VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Nima Razi & Samuli Snellman

VIRTUAALINEN ERILLISVERKKO

Liiketalous
2022

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijät	Nima Razi & Samuli Snellman
Opinnäytetyön nimi	Virtuaalinen erillisverkko
Vuosi	2022
Kieli	Suomi
Sivumäärä	71
Ohjaaja	Antti Mäkitalo

Tämän opinnäytetyön tarkoituksena on tutkia virtuaalista erillisverkkoa yleisesti ja tuoda esille sen hyödyllisiä ja haitallisia puolia, sekä myös kritiikkiä. Asiaa käsitellään niin kulutus- kuin yritysmaailman näkökulmasta, VPN:n taustaa, teknistä puolta, käyttöä COVID-19-pandemian aikana, sekä myös tulevaisuutta.

Tutkimme opinnäytetyötä tehdessämme verkkoartikkeleita ja blogeja. Hyödynnämme työssä myös kuvia ja kaavioita kyseisten verkkomateriaalien pohjilta. Työssä ei käytetty lainkaan fyysisiä materiaaleja, koska määrällisesti kirjallisuutta oli hyvin vähän tai ne saattavat sisältää vanhaa tietoa.

Tuloksena syntyi kattava tutkimustyö virtuaalisen erillisverkon eri osa-alueista, jonka uskomme hyödyttävän asiasta kiinnostuneita henkilöitä. Tuotimme mahdollisimman neutraalin näkökulman aiheesta, emmekä ole myös muuttaneet kantaamme.

Avainsanat VPN, Tutkimustyö, COVID-19, Kuluttaja, Yritys, Tulevaisuus

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Business Information Technology

ABSTRACT

Author	Nima Razi & Samuli Snellman
Title	Virtual private network
Year	2022
Language	Finnish
Pages	71
Name of Supervisor	Antti Mäkitalo

The purpose of this thesis is to widely examine virtual private networks, bring up their pros and cons and its criticism. The subject will be handled from consumers and business worlds point of view, background of VPN, technical parts, its usage during COVID-19 pandemic and its future.

During production of the thesis, we examined web articles and blogs. In this work, we also make use of images and graphs acquired from the said network sources. Physical copies weren't used at all, because the amount of literature was small or it contained expired information.

A comprehensive research work was created as a result for different sections of virtual private networks, which we believe will benefit anyone who's interested of the subject. We produced most neutral point of view as possible about the subject, and we haven't changed our stance.

Keywords VPN, Research, COVID-19, Consumer, Company, Future

SISÄLLYS

KUVA- ja TAULUKKOLUETTELO

SANASTO

2FA	Kaksivaiheinen todennus on turvallisuuskäytäntö, mikä vaatii käyttäjältä kaksi erilaista vaihetta tunnistautumista varten.
AES-256	Suojusmenetelmä, missä käytetään 256-bittistä avainta.
Adblocker	Ohjelma, millä voidaan estää mainoksia web-sivustoilla.
ARPANET	Pakettikytkentäinen tietokoneverkko.
DDoS	Palvelinestohyökkäys, missä sivuston palvelin kuormitetaan suurella märällä liikennettä.
DD-WRT	Laiteohjelmisto reitittimille ja tukiasemille.
DMZ	Demilitarisoitu vyöhyke.
DMVPN	Ciscon kehittämä dynaaminen monipisteiden virtuaalinen erillisverkko.
DNS	Muuttaa verkkotunnuksia IP-osoitteeksi.
Echelon	NSA:n johtamana toimiva sähköinen valvontajärjestelmä, mihin kuuluu läntisiä maita.
Flashing	Päivitysmenetelmä, missä käyttäjä päivittää laitteensa BIOS:n kautta ohjelmistoa.
GUI	Graafinen käyttöliittymä viittaa teksteihin kuviin ja muihin erilaisiin elementteihin, millä voi hallinnoida tietokoneita.
IKEv2	IPsec-pohjainen tunnelointiprotokolla.
IoT	Esineiden Internet.
IPsec	Internet-turvallisuusprotokolla.
ISP	Internet-palveluntarjoaja.

JavaScript	Ohjelmointikieli.
Kill switch	Pysäytyskytkin toiminto, löytyy useimmista VPN-ohjelmistoista.
L2TP&L2TP/IPsec	2-kerroksen tunnelointiprotokolla, jossa tarvitaan mukana Internet Protocol Securityä, koska L2TP ei itsessään tarjoa vahvaa salausta eikä todentamista.
Linux	Käyttöjärjestelmä mitä käytetään eri teknisissä laitteissa.
MFA	Todennustapa, missä käyttäjä hakee pääsyä tiettyyn sisältöön kahden tai useamman todennusmekanismin kautta.
Mesh-laitteisto	Yhdestä tai useammasta verkkolaitteesta koostuva WiFi-verkko.
NAT	Osoitteenmuunnos.
OpenVPN	Avoimen lähdekoodin teknologia.
Obfuskaatio	Teknologia, mikä peittää verkkoliikennettä esimerkiksi Internet-palveluntarjoajalta.
P2P	Vertaisverkko, eli verkko missä jokainen verkkoa käyttävä laite toimii sekä palvelimena että asiakkaana muille käyttäjille.
PfSense	Reititin- ja palomuurikäyttöjärjestelmä.
Proxy	Välityspalvelin, säilöö ja suodattaa verkonsiirrossa käytettäviä tiedostoja.
SaaS	Ohjelmiston tarjontaan palveluna asiakkaalle Internetin välityksellä.
Script	Komentokieli, millä voi suorittaa erilaisia tehtäviä järjestelmissä.
SDP	Ohjelmiston määrittämä kehä.
SSH	Tunnelointiprotokolla.

SSL/TLS	Salausprotokolla.
SSTP	Microsoftin kehittämä VPN-protokolla.
swIPe	Ensimmäinen versio nykyaikaisesta virtuaalisista erillisverkoista.
TCP/IP	Tietoliikenneprotokollan yhdistelmä.
WAN	Laajaverkko, mikä kattaa verkkoyhteydellään suuria maantieteellisiä alueita.
Widget	Pienoisohjelma tietylle sovellukselle, mikä on näkyvillä laitteen alkuvalikossa.
VPN	Virtuaalinen erillisverkko.
VPN-Concentrator	Liittää useita laitteita yhteen verkkoympäristöön VPN:ä hyödyntäen.
VyOS	Avoimen lähdekoodin verkkokäyttöjärjestelmä, joka perustuu Debianiin.
X86	Suoritinarkkitehtuuri, mitä käytetään useissa nykykoneissa.
Zero-trust model	Nollaluottamusmalli, joka on tietoturvakehys.

1 JOHDANTO

Tämä opinnäytetyö keskittyy VPN:n eli virtuaalisen erillisverkon tarkasteluun yleisestä näkökulmasta. Työssä otetaan huomioon muun muassa kyseisen teknologian keskeisimmät toimintatavat, hyödyt ja haitat. Lisäksi opinnäytetyössä käydään läpi virtuaalista erillisverkkoa kuluttaja- sekä yritysympäristössä, VPN-teknologian eri osa-alueita, COVID-19 pandemian vaikutukset etätyöskentelyn aikana liittyen virtuaalisen erillisverkon kasvukehitykseen, sekä miltä VPN:n tulevaisuus tulee näyttämään.

Työssä käytetään lähdemateriaalina verkosta löytyneitä artikkeleita ja blogeja. Kuvat sekä kaaviot, joita työssä käytetään ovat tuotu verkosta tai tehty työn kirjoittajien toimesta. Fyysisiä kopioita, esimerkiksi kirjoja tai lehtiä liittyen kyseiseen aihepiiriin on vaikeasti löydettävissä tai niiden sisältämä materiaali on vanhentunutta.

Tavoitteena on kehittää kattava työ, joka avaa virtuaalisen erillisverkon perusasioita, nykyistä toimintaa, sekä tulevaisuuden näkökulmia. Lisäksi VPN:n toimintaa käydään läpi kuluttajien, sekä yritysten näkökulmista. Työssä otetaan huomioon, että aihetta lähestytään mahdollisimman neutraalista näkökulmasta. Tarkoituksena on, että lukija pystyy helposti sisäistämään työssä käydyt aihepiirit ja tämän pohjalta muodostamaan oman mielipiteensä: kokeeko hän VPN:n käytännöllisenä ja turvallisena vaihtoehtona oman verkkoanonyymiytensä suojaamiseksi vai pärjääkö hän ilman sellaista. Tarkoituksena on luoda kokonaisvaltainen katselmus virtuaalisesta erillisverkosta.

2 MIKÄ ON VPN, SEN HISTORIA JA NYKYTILANNE

VPN (Virtual Private Network) eli suomeksi virtuaalinen erillisverkko, jonka tarkoituksena on muodostaa käyttäjälleen suojattu verkkoyhteys julkiseen verkkoliikenteeseen. VPN-yhteydet siis salaavat käyttäjänsä Internet-liikenteen sekä piilottavat käyttäjänsä oikean identiteetin verkkoliikenteessä. Näiden toimintojen vuoksi kolmansien osapuolten on haastavampaa päästä käsiksi VPN-käyttäjän verkossa tapahtuviin toimintoihin sekä varastaa tietoja, sillä tämä salaus tapahtuu aina reaaliajassa. (Kaspersky 2021.)

Virtuaalinen erillisverkon toiminta perustuu siihen, että se ohjaa verkkoliikenteen erityisesti konfiguroidun etäpalvelimen läpi, jota VPN-isäntä ylläpitää, tämän avulla käyttäjän oikea IP-osoite salataan. Tämä tarkoittaa sitä, että aina kun käyttäjä käyttää VPN-yhteyttä esimerkiksi selatessa Internettiä, niin tietosisällön lähteenä toimii virtuaalinen erillisverkko, joka puolestaan merkitsee sitä, että käyttäjän Internetpalveluntarjoaja (ISP) sekä kaikki muut ulkopuoliset tahot eivät pysty seuraamaan, millä sivustoilla käyttäjä käy ja millaista dataa hän lähettää sekä vastaanottaa verkossa. Virtuaalista erillisverkkoa voidaankin kutsua suodattimeksi, joka muuttaa käyttäjänsä datan täysin lukukelvottamaksi ja jos joku taho pääsisikin käsiksi tähän dataan, niin olisi se tälle hyödytöntä. (Kaspersky 2021.)

2.1 Historia

Internetin alkuajoista lähtien on pyritty suojaamaan sekä salaamaan selaustietoja, jo 1960-luvulla Yhdysvaltain puolustusministeriö oli tekemisissä projekteissa, jossa Internet-tietoyhteyksiä pyrittiin salaamaan. VPN oli pohjimmiltaan armeijakäyttöön suunniteltua teknologiaa, millä salattiin valtion arkaluonteista sisältöä viestinnässä. Kyseisen teknologian kehittäminen siihen aikaan on selitettävissä kylmän sodan aiheuttaman asevarustelun vaikutuksesta. Kuluttajakäyttöön siirtyminen vei kuitenkin aikaa. (Kaspersky 2021.)

2.2 VPN-verkkojen edeltäjät

Yhdysvaltojen puolustusministeriön lanseeraamalla projektilla luotiin ARPANET eli (Advanced Research Projects Agency Network), joka on siis pakettikytkentäinen tietokoneverkko, josta myöhemmin jatkokehitettiin TCP/IP-protokolla eli (Transmission Control Protocol/Internet Protocol). (Kaspersky 2021.)

TCP/IP sisältää neljä eri kerrosta, jotka ovat linkki, Internet, siirto sekä sovellus. Paikalliset verkot sekä laitteet pystytään yhdistämään yleiseen verkkoon Internet-kerroksessa, mutta juuri tässä kohtaan piilee riski tietojen paljastumisesta. Vuonna 1993 AT&T Bell Labs:sta sekä Columbian yliopistosta koostuva tiimi sai lopulta kehitettyä ensimmäisen version nykyaikaisesta VPN:stä. Tämä tunnetaan nimellä swIPe eli (Software IP encryption protocol). (Kaspersky 2021.)

Vuonna 1994 Wei Xu kehitti IPsec-verkon eli (IP Security Architecture), joka on Internet-turvallisuusprotokolla, jonka avulla todennetaan sekä salataan verkon välityksellä jaetut tietopaketit. Microsoftin työntekijä Gurdeep Singh-Pall loi vuonna 1996 PPTP-protokollan eli (Point to Point Tunneling Protocol). (Kaspersky 2021.)

2.3 Varhaiset VPN:t

Internetin suosio oli kasvussa sekä myös kuluttajille suunnattujen suojausjärjestelmien kysyntä kasvoi, kun Singh-Pall kehitteli kyseistä PPTP-protokollaa. Virustorjuntaohjelmistot olivat jo niihin aikoihin tehokkaita työkaluja torjumaan haittaohjelmia sekä suojaamaan tietokonejärjestelmiä vakoiluohjelmilta. Internetselaushistoriansa piilottaville salaustavoille alkoi kuitenkin olla kysyntää yritysten sekä kuluttajien keskuudessa. (Kaspersky 2021.)

Ensimmäiset VPN-ohjelmistot julkaistiin 2000-luvun alussa, mutta suurin osa näistä oli vain yrityksille suunnattuja, mutta etenkin 2010-luvun lukuisten tietomurto tapausten jälkeen VPN-verkkojen kuluttajamarkkinat aloittivat kasvun. (Kaspersky 2021.)

2.4 VPN:t ja niiden nykyinen käyttö

GlobalWebIndexin mukaan virtuaalista erillisverkkoa käyttävien ihmisten määrä kasvoi yli nelinkertaisiksi vuosien 2016 sekä 2018 välillä. Indonesian, Kiinan sekä Thaimaan kaltaisissa maissa, Internetin käyttämistä rajoitetaan sekä sensuroidaan. Näissä maissa jopa yksi viidestä Internettiä käyttävästä henkilöstä käyttää virtuaalista erillisverkkoa, kun taas Isossa-Britanniassa, Saksassa sekä Yhdysvalloissa virtuaalisen erillisverkkoa käyttävien henkilöiden osuus on pienempi eli noin 5 prosenttia, mutta myös näissä maissa käyttäjien määrä lisääntyy. (Kaspersky 2021.)

Virtuaalisen erillisverkon käyttöä on lisännyt viime vuosina huomattavasti kuluttajien tarve päästä käsiksi maantieteellisesti rajoitettuihin sisältöihin, kuten esimerkiksi Netflixin sekä YouTuben kaltaisissa videostriimauspalveluissa, joissa osa sisällöstä on asetettu nähtäväksi vain tietyn maan/alueen käyttäjille. Nykyaikaisia VPN-verkkoja käyttämällä käyttäjä pystyy salamaan oman IP-osoitteensa siten, että siitä syntyy vaikutelma, jossa käyttäjä selaisikin Internettiä jossain toisessa maassa, näin ollen käyttäjä voi käyttää rajoitettua sisältöä mielensä mukaan. (Kaspersky 2021.)

3 MIKSI VPN KANNATTAA HANKKIA

Käyttäjän Internet-palveluntarjoaja määrittelee normaalisti asetukset, kun Internettiin muodostetaan yhteys. Se pystyy seuraamaan käyttäjäänsä IP-osoitteen välityksellä, näin käyttäjän verkkoliikenne reititetään palvelimelle, joka kuuluu Internet-palveluntarjoajalle. Nämä kyseiset palvelimet pystyvät kirjaamaan ylös sekä tarkkailemaan kaikkea, mitä käyttäjä kulloinkin verkossa tekee. (Kaspersky 2021.)

Vaikka käyttäjän Internet-palvelutarjoaja saattaisikin vaikuttaa luotettavalta, niin silti se voi jakaa käyttäjänsä selaushistorian mainostajille, poliisille tai muulle viranomaiselle sekä muille kolmansille osapuolille. Lisäksi Internet-palveluntarjoajat saattavat joutua kyberrikosten kohteiksi, esimerkiksi jos heidän palvelunsa hakkeroitaisiin, niin käyttäjän yksityiset sekä henkilökohtaiset tiedot voisivat pahimmassa tapauksessa paljastua näille rikollisille. Tällainen uhka on suurempi, jos käyttäjä käyttää toistuvasti avoimia Wi-Fi-verkkoja, tällöin käyttäjä ei voi koskaan tietää, kuka tai mikä taho saattaisi valvoa Internet-liikennettä ja he saattaisivat varastaa käyttäjän tietämättä, esimerkiksi käyttäjän dataa, maksutietoja, salasanoja tai jopa käyttäjän koko henkilöllisyyden. (Kaspersky 2021.)

3.1 Hyvän VPN:n tunnusmerkit

Kun puhutaan hyvästä VPN:stä, niin tämän pitäisi kyetä huolehtimaan erityisen tärkeistä tehtävistä. Edellyttäen myös, että VPN:n on itsessään suojattu murtoja vastaan. Käyttäjän tulisikin kiinnittää huomio seuraaviin ominaisuuksiin, jotka kattava VPN-ratkaisu tulisi pitää sisällään. (Kaspersky 2021.)

IP-osoitteen salaus: Virtuaalisen erillisverkon ensisijaisena tehtävänä on piilottaa käyttäjänsä IP-osoite Internet-palveluntarjoajalta sekä myös kaikilta muilta kolmansilta tahoilta. Tämän toiminnon avulla käyttäjä voi sekä lähettää, että vastaanottaa tietoja verkossa ilman, että kukaan ulkopuolinen pääsisi näkemään näitä tietoja. (Kaspersky 2021.)

Salatut protokollat: Virtuaalisen erillisverkon tulisi kyetä estämään jälkien jättäminen muun muassa evästeiden sekä selaus- ja hakuhistorian muodossa. Erityisesti evästeiden piilottaminen on tärkeää, koska tämä toiminto estää ulkopuolisia toimijoita pääsemästä käsiksi luottamuksellisiin tietoihin, kuten muun muassa yksityiseen dataan, maksutietoihin sekä muihin verkkosivustojen sisältöihin. (Kaspersky 2021.)

Pysäytyskytkin toiminto eli (ns. kill switch): Jos käyttäjän käyttämä virtuaalinen erillisverkkoyhteys katkeaisi aivan yllättäen, niin tällöin myös suojattu yhteys katkeaisi. Kunnollinen VPN pystyy tunnistamaan tällaiset yllättävät katkeamiset ja pysäyttää entuudestaan määritetyt ohjelmat. Tämä toiminto vähentää riskiä datan salaamisen pettämisestä. (Kaspersky 2021.)

Kaksivaiheinen todennus eli (2FA): Hyvä VPN kykenee tarkistamaan kaikki sisäänkirjautumisyritykset hyödyntämällä useita erilaisia todennustapoja. Käyttäjää voidaan muun muassa pyytää antamaan salasana, jonka jälkeen käyttäjä saa koodin tekstiviestinä mobiililaitteeseensa, tällä tavalla vaikeutetaan ulkopuolisia osapuolia pääsemästä käsiksi suojattuun yhteyteen. (Kaspersky 2021.)

3.2 Välityspalvelin vai VPN?

Puhuttaessa etäyhteyksistä, VPN:n lisäksi vastaan tulee Proxy-Server eli välityspalvelin. Proxyn toiminta muistuttaa VPN:ä. Se toimii käyttäjän ja Internetin välissä, sekä sen tarkoituksena on suojata yksityisyyttä. Välityspalvelimen käytöllä on kuitenkin omat haittansa. (Hodges 2020.)

Välityspalvelin toimii siten, että se ohjaa käyttäjän laitteelta tulevan liikenteen itseensä, mistä se vie sen varsinaiselle web-sivulle. Samoin myös toisin päin: websivulta tuleva liikenne ohjautuu välityspalvelimeen ja sen jälkeen vasta käyttäjälle. Se tuo myös suojaa muuttaen käyttäjän IP-osoitteen yksityisyyden turvaamiseksi. VPN:n tavoin välityspalvelimella pystyy ohittamaan maantieteelliset estot, sekä mahdollisesti parantaa kaistanopeutta. (Hodges 2020.)

Välityspalvelin tallentaa tietoa myös välimuistin tavoin: se säilyttää nettisivujen tiedot ja tuo ne käyttöön, kun sama tai joku muu käyttäjä vierailee kyseisellä sivulla säästäen turhaa aikaa ja kaistaa. (Klimas 2021.) Välityspalvelimille voidaan myös asettaa estoja tietyille sivustoille. Tämä on hyödyllistä, esimerkiksi työpaikoilla tai lasten verkonkäytön rajaamisessa. Se toimii myös palomuurina eri hyökkäyksiä vastaan. (Hodges 2020.)

Suurin osa välityspalvelimista ei salaa verkkoliikennettä, minkä seurauksen käyttäjän IP-osoite ei myöskään pysy täysin piilossa. Välityspalvelimen omistaja pystyy näkemään sen käyttäjien toiminnan. Sama yksityisyysongelma kohtaa vastaan torrent-sivustoilla: itse sivustolle pääsee, mutta torrenttien käyttö ei ole turvattua. Verkon nopeuden kasvu ei ole myöskään täysin taattua. Välityspalvelin pystyy kyllä tarjoamaan nopeammat yhteydet tietylle sivulle, mutta vain jos käyttäjä on jo aiemmin vieraillut siellä. Sivustojen suorituskyky voi olla myös niin minimaalista, ettei käyttäjä sitä huomaa. (Kataja 2017.)

Vaikka välityspalvelimen ja VPN:n toiminnat muistuttavat toisiaan, ne eivät ole täysin sama asia. Välityspalvelin suojaa käyttäjiä vain vähän, kun taas VPN tuottaa suojaa pisteestä pisteeseen yksityisyyttä kohtaan. Tämä ei kuitenkaan tarkoita, etteikö välityspalvelin olisi täysin ohitettava vaihtoehto. Ne ovat helpoin tapa ohittaa maantieteelliset estot, sekä toimia osana esimerkiksi yrityksen tietoturvaa. Välityspalvelimen tarjonta on kuitenkin loppujen lopuksi huonompi kuin VPN:llä, minkä vuoksi VPN:n käyttö on niin suosittua. (Kataja 2017.)

4 VPN ERI KÄYTTÖÖNOTTOTAVAT

Virtuaalisen erillisverkon asentamisessa on useita erilaisia tapoja, joihin kannattaa tutustua aina ennen sen käyttöönottoa. Käyttöönottotavat ja menetelmät voitaisiin jakaa kuluttaja- sekä yrityspuolen omiin kategorioihin ja osiin. Kuluttajapuolella keskitytään helppokäyttöisyyteen, kun taas yrityspuolella kohteena olevat suuret organisaatiot ja ylläpito vaatii enemmän monimuotoisuutta. Lisäksi on myös olemassa niin sanottuja vähemmän käyttäjäystävällisiä menetelmiä, mutta hankaluuden vuoksi niiden käyttö on todennäköisesti hyvin vähäistä.

4.1 VPN-asiakasohjelmistot

VPN-asiakkaita varten on kehitetty erillisiä asennettavia ohjelmistoja, jossa ohjelmisto tarkoin määritetään vastaamaan päätepisteen asettamia edellytyksiä. VPN-ohjelmistoa asennettaessa, päätepisteiden välille luodaan yhteys muodostaen salaustunnelin. Mikäli kyseessä olisi yritys, niin tässä tapauksessa yleensä annetaan yritykseltä saatu salasana tai käyttäjän olisi asennettava sille määritetty varmenne. Salasanaa tai varmennetta käyttäen, palomuuri voi todentaa yhteyden olevan sallittu yhteys, tämän jälkeen työntekijä tunnistautuu saatujen tunnistetietojen avulla. (Kaspersky 2021.)

Kuva 1. Esimerkki VPN-asiakasohjelmistoista (Ruutukaappaus työpöydältä)

Kuvassa 1 näkyy suomalaisen F-Securen kehittämä VPN-asiakasohjelmisto FREEDOME.

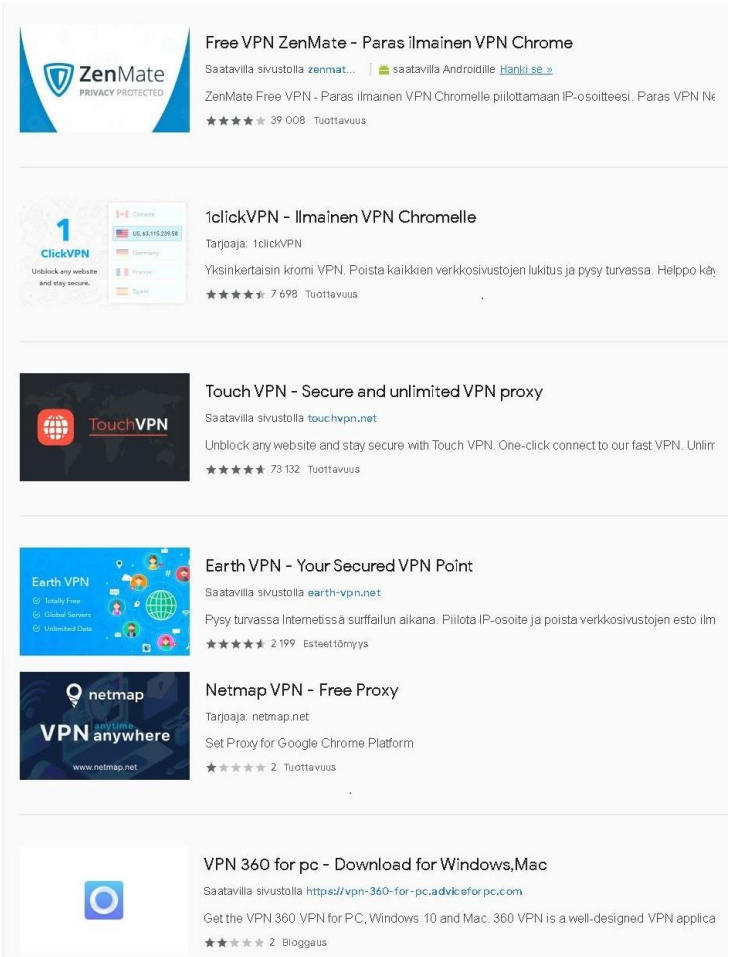
4.2 VPN-selainlaajennukset

Erilaisia VPN-selainlaajennuksia voidaan lisäillä moniin verkkoselaimiin, kuten esimerkiksi Google Chromeen tai Mozilla Firefoxiin. Joissakin selaimissa, on omat integroidut VPN-laajennukset Opera on yksi tällaisista selaimista. Käyttäjät pystyvät laajennusten avulla vaihtamaan hetkessä VPN-yhteyttä sekä tehdä tähän liittyviä määrityksiä samalla, kun käyttävät Internettiä. Selainpohjainen VPN-yhteys on käytettävissä vain selaimessa jaetuille tiedoille, jos käyttäjä käyttää muita selaimia tai esimerkiksi pelaa pelejä salaaminen selaimessa toimivalla VPN:llä ei olisi mahdollista. (Kaspersky 2021.)

Selainpohjaiset virtuaaliset erillisverkkoratkaisut eivät olekaan aivan yhtä laajoja kuin VPN-asiakasohjelmistot, mutta siitä huolimatta ne voivat olla riittävän hyviä ratkaisuja satunnaisesti Internetistä vieraileville käyttäjille, koska VPN-selainlaajennukset lisäävät Internet-suojauksen tasoa. Siltikin niiden käyttäjät ovat alttiimpia erilaisille murroille, koska erilaiset tietojen louhijat voivat yrittää käyttää VPN-

nimeä houkutuksena, siksi käyttäjiä suositellaankin lataamaan jokin hyvämaineinen laajennus. (Kaspersky 2021.)

Tätä aihetta kirjoittaessamme huomasimme, kuinka paljon erilaisia VPN-selainlaajennuksia esimerkiksi Google Chrome Web Store -kaupasta voi ladata. Käyttäjä joka ei kiinnitä huomiota laajennuksen alkuperään tai laatuun voi joutua helposti huonon tahon uhriksi. Tällaisten laajennuksien lataaminen edellyttää käyttäjältään erityistä tarkkaivaisuutta, koska tarjontaa on niin paljon.



Kuva 2. Esimerkki VPN-selainlaajennuksista. (Google Chrome Web Store 2021.)

Kuvassa 2 näkyy erilaisia VPN-selainlaajennuksia, jotka löytyvät Google Chrome Web Storesta.

4.3 Reititin VPN

Mikäli useampi eri laite on kytketty käyttämään samaa Internet-yhteyttä, silloin kannattaisi ennemmin harkita tai jopa toteuttaa VPN-yhteys reitittimellä, kuin alkaisi asentamaan jokaiseen laitteeseen erillisiä VPN-ohjelmistoja. Etenkin niiden laitteiden, joiden Internet-yhteyden määrittäminen on hankalaa, suositellaankin käytettäväksi reitittimen VPN:ä, koska se on hyödyllinen suojaamaan tällaisia laitteita. Näihin laitteisiin kuuluvat muun muassa älytelevisiot sekä pelikonsolit, reitittimen VPN pystyy mahdollistamaan, jopa maantieteellisesti rajoitetun sisällön hyödyntämisen kodin viihdejärjestelmässä. (Kaspersky 2021.)

Kyseinen VPN on helppo asentaa, lisäksi se tarjoaa käyttäjälleen pysyvää suojausta sekä tietosuojaa. Vaikka verkkoon kirjauduttaisiin suojaamattomilla laitteilla, niin reitittimen VPN:n verkon suojaus ei katoaisi edes tällöin. Mikäli reitittimelläsi ei ole omaa käyttöliittymää, silloin sitä voi olla hankalampi hallita. Tämä voisi johtaa siihen, että kaikki tulevat yhteydet estettäisiin. (Klusaite 2020.)

VPN on myös mahdollista asentaa reitittimeen fyysisesti, sekä virtuaalisesti. Sen myötä kaikki reitittimeen yhdistetyt laitteet ja niiden verkkoliikenne kulkee salatun tunnelin kautta. Hyötyinä nähdään katkeamaton yhteys VPN-palveluun, VPN:ä ei tarvitse asentaa uusiin laitteisiin, sekä myös se että yhteys verkkoon on salattua. Haittoina taas ovat VPN:n asetus ja hallinnointi, salaus ja tunnelointiprotokolla reitittimessä, ulkopuolisten käyttäjien yhdistäminen kyseiseen verkkoon, sekä myös VPN-palvelu laskee todennäköisesti reitittimen yhdeksi laitteeksi. (Klusaite 2020.)

Ennen kuin asennetaan VPN reitittimeen, on aluksi rekisteröidyttävä VPN-palveluun. Tässä vaiheessa on myös hyvä muistaa etsiä sellainen palveluntarjoaja, mikä ei estä asennusta reitittimelle, sekä ei rajoita kaistaa. Tämän jälkeen voi aloittaa asennusprosessin. Käyttäjän tulee nyt kirjautua reitittimelle. Kirjautumistiedot löytyvä yleensä reitittimen ohjekirjasta, minkä voi myös ladata verkosta valmistajan omilta sivuilta. Sitä voi jopa kysyä suoraan valmistajalta. Reititin tulisi konfiguroida siinä olevan sisäänrakennetun VPN-toiminnon kautta. (Welekwe 2021.)

VPN asentamisesta reitittimeen tulee vastaan myös ohjelmisto DD-WRT. DD-WRT on avoimen lähdekoodin ohjelmisto, jonka voi asentaa reitittimeen. Sen tarkoituksena on parantaa VPN käyttöä reitittimessä. Sen tarkoituksena on myös poistaa reitittimen oletusohjelmistosta sisäänrakennetut rajoitukset. DD-WRT on yhteensopiva monien reitittimien ja tukiasemien kanssa. (Welekwe 2021.)

Asennusprosessi hoituu ns. ”flashing” -termillä kutsutulla prosessilla. Asennus tuo kuitenkin omat haasteensa. Vääränlainen tai pieleen mennyt asennusprosessi voi jättää jälkeensä käyttökelvottoman reitittimen. Lisäksi kolmannen osapuolen ohjelmiston asentaminen mitätöi laitteen takuun. On kuitenkin olemassa myös reitittimiä, mihin DD-WRT on esiasennettu. Buffalo Technology, Asus ja Linksys tarjoavat tällaisia reitittimiä, missä DD-WRT voi tulla myös mukautettuna. (Welekwe 2021.)

Ennen DD-WRT asentamista on hyvä selvittää, tukeeko reititin ohjelmistoa. DD-WRT-laiteohjelmistosta on olemassa erilaisia versioita eri reitittimille, jotka ovat nähtävissä DD-WRT omalla sivustolla. Ohjelmistot voivat olla kuitenkin vanhoja, eivätkä saata sisältää kaikkia listattuja ominaisuuksia. Ohjelmiston ladattua, tulee resetoida kyseinen reititin niin sanotulla 30–30–30-ohjeella. Aluksi resetointinappia pidetään painettuna 30 sekunnin ajan. Sen jälkeen irrotetaan laitteen virtajohto myös 30-sekunniksi. Viimeiseksi kytketään laite takaisin virtaan ja pidetään taas resetointinappia pohjassa 30-sekunnin ajan. Verkkokytkennässä tulisi käyttää kiinteää verkkoa, langattoman sijaan. Tämän jälkeen tulee kirjautua reitittimen hallintapaneeliin. Sieltä tulisi löytyä välilehti nimellä ohjelmistopäivitys, mikä vaatii ladattavaksi kansion. Tähän tuodaan DD-WRT asennustiedosto. Tiedoston latauduttua, reitin käynnistyy itsestään uudelleen. Sitten tulee tehdä uudestaan sama 30–30–30-resetointi. Sen jälkeen kirjaudutaan DD-WRT oletus IP-osoitteella reitittimeen. Hallintapaneelin ulkoasu tulisi olla muuttunut. Kirjautumistiedot kannattaa muuttaa tässä vaiheessa. Muutosten jälkeen DD-WRT:n voi käynnistää. (Selmeczy 2016.)

Yhteyden muodostamista varten käyttäjän kuuluu asentaa DD-WRT:n seuraavaksi OpenVPN. OpenVPN on ohjelmisto, minkä avulla laitteen voi yhdistää VPN-verkkoon. Ohjelmiston määrittäminen ja VPN-palvelu asentaminen siihen onnistuu kahdella eri tavalla: GUI- tai Script-metodilla.

GUI-metodissa käyttäjän tulee aluksi kirjautua reitittimen hallintapaneeliin, mihin DD-WRT on asennettu. Siellä hänen kuuluu määritellä reititinasetukset siten, että yhteys muodostuu VPN-palveluntarjoajan omien tietojen mukaisesti, mitkä löytyvät VPN-palvelun omalta sivustolta. Tiedot sisältävät muun muassa DNS- ja IP-osoitteet, sertifikaatit, käytettävän VPN-palvelun käyttäjätunnukset, sekä komentorivit. (Welekwe 2021.)

Script-metodissa on ladattava alkuun Script- ja OpenVPN-tiedostot omalle laitteelle. Script-tiedostot sisältävät komentorivitekstiä. OpenVPN-tiedostossa ovat palvelinten sijainnit. Sen jälkeen on kirjauduttava reitittimen DD-WRT-ohjelmistoon ja liittää Script-tiedostoissa oleva sisältö komentokenttään. Ennen prosessin tallentamista käyttäjän on lisättävä Script-komennoissa käyttäjätunnus ja salasana, sekä OpenVPN palvelinsijainnit. (PureVPN Support 2020.)

4.4 VPN Yrityksissä

Yrityksien VPN-ratkaisut ovat mukautettuja kunkin yrityksen tarpeiden mukaan, tällaiset edellyttävätkin mukautettuja määrityksiä sekä teknistä tukea. Yleensä yrityksen IT-vastaavat luovat tämän VPN:n ratkaisun. Yrityksen työntekijä ei pysty itse hallitsemaan VPN:ä, joten työntekijän toiminnat sekä datansiirtelyt kirjautuvat yrityksen lokiin, tällä tavalla yritykset pystyvät minimoimaan tietovuotojen riskit. Yrityksien käyttämien VPN-yhteyksien suurimpana etuna on se, että ne mahdollistavat kokonaan suojatun yhteyden yrityksien intranettiin sekä palvelimiin, myös niille työntekijöille, jotka työskentelevät etänä. (Kaspersky 2021.)

4.4.1 VPN-Keskitin (VPN-Concentrator)

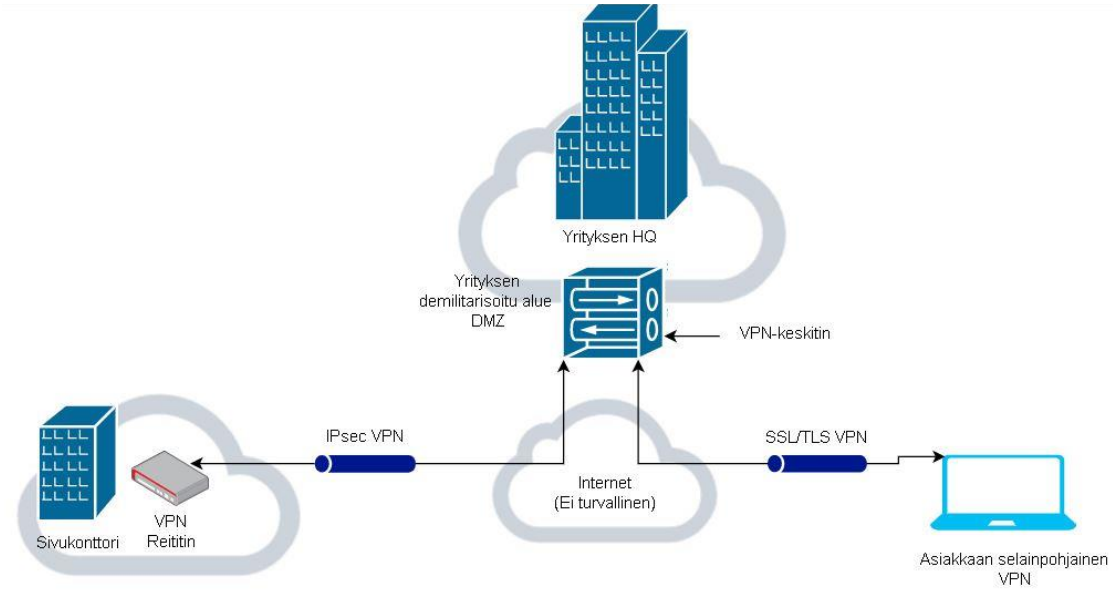
Kun yhä useampi työntekijä aloitti tekemään töitä etänä, tällöin myös virtuaalisten erillisverkkojen käyttäminen lisääntyi, minkä seurauksena VPN-keskittimistä tuli trendikkäitä. Mutta mitä VPN-keskitin tarkkaan ottaen, tekee ja kuinka yritys voi ottaa sellaisen käyttöönsä? (Slattery 2020 b.)

VPN-keskittimiä käytetään yhdistämään useita etäverkkoja sekä asiakkaita keskitettyyn yritysverkkoon. Keskittimiä käytetään suojaamaan etäkonttoreiden tai etäasiakkaiden, kuten työasemien, tablettien, puhelimien sekä IoT-laitteiden välistä viestintää yritysten verkkoihin. Sitä voidaan ajatella yritysverkon tietoturvarajan laajentamisena etähaaroihin tai etätietokoneisiin. (Slattery 2020 b.)

VPN-asiakkaiden, VPN-reitittimien ja VPN-keskittimien yhteyksien kummassakin päässä suoritetaan avainten neuvottelua, todennusta, salausta sekä salauksen purkamista. Salauksessa on kaksi menetelmää, jossa ensimmäistä kutsutaan kuljetusmuodoksi, joka siis salaa vain datan hyötykuorman jättäen alkuperäisten pakettien otsikot ennalleen. Toista menetelmää kutsutaan tunnelitilaksi, joka siis salaa koko paketin sekä kapseloi sen uuteen IP-datagrammiin. Tämän takia VPN-tietoturvasuunnittelu on aloitettava kuljetus- sekä tunnelitilojen ymmärtämisestä. (Slattery 2020 b.)

4.4.2 VPN-keskittimien edut ja kustannukset

Virtuaaliset erillisverkko-keskittimet otetaan käyttöön yritysten verkon reunalla, joko vain rajapalomuurin sisäpuolella yhdellä käyttöliittymällä tai rinnakkain palomuurin kanssa, joka on konfiguroitu läpivientitilassa sisä- tai ulkopuolisella käyttöliittymällä. Suunnittelun yksityiskohdat, mukaan lukien NAT sekä myyjän suositukset, auttavat valitsemaan ensisijaisen topologian. (Slattery 2020 b.)



Kuva 3. Esimerkki VPN-keskittimen käytöstä. (Slattery 2020 b.)

Kuvassa 3 esitetään yrityksen-keskittimen käyttö, jossa yrityksen pääkonttorin verkon reunalla on demilitarisoitu vyöhyke eli DMZ. Lisäksi kuvassa otetaan yhteys yrityksen sivukonttorilta yrityksen-keskittimeen käyttäen IPSec VPN:ä ja puolestaan asiakkaan tietokoneelta otetaan yhteys VPN-keskittimeen SSL/TLS VPN:llä.

Yritys tarvitsee virtuaalisen erillisverkon suojatakseen sivustojensa tai etäkäyttäjiensä välistä viestintää. Erillisistä VPN-keskittimistä tuleekin houkuttelevimpia, kun VPN-yhteyksien määrä lisääntyy tai yhteenlaskettu kaistanleveys kasvaa. (Slattery 2020 b.)

Myyjät tarjoavatkin VPN-keskittimiä erilaisissa hinta-laatusuhteissa. Pienemmät mallit voivat olla ohjelmistopohjaisia virtuaalikoneita tai säilöttyjä toteutuksia, kun taas suuremmat mallit, joissa on oma salauslaitteistonsa, voivat tukea tuhansia VPN-tunneleita. Suunnittelun tulisi myös sisältää muita vaatimuksia, kuten vikasietoisuutta sekä kuormituksen tasapainottamista, jotka määrittävät tarvittavien keskittimien määrän, kapasiteetin sekä ominaisuudet. (Slattery 2020 b.)

4.4.3 VPN-keskittimien tyypit

Useimmat VPN-keskittimet perustuvat erilliseen laitteistoon, jotka on mitoitettu tietylle määrälle VPN-yhteyksiä. On myös olemassa erityisiä laitteistoja suurten VPN-tunnelien salauksien suorittamiseen sekä niiden purkamiseen. (Slattery 2020 b.)

Suurien IPsec virtuaalisten erillisverkko-määrien määrittäminen verkosta toiseen on työlästä sekä monimutkaista, mutta sitä voidaan yksinkertaistaa käyttämällä Ciscon Dynamic Multipoint VPN:ä (DMVPN). Pilvikäyttöönottoa tukevat vain ohjelmistopohjaiset VPN-keskittimet, jotka toimivat virtuaalikoneissa tai säilötyissä ympäristöissä. (Slattery 2020 b.)

Organisaatiot, joilla on erityisen tiukat budjetit, useita etätoimistoja sekä motivoitunutta henkilökuntaa voivat hyödyntää avoimen lähdekoodin projektia oman VPN-keskittimen kokoamiseen. Esimerkiksi OpenVPN, pfSense, alkuperäiset Linux-toteutukset sekä VyOS, joka sisältää DMVPN-tuen. (Slattery 2020 b.)

4.4.4 Mikä VPN-protokolla on paras, kun käytetään keskitintä

Virtuaalisissa erillisverkoissa käytetään ensisijaisesti kahta protokollaa IPsec sekä SSL/TLS:ää, mutta toisinaan myös Secure Shell eli (SSH)-tunnelointia käytetään. IPsec luottaa käyttöjärjestelmälaajennukseen, se onkin ensisijainen mekanismi verkkojen yhdistämiseen sivukonttoreiden sekä yritysverkkojen välillä. SSL/TLS on puolestaan sisällytetty verkkoselaimeen, mikä taas tarjoaa laajemman saatavuuden useammille laitteille kuin IPsec. Sitä suositellaankin, kun halutaan yhdistää yksittäistä isäntää yritysverkkoon. (Slattery 2020 b.)

Protokollista on syytä ymmärtää niiden keskinäiset erot, nopeudet, tietoturvariskit sekä teknologiat. Lisäksi on syytä välttää suojausvirheitä, kun käytetään jaettua tunnelia, ellei lisäsuojatoimenpiteitä toteuteta. (Slattery 2020 b.)

4.4.5 Hyvän turvallisuuden säilyttäminen

Hyvä verkon turvajärjestelmä on rakennettu monista eri komponenteista, jossa VPN-järjestelmät ovat vain yksi komponentti koko järjestelmässä. Haittaohjelmien esiintyvyyden sekä tietojen menettämisen, kuten esimerkiksi luottokorttivarkauksien tai immateriaalioikeuksien paljastamisen, vuoksi organisaatioiden tulisi harkita omien turvajärjestelmien säännöllisiä tarkasteluita. Koska uusia turvallisuusuhkia syntyy säännöllisesti ja vain hyvä huolellisuus suojaa kriittisiä voimavaroja. (Slattery 2020 b.)

4.4.6 Nollaluottamusmalli

Nollaluottamusmalli eli (Zero-trust model) on tietoturvakehys, jonka tarkoituksena on vahvistaa yritystä poistamalla implisiittinen luottamus ja valvomaan tiukasti käyttäjiensä sekä laitteidensa todennusta koko verkkoympäristössä. (Fitzgibbons & Gittlen 2020.)

Nollaluottamuksen turvallisuuden pääperiaate on, se että haavoittuvuuksia ilmaantuu usein, kun yritykset luottavat liikaa ihmisiin sekä laitteisiinsa. Nollaluottamusmalli viittaa siihen, että yhteenkään käyttäjään, vaikka tällä olisi pääsy verkkoon, ei pitäisi oletuksena luottaa, koska he voivat joutua vaaraan. Siksi identiteettiä sekä laitteiden todennusta vaaditaan koko verkossa eikä vain sen kehällä. (Fitzgibbons & Gittlen 2020.)

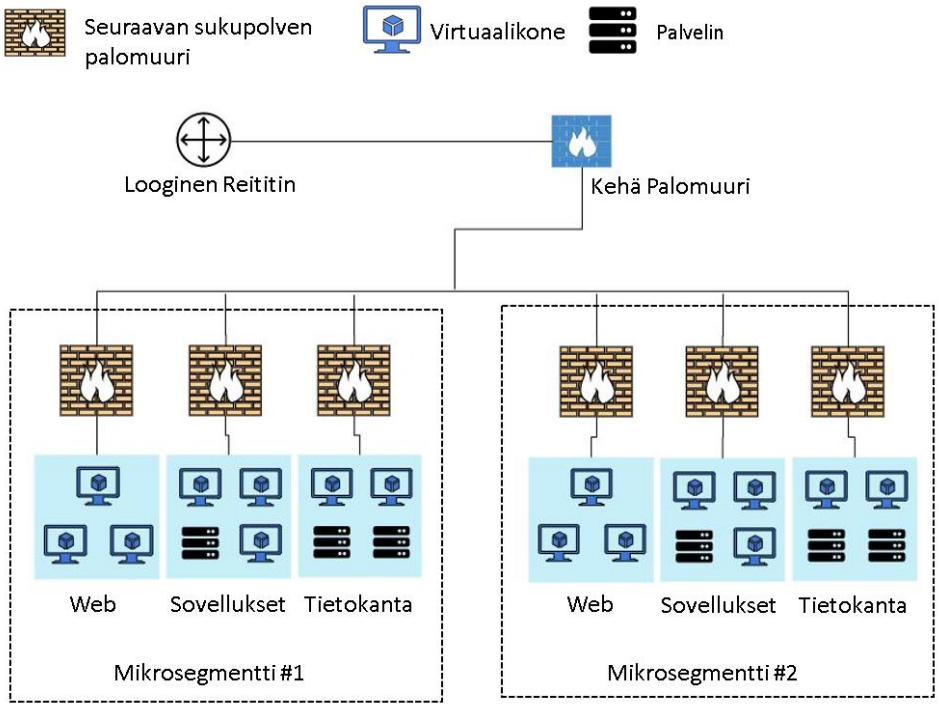
Rajoittamalla sitä, että kenellä on etuoikeus päästä verkon eri segmentteihin tai jokaiseen organisaation suojattuun laitteeseen, tällöin hakkereiden mahdollisuudet päästä käsiksi suojattuun sisältöön pienenevät huomattavasti. Nollaluottamusmallin otti ensimmäisenä käyttöön Forrester Researchin analyytikko vuonna 2010. Pian tämän jälkeen toimittajat, kuten Cisco sekä Google hyväksyivät kyseisen mallin. (Fitzgibbons & Gittlen 2020.)

4.4.7 Miksi nollaluottamusmalli on sitten tärkeä?

Perinteiset IT-suojaussrategiat, kuten palomuurit sekä virtuaalisen erillisverkot, luovat verkon ympärille kehyksen, jonka avulla todennetut käyttäjät sekä laitteet voivat kulkea verkon läpi ja käyttää resursseja helposti. Valitettavasti niin monet käyttäjät työskentelevät etänä sekä yhä enemmän organisaation omaisuudesta on sijoitettu pilveen. Pelkkä kehälähestymistapaan luottaminen on muuttumassa tehottomaksi sekä vaaralliseksi. (Fitzgibbons & Gittlen 2020.)

Nollaluottamusmalli päinvastoin tarjoaa vahvan suojan sellaisia hyökkäyksiä vastaan, jotka vaivaavat organisaatioita nykypäivänä, mukaan lukien heidän omaisuutensa sekä identiteettien varkaudet. Nollaluottamuksen ottaminen käyttöön antaa organisaatioille mahdollisuuden

- Suojata organisaation tietoja
- Parantaa kykyä tehdä vaatimustenmukaisia auditointeja
- Pienentää rikkomusriskiä sekä havaitsemisaikaa
- Parantaa verkkoliikenteen näkyvyyttä sekä lisätä hallintaa pilviympäristöissä. (Fitzgibbons & Gittlen 2020.)



Kuva 4. Esimerkki mikrosegmentoinnista. (Fitzgibbons & Gittlen 2020.)

Nollaluottamusmalli tukee mikrosegmentointia (kuva 4), joka on kyberturvallisuuden perusperiaate. Mikrosegmentointi mahdollistaa IT:n verkkoresurssien eristämisen, jotta mahdolliset uhat pystyttäisiin hallitsemaan helposti eivätkä ne leviäisi koko yritykseen. Organisaatiot pystyvät soveltamaan tarkkoja käytäntöjä, joita sitten sovelletaan roolipohjaisella pääsyllä suojattuihin arkaluonteisiin järjestelmiin sekä tietoihin. (Fitzgibbons & Gittlen 2020.)

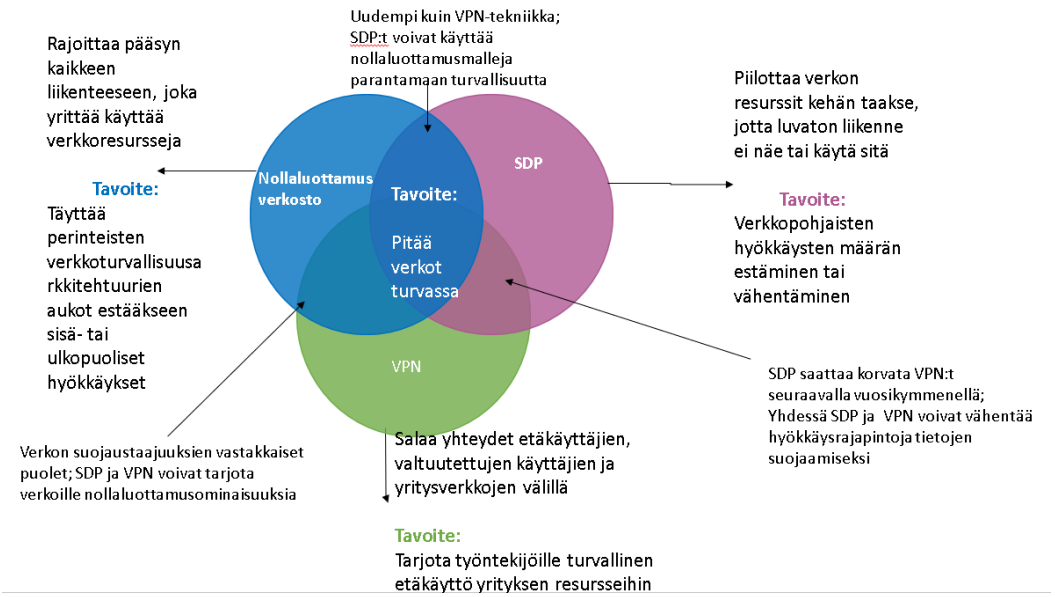
4.4.8 Nollaluottamus vs. SDP vs. VPN

Nollaluottamus, ohjelmiston määrittämä kehä eli (SDP) sekä VPN:t ovat kaikki verkkosuojauksia, joiden tehtävä on suojata yrityksen resursseja. Vaikka nämä kolme lähestymistapaa saattavat vaikuttaa siltä, että ne vastustaisivat toisiaan, silti ne voivat toimia yhdessä kattavamman turvallisuusstrategian luomiseksi. (Fitzgibbons & Gittlen 2020.)

SDP on peittoverkko, joka kätkee verkon resursseja kehän sisällä. SDP-ohjaimet todentavat valtuutetut käyttäjät sekä yhdistävät heidät yrityksen verkkoresursseihin tai sovelluksiin suojatun yhdyskäytävän kautta. SDP-tekniikka auttaa vähentämään verkkoon sisältyviä vaaroja, kuten palvelunesto- tai mies välissä-hyökkäyksiä. (Fitzgibbons & Gittlen 2020.)

VPN-verkot puolestaan luovat salattuja tunneleita yritysverkkojen ja valtuutettujen loppukäyttäjien laitteiden välille. Vaikka VPN-verkot auttavat lisäämään etäkäyttöä, ne eivät helposti käsittele nykyaikaisempia IoT-laitteita, jotka vaativat myös verkkoyhteyden. Organisaatiot voivat yhdistää SDP:n, joka voi käyttää nollaluottamuskonsepteja, kuten implisiittistä luottamusta sekä VPN:ä selkeän verkon kehän määrittämiseen ja siten luoda suojattuja vyöhykkeitä verkossa mikrosegmentoinnilla. (Fitzgibbons & Gittlen 2020.)

Tietohallintojohtaja sekä johtava tutkimusanalyytikko John Burke kirjoitti, että SDP on rakeisen pääsynhallinnan avulla nollaluottamuksen toteutus. Erona on siinä, että vaikka nollaluottamus vaatiikin dynaamista luottamuskarttaa, joka reagoi käyttäytymiseen, niin SDP ei pidä sitä perustavanlaatuisena. (Fitzgibbons & Gittlen 2020.)



Kuva 5. Mitä eroa on SDP-, VPN- ja Nollaluottamusverkostoilla. (Fitzgibbons & Gittlen 2020.)

Kuvassa 5 esitetään SDP-, VPN- ja Nollaluottamusverkostojen eroavaisuudet. SDP piilottaa verkon resurssit kehän taakse, jotta luvaton liikenne ei näkisi tai käyttäisi sitä. SDP:n tavoitteena on verkkopohjaisten hyökkäysten määrien estäminen tai niiden vähentäminen. VPN salaa yhteydet etäkäyttäjien, valtuutettujen käyttäjien sekä yritysverkkojen välillä. VPN:n tavoitteena on tarjota työntekijöille turvallinen etäkäyttö yrityksen resursseihin. Nollaluottamusverkosto rajoittaa pääsyä kaikkeen liikenteeseen, joka yrittää käyttää verkkoresursseja. Nollaluottamuksen tavoitteena on täyttää perinteisten verkkoturvallisuusarkkitehtuurien aukot estääkseen sisä- tai ulkopuoliset hyökkäykset. (Fitzgibbons & Gittlen 2020.)

4.5 VPN älypuhelimissa tai tietokoneissa

VPN-ratkaisuja on saatavilla kattavasti myös älypuhelimiin sekä muihin laitteisiin, jotka ovat yhteydessä Internettiin. Useat VPN-palvelut tarjoavatkin mobiiliratkaisuja. Nämä ovat ladattavissa suoraan Android- ja Apple-älypuhelimiin sovelluskaupasta. VPN:stä voi olla etenkin hyötyä silloin, jos tallennat älypuhelimeesi henkilötietojasi sekä maksutietojasi, mutta myös tavalliseen Internetin selaamiseen. (Kaspersky 2021.)

4.5.1 VPN asentaminen älypuhelimeen

Helppo tapa päästä käyttämään VPN on ladata se sovelluskaupasta. Tällä hetkellä suosituimmat sovelluskaupat ovat Apple App- ja Google Play -kauppa. Molemmista löytyy kirjava valikoima VPN-sovelluksia, sekä arvioita mitkä edesauttavat käyttäjien ostopäätöksiä. Hyvänä nyrkkisääntönä VPN hankkiessa on välttää ilmaisia VPN-sovelluksia. (Kaspersky 2021.)

VPN-sovelluksen käyttöönotossa luodaan alkuun käyttäjätili kyseisen palveluntarjoajan kantaan, minkä jälkeen pääsee aloittamaan sovelluksen käytön. Nykyisin lähes kaikki sovellukset on tehty mahdollisimman helppokäyttöisiksi. Tyypillisesti avattaessa juuri asennettua sovellusta käyttäjälle näytetään pieni opetusohjelma, millä hän pääsee nopeasti alkuun. Näin on myös VPN-sovelluksissa. Vaikka käyttäjällä ei olisi tietoakaan VPN toiminnasta, hän pystyy muutamassa minuutissa käyttämään sitä kuin tavallista sovellusta. (Kaspersky 2021.)

Käyttöönotto ja käytöstä poistaminen on myös helppoa. Sen voi tehdä yleensä sovelluksen aloitusnäytöllä napin painalluksella tai sovelluksesta voi luoda widgetin eli pienoisohjelman älypuhelimen kotinäyttöön, milloin käyttäjän tarvitsee vain käynnistää puhelimen VPN kytkentää varten. (Kaspersky 2021.)

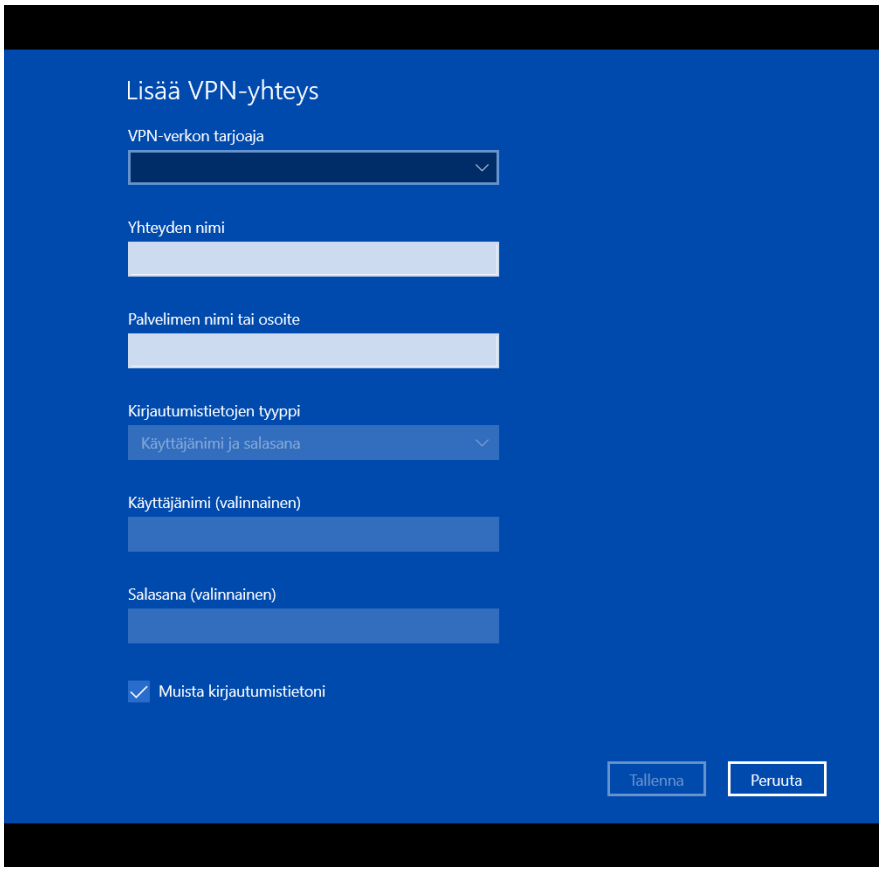
VPN-sovelluksissa olennaista on palvelinten vaihtaminen lennosta, mikä löytyy myös sovellusten älypuhelin versioista. Myös vianmääritykset, sekä salausmenetelmien muuttaminen ovat käyttäjän saatavilla. Näiden ominaisuuksien selvittäminen on kuitenkin hyvä tehdä ennen VPN-sovelluksen hankintaa. (Kaspersky 2021.)

Tietoturvasta, sekä omasta yksityisyydestään huolehtivan kannattaa myös selvittää VPN-tarjoajan datankäyttö- sekä tallennuskäytännöt ennen lopullista hankintaa. Käyttäjän toiminta verkossa on sidoksissa VPN-palvelun omille palvelimille, mitkä muodostavat yhteyden verkkoon käyttäjän puolesta. Jos datalokeja tallennetaan, olisi hyvä tietää mitä varten niitä säilytetään. Toinen asia mikä on hyvä

muistaa VPN käytössä älypuhelimella on mikä salataan ja mikä ei. Ainoastaan vain Internet-data on salattua eivätkä puhelut tai tekstiviestit. (Kaspersky 2021.)

4.5.2 VPN asentaminen tietokoneisiin

Windows- sekä Mac-tietokoneissa pystyy asentamaan VPN:n ladattavana sovelluksena tai käyttöjärjestelmän asetuksista. Sovelluksen asentaminen on näistä helpoin. Käyttäjän tarvitsee vain tietää haluamansa VPN-tarjoaja, avata sovelluskauppa ja asentaa sovellus. Käyttöjärjestelmästä asentaminen vie hiukan enemmän aikaa, mutta saa aikaan kuitenkin halutun tuloksen. (Anttila 2021.)



Kuva 6. Windowsin sisäinen VPN-yhteys. (Ruutukaappaus Windows koneelta.)

Windowsissa käyttäjän tulee ensiksi avata Asetukset-valikko. Asetuksista tulee valita Verkko ja Internet -välilehti. Välilehden vasemmalla menulla valitaan VPN ja sen avattua Lisää VPN-yhteys. (Kuva 6.) Käyttäjälle avautuu lomake. Ensimmäiseksi valitaan VPN-verkon tarjoaja, mikä on oletuksena Windows (sisäinen). Seuraavaksi

tulee nimetä VPN, sekä antaa kyseisen VPN-serverin osoite. VPN-tyypistä avautuu alastulovalikko, mistä käyttäjä valitsee tarvitsemansa protokollan. Sitten on vuorossa Käyttäjänimi ja Salasana, mikä ei ole se sama tunnuspari millä kirjaudutaan palveluntarjoajan kantaan. Tämän voi selvittää muualta tai kysyä palveluntarjoajalta. (Anttila 2021.)

Mac-koneille ohjeet ovat lähestulkoon samat kuin Windowsissa. Apple menusta avautuu valikko, mistä valitaan Järjestelmäasetukset ja Verkko. Vasemmalla olevan luettelon alapuolella näkyy + -merkki. Sitä painamalla avautuu Liitäntä-ponnahdusvalikko, mistä valitaan VPN ja tyyppi sekä lopuksi palvelun-nimi. Luotuaan sen käyttäjän tulee vielä antaa Palvelimen osoite ja Käyttäjätunnus. Sitten valitaan Todentamisasetukset ja annetaan VPN-verkon ylläpitäjältä saadut tiedot. Mahdollisesti ylläpitäjä saattaa myös vaatia käyttäjää käymään Lisävalinnoissa täyttämään muita tietoja. Lopuksi valitaan OK. (Anttila 2021.)

5 VPN PROTOKOLLAT

Virtuaalisessa erillisverkossa käytetään PPTP, L2TP & L2TP/IPsec, OpenVPN, SSTP sekä IKEv2 protokollia, nämä ovat siis viisi yleisintä protokollaa.

5.1 PPTP

PPTP eli Point-to-Point Tunneling on Microsoftin kehittämä teknologia, joka luo VPN-verkon dial-up-verkkoihin. PPTP-protokollaa on pidetty VPN-alan standardina sen kehittämisestään asti. Point-to-Point Tunneling on ensimmäinen Windowsin tukema VPN-protokolla, jonka tavoitteena on luoda turvallisuutta erilaisilla todentamismenetelmillä, joista yleisimpinä käytetään MS_CHAP v2 menetelmää. Kaikki VPN-laitteet sekä alustat tukevat tätä protokollaa, lisäksi koska se ei vaadi isoa määrää suoritustehoa, on se tämän vuoksi yksi nopeimmista saatavilla olevista VPN-protokollista. (Fawkes 2021.)

PPTP-protokollasta löytyy myös heikkouksia, vaikka se hyödyntääkin nykyisin useimmiten 128-bittistä salausta, sisältyy tähän protokollaan monenlaisia tietoturva-aukkoja, joista kaikista vakavin tietoturva-aukoista on kapseloimattoman MS-CHAP v2-todentamisen mahdollisuus. Tämän vakavuuden vuoksi PPTP pystytään murtamaan jo kahdessa päivässä. Vaikkakin Microsoft on korjannut tämän haavoittuvuuden, se suosittelee silti VPN-käyttäjiä käyttämään SSTP sekä L2TP-protokollia PPTP:n sijasta. Lisäksi NSA on mitä luultavammin purkanut kyseisen protokollan tai purkaa yhä tänäkin päivänä PPTP:llä suojattua viestintää. (Fawkes 2021.)

Lopuksi on hyvä muistaa, ettei PPTP-protokollaa saa missään tapauksessa käyttää virtuaalisessa erillisverkko toteutuksissa, sen tietoturva heikkouksien takia.

5.2 L2TP & L2TP/IPsec

L2TP eli Layer 2 Tunnel Protocol ei itsessään tarjoa yksityisyyttä tai salausta sen kautta liikkuvalle liikenteelle, toisin kuin muut VPN-protokollat, siksi sen käytön

yhteydessä käytetäänkin IPsec-nimistä protokollakokoelmaa, jonka tarkoituksena on tietojen salaaminen ennen sen lähtemistä, IPsec siis takaa käyttäjälleen yksityisyyden sekä turvallisuuden. Kaikki nykyaikaiset VPN-yhteensopivat laitteet sekä alustat pitävät sisällään L2TP:n/IPsecin. Asennus on yhtä nopeaa ja helppoa kuin PPTP:llä, mutta ongelmatilanteita voi aiheuttaa se, että kyseinen protokolla käyttää UDP-porttinumeroa 500, jonka käyttöä NAT-palomuurit pystyvät helposti estämään. Siksi sen käyttäminen palomuurin kanssa saattaa edellyttää käyttäjältään porttiohjauksen tekemistä. (Fawkes 2021.)

IPsec-salauksessa ei ole esiintynyt mitään huomattavia heikkouksia, siksi oikein suoritettuna se voi olla edelleen turvallinen ratkaisu. Vaikkakin Edward Snowdenin paljastukset antavatkin viittauksen siihen, että NSA olisi murtanut IPsecin. Electric Frontier Foundation perustajajäsen sekä turvallisuusalan asiantuntija John Gilmore syyttää, NSA:ta siitä, että he olisivat tarkoituksenmukaisesti heikentäneet kyseistä protokollaa. (Fawkes 2021.)

5.3 OpenVPN

OpenVPN on avoimen lähdekoodin teknologia, joka käyttää SSLv3-/TLSv1-protokollia sekä OpenSSL-kirjastoa toisiin tekniikoihin liitettynä tarjotakseen luotettavampaa ja vahvempaa VPN-ratkaisua. Protokollana OpenVPN on erittäin muokattavissa sekä se toimii parhaiten UDP-portin kautta, mutta se voidaan määrittää tarvittaessa myös mille tahansa muullekin portille, mikä tekee sen käytön estämisen hyvin vaikeaksi eri palveluissa, kuten esimerkiksi Googlessa. (Fawkes 2021.)

OpenVPN:n huomattavana etuna on myös se, että sen OpenSSL-kirjasto tukee monia eri salausalgoritmeja, kuten esimerkiksi 3DES, AES ja Blowfish, vaikka VPN-tarjoajat käyttävätkin pääosin vain AES- ja Blowfish-algoritmeja. OpenVPN-protokolla pitää sisällään sisäänrakennetun 128-bittisen Blowfish-salausalgoritmin, vaikka OpenVPN:ä pidetäänkin yleisesti ottaen turvallisena, silti siinäkin on joitakin tunnettuja haavoittuvuuksia. (Fawkes 2021.)

OpenVPN-protokollan toimintanopeus perustuu aina sen käytetystä salaustasosta. Se on yleisesti ottaen nopeampi, kuin IPsec. Lisäksi OpenVPN:ä pidetään nykyään useiden VPN-palveluiden oletusyhteytenä. OpenVPN:n asentamista pidetään hieman hankalampana kuin L2TP/IPseciin sekä PPTP:hen verrattuna, erityisesti silloin kun on käytössä yleinen OpenVPN-ohjelmisto. Asiakasohjelman lataamisen ja asentamisen jatkoksi myös erilliset määritystiedostot on syytä määritellä. Tämä vie sekä aikaa että lisää asentajalleen vaivannäköä. (Fawkes 2021.)

Lopuksi NSA ei ole pystynyt heikentämään tai murtamaan OpenVPN:ä. Sitä pidetään myös immuunina NSA:n hyökkäysyrityksille, koska OpenVPN:ssä on lyhytkestoinen avaintenvaihto. OpenVPN:n vahvan salakirjoituksen ansiosta sitä pidetään ainoana turvallisena VPN-protokollana. (Fawkes 2021.)

5.4 SSTP

Secure Socket Tunneling on Microsoftin kehittämä VPN-protokolla, vaikka se onkin edelleen pääasiassa Windows-alusta, niin se on myös muun muassa saatavilla Linuxille. SSTP käyttää SSL v3:a ja sen etuina on NAT-palomuuriongelmien estäminen. SSTP pidetään vakaana ja helppokäyttöisenä, koska se on integroitu Windowsiin. (Fawkes 2021.)

Koska kyseessä on Microsoftin ylläpitämä standardi ja teknologiajätti on ennenkin tehnyt yhteistyötä NSA:n kanssa niin voidaan pitää mahdollisena, että Windows-käyttöjärjestelmään on sisälletty takaportti, minkä vuoksi sen luotettavuudesta ei ole täysiä takeita verrattuna joihinkin muihin protokolliin. (Fawkes 2021.)

5.5 IKEv2

On IPsec-pohjainen tunnelointiprotokolla kokonimeltään Internet Key Exchange Version 2. Se on kehitetty Ciscon sekä Microsoftin yhteistyöllä ja se sisältyy Windows 7:aan sekä sitä uudempiin käyttöjärjestelmiin. IKEv2 sisältää myös yhteensopivat avoimen lähdekoodin toteutukset sekä Linuxille, että monille muille eri alustoille. Siksi myös BlackBerry-laitteille löytynee tuki. (Fawkes 2021.)

Microsoft Corporation VPN Connectiksi nimeämä palvelu on hyvä muodostamaan VPN-yhteyksiä uudelleen, jos Internet-yhteys sattuu katkeamaan väliaikaisesti. IKEv2 käytöstä hyötyvät eniten mobiilikäyttäjät, Mobility ja Multihoming-protokolla takaa eri verkkojen vaihtamisesta todella sulavaa. BlackBerryn käyttäjille IKEv2 on siitä loistava protokolla, että se kuuluu niihin harvoihin VPN-protokolliin, jotka tukevat näitä laitteita. IKEv2:en vakautta, turvallisuuta sekä suorituskykyä pidetään tasavertaisina IPsec:in kanssa, vaikka IKEv2 on saatavilla harvemmille alustoille, kuin IPsec. (Fawkes 2021.)

6 FIVE EYES, NINE EYES JA FOURTEEN EYES

VPN-yhteyksistä käytävissä keskusteluissa, etenkin sen tietosuojasta puhuttaessa voi törmätä tai on saattanut törmätä termeihin Five Eyes, Nine Eyes tai Fourteen Eyes. Vaikka nimet ei kuulostaisi siltä, että ne liittyisivät automaattisesti Virtuaaliseen erillisverkkoon, vaan kuulija saattaisi yhdistää ne esimerkiksi hämähäkkeihin tai suoranaisesti silmiin. Nämä termit kuitenkin liittyvät olennaisesti siihen, että mikä VPN-palveluntarjoaja käyttäjän kannattaisi valita. (Krohn 2021.)

6.1 Five Eyes

Ymmärtääksemme mistä näissä Five- Nine- sekä Fourteen Eyes termeissä on kyse, niin täytyy ensiksi perehtyä ihan perusasioihin. Terminä Five Eyes eli (FVEY) on tämän verkko liittouman perusta, joka on synonyymi UKUSA-sopimukselle, jonka Iso-Britannia sekä Yhdysvallat allekirjoittivat jo vuonna 1946, tällä voitiin mahdollistaa signaalitiedustelutietojen jakaminen. Pian tämän sopimuksen jälkeen joukkoon liittyivät myös Australia, Kanada sekä Uusi-Seelanti, tämän jälkeen jäseniä oli siis viisi. (Krohn 2021.)

Signaalitiedustelulla tarkoitetaan siis signaalien sieppaamiseen perustuvaa tiedonkeruu tapaa, oli kyseessä sitten ihmiseltä ihmiselle tapahtuvaa viestintää tai erilaiset sähköiset signaalit, joita ei suoranaisesti käytetty viestintätarkoitukseen. Koska kaikki arkaluontoiset asiat yleensä salataan, niin signaalitiedusteluun liittyy myös vahvasti kryptoanalyysi, jota käytetään viestien purkamiseen. (Krohn 2021.)

6.2 Echelon

Echelon on näiden kaikkien viiden maan käyttämä sähköinen valvontajärjestelmä, jonka avulla nämä maat pystyvät salakuuntelemaan yksittäisiä henkilöitä, alun perin Echelon otettiin käyttöön toisessa maailmansodassa ja sitä käytettiin silloin nimenomaan Neuvostoliiton sekä sen itäblokinliittolaisten välisen viestinnän salakuunteluun. Guardian-lehti kuvaili Echelonia maailmanlaajuiseksi sähköisten va-

koiluasemien verkostoksi, joka pystyy vakoilemaan puhelimia, faxeja sekä tietokoneita. Se pystyy jopa seuraamaan pankkitilejä, nämä kaikki tiedot tallennetaan Echelon-järjestelmiin, joissa saattaa olla jopa miljoonia eri tietueita yksityishenkilöistä. Echelon:ia on kehitetty toisen maailmansodan jälkeen, siten että se kattaa yksityisen sekä kaupallisen viestinnän, siksi tämä on merkittävä asia myös VPN-käyttäjille, jotka haluavat välttää tällaisten verkkoviestinnän joutumasta siepatuksi. (Krohn 2021.)

On olemassa lakeja, jotka mahdollistavat NSA:ta suorittamaan tietynlaisia valvontatoimia Yhdysvaltain kansalaisia kohtaa. Liittolaismaissa eli Five Eyes –sopimuksen alaisissa valtioissa on erilaiset lait sekä valvontalait. Toisinaan on taas helpompaa antaa toisen maan vakoojaviraston vakoilla oman maansa kansalaisia, sama pätee myös toiseen suuntaan. Miksi tällä on sitten merkitystä, jos käyttäjä käyttää VPN-yhteyksiä tai edes palvelimia, jotka sattuvat sijaitsemaan joissakin näistä maista. (Krohn 2021.)

Alkunsa jälkeen Five Eyes -ohjelma on kehittynyt ja tuonut mukaan myös kolmannen osapuolen kumppaneita, nämä valtiot ottavat osaa tähän ohjelmaan hyvin eri keinoin. Esimerkiksi Tanska on antanut luvan NSA:lle asennuttaa eri valvontalaitteita maasta lähteville sekä maahan tuleville valokuitukaapeleille. Vastineeksi tästä NSA on antanut omia laitteita sekä tekniikkaa Tanskan viranomaisten käyttöön. (Krohn 2021.)

6.3 Nine- Ja Fourteen Eyes

Sopimukseen myöhemmin liittyneet maat tunnetaan nimillä Nine- ja Fourteen Eyes. Nine Eyes-sopimus toi mukanaan Alankomaat, Norjan, Ranskan sekä Tanskan, kun taas Fourteen Eyes-sopimus sisällytti mukaansa Belgian, Espanjan, Italian, Ruotsin sekä Saksan. Nämä sekä alkuperäiset viisi maata ovat kaikki niitä maita, joita käyttäjän tulisi välttää valitessaan itselleen VPN-palvelua etenkin sellaista, jonka verkkoliikenne on lähtöisin jostakin näistä maista. (Krohn 2021.)

7 VPN KÄYTTÖ COVID-2019 AIKANA

COVID-2019-pandemian tulo vaikutti merkittävästi maailman menoon. Yksi nousevista aiheista oli etätyöt ja -opinnot. Miten suuri määrä ihmisiä saataisiin helposti ja turvallisesti, sekä mahdollisimman pian käsiksi etätyöskentelyn pariin? Uusi muutos arkeen hyödytti monia, mutta myös herätti uusia kysymyksiä IT-puolella.

7.1 VPN-käyttö kasvussa

Vuonna 2019 ilmestynyt COVID-19-pandemia lamautti ihmisten liikehdinnän täysin. Työpaikkojen karsinta, matkustamisen rajoittaminen, julkisten tapahtumien esto pakotti ihmiset koteihinsa. Tartuntojen ehkäisyä varten tehdyt toimet ja pitkäaikainen oleskelu sai ihmiset kääntymään Internetin puoleen. (McCarthy 2020.)

Etätyöskentely otettiin käyttöön niin työssäkäyville, kuin opiskelijoille. Viihteen nousu on saanut ihmiset hakemaan uutta katsottavaa oman alueidensa ulkopuolelta. Näiden seurauksena VPN:n kysyntä koki huiman nousun. Viihteenkäytön ohella, myös yritykset ovat vaatineet etätyöntekijöiltään VPN:n käyttöä mikä jo itsestään on kasvattaa kysyntää VPN:lle. (Hodge 2020 a.)

Taulukko 1. VPN käytön kasvu COVID-19 aikana. (Johnson 2021.)

Maat	COVID-19 tapaukset per viikko	VPN käytön nousu per viikko prosentteina
Italia	51,768	160
Yhdysvallat	33,005	124
Espanja	28,094	58
Saksa	23,833	40
Iran	15,072	49
Ranska	14,809	44
Sveitsi	7,142	12
Yhdistynyt kuningaskunta	5,405	18
Venäjä	400	57

Taulukko 1 näkyy että suurin kysyntä VPN-palveluja kohtaan oli vuonna 2020 maaliskuussa maissa, missä COVID-19 aiheutti eniten ongelmia. Listan kärjessä olivat Italia, Yhdysvallat ja Espanja.

7.2 Etätyöskentelyyn valmistautuminen

Etätyöskentely on noussut uudeksi normiksi monilla aloilla pandemian aikana. Siihen siirryttiin suurissa, sekä pienissä yrityksissä ja useimmat vaativat enemmistöä työväestään kommunikoimaan etänä. Uusien työskentelytapojen omaksuminen voi olla hankalaa, minkä vuoksi erityisesti suuryritysten valmius tällaisia tilanteita varten on välttämätöntä. (OpenVPN 2021.)

Yksi hyödynnetyimmistä teknologioista etätyöskentelyssä on VPN. Huolellinen suunnittelu on tärkeää valmistaessa etäkommunikointikäytäntöjä työntekijöiden välillä. (Kirvan 2020.) OpenVPN:n vuoden 2019 teettämään kyselyyn vastanneista yrityksistä 24 % ei ole uusinut etätyöskentelykäytäntöjään vuoteen ja 44 % ilmoitti, ettei sisäinen IT-osasto ollut johtamassa etätyöskentelyn turvallisuuskäytäntöjä. (OpenVPN 2021.)

Oikeanlainen etätyöskentelystrategia VPN:n avulla vaatii monta kysymystä. Mikä on etätyöntekijöiden maksimimäärä ja kuinka sitä sovelletaan verkon kaistaan? Kuinka pian yrityksellä on tarvetta suuremmalle kaistalle ja kuinka nopeasti sitä on tarjolla? Lisenssien, sekä muiden resurssien saanti kasvavalle kaistankulutukselle on myös huomioitava. Lisääntynyt verkonkulutus vaati myös uusia verkkokomponentteja. Niiden ja lisääntyneen kaistan hinnoittelusta on soviteltava. Pystyykö yritys hyödyntämään eri teknologioita etätyöskentelyssä kaistanleveyden tehokkuutta varten? Etätyöskentely tuottaa myös ongelmia tietoturvalle. Kuinka sen kannalta varaudutaan mahdollisiin ongelmiin, sekä turvataan ja valvotaan dataliikennettä? Tilanteen laantuessa ja kaistankulutuksen palautuessa oletusarvoille, kuinka edellä mainittujen uudistusten palauttaminen tapahtuu? Millaisia resursseja paikalliskeskus-, Internet- ja WAN-tarjoajilla on saatavilla. (Kirvan 2020.)

VPN:n valinnassa on otettava huomioon myös niiden turvallinen käyttö, sekä ominaisuudet. MFA (multi-factor authentication) takaa turvallisen pääsyn työntekijöille yhtiön resursseihin. MFA tarkoittaa sitä, että sisäänkirjautuminen vaati toi-

sen laitteen. Käyttäjä esimerkiksi syöttää tunnuksensa kirjautuessaan tietokoneesta ja varmistaa vielä kirjautumisensa älypuhelimen kautta. Toinen taso turvallisuuden takaamiseksi on pääsynhallinta, mikä varmistaa kuka näkee ja pääsee käsiksi mihin sisältöön. Lisäksi on taattava useiden laitteiden turvallinen käyttö päätepisteiden suojauksella. Sen avulla yrityksen verkkoon pääsee yhdistymään vain ne laitteet, jotka omaavat sille asetetut kriteerit. (OpenVPN 2021.)

IT-tiimien on siis otettava huomioon erityisesti kaista, sen turvaaminen, sekä siihen saatava avustava palvelu. VPN ovat kuitenkin alttiita menettämään tehokkuutensa kriisitilanteissa, missä niiden käyttö kasvaa dramaattisesti. Siksi saatavilla olevan avun kartoittaminen on hyvin tärkeää. Vaihtoehtojen vertailu, neuvottelut eri verkkoa ylläpitävien tahojen kanssa ja loppukartoitus vievät yrityksiä parempaan suuntaan oman toimintansa turvaamisessa. (Kirvan 2020.)

7.3 Kysyntä, tarjonta ja seuraukset

Vaikka kaistankulutus on kasvanut suuresti, VPN-tarjoajat ovat onnistuneet pitämään yllä palvelujaan sen sijaan, että niissä olisi ilmentynyt huomattavia ongelmia. Vuoden 2020 maaliskuusta huhtikuuhun NordVPN:n yrityksille suunnatun VPN:n käyttö on noussut maailmanlaajuisesti 165 %. Yritys kertoi rakentavansa uusia servereitä pysyäkseen kasvavan käyttäjäkunnan mukana. Internet-tarjoajat ovat vastanneet VPN kysyntään lanseeraamalla oman VPN-palvelunsa. Yhdysvaltalaisen AT&T julkaisema Anira-VPN koki yhtiön mukaan muutaman viikon sisällä huiman 700 % nousun käytössä. Tähän käyttäjäryhmään kuului tärkeitä sektoreita ympäri maailmaa, kuten muun muassa terveydenhuolto ja talous. AT&T onnistui pitämään yllä palveluitansa käyttämällä hyväksi ohjelmistotestauksenaan white box-menetelmää. (Hodge 2020 a.) Sen sijaan, että AT&T olisi testannut VPN:ä yrityksen sisällä tietyillä laitteilla, ohjelmisto julkaistiin testattavaksi monille yrityksille ja laitteille. Tämän avulla pystyttiin luomaan varma ja toimiva VPN-ohjelmisto toisistaan poikkeaville järjestelmille. (Fuetsch 2020.)

Kaistankulutuksen mittauksessa on myös huomattu päinvastaista kulutusta Virtuaalista erillisverkkoa kohtaan. Eräs toinen yhdysvaltalainen Internet-tarjoaja Verizon, raportoi huhtikuusta 2020 alkaen, VPN:n käytön alkaneen laskemaan. Laskun on arvioutu johtuvan obfuskoiduista VPN-palvelimista. (Hodge 2020 a.) Obfuskaatio-teknologia piilottaa VPN-liikenteen Internet-tarjoajalta, jolloin sitä ei voi hidastaa. Se saa VPN-liikenteen näyttämään tavalliselta verkkoliikenteeltä. (Hodge 2019.)

VPN-käytön nousu on myös tuonut esille tietoturvaongelmia. GlobalWebTKIndexin tilaston mukaan yli 400 miljoona yksittäiskäyttäjää ja yritystä käyttää VPN:ä tai muuta salattua verkkoliikennettä. Statista and Orbis Researchin ilmoitti vuonna 2018 VPN-markkinoiden olevan arvoltaan 20.6 biljoonaa dollaria ja arvioi sen nousevan vuoteen 2022 mennessä 36 biljoonaan dollariin. VPN-teknologia on jo itsestään altis hyväksikäytölle, vaikka sitä onkin pyritty tehostamaan eri uudistuksilla tietoturvan kannalta. Kun käyttäjien verkkoliikennettä ohjataan tietyn yrityksen kautta, se tekee datankeräämisestä ja myynnistä houkuttavan bisneksen. VPN:ä, mistä on tahallisesti tai huomaamatta puuttunut tärkeitä turvallisuuspiirteitä on tavattu muun muassa Googlen omistaman Play -kaupan valikoimassa. Nämä sovellukset voivat pysyä pitkään listoilla. Yleensä nämä sovellukset poistetaan, mutta pahimmassa tapauksessa sovellus on jo ehtinyt kylvää tuhoa laajasti. SuperVPN-sovellus, joka keräsi yli 100 miljoonan latausmäärän sisälsi haavoittuvuuden, mistä tehtiin VPN Pron toimesta helmikuussa 2020 ilmoitus Googlelle. Google poisti sovelluksen vasta huhtikuussa samana vuonna. (Hodge 2020 a.)

8 VPN VIIHDEKÄYTÖSSÄ

VPN-palveluita mainostetaan yleisesti niiden tarjoaman yksityisyyden vuoksi. Verkkokäyttäjien omien tietojen turvaaminen on keskeisimpänä kohteena. VPN:n käytölle on kuitenkin olemassa myös toinen syy. Eri alueiden viihdekirjastot vaihtelevat keskenään. Esimerkiksi YouTubessa oleva video voi näkyä suomalaisille katsojille, mutta ei esimerkiksi Yhdysvalloissa. Alueelliset rajoitukset koskevat lähes kaikkea mediaa ja viihdettä. Syy niiden käytölle voi johtua esimerkiksi maan lakiasetuksista tai harmaasta taloudesta. Median ja viihteen kannalta käyttäjät pystyvät kiertämään tällaiset rajoitukset VPN:n avulla. (Valentine 2018.)

GlobalWebIndex teetti kyselyn vuonna 2018 missä tiedusteltiin pääkäyttötarkoitusta VPN-palvelulle. Siihen osallistui 24 461 henkilöä, mistä enemmistö 49 % vastaajista kertoi käyttävänsä VPN:ä parempaa viihdettä varten ja loput taas listasivat syykseen anonyymin selaamisen. Yksilön oman toiminnan turvaaminen verkossa on siis jäämässä selkeästi jälkeen. Saman ilmiön huomaa myös VPN-mainoksissa, missä tuodaan esille pääsyä suurempaan viihdekirjastoon. Tilanne on kuitenkin saanut myös kyseisten sisällönhaltijoiden huomion. Heidän vastareaktionsa tulee olemaan merkittävä. (Valentine 2018.)

8.1 Pelaaminen

Videopelien, erityisesti moninpelien kohdalla virtuaalista erillisverkkoa mainostetaan lähinnä niiden takaaman turvallisuuden vuoksi. Joissain peleissä käytetään P2P-teknologiaa (peer-to-peer). Peer to peer eli vertaisverkossa perinteinen palvelin- ja asiakassuhde on korvattu toisella tavalla. Kiinteän palvelimen sijaan, kaikki verkon käyttäjät ovat sekä palvelimia, että asiakkaita muille käyttäjille. Käyttäjien laitteet jakavat resursseja toistensa kanssa, minkä yhteydessä he voivat myös löytää toistensa IP-osoitteet. IP-osoitteen voi käyttää hyväksi kyberturvallisuuden vaarantamisessa. DDoS-hyökkäykset ovat näistä tunnetuimpia. (Paul 2021.)

DDoS eli palvelinestohyökkäyksessä uhrin IP-osoite kuormitetaan ylimääräisellä verkkoliikenteellä. Tilannetta vaarantaa myös se, että DDoS-hyökkäyksiä tuotteina on helposti löydettävissä ja helppo luoda. Nämä hyökkäykset ovat lähes päivittäisiä suurissa IT-yrityksissä, missä on varauduttu kyseisiin tilanteisiin. Peruskäyttäjä ei pysty palautumaan näistä yhtä helposti. VPN:n käyttö nykyisissä moninpeleissa piilottaa pelaajien todelliset IP-osoitteet toisiltaan. Se ei kuitenkaan ole suurelta osin täysin tarpeellista. Moni pelaaja ei joudu kyseisen hyökkäyksen uhriksi. Suurimpana kohteena ovat peliyhtiöt. (Paul 2021.)

Toinen syy VPN:n käytölle pelaamisessa on mahdollinen parannus verkkoyhteyden suorituskyvyssä. VPN voit yhdistää pelaajan palvelimen lähemmäksi pelin omia palvelimia. Toisin kuin uskotaan, tämä voi kuitenkin aiheuttaa suurempia viivästyksiä ja hidastaa jo ennestään verkkonopeuksia. Erikoistilanteissa voi olla verkkopalveluntarjoaja, joka on asettanut pienemmän kaistan pelaamiseen verrattuna VPN-yhteyksiin. VPN:llä voi myös päästä pelaamaan eri alueiden palvelimille, esimerkiksi Pohjois-Amerikan serverille. VPN:ä voi myös käyttää alueellisten estojen ylittämiselle, mutta tämä on joskus johtanut pelikieltoon. (Paul 2021.)

VPN:n käyttö pelaamiselle ei tarpeellista kaikille. Sille on kuitenkin käyttöä pienelle käyttäjäryhmälle. Verkossa pelattavat pelit hyödyntävät vertaisverkkoa ja kärsivät muutenkin huonosta turvallisuudesta. Suorituskyvyn nostaminen ei ole taattua, mutta jos käyttäjä haluaa turvata oman pelaamisensa verkossa, VPN on sopiva siihen. (Paul 2021.)

8.2 Suoratoistopalvelu

Suoratoistopalveluiden tarjonta on suurelta osin vaihtelevaa ja samalla myös kattaa laajan valikoiman eri viihdettä. Tarkoituksena on, että jokaiselle löytyy katsottavaa. Tästä huolimatta, suoratoistolle on olemassa myös rajoituksia. VPN:llä on kuitenkin mahdollista kiertää erilaiset maantieteelliset rajoitukset. Sitä on hyödynnetty jo pitkään ja on yleensä esitetty myös mainoslauseena. (Barker 2021.)

Elokuvien, tv-sarjojen ja musiikin suoratoisto vie paljon kaistaa verkossa. Tästä syystä jotkut Internet palveluntarjoajat hidastavat tällaista liikennettä verkossa. VPN:n avulla käyttäjät voivat kiertää tällaiset kaistarajoitukset. Erityisesti jos VPN-palvelu käyttää esimerkiksi AES 256-bit:stä salausta, mikä peittää käyttäjän toiminnan verkossa Internet-tarjoajalta. Sen avulla käyttäjä välttyy suoratoistolle asetetuilta hidastuksilta. (Barker 2021.)

VPN:n käytölle on myös haittapuolena se, että haluttuja tuloksia ei välttämättä saada. Verkon nopeus voi olla huonompi kuin ilman virtuaaliverkkoa. VPN-yhteys on monimutkaisempi kuin tavallinen kotiverkko. Virtuaaliverkon salaus, sekä yhdistäminen etäpalvelimiin vaatii enemmän taustatyötä ja tämän seurauksena verkossa voi ilmentyä hidastumista. Tämän välttämiseksi käyttäjän tulisi panostaa valitsemalla hyvän ja luotettavan VPN-tarjoajan. Korkeatasoiset VPN-tarjoajat omaavat enemmän palvelimia eri alueilta, minkä ansiota käyttäjät pystyvät valitsemaan laajemmasta valikoimasta itselleen sopivan palvelimen erityisesti sellaisen, joka on lähempänä käyttäjän omaa sijaintiaan. (Barker 2021.)

Virtuaaliverkon käyttö suoratoiston kanssa on kuitenkin kannattavaa. Laajemman sisällön lisäksi, VPN pystyy tarjoamaan nopeampia verkkoyhteyksiä, sekä ennen kaikkea parantaa käyttäjän yksityisyyttä. Käyttäjän on valittava laadukas VPN-tarjoaja, jotta nämä ehdot täyttyisivät. (Barker 2021.)

9 OIKEAN VPN-PALVELUN LÖYTÄMINEN

Oikean VPN-palvelun löytäminen voi olla hankalaa erityisesti sellaiselle henkilölle, joka pyrkii huolehtimaan tiukasti omasta yksityisyydestään verkossa. Tavallinen kuluttaja sen sijaan hakee palvelua, josta mainostetaan eniten. VPN-tarjoajien määrä on suuri, mutta niin on myös niiden tekemät vääryydet ja erilaiset syytökset yksityisyydensuojan laiminlyönneistä. Täysin luotettavaa palvelua on siksi vaikea löytää. (Grauer & Huerta 2022.)

Ennen sopivan VPN löytöä, olisi kannattavaa käydä myös läpi omaa yksityisyyttä suojaavia tekijöitä. Näin vältyt turhilta lisäpalveluilta ja -maksuilta tilatessasi VPN-palvelua. Salasanojen hallinnointi, laitteiden salaaminen, verkkoselain ja -selain-laajennukset, verkonjako kodissa ovat niitä mihin kannattaa kiinnittää huomiota heti alkuun. Vältä salasanan uudelleenkäyttöä ja listaa kaikki käyttämäsi salasanat erikseen. Listauksella tarkoitamme, että olisi suositeltavaa ottaa ylös kaikki eri salasanat esimerkiksi muistiinpanoihin paperille. Mahdollista kaksi- tai monivaiheinen varmistus kaikille sivustoille ja sovelluksille. iOS-, sekä uusimmat Android-laitteet vaativat käyttäjän salaamaan laitteensa jo heti ensimmäisellä käytöllä, mutta esimerkiksi kannettavissa tietokoneissa on kannattavaa ottaa se käyttöön. (Grauer & Huerta 2022.)

Selaimille on olemassa laajennuksia, jotka auttavat estämään evästeiden ja yksilöivän mainonnan seuraamisen. Myös selainten asetuksista löytyy tällaisia työkaluja. Verkonjaon turvaaminen kotona onnistuu hankkimalla oikea reititin tai vaikkapa mesh-laitteisto, mikä pystyy päivittämään itsensä automaattisesti ja on mahdollista estää ulkopuolinen ylläpito. Yllä mainitut keinot eivät välttämättä takaa täyttä turvallisuutta verkossa oleskeluun. Jos käyttäjä haluaa viedä yksityisyyden suojansa vielä pitemmälle, lopputuloksena on kehno käyttökokemus. Esimerkiksi pelkästään JavaScriptin estäminen selaimessa vaikeuttaa huomattavasti selaamista. (Grauer & Huerta 2022.)

Luottamus Internet- sekä VPN-tarjoajia kohtaan voi vaihdella. Internet-tarjoajat voivat käyttää asiakkaan henkilökohtaista dataa markkinointia varten ja samoin voi tehdä myös VPN-tarjoajakin. Loppujen lopuksi kuluttajan verkkoliikenne tulee kulkemaan VPN-palvelinten kautta, joten hänen kuuluisi luottaa eniten VPN-tarjoajaan kuin siihen kuka tarjoaa hänelle verkkoyhteyden. (Grauer & Huerta 2022.)

10 VPN HYÖTY- JA HAITTAPUOLET SEKÄ TAPAUKSET NORDVPN JA EXPRESSVPN

VPN-teknologia perustuu tietoturvan edistämiseen käyttäjätasolla, mutta siihen liittyy kuitenkin haittapuolia. Hyöty- ja haittapuolien läpikäyminen on äärimmäisen tärkeää erityisesti, kun kyseessä yksilön oma toiminta verkossa ja se kuka sitä liikennettä valvoo.

10.1 Hyödyt

Virtuaalisen erillisverkon hyötynä on se, että se salaa käyttäjänsä tietoliikenteen verkossa sekä varmistaa, etteivät ulkopuoliset tahot pääse siihen käsiksi, kun taas salaamatonta tietoa voisi kuka tahansa katsella aivan vapaasti. Näin ollen, kun käyttäjä käyttää VPN-yhteyttä, niin hakkerit, kyberrikolliset sekä muut toimijat eivät pysty käsittelemään tätä tietoa. (Kaspersky 2021.)

Turvallinen salaus: Tietojen lukemiseen vaaditaan salausavain, ilman salausavainta tällaista salakirjoitettua koodia on hyvin vaikea murtaa, tai ainakin se veisi vuosikausia niin sanotulla väsytyshyökkäys-tavalla. VPN-yhteyden avulla käyttäjänsä toimet salataan yksityisten verkkojen lisäksi myös julkisissa verkoissa. (Kaspersky 2021.)

Sijainnin salaaminen: VPN-palvelimet toimivat käytännöllisesti katsoen käyttäjänsä välityspalvelimina Internetissä, koska niin sanottu demografinen sijaintitieto on lähtöisin toisen maan palvelimelta, niin käyttäjänsä todellista sijaintia ei pystytä selvittämään. Osa VPN-palveluista tallentavat tietoja käyttäjänsä toimista, mutta eivät anna niitä eteenpäin kolmansille osapuolille, mutta useimmat VPN-palvelut eivät tallenna palveluihinsa tällaisia lokitiedostoja käyttäjiensä toiminnoista. Tämä tarkoittaa sitä, että kaikki käyttäjänsä jäljet Internetissä jäävät loputtomasti piiloon. (Kaspersky 2021.)

Aluerajatun sisällön käyttäminen: Sisältö ei välttämättä ole aina käytettävänä kaikkialla. Eri palveluissa sekä verkkosivustoissa on yleensä sisältöä, jota voivat

käyttää vaan tietyn alueen käyttäjät. Tavallisesti yhteydet määrittävät käyttäjänsä sijainnin käyttäjänsä maan paikallisten palvelimien perusteella, tämä siis tarkoittaa sitä, että käyttäjä ei voi käyttää kotimaansa sisältöä ulkomailla tai toisinpäin. Tämä voidaan kiertää käyttämällä VPN-yhteyttä, jonka avulla pystytään liikkumaan virtuaalisesti maista sekä alueista toisiin, näin ollen käyttäjä pystyy käyttämään rajoitettua sisältöä. (Kaspersky 2021.)

Suojatun tiedon siirtäminen: Mikäli käyttäjä esimerkiksi tekee etätöitä, saattaa hän silloin tarvita pääsyn yrityksen sisäisen verkon tärkeisiin tiedostoihin, tietoturvasyistä tällainen edellyttää yhteyden suojaamista. Pääsyn saaminen yrityksen sisäiseen verkkoon edellyttää usein yhteyden virtuaaliseen erillisverkkoon. VPN-palveluiden hyötynä onkin, se että ne muodostavat yhteyden yksityisiin palvelimiin sekä hyödyntävät eri salausmenetelmiä estääkseen tietovuotojen syntymisen riskejä. (Kaspersky 2021.)

10.2 Haitat

Virtuaalisen erillisverkon käyttö saattaa pienentää käyttäjänsä nopeutta: Koska VPN reitittää sekä salaa Internet-yhteyden VPN-palvelimen kautta, niin yhteysnopeus voi laskea hieman. Tämän takia on järkevää testata VPN-nopeutta aina, kun testataan jotakin uutta palveluntarjoajaa. Useimmat niin sanotut Premium-tason VPN-palvelut, kuten ExpressVPN sekä NordVPN eivät hidasta käyttäjiensä Internet-nopeutta liikaa, mutta nopeus harvemmin pysyy täysin samana. (Bluvshtein 2021.)

Useimmat käyttäjät eivät kumminkaan huomaa mitään eroa, mutta se voi vaikuttaa käyttäjän nopeuteen silloin, kun tehdään jotakin, mikä vaatii paljon kaistanleveyttä sekä nopeampaa yhteyttä esimerkiksi videopelaaminen verkossa voi olla tällaista. Siksi käyttäjän kannattaakin tutkiskella eri VPN-palveluntarjoajia ja varmistaa mitkä palvelut soveltuvat pelaamiseen parhaiten. (Bluvshtein 2021.)

Jotkut palvelut saattavat estää VPN-käyttäjän: Internetissä on paljon sellaista sisältöä, mitkä on rajattu tiettyjen alueiden käyttäjien katsottaviksi, esimerkiksi Netflixillä on tällaista sisältöä. Tällaiset palvelut sulkevat ne käyttäjät ulos, joilla ei ole oikeutetta käyttää kyseistä sisältöä. Tämä johtuu siitä, että elokuvien jakajien kanssa on tehty sellaisia sopimuksia, jotka sallivat sisällön näkymisen vain tietyillä alueilla. (Bluvshtein 2021.)

Netflix ei ole ainut, joka käyttää alue-estoa, vaan näitä ovat esimerkiksi myös BBC iPlayer sekä HULU. Samaan aikaan eri maiden hallituksista estää sisältöä näkymästä, koska sellainen uhkaa heidän arvojaan. Tällaisissa tapauksissa käyttäjä voi kääntyä VPN-verkkojen puoleen ohittaakseen alueellisia estoja. Verkkosisältöjen estämisen lisäksi jotkut eri palvelut, verkkosivustot sekä hallitukset pyrkivät aktiivisesti kuitenkin estämää eri VPN-yhteydet. Tämä tarkoittaa siis sitä, että vaikka käyttäjä käyttäisikin VPN-yhteyttä saattaisi hän silti törmätä tilanteeseen, ettei hänellä olisi oikeutta nähdä valittua sisältöä. (Bluvshtein 2021.)

Netflixin tapauksessa Netflix yksinkertaisesti estää ne IP-osoitteet, jotka pyrkivät käyttämään palveluaan useilla yhteyksillä samanaikaisesti, koska VPN-käyttäjät jakavat palvelimen sekä siten myös IP-osoitteen, niin Netflix osaa tarkasti arvata milloin, joku käyttää VPN:ä. Lisäksi myös tietyt hallitukset ovat alkaneet estämään tunnettujen VPN-palveluntarjoajille kuuluvia IP-osoitteita. (Bluvshtein 2021.)

Virtuaalisen erillisverkon käyttäjän onneksi, jotkut VPN-palveluntarjoajat varmistavat käyttäjilleen sellaisen palvelimen, jota ei ole vielä estetty. Esimerkiksi ExpressVPN:llä ja NordVPN:llä on tuhansia palvelimia. Lisäksi nämä palveluntarjoajat ovat erinomaisia löytämään uusia VPN-palvelimia, joita eri hallitukset eivät ole vielä estäneet. (Bluvshtein 2021.)

Virtuaalisen erillisverkon käyttäminen ei ole laillista kaikissa maissa: VPN:n käyttäminen on laillista useimmissa maissa sekä useimmat suuret yritykset ja yhteisöt käyttävätkin virtuaalista erillisverkkoa osana turvallisuuttaan, mutta joitakin poikkeuksiakin löytyy. Jotkut hallitukset haluavat täysin valvoa sitä, että mitä heidän

kansalaisensa saavat nähdä Internetissä. Koska VPN:llä voidaan ohittaa eri valtioiden sensuurit. Tämän takia VPN:stä on tehty laiton työkalu joissakin totalitäärisissä maissa. (Bluvshtein 2021.)

Tietyissä maissa, kuten esimerkiksi Kiinassa, käyttäjä voi käyttää vain valtion hyväksymiä virtuaalisia erillisverkkoja. VPN:n käyttö ei siellä välttämättä ole laitonta, mutta sitä halutaan kontrolloida. Laadukkaat VPN-palveluntarjoajat, kuten vaikkapa NordVPN on kehittänyt erityisiä ’’ obfuskoituja palvelimia’’, joiden pitäisi silti olla käytettävissä Kiinan kaltaisissa maissa, vaikka hallitus ei niitä sallisi. Muissa maissa, kuten Pohjois-Koreassa virtuaalisen erillisverkon käyttäminen on kokonaan kiellettyä. Jos henkilö asuisi joissakin näistä maista missä VPN:n käyttö olisi joko rajattua tai kokonaan kiellettyä, voisi olla erittäin vaikeaa sekä jopa vaarallista suojata verkossa yksityisyyttään, turvallisuuttaa sekä vapauttaan. (Bluvshtein 2021.)

Käyttäjän on vaikea tarkistaa salauksen laatua: Voi olla vaikea tarkistaa, toimiiko VPN-palveluntarjoajat, niin kuin he lupaavat. Käyttäjä saa tietää tällaisesta vain, kun jokin asia menee pieleen. Keskimääräinen PC-käyttäjä ei ole perehtynyt salaustekniikkaan, joita käytetään tietojen salauskäytäntönä. Tämä tarkoittaa siis sitä, että keskimääräinen VPN-käyttäjä ei tiedä, miten VPN-salaus toimii, siksi he eivät myöskään tiedä, onko heidän käytössään oleva VPN-palvelu oikeasti turvallinen. (Bluvshtein 2021.)

Tästä syystä eri arviot ovat varsin tärkeitä tämän tekniikan kannalta. Ennen kuin käyttäjä sitoutuu VPN-palveluntarjoajan tilaukseen, kannattaa hänen lukea, mitä muut käyttäjät ovat olleet mieltä palvelusta. (Bluvshtein 2021.)

Internet-tapojesi kirjaaminen sekä mahdollinen jälleenmyynti kolmansille osapuolille: Kun käyttäjä muodostaa yhteyden VPN-palveluntarjoajaan, niin Internet-liikenne reititetään heidän palvelimiensa kautta. Ne salaavat käyttäjänsä tiedot sekä hänen oikean IP-osoitteensa ja korvaavat sen uudella. Käyttäjän on siis ostanut enemmän turvallisuutta sekä nimettömyyttä. Tämä tarkoittaa kuitenkin sitä,

että käyttäjän on luotettava siihen, ettei VPN-palvelu manipuloi tai väärinkäytä tietoja, jotka kulkevat heidän palvelimiensa kautta. Monet VPN-palveluntarjoajat pitävätkin kiinni sopimuksesta ja jättävät käyttäjän henkilökohtaiset tiedot kokonaan huomioimatta, he eivät kirjaa toimintoja eivätkä tallenna tietoja käyttäjistään. (Bluvshtein 2021.)

Jotkut VPN-palveluntarjoajat kirjaavat kuitenkin lokitietoja, etenkin monet ilmaiset VPN:t kirjaavat näitä, mutta myös jotkut palveluntarjoajat kertovat lisenssisopimuksissaan selvästi, että he saattavat kirjata käyttäjänsä selausaktiviteettia. Tällainen toiminta tietysti vesittää koko tarkoituksen hankkia virtuaalinen erillisverkko, siltikään nämä eivät ole pahimpia rikoksentekijöitä. (Bluvshtein 2021.)

Kaikista huolestuttavimmat tapaukset ovat kuitenkin niitä, jossa VPN-palveluntarjoaja on mainostanut, etteivät he kirjaa lokeja ollenkaan, mutta myöhemmin on paljastunut, että he todellisuudessa tekevätkin niin. Esimerkiksi kesäkuussa 2021 Alankomaiden kansallisen poliisin johtama maailmanlaajuisten lainvalvontaviranomaisten koordinoitu toiminta sulki VPN-palvelun, jota mainostettiin verkkorikollisten käyttämällä foorumilla. VPN-yhtiö lupasi käyttäjilleen mahdollisuuden salata verkkoliikenteensä kaksin- ja jopa kolminkertaisesti, jotta heidän sijaintinsa sekä henkilöisyytensä olisivat piilossa. (Bluvshtein 2021.)

DoubleVPN-nimisen palvelun sivusto takavarikoitiin 29. kesäkuuta. Lainvalvonta takavarikoi myös DoubleVPN:n hallussa olleita tietoja sen asiakkaistaan, kuten henkilökohtaisia tietoja, lokeja sekä tilastoja. Palvelimia takavarikoitiin eri puolilla maailmaa, joissa DoubleVPN oli ylläpitänyt sisältöä sekä heidän verkkotunnuksensa korvattiin lainvalvontasivuilla. Europol kertoi lehdistötiedotteessaan, että palvelun poistamisyritys sai tukea Alankomaiden, Saksan, Iso-Britannian, Kanadan, Yhdysvaltojen, Ruotsin, Italian, Bulgarian ja Sveitsin lainvalvonta- ja oikeusviranomaisilta sekä Europolilta ja Eurojustilta. (Ruiz 2021.)

Ennen kuin DoubleVPN:n nettisivut ajettiin alas, niin siellä mainostettiin palvelua sanoilla ei lokeja, mutta kuten asiassa on käynyt ilmi se, että todellisuudessa DoubleVPN:llä olikin lokitiedostoja asiakkaistaan. Tämä on siis hyvä muistutus kuluttajalle, että ennen kuin hän sitoutuu johonkin VPN-palveluntarjoajaan, olisi hänen suotavaa tarkastella kriittisesti useita eri lähteitä sekä VPN-arvosteluja. (Bluvshtein 2021.)

VPN-yhteyden katkeamiset mahdollisia: Useilla VPN-palveluntarjoajalla on ohjelmistoissaan pysäytyskytkin, joka on erittäin hyödyllinen ominaisuus. Jos yhteys VPN-palvelimeen katkeaa, niin käyttäjä jäisi ilman VPN:n tarjoamaa suojaa sekä anonymiteettiä. Siitä alkaen käyttäjän verkkokäyttäytyminen olisi linkitettynä todelliseen IP-osoitteeseen. (Bluvshtein 2021.)

Tämän estämiseksi pysäytyskytkin katkaisee välittömästi koko Internet-yhteyden ja palauttaa yhteyden vasta, kun yhteys VPN-verkkoon on taas luotu. Huonona puolena on se, että käyttäjä menettää yhteyden Internettiin, mutta laadukkaat VPN-palveluntarjoajat kohtaavat hyvin harvoin kyseistä ongelmaa. (Bluvshtein 2021.)

Ihmisen harhaluuloisuus koskemattomuudesta: Jotkut ihmiset uskovat, että heidän käyttämänsä VPN-yhteys tekee heistä täysin anonyymejä ja haittaohjelmat eivät voisi vaikuttaa heihin. Tämä johtaakin väärään uskomukseen, siitä että he olisivat jotenkin koskemattomia Internetissä. Tämä ei pidä ollenkaan paikkaansa, sillä haittaohjelmat pääsevät usein tietokoneille, kun käyttäjä tekee jotain mitä hänen ei pitäisi tehdä, täysin riippumatta yhteydestä. (Bluvshtein 2021.)

Käyttäjä voi silti altistua seuraaville haitoille, vaikka käyttäisikin vahvasti salattua sekä luotettavaa VPN-yhteyttä.

- Eri mainostajien, jäljittäjien, hakkereiden, tiedustelupalveluiden ja niin edelleen seurattavaksi.

- Joutua tietojenkalasteluhyökkäysten uhriksi klikkaamalla sähköpostien tai viestien haitallisia linkkejä.
- Saada tartunta tietyntyyppisistä haittaohjelmista lataamalla haitallisia tiedostoja tai käymällä epäselvissä verkkosivustoissa.
- Lukittua ulos tietyistä verkoista, tietokannoista, syvistä verkkosivustoista ja niin edelleen. (Bluvshtein 2021.)

Virtuaaliset erillisverkot varmistavat, että käyttäjän tiedot on salattu, IP-osoite on piilotettu sekä että käyttäjä voisi käyttää sisältöä, joka on estetty alueellansa. Ammattitaitoisen hakkerin tai tiedustelupalvelun jäljittäessä käyttäjän, IP-osoitteen lisäksi on olemassa muita tapoja tunnistaa käyttäjä. IP-osoite on vain ensimmäinen vihje, jota he saattavat etsiä. Sellaisenaan VPN-yhteys on kaikkea muuta, kuin lupa käyttäjälleen osallistua halventavaan, laittomaan tai holtittomaan käyttäytymiseen Internetissä, joten käyttäjän on aina käytettävä tervettä järkeä sekä oltava varovainen. (Bluvshtein 2021.)

Ilmainen VPN vai ilman: Jokainen ihminen tykkää saada jotain ilmaiseksi, minkä vuoksi jotkut haluavatkin kokeilla ilmaista VPN-palvelua ennen, kuin maksavat sellaisesta. Valitettavasti useat ilmaiset VPN-palveluntarjoajat eivät ole lainkaan kiinnostuneita käyttäjänsä yksityisyyden sekä anonymiteetin suojaamisesta verkossa, vaan haluavat tehdä rahaa. (Bluvshtein 2021.)

Esimerkiksi Hola VPN:n kaltaisten tarjoamia VPN-palveluiden käyttämistä kannattaa miettiä kahdesti. Tällaiset VPN:t eivät ole VPN-palvelun myymisen kannalla, vaan pikemminkin he myyvät käyttäjänsä henkilötietoja kolmansille osapuolille. Tämä on toisin kuin tilausmallilla varustetut VPN-palveluntarjoajat, jotka tekevät rahaa kuukausittaisista käyttömaksuista. (Bluvshtein 2021.)

Tämä on toinen syy siihen, miksi maksulliset VPN-palveluntarjoajat ovat huomattavasti turvallisempia. kuin ilmaiset. Vaarana on se, että ilmaista VPN käyttävän henkilön tiedot voivat päätyä mainostajien käsiin tai jopa vielä pahempaa. Käyttäjän kannattaakin miettiä ottaako ilmaisen VPN:n vai tulisiko paremmin toimeen

ilman virtuaalista erillisverkkoa, jos käyttäjä päättää valita, ettei hän ota VPN-palvelua tällöin kannattaa käyttää Adblockeria yhdessä muiden suojausominaisuuksien kanssa. (Bluvshtein 2021.)

Monilla ilmaisilla VPN-palveluntarjoajilla on käytössään myös data-, lataus- ja nopeusrajoituksia sekä mainoksia. Näiden rajoitusten vuoksi niiden käyttäminen koetaan epämiellyttävänä. Lisäksi useat ilmaiset VPN-sovellukset eivät ole turvallisia, koska niiden lataustiedostoihin on saatettu piilottaa vakoiluohjelmia tai haittaohjelmia. (Bluvshtein 2021.)

10.3 Tapaukset NordVPN & ExpressVPN

Seuraavassa kappaleessa halusimme nostaa esille kahden suuren VPN-markkinoilla olevien yrityksien moraalisesti arveluttavat toimet. Normaalisti kuluttaja ei etsisi yrityksen taustoja perinpohjaisesti, vaan tekisi ostopäätöksensä monesti arvostelujen perusteella.

10.3.1 NordVPN

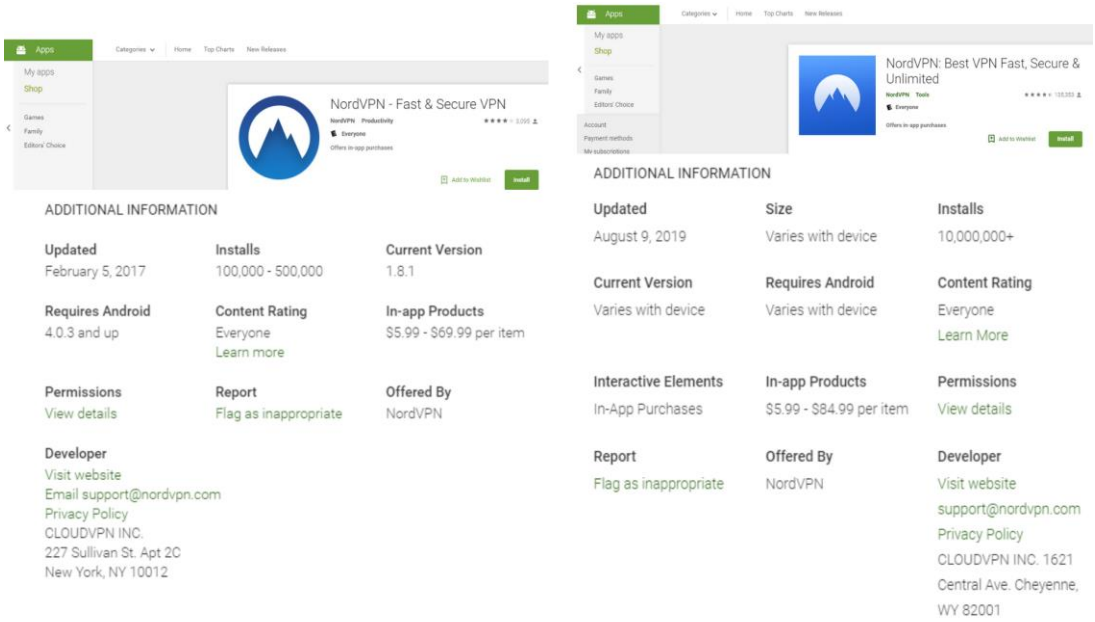
NordVPN:n laajat mainoskampanjat sosiaalisessa mediassa, sekä yleinen markkinointi verkossa edesauttoivat sen kasvua. Korkealaatuinen palvelu yksityisellä kuin myös yrityspuolella ylläpitää yhtiö korkeaa imagoa. Yhtiö sai alkunsa vuonna 2012 kun VPN-markkinat alkoivat vasta avautumaan ja on nykyisin VPN-listojen kärjessä. Yhtiö on rekisteröity Panamaan ja noudattaa kyseisen valtion tiukkoja lakeja tietoturvaa kohtaan. (MediaRadar 2021.) Panamassa ei ole pakollisia datan säilytystä vaativia lakeja, mikä tekee maasta täydellisen paikan VPN-tarjoajille, kuten esimerkiksi NordVPN:lle. (NordVPN 2021.)

NordVPN:ä on kritisoitu sen ympärillä toimivien yritysten, sekä osallisten sekavuudesta. Yhtiö kertoo sivuillaan tulleensa perustetuksi neljän lapsuudenystävän toimesta, joita ei kuitenkaan nimetty. Yhtiön rahaliikennettä valvova Tefincom S.A. toimii Panamassa, mutta samoin myös Kyproksella. Rahaliikenne kulkee kuitenkin

Panaman sijasta Kyproksen kautta, mikä herättää epäilyksiä rahanpesusta koska Kypros tunnetaan veroparatiisina. (Whistleblowing Cosmonaut 2020.)

Kuva 7. Euroopan Komission Arvonlisävero numeron rekisteri (Euroopan Komissio 2021.)

Kuvassa 7 on haettu EU-komission sivustolta yhtiön arvonlisänumerolla rahaliikennettä. Yhtiö on aiemmin antanut ilmi, heidän toimintansa mukaan lukien rahaliikenteen sijoittuvan Panamaan, mutta komission rekisteristä selviää sijainnin olevankin Kypros.



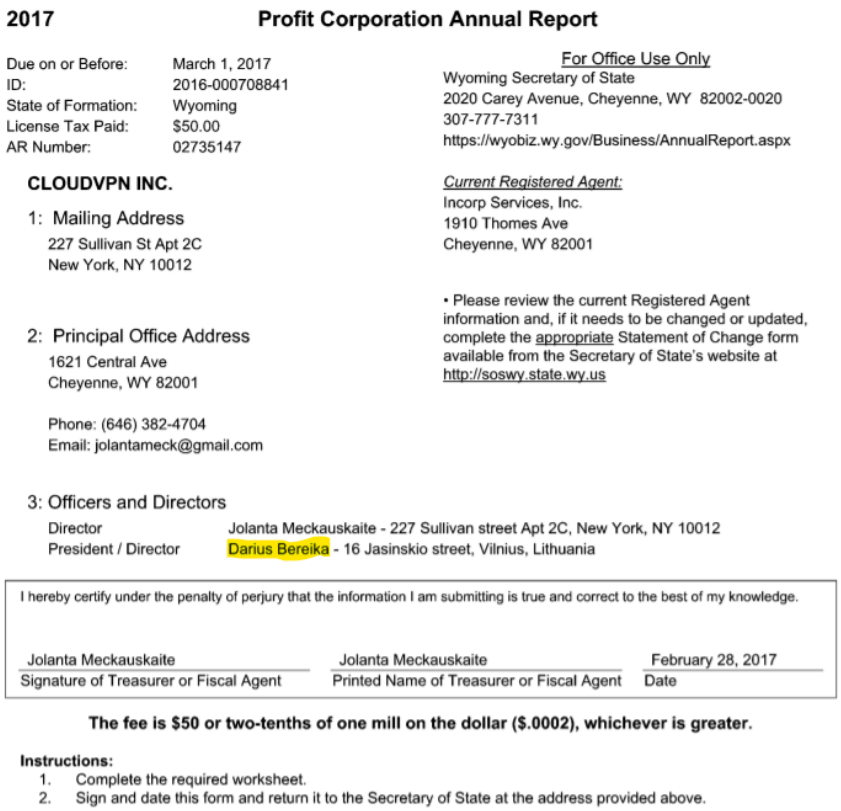
Kuva 8. NordVPN-sovellus Google Play Storessa vuosien 2017–2019 aikoina (Wayback Machine 2017; Wayback Machine 2019.)

Kuvassa 8 näkyy, että vuonna 2017, Android-puhelimille suunnattu Play-kauppa sisälsi NordVPN:n listallaan, mistä asiakkaat myös pääsivät näkemään, kuka oli sovelluksen kehittäjä. NordVPN:n kehittäjäksi listattiin CloudVPN, helmikuusta 2017 elokuuhun 2019 asti. CloudVPN listattiin myös Amazon.comissa NordVPN:n jälleenmyyjäksi. Kyseinen listaus on kuitenkin vanhentunut. CloudVPN on yhdysvaltalainen yritys, mikä herättää kysymyksiä käyttäjien yksityisyydensuojasta. (Whistleblowing Cosmonaut 2020.)

CloudVPN vuoden 2017 arkistoista käy ilmi, että yrityksen johtajana, sekä hallintoneuvoston puheenjohtajana työskenteli henkilö nimeltä Darius Bereika. Sama henkilö oli Tesonet-nimisen yhtiön toimitusjohtaja. Tesonet omistaa yrityksen nimeltä Oxylabs. Tesonet tuottaa muun muassa kyberturvapalveluja yrityksille. Oxylabs sen sijaan tuottaa datan keräämistä varten soveltuvia palveluita yrityksille. Henkilö, joka oli yhteyksissä NordVPN:n ja CloudVPN:n oli myös kytköksissä yritykseen, joka tuottaa datan keräämiseen soveltuvia palveluita. Molemmat, sekä Tesonetin että Oxylabsin toimistot sijaitsevat samassa kaupungissa Liettuassa, Vilna. (Whistleblowing Cosmonaut 2020.)

Vuonna 2017 Liettuassa tehtiin kantelu EU:n oikeusministeriölle. Maan kerrottiin keräävän tietoja asukkaistaan vanhentuneen EU direktiivin nojalla, mikä poistettiin EU:n toimesta jo kaksi vuotta sitten. Kantelun mukaan kyseinen laki rikkoo ihmisoikeuksia. (Human Rights Monitoring Institute 2017.) Liettua kuuluu myös MLAT eli Mutual Legal Assistance Treaties -maihin. Tähän kuuluvat maat voivat jakaa muun muassa Yhdysvaltojen kanssa tietoja mahdollisista epäilyistä rahanpesu, veropetos ja muihin rikoksiin liittyvissä asioissa. (U.S. Department of State 2017.)

Oxylabsin oikeudellisia tietoja ei ole helposti saatavilla. Ainoa helposti saatavilla oleva lähde on kuvankaappaus, mikä löytyy sivustolle medium.com kirjoitetusta blogista. Blogissa viitataan Whois-arkistoon, mistä voi selvittää sivustojen verkkotunnuksia, mutta pääsy kyseiseen tietoon on maksullista. (Whistleblowing Cosmonaut 2020.) NordVPN on nykyisin Nord Security:n omistuksessa. Nord Security:n toimitusjohtaja Tom Okman on myös yksi liettualaisen yrityksen Tesonetin perustajista. (Gewirtz 2022.)



2017 **Profit Corporation Annual Report**

Due on or Before: March 1, 2017
ID: 2016-000708841
State of Formation: Wyoming
License Tax Paid: $50.00
AR Number: 02735147

For Office Use Only
Wyoming Secretary of State
2020 Carey Avenue, Cheyenne, WY 82002-0020
307-777-7311
https://wyobiz.wy.gov/Business/AnnualReport.aspx

CLOUDVPN INC.

1: Mailing Address
227 Sullivan St Apt 2C
New York, NY 10012

Current Registered Agent:
Incorp Services, Inc.
1910 Thomes Ave
Cheyenne, WY 82001

• Please review the current Registered Agent information and, if it needs to be changed or updated, complete the appropriate Statement of Change form available from the Secretary of State's website at http://soswy.state.wy.us

2: Principal Office Address
1621 Central Ave
Cheyenne, WY 82001

Phone: (646) 382-4704
Email: jolantameck@gmail.com

3: Officers and Directors
Director — Jolanta Meckauskaite - 227 Sullivan street Apt 2C, New York, NY 10012
President / Director — Darius Bereika - 16 Jasinskio street, Vilnius, Lithuania

I hereby certify under the penalty of perjury that the information I am submitting is true and correct to the best of my knowledge.

Jolanta Meckauskaite	Jolanta Meckauskaite	February 28, 2017
Signature of Treasurer or Fiscal Agent	Printed Name of Treasurer or Fiscal Agent	Date

The fee is $50 or two-tenths of one mill on the dollar ($.0002), whichever is greater.

Instructions:
1. Complete the required worksheet.
2. Sign and date this form and return it to the Secretary of State at the address provided above.

Kuva 9. Arkistokuva CloudVPN Inc Vuodelta 2017 (Wyoming Secretary of State 2021.)

Vaikka NordVPN:n kytköksiä Liettuaan on epäilty, kuvassa 9 näkyy yhteyksien kuitenkin pitävän paikkaansa. CloudVPN kehitti NordVPN:n mobiilisovelluksen ja arkistokuvasta käy ilmi, että yhtiön johdossa työskentelee Liettuassa asuva henkilö nimeltä Darius Bereika.

Tavallinen VPN:stä maksava asiakas ei välttämättä tee taustaselvitystä käyttämästään palvelusta heti. Yleisesti voitaisiin olettaa, että tietoturvaan ja yksityisyyteen perustettu yhtiö, joka myös omistaa suuren osan kyseisestä asiakaskunnasta tekee asiansa oikein eikä ole millään tavoin epäilyksen alainen. NordVPN tilanne tulisi toimia kuitenkin herätteenä. Vaikka yhtiö markkinoi itseään laajasti tai on suosittu, ei välttämättä tarkoita, että siihen tulee suhtautua varomatta. Voitaisiin sanoa, että vastuu on sekä kuluttajalla että palvelua tarjoavalla yrityksellä. Vaikka lopullinen ostopäätös on kuluttajalla, silti yrityksellä on myös vastuu olla avoin taustoistaan.

10.3.2 ExpressVPN

Yksi tunnetuimmista VPN-palveluista ExpressVPN joutui syyskuussa 2021 Edward Snowdenin kritiikin kohteeksi. Snowden suositteli VPN-käyttäjiä välttämään kyseistä tarjoajaa sen johtajan, sekä omistajien vaihdoksen vuoksi. (Linnake 2021.)

ExpressVPN tietohallintojohtajana toimii Daniel Gericke, entinen yhdysvaltalainen tiedusteluagentti. Hän työskenteli ilman työnantajansa lupaa Project Raven -nimisen hankkeen parissa. Project Raven on Yhdistyneiden arabiemiirikuntien vakoilutyökalu, millä pystyy valvoa toisinajattelijoita. (Linnake 2021.) Yhdysvaltojen oikeusministeriö on nostanut syytteen Gerickiä ja kahta muuta hankkeessa toiminutta työntekijää kohtaan. Kaikki kolme syytettyä ovat kuitenkin suostuneet tekemään yhteistyötä viranomaisten kanssa, sekä maksavansa sakot. (Sharma 2021.)

ExpressVPN antoi myös oman lausuntonsa Snowdenin kritiikin seurauksena. Palkattuaan Gericken vuonna 2019, yhtiö ei tiennyt yksityiskohtia hänen aiemmasta työstään. Yhtiö sanoi, ettei hyväksy Project Ravenia, mutta arvostaa Gericken asiantuntemusta ja apua, joilla he turvanneet asiakkaansa. Heidän mukaansa tehokasta suojelua vaatii myös tietoa ja ymmärrystä vastapuolelta. (Linnake 2021.)

ExpressVPN myytiin brittiläisisraelilaiselle Kape Technologies omistukseen noin miljardilla dollarilla, tehden siitä suurimman VPN-markkinoilla solmitun kaupan. Kape Technologies on aiemmin toiminut eri nimellä ja sen historia on myös hyvin sekalainen. (Linnake 2021.) Sen perusti vuonna 2011 miljonääri Teddy Sangi, joka on suorittanut vankeutta sisäpiirikaupasta. Yhtiön nimi oli silloin Crossrider ja myi muun muassa työkaluja, millä he pystyivät sisällyttämään mainoksia muiden yhtiöiden verkkosivuille kaapaten muille kuulunutta mainostilaa ja tuloja, sekä dataa. (Gewirtz 2021.) Virustutkat usein nimesivät yhtiön haittaohjelmien jakelijaksi (Linnake 2021). Muutettuaan nimensä, Kape Technologies alkoi ostamaan muita yhtiöitä eri VPN- sekä kyberturvasektoreilta vuosina 2017–2021 (Gewirtz 2021).

11 TULEVAISUUS

VPN-teknologian kasvu ja markkinointi tavallisille kuluttajille on merkki aiheen suuresta huomiosta ja kiinnostuksesta. Monelle VPN on jo tullut suurelta osin tutuksi ja ymmärrys sen toiminnasta on varmasti kasvanut vuosien kuluessa. Kuinka VPN-palvelut tulevat suhtautumaan oman toimintansa läpinäkyvyyteen tulee herättämään kysymyksiä erityisesti kuluttajapuolella. Miten yritykset, erityisesti suoratoistopalvelut tulevat suhtautumaan oman sisällönjakoonsa? Kuinka palveluntarjoaja pystyy rakentaa ja ylläpitää luottamusta käyttäjille, sekä erityisesti IT-maailmassa?

11.1 Virtuaalisen erillisverkon tulevaisuus pandemian jälkeisessä maailmassa

Ennen pandemiaa useat asiantuntijat uskoivat VPN:n olevan tiensä päässä, mutta pandemian aikana Virtuaalisesta erillisverkosta tuli elinehto etätyöntekijöille tehdäkseen työnsä. Siksi VPN-verkkojen merkitys muuttui merkittävästi vuoden 2020 alussa, koska koronaviruspandemia aiheutti valtavan digitaalisen muutoksen monille yrityksille sekä toimistotyöntekijöille. Ennen pandemiaa alkaneet VPN-trendit kiihtyivät muutamassa päivässä. (Slattery 2020 a.)

11.2 Virtuaaliset erillisverkkoyhteydet nykyisin sekä niiden tulevaisuus

Pandemian aikana toimistotyöntekijöiden siirtyminen työpaikoilta kotiympäristöön loi uuden pulman. Kuinka organisaatioiden pitäisi tukea työntekijöitään, jotta he voisivat käyttää yritysten resursseja kotoa käsin, niin tietokoneilla kuin mobiililaitteilla. (Slattery 2020 a.)

Perinteinen VPN rakentaa raskaan asiakasmallin (fat client) avulla suojatun tunnelin asiakaslaitteesta yritysverkkoon. Kaikki tietoliikenneyhteydet käyttävät tätä tunnelia, mutta tämä malli tulee kuitenkin hyvin kalliiksi, koska päästääkseen julkisiin pilviresursseihin on ensin kuljettava VPN-tunnelin kautta yrityksen sivustolle, joka puolestaan välittää pääsyn takaisin Internet-pohjaisille pilvipalvelutarjoajille. Tätä kutsutaan nimellä hairpinning. (Slattery 2020 a.)

VPN-verkkojen tulevaisuuden kannalta päätejärjestelmien kasvava teho tulee helpottamaan ohjelmistopohjaisen VPN-teknologian siirtymistä päätepisteisiin. VPN-tekniikat kehittyvät hyödyntämään paikallisia prosessiominaisuuksia, jotka tulevat helpottamaan VPN-palveluita käyttäjille sekä verkon ylläpitäjille. Verkon ylläpitäjät tulevat hallitsemaan jatkossa VPN:n keskusjärjestelmien kautta. (Slattery 2020 a.)

Virtuaalisen erillisverkon tulevaisuus on hyvin sekalaista. Asiantuntijoiden joukossa väitetään, että laitteistot eivät ole tarpeellisia, kun taas toiset väittävät, että niitä tarvitaan yhä, koska jotakin on yhä tehtävä kiinteiden yhteyksien avulla. Todennäköisemmin x86-laskentajärjestelmät, jotka suorittivat aiemmin laitteistoissa olleita toimintoja, tulevat korvaamaan joitakin erillisiä laitteistoja etenkin verkon reunalla, jossa hajautetut laskentaresurssit ovat helposti saatavilla. Verkon ydin vaatii edelleen nopeuksia, joita vain erilliset laitteistot pystyvät tarjoamaan lähitulevaisuudessa. (Slattery 2020 a.)

VPN-verkot voivat myös alkaa toimimaan kuten ohjelmistomääritetyt WAN-tuotteet, joissa yhteys on riippumaton taustalla olevasta fyysisestä verkossa, kuten langallisesta, langattomasta tai matkapuhelimesta ja sekä sen osoitteesta. Näiden VPN-järjestelmien tulisi käyttää useita polkuja sekä vaihtaa niiden välillä läpinäkyvästi. (Slattery 2020 a.)

Yrityksien Virtuaalisista erillisverkoista löytyvät seuraavat kaksi päätoimintoa:

1. Tietovirtojen salaus sekä suojatut tietoliikenneyhteydet.
2. Päätepisteen suojaaminen luvattomalta käytöltä.

Salaustekniikan suoraviivainen käyttö on viestinnän turvaamista. Salaustekniikka on suhteellisen vanha ja se on sisäänrakennettu nykyaikaisiin selaimiin, mikä tekee selainten käyttämisestä helppoa. SSL tai TLS-VPN:t voivat tarjota tämän toiminnon. (Slattery 2020 a.)

Nykyaikaiset VPN-järjestelmät suojaavat päätepisteitä luvattomalta käytöltä, koska nämä järjestelmät edellyttävät, että kaikki verkkoviestinnät kulkevat VPN-verkon kautta päätepisteiden sekä yrityksen VPN-keskittimen välillä. Muut yrityksen resurssit, kuten palomuurit, tunkeutumisen havaitsemisjärjestelmät ja tunkeutumisen estämisjärjestelmät, suojaavat päätepisteitä sisällön suodatuksella, haittaohjelmien havaitsemisella ja tunnettujen huonojen toimijoiden suojatoimilla. (Slattery 2020 a.)

Tulevaisuudessa IT-alan ammattilaisten on syytä odottaa näkevänsä kyseisiin tietoturvatoimintoihin sovellettavaa tekoälyn sekä koneoppimisen esimerkkejä niiden tehokkuudesta ilman, että verkko- tai tietoturvajärjestelmänvalvojan tuki lisääntyisi. (Slattery 2020 a.)

VPN-polut vähenevät, kun päätepiste kommunikoi Internet-pohjaisten resurssien, kuten SaaS-järjestelmien kanssa. Päätepisteen on ensin lähetettävä tiedot VPN-keskittimelle, joka puolestaan välittää tiedot pilvipohjaiseen SaaS-sovellukseen, joka lisää näin ollen verkon viivettä. Lisäksi verkon kuormitus kasvaa VPN:n sisällä, koska SaaS-sovellus käyttää myös omaa salaustaan. (Slattery 2020 a.)

Jaettu tunnelointi on mahdollinen ratkaisu tällaiseen tehottomuuteen, mutta IT-tiimien on valittava VPN-liityntäpisteet huolellisesti tietoturva-aukkojen välttämiseksi. Integrointi älykkäiden DNS-palvelinten kanssa, kuten vaikkapa Cisco Umbrellan, mahdollistaa jaetun tunneloinnin tiettyihin sivustoihin verkon tai turvallisuuden ylläpitäjien valvonnassa. (Slattery 2020 a.)

Vielä parempi turvallisuusasenne perustuu nollaluottamusmalliin, joka olettaa, että päätepisteet ovat vaarassa riippumatta niiden sijainnista. Siitä on tullut uusi standardi, jota verkkojen tulisi noudattaa. Nollaluottamustietoturvakomponentit sisältävät sallittujen luettelon sekä mikrosegmentoinnin. VPN-verkkojen tulevaisuus sisältääkin automaattisia menetelmiä näiden suojaustoimintojen luomiseen

sekä ylläpitoon. IT-ammattilaiset voivat siis odottaa, että VPN-teknologian tulevaisuus tulee lisäämään turvallisuutta sekä vähentämään samalla turvallisuuden toteuttamiseen sekä ylläpitämiseen tarvittavia ponnisteluja. (Slattery 2020 a.)

12 YHTEENVETO

Opinnäytetyön tarkoituksena oli käydä läpi muun muassa virtuaaliseen erillisverkon historiaa, toimintaa, sen käsitteitä, nykymarkkinatilannetta, COVID-19-pandemian vaikutusta sekä tulevaisuutta. Työn tarkoituksena oli tuottaa kattava kokonaisuus kyseisestä aihepiiristä ja erityisesti tehdä alalle kouluttautuville ja työskenteleville, sekä myös ulkopuolisille henkilöille. Työssä käydään läpi aihetta neutraalista näkökulmasta, jotta lukija pystyisi itse kehittämään oman mielipiteensä: mitä ajatuksia hänelle nousee virtuaalisesta erillisverkosta ja onko hänellä mahdollista tarvetta siihen.

Työtä tehdessä opimme, että virtuaalinen erillisverkko ei ole vain pelkkä teknologia: se toimii sekä yksilövapautta edistävänä työkaluna, mutta myös kätkee itseensä oman varjopuolensa. Se edistää käyttäjän omaa yksityisyyttä ohittamalla esimerkiksi sensuuria, sekä rajoitettua sisältöä. Sen tarkoituksena ei ole korvata virustorjuntaohjelmia, vaan toimia niiden rinnalla. Kääntöpuolena siitä pyrkii hyötymään monet omia etujaan ajavat tahot turvallisuuden nimissä: esimerkiksi ilmaiset tai auktoritaaristen valtioiden omat VPN-palvelut.

Kehitimme lopuksi työn, mikä kattaa laajasti virtuaalista erillisverkkoa ja sitä käsitteleviä osia niin yritysten kuin myös tavallisen kuluttajan näkökulmasta. Kasvatimme osaamistamme aiheesta, mitä emme olisi välttämättä kohdanneet tavallisesti. Vaikka meiltä löytyykin jo ennestään kokemusta, sekä käyttöä VPN-palveluista, opimme paljon enemmän aiheesta kuin oletimme kohtaavamme. Toivomme että tämä työ tulisi jatkossa olemaan mahdollinen opetuskäyttöön soveltuva materiaali, sekä myös aloitusopas aiheesta kiinnostuneille.

LÄHTEET

Anttila, V. 2021. Mikä on VPN ja miten se toimii? Aloittelijan opas 2021. Viitattu 11.10.2021. https://fi.wizcase.com/blog/aloittelijan-kattava-vpn-opas/

Apple Inc. 2021. macOS:n käyttöopas: VPN-yhteyden käyttöönotto Macissa. Viitattu 11.10.2021. https://support.apple.com/fi-fi/guide/mac-help/mchlp2963/11.0/mac/11.0

Barker, L. 2021. Is it worth using a VPN when streaming?. Viitattu 30.05.2021. https://www.tomsguide.com/news/is-it-worth-using-a-vpn-when-streaming

Bluvshtein, C. 2021. Disadvantages of a VPN. Viitattu 25.08.2021. https://vpnoverview.com/vpn-information/disadvantages-vpn/

Euroopan Komissio 2021. Verotus ja Tulliliitto. VIES. Viitattu 31.08.2021. https://ec.europa.eu/taxation_customs/vies/

Fawkes, G. 2021. VPN-prokollien vertailu: PPTP, L2TP, OpenVPN, SSTP ja IKEv2. Viitattu 30.03.2021. https://fi.vpnmentor.com/blog/vpn-prokollien-vertailu-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

Fitzgibbons, L. & Gittlen, S. 2020. What is zero trust? Ultimate guide to the network security model. Viitattu 02.12.2021. https://www.techtarget.com/searchsecurity/definition/zero-trust-model-zero-trust-network

Fuetsch, A. 2020. How a Software-Centric Network Keeps Business Customers Connected in a Highly Safe Manner. Viitattu 22.06.2021. https://about.att.com/innovation-blog/2020/04/anira.html?CJPID=3586864&EI=20130822074250E&CI=CJ_AFFINITY&RI=CJ1&RD=37922

Gewirtz, D. 2021. Trust, but verify: An in-depth analysis of ExpressVPN's terrible, horrible, no good, very bad week. Viitattu 22.09.2021.

https://www.zdnet.com/article/trust-but-verify-an-in-depth-analysis-of-expressvpns-terrible-horrible-no-good-very-bad-week/

Gewirtz, D. 2022. Meet Nord Security: The company behind NordVPN wants to be your one-stop privacy suite. Viitattu 12.02.2022. https://www.zdnet.com/article/meet-nordsec-the-company-behind-nordvpn-wants-to-be-your-one-stop-privacy-suite/

Google Chrome Web Store. 2021. Viitattu 03.06.2021. https://chrome.google.com/webstore/search/vpn?hl=fi&_category=extensions

Grauer, Y. & Huerta, D. 2022. The Best VPN Service. Viitattu 15.01.2022. https://www.nytimes.com/wirecutter/reviews/best-vpn-service/

Hodge, R. 2019. All the VPN terms you need to know. Viitattu 22.06.2021. https://www.cnet.com/tech/services-and-software/all-the-vpn-terms-you-need-to-know/

Hodge, R. 2020. a. VPN use surges during the coronavirus lockdown, but so do security risks. Viitattu 09.06.2021. https://www.cnet.com/tech/services-and-software/vpn-use-surges-during-the-coronavirus-lockdown-but-so-do-security-risks/

Hodge, R. 2020. b. This VPN built on blockchain could be the next step in privacy tech. Viitattu 06.07.2021. https://www.cnet.com/tech/services-and-software/this-vpn-built-on-blockchain-could-be-the-next-step-in-privacy-tech/

Hodges, N. 2020. Proxy server: what is it and what does it do?. Viitattu 03.06.2021. https://surfshark.com/blog/proxy-server

Human Rights Monitoring Institute. 2017. Lithuania Continues Mass Collection of Personal Data Under Invalid EU Directive. Viitattu 20.08.2021. https://www.liberties.eu/en/stories/lithuania-mass-data-retention/12859

Johnson, J. 2021. VPN usage increase in selected countries impacted by the coronavirus between March 8 and March 22, 2020. Viitattu 30.03.2021. https://www.statista.com/statistics/1106137/vpn-usage-coronavirus/

Kaspersky. 2021. Mikä VPN on ja kuinka se toimii?. Viitattu 30.05.2021. https://www.kaspersky.fi/resource-center/definitions/what-is-a-vpn

Kataja, J. 2017. Proxy Eli Välitys – Virtuaalipalvelimen Käyttö Proxy Palvelimena. Viitattu 04.06.2021. https://www.zoner.fi/proxy-eli-valityspalvelin-virtuaalipalvelimen-kaytto-proxy-palvelimena/

Kirvan, P. 2020. Plan a VPN and remote access strategy for pandemic, disaster. Viitattu 18.06.2021. https://searchnetworking.techtarget.com/tip/Preparing-for-a-disaster-When-remote-employees-overload-your-VPN

Klimas, M. 2021. Proxy vs. VPN: what's the difference?. Viitattu 03.06.2021. https://surfshark.com/blog/vpn-vs-proxy

Klusaite, L. 2020. Miten asentaa VPN reitittimeen?. Viitattu 22.10.2021. https://nordvpn.com/fi/blog/asentaa-vpn-reitittimeen/

Krohn, D. 2021. Fourteen Eyes -maat: VPN-käyttäjän tulee tietää tämä. Viitattu 20.05.2021. https://fi.vpnmentor.com/blog/five-eyes-maat-tai-nine-eyes-fourteen-eyes-erittain-tarkea-asia-vpn-kayttajille/

Linnake, T. 2021. Edward Snowden varoittaa suositusta salauspalvelusta: ''Sinun ei pitäisi olla käyttäjä''. Viitattu 22.09.2021. https://www.is.fi/digitoday/tietoturva/art-2000008278319.html

McCarthy, N. 2020. VPN Usage Surges During COVID-19 Crisis [Infographic]. Viitattu 09.06.2021. https://www.forbes.com/sites/niallmccarthy/2020/03/17/vpn-usage-surges-during-covid-19-crisis-infographic/

MediaRadar. 2021. NordVPN Advertiser Profile. Viitattu. 20.08.2021. https://advertisers.mediaradar.com/nordvpn-advertising-profile

NordVPN. 2021. Jurisdiction we operate in. Viitattu 20.08.2021. https://support.nordvpn.com/General-info/Features/1061811142/Jurisdiction-we-operate-in.htm

OpenVPN. 2021. Why Companies Are Turning To VPNs During The CoronaVirus Outbreak. Viitattu 17.06.2021. https://openvpn.net/blog/why-companies-are-turning-to-vpns-during-the-coronavirus-outbreak/

Paul, I. 2021. Should You Use VPN for Gaming?. Viitattu 04.02.2021. https://www.howtogeek.com/711245/should-you-use-a-vpn-for-gaming/

PureVPN Support. 2020. OpenVPN Script Method for DD-WRT. Viitattu 26.05.2022. https://support.purevpn.com/openvpn-script-method-for-dd-wrt

Ruiz, D. 2021. Police seize DoubleVPN data, servers, and domain. Viitattu 26.08.2021. https://blog.malwarebytes.com/cybercrime/2021/06/police-seize-doublevpn-data-servers-and-domain/

Sharma, M. 2021. Edward Snowden warns ExpressVPN users to ditch the service immediately. Viitattu 22.09.2021. https://www.techradar.com/news/edward-snowden-warns-expressvpn-users-to-ditch-the-service-immediately

Selmeczy, P. 2016. The Ultimate DD-WRT Guide. Viitattu 22.10.2021. https://pro-privacy.com/vpn/guides/dd-wrt

Slattery, T. 2020. a. The future of VPNs in a post-pandemic world. Viitattu 16.09.2021. https://www.techtarget.com/searchnetworking/tip/The-future-of-VPNs-in-a-post-pandemic-world

Slattery, T. 2020. b. What does a VPN concentrator do?. Viitattu 20.09.2021. https://www.techtarget.com/searchnetworking/answer/How-does-the-VPN-concentrator-work

U.S. Department of State. 2017. Treaties, Agreements, and Asset Sharing. Viitattu 20.08.2021. https://2009-2017.state.gov/j/inl/rls/nrcrpt/2014/vol2/222469.htm

Valentine, O. 2018. VPNs Are Primarily Used to Access Entertainment. Viitattu 30.03.2021. https://blog.gwi.com/chart-of-the-day/vpns-are-primarily-used-to-access-entertainment/

Wayback Machine 2017. NordVPN – Fast & Secure VPN. Viitattu 20.08.2021. https://web.archive.org/web/20170221004432/https:/play.google.com/store/apps/details?id=com.nordvpn.android&hl=en

Wayback Machine 2019. NordVPN: Best VPN Fast, Secure & Unlimited. Viitattu 20.08.2021. https://web.archive.org/web/20190826075815/https:/play.google.com/store/apps/details?id=com.nordvpn.android&hl=en

Welekwe, A. 2021. Kuinka asentaa VPN reitittimeen. Viitattu 22.10.2021. https://fi.vpnmentor.com/blog/kuinka-asentaa-vpn-reitittimeen/

Whistleblowing Cosmonaut (nimimerkki). 2020. NordVPN-Moral compass not included. Viitattu. 20.08.2021. https://medium.com/@whistleblowingcosmonaut/nordvpn-moral-compass-not-included-68b5e03c0c53

Wyoming Secretary of State 2021. Business Center. Detail. CloudVPN Inc. History. 2017 Original Annual Report PDF. Viitattu 20.08.2021. https://wyobiz.wyo.gov/Business/FilingDetails.aspx?eFNum=005203253040182072024101188243235057222189038105