STADIA
HELSINGIN AMMATTIKORKEAKOULU

TEKNIIKAN JA LIIKENTEEN TOIMIALA

Tietotekniikka

Tietoliikennetekniikka

INSINÖÖRITYÖ

VPN-RATKAISUJEN VERTAILU

Työn tekijä: Tuomas Torro
Työn valvoja: Seppo Lehtimäki
Työn ohjaaja: Jani Koivisto

Työ hyväksytty: __. __. 2007

Seppo Lehtimäki
lehtori

ALKULAUSE

Tämä insinöörityö tehtiin WM-Data Oy:lle kesällä 2007. Haluan kiittää WM-Datan tietoliikenneasiantuntijoita ammattimaisesta tuesta työn parissa. Erityiskiitoksen on ansainnut insinöörityöni ohjaaja tietoliikenneasiantuntija Jani Koivisto, jonka tuella insinöörityön konfiguraatio- ja testausosuus oli mahdollista suorittaa. Kiitokset lehtori Seppo Lehtimäelle opastuksesta teoriaosuudessa. Haluan kiittää myös avovaimoani Sannaa, joka on kannustanut minua eteenpäin työssäni sitkeästi.

Helsingissä 16.9.2007

Tuomas Torro

STADIA
HELSINGIN AMMATTIKORKEAKOULU

INSINÖÖRITYÖN TIIVISTELMÄ

Tekijä: Tuomas Torro

Työn nimi: VPN-ratkaisujen vertailu

Päivämäärä: 16.9.2007 Sivumäärä: 37

Koulutusohjelma: Tietotekniikka Suuntautumisvaihtoehto: Tietoliikennetekniikka

Työn valvoja: Seppo Lehtimäki

Työn ohjaaja: Jani Koivisto

Tietoverkkojen käyttö lisääntyy maailmalla nopeaa vauhtia. Monet verkon käyttäjät tarvitsevat käyttöönsä myös yrityksen yksityisiä tietoja missä tahansa liikkuvatkin. Samalla on oltava mahdollista yhdistää yrityksen eri toimipisteitä samaan verkkoon. Virtuaaliset yksityisverkot eli VPN:t ovat nopea ja turvallinen vaihtoehto näihin tarpeisiin.

VPN saattaa tuottaa yritykselle suuria liiketoiminnalisia hyötyjä. VPN-ammattilaisten suunnittelema VPN:ää voidaan pitää myös turvallisena ratkaisuna yritykselle. Varsinkin IPSecin (Internet Protocol Security) kehittyminen luotetuksi standardoiduksi protokollaperheeksi on lujittanut uskoa VPN:iin.

Tässä insinöörityössä vertaillaan kahden suositun VPN-laitevalmistajan laitteistoa teknisten ominaisuuksien, hallittavuuden ja client-ratkaisujen pohjalta. Työn teoriaosuudessa keskitytään VPN:ien rakenteeseen ja VPN-laitteistojen käyttämiin tekniikoihin. Insinöörityön pohjalta on mahdollista saada kokonaiskuva VPN-tekniikasta ja tutustua VPN-reitittimien konfigurointiin.

Avainsanat: VPN, IP, IPSec, L2TP, PPTP

STADIA
HELSINGIN AMMATTIKORKEAKOULU

ABSTRACT

Name: Tuomas Torro

Title: VPN Solutions

Date: 16.9.2007 Number of pages: 37

Department: Information Technology Study Programme: Telecommunications

Instructor: Seppo Lehtimäki, MEng, Lecturer

Supervisor: Jani Koivisto, IT Expert

The purpose of this graduate study was to compare the VPN equipment produced by two notable manufacturers. The focus was on technical features, management and client solutions. The graduate project was assigned by the company WM-Data Ltd.

The global use of Internet has been increasing dramatically. In organizations and enterprises, it is vital for mobile staff to have remote access to their organization's or company's internal data in the company's private network. It is also important to be able to connect the company's offices into the same network. The Virtual Private Network (VPN) provides a suitable solution for these purposes.

The graduate project concentrated on the structure of the VPN and on the protocols behind them. The study focused on the VPN equipment made by two manufacturers. The technical features, management and client solutions of the VPN equipment were compared. Special attention was paid to VPN security.

As a result, the graduate study produced an overall description of VPN technologies. With the highly developed IPSec (Internet Protocol Security) in particular, VPNs offer a suitable and secure remote access solution.

Keywords: VPN, IP, IPSec, L2TP, PPTP

SISÄLLYS

LYHENTEITÄ JA MÄÄRITELMIÄ

3DES	*Triple DES*. DES-algoritmin versio, jonka salauksen vahvuus on kaksi tai kolme kertaa niin vahva kuin DES.
AES	*Advanced Encryption Standard*. Symmetrinen salausalgoritmi, jonka avaimen pituus on 128 - 256 bittiä.
AH	*Authenticating Headers*. IPSecin käyttämä todennusotsikko.
DES	*Data Encryption Standard*. Symmetrinen salausalgoritmi, jonka avaimen pituus on 64 bittiä.
DHCP	*Dynamic Host Configuration Protocol.* Verkkoprotokolla, jonka yleisin tehtävä on jakaa IP-osoitteita.
ESP	*Encapsulating Security Protocol*. IPSecin salausprotokolla.
HMAC	*Keyed-Hash Message Authentication Code*. Todennuksessa käytettävä tarkistussumma, joka käyttää tiivistefunktiota.
IETF	*Internet Engineering Task Force*. Internetin vapaaehtoinen kehittämistyöryhmä.
IKE	*Internet Key Exchange*. Avaintenhallintaprotokolla.
IP	*Internet Protocol*. TCP/IP:n standardiprotokolla.
IPSec	*Internet Protocol Security*. VPN:n yleisin salaustekniikka.
L2F	*Layer 2 Forwarding*. Ciscon kehittämä tunnelointiprotokolla.
L2TP	*Layer 2 Tunneling Protocol*. Microsoftin ja Ciscon kehittämä tunnelointiprotokolla.
MAC	*Message Authentication Code*. Todennuksessa käytettävä tarkistussumma.
MD5	*Message Digest 5*. Tiivistefunktio.
OSI-malli	*Open Systems Interconnection Reference Model.* Tiedonsiirtoprotokollien yhdistelmä seitsemässä kerroksessa.

PPP	*Point-to-Point Protocol.* Protokolla, jolla luodaan suora yhteys verkon laitteiden välille
PPTP	*Point-to-Point Tunneling Protocol*. Microsoftin kehittämä tunnelointi-protokolla.
RSA	Epäsymmetrinen julkisen avaimen salausalgoritmi.
SA	*Security Association*. IPSecin turvayhteys.
SHA-1	*Secure Hash Algorithm 1*. IPSecin käyttämä tiivistefunktio.
SPI	*Security Parameters Index*. Yksilöi IPSecin turvayhteydet.
UDP	*User Datagram Protocol.* Yhteyskäytäntö, jolla sovellus voi lähettää viestejä toiselle tietokoneelle.
VPN	*Virtual Private Network*. Virtuaalinen yksityisverkko.

1 JOHDANTO

Tulevaisuudessa tarve verkon käyttöön mistä tahansa lisääntyy nopeasti. Monille verkon käyttäjille ei enää riitä, että mistä tahansa pääsee vain Internetiin, vaan on päästävä käsiksi yrityksen palvelimiin ja tiedostoihin. Samalla on oltava mahdollista yhdistää yrityksen eri toimipisteiden verkkoja yhdeksi verkoksi. Kun yritykset ulkoistavat nykyisin paljon toimintojaan ja liiketoiminnot muuttuvat nopeaa tahtia, on löydettävä ratkaisu, joka yhdistää verkkoja ilman suuria muutoksia infrastruktuuriin. Virtuaaliset yksityisverkot eli VPN:t tarjoavat näihin tarpeisiin nopean ja turvallisen vaihtoehdon. VPN:ien siirtotienä toimivan Internetin laaja leviäminen onkin vauhdittanut VPN:ien yleistymistä paljon viime vuosina. Euroopassa VPN:t ovat syrjäyttäneet jo Frame Relay -tekniikan ja Yhdysvalloissakin VPN:t ovat nousseet Frame Relay -tekniikan rinnalle.

VPN on monimutkainen käsite ja sen määrittely yhdellä lauseella on mahdotonta. Jotta VPN:iä oppii ymmärtämään, on niiden laitteistojen parissa työskenneltävä myös fyysisesti. Laitteiston konfigurointi ja vianetsintä opettavat paljon verkon rakenteesta ja kertovat myös, mitä protokollia ja salausmenetelmiä on tunnettava. Tärkeää on myös pysyä mukana kehityksessä. Kun tietokoneiden laskutehot kehittyvät, vaaditaan myös vahvempia salausmenetelmiä.

VPN:ien suurin haaste tulevaisuudessa onkin säilyttää tiedonsiirron turvallisuus. Kun käytössä on julkinen verkko, niin yrityksen kaikella materiaalilla on mahdollisuus joutua vääriin käsiin. Samalla, kun salaustekniikoita ja protokollia on kehitettävä, on pidettävä huoli, että käytössä on tarpeeksi yleiset standardit. Muuten ongelmaksi voi koitua eri palveluntarjoajien välisten yhteyksien yhteensopimattomuus. Tämän vuoksi tässä työssä keskitytäänkin paljon salaustekniikoihin, avaintenhallintaan ja käyttäjien todennukseen. VPN-hallinnoijan on tunnettava nämä tekniikat voidakseen suunnitella ja toteuttaa VPN:t siten, että käyttäjien arkaluontoiset tiedot eivät joudu vääriin käsiin.

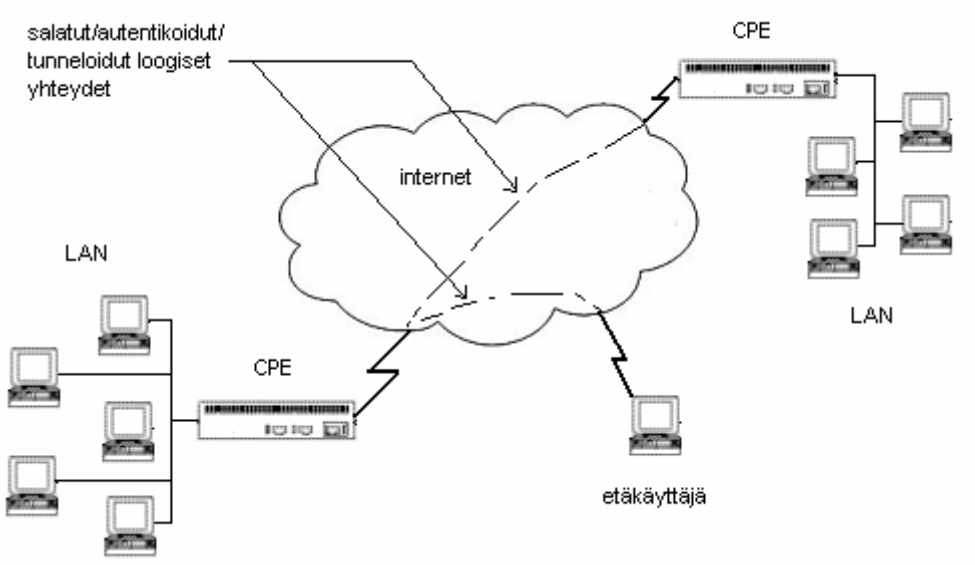
Tässä insinöörityössä vertaillaan kahden suositun VPN-laitevalmistajan laitteistoa teknisten ominaisuuksien, hallittavuuden ja client-ratkaisujen

pohjalta. Työn teoriaosuudessa keskitytään VPN:ien rakenteeseen ja VPN-laitteistojen käyttämiin tekniikoihin.

2 VPN-VIRTUAALIVERKOT

Virtuaaliset yksityisverkot (Virtual Private Networks, VPN) voidaan määritellä siten, että ne yhdistävät yrityksen verkkoja turvallisesti julkisen verkon yli. Näin erilliset verkot muodostavat näennäisesti yksityisen verkon. VPN:n avulla voidaan myös yhdistää yksittäinen etäkäyttäjä yrityksen verkkoon. VPN:n turvallisuudella tarkoitetaan sitä, että tieto liikkuu julkisen verkon läpi muuttumattona, käyttäjät tunnistetaan ja heidän käyttöoikeuksiaan hallitaan. [3.]

Etäkäyttäjät ja yrityksen erilliset sisäverkot muodostavat virtuaalisen yksityisverkon Internetin yli (kuva 1). Julkista infrastruktuuria käsitellään tässä tapauksessa internetinä, vaikka teknisesti internet on vain osa julkisesta infrastruktuurista. Internetin yli tehdään myös tunnelointi. Tunneloinnissa tehdään datan paketointi siten, että se kulkee päätepisteiden välin suojattuna ”tunnelissa”. Lähiverkkojen välisissä yhteyksissä nuo päätepisteet ovat usein asiakaspään laitteistoissa (Customer Premises Equipment, CPE), joita käsitellään tarkemmin luvussa 6. [1.]



Kuva 1. Internetin välityksellä toimiva VPN [1]

VPN:ien suuri suosio perustuu nykyisin suurilta osin liiketoiminnallisiin tosiseikkoihin. Nämä seikat koostuvat tietenkin monista tekijöistä. VPN:ien hyödyistä tässä tarkastellaan turvallisuutta, selkeyttä käyttäjälle, edullisuutta ja hallittavuutta. Haitoista tarkastellaan käyttöönoton hankaluutta, vianetsinnän hankaluutta, luotettavuutta ja internetin saatavuutta. [2.]

Turvallisuus

VPN:n käyttö ei poista kaikkia uhkia, joita yritykset kohtaavat. Se voi kuitenkin vahvistaa tietotekniikkaan liittyvää turvallisuutta ja vähentää ulkopuolisia riskitekijöitä. VPN:ien huolellinen suunnittelu on avaintekijä riskien minimoinnissa. Suunnittelussa on tärkeää huomioida, että ratkaisua tarkastelee mahdollisimman moni ammattilainen, jotta mahdolliset toimintahäiriöt ja tietoturva-aukot voidaan havaita jo suunnitteluvaiheessa. VPN:ien monimutkaisuuden takia ratkaisujen suunnittelussa tarvitaan myös muita kuin pelkästään teknisiä asiantuntijoita. [2.]

Selkeys käyttäjälle

VPN:ien sijainti toisistaan erillään ei aiheuta ongelmaa käyttäjän kannalta. VPN:n käyttämiseen ei tarvita VPN:ien osaamista tai edes tietoa siitä, että käytössä on VPN. Tämä on yksi VPN:ien parhaista eduista.

Edullisuus

VPN käyttää yhteyksiinsä paikallista internet-yhteyttä. Tämä vähentää huomattavasti kustannuksia, koska verkkojen välille ei tarvitse rakentaa puhelinlinjoja.

Hallittavuus

VPN:ien hallittavuutta helpottaa se, että VPN ei näy käyttäjille, sovelluksille eikä isännille (host). Tästä syystä näitä ei myöskään tarvitse hallinnoida erikseen.

Käyttöönoton hankaluus

VPN:n käyttöönotto yrityksessä ei vaikuta isolta operaatiolta. Esim. laitteiston konfiguraatio, avaintenhallinnan suunnittelu ja vianetsintä saattavat kuitenkin kuluttaa paljon aikaa. Tämän vuoksi suunnittelussa tulisi käyttää VPN:ien ammattilaisia. Tällöin esim. lähiverkkojen välisen (lan-to-lan) VPN:n suunnitelu voi viedä pari viikkoa. On kuitenkin muistettava, että tällöin käytettävien verkkojen tarkat yksityiskohdat on oltava jo valmiiksi tiedossa.

Vianetsinnän hankaluus

Vianetsinnän hankaluus muodostuu siitä, että VPN:ssä data siirtyy salaamattomana yhdyskäytävään ja lähtee sieltä salattuna. Täten VPN-hallinnoijan on tunnettava käytettävä ohjelmisto tarkasti, jotta vianetsintä onnistuu. Hallinnoijan kannalta vaikeita ratkaistavia ovat avainten synkronoinnissa ja oikeuksien tarkistamisessa tapahtuvat ongelmatilanteet.

Luotettavuus

Lähiverkkojen välisissä VPN:issä nousee esiin kysymys siitä, voidaanko toiseen verkkoon luottaa täydellisesti. Jos hakkeri onnistuu pääsemään toiseen verkkoon, niin hän saattaa samalla saada yhteyden molempiin. Tämän vuoksi varsinkin lähiverkkojen välisiä VPN:iä luotaessa on varmistettava, että jokaisen verkon turvallisuus on kunnossa.

Internetin saatavuus

VPN-ratkaisulla voi olla merkittäviä hyötyjä liiketoiminnalle, mutta sekään ei voi varmistaa 100-prosenttista saatavuutta. VPN käyttää siirtotienään Internetiä, jonka takia VPN-palvelu saattaa katketa etä- ja lähiverkon käyttäjiltä, jos internet-verkossa jokin linkki katkeaa. Näin VPN on siis riippuvainen internet-yhteyden toimivuudesta. [2.]

3 VPN-TUNNELOINTI

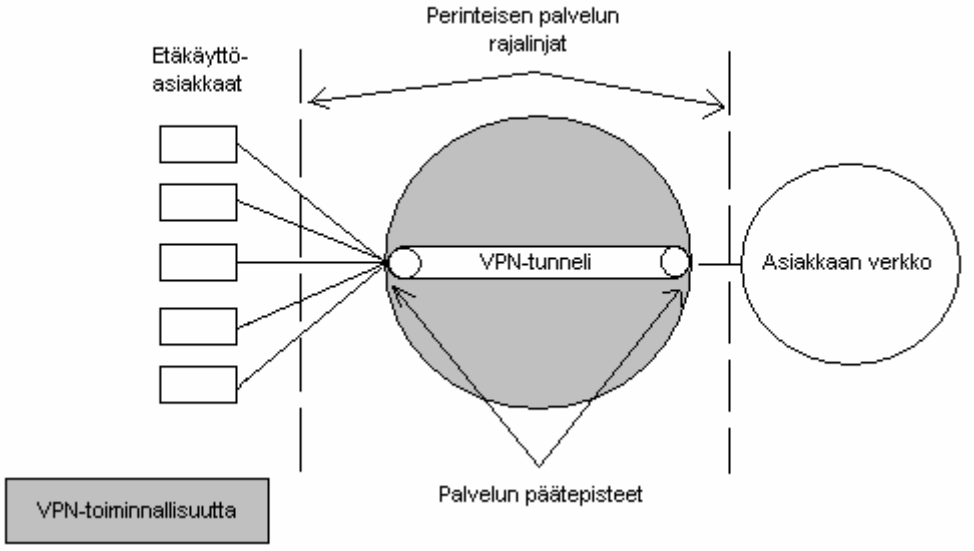
VPN-tunneloinnilla tarkoitetaan sitä, että kehykset tai paketit kapseloidaan toisten pakettien tai kehysten sisään. Täten data kulkee julkisen verkon yli turvallisesti. Tunnelin toisessa päässä salaus puretaan ja kehykset tai paketit saadaan esiin muuttumattomina.

3.1 VPN-mallit

VPN-verkkoja voidaan havainnollistaa kolmen rakenteellisen mallin avulla. Nämä kolme mallia ovat tarjoajamalli, sekamalli ja päästä päähän -malli. Mallit eroavat toisistaan siten, että palvelun päätepisteiden sijainti on jokaisessa eri. Jokainen VPN:n suunnittelija voi valita näistä kolmesta mallista itselleen sopivimman. Suurella todennäköisyydellä kuitenkaan mikään näistä malleista ei ole täysin sopiva yrityksen tarkoituksiin. Tämän takia malli muokataan suunniteltaessa yrityksen omiin tarpeisiin. [1.]

3.1.1 Tarjoajamalli

Tarjoajamalli perustuu siihen, että VPN-toiminnallisuus tapahtuu palveluntarjoajan verkossa. Täten asiakkaan ei tarvitse rakentaa VPN-palvelua varten verkkoonsa mitään lisälaitteita. Palveluntarjoajan verkkoon päästäkseen yritys tarvitsee reitittimen, mutta tämä kuuluu jo nykyään verkon peruslaitteisiin. Kuvasta 2 nähdään, että tarjoajamallin VPN-toiminnallisuuden rajat sijoittuvat samaan kohtaan kuin perinteisen palvelun rajalinjat.



Kuva 2. Tarjoajamallin vertailu perinteiseen palvelumalliin verrattuna [1.]

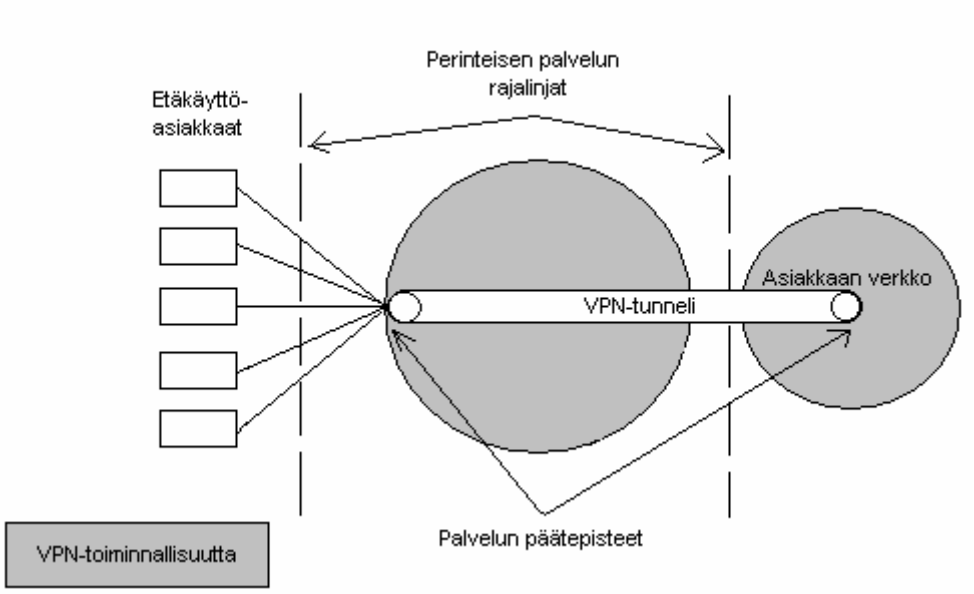
Tarjoajamallissa VPN-tunneli alkaa ja päättyy palveluntarjoajan verkossa. Tästä syystä mallissa tehdään selvä rajanveto siihen, että kaikki asiakkaan tiloissa olevat laitteet ovat itsehallittuja ja kaiken muun hoitaa palveluntarjoaja. Operaattorin kannalta tämä selkeyttää verkon toimintaa ja täten operaattori pystyy kontrolloimaan koko verkkoa. Tämä vähentää verkon konfiguroinnissa tehtävien virheiden lukumäärää. [1.]

VPN:n vakaus on tarjoajamallin vahvuus. Vakaus saavutetaan palveluntarjoajan laitteiden varmatoimisuudella ja sillä, että verkkoa ei varmasti jätetä konfiguroimatta kunnolla. Yritys hyötyy myös siitä, että operaattori kantaa vastuun hallinnoinnista. Tällöin ei tarvita asiantuntijoita VPN:n ylläpitämiseen. [1.]

Kun yrityksellä ei ole asiantuntijoita VPN:n ylläpitämiseen ja vastuu on palveluntarjoajalla, yritys on VPN:n osalta täysin riippuvainen palveluntarjoajasta. Jos operaattorin verkko ei toimi, niin tällöin yrityksen verkosta ei ole ulospääsyä. Toisena haittapuolena tarjoajamallista voidaan mainita kallis hinta. Kun vastuu on operaattorilla, perii se myös korkean hinnan laadukkaasta palvelusta. Vastuun tuoma haitta palveluntarjoajan näkökulmasta on se, että tajoajamallissa asiakaskohtaiset ratkaisut ovat hankalia toteuttaa. [1.]

3.1.2 Sekamalli

Sekamallissa VPN-toiminnallisuutta on sekä yrityksen omassa että palveluntarjoajan verkossa. Täten vastuunjako on hieman epäselvempi kuin tarjoajamallissa. Yrityksen verkossakin on tällöin oltava asiakaspään laitteisto (CPE). Sekamalli eroaa näin perinteisestä palvelumallista, kuten kuvasta 3 nähdään.



Kuva 3. Sekamallin vertailu perinteiseen palvelumalliin verrattuna [1]

Sekamallissa VPN-tunneli alustetaan palveluntarjoajan verkossa, mutta päätetään yrityksen verkossa. Tämä tarkoittaa siis sitä, että palveluntarjoajan on alustettava etäkäyttäjien VPN-tunnelit. Tällöin etäkäyttäjä autentikoidaan palveluntarjoajan verkossa ja tälle luodaan VPN-tunneli yrityksen verkkoon. Yrityksen verkossa on tuolloin oltava asiakaspään laitteisto, missä on VPN-tunnelin toinen päätepiste. Näin etäkäyttäjä saa samat oikeudet yrityksen sisäiseen kuin verkon sisällä olevat käyttäjät. [1.]

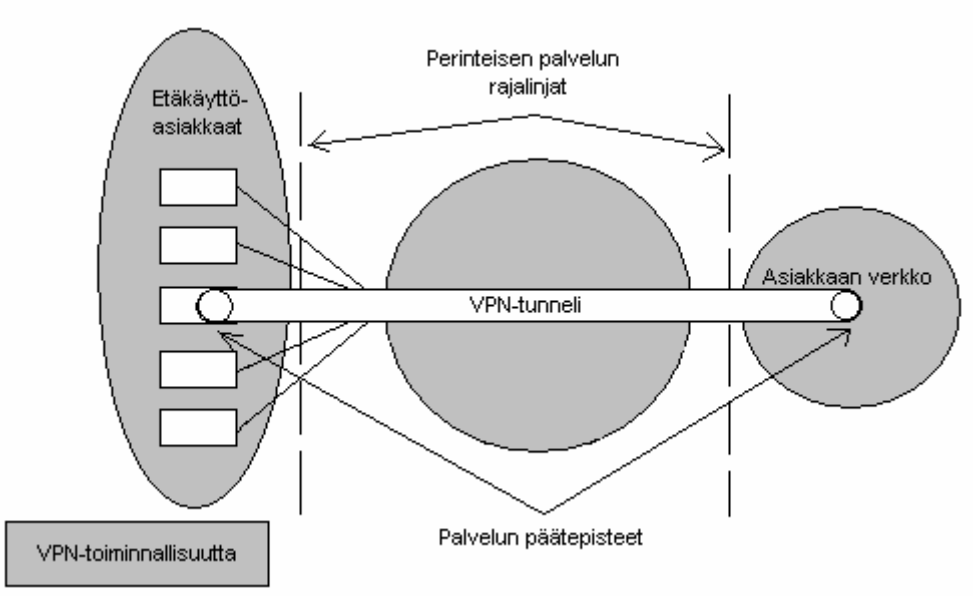
Sekamallin yleistyminen on standardisoinnin aikaansaannosta. Jatkossa tarkasteltavat VPN-tunnelointiprotokollat ovat mahdollistaneet siis sekamallin käytön tekemällä eri laitevalmistajien laitteet yhteensopiviksi. Kun eri verkkojen laitteet ovat keskenään yhteensopivia, voidaan VPN-toiminnallisuutta jakaa eri palveluntarjoajien ja asiakkaiden kesken. Palveluntarjoajalle aiheutuvat kustannukset ovatkin sekamallissa huomattavasti tarjoajamallia pienemmät. [1.]

Yrityksen kannalta sekamallin etuna on verkon hallittavuus. Tällöin yrityksen ei ole pakko tyytyä yhden palveluntarjoajan käyttämiseen. Siten yhden palveluntarjoajan verkon kaatuminen ei estä verkosta ulospääsyä. Sekamalli on myös yritykselle halvempi, jos tarkastellaan maksua operaattorille. Hankaluuksia sekamallissa aiheuttaa se, että VPN-yhteys ei ole täysin palveluntarjoajan hallittavissa. Asiakas voikin tehdä virheitä VPN:n

konfiguroinnissa. Siksi sekamallissa yritys tarvitsee VPN-osaajan asiakaspään laitteiden käyttämiseen.

3.1.3 Päästä-päähän -malli

Päästä-päähän –mallissa VPN-toiminnallisuutta on pelkästään yrityksen laitteistoissa. Palveluntarjoajan verkko toimii tässä mallissa vain siirtotienä. Asiakkaan vastatessa VPN-toiminnallisuudesta, eroaa päästä-päähän-malli eniten perinteisestä palvelumallista. Tämä voidaan havaita kuvasta 4.



Kuva 4. Päästä-päähän –mallin vertailu perinteiseen palvelumalliin verrattuna [1]

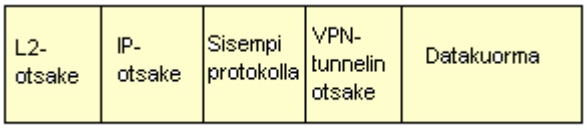
Päästä-päähän –mallissa VPN-tunneli muodostetaan etäkäyttäjän työkoneessa ja päätetään yrityksen verkon CPE:ssa. Päästä-päähän –mallia käyttävässä yrityksessä on oltava VPN-osaamista, jotta VPN:n suunnittelu, laitteiston konfigurointi ja ohjelmistojen jakelut saadaan tehtyä tehokkaasti ja oikein.

Päästä-päähän -mallin etuihin voidaan lukea riippumattomuus yhdestä palveluntarjoajasta ja turvallisuus. Kun data lähetetään ja vastaanotetaan yhdenmukaisilla turvallisuusjärjestelyillä, verkko on helpompi pitää turvallisena. Tarjoaja- ja sekamallikin ovat oikein toteutettuna kyllä turvallisia, mutta niissä tietoturvariskejä on enemmän. Turvallisuuteen vaikuttavat tuotteet, protokollat ja muut teknologiat, joita käytetään VPN:n toteutuksessa.

Päästä-päähän –mallissa etäkäyttäjien koneilla on oltava asiakasohjelmisto, joka tekee tunneloinnin ja salauksen eli muodostaa VPN-yhteyden. Tämä muodostaa haittapuolen päästä-päähän –mallille, koska ohjelmiston päivitys ja tukitoiminnot voivat olla hankalia toteuttaa. Vaikka päästä-päähän –mallin kustannukset yritykselle ovat pienet operaattorin suuntaan, niin laitteistojen hankinnat, suunnitteluhenkilöstön palkat, asennukset, käyttäjäkoulutukset ja ylläpito tuovatkin paljon kustannuksia.

3.2 VPN-tunnelointiprotokollat

VPN-yhteys muodostetaan tunneloimalla data jonkin salausprotokollan sisään. Nämä protokollat suojaavat kaiken Internetin yli VPN-tunnelissa kulkevan datan. [4.] Kuvassa 5 esitetään yleisen VPN-tunnelointipaketin rakenne. Rakennetta tarkastellaan kahden yleisen VPN-tunnelointiprotokollan kohdalla, jotka ovat PPTP ja L2TP.



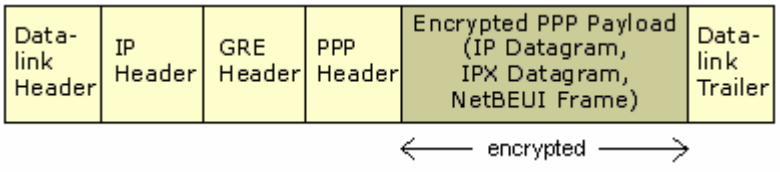
Kuva 5. ”Yleinen” VPN-tunnelointipaketti [1]

3.2.1 PPTP

PPTP (Point-to-Point Tunneling Protocol) on tunnelointikäytäntö, jonka avulla voidaan tunneloida PPP (Poin-to-Point Protocol) TCP/IP-verkon yli. PPTP ei muuta PPP:tä millään tavalla, mutta PPTP on luonut tavan kuljettaa PPP verkon yli. Tärkeää on huomata, että PPTP ei salaa dataa, vaan se vain alustaa VPN-tunnelin. PPTP on alunperin Microsoftin kehittämä tunnelointikäytäntö, josta muut tahot ovat kehittäneet VPN-yhteyksiin sopivan käytännön. [6.]

PPTP käyttää pakettien perustyypeistä datapaketteja ja valvontapaketteja. Datapaketit sisältävät käyttäjän datan. Nämä paketit kapseloidaan käyttämällä GRE-protokollaa (Generic Routing Protocol). Valvontapaketteja PPTP:ssä käytetään merkinantoon ja tilantiedusteluun. [1.] Koko PPTP-paketin rakenne on kuvassa 6. Kuvasta havaitaan, että GRE- (GRE Header) ja PPP-otsakkeen (PPP Header) lisäksi PPTP-pakettiin kuuluu IP-otsake (IP Header). Se sisältää PPTP-paketin lähtö- ja kohde-IP-osoitteen. PPP-hyötykuorma (Encrypted PPP Payload), joka sisältää käyttäjän datan, on

paketin salattu osa. OSI-mallin siirtokerrosta (Data link layer) käyttävään PPTP-pakettiin kuuluu myös siirtokerroksen otsake (Data-link Header) ja siirtokerroksen lopuke (Data-link Trailer). [10.]



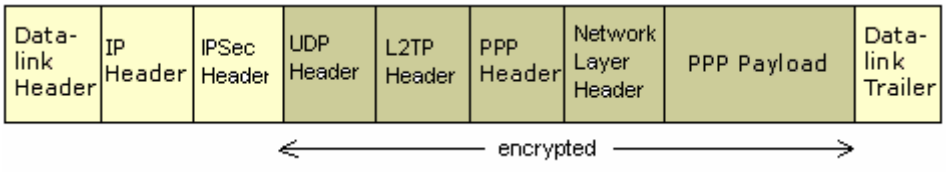
Kuva 6. Tunneloidun PPTP-paketin rakenne [10]

PPTP on viime vuosina menettänyt suosiotaan, koska siinä on huomattu vakavia tietoturvaongelmia. PPTP on silti yhä laajalti käytössä. Tietoturvaongelmien takia Microsoft ja Cisco ovat yhdessä kehittäneet, PPTP:n pohjalta, uudemman L2TP-protokollan.

3.2.2 L2TP

L2TP (Layer 2 Tunneling Protocol) yhdistää kahden aikaisemman tunnelointiprotokollan parhaat puolet. Nämä aikaisemmat protokollat ovat Ciscon kehittämä L2F (Layer 2 Forwarding) ja Microsoftin PPTP. L2TP, kuten PPTP:kin, toimii siten, että se tunneloi PPP-paketteja. L2TP erottuu PPTP:stä siten, että sen kaikki paketit ovat UDP:lla (User Datagram Protocol) kapseloituja. [11.]

L2TP:n turvallisuus PPTP:hen verrattuna perustuu siihen, että autentikointiin voidaan käyttää IPSec:iä. Kuvasta 7 nähdään L2TP-paketin rakenne. Kuvan tummennettu alue on salattu ja salaamatta ovatkin vain siirtokerroksen otsake ja lopuke sekä IP-otsake ja IPSec-otsake. Nämä eivät voi olla salattuna, koska ne vaaditaan siihen, että paketti pystyy kulkemaan IP-verkossa. Paketin salattuun osaan kuuluvat UDP-otsake ja L2TP-otsake sekä verkkokerroksen otsake (Network Layer Header), joka vaaditaan, koska IPSec toimii OSI-mallin verkkokerroksella.



Kuva 7. L2TP-paketin rakenne, kun käytössä on IPSec-kuljetustila[10]

L2TP:n vahvuus perustuu siihen, että se on laajalti tuettu protokolla. Nykyinen suuntaus on kuitenkin se, että lähes kaikkien laitevalmistajien suurin mielenkiinto kohdistuu IPSeciin.

4 IPSEC

IPSec (IP Security) mainitaan usein puhuttaessa tunnelointiprotokollista. Itse asiassa IPSec ei ole yksi protokolla, vaan se koostuu monista protokollista ja on oikeastaan internetin turvallisuusprotokollaperhe. IPSec toimii PPTP:stä ja L2TP:stä poiketen verkkokerroksella eli OSI-mallin 3. kerroksella. Tämä mahdollistaa sen, että IPSecin avulla voidaan salata kaikki 3. kerroksen yläpuolella kulkevat protokollat. Näistä tärkeitä ovat TCP (Transmission Control Protocol) ja UDP. IPSecin tärkeimpänä ominaisuutena pidetään kuitenkin sen läpinäkyvyyttä käyttäjän ja sovelluksen kannalta, koska niiden ei tarvitse huomioida IPSeciä mitenkään. [12.]

IPSec käyttää tietoliikenteen turvallisuuspalveluihinsa kolmea protokollaa, jotka ovat todennusotsikko (Authentication Header, AH), salausotsikko (Encapsulating Security Payload, ESP) ja IKE-avaintenhallintaprotokolla (Internet Key Exchange). [12.] Kun liikennettä verkon komponenttien välillä pitää salata, todentaa ja asettaa avaimia, pitää tiedon näistä olla jossain. Tämä tieto löytyy turvayhteydestä (Security Association, SA). SA on looginen yksisuuntainen tiedonsiirtokanava eli ”tunneli”. SA sisältää tiedot kolmesta asiasta:

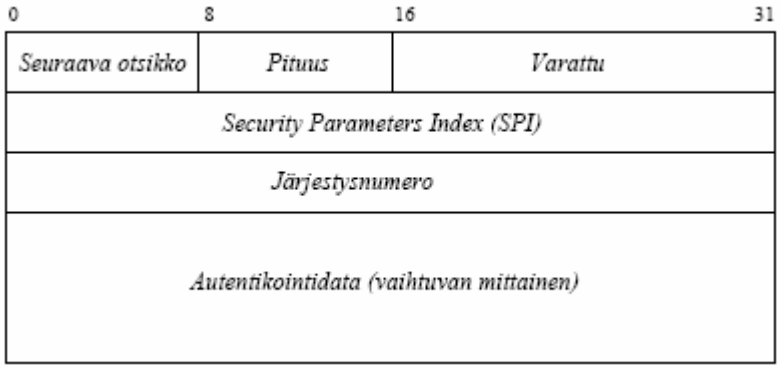
- SPI:n (Security Parameters Index), joka kertoo 32-bittisen index-numeron vastaanottajan turvayhteystietokantaan
- Kohteen IP-osoitteen
- IPSecin turvallisuusprotokollan (AH tai ESP)

SA:t sisältävät siis erittäin salaista tietoa ja ne säilytetään turvayhteystietokannassa (Security Associations Database, SAD). Arkaluontoisuuden takia SADin on sijaittava paikassa, johon pääsy on kielletty. [2.]

4.1 IPSecin todennus

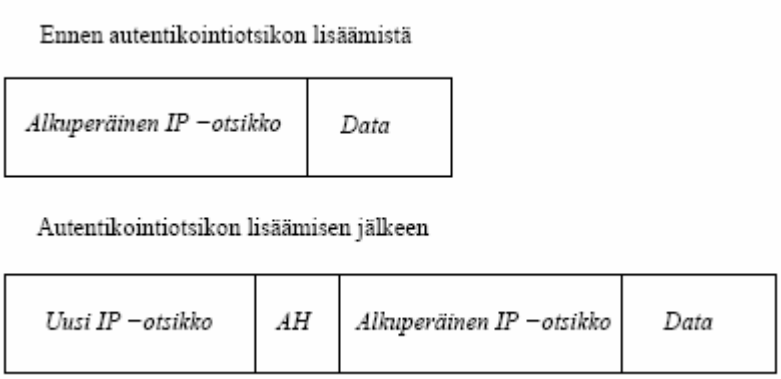
IPSec käyttää todennukseen todennusotsikkoa eli AH-protokollaa. Sen tehtävänä on paketin eheyden tarkistaminen ja alkuperän todennus. AH tarjoaa myös suojan keskeytyshyökkäyksiin. Tämä on toteutettu AH:ssa siten, että matkalla kaapattuja paketteja ei voi käyttää hyökkäyksiin lähettämällä niitä uudelleen, koska jokainen paketti on yksilöity järjestysnumerolla. [13.]

Todennusotsikon rakenne näkyy kuvassa 8. Seuraava otsikko on 8 bitin kenttä, josta nähdään seuraavan otsikon tai muun kuorman tyyppi. Pituus-kenttä määrittelee AH:n pituuden. Varattu-kenttä asetetaan nykyisin vielä aina nollaksi, sillä se on AH:n rakenteessa tulevaisuuden muutoksia varten. SPI (Security Parameters Index) on 32-bittinen kenttä, joka yksilöi turvayhteydet. Järjestysnumero, joka yksilöi paketit, on myös 32-bittinen kenttä. Autentikointidata-kentän bittimäärä vaihtelee. Se sisältää kryptografisen summan. Tuon summan avulla tarkistetaan paketin eheys ja todennetaan lähettäjä. [13.]



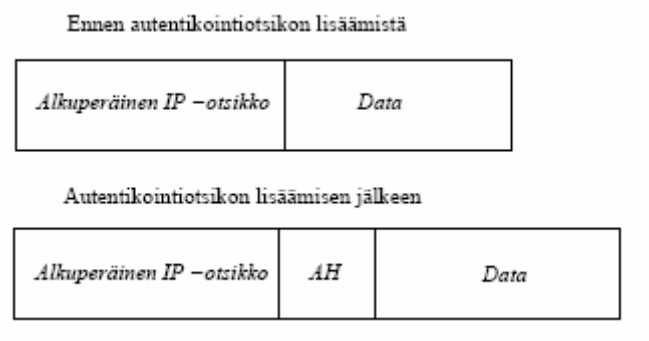
Kuva 8. AH:n rakenne [13]

AH:lla on kaksi erillistä toimintatilaa, jotka ovat tunnelitila ja kuljetustila. Tunnelitilassa autentikointiotsikko sijoitetaan alkuperäisen IP-otsikon väliin (kuva 9). Lisäämisen jälkeen alkuperäinen IP-otsikko ja data muuttuvat yhdessä hyötykuormaksi. Huomattavaa on, että myös uusi IP-otsikkokin otetaan mukaan, kun lasketaan kryptografista tarkistussummaa.



Kuva 9. AH:n lisääminen IP-pakettiin tunnelitilassa [2]

Kuljetustilassa todennusotsikko sijoitetaan alkuperäisen IP-otsikon ja datan väliin (kuva 10). Näin paketille jää sama IP-otsikko. Kuljetustilassa kryptografiseen tarkistussummaan lasketaan mukaan IP-otsikko ja data.

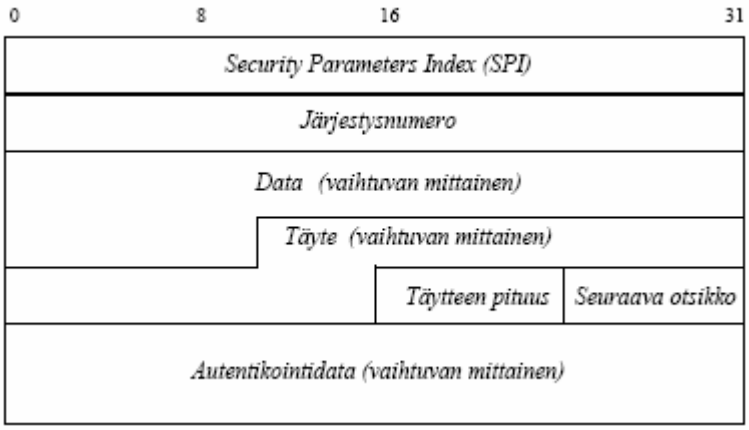


Kuva 10. AH:n lisääminen IP-pakettiin kuljetustilassa [2]

4.2 IPSecin salaus

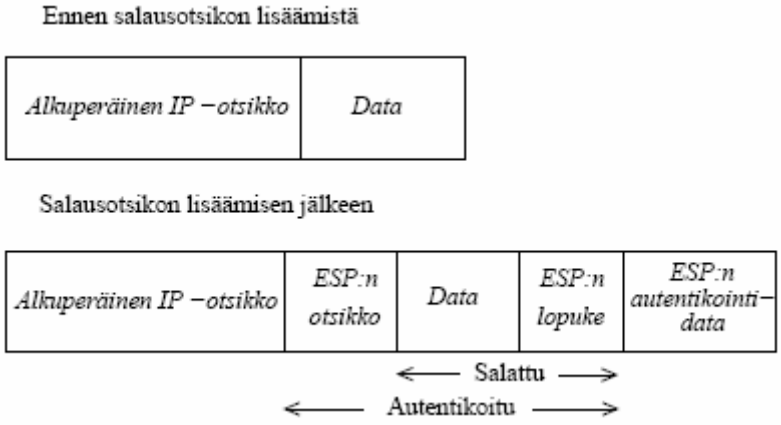
IPSec käyttää salausprotokollanaan ESP:tä. IPSecissä on mahdollista käyttää joko AH:ta tai ESP:tä, mutta yleisimmin käytetään molempia. Täten tietoturvallisuus on paremmalla tasolla. ESP takaa luottamuksellisuuden salauksella, tarkistaa paketin eheyden ja varmistaa paketin alkuperän. ESP:n todennus ei ole kuitenkaan AH:n tasolla, joten siksi protokollien yhteiskäyttöä IPSecissä suositellaan. [1.]

Salausotsikon rakenne näkyy kuvassa 11. AH:n yhteydessä selvitettiin jo suuri osa kentistä ja niiden selitykset ovat samat ESP:n kohdalla. AH:sta poikkeavia kenttiä ovat data-, täyte- ja täytteen pituus -kenttä. Data-kentän pituus vaihtelee, sillä kentässä kuljetetaan tarvittaessa esim. synkronointidataa. Data-kentän sisältö on kuvattu seuraava otsikko -kentässä. Täyte-kenttää käytetään nimen mukaisessa merkityksessä, jos esim. salausalgoritmi vaatii juuri tietynpituisen paketin. Täyte-kentän pituus siis myös vaihtelee ja se voi olla myös nolla. Täytteen pituus –kenttä kertoo täyte-kentän pituuden. [13.]



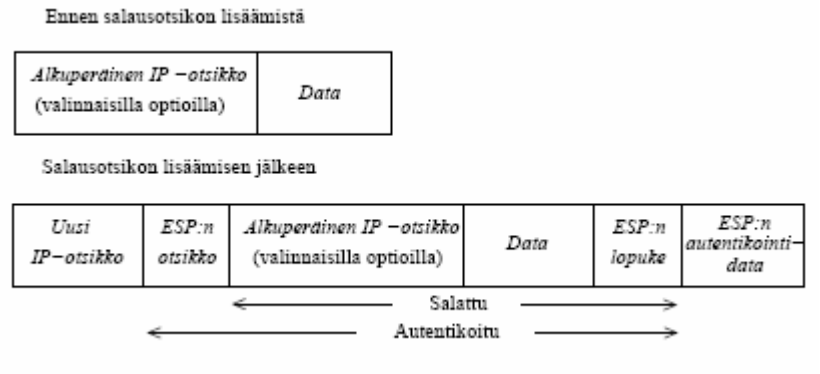
Kuva 11. ESP:n rakenne [13]

ESP:llä on AH:n tapaan kaksi eri toimintatilaa, jotka ovat kuljetustila ja tunnelitila. Kuljetustilassa salausotsikon lisääminen tapahtuu kuvan 12 mukaisesti. ESP:n heikkous todennuksessa on siinä, että lisäämisen jälkeen alkuperäistä IP-otsikkoa ja ESP:n autentikointidataa ei oteta huomioon kryptografista tarkistussummaa laskettaessa. Tämän takia ESP-salauksen jälkeen tehdään vielä todennus AH:lla. [13.]



Kuva 12. ESP:n lisääminen IP-pakettiin kuljetustilassa [13]

Tunnelitilassa salausotsikon lisääminen tapahtuu kuvan 13 mukaisesti. Tunnelitilassa alkuperäinen IP-otsikko lasketaan myös mukaan kryptografiseen tarkistussummaan. Tämän takia ESP:n käytössä tunnelitila on suositeltavampi kuin kuljetustila.



Kuva 13. ESP:n lisääminen IP-pakettiin tunnelitilassa [13]

4.3 IPSecin avaintenhallinta

IPSecin avaintenhallinnalla tarkoitetaan toimintoja, joita ovat avainten luonti, siirto, varmistus, poisto ja päivittäminen. Avaintenhallinnan tärkein tehtävä on avainten sopiminen salausta ja todennusta varten. IPSecin virallinen ja automaattinen avaintenhallintaprotokolla on IKE. Tästä huolimatta IPSecissä on mahdollisuus käyttää myös manuaalista avaintenhallintaa, mutta sitä ei suositella ison työmäärän vuoksi. [12.]

IKE:n avaintenvaihto perustuu Diffie-Hellman–algoritmiin. IKE:ssä määritellään Diffie-Hellman–ryhmä, joka määrittää salauksen vahvuuden. Ryhmät 1 (768-bittinen), 2 (1024-bittinen) ja 5 (1680-bittinen) ovat alkulukujen potenssiin perustuvia. Ryhmät 3 (155-bittinen) ja 4 (185-bittinen) perustuvat taas elliptisiin käyriin. Asiantuntijoiden suositus olisi käyttää vähintään ryhmää 2 turvallisuussyistä. [14.]

IKE:n pääasiallinen tehtävä on neuvotella turvayhteydet muita IPSecin osia varten. IKE:n turvayhteyksien neuvottelu tapahtuu kahdessa vaiheessa. Ensimmäinen vaihe voidaan suorittaa kahdessa eri tilassa: päätila (Main Mode) tai aggressiivinen tila (Aggressive Mode). Toinen vaihe on nopea tila (Quick Mode). Ensimmäisessä vaiheessa muodostetaan IKE:n turvayhteys (IKE SA) ja toisessa IPSecin turvayhteys (IPSec SA). IKE voi käyttää todennukseensa kolmea tapaa, jotka ovat digitaalinen allekirjoitus, RSA-salaus ja etukäteen jaettu avain (Pre-shared key, psk). Pre-shared key on IKE:ssä pakollinen. [14.]

5 TIEDON SALAUS

Tiedon salauksella tarkoitetaan selkokielisen tekstin muokkaamista siten, että sitä ei pysty enää tulkitsemaan. Erilaisilla salausmenetelmillä pyritään varmistamaan tietojen luottamuksellisuus, eheys ja kiistämättömyys.

5.1 Symmetriset salausalgoritmit

Symmetrisellä salauksella tarkoitetaan sitä, että lähettäjä ja vastaanottaja jakavat keskenään saman salaisen avaimen. Tätä salausavainta käytetään salaamisessa ja purkamisessa. Symmetrisen salauksen vahvuus onkin salausmenetelmän nopeus. Symmetrinen salaus pohjautuu siihen, että avainta ei pystytä murtamaan ja tällöin hakkerin on turvauduttava laskukapasiteettiin. Tässä tapauksessa avaimen laskemiseen kuluva aika on suoraan verrannollinen salausavaimen pituuteen. Siksi koneiden laskukapasiteetin kasvaessa on järkevää valita mahdollisimman pitkä salausavain. [16.]

Symmetrisen salauksen ongelmana on usein salausavaimen välittäminen osapuolille. Tähän on käytettävä joko epäsymmetristä salausta tai sitten salausavain on toimitettava henkilökohtaisesti. Symmetristä salausta voidaan pitää luotettavana salausmuotona, jos salainen avain ei joudu vääriin käsiin. Kohta käsiteltävistä salauksista kuitenkin DES alkaa olla jo nykypäivänä liian heikko salausavain. [16.]

5.1.1 DES

Data Encryption Standard (DES) on 1970-luvulla kehitetty symmetrinen lohkosalausmenetelmä. Lohkon pituus on 64 bittiä, mutta avaimen efektiivinen pituus on 56 bittiä. 8 bittiä lohkon lopussa ovat pariteetin tarkistusbittejä. DES:n heikkona puolena on juuri avaimen pituus. Nykyisillä tietokoneilla DES-avaimen pystyy laskemaan alle vuorokaudessa käymällä läpi koko avainavaruuden. Tämän vuoksi DES:n pohjalta on kehitetty sen laajennuksena 3DES ja myös kokonaan uutena salauksena AES. [15.]

5.1.2 3DES

Triple Data Encryption Standard (3DES) on DES:n laajennus. Siinä käytetään joko kahta tai kolmea 56 bitin salausavainta. Näin salauksen pituudeksi muodostuu 112 tai 168 bittiä. Useimmiten 3DES on nimestään

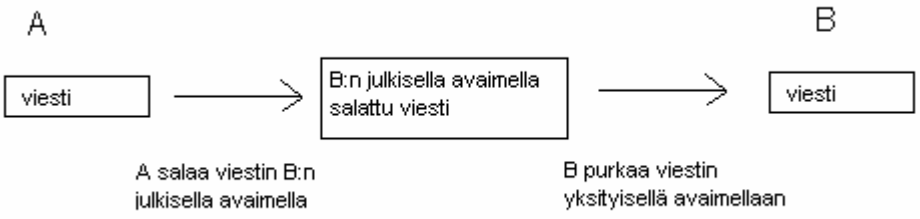
huolimatta vain kaksi kertaa niin vahva kuin DES. Tällöin avaimen todellinen pituus on 112 bittiä. 3DES:n toisessa versiossa käytetään kolmea yksittäistä DES-avainta. Tuolloin 3DES on kolme kertaa niin vahva kuin DES. Kuten jo aiemmin mainittiin, niin IPSecin tapauksessa käytetään juuri kolmea avainta. [1.]

5.1.3 AES

Advanced Encryption Standard (AES) on DES:n pohjalta kehitetty salausmenetelmä. AES:n synonyymina käytetään nimitystä Rijndael sen kehittäjien Joan Daemenin ja Vincent Rijmenin mukaan. AES otettiin käyttöön vuonna 2002. AES on noussut suosituimmaksi symmetriseksi salausavaimeksi. 3DES on silti edelleen myös laajalti käytössä. AES-avaimen pituus on 128, 196 tai 256 bittiä. AESia ei ole vielä nykytiedon mukaan pystytty murtamaan. [12.]

5.2 Epäsymmetriset salausalgoritmit

Epäsymmetrisessä salauksessa käytetään avainparia, joista toinen on julkinen ja toinen yksityinen. Avaimet toimivat siten, että julkisella avaimella salattu viesti voidaan avata yksityisellä avaimella ja toisinpäin. Esimerkkinä voidaan tarkastella kuvaa 14, jossa henkilö A lähettää viestin B:lle.



Kuva 14. Viestin kulku epäsymmetrisellä salauksella

Kuvan 14 mukaista salausta voitaisiin käyttää esim. sähköpostin lähetyksessä. Epäsymmetrinen salaus perustuu siihen, että yksityinen avain on vain kyseisen käyttäjän tiedossa ja sen laskeminen ulkopuoliselle on mahdotonta järjellisessä ajassa. [17.]

Epäsymmetrisen salauksen vahvuus on avaintenhallinnan yksinkertaisuus. Salausavainten välittämisen ongelmaa ei ole samalla tavalla kuin symmetrisessä salauksessa. Epäsymmetrisen salauksen heikkoutena on

kuitenkin hitaus, joka johtuu salauksen pituudesta. Julkisia avaimia käytettäessä avainten on oltava pidempiä kuin salaisia avaimia käytettäessä. [17.]

5.2.1 RSA

RSA-salausalgoritmi on epäsymmetrinen salausmenetelmä, jonka kehittivät Ron Rivest, Adi Shamir ja Leonard Adleman. RSA perustuu suurten lukujen tekijöihin jakamisen vaikeuteen. RSA on noussut suosituimmaksi epäsymmetriseksi salausalgoritmiksi yksinkertaisuutensa ja helpon toteutettavuutensa perusteella. [17.]

RSA toimii matemaattisesti siten, että salaukseen käytetään seuraavanlaista kaavaa:

$$C = M^{e} (\mathrm{mod}\, n)$$

Salauksessa M on salattava viesti, C salattu viesti ja e julkinen avain. Purkamiseen käytetään seuraavaa kaavaa:

$$M = C^{d} (\mathrm{mod}\, n)$$

Salauksen purkamisessa mukana oleva d on yksityinen avain. Avainparin yhteinen osa on n eli se on käytössä salauksessa ja purkamisessa. RSA:n matematiikkaan ei tutustuta tässä tarkemmin. [12.]

5.2.2 Diffie-Hellman

Diffie-Hellman–algoritmi perustuu diskreetin logaritmin ongelmaan. Se toimii siten, että viestien lähettäjä ja vastaanottaja jakavat saman salaisen avaimen. Diffie-Hellmania ei voida tuon takia pitää turvallisena todennusmenetelmänä. Jos kolmas osapuoli onnistuu sieppaamaan viestin ja muuntamaan sitä, hän voi tällöin pystyä seuraamaan liikennettä salaa. Tästä syystä Diffie-Hellmanin kanssa on käytettävä jotain erillistä todennusmenetelmää. Diffie-Hellman oli ensimmäinen julkisen avaimen salausmenetelmä, kun se julkaistiin vuonna 1976. Kuten jo IPSecin avaintenhallintaa käsiteltäessä mainittiin, Diffie-Hellmania käytetään nykyäänkin suojaamaan IP-liikennettä IPSec-protokollien IKE-avaintenhallintaprotokollassa. [12.]

5.3 Tiivistefunktiot

Tiivistefunktioita käytetään sekoittamaan julkisen avaimen menetelmällä lähetetty viesti. Siitä käytetään myös nimityksiä sekoite, hajautus- ja hash-funktio. Tiivistefunktio on matemaattinen funktio, joka ottaa syötteeksi pituudeltaan mielivaltaisen merkkijonon ja tuottaa kiinteämittaisen tulosteen. Tiivistefunktioiden vahvuus perustuu siihen, että määrätystä syötteestä on helppo laskea tiiviste, mutta on vaikeaa tai mahdotonta muodostaa alkuperäinen viesti tiivisteen perusteella. Kaksi tämän hetken yleisintä tiivistefunktiota VPN:issä ovat MD5 (Message Digest 5) ja SHA-1 (Secure Hash Algorithm). [18.]

MD5 on Ron Rivestin kehittämä ja se perustuu aikaisempaan MD4-algoritmiin. SHA-1 perustuu myös MD4-algoritmiin, mutta sen on kehittänyt NIST (National Institute of Standards and Technology). MD5-algoritmi tuottaa 128-bittisen tiivisteen ja onkin erittäin nopea algoritmi. SHA-1 on hieman hitaampi, mutta se tuottaa 160-bittisen tiivisteen. SHA-1:tä voidaankin pitää turvallisempana tiivistefunktiona kuin MD5. Tiivisteen pituus on suoraan verrannollinen sen turvalisuuteen. Tämän vuoksi on kehitetty myös tiivistefunktio SHA-2, jonka pituus on 256 bittiä. [12.]

5.4 Todennus

Viestien todennuksella tarkoitetaan sitä, että käyttäjän tai palvelun identiteetti varmennetaan. Perinteinen symmetrinen salaus toteuttaa todennuksen ja luottamuksellisuuden itsessään. Kun symmetrisessä salauksessa salattua viestiä ei voi purkaa kuin yhden käyttäjän omalla salaisella avaimella, niin sen purkaminen tai muuttaminen ei ole mahdollista muille. Täten viestin vastaanottaja tietää viestin olevan alkuperäinen ja voi luottaa viestin lähteeseen. Symmetrisessä salauksessa käytetään tästä huolimatta tarkistussummia todennukseen, koska joissain tapauksissa viestien muuttumattomuudesta ei voida olla täysin varmoja. Tarkistussumman avulla voidaan todeta salauksen purkamisen jälkeen, onko viesti järjellinen. [12.]

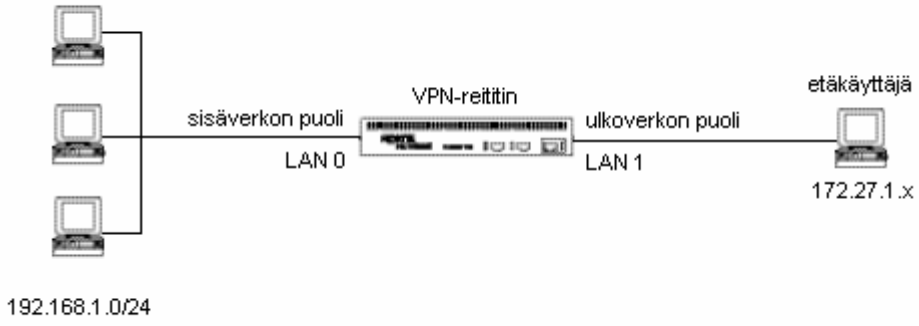
Epäsymmetrisessä salauksessa todennus toteutetaan siten, että lähettäjä salaa viestinsä omalla salaisella avaimellaan. Vastaanottaja voi purkaa viestin lähettäjän julkisella avaimella. Todennus toteutuu näin, mutta tällä ei varmisteta luottamuksellisuutta. Tämän vuoksi myös epäsymmetrisessä

salauksessa käytetään tarkistussummia, joista puhuttiin jo IPSecin todennuksen yhteydessä. Yleisimpiä tarkistussummia ovat MAC (Message Authentication Code) ja HMAC (Keyed-Hash Message Authentication Code). [1.]

MAC eli tarkistussumma käyttää salaista avainta ja todennettavaa viestiä, joista se luo kiinteämittaisen tiivisteen. MAC lasketaan jollain salausalgoritmillä kuten esim. DES:llä. Yleisin käytössä oleva tarkistussumma HMAC pystyy käyttämään salaisen avaimen kanssa yleisimpiä tiivistefunktioita. Se voi siis käyttää tarkistussumman laskemiseen esim. MD5:tä ta SHA-1:tä. HMAC:n vahvuus perustuukin siihen, että tiivistefunktiot kehittyvät nopeasti ja niitä vastaan on hankala hyökätä. [19.]

6 VPN-RATKAISUJEN VERTAILU

VPN-ratkaisujen vertailussa tarkastellaan kahden suositun VPN-laitteiden valmistajan ratkaisuja teknisten ominaisuuksien, hallittavuustyökalujen ja client-ratkaisujen osalta. Työssä konfiguroidaan VPN-reitittimeen asetukset, jotta etäkäyttöyhteyden muodostaminen onnistuu laitteen sisäverkkoon. Yhteys muodostetaan laitteen ulkoverkon puolella kiinni olevasta työasemasta, johon on tehty molempien laitevalmistajien VPN-client-asennukset. Testiverkon rakenne on esitetty kuvassa 15.



Kuva 15. Testiverkko

VPN-reitittimen sisäverkossa olevat työasemat saavat IP-osoitteet DHCP:n avulla. Ulkoverkossa olevat käyttäjät saavat osoitteen joko DHCP:n (Cisco) tai VPN-reitittimeen määritetyn staattisen IP-määrittelyn (Nortel) kautta. Molemmisssa laitteissa on mahdollisuus tehdä IP-osoitteiden määrittely eri tavoilla sisä- ja ulkoverkkoon, mutta nämä määrittelyt ovat hallinnoijan kannalta selkeimmät valinnat näillä laitteilla. Tärkeintä on, että käyttäjät saavat IP-osoitteensa automaattisesti.

Rakennetussa testiverkossa etäkäyttäjä muodostaa VPN-tunnelin reitittimeen ja pääsee näin sisäverkkoon. Etäkäyttäjä toimii näin esimerkkinä siitä, miten Internetissä oleva käyttäjä saa yhteyden reittittimeen ja sitä kautta sisäverkkoon. Sisäverkko toimii mallina yrityksen lähiverkosta normaalissa toimistossa.

6.1 Cisco PIX 501:n testaus ja asennus

6.1.1 Tekniset ominaisuudet

Ciscon VPN-reitittimeksi valittiin Cisco PIX 501 (Kuva 16). Reitittimen tekniset ominaisuudet (taulukko 1) ovat riittävät pienen yritysverkon VPN:ää varten. Cisco PIX 501:n tekniset arvot, kuten esim. siirtonopeudet, ovat huomattavasti pienempiä kuin Nortel Contivity 1010:ssa, mutta normaalille pienyritykselle siirtonopeudeuksien alhaisuus ei aiheuta haittaa työskentelylle. Cisco PIX 501:n hinta kaupoissa on n. 300 €.

Taulukko 1. Cisco PIX 501:n tekniset ominaisuudet [8]

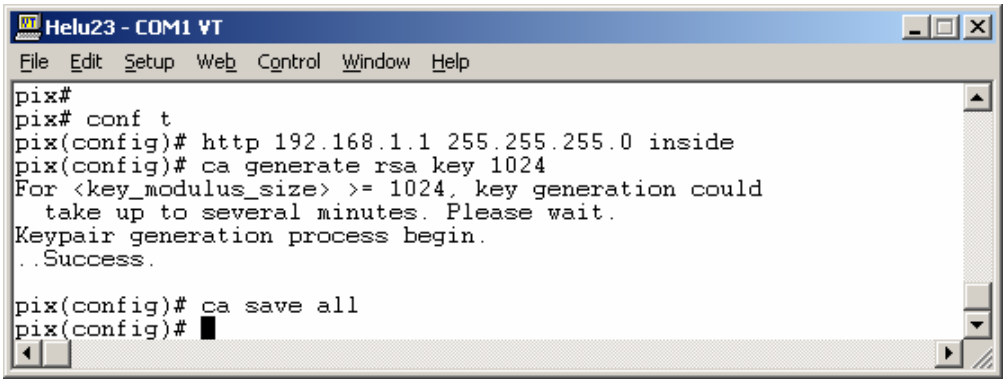
samanaikaisten VPN-tunneleiden määrä	10
prosessori	133 MHz AMD SC520
keskusmuisti	16 MB
flash-muisti	8 MB
VPN siirtonopeus AES-salauksella	4,5 Mbps
VPN siirtonopeus 3DES-salauksella	3 Mbps

Kuva 16. Cisco PIX 501

6.1.2 Laitteen porttien konfigurointi ja VPN-asetusten määrittely

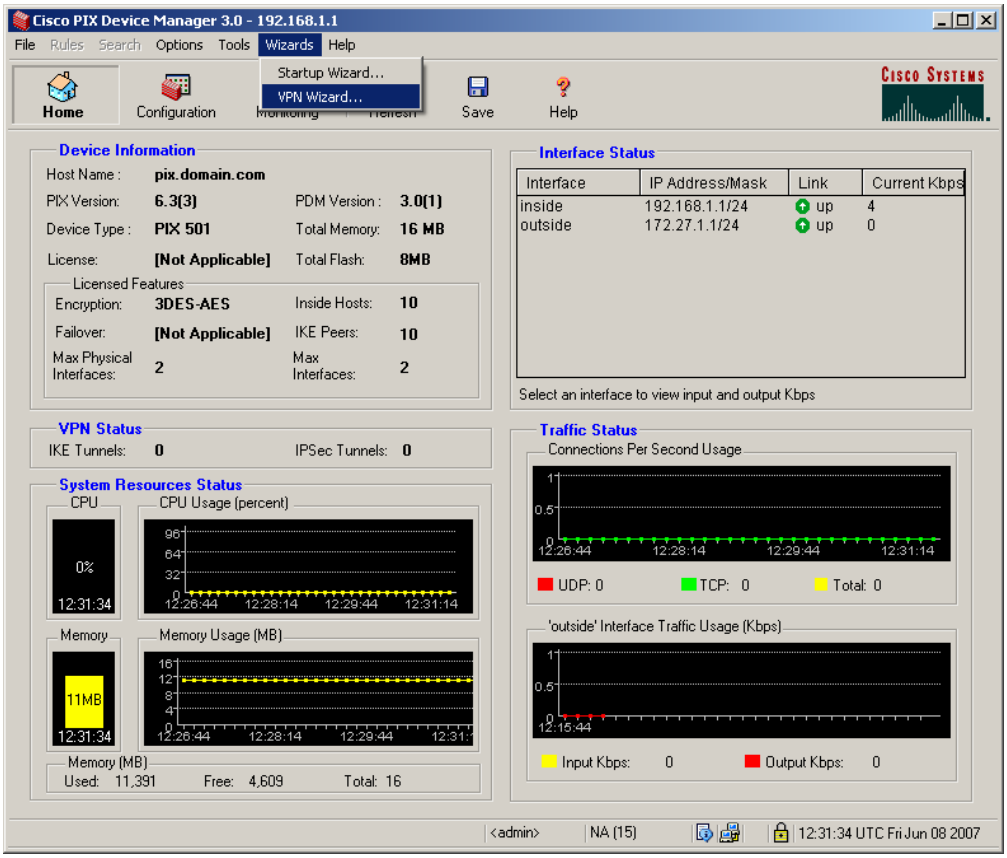
Cisco PIX 501 –reittittimen konfiguraatio aloitettiin resetoinnilla tehdasasetuksiin. Tämä tehtiin konsolissa käskyillä **write erase** ja **reload**. Tämän jälkeen konsolissa määriteltiin vielä hallintaosoite, jotta reitittimen konfigurointi onnistui selaimessa. Kuvassa 17 hallintaosoite asetettiin olemaan 192.168.1.1. Ongelmia selainyhteyden saamisessa tuotti sertifikaatin määrittelyn puuttuminen. Ciscon VPN-reitittimissä on aina

määritettävä sertifikaatti selainhallinnointia varten, joten se tehtiin käskyllä **ca generate rsa key 1024**.



Kuva 17. Cisco PIX 501:n määrittely konsolissa selain-hallinnointia varten

Onnistuneen sertifikaatin määrittelyn jälkeen avattiin PIX Device Manager 3.0 selaimen kautta asettamalla osoitteeksi https://192.168.1.1. Kuvassa 18 näkyy, että ulkoverkon puolelle määritettiin osoite 172.27.1.1. Tähän osoitteeseen etäkäyttäjiltä muodostetut VPN-tunnelit päätetään ja tunnelit toiseen suuntaan aloitetaan. Verkkojen määrittelyn jälkeen Ciscon VPN-asetukset laitettiin kuntoon VPN Wizardin avulla.



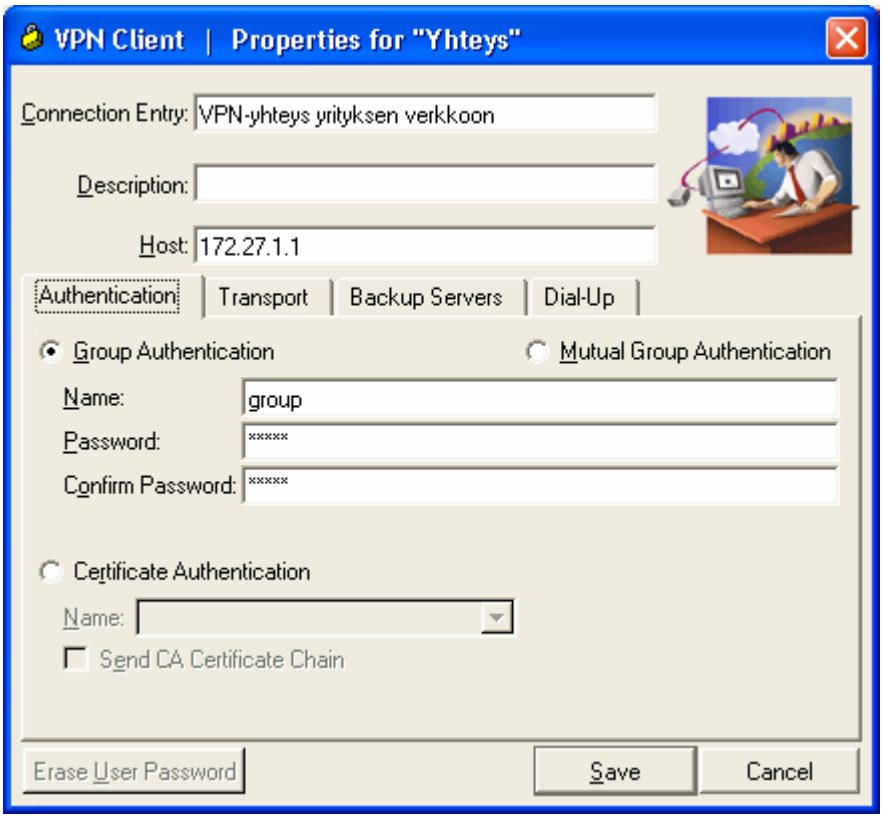
Kuva 18. Cisco PIX Device Manager 3.0

VPN Wizardissa voi määrittää VPN:n etäkäyttöä varten tai lähiverkkojen välisen VPN:n. Työssä asetettiin kuvan 18 mukaisesti VPN-määritykset ulkoverkossa oleville etäkäyttäjille. VPN Wizard:ssa määritettiin ryhmä **group**, jolle annettiin salasana (Pre-shared key). IKE-autentikoinniksi määriteltiin 3DES, jonka tiivistefunktioksi valittiin MD5 ja Diffie-Hellman – ryhmäksi valittiin numero 2. VPN-tunnelin salaukseksi valittiin 3DES, ja sen tiivistefunktioksi MD5. Ciscon reititin tarjoaa oletuksena salausprotokollaksi ESP:n. Jos todennukseen eli AH:iin pitäisi tehdä muutoksia, niin ne voi tehdä VPN Wizardin loputtua VPN-valikoista. Salauksen ja todennuksen määrittely voitiin työssä tehdä melko vapaasti, koska VPN:iin ei tässä liitetty muita VPN-reitittimiä. Jos verkossa olisi enemmän reitittimiä, niin jokaisessa reitittimessä olisi oltava sama salaus ja todennus, jotta salauksen purku ja todennus onnistuu kaikkialla. ESP-3DES-salauksen valinta on hyvä sen yleisyyden ja hyvän tietoturvallisuuden takia. IPSec-tunnelia salattaessa 3DES tarkoittaa kolminkertaista salausta DES-salaukseen verrattuna.

VPN Wizard:ssa saatiin VPN:lle välttämättömät asetukset, mutta lisäksi käytiin asettamassa DHCP serveri molempiin portteihin. Sisäverkon käyttäjille asetettiin käyttöön IP-osoitteet 192.168.1.10 – 192.168.1.15 ja ulkoverkon käyttäjille IP-osoitteet 192.168.2.1 – 192.168.2.5. Näin käyttäjien ei tarvitse välittää IP-osoitteista, kun he saavat ne DHCP:n välityksellä.

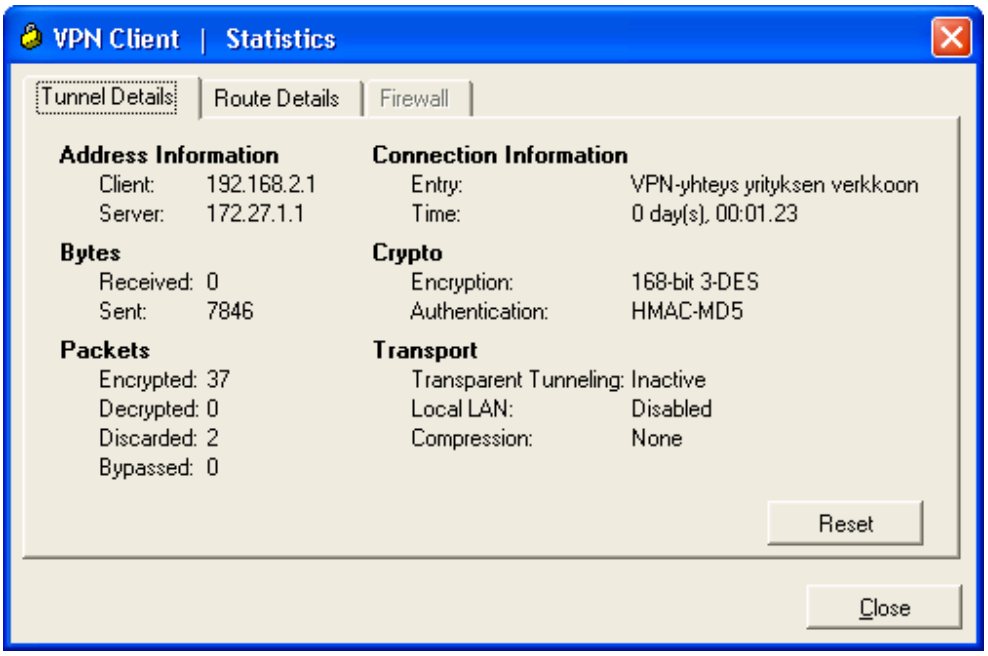
6.1.3 Cisco VPN Clientin käyttö

Etäyhteyttä varten otettiin käyttöön Cisco VPN Client 4.6. Sovelluksessa syötettiin kuvan 19 mukaisesti ryhmän nimi **group** ja sen salasana. Yhteys nimettiin olemaan ”VPN-yhteys yrityksen verkkoon”, joka on vain yhteyden tallennusnimi käyttäjälle. VPN-yhteys otettiin tunneleiden päätepisteeseen eli IP-osoitteeseen 172.27.1.1.



Kuva 19. Yhteyden määrittely Cisco VPN Client:ssa

Yhteyden määrittelyn jälkeen luotiin VPN-yhteys sisäverkkoon. Muodostetun VPN-tunnelin tietoja voitiin seurata Statistics-ikkunasta (kuva 20). Ikkunasta voidaan havaita aiemmin määritetyt salausalgoritmi ja IP-osoitteet sekä yhteyden kesto ja datan kulku.



Kuva 20. VPN-tunnelin tiedot Cisco VPN Clientissa

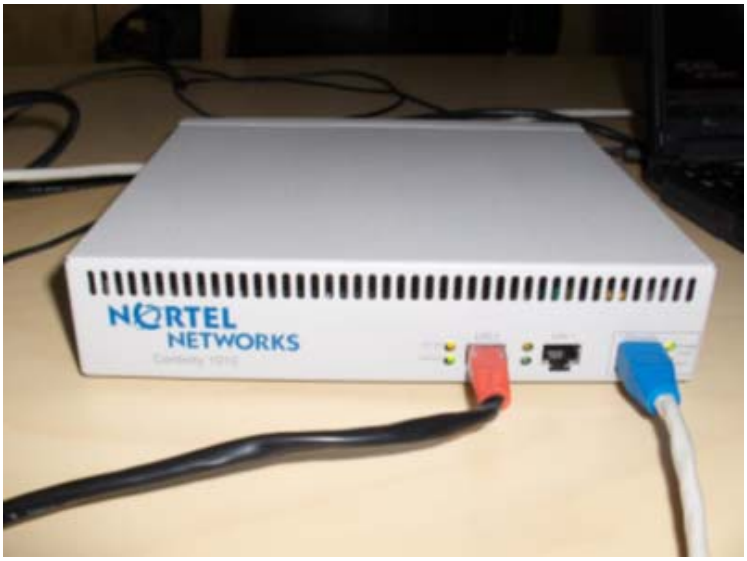
6.2 Nortel VPN Router 1010:n testaus ja asennus

6.2.1 Tekniset ominaisuudet

Nortelin reitittimeksi valittiin Nortel VPN Router 1010 (kuva 21). Nortel Contivity 1010:n hinta on n. 500 €, joten se on n. 200 € kalliimpi kuin Cisco PIX 501. Hinnalla saa kuitenkin teknisiltä ominaisuuksiltaan (taulukko 2.) laadukkaamman laitteen. Nortelin reitittimen siirtonopeudet ovat huomattavasti parempia kuin Ciscon laitteen. Nortel Contivity 1010:n tekniset ominaisuudet mahdollistavatkin keskisuuren yrityksen VPN:n rakentamisen yhden tai useamman VPN-reitittimen avulla.

Taulukko 2. Nortel VPN Router 1010:n tekniset ominaisuudet [9]

samanaikaisten VPN-tunneleiden määrä	30
prosessori	300 MHz Celeron
keskusmuisti	128 MB
flash-muisti	64 MB
VPN siirtonopeus AES-salauksella	30 Mbps
VPN siirtonopeus 3DES-salauksella	15 Mbps

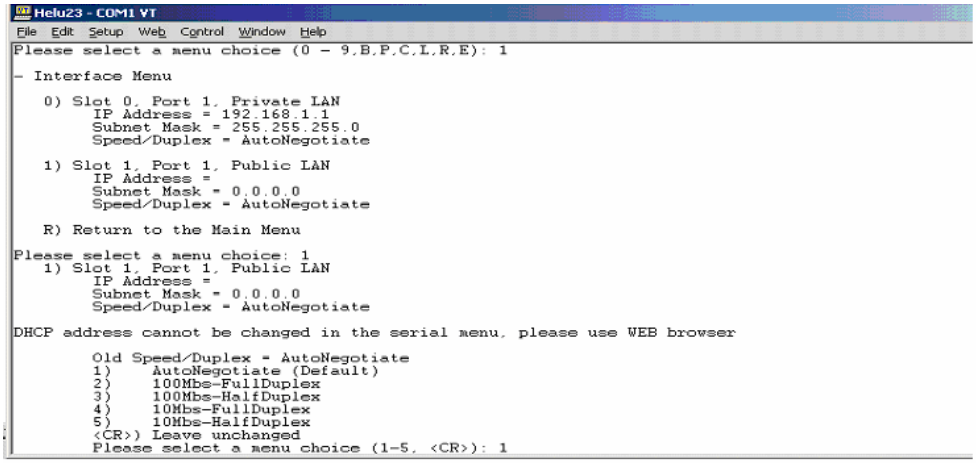


Kuva 21. Nortel VPN Router 1010

6.2.2 Laitteen porttien konfigurointi

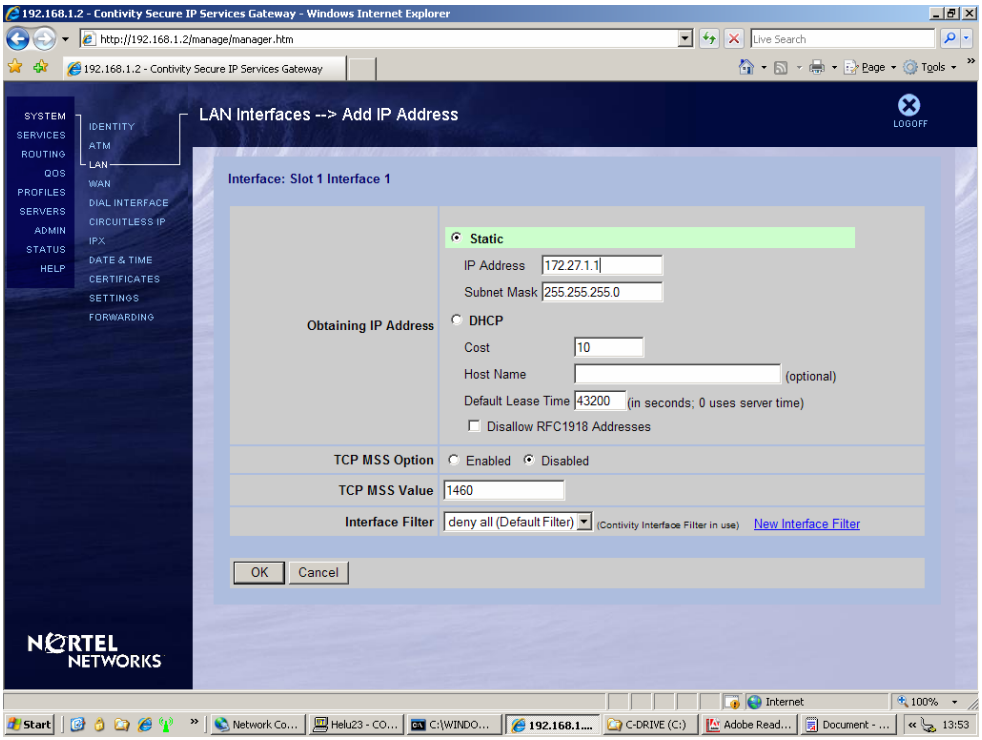
Asennus aloitettiin reitittimen resetoinnilla konsolissa. Resetoinnin jälkeen Nortel Contivity 1010 antoi tehdasasetuksenaan sisäverkkoon (Private LAN) IP-osoitteet 192.168.1.3 – 192.168.1.255. Osoite 192.168.1.1 on reitittimen sisäverkon puolen osoite, joka toimii sisäverkon koneiden

oletusyhdyskäytävänä ulkoverkkoon päin. Osoite 192.168.1.2 on reitittimen hallinta-osoite, jolla laitetta voi hallita internet-selaimessa. Kuten kuvasta 22 nähdään, ulkoverkon puoli (Public LAN) on Nortel Contivity 1010:ssa tehdasasetuksena konfiguroimatta.



Kuva 22. Nortel Contivity 1010:n tehdasasetukset konsolissa

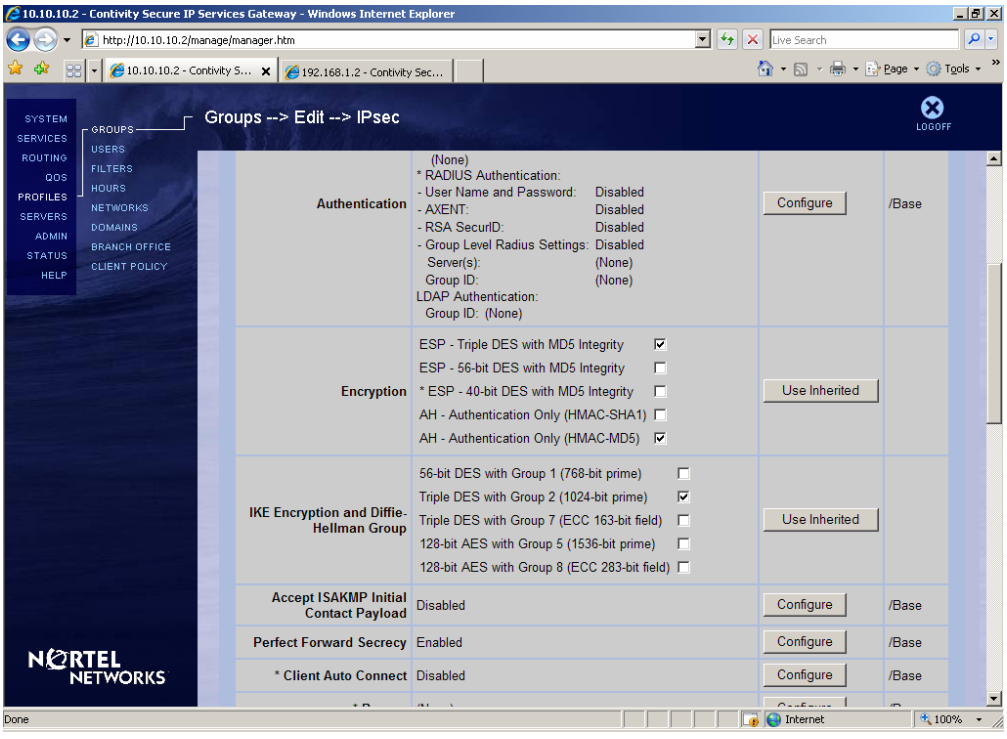
Resetoinnin jälkeen konfigurointi tehtiin internet-selaimessa. Kuvassa 23 reitittimen ulkoverkon IP-osoite asetettiin staattiseksi osoitteeksi 172.27.1.1. Tämä osoite on se, johon VPN-tunnelit päätetään ja mistä ne aloitetaan.



Kuva 23. Nortel Contivity 1010:n ulkoverkon IP-osoitteen määrittely

6.2.3 *Ryhmien ja käyttäjien määrittely*

Ulkoverkon määrittelyn jälkeen oli määriteltävä etäkäyttäjille profiilit, jotta heillä olisi tunnus ja salasana VPN-palveluun. Ensin määritellään käyttäjäryhmä, johon käyttäjät lisätään. Laitteessa on valmiina ryhmä Base, jonka alle muut ryhmät lisätään. Base-ryhmän määritykset periytyvät kaikkiin sen alle tehtyihin ryhmiin. Työssä tehtiin Base-ryhmän alle ryhmä **testgroup**, jonka asetuksista IPSec-asetuksiin tehtiin muutoksia (kuva 24). Reittimen tehdasasetuksiin kuuluu IPSec-ESP:n osalla AES-salaus. Tämä kuitenkin vaihdettiin 3DES-salaukseen. Tiivistefunktiona salauksessa käytettiin MD5:ta. AH-todennukseksi valittiin HMAC-MD5, joten käytössä oli siis todennus ja salaus. IKE-avaintenhallinnan salausalgoritmiksi valittiin myös 3DES, jonka Diffie-Hellman-ryhmäksi otettiin numero 2. Nortel Contivity 1010:n IPSec-asetuksia laitettaessa on huomioitava, että PFS (Perfect Forward Secrecy) ja Compression on asetettava pois käytöstä, jos VPN:ssä käytetään myös jonkin muun laitevalmistajan laitteita. Näin on toimittava, koska ne ovat Nortelin omia siirto- ja pakkausmenetelmiä, joita muiden valmistajien laitteet eivät tunnista.



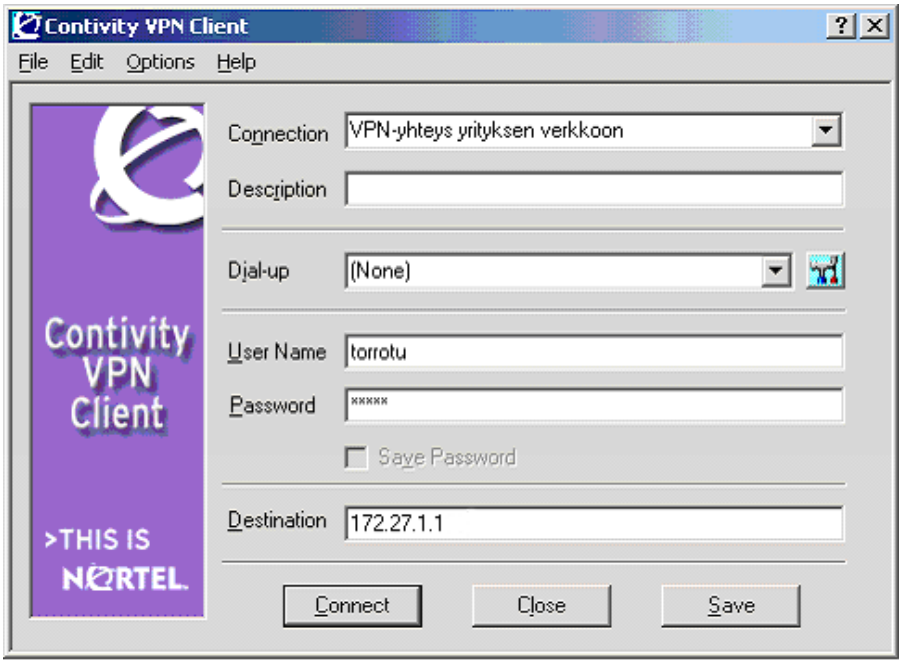
Kuva 24. Käyttäjäryhmän IPSec-asetusten määrittely

Edellä luotuun ryhmään tehtiin tuon jälkeen käyttäjä **torrotu**, jolle luotiin myös salasana. Käyttäjän ryhmän asetuksissa on määritys, että käyttäjät

saavat IP-osoitteensa DHCP:n kautta. Tässä tapauksessa kuitenkin asetettiin käyttäjälle staattinen IP-osoite 192.168.1.50, jonka hän saa aina ottaessaan VPN-yhteyden.

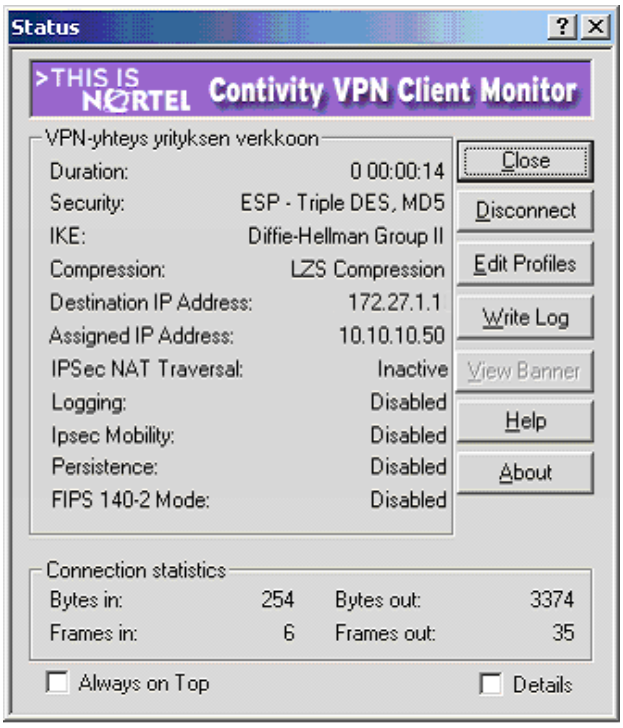
6.2.4 Nortel Contivity VPN Clientin käyttö

Nortel Contivity VPN Clientilla etäkäyttäjät ottavat yhteyden VPN-tunnelin päätepisteeseen eli VPN-reitittimen ulkoverkon IP-osoitteeseen. Tässä tapauksessa yhteys otettiin siis osoitteeseen 172.27.1.1. Lisäksi kirjautumisikkunaan (kuva 25) syötetään hallinnoinnissa tehty tunnus ja salasana. Salasanan tallennusta ei ole mahdollista valita, koska Nortelin VPN-reitittimien tehdasasetuksena on, ettei tallennusta hyväksytä. Hallinnoijan on tietoturvan kannalta järkevä pitää tuo asetus muuttamatta, koska tuolloin koneiden välimuistiin ei jää salasanoja hakkereita varten. Yhteyden nimi on, kuten myös Ciscon clientissa, vain tallennusnimi. Tässäkin yhteydelle annettiin nimi ”VPN-yhteys yrityksen verkkoon”.



Kuva 25. Yhteyden ottaminen Contivity VPN Client:lla

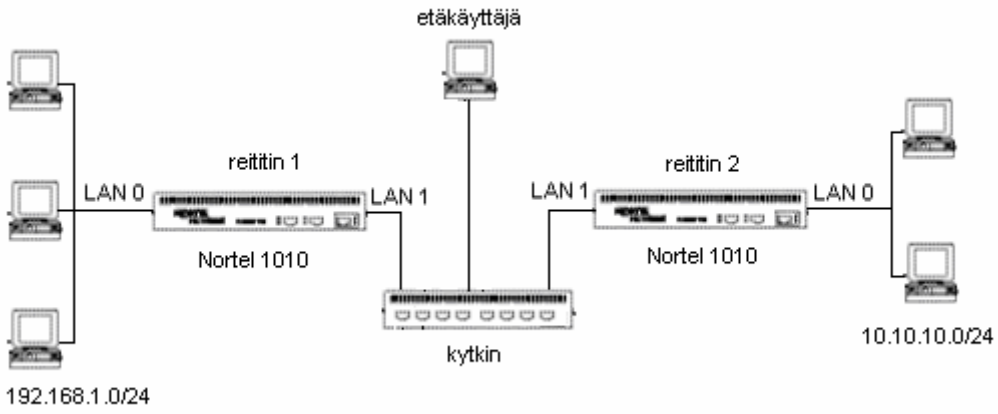
Yhteyden onnistuneen muodostamisen jälkeen etäkäyttäjä voi tarkastella yhteyden tilaa. Kuvan 26 mukaisesti etäkäyttäjä voi tarkastella Nortel Contivity VPN Client Monitorin avulla yhteyden tilaa. Näkyvissä on mm. aiemmin reitittimeen käyttäjäryhmälle määritetty salausalgoritmi, IKE-autentikointi ja IP-osoitteet sekä yhteyden kesto.



Kuva 26. Nortel Contivity VPN Client Monitor

6.2.5 Lähiverkkojen välisen tunnelin määrittely

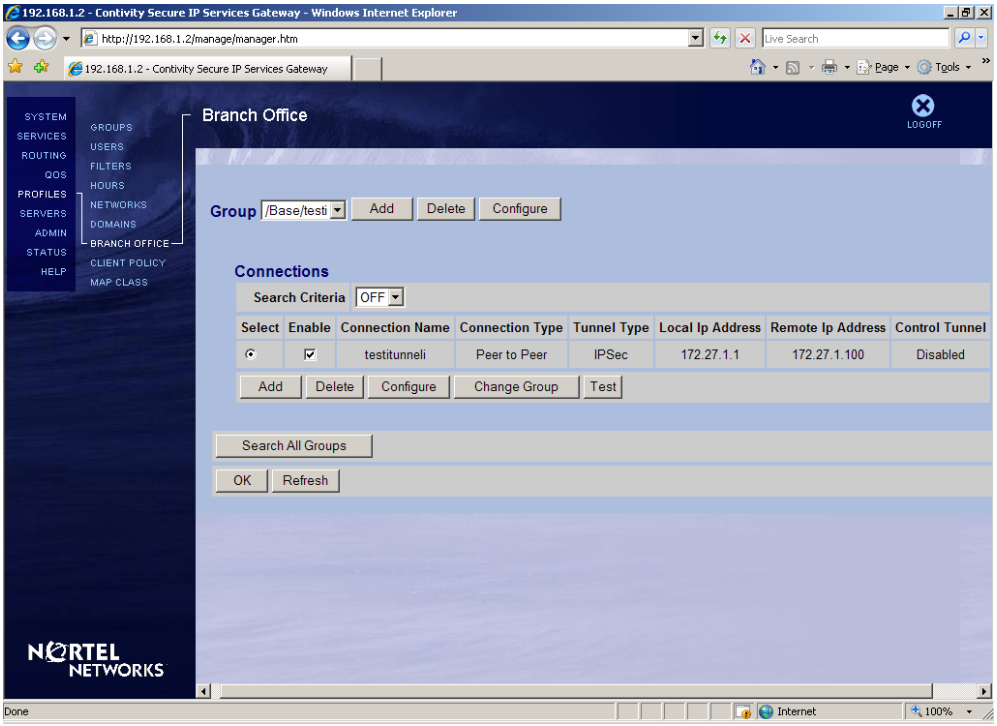
Nortel Contivity 1010 –reititin valittiin työssä jatkotarkastelun alle sen hyvän hallittavuuden ja vahvojen teknisten ominaisuuksien perusteella. Lähiverkkojen välisen (lan-to-lan) tunnelin muodostamista varten otettiin käyttöön kaksi Nortel Contivity 1010 –reititintä, jotka yhditettiin kuvan 27 mukaisesti Nortelin kytkimellä. VPN-tunneli muodostettiin kuvassa näkyvien reitittimien LAN 1-porttien väliin.



Kuva 27. Lähiverkkojen välisen VPN-tunnelin muodostaminen

Kuvan 27 reititin 1:n ulko- ja sisäverkko määritettiin jo aiemmin, joten reititin 2:n vastaavat asetukset määritettiin seuraavaksi. Reitittimen sisäverkon IP-osoitteeksi asetettiin 10.10.10.1 ja hallinta-osoitteeksi 10.10.10.2. Täten sisäverkon käyttäjille jäivät käyttöön osoitteet 10.10.10.3 – 10.10.10.255. Ulkoverkon IP-osoite määritettiin olemaan 172.27.1.100. Näiden määritysten jälkeen oli mahdollista määrittää Branch Office –tunneli lähiverkkojen välille.

Branch Office –tunnelin määrittely aloitettiin luomalla oma ryhmänsä Branch Office –asetuksiin. Base-ryhmän alle tehtiin ryhmä **testi**, jolle asetettiin IPSec-asetukset samalla tavalla kuin normaalille käyttäjäryhmälle kuvassa 24 aiemmin. Tämän jälkeen luotiin tunneli kuvassa 28 näkyvällä tavalla. IPSec-tunnelin nimeksi asetettiin testitunneli ja IP-osoitteet asetettiin vastaamaan reitittimien ulkoverkon osoitteita. Tunnelin määrittelyssä asetettiin myös salausavain (Pre-shared Key). Samat määritykset (Branch Office –ryhmä ja tunnelin asetukset) tehtiin myös reitittimeen 2. Erona tietenkin oli se, että paikallisen (Local Ip Address) ja etäpisteen (Remote Ip Address) IP-osoitteet oli vaihdettava toisinpäin. Tärkeää määrittelyssä oli antaa sama salausavain molempien reitittimien määrittelyihin.



Kuva 28. Branch Office –tunnelin määritykset

Nortel Contivity 1010 –reitittimillä on mahdollista luoda monenkin lähiverkon välisiä tunneleita. Kuvassa 28 näkyvä Test-nappi antoi hyvää tietoa

virheenetsintään tunnelin luonnin aikana. Testi-logista pystyi selvittämään syyn tunnelin toimimattomuuteen.

6.3 Ratkaisujen vertailun yhteenveto

6.3.1 Tekniset ominaisuudet

VPN-ratkaisujen vertailussa selvitettiin teknisten ominaisuuksien, hallittavuuden ja client-ratkaisujen eroavaisuuksia. Teknisiltä ominaisuuksiltaan suurempiin siirtonopeuksiin kykenevä Nortel Contivity 1010 nousi vertailussa kiinnostavimmaksi laitteeksi. Tämän takia sen hallittavuutta testattiin myös lähiverkkojen välisessä (lan-to-lan) ympäristössä käyttämällä kahta VPN-reititintä. Vaikka Nortelin reitittimen hinta on korkeampi, niin täytyy muistaa, että se on kuitenkin pieni hinta ajateltuna siitä saatavia etuja. Nopeammista siirtonopeuksista saatavat hyödyt voivat säästää yrityksen työntekijöiltä paljon aikaa.

6.3.2 Hallittavuus

Hallittavuusominaisuuksiltaan Cisco PIX 501:n etuihin voidaan laskea sen käyttöliittymässä oleva VPN Wizard. Sen avulla VPN:n perusasetukset saadaan asetettua nopeasti. Tämä helpottaa myös aloittelevaa VPN-hallinnoijaa löytämään kaikki tärkeimmät VPN-asetukset heti aluksi. Nortelin hallinnointityökalu toimii hieman monimutkaisemmin, mutta VPN-ammattilaiselle työkalujen käytön erot ovat melko pienet. Nortelin hallintatyökalussa monitorointi eli yhteyksien tarkkailu on hiukan epäselvempää, mutta vianselvityksessä Nortelin testaussysteemi toimii hyvin.

6.3.3 Client-ratkaisut

VPN:n käyttäjälle ratkaisut eivät tee kovin suurta eroa. Käyttäjälle jää molemmissa tapauksissa tiedettäväksi vain yhteysosoite, tunnus ja salasana. Jonkin verran hankaluuksia työssä aiheutti Ciscon VPN Client, joka kaatoi koko etäkäyttökoneen yhteyttä muodostettaessa. Tähän ongelmaan auttoi muiden valmistajien client-ohjelmien poisto. Ciscon VPN clientin vahvuudeksi voidaan mainita VPN-yhteyden tilaikkuna, joka antaa Nortelin vastaavaa tarkemman kuvauksen yhteydestä. Tämä informaatio ei ole etäkäyttäjälle välttämättä kovin mielenkiintoista, mutta hallinnoijalle yhteyden testaamiseen se saattaa olla hyvinkin tärkeää.

7 YHTEENVETO

Tietokoneiden kehitys on ollut viime aikoina nopeaa ja tästä syystä VPN-tekniikan on kehityttävä mukana. Protokollia ja salausmenetelmiä on koko ajan kehitettävä, jotta luottamukselliset tiedot pysyvät oikeissa käsissä. Tässä insinöörityössä keskityttiin VPN-tekniikan teoriaan sekä sen käyttämiseen laitekonfiguraatioissa ja laitteiston vertailussa.

VPN saattaa tuottaa yritykselle suuria liiketoiminnalisia hyötyjä. VPN ei vaadi juurikaan muutoksia yrityksen infrastruktuuriin, koska se käyttää siirtotienään julkista verkkoa eli Internetiä. VPN-ammattilaisten suunnittelemaa VPN:ää voidaan pitää myös turvallisena ratkaisuna yritykselle. Varsinkin IPSecin (Internet Protocol Security) kehittyminen luotetuksi IETF:n (Internet Engineering Task Force) standardoimaksi protokollaperheeksi on lujittanut uskoa VPN:iin.

VIITELUETTELO

[1] Kokkonen, Timo, *Virtuaaliset yksityisverkot*. Helsinki: Edita Oyj. 2001.

[2] Kolesnikov, Oleg, *Building Linux Virtual Private Networks (VPNs)*. Indianapolis: New Riders Publishing. 2002.

[3] Kaario, Kimmo, *TCP/IP-verkot*. Porvoo: Docendo Finland Oy. 2002.

[4] Viestintävirasto, *VPN*. [verkkodokumentti] 11.9.2006 [viitattu 29.4.2007]. Saatavissa: http://www.ficora.fi/index/palvelut/tietoturva/vpn.html

[5] Cisco Systems, *What Is a Virtual Private Network?*. [verkkodokumentti] [viitattu 5.5.2007]. Saatavissa: http://www.ciscopress.com/content/images/1587051796/samplechapter/1587051796content.pdf

[6] The Internet Engineering Task Force, *Point-to-Point Tunneling Protocol*. [verkkodokumentti] 7/1999 [viitattu 6.5.2007]. Saatavissa: http://www.ietf.org/rfc/rfc2637.txt

[7] Shinder, Deb, *Comparing VPN Options*. [verkkodokumentti] 6.4.2005 [viitattu 6.5.2007]. Saatavissa: http://www.windowsecurity.com/articles/VPN-Options.html

[8] Cisco Systems, *Cisco PIX 501 Security Appliance*. [verkkodokumentti] [viitattu 7.6.2007]. Saatavissa: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b18.html

[9] Nortel, *Nortel VPN Router Configuration – Basic Features*. [verkkodokumentti] 2/2007 [viitattu 7.6.2007] Saatavissa: http://www116.nortelnetworks.com/docs/bvdoc/contivity/VPNR_7.0/NN46110-500.pdf

[10] Microsoft Corporation, *Point-to-Point Tunneling Protocol* [verkkodokumentti] [viitattu 13.6.2007] Saatavissa: http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/intwork/inbe_vpn_naxe.mspx?mfr=true

[11] Cisco Systems, *Layer 2 Tunnel Protocol* [verkkodokumentti] 16.1.2003 [viitattu 14.6.2007] Saatavissa: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.htm#19656

[12] Heikkilä Tommi, *Verkonhallintajärjestelmän suojaaminen IPSecin avulla* [verkkodokumentti] 28.10.2002 [viitattu 14.6.2007] Saatavissa: http://tisu.it.jyu.fi/terabitti/20021028-vh-ipsec-gradu-final-2.pdf

[13] The Internet Engineering Task Force, *IP Authentication Header* [verkkodokumentti] 11/1998 [viitattu 14.6.2007] Saatavissa: http://www.ietf.org/rfc/rfc2402.txt

[14] The Internet Engineering Task Force, *The Internet Key Exchange (IKE)* [verkkodokumentti] 11/1998 [viitattu 19.6.2007] Saatavissa: http://www.ietf.org/rfc/rfc2409.txt

[15] U.S Department of Commerce, *Data Encryption Standard (DES)* [verkkodokumentti] 30.12.1993 [viitattu 1.9.2007] Saatavissa: http://www.itl.nist.gov/fipspubs/fip46-2.htm

[16] Viestintävirasto, *Symmetrinen salaus* [verkkodokumentti] 14.9.2006 [viitattu 1.9.2007] Saatavissa: http://www.ficora.fi/index/palvelut/tietoturva/salausmenetelmat/symmetrinensalaus.html

[17] Viestintävirasto, *Epäymmetrinen salaus* [verkkodokumentti] 14.9.2006 [viitattu 1.9.2007] Saatavissa: http://www.ficora.fi/index/palvelut/tietoturva/salausmenetelmat/epasymmetrinensalaus.html

[18] Viestintävirasto, *Tiivistefunktiot* [verkkodokumentti] 14.9.2006 [viitattu 11.9.2007] Saatavissa: http://www.ficora.fi/index/palvelut/tietoturva/salausmenetelmat/tiivistefunktiot.html

[19] The Internet Engineering Task Force, *HMAC: Keyed-Hashing for Message Authentication* [verkkodokumentti] 2/1997 [viitattu 11.9.2007] Saatavissa: http://www.ietf.org/rfc/rfc2104.txt