TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Tutkintotyö

Markus Lehtinen

VIRTUAALINEN YKSITYISVERKKO ETÄTYÖNTEON SUOJANA

Työn ohjaaja Yliopettaja Jorma Punju
Työn teettäjä Tampereen ammattikorkeakoulun tietokonekeskus
Tampere 2008

TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Lehtinen, Markus
Virtuaalinen yksityisverkko etätyönteon suojana
Tutkintotyö 33 sivua
Työn ohjaaja Yliopettaja Jorma Punju
Kesäkuu 2008
Hakusanat verkko, etätyö, salaus

TIIVISTELMÄ

Virtual Private Networkin (VPN) eli virtuaalisen yksityisverkon avulla voidaan suojata tietoliikenneyhteys julkisen verkon läpi. VPN-tekniikan avulla saadaan varmistettua tiedon lähettäjä, tiedon muuttumattomuus ja tiedon salaus. Tässä tutkintotyössä on tarkoituksena ollut käydä läpi VPN-tekniikkaa ja pohjustaa mahdollisia vaihtoehtoja Tampereen ammattikorkeakoulun (TAMK) tietokonekeskukselle.

Tutkintotyössä on keskitytty tarkastelemaan asioita pääosin etätyöyhteyksien kannalta, sillä muille tekniikan sallimille toiminnoille ei ole kyseisessa ympäristössä juurikaan käyttöä. Tekniikkaa ja VPN-tuotteiden käyttöliittymiä tarkastellessa on käytetty VMware Worksation -ohjelmaa, jonka avulla on virtuaalisesti rakennettu yksinkertaistettu yritysverkko. Tällä ohjelmistolla voidaan siis emuloida tietokonelaitteistoa ohjelmallisesti ja ajaa ns. virtuaalikoneita. Nämä pitävät sisällään omat käyttöjärjestelmänsä ja ohjelmansa, mutta toimivat ohjelman sisällä eivätkä omina fyysisinä laitteinaan. Perinteisiä laitteita käytettäen olisi tarvittu useampia tietokoneita ja tietoliikennelaitteita, joten jo pelkästään kustannussyistä virtualisointi oli tämän tutkintotyön kannalta järkevämpää.

VPN-palvelun käynnistäminen kannattaa suunnitella tarkkaan. Vaikka nykyiset VPN-laiteratkaisut on tehty käyttöönotoltaan ja ylläpidoltaan hyvin yksinkertaisiksi, voi kattavamman VPN-palvelun käynnistys kohdata monia ongelmia. VPN-palveluun kuluvat resurssit pienenevät suhteessa käyttäjämäärien lisääntyessä, joten organisaation koon kasvaessa, kattavan palvelinpohjaisen VPN-palvelun toteuttaminen muuttuu järkevämmäksi. TAMKissa on jo käytössä Citrix MetaFrame XP -palvelu, jolla saa suojatun yhteyden organisaation sisäverkossa oleviin verkkojakoihin ja käyttäjien omiin kotihakemistoihin. VPN-palvelun käyttöönotolle ei välttämättä ole perusteita kuin palvelutason varmistamiseksi toisena vaihtoehtona.

UNIVERSITY OF APPLIED SCIENCES
Information Technology
Telecommunications engineering
Lehtinen, Markus
Protecting Telecommuting with Virtual Private Network
Engineering Thesis 33 pages
Thesis Supervisor Senior teacher Jorma Punju
June 2008
Keywords network, telecommuting, encryption

ABSTRACT

VPN (Virtual Private Network) is a technique that is being widely used to protect IP network traffic over public networks. VPN allows for authentication and confidentiality of the transferred data. It can be used to secure data transfer over public networks like Internet. On this final thesis, we examine VPN technology and concentrate on its qualities for users that work from remote location. The examination of the VPN servers and services was done with the help of a program called VMware Workstation. It allows virtualizing PC hardware and then running operating system and programs on the emulated hardware. Virtualizing in this case means that there is no real hardware used for the servers and the network devices but those were emulated within a program. The servers function as normal and have their own operating systems and services installed but they just lack fysical form. Virtual machines were used, because the needed hardware would have been expensive to purchase.

VPN service usually needs fare amount of resources to start and administer. Because of that, smaller organizations with smaller VPN user base often consider hardware based solutions. These days, the networking hardware meant for smaller companies is fairly easy to set up but bigger networks and larger user bases can generate foreseeable problems. A full blown VPN server based solution becomes more valid an option, when the organization grows in size and the needed resources lessen per user. University of Applied Sciences (TAMK) already has a somewhat similar service called Citrix MetaFrame XP that allows, among other things, users to connect to network drives and home directories from a remote location. Unless there becomes a need for connecting to shared project databases or something similar, there is no real need to start a VPN service for the users working from remote locations.

SISÄLLYSLUETTELO

SANASTO

Autentikointi (Authentication)

Tunnistaminen. Käytetään kahden erillisen tekniikan kuvaamisessa: datan alkuperäisyyden todentamisen ja yhteyden todentamisen.

AH, Authentication Header

IPSecin yhteyskäytäntö, protokolla 51, jossa dataa ei suojata salaamalla. Laskee avaimellisen tiivisteen (hash) datapaketin otsikkokenttään.

ESP (Encapsulated Security Payload)

IPSecin yleisin yhteyskäytäntö, protokolla 50, jossa kaikki alkuperäinen data salataan.

DH (Diffie-Helman)

Salausmenetelmä, jota käytetään esimerkiksi VPN-autentikoinnissa. DH-1 käyttää 768 bitin salausavainta ja DH-2 käyttää 1024 bitin salausavainta.

DES (Data Encryption Standard)

Vanha symmetrinen salausmenetelmä, mitä ei nykyään enää pidetä riittävän tehokkaana. Salausavaimen pituus on 56 bittiä.

3DES (Triple-DES)

Nykyinen painos DESistä, joka on suosittu salaustapa VPN-tuotteissa. Käyttää samaa salausalgoritmia kuin DES, mutta tieto salataan kolme kertaa. Salausavaimen pituus 112 tai 168 bittiä riippuen siitä, käytetäänkö kolmessa salauskerrassa yhteensä kahta vai kolmea eri salausavainta.

GRE (Generic Routing Encapsulation)

Ciscon kehittämä tunnelointiprotokolla, jolla tunneloidaan normaalisti VPN-yhteyksiä tai tavallisia IP-paketteja. Nopea protokolla, mutta laitteiden tuki protokollalle on vaillinainen.

IKE (Internet Key Exchange)

Ipsecin käyttämä salausavainten vaihtamiseen tarkoitettu menetelmä eli toisin sanoen autentikointitapa. Määritelty IETF:n dokumentissa RFC 2409.

IP (Internet Protocol)

TCP/IP-protokollaperheen reitittävä yhteydetön datapakettipohjainen menetelmä.

IPSec (Internet Protocol Security)

Suosituin IP-pakettitason VPN-standardi, joka on määritelty IETF:n dokumentissa RFC 2401.

ISP (Internet Service Provider)

Internet palveluntarjoaja on yhteisö tai yritys, joka tarjoaa Internet-yhteyksiä ja mahdolisesti muita verkkopalveluja.

L2F (Layer Two Forwarding)

Ciscon OSI-mallin toisella kerroksella toimiva tunnelointistandardi.

L2TP (Layer 2 Transfer Protocol)

Microsoftin ja Ciscon yhdessä kehittämä ja IETF:n standardoima tunnelointimenetelmä. Toimii OSI-kerroksen toisella tasolla, joten sitä voidaan käyttää useiden tietoliikenneprotokollien kanssa.

MD5 (Message Digest 5)

Kevyt laskentamenetelmä, jota käytetään autentikoinnissa. Se salaa datan 128 bitin pituisella salausavaimella.

NAT (Network Address Translation)

Sisäverkon osoitteiden piilottaminen datapaketin otsikon osoitteiden muutoksella. Muuttaa organisaation sisäverkon yksityiset osoitteet julkiseen verkkoon siirryttäessä virallisiksi IP-osoitteiksi. Menetelmä muokkaa datapakettien otsikkokenttää, koska tämä pitää sisällään kohde- ja lähdeosoitteet.

PKI (Public Key Infrastructure)

Autentikointitapa, jossa käytetään julkista ja yksityistä salausavainta.

PPP (Point-to-Point Protocol)

TCP/IP:n protokollariippumaton etäyhteysprotokolla. Käytetään pääosin reitittimien välillä.

PPTP (Point-to-Point Tunneling Protocol)

Microsoftin vanhahko VPN-tekniikka, joka soveltuu yksittäisten koneiden yhteydeksi, mutta ei ole suojaukseltaan nykyaikaisempien standardien tasolla.

SA (Security Association)

VPN-yhteyden osapuolien sopima salausavainten ja asetusten yhdistelmä.

SHA (Secure Hash Algorith)

VPN-autentikointimenetelmä, joka antaa paremman salauksen kuin MD5.

SPI (Stateful Packet Inspection)

IP-pakettien ja yhteyden tilaan perustuva tarkkailumenetelmä.

TCP (Transmission Control Protocol)

OSI-mallin mukainen kuljetuskerroksen kuljetuspalvelu.

TCP/IP (Transmission Control Protocol / Internet Protocol)

Tietoliikenneprotokollien yhdistelmä, mitä käytetään Internetin tiedonsiirrossa. IP-protokollalla hallitaan laitteiden osoitteet ja tiedon reitittäminen, kun taas TCP-protokollalla toteutetaan datapakettien ajallinen järjestely ja virhetilanteiden menettelyt.

VPN (Virtual Private Network)

Virtuaalinen yksityisverkko, joka suojaa yhteyden julkisen verkon esim. Internetin ylitse. Suojaus perustuu autentikointiin ja salaukseen.

1 JOHDANTO

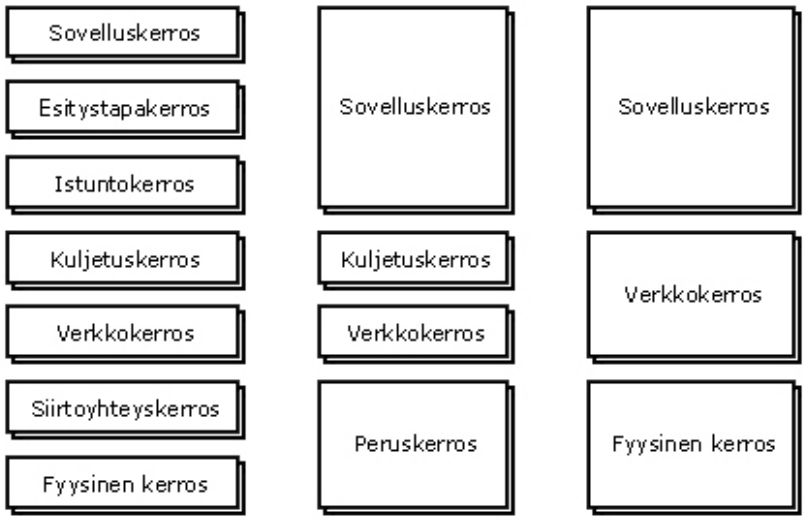
Internet Protocol (IP), on yleisin protokolla isoissa tietoliikenneverkoissa. /2/ Näistä parhaana esimerkkinä voi pitää Internetiä, joka toimii IP-tekniikalla. IP on joustava ja tehokas. Sillä saadaan muodostettua yhteys hyvin monimuotoisten tietokonelaitteiden välille. Joustavalla rakenteella on vastapainona siitä johtuvat heikkoudet. Nämä antavat mahdollisuuden esim. tiedon alkuperän varmentamisen ja muiden tietoturvaa lisäävien toimintojen kiertämiseen. IP-pohjainen data on siis itsessään avoin muokkaukselle ja salakuuntelijoille. /18/ Tätä varten on kehitetty VPN-tekniikoita, joilla voidaan tietoa siirtää turvattoman julkisen verkon ylitse. /2/

Tässä tutkintotyössä käydään läpi VPN-tekniikkaa enimmäkseen suositun Internet Protocol Security (IPSec) -protokollaperheen kautta. Tarkoituksena on tarkastella VPN-tekniikan etätyön kannalta merkittäviä ominaisuuksia, mikä pohjustaisi mahdollista VPN:n käyttöönottoa Tampereen ammattikorkeakoulussa.

Tapoja rakentaa VPN julkisen verkon yli on lukuisia, mutta tässä tutkintotyössä keskitytään ns. päästä päähän malliin, koska tarjoajamallin ja hybridimallin kanssa ollaan aina yhteistyössä palveluntarjoajan kanssa. VPN:n toiminnallisuus ja ylläpito eivät ole siis jälkimmäisissä täysin omassa hallinnassa, vaan näissä ainakin osan palveluista joutuu ostamaan Internet-runkoverkon omistavilta tahoilta, eli periaatteessa Internet-palveluntarjoajilta. Kuten eri mallien nimityksistäkin voidaan päätellä, tarjoajamallissa on kyse palveluntarjoajan myymästä palvelusta, ja hybridmalli tarkoittaa sitä, että osa palvelusta ostetaan palveluntarjoajalta ja osa jää organisaation omalle ylläpidolle. /2/

Verkko ajatellaan koostuvaksi kerroksista, joissa jokaisessa on omanlaiset toiminnallisuutensa. IP-verkkojen voidaan kuvitella koostuvan OSI-mallin mukaisesti seitsemästä kerroksesta: Fyysisestä kerroksesta, Siirtoyhteyskerroksesta, Verkkokerroksesta, Kuljetuskerroksesta, Istuntokerroksesta, Esityskerroksesta ja Sovelluskerroksesta. Jokainen näistä kerroksista tarjoaa palveluita ylemmälle kerrokselleen. /21/

Tietoliikenteen tekniikoista puhuttaessa voidaan mainita myös TCP/IP-viitemalli kuten myös yksinkertaistettu OSI-malli. Alkuperäisessä OSI-mallissa on seitsemän eri kerrosta, mutta verkon tarkastelussa selkeyttämiseksi voidaan käyttää TCP/IP-viitemallia, jossa on neljä kerrosta tai jopa yksinkertaistettua OSI-mallia, jossa on vain kolme kerrosta. Eri mallien kerrokset ja yhteydet toisiinsa on kuvattu alla (kuva 1). /2/



Kuva 1 OSI-malli, TCP/IP-viitemalli ja yksinkertaistettu OSI-malli

Käyttäen yksinkertaistettua OSI-mallia, tiedonsiirtoprotokollat jaotellaan vain kolmeen kerrokseen. Fyysinen eli linkkikerros on alin kerros. Se koostuu kaapeleista, verkkokorteista, kytkimistä sekä muista linkeistä, joita pitkin tieto liikkuu. Näissä käytetään yksinkertaisia protokollia, joilla tietoa vaihdetaan ylempien kerroksien kanssa. IP-verkossa, eri verkon osat käyttävät erityyppisiä fyysisiä laitteita: Ethernet-yhteyksiä toisissa osissa ja pisteestä pisteeseen tyyppisiä ratkaisuja toisaalla. /2/

Fyysisen kerroksen yläpuolella verkkokerroksen tehtävä on siirtää tietoa liityntäpisteestä toiseen koko verkon alueella. Se käyttää alemman kerroksen protokollia itse datansiirtoon ja omaa reitityslogiikkaansa päättäessään parhaat aliverkot, joiden kauttaa data siirretään. /2/

Verkkokerroksen yläpuolella on muutama korkeamman tason protokolla, jotka asettavat linkit reitittimien välille erityppiisiä tiedonsiirtoja varten ja

Sovelluskerros, jossa ohjelmat toimivat. Sovellukset käyttävät Verkkokerroksen palveluja datan siirtoon ja verkkokerros puolestaan käyttää Fyysistä kerrosta saadakseen datan verkkokortista toiseen. /2/

Merkittävä IP-verkkojen ominaisuus on se, että sen Verkkokerros on täysin yhtenevä. Tämä tarkoittaa sitä, että minkä tahansa tiedonsiirron verkkokerroksen läpi, myös Internet-liikenteen, täytyy käyttää IP-protokollaa. Silloin kun IP-protokolla on suojattu, niin koko tiedonsiirto on suojattua. /2/

Tähän perustuu moni VPN-tekniikka, jossa pelkkä Verkkokerroksen hallinnointi riittää suojatun yhteyden toteuttamiseen. Hieman yleistäen kahden muun kerroksen tekniikoista puhuttaessa, Sovelluskerroksen tekniikat on tehty suojaamaan ainoastaan tiettyjä ohjelmia ja Fyysisen kerroksen tekniikat taas vaativat runkoverkon hallinnan koko tiedonsiirtoreitin matkalle. /2/

2 VIRTUAALINEN YKSITYISVERKKO

Virtuaalisella yksityisverkolla (Virtual Private Network, VPN) muodostetaan yhteys maantieteellisesti erillään olevien tietokoneiden välille julkisen verkon eli periaatteessa Internetin kautta. Internet julkisena yhteytenä mahdollistaa ulkopuolisten tahojen pääsyn siirrettävään tietoon. VPN:ssä käytettyjen protokollien avulla voidaan tieto salakirjoittaa ja myös määritellä mille koneille se lähetetään. Rajatut käyttäjät tekevät verkosta yksityisen, mutta koska tietokoneiden välinen yhteys ei ole fyysisesti yksityisen tahon omistuksessa, kuten vaikka organisaation sisäverkko, käytetään siitä nimitystä ”virtuaalinen yksityisverkko”. /17/

Virtuaalisia yksityisverkkoja on hyvin monenlaisia, mutta perusidealtaan ne ovat yksinkertaisia: turvattomalla siirtotiellä data on salattua. Salaukseen ja salauksen purkuun tarvitaan lähettävässä ja vastaanottavassa päässä yhteinen salausavain. Näiden salausavainten jakelun ja vaihtamisen uusiin voi hoitaa useilla tavoilla, mutta kätevimmin se hoituu käyttämällä siihen erillistä protokollaa, kuten Internet Key Exchangea (IKE), jolla salausavainten vaihto hoituu automaattisesti yhteyttä

muodostettaessa. Salausavainten vaihdosta ja IKE-protokollasta hieman tarkemmin kohdassa 3.4. /17/

Suurin osa erilaisista virtuaalisen yksityisverkon toteutustavoista tukee ns. tunnelointia. Julkisen siirtotien yli muodostetussa yhteydessä datapaketit salataan kokonaan otsikoineen päivineen ja niille lisätään uusi otsikko tiedonsiirtoa varten. Tätä kutsutaan kapseloinniksi ja se peittää alkuperäiset lähde- ja kohdeosoitteet ulkopuoliselta tarkastelulta ja analysoinnilta. /9/

Kun puhutaan VPN:n toteutuksesta laitetasolla, se voidaan tehdä esimerkiksi palveluna palomuurina toimivassa palvelimessa tai vaikka palomuuritoiminnot sisältävässä reitittimessä. Tietoturvallisuuden kannalta on kuitenkin useimmiten suositeltavaa käyttää erillisiä laitteita palomuurille ja VPN-palveluille. /18/

Käyttökohteita VPN:lle on periaatteessa kolme: sillä voidaan yhdistää suojatusti maantieteellisesti erillään olevia sisäverkkoja, muodostaa yksittäisiltä koneilta etäyhteys organisaation sisäverkkoon ja suojata tai piilottaa osa organisaation sisäverkosta vain tietyn käyttäjäryhmän käyttöön. Alkuperäinen VPN:n käyttötarkoitus oli juuri maantieteellisesti etäällä toisistaan olevien sisäverkkojen suojattu yhdistäminen julkisen siirtotien ylitse. Etäkäytön tarve on kuitenkin viimevuosina lisääntynyt huimasti, joten tämä on VPN:n käyttökohteenakin tullut merkittäväksi. /2/

Sisäverkkojen yhdistäminen VPN:n avulla tarkoittaa yksinkertaisesti sitä, että kummankin sisäverkon palvelimet, tai VPN-palvelun toteuttavat laitteet, konfiguroidaan muodostamaan keskenään suojattu yhteys julkisen verkon ylitse. Kaikki liikenne sisäverkkojen välillä ohjataan sitten näiden palvelimien kautta. /2/

VPN-etäyhteys voidaan toteuttaa joko ohjelmistoilla, laitteilla tai ohjelmistojen ja laitteiden yhdistelmällä. Yhteyden muodostamisen jälkeen voi etäkäyttäjä hyödyntää VPN-palvelimen tai koko sisäverkon tarjoamia palveluita. Etäyhteys saadaan aikaiseksi siten, että VPN-asiakasohjelma (VPN client) etäpäätteessä tai tarvittavat protokollat sisältävä laite etäpäätteen ja Internet palveluntarjoajan

välissä ottaa yhteyden organisaation VPN-palvelua tarjoavaan palvelimeen tai reitittimeen Internetin ylitse. /2/

Kolmas VPN:n käyttökohteista, eli sisäverkon eri osien eriyttäminen toisistaan, on melko harvinainen, eikä se ole juurikaan esillä VPN:stä puhuttaessa. Tämä johtuu pääosin siitä, että usein on helpompiakin tapoja toteuttaa sama toiminnallisuus. Kyseessä on organisaation oma sisäverkko, jossa voidaan luoda yksityisiä verkon osia laitetasolla ja reitittää eri organisaation osat halutulla tavalla toisiltaan piiloon. /2/

3 IPSEC

Internet Protocol Security (IPSec) ei periaatteessa ole protokolla, kuten siitä yleensä puhutaan, vaan protokollakokoelma. Se mahdollistaa valinnat tietoturvaprotokollille ja käytettäville algoritmitmeille sekä tarjoaa tarvittavat salausavaimet pyydetyille palveluille. /6/

IPSecin on todettu toimivan hyvin ja se on laajalle levinnyt standardi. IPSec on myös sisällytetty tulevaan Internet-protokolla versio 6 -standardiin (IPv6). Tämä tarkoittaa sitä, että seuraavan Internet-protokollan myötä, IPSec tulee olemaan mukana yleisessä IP-liikenteessä.

IP on maailman yleisin verkkoprotokolla, koska se on koko Internetin pohjana. IP:n vahvuutena ovat pienet ja monipuolisesti reititettävät datapaketit, joiksi se paloittelee datavirran tiedonsiirron ajaksi tietoliikenneverkossa. IP:llä on kuitenkin heikkoutensa. Pakettien reitittämistavasta takia IP-verkot ovat alttiita tietyille tietoturvariskeille: verkkoon liitetty tietokone voidaan naamioida toiseksi koneeksi, kahden osapuolen välistä tiedonsiirtoa voidaan salakuunnella ja kun yhdistetään nämä kaksi keinoa, voidaan muodostaa tiedonsiirtotapahtuma naamioituneena yhdeksi keskustelukumppaneista. Näiden haavoituvuuksien takia Internet Engineering Task Force (IETF) kehitti IPSec-protokollakokoelman ja joukon IP-laajennuksia, joilla saadaan toteutettua tietoturvapalveluita verkkokerroksella. /18/

Periaatteessa IPSec sisältää kolme tietoturvaa lisäävää menetelmää, jotka ovat Authentication Header (AH), Encapsulation Security Payload (ESP) ja Internet Key Exchange (IKE). AH-otsake IP-paketille antaa liikennöivien osapuolten varmistaa, että siirretty datapaketti ei ole muuttunut matkan varrella ja että paketti on tullut juuri tietyltä koneelta, ESP salakirjoittaa datan salakuuntelijoiden varalta ja IKE taas antaa osapuolille mahdollisuuden neuvotella yhteyden salaustavasta ja toteuttaa salausavainten vaihto. /18/

3.1 Tunnelointi

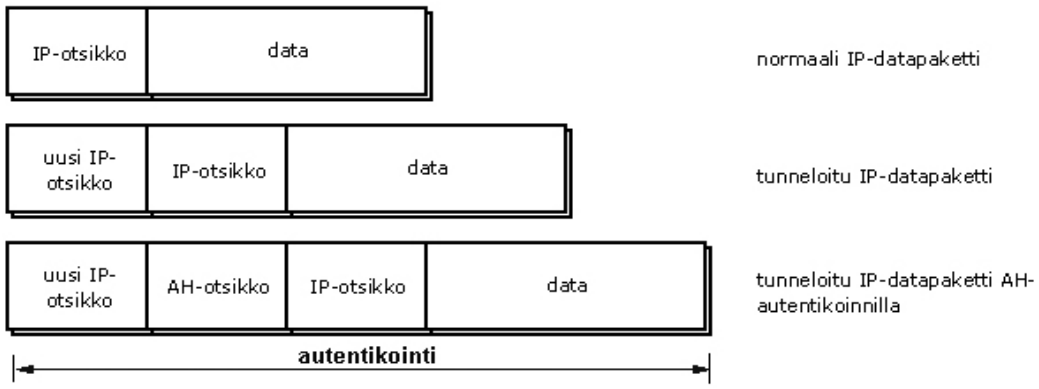
IPSec voitaisiin luokitella tunnelointitekniikaksi, mutta se sisältää paljon pelkän tunneloinnin ulkopuolisia tekniikoita, jotka tekevät siitä kattavamman kokonaisuuden. Tunneloinnilla saadaan aikaan toiminnallisuus, joka yleisimmin yhdistetään VPN-tekniikkaan. Tunneloinnissa IP-paketti kapseloidaan toisen paketin tai kehyksen sisälle ja sen sisältö puretaan vasta vastaanottavassa päässä. /12/ Yleisenä vertauksena käytetään kirjeen laittamista kirjekuoreen: kuoressa on osoite, johon kirje viedään, eivätkä ulkopuoliset näe, mitä kirje sisältää. Hieman tarkemmin tunnelointia kuvaava esimerkki voisi olla se, että sisäisen postin kirjekuori lähetetään ensin yrityksen sisäisellä postilla postitukseen, jossa se laitetaan kirjekuoreen julkisen siirtotien ylitykseen. Kun kirje saapuu perille yrityksen toiseen konttorin postinkäsittelyyn, niin tuo kirjekuori avataan ja sisältö siirretään sisäisen postin kirjekuoressa vastaanottajalle. Käytännössä tämä siis tarkoittaa yksityisten osoitteiden piilottamista, siksi aikaa, kun datapaketit kulkevat julkisessa verkossa. /2/

Tunnelointiin yleensä liitetään myös tiedon salaaminen, mutta se on periaatteessa erillinen toiminnalisuus, joka ei sinällään kuullu itse tunnelointiin. Tunnelointia voi siis periaatteessa olla ilman salauksen käyttämistä datapaketeissa. IPSecin tunnelointiprotokolla sisältää todennuksen ja juuri salauksen. /12/

3.2 Authentication Header

IPSec käyttää kahta protokollaa itse tiedonsiirron suojaamiseen: Authentication Header (AH) ja Encapsulating Security Payload (ESP). Näitä protokollia voidaan käyttää joko yksinään tai yhdessä. /8/

AH:ta käytetään yhteydettömässä yhteydessä datan muuttumattomuuden ja datan alkuperän todentamiseksi. AH todentaa IP-otsakkeesta niin paljon kuin mahdollista, mutta osa otsikkokentistä muuttuu pakettia reititettäessä, eikä lähettävä pää aina voi ennustaa tarkalleen, mitä nämä muutokset ovat. Matkalla muuttuvia tietoja ei täten voida todentaa AH:lla, joten sen antama tietoturva on vain osittainen. /8/



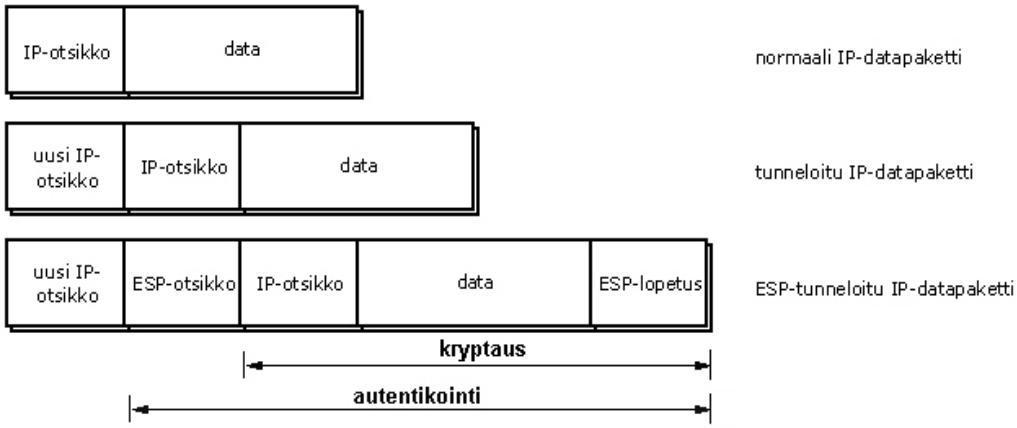
Kuva 2 AH-autentikointi tunneloidussa IP-datapaketissa

Yllä olevassa kuvassa (kuva 2) nähdään tunneloinnin ja AH-protokollan tekemät muutokset IP-datapakettiin.

Huomioitavaan on se, että AH-autentikointia ei voi käyttää Native Address Translationin (NAT) läpi. Käytettäessä ns. harmaita IP-osoitteita AH lakkaa toimimasta, sillä NAT-palvelussa IP-osoite vaihtuu, eikä AH pysty ennakoimaan muutosta. Tämä on kierrettävissä NAT-T-tekniikalla, mutta tästä enemmän kohdassa 3.7. /16/

3.3 Encapsulating Security Payload

Encapsulating Security Payloadilla (ESP) voidaan toteuttaa samankaltainen datan muuttumattomuuden varmistus kuin AH:lla, ja sillä voidaan myös tehdä tiedonsiirrosta luottamuksellista käyttämällä salausta. Suurin ero alkuperäisyyden varmistamisessa AH:n ja ESP:n välillä on niiden kattavuudessa. ESP ei lainkaan suojaa IP-otsikoita, vaan pelkästään datapaketin sisältöä, ellei niitä kapseloida käyttäen tunnelointitilaa. /8/ Kuljetustilaa käyttäen IP-paketeista salakirjoitetaan vain dataosio ja otsikko jätetään ennalleen. Hyvänä puolena tässä on se, että datapakettien koko ei kasva uuden otsikon verran, kuten tunnelointitilassa. Heikkoutena on se, että otsikon alkuperäiset lähettäjä- ja vastaanottajatiedot ovat luettavissa selkokielisinä, mikä vähentää tekniikan antamaa yksityisyyttä. /7/



Kuva 3 ESP-tunnelointi ja salaus IP-datapaketissa

Yllä olevassa kuvassa (kuva 3) nähdään ESP-tunneloinnin tekemät muutokset IP-datapakettiin. ESP-otsikko lisätään IP-otsakkeen jälkeen ja ennen seuraavan tason protokollan otsikkoa kuljetustilassa tai ennen kapseloitua IP-otsikkoa tunnelointitilassa. /9/

Huomionarvoista on se, että ESP ei itsessään määrittele salaustapaa, vaan se antaa vain kehyksen näiden toteutukselle. Itse salausalgoritmi on siis ylläpitäjän valittavissa ja ESP määrittelee, mitkä osat IP-paketista salataan. /7/

3.4 Internet Key Exchange

Käyttääkseen salausta verkkoympäristössä osapuolten on ensin vaihdettava keskenään salausavaimia. Koska kummankin osapuolen tarvitsee tietää käytetty salausalgoritmi, täytyy jollakin turvallisella tavalla saada tieto siirrettyä osapuolten välillä. /18/ Luotettava salaus perustuu luotettavaan salausavainten vaihtoon osapuolien välillä. Internet Key Exchange (IKE) on yksi yleisimmistä salausavaimen vaihtamiseen käytetyistä standardeista. /3/ Se suunniteltiin IPSec-järjestelmän osaksi, mutta sitä on otettu käyttöön muidenkin protokollien kanssa. /6/

Pienissä verkoissa on toki mahdollista antaa yhteinen salausavain manuaalisesti kaikille tarvitseville, mutta VPN-yhteyksien määrän noustessa kymmeniin tai satoihin, alkaa käsin salausavainten jakelu vaatimaan jo huomioitavissa määrin työtunteja. IKE ratkaisee salausavainten vaihtamisen ongelman varsinkin suurissa ympäristöissä, joissa manuaalinen avainten vaihto ei olisi järkevää. /18/

Automatisoitu salausavainten sopiminen osapuolten välillä helpottaa työtaakkaa ja antaa ylläpidon käyttää työaikaansa hyödylisemmin. IKE on valittu IPSecin avaintenvaihtomekanismiksi, jolla salausavaimet saadaan sovittua osapuolten välillä salattua yhteyttä muodostettaessa. /16/ IKE on teollisuuden standardi, joten sitä voidaan käyttää monenlaisten laiteratkaisuiden kanssa /3/. IKE-protokolla autentikoi kummankin osapuolen ja perustaa ns. turvallisuusliiton. Turvallisuusliitto määrää yhteyden molemmalle osapuolelle salausavaimen, jota hyödynnetään ESP:n, AH:n ja salausalgoritmien käytössä suojatussa yhteydessä. /5/

IPSecin avaintenvaihtoprotokolla on määritelty IETF:n dokumenteissa RFC 2407, RFC 2408 ja RFC 2409.

3.5 Salaus

IPSec-protokollat eivät määrittele käytettyä salaustapaa, joten sen valinta jää palvelun käyttöönottajien harteille. Salaustavan valinnan vapaus on antanut

palveluntarjoajille mahdollisuuden eritasoisten VPN-tuotteiden kehittämisen ja myymisen. Tämä on edesauttanut IPSecin leviämistä. /1/

Salauksen valinta kannattaa miettiä aina tapauskohtaisesti, koska se on aina kompromissi tietoturvan ja nopeuden välillä. Salattujen datapakettien kaappaus, yhdistäminen ja kryptauksen purkaminen ei ole mitenkään helppo tehtävä, joten salauksessa ei kannata liioitella. Yleisimpiä VPN-käytössä olevia salausalgoritmeja ovat DES ja 3DES. Ensimmäinen näistä eli DES on jo vanhahko algoritmi, ja sitä pidetään heikkona salauksena, koska sen käyttämä salausavain on vain 56 bittiä pitkä. Tästä uudempi painos 3DES tekee periaatteessa saman salauksen kolmeen kertaan kahdella tai kolmella erillisellä salausavaimella, ja sen salaus on joko 112 bittiä tai 168 bittiä pitkä. /2/

Vanhat ja heikot salausalgoritmit ovat murrettavissa ja tavat ovat yleisesti tiedossa, mutta toisaalta liian raskasta salausta käyttäessä tiedonsiirtonopeudet tippuvat merkittävästi. VPN-palvelimen tai -laitteen ruuhkautuminen täytyy ottaa huomioon varsinkin, jos VPN-palvelut toteuttavalle laitteelle on annettu myös muita palveluita, kuten esim. palomuuritoiminnot. Tällöin VPN-liikenteestä aiheutuva ruuhka ei kuormita ainoastaan VPN-tietoliikennettä, vaan myös koko tiedonsiirtoa palomuurin läpi.

3.6 Hash-algoritmit

Hash-algoritmi on matemaattinen kaava, joka laskee annetusta merkkijonosta aina tietyn kokoisen merkkijonon. Tätä voisi ajatella erittäin tiiviinä referointina, joka muuttuu aina jos alkuperäistä lähdettä muutetaan. Laskutoimitus on toistettavissa eli lähteen pysyessä samana, Hash-algoritmi saa siitä aikaan aina saman merkkijonon. /3/

Hash-algoritmeja käytetään tiedonsiirrossa tiedon muuttumattomuuden tarkistukseksi. Datapaketista lasketaan ns. tarkistussumma. Jos tarkistussumma on muuttunut matkan varrella, niin data hylätään, sillä silloin reitin varrella data on

joko korruptoitunut tai muokattu tarkoituksella jonkin kolmannen osapuolen toimesta. /3/

3.7 IPSec NAT-T

Koska Network Address Translationilla (NAT) eli osoitteenmuunnoksella voidaan piilottaa sisäisen verkon koneet ulkopuolisilta, ja sitä käytetään usein tietoturvaa lisäävänä tekniikkana. NAT:lla saadaan myös lisättyä usein rajallisesti tarjolla olevia IP-osoitteita verkossa, joten tekniikka on hyvin yleinen. Jos IPSecin tiedonsiirron täytyy kulkea verkossa, jossa on käytössä osoitteenmuunnos, niin IKE:n salausavainten vaihto epäonnistuu, eikä IPSec pysty suojaamaan yhteyttä. /2/

NAT aiheuttaa varsinkin hieman vanhempien VPN-tuotteiden kanssa ongelmia, sillä se muokkaa datapaketin otsikoita. Otsikoiden muuttumattomuus taas on tiettyjen VPN-toimintojen perustana, joten NAT-verkon osoitteiden muunnos estää IP-pohjaisen VPN-tietoliikenteen toiminnan. Ongelma voidaan kiertää käyttämällä UDP-paketointia NAT-verkossa. NAT-T-menetelmällä kapseloidaan datapaketit UPD-paketin sisälle siirryttäessä NAT-verkkoon. /1/ IETF on määritellyt tekniikan dokumenteissa RFC 3947 ja RFC 3948.

3.8 IPSec yhteenveto

IPSeciä voidaan käyttää suojaamaan tiedonsiirto kahden verkkoaseman (host), kahden suojatun yhdyskäytävän (security gateway) tai verkkoaseman ja suojatun yhdyskäytävän välillä. Suojattu yhdyskäytävä tarkoittaa erillistä laitetta, joka toteuttaa IPSec protokollat esim. reititin, palomuuri tai palvelin, johon on asennettu IPSec-palvelut. /2/

IPSec-protokollaperhe pitää sisällään tekniikat VPN-yhteyden muodostamiseksi ja suojaamiseksi. Salattu tunneli voidaan tehdä kahden suojatun yhdyskäytävän välille tai jokaisen TCP-yhteyden välille, jotka muodostavat yhteyden tiettyyn palvelimeen. IPSeciä hallinoidessa täytyy päättää mitä palveluita käytetään milläkin yhdistelmällä ja mitä algoritmeja käytetään salaukseen. /6/

Huomioitavaa on se, että alun perin IETF:n IPSec standardissa ei oltu määritelty tapoja, kuinka tarkalleen pitäisi suojattu etäyhteys yksittäisille etätyöntekijöille muodostaa. Tästä johtuen eri VPN-palveluntarjoajilla onkin hyvin erilaisia tekniikoiden yhdistelmiä osapuolten ja tiedonsiirron varmennuksessa. Tämä taas aiheuttaa yhteensopimattomuutta eri palveluntarjoajien tuotteiden välillä. Tämä tarkoittaa, että heti yksityisverkkojen käyttöönottoa suunnitellessa, täytyy tarkkaan harkita, minkä yhtiön ohjelmia tai valmistajan laitteita hankitaan. Myöhemmin toisen valmistajan tuotteisiin siirtyminen voi merkitä hankintojen yhteensopimattomuutta keskenään. /2/

4 MICROSOFT VPN

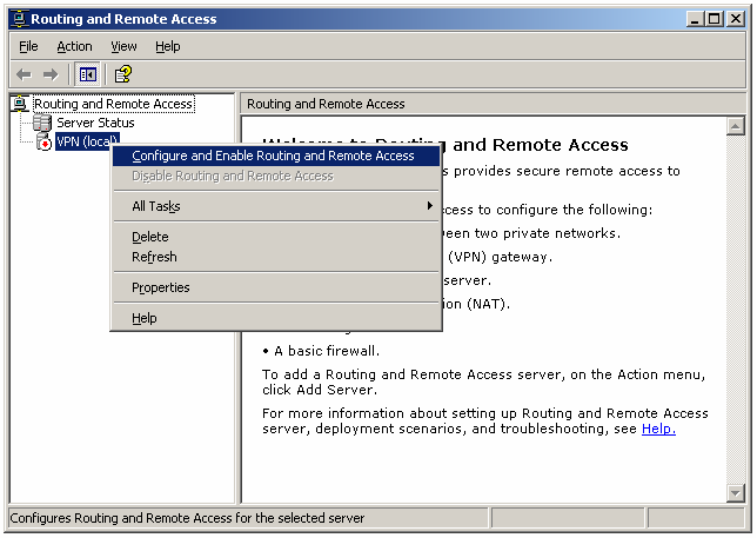
Microsoftin käyttöjärjestelmiin on sisällytetty toiminnallisuudet VPN-yhteyksille. Tekniikat joita Microsoft päättää liittää käyttöjärjestelmiinsä saavat hyvät lähtökohdat tekniikan nopealle käyttöönotolle. Microsoft on myös aktiivisesti ajanut omia tekniikoitansa IETF:n hyväksyttäväksi. /2/

Microsoftin käyttöjärjestelmissä Windows 2000, Windows XP, Windows Server 2003, Windows Vista ja Windows Server 2008 on sisällytettynä PPTP ja L2TP/IPSec -asiakasohjelmat (client). Tämän listäksi Windows Vista ja Windows Server 2008 sisältää Secure Socket Tunneling Protocol (SSTP) -tekniikkaan pohjautuvan asiakasohjelman. Microsoft on ottamassa uutta protokollaa käyttöön, koska vanhempien tekniikoiden kanssa on ongelmia palomuurien, NAT-verkkojen ja Internet-proxyjen kanssa. /22/ Yritysmaailmassa Vista ei saanut kovin hyvää vastaanottoa, joten uuden SSTP-tekniikan yleistyminen voi olla aikaisempiin Microsoftin VPN-tekniikoihin verrattuna hidasta.

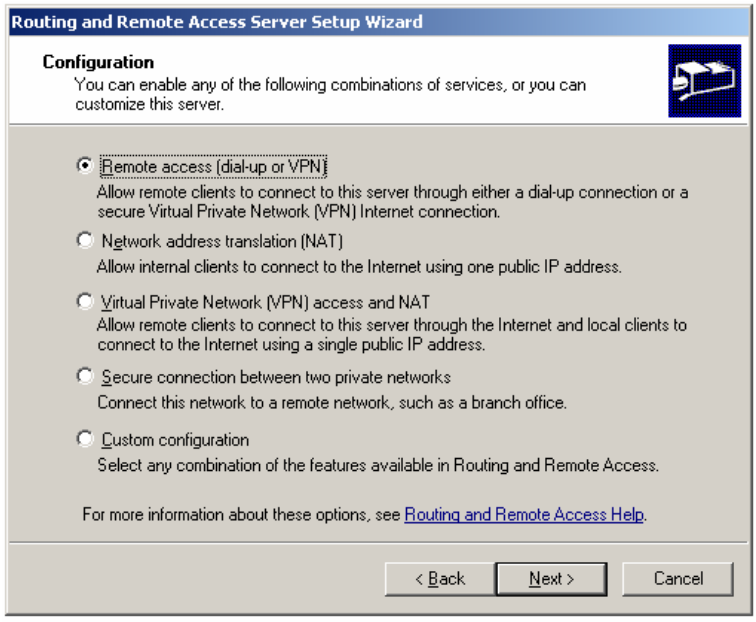
4.1 Microsoft VPN asennus Windows Server 2003 alustalle

Microsoftin VPN-palvelu on palvelinpohjainen ja toimii samoilla yleisillä periaatteilla kuten muutkin saman valmistajan pavelut. VPN-palvelun käyttöönotossa asennetaan ensin normaali Windows-palvelinkäyttöjärjestelmä PC-laitteistoon ja tämän jälkeen asennetaan käyttöjärjestelmään tarvitut palvelut ja konfiguroidaan ne tuotantoympäristöön sopiviksi. Seuraavat asennusohjeet ovat Windows 2003 Server -käyttöjärjestelmälle. Palvelin toimii eräänlaisena reitityspalvelimena, joten se tarvitsee kaksi erillistä verkkokorttia kumpaankin suuntaan: yksi sisäverkkoa ja yksi julkista verkkoa varten. /1/

Käyttöjärjestelmän asennuksen jälkeen”Administrator Tools” kansiosta avataan ”Routing and Remote Access” -konsolinäkymä. Vasemmalla puolella puurakenteesta löytyy VPN-palvelin. Alla olevassa kuvassa (kuva 4) tietokoneen nimi on ”VPN”. Valikko aukeaa oikealla hiiren napilla ja tästä valitaan ”Configure and Enable Routing and Remote Access”. /1/

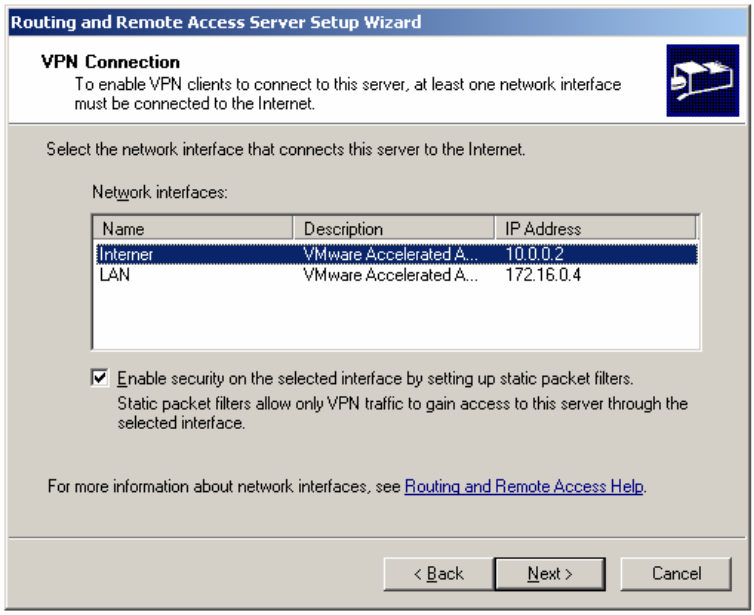


Kuva 4 Reitityksen ja etäyhteyksien konfigurointi



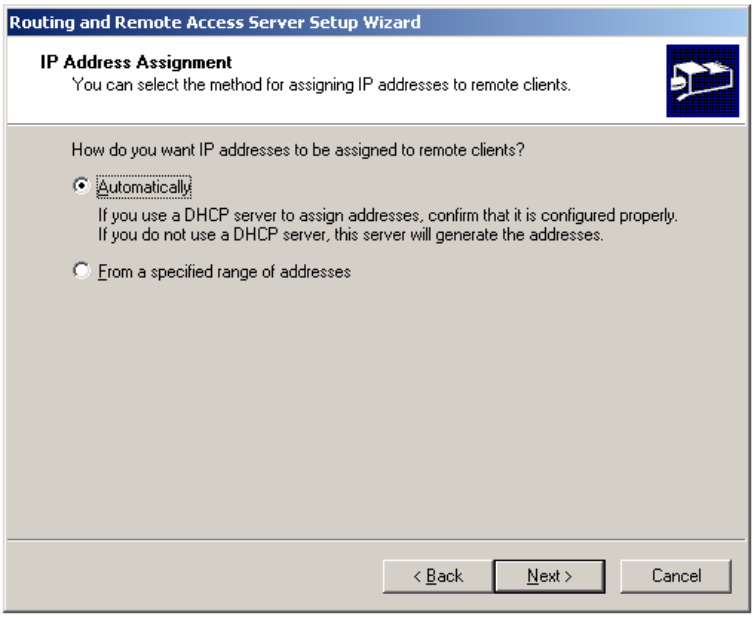
Kuva 5 Etäyhteyden konfiguroinnin valinta

Tämän jälkeen valitaan listasta lisättävän palvelun tyyppi eli tässä tapauksessa ”Remote access (dial-up or VPN)”, mikä nähdään yllä olevassa kuvassa (kuva 5). Etäyhteydeksi valitaan tämän jälkeen vielä ”VPN”. Seuraavaksi määritellään verkkoyhteys, johon palvelu halutaan lisätä. Tämä nähdään alla olevassa kuvassa (kuva 6), missä on valittuna julkisen verkon yhteys nimeltä ”Internet”. /1/



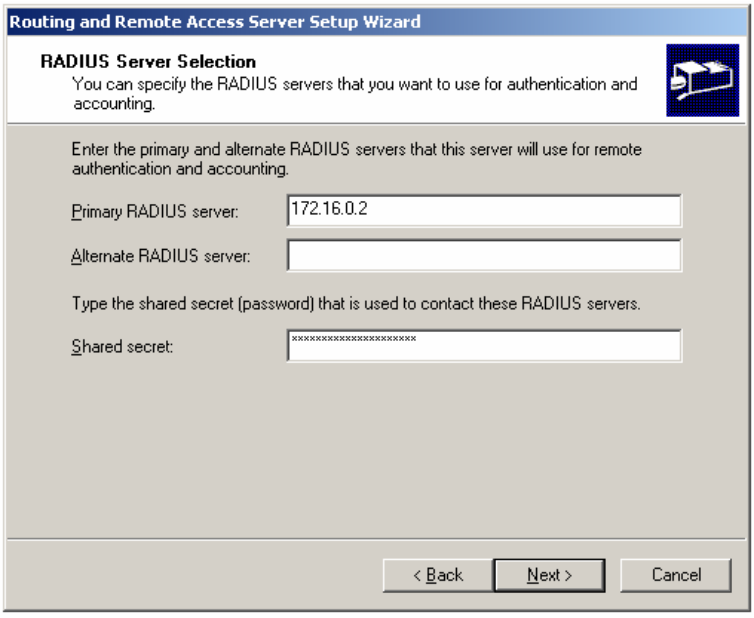
Kuva 6 Julkisen verkkoyhteyden valinta VPN-palvelulle

VPN-yhteyksille annettavat IP-osoitteet määritellään seuraavaksi. Alla olevassa kuvassa (kuva 7) on vaihtoehdoista valittuna ”Automatically”, jolla VPN-yhteyden muodostavat koneet saavan osoitteen verkon DHCP-palvelimelta ja tämän määritysten mukaisesti. Toisena mahdollisuutena on käyttää VPN-yhteyksille pienempää IP-osoiteavaruutta, mikä on rajattu pois normaalista DHCP:n käyttämästä osoiteavaruudesta. Tällöin organisaation verkossa olevista koneista erottaisi suoraan koneet, jotka ovat verkossa VPN-yhteydellä IP-osoitteen perusteella. /1/



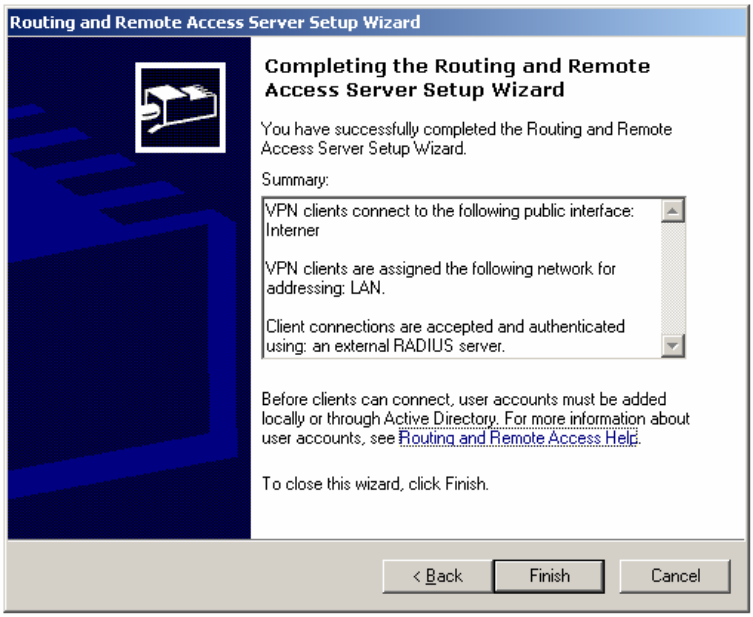
Kuva 7 VPN-yhteyksille annettavien IP-osoitteiden määritys

Tämän jälkeen valitaan käytetty RADIUS-palvelin. Erillinen RADIUS-palvelin autentikointia varten on suositeltavaa. /1/



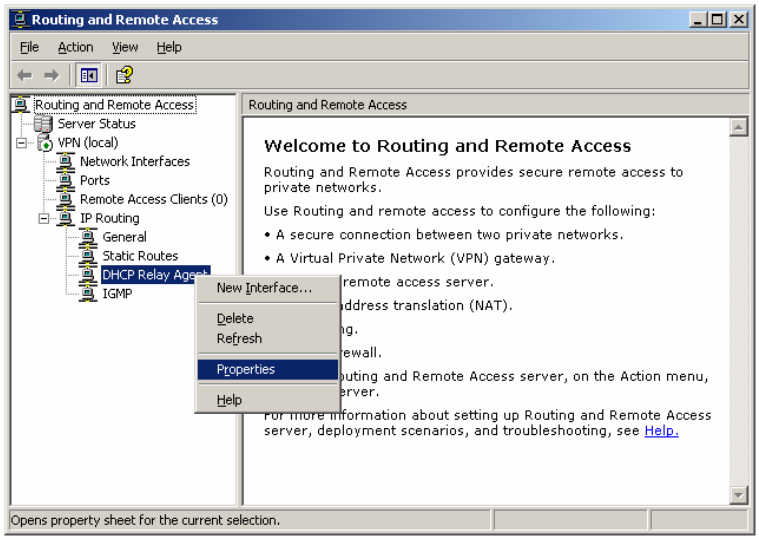
Kuva 8 RADIUS-palvelimen määritys

Yllä olevassa kuvassa (kuva 8) konfiguroidaan VPN-palvelimelle RADIUS-palvelimen IP-osoite ja annetaan Shared Secret, mikä on määritelty alun perin RADIUS-palvelimella. Tämä toimii salausavaimena palvelimia yhteenliitettäessä.



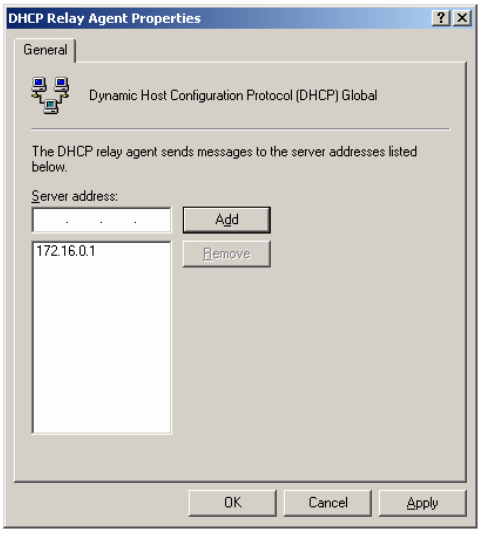
Kuva 9 VPN-palvelun asetusten yhteenveto

Yhteenvedossa (kuva 9) nähdään vielä, mitä valintoja on tullut tehtyä. Jos kaikki valinnat ovat olleet suunniteltuja, niin ”Finish”-napilla saadaan tehdyt muutokset käyttöön.



Kuva 10 DHCP Relay Agentin ominaisuudet

Palveluiden asennuksen jälkeen määritellään ”DHCP Relay Agent”-asetukset. Ikkuna saadaan auki valitsemalla ”Properties” oikean hiiren napin painalluksella avautuvasta valikosta (kuva 10). Asetusikkunaan lisätään periaatteessa vain DHCP-palvelimen IP-osoite, jotta VPN-palvelu tietää mistä IP-osoitteita pitää pyytää asiakaskoneille, kun ne muodostavat VPN-yhteyttä. Alla olevassa esimerkissä (kuva 11) on asetuksiin lisätty testiverkossa käytetty DHCP-palvelimen osoite 172.16.0.1. Testiverkossa sama palvelin toimi myös Domain Controllerina (DC). /1/



Kuva 11 DCHP Relay Agentin asetuksena DHCP-palvelin

Jokainen nykyinen Microsoftin käyttöjärjestelmä pitää sisällään VPN-asiakasohjelman, joka on yhteensopiva yrityksen nykyisten VPN-tuotteiden kanssa. /1/ Tämä tekee Microsoftin tekniikoiden käyttöönoton muita kilpailevia tuotteita helpommaksi, koska erillisiä ohjelmien valintoja ja asennuksia ei tarvitse tehdä.

4.2 Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) on määritelty dokumentissa RFC2637. Se ei ole IETF:n standardi. PPTP on myös jo vanhentunut tekniikka, mutta sillä on vielä paljon käyttäjiä /2/. PPTP käyttää Generic Routing Encapsulation (GRE) -protokollaa datan kapseloinnissa ja TCP-yhteyttä portiin 1723 tunneloinnin ylläpidossa. Microsoft sisällytti PPTP-tekniikan jo Windows NT 4.0 käyttöjärjestelmään ja oli ensimmäinen tekniikan käyttöönotossa. /1/

Jos organisaatiolla on käytössä Microsoftin palvelimista rakentuva sisäverkko, PPTP/GRE on helppo ottaa käyttöön, sillä se ei tarvitse Microsoftin palvelimien ja asiakaskoneiden lisäksi muita ohjelmistoja. /1/

Käyttöönoton helppouden vastapainona, PPTP-tekniikalla voi tulla ongelmia palomuurien, NAT-verkkojen ja välityspalvelinten kanssa. Palomuureihin joutuu erikseen sallimaan PPTP-yhteyksien pääsy läpi. GRE on standardi tapa kapseloita IP-paketit, mutta osa Internet-palveluntarjoajista estää silti protokollan kulun. Hotelleissa on usein sallittu vain sähköposti ja Internet-selaus tietoliikenteenä ja normaali NAT-verkko ei saa reititettyä GRE-paketteja. Etätyöntekijän kannalta suojatun yhteyden muodostuminen ei ole itsestään selvää. /22/

4.3 Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) on PPTP-protokollan jatke, jolla Internet-palveluntarjoaja voi mahdollistaa VPN-yhteyden Internetin ylitse. L2TP on yhdistelmä Ciscon L2F ja Microsoftin PPTP-protokollia. /20/ L2TP:llä luodaan autentikoimaton toisen OSI-kerroksen eli verkkokerroksen yhteys. Microsoftin käyttöjärjestelmät ovat Windows 2000 lähtien sisältäneet tarvittavat komponentit

yhteyden muodostamiseen. Microsoft käyttää protokollastaan nimitystä L2TP/IPSec, sillä salauksessa käytetään IPSec-protokollia. /4/ L2TP vastaa toiminnoiltaan suurimmaksi osaksi PPTP:tä. L2TP:n tunnelointi kapseloi IP-datapaketit UDP-paketin sisään. L2TP tarvitsee tunnelipalvelimen, jota kutsutaan LAC:ksi (Local Area Concentrator). Tämän kautta voidaan yhteys muodostaa yrityksen verkossa olevaan Secure Remote Access (RAS) -palvelimeen. LAC-palvelin sijaitsee yleensä organisaation sivukonttorin verkossa tai Internet-palveluntarjoajan hallusta. /20/

L2TP/IPSec-tekniikka käyttää salausavainten vaihdossa IKE-protokollaa ja tiedon kapseloinnissa ESP-protokollaa. Näiden takia L2TP/IPSec-tekniikalla on myös ongelmia palomuurien, NAT-verkkojen ja välipalvelimien kanssa. IPSeciin lisätyn NAT-T-protokollan ansiosta, voidaan yhteys muodostaa NAT-verkkojen läpi, jos niin lähettäjä kuin vastaanottajakin tukevat tekniikkaa.

Tekniikkana L2TP on ongelmallinen hyödyntää etätyönteon suojana, tekniikan tarvitseman LAC-palvelimen johdosta. Tekniikkaan on myös arvosteltu hitaaksi suhteessa muihin vaihtoehtoihin /22/.

4.4 Secure Socket Tunneling Protocol (SSTP)

Secure Socket Tunneling Protocol (SSTP) -tekniikalla muodostetaan päästä päähän -mallinen VPN-yhteys. Tekniikka perustuu SSL-protokollaan, joka on hyvin yleinen Internetissä. SSL-tekniikkaa käytetään verkkoselain pohjaisissa salatuissa yhteyksissä, kuten esim. pankkiyhteyksissä ja verkkokaupoissa. /22/

4.5 Microsoftin VPN-tuotteiden yhteenveto

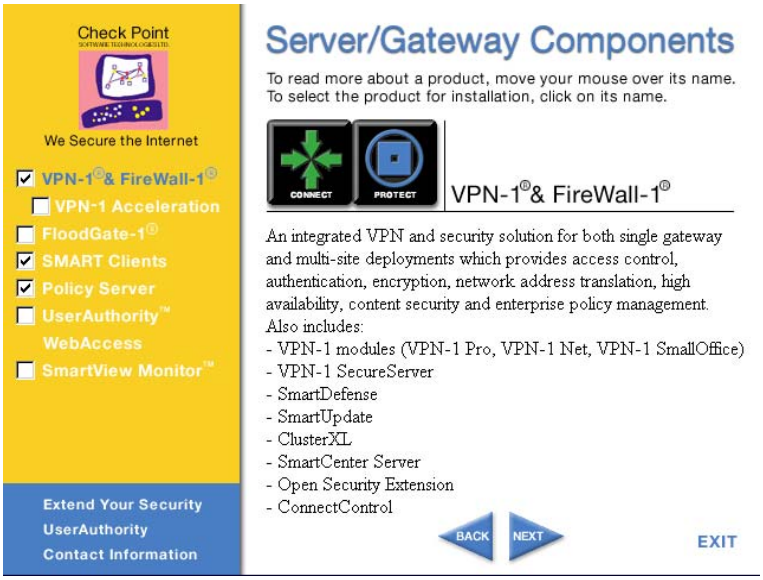
PPTP on jo vanha VPN tekniikka, mutta silti vielä laajasti käytössä organisaatioissa, missä ei ole haluttu ottaa käyttöön eri palveluntarjoajan tuotteita. Microsoftin Active Domain (AD) -ympäristöön Microsoftin oma VPN-palvelinpohjainen palvelu sopii hyvin. Tampereen teknisessä yliopistossa (TTY) käytetään etäyhteyksien suojana PPTP/GRE-protokollien yhdistelmää.

Kumpikaan Microsoftin tuotteista ei ole puhdas IPSec-tekniikkaan perustuva ratkaisu. L2TP-tunnelointi käyttää IPSecin salausta suojatakseen, mutta tunnelointi tehdään OSI-mallin toisella kerroksella keskittimen avulla. PPTP/GRE-tekniikka taas on vanhempaa perua ja on periaatteessa IPSecin kannalta kilpaileva yhdistelmä protokollia. /1/

5 CHECK POINT VPN

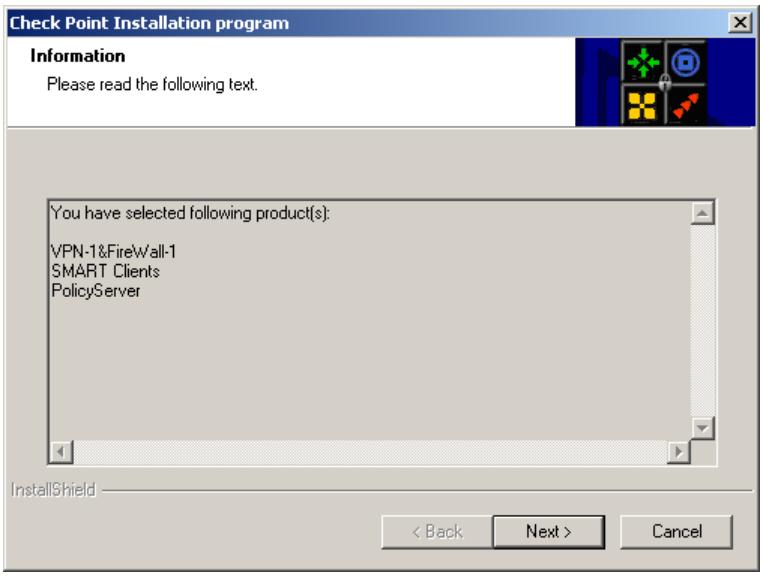
Palomuuripohjaiset VPN-ratkaisut, kuten Check Pointin NGX VPN-1/Firewall-1 voivat olla hyviä ratkaisuja yrityksen etäkäytön suojaamiseksi, sillä palomuurit toteuttavat jo normaalissa toiminnassaan samoja tehtäviä, joita VPN-yhteyksissä tarvitaan. Näitä ovat esim. autentikointi ja osoitteiden reititys. Jos käytössä oleva palomuuri pystyy VPN-palvelun toteuttamiseen, niin sen konfigurointi on mahdollisesti jonkin verran yksinkertaisempaa verrattuna uuden palvelimen asennukseen. Verkkoon ei tarvitse myöskään lisätä muita laitteita. /1/

On suositeltavaa käyttää Check Pointin tarjoamaa UNIX-käyttöjärjestelmää palvelimen alustaksi, mutta tätä tutkintotyötä varten asennus tehtiinWindows 2000 Pro -käyttöjärjestelmän päälle, koska tämä oli suoraviivaisempaa. Ohjelmiston käyttöliittymän toimintaan ei tällä ole merkitystä.

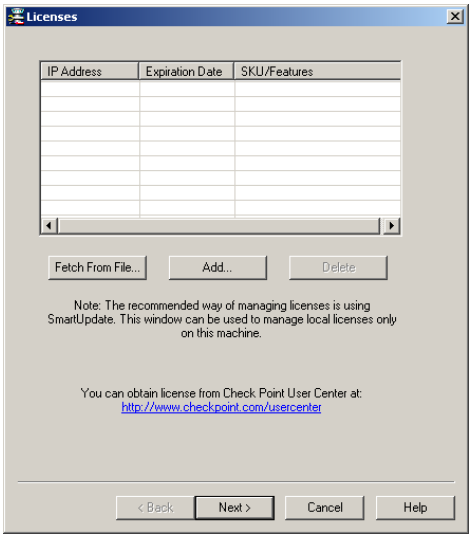


Kuva 12 Check Point VPN:n asennus

Ohjelmisto asennettiin oletusasetuksilla. Tällöin palvelimelle asentuu VPN-palvelut, asiakasohjelmien hallintaa helpottavat työkalut ja policy-palvelin. /3/ Tietoturvan kannalta olisi parempi jakaa palveluita useammalle koneelle, mutta tarkastelussa asennettiin yllä mainitut palvelut kaikki samalle koneelle (kuva 12 ja kuva 13).

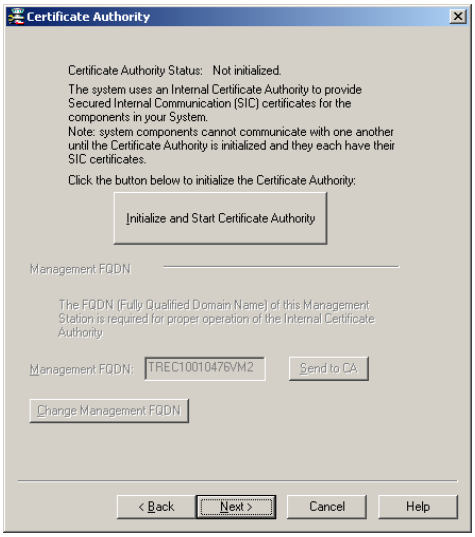


Kuva 13 Check Point VPN:n asennukseen valittujen työkalujen yhteenveto



Kuva 14 Check Point lisenssien käyttöönotto

Asennuksen yhteydessä kysytään lisenssitietoja (kuva 14), mutta ne voi antaa ohjelmistolle myöhemminkin. Asennusvaiheessa kysytään myös sertifikaattipalvelimen tietoja (kuva 15). Tämän jälkeen työkalujen asennus on valmis.



Kuva 15 Check Point sertifikaattipalvelimen määritys

Check Pointilla on kaksi VPN-asiakasohjelmaa: SecuRemote ja SecureClient. SecuRemote on yksinkertaisempi versio näistä kahdesta ja sillä saadaan toteutettua normaalit VPN-asiakasohjelman toiminnot. SecureClient on monipuolisempi siinä mielessä, että sillä voidaan hallinnoida yrityksen työntekijöiden käyttämiä koneita paremmin ja luoda niihin sääntöjä samankaltaisesti, kuten Microsoftin domainin säännöstöillä Active Directorystä (AD). /3/

Vanhemmalla NG-version palomuuriohjelmistolla ja asiakasohjelmalla ei onnistu esim. NAT-T-standardin käyttö, joten lisenssi täytyy hankkia uudemmalle NGX-ohjelmistolle, jos halutaan suojatun yhteyden toimivan yksityisten IP-osoitteiden kanssa. /3/

Kuten muidenkin eri valmistajien tuotteiden kanssa, yhteensopivuus ei ole taattua muiden vastaavien tuotteiden kanssa. Täytyy siis tarkaan miettiä käyttöönoton ja ylläpidon kustannuksia laitehankintojen lisäksi. Myöhemmin toiseen tuotteeseen siirtyminen voi olla kallista. /2/

7 YHTEENVETO

Microsoftin tuotteista vanhemmat PPTP/GRE ja L2TP/Ipsec eivät ole välttämättä parhaita vaihtoehtoja. Kummallakin on ongelmia palomuurien, NAT-verkkojen ja välityspalvelimien kanssa. Windows Vista ja Windows 2008 Server -käyttöjärjestelmissä mukana tulevaan SSTP-tekniikkaan ei kannata välttämättä vielä paneutua, koska siitä ei ole vielä paljoa kokemuksia. Tulevaisuudessa siitä voi kuitenkin tulla nykyisten VPN-tekniikoiden korvaaja, sillä sen luvataan poistavan VPN-yhteyksiin liittyviä ongelmia, kuten toimimattomat yhteydet NAT-verkkojen ja palomuurien läpi. /22/

CheckPoint FireWall-1/VPN-1 on tuotteena monipuolinen ja perustuu hyväksi havaittuun IPSec-protokollaperheeseen. IPSecin heikkoutena on sen vahvuudet eli monipuolisuus ja modulaarisuus. Nämä ominaisuudet tuovat mukanaan monimutkasuutta ja useita tapoja tuottaa sama palvelu. Check Pointin tuotteista vasta uudemmassa NGX-versiossa on käytössä NAT-T-tekniikka, jolla saadaan suojattu yhteys toimimaan myös NAT-verkoissa /2/.

VPN-yhteyksiin liittyvät salausalgoritmien laskennat kuormittavat palvelinta varsinkin isoilla käyttäjämäärillä, joten kuormaa ei kannata välttämättä lisätä palomuuritoimintoja tekevälle palvelimelle. Tämä voi päivän ruuhkaisimpina aikoina aiheuttaa ongelmia verkkoliikenteessä.

Etätyön kannalta CheckPoint FireWall-1/VPN-1 NGX on parempi vaihtoehto verrattuna Microsoftin PPTP ja L2TP-tekniikoihin. Vanhemman NG-version kanssa kohdataan NAT-verkkojen kanssa samoja ongelmia kuin Microsoftin tuotteilla.

Erillisiä pienille yrityksille suunnattuja VPN-laiteratkaisuja ei tähän tutkintotyöhön sisällytetty, sillä näistä tulee uusia versioita jatkuvasti. Pienemmän mittakaavan VPN-palveluun nämä valmiit tietoliikennelaitteet ovat hyviä vaihtoehtoja. Kyseisiä tuotteita myyviltä yrityksiltä saa laitteita testaukseen, joten hankinnoissa pystyy testauksella varmistamaan tuotteen sopivuuden ympäristöön.

Ennen VPN-palvelun käyttöönottoa on syytä tarkkaan suunnitella tarvitut verkon arkkitehtuurilliset muutokset ja se, että kuinka laajasti palvelu otetaan käyttöön. Nykyaikaisten vahvojen salakirjoitustekniikoiden takia on syytä myös miettiä minkälaisella laitetteella VPN-palvelua pidetään. Isommille organisaatioille kattava palvelinpohjainen VPN-palvelu on suositeltavaa. Palvelun lisääminen pääreittimeen tai palomuuriin voi vaikuttaa laitteiden normaalin palvelun tasoon myös myöhemmin VPN-liikenteen kasvaessa.

LÄHDELUETTELO

Kirjat

1 Davies, J. ja Lewis, E., Deploying Virtual Private Networks with Windows Server 2003. Microsoft Press. Redmond, Washington 2003. 496 s.

2 Perlmutter, Bruce ja Zarkower, Jonathan, kääntäjä: Timo Kokkonen, Virtuaaliset yksityisverkot. Edita Oyj, IT Press, Helsinki 2001. 270 s.

3 Stephens, Robert, Stefel, Barry J. ja Watkins, Stephen, Configuring Check Point NGX VPN-1 / FireWall-1. Syngress Publishing, Inc., Rockland 2005. 625 s.

IETF:n Internet-luonnokset:

4 Adoba, B., W. Dixon, G. Zorn ja S. Booth, RFC 3193 - Securing L2TP using IPsec. [Internet-luonnos, www-sivu]. The Internet Society, Network Working Group. Marraskuu 2001. [viitattu 25.11.2005] Saatavissa: http://rfc.net/rfc3193.html

5 Harkins, D ja D. Carrel, RFC 2409 - The Internet Key Exchange (IKE). [Internet-luonnos, www-sivu]. The Internet Society, Network Working Group. Marraskuu 1998. [viitattu 14.12.2005] Saatavissa: http://rfc.net/rfc2409.html

6 Kent, S. ja R. Atkinson, RFC 2401 - Security Architecture for the Internet Protocol. [Internet-luonnos, www-sivu]. The Internet Society, Network Working Group. Marraskuu 1998. [viitattu 25.11.2005] Saatavissa: http://rfc.net/rfc2401.html

7 Kent, S. ja R. Atkinson, RFC 2406 - IP Encapsulating Security Payload (ESP). [Internet-luonnos, www-sivu]. The Internet Society, Network Working Group. Marraskuu 1998. [viitattu 25.11.2005] Saatavissa: http://rfc.net/rfc2406.html (25.11.2005)

8 Kent, S., RFC 4302 - IP Authentication Header. Internet-luonnos, [www-sivu]. The Internet Society, Network Working Group. Joulukuu 2005. [viitattu 11.1.2006] Saatavissa: http://rfc.net/rfc4302.html

9 Kent, S., RFC 4303 - IP Encapsulating Security Payload (ESP). [Internet-luonnos, www-sivu]. The Internet Society, Network Working Group. Joulukuu 2005. [viitattu 11.1.2006] Saatavissa: http://rfc.net/rfc4303.html

10 Mannie E., RFC 3945 - Generalized Multi-Protocol Label Switching (GMPLS) Architecture. [Internet-luonnos, www-sivu]. The Internet Society, Network Working Group. Lokakuu 2004. [viitattu 14.12.2005] Saatavissa: http://rfc.net/rfc3945.html

11 Rosen, E. ja Y. Rekhter, RFC 2547 - BGP/MPLS VPNs. [Internet-luonnos, www-sivu]. The Internet Society, Network Working Group. Maaliskuu 1999. [viitattu 12.12.2005] Saatavissa: http://rfc.net/rfc2547.html

12 Patel, B., B. Aboba, S. Kelly ja V. Gupta, RFC 3456 - Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPSec Tunnel Mode. [Internet-luonnos, www-sivu]. The Internet Society, Network Working Group. Tammikuu 2003.[viitattu 27.12.2005] Saatavissa: http://rfc.net/rfc3456.html

13 Rosen, E., A. Viswanathan ja R. Callon, RFC 3031 - Multiprotocol Label Switching Architecture. [Internet-luonnos, www-sivu]. The Internet Society, Network Working Group. Tammikuu 2001. [viitattu 15.12.2005] Saatavissa: http://rfc.net/rfc3031.html

14 Taarud, J., Verthein, W., Pall, G., Hamzeh, K., Little, W., Zorn, G., RFC 2637 - Point-to-Point Tunneling Protocol (PPTP). [Internet-luonnos, www-sivu]. The Internet Society, Network Working Group. Heinäkuu 1999. [viitattu: 6.6.2008] Saatavissa: http://rfc.net/rfc2637.html

Internet sivut:

15 Cisco Systems. [www-sivu] Managed VPN - Comparison of MPLS, IPSec, and SSL Architectures [viitattu: 25.11.2005] Cisco Ltd., Saatavissa: http://www.cisco.com/en/US/netsol/ns341/ns121/ns193/networking_solutions_white_paper0900aecd801b1b0f.shtml

16 Steve Friedl's Unixwiz.net Tech Tips. [www-sivu] An Illustrated Guide to Ipsec. [viitattu: 25.11.2005] Saatavissa: http://www.unixwiz.net/techtips/iguide-ipsec.html

17 Symantec Co. [www-sivu] Symantecin VPN-opas. [viitattu 15.1.2006] Saatavissa: http://www.symantec.com/region/fi/resources/vpn.html

18 TimeStep Corporation. Joulukuu 1998. Understanding the IPSec protocol suite [viitattu:20.1.2006] Saatavissa: http://www.adimpleo.com/library/timestep/ipsecv2-Dec98.pdf

19 Wu, T., Riverstone Networks. [www-sivu]. MPLS VPNs - Layer 2 or Layer 3? [viitattu: 20.1.2006] Saatavissa: http://www.riverstonenet.com/pdf/mpls_vpns_layer2_or_layer3.pdf

20 TechTarget Networking Media. [www-sivu] Layer Two Tunneling Protocol [viitattu: 2.6.2008] Saatavissa: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci493383,00.html

21 International Organization for Standardization [www.sivu] Publicly Available Standards. [viitattu: 3.6.2008] Saatavissa: http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip

22 Microsoft Co. [www-sivu] The Cable Guy – The Secure Socket Tunneling Protocol. Microsoft TechNet [viitattu 6.6.2008] Saatavissa: http://technet.microsoft.com/en-us/magazine/cc162322.aspx