Opinnäytetyö (AMK)

Tietojenkäsittely

2019

Emil Oksanen

VPN-ERILLISVERKON KÄYTTÖÖNOTTO YRITYKSESSÄ

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2019 | 31 sivua

Emil Oksanen

VPN-ERILLISVERKON KÄYTTÖÖNOTTO YRITYKSESSÄ

VPN eli Virtual Private Network on erillisverkko, joka tuo yrityksille ja käyttäjille mahdollisuuden turvalliseen etätyöskentelyyn. Tämä luo erilaisen työskentelytavan, kun ei tarvitse olla paikan päällä yrityksessä. Tietoturva on ollut aina otsikoissa, jonka johdosta yritykset haluavat panostaa entistä enemmän tietoturvaan. VPN-etäyhteys mahdollistaa salatun yhteyden salausavaimien- ja protokollien avulla sekä kryptausmenetelmillä. Työn teoria koostui lyhyesti tietokoneiden kommunikointiin tarkoitetusta standardista, VPN-verkon protokollista ja vaatimuksista sekä uhkista ja riskeistä.

Työn tutkimusmenetelmä oli toiminnallinen. Opinnäytetyön aihe toteutetaan käytännön toteutuksena toimeksiantajalle tämän työn ulkopuolella. Käytännönosuudessa käytettiin OpenVPN-ohjelmistoa VPN-ratkaisun toteutuksessa, joka koostui esivalmistelusta, asennuksesta ja lopputestauksesta. Toteutuksessa hyödynnettiin internetissä saatavia VPN-aineistoja sekä muita aiheeseen liittyviä lähteitä ja ohjetekstejä.

Opinnäytetyön lopputuloksena oli toimiva suunnitelma VPN-erillisverkosta.

ASIASANAT:

VPN, Etätyö, Tietoturva, Verkko, OpenVPN

BACHELOR´S | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology

2019 | 31 pages

Emil Oksanen

COMMISSIONING VPN NETWORK IN A COMPANY

VPN (Virtual Private Network) is a separate network that grants companies as well as schools and users possibility of safe remote work. This gives a different working style when users do not need to be on the company/organization premises. The purpose of this thesis is to make a VPN network implementation plan for the commissioning company which they're going to use it for remote work when necessary. Information security has always been a hot topic which means that companies need to invest more on information security. VPN allows encrypted connection via keys, protocols and encrypting methods. The theoretical part of this thesis introduces and discusses computer communication standard, VPN protocols and their requirements, together with threats and risks.

The practical work contained preparation, installation and testing for the OpenVPN software which was used for the implementation of a VPN system for the commissioning company. VPN guides and other topic related sources were used for the implementation.

End result was a working plan for the VPN connection for the company. The VPN implementation was done outside of this scope.

KEYWORDS:

VPN, OpenVPN, Information Security, Network, Remote work

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET

AES	Advanced Encryption Standard on yksi salausmenetelmistä. (National Institute of Standards and Technology 2001.)
B2B	Business to Business eli yritysmarkkinointi. Tuotteita tai palveluita myydään yrityksille. (Fonecta 2018.)
B2C	Business to Customer eli kuluttajamarkkinointi. Tuotteita tai palveluita myydään kuluttajille. (Fonecta 2018.)
CA	Certificate Authority (lyh. CA) allekirjoittaa ja luo sertifikaatteja palvelimelle ja käyttäjille. (OpenVPN 2019e.)
HTTP	Hypertext Transfer Protocol, selaimien ja verkkosivustojen käyttävä protokolla tiedonsiirtoon. (w3schools.com 2019.)
IPsec	Internet Protocol Security, turvallisuusprotokolla, jonka tehtävä on salaa jokainen IP-paketti niiden lähetettäessä. (Rouse 2018.)
IKE	Internet Key Exhange, joka on IPsec-salaukseen perustuva protokolla VPN-yhteyksien luomiseen. (KeepSolid 2019.)
LAN	Local Area Network, rajoitettu maantieteellinen lähiverkko, esimerkiksi kodin tai yrityksen verkko. (Beal 2019.)
L2TP	Layer 2 Tunneling Protocol, VPN-tunnelointiprotokolla, jonka on luonut Cisco ja Microsoft. (Hoffman 2018c)
MAC	Media Access Control Address, Mac-osoite on jokaisen verkkosovittimen yksilöllinen osoite, jonka valmistaja on määrittänyt tehtaalla. (Dell 2019.)
NIC	Network Interface Card eli verkkosovitin. Tämän avulla tietokone liitetään verkkoon. (Mitchell 2018.)

OSI	Open System Interconnection. Mallin on kehittänyt International Organization for Standardization -organisaatio. Luotiin tietokoneiden kommunikaatio standardiksi. (Zimmermann 1980.)
SSTP	Secure Socket Tunneling Protocol, Microsoftin luoma VPN-protokolla. (PureVPN 2019.)
TCP	Transmission Control Protocol, tietoliikenneprotokolla tietokonelaitteiden yhteyksien luontiin. Mahdollistaa luotettavan tiedonsiirron koneiden välillä ilman että paketit tippuvat matkalla. (Kerrisk 2012.)
TLS / SSL	Transport Layer Security, yksi salausprotokollista, jolla salataan päästä päähän -yhteys internet verkon yli. Käytetään paljon esimerkiksi verkko-ostosten kanssa. TLS tunnettiin ennen nimellä SSL eli Secure Socket Layer. (Cloudflare 2019.)
UDP	User Datagram Protocol on yhteydettömätön protokolla. UDP-protokolla toimii samalla periaatteella kuin TCP-protokolla, mutta luotettavuutta ei ole, koska paketin lähettäjä ei saa vastausta takaisin. (Hoffman 2017b.)
VPN	Virtuaalinen erillisverkko (tulee englanninkielen sanoista Virtual Private Network), jolla voidaan kommunikoida tietokoneiden ja verkkojen välillä turvallisesti ulkoverkossa. (Sharma & Yadav 2015.)

1 JOHDANTO

Maailman digitalisoituessa etätyö on yleistynyt ja on koitunut hyvin merkittäväksi ja joustavaksi työskentelymenetelmäksi. Digitalisaatio on kaiken elämän ja toiminnan yhdistäminen digiteknologiaan. Etätyöllä tarkoitetaan siis työtä, jota tehdään työpaikan ulkopuolella. (Akava 2018) Tietoturva on kasvanut yhä merkittävämmäksi asiaksi, koska yhä useammat organisaatiot, yritykset sekä yhteisöt tarvitsevat internetiä, jotta liiketoiminta jatkuu. Tämä johtuu siitä, että esimerkiksi yritykset kommunikoivat B2B (Business to Business) tai B2C (Business to Customer) -tasolla. Yhä useammat pienemmät ja keskisuuret organisaatiot ovat haavoittuvaisia hyökkäyksille (Galvin 2018). Tämän takia on yrityksen liiketoiminnalle tärkeätä, että hyökkäykset arvioidaan sen mukaan, mikä on järkevintä huomioida. (Kumar ym. 2010.)

Tämän työn tarkoituksena on tutkia VPN eli Virtual Private Network -erillisverkon turvallisuutta sekä sen toteuttamista toimeksiantajayritykselle. Tavoitteena on toteuttaa etätyöskentelyratkaisu, joka mahdollistaisi yhteyden yrityksen järjestelmään ja sen tietoihin lähiverkon ulkopuolelta.

Opinnäytetyön teoriaosuudessa käydään läpi VPN-tekniikan perusteita sekä tietoturvaa. Työssä ei mennä syvällisesti VPN-tekniikkaan, vaan katsotaan enemmänkin yleisellä tasolla. Toteuttamisessa käytetään VPN-ratkaisua, josta kerrotaan yksityiskohtaisemmin luvussa 4. Työssä keskitytään etäyhteyden tietoturvaan, mahdollisiin tietoturva-aukkoihin, tietoliikenteen perusrakenteeseen sekä toimivuuteen. Työn käytännönosuudessa selitetään vaihe vaiheelta VPN-palvelimen sekä ohjelmiston asennuksesta, joka toteutetaan tämän työn ulkopuolella yritykselle.

Toimeksiantajana toimi Case Yritys X.

2 OSI-MALLI

OSI-malli tulee sanoista Open System Interconnection. Mallin on kehittänyt International Organization for Standardization -organisaatio. Malli kehitettiin siksi, että voitiin käyttää yhteistä standardia tietokoneiden kommunikaatiossa. OSI-malli sisältää 7 erilaista kerrosta (kuva 1.), joilla jokaisella on oma tarkoituksensa. Ylempi kerros käyttää aina alimman kerroksen toiminnallisuuksia. (Zimmermann 1980.)

Fyysinen kerros (Physical Layer)

Kerros 1 on fyysinen kerros ja OSI-mallin ensimmäinen kerros. Tämä kerros määrittelee laitteiston fyysisen määrityksen verkossa. Esimerkkinä on tietokoneen verkkokortti (NIC eli Network interface controller), jonka avulla voidaan kommunikoida muiden laitteiden välillä.

Siirtoyhteyskerros (Link Layer)

Kerros 2 on siirtoyhteyskerros. Sen tehtävänä on muuttaa tieto sellaiseen muotoon, että sen verkko ja fyysinen kerros pystyy kommunikoimaan. Tässä tapahtuu käytännössä datapakettien koodaamista sekä dekoodaamista.

Verkkokerros (Network Layer)

Kerros 3 on verkkokerros, jonka tehtävä on siirtää verkon dataa kahden verkkolaitteiston välillä mikä on reititystä. Verkkokerroksen oleellisin tehtävä on valita reitti vastaanottajan verkkoon, joka koostuu isoista ja monihaaraisista tietokoneverkoista.

Kuljetuskerros (Transport Layer)

Kerros 4 eli kuljetuskerros tarjoaa luotettavan yhteyden tietokoneiden välillä. Jos yhteys katkeaa jostain syystä, kuljetuskerros etsii tuolloin toisen reitin vastaanottajan verkkoon.

Istuntokerros (Session Layer)

Kerros 5 eli istuntokerros muodostaa tiedonsiirtoyhteyden koneiden välille. Tiedonsiirtoistunnossa istuntokerros synkronoi datan siirtoa, että paketit tulevat oikeassa järjestyksessä sekä tiedonsiirto ei sekoa, jos yhteys katkeaa.

Esitystapakerros (Presentation Layer)

Kerros 6 käsittelee esitystapakerrosta, jonka tehtävänä on muuntaa data siihen formaattiin, että se on sovelluskerroksen luettavissa.

Sovelluskerros (Application Layer)

Kerros 7 on sovelluskerros, joka tarjoaa sovelluksille verkkoyhteydet. Tämä käytännössä tarkoittaa, että ohjelma pystyy verkkoviestintään. Ohjelma kommunikoi vain tämän kerroksen kanssa. (Ala-Mutka ym. 2002.)

Kuva 1. OSI-malli kuvitettuna (Anon. 2018).

3 VIRTUAL PRIVATE NETWORK (VPN) - ERILLISVERKKO

VPN tulee sanasta Virtual Private Network, joka mahdollistaa turvallisen tiedonsiirron kahden tietokoneen välillä julkisen tai jaetun verkon kautta. Tämä tieto kulkee niinsanottua tunnelia pitkin, joka ensin kapseloidaan otsakkeella mikä mahdollistaa ensin reitityksen kohteeseen. Tiedonsiirron aikana tämä tieto myös salataan salausavaimilla. Tietoa on mahdoton purkaa ilman näitä salausavaimia. Tämä mahdollistaa käyttäjän etäyhteyden yrityksen verkkoon ja siitä yrityksen tiedostoihin, jonka johdosta voidaan hallita etäisesti järjestelmää ja esimerkiksi tilauksia, jos on kauppa kyseessä. (Sharma & Yadav 2015.)

3.1 Yleisimmät VPN-tyypit

Etäyhteys (Remote Access VPN)

VPN-verkko on mahdollista luoda kotiin tai toimistoon, johon asiakas ottaa salatun etäyhteyden tarvittaessa. Tämä on erittäin yleinen tapa käyttää VPN-yhteyttä. Käytännössä toimistoon on luotu ennaltamääritetty VPN-palvelin, johon on luotu tunnukset asiakkaalle. Asiakas pystyy ottamaan etäyhteyden toimistoon tai kotiin eri sijainneista. PPTP, L2TP, L2F ja IPsec -tunneliprotokollat tukevat tätä VPN-tyyppiä. Protokollista selitetään tarkemmin luvussa 3.3. (Sharma & Yadav 2015.)

Sivusto sivustoon (Site-to-Site VPN)

Tällä VPN-tyypillä kaksi VPN-palvelinta yhdistävät toisensa, jonka johdosta verkon käyttäjät voivat kommunikoida toistensa kanssa. Tässä VPN-tyypissä asiakas ei tarvitse koneelleensa VPN-asiakasohjelmistoa kommunikoidessaan toisen verkon kanssa. Sivusto sivustoon -tyypissä yhteys on salattu, kuten ylemmässä etäyhteys-tavassa. (Sharma & Yadav 2015.)

3.2 Virtuaalisen erillisverkon turvallisuuspolitiikka

VPN-verkon infastruktuuri tulee suunnitella sen mukaan, ettei hyökkääjät voi käyttää haavoittuvuuksia hyväksi vaikka sitä voisi ajatella, että VPN on monella asteella turvallinen jo valmiiksi. Turvallisuussuunnitelma omalle VPN-verkolla on nykypäivänä pakollinen sen takia. (Das 2019.)

Käyttöoikeudet

Käyttöoikeuksilla tarkoitetaan, että mitä kaikkia yrityksen resursseja ja palveluita työntekijä voi käyttää. Tässä huomioidaan myös, että milloin, missä ja miten resursseja ja palveluita käytetään VPN-verkon yli. (Das 2019.)

Pääsynvalvontaoikeudet

Pääsynvalvonnassa hallitaan IP-osoitteen lähdettä, mistä yhteys on tulossa. Valvotaan myös datapakettien määränpäätä VPN-verkkoinfastruktuurin sisällä ja tutkitaan pakettien sisältöä. (Das 2019.)

VPN-verkon hallinta

Hallinnassa huomioidaan VPN-verkon ylläpitäjä eli kuka tarkkailee ja valvoo VPN-verkkoa. VPN-verkolla täytyy olla myös henkilö, joka vastaa turvallisuudesta. Myös digitaalisten varmenteiden myöntämiseen ja jakamiseen tarvitaan valtuuttaja. Lopuksi sertifikaattien rekisteröinteihin tarvitaan suorittaja. (Das 2019.)

Salauksen tyypit ja asteikot

Huomioidaan päätökset, joilla asetetaan eri tyyppejä ja asetuksia IPsec-verkkoprotokollan kanssa. Julkisille sekä yksityisille avaimille tarvitaan hallinta ja jakelu. Toiminnan ja vanhenemisen aika tarvitaan digitaalisille varmenteille. (Das 2019.)

VPN-verkon päätepisteet

VPN-verkon päätepisteet ovat niitä laitteita, josta IP-tunnelointi kulkee. IP-tunneli on yhteystyyppi, jota käytetään VPN-verkossa. (Das 2019) Päätepisteet ovat yhdyskäytävästä yhdyskäytävään, yhdyskäytävästä työpöydälle ja työpöydästä työpöytään. (Das 2019.)

3.3 VPN-protokollat

PPTP

PPTP (Point-to-Point Tunneling Protocol) on verkkoprotokolla, jonka on luonut Microsoft. Se on yleinen sekä ollut käytössä Windows 95 -tietokoneista lähtien. Se on helposti luotavissa oleva VPN-yhteys. Tosin tämän protokollan yksi heikkouksista on lukuisat haavoittuvuudet, jonka takia se ei ole turvallinen vaihtoehto, kun luodaan VPN-yhteyksiä. Sitä ei siis suositella enää nykypäivänä. (ExpressVPN 2019.)

L2TP / IPsec

Layer 2 Protocol on VPN-protokolla, joka ei itsessään sisällä salausta. Tämän takia sitä käytetään IPSec -nimisen salauksen kanssa. Tästä syystä tämä toimii hitaammin mitä muut protokollat, koska joudutaan etenemään kaksivaiheisesti. Yleinen ongelma L2TP/IPsec kanssa on kommunikaatio-ongelmat palomuurin ja reitittimen kanssa. Tämä on silti parempi ratkaisu kuin PPTP. (Hoffman 2018c) L2TP käyttää UDP 1701 -porttia. (Savill 2005.)

OpenVPN

OpenVPN tarjoaa luotettavan VPN-ratkaisun, jota voidaan käyttää etäyhteyksiin, sivusto sivustoon -VPN-verkkoihin, Wi-Fi turvallisuuteen ja yritys-tason etätyöskentely ratkaisuihin. OpenVPN käyttää TLS/SSL –salausprotokollaa yhteyden luomisessa. OpenVPN on muokattavissa sekä jos sen asettaa käyttämään AES-salausta, on sitä lähes mahdotonta purkaa. OpenVPN on mahdollista asentaa monelle eri alustalle. (OpenVPN 2019c.)

SSTP

SSTP eli Secure Socket Tunneling Protocol on Microsoftin luoma VPN-tunneliprotokolla. SSTP on saatavilla Windows-, Linux- ja Mac-käyttöjärjestelmille. SSTP käyttää TCP 443 -porttia ja pystyy kiertämään kaiken tyyppiset palomuurit. Salauksessa käytetään 256-bittistä AES-salausta. (PureVPN 2019.)

IKEv2

IKE tulee sanasta Internet Key Exhange, joka on IPsec-salaukseen perustuva protokolla VPN-yhteyksien luomiseen. Ensimmäinen versio julkaistiin vuonna 1998 (IKEv1), kun taas 7 vuotta myöhemmin julkaistiin IKEv2. IKEv2 toimii nopeammin kuin PPTP ja L2TP sekä tukee turvallista salausta. IKEv2 käyttää vain UDP 500 -porttia, joka voi aiheuttaa joidenkin palomuurien estämisen siihen porttiin. (KeepSolid 2019.)

3.4 Uhat ja riskit

Vaikka VPN on todettu turvalliseksi, on kuitenkin olemassa turvallisuusriskejä mitä ei välttämättä osata täysin arvioida. Asiakkaan kone voi olla yksi hyökkäyksen kohde. Ilmaiset VPN-ohjelmistot eivät välttämättä anna sitä, mitä oletettaisiin. (Soon 2019.)

3.4.1 Ilmaiset VPN-palvelut

Ilmaiset VPN-palvelut voivat kuulostaa houkottelevalta. Totuus on kuitenkin toinen, sillä niissä piilee vaara. Tuntemattomissa ilmaisissa VPN-palveluissa on mahdollisuus, että palvelu myy käyttäjien tietoja kolmansille osapuolille tai jopa cyberkriminaaleille. Miten tämä käytännössä toimii: Käyttäjä ottaa salatun yhteyden omalla koneellaan VPN-palveluntarjoajan palvelimeen. Tämän jälkeen käyttäjä pääsee internetiin VPN-palvelimen kautta. Takana on kuitenkin synkkätotuus, sillä VPN-palveluntarjoaja, varsinkin jos kyseessä on hyvin epätunnettu tarjoaja, voi tarkkailla käyttäjän liikennettä. Tämä ei kuitenkaan tarkoita, että ilmaisia VPN-palveluita ei saisi käyttää. Maailmassa on tunnettuja ilmaisia palveluita, mutta käyttäjälle tarjotaan ilmaisuuden vuoksi hitaampaa yhteyttä. (Soon 2019.)

3.4.2 Man in the Middle attack

Man in the Middle attack (MitM), suomeksi sanottuna mies välissä -hyökkäys tai välistävetohyökkäys, on tietoturvahyökkäys, jossa hyökkääjä soluttautuu kahden keskustelun väliin esiittääkseen toista osapuolta toisen tietämättä. Vahingon aiheuttaja saattaa sabotoida viestejä joko poistamalla niitä tai vaihtaa viestin tarkoitusta. Välistävetohyökkäystä on esiintynyt paljon julkisissa kahviloissa, joissa on käytössä avoin suojaamaton langatonverkko. Hyökkääjä voi naamioitua kahvilan langattomaksi verkoksi, jonka seurauksena käyttäjät voivat kirjautua tähän verkkoon heidän tietämättään, että kyseessä on väärennös. VPN-yhteyksissä välistävetohyökkäykset on mahdollisia, jos et luota VPN-tarjoajaan. (Mallik ym. 2019.)

3.4.3 Virukset ja haittaohjelmat käyttäjän tietokoneessa

Työntekijä ottaessaan yhteyttä yrityksen verkkoon VPN:n kautta, tämä luo riskin samalla, että käyttäjän koneessa oleva virus tai haittaohjelma leviäisi samalla yrityksen verkkoon. VPN ei itsessään suojaa virusten leviämiseltä. Suojautumisessa yrityksen virustorjunta ja palomuurit ovat isossa asemassa siinä kohtaan, kun haittaohjelma on päässyt yrityksen verkkoon käsiksi. Parhaassa tilanteessa palomuuri on estänyt leviämisen, ennen kuin se olisi päässyt yrityksen verkkoon. Paras keino suojautumisessa on antaa yrityksen työntekijälle kattava perehdytys siihen, miten haittaohjelmilta ja viruksilta vältytään. (Skoudis 2004.)

3.5 VPN-yhteyden käyttötarkoituksia

Etäyhteys yrityksen tulostimiin on yksi hyödyllisistä keinoista käyttää VPN-yhteyttä. Työntekijä voi tulostaa asiakirjan työpaikalle ja hakea sen seuraavana päivänä, tai sitten ihan muuhun tarkoitukseen. Käyttötapoja löytyy varmasti yrityksen sisällä. (Hoffman 2017a.)

Yrityksen lähiverkon tiedostoja, kuten NAS-asemia, voidaan etähallita VPN-yhteydellä. Suuria määriä tiedostoja voidaan siirtää, poistaa tai kopioida, tai miksei jopa asentaa. Yrityksellä voi olla myös pilvipalveluita, palvelimia tai muita laitteita, joita pitää etäohjata kotoa tarvittaessa. (OpenVPN 2019d.)

3.6 IP-osoitteet

IP-osoite eli Internet Protocol Address on jokaisen tietokoneen oma osoite verkossa, jossa kommunikoidaan tietokonelaitteiden välillä. On julkisia ja yksityisiä IP-osoitteita. Julkiset IP-osoitteet näkyvät lähiverkon ulkopuolelle ja yksityiset ovat lähiverkon laitteiden omia osoitteita. (PCMag 2019.)

Asiakas-kone saa IP-osoitteen OpenVPN-palvelimelta. Normaalisti DHCP-palvelin jakaa IP-osoitteita lähiverkon laitteille, mutta tässä tapauksessa näin ei ole. OpenVPN-palvelin toimii niinikään DHCP-palvelimena, mutta jakaa IP-osoitteita yksityisessä aliverkossa. Asiakkaat saavat automaattisesti IP-osoitteen, kun ottavat yhteyden aliverkkoon. (OpenVPN 2019b.)

4 CASE: YRITYS X - KÄYTÄNNÖN SUUNNITTELU JA TOTEUTTAMINEN

Case-yritykselle luodaan VPN-ratkaisu heidän olemassa olevilla laitteilla. Pääsen luomaan ja testamaan yhteyttä ensin testiympäristössä, jonka jälkeen ratkaisu toteutetaan oikeaseen ympäristöön tämän opinnäytetyön ulkopuolella.

4.1 Esivalmistelut

Ennen varsinaista palvelimen asennusta yritys tarjoaa laitteita, joilla voidaan testata VPN-verkkoa testiympäristössä. Tässä työssä päädytään käyttämään OpenVPN-ohjelmistoa, joka on järkevin ratkaisu sen turvallisuuden ja ilmaisuuden vuoksi.

Yrityksen edustaja konfiguroi palomuurin valmiiksi käyttämään oletusporttia 1194 sekä lähettämään palomuurin MAC-osoitteen palveluntarjoajalle, jotta päivittäisivät tiedossa olevan kiinteän IP-osoitteen heidän järjestelmäänsä. Tämä tehdään sen takia, että VPN-palvelimeen saadaan yhteys myöhemmin.

OpenVPN-palvelin luodaan tekstipohjaiselle Linux Debian 9 -käyttöjärjestelmälle. Järjestelmään luodaan tavallinen käyttäjä ilman järjestelmänvalvojan oikeuksia. Tavallinen käyttäjä käyttää sudo-komentoa tehdessään järjestelmän muutoksia palvelimeen. Sudo-komennon avulla tavallinen käyttäjä suorittaa root eli järjestelmänvalvojan oikeuksia. Root-käyttäjää ei suositella ikinä normaalissa käytössä, sillä jos tunnus kaapataan, voidaan sillä tehdä suurta haittaa järjestelmään. (Ellingwood 2018)

UFW-palomuuri eli UncomplicatedFirewall on Linux-järjestelmissä mukana tullut netfilter-palomuuri -työkalu. Kyseinen työkalu saadaan asennettua ”apt install ufw” -komennolla.

4.2 Asennus

OpenVPN käyttää hyödykseen sertifikaatteja yhteyksien salaamiseksi. Sertifikaattien luontiin käytetään Certificate Authority (lyh. CA) -palvelua, joka luodaan OpenVPN-

palvelun lisäksi toiseen tietokoneeseen. Tällä tavalla riskejä voidaan minimoida: Näin hyökkääjä ei saisi haltuunsa sertifikaatteja, joilla pääsisi käsiksi VPN-palvelimeen. (Drake & Ellingwood 2018a.)

Aivan ensimmäisenä komentona OpenVPN-palvelimen asennuksessa käytetään sudo apt update -komentoa. Komennon tarkoitus on päivittää olemassa olevat pakettiluettelot, josta uusimmat päivitykset saadaan. Apt-käskyosa toimii tietokantana, josta löytyy saatavissa olevat paketit ja get-käskyosa hakee paketit tietokannasta. (Prakash 2018.)

Sudo apt update -komennon jälkeen suoritetaan OpenVPN-ohjelman asennus. Komennolla ”sudo apt install openvpn” saadaan toimenpide aikaiseksi (kuva 2).

```
sudo apt install openvpn
```

Kuva 2. Komento, jolla asennetaan OpenVPN.

Jotta voidaan rakentaa CA ja PKI (Public Key Infrastructure eli julkisten avainten hallinta) -infrastruktuuri, tulee ladata viimeisimmät versiot EasyRSA-apuohjelmasta kumpaankin palvelimeen käyttämällä wget-komentoa ja niihin liitettävää polkua (kuva 3). Tämän jälkeen pakattutiedosto puretaan molemmille tietokoneille komennolla kuvassa 4.

```
wget -P ~/ https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-3.0.6.tgz
```

Kuva 3. Komento, jolla haetaan uusin versio EasyRSA-apuohjelmasta GitHub-verkkosivusta. Tässä tapauksessa uusin versio oli 3.0.6.

```
cd ~
tar xvf EasyRSA-unix-v3.0.6.tgz
```

Kuva 4. Siirrytään käyttäjän hakemistossa Home-polulle sekä puretaan EasyRSA kyseiseen hakemistoon.

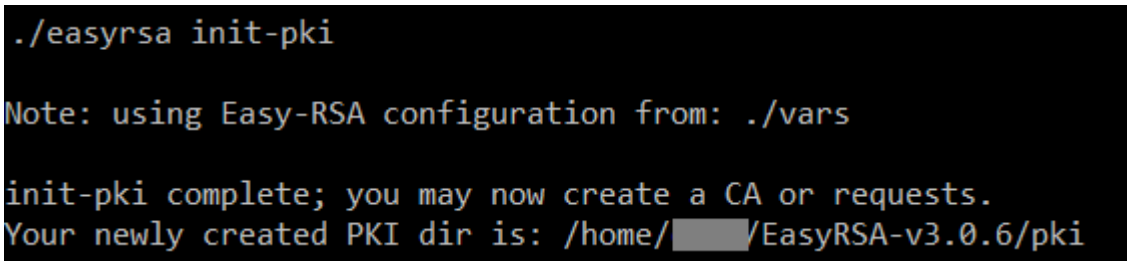
4.2.1 EasyRSA-ohjelmiston muuttujat ja CA-palvelimen rakentaminen

CA-koneella navigoidaan hakemistoon, jossa EasyRSA sijaitsee. Tämän sisältä löytyy kopio vars.example-tiedostosta, josta löytyy valmiiksi muuttujia, joita tullaan

konfiguroimaan. Vars.example-tiedostosta tehdään kopio samalle hakemistossa, jonka nimeksi tulee vars. Tämän jälkeen tiedosto avataan nano-komennolla, joka on tekstieditori. Vars-tiedoston sisältä etsitään kuvan 5 rivit sekä poistetaan #-merkit, jotta ne saadaan käyttöön. Seuraavaksi ”-lainausmerkkien sisälle kirjoitetaan jokaiselle osiolle vastaava tieto, joka voi olla mitä tahansa paitsi tietyt merkistöt. Tärkeintä on, että niitä ei jätetä tyhjäksi. Esimerkiksi ensimmäiselle riville voitaisiin kirjoittaa ”FI”. Kyseisten rivien tarkoitus on asettaa sertifikaateille oletusalue. Huomioidaan, että tässä työssä kentät on piilotettu (kuva 5). Kun tämä on valmista, tallennetaan ja suljetaan tiedosto.

Kuva 5. Sertifikaattien oletusalue vars-tiedostossa. Kuvassa kentät on piilotettu harmaalla.

Samasta hakemistosta löytyy easyrsa-komentosarja, jonka tarkoitus on luoda CA-palvelulle tarvittavat tiedostot sen pyörittämiseen. Se luo PKI-hakemiston, kun komentosarjaa käytetään seuraavanlaisesti kuvassa 6.



Kuva 6. Easyrsa-komentosarjan käyttäminen. Tämä ilmoittaa, että PKI on luotu hakemistoon, mikä kuvassa näkyy.

Toimenpiteen jälkeen easyrsa-komentosarjaa kutsutaan taas, mutta tällä kertaa build-ca -liitteellä, jonka tehtävä on luoda CA:lle kaksi tarpeellista tiedostoa: ca.crt ja ca.key.

Ca.crt on julkinen sertifikaatti, jota palvelin ja asiakas käyttävät kommunikoinnissa. Molemmat osapuolet tarvitsevat kopion tästä tiedostosta. (OpenVPN Security Advisory 2018a.)

Ca.key on yksityinen avain, jota CA-järjestelmä käyttää avaimien ja sertifikaattien allekirjoittamisessa. (OpenVPN Security Advisory 2018a.)

Komentosarjan jälkeen tämä kysyy nimeä CA:lle. Nimeksi voi asettaa oletusnimen (painamalla enteriä) tai halutessaan itse keksimän (kuva 7).

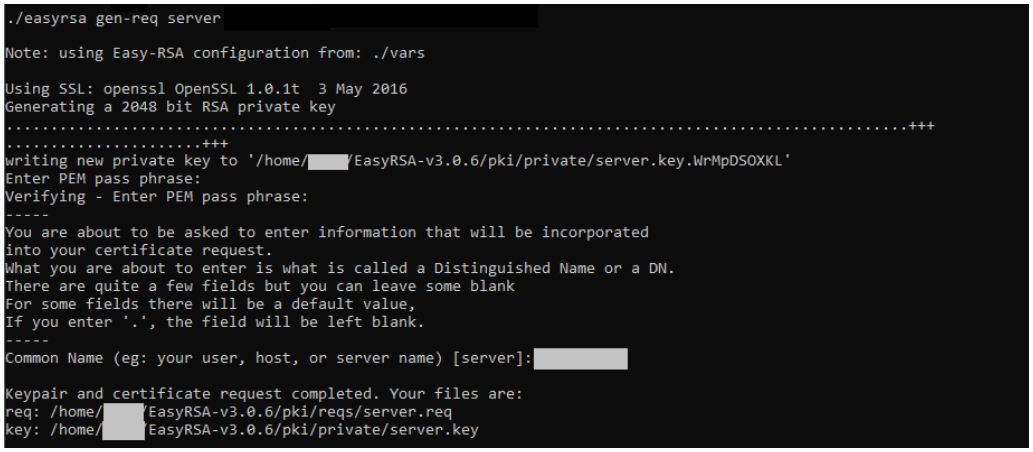
Seuraavassa askeleessa luodaan yksityinen avain ja sertifikaatti-pyyntö OpenVPN-palvelimella. Nämä siirretään lopuksi CA-palvelimelle, joka allekirjoittaa nämä pyynnöt.

```
./easyrsa build-ca

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.0.1t  3 May 2016

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Generating RSA private key, 2048 bit long modulus
..............................+++
.............+++
e is 65537 (0x10001)
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]:

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/[redacted]/EasyRSA-v3.0.6/pki/ca.crt
```

Kuva 7. Kuvassa komento, jolla tehdään ca.crt ja ca.key -tiedostot.

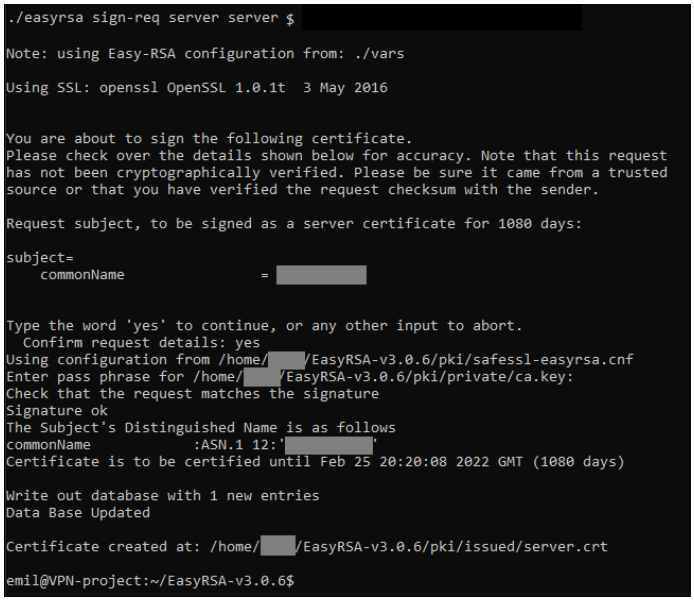
4.2.2 Palvelimen sertifikaatin, avaimen ja salaustiedostojen luominen

Navigoidaan hakemistoon, mihin EasyRSA asennettiin (kuva 4). Sen sisältä löytää saman easyrsa-komentosarjan, jota käytettiin aikaisemmin CA-palvelimessa (kuva 6). Komento suoritetaan uudestaan, mutta OpenVPN-palvelimessa. Seuraavaksi luodaan tälle palvelimelle yksityinen avain ja sertifikaatti-pyyntö (kuva 8). Tämä luo server.reg -nimisen tiedoston, joka kopioidaan /etc/openvpn -hakemistoon.



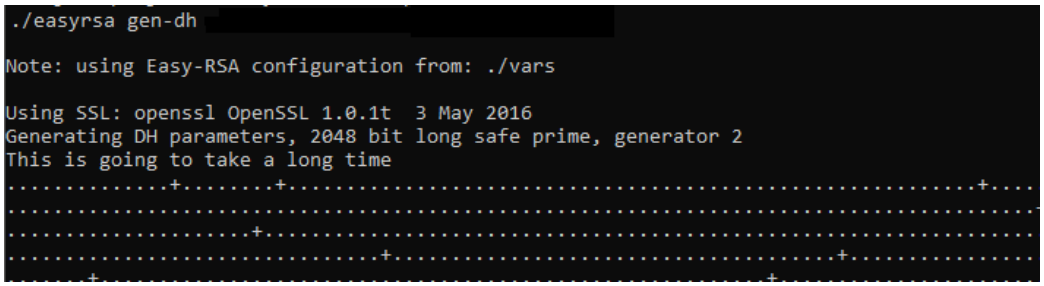
Kuva 8. Easyrsa-komentosarjan käyttäminen gen-req -etuliitteen kanssa. Komennossa laitteen nimeksi on annettu "server".

Lopuksi server.req -tiedosto siirretään CA-palvelimelle joko verkon yli tai fyysisesti USB-muistitikun kanssa. Tässä työssä tiedosto siirrettiin muistitikulla. Nyt CA-palvelimella navigoidaan EasyRSA-hakemistoon, jonka sisällä käytetään easyrsa-komentosarjaa sertifikaatin allekirjoittamiseen, joka luotiin edellisellä palvelimella (kuva 9). Ensimmäinen sana komennossa ”server” tarkoittaa tyyppiä. Tyyppejä voi olla joko server tai client, joka tässä tapauksessa on server. Toinen sana komennossa ”server”, on oleellinen kentän nimi, joka nimettiin server-nimiseksi aikaisemmin.



Kuva 9. Sertifikaatin allekirjoittaminen.

Nyt tämä allekirjoitettu sertifikaatti (nimeltänsä server.crt) siirretään takaisin OpenVPN-palvelimelle. Samalla myös ca.crt -tiedosto siirretään OpenVPN-palvelimelle. Nämä tiedostot kopioidaan lopuksi /etc/openvpn -hakemistoon. Tämän jälkeen navigoidaan taas EasyRSA-hakemistolla, jossa generoidaan Diffie-Hellman -avain (kuva 10). Sen avulla osapuolet voivat sopia yhteisen salaisuuden verkon ylitse. Prosessin jälkeen kirjoitetaan komento: ”sudo openvpn –genkey --secret ta.key”, joka generoi HMAC-allekirjoituksen vahvistaakseen palvelimen TLS-eheyden varmistusominaisuuksia (Drake & Ellingwood 2018b). Kun tämä on suoritettu, kopioidaan uudet tiedostot /etc/openvpn -hakemistoon.



Kuva 10. Diffie-Hellman -avaimen luonti, jonka luonnissa tyypillisesti kestää muutama minuutti.

4.2.3 Asiakas-sertifikaatin generointi ja avainparit

Tässä työssä käytetään valmista komentosarjaa, jonka tarkoitus on luoda valmiiksi asiakasasetukset sertifikaattien ja avainten kanssa. Ideana on, ettei tarvitse lähettää erikseen sertifikaatteja, avaimia tai asetuksia asiakkaille. OpenVPN-palvelimelle luodaan keys-niminen kansio, joka säilyttää asiakas-sertifikaatteja ja avaimia (kuva 11). Turvallisuussyistä kansiolle asetetaan oikeudet vain omistajalle (kuva 12). Navigoidaan EasyRSA-hakemistoon ja käytetään easyrsa-komentosarjaa gen-req -komennon kanssa (kuva 13). Sen eteen määritetään asiakkaan nimi, mikä on tässä tapauksessa ”client1”.

```
mkdir -p ~/client-configs/keys
```

Kuva 11. Keys-kansion luonti.

```
chmod -R 700 ~/client-configs
```

Kuva 12. Oikeuksien asettaminen kansiolle.

```
./easyrsa gen-req client1 nopass

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.0.1t  3 May 2016
Generating a 2048 bit RSA private key
..............................+++
```

Kuva 13. Easyrsa-komentosarjan käyttäminen gen-req -komennon kanssa. Samalla määritetään nimi asiakkaalle "client1".

Prosessin jälkeen client1.key -tiedosto kopioidaan aikaisemmin luodulle keys-kansiolle. Client1.req -tiedosto siirretään CA-palvelimelle, joka allekirjoitetaan miten tehtiin aikaisemmin OpenVPN-palvelimen puolella. Tällä kertaa käytetään ”client” liitettä, joka määrittelee, että se on asiakas (kuva 14). Allekirjoituksen jälkeen tämä luo tiedoston ”client1.crt”, mikä siirretään takaisin OpenVPN-palvelimelle. Siellä tiedosto kopioidaan aikaisemmin luodulle keys-kansiolle. Lopuksi ca.crt sekä ta.key -tiedostot kopioidaan myös keys-kansiolle.

```
./easyrsa sign-req client client1
```

Kuva 14. Pyynnön allekirjoittaminen. Sana "client" tarkoittaa asiakasta. Client1 on nimi, joka määritettiin asiakkaalle.

4.2.4 OpenVPN-palvelimen konfigurointi

Tässä vaiheessa OpenVPN-palvelimelle tehdään konfiguraatiot. Konfiguroinnissa käytetään saatavilla olevaa valmis-tiedostoa, josta saadaan kätevästi asetukset muokattua haluamalla tavalla. Tiedosto kopioidaan hakemistosta ja puretaan muokkaukseen tarkoitettuun hakemistoon (kuva 15). Sen jälkeen tiedosto avataan nano-tekstieditorilla, sen yksinkertaisuuden takia. Tässä tiedostossa keskitytään seuraaviin kohtiin:

1. Salauksen määrittäminen
2. TLS-autentikointi
3. Diffie-Hellman -parametrit
4. Käyttäjä- sekä ryhmien asetukset

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/serv
er.conf.gz /etc/openvpn/
sudo gzip -d /etc/openvpn/server.conf.gz
```

Kuva 15. Kopioidaan config-tiedosto openvpn-hakemistoon, jonka jälkeen tiedosto puretaan gzip-komennolla.

Muita asetuksia ei ole tarvetta muokata, koska ne pysyvät oletuksina. Suurimmaksi osaksi jokaisista kohdista otetaan ;-merkki pois, joka meinaa että tietty kohta on käytössä. Etsitään kohta, jossa määritetään salakirjoitus-tyyppi. Tässä työssä käytetään AES-256-CBC -salakirjoitusta, joka tarjoaa luotettavan ja ylläpidetyn ratkaisun. (Drake & Ellingwood 2018c) Kuvassa 16 otetaan ;-merkki pois sekä lisätään tämän alle ”auth SHA256” -direktiivi, jonka tarkoitus on valita HMAC-viestin algoritmi.

```
# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES
cipher AES-256-CBC
auth SHA256
```

Kuva 16. Salauksessa käytettävä cipher AES-256-CBC -salakirjoitus tarjoaa turvallisen salauksen. Sen alle lisätään ”Auth SHA256”, jonka tarkoitus on valita HMAC-viestin algoritmi.

Seuraavaksi etsitään kohta, missä määritetään Diffie-Hellman -parametrit (kuva 17). Tässä kohdassa poistetaan luku 2048, jotta se ei sekoitu aikaisemmin luodun avain-parametrin kanssa. Seuraavassa vaiheessa etsitään HMAC-osio, jossa halutaan varmistaa, että ”tls-auth” rivistä on poistettu ;-merkki. Sen alle lisätään ”key-direction 0”, joka määrittää palvelimen (kuva 18). Asiakkaalle tulee ”key-direction 1” -pääte

myöhemmin. Kuvassa 19 poistetaan kommenttimerkit user- ja group riveistä. Nämä vähentävät käyttöoikeuksia käyttöönoton jälkeen.

```
# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh.pem
```

Kuva 17. Diffie-Hellman -avaimen määrityksen muokkaaminen.

```
# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port
#
# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
tls-auth ta.key 0 # This file is secret
key-direction 0
```

Kuva 18. Key-direction 0 palvelimelle.

```
# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
user nobody
group nogroup
```

Kuva 19. User ja group.

4.2.5 OpenVPN-palvelimen verkon määrittäminen

OpenVPN-palvelimen verkkoasetuksia joutuu määrittämään, koska muutoin yhteydet eivät reitity oikein VPN-yhteyksien ja sisäverkon välillä. Palvelimen reititystä muokataan kuvan 20 hakemistossa löytyvästä sysctl-conf -tiedostosta, josta ipv4-osiolla otetaan #-merkki pois, että saadaan IPv4-reititys päälle (kuva 21). Tämän jälkeen suljetaan tiedosto.

```
sudo nano /etc/sysctl.conf
```

Kuva 20. Sysctl.conf -tiedoston hakemisto.

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Kuva 21. IPv4-reitityksen saa päälle, kun ottaa kommenttimerkin pois.

Palvelimen julkisen verkkosovittimen osoitteen saa selville komennolla kuvassa 22, joka esiintyy eth0-nimisenä. Tätä tullaan käyttämään seuraavassa vaiheessa, jossa maskeroidaan UFW-säännöt. Kuvassa 23 muokataan before.rules -tiedostoa, jossa näitä maskerointisääntöjä tehdään. Tämän sisältä etsitään kohta, missä UFW-säännöt asetetaan. Punaisella alueella kuvassa 24 on liitetty UFW-säännöt oikealle paikalle. Sen tarkoitus on asettaa POSTROUTING-ketjun oletuskäytännöt voimaan NAT-taulukossa ja peittää kaikki VPN:stä tulevan liikenteen. Tiedostosta varmistetaan, että eth0-verkkosovitin on korvattu omalla verkkosovittimella, joka tässä tapauksessa on eth0. Tämän jälkeen suljetaan tiedosto.

```
ip route | grep default
default via [redacted] dev eth0
```

Kuva 22. Verkkosovittimen osoite ip route -komennolla. Osoite on piilotettu harmaalla laatikolla.

```
sudo nano /etc/ufw/before.rules
```

Kuva 23. UFW-sääntöjä muokataan before.rules -tiedostossa.

```
#
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#


# START OPENVPN RULES
# NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]
# Allow traffic from OpenVPN client to eth0 (change to the interface you discovered!)
-A POSTROUTING -s 10.8.0.0/8 -o eth0 -j MASQUERADE
COMMIT
# END OPENVPN RULES


# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
```

Kuva 24. UFW-säännöt liitetty tiedostoon. Varmistetaan, että eth0-verkkosovitin on korvattu oikean nimisellä verkkosovittimella.

Seuraavaksi muokataan tiedostoa kuvan 25 löytyvästä hakemistosta. UFW:lle on kerrottava, että välittyvät paketit pitää sallia oletetusti. Etsitään kohta ”DEFAULT_FORWARD_POLICY”, missä arvo ”DROP” korvataan ”ACCEPT”-arvolla (kuva 26). Suljetaan tiedosto.

```
sudo nano /etc/default/ufw
```

Kuva 25. Komento, jolla UFW-sääntöjä muokataan.

```
# Set the default forward policy to ACCEPT, DROP or REJECT.  Please note that
# if you change this you will most likely want to adjust your rules
DEFAULT_FORWARD_POLICY="ACCEPT"
```

Kuva 26. DEFAULT_FORWARD_POLICY -arvo on korvattu ACCEPT-arvolla.

Viimeiseksi säädetään UFW-palomuuria, jolla saadaan liikenne OpenVPN-palvelimelle päin. Jos oletusportiksi laitettiin 1194 ja protokollaksi UDP, tullaan sitä käyttämään seuraavassa vaiheessa. Muussa tapauksessa korvataan se muulla protokollalla ja portilla, jos ei ole oletusporttimääritystä. Kuvan 27 mukaisesti sallitaan 1194/UDP ja OpenSSH UFW-palomuuriin. Toiminnon jälkeen käynnistetään palomuuri uudelleen.

```
sudo ufw allow 1194/udp
Rules updated
Rules updated (v6)
sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
sudo ufw disable
Firewall stopped and disabled on system startup
sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

Kuva 27. Sallitaan protokolla 1194/UDP sekä OpenSSH. Käynnistetään palomuuri uudelleen.

4.2.6 OpenVPN-palvelimen käynnistäminen

OpenVPN-palvelin käynnistetään kuvan 28 mukaisesti, jossa “@server” on konfiguraatio-tiedoston nimi /etc/open/ -hakemistossa. Jotta palvelu käynnistyi oikein, tarkistetaan se kuvan 29 komennon avulla.

```
sudo systemctl start openvpn@server
```

Kuva 28. OpenVPN-palvelimen käynnistäminen.

```
sudo systemctl status openvpn@server
```

Kuva 29. OpenVPN-palvelimen käynnistys varmistetaan kuvan mukaisella komennolla.

Palvelu käynnistyi oikein, jos Active-kentällä lukee vihreällä: active (running). Seuraavassa luvussa luodaan infastruktuuri, jolla voidaan helposti tehdä asiakkaalle oma konfiguraatio.

4.2.7 Asiakas-konfiguraatio -infastruktuurin rakentaminen

Infastruktuurin tekeminen auttaa konfiguraatio-tiedostojen luonnissa, sillä jokaiselle OpenVPN-asiakkaalle tehdään oma tiedosto. Manuaalisesti on mahdollista tehdä konfiguraatio-tiedosto, mutta se on hidasta. Siksi tässä työssä hyödynnetään valmista komentosarjaa, joka luo jokaiselle yksittäiselle asiakkaalle oman tiedoston. Luodaan

ensin hakemisto mallikappaleelle (kuva 30). Kopioidaan OpenVPN-hakemistosta mallikappale (kuva 31) ja liitetään se juuri tehdylle hakemistolle kuvassa 30 ja avataan se nano-tekstieditorilla.

```
mkdir -p ~/client-configs/files
```

Kuva 30. Hakemiston luominen.

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf
```

Kuva 31. Mallikappaleen kopioiminen OpenVPN-hakemistosta.

Tästä tiedostosta muokataan muutamaa kohtaa. Ensimmäiseksi etsitään remote-osio, johon kirjoitetaan OpenVPN-palvelimen julkinen ip-osoite, johon asiakas ottaa yhteyden (Kuva 32). Muistetaan samalla ottaa kommenttimerkki pois siltä riviltä. Määritetään protokollaksi UDP, joka säädettiin myös OpenVPN-palvelimelle (kuva 33). Tästäkin kohdasta otetaan kommenttimerkki pois. User ja group -riveiltä otetaan kommenttimerkki pois kuvassa 34.

```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote [redacted] 1194
;remote my-server-2 1194
```

Kuva 32. OpenVPN-palvelimen julkinen IP-osoite, joka on piilotettu harmaalla laatikolla.

```
# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp
```

Kuva 33. UDP-protokolla valittuna.

```
# Downgrade privileges after initialization (non-Windows only)
user nobody
group nogroup
```

Kuva 34. User ja group -rivit valittuna.

SSL/TLS -osiosta varmistetaan, että ca, cert ja key -kentät ovat kommentoitu, sillä ne sisältyvät tähän tiedostoon valmiiksi (kuva 35). Sama tehdään kuvan 36 kohdalle. Seuravaksi peilataan server.conf -tiedostosta salakirjoitus- ja autentikointitavat (kuva 37), mitkä asetettiin aikaisemmin kyseiseen tiedostoon (kuva 16). Lisätään mihin tahansa riville ”key-direction 1”, jotta VPN osaa toimia oikein asiakkaan koneella sekä kommentoidaan 3 viimeistä riviä (kuva 38). Niitä rivejä ei tarvitse kommentoida siinä tilanteessa, kun on Linux-käyttäjiä ottamassa yhteyden VPN-palvelimeen. Tallennetaan ja suljetaan tiedosto.

```
# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
#ca ca.crt
#cert client.crt
#key client.key
```

Kuva 35. Ca, cert ja key -kentät kommentoitu.

```
# If a tls-auth key is used on the server
# then every client must also have the key.
#tls-auth ta.key 1
```

Kuva 36. TLS-auth -rivi kommentoitu, sillä ta.key lisätään suoraan samaan tiedostoon.

```
# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
cipher AES-256-CBC
auth SHA256
```

Kuva 37. AES-256-CBC ja SHA256 valittuna salakirjoitus- ja autentikointitapana.

```
key-direction 1

# script-security 2
# up /etc/openvpn/update-resolv-conf
# down /etc/openvpn/update-resolv-conf
```

Kuva 38. Key-direction 1 -arvo lisätty. Kolme viimeistä riviä on kommentoitu, koska tässä suunnitelmassa ei käytetty Linux-käyttäjiä asiakkaana.

Viimeinen vaihe tässä luvussa on käyttää komentosarjaa, jonka tarkoitus on luoda asiakkaalle oma konfiguraatio-tiedosto. Käytämme internetissä saatavaa komentosarjaa. Luodaan ensin kuvan 39 mukaisesti tiedosto kyseiseen hakemistoon. Kuvan 40 komentosarjassa tärkeintä on korvata harmaalla laatikoilla olevat kentät omalla käyttäjänimellä, mistä kyseiset client-configs -tiedostot löytyvät omalta palvelimelta.

Varmistetaan vielä viimeiseksi, että komentosarjalla on suoritus-oikeudet (kuva 41). Komentosarja hakee kaikki sertifikaatit ja avaimet, jotka on tehty ja purkaa ne uuteen tiedostoon.

```
nano ~/client-configs/make_config.sh
```

Kuva 39. Make_config.sh -tiedoston luominen.

```
#!/bin/bash

# First argument: Client identifier

KEY_DIR=/home/[redacted]/client-configs/keys
OUTPUT_DIR=/home/[redacted]/client-configs/files
BASE_CONFIG=/home/[redacted]/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 40. Komentosarja, jolla luodaan valmiiksi asiakkaalle oma konfiguraatio-tiedosto. Harmaat laatikot korvataan omalla käyttäjänimellä, missä tiedostot sijaitsevat.

```
chmod 700 ~/client-configs/make_config.sh
```

Kuva 41. Suoritusoikeudet make_config.sh-tiedostolle.

4.2.8 Asiakas-konfiguraatioiden luominen

Tässä luvussa generoidaan aikaisemman luvun komentosarjaa käyttäen asiakas konfiguraatiota. Tässä käytännönosuudessa käytettiin client1-nimistä sertifikaattia ja

avainta, joten tälle luodaan nyt oma konfiguraatio. Selataan kuvan 42 hakemistoon ja suoritetaan kuvan 43 komento. Prosessin jälkeen tiedosto client1.ovpn on luotu.

```
cd ~/client-configs
```

Kuva 42. Hakemisto, missä komentosarja on.

```
sudo ./make_config.sh client1
```

Kuva 43. Komentosarjan suorittaminen.

Komentosarja luo client1.ovpn -tiedoston, joka lopuksi annetaan asiakkaalle joko USB-muistitikulla tai lähetetään etänä verkon yli. Asiakas käyttää tätä tiedostoa oman tietokoneen OpenVPN-ohjelmistolla, jolla hän saa yhteyden OpenVPN-palvelimeen.

5 TESTIYMPÄRISTÖN VIANMÄÄRITYS

Testiympäristössä ilmeni ongelmia, jonka vuoksi sitä jouduttiin selvittelemään. Ongelmana oli OpenVPN-palvelimen käynnistyksessä. Vianmääritys aloitettiin ensin konfiguraatio-tiedostoista, jos niissä oli vääriä arvoja. Näistä tiedostoista ei löydetty poikkeamia. Hakemistoja katsottiin seuraavaksi, josko polut ja tiedostot olisivat väärässä paikassa. Näistäkään ei myöskään löydetty poikkeumia.

Server.conf -tiedostosta korjaustoimenpiteeksi kokeiltiin laittaa dh.pem, ca.crt, server.cr ja server.key -tiedostoihin täysi hakemistopolku, että tiedosto osaisi löytää ne. OpenVPN-palvelimen uudelleenkäynnistäminen ei myöskään tepsinyt.

Lopulta ongelmana oli Proxmox-virtuaaliympäristön asetuksissa. Seuraavat rivit laitettiin /etc/pve/lxc/CONTAINERID.conf -proxmox tiedostossa:

```
lxc.mount.entry: /dev/net/tun dev/net/tun none bind,create=file
lxc.cgroup.devices.allow: c 10:200 rwm
```

Tämän jälkeen OpenVPN-palvelimen server.conf -tiedostoon lisättiin nämä rivit:

```
/etc/pve/lxc
581 conf
lxc.mount.entry: /dev/net/tun dev/net/tun none bind,create=file
lxc.cgroup.devices.allow: c 10:200 rwm
```

Tämän korjauksen johdosta OpenVPN-palvelin saatiin onnistuneesti päälle testiympäristössä.

6 TULOKSET JA JOHTOPÄÄTÖKSET

Opinnäytetyön tavoitteena oli laatia suunnitelma toimivasta VPN-verkosta yritykselle. Tuloksena oli suunnitelma VPN-verkosta, jota voidaan soveltaa yrityksen käytössä. Työtä tehdessäni aihe muuttui muutamaan otteeseen, mutta tarkennusten ja viimeistelyjen johdosta sain työn haluttuun määränpäähän. Työtä hankaloitti puutteellinen kokemus VPN-verkoista. Mielestäni työssä onnistuin luomaan materiaalia suunnitelmaan sekä selittämään VPN-verkon teoriasta.

Testiympäristössä ilmeni ongelmaa aluksi. Vikaa yritettiin selvittää monella eri tavalla, kuten konfiguraatioiden tarkistuksella, palvelimen uudelleenkäynnistyksellä sekä hakemistopolkujen varmentamisella. Lopulta muutaman koodirivin lisääminen auttoi asiaan.

Tulevaisuudessa kannattaa ottaa huomioon muuttuvat tietosuojariskit ja haavoittuvuudet. Internetistä on mahdollista löytää ajantasaiset tietoturva-aukot, jolloin palvelinta tulee päivittää ajan tasalle. CA-palvelin on hyvä pitää poissa päältä, kun ei ole tarkoitus allekirjoittaa avaimia. Tällä tehdään ennaltaehkäisevä toimenpide, ettei palvelimeen suoriteta tietoturvahyökkäystä.

Tämän työn tuloksia voidaan soveltaa monessa eri pienyrityksesä. Suositeltavaa on kuitenkin katsoa ajankohtaiset ja tarkemmat ohjeet internetistä saatavilta VPN-ohjeista. Jatkokehitys VPN-verkolle on esimerkiksi luoda enemmän asiakasprofiileja sekä luoda vielä turvallisempi kokonaisuus säätämällä OpenVPN-palvelimen konfiguraatio-tiedostoja ja palomuuria.

LÄHTEET

Akava 2018. Etätyö. Viitattu 8. Helmikuu 2019 https://www.akava.fi/tyoelama/tyossa/etatyo.

Ala-Mutka, K.; Rintala, M.; Savikko, V. & Palviainen, J. 2002. OSI-malli. Viitattu 10. maaliskuuta 2019 http://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html.

Anon. 2018. OSI-malli. Viitattu 1. maaliskuuta 2019 https://fi.wikipedia.org/wiki/OSI-malli.

Beal, V. 2019. LAN - Local-area network. Viitattu 28. toukokuuta 2019 https://www.webopedia.com/TERM/L/local_area_network_LAN.html.

Cloudflare 2019. What Is Transport Layer Security (TLS)? Viitattu 28. toukokuuta 2019 https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/.

Das, R. 2019. The Security Policy and Network Requirements of a Virtual Private Network. Viitattu 14. kesäkuuta 2019 https://resources.infosecinstitute.com/security-policy-network-requirements-virtual-private-network/.

Das, R. 2019. An Insight into Virtual Private Networks and IP Tunneling. Viitattu 14. kesäkuuta 2019 https://resources.infosecinstitute.com/insight-virtual-private-networks-ip-tunneling/#article.

Dell 2019. Verkkosovittimen MAC-osoitteen selvittäminen Windows-käyttöjärjestelmässä. Viitattu 28. toukokuuta 2019 https://www.dell.com/support/article/fi/fi/fidhs1/sln285183/verkkosovittimen-mac-osoitteen-selvitt%C3%A4minen-windows-k%C3%A4ytt%C3%B6j%C3%A4rjestelm%C3%A4ss%C3%A4?lang=fi.

Drake, m. & Ellingwood, J. 2018a. How To Set Up an OpenVPN Server on Debian 9. Viitattu 15. toukokuuta 2019 https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-debian-9.

Drake, M. & Ellingwood, J. 2018b. Creating the Server Certificate, Key, and Encryption Files. Viitattu 14. kesäkuuta 2019 https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-debian-9#step-3-%E2%80%94-creating-the-server-certificate,-key,-and-encryption-files.

Drake, M. & Ellingwood, J. 2018c. Configuring the OpenVPN Service. Viitattu 15. kesäkuuta 2019 https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-debian-9#step-4-%E2%80%94-generating-a-client-certificate-and-key-pair.

Ellingwood, J. 2018. Initial Server Setup with Debian 9. Viitattu 19. Toukokuu 2019 (https://www.digitalocean.com/community/tutorials/initial-server-setup-with-debian-9).

ExpressVPN 2019. What is PPTP? Viitattu 16. kesäkuuta 2019 https://www.expressvpn.com/what-is-vpn/protocols/pptp.

Fonecta 2018. B2b vs b2c – miten yritysmarkkinointi eroaa kuluttajamarkkinoinnista? Viitattu 17. kesäkuuta 2019 https://www.fonecta.fi/b/b2b-vs-b2c-miten-yritysmarkkinointi-eroaa-kuluttajamarkkinoinnista.

Galvin, J. 2018. 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here's How to Protect Yourself. Viitattu 2019. kesäkuuta 13 https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html.

Hoffman, C. 2017a. 4 Easy Ways to Remotely Print Over the Network or Internet. Viitattu 15. toukokuuta 2019 https://www.howtogeek.com/168769/4-easy-ways-to-remotely-print-over-the-network-or-internet/.

Hoffman, C. 2017b. What’s the Difference Between TCP and UDP? Viitattu 15. huhtikuuta 2019 https://www.howtogeek.com/190014/htg-explains-what-is-the-difference-between-tcp-and-udp/.

Hoffman, C. 2018c. Which is the Best VPN Protocol? PPTP vs. OpenVPN vs. L2TP/IPsec vs. SSTP. Viitattu 10. huhtikuuta 2019 https://www.howtogeek.com/211329/which-is-the-best-vpn-protocol-pptp-vs.-openvpn-vs.-l2tpipsec-vs.-sstp/.

KeepSolid 2019. What is IKE protocol? Viitattu 14. toukokuuta 2019 https://www.vpnunlimitedapp.com/en/info/more-about-vpn/vpn-protocols/ike-protocol.

Kerrisk, M. 2012. TCP Fast Open: expediting web services. Viitattu 28. toukokuuta 2019 https://lwn.net/Articles/508865/.

Kumar, G.; Kumar, K. & Sachdeva, M. 2010. The use of artificial intelligence based techniques for intrusion detection: a review. Introduction. Viitattu 9. huhtikuuta 2019.

Mallik, A.; Ahsan, A.; Tsou, J.-C. & Shahadat, M.M.Z. 2019. Man-in-the-middle-attack: Understanding in simple words. Survey Research. Growing Science.

Mitchell, B. 2018. Network Interface Cards Explained. Viitattu 17. kesäkuuta 2019 https://www.lifewire.com/definition-of-nic-817866.

National Institute of Standards and Technology 2001. Announcing the ADVANCED ENCRYPTION STANDARD (AES).

OpenVPN Security Advisory 2018a. Viitattu 22. toukokuuta 2019 https://openvpn.net/community-resources/how-to/.

OpenVPN 2019b. Assigning a static VPN client IP address to a user. Viitattu 22. toukokuuta 2019 https://openvpn.net/vpn-server-resources/assigning-a-static-vpn-client-ip-address-to-a-user/.

OpenVPN 2019c. Overview Of Openvpn. Viitattu 14. kesäkuuta 2019 https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn.

OpenVPN 2019d. Use-cases for the OpenVPN Access Server product. Viitattu 21. toukokuuta 2019 https://openvpn.net/vpn-server-resources/use-cases-for-the-openvpn-access-server-product/.

OpenVPN 2019e. Setting up your own Certificate Authority (CA). Viitattu 14. kesäkuuta 2019 https://openvpn.net/community-resources/setting-up-your-own-certificate-authority-ca/.

PCMag 2019. IP address. Viitattu 22. toukokuuta 2019 https://www.pcmag.com/encyclopedia/term/45349/ip-address.

Prakash, A. 2018. Using apt-get Commands In Linux [Complete Beginners Guide]. Viitattu 21. huhtikuuta 2019 https://itsfoss.com/apt-get-linux-guide/.

PureVPN 2019. SSTP VPN - The World's Most Secure VPN Protocol. Viitattu 14. kesäkuuta 2019 https://www.purevpn.com/what-is-vpn/protocols/sstp.

Rouse, M. 2018. IPsec (Internet Protocol Security). Viitattu 28. toukokuuta 2019 https://searchsecurity.techtarget.com/definition/IPsec-Internet-Protocol-Security.

Savill, J. 2005. Which ports do you need to open on a firewall to allow PPTP and L2TP over IPSec VPN tunnels? Viitattu 14. kesäkuuta 2019 https://www.itprotoday.com/security/which-ports-do-you-need-open-firewall-allow-pptp-and-l2tp-over-ipsec-vpn-tunnels.

Sharma, T. & Yadav, R. 2015. Security in Virtual private network. Bahadurgarh: P.D.M College of Engineering.

Skoudis, E. 2004. Guarding against malware infection from remote users. Viitattu 14. kesäkuuta 2019 https://searchenterprisedesktop.techtarget.com/tip/Guarding-against-malware-infection-from-remote-users.

Soon, A. 2019. Why using a free VPN is a no good, very bad idea. Viitattu 14. kesäkuuta 2019 https://www.hardwarezone.com.sg/blog-why-using-free-vpn-no-good-very-bad-idea.

w3schools.com 2019. What is HTTP? Viitattu 28. toukokuuta 2019 https://www.w3schools.com/whatis/whatis_http.asp.

Zimmermann, H. 1980. OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. IEEE. 15. maaliskuuta 2019https://ieeexplore.ieee.org/document/1094702.