

Timo Talja

# VPN ja OpenVPN

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

15.1.2015

Tekijä(t) Otsikko	Timo Talja VPN ja OpenVPN
Sivumäärä Aika	31 sivua + 1 liitettä 29.3.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Janne Salonen
<p>Tämän opinnäytetyön tarkoituksena on tutustua VPN-tekniikkaan sekä eri salausprotokolliin. Teoriaosuudessa käydään läpi erilaisia salausprotokollia. Käytännön osuuden aikana luodaan toimiva OpenVPN-palvelinympäristö Virtualbox-virtuaalikoneohjelmiston avulla. Kaikki opinnäytetyössä käytetyt sovellukset perustuvat avoimeen lähdekoodiin.</p> <p>Työssä käydään läpi tarvittavat asennusvaiheet sertifikaattien sekä avaimien luontiin palvelimelle. Työssä luodaan myös esimerkiksi älypuhelimelle OpenVPN-yhteysprofiili. Työssä esitellään myös Android-puhelimille suunniteltu sovellus OpenVPN Connect ja sen käyttöönotto.</p> <p>Teoriaosuudesta käy ilmi, että IPSec on suosittu protokolla yritysmaailmassa sen laajan laitetuen takia. MPLS-protokolla on yleistymässä kovaa tahtia. MPLS-protokollan etuina ovat sen hallittavuus ja nopeus.</p> <p>Jatkokehitettävää jäi esimerkiksi kaksivaiheisen tunnistuksen käyttöönotto sekä älykörtin hyödyntäminen käyttäjän autentikoinnissa.</p>	
Avainsanat	VPN, OpenVPN

Author(s) Title	Timo Talja VPN and OpenVPN
Number of Pages Date	31 pages + 1 appendices 29 March 2015
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Datanetworks
Instructor(s)	Janne Salonen, Principal Lecturer
<p>Purpose of this thesis is to explore the VPN technology, and various encryption protocols related to VPN.</p> <p>The theory part of this thesis concentrates on VPN itself and encryption protocols. The practical portion of the thesis is about making a working OpenVPN server environment using Virtualbox virtual machine software. All applications used in this thesis are open source.</p> <p>This work presents the necessary installation steps to create certificates and keys for the server. In this work I will also show how to create OpenVPN connection profile. The work also introduces an Android phone application called OpenVPN Connect and how to connect to OpenVPN server with it.</p> <p>Theory shows that the IPSec protocol is a popular in commercial use due to its broad hardware support. MPLS protocol is becoming widely used. Benefits of MPLS protocol are its configureability and speed.</p> <p>Further development regarding this thesis could include, for example, creating dual-factor authentication to an OpenVPN configuration using client-side smart cards.</p>	
Keywords	VPN, OpenVPN

## Sisällys

### Lyhenteet

1	Johdanto	1
2	VPN	2
2.1	VPN:n hyödyt	4
2.2	VPN yhteystavat	5
2.2.1	Etäyhteys (Host-to-Site) VPN	5
2.2.2	Host-to-Host VPN	5
2.2.3	Site-to-Site VPN	6
2.3	VPN-tunnelointiprotokollat	7
2.3.1	GRE	7
2.3.2	IPSec	7
2.3.3	L2F	8
2.3.4	PPTP	9
2.3.5	L2TP	10
2.3.6	MPLS VPN	11
2.3.7	SSL VPN	12
3	OpenVPN	13
3.1	OpenVPN:n asennus	14
3.2	Salaamattoman yhteyden luominen kahden koneen välille	15
3.3	Certificate Authorityn ja avaimen luonti palvelimelle.	16
3.4	Palvelimen konfiguraatiot	18
3.5	Asiakaslaitteiden sertifikaattien ja avaimien luonti	20
3.6	Yhtenäisen OpenVPN-profiilitiedoston luonti	22
3.7	Yhteyden muodostaminen ja tarkistaminen Windows-koneella	24
3.8	OpenVPN Connect	25
3.9	Huomioita	27
4	Yhteenveto	29
	Lähteet	30
	Liitteet	
	Liite 1. Yhteysprofiilitiedosto esimerkki	

## Lyhenteet

Extranet	Extranet on yrityksen tai muun yhteisön ja asiakkaan tai yhteistyökumppanin välinen Internet-teknologiaa hyödyntävä suljettu verkkopalvelu.
GRE	Generic Routing Encapsulation. Salaamaton yhteys IP-protokollan otsikkotietojen avulla.
IPSec	IP Security. IETF:n standardoima Internetin tietoturvaprotokolla.
L2F	Layer 2 Forwarding. Ciscon tunnelointiprotokolla.
L2TP	Layer 2 Tunnelin Protocol. RFC 2661. PPTP-protokollan seuraaja.
MPLS	Multi-Protocol Label Switching. Kuljettaa IP-paketteja ennalta määriteltyjen yhteyksien ylitse nopean runkoverkon solmujen kautta ilman.
PPP	Point-to-Point Protocol. Käytetään muodostamaan suora yhteys verkkolaitteiden välille.
PPTP	Point to Point Tunneling Protocol. RFC 1331. Suunniteltu analogisia puhelimia ja digitaalisia ISDN-puhelimia hyödyntäviin yhteyksiin.
SSH	Secure Shell. Salattuun tietoliikenteeseen tarkoitettu protokolla.
SSL	Secure Socket Layer. Salattuun tietoliikenteeseen tarkoitettu protokolla. TLS:n edeltäjä.
TLS	Transport Layer Security. Salattuun tietoliikenteeseen tarkoitettu protokolla.
VPN	Virtual Private Network. Virtuaaliset erillisverkot muodostavat yksityisen verkon julkisen verkon yli.

## 1 Johdanto

Käyn tässä opinnäytetyössä läpi VPN-tekniikkaa (Virtual Private Network). Työssä selvitetään, mitä se on, kuinka se kehittyi ja mihin sitä käytetään. Samalla käydään läpi mitä hyötyä ja ominaisuuksia VPN:n tarjoaa. Työssä käydään läpi myös eri tunnelointi- ja salustekniikoita liittyen VPN:n käyttöön.

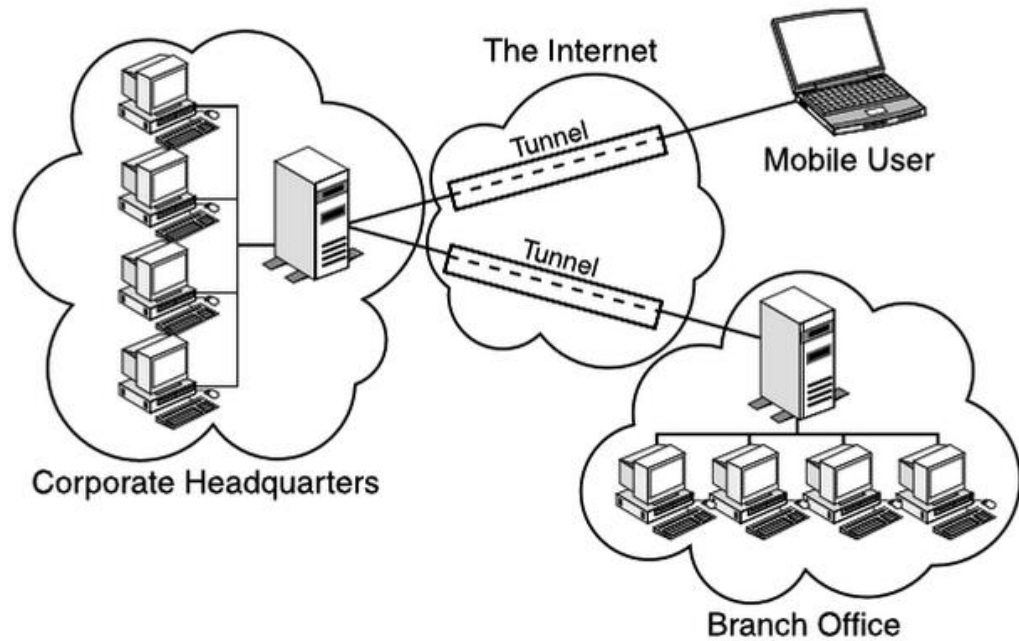
Lopuksi opinnäytetyössä tutustutaan OpenVPN-sovellukseen. Opinnäytetyössä käytetään virtuaalikoneiden luomiseen ilmaista Virtualbox-sovellusta. Virtuaalikonetta hyödyntäen näytetään käytännössä, miten yhteys luodaan esimerkiksi Windows- ja Linux -tietokoneen välille. Linux-koneen käyttöjärjestelmänä käytetään Ubuntun versiota 14.04. Työssä näytetään tarvittavat vaiheet ja työkalut, mitä vaaditaan salatun VPN-yhteyden luomiseen OpenVPN-ohjelmiston avulla. Tutustutaan myös Android-puhelimille saatavilla olevaan OpenVPN Connect -applikaatioon. Työssä käytetyt ohjelmistot ovat kaikki ilmaisia.

## 2 VPN

VPN-yhteydet luotiin järjestelmäylläpitäjien elämän helpottamiseksi etäyhteyksiä varten. Aikaisemmin vaihtoehtoina oli muodostaa suora yhteys modeemilla tai sitten rakentaa dedikoitu linja toimipisteiden välille. Ensimmäinen näistä vaihtoehdoista ei ollut turvallinen eikä nopea, minkä lisäksi se oli altis virheilylle. Jälkimmäinen vaihtoehto oli turvallinen, mutta kallis toteuttaa eikä soveltunut kaukaisille kohteille tai paljon liikkuvalla työntekijälle. [Casad 2009: 404.]

Ratkaisuksi keksittiin yhdistää toimipisteet Internetin yli. Tällöin yhteys ei ole kovin turvallinen, koska se kulkisi helposti nähtävissä ja kaapattavissa. Tästä syystä kehitettiin keino luoda tunneli kahden toimipisteen tai liikkuvan työntekijän välille, jossa tieto kulkee salattuna. Näitä salattuja yhteyksiä alettiin kutsua virtuaalisiksi erillisverkoiksi (VPN). [Casad 2009: 404.]

Täytyy muistaa, että vaikka VPN-yhteyden vähentävät riskiä altistua tietovuudolle, varsinkin Internetin yli, ne eivät poista sitä kokonaan. Yksi ongelmista voi olla toteutuksen heikkotasoisuus. Esimerkiksi käytettävän protokollan salausalgoritmi voi olla haavoittuvainen tai yhteyden muodostamiseen käytetyssä ohjelmistossa voi olla haavoittuvuuksia, joita hyökkääjät voivat hyödyntää. Toinen vaaratekijä ovat salausavaimien joutuminen väärin käsiin. Hyökkääjä, joka on saanut avaimet haltuunsa, voi tulkita salattua tietoa tai esiintyä autentikoituneena käyttäjänä. [Frankel ym. 2008.]



Kuva 1. Tyypillinen VPN-ratkaisu. [Gupta 2002: 5].

Kuvasta 1 selviää tyypillinen tapa hyödyntää VPN-yhteyksiä.

VPN-yhteyksiä voidaan käyttää kahdella eri menetelmällä: itsenäisenä laitteena tai ohjelmistopohjaisella ratkaisulla. Itsenäisen laitteen tapauksessa työntekijälle annetaan laite, joka yhdistää Internetiin automaattisesti ja muodostaa salatun yhteyden yrityksen VPN-palvelimeen tai -yhdyskäytävään. Tämän jälkeen työntekijä voi liittää tietokoneen tai IP-puhelimen laitteeseen ja käyttää niitä kuin olisi työpaikan verkossa. Ohjelmistopohjaisessa ratkaisussa käyttäjän koneelle asennetaan VPN-ohjelmisto, joka salaa kaikki lähtevät ja tulevat paketit. [Comer 2009: 527.]

Ensimmäiset VPN-ratkaisut tulivat markkinoille 80-luvun loppuvaiheilla AT&T:n toimesta ja ne tunnettiin SDN (Software Defined Networks) nimellä. SDN:t olivat käytännössä pitkän matkan laajaverkkoja ja hyödynsivät tietokantoja tulkitakseen, tuliko yhteyspyyntö paikallisesti vai etänä. Tämän tiedon perusteella data ohjattiin oikeaan kohteeseen julkisen verkon kautta.

Toinen sukupolvi ilmestyi 90-luvun alkupuolella X.25:n ja ISDN:n yhteydessä. Nämä uudet siirtoyhteydet sallivat pakettivirtojen lähettämisen jaetun julkisen verkon yli. Tämä oli



halvempaa kuin aiemmin ja luultiin, että X.25-protokolla löisi ISDN:n VPN-käytössä. Kuitenkin siirto yhteydet jäivät laadultaan ja luotettavuudeltaan heikoiksi.

Kolmas sukupolvi perustui Frame Relay- (FR) ja Asynchronous Transfer Mode (ATM) -teknologioihin. Nämä teknologiat hyödyntävät virtuaalista piirikytkentää, jolloin datapaketit eivät sisällä lähde- tai vastaanottajatietoa. Sen sijaan ne sisältävät pointtereita, jotka osoittavat nodeihin. Nodit puolestaan sisältävät tarpeelliset osoitetiedot.

Nykyiset VPN-yhteydet käyttävät tunnelointia, jolloin niitä on helppo toteuttaa ja hallinnoida, minkä lisäksi ne tarjoavat hyvän tietoturvan. [Gupta 2002: 6-7.]

## 2.1 VPN:n hyödyt

Virtuaaliset erillisverkot (VPN) mahdollistavat kahden tietokoneen yhteydenpidon keskenään turvallisesti julkisen verkon yli kuten Internetin. Tämä mahdollistaa työntekijöiden, yhteistyökumppaneiden ja muiden toimipisteiden tietokoneiden käyttää päätoimiston verkkoa. Esimerkiksi ollessaan matkalla myyjä voi tarkistaa yrityksen tuotekannasta tietoja matkalla ollessaan oman kannettavan tai älypuhelimien avustuksella. Seuraavassa on lueteltuna viisi VPN:n suurinta hyötyä.

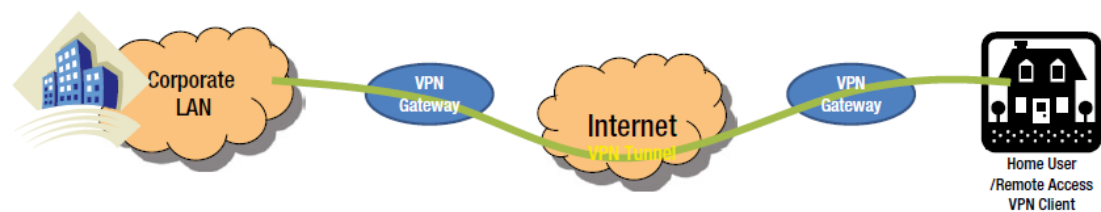
- **Säästö:** Yksityisten verkkojen käyttö oli ennen lähes ainoa järkevä ratkaisu laajaverkkoihin. Laajaverkot olivat kalliita eivätkä aina kannattavia. Ongelmana oli myös niiden heikko skaalautuminen ja turvallisuusominaisuuksien puuttuminen. VPN-yhteydet ratkaisevat nämä ongelmat käyttäen Internetiä halpana vaihtoehtona ja tarjoten paremmat turvallisuusominaisuudet.
- **Sulava integraatio:** VPN-yhteyksien muodostamiseen ei tarvita uusia laitehankintoja vaan voit hyödyntää jo olemassa olevaa infrastruktuuria.
- **Turvallinen etäyhteys:** Tärkein ominaisuus VPN-yhteyksissä on tarjota turvallinen etäyhteys organisaation sisäiseen verkkoon.
- **Extranet-yhteydet:** Liikekumppanit ovat tärkeä osa ekonomiaa ja oman yrityksen menestystä. Yritysten pitää pystyä jakamaan keskenään tiedostoja ja tärkeää tietoa luotettavasti.

- Helppo ylläpito: VPN-yhteydet eivät erikseen tarvitse uusia tunnistevaimia. [Nayak & Rao 2014: 246-247.]

## 2.2 VPN-yhteystavat

### 2.2.1 Etäyhteys (Host-to-Site) VPN

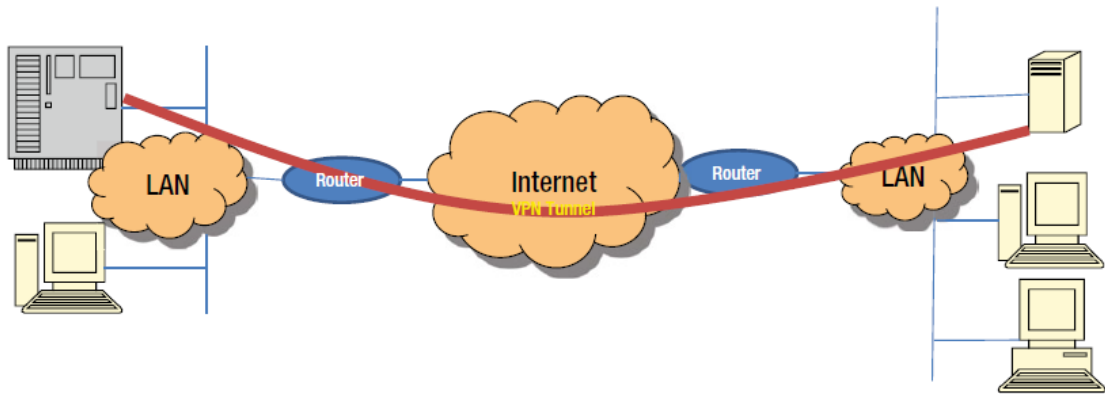
Perinteinen VPN-yhteys muodustuu käyttäjän tietokoneen ja yrityksen sisäisen verkon välille. Käyttäjinä ovat työntekijät, jotka tarvitsevat yhteyden yrityksen verkkoon esimerkiksi junasta. Käyttäjä ottaa VPN-ohjelmistolla yhteyden yrityksen verkkoon ja VPN-yhdyskäytävään (kuva 2). VPN-yhdyskäytävä autentikoi käyttäjän ja luo salatun tunnelin käyttäjän tietokoneen ja yhdyskäytävän välille. Tämän jälkeen käyttäjän kaikki data kulkee yrityksen verkon kautta, ja hän voi käyttää yrityksen verkossa olevia palveluita. [Nayak & Rao 2014: 247.]



Kuva 2. Perinteinen VPN-yhteys [Nayak & Rao 2014: 248.]

### 2.2.2 Host-to-Host VPN

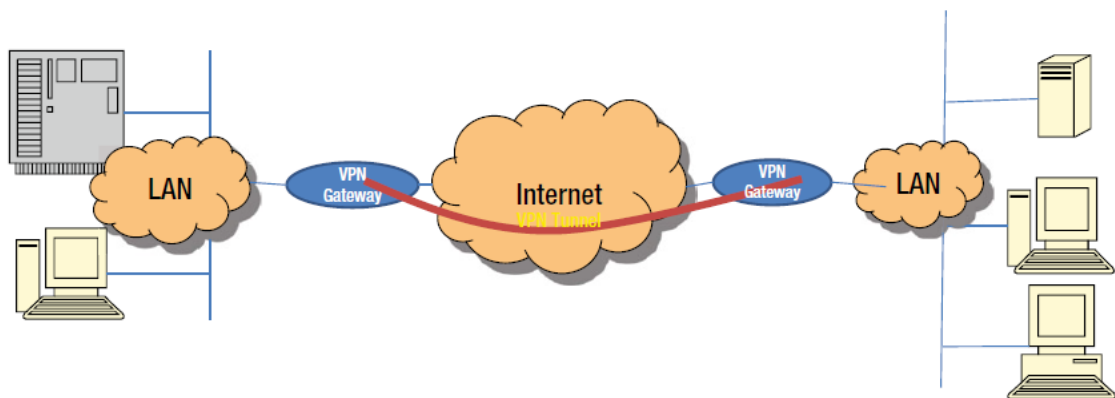
Host-to-Host VPN -yhteys on lähes sama kuin Host-to-Site VPN. Erona on se, että tässä luodaan yhteys suoraan kahden koneen välille ja ne muodostavat keskenään salatun VPN-yhteyden. Ennen yhteyden luomista koneet autentikoivat käyttäjät ja vaihtavat salausavaimet keskenään. Vasta tämän jälkeen voi tiedon siirto alkaa. Kuvasta 3 näkyy, kuinka tietokoneesta on luotu suora VPN-yhteys palvelimeen, joka voi sijaita esimerkiksi toisessa yrityksessä. [Nayak & Rao 2014: 248.]



Kuva 3. VPN-yhteys kahden tietokoneen välillä. [Nayak & Rao 2014: 248.]

### 2.2.3 Site-to-Site VPN

Site-to-Site VPN yhdistää kaksi lähiverkkoa toisiinsa Internetin yli, esimerkiksi kuten kuvassa 4 yrityksen toinen toimipiste on yhdistetty päätoimiston verkkoon. Tällöin VPN-tunneli luodaan molemmissa päissä VPN-yhdyskäytäviin. Tällöin ei tarvita erillisiä VPN-sovelluksia käyttäjien laitteilla, koska yhdyskäytävä hoitaa koko liikenteen ohjaamisen. VPN-yhdyskäytävät vastaavat käyttäjien ja verkon autentikoinnista, salauksesta ja tiedon eheydestä.



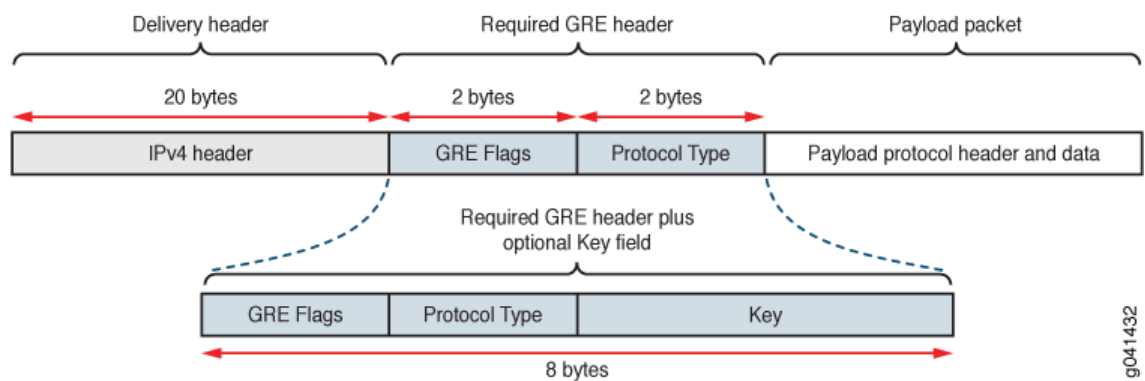
Kuva 4. VPN-yhteys kahden eri toimipisteen välillä [Nayak & Rao 2014: 249.]

## 2.3 VPN-tunnelointiprotokollat

VPN-verkoissa käytetään tunnelointiprotokollia, jotka ovat yleensä salattuja. Tunneloinnin voi tehdä myös salaamattomana, mutta nykyisin lähes kaikki VPN-yhteydet käyttävät vahvaa salausta ja käyttäjien tunnistusta.

### 2.3.1 GRE

GRE-protokollalla (Generic Routing Encapsulation) voidaan muodostaa salaamaton yhteys IP-protokollan otsikkotietojen avulla. GRE-protokolla kapseloi IP-datagrammin toisen IP-datagrammin sisälle. Tällöin lähtevä IP-datagrammi rakentuu toimitusotsakkeesta (Delivery Header), GRE-otsakkeesta sekä kapseloidusta IP-datagrammista (Payload).

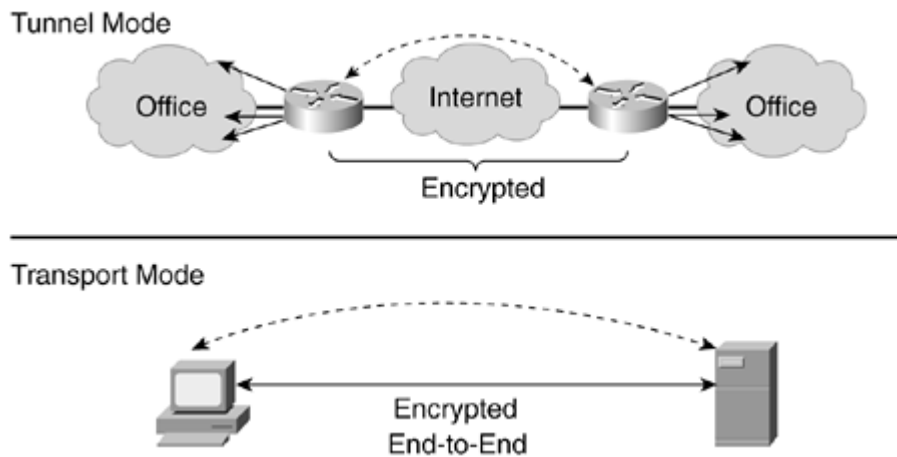


Kuva 5. GRE-paketin sisältö. [Juniper.net: Components of Filter-Based Tunneling Across IPv4 Networks]

Toimitusotsake on vastaavanlainen kuin IPv4-datagrammissa. Lähettäjäksi merkitään tunnelin alkupään julkinen IP-osoite ja vastaanottajan osoitteena toimii tunnelin loppupäänä toimiva laite. [Hakala & Vainio 2005: 382.]

### 2.3.2 IPSec

IETF:n standardoima tietoturvaprotokolla IP Security (IPSec) mahdollistaa datan luottamuksellisen siirron ja eheyden. IPSec sisältää protokollat avaintenhallintaan sekä turvalaajennuksen IP-protokollaan. IPSec-protokolla toimii OSI-mallin verkkokerroksen tasolla. Tämä tarkoittaa sitä että IPSec-protokollan toiminnot ovat sovelluksesta riippumattomia. [Kaario 2002: 315.]

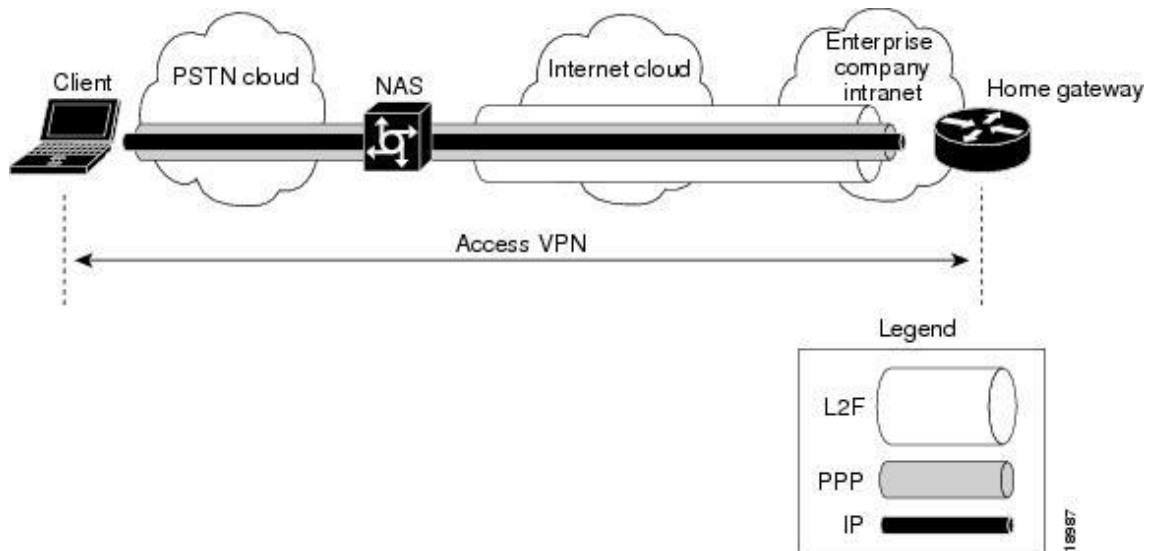


Kuva 6. IPsec tunnelointi- ja kuljetusmoodi. [etutorials.org: IPsec Overview.]

IPsec:ä voi käyttää joko kuljetusmoodissa tai tunnelointimoodissa. Kuljetusmoodissa data salataan IP-paketin sisälle. Tunnelointimoodissa koko IP-paketti kulkee salattuna. [Casaad 2009: 404.]

### 2.3.3 L2F

Ciscon kehittämä Layer 2 Forwarding -rotokolla toimii OSI-mallin toisella kerroksella hyödyntäen Point-to-Point-protokollaa (PPP) tai Serial Line Internet -protokollaa (SLIP). L2F-protokollaa käytetään vain Ciscon laitteissa. [thenetworkencyclopedia.com: Layer 2 Forwarding.]

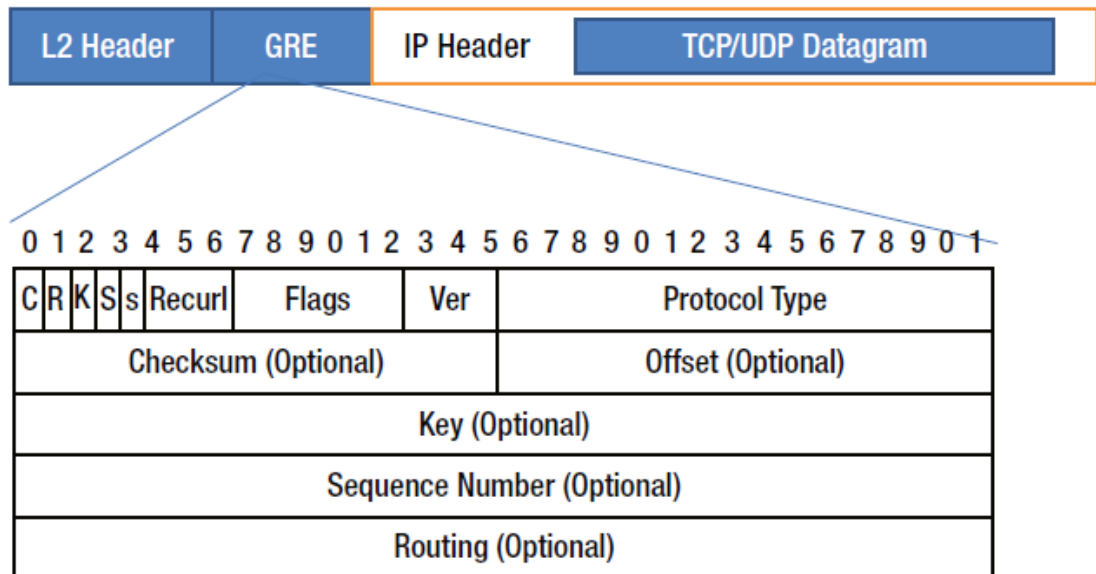


Kuva 7. Cisco Layer 2 Forwarding VPN. [Cisco.com: Cisco IOS Dial Technologies Configuration Guide, Release 12.2]

Protokolla on käytännössä poistunut kokonaan käytöstä ja sen on korvannut PPTP.

#### 2.3.4 PPTP

Point-To-Point Tunneling Protocol suunniteltiin alun perin analogisia puhelimia ja digitaalisia ISDN-puhelimia hyödyntäviin yhteyksiin. Nykyään modeemeihin ja ISDN-sovittimiin perustuvat yhteydet ovat harvinaisia. Protokollan tarkoituksena on kytkeä yhteydet piiriyhteyksien välikäytävien välille ja täten mahdollistaa yhteys pakettikytkentäiseen verkkoon, kuten Internetiin, operaattoreiden soittosarjojen avulla. Protokolla hyödyntää yhteyden muodostamiseen PPP-protokollaa (Point to Point Protocol). PPP-protokolla tarjoaa mekanismit yhteyden avaamiseen, käyttäjän tunnistukseen ja yhteyden hallintaan. [Hakala & Vainio 2005: 382-383.]



Kuva 8. IP-datagrammi, jossa GRE-otsake. [Nayak & Rao 2014: 253.]

PPTP-protokollassa sijoitetaan GRE-otsake PPP-kehukseen ja tämä kehys sijoitetaan IP-datagrammiin hyötykuormaksi. Samalla PPP-kehysten tiedot salataan. Salauksena käytetään salausavaimia tai vaihtoehtoisesti voidaan käyttää käyttäjätunnus-salasana - yhdistelmää (PAP, Password Authentication Protocol) tai haasteeseen perustuvaa tunnistusta (CHAP, Challenge Handshaking Authentication Protocol). CHAP:n kanssa käytetään erillistä tunnistuspalvelinta (EAP, Extensible Authentication Protocol). [Hakala & Vainio 2005: 382-383.]

### 2.3.5 L2TP

Layer 2 Tunneling Protocol toimii nimensä mukaisesti OSI-mallin toisella kerroksella eli siirtokerroksella. Protokollaa käytetään pakettikytkentäisissä verkoissa PPP-kehysten siirtämiseen. [Hakala & Vainio 2005: 383.]

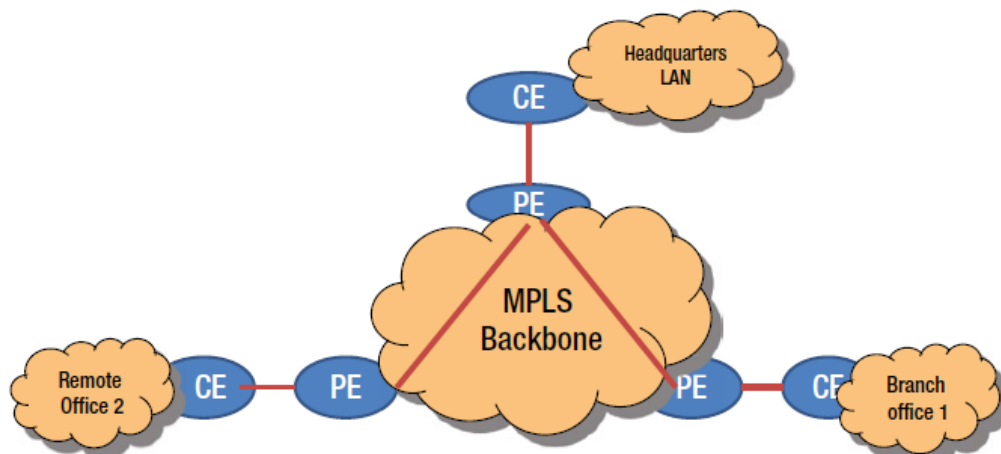
Protokolla salataan käyttämällä IPSec-protokollaa. L2TP-otsake sekä UDP-otsake lisätään alkuperäiseen PPP-kehukseen, joka salataan IPSecillä. Pakettiin lisätään IPSec Encapsulating Security Payload –otsakkeet sekä IPSec Authentication trailer. Lisätyistä ESP-otsakkeista (Encapsulating Security Payload) paketin alkuun sijoitettu IPSec ESP

header on salattu samoin kuin paketin loppuun sijoitettu IPSec ESP trailer. IPSec Authentication trailer on puolestaan salaamaton. Näistä kaikista muodostetaan paketti, joka sijoitetaan IP-datagrammin sisään. [Hakala & Vainio 2005: 383.]

### 2.3.6 MPLS VPN

Multi-Protocol Label Switching (MPLS) on uusi teknologia laajaverkkoyhteyksissä, erityisesti optisissa verkoissa. Ennen MPLS-verkkoja paketin liikkua verkosta ja reitittimestä toiseen jokainen reititin tarkistaa paketin otsakkeen sekä osoitetiedon ja vertaa tietoja reitityspöytänsä. Näiden perusteella reititin ohjaa paketin eteenpäin. Tämä toistuu jokaisen reitittimen kohdalla. [Nayak & Rao. 2014: 257-258.]

Tavalliset VPN-yhteydet ovat riippuvaisia tunnelointiprotokollasta, kuten GRE tai L2TP, mutta MPLS on itsessään jo tunneli julkisessa verkossa. MPLS-pohjaiset VPN-yhteydet käyttävät LSP:tä (Label Switch Path). LSP käytännössä tarkoittaa ennalta määrättyjä reittejä, jotka ovat reitittimien tiedossa. Paketeille annetaan tunniste (label), kun ne saapuvat palveluntarjoajan runkoverkkoon. [Sturt. 2014.]



Kuva 9. MPLS-pohjainen VPN-ratkaisu. [Nayak & Rao. 2014: 258.]

Kuvassa 6 näkyy MPLS-pohjainen VPN-ratkaisu. CE (Customer Equipment) on asiakkaan verkkolaite kuten esimerkiksi reititin tai kytkin. PE (Service Provider Equipment) on puolestaan osa palveluntarjoajan runkoverkkoa. PE-laitteet ovat vastuussa VPN yhteyksistä ja MPLS LSP-yhteyksistä toisten PE-laitteiden kanssa. [Nayak & Rao. 2014: 257-258.]



### 2.3.7 SSL VPN

SSL VPN (Secure Sockets Layer Virtual Private Network) voidaan käyttää tavallisella selaimella tai erillisellä ohjelmistolla kuten OpenVPN:llä. Yhteys käyttäjän tietokoneelta palvelimelle salataan joko SSL-protokollaa hyödyntäen tai uudempaa TLS-protokollaa (Transport Layer Security) käyttäen.

SSL VPN:ää on kahta mallia:

- SSL Portal VPN: Käyttäjä yhdistää itsensä SSL VPN -yhdyskäytävään ja tunnistautuu valitulla autentikointitavalla, jonka jälkeen hän voi käyttää käytettävissä olevia palveluita selaimen kautta.
- SSL Tunnel VPN: Tunneli muodostuu selaimen kautta, ja se tukee myös applikaatioita ja protokollia, jotka eivät ole selainpohjaisia. [Rouse. 2009.]

### 3 OpenVPN

OpenVPN-ohjelmiston on kehittänyt OpenVPN Technologies -yhtiö Kalifornian Pleasantonista. Yritys perustettiin Francis Dinhan ja James Yonan toimesta vuonna 2002 OpenVPN-projektin jälkeen, jotta OpenVPN-projektin kehitys jatkuisi vakaana. OpenVPN-ohjelmisto on ladattu jo yli kolme miljoonaa kertaa. [OpenVPN: About.]

OpenVPN on täysiverinen avoimeen lähdekoodiin perustuva SSL VPN -ratkaisu. Se sisältää useita mahdollisia konfiguraatioita kuten etäyhteydet, Site-to-Site-yhteydet, Wi-Fi-turvan ja yritystason etäratkaisut. OpenVPN hyödyntää SSL:ää, joka on tunnettu turvallisena tapana salata yhteyksiä Internetissä. OpenVPN käyttää OSI-mallin toista tai kolmatta tasoa hyödyntäen SSL/TLS-protokollaa liikenteen turvaamiseksi. OpenVPN tukee useita käyttäjän autentikointitapoja kuten esimerkiksi sertifikaatteja, älykortteja ja kaksivaiheista autentikointia.

OpenVPN:ää voi käyttää Linuxilla, Windows XP:llä tai uudemmalla Windowsilla, OpenBSD, FreeBSD, NetBSD, Mac OS X tai Solaris-käyttöjärjestelmillä. [OpenVPN: Overview].

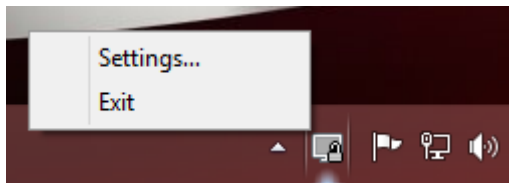
OpenVPN:n avulla voit esimerkiksi

- tunneloida minkä tahansa IP-aliverkon tai virtuaalisen verkkosovittimen yhteen UDP- tai TCP-porttiin
- konfiguroida skaalautuvan VPN-palvelinparin, joka pystyy käsittelemään tuhansia yhteyksiä
- ottamaan kaiken hyödyn irti OpenSSL-kirjaston salaus-, autentikointi- ja sertifiointiominaisuuksista
- valita staattiseen avaimen perustuvan salauksen tai sertifikaattipohjaisen julkisen avain -salauksen
- konfiguroida sitä Windows:lla tai Mac OS X:llä graafisesti
- tunneloida verkot NAT:n yli. [OpenVPN: What is OpenVPN].

### 3.1 OpenVPN:n asennus

OpenVPN on saatavilla ilmaiseksi OpenVPN:n nettisivuilta osoitteesta <http://openvpn.net/index.php/open-source/downloads.html> Windows- sekä Linux-koneille.

Windows-koneelle valitsin 64-bittisen ja tällä hetkellä uusinta versiota vastaavan asennuspaketin eli `openvpn-install-2.3.6-1601-x86_64.exe`. Tiedoston ladattua voidaan aloittaa asennus. Ensimmäisenä vastaan tulee tervetuloa-ikkuna ja heti perään käyttöehdot, jotka tulee hyväksyä asennuksen jatkamiseksi. Seuraavaksi päästään valitsemaan, mitkä komponentit asennetaan tai päivitetään. Oletusarvoisesti puhtaassa asennuksessa on lähes kaikki komponentit valittuna. Vain OpenSSL Utilities- ja OpenVPN RSA Certificate Management Scripts -komponentit eivät ole valittuina. Seuraavaksi valitaan asennuskansio, jonka jälkeen onkin jäljellä vain asennus. Asennuksen aikana Win8.1-koneelle aukesi Windows Securityn ikkuna, joka varmistaa, haluanko asentaa virtuaalisen verkkoadapterin. Hyväksytyään verkkoadapterin asennuksen asennusohjelma alkaa olla loppusuoralla. Viimeisellä sivulla voi valita, haluaako suoraan käynnistämään OpenVPN:n tai lukea Lueminut-tiedoston.



Kuva 10. OpenVPN GUI asennettuna Windows 8.1 -tietokoneeseen.

Linux-käyttäjärjestelmäksi valitsin Ubuntu 14.04 LTS -versio, koska sen käytöstä on en-tuudestaan kokemusta, minkä lisäksi Ubuntu on yleisestikin tunnettu ja hyvin tuettu Linux-versio. Ubuntu-käyttäjärjestelmä asennetaan VirtualBox-ohjelmiston avulla luotun virtuaalikoneelle. VirtualBox on täysin ilmainen sovellus, joka on saatavilla osoitteesta [www.virtualbox.org](http://www.virtualbox.org). VirtualBox-ohjelmisto toimii Linux-, Mac OS X-, Solaris- ja Windows-käyttäjärjestelmissä.

OpenVPN:n lisäksi tarvitaan `easy-rsa`-paketti, jolla luodaan tarvittavat varmenteet palvelimelle sekä yhdistäville laitteille. Molempien asennus Ubuntuun onnistuu helpoiten terminaalien kautta komennolla

```
sudo apt-get install openvpn easy-rsa
```

Asennus vaatii lisäksi paketin libpkcs11-helper1:n, joka tosin asentuu automaattisesti. Pakettien asennuksen jälkeen voi aloittaa asetusten muokkaamisen sekä muodostamaan ensimmäisen VPN-yhteyden.

### 3.2 Salaamattoman yhteyden luominen kahden koneen välille

Luodaan aluksi salaamaton yhteys, jotta päästään käytännössä heti näkemään ohjelman toimivuus. Tässä opinnäytetyössä virtuaalinen Linux-kone toimii palvelimena Virtualbox-ohjelman avustuksella.

Terminaalissa annetaan root-oikeuksin komento:

```
openvpn --ifconfig 10.200.0.1 10.200.0.2 --dev tun
```

Komento luo palvelimen päähän tunnelin IP-osoitteella 10.200.0.1 ja olettaa, että toinen pää tulee olemaan IP-osoitteella 10.200.0.2. Tunneli käyttää UDP-porttia 1194 yhteyden luomiseen. Parametri --dev tun ilmaisee, että käytetään TUN-tyyppistä virtuaalista verkotason "laitetta" eli toimitaan OSI-mallin tasolla kolme.

Windows-koneen puolella käynnistetään komentotulkki (cmd) järjestelmähaltijan oikeuksin ja navigoidaan OpenVPN.exe -tiedoston luokse. Oletussijainti tiedostolla on C:\Program Files\OpenVPN\bin -kansiossa. Kyseisen kansion juuressa voidaan antaa komento, jolla luodaan tunnelin toinen pää. Alla oleva komento tulee kirjoittaa kokonaisuudessaan yhdelle riville.

```
openvpn.exe --ifconfig 10.200.0.2 10.200.0.1 --dev tun  
--remote oppari.noip.me
```

Parametri --remote kertoo ohjelmalle, missä tunnelin toinen pää sijaitsee, jotta yhteys voidaan luoda. Tässä kohtaa voidaan käyttää myös staattista IP-osoitetta tai no-ip.comin tarjomaa ilmaista, dynaamista dns-palvelua, kuten esimerkissä olen käyttänyt.

```

C:\Program Files\OpenVPN\bin>openvpn.exe --ifconfig 10.200.0.2 10.200.0.1 --dev
tun --remote oppari.noip.me
Mon Mar 09 19:13:34 2015 OpenVPN 2.3.6 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO]
[PKCS11] [IPv6] built on Dec 1 2014
Mon Mar 09 19:13:34 2015 library versions: OpenSSL 1.0.1j 15 Oct 2014, LZO 2.08
Mon Mar 09 19:13:34 2015 ***** WARNING *****: all encryption and authenticat
ion features disabled -- all data will be tunneled as cleartext
Mon Mar 09 19:13:34 2015 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Mon Mar 09 19:13:34 2015 open_tun, tt->ipv6=0
Mon Mar 09 19:13:34 2015 TAP-WIN32 device [Ethernet 2] opened: \\.\Global\{AF129
407-8A6D-429B-876C-E7914A752913}.tap
Mon Mar 09 19:13:34 2015 Notified TAP-Windows driver to set a DHCP IP/netmask of
10.200.0.2/255.255.255.252 on interface {AF129407-8A6D-429B-876C-E7914A752913}
[DHCP-serv: 10.200.0.1, lease-time: 31536000]
Mon Mar 09 19:13:34 2015 Successful ARP Flush on interface [10] {AF129407-8A6D-4
29B-876C-E7914A752913}
Mon Mar 09 19:13:34 2015 UDPv4 link local (bound): [undef]
Mon Mar 09 19:13:34 2015 UDPv4 link remote: [AF_INET]89.27.100.93:1194
Mon Mar 09 19:13:44 2015 Peer Connection Initiated with [AF_INET]89.27.100.93:11
94
Mon Mar 09 19:13:50 2015 Initialization Sequence Completed

```

Kuva 11. Onnistunut yhteyden luonti Windows-koneelta katsottuna OpenVPN:llä.

Kuvassa kahdeksan näkyy onnistunut tunnelin luonti, minkä johdosta koneet voivat pingata toisiaan. Huomaa kuvassa näkyvä varoitus, joka kertoo, että kaikki tieto kulkee tässä esimerkissä täysin salaamattomana. Tämä tapa onkin käytännössä hyvä vain esimerkkinä ja yhteyden kokeilemisessa. F4-näppäimellä voidaan sulkea yhteys Windows-puolella ja Linuxilla vastaava onnistuu Ctrl+c-näppäinyhdistelmä.

### 3.3 Certificate Authorityn ja avaimen luonti palvelimelle

Tässä osiossa luodaan palvelimelle ja käyttäjille sertifikaatit ja avaimet. Tätä kokonaisuutta kutsutaan PKI:ksi (Public Key Infrastructure). Tämä on tärkeä ja olennainen osa siihen, miksi VPN-yhteydet ovat turvallisia ja että OpenVPN:n käyttö on turvallista. PKI koostuu julkisesta ja yksityisestä avaimesta palvelimelle sekä jokaiselle käyttäjälle. Siihen kuuluu myös pääavain, jolla allekirjoitetaan palvelimen ja käyttäjien sertifikaatit. Näiden tekoon tarvitaan easy-rsa-ohjelma, joka asennettiin aiemmin jo palvelimelle.

Kopioidaan ensiksi tarvittavat tiedostot oletuskansioista samaan kansioon kuin OpenVPN.

```
cp -r /usr/share/easy-rsa/ /etc/openvpn
```

Ja luodaan avaimia varten oma kansio.

```
mkdir /etc/openvpn/easy-rsa/keys
```

Navigoidaan `/etc/openvpn/easy-rsa`, josta pitäisi löytyä `vars`-niminen tiedosto. Kyseisestä tiedostosta voi muokata parametrit `KEY_COUNTRY`, `KEY_PROVINCE`, `KEY_CITY`, `KEY_ORG`, and `KEY_EMAIL` haluamikseen, mutta mikään ei saa jäädä tyhjäksi. `KEY_NAME` -parametriksi voi kirjoittaa esimerkiksi ”palvelin”.

Seuraavaksi muokataan OpenVPN:n palvelinkonfiguraatio tiedostosta kohta, jossa määritellään käyttämään avaimien luonnissa 2048-bittistä Diffie Hellman -salausprotokollaa. Diffie-Hellman-avaimenvaihtoprotokolla on salausprotokolla, jonka avulla kaksi osapuolta voivat sopia yhteisestä salauksesta turvattoman tietoliikenneyhteyden ylitse. [Wikipedia: Diffie-Hellman.]

```
nano /etc/openvpn/server.conf
```

Tiedostosta etsitään kohta `dh dh1024.pem` ja muutetaan `1024:n` tilalle `2048`. Tämän jälkeen luodaan parametrit käyttämällä komentoa

```
openssl dhparam -out /etc/openvpn/dh2048.pem 2048
```

Vielä `easy-rsa:n` kansiossa ollessa ajetaan komennot

```
./vars
./clean-all
./build-ca
```

Huomaa, että ennen `./vars` -komentoa on piste sekä yksi välilyönti, jotka ilmaisevat, että käytetään nykyistä kansiota, missä ollaan.

Viimeisellä `./build-ca` -komennolla luodaan palvelimelle Certificate Authority (CA). Näytölle ilmestyy aiemmin `vars`-tiedostoon määritetyt parametrit, ja ne voi kuitata painamalla enter-näppäintä.

Seuraavaksi luodaan palvelimelle oma avain komennolla

```
./build-key-server palvelin
```

Huomaa, että "palvelin"-parametri on sama kuin aiemmin muokatun vars-tiedoston parametri KEY\_NAME. Komennon annettuasi tulee samankaltaiset tiedot kuin ./build-ca -komennon jälkeenkin ja tässäkin tapauksessa ne voi kuitata enter-näppäintä painamalla. Näiden jälkeen tulee vielä kaksi ylimääräistä kyselyä, jotka voi jättää tyhjiksi. Seuraavaksi skripti kysyy, haluaako allekirjoittaa avaimen, johon vastataan kaksi kertaa myöntävästi. Tässä kohtaa siis aiemmin luotu CA-sertifikaatti allekirjoittaa digitaalisesti palvelimen avaimen. Onnistuneen allekirjoituksen jälkeen pitäisi tulla seuraavanlainen tuloste.

```
Write out database with 1 new entries
Data Base Updated
```

### 3.4 Palvelimen konfiguraatiot

Palvelimelta täytyy konfiguroida varsin montaa asiaa, jotta saadaan toimiva VPN-ympäristö luotua. Aloitetaan OpenVPN:n konfiguraatiosta. Avaimien teon aikana muokattiin OpenVPN:n server.conf -tiedostoa ja jatketaan sen muokkaamista hiukan. server.conf -tiedostohan sijaitsee /etc/openvpn/ kansiossa. Avataan tiedosto komennolla

```
nano /etc/openvpn/server.conf
```

Tiedostossa on paljon rivejä, jotka alkavat #-merkillä. Ne ovat kommenttirivejä ja toimivat ohjeistuksena. Puolipisteellä alkavat rivit ovat komentoja, jotka eivät ole käytössä eikä niitä huomioida OpenVPN-palvelimen ollessa päällä.

Etsitään ja poistetaan puolipiste seuraavasta parametrusta, jolloin OpenVPN-palvelin välittää asiakkaiden web-liikenteen oikein.

```
;push "redirect-gateway def1 bypass-dhcp"
```

Seuraavaksi muokataan palvelin välittämään asiakaslaitteille OpenDNS:n DNS-palvelinosoitteet. Poistetaan puolipisteet seuraavilta riveiltä

```
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"
```

Seuraavaksi rajoitetaan OpenVPN käyttämään käyttäjätunnusta *nobody* ja ryhmää *nogroup*. Oletuksena OpenVPN on päällä root-käyttäjänä. Etsitään ja poistetaan puolipisteet seuraavista riveistä. Tämä asetus koskee vain Linuxia, BSD:tä ja Unixin kaltaisia käyttöjärjestelmiä.

```
;user nobody
;group nogroup
```

Seuraavaksi konfiguroidaan pakettien ohjaus sekä palvelimen palomuuriasetukset. Pakettien ohjaus otetaan käyttöön sysctl-tiedostoa muokkaamalla, jolloin asiakaslaitteiden paketit menevät myös Internetiin eivätkä pysähdy palvelimelle. Pakettien ohjaus saadaan päälle seuraavalla komennolla.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Edellinen komento ei tee asetuksesta pysyvää, joten muokataan itse sysctl-tiedostoa. Avaa `/etc/sysctl.conf` ja poista kommenttimerkki seuraavalta riviltä

```
#net.ipv4.ip_forward=1
```

Muita asetuksia kyseiseen tiedostoon ei tarvitse tehdä.

Seuraavaksi konfiguroidaan Ubuntu 14.04:ssä valmiiksi olevan ufw-palomuurin (Uncomplicated Firewall) kuntoon. Ufw hallinnoi iptables-työkalua ja helpottaa palomuurisääntöjen tekemistä. Annetaan aluksi ufw:lle kaksi komentoa, joilla sallitaan SSH-yhteydet ja säädetään ufw sallimaan OpenVPN:n käyttämä UDP-portti 1194.

```
ufw allow ssh
ufw allow 1194/udp
```

Seuraavaksi muokataan ufw sallimaan pakettien välitys muokkaamalla ufw:n konfiguraatiotiedostoa.

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

Tiedostosta pitää muuttaa seuraava kohta siten, että "DROP"-tilalla lukee "ACCEPT".



```
DEFAULT_FORWARD_POLICY="DROP"
```

Enempää muutoksia kyseiseen tiedostoon ei tarvitse tehdä. Seuraavaksi lisätään muutama sääntö koskien NAT:ia. Avataan toinen konfiguraatitiedosto.

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

Lisää seuraavat säännöt tiedostoon ensimmäisen kommenttiosuuden jälkeen.

```
# OpenVPN
# NAT säännöt
*nat
:POSTROUTING ACCEPT [0:0]
# Liikenteen salliminen asiakalta verkkokortille
-A POSTROUTING -s 10.8.0.0/8 -o eth0 -j MASQUERADE
COMMIT
# Loppu
```

Näiden jälkeen ufw on valmis käyttöönotettavaksi. ufw otetaan käyttöön antamalla komento.

```
ufw enable
```

Vastaa myöntävästi näytölle tulevaan kysymykseen, joka on lähinnä vain varoitus, että nykyiset SSH-yhteydet saattavat katketa. ufw:n toimitilanteen voi tarkistaa komennolla.

```
ufw status
```

### 3.5 Asiakaslaitteiden sertifikaattien ja avaimien luonti

Seuraavaksi luodaan yhdistäville asiakaslaitteille omat sertifikaatit ja avaimet aiemmin luodun CA:n avulla. Seuraava vaihe pitää tehdä joka laitteelle erikseen. Tässä opinnäytetyössä käytän esimerkin vuoksi nimeä *client*-avaimille, jotka seuraavaksi tehdään. Avaimen nimi voisi hyvin olla esimerkiksi myös *kannettava* tai *puhelin*.

Avaimen tekoon tarvittava tiedosto löytyy samasta kansioista kuin palvelimen tekoinkin eli `/etc/openvpn/easy-rsa`. Kansiossa ollessa annetaan seuraava komento, jolloin avaimen luonti lähtee käyntiin.

```
./build-key client
```

Näytölle tulevat syötteet voi kuitata enter-näppäimellä pois ja kysymyksiin täytyy jälleen vastata myöntävästi. Nyt on onnistuneesti luotu tarvittavat sertifikaatit ja avaimet palvelimelle sekä yhdelle asiakaslaitteelle. Vielä tarvitsee kopioida esimerkki OpenVPN-profiilin pohjaksi. Esimerkkiprofiili kopioidaan seuraavalla komennolla.

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/easy-rsa/keys/client.ovpn
```

Samalla kopioinnin aikana tiedostopäätte muutettiin OpenVPN-profiilien mukaisesti `ovpn`-päätteeksi.

Keys-kansiossa pitäisi olla nyt seuraavat kolme tarvittavaa tiedostoa.

```
client.crt  
client.key  
client.ovpn
```

Lisäksi `/etc/openvpn/` kansiossa pitäisi olla tiedosto.

```
ca.crt
```

Kyseisestä neljästä tiedostosta `ca.crt`:ä ja `client.ovpn`:ää ovat tarpeellisia jokaisen eri laitteen kohdalla. Nämä neljä tiedostoa pitää siirtää asiakaslaitteelle eli tässä opinnäytetyössä siirsin itse tiedostot pöytäkoneelle, jossa on Windows-käyttöjärjestelmä. Huomioithan tehdä siirron käyttäen turvallista tiedoston siirtomenetelmää, kuten SCP (Secure Copy) tai SFTP (SSH File Transfer Protocol). Käytin tässä työssä Windows-koneelle asennettua WinSCP-sovellusta tiedostojen siirtoon. Versionumero oli 5.7. WinSCP on avoimeen lähdekoodiin perustuva ilmainen SFTP-, FTP-, WebDAV- ja SCP-yhteysohjelmisto Windows-käyttöjärjestelmälle.

### 3.6 Yhtenäisen OpenVPN-profiilitiedoston luonti

Tässä vaiheessa äskeisessä osiossa luodut neljä tiedostoa pitäisi olla kopioituna toiselle koneelle. Seuraavaksi muokataan OpenVPN:n esimerkkiprofiilitiedostoa *client.ovpn* tarpeisiimme sopivaksi. Tästä tiedostosta on hyvä ottaa kopio, jotta alkuperäistä voi käyttää jatkossa toisten profiilien luomiseen. Nimetään kopioitu tiedosto uudelleen *tietokone.ovpn* ja muokataan sitä.

Avataan tiedosto millä tahansa tekstieditorilla ja etsitään seuraava kohta

```
remote my-server-1 1194
```

Muokkaa *my-server-1* tilalle palvelin IP-osoite tai tämän opinnäytetyön tapauksessa käytin osoitetta *oppiari.noip.me*.

Mikäli tuleva asiakaslaite on muu kuin Windows-laite, niin poista kommenttimerkinnet seuraavilta riveiltä.

```
;user nobody  
;group nogroup
```

Seuraavaksi lisätään kommenttimerkit seuraaville riveille, jotta OpenVPN ei yritä käyttää kyseisiä sertifikaatteja ja avaimia yhdistämisvaiheessa.

```
ca ca.crt  
cert client.crt  
key client.key
```

Seuraavaksi yhdistetään sertifikaatit ja avaimet samaan *tietokone.ovpn*-tiedostoon. Avataan tiedostot *ca.crt*, *client.crt* ja *client.key* ja kopioidaan niiden sisältö *tietokone.ovpn*-tiedoston loppuun XML-syntaksin tapaan seuraavanlaisesti

```
<ca>  
(ca.crt-tiedoston sisältö tähän)  
</ca>  
<cert>
```

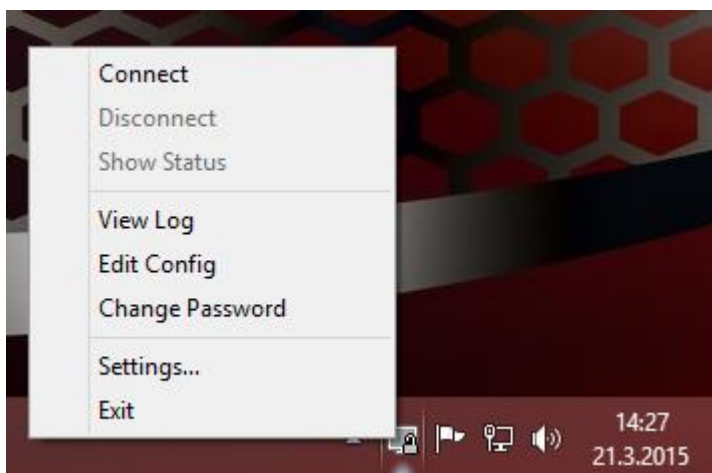
```
(client.crt-tiedoston sisältö tähän)
</cert>
<key>
(client.key-tiedoston sisältö tähän)
</key>
```

*Client.crt*-tiedostossa on aika paljon turhaa tekstiä, mutta siitä ei ole haittaa vaan tiedoston sisällön voi huoletta kopioida kokonaisuudessa.

Nyt yhtenäinen OpenVPN-profiilitiedosto on valmis ja sen voi siirtää haluamalleen asiakslaitteelle. Tässä esimerkissä tehty tiedosto oli tehty Windows-pöytäkonetta varten, joten siirretään *tietokone.ovpn*-tiedosto OpenVPN:n asetuskansioon.

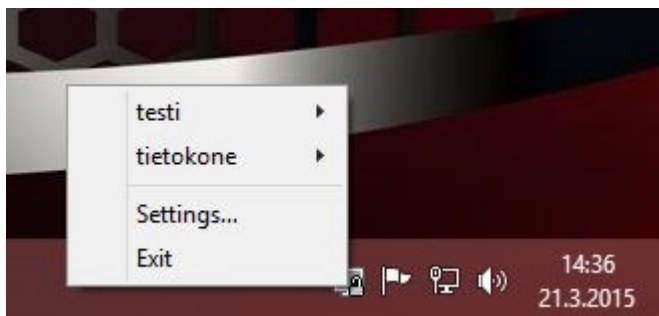
```
C:\Program Files\OpenVPN\config
```

OpenVPN havaitsee tiedoston automaattisesti ja OpenVPN GUI:n valikko muuttuu automaattisesti seuraavanlaiseksi.



Kuva 12. OpenVPN on havainnut profiilitiedoston kansiossaan.

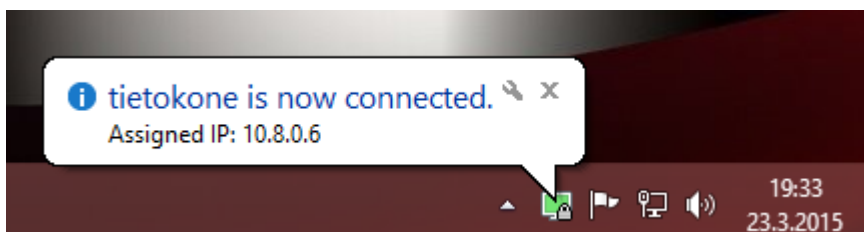
Mikäli tietokoneella on useita OpenVPN-profiilitiedostoja, niin tällöin valikkorakenne on hiukan erilainen.



Kuva 13. Valikkorakenne, kun koneella on useampi profiilitiedosto.

### 3.7 Yhteyden muodostaminen ja tarkistaminen Windows-koneella

Nyt kun profiilitiedosto on oikeassa paikassa, voidaan yhdistää palvelimeen. Yhdistäminen tapahtuu klikkaamalla oikealla hiirennäppäimellä OpenVPN GUI:n kuvaketta Windowsin ilmoitusalueella ja valitsemalla suoraan "Connect" tai valitsemalla ensin oikea yhteysprofiili ja sen alavalikosta "Connect". Näytölle ilmestyy yhdistämisen ajaksi ikkuna, jossa näkyvät yhdistämisen eri vaiheet.



Kuva 14. Onnistunut yhteyden muodostus.

Mikäli yhteys muodostuu onnistuneesti, tulee näyttöön näkyviin edellisen kuvan kaltainen ilmoitus. Ilmoituksesta näkyy, että yhdistävälle koneelle on annettu valitsemamme IP-avaruus. OpenVPN kuvakkeen vihreä väri kertoo myös yhteyden olevan päällä.

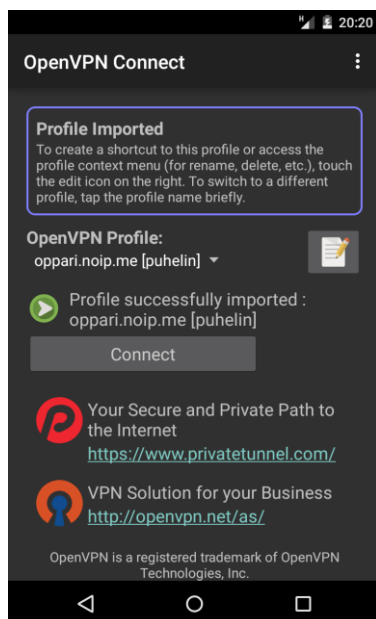
Seuraavaksi testataan, että yhteys varmasti toimii ja että yhteys käyttää OpenDNS:n DNS-palvelimia. Tähän tarkoitukseen käytämme [www.dnsleaktest.com](http://www.dnsleaktest.com)-sivuston testiä. Sivuston etusivulta näkee heti, että yhteys käyttää palvelimen IP-osoitetta. Painamalla "Extended Test" -nappia, sivusto ajaa kyselyitä selvittääkseen, mitä DNS-palvelimia käytetään. Hetken kuluttua kyselyt ovat valmiina ja sivusto näyttää tuloksen. Tuloksena pitäisi olla OpenDNS:n palvelin. Minulle tuli testauksen aikana palvelin Tanskasta.

### 3.8 OpenVPN Connect

OpenVPN Connect on sovellus Android-puhelimille, jolla voidaan yhdistää puhelin helposti OpenVPN-palvelimeen ja täten saada VPN-yhteys myös puhelimella. OpenVPN Connect on OpenVPN Technologiesin tekemä ohjelma. OpenVPN Connect on ladattavissa Googlen Play-kaupasta ilmaiseksi. Tämän opinnäytetyön aikana ohjelmiston versionumero oli 1.1.16 ja päivitetty 9. maaliskuuta 2015. Käytössä oli Nexus 4 -älypuhelin sekä Android-käyttöjärjestelmän versionumero 5.0.1.

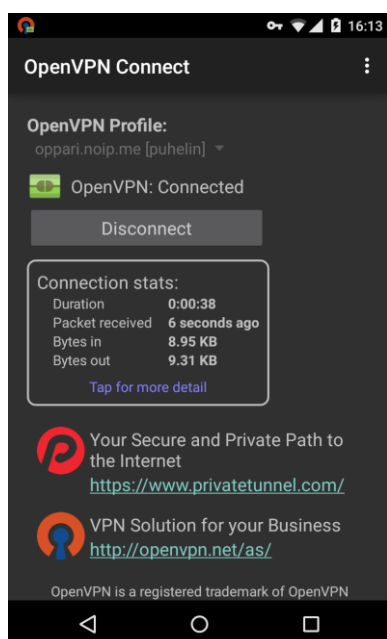
Älypuhelimelle tarvitsee luoda oma OpenVPN-yhteysprofiili, mikäli käytössä on myös muita laitteita. Yhteysprofiilin luonti onnistuu samaan tapaan kuin esimerkiksi pöytäkooneelle aiemmin. Yhteysprofiilin voi nimetä esimerkiksi nimellä *puhelin*. Kun yhteysprofiili on luotu, tarvitsee se vain siirtää enää älypuhelimeen.

Kun yhteysprofiili on siirretty puhelimeen, voidaan avata OpenVPN Connect -sovellus. Ensi näkymä ei ole kummoinen ja näytölle oleva teksti kehottaakin lisäämään yhteysprofiiliin. Tämä tehdään painamalla oikeasta yläkulmasta löytyviä kolmea pistettä, jolloin aukeaa pudotusvalikko. Pudotusvalikosta valitaan "Import" ja sen jälkeen aukeavasta valikosta valitaan "Import Profile from SD card". Tämän jälkeen navigoidaan kansioon, jonne yhteysprofiili on tallennettu. Valitaan oikea tiedosto, jonka jälkeen painetaan "SELECT"-nappia. Tämän jälkeen yhteysprofiili on ladattu, ja se näkyy valittuna näytöllä. Yhteysprofiilin vieressä oleva lehtiön kuvaa klikkaamalla, voidaan tehdä pikakuvake Androidin aloitusruutuun tai muokata yhteyden nimeä kuvaavammaksi.



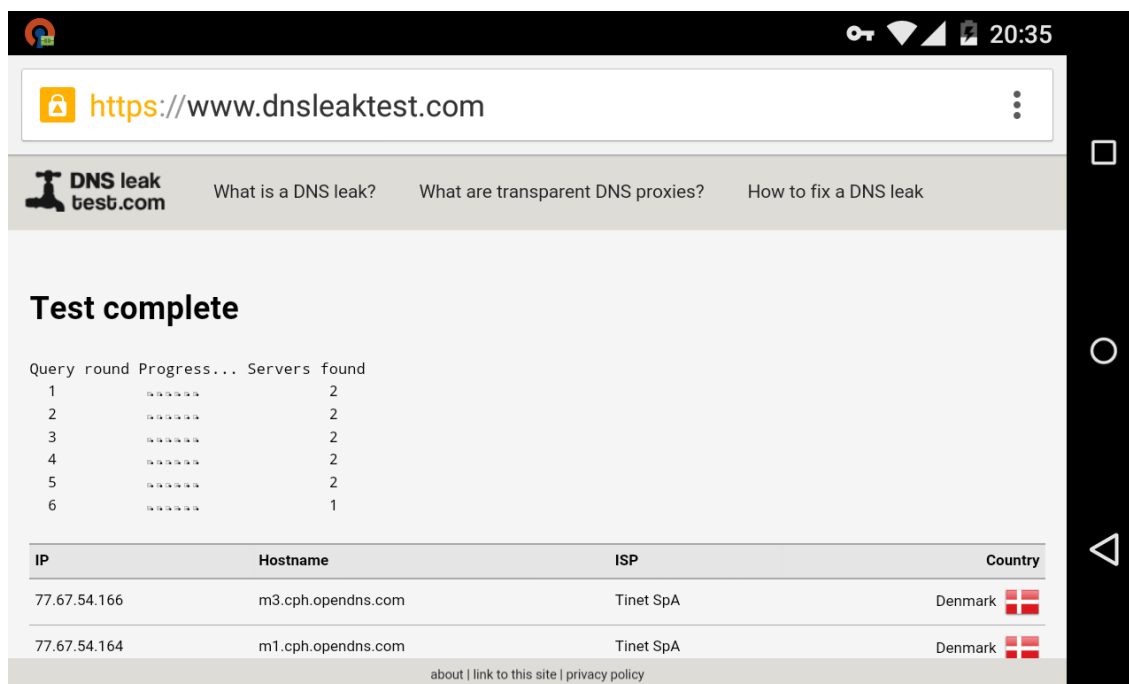
Kuva 15. OpenVPN Connect ja ladattu yhteysprofiili.

Connect-nappia painamalla sovellus yhdistää OpenVPN-palvelimeen. Tämän jälkeen näytölle ilmestyy teksti, joka ilmaisee yhteyden palvelimeen. Näytöltä löytyy myös tietolaatikko, josta näkee, kuinka kauan yhteys on ollut auki, milloin viimeisin paketti on saapunut ja paljonko dataa on liikkunut sisään ja ulos.



Kuva 16. OpenVPN Connect -yhteydessä OpenVPN-palvelimeen.

Ajetaan jälleen varmistukseksi dnsleaktest.com-sivuston testi ja todetaan, että kaikki toimii niin kuin pitäisi.



Kuva 17. dnsleaktest.com testitulokset.

Kuten kuvasta näemme yhteys, käyttää Tanskassa sijaitsevia OpenDNS-palvelun DNS-palvelimia.

### 3.9 Huomioita

OpenVPN GUI ei käynnisty Windowsin yhteydessä automaattisesti, vaan se on aina erikseen käynnistettävä. Logien tallentaminen tietokoneelle ei onnistu, mikäli ohjelmistoa ei suoriteta käyttöjärjestelmävalvojan oikeuksin.

Sertifikaatti- ja avaintiedostojen kopioinnissa palvelimelta toiselle koneelle saattaa ilmetä ongelmia luku- ja kirjoitusoikeuksien kanssa. Tästä selviää käyttämällä CHMOD-komentoa palvelimen puolella. Kunhan muistaa joko muuttaa oikeudet alkuperäisiksi tai poistaa tiedoston kokonaan, mikäli sitä ei enää tarvitse.



Mikäli palvelimeen ei saa yhteyttä, vaikka kaikki asetukset vaikuttaisivat olevan oikein, kannattaa tarkastaa omasta reitittimestä, että sinne on tehty porttiohjaus palvelimen suuntaan UDP-porttiin 1194.

Asiakaslaitteiden sertifikaattien poistaminen onnistuu palvelimella `easy-rsa`-kansiossa komennolla

```
. ./vars  
./revoke-full client
```

Tämä poistaa allekirjoituksen kyseiseltä *client*-sertifikaatilta eikä tällöin voi yhdistää palvelimelle enää.

## 4 Yhteenveto

VPN-pohjaiset ratkaisut ovat hyvä ja halpa ratkaisu yrityksen etätyöntekijöiden turvalliseen yhdistämiseen yrityksen verkkoon. Dedikoidut yhteyslinjat ovat kalliita ja hankalia verrattuna VPN-yhteyteen. IPSec on suosittu protokolla yritysmaailmassa sen laajan laitetuen takia. MPLS-protokolla on yleistymässä kovaa tahtia. MPLS-protokollan etuina ovat sen hallittavuus ja nopeus.

Tässä opinnäytetyössä tehty konfiguraatio suojaa yhteyten ja sijainnin hyökkääjiä vastaan. Matkoilla voi käyttää avoimia WLAN-verkkoja turvallisemmin yhdistämällä ensin tietokoneeseen taikka puhelimeen luodulla OpenVPN-yhteydellä. Tällöin tieto kulkee salattuna, vaikka WLAN-verkko olisi muuten suojaamaton.

Jatkokehitettävää tähän opinnäytetyöhön jäi esimerkiksi kaksivaiheisen autentikoinnin luomiseen hyödyntäen älykorttia. IPv6-tuen lisääminen olisi yksi mahdollinen lisättävä ominaisuus OpenVPN-palvelimeen. OpenVPN-versio 2.3 ja uudemmat ovat IPv6-yhteensopivia. Käyttöönottamalla tls-auth-ominaisuuden saisi lisäturvaa Denial-of-Service-hyökkäyksiä vastaan.

OpenVPN on helppo ja halpa ratkaisu VPN-yhteyden luomiseen. Sen käyttö ei maksa mitään ja tarvittavat palvelinohjelmistot ovat myös ilmaisia. Ainoa kustannus on laitekustannus.

## Lähteet

Casad, Joe. 2009. Sams Teach Yourself TCP/IP. Yhdysvallat: Pearson Education Inc.

Comer, Douglas E. 2009. Computer Networks and Internets. Yhdysvallat: Pearson Education Inc.

Cisco.com: Cisco IOS Dial Technologies Configuration Guide, Release 12.2. Verkkodokumentti. [[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/dial/configuration/guide/fdial\\_c.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/dial/configuration/guide/fdial_c.html)]. Luettu 29.3.2015.

etutorials.org: IPSec Overview. Verkkodokumentti. [<http://etutorials.org/Networking/MPLS+VPN+security/Part+III+Practical+Guidelines+to+MPLS+VPN+Security/Chapter+6.+How+IPsec+Complements+MPLS/IPsec+Overview/>]. Luettu 29.3.2015.

Frankel, S., Hoffman, P., Orebaugh, A., Park, R. 2008. NIST Special Publication 800-113: Guide to SSL VPNs. Verkkodokumentti. [<http://csrc.nist.gov/publications/nist-pubs/800-113/SP800-113.pdf>]. Luettu 27.1.2015.

Gupta, Meeta. 2002. Building a Virtual Private Network. Yhdysvallat: Thomson Learning.

Hakala & Vainio. 2005. Tietoverkon rakentaminen. Porvoo: WS Bookwell.

Juniper.net: Components of Filter-Based Tunneling Across IPv4 Networks. Verkkodokumentti. [[http://www.juniper.net/techpubs/en\\_US/junos13.2/topics/concept/firewall-filter-tunneling-ipv4-gre-components.html](http://www.juniper.net/techpubs/en_US/junos13.2/topics/concept/firewall-filter-tunneling-ipv4-gre-components.html)]. Luettu 29.3.2015.

Just Keijser, Jan. 2011. OpenVPN 2 Cookbook. Packt Publishing: Yhdistynyt kuningaskunta.

Kaario, Kimmo. 2002. TCP/IP-verkot. Porvoo: WS Bookwell

Layer 2 Forwarding (L2F). Verkkodokumentti. [<http://www.thenetworkencyclopedia.com/entry/layer-2-forwarding-l2f/>]. Luettu 9.2.2015.

Nayak & Rao. 2014. The InfoSec Handbook. Apress. E-kirja.

OpenVPN: About. Verkkodokumentti. [<http://openvpn.net/index.php/about-menu/>]. Luettu 12.2.2015.

OpenVPN: HOWTO. Verkkodokumentti [<http://openvpn.net/index.php/open-source/documentation/howto.html>]. Luettu 13.3.2015

OpenVPN: Overview. Verkkodokumentti. [<http://openvpn.net/index.php/open-source/245-community-open-source-software-overview.html>]. Luettu 12.2.2015.

OpenVPN: What is OpenVPN. Verkkodokumentti [<http://openvpn.net/index.php/open-source/333-what-is-openvpn.html>]. Luettu 12.2.2015.

Rouse, Margaret. 2009. SSL VPN (Secure Sockets Layer Virtual Private Network). Verkkodokumentti. [<http://searchsecurity.techtarget.com/definition/SSL-VPN>]. Luettu 9.2.2015.

Sturt, Robert. 2014. Multiprotocol Label Switching (MPLS) Verkkodokumentti. [<http://searchenterprisewan.techtarget.com/definition/Multiprotocol-Label-Switching>]. Luettu 26.3.2015.

VPN Consortium. 2008. VPN Technologies: Definitions and Requirements. Verkkodokumentti. [<http://www.vpnc.org/vpn-technologies.html>]. Luettu 9.2.2015.

## Yhteysprofiilitiedosto esimerkki

```
#####
```

```
# Sample client-side OpenVPN 2.0 config file #
```

```
# for connecting to multi-client server.  #
```

```
#                                     #
```

```
# This configuration can be used by multiple #
```

```
# clients, however each client should have #
```

```
# its own cert and key files.          #
```

```
#                                     #
```

```
# On Windows, you might want to rename this #
```

```
# file so it has a .ovpn extension      #
```

```
#####
```

```
# Specify that we are a client and that we
```

```
# will be pulling certain config file directives
```

```
# from the server.
```

```
client
```

```
# Use the same setting as you are using on
```

```
# the server.
```

```
# On most systems, the VPN will not function
```

```
# unless you partially or fully disable
```

```
# the firewall for the TUN/TAP interface.
```

```
;dev tap
```

```
dev tun
```

```
# Are we connecting to a TCP or
```

```
# UDP server? Use the same setting as
```

```
# on the server.
```

```
;proto tcp
```

```
proto udp
```

# The hostname/IP and port of the server.

# You can have multiple remote entries

# to load balance between the servers.

remote oppari.noip.me 1194

# Keep trying indefinitely to resolve the

# host name of the OpenVPN server. Very useful

# on machines which are not permanently connected

# to the internet such as laptops.

resolv-retry infinite

# Most clients don't need to bind to

# a specific local port number.

nobind

# Downgrade privileges after initialization (non-Windows only)

;user nobody

;group nogroup

# Try to preserve some state across restarts.

persist-key

persist-tun

# 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.

# Verify server certificate by checking

# that the certificate has the nsCertType

# field set to "server". This is an

# important precaution to protect against

# a potential attack discussed here:

```
# http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server". The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

<ca>
-----BEGIN CERTIFICATE-----
MIIFEjCCA/qgAwIBAgIJAMStyDkxvjOOMA0GCSqG-
S1b3DQEBCwUAMIG2MQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExFTATBgNVBACjDFNhbKZyYW5jaXNjb-
zEVMBMG
A1UEChMMRm9ydC1GdW5zdG9uMR0wGwYDVQQLEXRNeU9yZ2FuaX-
phdGlubmFsVW5p
dDEYMBYGA1UEAx-
MPRm9ydC1GdW5zdG9uIENBMRAwDgYDVQQPEwdFYXN5UINBMSEw
HwYJKoZIhvcNAQkBFhJtZUBteWhvc3QubXlkb21haW4wHhcNMTUwMzIzMTcyODU4
WhcNMjUwMzIzMTcyODU4WjCBtjELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAk-
NBMRUw
EwYDVQQHEwxTYW5GcmFuY2lzY28xFTATBgNVBAoTDEZvcnQtRnVuc3RvbGEd-
MBsG
A1UECXMUTXIPcmdhbml6YXRpb25hbFVuaXQxGDAwBgNVBAMTD0ZvcnQtRn-
Vuc3Rv
biBDQTEQMA4GA1UEKRMHRWFzeVJTQTEhMB8GCSqG-
S1b3DQEJARYSbWVAbXlob3N0
```

Lm15ZG9tYWluMIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAo4fbUgK0  
u/QIS7MYbQ/6MAz+1qSAvE0DvFSL5eXaE814B00hulNnnhCxchaBoTt1293eYX+9  
xnz9O6IHEAHvW30GJEuuKAUBlrWxXAgN/urohW1YmgJw08dB2NAoVDiJskjSfZPc  
o1fF5cfXuBYnd7b2tUQKFWPk99W/kmxeFZ+Zk4g69rDxHkXlXLIqMBDUGjNV53JOI  
m+ID5MuNj3PUn1nL6kPFuhiPYK0ftdfqPDIWySwyiJXd/YzoEMLpsQLCxoUInfH1  
r2WYQAQoQpbmDoZ+ile1D2g25kYnH4SWkfchndZnkx9O0ub6olvel+DSETqbLDgQo  
CRfAiYwegVLEOwiDAQABo4IBHzCCARswHQYDVR0OBBYEF0HKNjDFucRS8dlk-  
lvIE  
QHWAln4BMIHrBgNVHSMEgeMwgeCAFOHKNjDFucRS8dlk-  
lvIEQHWAln4BoYG8pIG5  
MIG2MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFTATBgNVBAc-  
TDFNhbKZyYW5j  
aXNjb-  
zEVMBMGA1UEChMMRm9ydC1GdW5zdG9uMR0wGwYDVQQLEXRNuU9yZ2Fu-  
aXph  
dGlvmFsVW5pdDEYMBYGA1UEAx-  
MPRm9ydC1GdW5zdG9uIENBMRAwDgYDVQQpEwdF  
YXN5UINBMSEwHwYJKoZIhvcNAQkBFhJtZUBteWhvc3QubXlk21haW6CCQDErcg5  
Mb4zjjAMBgNVHRMEBTADAQH/MA0GCSqGSIB3DQEBCwUAA4IBAQAAXrw-  
dAVEEe5Alu  
G7QxXNo3uKOyRUCzWfcDrxUtttdtCyUr48NXZrmPo0s8eYoWiPM0FnglNjt7sZZ4  
4EiUFwF8fVcQq0sJfYuaGP9Nm82yLyUlu6uel0d+yQhxvad0ViRHxVZJTW3m3bR2  
zGGkE8kz0SuOLD5/tX6Suqh31XfxNhnR0sPWI/6DjeKAv5pfCWtHv9rK8QIhL8Ur  
OOxW8CP5gN7nGgvgfXBtKMbZtNxmxaZeNSStha2wRSbznzgzEj+q8Ju0y5qHS3  
8C12S0BNLDObAtIFXzOov1JfUWajLzX5giPkd+dyP3oqQK5Fml2MtFuH0YPT+gFZ  
+onR1iG3  
-----END CERTIFICATE-----  
</ca>  
<cert>  
-----BEGIN CERTIFICATE-----  
MIIFUDCCBDigAwIBAgIBAzANBgkqh-  
kiG9w0BAQsFADCBtjELMAkGA1UEBhMCVVMx  
CzAJBgNVBAgTAkNBMRUwEwYDVQQHEwxTYW5Gcm-  
FuY2lzY28xFTATBgNVBAoTDEZv



cnQtRnVuc3RvbjEdMBsGA1UECXMUTXIPcmdhbml6YXRpb25hbFVuaXQxGDAW-  
BgNV  
BAMTD0ZvcnQtRnVuc3RvbiBDQTEQMA4GA1UEKRM-  
HRWFzeVJTQTEhMB8GCSqGSib3  
DQEJARYSbWVAbXlob3N0Lm15ZG9tYWluMB4XDTE1MDMyMzE3MzE1NFoXDTI1M  
DMy  
MDE3MzE1NFowga4xCzAJBgNVBAY-  
TAIVTMQswCQYDVQIEwJDQTEVMBMGA1UEBxMM  
U2FuRnJhbmNpc2NvMRUwEwYDVQQKEwxB3J0LUZ1bnN0b24xHT-  
AbBgNVBAsTFE15  
T3JnYW5pemF0aW9uYWxvbmI0MRAwDgYDVQQDEwdwdWhlbGluM-  
RAwDgYDVQQpEwdF  
YXN5UINBMSEwHwYJKoZlhcNAQkBFhJtZUBteWhvc3QubXlk21haW4wggEiMA0G  
CSqGSib3DQEBAQUAA4IBDwAwggEKAoIBAQDZfdp42PfN9un-  
MxUDvam2hUf59P1gp  
8PywYEVraYDmsl6Eefwnmo38dOvTrPZlpUh3iq1ayTxobn+yn0ih+NDf5otMiEEv  
lbAnj1ZV84GEw/Wu1qJH/9Z7uJsnDQHIE7kxeYk5kUNH7wPyDujkxAp+EoS3zwS  
nqii5TIUPlDaq+JHO+NFaaaNjJK9vuZ/zlfqwlCoaxHUBwWGI1uAFMOSMDv+y3FL  
pk3WEclfhkb1rWgoSyFIDnsyqTbFstlY9mGHvQ0gyWOzUtzOm9kmg2OQu9Vld72t  
JsBaml/kaB+VJSArncv8grr7RgyQ3MfMqTytRC4vcKMhRB5l8un7qKcdAgMBAAGj  
ggFtMIIBaTAJBgNVHRMEAjAAMC0GCWCG-  
SAGG+EIBDQQgFh5FYXN5LVJTSBHZW5I  
cmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFKoUgqWMCDmvX-  
SEtnzAySR+1kl7c  
MIHrBgNVHSMEgeMwgeCAFOHKNjDFucRS8dlk-  
IvIEQHWAln4BoYG8pIG5MIG2MQsw  
CQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFTATBgNVBAC-  
TDFNhbKZyYW5jaXNjbzEV  
MBMGA1UEChMMRm9ydC1GdW5zdG9uMR0wGwYDVQQLEXRNeU9yZ2FuaX-  
phdGlvmFs  
VW5pdDEYMBYGA1UEAx-  
MPRm9ydC1GdW5zdG9uIENBMRAwDgYDVQQpEwdFYXN5UINB  
MSEwHwYJKoZlhcNAQkBFhJtZUBteWhvc3QubXlk21haW6CCQDErcg5Mb4zjjAT  
BgNVHSUEDDAKBggrBgEFBQcDAjALBgNVHQ8EBAMCB4AwDQYJKoZlhc-  
NAQELBQAD

ggEBAGUN2/dtcUu7m/plctAoL57efjel7KA49LV4NCU/nZqUHWYJh4oNJt21bEHg  
58Dk6/J3R3veZE2LqWS9bPO3ISCHagt57xcXVohhJh3ecNb83/VArs2GoosaDFgk  
G5h0j8UgMF41UjyeYQxMF49djkhja4HKVTRiT9NNLQcX8A5IzwHtMhAHQH2CTtx0  
sreUOK7ImGqw5WjgmHcLs6pn+VRZb4TukaUF7xyd5vLJmEaCyhnc+XYOyx4wE3H  
+7MQkoQT7F2gX33SkPuSRj+Zq+3zjyIRE5z6iQLOr3Vk3AmUSfcrCjOZCC6OmUYb  
8uruyXC5hJwnVC4XHdt51aJ3aCU=

-----END CERTIFICATE-----

</cert>

<key>

-----BEGIN PRIVATE KEY-----

MIIEvglBADANBqkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQDZfdp42PfN9unM  
xUDvam2hUf59P1gp8PywYEVraYDmsl6Eefwnmo38dOvTrPZlpUh3iq1ayTxobn+y  
n0ih+NDf5otMiEEvibAnj1ZV84GEw/Wu1qJH/9Z7uJsnDQhIE7kxeYk5kUNH7wPy  
DuwjxAp+EoS3zwSnqii5TIUPIdAq+JHO+NFaaaNjJK9vuZ/zlfqwCoaxHUbWwG  
l1uAFMOSMDv+y3FLpk3WEclfhkb1rWgoSyFIDnsyqTbFstlY9mGHvQ0gyWOzUtzO  
m9kmg2OQu9Vld72tJsBaml/kaB+VJSArncv8grr7RgyQ3MfMqTytRC4vcKMhRB5l  
8un7qKcdAgMBAAECggEAUGWHdxitMcPOVWVtVVNAR1vp+R6LVqW-  
wovpTZW7cqWom  
pK37GiC1z9bgvhS32lqqrJXk0ySEYg5Gwh7DWKyDeeDdKWNMxWxN+7GutoMXI57U  
mNbakkbuYDmzknHud8ZitPk6Ur9x4YtnJ/mALP5WAU25BBTIPfTMXbrfsj9Vt/+j  
MvWxJuuLyWmYcDSswU/wCdGsqliNo/Rr+yx4Jgi7dyHyIsnxVv1H9JEViBuxm9Oau  
zSVIKiO+JZD0+f90AozN9IQ+NxTArRjLLcSFzXh+42rHDZvaqIhIMMin4drHNPIM  
lhNrv3yFWG1fPrbWpmp0loK6YwcMclBtPu47r9dVwQKBgQD3x4jBexUx3/Xyzs6  
O7ccHs0K0garqxxvafoFenU71vxG/7wZbsJp2UkIS9grWDjbczJvM24KpySwxRiw  
EYzCSzExyOhOBtL1d0zIPPUmZLuCNW5jYPVZ2411bOa3wJeXhp2NAIbOg29I5emm  
WuEn6urp+jIRC8AL1uvE8wTnOQKBgQDgtRNA+SsBeAyrHqxeEbEwGEbZr7c1ZimH  
sg6hZ99mAfp69LxlatTA5tc2mNEF5Xa1XyQgXzmY1ZTwZ0949I61GLi3nL7pvLca  
hb5goJjH+6ZEq0JZYoa5R1pCrRLySLxwyFed/M9+mhcO8oJ4Zh/31IPuXOtkOrP9  
F9CRv3Y7BQKBgQDqMfbYqXflcCgt1zHMANU6BwLWz1zutXTS+eAPfYeBX9pjYSR  
BXdMhMvWLLHNhj13bpKk+H9yljiTu3dyM6RPoLKG09Z+qYSL7o8HvW4ZM+znTYlg  
9SvyGsrByoTn+WIPFzWjKirSVvjAdk85pXxbNneDX7Ai3HBQwHtoVCq2QQKBgG+I  
URgZjsgG3zrcWa/DVIBJ7IWt1ODTWY+5yFtC5HaMStHWu1GyfPFWYsH9rdogYAB8  
PcE3oq4CbQ+6J48gy+iFYcH5MiVv/u5SLgFmFQ9GD+vX+onFQ2Gq0dIAcKQDiEzu  
k9aeEhuDvig0JKBACGQKZNRuGIRCQu4/sM122+dFAoGBAMO9te6brE3sD26YVtxo

m580Gln8EPLZn1bnowAZ8PmBHxhUV2N0KTke5zScp3Hi/RFa7PNOV2zE6RRO1MM

j

hNSXz9t/kyC5ByjHhRsybTxZOJTheiuTB3aDBOh92vyic1UnGjKoadPPtTtU1NVG

zAZfj09EE1RC3LSBCqbbYGh

-----END PRIVATE KEY-----

</key>