Teemu Urpilainen

OPENVPN-PALVELIMEN ASENNUS GCP-YMPÄRISTÖÖN

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutus
Elokuu 2022

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Elokuu 2022	**Tekijä/tekijät** Teemu Urpilainen
Koulutus Tieto- ja viestintätekniikka		☒ AMK ☐ YAMK
Työn nimi OPENVPN-PALVELIMEN ASENNUS GCP-YMPÄRISTÖÖN		
Työn ohjaaja Tero Niemi		**Sivumäärä** 28
Työelämäohjaaja Toni Penttilä		

Tämän opinnäytetyön tavoitteena oli perehtyä erilaisiin etäyhteystekniikoihin ja Googlen pilviympäristön toimintaan. Teoriaosuudessa keskitytään erilaisiin etäyhteystekniikoihin ja opinnäytetyön toiminnallisessa osuudessa asennettiin virtuaalikone Googlen pilviympäristöön ja testattiin sen soveltuvuus OpenVPN-palvelinohjelmiston suorittamiseen.

Opinnäytetyön tavoitteet saavutettiin niin oppimistavoitteiden kuin toiminnallisenkin osuuden osalta.

Mahdollisia jatkokehityspolkuja opinnäytetyölle on tietoturvan parempi huomioiminen palvelimella, etäyhteyden muodostamisen automatisoiminen ja helpompi hallinta.

Asiasanat
Etäyhteys, GCC, Google, OpenVPN, Palvelin, VPN

centria
University of Applied Sciences

ABSTRACT

Centria University of Applied Sciences	**Date** August 2022	**Author** Teemu Urpilainen
Degree programme Information and communication technologies		
Name of thesis INSTALLING AN OPENVPN SERVER TO THE GOOGLE CLOUD PLATFORM		
Instructor Tero Niemi		**Pages** 28
Supervisor Toni Penttilä		

The goal of this thesis was to learn about different remote connection technologies and the operation of Google's cloud environment. The theoretical part focused on various remote connection technologies, and in the functional part of the thesis a virtual machine was installed in Google's cloud environment and its suitability for running the OpenVPN server software was tested.

The objectives of the thesis were achieved both in terms of learning objectives and the functional part.

Possible further development paths for the thesis are the better consideration of information security on the server, automating the establishment of a remote connection and easier management.

Key words
GCC, Google, OpenVPN, Server, Remote connection, VPN

KÄSITTEIDEN MÄÄRITTELY

AES

Advanced Encryption Standard on yksi salausmenetelmistä.

DH

Diffie-Hellman-algoritmi.

GCP

Google Cloud Platform on Googlen tarjoama pilvipalvelupaketti, josta on mahdollista ostaa laskentatehoa, tallennustilaa ja tietokantapalvelua.

TLS / SSL

Transport Layer Security / Secure Socket Layer on yleisesti käytössä oleva salausprotokolla, jota käytetään salaamaan yhteys päästä päähän internet verkon yli. Salausprotokollan toiminta perustuu varmenteisiin, joiden avulla voidaan varmistua, että yhteys on muodostettu juuri sinne, minne pitääkin.

VPN

Virtual private network on etäyhteyksissä käytetty teknologia, joka mahdollistaa yksityisen verkon käyttämisen julkisen verkon ylitse.

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

1 JOHDANTO 1

2 ETÄYHTEYSPROTOKOLLAT 2
2.1 PPTP 2
2.2 L2TP/IPsec 3
2.3 OpenVPN 3
2.4 SSTP 3
2.5 IKEv2 4

3 VPN 5
3.1 VPN-sovellukset 5
3.1.1 Cisco AnyConnect 5
3.1.2 Check Point IPsec -VPN 6
3.1.3 Citrix Workspace 6
3.2 Fyysiset VPN-laitteet 7
3.2.1 TOSIBOX 7
3.2.2 eWon 7
3.2.3 Secomea 7

4 GOOGLE CLOUD PLATFORM 8
4.1 Google Compute Engine 8
4.2 Google App Engine 8
4.3 Google Cloud Storage 8
4.4 Google Kubernetes Engine 8
4.5 Google Clouds operations suite 9
4.6 Serverless computing 9
4.7 Databases 9

5 OPEN VPN PALVELIMEN ASENTAMINEN GOOGLE CLOUD PLATFORMIIN 10
5.1 Käytettävän teknologian valinta 10
5.2 Virtuaalikoneen asentaminen Google Cloud Platform ympäristöön 11
5.2.1 Virtuaalikoneen luominen 11
5.2.2 Palomuurisäännöt 14
5.2.3 OpenVPN-ohjelmiston asennus 16
5.2.4 Testaus 25
5.2.5 Yhteenveto tuloksista 26

6 POHDINTA 27

LÄHTEET 28

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena oli tutkia ja toteuttaa esimerkkiratkaisu Vitec Alma Oy:lle, miten saada tietoturvallinen ja helposti hallittavissa oleva pääsy Google Cloudissa sijaitsevaan tuotantoympäristöön. Opinnäytetyön teoriaosuudessa käydään läpi erilaisia Virtual Private Network (VPN) protokollia, erilaisia VPN ratkaisuja ja Google Cloud Platformin (GCP) toimintaa. Toiminnallisessa osuudessa asennettiin Debian 11 käyttöjärjestelmällä varustettu virtuaalikone GCP ympäristöön ja asennettiin ja testattiin OpenVPN-palvelinohjelmisto kyseiselle koneelle.

Opinnäytetyön teoriaosuudessa keskitytään eri VPN-protokollien yleiseen esittelyyn ja erilaisten jo olemassa olevien ratkaisujen läpikäyntiin. Luvussa 2.3 esitellään ja käydään tarkemmin lävitse toiminallisessa osuudessa käytetyn OpenVPN-protokollan toiminta ja luku 4 keskittyy Google Cloud Platformin läpikäyntiin.

Opinnäytetyön oppimistavoitteena oli eri etäyhteystekniikoiden hallinta, etäyhteystekniikoihin liittyvien salausmenetelmien hallinta ja Googlen pilviympäristössä toimiminen.

Vitec ALMA oy on Kokkolassa sijaitseva ohjelmistoalan yritys. Heidän tuotteensa on ALMA elinkaarenhallinta ohjelmisto. Ohjelmistoa toimitetaan teollisuuden eri toimialojen yrityksille hallinnoimaan olemassa olevaa omaisuutta, laitteiden ja niihin liittyvien dokumenttien sekä kunnossapitotapahtumien suunnitteluun ja toteutukseen ja instrumentti- ja sähköpiirien suunnitteluun. ALMA-ohjelmiston vahvuus onkin juuri sen konfiguroitavuudessa ja mahdollisuuksissa mukautua erilaisten asiakkaiden tarpeisiin.

2 ETÄYHTEYSPROTOKOLLAT

Etäyhteydellä tarkoitetaan kahden tietolaitteen välistä yhteyttä tietoverkkojen välityksellä. Etäyhteyden tarkoituksena on luoda käyttäjälle yhteys kahden laitteen välillä niin, että kohteena olevaa laitetta pystytään hallitsemaan samalla tavalla, kuin olisi itse paikan päällä käyttämässä kyseistä laitetta. (Hakala, Vainio 2005, 381–382.)

Etäyhteydet voivat tapahtua saman verkon sisällä tai välissä voi olla useampikin tietoverkko. Jos etäyhteys luodaan kahden laitteen välille, jotka sijaitsevat eri verkoissa ja yhteys halutaan luoda tietoturvallisesti, käytetään yleensä erilaisia VPN- tekniikoita. Etäyhteys voidaan luoda myös kahden verkon välille, esimerkiksi yrityksen kaksi eri toimipistettä yhdistävät lähiverkkonsa VPN avulla. (Perlmutter, Zarkower, 2001, 10–12.)

2.1 PPTP

Point-to-point Tunneling Protocol eli PPTP on verkkoprotokolla, joka mahdollistaa salatun tiedonsiirron etäkoneen ja palvelimen välillä. PPTP luo virtuaalisen yksityisen verkon (virtual private network VPN) TCP/IP-yhteyksiä hyödyntävien verkkojen välityksellä. PPTP-protokolla toimii samaan tapaan kuin PPP-protokolla mutta siinä PPP-protokolla kapseloidaan IP-paketin sisään. Tämä mahdollistaa PPP-pakettien käsittelyn IP-pakettien tapaan ja niiden ohjaamisen eri IP-aliverkkojen välillä. (Hakala 2005, 382–383.)

PPTP on Microsoftin kehittämä ja se on ollut yleisesti käytössä Windows 95 -käyttöjärjestelmän ajoista lähtien. PPTP protokollan etuna on helppokäyttöisyys, mutta nykyisellään sitä ei suositella käytettäväksi sen lukuisien haavoittuvuuksien takia. PPTP:n käyttämät käyttäjän autentikointimetodit MS-CHAP ja MS-CHAPv2 ovat olleet alusta asti suhteellisen helposti murrettavissa ja näiden ominaisuuksien takia PPTP-protokollaa ei pidä käyttää VPN-yhteyksissä, joissa tarvitaan luotettavaa salausta. (Schneier, 1998.)

PPTP-yhteyttä voidaan käyttää yhteyksissä, joissa tietoturvallisuudella ei ole käytännön merkitystä. Periaatteessa tämä voisi tarkoittaa pelaamista, suoratoistoa tai tiedostojen lataamista palvelimelta.

2.2 L2TP/IPsec

Layer 2 tunneling protocol eli L2TP on PPTP-protokollan ja L2F-protokollan yhteensulautumisen tulos. L2TP on toiminnaltaan hyvin samankaltainen kuin PPTP-protokolla, mutta rakenteeltaan se on kuitenkin monimutkaisempi. L2TP-protokolla ei itsessään sisällä liikenteen salausta, vaan sitä käytetäänkin usein IPsec eli Internet Protocol Security -turvallisuusprotokollan kanssa. IPsec salaa ja todentaa jokaisen yksityisen IP-paketin viestinnässä ja on hyvin joustava ja perusteellinen turvallisuusprotokolla. Yhdessä käytettynä L2TP ja IPsec tarjoavat huomattavasti turvallisempaa liikennöintiä julkisissa verkoissa kuin PPTP-protokolla. (Perlmutter, 2001, 124–133.)

2.3 OpenVPN

OpenVPN-protokolla on yksi suosituimmista VPN-protokollista tällä hetkellä, sen avoimen lähdekoodin takia. Siinä käytetään kustomoitua turvallisuusprotokollaa yhdessä SSL/TLS:n kanssa avaimien vaihtoon. Näin mahdollistetaan erittäin turvalliset verkosta verkkoon tai pisteestä pisteeseen yhteydet. OpenVPN voi toimia joko UDP- tai TCP-protokollien päällä mahdollistaen turvalliset ja vaikeasti havaittavat yhteydet eri verkkojen välillä. (OpenVPN A 2022.)

OpenVPN-yhteyden luomiseen voidaan käyttää kaikkia SSL-kirjaston tukemia salaus-, tunnistautumis- ja sertifiointimenetelmiä. Käyttäjien tunnistamiseen voidaan käyttää ennalta jaettuja salaisia avaimia, sertifikaatteja tai käyttäjänimi salasana -yhdistelmää. (OpenVPN A 2022.)

Oletuksena OpenVPN käyttää siirrettävän datan ja ohjauskäytävän salaamiseen 256-bittistä AES-GCM-salausta ja vanhempien yhteyssovellusten varalta on käytössä AES-256-CBC ja sitä vanhempien BF-CBC-salaus. Käyttäjän valittavissa on AES:n eri variaatiot, CHACHA20-, POLY1305-, 3DES- ja Blowfish-salaukset. (Open VPN B 2022.)

2.4 SSTP

SSTP (Secure Socket Tunneling Protocol) on yleinen VPN- yhteyksissä käytetty protokolla. Protokollan on kehittänyt Microsoft, joten se on yleisempi Windows-ympäristössä kuin Linuxissa. Microsoft kehitti tekniikan korvaamaan Windowsin ei niin turvalliset PPTP- tai L2TP/IPSec-vaihtoehdot. (CactusVPN 2022.)

SSTP:tä käytetään turvallisiin yhteyksiin ja sen takana oleva tekniikka hyödyntää SSL/TLS-kättelyjä. Se käyttää samaa porttia kuin SSL/TLS (portti 443) ja sen perustana toimii käyttäjän tunnistaminen laitteen tunnistamisen sijaan. SSTP on suosittu vaihtoehto käytettäessä internetyhteyksiä, joissa suojauksen on oltava parempaa kuin perus SSL/TLS-yhteyden. SSTP:tä verrataan usein OpenVPN-standardiin, jota pidetään turvallisimpana etäyhteysprotokollana. (CactusVPN 2022.)

SSTP-protokolla käyttää AES-salausta (Advanced Encryption Standard), mikä tekee siitä turvallisen. Käytössä on 256-bittinen AES-salaus, jota pidetään tällä hetkellä kryptografisesti turvallisena. Vaikka AES-256-salaus voi olla hidasta, SSTP:tä pidetään edelleen nopeana tunneloidun ja salatun viestinnän protokollana. (CactusVPN 2022.)

2.5 IKEv2

IKEv2 (Internet Key Exchange versio 2) on Microsoftin ja Ciscon yhdessä kehittämä VPN salausprotokolla ja se on IKEv1:n seuraaja, joka käsittelee pyyntö- ja vastaustoimintoja. IKEv2 protokollassa käytetään SA (Security Association) -attribuuttia todennuspaketissa varmistamaan liikenteen turvallisuus. (Vojinovic, 2022.)

Kuten muissakin VPN protokollissa on IKEv2 vastuussa tunnelin muodostamisesta VPN-asiakkaan ja VPN-palvelimen välille. Se tekee sen todentamalla ensin sekä asiakkaan, että palvelimen ja sitten sopimalla, mitä salausmenetelmiä käytetään. (Vojinovic, 2022.)

IKEv2 protokollassa käsitellään SA-attribuuttia, jossa määritetään suojausattribuutteja kahden verkkoyksikön (tässä tapauksessa VPN-asiakkaan ja VPN-palvelimen) välille. Se tekee sen luomalla saman symmetrisen salausavaimen molemmille entiteeteille. Mainittua avainta käytetään sitten kaiken VPN-tunnelin läpi kulkevan tiedon salaamiseen ja salauksen purkamiseen. IKEv2 tukee 256-bittistä salausta ja halutessa voidaan käyttää myös muita salauksia, kuten AES, 3DES, Camellia ja ChaCha20. (Vojinovic, 2022.)

3 VPN

VPN tulee sanoista "Virtual Private Network" ja kuvaa mahdollisuutta muodostaa suojattu verkkoyhteys julkisia verkkoja käytettäessä. VPN:t salaavat Internet-liikenteen ja naamioivat online-identiteetin. Tämä tekee kolmansille osapuolille vaikeampaa seurata toimintaa verkossa ja varastaa tietoja. Salaus tapahtuu reaaliajassa. (Hakala 2005, 381–382.)

Mikä tahansa VPN-yhteys vaatii asiakkaan ja palvelimen. Sekä asiakkaan että palvelimen tulee "sopia" protokollasta ja tukea yhteyttä. Perinteiset Point-to-Point Tunneling Protocol (PPTP) -yhteydet eivät käytä SSL/TLS:ää, joten SSTP otettiin käyttöön tiedonsiirron turvallisuuden parantamiseksi ja tiettyjä portteja estävän palomuurien asettamien rajoitusten välttämiseksi. (Hakala 2005, 381–382.)

3.1 VPN-sovellukset

VPN-client on ohjelmistopohjainen tekniikka, joka muodostaa suojatun yhteyden käyttäjän ja VPN-palvelimen välille. Jotkut VPN-clientit toimivat taustalla automaattisesti, kun taas toisissa on käyttöliittymät, joiden avulla käyttäjät voivat olla vuorovaikutuksessa niiden kanssa ja määrittää niitä. VPN-clientit ovat usein tietokoneelle asennettuja sovelluksia. (Barracuda 2022.)

3.1.1 Cisco AnyConnect

Cisco AnyConnect on työkalu, joka mahdollistaa suojatun yhteyden luomisen organisaation sisäverkkoon turvallisesti ja helposti. Cisco AnyConnect on yhteensopiva käytännössä kaikkien laitteiden kanssa. Ohjelmiston etuihin voidaan laskea helpohko laitteiden ja käyttäjien hallinta. Erilaisilla ominaisuuksilla pystytään helposti määrittämään, kenellä on verkkoon pääsy. (Cisco 2022.)

Cisco AnyConnectin toiminta perustuu Ciscon verkkolaitteissa olevaan VPN-ohjelmistoon ja käyttäjän laitteelle asennettavaan yhteysohjelmaan. Käyttäjän tunnistukseen voidaan käyttää RADIUS-, sertifikaatti-, AD/Kerberos- ja LDAP-tunnistautumista. Salaukseen käytetään AES-256 ja 3DES-168 salausta. (Cisco 2022.)

3.1.2 Check Point IPsec -VPN

Check Point VPN tarjoaa käyttäjälle helpon etäyhteysratkaisun, jonka tarkoituksena on tehdä käyttäjälle mahdollisimman helpoksi koneen käyttäminen eri verkoissa mutta säilyttää kuitenkin yhteys yrityksen verkkoon. Check Point VPN:ää on mahdollista käyttää koneelle asennettavan sovelluksen avulla tai selainpohjaisena ratkaisuna. (CheckPoint 2022.)

Check Point VPN tukee käyttäjän tunnistuksessa RADIUS, käyttäjänimi ja salasana -yhdistelmää sekä sertifikaattia. Yhteyden salaukseen käytetään IPSec-protokollaa ja tämän tukemia salausmenetelmiä. (CheckPoint 2022.)

3.1.3 Citrix Workspace

Citrix Workspace ei varsinaisesti ole etäyhteysratkaisu, mutta tarjoaa hieman vastaavaa. Citrix Workspace on keskitetty sovelluksien hallintajärjestelmä, joka tarjoaa käyttäjälle mahdollisuuden käyttää yrityksen ympäristössä sijaitsevia omia tiedostoja ja sovelluksia virtuaalisesti. (SankaraSubramanian, 2018.)

3.2 Fyysiset VPN-laitteet

Fyysisellä VPN-laitteella tarkoitetaan tässä laitetta, joka verkkoon liitettäessä tarjoaa mahdollisimman helposti käyttöön otettavan ja suojatun yhteyden verkon ulkopuolelta kyseiseen sisäverkkoon. Laitteen ominaisuuksiin kuuluu reitittäminen, mahdollinen modeemi, yhteyden salaaminen ja purkaminen ja käyttäjien hallinta.

3.2.1 TOSIBOX

Tosibox on suomalainen tuote, joka tarjoaa helpon ja turvallisen etäyhteyden kahden laitteen tai verkon välille. Tosiboxin toiminta perustuu fyysiseen avaimeen ja lukkoon. Tosiboxin tapauksessa fyysinen avain on USB-tikku, mikä paritetaan tosibox lukon kanssa, ja kun paritus on onnistuneesti tehty, voidaan avain kytkeä toisessa verkossa sijaitsevaan koneeseen, jolla on internetyhteys. Tämän jälkeen Tosibox osaa luoda suojatun yhteyden parina olevan päätelaitteen kanssa. (UC-Enviro 2022.)

Tosiboxin tuotevalikoimaan kuuluu fyysisten laitteiden lisäksi virtuaalisia lukkoja ja avaimia. Näiden toimiminen vaatii kuitenkin aina vähintään yhden fyysisen USB-avaimen käyttöä pääavaimena. Tällä pääavaimella voidaan sitten hallita sille määriteltyjä virtuaalisia avaimia ja sen kanssa paritettuja lukkoja. (UC-Enviro 2022.)

3.2.2 eWon

Ewon on belgialainen yritys, joka tarjoaa etäyhteysratkaisuja teollisuusympäristöön. Ewonin tuotevalikoimaan kuuluu erilaisia lähinnä teollisuusympäristöön suunniteltuja reitittimiä, joihin on mahdollista ottaa yhteys keskitetyn pilvipalvelun kautta erillisellä sovelluksella. (Ewon 2022.)

3.2.3 Secomea

Secomea on tanskalainen yritys, joka tarjoaa etähallinta ja datan keruu ratkaisuja teollisuusympäristöihin. Tuotevalikoimaan kuuluvat erilaiset reitittimet ja näiden hallintaan ja niistä saadun datan hallintaan tarkoitetut sovellukset. (Secomea 2022.)

4 GOOGLE CLOUD PLATFORM

Google Cloud Platform (GCP) on osa Googlen ylläpitämää Google Cloudia. GCP tarkoituksena on tarjota käyttäjille ympäristö, missä pystytään organisaatio tasolla määrittelemään käyttäjien ja resurssin oikeuksia käyttää ja suorittaa siellä olevia palveluita. GCP:n tarjoamiin palveluihin kuuluvat laskeminen, tallennus ja tietokanta, verkot, big data ja koneoppiminen. (Posin 2022.)

4.1 Google Compute Engine

Google Compute Engine (GCE) on Googlen tarjoama Infrastructure-as-a-service (IaaS) -virtuaalikoneympäristö. GCE ympäristön tarkoituksena on korvata tai täydentää perinteiset yrityksen omaan verkkoon sijoitettavat palvelimet ja reitittimet pilviympäristössä sijaitsevilla virtuaalikoneilla. Käyttäjät voivat itse räätälöidä käyttötarkoitukseen sopivan virtuaalikoneen tai asentaa tarpeisiinsa soveltuvan koneen valmiista malleista. (Posin 2022.)

4.2 Google App Engine

Google App Engine (GAE) on Platform-as-a-Service (PaaS) ja se tarjoaa kehittäjille alustan, johon pystytään rakentamaan skaalautuvia ohjelmia. Käyttäjä tekee ohjelman ja julkaisee sen alustalle ja tämän jälkeen Google hoitaa taustalla tarvittavan laskentatehon ja resurssien toimittamisen. (Bigelow 2022.)

4.3 Google Cloud Storage

Google Could Storage (GCS) on paikka tallentaa tietoa Googlen sisällä. GCS sisällä oleva data jaetaan ämpäreihin (buckets) ja näihin voidaan määritellä käyttöoikeuksia eri ryhmille. (Bigelow 2022.)

4.4 Google Kubernetes Engine

Google Kubernetes Engine (GKE) tarjoaa alustan konttitekniikalle rakennetuille sovelluksille. GKE-ympäristössä useampi kone ryhmitellään isommiksi klustereiksi, jonka sisällä ohjelmiston tarvitsemaa laskentatehoa voidaan helposti jakaa koneiden kesken. (Bigelow 2022.)

4.5 Google Clouds operations suite

Google Clouds operations suite tarjoaa työkalut, joilla pystytään selvittämään ja ennalta ehkäisemään ongelmatilanteita. Se sisältää erilaisia kojelautanäkymiä, logitusta ja tilannetietoa ohjelmista. (Bigelow 2022.)

4.6 Serverless computing

Google Serverless computing on nimensä mukaisesti palvelitonta laskentatehoa eli Google hoitaa kaikki taustalla pyörivän ja käyttäjä tekee pelkästään ohjelmiston, jota halutaan ajaa, esimerkiksi internetsivut. (Bigelow 2022.)

4.7 Databases

Google Cloud Databases on tietokantojen ylläpitöön tarkoitettu palvelu. Google on jakanut palvelun kolmeen eri osioon: Cloud SQL, Cloud Spanner ja BigQuery. (Bigelow 2022.)

5 OPEN VPN PALVELIMEN ASENTAMINEN GOOGLE CLOUD PLATFORMIIN

Opinnäytetyön tavoitteena oli löytää ratkaisu, miten Vitec Almalla toteutetaan turvallinen ja helposti hallittava etäyhteys Googlen pilviympäristöön. Tätä varten tutkittiin useita eri vaihtoehtoja ja näistä vaihtoehdoista Tosiboxin ratkaisua ja OpenVPN-palvelinta ryhdyttiin lopulta tutkimaan vielä enemmän ja selvitettiin näiden ratkaisujen soveltuvuutta Vitec Alman tarpeisiin.

Tähän prosessiin kuului taustatietojen hankkiminen valmistajilta ja tarvittavien pohjatietojen etsiminen testausympäristöjen rakentamista varten.

5.1 Käytettävän teknologian valinta

Ensimmäinen vaihtoehto oli suomalainen Tosibox. Tosiboxilla oli tarjota helposti hallittavissa oleva etäyhteys ja luotettava tausta etäyhteyksien toimittamisessa teollisuuden tarpeisiin. Tämän vaihtoehdon merkittävä positiivinen tekijä oli myös kotimaisuus.

Tosiboxilta oli tarkoituksena asentaa Googlen pilviympäristöön Virtual Central Lock -niminen järjestelmä, joka mahdollistaa useiden eri yhteyksien ja käyttäjien hallinnan keskitetysti. Toimiakseen tämä järjestelmä tarvitsee virtuaaliympäristön ja hallintaa varten Tosiboxin fyysisen USB-väylään kytkettävän avaimen, joka paritetaan keskuslukon kanssa.

Tosibox ei virallisesti tue Googlen pilviympäristöä, mikä aiheuttikin alkuun hieman epäilyksiä siitä, että saadaanko tämä järjestelmä asennettua ja toimimaan. Valitettavasti nämä epäilykset olivat aiheellisia, eikä Tosiboxin Virtual Central Lockia saatu useista yrityksistä huolimatta asennettua Googlen ympäristöön. Näiden haasteiden myötä päädyttiin kokeilemaan jotain muuta järjestelmää.

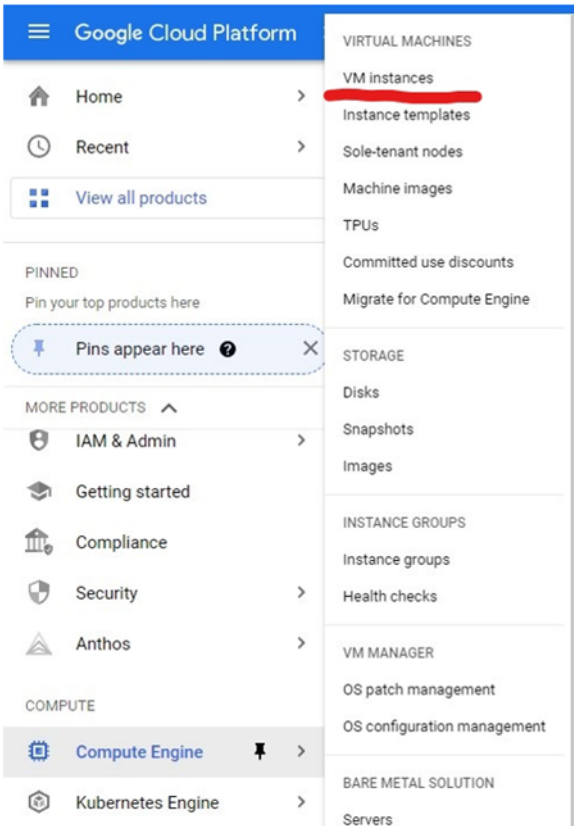
Seuraava vaihtoehto oli OpenVPN-palvelimen asentaminen Googlen ympäristöön. Tähän vaihtoehtoon päädyttiin sen avoimen lähdekoodin ja hyvien asennusohjeiden takia. OpenVPN on myös oikein käytettynä erittäin tietoturvallinen vaihtoehto.

5.2 Virtuaalikoneen asentaminen Google Cloud Platform ympäristöön

Virtuaalikoneen lisääminen Google Cloud Platformiin on tehty asiakkaalle mahdollisimman helpoksi mutta yleisimpien tietotekniikan termien osaaminen saattaa hieman auttaa asennuksen kanssa. Asennusta varten tarvitaan tili Google Cloud Platformiin, projekti, jonka alle virtuaalikone luodaan ja käyttäjätili riittävillä käyttöoikeuksilla.

5.2.1 Virtuaalikoneen luominen

Virutaalikone luodaan valitsemalla navigointimenusta ”Compute Engine” ja sieltä VM instances.

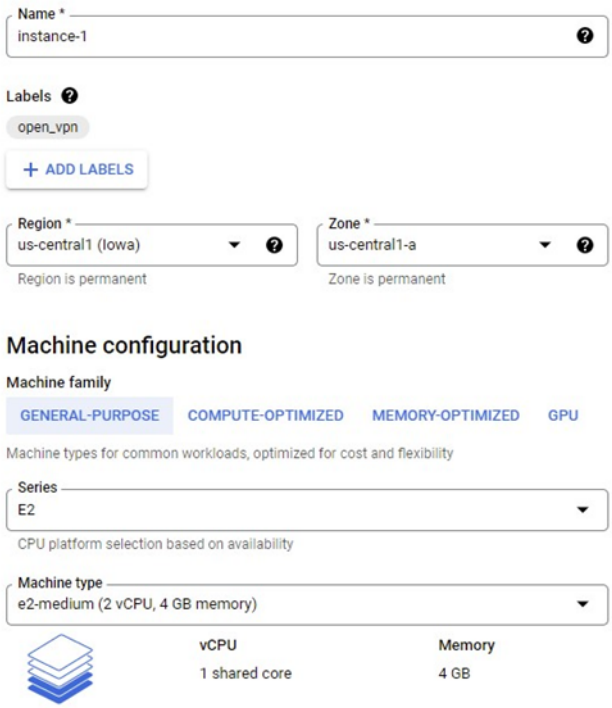


KUVA 1. Navigointimenu ”Compute Engine” ja “VM instances”

VM instances sivulta klikataan yläreunasta löytyvää “CREATE INSTANCE” -painiketta.

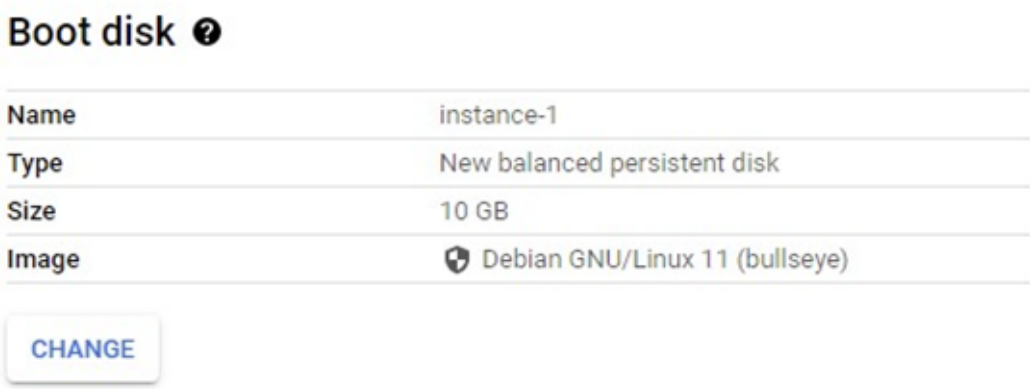
KUVA 2. Virtuaalikoneen luominen “CREATE INSTANCE” painikkeen kautta

Tämän jälkeen valitaan luotavalle koneelle tarvittavat asetukset. Testikäytössä meille riittää Googlen oletuksena tarjoama ”General purpose” -kone. Tärkeää tässä vaiheessa on valita koneelle oikea Region ja Zone, koska näitä ei pysty enää koneen luomisen jälkeen vaihtamaan.

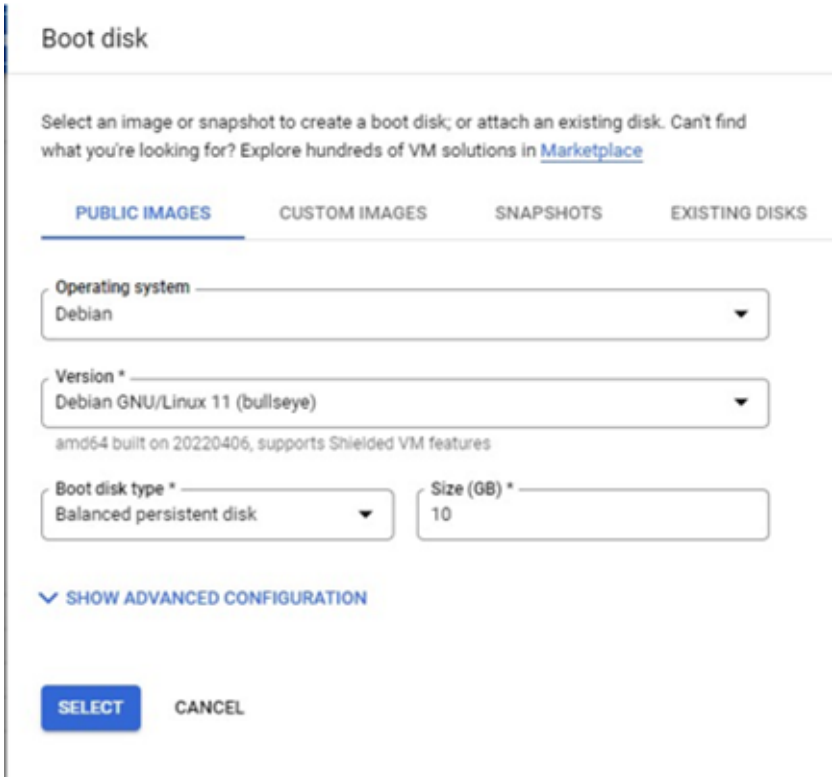


KUVA 3. Luotavan koneen tiedot

Boot disk -kohdassa on mahdollista valita luotavalle koneelle käyttöjärjestelmä. Tätä testiä varten annamme valinnan olla Debianin 11 -versiossa, mutta tarvittaessa tässä vaiheessa voidaan muokata luotavan käynnistyslevyn sisältö ja koko.

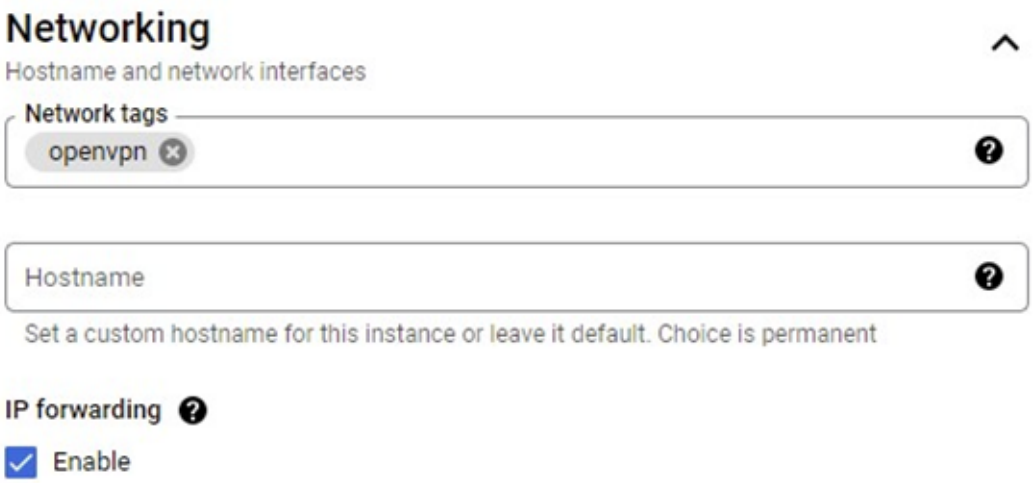


KUVA 4. Käynnistyslevy



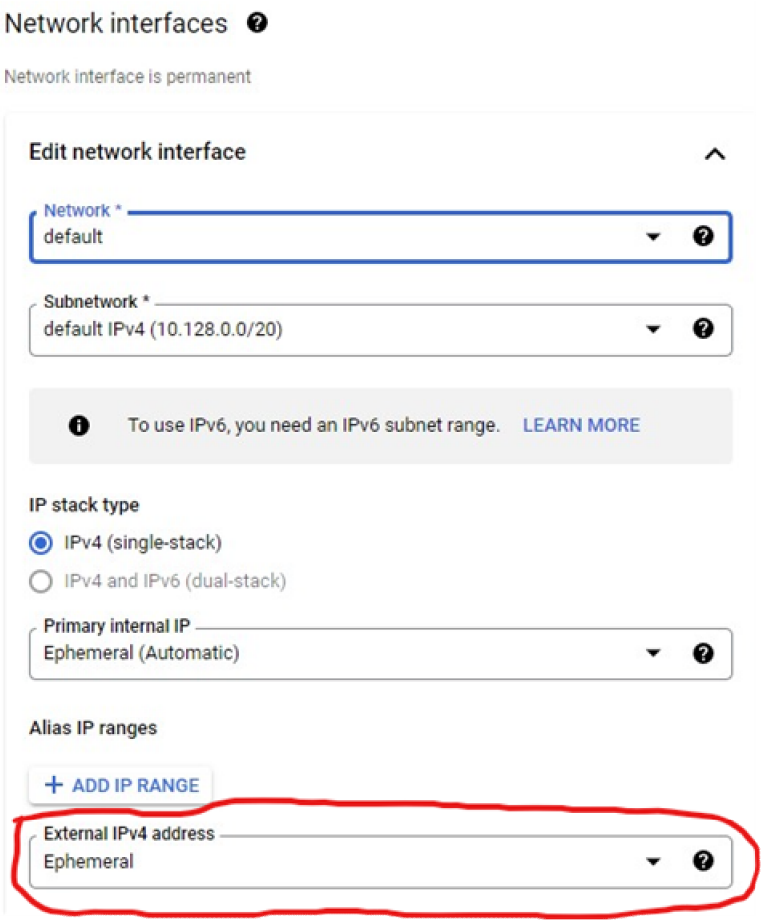
KUVA 5. Käynnistyslevyn tietojen vaihtaminen

Seuraava tärkeä vaihe on Networking kohdassa olevat tiedot. ”Network tags” -kohtaan on lisättävä jokin tieto palomuurisääntöjä varten. Tässä on käytetty ”openvpn” tagia. OpenVPN-palvelimen toiminnan kannalta on myös oleellista, että kone pystyy reitittämään sille tulleita paketteja, joten ”IP forwarding” pitää olla valittuna.



KUVA 6. Network tags ja IP forwarding

OpenVPN-palvelimen toiminnan kannalta on tärkeää, että koneella on käytössä julkinen IP-osoite, johon yhteydet muodostetaan.

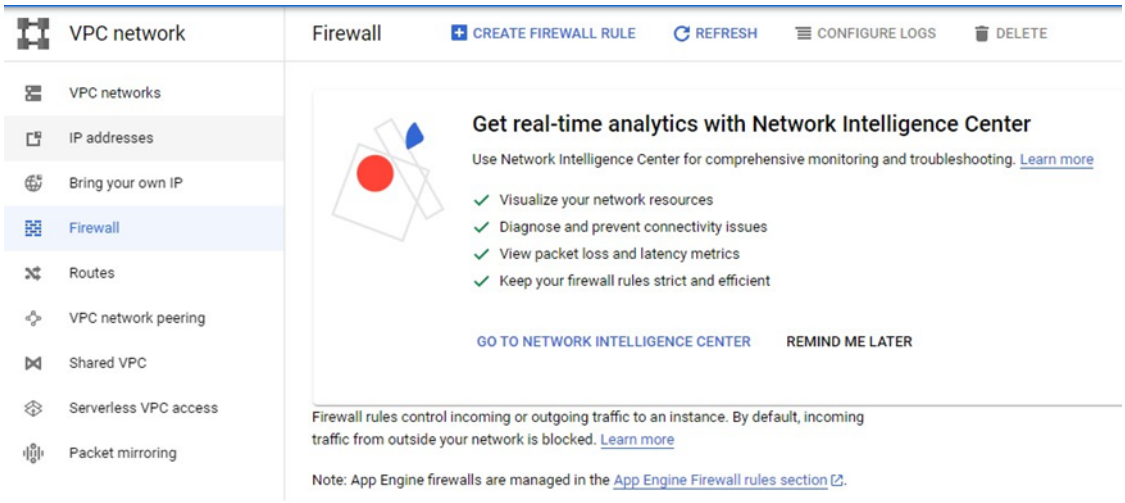


KUVA 7. Koneen julkinen IP osoite

Lopuksi vieritetään näkymä alas ja painetaan ”Create”-nappia. Kone on muutaman minuutin kuluttua käyttövalmis.

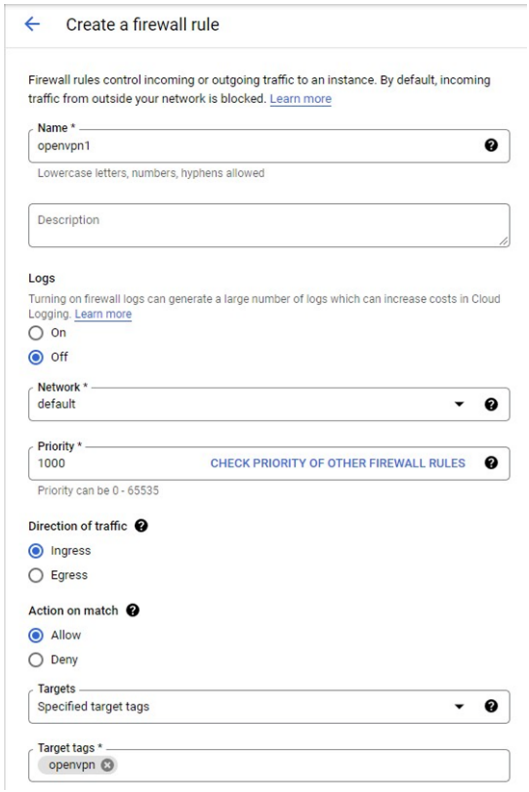
5.2.2 Palomuurisäännöt

Virtuaalikoneen luonnin jälkeen tarvitsemme vielä palomuurisäännöt, jotta saamme juuri luotuun koneeseen yhteyden ulkoapäin. GCP-alustan palomuurisäännöt löytyvät navigointimenun ”VPC network” -kohdasta ja sieltä kohdasta ”Firewall”. Uusi sääntö luodaan painamalla ”CREATE FIREWALL RULE” -painiketta.



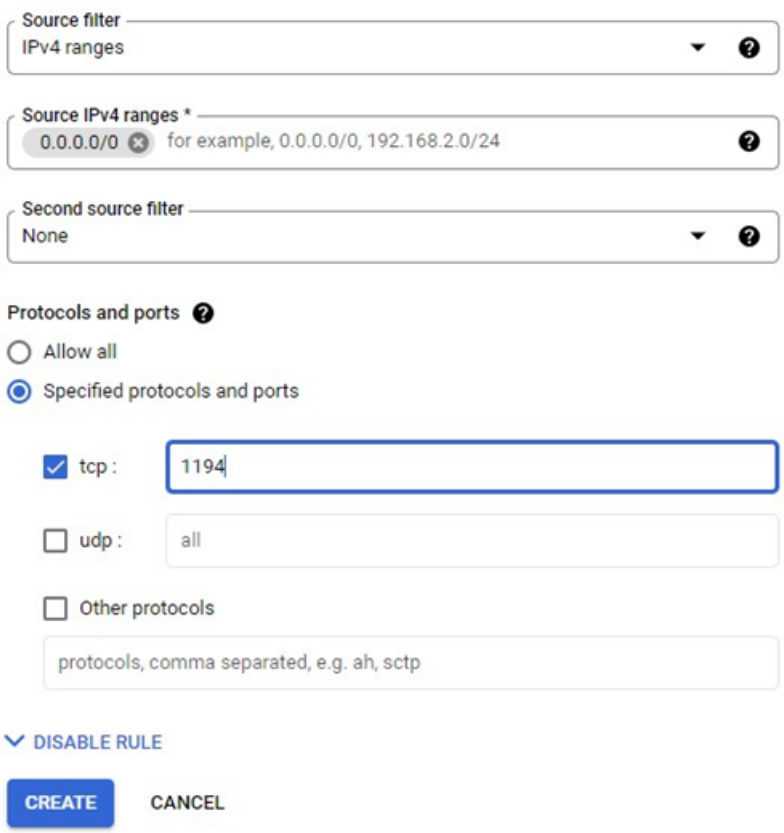
KUVA 8. GCP palomuurisäännöt

Napin painalluksen jälkeen valitaan luotavan säännön tiedot. Oleellisia tietoja tässä on ”Network”-valinta. Se pitää olla sama kuin mihin juuri luotu virtuaalikone on sijoitettu. ”Direction of traffic” -valinta pitää olla ”Ingress”, koska halutaan sallia sisäänpäin tulevaa liikennettä. ”Action on match” on salliva eli ”Allow”. ”Targets” kohdasta valitaan ”Specified target tags” ja ”Target tags” -kohtaan luodun koneen network tag eli ”openvpn”. Näin GCP-alusta tietää mitä konetta luotu sääntö koskee, ja osaa reitittää liikenteen sisäisesti oikein.



KUVA 9. Uuden palomuurisäännön luominen

Seuraavassa kohdassa valitaan, mistä osoitteista liikenne sallitaan, joten ”Source IPv4 ranges” -kohtaan lisätään 0.0.0.0/0 eli kaikista osoitteista. Lopuksi määritellään vielä protokolla, jota sääntö koskee. Tässä tapauksessa protokollaksi tuli tcp ja OpenVPN-palvelin asetetaan kuuntelemaan porttia 1194, joten valitaan ”tcp” ja annetaan sille arvoksi 1194. OpenVPN-palvelin voidaan määritellä toimimaan joko tcp- tai udp-protokollalla.

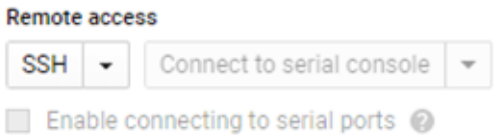


KUVA 10. Palomuurisäännön protokolla ja portti

Create-napin painamisen jälkeen kaikki on valmista OpenVPN-ohjelmiston asentamista varten.

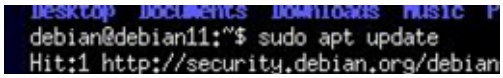
5.2.3 OpenVPN-ohjelmiston asennus

Luodulle virtuaalikoneelle päästään kirjautumaan sisään valitsemalla kyseinen kone Compute Enginen Virtual intances kautta. Klikataan koneen nimeä ja sieltä valitaan SSH tai Connect to serial console, jos se on aktivoitu.



KUVA 11. Kirjautuminen virtuaalikoneelle

Kun virtuaalikoneelle on päästy kirjautumaan sisään, päivitetään ensimmäisenä pakettiluettelo ajan tasalle käyttäen ”sudo apt update” komentoa. Koska käytössä on Debian, löytyy OpenVPN-asennuspaketti jo valmiina pakettiluettelosta. Käyttämällä komentoa ”sudo apt install openvpn” saadaan OpenVPN-ohjelmisto asennettua koneelle.



KUVA 12. ”sudo apt update” -komennon käyttäminen

KUVA 13. ”sudo apt install openvpn” -komennon käyttäminen

OpenVPN-ohjelmiston lisäksi tarvitaan EasyRSA-ohjelma sertifikaattien luontiin ja hallintaan. Näitä tarvitaan SSL/TLS-yhteyttä varten. EasyRSA-ohjelma asennetaan käyttämällä komentoa:
wget -P ~/ https://github.com/OpenVPN/easy-rsa/releases/download/v3.1.0/EasyRSA-3.1.0.tgz

KUVA 14. EasyRSA-ohjelman lataus

Ladattu asennuspaketti puretaan ”tar xvf EasyRSA-3.1.0.tgz” -komennolla (KUVA 15). Paketin purkamisen jälkeen siirrytään asennuskansioon ”cd ~/EasyRSA-3.1.0/” ja kopioidaan siellä oleva esimerkki tiedosto ”cp vars.example vars” (KUVA 16) käytettäväksi sertifikaattien luomista varten. Kopioinnin jälkeen avataan tiedosto tekstieditoriin ”nano vars” -komennolla (KUVA 16). Tiedostosta muokataan kohtaa:

set_var EASYRSA_REQ_COUNTRY "US"
set_var EASYRSA_REQ_PROVINCE "NewYork"
set_var EASYRSA_REQ_CITY "New York City"
set_var EASYRSA_REQ_ORG "DigitalOcean"

set_var EASYRSA_REQ_EMAIL "admin@example.com"
set_var EASYRSA_REQ_OU "Community"

Nämä asetukset käyttäjä määrittelee vastaamaan oman yrityksen tietoja.

```
debian@debian11:~$ tar xvf EasyRSA-3.1.0.tgz
```

KUVA 15. Ladatun asennuspaketin purkaminen

Asetustiedoston muokkauksen ja tallennuksen jälkeen ajetaan komento ”./easyrsa init-pki” (KUVA 16), joka luo tarvittavan julkisenavaimen ympäristön palvelimelle (Public Key Infrastructure).

```
debian@debian11:~$ cd EasyRSA-3.1.0/
debian@debian11:~/EasyRSA-3.1.0$ ls
ChangeLog   doc      gpl-2.0.txt  openssl-easyrsa.cnf  README.quickstart.md  x509-types
COPYING.md  easyrsa  mktemp.txt   README.md            vars.example
debian@debian11:~/EasyRSA-3.1.0$ cp vars.example vars
debian@debian11:~/EasyRSA-3.1.0$ nano vars
debian@debian11:~/EasyRSA-3.1.0$ ./easyrsa init-pki
* Notice:

  init-pki complete; you may now create a CA or requests.

  Your newly created PKI dir is:
  * /home/debian/EasyRSA-3.1.0/pki

* Notice:
  IMPORTANT: Easy-RSA 'vars' file has now been moved to your PKI above.
```

KUVA 16. Esimerkkitiedoston kopiointi ja muokkaus. PKI-ympäristön luominen

Kun ympäristö on saatu luotua, ajetaan komento ”./easyrsa build-ca nopass” (KUVA 17). Nopass-lisämääre kertoo, että ei haluta käyttää ylimääräistä salasanaa tiedoston käytön yhteydessä. Tällä komennolla luodaan SSL-sertifikaatin julkinen ja salainen avain. Näistä tiedostoista julkinen avain tarvitaan kaikille osapuolille kertomaan, että olemme tunnettuja ja salaista avainta tarvitaan allekirjoittamaan muiden käyttäjien sertifikaatit. Tässä tapauksessa OpenVPN-palvelin itsessään toimii myös sertifikaattien allekirjoittajana, mikä ei ole tietoturvallinen ratkaisu, mutta testiympäristössä tämä sallittakoon. Oikea tietoturvallinen tapa olisi tehdä erillinen verkosta irti kytketty kone, jolla allekirjoitetaan uusien käyttäjien sertifikaatit.

```
debian@debian11:~/EasyRSA-3.1.0$ ./easyrsa build-ca nopass
* Notice:
Using Easy-RSA configuration from: /home/debian/EasyRSA-3.1.0/pki/vars

* Notice:
Using SSL: openssl OpenSSL 1.1.1k  25 Mar 2021

.....................................................+++++
.................................+++++
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:

* Notice:

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/debian/EasyRSA-3.1.0/pki/ca.crt
```

KUVA 17. CA ympäristön luominen

Koska käytössä on testiympäristö, voidaan samalla kertaa luoda OpenVPN-palvelimen ja käyttäjän tarvitsemat avaimet. Palvelimen avaimet luodaan käyttämällä komentoa ”./easyrsa build-server-full “server" nopass” (KUVA 18) ja käyttäjän tarvitsemat avaimet luodaan käyttämällä komentoa ”./easyrsa build-client-full "testi" nopass” (KUVA 19).

```
debian@debian11:~/EasyRSA-3.1.0$ ./easyrsa build-server-full "server" nopass
* Notice:
Using Easy-RSA configuration from: /home/debian/EasyRSA-3.1.0/pki/vars

* Notice:
Using SSL: openssl OpenSSL 1.1.1k  25 Mar 2021

Generating a RSA private key
.....................................................+++++
.....................................+++++
writing new private key to '/home/debian/EasyRSA-3.1.0/pki/1f85f760/temp.2ec04384'
-----
* Notice:

Keypair and certificate request completed. Your files are:
req: /home/debian/EasyRSA-3.1.0/pki/reqs/server.req
key: /home/debian/EasyRSA-3.1.0/pki/private/server.key

Using configuration from /home/debian/EasyRSA-3.1.0/pki/1f85f760/temp.b19412c5
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'server'
Certificate is to be certified until Oct  7 07:30:45 2024 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

* Notice:
Certificate created at: /home/debian/EasyRSA-3.1.0/pki/issued/server.crt
```

KUVA 18. OpenVPN-palvelimen sertifikaatin ja salaisen avaimen luominen

```
debian@debian11:~/EasyRSA-3.1.0$ ./easyrsa build-client-full "testi" nopass
* Notice:
Using Easy-RSA configuration from: /home/debian/EasyRSA-3.1.0/pki/vars

* Notice:
Using SSL: openssl OpenSSL 1.1.1k  25 Mar 2021

Generating a RSA private key
..................+++++
.....................................................................................+++++
writing new private key to '/home/debian/EasyRSA-3.1.0/pki/2f37dac0/temp.a8c39973'
-----
* Notice:

Keypair and certificate request completed. Your files are:
req: /home/debian/EasyRSA-3.1.0/pki/reqs/testi.req
key: /home/debian/EasyRSA-3.1.0/pki/private/testi.key

Using configuration from /home/debian/EasyRSA-3.1.0/pki/2f37dac0/temp.42b43164
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'testi'
Certificate is to be certified until Oct  7 07:52:41 2024 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

* Notice:
Certificate created at: /home/debian/EasyRSA-3.1.0/pki/issued/testi.crt
```

KUVA 19. Käyttäjän sertifikaatin ja salaisen avaimen luominen

Seuraavaksi luodaan vielä Diffie-Hellman-avain avainten vaihtoa varten ”./easyrsa gen-dh” -komennolla (KUVA 20) ja HMAC-allekirjoitus parantamaan palvelimen TLS-eheyden varmistamisessa ”sudo open-vpn --genkey secret ta.key” -komennolla (KUVA 21).

```
debian@debian11:~/EasyRSA-3.1.0$ ./easyrsa gen-dh
* Notice:
Using Easy-RSA configuration from: /home/debian/EasyRSA-3.1.0/pki/vars

* Notice:
Using SSL: openssl OpenSSL 1.1.1k  25 Mar 2021

Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.........+.....................................................................................................
..................+.............................................................................................
...................................................+.....................+..+.........................................
.......................................................................+.......................................
..............+.........................+.....................+..............++*++*++*++*

* Notice:

DH parameters of size 2048 created at /home/debian/EasyRSA-3.1.0/pki/dh.pem
```

KUVA 20. Diffie-Hellman-avaimen luominen

```
debian@debian11:~/EasyRSA-3.1.0$ sudo openvpn --genkey secret ta.key
```

KUVA 21. HMAC-allekirjoitus

Tämän jälkeen kopioidaan juuri luodut tiedostot OpenVpn-ohjelmiston kansioon komennoilla:

sudo cp ~/EasyRSA-3.1.0/pki/ca.crt /etc/openvpn/

sudo cp ~/EasyRSA-3.1.0/pki/issued/server.crt /etc/openvpn/

sudo cp ~/EasyRSA-3.1.0/pki/private/server.key /etc/openvpn/

sudo cp ~/EasyRSA-3.1.0/ta.key /etc/openvpn/

sudo cp ~/EasyRSA-3.1.0/pki/dh.pem /etc/openvpn/

Kopioidaan OpenVPN-ohjelman tarvitsema asetustiedosto mallista ja muokataan se halutuksi käyttäen komentoa:

sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf /etc/openvpn/

cd /etc/openvpn/

sudo nano server.conf

```
debian@debian11:~/EasyRSA-3.1.0$ sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf /etc/openvpn/
debian@debian11:~/EasyRSA-3.1.0$ cd /etc/openvpn/
debian@debian11:/etc/openvpn$ ls
ca.crt  client  dh.pem  server  server.conf  server.crt  ta.key  update-resolv-conf
debian@debian11:/etc/openvpn$ sudo nano server.conf
```

KUVA 22. OpenVPN-ohjelman tarvitseman malliasetustiedoston kopiointi ja muokkaus

Asetustiedostosta muokataan porttitiedot, protokolla, käytetyt avaimet ja salausmenetelmät vastaamaan haluttua. Huomioitavaa on, että kaikkea liikennettä ei haluta ohjata OpenVPN-palvelimen kautta vaan pelkästään liikenne, joka on tarpeellista. Tarvittaessa voisimme määritellä ”push ”route 192.168.10.0 255.255.255.0” -komennolla, että palvelimen takaa löytyy kyseinen aliverkko ja käyttäjän OpenVPN-client osaa ohjata liikenteen oikeaan osoitteeseen.

```
GNU nano 5.4                                        server.conf *
port 1194
proto tcp
dev tun
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret
dh dh.pem
;topology subnet
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist /var/log/openvpn/ipp.txt
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"
keepalive 10 120
tls-auth ta.key 0 # This file is secret
cipher AES-256-CBC
auth SHA256
user nobody
group nogroup
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
verb 3
explicit-exit-notify 0
```

KUVA 23. server.conf tiedoston sisältö

Seuraava vaihe on tarpeeton Googlen pilviympäristössä, koska kyseinen asetus määriteltiin jo virtuaalikonetta luotaessa. Portin siirto saadaan aktivoitua päälle seuraavilla komennoilla:

sudo nano /etc/sysctl.conf

Avautuvasta tiedostosta etsitään kohta ”net.ipv4.ip_forward” ja muutetaan sen arvoksi net.ipv4.ip_forward = 1. Päivitetään vielä muutettu arvo kyseiselle istunnolle ”sudo sysctl -p”.

Käynnistetään OpenVPN-palvelu käyttämällä komentoa ”sudo systemctl start openvpn@server” (KUVA 24).

```
debian@debian11:~/EasyRSA-3.1.0/pki/private$ sudo systemctl start openvpn@server
```

KUVA 24. OpenVPN käynnistys

Palvelun tila saadaan tarkastettua käyttämällä komentoa ”sudo systemctl status openvpn@server” (KUVA 25).

```
debian@debian11:~/EasyRSA-3.1.0/pki/private$ sudo systemctl status openvpn@server
● openvpn@server.service - OpenVPN connection to server
     Loaded: loaded (/lib/systemd/system/openvpn@.service; enabled-runtime; vendor preset: enabled)
     Active: active (running) since Tue 2022-07-05 03:50:02 CDT; 3min 6s ago
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 4378 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 2321)
     Memory: 956.0K
        CPU: 49ms
     CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
             └─4378 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/server.status 10 --cd /etc/openvpn --config /etc/

Jul 05 03:50:02 debian11 ovpn-server[4378]: Listening for incoming TCP connection on [AF_INET][undef]:1194
Jul 05 03:50:02 debian11 ovpn-server[4378]: TCPv4_SERVER link local (bound): [AF_INET][undef]:1194
Jul 05 03:50:02 debian11 ovpn-server[4378]: TCPv4_SERVER link remote: [AF_UNSPEC]
Jul 05 03:50:02 debian11 ovpn-server[4378]: GID set to nogroup
Jul 05 03:50:02 debian11 ovpn-server[4378]: UID set to nobody
Jul 05 03:50:02 debian11 ovpn-server[4378]: MULTI: multi_init called, r=256 v=256
Jul 05 03:50:02 debian11 ovpn-server[4378]: IFCONFIG POOL IPv4: base=10.8.0.4 size=62
Jul 05 03:50:02 debian11 ovpn-server[4378]: IFCONFIG POOL LIST
Jul 05 03:50:02 debian11 ovpn-server[4378]: MULTI: TCP INIT maxclients=1024 maxevents=1028
Jul 05 03:50:02 debian11 ovpn-server[4378]: Initialization Sequence Completed
```

KUVA 25. OpenVPN-palvelun tila

Käyttäjien helpompaa hallintaa varten luodaan heille erillinen kansio ”mkdir -p ~/client-configs/keys” komennolla ja kopioidaan sinne käyttäjän asetustiedoston tarvitsemat avaimet (KUVA 26). Käyttäjien asetustiedostoja varten luodaan vielä toinen kansio ”mkdir -p ~/client-configs/files” komennolla (KUVA 27) ja kopioidaan sinne käyttäjien luontiin tarvittava asetustiedosto ”cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf”.

```
debian@debian11:~/EasyRSA-3.1.0$ sudo cp pki/private/testi.key ~/client-configs/keys/
debian@debian11:~/EasyRSA-3.1.0$ sudo cp pki/issued/testi.crt ~/client-configs/keys/
debian@debian11:~/EasyRSA-3.1.0$ sudo cp ~/EasyRSA-3.1.0/ta.key ~/client-configs/keys/
debian@debian11:~/EasyRSA-3.1.0$ sudo cp /etc/openvpn/ca.crt ~/client-configs/keys/
```

KUVA 26. Käyttäjän tarvitsemien tiedostojen kopiointi helpompaa hallintaa varten

```
debian@debian11:~/client-configs$ mkdir -p ~/client-configs/files
debian@debian11:~/client-configs$ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf
```

KUVA 27. Asetuskansion luonti ja esimerkki asetustiedoston kopiointi

Muokataan asetustiedosto komennolla ”nano base.conf” (KUVA 28) halutuksi (KUVA 29) ja tehdään uusi skriptitiedosto ”nano ~/client-configs/make_config.sh” -komennolla (KUVA 28) ja muokataan siitä haluttu (KUVA 30). Tällä tiedostolla saadaan tehtyä uusia käyttäjiä helpommin. Tehdään luodusta tiedostosta vielä ajettava komennolla “sudo chmod +x make_config.sh”.

```
debian@debian11:~/client-configs$ nano base.conf
debian@debian11:~/client-configs$ nano ~/client-configs/make_config.sh
```

KUVA 28. Asetustiedoston muokkaus ja käyttäjän lisäys -skripti

Asetustiedostosta muokataan asetukset vastaamaan palvelimen asetuksia ja huomioitavaa on ”key-direction” pitää olla käyttäjällä 1.

```
GNU nano 5.4                                        base.conf
client
dev tun
proto tcp
remote 10.0.2.15 1194.
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-CBC
auth SHA256
verb 3
key-direction 1
```

KUVA 29. Käyttäjän asetustiedoston sisältö

```
GNU nano 5.4                                        make_config.sh
#!/bin/bash

# First argument: Client identifier

KEY_DIR=/home/debian/client-configs/keys
OUTPUT_DIR=/home/debian/client-configs/files
BASE_CONFIG=/home/debian/client-configs/base.conf

cat ${BASE_CONFIG} \
    <(echo -e '<ca>') \
    ${KEY_DIR}/ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${KEY_DIR}/${1}.crt \
    <(echo -e '</cert>\n<key>') \
    ${KEY_DIR}/${1}.key \
    <(echo -e '</key>\n<tls-auth>') \
    ${KEY_DIR}/ta.key \
    <(echo -e '</tls-auth>') \
    > ${OUTPUT_DIR}/${1}.ovpn
```

KUVA 30. Käyttäjän luonti -skripti tiedoston sisältö

Luotu skriptitiedosto voidaan ajaa käyttämällä komentoa “sudo ./make_config.sh testi” (KUVA 31).

```
debian@debian11:~/client-configs$ sudo ./make_config.sh testi
```

KUVA 31.

Skriptin ajon jälkeen kopioidaan luotu asetustiedosto käyttäjän koneelle OpenVPN clientin käyttämistä varten.

5.2.4 Testaus

Testiympäristössä riitti, että käyttäjä sai yhteyden palvelimelle ja liikenne sinne ohjautui oikein. Yhteyden toimivuus voidaan todentaa käyttämällä ”ping”-komentoa. Palvelimella on käytössä osoite 10.8.0.1 osoite. Tätä voitiin pingata käyttäjän koneelta komennolla ”ping 10.8.0.1” (KUVA 33) ja sieltä saatiin vastaus. Sama toiminto voitiin suorittaa myös palvelimelta käyttäjän koneelle käyttämällä komentoa ”ping 10.8.0.6” (KUVA 32).

```
debian@debian11:~/client-configs/files$ ping 10.8.0.6
PING 10.8.0.6 (10.8.0.6) 56(84) bytes of data.
64 bytes from 10.8.0.6: icmp_seq=1 ttl=128 time=0.950 ms
64 bytes from 10.8.0.6: icmp_seq=2 ttl=128 time=1.64 ms
64 bytes from 10.8.0.6: icmp_seq=3 ttl=128 time=1.56 ms
64 bytes from 10.8.0.6: icmp_seq=4 ttl=128 time=0.997 ms
64 bytes from 10.8.0.6: icmp_seq=5 ttl=128 time=0.744 ms
64 bytes from 10.8.0.6: icmp_seq=6 ttl=128 time=1.47 ms
^C
--- 10.8.0.6 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5035ms
rtt min/avg/max/mdev = 0.744/1.225/1.636/0.340 ms
debian@debian11:~/client-configs/files$
```

KUVA 32. Pingaus palvelimelta käyttäjän koneelle

```
C:\Windows\system32>ping 10.8.0.1

Pinging 10.8.0.1 with 32 bytes of data:
Reply from 10.8.0.1: bytes=32 time<1ms TTL=64
Reply from 10.8.0.1: bytes=32 time=1ms TTL=64
Reply from 10.8.0.1: bytes=32 time=1ms TTL=64
Reply from 10.8.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 10.8.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

KUVA 33. Pingaus käyttäjän koneelta palvelimelle

5.2.5 Yhteenveto tuloksista

Virtuaalikone saatiin onnistuneesti asennettua ja konfiguroitua Googlen pilviympäristöön ja siihen saatiin onnistuneesti asennettua OpenVPN-ohjelmisto. Testausten perusteella OpenVPN-palvelin on toimiva ratkaisu Googlen pilviympäristössä sijaitsevan tuotantoympäristön etähallintaan. Jatkoa varten ympäristö vaatisi huomattavaa parantamista tietoturvan osalta lähinnä asetusten kannalta ja kattavampaa testausta, kun käyttäjiä on useampia.

Testauksien ja tuloksien perusteella asennettua kokoonpanoa voitaisiin käyttää kohdeyrityksen toiminnassa helpottamassa Googlen pilviympäristössä sijaitsevaa tuotantoympäristöä käytettäessä. OpenVPN-palvelimen avoimenlähdekoodin periaate ja maine luotettavana etäyhteystekniikkana on lähtökohtaisesti erittäin tietoturvallinen ratkaisu, jos sitä käytetään oikein ja tarvittavat konfiguraatiot tehdään tarkoituksenmukaisesti.

6 POHDINTA

Opinnäytetyön tavoitteena oli oppia eri etäyhteystekniikoiden toimintaa, pilviympäristöjen toimintaa ja löytää mahdollinen ratkaisu kohde yritykselle hallinnoida pilviympäristössä sijaitsevaa tuotantoympäristöä. Näihin kaikkiin tavoitteisiin päästiin tutkimalla asiaan liittyvää tutkimusmateriaalia ja alan artikkeleita. Tämän lisäksi päästiin toteuttamaan käytännössä virtuaalikoneen asentaminen pilviympäristöön ja tähän etäyhteysohjelmisto.

Erittäin opettavaista oli päästä ensin tutkimaan aiheeseen liittyvää teoriaa ja tämän jälkeen toteuttamaan sitä käytännössä. Ensimmäiseksi toteutusvaihtoehdoksi valikoitunut Tosibox oli myös mielenkiintoinen vaihtoehto. Valitettavasti Tosiboxin ratkaisua ei päästy testaamaan sen enempää asennusvaiheessa ilmenneiden ongelmien takia, mutta asennuksen kokeileminen ja mahdollisen ratkaisun löytäminen asennusvaikeuksiin opetti paljon varsinkin Googlen pilviympäristön toiminnasta.

Opinnäytetyön tekeminen on ollut pitkä prosessi, joka työn ohessa tehtynä on vaatinut joustamista ja opettanut myös suunnitelmallisen ajankäytön tärkeyden. On ollut mielenkiintoista päästä suunnittelemaan oikean yrityksen tarpeista lähtevää palvelua, vaikka sen käyttöönotto yrityksessä on ainakin toistaiseksi jäänyt testaus-tasolle. Kaiken kaikkiaan etäyhteysympäristön suunnittelu ja testaus antoi arvokasta tietoa ja kokemusta tuotantoympäristön hallinnan toteutuksesta.

LÄHTEET

Barracuda. 2022. What is a VPN Client? Saatavissa: https://www.barracuda.com/glossary/vpn-client Viitattu: 11.7.2022.

Bigelow, S. 2022. Google Cloud. Saatavissa: https://www.techtarget.com/searchcloudcomputing/definition/Google-Cloud-Platform Viitattu: 21.6.2022.

CactusVPN. 2022. What Is SSTP? (Your Guide to the SSTP VPN Protocol). Saatavissa: https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-sstp/ Viitattu: 21.6.2022.

CheckPoint. 2022. Check Point Endpoint Remote Access VPN Software. Saatavissa: https://www.checkfirewalls.com/endpoint-remote-access-vpn-software-blade.asp Viitattu: 21.6.2022.

Cisco. 2022. Cisco Secure Client Data Sheet. Saatavissa: https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/datasheet-c78-733184.html Viitattu: 22.6.2022.

Ewon. 2022. Saatavissa: https://www.ewon.biz/home Viitattu: 5.7.2022.

Hakala, M., Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo. Viitattu: 11.5.2022.

Open VPN. 2022a. OpenVPN (OSS). Saatavissa: https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn Viitattu: 15.5.2022.

Open VPN. 2022b. Change encryption cipher in Access Server. Saatavissa: https://openvpn.net/vpn-server-resources/change-encryption-cipher-in-access-server/ Viitattu: 15.5.2022.

Perlmutter, B. Zarkower, J. 2001. VPN: virtuaaliset yksityisverkot. Helsinki: Edita, IT Press. Viitattu: 11.5.2022.

Posin, D., 2022. Getting to Know Google Compute Engine and How to Use It. Saatavissa: https://dzone.com/refcardz/getting-to-know-google-compute-engine-and-how-to-u Viitattu: 21.6.2022.

SankaraSubramanian, A. 2018. Citrix Workspace App – Everything You Need to Know. Saatavissa: https://www.citrix.com/blogs/2018/06/12/citrix-workspace-app-everything-you-need-to-know/ Viitattu: 22.6.2022.

Schneier, B., 1998. Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP). Saatavissa: https://www.schneier.com/wp-content/uploads/2016/02/paper-pptp.pdf Viitattu: 12.5.2022.

Secomea. 2022. Saatavissa: https://www.secomea.com/product-overview/ Viitattu: 5.7.2022.

UC-Enviro. 2022. Saatavissa: http://www.uc-enviro.com/tosibox/about-the-tosibox-howdoesitwork.html Viitattu: 5.7.2022.

Vojinovic, I. 2022. What Is IKEv2 VPN Protocol? Saatavissa: https://dataprot.net/guides/what-is-ikev2-vpn/ Viitattu 16.5.2022.