedTest-palvelimen docker-kontin status

Lopuksi suoritettiin OpenSpeedTest palvelimen testaus kannettavan tietokoneen selaimella. Molemmat työasemat olivat edelleen kaapeliyhteydellä samassa lähiverkossa, joten tulokseksi saatiin tälläkin kertaa lähes gigabitin tiedonsiirtonopeus., ja OpenSpeedTest-selainkäyttöliittymä on esitettynä kuviossa 22.



Kuvio 20. OpenSpeedTest-selainkäyttöliittymä

5.2 Reititin

Käytännön testissä kiinteään verkkoon kytkettävänä palvelinpään reitittimenä käytettiin Mikrotik RB750Gr3 -reititintä. Reitittimeen luotiin valmius toimia VPN-palvelimena kaikilla tutkittavilla menetelmillä. Tähän reitittimeen kytkettiin myös nopeusmittauksessa käytettävä palvelin sekä videonhallintajärjestelmä. IPsec- ja OpenVPN-tunneleiden osalta turvallisuusalgoritmien valinnassa noudatettiin

CNSA:n suositusta IPsec-salausalgoritmeista. Konfigurointi toteutettiin mahdollisimman hyvin noudattelemaan RFC 9206:ssa määriteltyä CNSA-GCM-256-ECDH-384-salaussarjaa, sillä se vastaan parhaiten WireGuardin käyttämää ChaCha20-Poly1305-algoritmia. AES-GCM on ChaCha20-Poly1305:n tapaan AEAD-tyyppinen algoritmi, toisin kuin vanhempi AES-CBC. Tällä valinnalla voi olla merkitystä pienitehoisten reititinlaitteiden suorituskyvyn kannalta. (Corcoran & Jenkins 2022.)

Mikrotik-reitittimen konfiguroinnin apuna käytettiin erityisesti Johnny Van Den Bergin ”The Network Berg” Youtube-kanavan tutoriaalivideoita. IPsec (Van Den Berg 2022a) ja WireGuard (Van Den Berg 2022b) site-to-site-tunneleiden konfigurointiin löytyy suoraan hyvät tutoriaalivideot Van Den Bergin kanavalta. OpenVPN-tunnelin konfigurointiin löytyy ohjeita OpenVPN:n omalta verkkosivulta (OpenVPN 2024a) sekä mobiilireititinvalmistaja Teltonikan verkkosivuilta (Teltonika Networks 2023).

5.3 Mobiilireititin

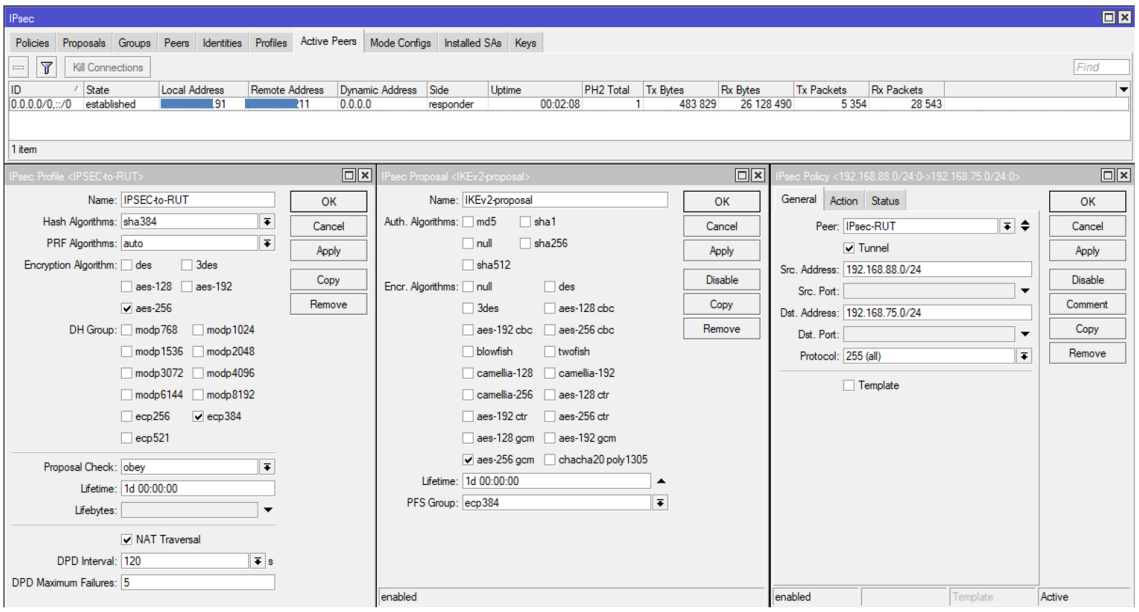
Mobiilireitittimenä käytettiin Teltonika RUTX50 -mallista 5G-reititintä. Tältä reitittimeltä luotiin VPN-tunnelit kiinteän verkon reitittimeen kaikilla tutkittavilla menetelmillä. Tähän reitittimeen kytkettiin kannettava tietokone teknistä suorituskykymittausta varten, sekä IP-kamera käytännön suorituskykytestiä varten.

Mobiilireitittimen konfigurointiin käytetään samoja ohjelähteitä kuin palvelinpään reitittimen konfigurointiin, mutta niiden lisäksi reititinvalmistajan verkkosivuilta löytyi vielä yksi ohje IPsec määrityksiin (Teltonika Networks 2024), joka koskee vain mobiilireititintä. Mobiilireitittimen VPN-määrityksen tehdään vastaamaan VPN-palvelimen määrityksiin, joten suurempi konfiguraatiotyö tehtiin Mikrotik-reitittimeen.

5.4 IKEv2/IPsec-konfiguraatio

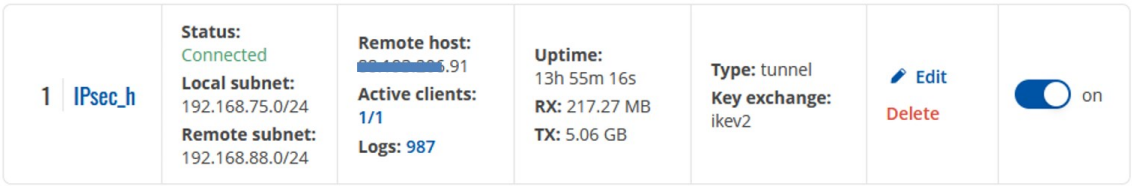
IPsec-tunnelin muodostusta varten Mikrotik-reitittimessä määriteltiin muun muassa käytettävät kättelytapa IKEv2, salausalgoritmit sekä lähiverkot, jotka yhdistettiin toisiinsa tunnelin kautta. Reitittimelle ei annettu vastaosapuolen IP-

osoitetta, vaan se odotti yhteydenottoa mobiilireitittimeltä. Mikrotik-reitittimen IPsec-konfiguraatio on esitetty kuviossa 23.



Kuvio 21. Mikrotik-reitittimen IPsec-konfiguraatio

Teltonikan mobiilireitittimeen määriteltiin kaikki samat asetukset kuin Mikrotik-reitittimeen, mutta sen lisäksi konfiguraatioon täytyi antaa myös VPN-palvelimena toimivan reitittimen kiinteä IP-osoite. Mobiilireitittimen muodostama IPsec-tunneli on esitettynä kuviossa 24.

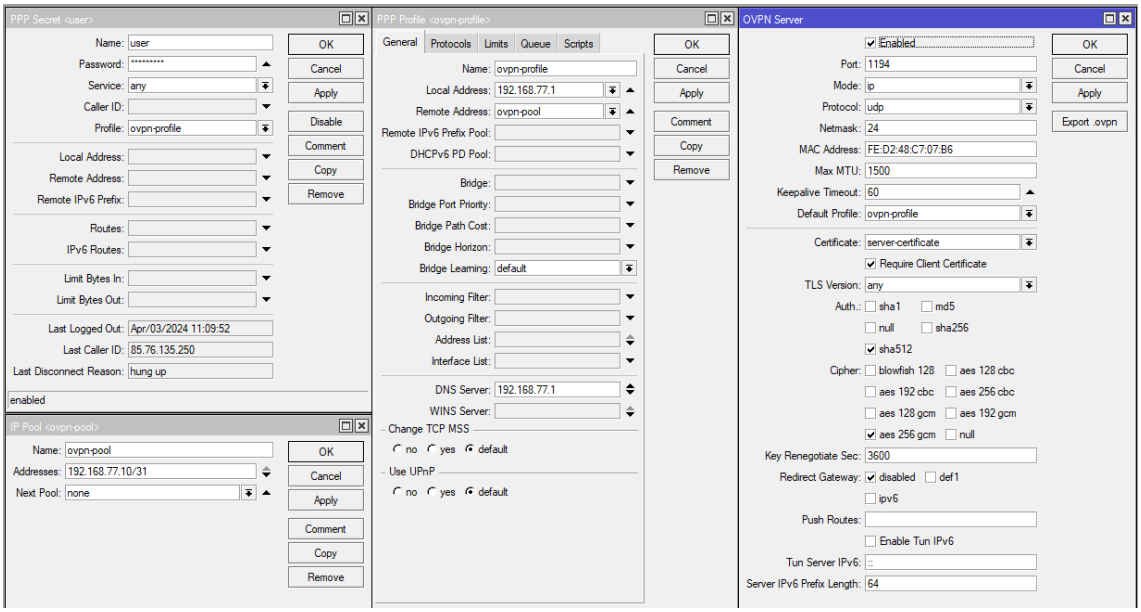


Kuvio 22. Teltonika-mobiilireitittimen IPsec-tunneli

5.5 OpenVPN-konfiguraatio

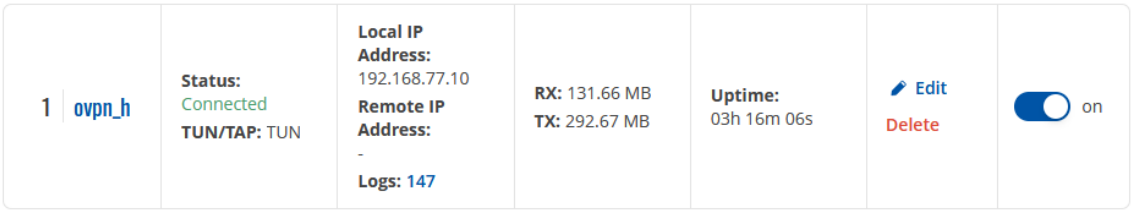
OpenVPN-konfiguraatiossa Mikrotik-reitittimellä ensin luotiin ja allekirjoitettiin varmennussertifikaatit palvelimelle ja mobiilireitittimelle. OpenVPN-tunneli toimii siten, että se ei suoraan reititä tunnelin eri päiden lähiverkkoja yhteen. Tämän vuoksi tunnelin molemmille päille luotiin omat IP-osoitteet, jotka toimivat gatewayna lähiverkkoon. Tässäkin tapauksessa Mikrotik-reititin odotti

passiivisena yhteydenottoa mobiilireitittimeltä tunnelin muodostamiseksi. Mikrotik-reitittimen OpenVPN-konfiguraatio on esitettynä kuviossa 25.



Kuvio 23. Mikrotik-reitittimen OpenVPN-konfiguraatio

OpenVPN-konfiguraatio mobiilireitittimessä noudatteli samaa kaavaa kuin IPsec-konfiguraatio, eli luotiin vastaavat asetukset kuin Mikrotik-reitittimessä sekä lisättiin VPN-palvelimen kiinteä IP-osoite. Mobiilireitittimen muodostama OpenVPN-tunneli on esitettynä kuviossa 26.

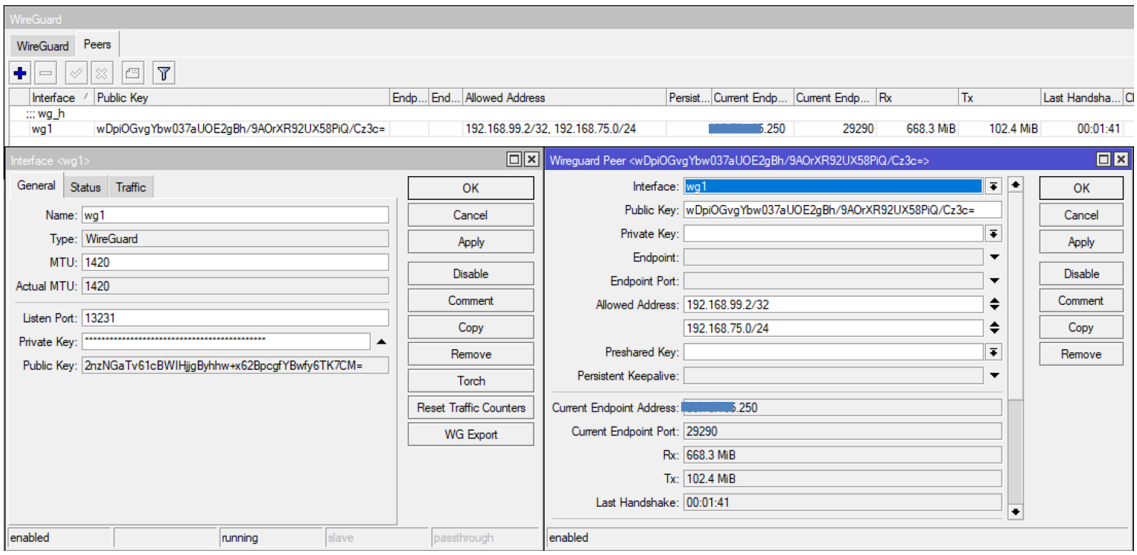


Kuvio 24. Teltonika-mobiilireitittimen OpenVPN-tunneli

5.6 WireGuard-konfiguraatio

WireGuard-konfiguraatiossa reitittimeen muodostui uusi virtuaalinen liityntärajapinta, jota käytettiin gatewayna lähiverkkojen reitityksessä. Molempien päiden virtuaalirajapinnoilla oli omat, lähiverkosta erilliset IP-osoitteensa. WireGuard-konfiguroinnissa ei määritelty lainkaan salausalgoritmien asetuksia, vaan siinä määriteltiin pelkästään tunnelin käyttöön oikeutetut verkot, käytettävä UDP-portti sekä

vastapään rajapinnan julkinen avain. Mikrotik-reitin tässäkin tapauksessa odotti passiivisena yhteydenottoa mobiilireitittimeltä. Mikrotik-reitittimen WireGuard-konfiguraatio on esitettynä kuviossa 27.



Kuvio 25. Mikrotik-reitittimen WireGuard-konfiguraatio

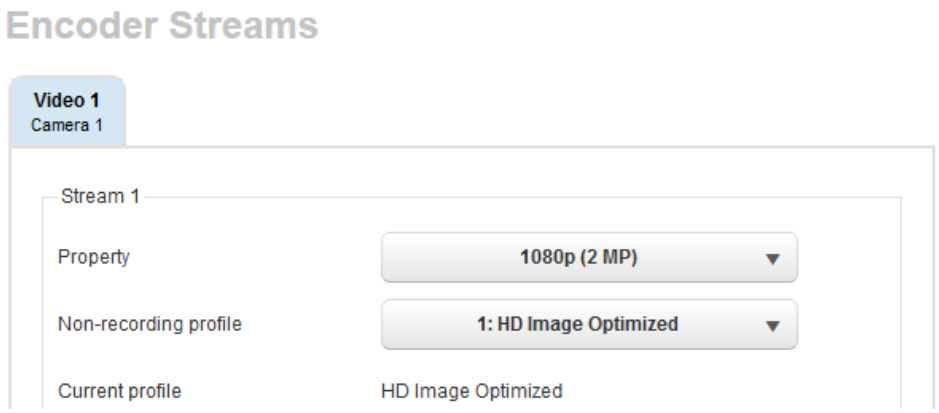
Mobiilireitittimessä WireGuard-tunneliin asetettiin Mikrotik-reitittimessä käytettävien asetusten lisäksi VPN-palvelimen IP-osoite, tunnelin UDP-portti sekä persistent keepalive -arvo, joka lähetti tunnelin ylläpitämiseksi tyhjiä paketteja, ellei muuta liikennettä ollut. Mobiilireitittimen luoma WireGuard-tunneli on esitettynä kuviossa 28.

```
   Firmware:    RUTX_R_00.07.06.8
   Build:       ba806d4906
   Build date: 2024-03-21 14:54:27
-----------------------------------
root@RUTX50:~# wg show
interface: wg_h
  public key: wDpiOGvgYbw037aUOE2gBh/9AOrXR92UX58PiQ/Cz3c=
  private key: (hidden)
  listening port: 51820

peer: 2nzNGaTv61cBWIHjjgByhhw+x62BpcgfYBwfy6TK7CM=
  endpoint: [redacted].91:13231
  allowed ips: 192.168.99.1/32, 192.168.88.0/24
  latest handshake: 19 seconds ago
  transfer: 108.97 MiB received, 8.94 GiB sent
  persistent keepalive: every 25 seconds
root@RUTX50:~#
```

Kuvio 26. Teltonika-mobiilireitittimen WireGuard-tunneli

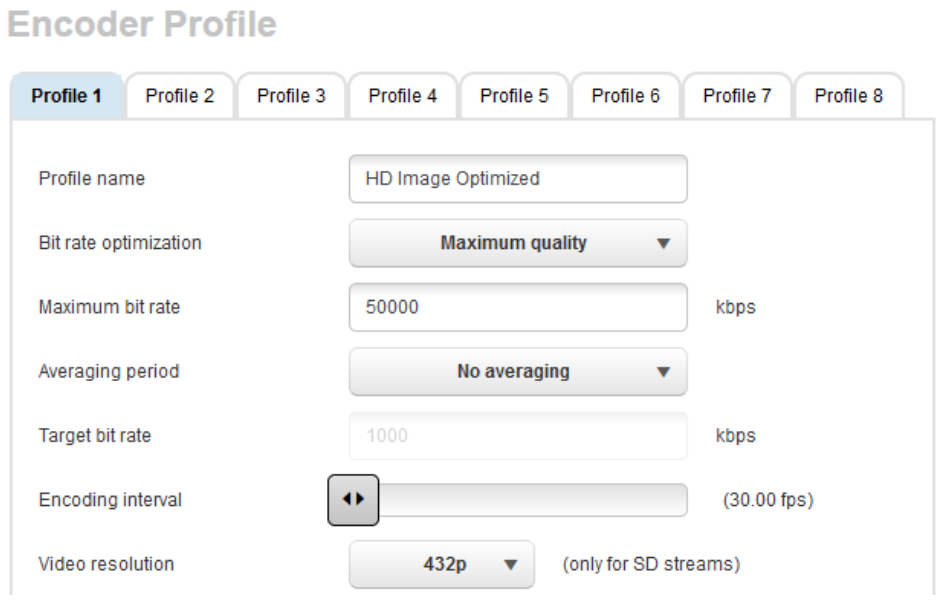
5.7 IP-kamera

Käytännön testiosuudessa käyttökokemuksen ja suorituskyvyn tutkimiseen käytettiin Bosch Flexidome 4000i -mallista IP-kameraa. Tämä kamera oli toimeksiantajan puolesta heti saatavilla ja käytettävissä tähän tutkimukseen. Kamera tukee 1080p-tyypin kuvantarkkuutta (kuvio 29), ja sen suurin kuvatiheys on 30 kuvaa sekunnissa.



Kuvio 29. IP-kameralta lähetettävä enkooderin kuvavirta

Kameran konfiguraatio tehtiin aikaisemman työkokemuksen perusteella siten, että se lähetti videota parhaalla mahdollisella laadulla ja kuvatiheydellä. Tämän lisäksi kameralle asetettiin kiinteä IP-osoite mobiilireitittimen lähiverkosta. IP-kameran asetukset ovat esitettyinä kuviossa 30.



Kuvio 30. IP-kameran enkooderiprofiili

5.8 Yhteenveto

Ensimmäinen testikonfiguraatio tehtiin käyttämällä Virve 2 Data -liittymää mobiilireitittimessä ja kiinteän verkon reititintä toimeksiantajan sisäisessä verkossa. Ensimmäisessä testauksessa kävi ilmi, että vaikka konfiguraatio toimi hyvin ja data liikkui VPN-tunnelia pitkin, ei kiinteän verkon liitynnän kapasiteetti soveltunut VPN-suorituskyvyn testaamiseen. Koska kapasiteettia ei lyhyessä ajassa ollut mahdollista kasvattaa, ei VPN-protokollien vertailua voitu suorittaa Virve 2 -liittymällä ja toimeksiantajan verkolla. Tämän johdosta testit suoritettiinkin tavallisella Elisan 5G-mobiililaajakaistaliittymällä sekä Telian kiinteällä laajakaistalla jonka nopeus oli 200 megabittiä sekunnissa.

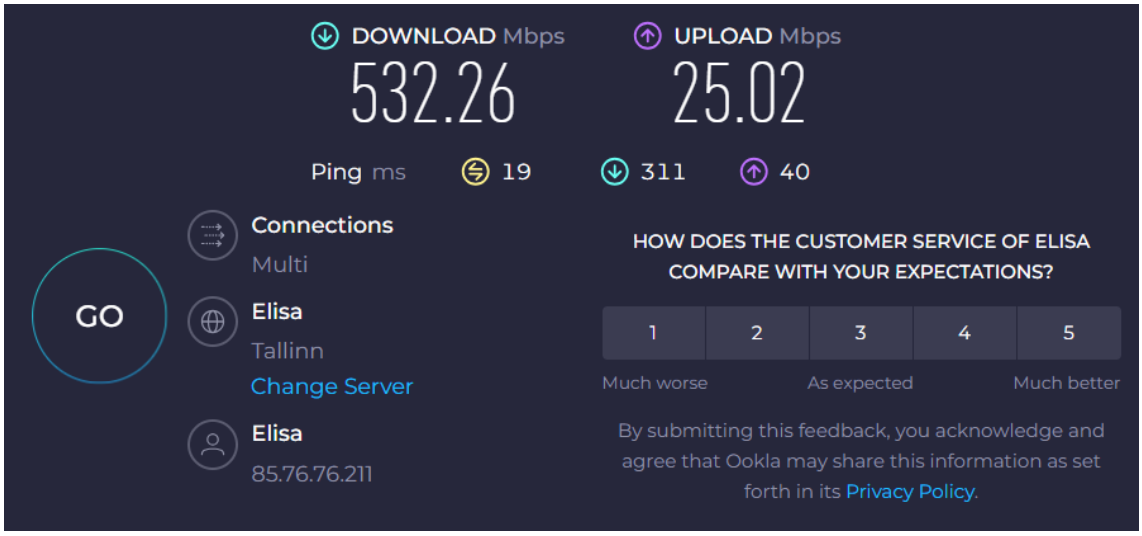
Ennen konfigurointia molemmat reitittimet päivitettiin uusimpaan saatavilla olevaan firmware-versioon. Mikrotik-reititin päivitettiin versioon 7.14.2 stable, ja Teltonika-reititin versioon R_00.07.06.6. Kaikkien eri protokollien konfiguraatiot saatiin tehtyä reitittimiin, ja tunnelit muodostuivat jokaisella kuten kuuluukin.

Testaus aloitettiin IKEv2/IPsec-protokollalla, ja testit saatiin vietyä läpi. OpenVPN-protokollan testauksessa ei tunnelin päissä olevien lähiverkkojen reititystä saatu toimimaan halutulla tavalla, vaikka konfiguraatiot tarkistettiin useaan otteeseen. Tämän johdosta testejä yritettiin tehdä sen sijaan WireGuard-protokollalla, sillä se oli tutkijalle ennestään tutuin ja sen toiminnan piti olla varmaa. Lähiverkkojen reititys ei kuitenkaan toiminut myöskään WireGuardilla, joten useiden muutosten ja tarkistusten jälkeen reitittimille tehtiin tehdasasetusten palautus. Tämän jälkeen kaikki konfiguraatiot tehtiin uudelleen, jotka tällä kertaa onnistuivat huomattavasti nopeammin kuin ensimmäisellä kerralla. Tämän jälkeen saatiin nopeasti myös todettua että nyt reititys toimii kuten pitääkin. OpenVPN- ja WireGuard-testit saatiin siten tehtyä onnistuneesti.

6 TESTAUS

6.1 Tekninen testi

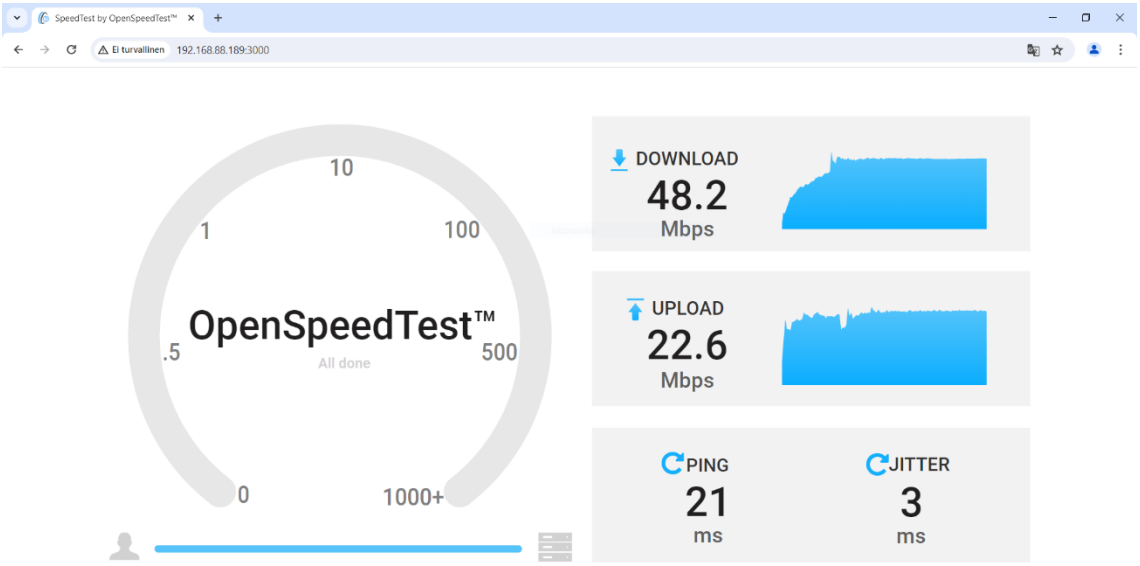
Teknistä testiä varten tarkistettiin ensin 5G-reitittimen nopeus internetin suuntaan. Download-nopeus alaspäin vaihteli välillä 300–500 megabittiä sekunnissa, ja upload-nopeus välillä 20–70 megabittiä sekunnissa. Kuvankaappaus Ooklan nopeustestauspalvelusta on esitettynä kuviossa 31. Varsinainen tekninen nopeustesti VPN-tunneleiden läpi tehtiin testipalvelimella olevia iperf3- ja OpenSpeedTest-sovelluksia vasten.



Kuvio 27. 5G-reitittimen internetnopeustesti (Ookla 2024)

6.1.1 IKEv2/IPsec

IKEv2/IPsec-tunnelin läpi tehdyissä mittauksissa OpenSpeedTest-palvelin antoi tulokseksi hieman alle 50 megabittiä sekunnissa (kuvio 32). Upload-nopeus oli noin 20 megabittiä sekunnissa.



Kuvio 28. IPsec-protokollan OpenSpeedTest-testitulos

Iperf3-mittauksessa tunnelin läpi saatiin keskimäärin tulokseksi noin 14 megabittiä sekunnissa (kuvio 33). Tämä on tuloksena huomattavasti pienempi kuin OpenSpeedTest-mittauksessa.

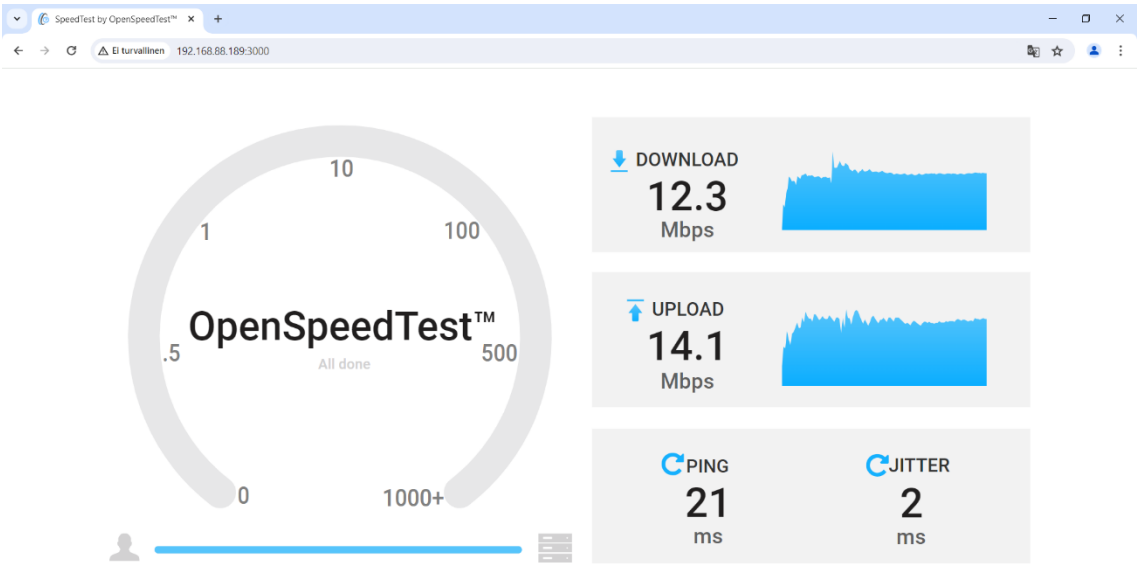
```
C:\Users\KK>iperf3 -c 192.168.88.189
Connecting to host 192.168.88.189, port 5201
[  4] local 192.168.75.194 port 51289 connected to 192.168.88.189 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.01   sec  1.62 MBytes  13.5 Mbits/sec
[  4]   1.01-2.01   sec  1.88 MBytes  15.7 Mbits/sec
[  4]   2.01-3.01   sec  1.88 MBytes  15.7 Mbits/sec
[  4]   3.01-4.01   sec  2.00 MBytes  16.9 Mbits/sec
[  4]   4.01-5.01   sec  1.50 MBytes  12.6 Mbits/sec
[  4]   5.01-6.01   sec  1.12 MBytes  9.43 Mbits/sec
[  4]   6.01-7.00   sec  1.50 MBytes  12.6 Mbits/sec
[  4]   7.00-8.00   sec  1.62 MBytes  13.6 Mbits/sec
[  4]   8.00-9.01   sec  1.88 MBytes  15.7 Mbits/sec
[  4]   9.01-10.01  sec  1.88 MBytes  15.7 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec  16.9 MBytes  14.1 Mbits/sec                  sender
[  4]   0.00-10.01  sec  16.8 MBytes  14.0 Mbits/sec                  receiver

iperf Done.
```

Kuvio 29. IPsec-protokollan iperf3-testitulos

6.1.2 OpenVPN

OpenVPN-tunnelin läpi mitattuna OpenSpeedTest-palvelimella mittaustulokset vaihtelivat suuresti välillä kymmenen ja neljäkymmentä megabittiä sekunnissa, ollen kuitenkin useimmin alle 20 megabittiä sekunnissa. (kuvio 34). Erikoisena

yksityiskohtana havaittiin se, että upload-nopeus oli usein suurempi kuin download-nopeus.



Kuvio 30. OpenVPN-protokollan OpenSpeedTest-testitulos

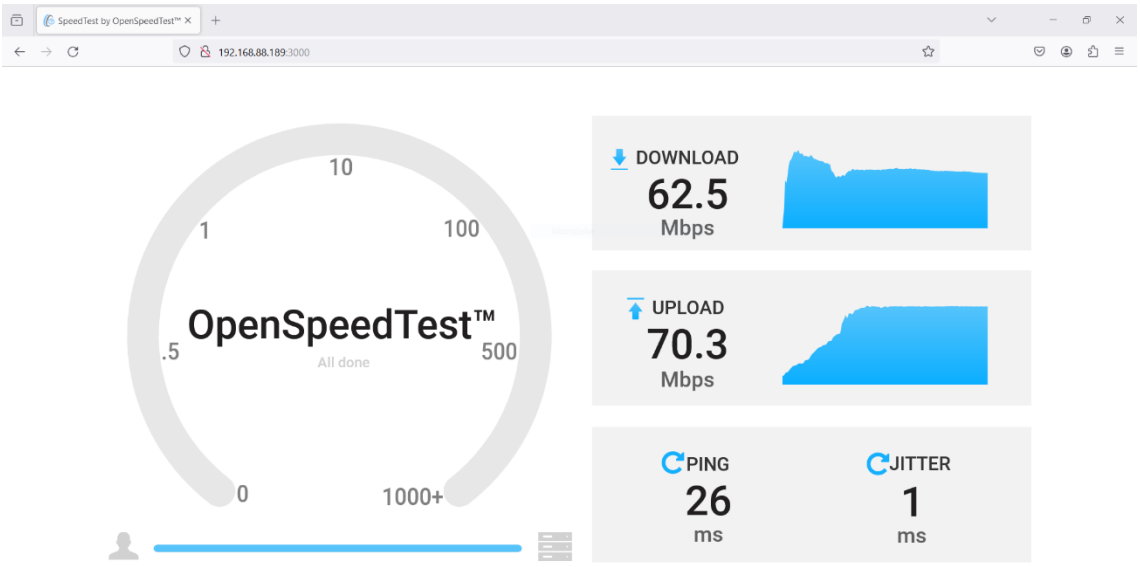
Iperf3-mittauksissa tuloksissa oli myös paljon vaihtelua. Tässäkin tapauksessa mittausarvot jäivät pienemmiksi kuin OpenSpeedTest-mittauksessa, jääden useimmiten nopeuteen hieman yli kymmenen megabittiä sekunnissa (kuvio 35).

```
C:\Users\KK>iperf3 -c 192.168.88.189
Connecting to host 192.168.88.189, port 5201
[  4] local 192.168.75.194 port 50026 connected to 192.168.88.189 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec  1.62 MBytes  13.6 Mbits/sec
[  4]   1.00-2.01   sec  2.00 MBytes  16.7 Mbits/sec
[  4]   2.01-3.01   sec  1.62 MBytes  13.6 Mbits/sec
[  4]   3.01-4.01   sec  1.75 MBytes  14.7 Mbits/sec
[  4]   4.01-5.01   sec  1.25 MBytes  10.4 Mbits/sec
[  4]   5.01-6.00   sec  1.12 MBytes  9.54 Mbits/sec
[  4]   6.00-7.00   sec  1.12 MBytes  9.45 Mbits/sec
[  4]   7.00-8.01   sec  1.00 MBytes  8.31 Mbits/sec
[  4]   8.01-9.00   sec  1.25 MBytes  10.6 Mbits/sec
[  4]   9.00-10.01  sec  1.38 MBytes  11.5 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec  14.1 MBytes  11.8 Mbits/sec                  sender
[  4]   0.00-10.01  sec  14.1 MBytes  11.8 Mbits/sec                  receiver

iperf Done.
```

Kuvio 31. OpenVPN-protokollan iperf3-testitulos

6.1.3 WireGuard

WireGuardin-tunnelin läpi molempien suuntien latausnopeus OpenSpeedTest-mittauksessa oli valituista protokollista selvästi suurin. Tulos oli keskimäärin noin 60 megabittiä sekunnissa (kuvio 36).



Kuvio 32. WireGuard-protokollan OpenSpeedtest-testitulos

Myös iperf3-mittauksessa tulos oli selvästi muita parempi, useimmiten hieman alle 20 megabittiä sekunnissa (kuvio 37). Tässäkin tapauksessa iperf3 antoi huomattavasti pienemmät latausnopeudet kuin OpenSpeedTest.

```
C:\Users\KK>iperf3 -c 192.168.88.189
Connecting to host 192.168.88.189, port 5201
[  4] local 192.168.75.194 port 50000 connected to 192.168.88.189 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.01   sec  2.12 MBytes  17.7 Mbits/sec
[  4]   1.01-2.01   sec  2.00 MBytes  16.8 Mbits/sec
[  4]   2.01-3.01   sec  2.50 MBytes  20.9 Mbits/sec
[  4]   3.01-4.01   sec  2.25 MBytes  19.0 Mbits/sec
[  4]   4.01-5.01   sec  2.12 MBytes  17.8 Mbits/sec
[  4]   5.01-6.01   sec  2.38 MBytes  20.0 Mbits/sec
[  4]   6.01-7.00   sec  2.25 MBytes  19.0 Mbits/sec
[  4]   7.00-8.00   sec  2.25 MBytes  18.9 Mbits/sec
[  4]   8.00-9.01   sec  2.25 MBytes  18.9 Mbits/sec
[  4]   9.01-10.01  sec  2.38 MBytes  19.9 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec  22.5 MBytes  18.9 Mbits/sec                  sender
[  4]   0.00-10.01  sec  22.4 MBytes  18.7 Mbits/sec                  receiver

iperf Done.
```

Kuvio 33. WireGuard-protokollan iperf3-testitulos

6.2 Käyttötapaustesti

Käyttötapaustestiä varten piti miettiä IP-kameran sijoitusta. Kamera asetettiin ensin kuvaamaan ikkunasta takapihaa, mutta koska siellä ei juurikaan ollut liikettä, niin kamera ei myöskään välittänyt paljon datavirtaa. Kamera asetettiinkin sitten TV:n eteen kuvaamaan Youtube-videota Tokion vilkkaista kaduista (4K World Wanderings 2023), joilla on jatkuvaa liikettä eri suuntiin. Tällä saatiin hyviä tuloksia kameran datavirrasta, ja näyte jokaisen protokollan suorituskyvystä otettiin kuvakaappauksena samasta kohtaa videota.

Valokuva testausasetelmasta on esitettynä kuviossa 38. Mitattavina arvoina käytettiin kameralta VMS-järjestelmään välittynyttä kuvatiheyttä ja bitrate-arvoa. VMS-järjestelmänä testissä käytettiin Synologyn verkkolevyasemalle asennettua Synology Surveillance Station -järjestelmää, jolla voitiin katsella ja tallentaa IP-kameroiden kuvia.

Kuvio 34. Käyttötapaustestin testausasetelma

6.2.1 IKEv2/IPsec

IKEv2/IPsec-tunnelin läpi kuva välittyi VMS-järjestelmään tasaisesti noin viidestä kahdeksaan kuvaa sekunnissa, bitrate-arvon ollessa hieman yli kymmenen megabittiä sekunnissa. Kuvaa katseltaessa tämä esiintyi erittäin nykivänä kuvana. IKEv2/IPsec-protokollan suorituskyky videokuvan siirrossa on esitettynä kuviossa 39.

Kuvio 35. IPsec-protokollan suorituskyky VMS-järjestelmässä

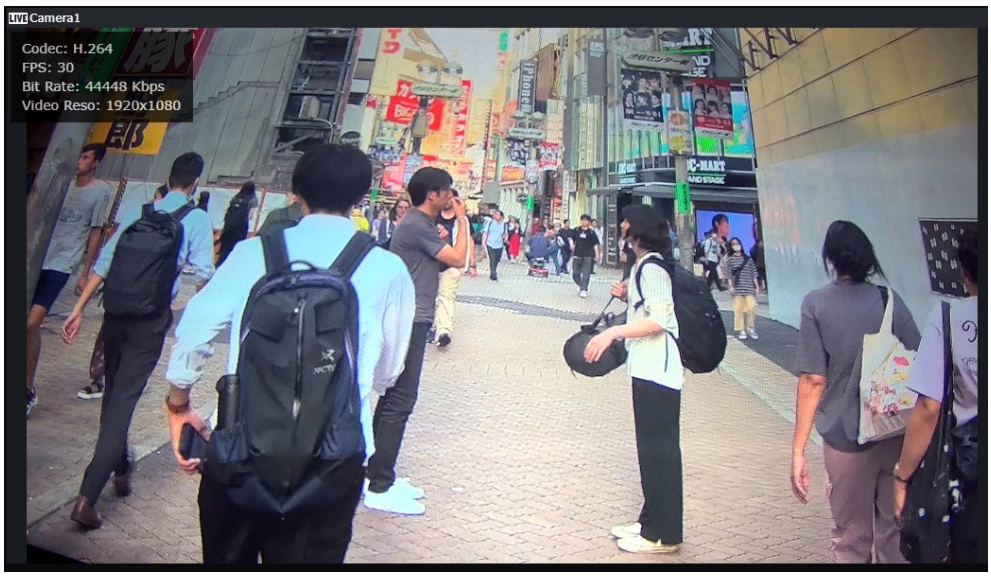
6.2.2 OpenVPN

Käytännön testiä suorittaessa oli havaittavissa huomattavaa heittelyä niin kuvatiheyden kuin bitrate-arvon kohdalla, kun videokuvaa lähetettiin OpenVPN-tunnelin läpi VMS-järjestelmään. Hetkittäin suorituskyky oli samaa tasoa IPsec-protokollan kanssa, mutta kuvatiheys heitteli yhden ja kymmenen välillä bitrate-arvon ollessa yhdestä viiteentoista megabittiä sekunnissa. Kuva näky VMS-järjestelmässä erittäin katkonaisena. OpenVPN-protokollan suorituskyky videokuvan siirrossa on esitettynä kuviossa 40.

Kuvio 36. OpenVPN-protokollan suorituskyky VMS-järjestelmässä

6.2.3 WireGuard

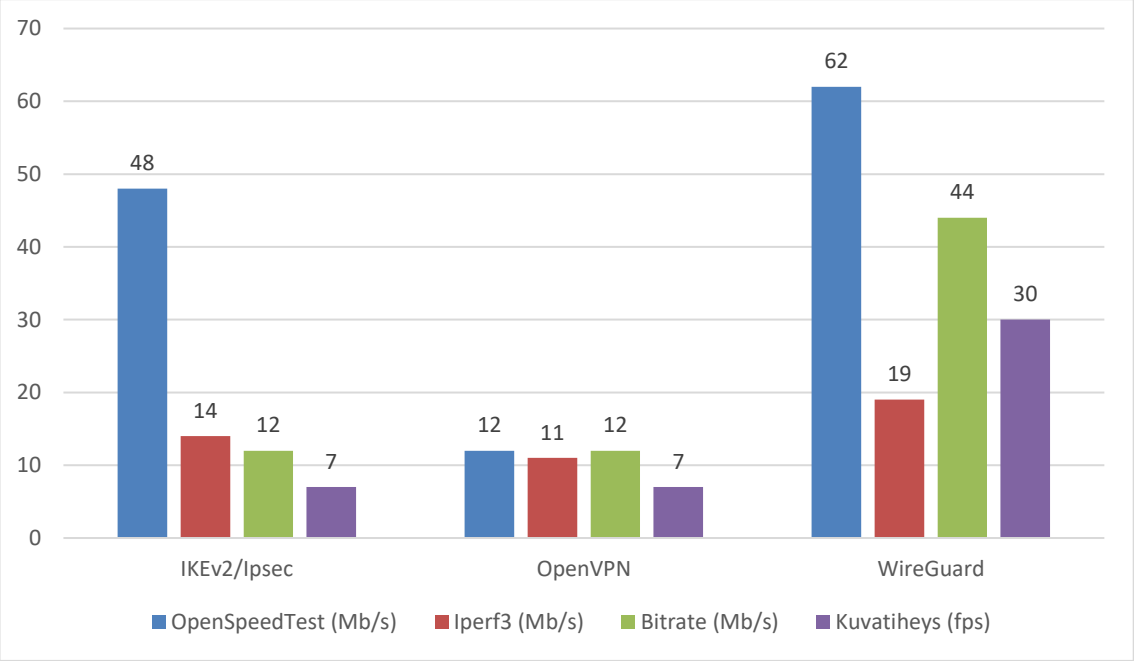
Wireguardin tunnelin läpi lähetetty videokuva siirtyi VMS-järjestelmään samalla kuvatiheydellä kuin kamera lähetti eli 30 kuvaa sekunnissa. Lähetyksen bitrate oli useita kymmeniä megabittejä sekunnissa ja tarkasteluhetkellä noin 44 megabittiä sekunnissa. Lähetetty videokuva näkyi siis VMS-järjestelmässä erittäin sulavasti. WireGuard-protokollan suorituskyky on esitettynä kuviossa 41.



Kuvio 37. WireGuard-protokollan suorituskyky VMS-järjestelmässä

6.3 Yhteenveto

Teknisissä testeissä ja käytännön testeissä saatiin hyvin esiin eroja protokollien suorituskyvyssä. Parhaiten suoriutui WireGuard, ja toiseksi parhaat tulokset tulivat IKEV2/IPsec-protokollaa käyttäen. OpenVPN ylsi keskimäärin samaan suorituskykyyn kuin IPsec, mutta sen tunnelin läpi kulkiessa datamäärässä ja kuvatiheydessä oli huomattavasti enemmän heittelyä tarkastelun aikana. Myös OpenSpeedTest-mittauksessa IPsec suoriutui huomattavasti OpenVPN-protokollaa paremmin. Molempien testien mittausten tulokset on esitetty yhtenä kokonaisuutena kuviossa 42.



Kuvio 38. VPN-protokollien suorituskykymittauksen tulosten vertailu

7 POHDINTA

Tässä opinnäytetyössä oli tarkoituksena vertailla kolmea suosittua ja eri menetelmillä toimivaa VPN-protokollaa ja niiden suorituskykyä pienitehoisilla reititinlaitteilla mobiiliyhteyden yli. Tavoitteena oli saada esiin havaittavia eroja protokollien suorituskyvyssä teknisessä mittaustestissä sekä opinnäytetyön käyttötapauksena olleen IP-kameran kuvan turvallista välittämistä havainnollistavassa käytännön testissä. Tässä työssä ei niinkään tutkittu eri protokollien tietoturvan tai salauksen tasoa, vaan tunnelit konfiguroitiin viranomaissuositusten mukaan niiltä osin mitä konfiguroitavissa oli. Huomioitavaa on myös se, että pelkkä VPN-yhteys ei itsessään takaa tietoturvaa missään käyttöympäristössä, vaan järjestelmän tietoturvallisuuteen vaikuttaa myös sen kaikkien muiden osa-alueiden toteutus.

Opinnäytetyön toiminnallisen osuuden valmisteluissa tuli yllättävän paljon viivästyksiä, kun käytettävien reititinlaitteiden toiminta piti ensin varmistaa opinnäytetyössä käytettäväksi suunnitellun Virve 2 -dataliittymän kanssa. Tämä johti siihen, että lisäviiveiden välttämiseksi toiminnallinen testausosuus suoritettiin käyttämällä kaupallisen operaattorin laajakaistaa sekä mobiilidataliittymää. Reititinlaitteiden konfigurointivaiheessa oli myös vaikeuksia saada VPN-tunneleita toimimaan halutulla tavalla verkkojen reitityksen suhteen. Tämä ongelma johtui luultavasti siitä, että kiinteässä verkossa käytetyn Mikrotik-reitittimen firmware-päivityksen jäljiltä reitittimeen oli jäänyt joitain virheellisiä asetuksia vanhasta konfiguraatiosta, sillä asia korjaantui palauttamalla reitin tehdasasetuksille ja tekemällä konfiguraatiot uudestaan.

Onnistuneiden konfigurointitöiden jälkeen testit saatiin suoritettua onnistuneesti, ja molemmissa testiosuuksissa saatiin esille hyvinkin huomattavia eroja VPN-protokollien suorituskyvyssä. WireGuard suoriutui molemmissa testitapauksissa protokollista parhaiten. Samanlaiseen lopputulokseen päätyivät myös Pudelko, Emmerich, Gallenmüller & Carle (2020) tutkimuksessaan juuri näiden samojen kolmen VPN-protokollan sopivuudesta suurikapasiteettisten 10–40 gigabittiä sekunnissa siirtävien verkkoyhteyksien salaamiseen. Vaikka heidän mukaansa yksikään protokollista ei suoraan sovellu näin suurien datamäärien salaukseen, on WireGuard kuitenkin suositeltavin protokolla käyttöönotettavaksi ja kehitettäväksi

sen modernin ja yksinkertaisen rakenteensa vuoksi. Vastaavaa vertailua olivat tehneet myös Phan Hai, Nguyen Hong, Quoc & Hoang (2021) ja päätyneet myös siihen, että WireGuard on näistä protokollista suorituskykyisin. He toivat myös esiin kuitenkin sen, että WireGuard ei ole protokollana kovin joustava, eikä sen tuki ja tunnettuus ole vielä kovin korkealla tasolla.

WireGuardille ei tosiaan ole juurikaan vielä esimerkiksi suuryritysten tarpeisiin skaalautuvia hallintaratkaisuita kuten vertailun muille protokollille. Tämän puutteen tuo artikkelissaan esiin myös Feiszli (2021), joka toteaa, että yritysten on vaikeaa ottaa WireGuardia käyttöön sen huonon tunnettuuden ja hallintaratkaisuiden puutteen vuoksi. Hän kuitenkin esittelee samalla tähän tarpeeseen vastaavan Netmaker-alustan, jolla voidaan hallita WireGuard-verkkoja. Parannusta asiaan on siis varmasti luvassa tulevaisuudessa.

Opinnäytetyölle asetetut tavoitteet saavutettiin onnistuneesti työn aikana, ja samalla kertyi paljon kokemusta eri protokollien VPN-tunneleiden muodostamisesta ja reititinlaitteiden hallinnasta. Työn tuloksien tulkinnassa on kuitenkin otettava huomioon se, että VPN-protokollia vertailtiin käyttämällä vain yhdenlaisia algoritmiyhdistelmiä ja algoritmeja vaihtamalla olisi voitu saada aikaan myös erilaisia tuloksia. Erityinen vaikutus on myös sillä, että niin tässä työssä käytetyistä, kuin suuresta osasta muistakin pienitehoisista verkkolaitteista puuttuu laitteistokiihdytystuki AES-GCM-salaukselle. Opinnäytetyöstä saadut tulokset joka tapauksessa huomioidaan toimeksiantajan tulevissa kehitysprojekteissa.

LÄHTEET

4K World Wanderings 2023. Tokyo walking tour – Walk the streets of Japan day & night | 4K HDR - 60fps. Viitattu 3.4.2024 https://www.youtube.com/watch?v=28ZjrtD_iL0.

Cho, J. Y., Sergeev, A., & Zou, J. 2020. Securing Ethernet-based Optical Fronthaul for 5G Network. Journal of Cyber Security and Mobility, 9(1), 91–110. Viitattu 25.3.2024 https://doi.org/10.13052/jcsm2245-1439.913.

Corcoran, L. & Jenkins, M. 2022. Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec). RFC 9206. Viitattu 25.3.2024 https://doi.org/10.17487/RFC9206.

Davis, J. 2023. SSTP VPN: Everything You'd Like to Know. Viitattu 25.3.2024 https://drfone.wondershare.com/vpn/sstp-vpn.html.

Donenfeld, J. A. 2020. WireGuard: Next Generation Kernel Network Tunnel. Viitattu 25.3.2024 https://www.wireguard.com/papers/wireguard.pdf.

Farag, H. 2017. CCNA-SEC Lec#7 | All about IPSec. Viitattu 25.3.2024 https://networkmasters.wordpress.com/2017/02/28/ccna-sec-lec7-all-about-ipsec/.

Feiszli, A. 2021. How to Deploy a Highly Available WireGuard® Network Management Server on Kubernetes. Viitattu 4.4.2024 https://itnext.io/how-to-deploy-a-highly-available-wireguard-network-management-server-on-kubernetes-294e23c7abcb.

Gillis, A. 2021. VPN (virtual private network). Viitattu 23.3.2024 https://www.techtarget.com/searchnetworking/definition/virtual-private-network.

Guéant, V. 2024. Download iPerf3 and original iPerf pre-compiled binaries. Viitattu 11.4.2024 https://iperf.fr/iperf-download.php.

IBM 2023. Security associations. Viitattu 25.3.2024 https://www.ibm.com/docs/en/aix/7.3?topic=overview-security-associations.

Kaufman, C., Hoffman, P., Nir, Y., Eronen, P. & Kivinen, T. 2014. Internet Key Exchange Protocol Version 2 (IKEv2). STD 79, RFC 7296. Viitattu 25.3.2024 https://doi.org/10.17487/RFC7296.

Kent, S. & Seo, K. 2005. Security Architecture for the Internet Protocol. RFC 4301. Viitattu 25.3.2024 https://doi.org/10.17487/RFC4301.

Kobeissi, N., Nicolas, G. & Bhargavan, K. 2019. Noise Explorer: Fully Automated Modeling and Verification for Arbitrary Noise Protocols. 2019 IEEE European Symposium on Security and Privacy (EuroS&P). Viitattu 25.3.2024 https://doi.ieeecomputersociety.org/10.1109/EuroSP.2019.00034.

Mash, S. 2022a. PPTP VPN-Protocol. Viitattu 25.3.2024 https://privacyhq.com/documentation/pptp-vpn-protocol/.

Mash, S. 2022b. L2TP VPN-Protocol. Viitattu 25.3.2024 https://privacyhq.com/documentation/l2tp-vpn-protocol/.

Mash, S. 2022c. SSTP VPN-Protocol. Viitattu 25.3.2024 https://privacyhq.com/documentation/sstp-vpn-protocol/.

McClure, M. 2021. IPSec vs OpenVPN: Cloud+ Encryption Technologies. Viitattu 11.4.2024 https://www.cbtnuggets.com/blog/certifications/cloud/ipsec-vs-openvpn-cloud-encryption-technologies.

Mendenhall, R. 2022. Steps for Selecting and Setting Up a Small Business VPN-Viitattu 6.4.2022 https://yarro.org/steps-for-selecting-and-setting-up-a-small-business-vpn/.

Microsoft 2012. VPN-Tunneling Protocols. Viitattu 25.3.2024 https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771298(v=ws.10).

Naby, S. A., Arslan, S. & Kim, H. 2017. IKE hardware engine based on CAM for concurrent processing of massive user sessions. 2017 13th International Computer Engineering Conference (ICENCO). Viitattu 25.3.2024 https://doi.org/10.1109/ICENCO.2017.8289780.

National Security Agency 2022. Announcing the Commercial National Security Algorithm Suite 2.0. Viitattu 25.3.2024 https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF.

Nir, Y. & Langley, A. 2018. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439. Viitattu 2.4.2024 https://www.rfc-editor.org/info/rfc8439.

Novickis, A. 2016. Protocol state fuzzing of an OpenVPN. Master thesis, Radboud Universiteit Nijmegen. Viitattu 25.3.2024 https://api.semanticscholar.org/CorpusID:34804460.

Ookla 2024. Speedtest. Viitattu 11.4.2024 https://www.speedtest.net/.

OpenSpeedTest 2024. OpenSpeedTest for Server (Docker Image & Source Code). Viitattu 11.4.2024 https://openspeedtest.com/selfhosted-speedtest#Source-Code-Docker.

OpenVPN 2024a. Expanding the scope of the VPN-to include additional machines on either the client or server subnet. Viitattu 2.4.2024 https://openvpn.net/community-resources/expanding-the-scope-of-the-vpn-to-include-additional-machines-on-either-the-client-or-server-subnet/.

OpenVPN 2024b. The History of OpenVPN. Viitattu 25.3.2024 https://openvpn.net/blog/the-history-of-openvpn/.

OpenVPN 2024c. OpenVPN cryptographic layer. Viitattu 25.3.2024 https://openvpn.net/community-resources/openvpn-cryptographic-layer/.

Palo Alto Networks 2024. What Is the History of VPN? Viitattu 11.4.2024 https://www.paloaltonetworks.com/cyberpedia/history-of-vpn.

Perrin, T. 2018. The Noise Protocol Framework. Viitattu 25.3.2024 http://www.noiseprotocol.org/noise.html.

Phan Hai, P. N., Nguyen Hong, H., Quoc B. B. & Hoang, T. 2021. A Comparative Research on VPN Technologies on Operating System for Routers. 2021 International Conference on Advanced Technologies for Communications (ATC). Viitattu 4.4.2024 https://doi.org/10.1109/ATC52653.2021.9598334.

Pudelko, M., Emmerich, P., Gallenmüller S. & Carle, G. 2020. Performance Analysis of VPN-Gateways. 2020 IFIP Networking Conference (Networking). Viitattu 4.4.2024 https://ieeexplore.ieee.org/document/9142755.

PyNetLabs 2024. What is GRE (Generic Routing Encapsulation) Protocol? Viitattu 25.3.2024 https://www.pynetlabs.com/generic-routing-encapsulation-protocol/.

Shbair, W. M., Cholez, T., Francois, J. & Chrisment, I. 2016. A multi-level framework to identify HTTPS services. NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium. Viitattu 25.3.2024 https://doi.org/10.1109/NOMS.2016.7502818.

SSL.com 2023. SSL/TLS Handshake: Ensuring Secure Online Interactions. Viitattu 11.4.2024 https://www.ssl.com/article/ssl-tls-handshake-ensuring-secure-online-interactions/.

Suomen Erillisverkot Oy 2024. Virve siirtyy uuteen teknologiaan 2020-luvulla. Viitattu 25.3.2024 https://www.erillisverkot.fi/virve2-0/.

Teltonika Networks 2023. Setting up an OpenVPN tunnel between Teltonika Neworks and Mikrotik devices. Viitattu 2.4.2024 https://wiki.teltonika-networks.com/view/Setting_up_an_OpenVPN_tunnel_between_Teltonika_Neworks_and_Mikrotik_devices.

Teltonika Networks 2024. IPsec RUTOS configuration example. Viitattu 2.4.2024 https://wiki.teltonika-networks.com/view/IPsec_RUTOS_configuration_example.

Traefik Labs 2024. Network Tunneling: What Is It and How Is It Used? Viitattu 25.3.2024 https://traefik.io/glossary/network-tunneling/.

Van Den Berg, J.2022a. Easy IPSEC Site-To-Site VPN-Guide, MikroTik ROSv7. Viitattu 2.4.2024 https://www.youtube.com/watch?v=uVag_e475zc.

Van Den Berg, J.2022b. Ultimate MikroTik Wireguard Site-to-Site Guide. Viitattu 2.4.2024 https://www.youtube.com/watch?v=P6f8Qc4EItc.

Vaughan-Nichols, S. J. 2021. But why that VPN? How WireGuard made it into Linux. Viitattu 25.3.2024 https://www.theregister.com/2021/12/08/wireguard_linux/.

VyprVPN 2023. What are the security parameters for OpenVPN? Viitattu 25.3.2024 https://support.vyprvpn.com/hc/en-us/articles/360037728512-What-are-the-security-parameters-for-OpenVPN.

WireGuard 2024. Protocol & Cryptography. Viitattu 25.3.2024 https://www.wireguard.com/protocol/.

Zahorski, A. 2022. How VPNs Have Shaped the Internet Over the Years. Viitattu 25.3.2024 https://www.makeuseof.com/how-vpns-shaped-internet/.