

OPINNÄYTETYÖ
VILLE-MATTI NIKKONEN 2010

TIETOTURVALLISET ETÄYHTEYDET IPSEC VPN-TEKNIIKAN AVULLA



Rovaniemen
ammattikorkeakoulu
University of Applied Sciences

TIETOJENKÄSITTELY

ROVANIEMEN AMMATTIKORKEAKOULU

LUONNONTIETEET

Tietojenkäsittelyn koulutusohjelma

Opinnäytetyö

TIETOTURVALLISET ETÄYHTEYDET IPSEC VPN- TEKNIIKAN AVULLA

Nikkonen Ville-Matti

2010

Rovaniemen ammattikorkeakoulu

Ohjaaja Martti Kemppainen

Hyväksytty _____ 2010 _____



Rovaniemen
ammattikorkeakoulu
University of Applied Sciences

Tekijä

Ville-Matti Nikkonen

Vuosi 2010

Toimeksiantaja
Työn nimi

RAMK
Tietoturvalliset etäyhteydet IPSec VPN-tekniikan
avulla

Sivu- ja liitemäärä 25 + 4

Opinnäytetyössä käydään lyhyesti läpi puhelinverkkojen kehitys nykyaikaisiksi pakettikytkentäisiksi viestintäverkoiksi.

Työssä tarkastellaan erilaisia Virtual Private Network ratkaisuja, keskittyen kuitenkin pääsääntöisesti Internetin kautta toteutettujen VPN ratkaisujen tarkasteluun ja niistä erityisesti Internet Protocol Security VPN-tekniikkaan. Tavoitteena on tarkastella etäyhteyksien muodostamista ja niiden tietoturvaa Internetiä hyödyntävissä yhteyksissä.

IPSec:in avulla toteutettujen yhteyksien toimintaa havainnollistetaan kolmen eri näkökulmista katsotun esimerkin avulla.

Lopuksi tarkastellaan tulevaisuuden näkymiä, viestintäverkkojen matkaa yhä enemmän langattomien ratkaisujen suuntaan ja loppukäyttäjän tärkeyttä järjestelmien lopullisen tietoturvan rakentamisessa.

Avainsana(t): VPN, IPSec

Commissioned by RAMK

Subject of thesis Secure VPN connections using IPSec VPN

Number of pages 25 + 4

The main purpose of this thesis was to look at Secure Virtual Private Network (VPN) connections which were using Internet Protocol Security (IPSec).

Also, included in this study was a brief description of the history and the development of the communication networks.

Virtual Private Network solutions were briefly explained and then the study was concentrated on VPN solutions that used the Internet, specifically solutions that used Internet Protocol Security as a means for achieving VPN. The security options for IPSec VPN were looked at including tunnelling and encryption. Also, three examples of systems were presented that were using IPSec for VPN connections.

In conclusion, the future of communication networks was examined and also the importance of end user actions in regard to system security.

Key words: VPN, IPSec

SISÄLLYSLUETTELO

1 JOHDANTO.....	1
2 TIETOLIIKENNEVERKOT.....	2
2.1 Puhelinverkot.....	2
2.2 Matkaviestinverkot.....	3
2.2.1 Ensimmäisen sukupolven matkapuhelinverkot (1G).....	3
2.2.2 Toisen sukupolven matkapuhelinverkot (2G).....	3
2.2.3 Parannellut toisen sukupolven matkapuhelinverkot (2,5G).....	4
2.2.4 Kolmannen sukupolven matkapuhelinverkot (3G).....	4
2.3 Muita yhteysmenetelmiä.....	5
2.4 IP-verkot.....	6
3 VIRTUAALISET YKSITYISVERKOT.....	8
3.1 VPN-yhteyden toiminta.....	8
3.2 Internet Protocol Security (IPSec).....	9
3.2.1 IPSec ja sen toiminta.....	9
3.2.2 Authentication Header (AH).....	10
3.2.3 Encapsulating Security Payload (ESP).....	10
3.2.4 Security Association (SA).....	11
3.2.5 Avaimenhallinta.....	11
3.3 Muita VPN-protokollia.....	12
3.3.1 Generic Routing Encapsulation (GRE).....	12
3.3.2 Point to point tunneling protocol (PPTP).....	12
3.3.3 Layer 2 tunneling protocol (L2TP).....	13
3.4 Datakuorman salaaminen.....	14
3.4.1 Salausmenetelmät.....	14
3.4.2 Salausalgoritmeja.....	14
4 VPN ESIMERKIT.....	16
4.1 IPSec VPN matkapuhelinverkon avulla (liite 1).....	16
4.1.1 Laitteisto.....	16
4.1.2 Käyttäjän tunnistaminen matkaviestinverkossa.....	17
4.1.3 VPN-yhteyden muodostaminen.....	17
4.2 IPSec VPN yrityksen kahden toimipaikan välillä (Liite 2).....	19
4.2.1 Laitteisto.....	19
4.2.2 VPN yhteys.....	19
4.3 VPN kotitoimiston ja työpaikan välillä (liite 3).....	20
4.3.1 Laitteisto.....	20
4.3.2 VPN-yhteys.....	20
5 JOHTOPÄÄTÖKSIÄ, POHDINTOJA JA TULEVAISUUDEN NÄKYMİÄ. .	21
LÄHTEET.....	24
LIITTEET.....	25

1 JOHDANTO

Sain idean opinnäytetyöhöni työskennellessäni eräässä pienessä itäsuomalaisessa IT-alan yrityksessä. Idea muokkautui monen mutkan kautta tietystä mobiilista Virtual Private Network ratkaisusta pienten ja keskisuurien yritysten tarpeisiin soveltuvien Internet Protocol Security protokollaperhettä käyttävien VPN-ratkaisujen tarkasteluun. Mobiilien laitteiden näkökulma on otettu opinnäytetyössäni voimakkaasti huomioon, sillä yhä enemmän mobiilien järjestelmien suuntaan kulkevassa verkottumisessa on entistä tärkeämpää hallita verkkoyhteyksien rakentamista ja suunnittelua erityisesti matkaviestinverkkoja hyödyntäen. Käyn nopeasti opinnäytetyössäni läpi puhelinverkkojen kehittymistä painottaakseni niiden kehittymistä langattomien järjestelmien suuntaan, pyrin esittelemään matkaviestinverkon eri yhteystekniikoita ja käymään myös yleisesti läpi erilaisia Virtual Private Network tekniikoita, sekä niiden toteutuksia. Keskityn kuitenkin Virtual Private Network tekniikoista erityisesti Internet Protocol Security protokollanippuun perustuviin ratkaisuihin ja esittelen lopuksi muutamien ratkaisujen käytännön toteutuksia esimerkkien avulla.

2 TIETOLIIKENNEVERKOT

2.1 Puhelinverkot

Suomen puhelinverkko, sekä kiinteä että matkaviestinverkko, koostuu pääasiassa kolmen valmistajan, Nokian, Eriksonin ja Siemensin laitteista, näiden eri järjestelmien yhteistoiminta verkossa on mahdollista yhteysrajapintojen kansainvälisen yhteensopivuus standardoinnin ansiosta. Puhelinverkkoa käytetään nykypäivänä laajasti datayhteyksien luomiseen ja tulevaisuuden suuntana onkin langattomien, etenkin matkaviestinverkkojen kasvava käyttö datayhteyksien siirtotienä. Muodostettiinpa datayhteys miten tahansa, sitä käytetään useimmiten Internetin selaamiseen tai etäyhteyksien luomiseen Internetin välityksellä. (Penttinen 2006a, 19.)

Yleistä puhelinverkkoa (lankapuhelinverkko) käytetään nykyään lähes yksinomaan datayhteyksiin, sopivampi nimi verkolle lieneekin ”televerkko”, erittäin yksinkertaistettuna verkko koostuu digitaalisista puhelinkeskuksista jotka on sitten yhdistetty toisiinsa. (Penttinen 2006a, 17.)

Suuri osa suomen kotitalouksien Internetyhteyksistä on nykyään toteutettu erilaisilla DSL eli Digital Subscriber Line tekniikoilla, yleensä eri DSL tekniikoihin viitataan lyhenteellä xDSL, yleisin xDSL tekniikka on ADSL eli Asynchronous Digital Subscriber Line, muita xDSL tekniikoita ovat HDSL, SDSL, VDSL ja IDSL. (Penttinen 2006a, 40.)

ISDN eli digitaalinen monipalveluverkko on suunniteltu alueelliseksi järjestelmiksi, Suomessa on käytössä Euro-ISDN. ISDN oli kehitysaskel puhelinverkkojen muututtua analogisista digitaalisiin järjestelmiin, se tarjoaa myös analogisia järjestelmiä laajempia palveluita käyttäjilleen. (Penttinen 2006a, 17, 24–25.)

VPN-yhteyksiä voidaan toteuttaa millä tahansa edellä mainitulla yhteystekniikalla.

2.2 Matkaviestinverkot

2.2.1 Ensimmäisen sukupolven matkapuhelinverkot (1G)

Tärkein ensimmäisen sukupolven matkapuhelinjärjestelmistä oli NMT (Nordisk Mobiltelefon). Järjestelmä koostui tukiasemista, NMT-keskuksista ja puhelinlaitteista, tämä analoginen järjestelmä mahdollisti lähinnä puheen siirtämisen radioverkkoa pitkin ja se poistui Suomessa käytöstä 2000-luvun taitteessa. Muita ensimmäisen sukupolven järjestelmiä olivat muun muassa kaukohakujärjestelmä KAUHA ja Euroopan laajuinen kaukohakujärjestelmä ERMES, myös nämä järjestelmät lakkautettiin samoihin aikoihin NMT-järjestelmän kanssa. Ensimmäisen sukupolven järjestelmien lakkauttamisella niiden käyttämät radioverkon taajuualueet saatiin vapautettua uusien järjestelmien käyttöön. (Penttinen 2006b, 102–103.)

2.2.2 Toisen sukupolven matkapuhelinverkot (2G)

Toisen sukupolven tunnetuin matkapuhelinjärjestelmä GSM (Global System for Mobile Communication) on täysin digitaalinen, sen läpi voidaan siirtää puhetta ja dataa, datan siirto on tosin perus GSM:ssä nykystandardein erittäin hidasta. GSM-järjestelmä on myös aiempia järjestelmiä tietoturvalisempi, sillä se kykenee salaamaan radioliikenteensä. GSM on soluverkko joka koostuu keskus-, tukiasema- ja käytönhallintajärjestelmistä, pitkälle viedyn standardoinnin ansiosta ei GSM ole missään alijärjestelmässään sidottu mihinkään tiettyyn laitevalmistajaan vaan siinä voidaan käyttää useiden laitevalmistajien laitteita. GSM:ää ei ole pyritty korvaamaan uudemmillä järjestelmillä vaan uudet järjestelmät on pikemminkin rakennettu tukemaan sitä ja toimimaan sen kanssa. (Penttinen 2006a, 121–122.)

2.2.3 Parannellut toisen sukupolven matkapuhelinverkot (2,5G)

GPRS (General Packet Radio Service) on GSM-verkon datansiirtomenetelmä jolla saadaan toteutettua pakettikytkentäisiä yhteyksiä Internetiin tai vastaaviin verkkoihin. GPRS-verkko on IP-verkko jossa käytetään IPv4:ää, sen suunnittelussa on kuitenkin otettu huomioon myös tulevaisuus ja siksi GPRS tukeekin myös IPv6:tta. GPRS:n etu aikaisemmin käytössä olleisiin menetelmiin on korkeampien siirtonopeuksien lisäksi nimenomaan sen pakettikytkentäisessä toimintaperiaatteessa, fyysistä siirtotietä varataan vain silloin kun yhteydellä siirretään dataa. (Penttinen 2006a, 158.)

EDGE on GSM verkkotekniikka jolla on onnistuttu nostamaan verkon siirtonopeuksia moninkertaiseksi aikaisempaan verrattuna, nopeuden nousu perustuu kehittyneempään modulointitekniikkaan. Koska samoissa verkoissa täytyy kyetä kuljettamaan sekä GSM- että EDGE-liikennettä, on verkon radio liikenteen rakenne täytynyt säilyttää muuttumattomana. EDGE:ä käytetään ensisijaisesti datayhteyksissä GPRS:n yhteydessä, tällöin käytetään nimitystä Enhanced GPRS eli EGPRS. EGPRS yhteydet sopivat jo erittäin hyvin mobiilien VPN ratkaisujen toteuttamiseen. (Granlund 2007, 415–417.)

2.2.4 Kolmannen sukupolven matkapuhelinverkot (3G)

Kolmannen sukupolven matkapuhelinverkkoja on kehitetty nimenomaan tarjoamaan suurempia datanopeuksia radioverkkojen lävitse, tarvetta kasvattaa yleistymässä oleva multimedian, erityisesti videokuvan, tarjonta matkaviestinverkossa. Uusia, nopeampia tekniikoita kehitetään jatkuvasti ja ne kilpailevatkin jo paikoittain perinteisempien verkkotekniikoiden kanssa joustavuutensa ja jatkuvasti kohoavien siirtonopeuksien ansiosta. Vaikka 3G-tekniikoissa onkin keskitytty pääasiassa datanopeuksien kasvattamiseen ei puheyhteyksiäkään ole unohdettu, esimerkiksi UMTS-järjestelmän spesifikaatioihin kuuluukin myös äänenlaadun nostaminen kiinteän verkon tasolle.

Kolmannen sukupolven tekniikoita on käytössä useita erilaisia eri alueilla, esimerkiksi Japanissa ja Yhdysvalloissa on käytössä CDMA 2000-tekniikka kun taas Euroopassa on käytössä WCDMA-tekniikka, kumpikin näistä tekniikoista ovat Universal Mobile Telecommunications System eli UMTS tekniikoita. (Granlund 2007, 417.)

UMTS:in kehittyessä on siirrytty yhä nopeampiin siirtotekniikoihin, High Speed Packet Access (HSPA) on mahdollistanut tiedonsiirtonopeuksien kasvun sekä alavirtaan High Speed Downlink Packet Access (HSDPA) muodossa, että ylävirtaan High Speed Uplink Packet Access (HSUPA) muodossa. HSPA vaatii toimiakseen tuen päätelaitteilta eli jos tämän tekniikan tarjoamia hyötyjä halutaan käyttää täytyy verkon laitteisto päivittää sen kanssa yhteensopivaksi. (Granlund 2007, 430–433.)

2.3 Muita yhteysmenetelmiä

Kaapelimodeemi yhteydet ovat yleisiä etenkin kotitalouksissa, tällä tavalla toteutetussa yhteydessä tietokoneesta luodaan yhteys dataverkkoon kuten Internetiin käyttäen kaapelitelevisio verkkoa, yhteyden muodostamiseen tarvitaan tarkoitukseen sopiva modeemi.

Tietokone voidaan myös liittää verkkoon käyttämällä sähkönjakeluverkkoa siirtotienä, tämä liittymätapa ei tosin ainakaan vielä ole kovin yleinen ja henkilökohtaisesti olen törmännyt tähän vain Kuopiossa mutta muuallakin näitä järjestelmiä on varmasti käytössä.

WiMAX on langaton yhteystekniikka jolla saavutetaan varsin suuret siirtonopeudet hyvinkin pitkiin matkoihin. Yhteyden nopeus riippuu välimatkasta tukiasemaan ja siitä onko tukiasemaan suora näköyhteys, lyhyemmillä matkoilla

saavutetaan suuremmat siirtonopeudet. WiMAX verkossa yhteydet voidaan toteuttaa sekä kiinteään- että mobiiliin kohteeseen. (Granlund 2007, 437.)

Käytöstä poistuneen NMT-verkon taajuusalueelle on otettu käyttöön @450 mobiililaajakaista verkko, joka perustuu Fast Low-latency Access with Seamless Handoff, Orthogonal Frequency Division Multiplexing lyhyesti Flash-OFDM tekniikkaan. Verkko on tarkoitettu nimenomaan datayhteyksiä varten ja siihen liittyäkseen käyttäjä tarvitsee liittymän lisäksi erillisen modeemin. Suomessa @450-verkko kattaa jo lähes koko maan ja sitä rakentaa Digita.

2.4 IP-verkot

Internet Protokolla eli IP-verkoissa voidaan siirtää puhetta tai dataa, tunnetuin esimerkki IP-verkosta on Internet, jota käytetään nykyään hyvin yleisesti erilaisten VPN-yhteyksien toteuttamisessa. IP-verkot ovat pakettikytkentäisiä ja niiden toiminta perustuu reitittimiin jotka reitittävät paketteja verkon lävitse oikeaan kohdeosoitteeseen, vaikka reititin ei tietäisikään kohdeosoitteen sijaintia se tietää kuitenkin aina seuraavan reitittimen osoitteen jonne paketti lähetetään, verkko voi käyttää eri reittejä pakettien perille kuljettamiseen. IP ei protokollana ota kantaa pakettien virheidenkorjaukseen tai muuhunkaan vastaavaan kuljetuksen aikana, joten se tarvitsee avukseen toisia protokollia kuten Transmission Control Protocol (TCP) huolehtimaan pakettien luotettavasta perille menosta. (Penttinen 2006a, 49–52.)

Internet protokollan tällä hetkellä yleisesti käytössä oleva versio on IPv4. On kuitenkin jo jonkin aikaa ollut ilmeistä että aletaan olla IPv4:n osoiteavaruuden riittävyyden äärirajoilla, tilannetta on pyritty helpottamaan esimerkiksi osoite muunnoksen (Network Address Translationin (NAT)) avulla Internet protokollan seuraavan kehitysversion IPv6 yleisempää käyttöönottoa odoteltaessa.

NAT:in tai nykyään useimminkin Network Address and Port Translation (NAPT) avulla voidaan esimerkiksi pienen yrityksen koko Internet liikenne hoitaa vain yhden julkisen IP-osoitteen avulla, suuremmissa yrityksissä julkisia osoitteita tarvitaan hieman enemmän muuta silti yleensä vain muutamia. NAPT osoitteenmuunnos voidaan hoitaa esimerkiksi Internet yhteydestä huolehtivassa reitittimessä tai muunnoksesta huolehtimaan voidaan asettaa NAPT-palvelin. NAT:in tai NAPT:in käyttäminen paikallisverkoissa aiheuttaa kuitenkin joitain rajoituksia VPN-yhteyksien suhteen, kaikkia VPN-tekniikoita ei pystytä käyttämään ”yksityisten”, intranet, verkko-osoitteiden kanssa. (Hakala 2005, 212–214.)

Internet protokollan seuraavan version IPv6:n osoiteavaruus on huomattavan paljon IPv4:ää suurempi, jopa siinä määrin että esimerkiksi mobiililaitteille voitaisiin antaa kertakäyttöiset osoitteet, jotka poistuisivat käytöstä laitteen käyttöänsä umpeuduttua, tämä helpottaisi tuntuvasti mobiilien VPN yhteyksien muodostamista ja niiden hallinnointia. IPv6 on pyritty suunnittelemaan siten, että se vastaisi paremmin nykyisen Internetin vaatimuksiin, IPv4:ssä käytössä olevasta osoitteiden luokkajaosta on luovuttu kokonaan ja osoitteet on järjestetty hierarkkisesti siten, että niistä käy ilmi osoitteen omistaja ja maantieteellinen sijainti, IPv6 osoitteissa yhdistyy myös laitteen fyysinen ja looginen osoite. IPv6:tta ei ole vielä otettu laajamittaisesti käyttöön, mutta käyttöönotto tulee mitä luultavimmin tapahtumaan lähitulevaisuudessa mobiililaitteiden edelleen yleistyessä. (Hakala 2005, 215–223.)

3 VIRTUAALISET YKSITYISVERKOT

3.1 VPN-yhteyden toiminta

VPN:n (Virtual Private Network) tarkoituksena on luoda tietoturvallinen tietoliikenneverkko kahden pisteen välille hyödyntäen julkisia verkkoja kuten Internetiä. Yrityksmaailmassa tämä tarkoittaa lähinnä tietojärjestelmien etäkäyttöä tai esimerkiksi yrityksen eri kaupungeissa sijaitsevien toimipaikkojen yhdistämistä tietoturvalisesti toisiinsa. VPN-verkoksi voisi myös periaatteessa kutsua vuokrakaapeli yhteyksiä mutta ne ovat kalliita ja epäkäytännöllisiä Internetin kautta toteutettuun VPN-yhteyteen verrattuna. Internetin etua siirtotienä korostaa vielä erityisesti sen levinneisyys, periaatteessa Internetiä voi nyky-päivänä käyttää mistä tahansa. Keskitynkin jatkossa kuvaamaan VPN-yhteyksiä nimenomaan Internetin kautta toteutetun VPN:n näkökulmasta. (Perlmutter, Bruce – Zarkower, Jonathan 2001, 10–12.)

VPN-yhteydessä yhteysosapuolten välille luodaan virtuaalinen tunneli jossa voidaan siirtää dataa julkisia verkkoja hyödyntäen. Nykytilanteessa pelkän tunnelin luominen ei kuitenkaan riitä vaan yhteydeltä vaaditaan enemmän tietoturvaa, tämä edellyttää siirrettävän datan vahvaa salausta ja käyttäjien tunnistamista. Jos yhteys luodaan esimerkiksi yrityksen kahden toimipaikan välille, käytetään yhteyden luomiseen siihen kykeneviä reitittämiä yhteyden molemmissa päissä, yhden käyttäjän etäyhteys muodostetaan tavallisesti käyttäjän tietokoneen ja etäkäyttöpalvelimen välille. (Hakala 2005, 381–382.)

VPN-tunneloinnilla tarkoitetaan pakettien tai kehysten sijoittamista toisten pakettien tai kehysten sisään, tätä toimenpidettä kutsutaan kapseloinniksi, näin voidaan helposti siirtää yksityisiä paketteja yleisen julkisen verkon, vaikkapa Internetin, välityksellä. Kapselointia kuvaa hyvin vertaus ”kirjekuoren laittaminen toisen kirjekuoren sisään”. Tunneloinnin toteuttamiseen on olemassa useita eri protokollia, joista käytetyimpien joukossa ovat IPSec, PPTP GRE ja

L2PT protokollat. Liitteessä 4 on kuvattu VPN-protokollien sijoittuminen Open System Interconnection eli OSI-mallin tasoille. (Perlmutter, Bruce – Zarkower, Jonathan 2001, 104–106.)

3.2 Internet Protocol Security (IPSec)

3.2.1 IPSec ja sen toiminta

IPSec protokolla on itseasiassa kokoelma protokollia ja se on ollut muodollisesti olemassa jo suhteellisen kauan, vuodesta 1995 lähtien. IPSec:in protokollia voidaan käyttää sekä VPN-tunnelin muodostamiseen, että jonkin toisen tunnelointiprotokollan datakuorman salaamiseen. IPSec toimii IPv4:n kanssa ja se on sisällytetty osaksi uudempaa IPv6 protokollaa. Haittapuoleksi voi IPSecin kohdalla laskea sen, että sitä ei voi suoraan käyttää muissa kuin IP pohjaisissa verkoissa, tosin nykypäivänä alkaa olla hankala löytää verkkoja jotka eivät ole IP pohjaisia. IPSec protokollan perustekijät, joita käytetään suojaamaan yhteydellä liikkuva dataa ovat todennus, salaus ja avaimenhallinta. IPSec toimii OSI-mallin tasolla 3 (liite 4). (Perlmutter, Bruce – Zarkower, Jonathan 2001, 106–109.)

Todennus (authentication), varmistaa, että datan lähettäjä on se kuka sanoo olevansa ja että lähetetty data on yhtäläinen vastaanotetun datan kanssa.

Salaus (encryption), muuttaa/sekoittaa lähetettävän viestin siten, että se on mahdotonta (tai ainakin erittäin vaikeaa) tulkita jos hallussa ei ole oikeaa avainta salauksen purkamiseen. Joitain salausalgoritmeja joita voidaan käyttää viestien salakirjoittamiseen, DES (Data Encryption Standard), 3DES, AES (Advanced Encryption Standard), Blowfish.

Avaimenhallinta, muodostaa salatun avainarvon data lähettäjän ja vastaanottajan välillä, avainarvoa käytetään IPSec-yhteydellä liikkuvien viestien salaamiseen ja salauksen purkamiseen.

IPSec'in toiminnassa on aina kaksi osapuolta lähettäjä ja vastaanottaja. Aluksi näiden kahden kesken sovitaan sovitaan salausavaimesta, tämä avainarvo voidaan sopia ja asettaa manuaalisesti tai sen luomiseen voidaan käyttää jollain IPSec'in tukemaa dynaamista avaimenluontimenetelmää. Kun molemmilla yhteysosapuolilla on sama avainarvo tiedossa ja yhteyden muistakin ominaisuuksista on sovittu, on IPSec muodostanut niin sanotun turvallisuusliiton osapuolten välille, tämän jälkeen lähettävä osapuoli muodostaa sovitun avaimen perusteella digitaalisen allekirjoituksen jonka voi lukea vain samalla avaimella varustettu vastaanottaja, lisäksi lähetettävän datan voi salakirjoittaa jollain IPSec'in tukemalla salausalgoritmeilla. (Perlmutter, Bruce – Zarkower, Jonathan 2001, 109–111.)

3.2.2 Authentication Header (AH)

AH:ta käytetään IPSec:ssä todentamaan että viestien lähettäjä on se kuka sanoo olevansa sekä estämään viestien toistamista. AH-todennus tapahtuu pakettitasolla, siinä pakettiin lisätään AH-otsake. AH-otsakkeeseen kuuluu muun muassa tarkistussumma jolla varmistetaan viestin eheys. AH:ta ei voida käyttää yksityisten (intranet) IP-osoitteiden välisen liikennöinnin suojaamiseen. (Perlmutter, Bruce – Zarkower, Jonathan 2001, 107).

3.2.3 Encapsulating Security Payload (ESP)

IPSec tukee datakuorman salaamista ESP-protokollaa käyttäen, ESP toimii kahdessa tilassa joita ovat tunnelitila ja kuljetustila, eri tiloja voidaan käyttää hieman eri tarkoituksiin. ESP:n molempia tiloja käytetään VPN:issä, tunneliti-

laa voidaan käyttää myös yksinään. (Perlmutter, Bruce – Zarkower, Jonathan 2001, 107.)

Tunnelitilassa alkuperäinen paketti kapseloidaan sellaisenaan uuden IP-paketin sisään, alkuperäinen paketti muuttuu uuden paketin data-kuormaksi.

Kuljetustilassa pakettiin lisätään ESP-osoite ennen sen lähettämistä eteenpäin.

3.2.4 Security Association (SA)

Security Association eli turvallisuusliitto, määrittää tietyn menetelmän jolla VPN-yhteyttä suojataan. Yhdelle VPN-yhteydelle voi olla määritelty useita SA:ta, esimerkiksi yhteydellä liikkuvien viestien salakirjoitus ja niiden eheyden varmentaminen. Jos yhteydelle on määritetty enemmän kuin yksi SA, voidaan SA:ta muodostaa nippuja helpottamaan niiden käsittelyä, nippua käytettäessä käytetään yhteydelle kaikkia nipun sisältämiä SA:ta. Kaikki yhteyden SA:t tallennetaan Security Association Database (SAD) tietokantaan. (Ruohonen 2002, 293–297.)

3.2.5 Avaimenhallinta

Viestien salakirjoittamiseen tarvittavista avaimista täytyy sopia jollain tavalla yhteysosapuolten kesken, sopimiseen voidaan käyttää joko julkisen tai salaisen avaimen menetelmiä. Julkisen avaimen menetelmiä käytettäessä voivat käyttäjät yksinkertaisesti jakaa julkiset avaimensa toisilleen, salaisen avaimen menetelmät puolestaan vaativat avainten sopimisen siten, etteivät ulkopuoliset tahot pääse missään vaiheessa käsiksi avaimeen. Salaisen avaimen menetelmiä käytettäessä voidaan käyttää jotain avaimensopimisprotokollaa

kuten Diffie-Hellman protokolla, jos salausavain on jo luotu ja se halutaan vain jakaa toisille käyttäjille, käytetään avaimenjakoprotokollaa.

IPSec:ssä käytetään Internet Key Exchange Protokollaa (IKE) muodostamaan Security Association (SA), IKE käyttää Diffie-Hellman protokollaa avainten jakamiseen.

3.3 Muita VPN-protokollia

3.3.1 Generic Routing Encapsulation (GRE)

GRE-protokollan tarkoitus on kapseloida toisia protokollia, se pystyy kapseloimaan paria kymmentä erityyppistä pakettia, nykyään suurin osa dataliikenteestä on kuitenkin IP-paketteja. GRE-paketin rakenne on hyvin yksinkertainen, tästä huolimatta GRE pystyy autentikoimaan ja tunnistamaan paketin lähteen. Riippuen protokollasta joka GRE:llä kapseloidaan, voi se toimia OSI-mallin verkko- tai siirtoyhteysskerroksessa (liite 4). (Perlmutter, Bruce – Zarkower, Jonathan 2001, 134–135.)

3.3.2 Point to point tunneling protocol (PPTP)

PPTP on alunperin suunniteltu yhdistämään puhelinverkkojen piiriyhteyksiset yhteydet ja mahdollistamaan pakettiyhteyksiset yhteydet, esimerkiksi Internet yhteydet. PPTP:n toiminta perustuu PPP-kehysten tunnelointiin TCP/IP verkon läpi, näin voidaan muodostaa PPTP VPN-yhteys esimerkiksi Internetin välityksellä. PPP-kehysten data salakirjoitetaan ennen kapselointia käyttäjän tunnistuksen yhteydessä luotujen salausavainten avulla, käyttäjän tunnistamiseen voidaan käyttää Password Authentication Protokollaa (PAP), Challenge Handshaking Authentication Protokollaa (CHAP) tai sitten voidaan käyttää erillistä tunnistuspalvelinta ja Extensible Authentication Protokollaa (EAP). (Hakala 2005, 382–383.)

PPTP:tä on aikaisemmin käytetty paljonkin virtuaalisia yksityisverkkoratkaisuja tuottaessa sen joustavuuden takia ja osittain myös siksi että Microsoft Windows käyttöjärjestelmät Windows 95:tä lähtien ovat sisältäneet PPTP asiakasohjelmiston. Protokollan joustavuudesta kertoo se, että sen toteuttamiseen on useita erilaisia tapoja ja sitä voidaan käyttää sekä WAN (Wide Area Network) että LAN (Local Area Network) ratkaisuissa. Modeemi ja ISDN yhteyksien käydessä yhä harvinaisemmiksi, käytetään PPTP:tä lähinnä pienien ja yksinkertaisten etäyhteyksien toteuttamiseen. PPTP on OSI-mallin siirtoyhteyshierarkiassa toimiva protokolla (liite 4). (Perlmutter, Bruce – Zarkower, Jonathan 2001, 114–115.)

3.3.3 Layer 2 tunneling protocol (L2TP)

L2TP on aikoinaan syntynyt PPTP ja L2F (Layer 2 Forwarding) protokollien yhteensulautumisen tuloksena, L2F on myöhemmin kadonnut kokonaan markkinoilta ja VPN-laitteisto- ja ohjelmistovalmistajat ovat siirtyneet käyttämään L2TP:tä sen sijaan. Vaikka L2TP on saman tyylinen protokolla kuin PPTP, on se kuitenkin rakenteeltaan monimutkaisempi. L2TP-protokollaa käytetään PPP-pakettien siirtämiseen pakettikytkentäisissä verkoissa, L2TP liikenne koostuu UDP-kapseloiduista valvonta-, komento- ja datapaketeista. L2TP toimii OSI-mallin toisessa- eli siirtoyhteyshierarkiassa (liite 4). L2TP tunnelointiprotokolla ei itsessään sisällä datan minkäänlaista salausta mutta sen paketteja voidaan suojata käyttämällä apuna IPSec'in kuljetustilaa ja salausta. (Perlmutter, Bruce – Zarkower, Jonathan 2001, 124–133.)

L2TP:tä käytetään yleensä VPN-etäyhteyksien muodostamiseen käyttäjän ja etäyhteyshierarkiavälillä, etäyhteyshierarkiavälillä ominaisuus on mukana Microsoftin Windows-palvelin käyttöjärjestelmissä. Palvelu otetaan käyttöön yksin-

kertaisesti avaamalla etäkäyttöpalvelimelta portteja L2TP-protokollan käyttöön.

3.4 Datakuorman salaaminen

3.4.1 Salausmenetelmät

Käyn seuraavassa läpi IPSec VPN:issä käytettyjä salakirjoitusmenetelmiä ja joitain salakirjoitus algoritmeja hyvin yleisellä tasolla. Salakirjoitusmenetelmät luokitellaan sen mukaan miten ne salaavat datan. Siirtosalaajat käyttävät aina samaa matemaattista kaavaa datan selväkielisen osan ja vastaavan salakirjoitetun osan välillä, korvaussalaajat puolestaan korvaavat selväkielisen osan datasta jollain vastaavan salakirjoitetun datan osalla, osien välillä ei välttämättä ole minkäänlaista loogista yhteyttä, sekoitussalaaja puolestaan sekoittaa selväkielisen datan jollain ennalta määrätyllä tavalla. Tulossalaajat käyttävät datan salaamiseen useita salakirjoitusmenetelmiä, kun taas virtasalaajat tuottavat datan jokaiselle osalle oman avaimen jota sitten käytetään datan salakirjoittamiseen. Salakirjoitusmenetelmät jaetaan myös julkisen avaimen ja salaisen avaimen menetelmiin riippuen siitä käytetäänkö data salakirjoittamiseen ja salakirjoituksen purkamiseen samaa vai eri avainta, salaisen avaimen menetelmä käyttää yhtä ja julkisen avaimen menetelmä kahta salausavainta. (Ruuhonen 2002, 261–263.)

3.4.2 Salausalgoritmeja

Data Encryption Standard eli DES on jo vanhentunut salausalgoritmi mutta se on yhä käytössä, se on virta- ja korvaussalaaja. DES salaus voidaan toteuttaa joko laitteisto tai ohjelmisto pohjalta. Laitteisto pohjaisena DES on hyvin nopea ja sopii käytettäväksi suurissa järjestelmissä, täytyy kuitenkin muistaa, että DES salaus on murrettavissa. 3-DES salaus on kehittyneempi ja tietoturvasempi versio DES-salauksesta, siinä data salakirjoitetaan DES algo-

ritmilla kolmeen kertaan käyttäen kahta tai kolmea eri avainta. 3-DES menetelmällä saavutetaan vahvempi salaus, aikaa salakirjoittamiseen kuluu vastaavasti kaksi tai kolme kertaa enemmän kuin pelkkää DES-salausta käyttämällä. (Ruohonen 2002, 274.)

RSA on julkisen avaimen salausalgoritmi, vaikka se on jo iäkäs ei sitä ole onnistuttu murtamaan. RSA on siirtosalaaja ja siinä voidaan käyttää eri kokoisia salausavaimia, suurempien avainten käyttö hidastaa algoritmia mutta salaus on myös vastaavasti vahvempi. (Ruohonen 2002, 275–276.)

Blowfish algoritmi on erittäin nopea, vapaaseen käyttöön julkaistu korvaussalaaja. (Ruohonen 2002, 276)

Advanced Encryption Standard eli AES on vapaassa käytössä oleva salausalgoritmi joka on suunniteltu korvaamaan nyt jo vanhentunut DES. AES on tulossalaaja ja käyttää tietojen salaamiseen Rijndael-algoritmia. (Ruohonen 2002, 277)

4 VPN ESIMERKIT

4.1 IPsec VPN matkapuhelinverkon avulla (liite 1)

4.1.1 Laitteisto

VPN:n kannalta tärkeimpiä laitteita ovat tässä tapauksessa 3G-reititin ja Cisco PIX/ASA, VPN-yhteys muodostetaan näiden laitteiden välille.

3G VPN-reititin, niin kuin nimestä voi päätellä 3G-reitittimen määrittelevänä ominaisuutena on yhteyksien muodostaminen matkaviestinverkon välityksellä. Yhteyden muodostamiseen voidaan yleensä käyttää UMTS:n lisäksi myös GSM-verkon GPRS osaa. Reititin on matkaviestinverkko ominaisuudet pois lukien normaalin reitittimen kaltainen niin porteiltaan kuin muiltakin ominaisuuksiltaan, mahdollisesti mukana on myös WLAN-ominaisuus ja usein niissä on myös GPS paikannus ominaisuus, ainakin lisävarusteena. Tällaisten reitittimien käyttö on tarkoituksenmukaista silloin, jos halutaan luoda liikuteltava VPN-tunneli jonka avulla useammat laitteet voidaan liittää verkkoon.

Cisco PIX/ASA, PIX (Private Internet eXchange) on Cisco Systemsin jo 90-luvulla kehittämä palomuuuri ja VPN laiteratkaisu, PIX tuotteiden valmistus on lopetettu vuonna 2008 mutta niitä on käytössä paljon ja tuki jatkuu vielä ainakin vuoteen 2013 saakka. PIX tuoteperheen tilalle on tullut ASA (Adaptive Security Appliance), jossa on kaikki PIX:in ominaisuudet sekä muutamia parannuksia, suorituskykyä on myös parannettu. Nämä laitteet pystyvät mallista riippuen ylläpitämään useita VPN-tunneleita, alkaen kahdestakymmenestäviidestä aina kymmeentuhanteen saakka. Esimerkki olettaa useita mallin kaltaisia yhteyksiä sisältävää järjestelmää jolloin ”normaali” reititin ei yksinkertai-

sesti riittää käsittelemään yhtä aikaa aktiivisina olevien VPN-yhteyksien määrää.

4.1.2 Käyttäjän tunnistaminen matkaviestinverkossa

Käyttäjän tunnistamiseen käytetään matkaviestinverkossa SIM (Subscriber Identity Module)-korttia, UMTS verkossa vastaava on nimeltään USIM (Universal Services Identity Module), kortille on tallennettu käyttäjää koskevaa tunnistetietoja sekä operaattorikohtaisia tunnistusalgoritmeja. SIM-kortti sijoitetaan järjestelmässä laitteeseen, Mobile Station (MS). Matkaviestinjärjestelmän keskusjärjestelmässä ja laitteen SIM kortissa lasketaan salausavaimet käyttäen tunnistusalgoritmeja, saatuja lukuja verrataan sitten toisiinsa käyttäjän tunnistamiseksi. IMEI (International Mobile Equipment Identity) numeron avulla tunnistetaan verkossa viestintään käytettävä laite, esimerkiksi puhelin tai matkaviestinverkkoa käyttävä reititin. (Penttinen 2006a, 135, 146–148, 163.)

4.1.3 VPN-yhteyden muodostaminen

Esimerkissä 3G reitittimen ja PIX/ASA laitteen välille luodaan IPSec VPN-tunneli joka varmistaa tietoturvallisen tiedonsiirron lähettäjän ja vastaanottajan välillä. Menetelmää voidaan käyttää hyödyksi monissa erilaisissa tilanteissa, sillä voidaan esimerkiksi yhdistää jonkin yrityksen toimipaikkoja toisiinsa, reitittimiä voidaan sijoittaa ajoneuvoihin tai voidaan tarjota reititintä vuokralle esimerkiksi jos tarvitaan verkkoyhteys kahdeksi viikoksi jonnekin johon ei ole kiinteää kaapeliyhteyttä. Käytettäessä 3G-reitittimiä joudutaan tekemään läheistä yhteistyötä radioverkko-operaattorin kanssa.

Yhteyden muodostus alkaa siitä kun 3G-reititin tulee ”online” tilaan ja alkaa hakea verkkoa, ensimmäisenä tarkastetaan mistä tukiasemasta saadaan voi-

makkain signaali, kun tämä on selvillä matkaviestinverkon keskusjärjestelmä tarkasta onko reitittimen SIM-kortilla oikeutta käyttää verkkoa, jos SIM hyväksytään voidaan yhteys muodostaa ja matkaviestinjärjestelmä siirtyy salaamaan yhteyttä, muussa tapauksessa matkaviestinjärjestelmän keskusjärjestelmä sulkee yhteyden. Matkaviestinverkon hyväksyttyä SIM:in, yhdistää GGSN (Gateway GPRS Support Node) yhteyden edelleen Internetiin, SGSN (Serving GPRS Support Node) puolestaan yhdistää verkon GPRS-osan sen GSM-osaan pitää huolen 3G-reitittimen liikkuvuuden hallinnasta verkossa, esimerkiksi vaihdot tukiasemasta toiseen. Sekä GGSN että SGSN ovat käytännössä reitittäjiä jotka reitittävät matkaviestinverkossa (GPRS) pakettikytkentäisiä yhteyksiä. (Penttinen 2006a, 148, 158–161.)

Kun yhteys Internetiin on saatu muodostettua reititetään yhteys vastaanottavan tahon VPN-verkkolaitteeseen, tässä esimerkissä Cisco PIX/ASA ja IPSec VPN yhteyden muodostus voi alkaa. VPN-tunnelin muodostamiseen käytetään IPSec:iä tunneli moodissa. SA:ssa tai SA nipussa jota yhteydellä käytetään on määritetty yhteydellä käytettävät tietoturvakäytännöt, aina avaimenhallinnasta tiedon salakirjoittamiseen käytettävään algoritmiin. Jokaisella yhteydellä on omat yksilölliset SA:sa mutta yleisesti voisi todeta, että ainakin yhteysosapuolten tunnistamiselle, salausavaimen muodostamiselle ja salausalgoritmille on määritetty SA:t lähes jokaisessa IPSec yhteydessä. Tämän esimerkin kaltaisessa järjestelmässä kaikki liikenne 3G-reitittimeltä ohjataan VPN-tunneliin, järjestelmässä on useita vastaavia tunneleita joita hallinnoidaan PIX/ASA:n ja 3G reitittimen valmistajan tarjoaman hallintaohjelmiston avulla.

4.2 IPSec VPN yrityksen kahden toimipaikan välillä (Liite 2)

4.2.1 Laitteisto

Tärkeimmät laitteet tässä esimerkissä ovat reitittimet (VPN-yhdyskäytävät) jotka hoitavat IPSec VPN-tunnelin luomisen ja tunnelissa liikkuvan tiedon salaamisen ja salauksen purkamisen SA:ssa määritetyillä tavoilla. Yhdyskäytävänä toimivissa reitittimissä hoidetaan myös mahdolliset NAT osoitteen muunnokset. Reitittimet kannattaa valita jonkin hyväksi tiedetyn valmistajan valikosta ja kannattaa varmistaa, että hankitaan todellakin tarkoitukseen sopivat laitteet.

4.2.2 VPN yhteys

Kun ryhdytään luomaan VPN-yhteyttä yrityksen kahden toimipaikan välille, esimerkiksi jos halutaan muodostaa yhteys yrityksen myymälän ja eri osoitteessa sijaitsevan varaston välillä, yhteys toteutetaan käyttäen kahta tarkoitukseen sopivaa reititintä. Reitittimet huolehtivat VPN-tunnelin luomisesta, avaimenhallinnasta, tunneliin lähtevän tiedon salaamisesta ja saapuvan tiedon salauksen purkamisesta, molemmista reitittimistä on löydyttävä tuki kaikille yhteydessä käytettäville protokollille ja tekniikoille. Käytettäessä kahden reitittimen tekniikkaa VPN-yhteyden luomiseen ei verkkojen yksittäisiin työasemiin tarvitse tehdä minkäänlaisia muutoksia. Reitittimien välisissä VPN-yhteyksissä käytetään yleisesti IPSec protokollaa tunneli moodissa VPN tunnelin muodostamiseen, muut yhteyden ominaisuudet on määritetty yhteydellä käytettävässä SA:ssa (Security Association). Yritysten omissa verkoissa on todennäköisesti käytössä yksityiset IP-osoitteet, julkiset osoitteet on varattu Internet liikennöintiin. Jos lähtevän paketin kohdeosoite on toisen toimipaikan verkossa, reititetään se VPN-tunneliin muussa tapauksessa käytetään normaalia suojaamatonta siirtotietä.

Kun lähtevän paketin kohdeosoite on yrityksen toisessa toimipisteessä, VPN-yhdyskäytävänä toimiva reititin salakirjoittaa paketit SA:ssa määritetyllä tavalla ja kapseloi ne sitten käyttäen IPSec protokollaa ja lähettää ne edelleen VPN-yhteyden toisessa päässä odottavalle reitittimelle, joka purkaa kapseloinnin ja salauksen ja lähettää paketin edelleen kohdeosoitteeseensa.

4.3 VPN kotitoimiston ja työpaikan välillä (liite 3)

4.3.1 Laitteisto

Tässä esimerkissä tärkeimpiä laitteita ovat tietokone kotitoimistolla, yrityksen palomuri/reititin joka laskee tietyn Internetin kautta tulevan yhteyden lävitseen ja etäkäyttöpalvelin johon VPN-tunneli muodostetaan.

4.3.2 VPN-yhteys

Tämän tyylisissä etäyhteyksissä käytetään yleisesti L2TP tunnelointi protokollaa jonka paketit sitten suojataan käyttäen IPSec protokollanippua. Käytännössä L2TP-pakettien salakirjoittamiseen käytetään joko DES tai 3DES salausalgoritmia.

Jos käytössä on Windows palvelin, voidaan etäkäyttöpalvelin vain yksinkertaisesti ottaa käyttöön Microsoft Management Consolen avulla, palvelua aktivoitaessa asetetaan halutut tietoturvakäytännöt ja määritetään käyttäjätunnukset joilla yhteyden voi avata, tunnelointi protokollaksi voi halutessaan valita myös PPTP:n mutta vakiona tunneloidaan L2TP protokollalla. Käyttäjän tunnistuksen lisäksi voidaan yhteyden muodostamiselle asettaa lisäehtoja, kuten IP- tai MAC-osoitteet joista yhteys etäkäyttöpalvelimeen voidaan muodostaa.

5 JOHTOPÄÄTÖKSIÄ, POHDINTOJA JA TULEVAISUUDEN NÄKYMIÄ

Hyvin toteutetun VPN-yhteyden ei tulisi näkyä lainkaan loppukäyttäjälle (liite 4), loppukäyttäjän on myös voitava luottaa siihen että VPN-yhteydellä lähetetyt viestit on asianmukaisesti suojattu. Jotta nykyisille VPN-yhteyksille asetettua tietoturva tavoitteet saavutettaisiin, vaaditaan VPN-ratkaisujen suunnitteluun ja toteuttamiseen ehdottomasti IT-alan ammattilaisia. VPN-järjestelmän suunnittelu ja toteutuksessa käytetyt asetukset tulee ehdottomasti dokumentoida kuten missä tahansa muussa verkkoihin liittyvässä projektissa, dokumentointi tulee toteuttaa niin selkeästi, että toinen IT-alan ammattilainen saa dokumenteista helposti selville järjestelmän asetukset ja käytetyt protokollat, toisin sanoen dokumentointiin valitaan joku standardi jota noudatetaan koko järjestelmän asiakirjoissa.

Pystytettäessä VPN:ä joudutaan yleensä hankkimaan jonkin verran uutta laitteistoa, esimerkiksi reitittimien on oltava kykeneviä toimimaan VPN-yhdyskäytävinä. Etäyhteyksien hoitamiseen saatetaan tarvita palvelin, harvassa pienessä yrityksessä on omaa palvelinkonetta, yleisesti palvelimen virkaa hoitaa yksinkertaisesti jokin verkon työasemista.

Se että VPN on rakennettu ja otettu käyttöön ei vielä takaa yhteyksien tieturvallisuutta, järjestelmien ylläpitäminen tietyllä tieturvan tasolla vaatii jatkuvaa panostusta sekä laitteisiin ja ohjelmistoihin, että ennen kaikkea järjestelmiä ylläpitävän tahon ammattitaidon ylläpitämiseen. Etenkään pienissä yrityksissä ei useinkaan ole IT-tukihenkilöä joka pystyisi huolehtimaan verkon ja VPN:n tarpeista, tällaisessa tilanteessa kannattaakin ennemmin ulkoistaa järjestelmien ylläpito koulutetuille IT-alan ammattilaisille, tästä tietenkin koituu yritykselle hieman lisämenoja mutta samalla järjestelmiin kohdistuvat tietoturva vaatimukset pysyvät ajan tasalla.

Tulevaisuudessa kun IPv6 otetaan laajempaan käyttöön helpottuu VPN-yhteyksien toteuttaminen huomattavasti etenkin mobiilien laitteiden osalta, koska jokaiselle laitteelle voidaan osoittaa oma yksiselitteinen verkko-osoite jonka avulla laite tunnistetaan verkossa. IPv6 on myös tietoturvaominaisuuksiltaan ylivoimainen IPv4:ään verrattuna.

Vanhemmissa julkaisuissa IPsec mainitaan usein tunneloinnin yhteydessä mutta uudemmat julkaisut niputtavat sen enemmänkin yhteen tietoturvan kanssa. Uudempi näkökulma tuntuu sopivan IPsec'in luonteeseen paremmin, sillä sitä voidaan käyttää ja usein käytetäänkin toisten protokollien pakettien suojaamiseen.

Matkaviestin verkon käyttäminen sopii mainiosti VPN-toteutuksiin jo siitäkin syystä, että matkaviestinverkon salaus standardit ovat hyvin kehittyneet verrattuna esimerkiksi Wireless LAN:iin, tämä lisää ylimääräisen tason tietoturvaa matkaviestinverkon yhteyksille. Matkaviestinverkkojen käyttöä tukee myös niiden kattavuus, lähes mistä tahansa Suomen sisällä voidaan muodostaa VPN-yhteys, yhteys toki toimii ulkomailatakin mutta hinnoittelun kanssa saattaa tulla yllätyksiä.

Neljännän sukupolven matkapuhelinverkkoja (4G) ollaan parhaillaan ottamassa käyttöön, Suomessa ei kuitenkaan vielä tällä hetkellä ole kaupallista 4G verkkoa saatavissa, ensimmäiset toteutukset tulevat kuitenkin luultavasti käyttöön vuoden 2010 aikana. 4G verkot ovat 3G verkoista poiketen täysin pakettikytkentäisiä ja siirtonopeuksia on edelleen nostettu ja palveluiden laadua pyritty parantamaan entisestään. 4G:n spesifikaatioissa mainitaan jopa 1gb/s nopeus paikallaan olevaan kohteeseen, liikkuvaan kohteeseen pyritään 100mbit/s nopeuteen. Toteutuessaan tämä tarkoittaisi hyvin nopeita yhteyksiä mobiililaitteisiin, suuremman mittakaavan käytännön toteutukset ovat kuitenkin luultavasti vielä vuosien päässä.

Yleisesti järjestelmien tietoturvasoon näyttäisi vaikuttavan kaikkein eniten ammattitaitoisen ylläpidon puuttuminen. CERT-FI:n vuosineljännes raporteista käy ilmi, että hyvin suuri osa tietoturvariskeistä ja ongelmista johtuu päivitämättömistä järjestelmistä, voi tietenkin miettiä myös sitä, miten esimerkiksi nykyisissä käyttöjärjestelmissä ja ohjelmissa voi olla niin suuri määrä tieturvaongelmia. Vaikka käytössä olisi ammattitaitoisesti ylläpidetyt VPN-järjestelmät palomureineen ja muine tietoturvaratkaisuineen on järjestelmän lopullinen tietoturvaso kiinni myös käyttäjien, erityisesti etäkäyttäjien käyttämien päätelaitteiden tietoturvasosta. Puhelinten alkaessa muistuttaa yhä enemmän kannettavaa tietokonetta (tai toisinpäin), alkavat tietokone maailmassa yleiset lieveilmiöt kuten virukset ja haittaohjelmat olla yhä suurempi riesa matkapuhelinten käyttäjille. Tulevaisuudessa nämä seikat tulee ottaa enenevässä määrin huomioon suunniteltaessa mobiileja järjestelmiä. (CERT-FI tieturvakatsaus 2009.)

LÄHTEET

CERT-FI, tietoturvakatsaus 2009, osoitteessa: <http://www.cert.fi/> 16.12.2009

Granlund, Kaj 2007. Tietoliikenne. Docendo, Jyväskylä.

Hakala, Mika – Vainio, Mika 2005. Tietoverkon rakentaminen. Docendo, Jyväskylä.

Penttinen, Jyrki 2006a. Tietoliikennetekniikka : perusverkot ja GSM. WSOY, Helsinki.

Penttinen, Jyrki 2006b. Tietoliikennetekniikka : 3G ja erityisverkot. WSOY, Helsinki.

Perlmutter, Bruce – Zarkower, Jonathan 2001. VPN : virtuaaliset yksityisverkot. Edita, IT Press, Helsinki.

Ruohonen, Mika 2002. Tietoturva. Docendo, Jyväskylä.

LIITTEET

IPSec VPN matkapuhelinverkon avulla (Liite 1)

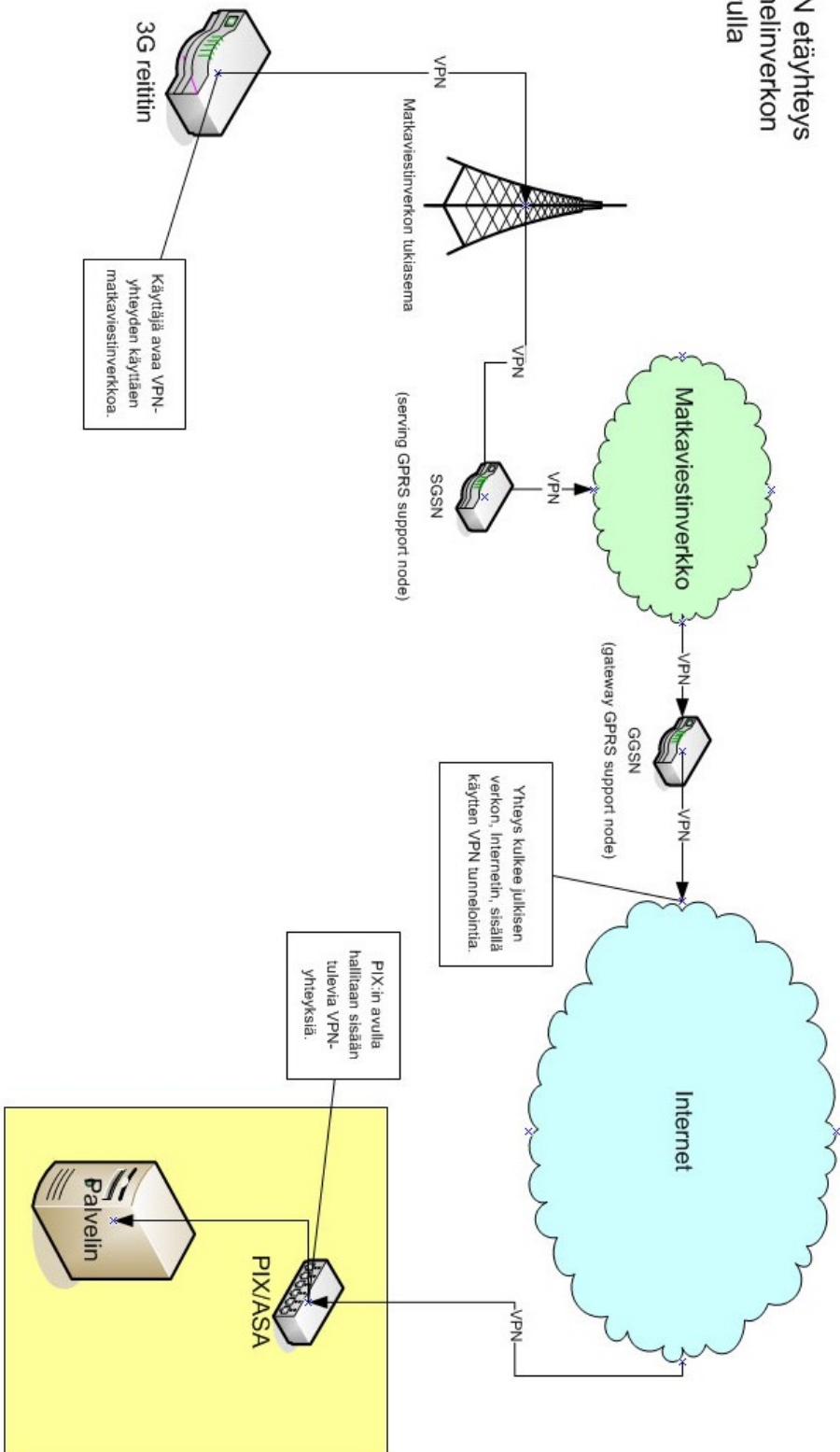
IPSec VPN yrityksen kahden toimipaikan välillä (Liite 2)

VPN kotitoimiston ja työpaikan välillä (Liite 3)

OSI-malli (Liite 4)

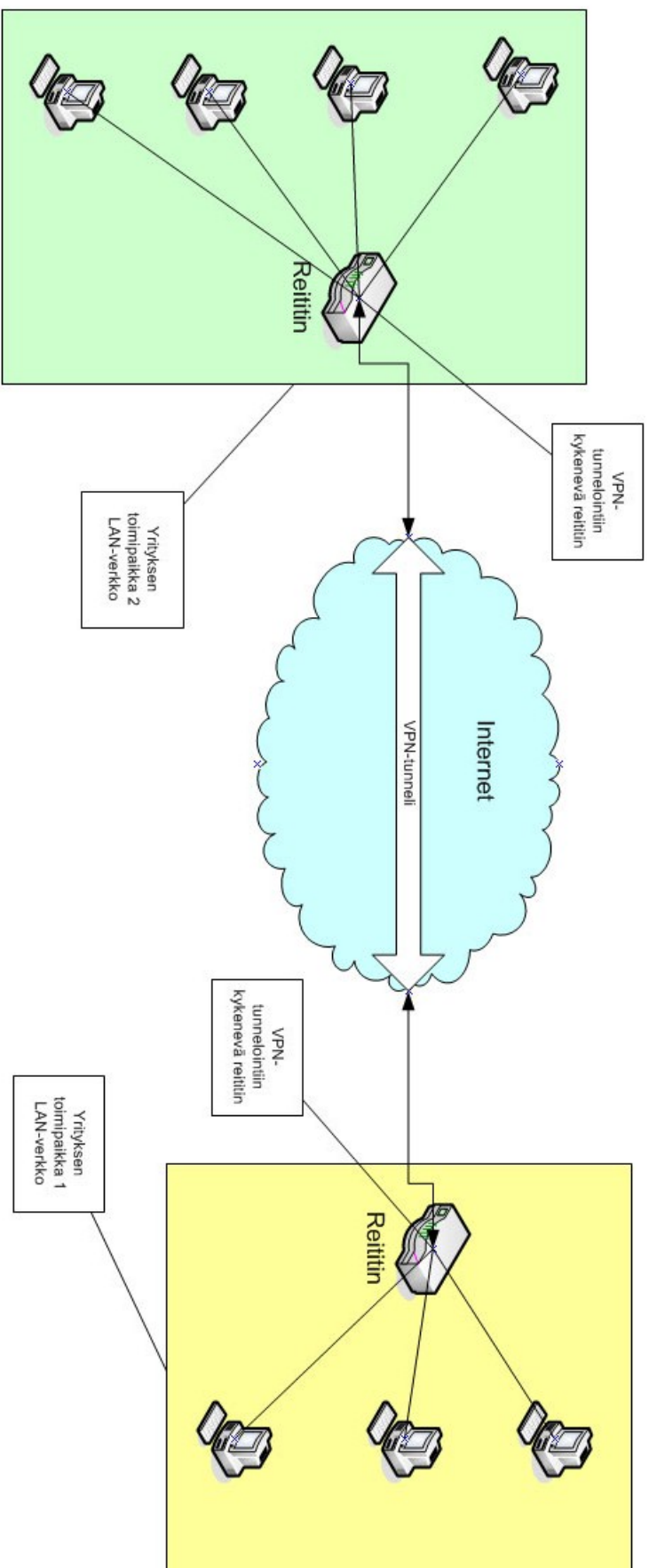
Lite 1

IPSec VPN etäyhteys matkapuhelinverkon avulla



Lite 2

VPN-yhteys
yrityksen kahden
toimipaikan
välillä



Lite 3

Etäyhteys VPN

