Jussi Ervast

MIKKELIN KAUPUNGIN TYÖNTEKIJÖIDEN SAFEMOVE-YHTEYKSIEN KÄYTTÖ

Opinnäytetyö
Tietotekniikan koulutusohjelma

Toukokuu 2013

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

KUVAILULEHTI

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Opinnäytetyön päivämäärä** 13.5.2013
Tekijä(t) Ervast, Jussi	**Koulutusohjelma ja suuntautuminen** Tietotekniikan koulutusohjelma

Nimeke

Mikkelin kaupungin työntekijöiden Safemove-yhteyksien käyttö

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli tutkia Mikkelin kaupungin työntekijöiden Safemove VPN-ohjelman tietoliikenneyhteyksien käyttöä työssään, eli kuinka paljon erilaisia yhteystapoja käytetään ja kuinka tyytyväisiä käyttäjät ovat niiden toimintaan. Työ tehtiin Kuntien Tiera Mikkelin toimipisteelle, joka tarjoaa tietohallintopalveluja Mikkelin kaupungin työntekijöille.

Työn teoriaosiossa perehdytään siihen, mikä VPN on ja miten se toimii käymällä läpi muutamia oleellisia protokollia ja tekniikoita. Lisäksi tutkitaan Kuntien Tieralla käytössä olevan Safemove VPN -ohjelmiston toimintaa tarkemmin.

Käytännön osuudessa lähetettiin asiakaskysely niille Mikkelin kaupungin työntekijöille, joilla on käytössään kannettava tietokone ja siinä Safemove-ohjelma. Kyselyssä kysyttiin erilaisten käyttöpaikkojen osuutta ja yhteyksien toimivuutta niissä, sekä mielipidettä hieman aiemmin suoritetusta 3G-operaattorin vaihdosta. Kysely lähetettiin 436 henkilölle joista 151 vastasi.

Kyselyn mukaan yhteydet toimivat oman työpisteen ulkopuolellakin kohtuullisen hyvin. Eniten ongelmia oli 3G-yhteyksissä. 3G-operaattorin vaihto ei tuonut muutosta tai paransi toimintaa hieman suurimmalle osalle käyttäjistä. Oli kuitenkin pieni osuus käyttäjiä, joilla 3G-yhteydet muuttuivat huomattavasti huonommin toimiviksi.

Asiasanat (avainsanat)

Kyselytutkimus, etäkäyttö, protokollat, tietoliikenne

Sivumäärä	**Kieli**	**URN**
42+2	Suomi	

Huomautus (huomautukset liitteistä)

Liitteessä kyselyrunko

Ohjaavan opettajan nimi	**Opinnäytetyön toimeksiantaja**
Matti Koivisto	Kuntien Tiera Mikkelin toimipiste

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

Date of the bachelor's thesis
May 13, 2013

Author(s)
Ervast, Jussi

Degree programme and option
Information Technology

Name of the bachelor's thesis

The use of Safemove connections by Mikkeli city employees

Abstract

The purpose of this thesis was to study how Mikkeli city employees used Safemove VPN program in their work, how much they used different network connection methods and how well these worked. This thesis was made for Kuntien Tiera Mikkeli office, the provider of IT management services to the city of Mikkeli.

In the theory section of this thesis VPN and some of its protocols were explored as well as how the Safemove program worked. In the practical part, a survey was carried out for those Mikkeli city employees who used laptops and had Safemove installed on it. The survey asked how much they used their computers in different locations, and how the data connections worked there. It also asked how the recently carried out change to another 3G service provider affected the 3G connections. Altogether 151 out of 436 people answered the survey.

According to the survey the network connections worked quite well even outside the workplace, 3G connections being the most problematic. For most users, change to another 3G service provider did not change the connection much or slightly improved it. However, it did affect a small group of people very negatively.

Subject headings, (keywords)

Survey, remote access, protocols, data communications

Pages	Language	URN
42+2	Finnish	

Remarks, notes on appendices

A survey as an appendix

Tutor	Bachelor's thesis assigned by
Matti Koivisto	Kuntien Tiera Mikkeli office

SISÄLTÖ

1 JOHDANTO

Yritysten työntekijöillä on usein tarve päästä käsiksi yrityksen tietojärjestelmiin myös työhuoneensa ulkopuolelta. He voivat viedä kannettavan tietokoneensa mukanaan esim. neuvotteluhuoneeseen, hotelliin tai kotiin. Usein samalla vaihtuu myös yhteystapa verkkoon langallisesta lähiverkkoyhteydestä esim. langattomaan WLAN-yhteyteen tai 3G-yhteyteen. Hyvä ratkaisu tarvittavien etäyhteyksien toteuttamiseen on VPN (Virtual Private Network), joka muodostaa tietoturvallisen virtuaalisen tunnelin käyttäjän tietokoneelta työpaikan verkkoon.

Teen tämän opinnäytetyön Kuntien Tiera Oy:lle, joka tarjoaa tietohallintopalveluita mm. Mikkelin kaupungille. Kaupungin henkilökunnasta noin 450:llä on käytössä Safemove VPN-yhteys, jonka avulla he voivat päästä mistä tahansa käsiksi työpaikkansa tietojärjestelmiin. Käyttäjien kannettaviin tietokoneisiin on asennettu Safemove asiakasohjelma, joka automaattisesti valitsee parhaan saatavilla olevan yhteystavan ja muodostaa ennalta määritellyn VPN-yhteyden.

Opinnäytetyön tarkoitus on tehdä tutkimus Safemove Mobile VPN:n käytöstä ja toimivuudesta. Asiakaskyselystä saadaan tietää, kuinka tyytyväisiä käyttäjät ovat Safemove-yhteyteen ja kuinka tarpeelliseksi he sen kokevat. Kyselystä selviää myös, onko toimivuudessa tapahtunut muutosta hiljattain tehdyn 3G-yhteyden palveluntarjoajan vaihdon seurauksena.

Työn aluksi selvitän, mikä VPN-yhteys on ja kuinka se toimii selvittämällä siinä käytettäviä protokollia ja tekniikoita. Sen jälkeen selvitän Safemove -tuotteen toimintaa. Näiden jälkeen esittelen tutkimukseni Safemove-yhteyksien käytöstä eli asiakaskyselyn ja sen vastaukset. Lopuksi teen yhteenvedon tutkimuksieni tuloksista.

2 VIRTUAL PRIVATE NETWORK

2.1 Yleistä

Virtual Private Network (VPN) tarkoittaa tietoliikenneverkkoa, joka on rakennettu yrityksen yksityiseen käyttöön julkisen verkkoinfrastruktuurin (yleensä Internetin) välityksellä [1, s. 10]. Niitä voidaan käyttää yhdistämään yrityksen toimipaikkojen verkkoja toisiinsa tai esim. yksittäinen etätyöntekijän tietokone työpaikan verkkoon, mikä on käyttäjän kannalta kuin hän olisi kytkeytynyt siihen suoralla pisteestä pisteeseen (point-to-point) yhteydellä [2]. Kolmas, harvinaisin tapa käyttää VPN:ää on kahden tietokoneen välinen yhteys (host-to-host), jota voidaan käyttää esim. etähallittaessa yksittäistä palvelinta [3].

VPN:n käyttö on yleistynyt viime vuosina mm. riittävän nopeiden Internet-yhteyksien leviämisen ansiosta. Toinen syy on joidenkin asiantuntijapalveluiden ulkoistamisen yleistyminen [1, s. 13]. Tässä luvussa käyn läpi VPN:n historiaa ja siinä käytettäviä protokollia ja tekniikoita.

VPN oli alun perin termi, joka viittasi yksityisten puhelinvaihteiden välisiin yhteyksiin yksityisissä puhelinverkoissa. Kaukopuheluoperaattorien välisen kilpailun kiristyessä 1980-luvulla yhdysvaltalainen puhelinyhtiö AT&T kehitti tavan, jolla asiakkaiden kaukana toisistaan sijaitsevat toimipisteet pystyivät soittamaan toisilleen sisäisillä puhelinnumeroilla, jolloin puhelujen hinta oli huomattavasti halvempi kuin aiemmin käytössä olleilla kaukopuhelunumeroilla. Lyhyempien puhelinnumerojen ja halvempien hintojen lisäksi asiakkaat saattoivat myös keskittää puhepostin kaltaisia palveluja, eli käyttää niitä mistä tahansa yrityksen tiloista lyhyellä alanumerolla. [1 s. 29–30.]

Varhaisia virtuaalisia dataverkkoja toteutettiin OSI (Open Systems Interconnection) -mallin siirtokerroksella (kerros 2). Esimerkiksi yritysten toimipisteiden välisessä datakäytössä WAN (Wide Area Network) -protokolla Frame Relayn SVC:illä (Switched Virtual Cirtcuit) ja PVC:illä (Permanent Virtual Circuit) muodostetut verkot voidaan ajatella virtuaalisina yksityisverkkoina. Niissä kytkimet ja runkoyhteydet jaetaan muiden palvelun käyttäjien kesken, mutta jokainen käyttäjä näkee vain oman verkkonsa ja datansa, vaikka ne kulkevat samassa runkoverkossa. [1, s. 45–46.]

Internetin yleistyessä virtuaaliset dataverkot ovat siirtyneet käyttämään enemmän OSI-mallin verkkokerrosta (kerros 3), kuten esim. IPsec käyttää. Nykyään VPN:llä yleensä tarkoitetaan Internetin välityksellä muodostettavia virtuaalisia yksityisverkkoja. Tässä opinnäytetyössä selvitänkin vain tällaista VPN-teknologiaa.

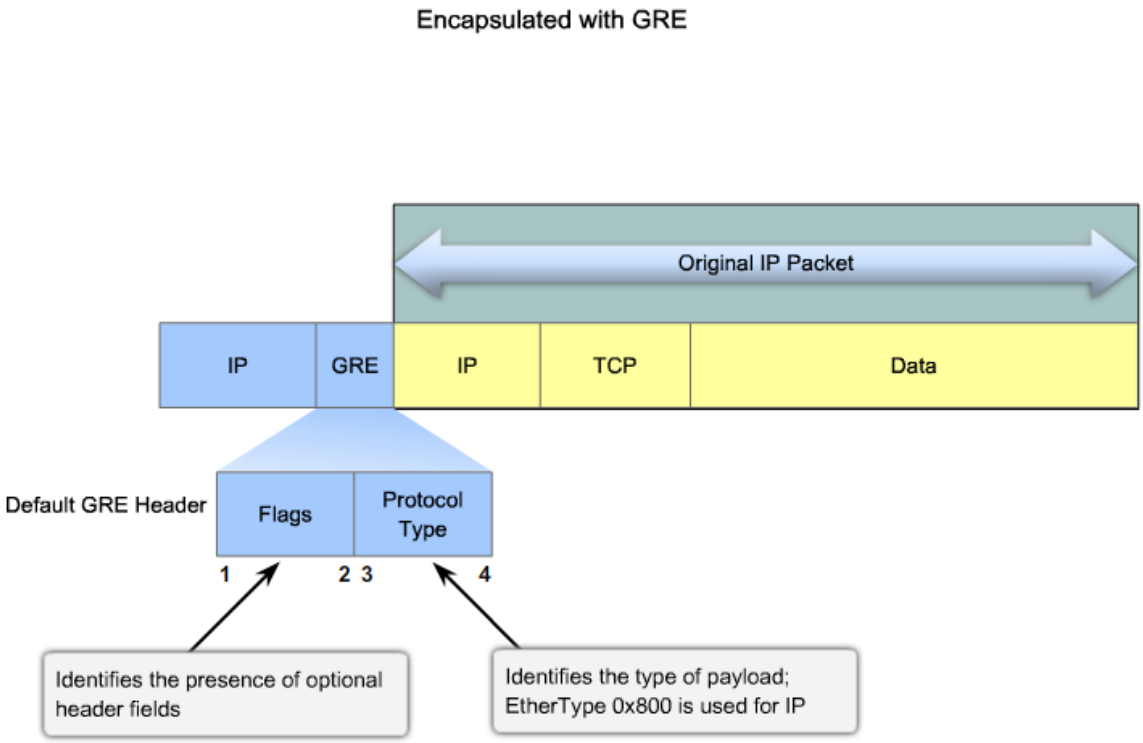
2.2 VPN-protokollat

VPN mahdollistaa datan luottamuksellisuuden, eheyden ja todennuksen. Luottamuksellisuus tarkoittaa sitä, että siirrettävään dataan eivät pääse käsiksi tahot joilla ei ole siihen oikeutta. Tämä saavutetaan tunnelointiprotokollien ja salauksen avulla. Datan eheys tarkoittaa sitä, että tieto pysyy muuttumattomana. Tähän käytetään hash-algoritmeja. Todennuksella eli autentikoinnilla (Authenticating) varmistetaan, että lähettäjä on valtuutettu käyttäjä, mitä varten käytetään esim. erilaisia salasanoja. [4, luku 6.3.4.]

Generic Routing Encapsulation

Generic Routing Encapsulation (GRE) on Ciscon vuonna 1994 kehittämä tunnelointiprotokolla, joka voi kapsuloida useita eri protokollia [1, s. 134] Se käyttää virtuaalisia point-to-point tunneleita IP-verkossa. Se osaa myös kapsuloida multicast-, broadcast- ja IPv6-liikennettä. [5, luku 8.2.1]

GRE-tunnelit ovat tilattomia, eli tunnelin päät eivät erikseen avaa ja sulje yhteyttä tai ylläpidä tietoa siitä, missä tilassa se kulloinkin on. GRE kapsuloi koko alkuperäisen paketin lisäämänsä IP- ja GRE-otsikon sisään (kuva 1). Sen avulla palveluntarjoajat voivat tarjota IP-tunneleita niin, että heidän asiakkaansa voivat muuttaa omaa IP-osoitteestoaan ilman että se vaikuttaa tunnelin toimintaan. [5, luku 8.2.1]

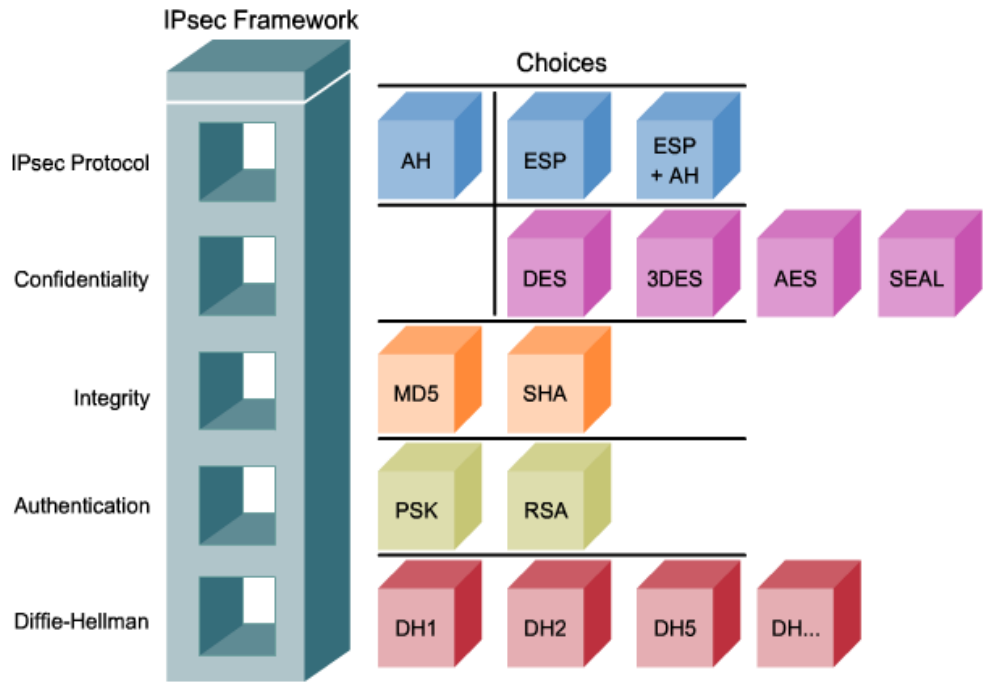


KUVA 1. IP-paketti kapsuloituna GRE:llä [5, luku 8.2.1]

IPsec

IPsec (IP Security) on protokollakokoelma [1s. 106], joka toimii TCP/IP-mallin internetkerroksella, eli OSI-mallissa verkkokerroksella (Kerros 3) [6]. Sitä kehitettiin samanaikaisesti IPv6:n kanssa, mutta koska IPv6 on yleistynyt niin hitaasti, on IPsecistä tullut suosituin tapa suojata IP4-liikenne [7]. Sen ominaisuuksia ovat mm. käyttäjän datan salaus eli kryptaus, viestin eheyden todennus, suoja joitakin hyökkäyksiä vastaan ja se mahdollistaa laitteiden neuvotella tarvittavat tietoturva-algorimit ja avaimet. Siinä on kaksi eri tietoturvatilaa, tunnelointi (tunnel) ja siirto (transport). [6.]

Kun kaksi laitetta (end tai intermediate) haluaa kommunikoida tietoturvallisesti, ne tarvitsevat varmistetun polun (secure path) jota pitkin kommunikointi tapahtuu. Kyseisen polun varrella on useita ei-tietoturvallisia laitteita. Tätä varten niiden pitää sopia mitä tietoturvaprotokollia käyttää, jotta ne ymmärtävät toisiaan, päättää mitä salausalgoritmia käyttää datan salaukseen sekä vaihtaa avaimia, joita käytetään salatun datan avaamiseen. Sen jälkeen kun em. asiat on tehty, täytyy laitteiden vielä lähettää data käyttäen sovittuja metodeja. [6.]



KUVA 2. IPsecin runkorakenne [5, luku 8.3.1]

IPsec muodostuu useista osista (kuva 2). Sen pääprotokollat ovat AH (Authentication Header) ja ESP (Encapsulation Security Payload). Näitä voidaan käyttää myös yhdessä. [1, s. 107.] AH mahdollistaa viestin vastaanottajan tietää, että viesti on pysynyt muuttumattomana eikä viestin lähettäjätietoakaan ole muutettu. Se turvaa myös ns. replay-hyökkäystä vastaan, jossa välillä viestin on vastaanottanut ja lähettänyt uudelleen käyttäjä, jolla ei ole oikeuksia. ESP-protokolla salaa hyötydatan IP-paketissa. [6.]

IPsecin muihin osiin kuuluvat datan luotettavuuden tarjoavat salausalgoritmit. Algoritmin käyttämän avaimen pituus vaikuttaa siihen kuinka vaikeasti murrettava kryptaus on. Tarvittavasta turvallisuustasosta riippuen voidaan valita esim. DES (Data Encryption Standard), 3DES, AES (Advanced Encryption Standard) tai SEAL (Software-Optimized Encryption Algorithm). AH ei tarjoa mahdollisuutta varmistaa datan luotettavuutta. [5, luku 8.3.1.]

Tukeviin osiin kuuluu myös datan eheyden varmistava hash-algoritmi [6]. Se laskee viestin ja jaetun salaisen avaimen perusteella hash-arvon eli tiivisteen, ja vertaamalla ennen lähetystä laskettua arvoa lähetyksen jälkeen samasta viestistä laskettuun, voidaan päätellä, onko data muuttunut matkalla. On mahdollista käyttää useita eri algorit-

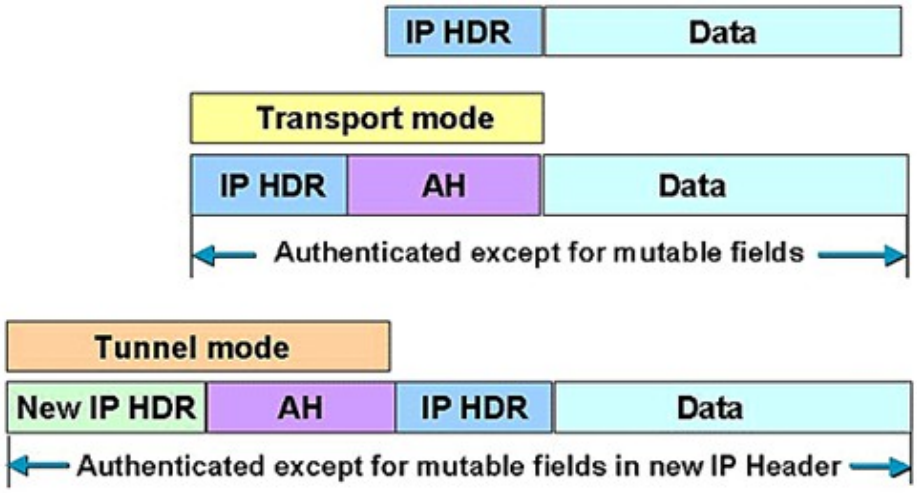
meja, yleisiin kuuluvat esim. MD5 (Message Digest 5) ja SHA (Secure Hash Algorithm). Näistä SHA:ta pidetään vaikeammin murrettavana. Todennuksella (authentication) varmistetaan, että käyttäjällä tai laiteella on riittävät valtuudet päästä käsiksi dataan. Dokumentti allekirjoitetaan lähettäjän digitaalisella allekirjoituksella eli yksityisellä salausavaimella. Allekirjoitus todennetaan avaamalla salaus lähettäjän julkisella avaimella. IPsecissä todennukseen käytetään joko PSK:ta (Pre-shared Keys) tai RSA:ta. [5, luku 8.3.1.]

Muita tukevia osia ovat tietoturvakäytännöt (Security Policies / Security Associations), jotka ovat keinoja, joilla hallitaan tietoturvakäytäntöjä eri laitteiden välillä [6]. Näihin IPsec käyttää esim. IKE (Internet Key Exchange) tai IKE 2 protokollaa [8]. Ne käyttävät Diffie–Hellman -avaimenvaihtoalgoritmeja useiden eri protokollien, kuten DES, 3DES, AES, MD5 ja SHA-1 edellyttämien salattujen avaimien vaihtoon ei-turvallisen verkon yli. Diffie–Hellman -algoritmit on jaettu ryhmiin niiden vahvuuden, eli algoritmin ja niiden käyttämän bittimäärän mukaan. [5, luku 8.3.1.]

IPseciä voidaan käyttää kahdessa eri toimintatilassa, toinen niistä on kuljetustila (Transport mode) joka suojaa vain hyötydatan eli kuorman, tässä tapauksessa data on turvattu koko matkan ajan ja päätepisteiden tietokoneet hoitavat salauksen. Siinä alkuperäiseen otsakkeeseen on lisätty ESP- tai AH-otsake. [9.]

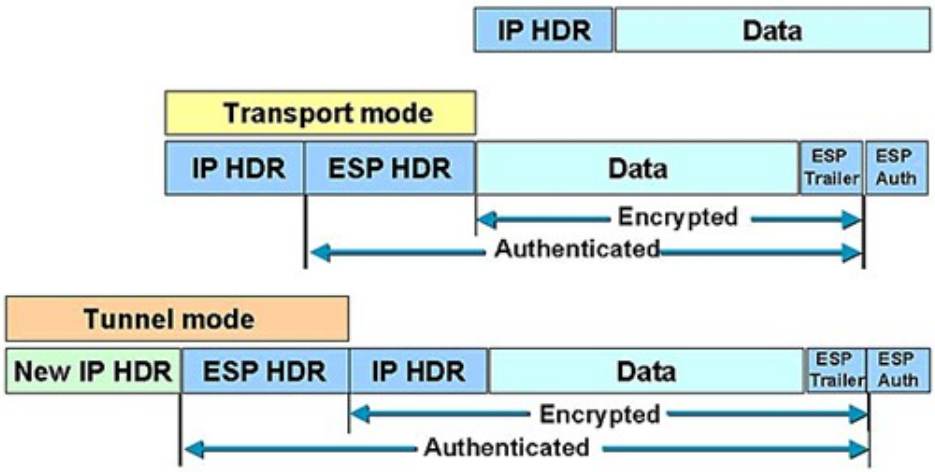
Toinen toimintatila on tunnelointitila (Tunnel mode), jossa koko IP-paketti on salattu, eli alkuperäinen paketti on kapsuloitu kokonaan uuden ulomman IP-paketin sisään. Tässä tilassa päätelaitteet eivät yleensä suojaa dataa, vaan sen tekee jotkin muut laitteet, esim reitittimet, joita kutsutaan tässä tapauksessa VPN-yhdyskäytäviksi (VPN gateway). [9.]

Kuljetustilassa AH suojaa niitä otsikon kenttiä jotka eivät muutu matkan varrella hyötydatan lisäksi. AH sijaitsee IP-otsikon jälkeen. Jos myös ESP:tä käytetään samalla, se tulee AH:n jälkeen. Tunnelointitilassa koko alkuperäinen otsikko todennetaan ja luodaan uusi IP-otsikko. [10.] (Kuva 3.)



KUVA 3. Normaali IP-paketti ja AH kuljetus- ja tunnelointitilassa [11]

Kuljetustilassa ESP salaa hyötydatan eikä muuta alkuperäisiä otsikkotietoja. ESP-otsikko sijaitsee IP-otsikon jälkeen. Alkuperäista IP-otsikkoa ei todenneta. Tunnelointitilassa koko alkuperäinen IP-paketti salataaan ja todennetaan. Myös ESP-otsikko todennetaan, mutta uutta IP-otsikkoa ei todenneta. [10] (Kuva 4.)



KUVA 4. Normaali IP-paketti ja ESP kuljetus- ja tunnelointitilassa [11]

Merkittävin ero AH ja ESP todennuksessa on se, että ESP ei todenna muita IP-otsikoita kuin tunnelointitilassa ESP-otsikon sisään jäävän. [10]

PPTP

PPTP (Point-to-Point Tunneling Protocol) on Microsoftin, ECI/Telematicin, Ascend Communicationsin ja US Roboticsin kehittämä VPN-protokolla. IPsecistä poiketen PPTP:tä voidaan käyttää useiden erilaisten verkkoprotokollien kanssa. [1, s. 115.] Se on PPP-protokollan (Point-to-Point Protocol) laajennus, joka kapsuloi PPP-paketit IP-pakettiin [12]. PPTP toimii OSI-mallin siirtokerroksella (kerros 2).

PPTP käyttää kahta pakettityyppiä, data- ja valvontapaketteja, joista datapaketeissa kulkee varsinainen hyötydata, ja valvontapaketeissa merkinanto- ja tilatiedustelut [1, s.116]. PPTP tunneli luodaan ottamalla yhteys TCP porttiin 1723. Tällä TCP-yhteydellä aloitetaan ja hallitaan toista GRE (Generic Routing Protocol) -tunnelia samaan kohteeseen. [13.] Lopuksi istunto lopetetaan kun PPTP asiakas lähettää valvontapaketin palvelimelle [1, s. 116].

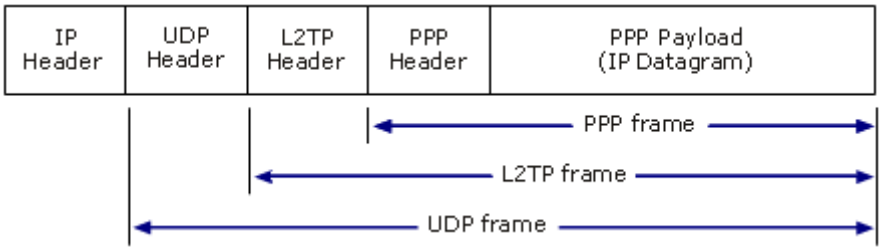
PPTP:n ominaisuuksia ovat esim. kryptaus eli salaus ja käyttäjien todennus. Salaukseen käytetään MPPE (Microsoft's Point-to-Point Encryption) protokollaa, joka käyttää RSA RC4 salausalgoritmia. Alkuperäinen avain luodaan käyttäjän todentamisen yhteydessä ja se regeneroidaan säännöllisesti. Käyttäjien todennuksessa käytetään PPP:n autentikointiprotokollia, kuten PAP (Password Authentication Protocol), CHAPv1 (Challenge-Handshake Authentication Protocol), CHAPv2 tai EAP (Extensible Authentication Protocol). [9.]

PPTP asiakasohjelma on tullut jokaisen Microsoft Windows -version mukana Windows 95:stä lähtien, eli se on erittäin laajasti yhteensopiva. Kuitenkin PPTP:stä on löydetty useita vakavia tietoturvahaavoittuvuuksia, ja lokakuusta 2012 lähtien PPTP:n kryptausta pidetään murrettuna eikä Microsoft suosittele sen käyttämistä enää. Nykyään protokollan kehitys on pysähtynyt, ja sen ominaisuuksia on otettu osaksi L2TP:tä (Layer 2 Tunneling Protocol). [13.]

L2TP

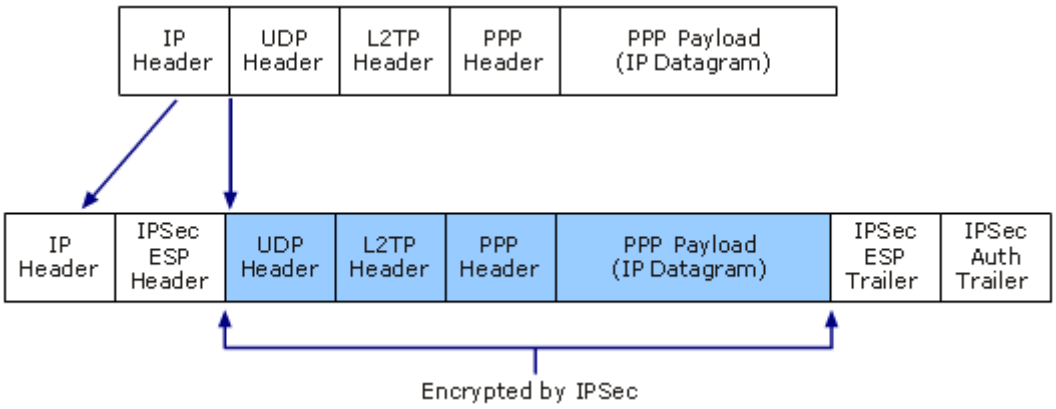
L2TP (Layer 2 Tunneling Protocol) on vuonna 1999 julkaistu tunnelointiprotokolla, jossa on yhdistetty ominaisuuksia kahdesta vanhemmasta protokollasta, PPTP:stä ja

Ciscon kehittämästä L2F:stä (Layer 2 Forwarding) [1. s. 125; 18]. Niinpä siinä on useita yhtäläisyyksiä PPTP:n kanssa. Se käyttää PPP:tä kapsuloidessaan dataa, ja myös sillä on mahdollista paketoida useita eri protokollia. L2TP kapsuloi datan PPP-kehyksiin ja lähettää ne IP-verkossa. L2TP on kuitenkin tietoturvallisempi, koska sitä voidaan käyttää IPsecin kanssa, jonka avulla saavutetaan datan luottamuksellisuus ja eheys sekä käyttäjän todennus. [9.]



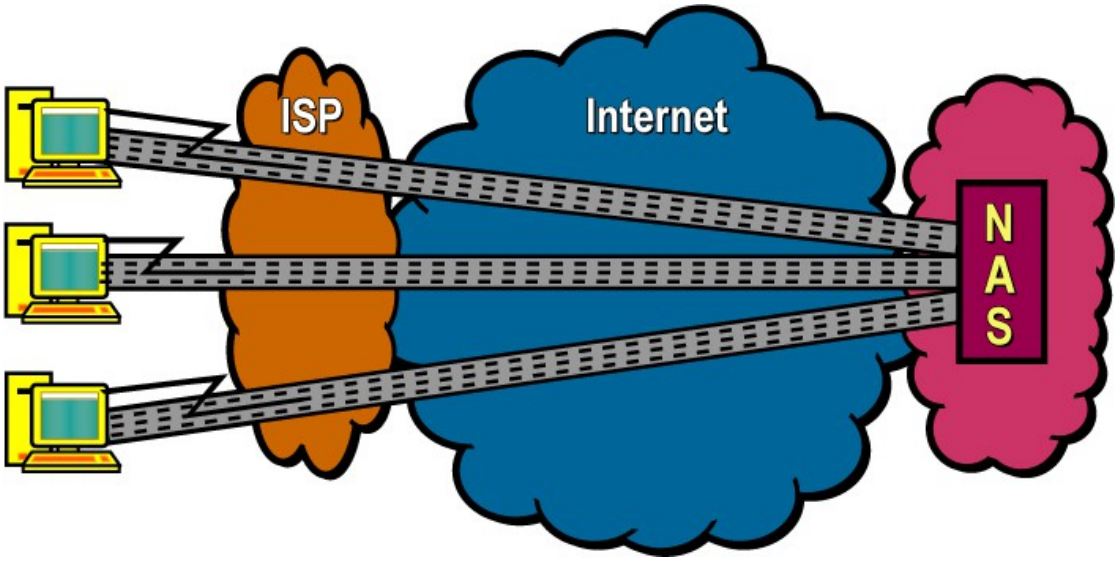
KUVA 5. L2TP-paketin rakenne [14]

L2TP kapsuloi sekä käyttäjän datan että hallintainformaation käyttäen UDP:tä, joka kapsuloidaan IP-pakettiin (kuva 5). Protokolla itsessään ei voi varmistaa datan luottamuksellisuutta tai todennusta, joten sitä usein käytetäänkin IPsecin kanssa (kuva 6). Näiden protokollien yhdistelmästä käytetään tunnusta L2TP/IPsec. [14 & 15.]

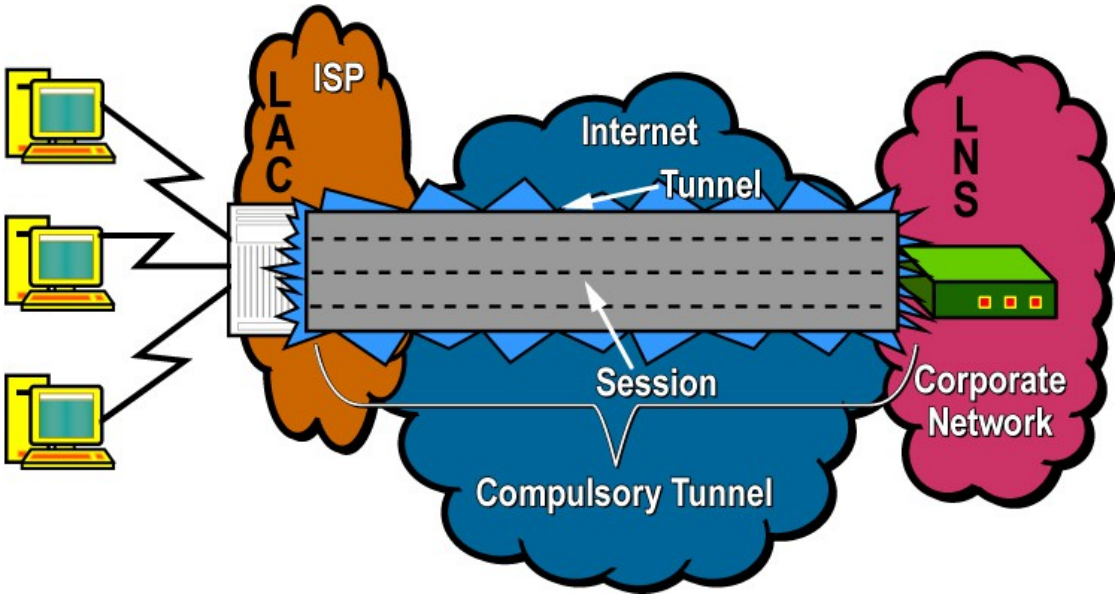


KUVA 6. L2TP-paketti salattu IPsec:llä [14]

L2PT voidaan jakaa kahteen tunnelityyppiin, kuvissa 7 ja 8 esitettyyn vapaaehtoiseen (volyntary) ja pakolliseen (compulsory). Vapaaehtoisessa tunnelissa käyttäjän tietokone ja palvelin ovat tunnelin päätepisteet. Pakollisessa tunnelissa käyttäjän tietokoneen korvaa toisena päätepisteenä jokin sitä ennen oleva laite, kuten etäkäyttöpalvelin. [9.]



KUVA 7. Vapaaehtoinen L2TP-tunneli [16]



KUVA 8. Pakollinen L2TP-tunneli [16]

L2TP-tunnelin päistä käytetään nimiä LAC (L2TP Access Concentrator) ja LNS (L2TP Network Server). LAC aloittaa tunnelin muodostuksen ja LNS on palvelin joka odottaa uutta tunnelia. Kun tunneli on muodostettu, data liikkuu siinä kumpaankin suuntaan. Ylempien kerrosten protokollia suoritetaan L2TP tunnelin läpi. Jokaista tällaista protokollaa varten täytyy avata istunto. L2TP eristää jokaisen istunnon liikenteen, jonka ansiosta yhdessä tunnelissa voi olla useita virtuaalisia verkkoja. Tunnelissa

kulkevat paketit ovat joko data- tai kontrollipaketteja. Protokollassa on ominaisuuksia, joilla kontrollipakettien luotettavuus voidaan varmistaa, mutta ei datapakettien. Niinpä luotettavuus täytyy taata jollain toisella protokollalla. Data- ja kontrollipakettien rakenne on L2TP:ssä sama. [9.]

TLS (Transport Layer Security) ja SSL (Secure Sockets Layer)

TLS (Transport Layer Security) on salausprotokolla, jonka edeltäjä on Secure Sockets Layer (SSL) [17]. Nimeämiskäytännöt näistä protokollista puhuttaessa vaihtelevat, esim. nimi SSL VPN on jäänyt vielä osittain käyttöön, vaikka VPN toteutettaisiinkin sen korvanneella TLS:llä. Protokollat eroavat vain vähän toisistaan [18]. Käytän tässä tekstissä nimitystä TLS/SSL, kun käsittelen molempia protokollia.

Alun perin SSL kehitettiin Netscape-selaimeen WWW-sivujen suojaamiseen, mutta sillä voidaan kapsuloida HTTP:n lisäksi muitakin sovelluskerroksen protokollia, kuten FTP, SMTP, NNTP, POP tai IMAP [19]. TLS/SSL:n ero muihin VPN-protokolliin on se, että se toimii OSI-mallin kerroksilla 4-7, kun VPN-protokollat yleensä toimivat kerroksilla 2 tai 3 [20].

TLS/SSL on IPsec:n ohella yleisimmin käytetty tapa toteuttaa etäkäyttö VPN-hteys. Eräs TLS/SSL:n eduista on helppokäyttöisyys, sitä voidaan käyttää nettiselaimella mistä tahansa tietokoneesta ilman asiakashjelmaa, mistä tahansa paikasta jossa on Internet-yhteys. Sen ansiosta yritysten on helppoa lisätä käyttäjiä, joilla on valtuuksia päästä käsiksi yrityksen verkkoresursseihin. Toisaalta IPsecin etuja ovat laaja tuki eri sovelluksille ja parempi tietoturvan taso esim. todennuksessa ja kryptauksessa. [5, luku 8.6.2.]

TLS/SSL VPN:ssä käyttäjän asiakasasema ottaa yhteyden palvelimen ennalta määritettyyn porttiin ja muodostaa tunnelin siihen, antaa itselleen suljetun verkon IP-osoitteen ja luo virtuaaliverkon asiakasaseman ja palvelimen välille. Protokolla salaa liikenteen näiden välillä. [20]

TLS/SSL VPN mahdollistaa eri tyyppisiä yhteyksiä, ilman asiakasohjelmaa olevan lisäksi voi käyttää eri tasoisia asiakasohjelmia, kuten ohut client (Thin client) ja täysi

client (Full client) joilla voi saada laajemman pääsyn ohjelmiin ja verkkoresursseihin [5, luku 8.6.3].

TLS/SSL VPN:iä on kahta päätyyppiä, SSL Portal VPN ja SSL Tunnel VPN [21]. SSL Portal VPN:ssä otetaan yksi SSL-yhteys nettisivulle, jotta käyttäjä pääsee käsiksi verkkopalveluihin tietoturvallisesti. Siinä on yksi sivu, jota kutsutaan portaaliksi, jonka kautta päästään käsiksi useisiin resursseihin. Etäkäyttäjä ottaa yhteyden SSL VPN yhdyskäytävään, tunnistautuu jollakin yhdyskäytävän tukemista todennustavoista, ja pääsee käsiksi verkkosivuun, joka toimii portaalina muihin palveluihin, jossa on linkkejä muihin palvelimiin, jaettujen tiedostojen hakemistoja, web-pohjaisia sähköpostipalveluita, palvelimella suoritettavia sovelluksia tai mitä tahansa palveluita joita voidaan käyttää nettisivun kautta. Tällaista tunnelia voi käyttää millä tahansa nykyaikaisella verkkoselaimella. [22 & 23.]

SSL Tunnel VPN:ssä käyttäjän nettiselain pääsee tietoturvallisesti käsiksi moniin verkkopalveluihin, myös sellaisiin protokolliin ja sovelluksiin, jotka eivät ole verkkopohjaisia käyttäen SSL:ää käyttävää tunnelia. Tämäntyyppinen tunneli mahdollistaa toiminnallisuutta mikä ei ole mahdollista SSL Tunnel VPN:ssä. Edellytyksenä on, että käytössä oleva nettiselain voi käsitellä aktiivista sisältöä, kuten Java, JavaScript, Active X tai flash -sovelluksia tai plugineja. [22 & 23.]

2.3 Avainten hallinta

VPN-protokollat voivat käyttää erilaisia algoritmeja datan salaukseen eli kryptaukseen. Siirrettävä data salataan lähetettäessä, ja se täytyy saada avattua eli dekryptattua vastaanottopäässä. Sitä varten vastaanottajalla täytyy olla oikeanlainen avain. Niitä tarvitaan myös esim. lähettäjän todennukseen tarvittavien HMAC-funktioiden laskemiseen [5, luku 7.2.3]. Näitä varten lähettäjällä ja vastaanottajalla täytyy olla keino vaihtaa salausavaimia. Tässä luvussa tarkastelen avainten hallintaa. Useimmat hyökkäykset salausjärjestelmiin kohdistuvat juuri avaintenhallintaan, ei itse salausalgoritmiin.

Erilaisia salausavaintyyppejä ovat symmetriset avaimet, jotka voidaan vaihtaa kahden VPN:ää tukevan reitittimen välillä. Asymmetrisiä avaimia käytetään HTTPS:n kanssa.

Hash-avaimia käytetään esim. symmetristen ja asymmetristen avainten luontiin ja digitaalisten allekirjoitusten kanssa. [5, luku 7.2.4.]

Symmetriset salausalgoritmit

Avainten suojelemiseen käytetyt salausalgoritmit voidaan jakaa kahteen perusluokkaan, symmetrinen ja asymmetrinen. Symmetriset avaimet käyttävät samaa ennalta jaettua avainta (pre-shared key) tiedon salaamiseen ja salauksen purkamiseen. Niitä käytettäessä lähettäjä ja vastaanottaja ovat ennalta jakaneet salaisen avaimen. Tällaisia algoritmeja käytettäessä avaimet voivat olla suhteellisen lyhyitä, jonka ansiosta niiden käyttö on nopeaa ja vähän suorituskykyä vaativaa. Symmetrisiä salausalgoritmeja ovat esim. DES, 3DES, AES, SEAL ja RC.
[5, luku 7.3.1] [24]

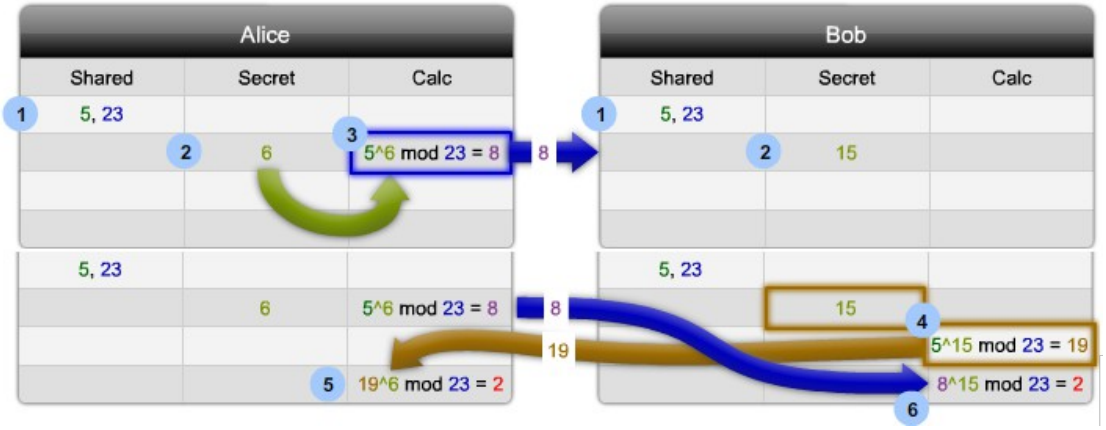
Symmetriset salausalgoritmit voivat käyttää joko lohko- (block cipher) tai jonosalausmenetelmää (stream cipher) [25]. Lohkosalauksessa algoritmi ottaa tietyn kokoisen palan alkuperäisestä viestistä ja salaa sen esim. 64 tai 128 bitin kokoiseksi lohkoksi. Lohkosalausta käyttävistä algoritmeista DES käyttää 64 bitin, AES 128 bitin ja RSA vaihtelevan kokoisia lohkoja. Jonosalauksessa data salataan bitti tai tavu kerrallaan, eli ikään kuin lohkosalaus jossa lohkon koko on yksi bitti. Jonosalausta käyttävät A5, RC4 ja myös DES:ä voi käyttää jonosalaustilassa. Lohkosalauksessa viestin koko voi usein kasvaa, koska alkuperäinen viesti ei välttämättä mene tasan lohkojen koon mukaan, jolloin dataan pitää lisätä keinotekoista dataa. Jonosalaus on yleensä nopeampi menetelmä. [5, luku 7.3.1.]

Asymmetriset salausalgoritmit

Ongelmana symmetrisissä salausalgoritmeissa on avainten hallinta, eli kuinka saada sama salainen avain lähettäjälle ja vastaanottajalle tietoturvallisesti. Asymmetriset kryptausalgoritmit käyttävät eri avaimia tiedon salaamiseen ja salauksen purkamiseen [26]. Niitä käytettäessä ei lähettäjän ja vastaanottajan tarvitse jakaa omia salaisia avaimiaan ennalta käsin, ja sen ansiosta ne ovat symmetrisiä algoritmeja tietoturvallisempia. Avainten täytyy olla paljon pitempiä kuin symmetrisessä kryptausalgoritmeissa, joka aiheuttaa niiden käyttöön hitautta ja suurempia suoritintehovaatimuksia. Asym-

metrisiä kryptausalgoritmeja ovat esimerkiksi RSA, EIGamal ja Diffie–Hellman. Niitä käytetään muutamien eri protokollien kanssa kuten IPsec VPN:n IKE (Internet Key Exchange) komponentissa, TLS/SSL:ssä, SSH:ssa ja PGP:ssä (Pretty Good Privacy). [5, luku 7.4.1.]

Diffie–Hellman -algoritmi on perusta useimmille nykyisin käytössä oleville tavoille suorittaa salausavainten vaihto. Sen avulla kaksi tietokonetta voi luoda yhteisen salaisen avaimen, jota kummankaan osapuolen ei tarvitse missään vaiheessa lähettää toiselle (kuva 9). Kuten asymmetriset algoritmit yleensäkin, Diffie–Hellman käyttää salaisen yksityisen avaimen lisäksi julkista avainta. [5, luku 7.3.6].



KUVA 9. Diffie–Hellman avaintenvaihto [5, luku 7.3.6]

Avainten vaihto etenee kuvaan merkitysti seuraavien kuuden vaiheen kautta:

1. Alice ja Bob sopivat käyttävänsä käyttävät kahta samaa lukua, alkulukua p = 23 ja primitiivistä alkiota g = 5
2. Alice luo salaisen luvun Xa = 6. Bob luo salaisen luvun Xb =15
3. Alice suorittaa DH algoritmin, g^Xa mod p = Ya ; (5^6 mod 23) = 8 = Ya. Tämä luku lähetetään Bobille.
4. Bob suorittaa DH algoritmin, g^Xb mod p = Yb; (5^15 mod 23) = 19 = Yb. Tämä luku lähetetään Alicelle.
5. Alice laskee uuden DH algoritmin Yb^Xa mod p = Z; (19^6 mod 23) = 2
6. Bob laskee uuden DH algoritmin Ya^Xb mod p = Z; (8^15 mod 23) = 2

Kuvassa 9 käytettiin esimerkin vuoksi lukuina p, Xa ja Xb pieniä lukuja, normaalisti ne ovat huomattavasti suurempia [27].

Sopivan pituisen avaimen valinta on tärkeää. Luotettavaa avainta käytettäessä ainoa keino sen murtamiseen on ns. brute-force hyökkäys, jossa kokeillaan kaikkia mahdollisia ratkaisuja kunnes löydetään oikea. Jos avain on riittävän pitkä, kestää oikean ratkaisun löytäminen kokeilemalla keskimäärin aivan liian kauan että se olisi järkevää, jopa miljoonia vuosia nykyisin käytettävissä olevalla prosessoriteholla. Pitkissä avaimissa haittapuolena on niiden vaatima suorituskyky. Niinpä avainta valittaessa täytyy löytää tasapaino turvallisuuden ja suorituskyvyn väliltä. Koska hyökkääjien käytössä oleva suoritinteho ja tieto salausten murtamisesta kasvaa jatkuvasti, täytyy myös käytettävien avainten pidentyä jatkuvasti. [5, luku 7.2.4.]

Hash-algoritmit

Hash-algoritmeja käytetään varmistamaan tiedon eheys, eli että se on pysynyt samana. Siinä viestistä tehdään määritellyn pituinen tiivistetty esitys (Message digest) eli hash matemaattisella funktiolla, joka on suhteellisen helppo suorittaa, mutta jonka laskeminen takaisin alkuperäiseksi viestiksi on äärimmäisen vaikeaa. Datan eheyden varmistamisen lisäksi sitä voidaan käyttää todentamisessa. Toisin kuin samantapaisessa CRC-algoritmissa (Cyclic Redundancy Check), on käytännössä mahdotonta muodostaa kaksi eri viestiä, jotka muodostaisivat saman hashin. Ne ovatkin kuin digitaalinen sormenjälki. [5, luku 7.2.1]. Tarkoituksena on, että hashista ei voi päätellä mitään itse viestin sisällöstä, esim. jos lauseesta muutetaan yksi pieni kirjain isoksi, muuttuu siitä muodostettu hash yleensä aivan erilaiseksi [28].

Hashien avulla voidaan esim. löytää tiedostojen kaksoiskappaleita, havaita tiedoston versiomuutoksia ja havaita onko data korruptoitunut [29]. Niitä käytetään esim. todentamisessa käytettäessä symmetristä salaista todennusavainta, kuten IPsecissä tai reititysprotokollan todennuksessa. Muita käyttökohteita ovat todennusprotokollien, kuten CHAP, kanssa vastausten luominen kysymyksiin. Hasheja käytetään myös varmistamaan tiedon eheys digitaalisesti allekirjoitettujen sopimusten kanssa ja PKI-sertifikaateissa (Public Key Infrastructure) jollaisia käytetään esim. kun otetaan yhteys suojattuun sivustoon verkkoselaimella. [5, luku 7.2.1.]

Hash-algoritmit ovat hyödyllisiä havaitsemaan, milloin data on muuttunut vahingossa, mutta ne eivät havaitse jos sitä on muutettu tarkoituksella. Lähetettäessä viestistä lasketaan hash ja se liitetään viestiin. Jos matkan varrella hyökkääjä saa viestin, muuttaa sitä ja laskee uuden hashin, joka tulee viestiin mukaan, ei vastaanottaja voi päätellä hashista kuka sen on laskenut tai onko viesti muuttunut matkalla. [5, luku 7.2.1.]

Jos hash-algoritmia käytetään yhdessä salaisen avaimen kanssa, voidaan varmistaa tiedon muuttumattomuus ja varmistua lähettäjästä. Sitä kutsutaan HMAC:ksi (Keyed-hash message authentication code). [30.] HMAC:ia käytettäessä lähettäjällä ja vastaanottajalla on sama salainen avain, jota käytetään viestin lisäksi lähtödatana suoritettaessa hash-funktio. Jos vastaanottaja saa laskettua datan ja salaisen avaimen perusteella saman arvon kuin mikä on viestiin liitetty, on viesti pysynyt muuttumattomana ja tiedetään, että sen on lähettänyt taho, jonka kanssa salainen avain on vaihdettu. HMAC perustuu normaaleihin käytössä oleviin hash-funktioihin. Sitä käytetään esim. IPsec VPN:ssä varmistamaan jokaisen paketin lähettäjä ja varmistamaan datan eheys. Tietoturvallisuus riippuu salaisen avaimen pituudesta. Vaihtoehtona HMAC:lle ovat digitaaliset allekirjoitukset. [5, luku 7.2.3.]

Tunnettuja hash-funktioita ovat esim. MD5 ja SHA-1. MD5 on monimutkainen sarja yksinkertaisia binäärioperaatioita, joita suoritetaan minkä tahansa pituiseen dataan ja josta tuotetaan 128-bittinen hash-arvo. Sitä käytetään esim. havaitsemaan onko tiedosto korruptoitunut tai siirto keskeytynyt ja salasanatietokannoissa, jolloin niissä säilytetään vain salasanojen hashit [28]. [5, luku 7.2.1.]

MD5:stä on löytynyt vuonna 2004 heikkous, eli löydettiin tapa luoda kaksi eri data-arvoa, joista muodostuu sama hash. Myöhempinä vuosina algoritmin murtamisessa edistyttiin lisää, eikä sitä pidetä enää kovinkaan tietoturvallisena. Niinpä sitä ei enää suositella käytettäväksi esim. SSL-sertifikaattien tai digitaalisten allekirjoitusten kanssa, koska tällainen haavoittuvuus mahdollistaa niiden väärentämisen. [31.]

SHA-1 on algoritmi, joka muodostaa korkeintaan 2^64 bitin pituisesta datasta 160-bittisen hash-arvon. Se muistuttaa monin tavoin MD5:ttä, koska molemmat kehitettiin samasta MD4 algoritmista. [32.] SHA-1 on hieman hitaampi kuin MD5, mutta myös tietoturvallisempi pidemmän hashin ansiosta. Sitä pidetään MD5:n seuraajana ja käy-

tetään useissa kohteissa esim. TLS/SSL:n, SSH:n ja IPsecin kanssa [33]. SHA:sta on kehitetty myös tietoturvallisempia versiota, jotka muodostavat vielä pidempiä hasheja, kuten SHA-224, SHA-256, SHA-384 ja SHA-512, joista käytetään nimeä SHA-2. [5, luku 7.2.2]

3. SAFEMOVE

3.1 Yleistä

Safemove on Birdstep Technology Oy:n kehittämä VPN-ohjelmisto, jota Kuntien Tiera käyttää Mikkelin kaupungin työntekijöiden VPN-yhteyksissä. Tämä luku perustuu pääosin Birdstepiltä saamaani materiaaliin Safemove 5.6.3 Technical Description [34], lukuunottamatta lukua 3.2 Mobile IP.

Safemove on VPN-ohjelmisto, jonka avulla yrityksen työntekijöillä on mahdollisuus päästä käsiksi työpaikan verkkoon mistä tahansa. Sen pääominaisuudet ovat käyttäjän todentaminen ja tietoliikenneyhteyksien turvaaminen, saumaton liikkuminen eri verkkojen välillä ja keskitetty hallinta. Siinä on pyritty tekemään mahdollisimman helppokäyttöinen, VPN-yhteys muodostetaan ilman mitään toimia käyttäjältä.

Safemove-käyttäjät voivat siirtyä verkosta toiseen, esim 3G-verkosta langattomaan WLAN-verkkoon tai langalliseen LAN-verkkoon, ilman että etäyhteys katkeaa. Ohjelmat säilyvät käytössä, eikä verkon vaihtaminen vaadi minkäänlaista uudelleenkirjautumista. Käyttäjän kannalta ainoa mahdollinen muutos on mahdollinen verkon nopeuden muutos. Safemove käyttää IPsec, IKE ja Mobile IP -standardeja.

Safemoven päätarkoitus on tarjota tietoturvallinen ja saumattomasti toimiva liikkuva yhteys yritysverkkoon niin että se on ylläpitäjien helposti hallittavissa ja käyttäjien helposti käytettävissä. Safemove muodostuu muutamasta komponentista. Ne ovat Birdstep Crypto IP, Birdstep Mobile IP ja Safemove Manager. Birdstep Crypto IP mahdollistaa IP dataliikenteen turvallisuuden käyttäen IPsec VPN -yhteensopivia standardeja. Birdstep Mobile IP mahdollistaa saumattoman liikkuvuuden, eli eri verkkoon siirtyminen on käyttäjälle näkymätöntä. Se on yhteensopiva mobile IP-standardin

kanssa. Safemove Manager mahdollistaa Safemoven integraation yritykseen ja sen komponenttien keskitetyn hallinnan.

Safemoven muihin ominaisuuksiin kuuluvat esim. korkea saatavuus ja kuorman tasaus. Safemove-palvelinta voi käyttää joko yhdellä palvelimella, tai korkeintaan kahdeksan palvelimen klusterissa joka tarjoaa kuorman tasausta ja parantaa saatavuutta. Dynaaminen kuormantasaus ylläpitää tasaista kuormaa kaikilla palvelimilla, joka osaa ottaa varapalvelimen käyttöön täysin käyttäjän huomaamatta. Safemove-palvelin tukee myös useiden kotiagenttien käyttöä, jotka myös parantavat vikasietoisuutta ja eliminoivat pullonkauloja.

Hotspot Login Assistant helpottaa käyttäjiä käyttämään julkisia langattomia WLAN-verkkoja muodostamalla kaikki IPsec ja Mobile IP -yhteydet automaattisesti kun hotspottiin on kirjauduttu verkkoselaimella. Jos langaton WAN-yhteys on saatavilla hotspot-kirjautumista suoritettaessa, käyttäjän yhteys yritysverkkoon säilyy käyttämällä langatonta WAN-yhteyttä kun hotspot kirjautumisprosessi on aktiivinen, ja kun WLAN-autentikaatio on suoritettu, siirrytään käyttämään WLAN-yhteyttä. Etuna moniin muihin VPN-ratkaisuihin on se, että Safemove huolehtii liikkuvan laitteen tietoturvasta myös hotspot-kirjautumisprosessin aikana, eikä käyttäjältä edellytetä mitään toimia sammuttaa tai käynnistää VPN-yhteyttä tai säätää tietokoneen palomuuria.

Safemoven ominaisuuksiin kuuluu myös mahdollisesti vikaantuneiden laitteiden karanteeni. Anti-virus Quarantine ominaisuus havaitsee milloin kannettavan tietokoneen antivirusohjelma tai virustietokanta eivät ole ajan tasalla, ja asettaa henkilökohtaisen palomuurin tilaan jossa se estää pääsyn yritysverkkoon. Tässä tilassa käyttäjällä on pääsy vain palvelimelle, jota käytetään antiviruspäivityksiin. Kun ohjelmisto ja virustietokanta ovat taas ajan tasalla, pääsy sallitaan automaattisesti yritysverkkoon.

Safemoven valinnainen sisäverkon havaitsemisominaisuus tunnistaa milloin käyttäjä ottaa yhteyden yrityksen sisäverkosta ja ottaa asiakasohjelmasta tunneloinnin ja salauksen pois käytöstä parantaakseen suorituskykyä.

3.2 Mobile IP

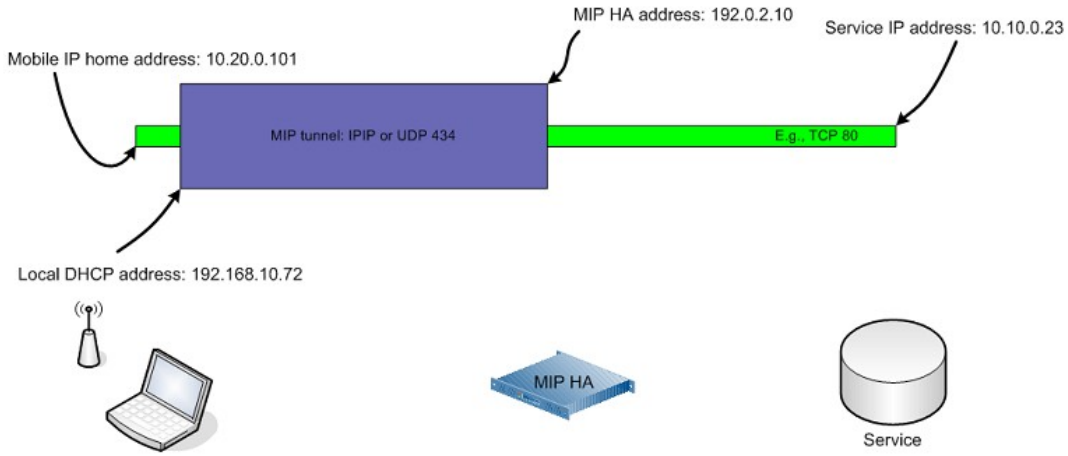
Jotkin Internetiin kytketyt laitteet, kuten kannettavat tietokoneet tai älypuhelimet ovat verkossa liikkuvia. Internet-protokollaa suunniteltaessa sitä ei otettu huomioon. Internet-osoitteet ovat sidottuja laitteisiin, jotka muodostavat Internetin, ja siten sidottuja paikkaan. Kun laite siirtyy eri paikkaan, sen täytyy käyttää toista Internet-osoitetta. Esim. DHCP (Dynamic Host Configuration Protocol) voi asettaa laitteelle uudet IP-asetukset automaattisesti. Langattomien verkkojen yleistyessä on kuitenkin alkanut yleistyä, että langattomassa verkossa oleva laite liikkuu verkkojen välillä saman session, esim. VOIP-puhelun aikana. Jos Internet-osoite vaihtuu, kaikki TCP- ja UDP-sessiot hajoavat. Mobile IP ratkaisee tämän mahdollistamalla sen, että laite säilyttää osoitteensa siirtyessä eri verkkoihin. Safemoven osa joka implementoi Mobile IP:n on nimeltään Birdstep Mobile IP client. [34.]

Liikkuvaa laitetta joka käyttää Mobile IP:tä kutsutaan mobile nodeksi (MN). Se tunnistetaan aina kotiosoitteensa (home address) perusteella, riippumatta mistä se on kytkeytynyt Internetiin. Ollessaan jossain muualla kuin kotiverkossaan, MN saa väliaikaisen osoitteen eli care-of addressin (COA), joka on sen verkon osoite, jossa MN on sillä hetkellä. [35.] Home Agent (HA) sijaitsee MN:n kotiverkossa, ja pitää kirjaa COA:sta. Foreign Agent (FA)sijaitsee vieraassa verkossa, ja se säilyttää tietoa MN:stä joita sen verkossa on. Se myös mainostaa COA:a. [34.]

Kun jokin laite haluaa kommunikoida MN:n kanssa, joka on poissa kotiverkostaan, se lähettää datapaketit MN:n kotiosoitteeseen. HA kapsuloi datan uuteen IP-pakettiin ja ohjaa MN:lle kohdistetun liikenteen sen väliaikaiseen osoitteeseen IP-tunnelia pitkin. [35.] FA avaa paketin ja lähettää sen omassa verkossaan olevalle MN:lle. Tarvittaessa FA toimii oletusyhdyskäytäväreitittimenä MN:lle. Safemoven osa, jossa on HA ja FA -toiminnallisuus on nimeltään Birdstep Mobile IP server. Kun liikkuva laite on kotiverkossaan se käyttää kotiosoitettaan ja toimii samalla tavalla kuin mikä tahansa muu laite IP-verkossa. [34.]

3.3 Safemove tunnelointi

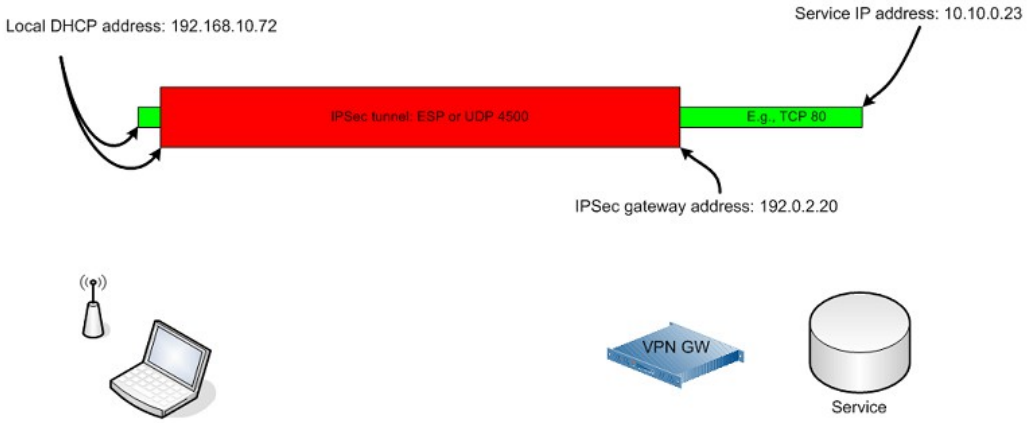
Safemove käyttää Mobile IP:tä. Laite, joka käyttää Mobile IP asiakasohjelmaa (eli Mobile Node), saa kaksi tai enemmän IP-osoitteita. Yhden jokaista aktiivista fyysistä verkkoliitäntää varten, esim. langallinen LAN ja langaton WLAN, ja yhden Mobile IP:lle.



KUVA 10. Mobile IP tunnelointi [34]

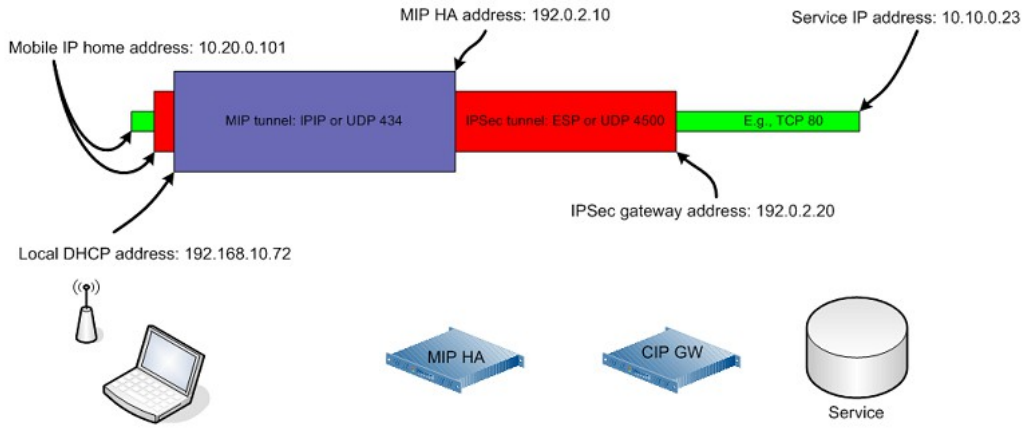
Mobile IP -asiakas rekisteröityy käyttäen fyysistä osoitettaan Mobile IP kotiagenttiin, ja muodostaa Mobile IP -tunnelin. Kun se on muodostettu, sovellukset käyttävät Mobile IP -kotiosoitetta kommunikoidessaan palveluiden kanssa ja liikenne kulkee Mobile IP -tunnelia pitkin. (Kuva 10.)

IPsec tunnelointitilassa VPN:ää käyttävä laite konfiguroidaan tunnelointiasetuksilla. Kun sellaiseen IP-osoitteeseen, joka on asetettu tunneloitavaksi, on liikennettä, VPN-asiakas tulkitsee liikenteen ja aloittaa IKE -neuvottelut toisen VPN päätepisteen eli VPN yhdyskäytävän kanssa. Kun tietoturvallinen tunneli on muodostettu, liikenne kulkee VPN-tunnelissa VPN yhdyskäytävään asti (Kuva 11). Siitä eteenpäin liikenne kulkee kryptaamattomana lopulliseen kohteeseensa. On mahdollista, että sitä ennen liikenne kulkee vielä toisen VPN-tunnelin läpi.



KUVA 11. IPsec tunnelointi [34]

Safemove-tunneloinnissa käytetään sekä Mobile IP:tä että IPsec VPN:ää. Ensin muodostetaan Mobile IP -tunneli asiakkaan ja Safemove-palvelimen, joka toimii Mobile IP HA:na, välille. VPN-suojausta tarvitseva liikenne kulkee käyttäen Mobile IP HA:a Safemove asiakasohjelmasta Safemove-palvelimelle, joka toimii VPN yhdyskäytävänä. (eli Birdstep Crypto IP gateway). VPN yhdyskäytävästä eteenpäin liikenne kulkee suojaamattomana kohteeseensa. (Kuva 12.)



KUVA 12. Safemove tunnelointi [34]

Näin uloin tunneli, eli Mobile IP -tunneli mahdollistaa saumattoman liikkuvuuden Safemove-käyttäjille. Sisempi tunneli, eli IPsec VPN-tunneli toteuttaa vahvan todennuksen ja liikenteen salauksen. Birdstep Mobile IP palvelin ja Birdstep Crypto IP yhdyskäytävä voivat sijaita joko samassa tai eri palvelimissa.

3.4 Safemoven komponentit

Birdstep Mobile IP

Birdstep Mobile IP koostuu kolmesta tuotteesta, client, server ja mobile router. Näistä client ja router käyttävät Mobile Node (MN) -toiminnallisuutta ja server käyttää Home Agent (HA) ja Foreign Agent (FA) -toiminnallisuutta MN:n lisäksi.

HA on käyttäjän kotiverkossa oleva palvelin. Se pitää kirjaa kaikkien liikkuvien käyttäjien sijainnista. Kun liikkuvalle käyttäjälle kohdistettu liikenne saapuu kotiverkkoon, HA ohjaa liikenteen käyttäjän sen hetkiseen sijaintiin käyttäen IP-tunnelia. Se saattaa joutua hallitsemaan satojen tai tuhansien käyttäjien liikennettä reaaliajassa, joten siltä edellytetään paljon suorituskykyä.

FA on reitittävä komponentti, joka mahdollistaa liikkuvan käyttäjän käyttää Mobile IP:tä vieraassa verkossa. Se voi sallia tai estää pääsyn ja se myös sisältää kirjanpito- ja laskutustietoa. FA:n käyttö ei ole välttämätöntä Mobile IP:tä käytettäessä, mutta se tekee protokollan toiminnan tehokkaammaksi ja mahdollistaa verkon tilinhallinnan ja liikenteen hallinnan. Sitä voidaan suorittaa heikkotehoisellakin laitteistolla ja se voi toimia myös reitittimessä tai langattomassa access pointissa.

MN on ohjelmistokomponentti, joka on asennettu liikkuvaan laitteeseen, kuten kannettavaan tietokoneeseen. Kun MN havaitsee muutoksen sijainnissaan, rekisteröi se uuden sijaintinsa HA:in.

Mobile Router (MR) on kuten Mobile Node joka pystyy reitittämään kokonaisen verkon takanaan. Eli kun MR liikkuu toisen sijaintiin verkossa, koko siihen liittynyt verkko vaihtaa sen mukana sijaintiaan.

Birdstep Crypto IP

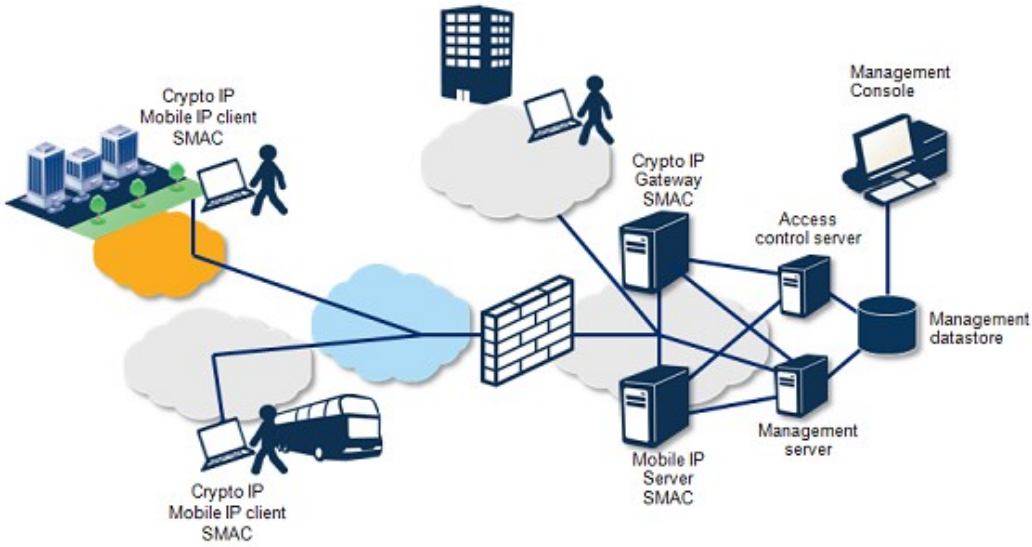
Birdstep Crypto IP tarjoaa käyttäjille turvallisen pääsyn yrityksen verkkoon ja suojelee liikennettä verkon sisä- tai ulkopuolelta tulevia hyökkäyksiä vastaan. Sen toimintoja ovat myös käyttäjien todennus ja pääsyn hallinta. Sen avulla voidaan yhdistää

kaukana olevia laitteita olemassaoleviin verkkoihin julkisten verkkojen yli. Pakettien sisältö on suojattu ja sekä lähettäjä että vastaanottaja todennetaan. Birdstep Crypto IP muodostuu kahdesta osasta. Birdstep Crypto IP gateway salaa yhteydet ja Birdstep Crypto IP client on VPN client-ohjelma.

Birdstep Crypto IP tukee IKE-standardia todennuksessa. Sitä käytetään IPsec:ssä tietoturvakäytäntöjen (Security associations) neuvottelussa. IKE toimii kahdessa vaiheessa. Ensimmäisessä vaiheessa muodostetaan turvallinen kaksisuuntainen yhteys avainten luontiin ja vaihtoon, ja toisessa vaiheessa osapuolet neuvottelevat yleiset kommunikaatiossa käytettävät tietoturvakäytännöt.

Safemove Manager

Safemove Managerilla voidaan hallita ja tarkkailla kaikkia Safemoven komponentteja. Se koostuu Birdstep Management Server:stä ja useista auttavista client-komponenteista. Se koostuu neljästä komponentista, Birdstep Network Enablerista, Safemove Management Agentista (SMAC), Birdstep Management Serveristä ja Birdstep Easy Setupista (Kuva 13). Näitä komponentteja voidaan käyttää myös erikseen muiden kolmannen osapuolen järjestelmänhallintatyökalujen kanssa.



KUVA 13. Safemove Manager -arkkitehtuuri [34]

Birdstep Management Server on palvelinohjelmisto, joka mahdollistaa Safemoven komponenttien hallinnan ja tarkkailun. Se on jaettu komponentteihin, joka mahdollistaa eri hallintatoimintojen suorittamisen yhdellä ytimellä. Silloin etuna on se, että sama binääripaketti asennetaan kaikkiin palvelimiin ja valitut ominaisuudet voidaan kytkeä käyttöön tai pois käytöstä tarpeen mukaan. Tavoitteena on yksinkertaistaa palvelimen käyttöönottoa ja hallintapalveluiden ylläpidon mukautuvuus.

Birdstep Management Serverin ominaisuuksia ovat hallintatehtävien jako Safemove Management Agenteille sekä Safemove-asiakkaiden tilan tarkkailu ja reaaliaikainen liitettävyys. Sen lisäksi se säilyttää ja jakaa ohjelmistopäivitykset ja asetukset sekä hallinnoi Birdstep Crypto IP -yhdyskäytäviä ja Birdstep Mobile IP -palvelimia. Sen toimintoja ovat myös tilastotiedon kerääminen ja raporttien tekeminen.

Access Control Service (ACS) on järjelmä, joka ylläpitää VPN-käyttäjien ja -laitteiden käyttöoikeuksia. Esimerkiksi Active Directoryä käytettäessä asiakkaiden sertifikaatit on liitetty AD käyttäjiin tai tietokoneen tileihin, ja pääsy on sallittu vain jos käytetty tili löytyy eikä sitä ole poistettu käytöstä. Rajoitetun pääsyn kohteisiin pääsee sen mukaan mihin AD ryhmään käyttäjä kuuluu. Tämän ansiosta jos esim. kannettava tietokone on varastettu, voidaan käyttäjän tili poistaa käytöstä Active Directoryssä, jolloin IPsec-yhteydet laitteesta eivät enää onnistu. Jos tietokone saadaan takaisin, tili saadaan helposti otettua takaisin käyttöön.

Kun VPN asiakasohjelma ottaa yhteyden Crypto IP VPN yhdyskäytävään, sen sertifikaatista tarkistetaan että se on saatu luotettavalta Certificate Authorityltä (CA), että se on voimassa ja että se ei ole Certificate Revocation Listillä (CRL) eli sitä ei ole kuoletettu. Jos yhdyskäytävä on asetettu käyttämään ACS:ä (Access Control Service), se pyytää siltä käyttöoikeutta.

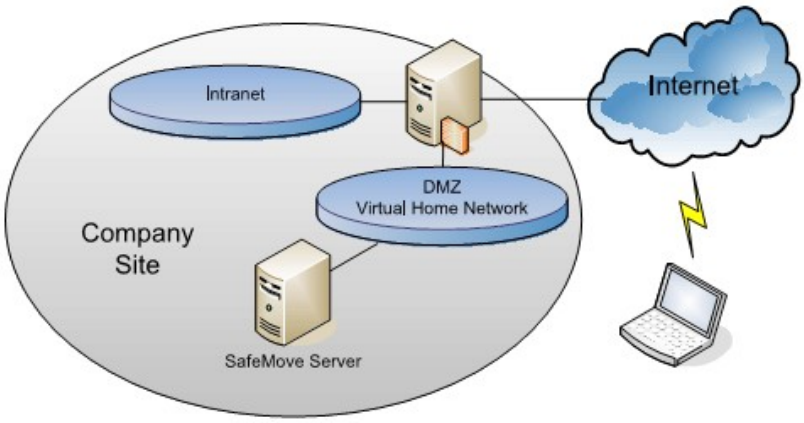
Birdstep Network Enabler on ohjelma, joka integroituu Safemove client-ohjelmaan ja sen ominaisuuksia ovat esim. viruskaranteeni, hotspot-kirjautumisavustaja ja sisä/ulkoverkon tunnistaminen. Ohjelma tarkkailee Birdtep Mobile IP -palvelun ja muiden lähteiden, kuten Windowsin Security Centerin anti-virus API:n tiloja. Niiden perusteella Network Enabler voi suorittaa erilaisia toimintoja, kuten muuttaa Birdstep Crypto IP -profiilia tai Birstep Mobile IP:n tilaa. Ohjelmassa on myös hotspot -kirjau-

tumisavustaja, jonka avulla käyttäjä voi tietoturvallisesti ohittaa selaimen välityspalvelinasetukset ja VPN ja Mobile IP -tunnelit ja -käytännöt verkkopohjaisen verkkoon kirjautumisen aikana.

Safemove Management Agent (SMAC), on taustaprosessina suoritettava palvelu hallituissa laitteissa, kuten Safemove asiakkaissa ja palvelimissa. Sen päätarkoituksia ovat ohjelmiston päivittäminen ja asentaminen hallituissa laitteissa, Safemoven komponenttien konfigurointi ja raporttien kerääminen ja niiden toimittaminen hallintapalvelimelle. SMAC muodostaa käyttöönotettaessa automaattisesti yhteyden Birdstep Management Serveriin.

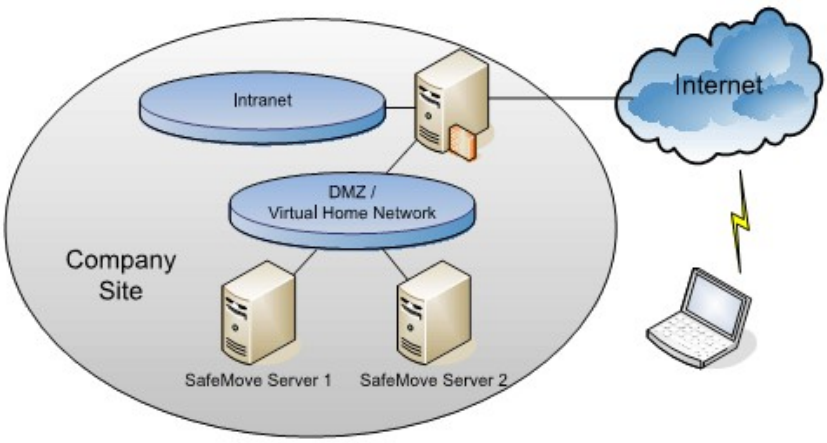
3.5 Safemove-palvelinten tyyppejä

Safemove-palvelin tukee kolmea eri asetustyyppiä, Basic, Failover ja Cluster. Basicissa on vain yksi palvelin (kuva 14), muut tyypit käyttävät useaa palvelinta saavuttaakseen korkean saatavuuden ja kuorman tasauksen.



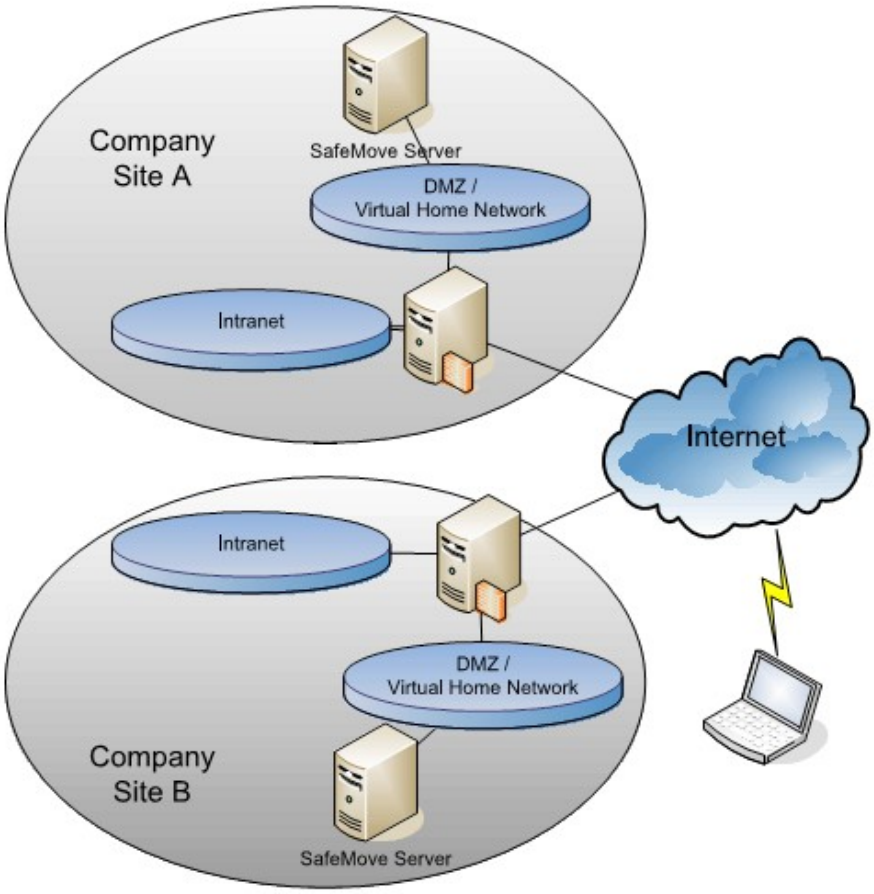
KUVA 14. Safemove Basic [34]

Failoverissa on kaksi palvelinta, jotka voivat sijaita samassa (kuva 15) tai eri paikoissa (kuva 16).



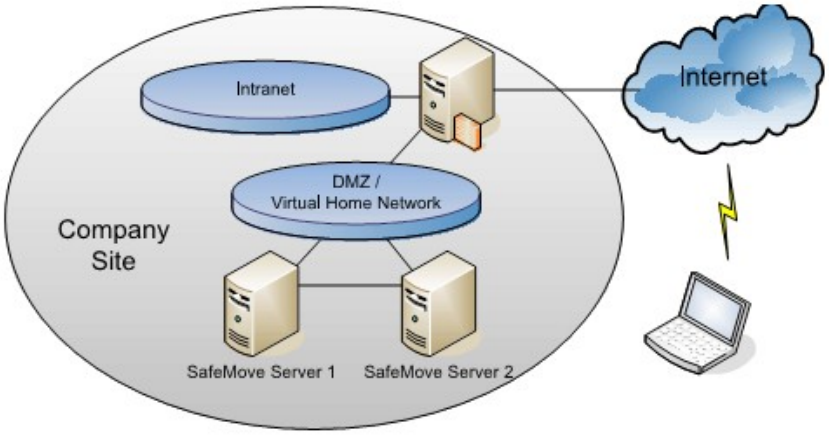
KUVA 15. Failover, palvelimet yhdessä paikassa [34]

Eri paikkoihin sijoittamalla saavutetaan parempi saatavuus jos esim. toisessa yrityksen palvelimen sijainneista olisi verkko-ongelmia. Asiakasohjelmat valitsevat automaattisesti palvelimen, joka oli lähin ohjelman käynnistyessä



KUVA 16. Failover, palvelimet eri paikoissa [34]

Cluster-mallissa käytetään neljää Safemove-palvelinta, joiden täytyy olla samassa aliverkossa (kuva 17). Kaksi niistä toimii Mobile IP Home Agenttina ja kaksi suorittaa VPN:ää. Tässä mallissa palvelimet jakavat toistensa tilatiedot asiakkaiden yhteyksistä, jonka ansiosta vikasietoisuus toimii nopeammin kuin Failover-mallissa.



KUVA 17. Cluster [34]

4. ASIAKASKYSELY

4.1 Yleistä

Tämän työn toimeksiantaja oli Kuntien Tiera Mikkelin toimipiste. Aikaisemmin se toimi nimellä Etelä-Savon tietohallinto Oy, joka muodostettiin vuonna 2007, kun Mikkelin kaupungin tietohallintopalvelut ulkoistettiin. Heidän asiakkaitaan ovat Hirvensalmen, Kangasniemen, Mäntyharjun, Puumalan ja Ristiinan kunnat, Mikkelin ja Pieksämäen kaupungit sekä Etelä-savon sairaanhoitopiiri, Etelä-savon koulutuksen kuntayhtymä ja Mikkelin ammattikorkeakoulukuntayhtymä. Sen lisäksi heidän asiakkaisiinsa kuuluu osin Mikkelin kaupungin konserniin kuuluvia tytäryhteisöjä (liikelaitokset ja osakeyhtiöitä). Kuntien Tiera Oy, joka tarjoaa tietohallintopalveluja mm. useille eri kunnille, osti Etelä-Savon tietohallinto Oy:n koko osakekannan vuonna 2011. [36.]

Kuntien Tiera oli ottanut Safemoven käyttöönsä jo joitakin vuosia aiemmin, mutta siitä ei ollut tehty vielä minkäänlaista asiakaskyselyä miten se on toiminut tai ovatko käyttäjät pitäneet sen käytöstä, ja kuinka paljon tarvetta tällaisille VPN-yhteyksille on.

Kyselyn tavoitteena oli siis selvittää Safemoven käyttäjien tietoliikenneyhteyksien käyttö eri käyttöpaikoissa ja niiden toimivuus asiakkaiden näkökulmasta.

Kysymykset laadittiin toimeksiantajan toiveiden mukaisiksi yhteistyössä Kuntien Tieran Mikkelin toimipisteen toimitusjohtajan Jarmo Tiaisen kanssa. Oli tärkeätä muotoilla kysymykset siten, että ne ymmärtää helposti myös muut kuin tietotekniikan ammattilaiset. Esim. tuotteen nimi Safemove ei olisi ollut useimmille käyttäjistä tuttu, onhan sen idea olla käyttäjän kannalta näkymätön, eli se ei vaadi mitään toimenpiteitä VPN-yhteyden muodostamiseksi. Safemove myös osaa vaihtaa automaattisesti esim 3G-yhteydestä WLAN-yhteyteen, kun nopeampi yhteys tulee tarjolle. Niinpä kyselyssä kysyttiin yleisesti tietoliikenneyhteyksien toimivuudesta ja käytöstä eri paikoissa. Mikkelin kaupungin käyttämä 3G-yhteyksien palveluntarjoaja oli vaihdettu hieman aikaisemmin, joten myös mielipiteitä siitä oli luontevaa kysyä tässä kyselyssä. Oli myös tärkeää pitää kysely lyhyenä niin että mahdollisimman moni vastaisi siihen.

Kyselyissä halutaan tietysti mahdollisimman suuri määrä vastaajia, jotta vastaukset edustavat mahdollisimman hyvin koko käyttäjäjoukkoa. Tässä kyselyssä käytettiin muutamia eri keinoja vastaajien osuuden kasvattamiseksi.

Kysely pidettiin lyhyenä, ja siitä mainittiin saateviestissä, eli että kyselyyn ei mene montaa minuuttia työajasta. Jarmo Tiainen kirjoitti saateviestin sähköpostiin, jossa on linkki kyselyyn. Viestissä kerrottiin, miten Tiera pyrkii parantamaan palveluaan ja että kysely auttaa heitä siinä tehtävässään. Monet vastaajista tuntevat hänet, ja tämä tunnettavuus saattaa tuoda lisää vastaajia. Vastaamiseen annettiin aikaa noin kaksi viikkoa, niin että siihen voi vastata vaikka juuri silloin kun kyselykutsu lähetettiin olisikin kiireinen. Kun oli viikko vastausaikaa jäljellä, niille jotka eivät olleet vielä vastanneet lähetettiin ajastettu muistutusviesti, jossa oli linkki kyselyyn.

Kysely lähetettiin niille Mikkelin kaupungin työntekijöille, joilla oli Safemove käytössään kannettavassa tietokoneessaan. Tällaisia henkilöitä oli 436, joista 151 vastasi, eli vastausprosentti on 35. Kysely toteutettiin 7.6.2012 – 25.6.2012, ja muistutusviesti lähetettiin 19.6.2012.

Kysely toteutettiin Webropolilla, joka on verkkoselaimella toimiva Internet-pohjainen kyselyohjelma. Kysely tehtiin käyttäen Tieralta saatua käyttäjätunnusta, minkä ansiosta kysely ja sen tulokset ovat jatkossakin heidän käytettävissään. Kun kysymykset oli laadittu, testattiin kyselyn lähettämistä Tieran työntekijän sähköpostiin. Kävi ilmi, että testilähetyksissä ne jäivät roskapostifiltteriin. Ongelma ratkesi varsin helposti, kun käytettiin pidempää saateviestiä pelkän linkin lisäksi, jolloin sitä ei enää tulkittu roskapostiksi.

4.2 Kysymykset ja tulokset

Kyselyssä on seitsemän kysymystä, joista yksi vapaa tekstikenttä ja muut monivalintakysymyksiä, joissa valitaan viidestä vaihtoehdosta sopivin (Liite 1). Monivalintakysymykset ovat pakollisia, mutta niissä on viiden vastausvaihtoehdon lisäksi myös ”En osaa sanoa / En tiedä” -valinta. Kaikilla vastaajistahan ei ole esim. 3G-yhteyttä käytössään, joten he eivät voi tietää sen toimivuudesta. Useimmissa monivalintakysymyksissä on lisäksi kommenttikenttä, johon voi halutessaan kirjoittaa kommentteja.

Ensimmäinen kysymys on vapaa tekstikenttä, jossa kysytään oman työpisteen tai työaseman pääasiallisen käyttöpaikan osoitetta. Tämän avulla voi päätellä, onko jossain tietyssä käyttöpaikassa verkon toimivuudessa puutteita. Webropolissa on mahdollista suodattaa vastauksia, esim. esiintyykö vastauksessa Raatihuoneenkatu 8-10, jolloin näkee vain niiden vastaukset, joiden työpaikka on kaupungintalolla. Webropolissa olisi myös mahdollista toteuttaa kysymys alasvetovalikkona, josta valita oikea vastausvaihtoehto, mikä olisi usein käyttäjäystävällisempi vastaustapa. Tässä tapauksessa sitä ei käytetty, koska Mikkelin kaupungilla on useita eri toimipaikkoja, ja lista olisi ollut epäkäytännöllisen pitkä. Siitä oikean osoitteen etsiminen ja valitseminen olisi työläämpää kuin katuosoitteen kirjoittaminen. Tätä kysymystä ei asetettu pakolliseksi, koska joillakin kyselyn saaneista ei ole varsinaista työpistettä tai pääasiallista käyttöpaikkaa.

Toisena kysymyksenä kysytään arvioita prosentteina, kuinka paljon käyttää työasemaa eri käyttöpaikoissa. Käyttöpaikkoja ovat oma työpiste, neuvotteluhuone, koti, ”hotspot”, ja muu. Hotspotilla tarkoitetaan WLAN-yhteyspaikkaa. Muu voi tarkoittaa esim. hotellia. Tässä kysymyksessä ei varsinaisesti mainita verkkoyhteyksiä tai Safemovea

tai VPN:ää, koska kysemykset haluttiin pitää mahdollisimman ei-teknisinä. Kuitenkin käytännössä aina, kun työasemaa käytetään, tarvitaan verkkoyhteyksiä työpaikan verkkoon, jo kirjautumisessa ja muutenkin sähköpostit ja omat tiedostot sijaitsevat verkossa. Tämä kysymys asetettiin pakolliseksi, ja siten että ohjelma antaa virheilmoituksen lopussa vastauksia lähetettäessä, jos prosenttilukujen summa ei ole sata.

TAULUKKO 1. Arvioi minkä verran keskimäärin käytät työasemaasi eri käyttöpaikoissa prosentteina.

	Minimiarvo	Maksimiarvo	Keskiarvo	Mediaani
Oma työpiste	0	100	72,88	80
Neuvotteluhuone	0	90	8,46	5
Koti	0	90	9,65	5
"Hotspot"	0	50	1,72	0
Muu	0	50	7,19	1

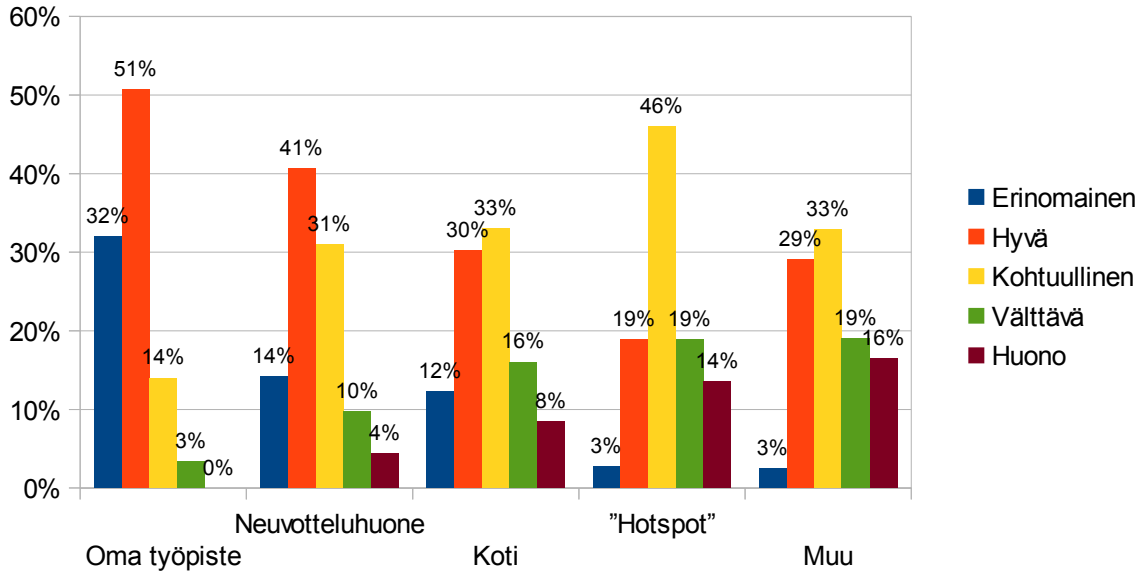
Selvästi eniten työasemaa käytettiin omassa työpisteessä, kuten oli olettavaa. Muissa paikoissa käytettiin keskimäärin alle 10 % ajasta. Kaikkein vähiten käytettiin vapaasti käytettävissä olevissa WLAN-hotspoteissa. (Taulukko 1.)

Kolmannessa kysymyksessä kysytään tietoliikenneyhteyksien toimivuudesta eri käyttöpaikoissa. Tässäkin kysymys piti asetella siten, että kaikki vastaajat ymmärtävät sen. Käyttöpaikat ovat samat kuin edellisessä kysymyksessä ja viisi vaihtoehtoa toimivuudelle erinomaisesta huonoon. Lisäksi vaihtoehtona on jokaisessa ”En käytä / En osaa sanoa” -vaihtoehto, jota ei lasketa tuloksiin. Loppuun on laitettu vielä tekstikenttä, johon voi kirjoittaa vapaasti omia kommentteja. Monivalintakysymys on pakollinen, mutta omat kommentit eivät. Tämän kysymyksen tulokset ovat taulukossa 2.

TAULUKKO 2. Kuinka arvioisit työasemasi tietoliikenneyhteyksien toimivuutta eri käyttöpaikoissa? Keskiarvolaskussa erinomainen = 5, huono = 1.

	Erinomainen	Hyvä	Kohtuullinen	Välttävä	Huono	Yhteensä	Keskiarvo
Oma työpiste	48	76	21	5	0	150	4,11
Neuvotteluhuone	16	46	35	11	5	113	3,5
Koti	13	32	35	17	9	106	3,22
"Hotspot"	1	7	17	7	5	37	2,78
Muu	2	23	26	15	13	79	2,82
Yhteensä	**80**	**184**	**134**	**55**	**32**	**485**	**3,29**

Kuvassa 18 havainnollistetaan taulukon 2 tuloksia pylväskaaviossa, jossa arvosanojen osuus eri käyttöpaikoissa on prosentteina. Näin eri käyttöpaikkoja voi verrata toisiinsa vaikka niissä on eri määrä vastaajia.



KUVA 18. Kuinka arvioisit työasemasi tietoliikenneyhteyksien toimivuutta eri käyttöpaikoissa?

Omassa työpisteessä tietoliikenneyhteydet, eli useimmiten langallinen LAN-yhteys, toimivat kaikkein parhaiten, yli 80 % mukaan joko erinomaisesti tai hyvin. Vain viidellä vastaajalla yhteydet toimivat välttävästi, huonosti ne eivät toimineet yhdelläkään. Tätä käyttöpaikkaa arvioi 150 vastaajaa, eli lähes kaikki vastaajista.

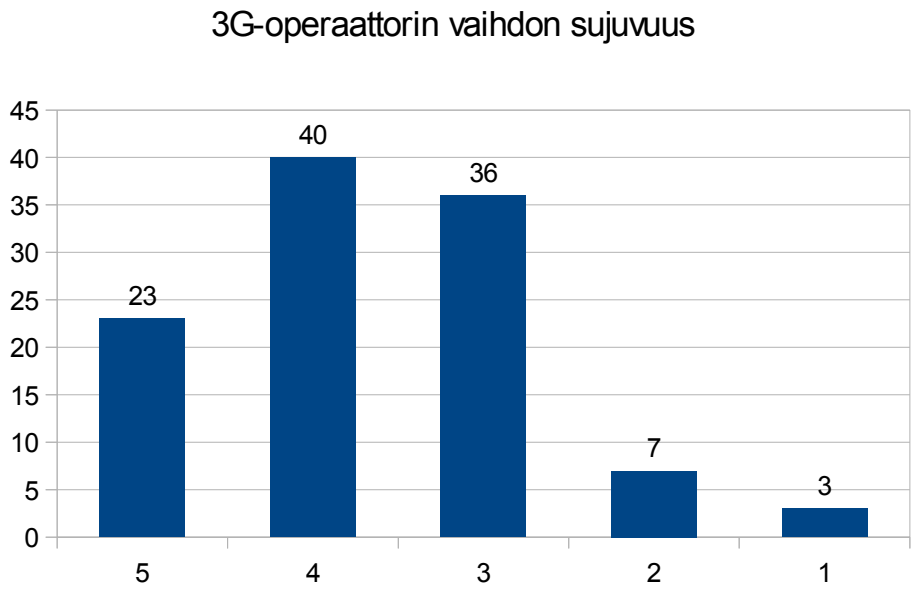
Neuvotteluhuoneessa yhteyksien laadusta vastasi 113 vastaajaa eli noin kolme neljännestä. Siellä käytettävä yhteys on useimmiten WLAN. Sen toimivuutta ei pidetty aivan yhtä hyvänä kuin omassa työpisteessä, mutta sielläkin alle 15 prosentilla toimivuus oli huono tai välttävä. Valtaosan mielestä yhteys neuvotteluhuoneissa toimi joko hyvin tai kohtuullisesti.

Kotoa käsin yhteydet toimivat hieman huonommin kuin neuvotteluhuoneista, mutta kuitenkin melko hyvin saaden keskiarvoksi 3,22 asteikolla 1–5. Kotona ihmisillä on tietysti vaihtelevia yhteystapoja, esim. osalla oma ADSL-yhteys ja osalla 3G-yhteys. Vastaajista 106 vastasi tähän.

Langattomien yhteyksien hotspottien laadusta vastasi 37 vastaajaa, eli noin 25 prosenttia. Pääosin vastaajat pitivät yhteyttä niistä kohtuullisena. Kommenteista käy ilmi, että kaikki eivät ymmärtäneet mitä käyttöpaikka ”Hotspot” tarkoittaa, eli sen olisi voinut ehkä nimetä toisin, esim. WLAN-hotspot, tai vaihtoehtoisesti antaa selityksen siitä mikä se on kysymyksen yhteydessä. Sama muutos olisi kannattanut tehdä myös edelliseen kysymykseen.

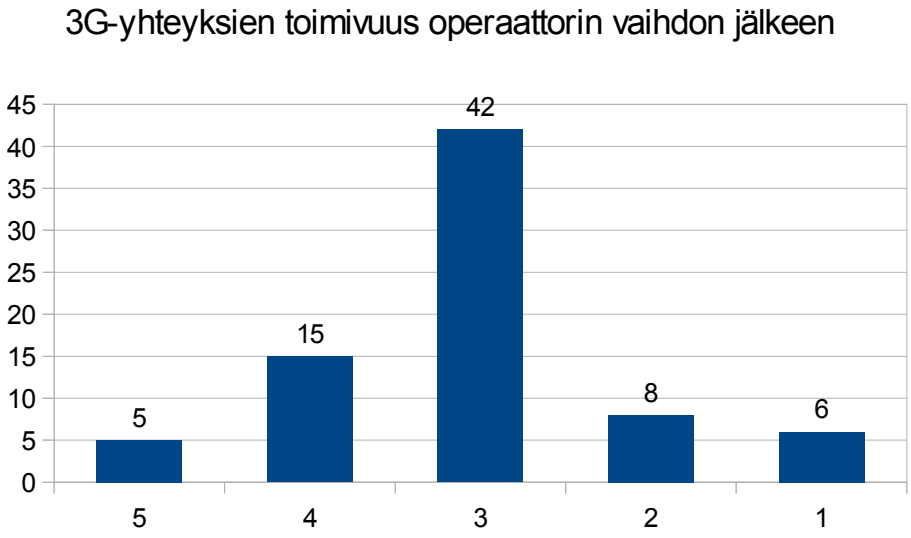
Vastaajista 79 eli hieman yli puolet arvioi yhteyttä muissa käyttöpaikoissa. Näissä yhteys arvioitiin keskimäärin noin saman laatuiseksi kuin WLAN-hotspoteissa, mutta suurempi osuus vastaajista vastasi sekä hyvä että välttävä. On tietenkin luontevaa, että vastaukset jakautuvat tasaisemmin, koska kohtaan ”Muu” sisältyy monia erilaisia käyttöpaikkoja.

Neljäs ja viides kysymys ovat toisiinsa liittyviä. Niissä kysyttiin 3G-tietoliikenneoperaattorin vaihdosta, miten itse vaihto sujui ja onko yhteyden laatu muuttunut sen jälkeen. Molemmissa kysymyksissä käytettiin samanlaista viiden portaan valintaa ja mahdollisuutta vastata ”En tiedä / En osaa sanoa”, ja kummassakin on valinnainen tekstikenttä omia kommentteja varten.



KUVA 19. Kun työasemien 3G-tietoliikenneoperaattori vaihdettiin keväällä Elisasta Soneraan, miten vaihto mielestäsi sujui? 5 = erittäin hyvin, 1 = erittäin huonosti

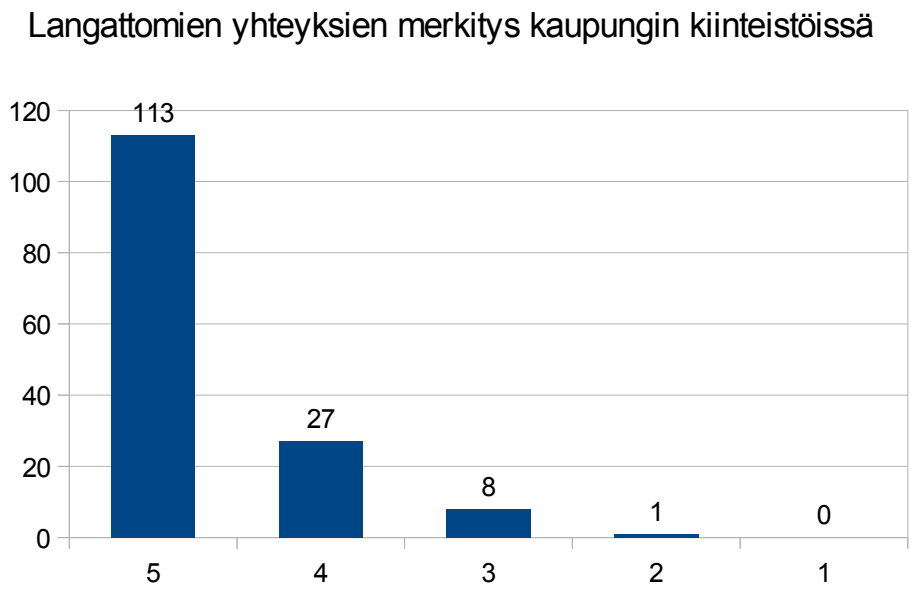
109 vastaajaa eli noin 72 % vastasi kysymykseen 3G-operaattorin vaihdon sujuvuudesta. Vain kymmenen vastaajan mielestä se sujui huonosti tai erittäin huonosti. (Kuva 19.)



KUVA 20. Onko työaseman yhteyden toimivuudessa tapahtunut muutosta sen jälkeen kun 3G-tietoliikenneoperaattori vaihdettiin? 5 = parantunut selvästi, 1 = huonontunut selvästi

Kysymykseen 3G-yhteyden toimivuuden muutoksesta operaattorin vaihdon jälkeen vastasi 76 vastaajaa eli noin puolet. Suurimman osan mielestä yhteyksien toimivuus ei muuttunut vaihdon jälkeen. Muista vastaajista hieman useampi on vastannut toimivuuden parantuneen kuin huonontuneen. (Kuva 20.) Kommenteista käy ilmi, että muutamilla yhteys on heikentynyt huomattavasti.

Kuudennessa ja seitsemännessä kysymyksessä kysytään kuinka tärkeänä käyttäjät erilaisia langattomia tietoliikenneyhteyksiä pitävät, kuudennessa kaupungin kiinteistöissä, seitsemännessä myös niiden ulkopuolella. Näissäkin kysymyksissä on valinnainen kommentointikenttä.



KUVA 21. 5 = Erittäin tarpeellinen, 1 = Ei lainkaan tarpeellinen

Kysymykseen langattomien yhteyksien tärkeyteen kaupungin kiinteistöissä vastasi 149 vastaajaa, eli lähes kaikki. Valtaosa piti niitä erittäin tarpeellisina (Kuva 21). Kommenteissa kerrotaan, että langattomuus mahdollistaa erilaisten materiaalien muokkausta ja tarkistamista mistä tahansa työpisteistä ja vähentää kaksinkertaista työtä. Se vähentää myös ylimääräistä paperien tulostamista ja helpottaa työn sujuvuutta ja reaaliaikaisuutta.

KUVA 22. 5 = Erittäin tarpeellinen, 1 = Ei lainkaan tarpeellinen

Viimeiseen kysymykseen sellaisten langattomien yhteyksien tärkeydestä, jotka toimivat myös kaupungin kiinteistöjen ulkopuolella, vastasi myös lähes kaikki. Niitäkin pidettiin erittäin tärkeänä, muttei aivan yhtä merkittävänä kuin kaupungin kiinteistöissä (Kuva 22). Kommenteissa käy ilmi, että osalla vastaajista on liikkuva työ, jossa säästää aikaa, kun voi suorittaa vaadittavat kirjaukset paikan päältä. Siten ne ovat hyvin ajantasaiset, joka auttaa myös muita, jotka tarvitsevat niitä työssään. Myös nopeudesta kommentoitiin, että 3G-yhteydet pitää saada riittävän nopeaksi, koska verkkotallennuksia tarvitaan koko ajan.

4.3 Tulosten arviointia

Useimmat tekevät töitä pääosin omassa työpisteessään, joten siellä toimivat tietoliikenneyhteydet ovat erittäin tärkeitä. Asteikolla 1-5 vastaajat arvioivat yhteyden toimivuuden olevan keskimäärin 4,11 mikä on hyvä tulos.

Kyselyn kolmannessa kysymyksessä hyvin harvat vastasivat yhteyden toimivan erinomaisesti muualla kuin omassa työpisteessä. Tämän arvioisin johtuvan siitä, että toimivuutta ja nopeutta omassa työpisteessä, jossa on usein luotettava ja nopea langallinen LAN-yhteys ja nopeat yhteydet palvelimille, pidetään mittana, mihin muita paik-

koja verrataan. Harvassa paikassa ylletään samaan, joten on luontevaa antaa muille sijainneille huonompi arvosana.

Safemovea tarvitaan kun täytyy muodostaa VPN-yhteys jostakin muualta, esim. joissakin tapauksissa neuvotteluhuoneesta tai kotoa. Toisessa kysymyksessä käy ilmi, että keskimäärin oman työpisteen ulkopuolella kannettavaa työasemaa käytetään alle 30 % ajasta. Kuitenkin kysymysten 6 ja 7 (Kuvat 21 ja 22) mukaan langattomia yhteyksiä kaupungin kiinteistöissä ja muuallakin pidetään erittäin tärkeinä. Kommenteissa kerrotaan, että esim. joitakin kiireellisiä työasioita täytyy hoitaa kotoa, niinpä toimiva yhteys sieltä työkoneella on erittäin tärkeää. Sama pätee tietenkin myös neuvotteluhuoneisiin, vaikka siellä ollaan keskimäärin alle 10 % ajasta, on toimimaton tai hitaasti toimiva yhteys suuri haitta joka voi viedä omaa ja myös muiden työaikaa.

3G-yhteyden toimivuudesta kysyttiin erityisesti kysymyksessä 5 (Kuva 20), mutta myös tietysti joissakin kysymyksen 3 käyttöpaikoissa sitä käytetään. Sen kommenteista useat olivatkin 3G:hen liittyviä. Mainittuja ongelmia ovat yhteyden pätkiminen ja hitaus. Vaikka operaattorin vaihdon jälkeen yhteys on joko pysynyt ennallaan tai parantunut valtaosan mukaan, on pienellä osalla huomattavia ongelmia nyt Soneran yhteydellä mitä ei ollut aikaisemmin Elisaa käytettäessä. Mahdollisesti niissä tapauksissa voisi harkita, onko ehdottoman välttämätöntä, että kaikilla on käytössä sama 3G-operaattori. Joissakin kommenteissa kritisoitiin operaattorin vaihtoa, koska se aiheuttaa ylimääräisiä työaikakustannuksia suhteellisen pienen hyödyn takia.

Kun Webropolista suodatetaan tuloksia vastaajien työpaikan osoitteen mukaan, voidaan vertailla eri paikkojen tietoliikenneyhteyksien toimivuutta keskenään. Esimerkiksi kun vertaillaan muutamaa kohdetta, joista oli suurimpia vastaajamääriä, nähdään että keskiarvo oman työpisteen yhteyksien toimivuudesta on yli 4 asteikolla 1-5. Kohtuullisesti ne toimivat lähes kaikilla.

Kun vertaillaan yhteyksien toimivuutta neuvotteluhuoneessa, on sitä arvioinut huonoksi tai välttäväksi 16 vastaajaa 113:sta. Näillä vastaajilla työpaikan osoitteena on useimmin eli viisi kertaa Maaherrankatu 9-11, jossa sijaitsee kaupungin virastotalo. Keskimäärin ne, joilla on tuo sama työpaikan osoite, ovat antaneet neuvotteluhuoneen yhteyksien toimivuudelle arvosanan 3. Se on vain hieman koko vastaajajoukon keski-

arvoa 3,5 heikompi ja joukossa on myös kaksi erinomaisen ja hyvän arvosanan antaneita. On mahdollista, että osassa virastotalon neuvotteluhuoneista langaton verkko toimii huonosti, yhdessä kommentissa mainitaankin, että joskus on ongelmia virastotalon neuvotteluhuoneessa. On myös mahdollista, että huonosti toimivia yhteyksiä on jossain muussa kohteessa tai kohteissa, joissa virastotalolla työskentelevät käyvät palavereissa.

5. YHTEENVETO

Työn tavoitteena oli tutkia Mikkelin kaupungin työntekijöiden erilaisten tietoliikenneyhteyksien käyttöä, erityisesti millaisilla yhteystavoilla he käyttävät Safemove VPN-ohjelmaa ja kuinka hyvin ne heidän mielestään toimivat. Tein työn Kuntien Tieran Mikkelin toimipisteelle, joka tarjoaa Mikkelin kaupungille tietohallintopalveluja. Ennen varsinaista asiakastyytyväisyystutkimusta kävin työssäni läpi VPN-ratkaisuihin liittyvää tekniikkaa sekä Kuntien Tieralla käytössä olevan Safemove-tuotteen ominaisuuksia. Työn käytännön osuudessa toteutettiin asiakastyytyväisyystutkimus Internet-kyselynä. Pyyntö kyselyyn vastaamiseen lähetettiin sähköpostilla 436 käyttäjälle.

Pidän kyselyn vastausprosenttia 35 eli 151 vastaajaa hyvänä tuloksena, se todennäköisesti edustaa kaikkia kyselyn saaneita hyvin. Kysely tuli laadittua melko nopeasti, ja siinä on joitakin kohtia joissa olisi parantamisen varaa. Se haluttiin saada suoritettua ennen Juhannusta, jolloin suuri osa kaupungin työntekijöistä aloittaisi kesälomansa. Muussa tapauksessa kyselyn olisi voinut tehdä vasta elo- tai mahdollisesti vasta syyskuussa.

Parannettavaa olisi ollut ainakin eri käyttöpaikkojen nimeämisessä, ”Hotspot” ei ole tuttu termi kaikille. Sen olisi voinut nimetä vaikka WLAN-Hotspotiksi, tai kirjoittaa kysymyksen yhteyteen selityksen.

Pienellä osalla vastaajista oli ollut välttävä tai huono yhteys neuvotteluhuoneesta. Tätä tietoa ei kuitenkaan ole kovin helppoa käyttää korjaamaan ongelma, koska ei ole tietoa missä neuvotteluhuone sijaitsee ja käytetäänkö siellä esim. WLAN- vai 3G-yhteyttä. Toisaalta kysely halutaan kuitenkin pitää selkeänä, niin ettei vastaajien tarvitse kirjoitella esim. useita neuvotteluhuoneiden osoitteita. Lisäksi tässä kyselyssä on tarkoi-

tuksena enemmänkin saada tulos miten ongelmallisia tai ongelmattomia yhteydet eri paikoista ovat keskimäärin, ei niinkään toimia vikatikettien vastaanottajana, joten niin tarkka tieto ei ole välttämätöntä.

Joissakin kommenteissa kysymykseen 3G-operaattorin vaihdon sujuvuudesta tuli kommentteja itse yhteyden toimivuudesta, joten on ehkä mahdollista, että vastaajat valitsivat myös vastausvaihtoehdon sen mukaan. Tämän olisi voinut estää vaihtamalla kysymysten 4 ja 5 järjestystä, jolloin ensin vastataan, onko 3G-yhteyden toimivuudessa esiintynyt muutosta operaattorin vaihdon jälkeen ja vasta sen jälkeen miten sujuvasti itse vaihto sujui.

Pääosin yhteydet toimivat kyselyn mukaan hyvin, mutta joitakin yhteyden pätkimisiä esiintyy. Ne vaikuttavat liittyvän pääosin 3G-yhteyksiin. Ongelmana kyselyn tulosten tulkinnassa on se, että ei ole varmuutta mistä kommenteissa kerrottu hidastelu johtuu. On mahdollista että se johtuu tietokoneesta tai käytettävästä yhteydestä, tai ongelmaa saattaa olla Safemove-palvelimella.

Ajattelin alun perin lisääväni tähän työhön myös teknisen osion, jossa tarkastelisin lokitietoja Safemove-palvelimelta. Siitä mahdollisesti olisi saanut myös käyttäjien yhteyksistä eri yhteystavoilla ja tietoa onko itse Safemove-palvelin aiheuttanut käyttäjien kokemia katkoksia yhteyksissä. Sellaista tietoa ei kuitenkaan ilmeisesti saa helposti palvelimelta, manuaalisesti lokien läpikäyminen ei ole oikein järkevää, koska käyttäjiä on päivittäin satoja, joten tietoa olisi valtavasti. Työn päätarkoituksena oli tutkia miten käyttäjät käyttävät eri yhteystapoja, ja onko niiden käytössä ongelmia. Onnistuin mielestäni tässä kohtuullisen hyvin. Tämän työn tuloksista voi päätellä, että erityisesti langattomien yhteyksien toimivuuteen ja nopeuteen on syytä kiinnittää jatkossakin paljon huomiota.

LÄHTEET

1. Perlmutter, Bruce & Zarkower, Jonathan. Virtuaaliset yksityisverkot. Helsinki: Edita 2001.

2. Virtual Private Network. WWW-dokumentti. http://en.wikipedia.org/wiki/Virtual_private_network. Päivitetty 9.4.2013. Luettu 9.4.2013.

3. Frankel, Sheila; Kent, Karen; Lewkowski, Ryan; Orebaugh Angele D; Ritchey, Ronald W & Sharma, Steven R. Guide to IPSec VPNs. PDF-dokumentti http://www.nist.gov/customcf/get_pdf.cfm?pub_id=150393. National Institute of Standards and Technology 2005. Luettu 29.11.2012.

4. Cisco Systems Inc. CCNA Exploration, Accessing the WAN. Sähköinen kurssimateriaali. http://www.cisco.com/web/learning/netacad/index.html. Päivitetty 20.1.2009. Luettu 29.11.2012.

5. Cisco Systems Inc. CCNA Security. Sähköinen kurssimateriaali. http://www.cisco.com/web/learning/netacad/index.html. Päivitetty 5.3.2012. Luettu 9.3.2013.

6. Kozierok, Charles M. The TCP/IP Guide. WWW-dokumentti. http://www.tcpipguide.com/free/index.htm. Päivitetty 20.9.2005. Luettu 29.11.2012.

7. IPsec. WWW-dokumentti. http://en.wikipedia.org/wiki/IPsec. Päivitetty 3.4.2013. Luettu 8.4.2013.

8. Internet Key Exchange. WWW-dokumentti. http://en.wikipedia.org/wiki/Internet_Key_Exchange. Päivitetty 6.4.2013. Luettu 8.4.2013.

9. Deal, Richard. Cisco Press. The Complete Cisco VPN Configuration Guide. WWW-dokumentti. http://fengnet.com/book/vpnconf/. Päivitetty 17.2.2009. Luettu 29.11.2012.

10. Mason, Andrew. Cisco Press. VPNs and VPN Technologies. WWW-dokumentti. http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=3. Päivitetty 4.1.2002. Luettu 29.11.2012.

11. IPsec made simple. WWW-dokumentti. http://briolidz.wordpress.com/2012/01/23/ipsec-made-simple/. Päivitetty 23.1.2012. Luettu 6.3.2013.

12. Understanding PPTP (Windows NT 4.0). WWW-dokumentti. http://technet.microsoft.com/en-us/library/cc768084.aspx. Ei päivitystietoa. Luettu 29.11.2012.

13. Point-to-Point Tunneling Protocol. WWW-dokumentti. http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol. Päivitetty 13.3.2013. Luettu 8.4.2013.

14. VPN Tunneling Protocols. WWW-dokumentti. http://technet.microsoft.com/en-us/library/cc771298%28v=ws.10%29.aspx. Ei päivitystietoa. Luettu 29.11.2012.

15. Layer 2 Tunneling Protocol. WWW-dokumentti. http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol. Päivitetty 25.2.2013. Luettu 26.3.2013.

16. Layer 2 Tunneling Protocol. WWW-dokumentti. http://www.hill2dot0.com/wiki/index.php?title=L2TP. Päivitetty 22.7.2007. Luettu 6.3.2013.

17. Transport Layer Security. WWW-dokumentti. http://en.wikipedia.org/wiki/Transport_Layer_Security. Päivitetty 8.4.2013. Luettu 8.4.2013.

18. What is TLS/SSL? WWW-dokumentti. http://technet.microsoft.com/en-us/library/cc784450%28v=WS.10%29.aspx. Päivitetty 28.3.2003. Luettu 14.3.2013.

19. TLS. WWW-dokumentti. http://fi.wikipedia.org/wiki/TLS. Päivitetty 8.3.2013. Luettu 8.4.2013.

20. SSL VPN. WWW-dokumentti. http://fi.wikipedia.org/wiki/SSL_VPN. Päivitetty 8.3.2013. Luettu 26.3.2013.

21. SSL VPN (Secure Sockets Layer virtual private network) http://searchsecurity.techtarget.com/definition/SSL-VPN. Päivitetty tammikuu 2009. Luettu 8.3.2013.

22. Janssen, Cory. Secure Sockets Layer Virtual Private Network (SSL VPN). WWW-dokumentti. http://www.techopedia.com/definition/17006/secure-socket-layer-virtual-private-network-sslvpn. Päivitysaika tuntematon. Luettu 8.3.2013.

23. Frankel Sheila 2008. National Institute of Standards and Technology. Guidelines on Implementing a Secure Sockets Layer (SSL) Virtual Private Network (VPN). PDF-dokumentti. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=890029. Päivitetty 23.7.2008. Luettu 8.3.2013.

24. Symmetric Encryption, Asymmetric Encryption, and Hashing. WWW-dokumentti. http://packetlife.net/blog/2010/nov/23/symmetric-asymmetric-encryption-hashing/. Päivitetty 23.11.2010. Luettu 8.4.2013.

25. Symmetric-key algorithm. WWW-dokumentti. http://en.wikipedia.org/wiki/Symmetric_key_algorithm. Päivitetty 25.3.2013. Luettu 8.4.2013.

26. What is Asymmetric Encryption? WWW-dokumentti. http://www.omnisecu.com/security/public-key-infrastructure/what-is-asymmetric-encryption.htm. Päivitetty 3.2.2011. Luettu 14.3.2013.

27. Diffie-Hellman. WWW-dokumentti. http://fi.wikipedia.org/wiki/Diffie-Hellman. Päivitetty 8.3.2013. Luettu 14.3.2013.

28. MD5. WWW-dokumentti. http://fi.wikipedia.org/wiki/MD5. Päivitetty 7.3.2013. Luettu 8.4.2013.

29. Cryptographic hash function. WWW-dokumentti. http://en.wikipedia.org/wiki/Cryptographic_hash_function. Päivitetty 2.4.2012. Luettu 8.4.2013.

30. Hash-based message authentication code. WWW-dokumentti. http://en.wikipedia.org/wiki/Hash-based_message_authentication_code. Päivitetty 30.3.2013. Luettu 8.4.2013.

31. MD5. WWW-dokumentti. http://en.wikipedia.org/wiki/MD5. Päivitetty 6.4.2013. Luettu 8.4.2013.

32. Desautels, Philip A. 1997. SHA1 Secure Hash Algorithm – Version 1.0. WWW-dokumentti. http://www.w3.org/PICS/DSig/SHA1_1_0.html. Päivitetty 31.12.2001. Luettu 8.4.2013.

33. SHA-1. WWW-dokumentti. http://en.wikipedia.org/wiki/SHA-1. Päivitetty 6.4.2013. Luettu 8.4.2013.

34. Birdstep Technology Oy. Safemove 5.6.3 Technical Description. Birdstep-safemove-technical-description-5.6.3.pdf. PDF-dokumentti. Päivitetty 2012. Luettu 21.3.2013.

35. Mobile IP. WWW-dokumentti. http://en.wikipedia.org/wiki/Mobile_IP. Päivitetty 14.3.2013. Luettu 21.3.2013.

36. Kuntien Tiera Oy. WWW-dokumentti. http://www.tiera.fi/. Ei päivitystietoa. Luettu 19.4.2013.

Kysely työasemien tietoliikenneyhteyksistä

Tämä kysely on lähetetty niille Tieran Mikkelin toimipisteen asiakkaille, joilla on työasemana kannettava tietokone. Kysymykset koskevat erityisesti työasemien tietoliikenneyhteyksiä. Kysymyksen alla olevaan tekstilaatikkoon voit halutessasi jättää kommentin.

1. Työpisteesi katuosoite tai pääasiallisen käyttöpaikan katuosoite

2. Arvioi minkä verran keskimäärin käytät työasemaasi eri käyttöpaikoissa prosentteina. *

Syötä jokaiseen käyttöpaikkaan pelkkä luku väliltä 0-100 ilman prosenttimerkkiä niin että luvut ovat yhteensä 100.

Oma työpiste
Neuvotteluhuone
Koti
"Hotspot"
Muu

3. Kuinka arvioisit työasemasi tietoliikenneyhteyksien toimivuutta eri käyttöpaikoissa? *

	Erinomainen	Hyvä	Kohtuullinen	Välttävä	Huono	En käytä / En osaa sanoa
Oma työpiste	○	○	○	○	○	○
Neuvotteluhuone	○	○	○	○	○	○
Koti	○	○	○	○	○	○
"Hotspot"	○	○	○	○	○	○
Muu	○	○	○	○	○	○

Oma kommentti tietoliikenneyhteyksien toimivuudesta eri käyttöpaikoissa

4. Kun työasemien 3g-tietoliikenneoperaattori vaihdettiin keväällä Elisasta Soneraan, miten vaihto mielestäsi sujui? *

5 = Erittäin hyvin, 1 = Erittäin huonosti

5	4	3	2	1	En osaa sanoa
○	○	○	○	○	○

Oma kommentti tietoliikenneoperaattorin vaihdosta

5. Onko työaseman yhteyden toimivuudessa tapahtunut muutosta sen jälkeen kun 3g-tietoliikenneoperaattori vaihdettiin? *

5 = Parantunut selvästi, 1 = Huonontunut selvästi

5	4	3	2	1	En osaa sanoa
○	○	○	○	○	○

Oma kommentti, miten muutos on ilmennyt?

6. Kuinka tarpeelliseksi koet työssäsi työaseman, jonka tietoliikenneyhteydet toimivat työpisteessäsi ja muissa kaupungin kiinteistöissä langattomasti? *

5 = Erittäin tarpeellinen, 1 = Ei lainkaan tarpeellinen

5	4	3	2	1	En osaa sanoa
○	○	○	○	○	○

Oma kommentti

7. Kuinka tarpeelliseksi koet työssäsi työaseman, jonka tietoliikenneyhteydet toimivat kaikkialla langattomasti? *

5 = Erittäin tarpeellinen, 1 = Ei lainkaan tarpeellinen

5	4	3	2	1	En osaa sanoa
○	○	○	○	○	○

Oma kommentti