Riku Huuhka

TURVALLISEN ETÄYHTEYDEN LUOMINEN

VPN ja Direct Access

TURVALLISEN ETÄYHTEYDEN LUOMINEN

VPN ja Direct Access

Riku Huuhka

Opinnäytetyö

Kevät 2011

Tietojenkäsittelyn koulutusohjelma

Oulun seudun ammattikorkeakoulu

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

Tekijä: Riku Huuhka
Opinnäytetyön nimi: Turvallisen etäyhteyden luominen
Työn ohjaaja: Jukka Kaisto
Työn valmistumislukukausi ja -vuosi: Kevät 2011 Sivumäärä: 53+5 liitesivua

---

TIIVISTELMÄ

Etätyöskentelyn merkitys osana yrityksien työkulttuuria on kasvanut huomattavasti ja etäyhteystekniikat kuten VPN (Virtual Private Network) sekä Direct Access mahdollistavat turvallisen tavan etätyöskentelyyn. Tässä opinnäytetyössä tarkastellaan näiden etäyhteystekniikoiden toimintaperiaatteita, turvallisuutta sekä asennuksen työvaiheita. Tarkastelun pääpaino on VPN- tekniikassa.

Opinnäytetyö on toteutettu pääasiallisesti kirjallisuuteen pohjautuen. Lähteinä työssä on käytetty alan julkaisuja sekä luotettavina pidettäviä Web- sivustoja. Toiminnallinen osuus, VPN- tekniikan asennus, suoritettiin Oulun seudun ammattikorkeakoulun tiloissa.

VPN- tekniikan turvallisuus perustuu siinä käytettäviin tunnelointi- ja autentikointiprotokolliin. Tunnelointi on VPN- tekniikan tärkein osa-alue, koska muodostettavalla tunnelilla yhteys salataan ulkopuolisilta. Autentikointiprotokollilla etäyhteyden osapuolet todennetaan oikeiksi. VPN- tekniikan asennuksessa tulee huomioida sen käyttötarkoitus, joka vaikuttaa myös sopivan topologian valintaan. Asennuksessa keskeisimpinä työvaiheina on Remote Access Service- toiminnon konfigurointi palvelimelle sekä käyttäjätilien, käyttöoikeuksien ja tietoresurssien määrittely.

Direct Access -toiminto mahdollistaa automaattisen yhteyden muodostuksen yrityksen verkkoon MS-IPHTTPS (Microsoft IP over HTTPS Tunneling Protocol) tunnelointiprotokollalla. Kyseinen protokolla on kehitetty, koska palomuurien ja välityspalvelimien yleistyttyä VPN- yhteyden muodostaminen ei ole aina mahdollista. MS-IPHTTPS- tunnelointiprotokollan turvallisuus perustuu IPv6 ja IPsec- protokolliin. Direct Access- toiminnon asennus tapahtuu asiakaskoneella ryhmätoiminnon kautta ja palvelimella Direct Access Management Console- toiminnon kautta.

Asiasanat: VPN, MS-IPHTTPS, Direct Access, Autentikointiprotokolla, Tunnelointiprotokolla, Topologia, OSI- malli

ABSTRACT

Oulu University of Applied Sciences
Degree programme in Business Information Systems

Author: Riku Huuhka
Title of thesis: Configuring secure remote access networks
Supervisor: Jukka Kaisto
Term and year when the thesis was submitted: Spring 2011 Number of pages: 53+5 appendices

---

ABSTRACT

The significance of remote working has increased and remote access techniques such as VPN (Virtual Private Network) and Direct Access enable a secure way for remote working. This thesis is about the operational principles, the security and the configuration stages of VPN and Direct Access. The emphasis is on the VPN technique.

This thesis is mainly based on literature and reliable Web pages. The practical part of this thesis was to configure the VPN remote access, this was performed in premises of Oulu University of Applied Sciences.

The security of the VPN technique is based on tunneling and authentication protocols. Tunneling is the most important part of the VPN technique since the connection is encrypted with the help of tunneling protocol. The users of the remote access are authenticated by authentication protocols. When configuring the VPN technique, the main purpose of the use must be specified carefully because it contributes to the selection of a suitable topology. The main stages of the VPN configuration are configuring the Remote Access Service to the server, as well as defining user accounts, user permissions and shared information resources.

Direct Access is an automatic connectivity solution that allows clients to connect to the corporate intranet by using MS-IPHTTPS (Microsoft IP over HTTPS Tunneling Protocol). Due to an intervening firewalls and proxy servers the VPN connection is not always possible. MS-IPHTTPS was designed to solve this problem. The security of MS-IPHTTPS is based on the IPv6 and IPsec protocols. The Direct Acces client configuration is performed through Group Policy and server configuration through Direct Access Management Console.

Keywords: VPN, MS-IPHTTPS, Direct Access, Authentication Protocol, Tunneling Protocol, Topology, OSI Model

SISÄLLYS

1 JOHDANTO

Etätyöskentelyn merkitys yrityksissä osana työkulttuuria on kasvanut merkittävästi. Turvallinen etäyhteystekniikka kuten VPN (Virtual Private Network), mahdollistaa etäkäyttäjän turvallisen pääsyn yrityksen tietoresursseihin. VPN- tekniikan turvallisuus perustuu tunnelointi ja autentikointimenetelmiin, jossa käyttäjän muodostama etäyhteys salataan ulkopuolisilta sekä muodostettavan yhteyden osapuolet todennetaan oikeiksi. Palomuurien ja välityspalvelimien yleistyttyä esimerkiksi hotelleissa, VPN-tekniikalla luotava etäyhteys ei kuitenkaan ole aina mahdollista. Tähän ongelmaan yhdeksi ratkaisuksi on kehitetty uudentyyppinen etäyhteystekniikka, MS-IPHTTPS (Microsoft IP over HTTPS Tunneling Protocol), jossa etäyhteys muodostetaan suojatun intranet- sivuston kautta. Yhteyden muodostamiseen käytetään Microsoft Windows 7- käyttöjärjestelmässä olevaa Direct Access -toimintoa, joka tällä hetkellä löytyy kuitenkin vain Enterprise ja Ultimate versioista. MS-IPHTTPS- tekniikka edustaa uudempaa etäyhteystekniikkaa ja siinä käytettävät protokollat poikkeavat hyvin paljon VPN- yhteydessä käytettävistä protokollista

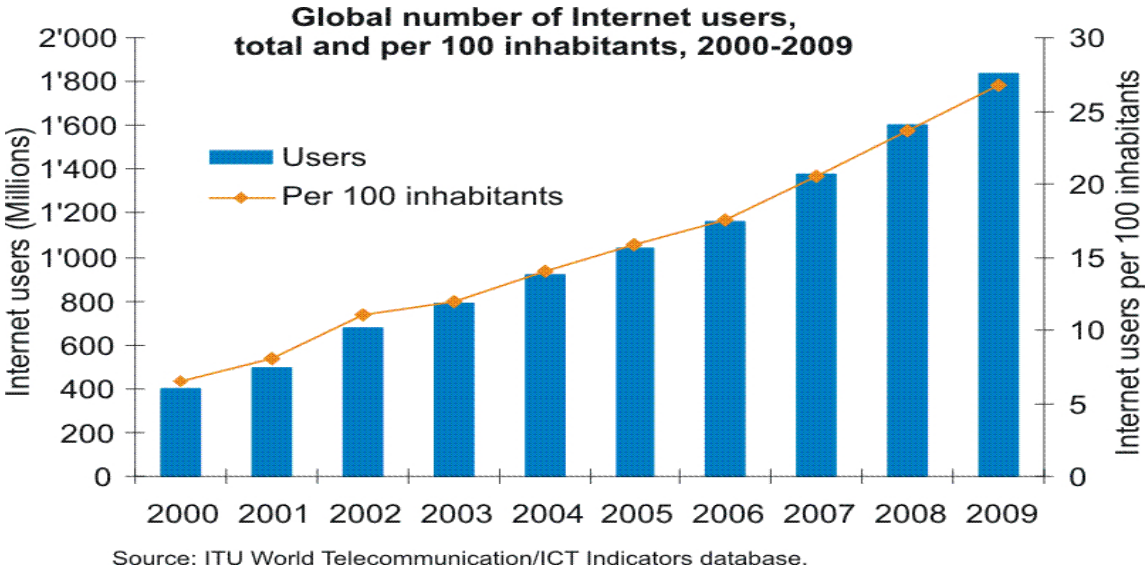
Tässä opinnäytetyössä tarkastellaan VPN- tekniikan topologioita, sen turvallisuuteen vaikuttavia protokollia sekä kuvataan VPN- tekniikan asennuksen keskeisimmät työvaiheet. Opinnäytetyössä tarkastellaan lisäksi MS-IPHTTPS- tunnelointiprotokollan toimintaperiaatetta, turvallisuutta sekä kuvataan Direct Acces- tekniikan asennuksen keskeisimmät työvaiheet.

Opinnäytetyössä ei ole toimeksiantajaa, vaan aihe on valittu oman mielenkiinnon pohjalta. VPN- tekniikka on yleisesti varsin käytetty etäyhteystekniikka ja opinnäytetyö tarjoaa hyvän mahdollisuuden tietojen syventämiseen aiheesta. Direct Access- etäyhteystekniikalla muodostettava MS-IPHTTPS- etäyhteys on vielä suhteellisen uusi asia ja Microsoft odottaa sen syrjäyttävän VPN- tekniikan vielä tulevaisuudessa. Sen vuoksi on perusteltua käsitellä myös tätä aihetta opinnäytetyössä.

Työssä käsitellään aluksi tietoturvaa niiltä osin, kuin se on etäyhteystekniikoissa oleellista sekä kuvataan tiedonsiirtoon vahvasti liittyvän OSI- mallin merkitys. Tämän jälkeen työssä käsitellään VPN- tekniikkaan liittyvät topologiat sekä autentikointi- ja tunnelointiprotokollat. Seuraavaksi työssä käsitellään MS-IPHTTPS yhteyden muodostus Direct Access toiminolla sekä esitellään siihen liittyvät protokollat. Viimeisenä käsiteltävänä aiheena työssä kuvataan VPN sekä Direct Access tekniikoiden asennuksen keskeisimmät työvaiheet. Lopuksi vedetään yhteen työn tärkeimmät asiat ja pohditaan työn onnistumista.

2 TIETOTURVA

Internetin käyttäjien kasvun myötä (KUVIO 1) tietoverkoissa tapahtuva rikollisuus on myös kasvanut räjähdysmäisesti ympäri maailman. Yrityksiin suunnatut tietomurrot sekä palvelunestohyökkäykset ovat muuttuneet kymmenessä vuodessa yhä ammattimaisemmaksi toiminnaksi. Ciscon johtavan tietoturvatutkijan Patrick Petersonin mukaan Internet-rikollisuus on muuttumassa yritystoiminnan kaltaiseksi, missä nettirikolliset toimivat matkimalla tavallisten organisaatioiden strategioita ja parhaita käytäntöjä sekä liittoutumalla keskenään (Cisco 2009a, hakupäivä, 24.9.2010).



KUVIO 1. *Internet-käyttäjien määrä globaalisti vuosina 2000 – 2009* (ITU 2010a, hakupäivä 24.9.2010.)

Kuviosta nähdään internetin käyttäjien määrän kasvu vuodesta 2000 vuoteen 2009. Käyttäjien määrä vuonna 2000 on ollut noin 400 miljoonaa, joista se on kasvanut vuoteen 2009 noin 1,8 miljardiin. Prosentuaalisesti koko maailman väestöstä internetiä käytti vuonna 2000 noin 7 %, kun taas vuonna 2009 vastaava prosenttiluku oli jopa noin 28 %.

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI, määrittelee tietoturvaoppaassaan tietoturvan seuraavasti:

> Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta. (VAHTI 2003, 2.)

Viestintäviraston tietoturvaorganisaatiolle (CERT-FI) tulleiden ilmoitusten perusteella (TAULUKKO 1) haavoittuvuudet Suomessa ovat lisääntyneet merkittävästi vuoden aikana. Lisäksi Social Engineering ilmoitukset ovat olleet pienessä nousussa ja palvelunestohyökkäykset rajussa laskussa.

TAULUKKO 1. *CERT-FI yhteydenotot 2009- 2010* (CERT-FI 2010, hakupäivä 27.9.2010.)

CERT-FI-yhteydenotot nimikkeittäin	1-6/2010	1-6/2009	Muutos
Haastattelu	**49**	61	-20 %
Haavoittuvuus tai uhka	**104**	65	+60 %
Haittaohjelma	**789**	1055	-25 %
Neuvonta	**244**	188	+30 %
Hyökkäyksen valmistelu	**22**	24	-8%
Tietomurto	**65**	65	±0 %
Palvelunestohyökkäys	**22**	40	-45 %
Muu tietoturvaongelma	**31**	46	-33 %
Social Engineering	**69**	59	+17 %
Yhteensä	**1395**	**842**	**-12 %**

Nykyisin tietoturva mielletään useasti vain tietotekniikassa ilmeneviin ongelmiin, kuten tietomurtoihin, viruksiin ja matoihin vaikka käsitteenä tietoturva on huomattavasti laajempi. Ohjelmistojen haavoittuvuuksiin perustuvat tietomurtohyökkäykset ovat lisääntyneet merkittävästi 2000- luvulla.

Hyökkäysmenetelmät jaetaan kolmeen luokkaan, tiedusteluhyökkäys (Reconnaissance Attack), pääsyhyökkäys (Access Attack) sekä palvelunestohyökkäys (Dos Attack). Palvelunestoyökkäys eivät kuitenkaan ole uhka turvallisille etäyhteyksille ja sen vuoksi asiaa ei käsitellä tässä syvemmin.

Tiedusteluhyökkäyksissä hakkerit pyrkivät paljastamaan käytössä olevan järjestelmän sekä keräämään tietoa varsinaista pääsy- tai palvelunestohyökkäystä varten. Tyypillisessä tiedusteluhyökkäyksessä hakkeri pingaa IP- osoitteita ja löydettyään sopivan kohteen suorittaa porttiskannauksen nähdäkseen millaisia ohjelmia uhrilla on päällä ja millainen käyttöjärjestelmä hänellä on. (Liu, Lucas & Singh 2006, 77.) Yksi tehokkaimmista tiedusteluhyökkäysmetodeista on salakuuntelumenetelmä, (Eavesdropping) mies välissä hyökkäys (Man in the middle). Man in the middle- hyökkäyksen tarkoituksena on murtaa kahden pisteen välinen verkkoyhteys asettumalla niiden väliin. Murrettuaan yhteyden, hyökkääjän on mahdollista salakuunnella ja seurata dataliikennettä, sekä halutessaan myös muokata tai muuttaa lähetettyä dataa.

Pääsyhyökkäyksessä hakkeri pyrkii murtautumaan verkkoon ja sen resursseihin, kuten tiedostoihin, sähköposteihin ja web- palvelimiin. Murtautuminen tapahtuu useasti erityisellä salasanamurto-ohjelmalla tai tutkimalla verkkoliikenteessä liikkuvia IP- paketteja, joissa salasanoja ei ole salattu mitenkään. Yksi tunnetuimmista pääsyhyökkäysmetodeista on esimerkiksi Unauthorized Access Attack. (Deal 2005, 22, 23.)

Suojaamattomilla etäyhteyksillä on riski joutua tiedustelu- ja pääsyhyökkäysten kohteiksi. Turvallisilla etäyhteystekniikoilla, kuten VPN (Virtual Private Network), hyökkäyksen kohteeksi joutuminen estetään erilaisilla tunnelointi- ja autentikointiprotokollilla.

3 OSI-MALLI

Open Systems Interconnection Reference Model eli OSI- mallilla kuvataan kerroksittain kaikki ne palvelut ja tiedonsiirtoprotokollat, joita tiedonsiirrossa tarvitaan. Kerroksia on kaikkiaan seitsemän, joista jokainen kerros tarjoaa palveluja aina yhtä kerrosta ylemmäksi sekä käyttää yhtä alemman kerroksen palveluja.

TAULUKKO 2. *OSI- mallin kerrokset* (Mukaillen Holttinen 2002, 428-432)

7. Sovelluskerros	**FTP, HTTP, SMTP, NFS, SNMP**
6. Esitystapakerros	**GIF, JPEG, MPEG, MP3, FLASH**
5. Istuntokerros	**SQL, Apple talk, WinSock**
4. Kuljetuskerros	**TCP, UDP, SPX**
3. Verkkokerros	**IP, ICMP, ARP, RARP, RIP, IGRP,OSPF, EIGRP**
2. Siirtoyhteyskerros	**HLDC, LLC, MAC**
1. Fyysinen kerros	**Ethernet, Token Ring**

OSI- mallin seitsemäs kerros eli sovelluskerros on kaikkein lähimpänä käyttäjää. Loppukäyttäjäsovellukset, kuten Internet- selain on yksi esimerkki sovelluskerroksen käyttäjälle tarjoamista palveluista. Sovelluskerros lisäksi muodostaa yhteyden toisen osapuolen kanssa sekä synkronoi sopimukset viankorjaukseen liittyvistä menettelytavoista. (Holttinen, 2002, 428.)

Esitystapakerroksen tehtävänä on varmistaa, että lähettäjän sovelluskerroksesta lähetetty informaatio vastaanottajan sovelluskerrokselle on luettavissa. Esitystapakerros salaa myös tarvittaessa verkon läpi lähetettävän datan sekä purkaa salauksen vastaanotettaessa ja lähettää sen sovelluskerrokselle. (Holttinen 2002, 429.)

Istuntokerros muodostaa kahden päätelaitteen väliset istunnot, valvoo niiden tiedonsiirtoa, synkronoi keskustelut sekä purkaa istunnot. Istuntokerros tarjoaa myös provisioinnin tehokkaalle tiedonsiirrolle, palveluluokille, tietoturva-auktorisoinnille ja istunto-, esitystapa- ja sovelluskerrosten ongelmien poikkeusraportoinnille. (Holttinen, 2002, 429.)

Kuljetuskerros vastaanottaa datan istuntokerrokselta ja pilkkoo sen lähetystä varten ja varmistaa että lähetys tapahtuu virheettömästi sekä oikeassa järjestyksessä. Lähetyksen jälkeen vastaanottajan kuljetuskerros kokoaa datan yhtenäiseksi datavirraksi. Kuljetuskerros myös kontrolloi tiedonsiirtoa siten että lähettäjä ei voi lähettää enempää dataa kuin vastaanottaja voi vastaanottaa. (Cisco 1999, hakupäivä 29.11.2010.)

Verkkokerroksen tehtävänä on määritellä verkko-osoitteet. Osa verkkokerroksen toteutuksista, kuten IP (Internet Procotol), määrittelee verkko-osoitteet reittivalinnan mukaan vertaamalla lähettäjän verkko-osoitetta vastaanottajan verkko-osoitteeseen sekä käyttämällä aliverkon peitettä. Koska verkkokerroksessa määritellään myös verkon topologia, reitittimet voivat tämän kerroksen ansiosta määritellä kuinka paketit välitetään eteenpäin. Suurin osa verkon suunnittelu ja konfiguraatiotyöstä tapahtuu verkkokerroksella. (Cisco 1999, hakupäivä 29.11.2010.)

Siirtoyhteyskerros tarjoaa luotettavan datan siirron fyysisen yhteyden yli ja se on jaettu kahteen alikerrokseen, jotka ovat LLC (Logical Link Control) sekä MAC (Media Access Control). LLC muodostaa ja ylläpitää yhteyden muiden laitteiden kanssa sekä tarjoaa palvelinyhteydet tiedonsiirtoa varten. MAC-alikerros ylläpitää taulua fyysisistä laiteosoitteista. Fyysinen osoitteistus määrittelee sen kuinka laitteet on osoitteistettu siirtoyhteyskerroksella. Verkkotopologia koostuu siirtoyhteyskerroksen spesifikaatioista, jotka määrittelevät miten laitteet tulee olla fyysisesti kytkettynä missäkin topologiassa. (Holttinen, 2002, 431.)

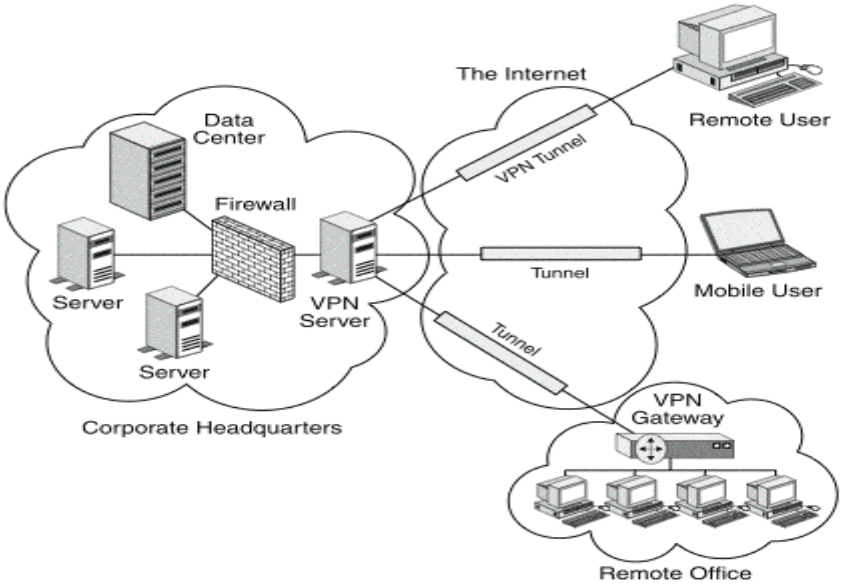
Fyysinen kerros määrittelee sähköiset, mekaaniset sekä toiminnalliset spesifikaatiot verkossa olevien päätelaitteiden fyysisen yhteyden aktivointiin,

ylläpitoon sekä yhteyden katkaisemiseen. Fyysisen kerroksen määritelmiin kuuluvat esimerkiksi jännitetasot, fyysiset tiedonsiirtonopeudet sekä siirtoyhteyksien enimmäispituudet ja erilaiset liittimet. Fyysisen kerroksen tehtävänä on siirtää databitit fyysisessä mediassa. Databitit koostuvat ykkösistä ja nollista mutta ne muutetaan fyysisen kerroksen toimesta sähkösignaaleiksi, valopulsseiksi tai langattomiksi signaaleiksi. Signaalit siirretään verkkokortin kautta kupari- tai kuitukaapeliin tai ne lähetetään langattomina signaaleina. Dataa vastaanotettaessa, verkkokortti muuntaa signaalit tai pulssit takaisin ykkösiksi ja nolliksi ja lähettää ne sitten OSI- mallin ylemmälle tasolle. (Holttinen, 2002, 432.)

4 VPN

VPN (Virtual Private Network) mahdollistaa turvallisen etäyhteyden esimerkiksi yrityksen tai organisaation lähiverkkoon turvattoman internetin yli. VPN mahdollistaa yrityksen työntekijöille varsin turvallisen tavan etätyöskentelyyn mistäpäin tahansa toimiston ulkopuolelta ja pääsyn yrityksen järjestelmiin, kuten sähköpostiin, tietokantoihin, tulostimiin sekä dokumentteihin. VPN- ratkaisun turvallisuus perustuu tunnelointitekniikkaan etäyhteyttä muodostettaessa. Kahden pisteen välinen yhteys salataan erityisellä tunnelointiprotokollalla kuten Point- to- Point Tunneling Protocol (PPTP), sekä autentikointiprotokolalla kuten PAP. Yhteyden tunneloinnilla salataan siis kahden tai useamman pisteen välinen dataliikenne ulkopuolisilta ja yhteyden autentikoinnilla varmistetaan VPN- yhteyden osapuolet oikeaksi.

VPN tekniikoita on käytännössä kahdenlaisia, Remote Access VPN sekä Site - to -Site VPN (Held 2005, 5). Remote Access VPN tekniikalla (KUVIO 2) voidaan nimensä mukaisesti luoda etäyhteys esimerkiksi yrityksen lähiverkkoon, joka puolestaan mahdollistaa pääsyn yrityksen tietoresursseihin. Etäyhteyden muodostamisessa käytetään erityistä etäyhteyspalvelinta (Remote Access Server), jonka tehtävänä on autentikoida sekä vahvistaa sille tulevat etäyhteyspyynnöt. (Gupta 2002, 13.) Remote Access VPN tekniikan avulla yrityksen työntekijät voivat halutessaan muodostaa turvatun etäyhteyden yrityksen tietokoneisiin sekä päästä näin käsiksi tarvitsemiinsa tietoihin vaikkapa kotoa käsin. Työntekijät jotka matkustavat paljon voivat myös halutessaan muodostaa etäyhteyden yrityksen päätelaitteisiin esimerkiksi hotellihuoneestaan. (Held 2005, 5.)



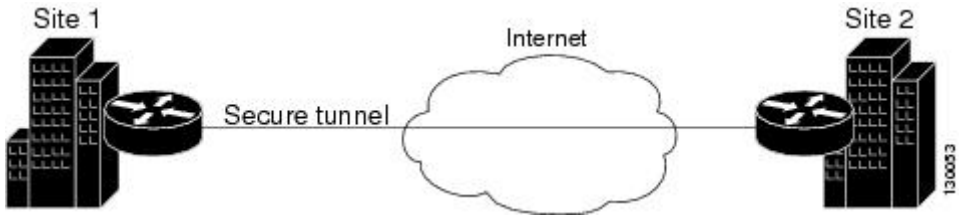
KUVIO 2. *VPN arkkitehtuurimalli* (Gupta 2002, 13.)

Vanhemmissa teoksissa Site -to -Site VPN yhteyksiä kutsutaan myös Intranet ja Ekstranet VPN- yhteyksiksi. Site -to -Site VPN yhteyksissä muodostettava tunneli tehdään kahden reitittimen välille. Intranet VPN mahdollistaa esimerkiksi yrityksen päätoimipaikan sekä sivutoimipisteen lähiverkon yhdistämisen. Lähiverkkojen yhdistämisellä mahdollistetaan sivutoimipisteen pääsy samoihin järjestelmiin ja tietokantoihin mitä yrityksen päätoimipaikassa käytetään. Hyödyntämällä VPN-tekniikkaa voidaan myös saavuttaa huomattavia taloudellisia säästöjä yrityksen lähiverkkojen yhdistämisessä, varsinkin jos Intranetin käyttäjiä on useissa toimipaikoissa ympäri maailman. Ekstranet VPN poikkeaa Intranet VPN:stä siltä osin, että se ei ole täysin suljettu ulkopuolisilta. Ekstranet VPN mahdollistaakin kontrolloidun pääsyn yrityksen verkossa oleviin järjestelmiin ja tietoihin muun muassa asiakkaille, yhteistyökumppaneille sekä tavaran toimittajille. (Gupta 2002, 36, 38.) Held kuitenkin tyrmää teoksessaan, että ei ole olemassa minkäänlaista Ekstranet VPN- tekniikkaa, vaan rajaa tekniikat hyvin jyrkästi kahteen olemassa olevaan VPN-tekniikkaan, eli Site -to -Site, sekä Remote Access tekniikkaan (Held 2005, 5).

4.1 VPN topologiat yhteyden muodostuksessa

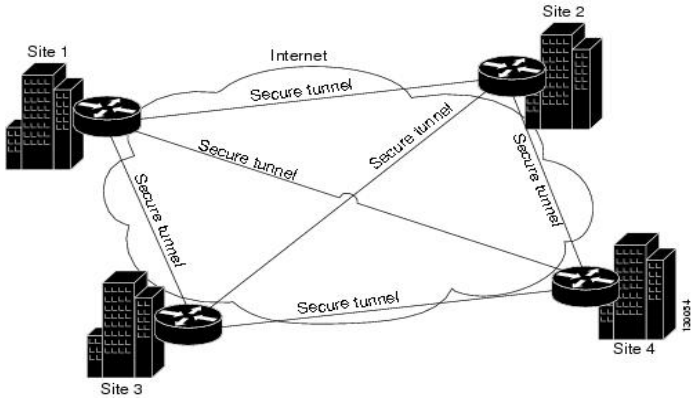
VPN- tekniikan käyttöönotossa, ennen konfigurointia, tulisi ensiksi suunnitella hyvin tarkkaan, millaiseen käyttöön virtuaalista yksityisverkkoa mahdollisesti tarvittaisiin, ketkä sitä yrityksessä mahdollisesti tulisivat käyttämään ja miten se toisi lisäarvoa yritykselle. Käyttämällä aikaa huolelliseen suunnittelutyöhön vältytään mahdollisilta ikäviltä yllätyksiltä, joita esimerkiksi yrityksen laajeneminen voisi tuoda tullessaan. Seuraavassa esittellään yleisimmät käytössä olevat VPN- topologiat eli konfiguraatiometodit.

Point- to- Point VPN- topologialla (KUVIO 3) tarkoitetaan tunneloitua yhteyden muodostusta kahden laitteen välille, kuten käyttäjän tietokoneen sekä yrityksen palvelimen välille. Tämä on VPN- topologioista yksinkertaisin malli.



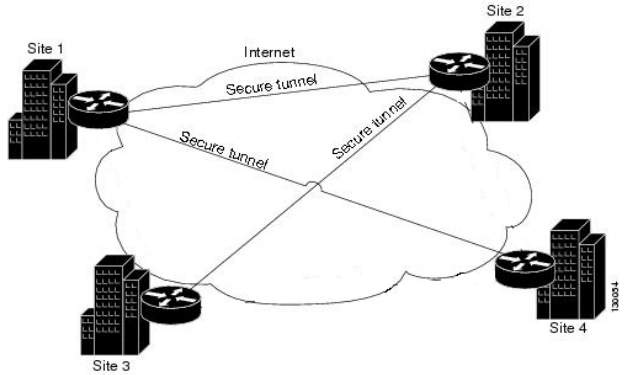
KUVIO 3. *Point- to- Point topologia* (Cisco 2010, 21-3, hakupäivä 21.10.2010.)

Meshed topologioita on olemassa kahdenlaisia, Fully Meshed (KUVIO 4) ja Partially Meshed (KUVIO 5) topologiat. (Lucas, 2006, 217). Fully Meshed topologia on erittäin luotettava, koska näin konfiguroidut laitteet ovat kaikki yhteydessä toisiinsa sekä esimerkiksi yhden yhteyden mennessä poikki, kaikki muut yhteydet ovat silti vielä toimivia. Yhteyden mennessä poikki yhdestä solmusta dataliikenne ohjataan automaattisesti toimivien solmujen kautta, jolloin myöskään suuria katkoksia tiedonsiirrossa ei pääse syntymään. (Cisco 2010, 21-4, hakupäivä 21.10.2010.) Huonona puolena topologiassa on sen ylläpidolliset vaikeudet, koska lisättäessä uusi solmu (reititin) topologiaan, joudutaan kaikki muutkin topologiaan kuuluvat solmut päivittämään. Tällaisen topologian ylläpito voi tulla myös hyvin kalliiksi, koska joka yhteydelle joudutaan hankkimaan oma VPN- laitteensa. (Liu, Lucas, Singh, 2006, 217.)



KUVIO 4. *Fully Meshed topologia* (Cisco 2010, 21-4, hakupäivä 21.10.2010.)

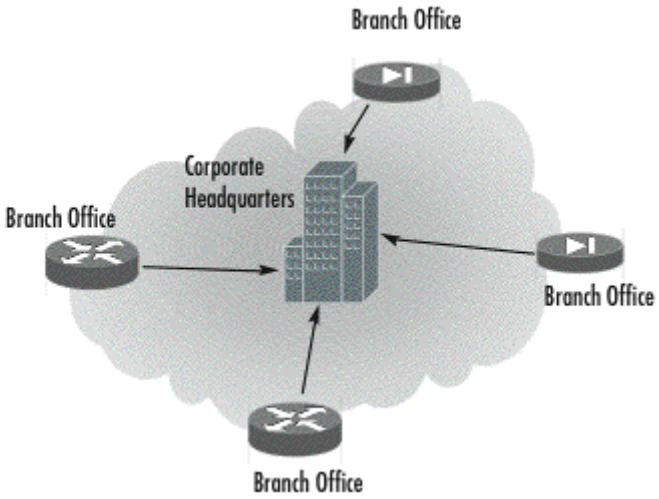
Partially Meshed topologia (KUVIO 5) on yksinkertaistetumpi malli Full- Mesh topologiasta. Tässä jokaista laitetta ei yhdistetä toisiinsa, vaan lisätään pelkästään muutama vaihtoehtoinen reitti, jonka avulla yhteys saavutetaan jokaiseen pisteeseen. (Learn Networking 2008, hakupäivä 21.10.2010.)



KUVIO 5. *Partially Meshed topologia* (Mukaillen Cisco 2010, 21-4, hakupäivä 21.10.2010.)

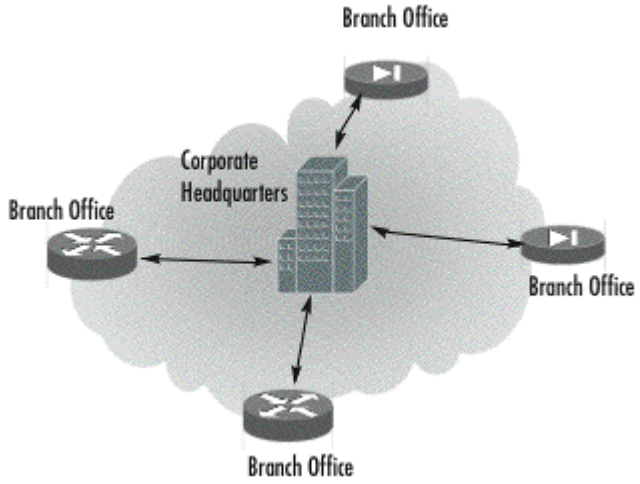
Star topologiassa (KUVIO 6) jokainen solmu yhdistetään vain keskukseen, eikä solmujen välistä dataliikennettä sallita. Yritykset käyttävät useasti tätä mallia lisätessään sivutoimipaikkojaan, koska tällaisen topologian ylläpito on helppoa. Muodostettaessa etäyhteys uudesta toimipaikasta keskukseen (yleensä yrityksen päätoimipaikkaan), riittääkin vain että tiedot päivitetään keskukseen.

Tässä topologiassa keskuksen merkitys korostuu huomattavasti, sillä mikäli keskuspisteen yhteydet lakkaavat toimimasta, myös kaikkien sivutoimipaikkojen yhteydet menevät poikki. Mikäli yhteys halutaan luoda kahden sivutoimipisteen välille, on se mahdollista vain ohjaamalla dataliikenne keskuspisteen kautta. (Liu, Lucas, Singh 2006, 219.)



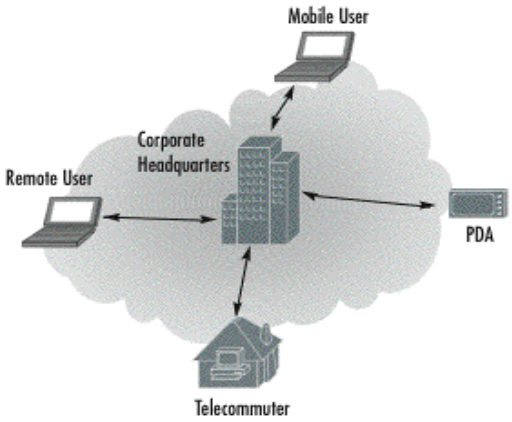
KUVIO 6. *Star topologia* (Liu, ym. 2006, 219.)

Hub and Spoke topologia (KUVIO 7) on hyvin pitkälle samankaltainen Star topologian kanssa ja sitä käytetään yleensä Intranet VPN- yhteyden muodostamiseen. Näiden kahden topologian suurin ero on siinä, että Hub and Spoke topologia mahdollistaa yhteydenmuodostuksen myös sivupisteiden kesken. Tässä mallissa keskuspiste toimii ainoastaan datan tarkastus sekä välityspisteenä. Kaiken keskuspisteen kautta kulkevan datan salaus puretaan, tarkistetaan, salataan uudestaan sekä lähetetään eteenpäin oikeaan sivutoimipisteeseen. Tämän topologian käyttö on kuitenkin riskialttiimpaa kuin Star topologian, sillä hyökkääjään päästyä yhden sivutoimipisteen verkkoon on hänen mahdollista murtautua myös muiden sivutoimipisteiden verkkoon ilman että hänen tarvitsisi ensiksi murtautua parhaiten suojattuun keskuspisteeseen. (Liu, ym. 2006, 219.)



KUVIO 7. *Hub and spoke topologia* (Liu, ym. 2006, 219.)

Remote Access topologia (KUVIO 8) perustuu Hub and Spoke topologiaan. Tämä topologiamalli mahdollistaa esimerkiksi yrityksen etätyöntekijöiden turvalliset mobiiliyhteydet. (Liu, ym. 2006, 219.) Tämä mahdollistaa yrityksen työntekijöille joustavamman tavan työskennellä sekä tehostaa yrityksen toimintoja merkittävästi. Remote Access – yhteyden muodostamisessa käytetään yleensä kahta mahdollista tekniikkaa, IP-Security (IPsec) sekä Secure Sockets Layer (SSL). (Cisco 2008, hakupäivä 25.10.2010.)



KUVIO 8. *Remote Access topologia* (Liu, ym.2006, 219.)

4.2 Autentikointiprotokollat

Autentikoinnilla eli todentamisella tarkoitetaan prosessia, jonka avulla varmistutaan lähettäjän, sekä vastaanottajan oikeellisuudesta. Yksinkertaisimmillaan autentikoinnissa vaaditaan pelkästään käyttäjätunnus ja salasana, mutta turvallisimmissa sekä myös teknisesti haastavammissa yhteyksissä autentikointi perustuu julkisen avaimen, sekä salatun avaimen salaukseen.

PAP

Password Authentication Protocol (PAP) on yksi vanhimpia salasanaan pohjautuvia autentikointimenetelmiä etäyhteyksissä ja se perustuu kaksisuuntaiseen kättelytoimenpiteeseen. Yhteyden muodostuksessa etäkäyttäjän ja kohteen välille etäkäyttäjä lähettää vastaanottajalle käyttäjätunnuksen sekä salasanan. Vastaanottavana osapuolena toimii hyvin useasti palvelin johon salasana on konfiguroitu valmiiksi jokaiselle käyttäjätunnukselle. Mikäli palvelin hyväksyy annetun käyttäjätunnuksen sekä salasanan, siitä lähetetään hyväksymiskuittaus käyttäjälle, muussa tapauksessa palvelin lähettää virheviestin käyttäjälle sekä katkaisee yhteyden. PAP autentikoinnissa on myös muutamia heikkouksia. Kyseisellä protokollalla suojatuissa yhteyksissä salasanat lähetetään selkeässä muodossa salaamattomina ja tämä altistaa kolmannen osapuolen salakuuntelulle sekä palvelimelle murtautumiseen. (Held 2005, 24.)

CHAP

Challenge- Handshake Authentication Protocol (CHAP) on edistyneempi sekä turvallisempi autentikointimenetelmä kuin PAP autentikointimenetelmä ja se perustuu kolmensuuntaiseen kättelytoimenpiteeseen. CHAP- autentikoinnissa käyttäjän muodostaessa yhteyttä esimerkiksi palvelimeen, palvelin lähettää käyttäjälle haasteviestin, missä pyydetään käyttäjätunnusta sekä salasanaa. Käyttäjän salasana salataan saadulla haasteella esimerkiksi MD5- algoritmilla sekä muodostetaan tarkistussumma (hash value) ja lähetetään se tämän

jälkeen käyttäjätunnuksen kanssa palvelimelle. Mikäli hash value palvelimella täsmää, on todentaminen onnistunut ja siitä lähetetään käyttäjälle success-viesti. Muussa tapauksessa yhteys katkaistaan. CHAP on huomattavasti edistyneempi sekä turvallisempi autentikointimenetelmä kuin PAP, koska lähetettävät salasanat eivät ole selkokielisessä muodossa vaan algoritmilla salattuina. Turvallisuutta lisää myös huomattavasti muuttuvat istuntotunnukset, sekä todentamisessa lähetettävien haasteviestien sattumanvaraisuus. CHAP ehkäiseekin tehokkaasti mahdollisia toisto sekä mies välissä hyökkäyksiä. (Held 2005, 27 - 29.)

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) on Microsoftin luoma hieman kehittyneempi versio CHAP autentikointi-menetelmästä ja se toimii vain Windows järjestelmissä. MS-CHAP:sta on olemassa kaksi erillistä versiota ja nämä molemmat versiot ovat hyvin yleisiä autentikointimenetelmiä. Kuten CHAP- yhteyksissä myös tässäkin käytetään yhteydenmuodostuksessa haaste-vastaus yhteyskäytäntöä, mutta salauksessa käytetään MD 4 algoritmia. MS-CHAP sallii lisäksi salasanojen tallentamisen palvelimelle salatussa muodossa, kun CHAP- protokollalla palvelimelle tallennetut salasanat ovat selkokielisessä muodossa. Lisäksi MS-CHAP-protokollaan on kehitetty sekä laajennettu useita erilaisia vikailmoituskoodeja, kuten vikailmoitus käyttäjälle salasanan vanhentumisesta. MS-CHAPv2-protokollassa, eli sen toisessa versiossa, on kehitetty lisää muutamia turvallisuutta parantavia asioita alkuperäiseen versioon verrattuna. MS-CHAPv2 on kaksisuuntainen autentikointiprotokolla ja mahdollistaa näin palvelinautentikoinnin. Tässä palvelin kerää todennusdataa ja vahvistaa tiedot vertailemalla niitä omaan tai johonkin keskitettyyn autentikointitietokantaansa. Tämä mahdollistaakin Remote Authentication Dial-In User Service (RADIUS) – palvelimen käytön yrityksissä. MS-CHAPv2 sisältää myös salasanan vaihto-ominaisuuden, mikä ei ole mahdollista aiemmassa versiossa. Tämän avulla voidaan esimerkiksi vaihtaa tilin salasana, mikäli Radius- palvelin ilmoittaa sen vanhentuneen. (Held 2005, 27 - 29.)

EAP

Extensible Authentication Protocol (EAP) on laajennettu protokolla PPP:sta (Point- to- Point Protocol) ja se toimii linkkitasolla. EAP mahdollistaa laajemman tuen eri autentikointimenetelmille kuten Token-korttien, kertakäyttöisten salasanojen, julkisen avaimen autentikoinnin, sekä digitaalisten sertifikaattien käytön. EAP- protokollasta on johdettu useita eri protokollia, jotka toimivat kaikki hieman eri tavalla. Näitä protokollia ovat esimerkiksi Lightweight EAP (LEAP), Protected EAP (PEAP), EAP- Transport Layer Security (EAP-TLS), sekä EAP-Tunneled TLS (EAP TTLS). (Cisco 2009b, hakupäivä 2.11.2010). Esimerkkinä näistä mainittakoon PEAP, missä autentikointi tapahtuu digitaalisilla sertifikaateilla suoraan autentikointipalvelimen sekä käyttäjän välillä, eikä erillistä autentikaattoria tarvita. LEAP autentikointimenetelmällä turvataan langattomat yhteydet. Tässä tekniikassa käyttäjä todentautuu ensiksi autentikaattorille ja tämän jälkeen autentikaattori todentautuu käyttäjälle. Autentikaattori on hyvin useasti tukiasema tai kytkin. Mikäli todentautuminen onnistuu molempiin suuntiin, yhteys luodaan. Toisin kuin PEAP:ssa sekä EAP-TLS:ssa, missä todentautuminen tapahtuu digitaalisten sertifikaattien avulla, tässä todentautuminen tapahtuu käyttäjätunnuksen sekä salasanan avulla. Tämä helpottaa huomattavasti myös ylläpitoa. (Kwan 2003, 10.)

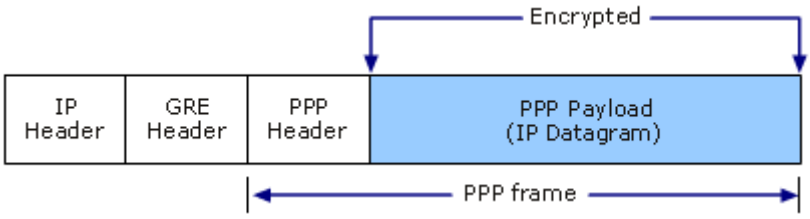
4.3 Tunnelointi

Tunnelointi on VPN- tekniikan tärkein osa-alue. Tunnelointi on tekniikka jolla kapseloidaan datapaketti kokonaan toiseksi protokolla formaatiksi lisäämällä tunnelointiprotokollan otsikko alkuperäiseen pakettiin. Tunnelointia voidaankin verrata esimerkiksi kirjeen lähetykseen. Kirjoitettu kirje laitetaan ensiksi kirjekuoreeseen, mistä ilmenee vastaanottajan osoite. Kun kirje postitetaan, se lähetetään kuoressa kerrottuun osoitteeseen ja tämän jälkeen vastaanottajan on avattava kirjekuori, lukeakseen viestin. Tunneloinnissa kirje edustaa alkuperäistä datapakettia ja kirjekuori edustaa reitittävää protokollaa millä alkuperäinen datapaketti on kapseloitu. Kirjekuoressa oleva lähetysosoite edustaa reititystietoja, jotka pakettiin on lisätty. (Gupta 2002, 88.) Tunneloinnissa käytetään kolmea protokollatyyppiä, näitä ovat Passenger-

protokolla (esim. PPP), Kapselointi-protokolla (esim. PPTP) sekä Carrier-protokolla(esim. IP ja UDP).

PPTP

Point- to- Point Tunneling Protocol (PPTP) on mekanismi jonka avulla turvataan etäkäyttäjän datalähetys verkkopalvelimelle, käytettäessä IP-pohjaista julkista verkkoa, kuten Internet. PPTP on tarkoitettu käytettäväksi Remote Access sekä Site-to-Site VPN- yhteyksissä. PPTP kapseloi PPP-kehykset IP- paketeiksi kuljetusta varten sekä käyttää TCP- yhteyttä tunnelin muodostuksessa ja hallinnassa. PPTP käyttää PPP- kehyksien kapseloimiseen muokattua versiota GRE:sta (Generic Routing Encapsulation) (KUVIO 9). Kapseloidun PPP-kehyksen hyötykuorma voidaan myös salata, kompressoida tai tehdä molemmat. PPP- kehys salataan käyttämällä siihen Microsoft Point- to- Point Encryption (MPPE) salausavaimia, MS-CHAPv2:den tai EAP-TLS autentikointiprosessin käynnistyttyä. PPTP tukeekin vain edellä mainittuja autentikointiprotokollia ja käyttäjän tulisi varmistua että kyseiset protokollat ovat käytössä PPP- kehyksien salaamiseen PPTP- tunnelia muodostettaessa. (Microsoft TechNet 2010, hakupäivä 3.11.2010.)

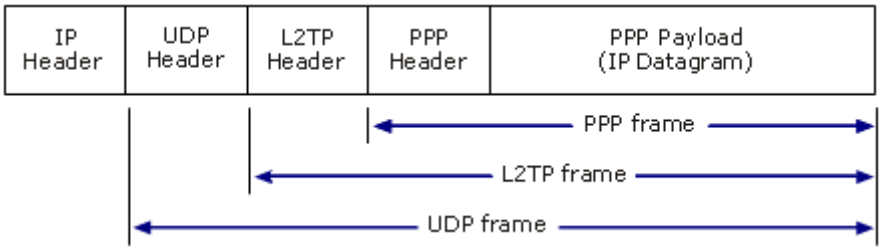


KUVIO 9. *PPTP- paketin rakenne* (Microsoft TechNet 2010, hakupäivä 3.11.2010.)

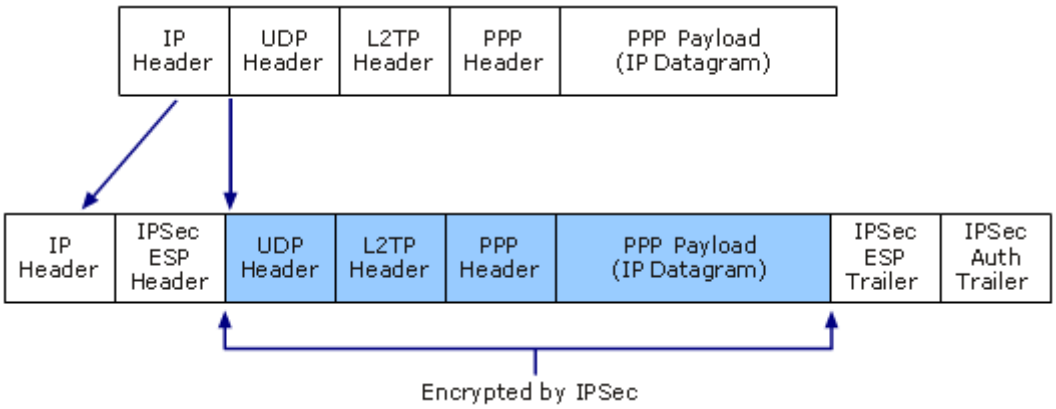
L2TP

Layer 2 Tunneling Protocol (L2TP) (KUVIO 10) on Ciscon kehittämä tunnelointiprotokolla, missä yhdistyvät Layer 2 Forwarding (L2F) sekä PPTP tunnelointiprotokollien parhaat ominaisuudet. L2TP kykenee kapsuloimaan PPP- kehykset kuten PPTP, mutta mahdollistaa myös pakettien lähetyksen IP, ATM sekä frame relay tyyppisissä verkoissa. (Lucas, Singh, Liu 2006, 245.)

L2TP:le ei ole määritelty mitään tiettyä salausmenetelmää, mutta hyvin yleisenä menetelmänä on pidetty IPsec suojausprotokollan käyttämistä yhteyden salaamiseen kyseisen tunnelointiprotokollan kanssa (KUVIO 11). L2TP on erittäin turvallinen tunnelointiprotokolla verrattuna PPTP- protokollaan, koska tässä salataan datapaketin lisäksi myös kontrollipaketit, kun PPTP-protokollassa salataan pelkästään datapaketti. (Held 2005, 16). Suurimmat erot näiden kahden tunnelointiprotokollan väliltä löytyvätkin yhteyden muodostuksessa tapahtuvista eroista. PPTP:n käyttämä autentikointiprotokolla MPPE ei salaa todentamisprosessia käyttäjän sekä VPN- palvelimen välillä ollenkaan. IPsec salauksella, todentaminen on käytössä jo ennen L2TP-yhteyden muodostusta. (Lucas, Singh, Liu 2006, 245.)



KUVIO 10. *L2TP- paketin rakenne* (Microsoft TechNet 2010, hakupäivä 3.11.2010)



KUVIO 11. *L2TP- paketin rakenne IPSec ESP:llä salattuna* (Microsoft TechNet 2010, hakupäivä 3.11.2010)

IPsec

Internet Protocol Security (IPsec) on Internet Engineering Task Force- yhteisön (IETF) kehittämä kokoelma protokollia, joka mahdollistaa turvallisen tavan tietoliikennepakettien lähettämisen sekä vastaanottamisen IP- verkoissa. IPsecin yleisesti käytetyimpiä protokollia ovat Encapsulating Security Payload (ESP), Authentication Header (AH), sekä Internet Key Exchange (IKE). (Frankel 2005, 3-1, hakupäivä 3.11.2010.)

Authentication Header (AH) mahdollistaa todentamisen sekä eheyden pakettien otsikoille sekä datalle, mutta pakettien salaus sillä ei onnistu. IPsecin alkuperäisessä versiossa ESP protokolla mahdollisti vain salauksen mutta ei autentikointia, joten AH sekä ESP protokollia käytettiin hyvin useasti molempia yhdessä, datan luotettavuuden sekä eheyden saavuttamiseksi. IPsecin toisessa versiossa ESP protokollaan lisättiin myös kyky autentikoimiseen ja tämä kehitys onkin syrjäyttänyt AH protokollan käytön lähes kokonaan. AH:lla voidaan kuitenkin autentikoida sellaisia paketin osia mitä ESP:llä ei voida. AH käytäntöjä on olemassa kahdenlaista, kuljetuskäytäntö (transport mode) sekä tunnelikäytäntö (tunnel mode). (Frankel 2005, 3-1, hakupäivä 3.11.2010.)

Tunnelikäytännössä AH luo uuden IP-otsikon jokaiselle paketille, mutta kuljetus-käytännössä tätä ei tehdä. Käytettäessä IPsecia yhdyskäytäväpohjaisissa yhteyksissä, on lähde tai vastaanottajan IP-osoitetiedot paketeissa muutettava kyseisen yhdyskäytävän IP-osoitteiksi. Koska kuljetuskäytännössä (transport mode) ei ole mahdollista muuttaa alkuperäisiä IP-otsikoita, eikä luoda uusia IP-otsikoita, kuljetuskäytäntöä käytetään vain Host- to- Host yhteyksissä. (Frankel 2005, 3-1, hakupäivä 3.11.2010.)

Datan eheyden varmistamisessa käytetään avaimeen perustuvaa tiivistealgoritmia nimeltä Message Autentication Code (MAC), minkä tarkoituksena on luoda tiiviste viestin sekä salatun avaimen pohjalta. Kyseinen tiiviste lisätään pakettiin ja lähetetään vastaanottajalle, joka voi tämän jälkeen uudelleen muodostaa tiivisteen käyttämällä jaettua avainta sekä vahvistaa että kyseiset tiivisteet täsmäävät. IPsec käyttää kahden avaimen tiivisteisiin erityistä

algoritmia nimeltä Hash Message Authentication Code (HMAC), esimerkkeinä tällaisista algoritmeista mainittakoon HMAC-MD5, sekä HMAC-SHA1. (Frankel 2005, 3-2, hakupäivä 3.11.2010)

Encapsulating Security Payload (ESP) protokolalla on myös kaksi erillistä käytäntöä, tunnelikäytäntö sekä kuljetuskäytäntö. Näistä käytännöistä tunnelikäytäntö on huomattavasti käytetympi. Tunnelikäytännössä ESP luo jokaiselle paketille uuden IP-otsikon, mistä ilmenee ESP- tunnelissa lähetettävän paketin lähettäjä sekä vastaanottaja. Tunnelikäytäntö mahdollistaakin pakettien alkuperäisten IP-otsikoiden sekä myös datan salauksen. Datan salaamisella ehkäistään tehokkaasti sen luvaton käyttö sekä tiedon muuntelumahdollisuudet. IP- otsikoiden salaamisella peitetään kaikki tietoliikenteeseen kuuluvat tiedot, kuten oikean lähettäjän sekä vastaanottajan tiedot. (Frankel 2005, 3-5, hakupäivä 3.11.2010.)

Kuljetuskäytännössä ESP käyttää alkuperäistä IP-otsikkoa sen sijaan että se loisi kokonaan uutta otsikkoa, kuten tapahtuu tunnelikäytännössä. Se onkin huomattavasti turvallisempi kuljetuskäytäntöön verrattuna, sillä kuljetuskäytäntö ei pysty salamaan paketista IP-otsikoita, vaan pelkästään itse datan, sekä joitain yksittäisiä ESP-komponentteja. ESP:n kuljetuskäytäntö, kuten myös AH:n kuljetuskäytäntö on ensisijaisesti tarkoitettu käytettäväksi Host- to- Host yhteyksissä, eikä kummankaan protokolan kuljetuskäytäntö ole yhteensopiva NAT:n (Network Address Translation) kanssa. Salausprosesissaan ESP käyttää symmetristä salausmenetelmää IPsec- paketeille. IPsec- yhteydessä, missä käytetään ESP- salausta, on yhteyden molempien osapuolien käytettävä samaa avainta pakettien salaamiseen sekä purkamiseen. Salauksessa käytetään AES-128-algoritmia, mikä jakaa datan pienempiin lohkoihin. Muita ESP:n käyttämiä salausalgoritmeja ovat AES-Cipher Block Chaining (AES-CBC), AES-Counter Mode (AES-CTR), sekä Triple DES (3DES). (Frankel 2005, 3-6, hakupäivä 3.11.2010.)

Internet Key Exchange (IKE) on protokolla, jonka avulla yhteyden muodostavat osapuolet voivat neuvotella käytettävistä turvaehdoista sekä luoda ja hallita niitä. Turvaehdoilla, eli Security Association, (SA) tarkoitetaan niitä IPsec

turvallisuusominaisuuksia sekä arvoja, joita yhteyden muodostuksessa tullaan soveltamaan. Yhteyden muodostus tapahtuu kaksivaiheisena operaationa. Ensimmäisessä vaiheessa luodaan turvattu yhteys IKE SA käyttäjien välille. Se mahdollistaa yhteyden muodostuksen toisessa vaiheessa tapahtuvan varsinaisen neuvottelun turvaehdoista IPsec- yhteyden käyttäjien välillä ja tätä kutsutaan IPsec SA:ksi. (Frankel 2005, 3-10, hakupäivä 3.11.2010.)

IKE SA on mahdollista toteuttaa kahdella tavalla, main modella sekä aggressive modella. Main modessa IKE SA:n toteutus neuvotellaan käyttämällä siihen kolme paria viestejä. Ensimmäisessä viestiparissa, osapuolet ehdottavat turvaehdoissa käytettävistä parametreistä, toisessa viestiparissa vaihdetaan avaimia (DH), kolmannessa viestiparissa yhteyden osapuolet todentuvat toisilleen. Käytettäviä parametreja ovat esimerkiksi salausalgoritmit, kuten DES, 3DES, CAST, RC5, IDEA, Blowfish, sekä AES. Eheyttä suojaavat algoritmit, kuten HMAC-MD5 sekä HMAC-SHA-1. Autentikointimenetelminä voidaan käyttää muun muassa ennalta jaettuja avaimia, digitaalisia allekirjoituksia sekä yleisen avaimen salausta. Diffie-Hellman(DH)- avaimenvaihtoprotokollan avulla osapuolet voivat kehittää yhteisen salaisuuden turvallisesti ensimmäisen vaiheen yhteyden muodostuksessa. (Frankel 2005, 3-10, hakupäivä 3.11.2010.)

Aggressive mode on nopeampi vastine main modelle mutta huomattavasti turvattomampi, koska se ei salaa osapuolten identiteettiä. Siinä IKE SA:n toteutuminen neuvotellaan vain kolmella viestillä, kolmen viestiparin sijaan. Kahdessa ensimmäisessä viestissä neuvotellaan IKE SA:n parametreistä sekä suoritetaan avainten vaihto ja kolmannessa viestissä todennetaan osapuolet. (Frankel 2005, 3-15, hakupäivä 3.11.2010.)

Yhteyden muodostuksen toisen vaiheen tarkoituksena on toteuttaa turvaehdot varsinaiselle IPsec- yhteydelle ja tätä kutsutaan IPsec SA:ksi. IPsec SA toimii pelkästään yksisuuntaisesti ja tämän vuoksi kahden laitteen välille muodostettavalle IPsec- yhteydelle (AH tai ESP) tarvitaan myös turvaehtoparit. IPsec turvaehtopari luodaan käyttämällä guick mode tapaa ja se käyttää ensimmäisessä vaiheessa IKE SA:n määrittelemää salausta. Guick modessa käytetään kolme viestiä turvaehdon muodostukseen. Ensimmäisessä viestissä

aloittava osapuoli A lähettää avaimet sekä IPsec- turvaehtojen parametriehdotukset vastaanottajalle B. Toisessa viestissä osapuoli B lähettää avaimet, käytettävät IPsec turvaehtoparametrit sekä todentamiseen käytettävän tiivisteen. Kolmannessa viestissä osapuoli A lähettää tiivisteen todennusta varten. Osapuoli B:n vahvistettua kolmannen viestin, IPsec turvaehdot toteutuvat. Kaikki aktiiviset turvaehdot tallentuvat turvaehtotietokantaan (SAD). (Frankel 2005, 3-15, 3-16, hakupäivä 3.11.2010.)

Internet Key Exchange protokollasta on myös kehitetty uudempi versio IKEv2. Uuden version kehityksen tuloksena mainittakoon että IKEv2 tukee Extensible Authentication Protocol (EAP) sekä IPv6 protokollia. Merkittävin uudistus IKEv2:ssa on kuitenkin siinä, että IKE SA sekä IPsec SA on mahdollista toteuttaa tässä pelkästään neljällä viestillä. (Frankel 2005, 3-18, hakupäivä 3.11.2010.)

5 MS-IPHTTPS

Monet VPN- tekniikalla toteutetut palvelut mahdollistavat etätyöntekijöiden turvallisen pääsyn yrityksen verkkoon etäyhteyden avulla, käyttäen esimerkiksi Point-to-Point Tunneling Protokollaa (PPTP) sekä Layer Two Tunneling Protokollaa / Internet Protocol securitya (L2TP/IPsec). Palomuurien sekä välityspalvelimien lisääntyneen käytön vuoksi esimerkiksi hotelleissa ei PPTP tai L2TP/IPsec liikenne ole välttämättä mahdollista ja tämän takia VPN- yhteys yrityksen verkkoon ei ole mahdollista. MS-IPHTTPS (Microsoft IP over HTTPS Tunneling Protocol) on Windows 7- käyttöjärjestelmään kehittämä tunnelointiprotokolla, jolla IP-liikenne kapseloidaan HTTPS-protokollan yli. Se mahdollistaa etäyhteyden luomisen palomuurien tai välityspalvelimien takaa, jolloin tiedonsiirto ei ole estetty. (Microsoft TechNet 2010, 6, hakupäivä 3.11.2010.)

Yhteyden muodostus Windows 7- käyttöjärjestelmässä tapahtuu Direct Access toiminnon avulla. Direct Access -toiminto mahdollistaa automaattisen yhteyden muodostuksen organisaation sisäverkkoon. Yhteyden muodostaminen alkaa välittömästi asiakaskoneen kytkeydyttyä verkkoon, eikä yhteyden muodostaminen sisäverkkoon vaadi erillistä sisään kirjautumista.

Asiakaskoneen kytkeydyttyä verkkoon, se yrittää muodostaa yhteyttä organisaation Web- sivustolle, joka on konfiguroitu Direct Access- palvelimelle. Mikäli yhteyden muodostaminen suoraan Web- sivustolle ei onnistu, asiakaskone yrittää löytää IPv6- verkkoa muodostaakseen yhteyden Direct Access- palvelimelle. Jos IPv6- verkkoa ei ole saatavilla, asiakaskone yrittää seuraavaksi muodostaa IPv6 yhteyden IPv4- tunnelilla käyttäen ensiksi 6to4 ja seuraavaksi Teredo- siirtymätekniikoita. Mikäli yhteyden muodostus ei onnistu kyseisillä siirtymätekniikoilla palomuurin tai välityspalvelimen vuoksi, etäyhteys muodostetaan IP- HTTPS- yhteydellä. Yhteyden muodostusta yritetään viimeiseksi IP-HTTPS- yhteydellä koska sillä on heikoin suorituskyky verrattuna muihin metodeihin. (McLean & Thomas 2010, hakupäivä 19.12.2010.)

5.1 Käytettävät protokollat

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) on turvallinen hypertekstin siirtoprotokolla, jota käytetään ensisijaisesti tiedon suojaamiseen www-yhteyksissä. HTTPS yhteys muodostetaan Transport Layer Security (TLS) salausprotokollan avulla. TLS on korvannut aiemmin käytössä olleen salausprotokollan Secure Sockets Layer (SSL). Transport Layer Security-protokollaa käytetään myös muihin sovelluskerroksen protokolliin, kuten File Transfer Protocol (FTP), Light Weight Directory Access Protocol (LDAP) sekä Simple Mail Transfer Protocol (SMTP). TLS mahdollistaa palvelintodennuksen, käyttäjätodennuksen sekä tiedon salauksen ja eheyden TCP- yhteyksissä. (Microsoft TechNet 2003a, hakupäivä 14.11.2010.)

SSL/TLS

SSL/TLS- protokolla voidaan jakaa kahteen kerrokseen. Ensimmäistä kerros on Handshake Protocol- kerros ja se koostuu kolmesta alaprotokollasta: Handshake Protocol, Change Cipher Spec Protocol sekä Alert Protocol. Toinen kerros on Record Protocol- kerros. Handshake protokolla neuvottelee käytettävistä istuntotiedoista palvelimen ja käyttäjän välillä. Istuntotiedot sisältävät tiedon esimerkiksi käytettävistä istuntotunnuksista, sertifikaateista sekä jaetun salaisuuden avainten luomiseen. (Microsoft Technet 2003b, hakupäivä 14.11.2010.)

Salauksessa käytetään sekä symmetristä että epäsymmetristä salausta. Symmetrisessä salauksessa käytetään samaa avainta viestin salaamiseen sekä purkamiseen. Salaukseen käytetään jotakin seuraavista salausalgoritmeistä: Data Enryption Standard (DES), 3-DES, RC2, RC4 tai Advanced Encryption Standard (AES). Epäsymmetrisen salauksen, eli julkisen avaimen salauksessa käytetään avainpareja, jotka johdetaan monimutkaisesta matemaattisesta prosessista ja joita käytetään aina yhdessä. Julkisella avaimella salattaessa salauksen purkuun käytetään salaista avainta ja salaisella avaimella

salattaessa salauksen purkuun käytetään julkista avainta. SSL/TLS käyttää yleisen avaimen salausta myös palvelimen todentamiseen käyttäjälle. Kättelyprosessin aikana sovitaan myös käytettävistä tiivistealgoritmeista kuten esimerkiksi Message Digest (MD5) tai Standard Hash Algorithm 1 (SHA-1). Tiivistealgoritmit sisältävät tiedon, jolla tarkastetaan lähetetyn tiedon eheys. Tämä tieto tai arvo toteutetaan käyttämällä joko Message Authentication Codea (MAC) tai Hash-based Message Authentication Codea (HMAC). (Microsoft TechNet 2003c, hakupäivä 15.11.2010)

Record Protocol- kerroksessa, protokolla salaa vastaanottamansa tiedon järjestelmäkerrokselta sekä toimittaa sen kuljetuskerrokselle. Record- protokolla sirpaloi datan sopivaksi salausta varten tai mahdollisesti kompressoi sen sekä suorittaa salauksen tai salauksen purun. (Microsoft TechNet 2003b hakupäivä 15.11.2010)

TCP

Transmission Control Protocol (TCP) on kuljetuskerroksen protokolla ja myös keskeisimpiä Internet-protokollia IP- protokollan lisäksi. Sen tehtävänä on muodostaa ja ylläpitää yhteyttä luotettavasti päätelaitteiden välillä. Yhteyden muodostus tapahtuu kolmivaiheisena kättelyprosessina. TCP:ssa on myös mekanismi virheen havaitsemista sekä korjausta varten. Tämä tekee siitä erittäin luotettavan, koska mahdollisesti kadonneet paketit huomataan ja ne voidaan lähettää uudelleen vastaanottajalle. TCP varmistaa myös, että paketit siirtyvät vastaanottajalle oikeassa järjestyksessä. TCP- protokollaa käyttäviä muita protokollia ovat esimerkiksi HTTP, FTP, SSH ja Telnet. (TCP 2010, hakupäivä 20.11.2010.)

IP

Internet Protocol (IP) on yksi verkkokerroksen protokollista ja koko Internetin ydin, koska se huolehtii IP- pakettien toimittamisesta esimerkiksi Internetissä. IP- paketit sisältävät tiedon muun muassa lähde ja kohdeosoitteista, joiden avulla ne toimitetaan oikeaan paikkaan. Jokaisella verkkoon kytketyllä tietokoneella tai muulla laitteella on oltava oma yksilöllinen IP- osoitteensa, jotta

tiedonsiirto olisi mahdollista. IP on kehitetty alkujaan jo 1970- luvulla ja nykyään tästä protokollasta on käytössä neljäs versio, IPv4. Internetin suosion kasvaessa 90- luvulla aloitettiin myös uuden Internet protokollan kehittäminen nimeltä IPng eli Internet Protocol Next Generation. Internet Engineering Task Force (IETF) hyväksyi sen IPv4:n syrjäyttäjäksi vuonna 1998, mutta vieläkään sitä ei kuitenkaan ole syrjäytetty. (Blank, 2004, 232.) Verkkoon liitettävien laitteiden määrä on lisääntynyt räjähdysmäisesti läpi 2000- luvun ja tästä johtuen IPv4:än osoiteavaruudessa olevien vapaiden osoitteiden määrä on nyt uhkaavasti loppumassa, joidenkin ennusteiden mukaan viimeiset vapaat osoitteet otettaisiin käyttöön jo vuonna 2011. IPng:n kehityksen myötä protokolla tunnetaan nykyään nimellä IPv6.

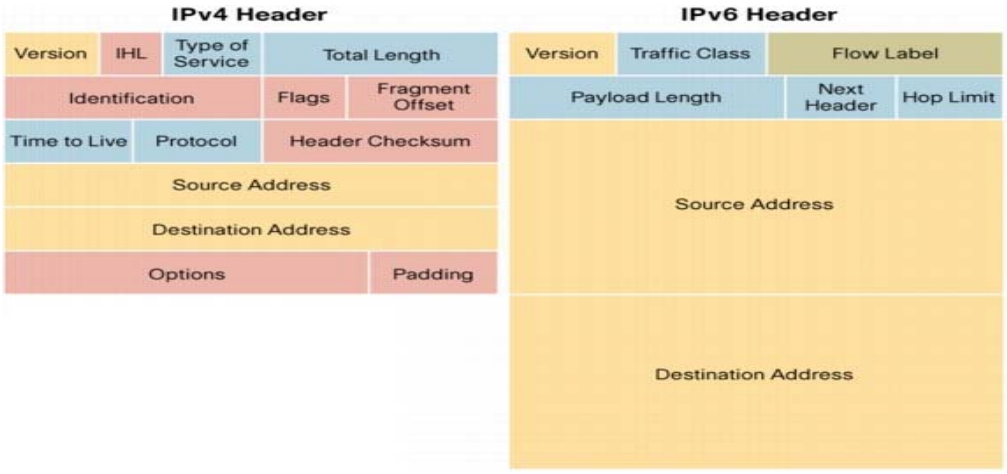
IPv6

Internet Protocol Version 6 (IPv6) on siis kehittyneempi versio IPv4:sta. Versio 6:den suurimmat uudistukset ovat paketin otsikoinnissa sekä merkittävästi suuremmassa osoiteavaruudessa. Se on myös huomattavasti turvallisempi protokolla kuin edeltäjänsä, koska se tukee IPseciä. IPv6:en tärkein uudistus on varmasti sen huomattavasti suurempi osoiteavaruus. Siinä käytetään 128 bittisiä osoitteita, kun taas IPv4 versiossa käytetään vain 32 bittisiä osoitteita. Osoitepituus on näin ollen neljä kertaa suurempi kuin IPv4 versiossa. Kun 32 bittinen osoitepituus mahdollisti 2^{32} eli 4 294 967 296 mahdollista osoitetta, 128 bitillä mahdollisia osoitteita saadaan jopa 2^{128} eli 340 282 366 920 938 463 463 374 607 431 768 211 456 kappaletta. (Windows Server 2008, 8.)

128 bittisen osoitteen syntaksi on myös muuttunut merkittävästi edeltäjäänsä verrattuna. IPv4:ssa osoitteet esitetään desimaali muodossa, jossa on neljä 8 bitin ryhmää pisteillä eroteltuina, kuten esimerkiksi 192.68.10.2. IPv6:ssa 128-bittinen osoite on jaettu kahdeksaan 16 bitin heksadesimaalin ryhmään (kolonna), missä käytetään kirjaimia A- H, sekä numeroita 0- 9. Kolonnat erotellaan käyttämällä kaksoispistettä, IPv6- osoitteet ovat muotoa: 2001:0db8:0000:2F3B:02AA:00FF:FE28:9C5A. (Windows Server 2008, 8-9.)

IPv6 osoitteita on kolmenlaisia, Unicast, Multicast sekä Anycast. IPv4:ssa käytettävä Broadcast- osoite on korvattu IPv6:ssa kokonaan Multicast-osoitteella. Unicast osoite tunnistaa pelkästään yhden rajapinnan ja paketit, jotka on osoitettu Unicast- osoitteiksi, lähetetään yksittäiselle rajapinnalle. Multicast- osoitteet tunnistavat useita rajapintoja ja Multicast- osoitteiksi osoitetut paketit lähetetään kaikille rajapinnoille, jotka osoitteeseen on määritelty. Sitä käytetäänkin yhdeltä- monille tyyppisessä tiedonsiirrossa. Anycast- osoite tunnistaa myös useita rajapintoja mutta Anycast- paketit lähetetään vain lähimmälle rajapinnalle, joka osoitteeseen on merkitty. (Windows Server 2008, 9-10.)

IPv6 paketin otsikointia (header) on virtaviivaistettu (KUVIO 12) merkittävästi poistamalla siitä kokonaan tarpeettomia tai harvemmin käytettyjä kenttiä ja tämä mahdollistaa entistä nopeamman reitityksen. Lisäksi siihen voidaan myös lisätä kenttiä jotka mahdollistavat paremman tuen reaaliaikaiselle tiedonsiirrolle, kuten puheelle. IPv6:ssa paketin kuljetus sekä välitysvaihtoehdot on siirretty kokonaan otsikoinnin laajennusosalle (Extension Header). Tyypillisessä IPv6 paketissa otsikoinnin laajennusosaa ei tarvita, mutta mikäli reitittimet tai vastaanottaja tarvitsee onnistuneeseen tiedonsiirtoon erikoismenettelyä, lähettäjäpää lisää yhden tai useamman otsikon laajennusosan pakettiin. Mahdollisia otsikoinnin laajennusosia ovat esimerkiksi Hop-by-Hop Options header, Destination Options header, Routing header, Fragement header, Authentication header sekä Encapsulating Security Payload header. (Windows Server 2008, 27,32.)



KUVIO 12. *IPv4 ja IPv6- kehyksien erot.* (Cisco 2006, 1)

5.2 Yhteyden muodostus

Muodostettavan IP-HTTPS yhteyden osapuolia ovat asiakaskone (client), palvelin (server) sekä mahdollinen päätepiste (end point). Asiakaskoneen yhteyden muodostus voi tapahtua joko automaattisesti, jolloin sen on oltava palomuurin tai välityspalvelimen takana tai yhteyden muodostus voi perustua myös hallinnolliseen menettelytapaan, missä yhteys voidaan määritellä olevan aina päällä. IP-HTTPS- palvelin toimii kuten VPN- palvelinkin. Palvelin hyväksyy suoraan asiakaskoneelta tulevan HTTPS- yhteydenottopyynnön ja se on tyypillisesti sijoitettu verkon reunalle. IP-HTTPS protokollassa ei itsessään ole minkäänlaisia turvallisuus tai todennusmetodeja käytössä, vaan se pohjautuu HTTPS protokollan tarjoamaan molemminpuoliseen todennukseen, datan eheyteen sekä luotettavuuteen. Yhteyden muodostukseen vaadittavia protokollia ovat IPv6 sekä HTTP tai HTTPS. Mikäli yhteyden muodostukseen käytetään HTTPS- protokollaa, tarvitaan siihen myös TLS/SSL- protokolla. Käytettäessä HTTPS- protokollaa, IP-HTTPS- protokolla vaatii asentamaan sertifikaatit jokaiselle asiakas sekä palvelinkoneelle. Asiakaskoneiden tulee myös pystyä käyttämään yhteyden muodostuksessa palvelimen käyttämää URI:a (Uniform Resource Identifier). HTTPS- yhteys voidaan muodostaa yli IPv4 tai IPv6 verkon. IP-HTTPS- protokolla ei tue kuitenkaan välityspalvelimien todennusta ja tästä syystä asiakaskoneet jotka ovat sellaisten välityspalvelimien takana, jotka vaativat todennusta eivät kykene muodostamaan yhteyttä IP-HTTPS palvelimeen. Yhteyden muodostuksessa IP-HTTPS- protokolla kapseloi

IPv6 paketit HTTPS yhteydelle muodostamalla tunneloidun rajapinnan ja tämä mahdollistaa symmetrisen linkin muodostuksen multicast sekä viereisen laitteen tunnistusmahdollisuudella. (Microsoft TechNet 2010, 6, 7, 11, hakupäivä 4.11.2010.)

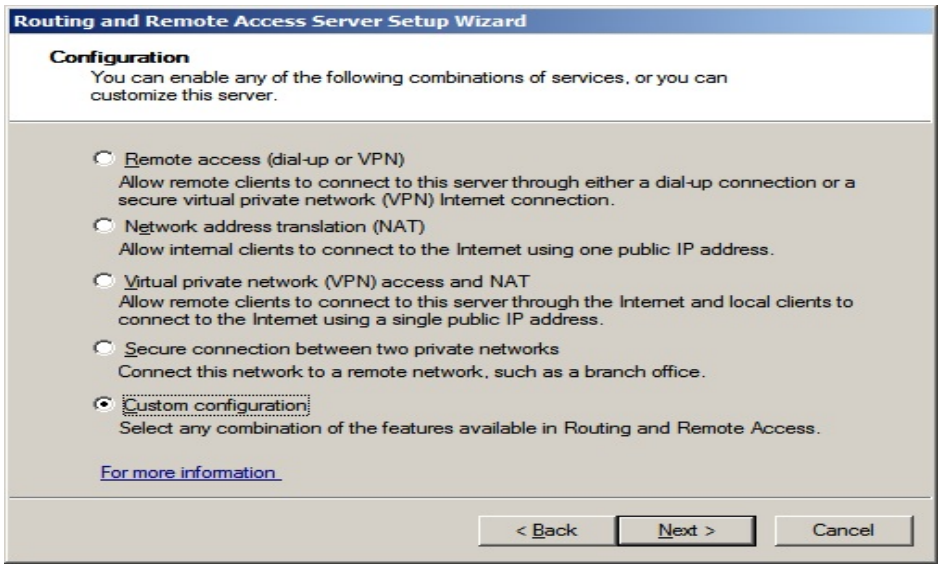
Yhteyden muodostuksessa asiakaskoneella voi olla viisi erilaista tilaa. Nämä tilat ovat Enabled, LinkDown, Established, LinkUp sekä Disabled. Enabled tilassa asiakaslaite on odotustilassa ja yhteyttä ruvetaan muodostamaan heti, mikäli yksi seuraavista ehdoista täyttyy: asiakaskone huomaa olevansa välityspalvelimen tai palomuurin takana, hallinnollisessa menettelytavassa on määritelty että yhteyden on oltava aina päällä tai jos käyttäjä haluaa itse muodostaa IP-HTTPS- yhteyden. Mikäli yksi edellä mainituista ehdoista täyttyy, asiakaskone siirtyy LinkDown- tilaan. LinkDown tilassa asiakaskone yrittää muodostaa HTTPS- yhteyden palvelimelle ja mikäli yhteyden muodostus onnistuu, se siirtyy Established tilaan. Established- tilassa asiakaskone muodostaa kaksisuuntaisen HTTP-streamin lähettämällä HTTP- pyynnön palvelimelle. Mikäli asiakaskone saa onnistuneen vastauksen palvelimelta, se siirtyy nyt LinkUP- tilaan. LinkUP- tilassa yhteys on muodostettu ja IPv6-pakettien lähettäminen sekä vastaanottaminen on nyt mahdollista. Disabled-tilassa yhteys on katkaistu, eikä tiedonsiirto onnistu (Microsoft TechNet 2010, 13, hakupäivä 4.11.2010.)

Yhteyden muodostuksessa palvelimella voi olla kolme erilaista tilaa ja nämä tilat ovat Listen, Accept sekä Disabled. Listen tilassa palvelin odottaa asiakaskoneen yhteyden muodostusta ja mikäli asiakaskone muodostaa onnistuneesti HTTPS- yhteyden, palvelin siirtyy Accept- tilaan. Accept- tilassa palvelin yrittää muuttaa asiakaskoneen tilan LinkUp- tilaan, vastaamalla sen lähettämään HTTP- pyyntöön. Mikäli tiedonsiirto asiakaskoneen kanssa päättyy onnistuneesti, palvelin siirtyy takaisin Listen- tilaan. Mikäli palvelin on asetettu Disabled- tilaan käyttäjän toimesta, yhteyden muodostus ei ole mahdollista (Microsoft TechNet 2010, 15, hakupäivä 4.11.2010)

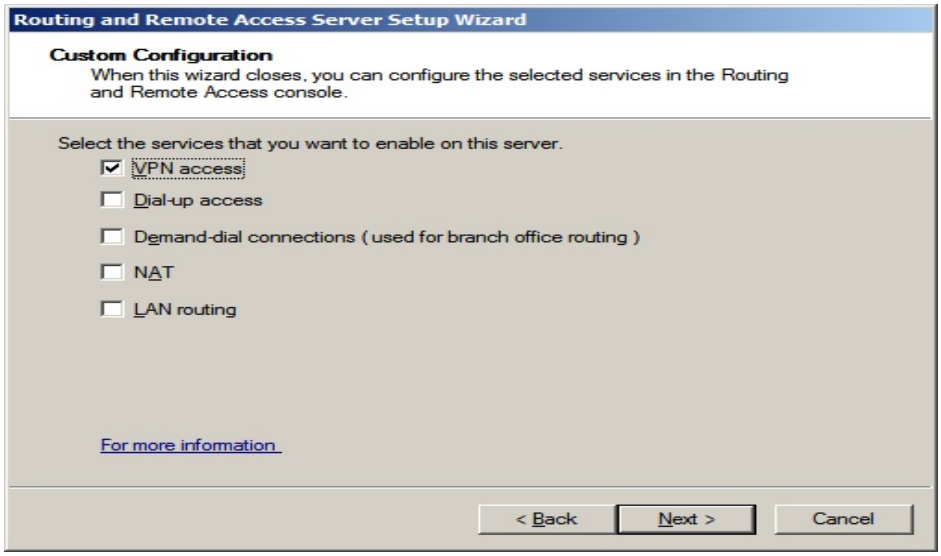
6 VPN- TEKNIIKAN ASENNUS

Ennen varsinaista VPN- tekniikan asennustyötä tulisi määritellä hyvin tarkkaan sen käyttötarkoitus ja käyttäjät. Määrittelemällä sopivat yhteyskäytännöt etukäteen voidaan asennustyössä säästää merkittävästi aikaa ja resursseja. Tässä luvussa kuvataan Point- to- Point VPN- tekniikan käyttöönoton keskeisimmät työvaiheet. Asennuksessa on käytetty Windows 7 Professional sekä Windows Server 2008 R2- käyttöjärjestelmiä.

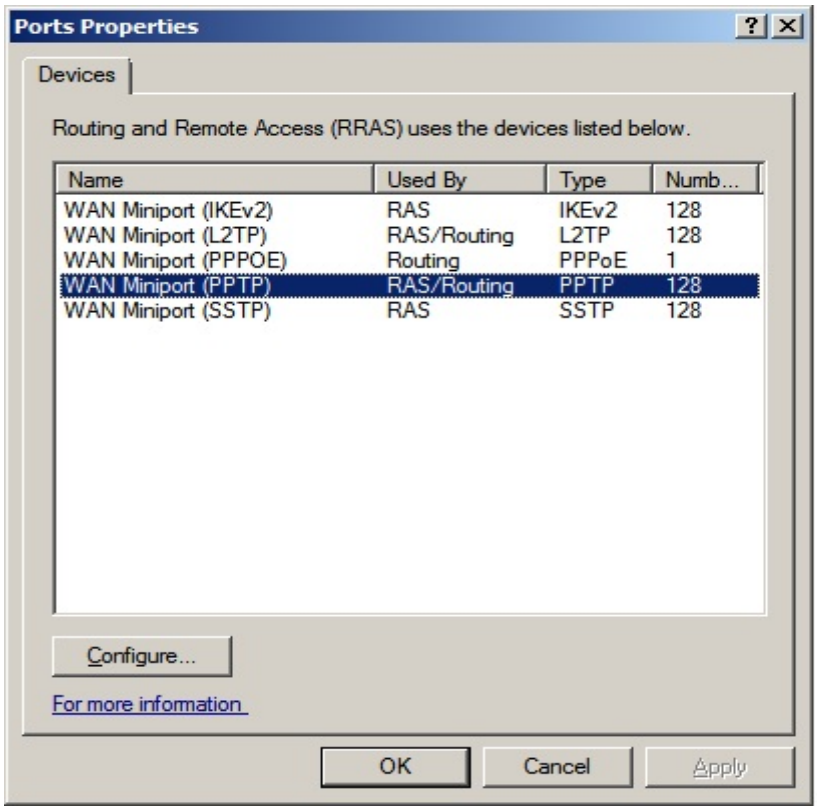
Asennustyö aloitetaan lisäämällä palvelimelle Routing and Remote Access Services- toiminto (liite 1), joka mahdollistaa Remote Access Service (RAS) konfiguroinnin. RAS- asennuksessa määritellään ensiksi käytettävä etäyhteysmuoto, vaihtoehtoja on kaikkiaan viisi (KUVIO 13). Valitaan Custom configuration vaihtoehto ja sen jälkeen VPN access (KUVIO 14). Tämän jälkeen valitaan käytettävä tunnelointiprotokolla (KUVIO 15) sekä porttien määrä Ports- toiminnon alta. Mikäli jaettavat tietoresurssit on luokiteltu alemmalle turvallisuustasolle, voidaan yhteyden muodostamiseen käyttää PPTP- tunnelointiprotokollaa, koska se on asennuksessa myös helpoin toteuttaa. Mikäli siirrettävä tieto on kuitenkin luokiteltu korkeammalle turvallisuustasolle, tulisi tunnelointiprotokollaksi valita tässä vaiheessa L2TP. Tässä työssä valitaan kuitenkin käytettäväksi PPTP- protokolla. Viimeiseksi palvelimelle määritellään käyttäjät (liite 2) sekä jaettavat tietoresurssit (liite 3) ja niiden käyttöoikeudet (Liite 4).



KUVIO 13. *Käytettävän etäyhteysmuodon valinta*.

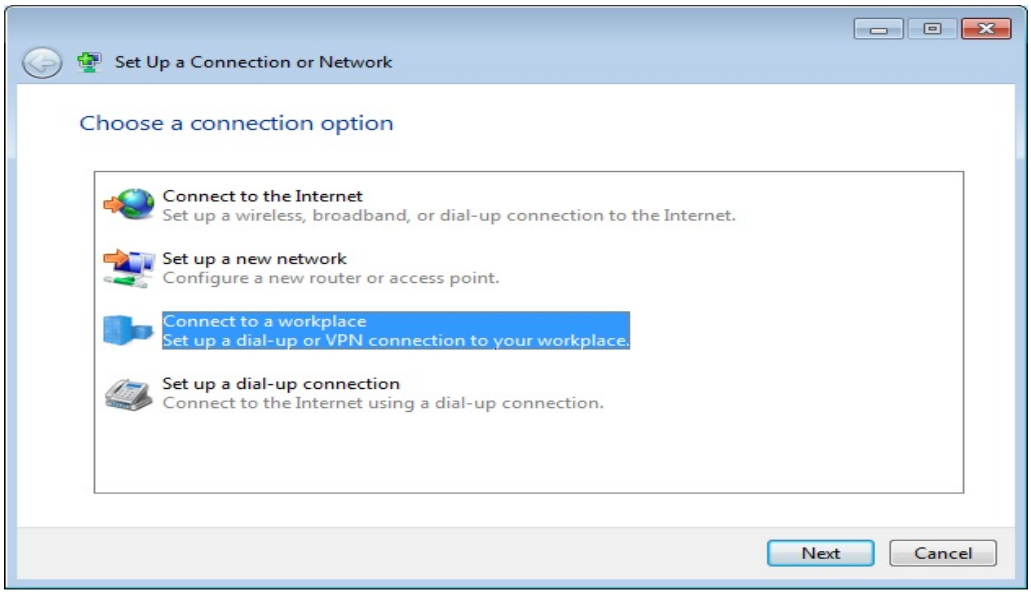


KUVIO 14. *Käytettävän etäyhteysmuodon valinta*.

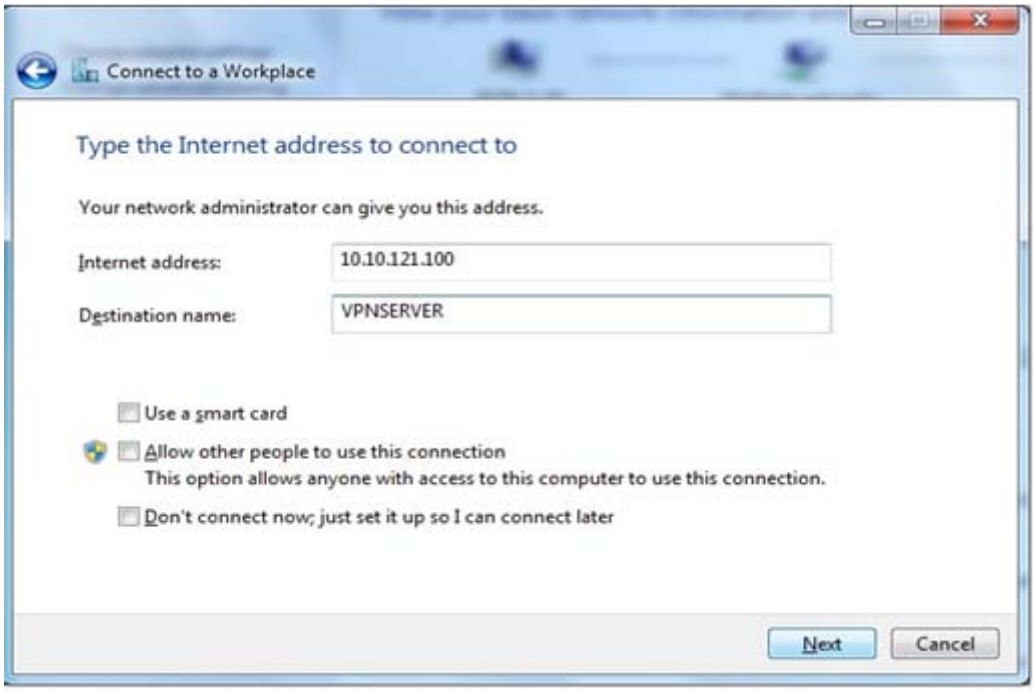


KUVIO 15. *Käytettävän protokollan valinta*.

Muodostettaessa yhteyttä palvelimelle ensimmäistä kertaa, käyttäjän on ensiksi määriteltävä oikea yhteyskäytäntö, palvelimen osoite sekä käytettävät käyttäjätunnukset sekä salasanat. Tämä tapahtuu Set Up a Connection or Network- toiminnolla. Ensimmäiseksi valitaan Connect to a workplace vaihtoehto (KUVIO 16), jonka jälkeen annetaan palvelimen IP- osoite ja nimi (KUVIO 17). Tämän jälkeen annetaan vain käyttäjätunnus sekä salasana ja muodostetaan yhteys Connect- painikkeella (KUVIO 18). Onnistunut yhteyden muodostus voidaan tarkistaa Windows 7:ssä ohjauspaneelista Network and Sharing Center- toiminnolla (KUVIO 19). Onnistunut yhteydenmuodostus voidaan tarkistaa palvelimelta Remote Access Clients- toiminnolla, missä näkyy kaikki palvelimelle luodut etäyhteydet (Liite 5). Tämän toiminnon avulla palvelimelta voidaan myös tarvittaessa katkaista muodostettu etäyhteys. Etäyhteyden muodostuttua palvelimelle, jaetut tietoresurssit saadaan käyttöön kirjoittamalla komentoriville ”net use-komento”, missä määritellään palvelimen nimi sekä jaettava tietoresurssi (KUVIO 20). Tietoresursseja voidaan nyt käyttää normaalisti Computer- toiminnon kautta (KUVIO 21).

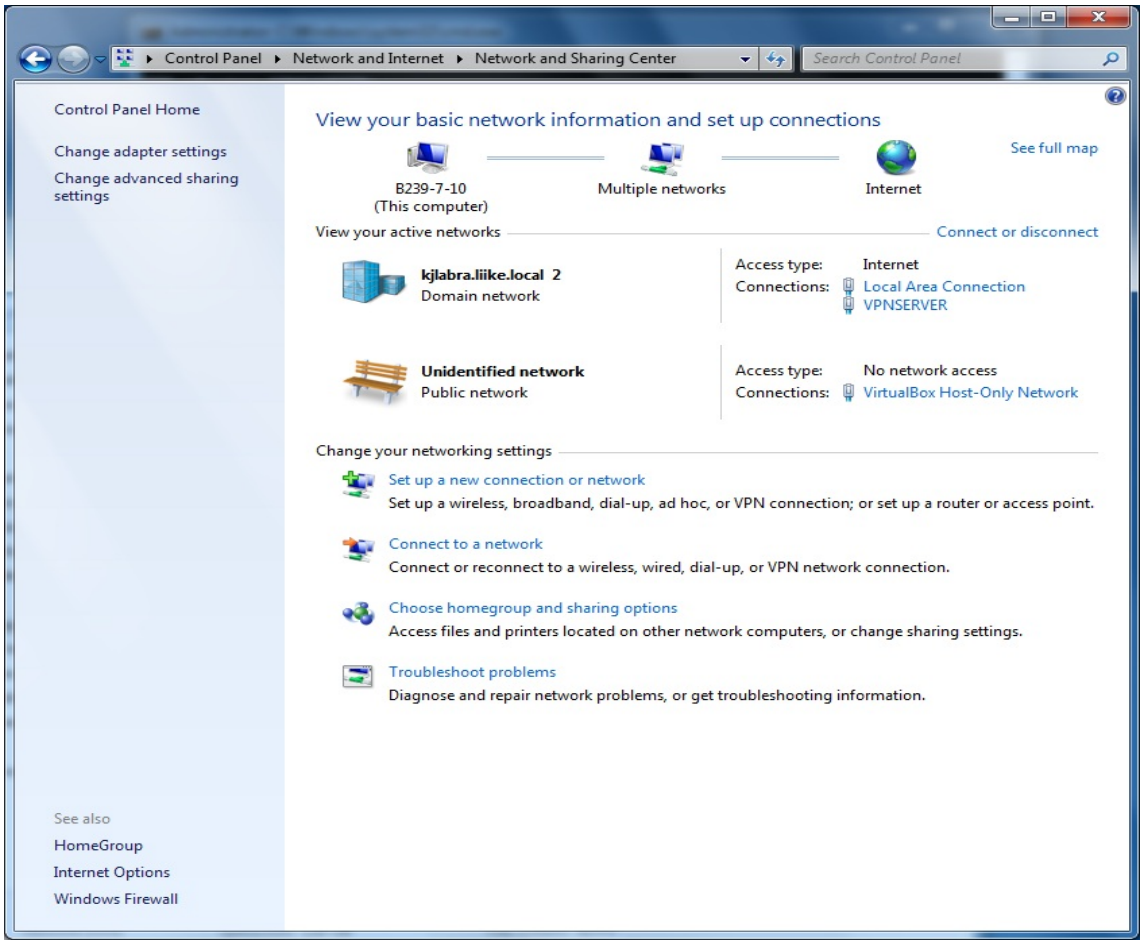


KUVIO 16. *Yhteystavan valinta*.

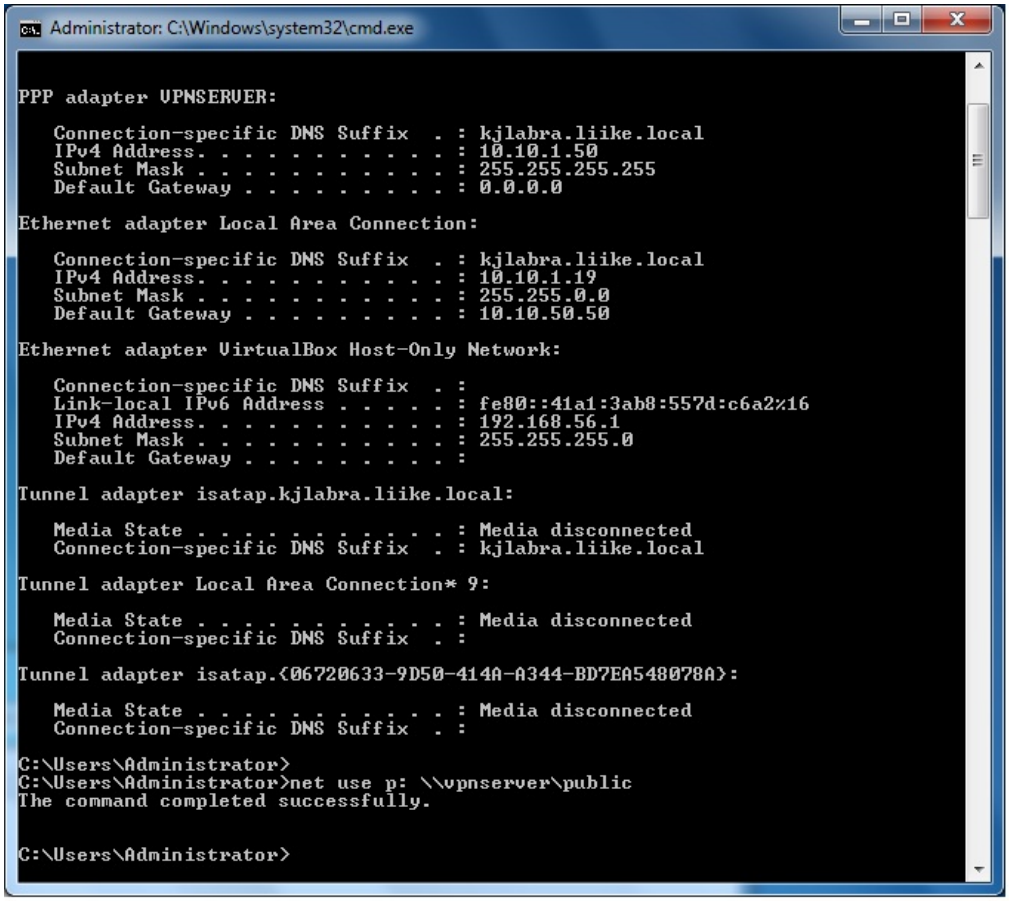


KUVIO 17. *Muodostettavan etäyhteyskohteen tiedot.*

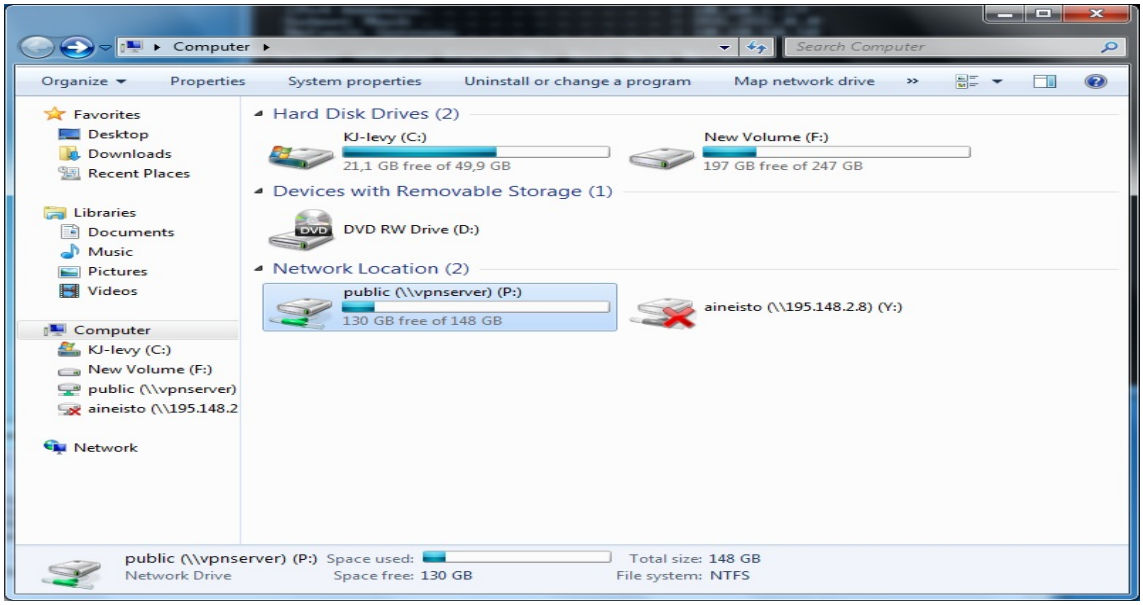
KUVIO 18. *Käyttäjätunnuksen ja salasanan kysely*.



KUVIO 19. *Onnistunut VPN- yhteys*.



KUVIO 20. *Komentorivillä tehtävä net use- komento*.

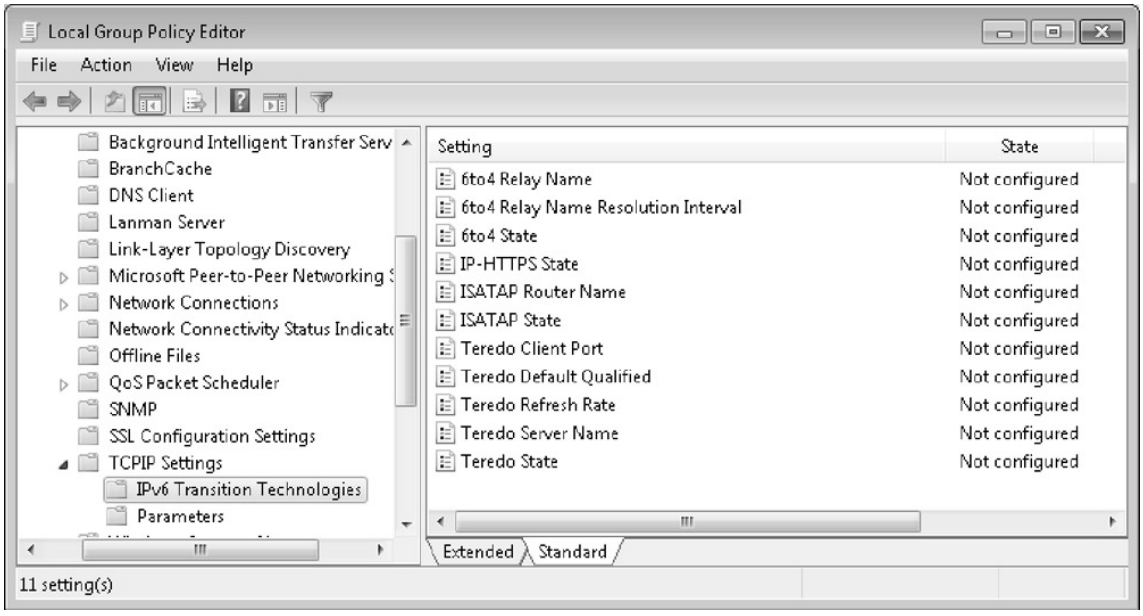


KUVIO 21. *Käytössä oleva Public- tietoresurssi etäyhteydellä.*

7 DIRECT ACCESS- TEKNIIKAN ASENNUS

Ennen Direct Access asennusta tulee tiedostaa siihen liittyvät käyttöjärjestelmärajoitukset. Tällä hetkellä Direct Access toimii ainoastaan Windows 7 Enterprise ja Ultimate käyttöjärjestelmillä sekä Windows Server 2008 R2 palvelinkäyttöjärjestelmässä. (McLean & Thomas 2010, hakupäivä 19.12.2010.) Tässä luvussa perehdytään Direct Access- asiakaskoneen sekä Direct Access- palvelimen asennuksen keskeisimpiin työvaiheisiin. Asennus on kuvattu Configuring Windows 7 Training Kit- oppaan mukaisesti.

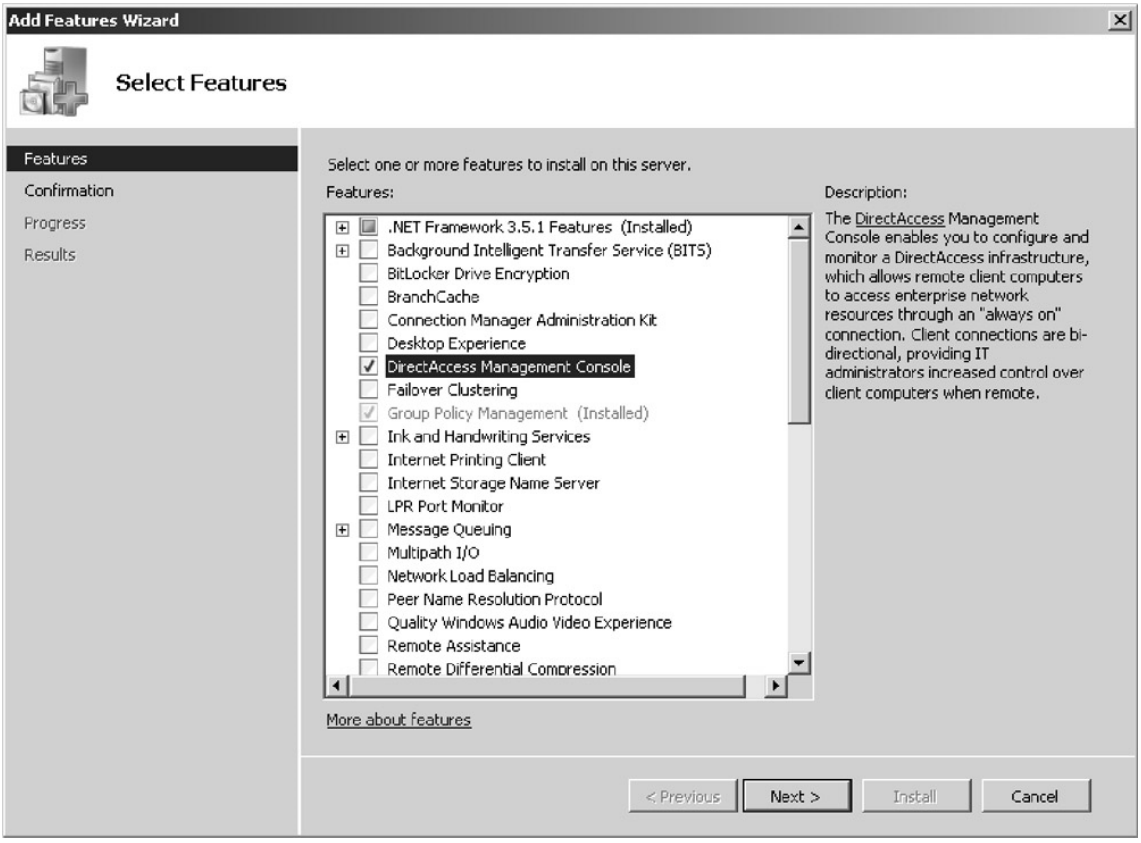
Asiakaskoneessa Direct Access- toiminnon asennus tapahtuu ryhmätoiminnon (Group Policy) kautta (KUVIO 22). Kun koneen asiakastili on lisätty määriteltyyn turvallisuusrymään (Security Group), pitää koneelle vielä asentaa sertifikaatti Direct Access autentikointia varten. (McLean & Thomas 2010, hakupäivä 19.12.2010.)



KUVIO 22. *Direct Acces ryhmätoiminnot* (McLean & Thomas 2010, hakupäivä 19.12.2010.)

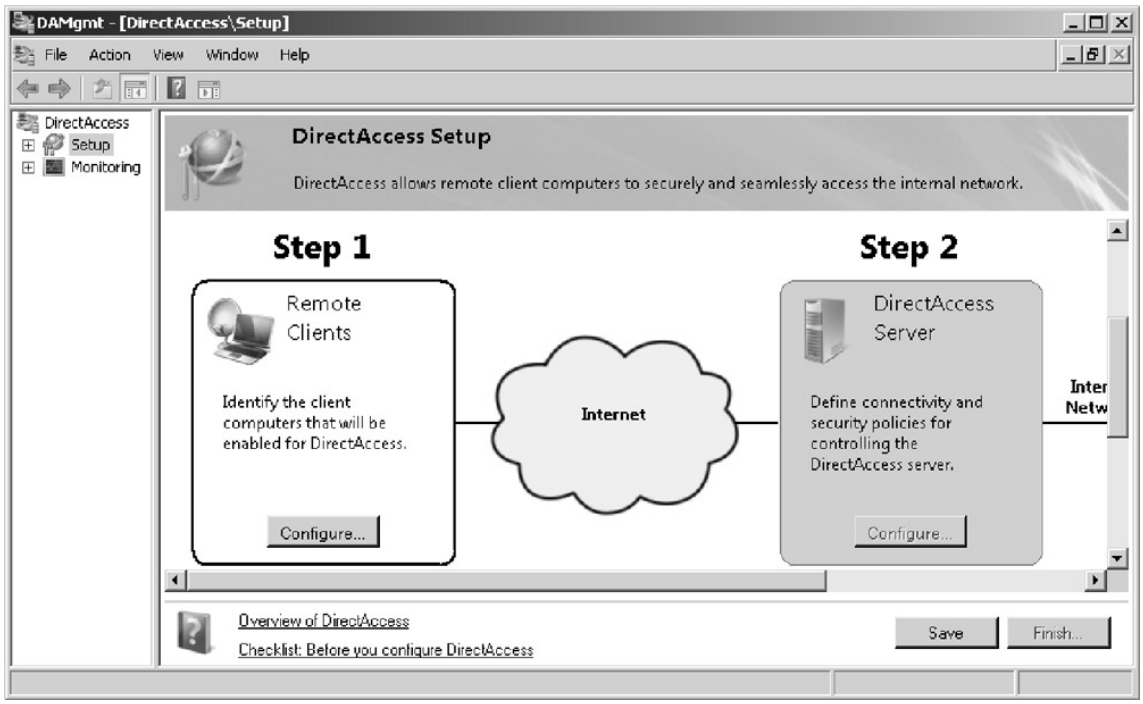
Palvelimella Direct Access- toiminnon asennus aloitetaan lisäämällä Direct Access Management Console- toiminto, jonka avulla voidaan asentaa ja hallita

Direct Access -toimintoja (KUVIO 23). Toiminnon lisääminen edellyttää myös Group Policy Management- toiminnon lisäämistä, koska sen avulla luodaan ryhmätoiminnot, joita käytetään asiakaskoneen asennuksessa. (McLean & Thomas 2010, hakupäivä 19.12.2010.)

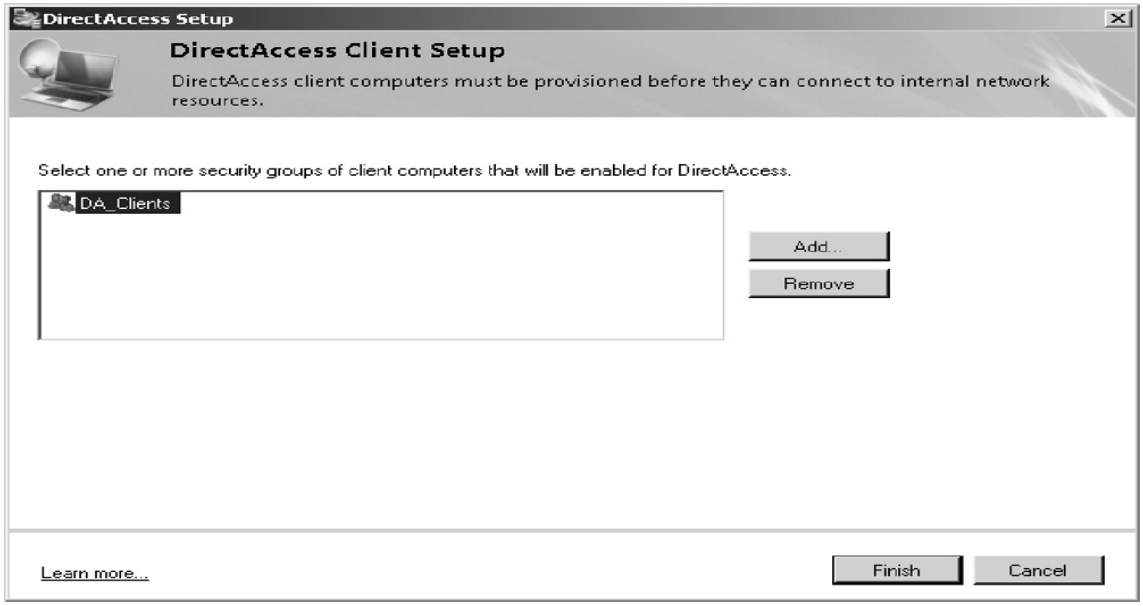


KUVIO 23. *Direct Acces Management Console- toiminnon lisäys palvelimelle* (McLean & Thomas 2010, hakupäivä 19.12.2010.)

Kun Direct Access Management Console- toiminto on asennettu onnistuneesti, voidaan varsinainen Direct Access- palvelimen asennustyö aloittaa. Ensimmäiseksi avataan Adminstrative Tools- valikosta Direct Access Management Console- toiminto (KUVIO 24). Setup valikosta valitaan Configure ja edelleen Add sekä määritellään turvallisuusryhmälle nimi. Turvallisuusryhmään määritellään kaikki ne käyttäjät, joille halutaan myöntää Direct Access- yhteys (KUVIO 25). (McLean & Thomas 2010, hakupäivä 19.12.2010.)

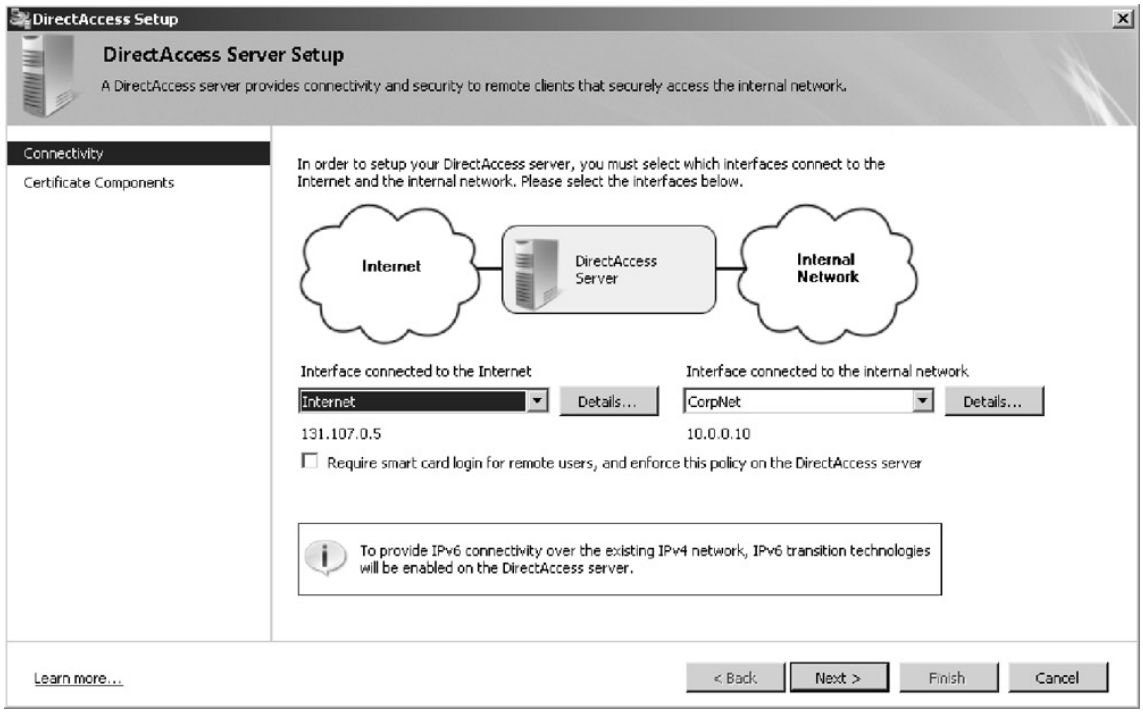


KUVIO 24. *Direct Acces Management Console* (McLean & Thomas 2010, hakupäivä 19.12.2010.)



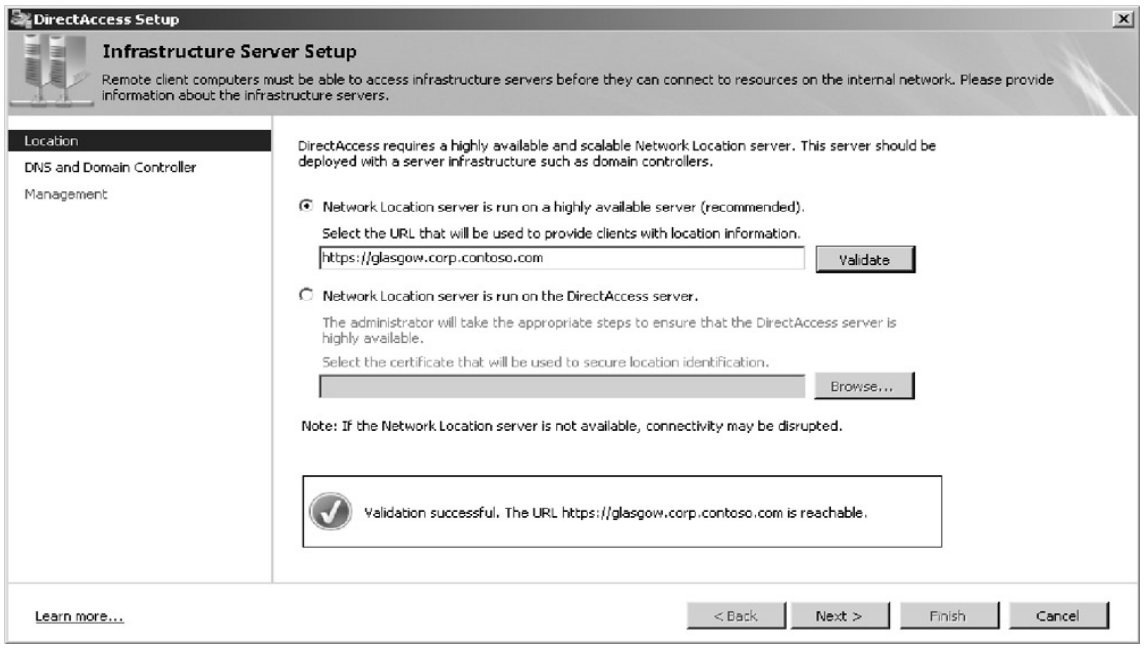
KUVIO 25. *Direct Acces- turvallisuusryhmät* (McLean & Thomas 2010, hakupäivä 19.12.2010.)

Direct Access Server Setup valikosta (KUVIO 26) määritellään liitännät sisäiseen verkkoon sekä internetiin. Tämä vaihe lisää palvelimelle myös IPv6 siirtymätekniikat.



KUVIO 26. *Direct Acces Server Setup* (McLean & Thomas 2010, hakupäivä 19.12.2010.)

Infrastructure Server Setup kohdassa (KUVIO 27) määritellään intranet-sivuston sijainti, jonne asiakaskoneet yrittävät muodostaa yhteyttä. Web-sivusto tulee olla suojattu Web server- sertifikaatilla. Viimeisessä vaiheessa määritellään jaettavat tietoresurssit. Oletusarvoisesti pääsy hyväksytään kaikkiin tietoresursseihin, mutta käyttöoikeuksia voidaan myös tarvittaessa rajata. (McLean & Thomas 2010, hakupäivä 19.12.2010.)



KUVIO 27. *Web- sivuston sijainnin määrittely* (McLean & Thomas 2010, hakupäivä 19.12.2010.)

8 JOHTOPÄÄTÖKSET JA POHDINTA

Etätyöskentelyn merkitys yrityksissä osana työkulttuuria on kasvanut merkittävästi. Tästä olen saanut omakohtaista kokemusta työskennellessäni erään yrityksen IT- osaston tehtävissä harjoittelijana, missä VPN- tekniikan käyttöönotto oli juuri tuolloin käynnissä. VPN- tekniikan käyttöönotolla yritys mahdollisti sellaisten henkilöiden etätyöskentelyn, jotka sitä työnsä luonteen vuoksi tarvitsivat. VPN- tekniikan käyttöönotto voi olla varsin haastava prosessi ja tämän sain tuolloin huomata, vaikka en kyseisessä projektissa täysin mukana ollutkaan. Kokemus kuitenkin herätti mielenkiintoni VPN- tekniikkaan ja sain ensimmäiset ajatukset opinnäytetyöni aiheesta.

VPN- tekniikassa on erilaisia topologioita, jotka on suunniteltu erilaisiin käyttötarkoituksiin. Yksinkertaisimmillaan etäyhteys voidaan luoda Point- to Point topologian mukaisesti, jossa yhteys muodostetaan etäkäyttäjän sekä palvelimen välille. Tätä topologiaa käytetään tyypillisesti silloin kun halutaan mahdollistaa yhteyden muodostus yksittäisen tai yksittäisten henkilöiden ja yrityksen palvelimen välille. Monimutkaisempia topologioita, kuten Star-topologiaa käytetään silloin kun halutaan esimerkiksi muodostaa etäyhteys yrityksen sivutoimipisteiden tai alihankkijoiden ja yrityksen päätoimipaikan välille. Star- topologialle on ominaista, että kaikki tietoliikenne ohjataan päätoimipaikan kautta, eikä sivutoimipisteiden välinen tietoliikenne ole sallittua. Ylläpidollisesti kyseinen topologiamalli on suhteellisen helppo ja edullinen ja sen vuoksi melko yleisesti käytetty malli.

VPN- yhteyden turvallisuus perustuu siinä käytettäviin tunnelointi- ja autentikointiprotokolliin. Tunnelointiprotokollilla yhteys tunneloidaan eli salataan ulkopuolisilta. Tunnelointi on VPN- tekniikan tärkein osa-alue ja siinä datapaketti kapseloidaan kokonaan toiseksi protokolla formaatiksi lisäämällä tunnelointiprotokollan otsikko alkuperäiseen pakettiin. Tunnelointiprotokollat eroavat toisistaan turvallisuudessa ja käytettävän protokollan valintaan vaikuttaa siirrettävän tiedon arkaluonteisuus. PPTP- tunnelointiprotokolla on ylläpidollisesti helpoin ja nopein, mutta on turvallisuudeltaan huomattavasti

heikompi kuin esimerkiksi L2TP- tunnelointiprotokolla. L2TP- protokollan turvallisuus verrattuna PPTP- protokollaan perustuu kontrollipakettien salaukseen datapaketin lisäksi.

Autentikointiprotokollien avulla todennetaan etäyhteyden osapuolet oikeiksi. Todentamiseen käytetään erilaisia protokollia, joka yksinkertaisimmillaan tarkoittaa tunnistautumista pelkän käyttäjätunnuksen ja salasanan avulla, kuten PAP- protokollassa. Tämä altistaa kuitenkin kolmannen osapuolen salakuuntelulle sekä palvelimelle murtautumiseen, koska salasanat lähetetään selkeässä muodossa. Vastaavasti EAP- protokollalla todentaminen voidaan suorittaa käyttämällä esimerkiksi digitaalisia sertifikaatteja, kertakäyttöisiä salasanoja tai Token- kortteja. Tämän vuoksi EAP- autentikointiprotokolla on turvallisin vaihtoehto yhteyden osapuolten todentamiseen.

VPN- tekniikan asennustyö suoritettiin Oulun seudun ammattikorkeakoulun tiloissa. Ennen asennustyön aloittamista on määriteltävä etäyhteyden käyttötarkoitus ja siihen sopiva topologia. Tässä tapauksessa käytettiin Point- to Point topologiaa. Asennustyö aloitettiin konfiguroimalla palvelimeen Remote Access Service (RAS). Tämän jälkeen palvelimelle määriteltiin käyttäjätilit sekä jaettavat tietoresurssit ja käyttöoikeudet. Asiakaskoneelle määriteltiin tämän jälkeen palvelimen IP- osoite sekä annetut käyttäjätunnukset ja salasanat. Tietoresurssit saatiin lopuksi käyttöön NetUse- komennolla.

Toinen osa-alue opinnäytetyössä käsitteli uudempaa etäyhteystekniikkaa, MS-IPHTTPS- tunnelointiprotokollaa. MS-IPHTTPS on kehitetty koska palomuurien ja välityspalvelimien yleistyttyä VPN- yhteyden muodostaminen ei ole aina mahdollista. Yhteyden muodostamiseen käytetään Direct Access -toimintoa, joka mahdollistaa automaattisen yhteyden muodostuksen yrityksen sisäverkkoon. Yhteyden muodostus palvelimelle tapahtuu suojatun Web-sivuston kautta ja sen turvallisuus perustuu IPv6 sekä IPsec- protokolliin.

Ennen Direct Access asennusta on huomioitava siihen liittyvät käyttöjärjestelmärajoitukset, koska tällä hetkellä se toimii ainoastaan Windows 7 Enterprise ja Ultimate käyttöjärjestelmillä sekä Windows Server 2008 R2

palvelinkäyttöjärjestelmässä. Direct Access- toiminnon asennus asiakaskoneella tapahtuu ryhmätoiminnon (Group Policy) kautta jossa asiakastili lisätään määriteltyyn turvallisuusryhmään (Security Group). Asiakaskoneelle tulee myös asentaa sertifikaatti autentikointia varten. Palvelimella asennustyö tapahtuu Direct Access Management Console- toiminnon kautta, jonka avulla voidaan asentaa sekä hallita Direct Access toimintoja. Asennuksessa kyseisen toiminnon avulla määritellään turvallisuusryhmän nimi sekä lisätään käyttäjät, joille halutaan myöntää Direct Access- yhteys. Palvelimelle määritellään lisäksi liitännät yrityksen sisäiseen verkkoon sekä internetiin.

Opinnäytetyöni tarkoituksena oli selvittää VPN- etäyhteystekniikan toimintaan liittyvät yksityiskohdat sekä asennuksen työvaiheet. Toimintaan liittyviä yksityiskohtia olen selvittänyt aiheeseen liittyvän kirjallisuuden sekä digitaalisten lähteiden pohjalta ja tämä muodostaa työni varsinaisen tietoperustan. Työn toiminnallinen osuus muodostui VPN- tekniikan asennuksesta, jonka suoritin Oulun seudun ammattikorkeakoulun tiloissa. Asennettavaksi topologiaksi valitsin Point- to- Point topologian ja käytettäväksi tunnelointiprotokollaksi PPTP- protokollan, koska ne olivat aikataulullisesti ja työn luonteen vuoksi oleellisimpia. Vaativampien topologioiden kuvaus olisi vaatinut reitittimien asennusta ja näin ollen venyttänyt aikataulua ja työn pituutta.

Direct Access- toiminnosta sekä siihen liittyvästä MS-IPHTTPS- tunnelointiprotokollasta odotetaan VPN- tekniikan syrjäyttäjää ja tämän vuoksi halusin perehtyä myös tähän aiheeseen. Halusin kuitenkin pitää pääpainon VPN- tekniikassa ja tämän vuoksi tutustuin Direct Acces- toiminnon asennukseen vain teoria pohjalta. Tämä ratkaisu auttoi mielestäni ymmärtämään riittävästi Direct Access- toiminnon asennusta sekä käyttöä. Mielestäni on hyvinkin mahdollista, että Direct Access tulee syrjäyttämään VPN- tekniikan, koska se vaikuttaa käytettävyydeltään ja asennettavuudeltaan paremmalta ratkaisulta. VPN- tekniikan asennuksessa, L2TP- protokollan konfigurointi voi olla erittäin haasteellista ja aikaa vievää. Direct Access- toiminnon asennus tapahtuu huomattavasti yksinkertaisemmin. Käyttöjärjestelmärajoitukset hidastavat vielä tällä hetkellä kuitenkin merkittävästi

Direct Access- toiminnon yleistymistä mutta uskoisin tilanteen parantuvan huomattavasti muutamassa vuodessa.

Sopivien lähteiden löytäminen oli melkoisen haasteellista sekä aikaa vievää. Etenkään MS-IPHTTPS- protokollasta ei ollut saatavilla sopivia lähteitä juurikaan, koska se on vielä suhteellisen uusi tekniikka. Työni lähes koko tietoperusta on käännetty englanninkielisistä lähteistä ja kirjoitusprosessi oli ajoittain hyvinkin haasteellista termien käännöstyötä. Työssäni olen käyttänyt lähteinä alan kirjallisuutta sekä yleisesti luotettavina pidettyjä Web- sivustoja, kuten Cisco ja Microsoft.

Opinnäytetyöni lähti liikkeelle elokuussa 2010 sisällysluettelon hahmottelulla ja tietoperustan kirjoittaminen alkoi syyskuussa. Työn toiminnallinen osuus suoritettiin koulun tiloissa joulukuun 2010 aikana. Alkuperäinen tavoitteeni oli valmistua joulukuussa 2010, mutta työn toiminnallinen osuus viivästytti valmistumistani kuukaudella.

LÄHTEET

Cert-fi. 2010. Tietoturvakatsaus. 7.7.2010. Hakupäivä 27.9.2010, http://www.cert.fi/attachments/tietoturvakatsaukset/5r1CddYUK/CERT-FI_tietoturvakatsaus_2_2010.pdf

Cisco. 1999. Internetworking Basics. Hakupäivä 29.11.2010. http://docwiki.cisco.com/wiki/Internetworking_Basics#OSI_Model_and_Communication_Between_Systems

Cisco. 2006. IPv6 Extension Headers Review and Considerations. Cisco Systems. Hakupäivä 22.11.2010. http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

Cisco. 2008. Remote-Access VPNs: Business Productivity, Deployment and Security Considerations. Hakupäivä 25.10.2010 http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_white_paper0900aecd804fb79a.html

Cisco. 2009a. Internet-rikollisuudesta tulee yhä enemmän liiketoiminnan kaltaista. Lehdistötiedote 4.9.2009. Hakupäivä 24.9.2010, http://www.cisco.com/web/FI/press/press_releases/2009/tiedote_04092009.html

Cisco. 2009b. EAP Authentication vith RADIUS Server. Hakupäivä 2.11.2010 http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801bd035.shtml

Cisco. 2010.User Guide for Cisco Security Manager 4.0. Hakupäivä 21.10.2010. http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.0/user/guide/vpchap.pdf

Deal, R. 2005. Cisco Router Firewall Security. Hakupäivä 28.9.2010 http://books.google.fi/books?id=vTfFNrkm5YcC&printsec=frontcover&dq=Cisco+Router+Firewall+Security&source=bl&ots=IO-wQ-Hks6&sig=3RCEeWIdRkL7wcsP-tVxJ1lJqHE&hl=fi&ei=phr5TLv8H5HpOfaa9dQK&sa=X&oi=book_result&ct=result&resnum=2&ved=0CCcQ6AEwAQ#v=onepage&q&f=false

Frankel, S. 2005.Guide to IPsec VPNs. Recommendations of the National Institute of Standards and technology. National Institute of Standards and Technology. Special Publication 800-77. Hakupäivä 3.11.2010 http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

Gupta, M. 2002. Building a Virtual Private Network. Hakupäivä 28.9.2010 http://site.ebrary.com.ezp.oamk.fi:2048/lib/oamk/docDetail.action?docID=10054334&p00=building%20virtual%20private%20network

Held, G. 2005. Virtual Private Networking: A Construction, Operation and Utilization Guide. Hakupäivä 29.9.2010 http://site.ebrary.com.ezp.oamk.fi:2048/lib/oamk/docDetail.action?docID=10113984

Holttinen, J. 2002. Ciscon verkkoakatemia -2. vuosi

ITU. International Telecommunication Union. 2010. Hakupäivä 24.9.2010, http://www.itu.int/ITU-D/ict/statistics/material/graphs/Internet_users_00-09.jpg

Kwan, P. 2003. White Paper:802.1X Authentication & Extensible Authentication Protocol (EAP). Foundry Networks. Hakupäivä 2.11.2010 http://www.foundrynet.com/pdf/wp-8021x-authentication-eap.pdf.

Learn Networking. 2008. A Guide to Network Topology. Hakupäivä 22.10.2010 http://learn-networking.com/network-design/a-guide-to-network-topology

Lucas, M., Singh, A. & Liu, D. 2006. Firewall Policies and VPN Configurations. Hakupäivä 28.9.2010 http://site.ebrary.com.ezp.oamk.fi:2048/lib/oamk/docDetail.action?docID=10142565

McLean, I & Thomas, O. 2010. MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7. Hakupäivä 19.12.2010, http://microsofteref.books24x7.com/viewer.asp?bookid=32623&chunkid=565500389

Microsoft TechNet. 2003a. What is TLS/SSL? Hakupäivä 14.11.2010, http://technet.microsoft.com/en-us/library/cc781476%28WS.10%29.aspx

Microsoft TechNet. 2003b.Overview of SSL/TLS Encryption. Hakupäivä 14.11.2010, http://technet.microsoft.com/en-us/library/cc781476%28WS.10%29.aspx

Microsoft TechNet. 2003c. How TLS/SSL Works. Hakupäivä 15.11.2010, http://technet.microsoft.com/en-us/library/cc783349%28WS.10%29.aspx

Microsoft TechNet.2010.IP over HTTPS (IP-HTTPS) Tunneling Protocol Specification . Hakupäivä 4.11.2010, http://technet.microsoft.com/en-us/library/cc771298%28WS.10%29.aspx

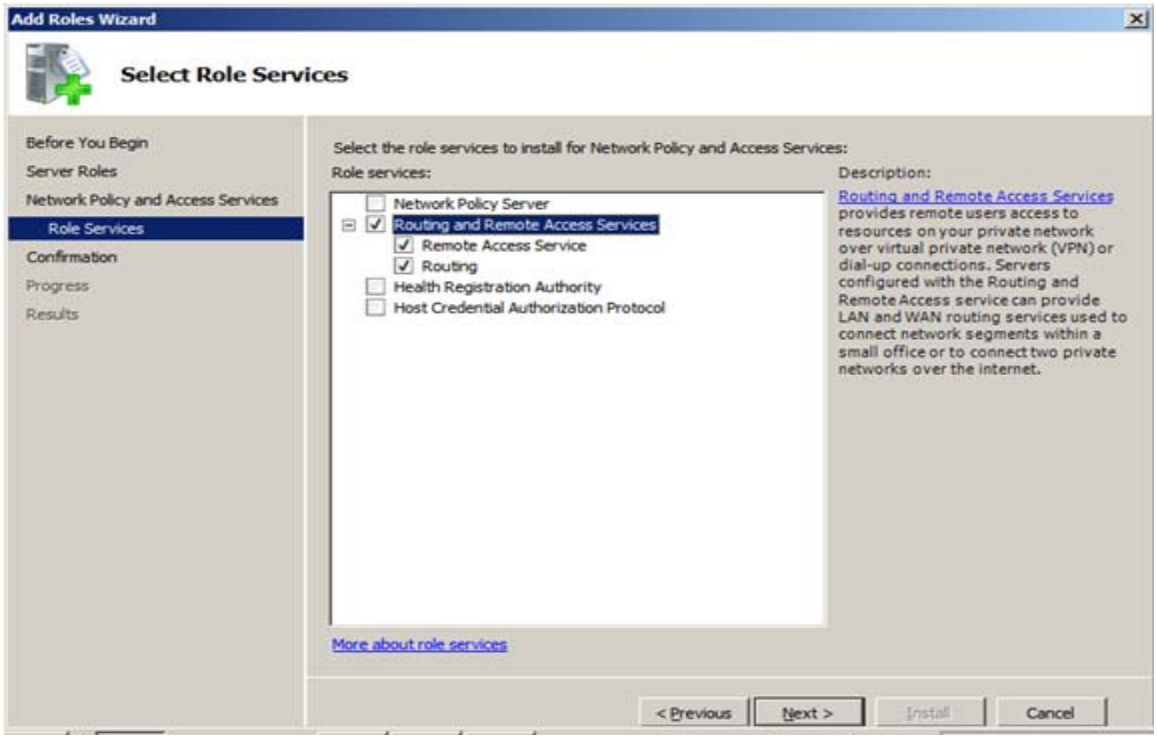
TCP. 2010.TopBits.com Tech Community. Hakupäivä 20.11.2010, http://www.tech-faq.com/tcp.html

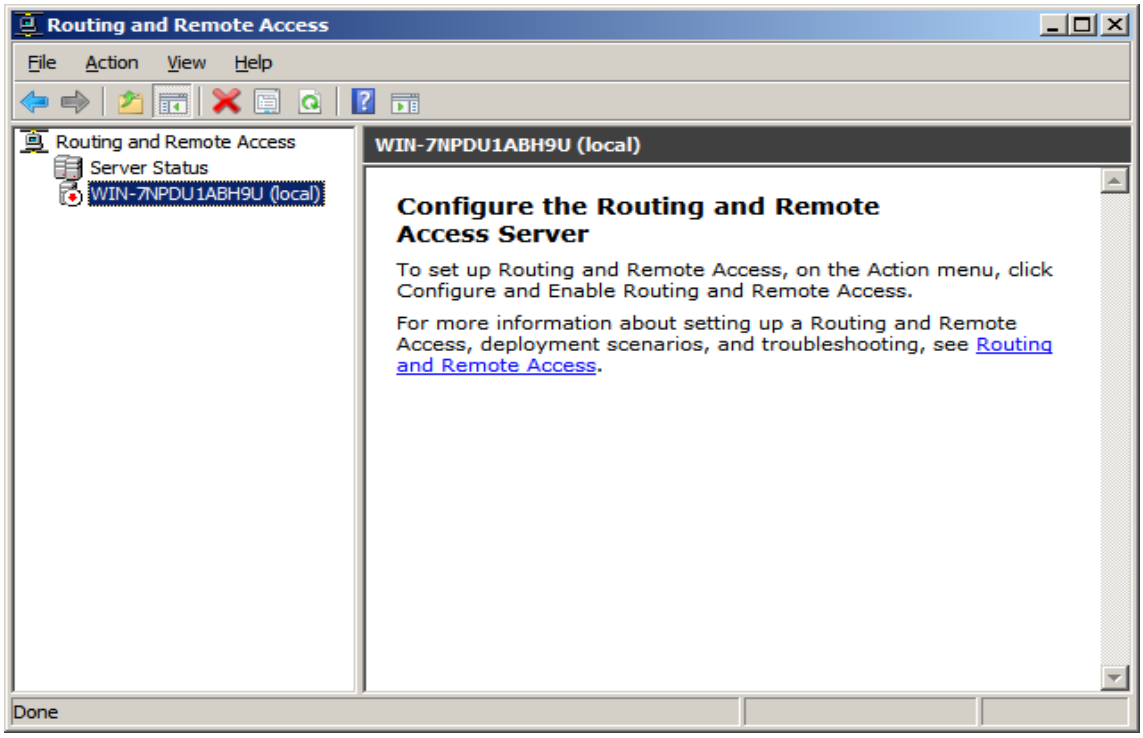
VAHTI. Valtionhallinnon tietoturvallisuuden johtoryhmä.2003. Käyttäjän tietoturvaohje. Hakupäivä 24.11.2010, http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/aineisto/PDF-muodossa/VAHTI_kayttajan_tietoturvaohje.pdf

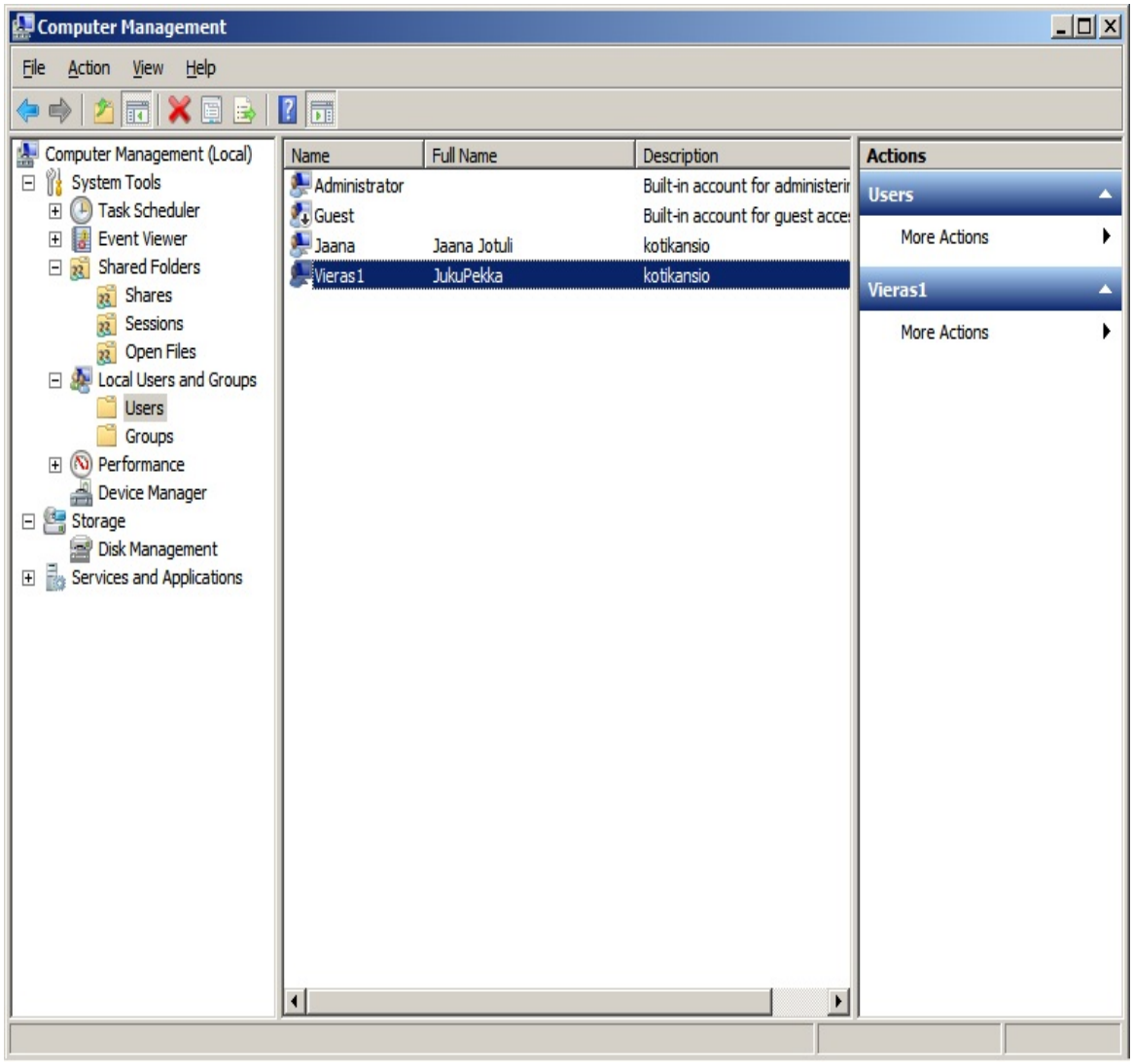
Windows Server 2008. Introduction to IP Version 6. Microsoft Corporation. Hakupäivä 22.11.2010. http://technet.microsoft.com/fi-fi/library/bb726944%28en-us%29.aspx

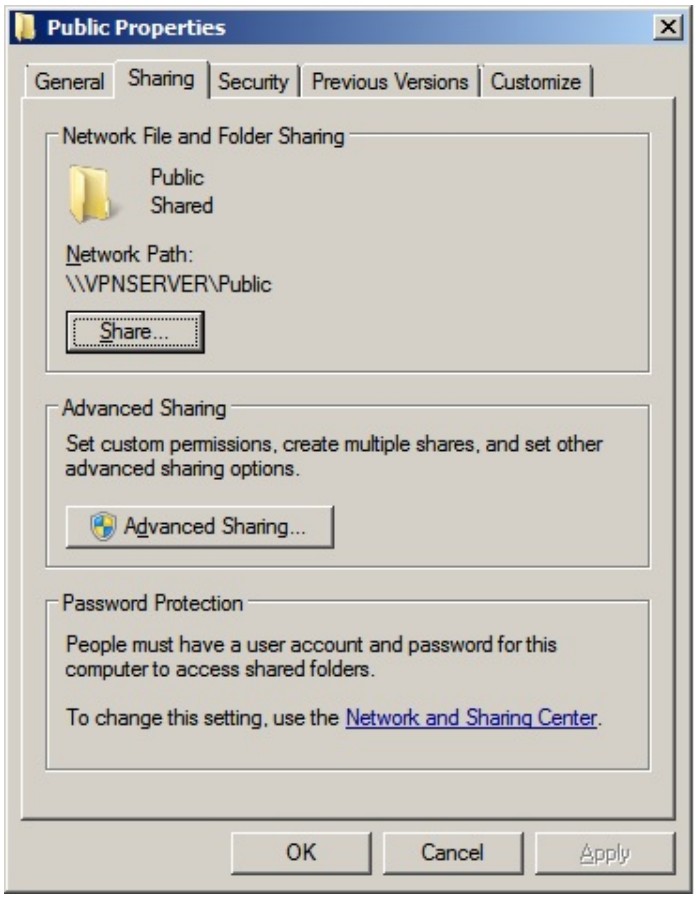
LIITTEET

ROUTING AND REMOTE ACCESS SERVICES LIITE 1

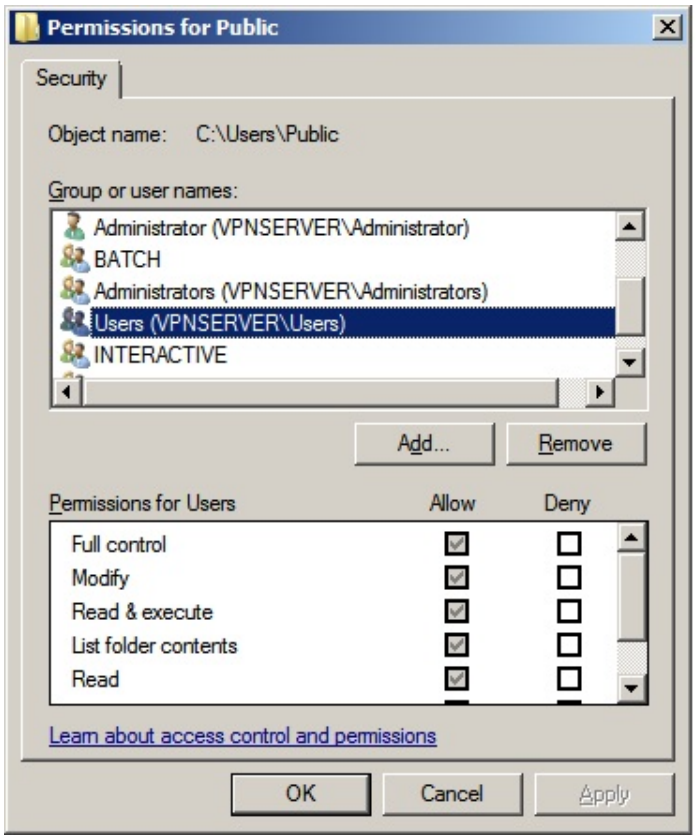





Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Shares
Sessions
Open Files
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administerir
Guest
Built-in account for guest acce
Jaana
Jaana Jotuli
kotikansio
Vieras1
JukuPekka
kotikansio
Actions
Users
More Actions
Vieras1
More Actions


Public Properties
General
Sharing
Security
Previous Versions
Customize
Network File and Folder Sharing
Public
Shared
Network Path:
\\VPNSERVER\Public
Share...
Advanced Sharing
Set custom permissions, create multiple shares, and set other advanced sharing options.
Advanced Sharing...
Password Protection
People must have a user account and password for this computer to access shared folders.
To change this setting, use the Network and Sharing Center.
OK
Cancel
Apply

TIETORESURSSIN KÄYTTÖOIKEUDET LIITE 4



REMOTE ACCESS CLIENTS LIITE 5