SAVONIA

Suojattu Windows-pohjainen VPN-yhteys yrityskäyttöön

Antti Venäläinen

Opinnäytetyö

___. ___. _____ _____

Ammattikorkeakoulututkinto

SAVONIA-AMMATTIKORKEAKOULU **OPINNÄYTETYÖ**
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Antti Venäläinen	
Työn nimi Suojattu Windows-pohjainen VPN-yhteys yrityskäyttöön	
Päiväys 28.11.2012	Sivumäärä/Liitteet 42
Ohjaaja(t) lehtori Veijo Pitkänen, ICT-päällikkö Markku Manninen	
Toimeksiantaja/Yhteistyökumppani(t) Voimatel Oy	

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli tutkia Windows-käyttöjärjestelmässä toimivaa SSTP-tunnelointiprotokollaa nykyisen L2TP/IPSec VPN -yhteyden seuraajaksi sekä toteuttaa näiden tietojen pohjalta uuden järjestelmän suunnitelma ja testijärjestelmä. Opinnäytetyö on tehty Voimatel Oy:n toimeksiannosta. Työn lähtökohtana oli ottaa huomioon käytettävyys, tietoturva sekä kustannukset uuden järjestelmän suunnittelussa.

Etätyö on nykyään tullut entistä suosituimmaksi vaihtoehdoksi työssäkäyville ihmisille. Nykyaikaiset tietoverkot mahdollistavat vaivattoman etätyöskentelyn kotoa käsin myös esimerkiksi langattomasti 3G-yhteyden avulla. Käyttääkseen yrityksen verkosta löytyviä resursseja täytyy työntekijöillä olla käytössään VPN-yhteys.

Opinnäytetyön ensimmäisessä vaiheessa tutkittiin nykyisen VPN-yhteyden parannuksia kaipaavia osa-alueita sekä käytettävissä olevia VPN-tunnelointiprotokollia ja VPN-palvelua varten tarvittavia rooleja Windows-käyttöjärjestelmässä. Seuraavassa vaiheessa tehtiin uuden VPN-järjestelmän suunnitelma ja määritettiin sen vaatimukset. Työn viimeisessä vaiheessa toteutettiin testijärjestelmä ja kirjattiin testaustulokset.

Tässä opinnäytetyössä saavutettujen tulosten perusteella Voimatel Oy voi tulevaisuudessa halutessaan rakentaa uuden ja toimivan VPN-järjestelmän.

Avainsanat
etätyö, VPN, SSTP

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Antti Venäläinen			
Title of Thesis Secure Windows-Based VPN Access for Business			
Date	28 November, 2012	Pages/Appendices	42
Supervisor(s) Mr Veijo Pitkänen, Principal Lecturer and Mr Markku Manninen, ICT-manager			
Client Organisation/Partners Voimatel Oy			

Abstract

The main goal of this thesis was to do a research on the SSTP tunneling protocol which operates under the Windows operating system and also to implement the plan for a new VPN connection and test system based on the research. The thesis was commissioned by Voimatel Oy. The starting point of this thesis was to take usability, security and costs into consideration when planning the new VPN connection.

Remote work has become more popular for workers. Modern networks make remote work from home possible even with the wireless 3G connection. To use resources from the corporate network, users must have a VPN connection in use.

The first step of this thesis was to study improvements of the existing VPN connection together with usable VPN tunneling protocols and necessary roles for the VPN connection in the Windows operating system. In the next step the plan and requirements for the new VPN connection were made. The last step was to implement the test system and to write down the testing results.

As a result of this thesis Voimatel Oy can build a new and operational VPN connection in the future based on this thesis.

Keywords
Remote work, VPN, SSTP

ALKUSANAT

Tämä opinnäytetyö on tehty vuonna 2012 Savonia-ammattikorkeakoulun tietotekniikan koulutusohjelmassa. Haluan kiittää työn ohjaajia, lehtori Veijo Pitkästä Savonia-ammattikorkeakoulusta ja ICT-päällikkö Markku Mannista Voimatel Oy:stä. Haluan kiittää myös avovaimoani tuesta opinnäytetyön teon aikana.

Helsingissä
28.11.2012

Antti Venäläinen

SISÄLTÖ

1 JOHDANTO

Tämä opinnäytetyö on tehty Voimatel Oy:n toimeksiannosta Toivalassa Siilinjärvellä vuonna 2012. Työn tavoitteena on tutkia uutta Windows-pohjaista Secure Socket Tunneling Protocol (SSTP) -tunnelointiprotokollaa yrityksen käyttöön sekä toteuttaa testijärjestelmä, jonka avulla pystytään havainnollistamaan uuden ratkaisun toimivuutta. SSTP-tunnelointiprotokolla valittiin toteutettavaksi järjestelmäksi, koska se integroituu hyvin yrityksen työasemissa paljon käytettyyn Windows 7 -käyttöjärjestelmään.

Voimatel Oy on vuonna 2001 perustettu pohjoissavolainen yritys, jonka toiminta on kasvanut alueellisesti Pohjois-Savosta maanlaajuiseksi. Voimatel Oy:n liiketoiminta-alueita ovat sähkö- ja televerkkojen rakentaminen ja ylläpito sekä teollisuuden ja energiantuotannon kunnossapito.

Opinnäytetyön alkuosassa käsitellään yleisesti etätyötä yrityksissä ja sen tuomia haasteita. Tässä osassa esitellään myös nykyisen järjestelmän kehitystarpeet, Windows-käyttöjärjestelmän tuetut VPN-tunnelointiprotokollat ja VPN-yhteyttä varten tarvittavat roolit Windows Server -palvelimella. Näin saadaan yleiskuva opinnäytetyön vaatimuksista.

Opinnäytetyön loppuosassa esitellään suunnitelma uudesta järjestelmästä sekä yleiskatsaus toteutetun testijärjestelmän asennusvaiheista ja testauksesta. Loppuosassa käsitellään myös tulevaisuuden näkymiä ja esitetään yhteenveto opinnäytetyöstä.

2 ETÄTYÖ

2.1 Etätyö käsitteenä

Etätyöskentely tarkoittaa työskentelemistä osittain kotona, työnantajan eri toimipisteissä, työkohteissa, asiakkaan luona tai matkoilla. Etätyössä työntekijä hyödyntää nykyaikaisia viestintäteknologian työkaluja. Etätyö tarjoaa työntekijöille mahdollisuuden työ- ja perhe-elämän yhteensovittamiseen sekä joustavuutta työ- ja asuinpaikan sijoittumiseen. Etätyön avulla voidaan myös saavuttaa huomattavia säästöjä työmatkakustannuksiin sekä työmatkoihin käytettävään aikaan. (Työ- ja elinkeinoministeriö 2008.)

2.2 Etätyö tänään

Etätyö on viime vuosina lisääntynyt erityisesti IT-yrityksissä. Esimerkiksi tietokoneen tai puhelimen avulla tehtävät työt voidaan suorittaa myös työpaikan ulkopuolella.

Vuonna 2008 tehdyn käyttötutkimuksen mukaan joka kolmas työssäkäyvä teki etätöitä. Kun verrataan näitä tuloksia vuonna 2004 tehtyyn tutkimukseen, jolloin joka viidennessä kotitaloudessa ainakin yksi henkilö teki etätöitä, voidaan todeta etätyön yleistyneen neljän vuoden aikana. (Sirkiä 2009.)

Etätyö edellyttää verkkoyhteyttä työntekijän päätelaitteen ja yrityksen tietoverkon välillä. Aiemmin etätyöntekijöiden vaivana olivat hitaat verkkoyhteydet, joiden avulla verkkoyhteyttä vaativien sovellusten käyttö oli hidasta ja vaivalloista. Matkapuhelin- ja WLAN-verkkojen saatavuus ja nopeudet ovat kasvaneet kilpailukykyisiksi kiinteiden verkkojen rinnalle ja langattomista yhteyksistä on tullut erinomainen ratkaisu etätyöntekijälle. Esimerkiksi 3G-verkon avulla internetyhteyden saa muodostettua lähes kaikilla taajama-alueilla Suomessa ja 3G-verkon peittoalue kasvaa jatkuvasti. Lisäksi rakenteilla oleva 4G-matkapuhelinverkko tulee nopeuksillaan kilpailemaan kiinteiden verkkoyhteyksien kanssa. Myös WLAN-tukiasemia on nykyään monissa julkisissa paikoissa, kuten lentokentillä, junissa, kahviloissa, kirjastoissa ja ravintoloissa.

Useimmiten etätyöntekijän tarvitsemat tiedot ja sovellukset sijaitsevat yrityksen sisäisessä verkossa, ja päästäkseen niihin käsiksi työntekijällä täytyy olla internetyhteyden lisäksi käytössään myös VPN-yhteys. Työkalut VPN-yhteyden muodostamiseksi

tarjoaa työnantaja. Yrityksillä voi olla myös järjestelmiä, joihin pääsee kirjautumaan suoraan internetistä verkkoselaimen kautta, jolloin VPN-yhteyttä ei tarvitse muodostaa. Tämä on tietoturvan kannalta huonompi ratkaisu, koska tällöin sivusto voi joutua helpommin verkkohyökkäysten kohteeksi.

2.3 Etätyöntekijän työkalu – VPN

VPN on lyhenne sanoista Virtual Private Network, joka tarkoittaa suomeksi virtuaalista yksityisverkkoa. Virtuaalisen yksityisverkon avulla voidaan yhdistää fyysisesti erillään olevat yksityiset lähiverkot tai mobiililaitteet turvallisesti julkisen verkon kautta. Turvallisuudella tarkoitetaan tässä yhteydessä tiedon muuttumattomuuden ja luottamuksellisuuden säilymistä sekä käyttäjien tunnistamista ja heidän käyttöoikeuksiensa hallintaa. VPN-yhteyden avulla työntekijät voivat käyttää yrityksen verkosta löytyviä resursseja esimerkiksi kotoa käsin. (Kaario 2002, 314.)

Windows-palvelimilla toimivat VPN-tunnelointiprotokollat esitellään tässä työssä luvussa 4.

3 MUUTOKSEN TARVE

3.1 Käytettävyys

Käytettävyys on merkittävä vaatimus suunniteltaessa Voimatel Oy:n työntekijöille päivitettyä ratkaisua etäyhteyden muodostamiseksi yrityksen verkkoon. Nykyisin kaikissa yrityksen työasemissa on käytössä erillinen ohjelmisto VPN-yhteyden muodostamista varten. Kaikki eivät ole tottuneet käyttämään tietokoneita päivittäin, ja monet kokevat erillisen sovelluksen käytön VPN-yhteyden luomiseksi hieman hankalaksi. Sulauttamalla VPN-yhteys osaksi Windowsin verkkoyhteyksiä saadaan yksi välivaihe vähemmän yhteyden muodostamisessa sekä VPN-yhteys voidaan myös asettaa käynnistymään automaattisesti, kun esimerkiksi 3G-internetyhteys on luotu. Näin ollen VPN-yhteyden luomiseen ei välttämättä tarvitse ollenkaan käyttäjän toimia.

3.2 Tietoturva

Etätyön määrän lisääntyessä arkaluontoista tietoa liikkuu yhä enemmän VPN-tunneleissa. Tiedot täytyy pyrkiä pitämään salassa, jotta ne eivät joutuisi vääriin käsiin. Nykyinen käytössä oleva L2TP/IPSec-järjestelmä on sinällään riittävä tietoturvatasoltaan, mutta laitekannan uudistuessa on viisasta miettiä uudempaa tekniikkaa uudempien käyttöjärjestelmien rinnalle.

3.3 Kustannukset

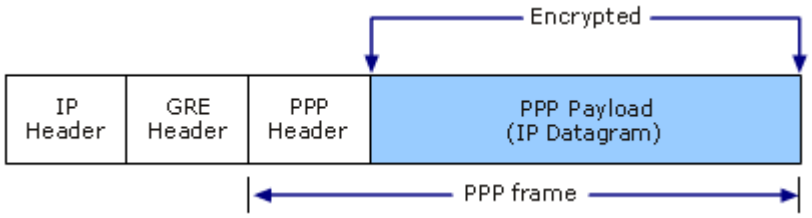
Nykyisestä järjestelmästä koituu kuukausittain kuluja VPN-palvelun ylläpidosta sekä VPN-yhteyden muodostamiseen käytettävän kolmannen osapuolen ohjelmiston lisensseistä. Uuden järjestelmän toimiessa kolmannen osapuolen lisenssimaksut jäävät pois ja käyttöön tulevat työasemiin asennetut Windows 7 -käyttöjärjestelmän työkalut, joiden lisenssimaksut on jo maksettu. Kolmannen osapuolen lisenssimaksun suuruuteen vaikuttaa myös VPN-käyttäjien määrä.

4 VPN-TUNNELOINTIPROTOKOLLAT WINDOWS-KÄYTTÖJÄRJESTELMÄSSÄ

4.1 Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) mahdollistaa useiden protokollien tietoliikenteen salauksen ja kapseloinnin lähetettäessä dataa yksityisessä IP-verkossa tai julkisessa IP-verkossa, kuten internetissä. PPTP-tekniikkaa voidaan käyttää yksittäisten käyttäjien etäyhteyksissä sekä palvelimien tai reitittimien välisissä yhteyksissä, esimerkiksi yritysten sivukonttoreiden välillä. (Microsoft Corporation 2012.)

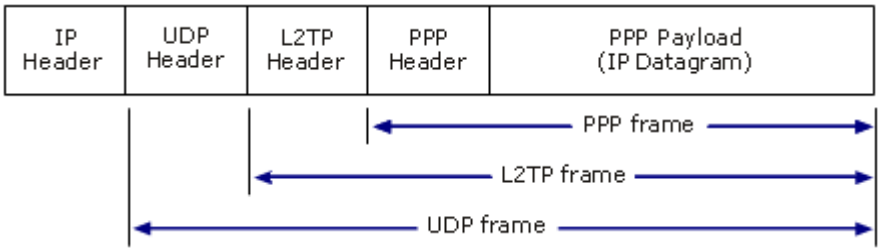
PPTP kapseloi PPP-kehykset IP-datagrammeiksi verkon yli lähetystä varten. PPTP käyttää TCP-protokollaa tunnelin hallinnointiin sekä GRE-tunnelointiprotokollan laajennettua versiota PPP-pakettien kuljetukseen. Kapseloidut PPP-kehykset voidaan salata tai pakata sekä salata ja pakata. (Microsoft Corporation 2012.) PPTP-paketin rakenne kuvataan kuvassa 1.



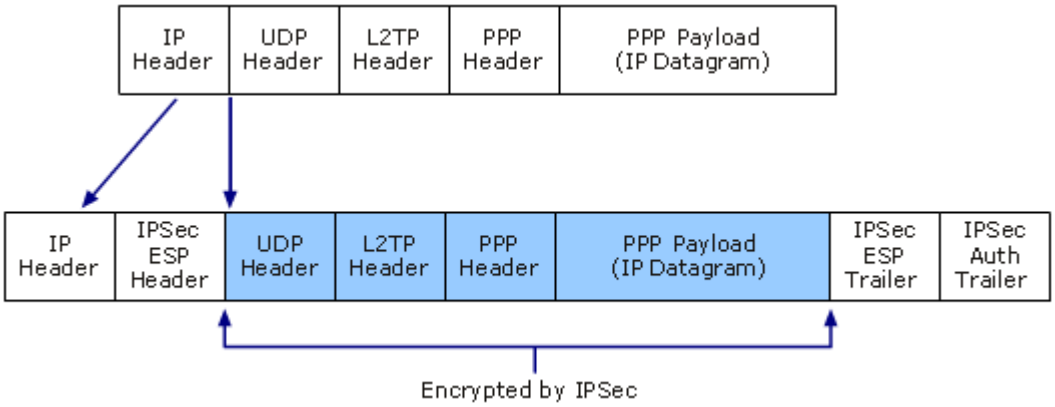
KUVA 1. PPTP-paketin rakenne. (Microsoft Corporation 2012.)

4.2 Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) on PPTP ja L2F -protokollien yhdistelmä, ja se pitää sisällään molempien tekniikoiden parhaat ominaisuudet. Toisin kuin PPTP, L2TP ei käytä MPPE-salausta PPP-paketeille. L2TP tukeutuu pakettivirtojen salauksessa Internet Protocol Security (IPsec) -protokollaan. L2TP ja IPsec -protokollien yhdistelmä tunnetaan nimellä L2TP/IPsec. (Microsoft Corporation 2012.) L2TP-paketin rakenne kuvataan kuvassa 2. Kuvassa 3 kuvataan IPSec-salauksen vaikutus L2TP-pakettiin.



KUVA 2. L2TP-paketin rakenne. (Microsoft Corporation 2012).



KUVA 3. IPSec-salauksen vaikutus L2TP-pakettiin. (Microsoft Corporation 2012).

4.3 Secure Socket Tunneling Protocol

Uusin käytettävistä VPN-tekniikoista on Secure Socket Tunneling Protocol (SSTP), jonka ominaisuudet mahdollistavat verkkoliikenteen pääsyn palomuurien läpi, jotka normaalisti torjuvat L2TP/IPSec-verkkoliikenteen. SSTP-tekniikka mahdollistaa PPP tai L2TP -liikenteen kuljetuksen SSL 3.0 -kanavan läpi. PPP-protokollan käyttö takaa vahvat tunnistusmenetelmät, kuten EAP-TLS-menetelmän. Koska SSTP hyödyntää HTTPS-protokollaa, yhteys asiakaslaitteen ja palvelimen välille muodostetaan käyttäen TCP 443 -porttia. (Microsoft Corporation 2012.)

Windowsille SSTP on ollut saatavilla Windows Vista SP1 -versiosta saakka. SSTP on saatavilla myös Linux, Mac OS ja BSD -käyttöjärjestelmille. Windowsissa SSTP on täysin integroitu RRAS-arkkitehtuuriin, joka mahdollistaa Windows-käyttäjätunnusten käytön, tunnistautumisen älykortin avulla, etäyhteysäännösten käytön sekä Windows VPN Clientin käytön. (SSTP Wikipedia 2012.)

SSTP on tarkoitettu käytettäväksi vain asiakas-VPN-yhteyksiin eikä site-to-site VPN -yhteyksiä ole tuettu (SSTP Wikipedia 2012).

SSTP-yhteyksiin pätevät samat suorituskykyyn liittyvät ongelmat kuin mihin tahansa muihin IP-over-TCP-yhteyksiin (SSTP Wikipedia 2012).

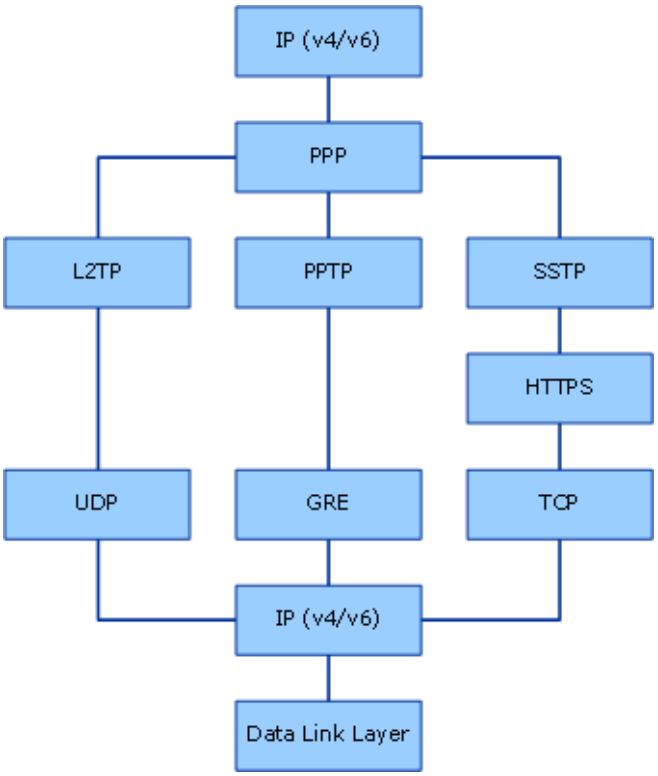
TCP-tunnelin suorituskyky laskee, kun kaksi TCP-ruuhkanhallintamekanismia toimii samanaikaisesti ja häiritsee toistensa toimintaa. Tätä ilmiötä kutsutaan nimellä TCP meltdown -ongelma. (Honda, Ohsaki, Imase, Ishizuka & Murayama 2012.)

Tieto kulkee palvelimen ja VPN yhteyden muodostavan ohjelmiston välillä seuraavasti:

1. SSTP-asiakas muodostaa TCP-yhteyden palvelimen TCP-portin 443 ja asiakkaan dynaamisesti valitun TCP-portin välille.
2. SSTP-asiakas osoittaa palvelimelle haluavansa muodostaa SSL-istunnon lähettämällä palvelimelle SSL viestin Client-Hello.
3. SSTP-palvelin lähettää asiakkaalle oman tietokonekohtaisen varmenteensa.
4. Asiakas vahvistaa varmenteen, määrittää salausmenetelmän, luo avaimen SSL-istuntoa varten ja salaa sen SSTP-palvelimen julkisen avaimen avulla. Tämän jälkeen asiakas lähettää salatun SSL-istunnon avaimen SSTP-palvelimelle.
5. SSTP-palvelin purkaa SSL-istunnon avaimen salauksen oman tietokonekohtaisen sertifikaattinsa avulla. Kaikki tuleva tietoliikenne palvelimen ja asiakkaan välillä on salattu neuvotellun salausmenetelmän ja SSL-istunnon avaimen avulla.
6. SSTP-asiakas lähettää SSL over http -pyynnön SSTP-palvelimelle.
7. SSTP-asiakas neuvottelee SSTP-tunnelin SSTP-palvelimen kanssa.
8. SSTP-asiakas neuvottelee PPP-yhteyden SSTP-palvelimen kanssa. Tähän vaiheeseen kuuluu käyttäjätietojen tunnistus PPP-tunnistusmenetelmän avulla sekä IP-osoitteiden määritys (IPv4 tai IPv6).
9. SSTP alkaa lähettää IPv4- tai IPv6-liikennettä PPP-linkin yli.

(Microsoft Corporation 2012.)

Kuvassa 4 on esitelty Windows-käyttöjärjestelmissä toimivien VPN-protokollien toimintamalli.



KUVA 4. VPN-protokollien toimintamalli. (Microsoft Corporation 2012).

5 VPN-YHTEYTTÄ VARTEN TARVITTAVAT ROOLIT

Windows Server –käyttöjärjestelmässä voidaan palvelimelle asentaa useita erilaisia rooleja eri käyttötarkoituksiin, kuten esimerkiksi toimialueen tulostuspalvelu (Print and Document Services) ja tiedostonjakopalvelu (File Services) (Microsoft Corporation 2008).

Tässä luvussa esitellään ne roolit, jotka ovat tärkeitä VPN-palvelinta suunniteltaessa.

5.1 Domain Name System

Domain Name System eli lyhemmin DNS on nimipalvelu, joka hallitsee IP-osoitteiden kuvaamisen nimiksi ja päinvastoin. DNS perustuu DNS-kyselyihin, joita lähetetään palvelimelle, kun halutaan tietää jollekin nimelle kuuluva IP-osoite. (Kaario 2002, 75 - 78.) Esimerkiksi osoite www.savonia.fi kääntyy IPv4-osoitteeksi 193.167.78.120 DNS-nimipalvelun avulla.

Toimialueella tarvitaan oma nimipalvelu, jotta toimialueella olevien työasemien sekä palvelimien IP-osoitteet ja nimet voidaan yhdistää toisiinsa. Toimialueen DNS-nimipalvelu sijaitsee yleisimmin Active Directory -palvelimella.

5.2 Dynamic Host Configuration Protocol

DHCP eli Dynamic Host Configuration Protocol on IP-osoitteiden ja muiden verkko-asetusten automaattisen konfiguroinnin mahdollistava protokolla. Verkossa on oltava toimiva DHCP-palvelin, jotta DHCP:n avulla verkkoasetuksensa hakevat asiakaslaitteet voivat käynnistyä verkossa. (TCP/IP-verkot 2002.)

Toimialueella DHCP-palvelua käytetään yleisimmin työasemien verkkoasetusten määrittämiseen. Palvelimet on määritetty käyttämään kiinteitä IP-osoitteita. DHCP:n avulla IP-osoitteet annetaan työasemille ikään kuin lainaksi tietylle ajanjaksolle. Toimialueen pääkäyttäjät määrittelevät jaettavat IP-osoiteavaruudet sekä lainattavan osoitteen ajanjakson pituuden.

VPN-palvelua varten tarvitaan toimiva DHCP-palvelin, jotta VPN-yhteyden muodostaville työasemille voidaan jakaa IP-osoitteet. Tässä tapauksessa voidaan hyödyntää

joko toimialueelle valmiiksi asennettua DHCP-palvelua tai konfiguroida VPN-palvelin jakamaan työasemille IP-osoitteet joltain tietyltä osoitealueelta.

5.3 Active Directory Certificate Services

Active Directory Certificate Services eli AD CS on Windows Server -palvelimen palvelu, jonka avulla voidaan sitoa henkilön, laitteen tai palvelun identiteetti tiettyyn yksityiseen avaimeen. AD CS -palvelun avulla yritykset saavat tehokkaan ja turvallisen työkalun varmenteiden jakeluun ja käyttöön. (Microsoft Corporation 2008.)

AD CS -palvelun tarjoamia varmenteita voidaan käyttää tietojen salaukseen ja elektronisten dokumenttien digitaaliseen allekirjoittamiseen. Varmenteita voidaan myös käyttää tietokoneen, käyttäjän tai laitteen tunnistamiseksi verkossa. (Microsoft Corporation 2008.)

Digitaalisia sertifikaatteja käytetään takaamaan seuraavat:

- tiedon luottamuksellisuus
- tiedon eheys
- laitteiden ja käyttäjien tunnistaminen.

AD CS -palvelua voidaan käyttää useiden sovellusten yhteydessä, kuten kirjautumisessa langattomaan verkkoon, VPN-yhteyksiin, tietojen salaukseen (Encrypting File System, EFS) ja digitaalisiin allekirjoituksiin (Microsoft Corporation 2008). Tämän opinnäytetyön kannalta tärkein sertifikaatin käyttökohde on tietokoneen tunnistaminen ja tiedon salaus VPN-tunnelissa.

5.4 Network Policy and Access Services

Asentamalla Network Policy and Access Services (NPAS) -rooli palvelimelle voidaan toteuttaa palvelimella seuraavat toiminnot:

- VPN-yhteys
- puhelinverkkoyhteys
- 802.11-suojattu langaton yhteys.

NPAS-roolin avulla voidaan määritellä asiakkaan tunnistamisen, valtuuttamisen ja aitouden tarkastamisen säännökset verkkoon pääsyä varten seuraavien komponenttien avulla:

- Network Policy Server (NPS)
- Routing and Remote Access Service (RRAS)
- Health Registration Authority (HRA)
- Host Credential Authorization Protocol (HCAP).

Edellä mainituista komponenteista tätä opinnäytetyötä koskee Routing and Remote Access, joka on oleellisin osa VPN-palvelinta. (Microsoft Corporation 2012.)

Routing and Remote Access Service eli suomeksi reititys- ja etäyhteyspalvelut tarjoaa etäkäyttäjille mahdollisuuden päästä käsiksi sisäverkossa oleviin palveluihin VPN- tai puhelinverkkoyhteyden yli. Näitä palveluita ovat esimerkiksi verkkolevyt, tulostimet ja intranetsivustot. Palvelin, jolle RRAS-palvelu on asennettu, mahdollistaa LAN ja WAN -verkkojen reitityspalvelun, jonka myötä on mahdollista yhdistää eri verkko segmenttejä internetin ylitse. Näitä segmenttejä voivat olla esimerkiksi fyysisesti eri paikoissa sijaitsevat toimistot tai etätyössä oleva työntekijä. (Microsoft Corporation 2012.)

6 UUSI JÄRJESTELMÄ

Uutta järjestelmää suunniteltaessa oli otettava huomioon seuraavat osa-alueet:

- käytettävyys
- tietoturva
- skaalautuvuus
- kustannukset.

Näiden palasten avulla pyrittiin saavuttamaan sekä käyttäjiä että yrityksen taloutta hyödyttävä ratkaisu.

6.1 Toimintamalli

VPN-palvelu suunnitellaan käytettäväksi vain Voimatel Oy:n työasemissa, joissa käyttöjärjestelmä on Windows 7. Voimatel Oy:n työasemista noin 70 % sisältää Windows 7 -käyttöjärjestelmän, joten suunnittelua voidaan pitää perusteltuna.

Ennen kuin VPN-yhteyttä voidaan käyttää työasemissa, se täytyy ensin määrittää. Määritys voidaan tehdä manuaalisesti tai asennuspaketin avulla. CMAK (Connection Manager Admistration Kit) -työkalun avulla voidaan luoda asennuspaketti, joka sisältää VPN-yhteyden asennuksen sekä tarvittavat yhteystiedot yhteyttä varten. Asennuspaketin luomisesta kerrotaan lisää luvussa 7.6.2.

Asennuspaketti voidaan jakaa ja asentaa työasemiin automaattisesti toiminnassa olevan SCCM-järjestelmän avulla. Näin ollen käyttäjän ei tarvitse itse asentaa työasemalleen VPN-yhteyttä.

VPN-yhteys muodostuu seuraavien vaiheiden kautta:

1. Käyttäjä yhdistää työaseman internetiin. Internetyhteys voidaan muodostaa Ethernet-, WLAN- tai 3G-verkon kautta.
2. Kun internetyhteys on muodostettu, käyttäjä muodostaa VPN-yhteyden kahdella hiiren painalluksella.
3. Käyttäjän työasema ottaa yhteyden VPN-palvelimeen ja pyytää palvelimelta sen sertifikaatin, jonka avulla palvelimen identiteetti todennetaan. Samalla työasema myös määrittää istuntokohtaisen avaimen ja käytettävän salausmenetelmän.

4. Seuraavaksi käyttäjä tunnistetaan automaattisesti käyttäen Windows-toimialueen käyttäjätunnusta. Tässä vaiheessa työasemalle määritetään myös VPN-tunnelin IP-asetukset.
5. Nyt VPN-yhteys työpaikan verkkoon on luotu ja käyttäjä voi alkaa käyttämään verkkopalveluja, jotka toimivat vain sisäverkosta. VPN-yhteyden luomiseen kuluu aikaa työasemasta ja verkkoyhteydestä riippuen noin 3 – 10 sekuntia.

6.2 Tietoturva

Tietoturva on tärkeä osa-alue, joka täytyy ottaa huomioon parhaalla mahdollisella tavalla. Yrityksen verkossa liikkuu paljon arkaluontoista ja salaista tietoa, joka ei missään tapauksessa saa joutua ulkopuolisten tahojen käsiin. Seuraavat alaluvut käsittelevät tässä opinnäytetyössä huomioon otettuja tietoturvaratkaisuja.

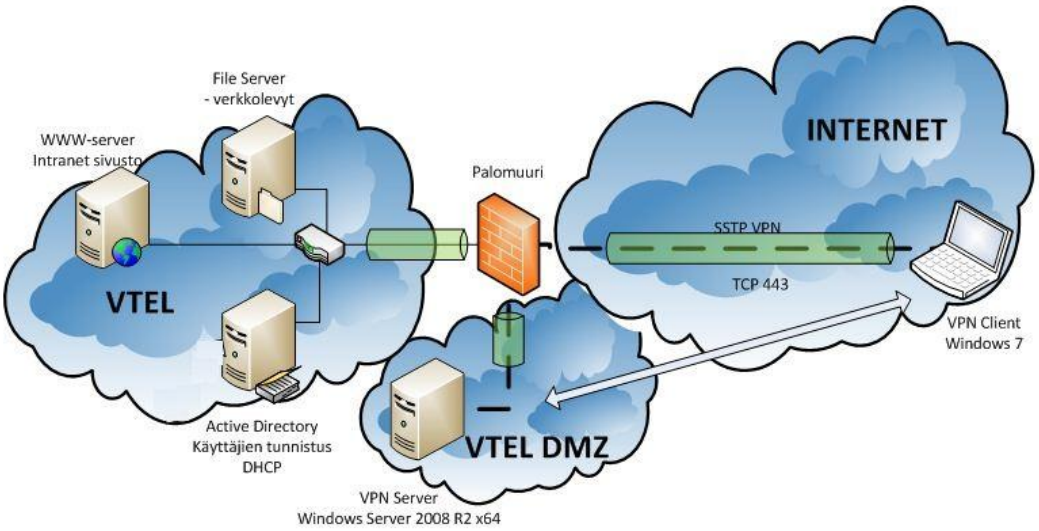
6.2.1 Fyysinen tietoturva

VPN-palvelin sijoitetaan palvelinsaliin, jossa sijaitsevat myös muut Voimatel Oy:n palvelimet. Kulkuoikeudet palvelinsaliin on rajattu vain tietyille palvelimien ylläpitäjille ja ulkopuolisien henkilöiden kulku palvelinsaliin on kielletty.

Palvelinsaliin sijoittaminen on järkevää, koska palvelinsalissa on myös paloturvallisuus ja ilmanvaihto huolehdittu asian mukaisella tavalla.

6.2.2 Sijoittaminen verkkoon

VPN-palvelin sijoitetaan yrityksen demilitarisoidulle alueelle eli DMZ-alueelle, jossa sijaitsevat myös muut julkisesta verkosta pääsyn omaavat palvelimet, kuten esimerkiksi sähköpostipalvelin. DMZ-alue sijaitsee palomuurin takana, jolloin palvelin on paremmin suojattu internetistä tulevilta uhkilta, kuten palvelunestohyökkäyksiltä. (Kaario 2002, 308.) Kuva 5 havainnollistaa VPN-palvelimen sijoittumisen verkkorakenteeseen.



KUVA 5. Toteutettavan järjestelmän looginen verkkokaavio.

6.2.3 Palvelimen etähallinta

Palvelinta voidaan hallita etäyhteyden avulla Windows-käyttöjärjestelmän etätyöpöytäyhteys-työkalulla sekä Voimatel Oy:n hankkimilla kolmannen osapuolen työkaluilla. Palvelimen hallinta sallitaan vain toimialueen pääkäyttäjille Voimatel Oy:n sisäverkosta.

6.2.4 Palomuuri ja virustorjuntaohjelmisto

Palvelimella olevan palomuuriohjelmiston tulee sallia ulkoverkosta tulevista pyynnöistä vain palvelimen TCP-porttiin 443 tulevat SSTP-yhteyspyynnöt.

Työasemien palomuurisäännöt määräytyvät toimialueen GPO (Group Policy Object) -määritysten mukaisesti.

Virustorjuntaohjelmistona käytetään samaa ohjelmistoa kuin myös muissa Voimatel Oy:n palvelimissa.

6.2.5 Tietokoneiden ja käyttäjien tunnistaminen

Tunnistaminen uudessa järjestelmässä pyritään hoitamaan AAA periaatteen mukaisesti. AAA muodostuu englannin kielen sanoista authorization, authentication ja accounting. Nämä sanat ovat suomeksi todennus, valtuutus ja tilastointi. Näillä sanoilla

tarkoitetaan kolmea tietoturvan osa-aluetta, joiden avulla pyritään sallimaan luvalliset käyttäjät ja estämään luvattomat käyttäjät. (Odom 2004, 356.)

Tässä järjestelmässä todennus tapahtuu seuraavasti:

1. Asiakaslaite pyytää VPN-palvelimelta sen tietokonekohtaista varmennetta, jolloin laitteet tunnistetaan kuuluvan samalle toimialueelle. Tietokonekohtaista varmennetta verrataan toimialueen päävarmenteiden myöntäjän (CA) asiakaslaitteelle myöntämään sertifikaattiin. Varmenteiden julkisten avainten arvojen täytyy olla samat. Tässä vaiheessa muodostetaan SSL-yhteys VPN-palvelimen ja asiakkaan välille.
2. Käyttäjät tunnistetaan käyttämällä heidän henkilökohtaista Windows-käyttäjätunnusta ja salasanaa. Käyttäjien tunnistus tapahtuu PPP vaiheessa VPN-yhteyttä muodostettaessa EAP-MS-CHAPv2 tunnistusmenetelmän avulla. Käyttäjät tunnistetaan käyttämällä ulkoista RADIUS-palvelinta. VPN-palvelin lähettää saamansa käyttäjätiedot edelleen luotetulle RADIUS-palvelimelle. RADIUS-palvelin voi olla toisella Windows-palvelimella käytössä oleva IAS- tai NPS -palvelu. Tällä tavoin on helpompi hallita käyttäjien tunnistusta keskitetysti ja VPN-käyttäjiä varten voidaan luoda oma käyttäjäryhmä, joka voi olla nimeltään esimerkiksi ”Sallitut VPN-käyttäjät”. RADIUS-palvelin täten vahvistaa ensiksi käyttäjätunnuksen ja salasanan voimassaolon toimialueella sekä tarkastaa käyttäjän oikeudet VPN-palvelua varten. Tarkastuksen tehtyään RADIUS-palvelin lähettää tiedon takaisin VPN-palvelimelle, onko käyttäjä tunnistettu luotetuksi vai ei.

6.2.6 Tiedon salaus

SSTP tekniikkaan perustuva VPN-yhteys käyttää tiedon salaukseen SSL-salausta. VPN tunneli salataan yhteydenmuodostuksen ensimmäisessä vaiheessa, kun VPN asiakas on varmentanut palvelimen identiteetin. Tällöin VPN asiakas ja palvelin sopivat yhteyskohtaisista ja kertakäyttöisistä salausavaimista (If Vahinkovakuutusyhtiö Oy 2012).

SSL 3.0 -kanavan käyttö takaa tietojen 128-bittisen salauksen. Tätä samaa suojaustasoa käyttävät myös muun muassa verkkopankit ja verkkokaupat, joissa tiedot on ehdottoman tärkeää salata.

6.3 Skaalautuvuus

Suunniteltaessa uutta järjestelmää täytyy ottaa huomioon tulevaisuuden näkymät, kuten kuinka paljon yrityksen henkilöstö ja VPN-käyttäjien määrä lisääntyy. Järjestelmä täytyy suunnitella siten, että käyttäjämäärien kasvaessa järjestelmää ei tarvitsisi heti päivittää.

Toteutettaessa VPN-palvelu Windows-palvelimella käyttäjämäärä on rajaton. Rajattomalle käyttäjämäärälle on edellytyksenä Windows Server 2003/2008 Enterprise tai Datacenter -versio sekä palvelimen laitteiston tehokkuus. (Microsoft Technet 2012.)

6.4 Kustannukset

Kustannuksia koituu uuden järjestelmän toteuttamisesta palvelinlaitteiston hankinnasta ja sijoittamisesta sekä käyttöjärjestelmän hankinnasta. Kustannusten määrä riippuu myös siitä, toteutetaanko palvelin fyysisenä vai virtuaalisena.

VPN-palvelun ylläpito voidaan hoitaa joko Voimatel Oy:n ICT-osaston toimesta tai ostaa palvelun ylläpito kolmannelta osapuolelta. Kertakustannuksia koituu palvelinlaitteiston ja sen käyttöjärjestelmän hankinnasta.

7 TESTIJÄRJESTELMÄN TOTEUTUS

Testijärjestelmän toteutuksessa ei ollut mahdollista käyttää kaikkia suunniteltuja komponentteja ja menetelmiä kustannussyistä. Suunnitellun VPN-järjestelmän täydellinen toteutus olisi vaatinut muutoksia myös yrityksen Active Directory -infrastruktuurissa ja tietoliikenneyhteyksissä.

Testijärjestelmän toteutuksessa hyödynnettiin Microsoft Technetin (2007) *SSTP Remote Access Step-by-Step Guide: Deployment* -ohjeistusta.

7.1 Palvelinlaitteisto ja käyttöjärjestelmä

Palvelinlaitteistoksi oli saatavilla testikäyttöön tarkoitettu palvelin. Palvelimen tekniset ominaisuudet on lueteltu taulukossa 1.

TAULUKKO 1. Palvelimen tekniset ominaisuudet

Valmistaja	Fujitsu
Malli	Primergy TX150 S7
Prosessori	Intel ® Xeon® CPU X3430, 4 ydintä
Keskusmuisti	8 GB
Verkkokortti 1	Intel 82574L
Verkkokortti 2	A-link LAN7500 10/100/1000
Käyttöjärjestelmä	Microsoft Windows Server 2008 R2 Enterprise

Palvelimella oli asennettuna yksi verkkokortti, joten palvelimelle tuli hankkia toinen verkkokortti, jotta yhteys sisä- ja ulkoverkon välillä oli mahdollista muodostaa.

Palvelimen käyttöjärjestelmäksi valittiin suunnitelman mukaisesti Windows Server 2008 R2 x64 Enterprise.

7.2 Valmiiden palveluiden hyödyntäminen

Testijärjestelmän toteutuksessa hyödynnettiin toimialueelle ennestään asennettuja palveluita. Hyödynnettyjä palveluita olivat Dynamic Host Control Prorocol (DHCP) ja Active Directory Certificate Services (AD-CS). Koska palvelin liitettiin toimialueelle, siihen vaikuttivat myös toimialueen ryhmäkäytännöt.

7.3 Tietoliikenneyhteydet

Yhteys sisäverkkoon toteutettiin liittämällä VPN-palvelin Ethernet-verkkokaapelilla Voimatel Oy:n toimistoverkkoon. Palvelin asetettiin käyttämään kiinteää IP-osoitetta ilman oletusyhdyskäytävää. Reitit sisäverkkoon lisättiin staattisina reitteinä (static route). Staattisille reiteille asetettiin *metric*-arvot manuaalisesti. *Metric*-arvot täytyi asettaa pienemmiksi kuin julkisen verkkokortin oletusyhdyskäytävän *metric*-arvo, jotta kaikki sisäverkkoon kuuluva liikenne käyttää asetettuja reittejä.

Yhteys ulkoverkkoon eli julkinen internetyhteys täytyi toteuttaa erillisen ADSL-yhteyden avulla. IP-osoite ulkoverkkoon asetettiin DHCP:n avulla. Testausvaiheessa IP-osoite voi olla myös dynaaminen, koska osoite on katsottavissa palvelimelta ja se voidaan vaivattomasti vaihtaa myös VPN-asiakaskoneen päähän.

7.4 Varmenteen hankinta VPN-palvelimelle

VPN-palvelimelle täytyy hankkia ja asentaa oma tietokonekohtainen varmenne toimialueen päävarmenteiden myöntäjältä, jotta asiakastyöasemat voivat varmentaa VPN-palvelimen henkilöllisyyden. Varmenteen avulla myös salataan tietoliikenne VPN-tunnelissa.

Ennen varmenteen hankkimista palvelimelta täytyi ottaa pois käytöstä *Internet Explorer Enhanced Security Configuration* (IE ESC), jotta selaimen suojausasetuksia pystytään muuttamaan. Internet Explorerin suojausasetuksia täytyy laskea, että se sallii varmenteiden asennuksen. IE ESC:n sulkeminen tapahtuu valitsemalla *Server Manager* -ikkunasta *Configure IE ESC* ja valitsemalla avautuvasta ikkunasta *Administrators*-kohdan alta *Off*.

Varmenne hankitaan toimialueen varmenteiden päämyöntäjältä seuraavasti:

1. Internet Explorer käynnistetään VPN-palvelimella järjestelmänvalvojan oikeuksilla.
2. Tietoturvatasoa lasketaan asetuksista, jotta selain ei torju kaikkia yhteyspyyntöjä.
3. Yhdistetään selaimella päävarmenteiden myöntäjän url-osoitteeseen *http://palvelimen_nimi/certsrv*
4. Valitaan *Request a certificate.*
5. Valitaan *advanced certificate request*.
6. Sallitaan ActiveX–komponentin suoritus.

7. Täytetään *Name*-kenttään palvelimen nimi ja *Country/Region*-kenttään alue, esimerkiksi *vpntesti.testi.com* ja *FI.*
8. Lähetetään varmennepyyntö varmenteiden päämyöntäjälle *Submit*-painikkeella.

(Microsoft Corporation 2007.)

Tässä tapauksessa toimialueella on käytössä *auto-enrollment*, jolloin toimialueelle kuuluvien tietokoneiden ja käyttäjien pyytämät varmenteet hyväksytään automaattisesti.

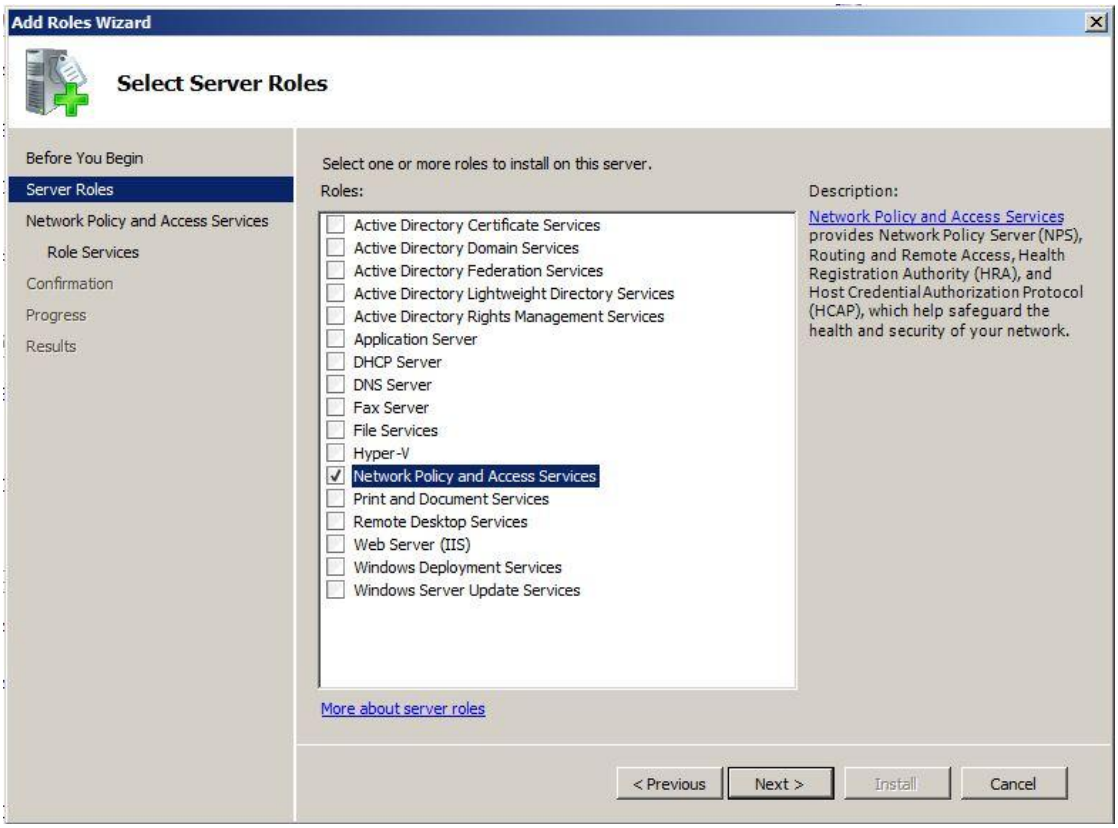
Varmenne asennetaan automaattisesti palvelimella nykyisen käyttäjän henkilökohtaiseen varmennesäilöön. Varmenne täytyy kuitenkin saada siirrettyä paikallisen tietokoneen henkilökohtaiseen varmennesäilöön, jolloin sitä voidaan käyttää palvelimen identiteetin varmentamiseen. Varmennetta hankittaessa ei ollut mahdollista asettaa vaihtoehtoa *Mark keys as exportable*, minkä vuoksi sitä ei voida siirtää käyttämällä *import/export*-menetelmää. Varmenne voidaan kuitenkin siirtää sen oikeaan paikkaan tavallisella leikkaa-liimaa-menetelmällä. Kun varmenne on siirretty oikeaan paikkaan, voidaan palvelimelle asentaa *Routing and Remote Access Services* -palvelu.

7.5 Routing and Remote Access Services -ominaisuuden asennus

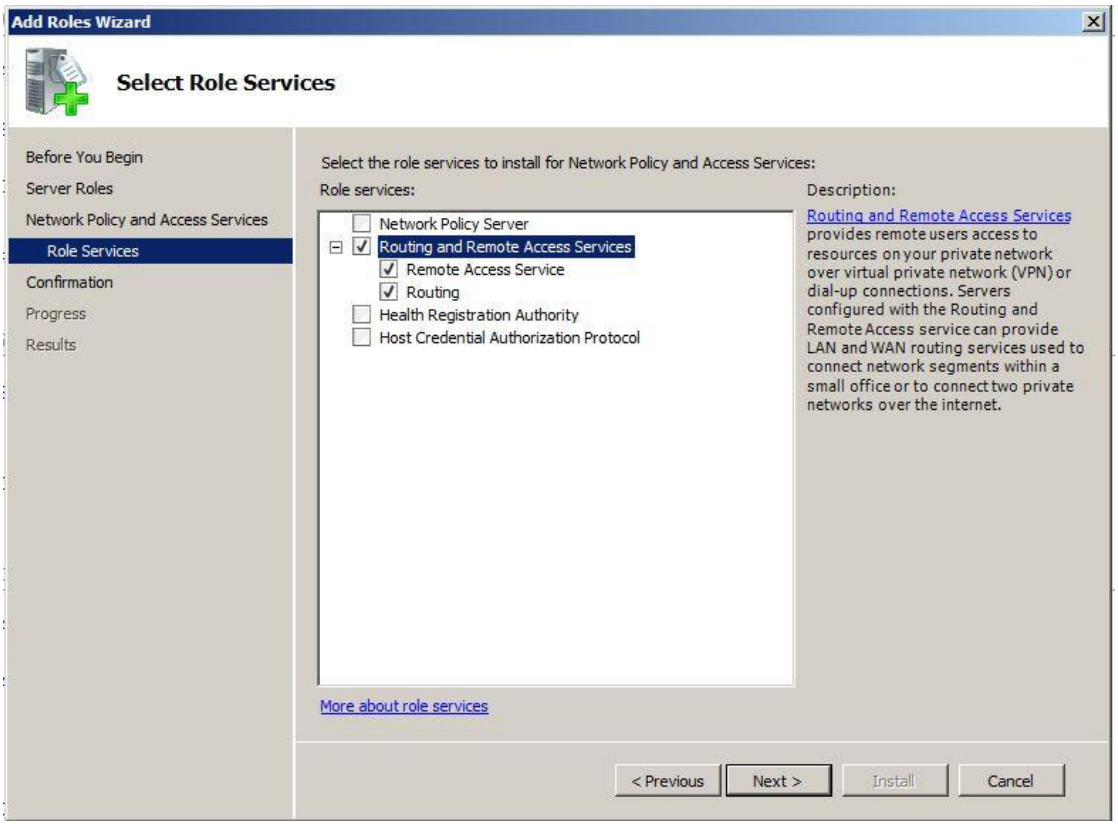
RRAS-ominaisuus asennetaan palvelimelle seuraavasti:

1. Avataan *Server Manager* -ohjelma käynnistävalikon oikealla puolella sijaitsevasta painikkeesta.
2. Valitaan *Server Manager* -ikkunasta vasemmasta navigointivalikosta *Roles* ja tämän jälkeen oikeasta reunasta *Add Roles*.
3. *Add Roles Wizard* -näyttöruudusta mennään eteenpäin *Next*-painikkeella
4. Valitaan *Network Policy and Access Services* -valintaruutu ja mennään eteenpäin painamalla kaksi kertaa *Next*-painiketta.
5. *Select Role Services* -ikkunassa valitaan *Routing and Remote Access Services* -valintaruutu.
6. Painetaan *Next*-painiketta ja tämän jälkeen *Install*-painiketta, jolloin asennus alkaa.
7. *Installation Results* -ikkunasta poistutaan *Close*-painikkeella.

(Microsift Corporation 2007.)



KUVA 6. Network Policy and Access Services -roolin valinta

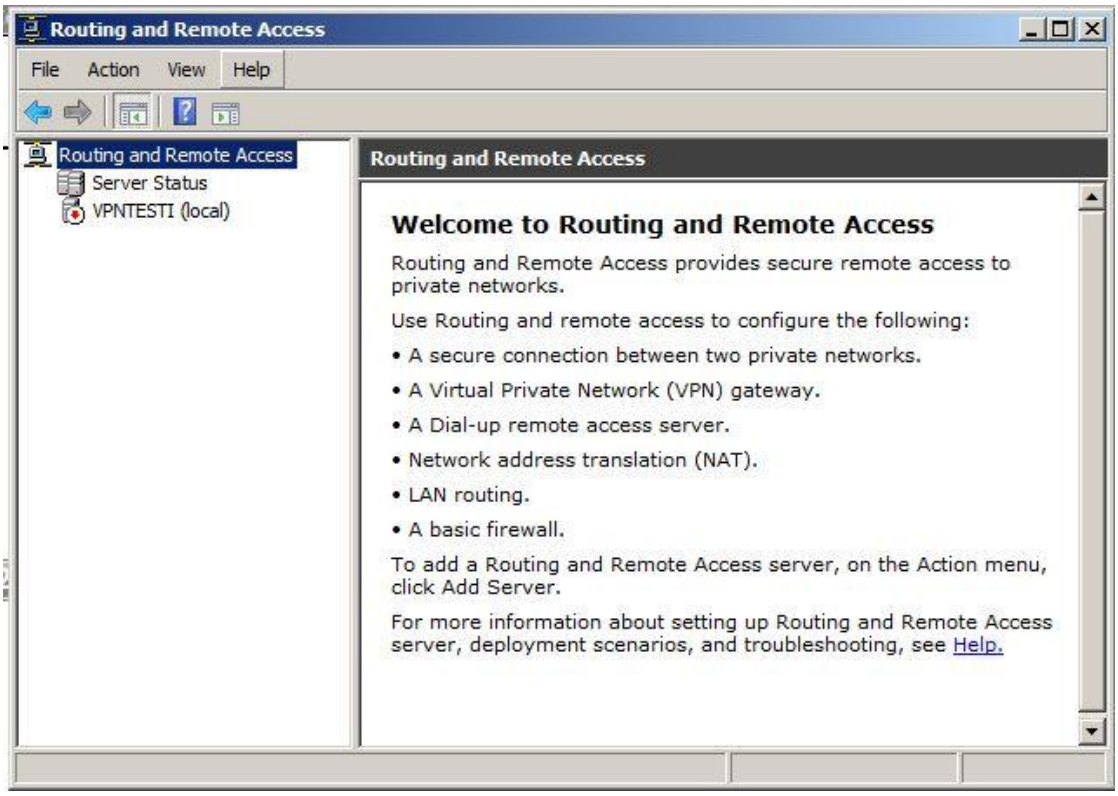


KUVA 7. Roolin sisältämien palveluiden valinta

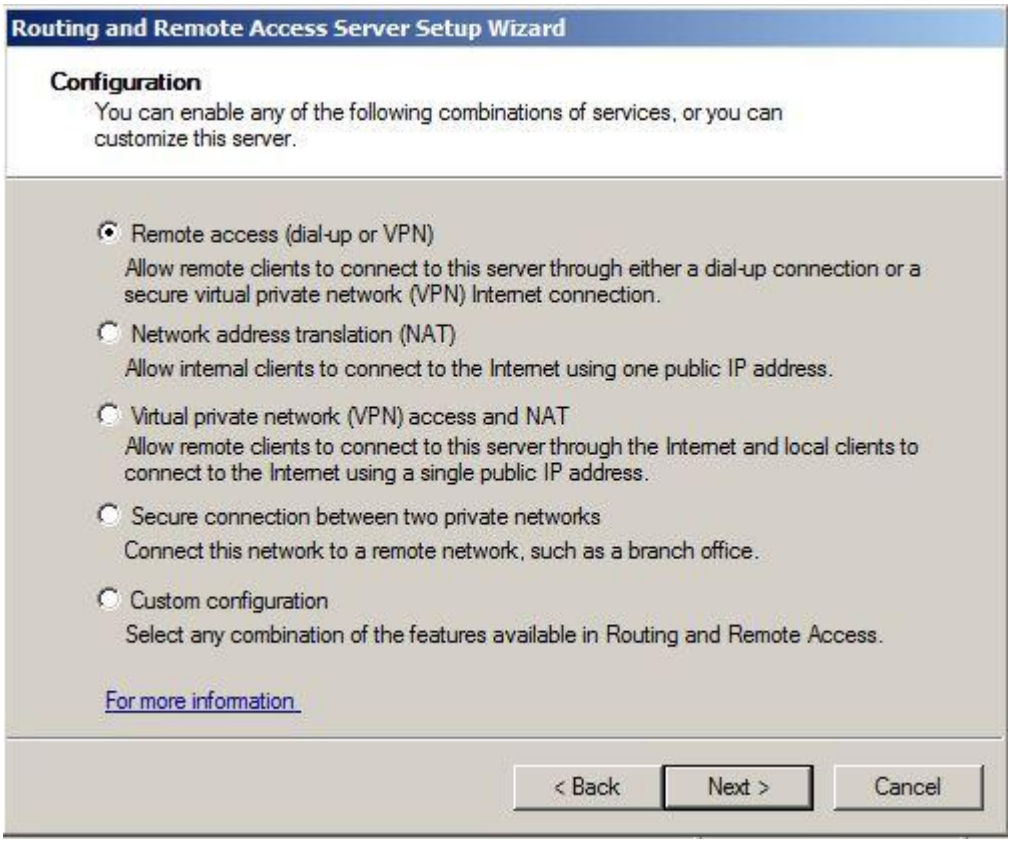
Roolin asennuksen jälkeen *Routing and Remote Access Services* konfiguroidaan ennen käyttöönottoa. Konfigurointi tapahtuu seuraavasti:

1. Avataan Käynnistä-valikko, valitaan *Administrative tools* ja painetaan *Routing and Remote Access*.
2. Painetaan avautuvassa ikkunassa palvelimen nimeä hiiren oikealla painikkeella ja valitaan *Configure and Enable Routing and Remote Access*.
3. Mennään eteenpäin *Next*-painikkeella.
4. Hyväksytään oletusasetus *Remote access (dial-up or VPN) Next*-painikkeella.
5. Valitaan *VPN*-valintaruutu ja mennään eteenpäin *Next*-painikkeella.
6. Seuraavaksi valitaan verkkokortti, joka on yhteydessä internetiin. Samassa ikkunassa oleva *Enable security on the selected interface by setting up static packet filters* -valintaruutu jätetään tyhjäksi. Normaalisti tämä täytyy jättää käyttöön, mutta testausvaiheessa tämä voidaan jättää pois.
7. Seuraavaksi asetetaan VPN-asiakkaille jaettavat IP-osoitteet. IP-osoitteet voidaan jakaa DHCP-palvelimen avulla tai VPN-palvelin voidaan asettaa jakamaan osoitteet manuaalisesti määritetyltä osoitealueelta. Testivaiheessa valitaan tavaksi *From a specified range of addresses*. Näin tehdään siksi, koska testausvaiheessa käytettävissä olevalla DHCP-palvelimella on hyvin rajattu määrä vapaita IP-osoitteita ja VPN-palvelin varaa osoitteita käyttöönsä 10 kappaletta kerrallaan. Siirrytään määrittämään käytettävät osoitteet Next-painikkeella.
8. Painetaan *New*-painiketta ja *Start IP address* kohtaan asetetaan IP-osoitteeksi *xxx.xxx.xxx.244* sekä *End IP addess* kohtaan *xxx.xxx.xxx.245*, jolloin VPN-asiakkaille jaettavien osoitteiden yhteismäärä on 2. Mennään jälleen eteenpäin *Next*-painikkeella.
9. Hyväksytään oletusasetus *Next*-painikkeella, jolloin VPN-palvelinta ei aseteta toimimaan RADIUS-palvelimen kanssa. VPN-palvelin tunnistaa käyttäjät ilman RADIUS-palvelinta Windows-käyttäjätunnusten avulla. Tässä testausvaiheessa RADIUS-palvelimen käyttö ei ole mahdollista, koska se vaatisi suurempia toimenpiteitä tuotantokäytössä olevilla palvelimilla ja näiden palvelimien asetusten muuttaminen olisi turhan suuri riski.
10. Päätetään asennus *Finish*-painikkeella. Kuitataan myös avautuva *DHCP Relay Agent* -ponnahdusikkuna *Ok*-painikkeella.

(Microsoft Corporation 2007.)



KUVA 8. Routing and Remote Access konfigurointi ikkuna



KUVA 9. Määritettävän etäyhteystavan valinta

Routing and Remote Access täytyy vielä määrittää käyttämään oikeaa varmennetta. Luvussa 7.4 asennettu varmenne otetaan käyttöön RRAS-palvelulle. Tämä varmenne lähetetään palvelimeen yhdistävälle VPN-asiakkaalle. Määritys tapahtuu seuraavasti:

1. Painetaan hiiren oikealla painikkeella palvelimen nimeä *Routing and Remote Access* -ikkunassa ja valitaan avautuvasta valikosta *Options*.
2. Mennään *Security*-välilehdelle ja valitaan ikkunassa alimmaisena olevasta alasvetovalikosta oikea varmenne.
3. Kuitataan valinta *Apply*-painikkeella, jonka jälkeen *Routing ja Remote Access Services* käynnistetään uudelleen.

7.6 Connection Manager Administration Kit

Connection Manager Administration Kit eli lyhemmin CMAK on ohjelmisto, jonka avulla voidaan luoda itse määritelty asennuspaketti VPN-yhteyden asennusta varten. Asennuspakettiin voidaan määrittää valmis yhteysprofiili VPN-yhteyttä varten, jolloin käyttäjän ei tarvitse itse määrittää profiilin asetuksia manuaalisesti. CMAK on valinnainen ominaisuus seuraavissa Windows-käyttöjärjestelmissä: Windows Server 2008 R2, Windows 7, Windows Server® 2008, ja Windows Server 2003. (Microsoft Corporation 2008.)

Asennuspaketti täytyy tehdä Windows versiolla, joka käyttää samaa prosessorin arkkitehtuuria kuin asiakaskoneet, joihin asennuspakettia aiotaan käyttää. Näin ollen 32-bittiselle Windows-työasemalle asennuspaketti täytyy tehdä 32-bittisellä Windows-versiolla ja 64-bittiselle Windows-työasemalle 64-bittisellä Windows Server 2008 R2 palvelimella. CMAK -ohjelmistoa ei voi asentaa 64-bittiseen Windows 7 -työasemaan. (Microsoft Corporation 2012.)

7.6.1 CMAK-ohjelmiston asennus Windows Server ja Windows 7 -käyttöjärjestelmiin

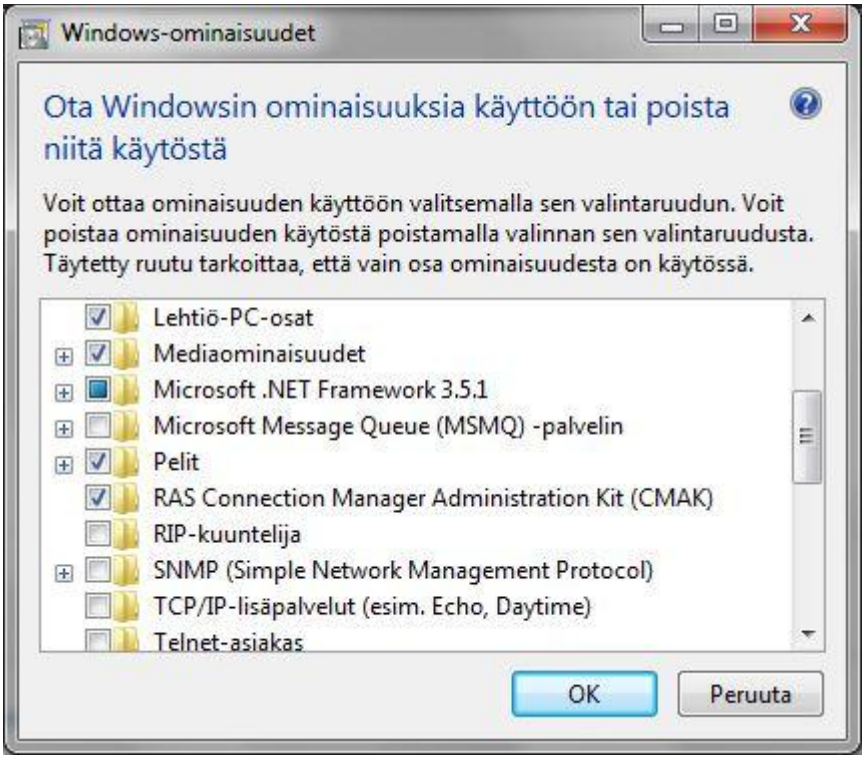
CMAK-ohjelmiston asennus 64-bittiselle Windows Server 2008 R2 -versiolle:

1. Paina *Start* ja valitse *Administrative Tools* ja *Server Manager*
2. Paina avautuvan ikkunan vasemmassa valikossa hiiren oikeaa painiketta kohdassa *Features* ja valitse *Add Features*.
3. Valitse *Features*-listalta *Connection Manager Administration Kit* ja paina *Next.*
4. Paina *Install*-painiketta *Confirm Installation Selections* sivulla
5. Kun asennus on valmis, paina *Close*-painiketta.

CMAK-ohjelmiston asennus 32-bittiselle Windows 7 työasemalle:

1. Mene *Käynnistä*-valikon kautta *Ohjauspaneeliin*, valitse *Ohjauspaneelista Ohjelmat* ja paina *Ota Windowsin ominaisuuksia käyttöön tai poista niitä käytöstä*.
2. Valitse listalta *RAS Connection Manager Administration Kit (CMAK)* ja paina *Ok*-painiketta.

(Microsoft Corporation 2012.)



KUVA 10. CMAK -ohjelmiston asennus 32-bittiseen Windows 7 -työasemaan

7.6.2 Asennuspaketin määritys

Asennuspaketti työasemiin määritetään seuraavasti Windows 7 ja Windows Server 2008 R2 -käyttöjärjestelmissä:

1. Avaa *Käynnistä-valikko* ja kirjoitetaan hakukenttään *Connection Manager Administration Kit* ja avataan ohjelma.
2. Mennään eteenpäin *Next*-painikkeella.
3. Valitaan kohde käyttöjärjestelmäksi Windows 7 tai Windows Vista.
4. Valitaan *New Profile* ja mennään eteenpäin *Next*-painikkeella.
5. Seuraavaksi *Service Name* -kenttään kirjoitetaan palvelun nimi, esimerkiksi Yrityksen VPN ja *File Name* -kenttään kirjoitetaan luotavien tiedostojen yksilöivä nimi, esimerkiksi *vpn1*.
6. Seuraavista kahdesta ikkunasta mennään eteenpäin Next-painikkeella.
7. *Add Support for VPN Connections* -ikkunassa valitaan *Phone book from this profile* ja kirjoitetaan *Always use the same VPN server* -kenttään palvelimen nimi. Palvelimen nimi tulee olla sama kuin luvussa 7.4 määritetty palvelimen nimi. Lopuksi mennään eteenpäin *Next*-painikkeella.

8. *Create or Modify a VPN Entry* -ikkunassa painetaan *Edit*-painiketta ja avautuvassa ikkunassa tehdään seuraavat toimenpiteet:
   - *General*-välilehdellä valitaan alasvetovalikosta *Only IPv4 Address.*
   - *IPv4*-välilehdellä poistetaan valinta kohdasta *Make this connection the client's default gateway.*
   - *Security*-välilehdellä valitaan ylimmästä alasvetovalikosta *Only use Secure Socket Tunneling Protocol (SSTP).* Valitaan testausvaiheessa käytettäväksi tunnistusmenetelmäksi *Microsoft CHAP Version 2 (MS-CHAP v2).*
   - Kuitataan lopuksi tehdyt valinnat *Ok*-painikkeella.
9. Poistetaan *Automatically download phone book updates* -valinta ja mennään eteenpäin *Next*-painikkeella.
10. Hyväksytään *Dial-up networking entries* painamalla *Next*-painiketta.
11. Tämä VPN-yhteys on suunniteltu toimivan split routing -tekniikalla, joten *Specify Routing Table Updates* -ikkunassa asetetaan VPN-ohjelmisto hakemaan staattiset reitit sisäverkkoon tekstitiedostosta. Tekstitiedoston muoto tulee olla esimerkiksi seuraava:

    add 10.0.0.0 mask 255.0.0.0 default metric default if default

    Kun käytetään arvoa *default*, yhteyden muodostuessa luodut reitit poistetaan, kun yhteys katkaistaan.
12. Seuraavissa kahdessa ikkunassa hyväksytään oletusasetukset *Next* -painikkeella.
13. Seuraavat kolme ikkunaa käsittelevät grafiikan lisäystä yhteyden sisäänkirjautumisikkunaan. Ikkunaan voidaan halutessaan lisätä esimerkiksi yrityksen oma logo. Testausvaiheessa grafiikkaa ei kuitenkaan lisätä, joten oletusasetukset ikkunoissa voidaan hyväksy *Next*-painikkeella.
14. Seuraavassa ikkunassa on mahdollista lisätä oma ohjetiedosto yhteyden ongelmienmääritystä varten. Tämä jätetään kuitenkin testausvaiheessa tekemättä, joten voidaan edetä seuraavaan vaiheeseen.
15. *Display Custom Support Information* -ikkunassa voidaan lisätä esimerkiksi Help Desk -yhteystiedot, jotka näkyvät VPN-asiakkaalle yhteyden sisäänkirjautumisikkunassa. Yhteystietojen lisäyksen jälkeen mennään seuraavaan vaiheeseen.
16. Seuraavassa ikkunassa voidaan asennuspaketin mukaan lisätä oma käyttöoikeussopimus, joka täytyy hyväksyä yhteyden asennusvaiheessa. Testausvaiheessa tämä jätetään huomioimatta ja voidaan edetä seuraavaan vaiheeseen.
17. Seuraava ikkuna hyväksytään *Next*-painikkeella, koska mitään ylimääräisiä tiedostoja ei lisätä asennuspakettiin.
18. Valitaan *Advanced Customizations* ja mennään eteenpäin. Seuraavassa ikkunassa syötetään taulukon 2 mukaiset arvot, koska yhteyden muodostuksen halutaan käyttävän automaattisesti käyttäjän Windows-käyttäjätunnuksia sekä *dialup*-yhteyttä ei oteta käyttöön. Jokaisen syötetyn arvon *Section name* -kentän arvo tulee olla *Connection Manager*. Jokainen syötetty arvo kuitataan *Apply*-painikkeella ja *Next*-painikkeella luodaan asennuspaketti.

(Microsoft Corporation 2012.)

TAULUKKO 2. VPN-yhteyden automaattista Windows-tunnistautumista varten tarvittavat arvot

Key name	**Value**	**File**
DialAutomatically	1	*.cmp
Dialup	1	*.cms
UseWinLogonCredentials	1	*.cms
PasswordOptional	1	*.cms
UserNameOptional	1	*.cms
DomainOptional	1	*.cms
HidePassword	1	*.cms
HideUserName	1	*.cms
HideDomain	1	*.cms

Jos asennuspaketin nimeksi asetettiin vpn1, asennuspaketti on näiden toimenpiteiden jälkeen saatavilla työasemalla seuraavasta kansiosta:

C:\Program Files\CMAK\Windows 7 and Windows Vista\vpn1\vpn1.exe

Asennuspaketti on mahdollista kopioida esimerkiksi verkkolevylle, josta se voidaan jakaa asennettavaksi työasemille.

7.7 Testaus

Testauksessa oli tärkeää ottaa huomioon SSTP VPN -yhteyden toiminta matkapuhelinverkon kautta luodun internetyhteyden kautta eli 2G- ja 3G-yhteyden avulla. Työntekijät käyttävät sisäverkon palveluita kenttätyössä ollessaan pääsääntöisesti matkapuhelinverkon kautta, koska maastossa ei ole saatavilla WLAN- tai Ethernet-verkkoyhteyttä. SSTP:n toiminta tuli testata kuitenkin myös WLAN- ja Ethernet-verkkoyhteyden kautta.

7.7.1 Työaseman määritykset ennen testausta

Palvelimen nimeä ei löydy testausvaiheessa ulkoisesta DNS-palvelusta, joten työasemaan täytyy määrittää manuaalisesti palvelimen IP-osoite ja palvelimen nimi, jotta

IP-osoitteen ja nimen yhteys voidaan ratkaista. Manuaalinen määritys tapahtui seuraavasti:

1. Kirjoitetaan käynnistävalikon hakukenttään Muistio, painetaan Muistiota hiiren oikealla painikkeella ja valitaan *Suorita järjestelmänvalvojana*.
2. Valitaan *Avaa* ja selataan kansioon *C:\Windows\System32\drivers\etc*, valitaan tiedostomuodoksi Kaikki tiedostot ja avataan tiedosto *hosts*.
3. *Hosts*–tiedostoon lisätään tiedoston loppuun rivi, jossa on VPN-palvelimen IP-osoite ja palvelimen nimi. Rivi näyttää seuraavalta:

   xxx.xxx.xxx.xxx vpntesti.yritys.fi

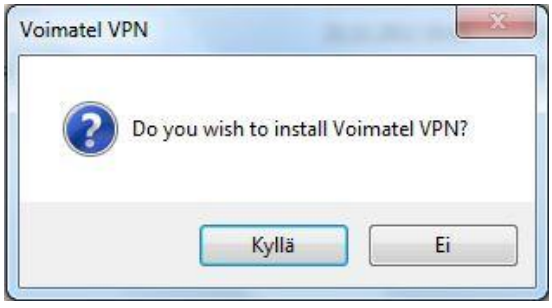
4. Tallennetaan tiedosto ja suljetaan Muistio.

(Microsoft Corporation 2012.)

Testausvaiheessa myöskään varmenteen CRL-tarkistusta ei ole mahdollista tehdä julkisen internetin puolelta. Rekisteriin joudutaan tekemään yksi uusi rekisteriavain, jotta yhteyttä muodostettaessa ei tule virheilmoitusta ja jotta CRL-tarkistus jätetään suorittamatta. Rekisteriavain lisätään *regedit*-sovelluksen avulla. Rekisteriavaimen tulee olla muotoa DWORD ja avaimen arvon tulee olla 1. (Microsoft Corporation 2012.)

7.7.2 Asennuspaketin asennus työasemaan

CMAK-työkalun avulla luotu vpn1.exe-tiedosto kopioitiin työasemaan verkkolevyn kautta työaseman ollessa toimistoverkossa. Asennus käynnistettiin tuplaklikkaamalla *vpn1.exe*-tiedostoa ja ensimmäinen ponnahdusikkuna hyväksyttiin *Yes*–painikkeella. Asennus hyväksyttiin vain sisäänkirjaantuneelle käyttäjälle. Asennuksen vaiheet näkyvät kuvissa 11 ja 12.



KUVA 11. Asennuspaketin asennuksen ensimmäinen vaihe

KUVA 12. Asennuspaketin asennuksen toinen vaihe

7.7.3 VPN-yhteyden testaus

VPN-yhteyden toimivuutta testattiin kahdella toimialueelle asennetulla Windows 7 -työasemalla, joilla oli mahdollista muodostaa yhteys julkiseen internetiin mobiililaajakaistan, WLAN-yhteyden ja Ethernet-yhteyden avulla. Yhteyden testaukseen osallistui kaksi henkilöä Voimatel Oy:n ICT-palveluiden osastolta. Testauksessa suoritettiin seuraavat vaiheet:

1. Työasema yhdistettiin internetiin.
2. Muodostettiin SSTP VPN -yhteys yrityksen verkkoon painamalla *Yhdistä*-painiketta.
3. Varmistettiin sisäverkon reittien päivittyminen työaseman reititystaulukoon kirjoittamalla komentokehotteeseen (cmd) komento *route print*.
4. Testattiin split routing -toimivuus komentokehotteessa *tracert*-komennolla. Tällä komennolla katsottiin reitti jollekin verkkosivustolle tai palvelimelle ja etenkin lähtevätkö paketit työasemalta julkisen internetyhteyden vai VPN-yhteyden kautta. Testattaviksi osoitteiksi valittiin julkisia internetsivustoja sekä yrityksen sisäverkosta löytyviä palvelimia ja sivustoja.
5. Testattiin verkkolevyjen toimivuus.
6. Testattiin palvelimien etäyhteyksien toimivuus.

Testit suoritettiin käyttäen langatonta mobiililaajakaista- ja WLAN-yhteyttä sekä Ethernet-kaapelilla ADSL- ja kaapelimodeemin kautta. Jokaisen yhteystyypin kautta VPN-yhteyden muodostus onnistui sekä verkkolevyt ja etäyhteydet toimivat halutulla tavalla. Reititys toimi myös halutulla tavalla, sisäverkkoon menevä verk-

koliikenne ohjattiin VPN-tunneliin ja kaikki muu verkkoliikenne julkiseen internetiin.

Mobiililaajakaistayhteyden kautta yhteyden muodostaminen ja sisäverkon palveluiden käyttäminen on hitaampaa, jos 3G-verkkoa ei ole saatavilla ja signaalin vahvuus on heikko.

8 YHTEENVETO

Opinnäytetyössä saavutettiin aloituspalaverissa sille asetetut tavoitteet. Työn tekeminen vaati syvällistä perehtymistä niin käytössä olevaan VPN-yhteyteen kuin Windows-käyttöjärjestelmässä toimiviin VPN-tunnelointiprotokolliin. Työssä perehdyttiin myös laajasti Windows Server -palvelimella toimiviin rooleihin ja siihen, kuinka eri rooleja hyödynnetään yrityksen tietoverkossa. Työn aikana myös ongelmanratkaisutaidot kehittyivät ja tietoa ongelmiin jouduttiin etsimään internetistä. Pari kertaa ongelmia työn aikana aiheuttivat esimerkiksi Windows-päivitykset, jolloin kaikki etäyhteydet palvelimeen katkesivat. Ongelmat saatiin kuitenkin ratkaistua ja työ saatiin tehtyä valmiiksi.

Tämän opinnäytetyön sisältöön kuului uuden Windows-pohjaisen VPN-yhteys ratkaisun suunnitelma ja uuden ratkaisun havainnollistaminen testijärjestelmän avulla. Sisältöön ei kuulunut uuden ratkaisun toteuttaminen. Voimatel Oy voi päättää, haluaako yritys tulevaisuudessa toteuttaa suunnitellun VPN-yhteyden. Uusi VPN-yhteys on suunniteltu käytettäväksi Windows 7 -käyttöjärjestelmässä, joten nykyistä L2TP/IPSec VPN -yhteyttä ei tule poistaa käytöstä niin kauan kuin yrityksessä on käytössä Windows XP -käyttöjärjestelmällä olevia työasemia.

Opinnäytetyön aihe on Voimatel Oy:n kannalta hyvin ajankohtainen, koska yritys pyrkii lisäämään etätyön määrää. Esimerkiksi tietoliikenneasentajat lähtevät työmaalle suoraan kotoa ja hoitavat tarvittavat työkohtaiset dokumentoinnit ja tuntikirjaukset internetin kautta. Tällöin VPN-yhteyden toimivuus on tärkeää.

Tästä opinnäytetyöstä valmistui hyvä perustietopaketti Voimatel Oy:n ICT-palveluiden henkilöstön käyttöön. Testijärjestelmän toteutuksesta laadittiin Voimatel Oy:n sisäiseen käyttöön myös asennusraportti, josta selviää, mitä asennuksia palvelimella tehtiin.

9 POHDINTA

Etätyö on kasvattanut viime vuosina suosiotaan ja uskon etätyön määrän lisääntyvän tulevaisuudessa entisestään. Mielestäni on tärkeää, että VPN-yhteyden käytettävyys ja tietoturva ovat tasapainossa, jotta VPN-yhteyden käyttäminen ei olisi liian vaikeaa kokemattomille käyttäjille ja jotta VPN-yhteys ei olisi tietoturvatasoltaan liian heikko.

Mielestäni tämä opinnäytetyö voi toimia hyvänä pohjustuksena toteuttamisvaiheessa tehtävien lisäselvitysten tekemiselle. Tietotekniikka sekä tietoverkot kehittyvät ja myös tässä opinnäytetyössä tehdyn uuden VPN-yhteyden suunnitelman täytyy päivittyä kulloistenkin kriteereiden mukaiseksi. Tulevaisuudessa kannattaa myös pohtia yhteistyökumppanien VPN-yhteyksien sulauttamista samaan kokonaisuuteen, jolloin VPN-yhteys olisi mahdollista luoda yhdellä kirjautumiskerralla niin oman yrityksen kuin yhteistyökumppanin verkkoon.

Mielenkiintoinen työkalu etätyöskentelyyn voi tulevaisuudessa olla myös Microsoftin kehittämä DirectAccess. Tämän tekniikan avulla yrityksen tietokoneet voivat olla yhteydessä sisäverkkoon aina internetiin yhdistettäessä ilman erillistä yhdistämistä VPN-palvelimeen. DirectAccess käyttää IPv6-osoitteita yhteyden muodostamiseen. DirectAccess-toteutus olisi mielestäni järkevä ratkaisu, kun yrityksen palvelimia ja verkkolaitteita päivitetään uudempiin versioihin. Yrityksen nykyiseen verkon rakenteeseen on SSTP VPN sopiva ratkaisu.

TERMIT JA LYHENTEET

3G	Kolmannen sukupolven matkapuhelinverkko.
4G	Neljännen sukupolven matkapuhelinverkko.
Active Directory	Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu.
ADSL	Asymmetric Digital Subscriber Line on tavallisen puhelinverkon kautta käytettävä tiedonsiirtotekniikka.
CRL	Certificate Revocation List on lista vanhentuneista varmenteista.
EAP	Extensible Authentication Protocol on käyttäjien tunnistamiseen käytettävä protokolla.
Ethernet	IEEE:n standardissa 802.3 määritelty pakettipohjainen lähiverkkotekniikka.
GRE	Generic Routing Encapsulation on IP-tunnelointiprokolla, jonka avulla tunneloidaan VPN-yhteyksiä.
HTTPS	Hypertext Transfer Protocol Secure on suojattuun tiedonsiirtoon käytetty protokolla.
IAS	Internet Authentication Service on Windows Server käyttöjärjestelmän komponentti keskitettyyn käyttäjien tunnistamiseen.
IPSec	IP Security Architecture on joukko tietoliikenneprotokollia Internet-yhteyksien turvaamiseen.
L2F	Layer 2 Forwarding on Ciscon kehittämä tunnelointiprotokolla.
L2TP	Layer 2 Tunneling Protocol on tunnelointiprokolla, joka on yhdistelmä PPTP ja L2F protokollista.
LAN	Local Area Network on esimerkiksi rakennuksen sisäisten verkkolaitteiden muodostama lähiverkko.
MPPE	Microsoft Point-to-Point Encryption on PPP ja VPN-yhteyksissä käytettävä tiedon salausmenetelmä.
MS-CHAPv2	Microsoft Challenge-Handshake Authentication Protocol on käyttäjien tunnistamiseen käytettävä protokolla.

NPS	Network Protection Service on IAS roolin korvaaja Windows Server 2008 käyttöjärjestelmässä.
PPP	Point-to-Point Protocol on protokolla, jonka avulla muodostetaan suora yhteys verkkolaitteiden välillä.
PPTP	Point-to-Point Tunneling Protocol on PPP-protokollaan pohjautuva VPN-tunnelointiprotokolla.
RADIUS	Remote Authentication Dial In User Service on käyttäjien tunnistukseen käytetty protokolla.
SCCM	System Center Configuration Manager on toimialueen tietokoneiden hallinnointiin tarkoitettu ohjelmisto.
SSL	Secure Sockets Layer on salausprotokolla, jonka avulla Internet-sovellusten verkkoliikenne voidaan suojata.
SSTP	Secure Socket Tunneling Protocol on VPN-tunnelointiprotokolla, joka käyttää SSL-salausta verkkoliikenteen suojaukseen.
TCP	Transmission Control Protocol on tietoliikenneprotokolla, jonka avulla luodaan yhteyksiä tietokoneiden välille.
WAN	Wide Area Network on tietoverkko, joka on suurempi kuin esimerkiksi kaupungin sisäinen verkko.
WLAN	Wireless Local Area Network eli langaton lähiverkko.
VPN	Virtual Private Network eli virtuaalinen yksityisverkko.

LÄHTEET

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

Odom, W. 2004. *Tietoverkot perusteet.* Helsinki: Edita.

Honda, O., Ohsaki, H., Imase, M., Ishizuka, M. & Murayama, J. 2005. *Understanding TCP over TCP: effects of TCP tunneling on end-to-end throughput and latency* [verkkojulkaisu]. [viitattu 23.10.2012]. Saatavissa: http://adsabs.harvard.edu/abs/2005SPIE.6011..138H

SSL-suojaus. [verkkosivu] If Vahinkovakuutusyhtiö Oy 2012. [viitattu 4.1.2012]. Saatavissa: http://www.if.fi/web/fi/henkiloasiakkaat/ifkansio/pages/ssl-suojaus.aspx

How Autoenrollment Works. [verkkosivu] Microsoft Corporation 2003. [viitattu 8.11.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/cc787781%28v=ws.10%29.aspx

SSTP Remote Access Step-by-Step Guide: Deployment. [verkkosivu] Microsoft Corporation 2007. [viitattu 13.11.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/cc731352%28v=ws.10%29.aspx

Connection Manager Administration Kit. [verkkosivu] Microsoft Corporation 2008. [viitattu 6.11.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/cc753977%28v=ws.10%29.aspx

Server roles in Windows Server 2008. [verkkosivu] Microsoft Corporation 2008. [viitattu 9.10.20120]. Saatavissa: http://technet.microsoft.com/en-us/library/dd283014%28v=ws.10%29.aspx

Active Directory Certificate Services (AD CS) Overview. [verkkosivu] Microsoft Corporation 2012. [viitattu 10.10.2012]. Saatavisssa: http://social.technet.microsoft.com/wiki/contents/articles/1137.active-directory-certificate-services-ad-cs-overview.aspx#Benefits

Configure RRAS with a Computer Authentication Certificate. [verkkosivu] Microsoft Corporation 2012. [viitattu 21.11.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/dd458982

Install CMAK. [verkkosivu] Microsoft Corporation 2012. [viitattu 6.11.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/cc771679.aspx

Routing and Remote Access Service. [verkkosivu] Microsoft Corporation 2012. [viitattu 12.10.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/cc754692%28v=ws.10%29.aspx

Run the CMAK Wizard to Create a Connection Profile. [verkkosivu] Microsoft Corporation 2012. [viitattu 20.11.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/cc726035.aspx

VPN tunneling protocols. [verkkosivu] Microsoft Corporation 2012. [viitattu 18.9.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/cc771298%28v=ws.10%29.aspx

Sirkiä, T. 2009. *Joka kolmas tehnyt etätöitä*. [verkkojulkaisu] Tilastokeskus 2009. [viitattu 10.9.2012]. Saatavissa: http://www.stat.fi/artikkelit/2009/art_2009-07-15_003.html

Point-to-Point Tunneling Protocol (PPTP), RFC 2637. [verkkojulkaisu] The Internet Society 1999. [viitattu 19.9.2012]. Saatavissa: http://datatracker.ietf.org/doc/rfc2637/

Etätyö. [verkkosivu] Työ- ja elinkeinoministeriö 2008. [viitattu 9.9.2012]. Saatavissa: http://www.mol.fi/mol/fi/02_tyosuhteet_ja_lait/0161_etatyo/index.jsp

Secure Socket Tunneling Protocol. [verkkosivu] Wikipedia 2012. [viitattu 22.10.2012]. Saatavissa: http://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol