TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

TUTKINTOTYÖRAPORTTI

Toimipisteiden välisen VPN-toteutuksen suunnittelu

Kimmo Salonen

Tietojenkäsittelyn koulutusohjelma
joulukuu 2005
Työn ohjaaja: Harri Hakonen

TAMPERE 2005

TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

Tekijä: Kimmo Salonen

Koulutusohjelma: Tietojenkäsittely/Tietoverkkopalvelut

Tutkintotyön nimi: Toimipisteiden välisen VPN-toteutuksen suunnittelu

Työn valmistumis-kuukausi ja -vuosi: 12/2005

Työn ohjaaja: Harri Hakonen **Sivumäärä:** 52

TIIVISTELMÄ

Tutkintotyön aiheena oli selvitellä virtuaalisten yksityisverkkojen (Virtual Private Network) toteuttamisen edellytyksiä. Työssä keskityin yritysten toimipisteiden välisien VPN-yhteyksien toteutussuunnitteluun.

Yritysten laajentuessa niiden toimipisteet lisääntyvät ja yritykset haluavat saada tietoturvalliset tietoliikenneyhteydet toimipaikkojensa välille. Kokonaisedullisesti tietoliikenneyhteydet tehdään julkisen tietoverkon yli. Tällöin tietoturva ei ole kattava, sillä julkisessa tietoverkossa ulkopuoliset pääsevät helposti käsiksi siellä liikkuvaan tietoon.

Tutkintotyössä hyödynnettiin IT-alan yrityksen VPN-projektia, jota olin tekemässä. Yritys oli toteuttamassa VPN-yhteyksiä muihin toimipisteisiinsä julkisen tietoverkon välityksellä. Projekti toteutettiin yrityksen ja kolmannen osapuolen välillä.

VPN-yhteyksien toteutusten laajan valikoiman vuoksi on erittäin tärkeää, että niitä tarvitseva yhteisö ottaa tarkasti selvää omista vaatimuksistaan ja peilaa näitä asioita erilaisiin toteutusmahdollisuuksiin, jotta saa valittua kerralla oikean ratkaisun. Yksinkertaiselta kuulostava asia voikin sisältää monia ongelmallisia osa-alueita, ja siksi onkin tärkeää, että on perehdytty perusteellisesti tarpeisiin ja toteutusvaihtoehtoihin.

Avainsanat: virtuaalinen yksityisverkko tietoturva VPN

TAMPERE
POLYTECHNIC

BUSINESS SCHOOL

Author: Kimmo Salonen

Department/Area of specialsation: Business Information Systems

Title: Designing a Virtual Private Network implementation

Month and year: 12/2005

Supervisor: Harri Hakonen **Pages:** 52

ABSTRACT

The aim of this final thesis was to find out different preconditions when designing a Virtual private network implementation. This final thesis concentrates on VPN-connections between a company's different offices.

As companies get bigger and bigger, the number of its branch offices increases. At the same time they want to have secure connections between different offices. And in order to be cost efficient the connections are made through public networks. In these cases the connection is not so secure. In public networks an outsider can access a company's data quite easily.

In this final thesis the data was collected from an IT-company that was implementing VPN-connections between its two offices through the public network. The project was then carried out by a third party.

Because of the wide range of VPN-implementations it's extremely important that the community that needs VPN-connections really examines and identifies its own requirements. After establishing the requirements, it's easier to find the right implementation model. This may sound simple, but it involves many different problematic areas. So it's crucial to get acquainted with the company's needs and implementation options.

Keywords: virtual private network data security VPN

Sisällysluettelo

1 Johdanto

Tietoliikenneverkkojen turvattomuus on ollut viime aikoina paljon esillä ja tulee varmasti vielä tulevaisuudessakin olemaan paljon käsitelty asia viruksien, matojen ja niin yrityksiin kuin kotikäyttäjiinkin kohdistuvien hyökkäyksien vuoksi. Monissa yrityksissä tietoliikenneverkkojen toimivuus on yrityksen elinehto; ilman sitä yritys ei pysty tehokkaasti toimimaan asiakkaidensa ja yhteistyökumppaneidensa kanssa. Yritykset tarjoavat yhteistyökumppaneilleen ja asiakkailleen ekstranet-palveluita, hakevat Internetistä tietoja ja kommunikoivat sähköpostin välityksellä. Kaikki edellä mainitut toiminnot tarvitsevat vakaasti ja luotettavasti toimivan tietoliikenneyhteyden.

Yrityksien laajentuessa on tärkeää, että tietoliikenneyhteydet sivu- ja pääkonttorien välillä toimivat nopeasti ja vaivattomasti. Toimintojen kannalta tärkeät palvelimet ja tiedot säilytetään pääkonttoreiden konesaleissa. Ongelmana sivukonttorien ja etätyöntekijöiden yhdistämisessä päätoimipisteen tietoliikenneverkkoon on se, kuinka tehdä nämä yhteydet julkisen tietoliikenneverkon yli. Tärkeää on myös miettiä kuinka olisi mahdollista säilyttää samantasoinen tietoturva kuin toimittaisiin yrityksen lähiverkossa, vaikka kyseessä onkin kokonaan eri toimipiste.

Nykyisin tulee tietoliikenneyhteyksistä puhuttaessa vastaan yhä useammin termi VPN (Virtual Private Network) – Virtuaalinen yksityisverkko. Termiä käytetään hyvin usein edellä mainittujen tapauksien yhteydessä. Tietoliikenneyhteyksien yleistymisen ohessa on kehitelty tekniikka, miten julkisen tietoliikenneverkon yli luodaan virtuaalisia yksityisverkkoja. Nämä VPN-palvelut mahdollistavat muun muassa pää- ja sivukonttoreiden tietoturvalliset yhteydet.

Tutkintotyön aiheen sain IT-alalla työskentelevältä pk-yritykseltä, joka on tekemässä suunnitelmaa siitä, miten saataisiin tietoturvalliset yhteydet julkisen tietoliikenneverkon (Internet) yli. Työssä haluttiin tuoda esille niitä kohtia, mitä VPN-yhteyksien suunnittelussa pitää ottaa huomioon, jotta oikeanlainen VPN-ratkaisu löytyisi monen vaihtoehdon joukosta. Työ keskittyi VPN-yhteyksien suunnittelussa toimipisteiden välisiin yhteyksiin, joten etäkäyttäjiin kohdistuvat asiat jätettiin huomioimatta suurimmilta osin.

Tutkintotyön aiheen antaneella yrityksellä on toimipisteitä muun muassa Suomessa, Ruotsissa ja Baltian maissa. Tietoturvalliset VPN-yhteydet otetaan käyttöön mahdollisimman nopeasti, jotta kaikki toimipisteet voivat tehokkaasti hyödyntää Suomessa sijaitsevia keskitettyjä IT-palveluita.

2 VPN taustat ja käyttökohteet

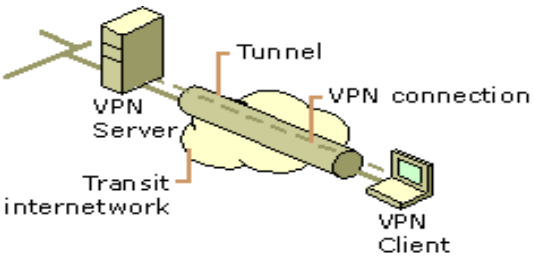
2.1 Taustaa

VPN terminä on ollut käytössä jo pitkän aikaa. Puhelinyhtiöitä houkutteli ajatus käyttää julkisia puhelinverkkoja yksityisen kommunikaation helpottamiseksi. Tämä auttoi puhelinyhtiöiden asiakkaita laajentamaan yksityisiä puhelinverkkojaan kaukana sijaitseviin toimipisteisiinsä. Tällöin alettiin puhua puhe-VPN:stä. Yhdysvalloissa termiä VPN käytettiin alunperin yksityisten puhelinvaihteiden välisien yhteyksien yksityisissä puheverkoissa. 1980-luvulla puhelinyhtiöiden kilpailu kaukoyhteyksien tarjoamisesta johti siis lopulta puhe-VPN:ään. AT&T (American Telephone and Telegraph) kehitti tavan, jolla voitiin muuttaa puhelinvaihteissa käyttävien ohjelmien asetuksia siten, että toimipaikkojen yksityiset numerot korvattiin yrityksen julkisilla numeroilla koko organisaatiossa, eli jokaisessa yrityksen toimipisteessä. Näin uusia kaukopuheluita pystyttiin laskuttamaan vähemmän kuin tavanomaisia kaukopuheluita. (Perlmutter & Zarkower 2001: 30.)

Lyhenne VPN tulee sanoista Virtual Private Network, joka vapaasti suomennettuna tarkoittaa virtuaalista yksityisverkkoa. VPN:ää käytetään yksityisen verkon laajennukseen, jolloin luodaan salattu, suljettu ja luotettavaksi todettu tietoliikenneyhteys julkisten tai jaettujen verkkojen yli. VPN toteuttaa tiedon lähettämisen kahden tietokoneen välillä jäljittelemällä point-to-point yhteyksiä. Lähetetty tieto paketoidaan ja siihen lisätään reititystiedot. Tämä mahdollistaa paketin kulkemisen julkisen tai jaetun verkon yli kohteeseensa. VPN jäljittelee fyysisen yksityisverkon ominaisuuksia salaamalla lähetetyn tiedon eri menetelmin. Datapaketit, jotka joutuvat vääriin käsiin julkisessa tai jaetussa verkossa, eivät ole hyödyllisiä ilman salauksen purkavia salausavaimia. VPN voidaan toteuttaa laitteistolla, ohjelmistolla tai niiden yhdistelmällä. Vaihtoehtoja VPN-toteutuksiin tulee koko ajan lisää.

VPN-toteutukset mahdollistavat yrityksien eri toimipisteiden tai yrityksien yhteistyökumppanien liittymisen yrityksen verkkoon turvallisia ja luotettavia yhteyksiä käyttäen. Julkisen verkon kautta muodostettu VPN-yhteys toimii samalla tavalla kuin yhteyttä varten varattu WAN (Wide Area Network) -yhteys.

VPN mahdollistaa myös käyttäjiensä turvallisen yhteydenoton yrityksen verkkoon matkalta tai käyttäjien kotoa, käyttäen hyväkseen julkista tai jaettua verkkoa. Yhteys on yleensä point-to-point yhteys käyttäjän tietokoneen ja yrityksen palvelimen välillä. Sillä, minkälaista verkkoa yhteydessä hyödynnetään, ei ole käyttäjän kannalta mitään merkitystä. Tiedot kulkevat vain kyseessä olevaa yhteyttä varten luotua virtuaalista yksityistä linjaa pitkin. Alla oleva kuva (kuva 1) kertoo pelkistetysti millainen VPN-yhteys käytännössä on.



*Kuva 1: VPN yhteys julkisen verkon yli (*Microsoft 2004)

2.2 Sähköinen kaupankäynti (Perlmutter & Zarkower 2001: 52-55.)

VPN:än tuloa on vauhdittanut sähköisen kaupankäynnin kasvu. Jo ennen julkisen Internetin laajalle levinnyttä hyväksyntää useat yhtiöt tunnustivat yhtiöidenvälisen sähköisen datasiirron käyttökelpoisuuden. Auto-, lentokone- ja rahoitusteollisuus, samoin kuin organisaatiot, kuten valtionhallinto ja puolustusvoimat, jakavat valtavan määrän paperityötä heidän yhteistyökumppaneistaan koostuvan laajan verkoston kanssa. Tänä päivänä nämä organisaatiot edellyttävät kumppaneiltaan, että he kykenevät tekemään kaupankäyntiä sähköisesti. Joillekin yhtiöille web-pohjaiset sähköiset kaupankäynnin ratkaisut voivat olla vaihtoehto VPN-teknologialle.

Sähköisessä kaupankäynnissä kohti VPN:ää ovat johdattaneet muun muassa EDI VAN, extranetit ja web-pohjainen sähköinen kaupankäynti. Toisaalta myös monet näistä teknologioista voidaan nähdä nykyisin myös VPN:än kilpailijoina.

EDI (Electronic Data Interchange), suomennettuna Organisaatioiden välinen tiedonsiirto, on standardisoitu formaatti, joka on suunniteltu asiakirjoihin, kuten laskuihin ja ostotilauksiin, sisältyvien päivittäisten liiketoimintatietojen vaihtoon. VAN (Value Added Networks), lisäarvoverkot, helpottavat EDI-kykyisten yritysten toimintaa liikekumppaneidensa kanssa. Organisaatio, joka haluaa lähettää sähköisen asiakirjan, voi soittaa VAN:iin EDI-ohjelmiston avulla ja siirtää standardin muotoisen asiakirjan yhteistyökumppanin EDI-postilaatikkoon.

Extranet on yritysten sidosryhmien välinen verkko, joka hyödyntää Internetiä täyttääkseen samoja päämääriä kuin EDI. Extranetiä voivat käyttää asiakkaat, yhteistyökumppanit, jälleenmyyjät tai tavarantoimittajat. Käytännössä extranetiä hyödynnetään kuitenkin huomattavasti laajemmin kuin EDI:ä. EDI on käytännössä vain yksi sovellus. Extranetiin voidaan sijoittaa esimerkiksi tuotedokumentteja, sähköisiä esitteitä, hinnastoja ja tiedotteita. Verratessa extranetiä EDI:in, extranetin tietoja jaetaan laajalla yleisölle, esimerkiksi web-sivujen välityksellä, kun taas EDI on tarkasti rakenteistettu ja tiukasti määritelty ympäristö.

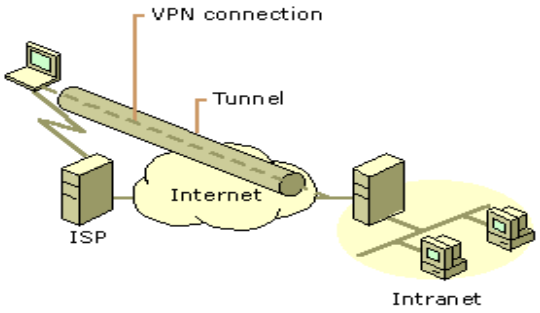
Internetin kasvun ohessa myös web-pohjainen sähköinen kaupankäynti on lisääntynyt. Mahdollisuudet, mitä internetissä voi nykyisin tehdä, tulevat koko ajan monipuolisemmiksi. Kaupankäyntiin liittyen, nykyiset web-selaimet tukevat protokollia, jotka mahdollistavat salatun yhteyden muodostamisen asiakkaan selaimen ja palvelimen välille turvallista tiedonsiirtoa varten. Web-pohjainen rajapinta tarjoaa myös käyttökelpoisen rajapinnan useille yritysten välisille liiketoimille.

2.3 Etäkäyttö

Etäkäyttö ja etätyö ovat lisänneet suosiotaan merkittävästi tietoliikenneyhteyksien parantuessa. Kaikki kuitenkaan eivät ole välttämättä innoissaan tämän suuntaisesta kehityksestä. Yrityksien IT-puolella etäkäytöt ja etätyöt tietävät aina monimutkaisia asioita selvitettäväksi. Tietoturvaan liittyvät asiat tulevat poikkeuksetta ensimmäisenä esille, kun etäkäyttäjät ottavat suoraan yhteyden yrityksen sisäverkkoon. IT-puolen vastaavien onkin varmistettava, että kaikki tulevat yhteydet ovat yhdenmukaisia ja muut, kuten palomuuri- ja käyttöoikeusasetukset, ovat kunnossa. On myös varmistettava, ettei mikään etäkäyttäjän ohjelmistoista pääse vahingoittamaan yrityksen tietojärjestelmiä ja jopa varauduttava ennalta Internet-palveluntarjoajan kautta tapahtuviin yrityksiin päästä yrityksen tietoihin käsiksi. (Symantec 2004.)

Etäkäyttö VPN tarjoaa yhden vaihtoehdon yrityksen sisäverkon etäkäyttömahdollisuuteen julkisen verkon, kuten Internetin, yli tietoturvan ja yksityisyyden säilyttäen. Etäkäyttö VPN:än peruslähtökohtana on tarjota etäkäyttömahdollisuudet toimipisteen ulkopuolelta ja esimerkiksi maailmalla matkustaville työntekijöilleen. Näin etäkäyttäjät pystyvät hyödyntämään yrityksen resursseja mahdollisimman tehokkaasti. (BT 2005.)

Kuvassa 2 on esimerkki ympäristö etäkäyttö VPN-yhteydestä Internetin yli. Kuvassa etäkäyttäjä ottaa yhteyden Internet-yhteyden palveluntarjoajan avulla ja VPN-tunnelia hyväksi käyttäen pääsee käyttämään yrityksen palvelimia ja intranetiä.



*Kuva 2: Etäkäyttö VPN yhteys julkisen verkon yli (*Microsoft 2004)

2.4 Yhdistäminen Internetin yli

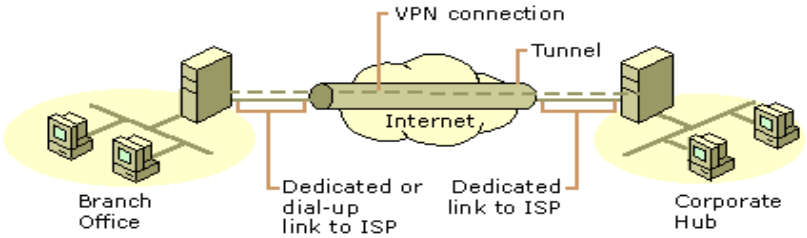
2.4.1 Verkkojen yhdistäminen Internetin yli

Yrityksen kahden eri toimipisteen tietoliikenneverkkojen yhdistämisessä Internetin yli on kaksi vaihtoehtoa. Yhdistämisessä voidaan käyttää joko valintalinjoja tai kiinteitä linjoja.

Valintalinjoja käytettäessä sivutoimipisteen reititin muodostaa yhteyden paikalliseen Internet-yhteyden palveluntarjoajaan sen sijaan, että reititin soittaisi kaukopuhelun yrityksen omaan tai ulkoistettuun NAS (Network Access Server) -palvelimeen. Paikallisen Internet-yhteyden palveluntarjoajan avulla avatun yhteyden yli luodaan VPN-yhteys sivutoimipisteen reitittimen ja päätoimipisteen reitittimen välille, Internetin yli. VPN-palvelimena toimivan yrityksen keskittimen tai reitittimen tulee olla yhdistettynä paikalliseen Internet- palveluntarjoajaan kiinteällä linjalla. Tässä tapauksessa yrityksen VPN-palvelimen tulee kuunnella sisään tulevaa liikennettä 24 tuntia vuorokaudessa.

Kiinteitä linjoja käytettäessä hyväksikäytetään paikallisen Internet-yhteyden palveluntarjoajan yhteyttä; VPN-yhteys pääkonttorin ja sivukonttorin reitittimien välille luodaan Internetin yli. Näin sivukonttorin ja pääkonttorin keskittimiä ei tarvitse yhdistää toisiinsa kalliilla kiinteällä linjalla, vaan reititin yhdistetään Internetiin Internet-yhteyden palveluntarjoajan kautta.

Kuva 3 kuvaa pelkistetysti yrityksen sivutoimipisteen ja päätoimipisteen lähiverkkojen yhdistämisen julkisen verkon, Internetin yli. Yhteys lähiverkkojen välillä kulkee VPN-tunnelia pitkin.



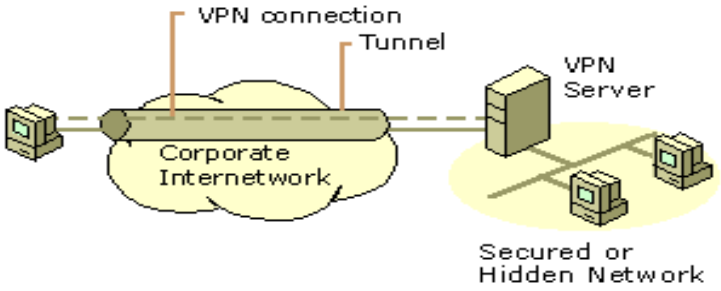
*Kuva 3: Verkkojen yhdistäminen julkisen verkon yli (*Microsoft 2004)

2.4.2 Tietokoneiden yhdistäminen Internetin yli

Joissakin tapauksissa yritysten tiettyjen osastojen tiedot halutaan pitää erillään muusta lähiverkosta. Tällä tavoin yritysten luottamukselliset tiedot eivät pääse leviämään helposti, eikä asiaankuulumattomilla henkilöillä ole pääsyä tähän osaan lähiverkkoa. Tällä tavalla suojataan helposti osaston tiedot, mutta ongelmaksi muodostuu se, että kuinka käyttäjät, jotka eivät ole liittyneenä tämän osaston verkkoon, pääsevät käsiksi tarvitsemiinsa tietoihin. Apua näissä tapauksissa tuo VPN, joka mahdollistaa osastojen verkkojen liittämisen yrityksen verkkoon VPN-palvelimen kautta.

VPN-tekniikka mahdollistaa muun muassa osastojen verkkojen liittämisen yrityksen yhteisverkkoon VPN-palvelimen kautta. Pitää kuitenkin muistaa, että VPN-palvelin ei toimi reitittimenä yrityksen verkkojen välillä vaan ainoastaan VPN-käytössä. Yrityksen yhteisverkkoon liittyneet käyttäjät, joilla on myös käyttöoikeudet sisäverkkoon, voivat avata yhteyden VPN-palvelimen avulla ja käyttää sen kautta osaston suojattuja resursseja. Kaikki VPN-yhteyden kautta kulkevat tiedot voidaan myös suojata salaamalla. Osaston sisäinen verkko pysyy täysin näkymättömänä niille käyttäjille, joilla ei ole sen käyttöön oikeuttavia käyttöoikeuksia.

Seuraavalla sivulla oleva kuva 4 kuvaa pelkistetysti, kuinka yrityksen sisällä voidaan hyödyntää VPN-tekniikkaa ja yhdistää esimerkiksi eri osastojen tietokoneita VPN-tunneleiden avulla.



*Kuva 4: Tietokoneiden yhdistäminen verkon yli (*Microsoft 2004)

3 Tunnelointi

3.1 Tunneloinnin perusteet

Tunnelointi tarkoittaa julkisen verkon, kuten Internetin läpi kulkevaa tietoturvallista tunnelia, jonka VPN-tekniikka on mahdollistanut. Esimerkiksi yritysten eri toimipisteiden välille tehdään VPN:n avulla tunnelointi, jotta kaikki tieto mikä toimipisteiden välillä kulkee ei tulisi muiden julkisen verkon käyttäjien tietoon. Tunnelointi on prosessi, jossa tapahtuu kapselointi ja pakettien lähetys. Prosessi tunnetaan myös nimellä kapselointi. Prosessissa yhteisverkon infrastruktuuria hyödyntämällä voidaan siirtää hyötykuormaa. Hyötykuorma voi olla esimerkiksi jonkin protokollan paketteja tai kehyksiä. Prosessi toimii siten, että kehykset kapseloidaan lisäämällä niihin otsikko, muuten kehys siirrettäisiin lähettäjän määrittämässä muodossa verkon yli. Edellä mainittu otsikko sisältää reititystiedot, joiden perusteella kapseloidut tiedot osataan siirtää julkisen verkon yli. Kapseloidut paketit siirretään tunnelissa päätepisteestä toiseen siirtotienä toimivan verkon yli. Kun kapseloidut paketit saapuvat lopulta tunnelin toiseen päähän, niistä poistetaan ylimääräinen kehys ja paketti ohjataan lopulliseen kohteeseensa.

3.2 Tunnelin luominen ja sulkeminen

Ennen kuin tietoja voidaan esimerkiksi yrityksen kahden toimipisteen välillä siirtää, on luotava tunneli. Jotta tunneli voidaan muodostaa, on sekä tunnelipalvelimen ja -asiakkaan tuettava samaa tunnelointiprotokollaa. Toisessa päässä oleva tunneliasiakas aloittaa tunnelin luomisen, tunnelipalvelin tunnelin toisessa päässä vastaanottaa yhteyspyynnön.

Tunneli päätepisteiden välille luodaan käyttäen prosessia, joka vastaa PPP (Point-to Point Protocol) -yhteyden luomisessa käytettävää prosessia. Tunnelin muodostamiseksi tunnelinpalvelin edellyttää, että tunneliasiakas lähettää kaikki tarvittavat tunnistustiedot. Jos palvelin hyväksyy pyynnön, yhteys tunnelin kautta voidaan luoda ja tietojen siirtäminen voidaan aloittaa. Kun tunneli on muodostettu ja tiedonsiirto tunnelin kautta aloitettu, tunnelin tiedonsiirtoprotokolla kapseloi tunnelin kautta lähetettävät tiedot. Tunneliasiakkaan lähettäessä kapseloitua hyötykuormaa tunnelipalvelimelle, tunneliasiakas lisää paketteihinsa tunnelin tiedonsiirtoprotokollan oman otsikon. Näin ollen kapseloidut kehykset lähetetään siirtoon käytettävän verkon läpi vastaanottavalle tunnelipalvelimelle. Kun tiedot ovat siirtyneet tunnelipalvelimelle, tunnelipalvelin poistaa vastaanottamistaan tiedoista tunnelin tiedonsiirtoprotokollan otsikot ja välittää paketit eteenpäin. Tietojen

lähettäminen myös tunnelipalvelimelta tunneliasiakkaalle tapahtuu täsmälleen samalla tavalla.

3.3 Tunnelin ylläpito

Tunneleita hallitaan ylläpitoprotokollan avulla. Muutamissa tunnelointiteknologioissa, kuten L2TP (Layer 2 Tunneling Protocol) ja PPTP (Point-to-Point Tunneling Protocol), tunneli vastaa istuntoa (session). Tunnelin molempien päätepisteiden on hyväksyttävä tunneli ja tiedettävä sen olemassaolo. Tunneli ei kuitenkaan ole täysin kuin istunto, sillä tunneli ei takaa luotettavaa tiedonsiirtoa pisteestä toiseen. Tiedot tunnelissa siirretään tavallisesti datagram -pohjaisella protokollalla, joka on PPTP:tä käytettäessä TCP (tunnelin hallinta) sekä modifioitu GRE (Generic Routing Encapsulation) ja L2TP:tä käytettäessä UDP (User Datagram Protocol).

Muutamia tunnelointiteknologioita, kuten L2TP:tä ja PPTP:tä käytettäessä, tunnelia on ylläpidettävä sen avaamisen jälkeen. Tunnelin päätepisteiden on tiedettävä toisen pään tila siinä tapauksessa, että pisteiden välille syntyy yhteyskatko. Tunnelin ylläpitäminen tapahtuu tavallisesti säännöllisin väliajoin lähetettävillä kyselyviesteillä tunnelin toiseen päähän. Näitä viestejä lähetään silloin kun muuta siirrettävää tietoa ei ole.

3.4 Tunnelilajit

Tunneleita on kahdenlaisia: pakollisia tunneleita (compulsory tunnels) ja vapaaehtoisia tunneleita (voluntary tunnels). Pakolliset tunnelit voivat olla joko staattisia tai dynaamisia riippuen asiakkaan asetuksista.

3.4.1 Pakolliset tunnelit

Pakolliset tunnelit luodaan ja määritellään aina automaattisesti käyttäjien tietämättä. Käyttäjien ei tarvitse tehdä mitään toimenpiteitä asian suhteen. Pakollisen tunnelin käyttäjän tietokone ei ole tunnelin päätepiste, vaan tunnelin päätepisteenä on jokin toinen tietokone, joka on asiakastietokoneen ja tunnelipalvelimen välissä. Tämä tietokone toimii tunneliasiakkaana.

Jos asiakastietokoneeseen ei kuitenkaan ole asennettu tunnelointiprotokollaa, mutta tunnelointia toivotaan, on mahdollista, että joku toinen tietokone tai verkon muu laite luo tunnelin asiakastietokoneen puolesta. Tällaista laitetta kutsutaan etäkäyttökeskittimeksi. Jotta keskitin pystyisi suoriutumaan tehtävästään, siihen on oltava asennettuna asiaan kuuluva

tunnelointiprotokolla. Keskittimen tulee pystyä muodostamaan tunneli kun asiakastietokone avaa yhteyden.
Kun asiakastietokone ottaa yhteyden Internetin kautta, se soittaa Internet-palveluntarjoajan tunnelointia suorittavalle NAS-palvelimelle. Yritys on esimerkiksi sopinut Internet- palveluntarjoajan kanssa siitä, että yritys saa hyödyntääkseen koko maan laajuisen etäkäyttökeskittimien verkoston. Verkostoon kuuluvat keskittimet voivat muodostaa tunneleita Internetin yli yrityksen omaan verkkoon liitettyihin tunnelipalvelimiin. Kyseessä olevaa menettelyä kutsutaan siis pakolliseksi tunneloinniksi, koska tunneliasiakkaan on käytettävä etäkäyttökeskittimien luomia tunneleita. Pakollista tunnelointia käytettäessä asiakastietokone muodostaa vain yhden PPP-yhteyden ja tunneli luodaan silloin kun asiakas soittaa NAS-palvelimelle. Kun yhteys on muodostettu, kaikki liikenne asiakkaan verkosta ja takaisinpäin kulkee automaattisesti tunnelin läpi.

3.4.2 Staattiset pakolliset tunnelit

Staattiset pakolliset tunnelit tarvitsevat toimiakseen staattisia tunnelikonfiguraatioita. Staattiset tunnelikonfiguraatiot vaativat yleensä tähän tehtävään tarkoitettuja laitteita (automaattiset tunnelit) tai manuaalista konfigurointia (aluepohjaiset tunnelit).

Automaattinen tunnelointi toimii siten, että kaikki etäkäyttökeskittimen valintalinja-asiakkaat voidaan tunneloida automaattisesti tiettyyn käytettävissä olevaan tunnelipalvelimeen. Tämä taas edellyttää asiakkaalta kiinteitä linjoja paikallisella tasolla ja tietoliikenneverkko-liitäntälaitteita. Käytännössä automaattinen tunnelointi toimii esimerkiksi siten, että käyttäjät soittavat tiettyyn puhelinnumeroon, jonka avulla he luovat yhteyden etäkäyttökeskittimeen, joka tunneloi yhteyden automaattisesti tiettyyn tunnelipalvelimeen.

Aluepohjaisessa tunneloinnissa taas etäkäyttökeskitin tutkii osan käyttäjän nimestä voidakseen päättää, mihin käyttäjää koskeva liikenne tunneloidaan. Esimerkiksi eri alueiden käyttäjät tunneloidaan eri kohteisiin. Aluepohjaisen tunneloinnin toteuttaminen on kohtalaisen helppoa, sillä se ei edellytä mitään erityisiä laitteita ja sen hallinnointi konfiguroinnin jälkeen vaatii vain vähän työtä. Toisaalta olemassa olevan konfiguroinnin muuttaminen voi olla aikaa vievää ja kallista. Tämän lisäksi kaikkien samaan alueeseen kuuluvien käyttäjien mahdollinen liikenne tunneloidaan samaan kohteeseen.

3.4.3 Dynaamiset pakolliset tunnelit

Dynaaminen pakollinen tunnelointi toimii siten, että tunneloinnissa tunnelin kohde valitaan aina tapauskohtaisesti sen jälkeen kun käyttäjä luo yhteyden etäkäyttökeskittimeen. Samalta alueelta yhteyden ottaneet käyttäjät voidaan tunneloida eri kohteisiin sellaisten parametrien, kuten käyttäjän nimen, osaston, sijaintipaikan, soitetun tai soittajan puhelinnumeron perusteella. Dynaaminen tunnelointi tarjoaa suurimmat muuntelumahdollisuudet pakollisista tunnelointimenetelmistä.

Etäkäyttökeskittimet, joita käytetään dynaamisessa tunneloinnissa, voivat olla esimerkiksi monikäyttöisiä NAS-palvelimia, joihin voivat kytkeytyä sekä tavalliset Internet-asiakkaat (ei tunneloidut) että tunnelointiasiakkaat. Erityistä puhelinlinjaa tai etäkäyttökeskitintä ei tarvita. Etäkäyttökeskittimet tietävät tietokantaan tallennettujen tietojen perusteella tunneloidaanko asiakkaan liikenne vai ei.

Dynaaminen pakollinen tunnelointi ei ole hallinnallisesti helposti skaalautuva, koska jokaisella etäkäyttökeskittimellä voi olla oma käyttäjätiedot sisältävä tietokanta. Ratkaisua voi parantaa tallentamalla käyttäjien tiedot keskitetysti ja ohjata etäkäyttökeskittimet tiedustelemaan tarvitsemansa tiedot sieltä mihin ne on keskitetysti tallennettu, kun valintalinja- asiakas soittaa.

3.4.4 Vapaaehtoiset tunnelit

Vapaaehtoiset tunnelit luodaan ja määritellään aina tunnelin asiakastietokoneen käyttäjän toimesta. Käyttäjän tietokone toimii tunneliasiakkaana ja se on tunnelin päätepisteessä.

Vapaaehtoinen tunnelointi aloitetaan sillä, että asiakastietokone tarjoutuu luomaan tunnelipalvelimeen johtavan tunnelin. Jotta tunneli voidaan muodostaa, tunneliasiakkaana toimivaan tietokoneeseen on oltava asennettuna tarvittava tunnelointiprotokolla.

Vapaaehtoinen tunnelointi toimii seuraavissa tilanteissa:

1. Asiakkaalla on yhteys toimivaan tietoliikenneverkkoon, joka pystyy reitittämään kapseloidut paketit asiakastietokoneen ja sen haluaman tunnelipalvelimen välillä.
2. Asiakas voi joutua muodostamaan yhteyden siirtoverkkoon, valintalinjaa käyttäen, ennen kuin tunneliasiakas voi luoda yhteyden. Esimerkkinä tällaisesta tilanteesta on valintalinjan kautta Internetiin yhdistyvä käyttäjä. Internet- käyttäjien on avattava yhteys palveluntarjoajaan, ennen kuin Internetin läpi kulkeva tunneli voidaan luoda.

4 VPN Protokollat

VPN tunnelointi on kehysten tai pakettien kapselointia toisten kehysten tai pakettien sisään. Käytännössä on kuitenkin tärkeää muistaa, että tunnelit eivät ole VPN:iä ja VPN:ät eivät ole tunneleita. VPN-tunnelit toteutetaan VPN-tunnelointiprotokollien avulla, joista seuraavissa kappaleissa on kerätty muutamia tärkeitä seikkoja. Tällä hetkellä kolme protokollaa, IPSec (IP Security), L2TP ja PPTP ovat käytössä suosituimpia. (Perlmutter & Zarkower 2001.)

4.1 IPSec

Perlmutterin ja Zarkowerin (2001:106) mukaan yleisesti IPSec:iin viitataan protokollana, vaikka IPSec on todellisuudessa protokollien kokoelma. Nämä protokollat ovat määritelty IETF:n RFC- asiakirjoissa (Request for Comments) ja määrittelyluonnoksissa, ja niitä valvoo IETF:n IPSec Working Group. Vuonna 2001 IPSec-protokolla koostui yli neljästäkymmenestä RFC:stä ja luonnoksesta.

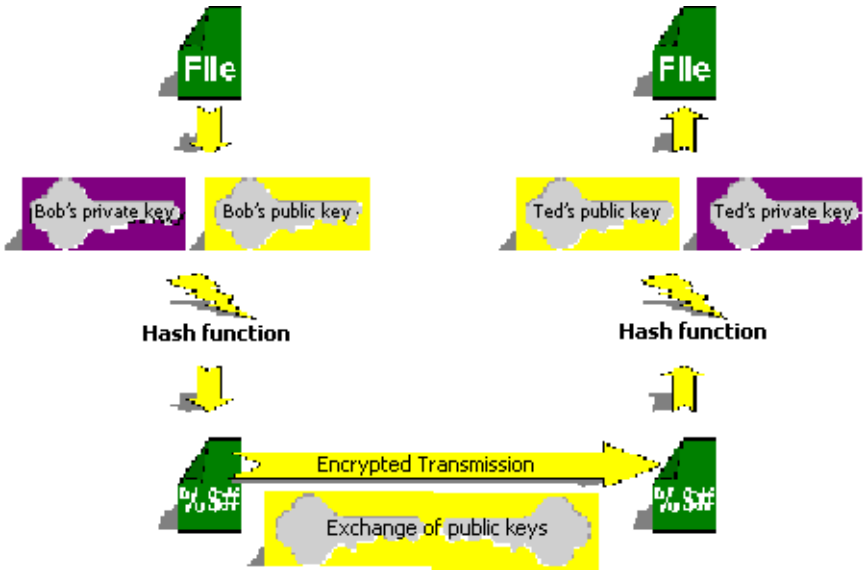
4.1.1 IPSec:in toiminta

IPSec tarjoaa IP (Internet Protocol) -paketeille luottamuksellisuuden ja koskemattomuuden. Sen peruspilareina ovat salaus, todennus ja avaimenhallinta. IPSec-toiminnassa on aina lähettäjä ja vastaanottoja. Nämä osapuolet muodostavat niin sanotun turvallisuusliiton. Turvallisuusliittoa hyväksi käyttäen koneet varmistavat turvallisen tiedon siirron. (Perlmutter & Zarkower 2001.)

IPSec toiminta on lyhyesti selitettynä seuraavanlainen. Ensimmäisenä tapahtumana toiminnassa on se, että vastaanottajan ja lähettäjän on saatava käyttöönsä yhteinen avain. Yhteisen avaimen saamiseksi osapuolien on käytettävä jotain IPSec:in tukemaa menetelmää. Avain voidaan ottaa käyttöön dynaamisesti tai manuaalisesti, staattisen konfiguraation kautta.

Kun sekä vastaanottajalla että lähettäjällä on identtiset avaimet, turvallisuusliitto on voimassa. Yhteisen avaimen avulla lähettäjä luo digitaalisen allekirjoituksen, jonka voi lukea vain ja ainoastaan oikealla avaimella varustettu vastaanottaja. Identtisten avainten avulla sekä lähettäjä että vastaanottaja myös avaavat salakirjoituksen. Salakirjoitukseen liittyviä salausalgoritmeja on monia ja niistä suosituimpia ovat DES, 3DES ja RC4. Salauksen jälkeen lähettäjä lähettää turvatun paketin julkisen verkon yli määräpaikkaansa. Kun vastaanottaja toisessa päässä saa paketin, se käyttää yhteistä avainta ja

suorittaa algoritmin käänteisessä järjestyksessä. Samalla se muuntaa datan alkuperäisen kaltaiseen, selväkieliseen kirjoitusmuotoonsa. Vastaanottajan ollessa VPN-sovellus tai VPN-käyttöön tarkoitettu laite, se on vastuussa useiden IPSec-turvallisuusliittojen hoitamisesta. Sovelluksen tai laitteen on pidettävä avaimille ja algoritmeille tietokantaa, joista yksi kuuluu yhdelle assosiaatiolle. Kyseinen vaatimus täytyy muistaa ottaa huomioon aihetta suunniteltaessa. Sovellus tai laite voi joutua hallitsemaan satoja tai jopa tuhansia samanaikaisia turvallisuusliittoja. (Perlmutter & Zarkower 2001.)



Kuva 5. Avainten käyttö IPSec-liikenteessä (Netopia 2005)

4.1.2 IPSec ESP Tunnel ja IPSec ESP Transport

RFC 1826:ssa määritellyn ESP (Encapsulating Security Payload)-protokollan avulla IPSec tukee tietosähkeiden salausta. Tätä menetelmää kutsutaankin yleisesti nimellä IPSec ESP. ESP:llä on kaksi toimintatilaa, Tunnel ja Transport -tila. (Perlmutter & Zarkower 2001:107.)

Isoin ero ESP Transport ja ESP Tunnel -tilan välillä on se, että ESP Tunnel-tilassa käytetään kapseloitua IP-otsikkoa. Tämän IP-otsikon ansiosta tunnelissa oleva paketti voidaan reitittää lopulliseen määränpaikkaansa, kun IPSec-salaus ja kapselointi on poistettu. IPSec Transport-tilassa paketin salaus puretaan, kun paketti saapuu kohteeseensa.

ESP:n Transport ja Tunnel -tilan erot voidaan tiivistää seuraaviin kohtiin:
- Transport-tila vain lisää ESP-otsakkeen alkuperäiseen pakettiotsakkeeseen, ennen kuin se välitetään eteenpäin.
- Tunnel-tila kapseloi alkuperäisen IP-paketin, muodostaen täysin uuden paketin, jonka kuormana on alkuperäinen paketti. (Perlmutter & Zarkower 2001:107.)

4.1.3 IPSec:in edut ja rajoitukset

IPSec on todella suosittu VPN-tunnelointiprotokollana. Se on itse asiassa suosituin VPN:ssä käytettävistä lähestymistavoista Layer 3 -tunnelointiin. Suosituimmuuteen ei ole mitään yksittäistä syytä. Yksi hyvä syy on se, että IPSec tukee sisäänrakennettua salausta ja on todellisuudessa hyvin joustava salauksen toteutuksen suhteen. IPSec ei myöskään määrää mitään tiettyä salausalgoritmia vaan määrittelee ainoastaan formaatin jota salausotsake käyttää. Varsinkin salausalgoritmin vapaus on tehnyt IPSec:stä suositun VPN-ratkaisujen kehittäjien piirissä. He ovat hyödyntäneet tätä joustavuutta käyttämällä IPSec:iä VPN-kehittämisensä perusosana. IPSec:in etuihin voidaan myös lukea se, että IPSec hyödyntää IP:tä ja useimmat sovellukset toimivat tällä hetkellä IP-verkkojen välityksellä. Eikä myöskään sovi unohtaa laajaa kehittämis- ja standardisointityötä mitä tehdään ja mitä on tehty IPSec:in ympärillä. Myös tulevaisuutta ajatellen IPSec on hyvin käyttökelpoinen, sillä IPSec-otsakkeet on sisäänrakennettu Ipv6- pakettiformaattiin, joka puolestaan varmistaa IPSec käyttökelpoisuuden pitkälle tulevaisuuteen. (Perlmutter & Zarkower 2001:113.)

IPSec:in rajoituksia ovat yhteensopimattomuus ja se, että IPSec ei kohdistu muihin verkkoprotokolliin kuin IP:hen. Useat saatavissa olevat IPSec:in versioista eivät ole yhteensopivia eri toimittajien välillä. Saatavilla on monia vaihtoehtoja muun muassa avaimenhallintaan, salaukseen ja todennukseen. IPSec:in kohdistumattomuutta muihin kuin IP-protokollaan ei nähdä suurena ongelma, koska nykyisin useimmat sovellukset ovat kuitenkin tehty toimimaan IP-verkkojen välityksellä. Jos kuitenkin muita protokollia, esimerkiksi IPX/SPX tai AppleTalk, halutaan suojella IPSec:in avulla, on liikenne ensin tunneloitava IP:n sisälle. (Perlmutter & Zarkower 2001:114.)

4.1.4 Yhteenveto

IPSec on kolmannen tason VPN-tunnelointiprotokolla, joka tukee suojattua tiedonsiirtoa IP-verkoissa. IPSec ESP Tunnel-tilassa on mahdollista kokonaisten IP-tietosähkeiden salaaminen ja kapselointi, sekä turvallinen lähetys yksityisen tai julkisen IP-verkon kautta.

IPSec VPN-tunnelointiprotokollaa kannattaa miettiä kun:

- Halutaan varmaa yhteistoimivuutta muiden VPN-ratkaisujen valmistajien kanssa.
- Ei ole mitään tarvetta kapseloida useita protokollia.
- Halutaan hyödyntää yksittäistä laitetta huolehtimaan turvallisuudesta. Markkinoilta löytyy useita IPSec-sovelluksia ja laitteita, jotka tukevat lähiverkkojen välistä VPN:ää.
- Sisäänrakennettu turvallisuus on erittäin tärkeää, IPSec sisältää sisäänrakennetun todennuksen ja salauksen.
  (Perlmutter & Zarkower 2001: 114.)

4.2 L2TP

L2TP on verkkoprotokolla, joka kapseloi IP-, Frame Relay- ja ATM-verkkojen kautta lähetettävät PPP-kehykset. Internetissä L2TP-protokollaa voidaan hyödyntää tunnelointiprotokollana, kun tietosähkeiden siirtoon käytetään IP-protokollaa. Lisäksi L2TP verkkoprotokollaa voidaan käyttää myös yksityisten lähiverkkojen välisissä yhteyksissä. L2TP on Cisco Corporation-yhtiön kehittämän L2F (Layer 2 Forwarding) -teknologian ja PPTP:n yhdistelmä. L2TP:ssä yhdistyvät L2F:n ja PPTP:n parhaat ominaisuudet.

4.2.1 L2TP:n toiminta

Perlmutterin ja Zarkowerin (2001: 129) mukaan L2TP vastaa toiminnoiltaan suurimmilta osin PPTP:tä. L2TP-asiakkaan ja L2TP-palvelimen väliin luodaan L2TP-tunneli. Asiakas voi olla esimerkiksi liittyneenä lähiverkkoon, jonka kautta luodaan yhteys tunnelipalvelimeen tai käyttäjä joutuu luomaan IP-yhteyden NAS-palvelimeen muuta kautta. L2TP-tunnelia luotaessa tehdään samanlainen tunnistus kuin PPP-yhteyksiä luotaessa (EAP, CHAP, MS-CHAP ja PAP). L2TP onkin perinyt PPP:n käyttämän pakkausmenetelmän, mutta ei PPP:n salausmenetelmää. L2TP käyttää tietojen salaukseen IPSec:iä. PPP-salauksen käyttämistä yhdessä IPSec:in kanssa lisäisi prosessointikuormaa antamatta mitään merkittäviä etuja. Tunnelin ylläpidossa L2TP käyttää UDP:tä ja erityisiä L2TP-pohjaisia viestejä. Toisin kuin PPTP, joka käyttää TCP-istuntoa komento- ja valvontapakettien kuljetukseen, L2TP ei tee mitään eroa pakettien välillä, vaan kaikki paketit ovat UDP-kapseloituja. (Perlmutter & Zarkower 2001: 129.)

4.2.2 L2TP:n edut ja rajoitukset

Suurimmat ongelmat L2TP-protokollan toiminnassa liittyvät sen suorituskykyyn ja laajennettavuuteen. Verrattuna muihin protokolliin se jää selvästi muista jälkeen edellä mainituilla osa-alueilla. Lisäksi yhtenä tämän protokollan ongelmana on ollut myös sen versioiden paljous. Useita eri versioita on ollut saatavilla, mutta pieni määrä eri versioita on toteuttanut protokollaa kokonaisuudessaan. Versioiden paljous on huono asia ajatellen yhteensopivuutta. (Perlmutter & Zarkower 2001: 133.)

L2TP-protokollan hyvänä puolena voidaan pitää muun muassa sitä, että tämä protokolla on erittäin laaja-alaisesti tuettu. Tuella tarkoitetaan sitä, että on olemassa useita IETF-määrittelyluonnoksia, jotka suosittelevat ehdotettuja parannuksia L2TP:aan. (Perlmutter & Zarkower 2001: 134.)

4.2.3 Yhteenveto

Vaikka L2TP-protokollassa onkin tiettyjä rajoituksia, se ei silti ole mikään huono tunnelointiprotokolla. Perlmutterin ja Zarkowerin (2001) mukaan L2TP:n laaja-alainen tuki on esimerkiksi erittäin tärkeä asia. IETF määrittelyluonnoksista löytää esimerkiksi palvelunlaatuun (QOS) liittyvät ehdotukset. Lisäksi ensimmäisien versioiden ongelmat, liittyen puutteellisuuteen ja kypsymättömyyteen, ovat poistuneet suurimmilta osin nykyisestä versiosta. (Perlmutter & Zarkower 2001: 134.)

4.3 PPTP

PPTP suunniteltiin alunperin helpottamaan tiedon siirtoa etäasiakkaalta yksityiselle yrityspalvelimelle käyttäen Internet-yhteysinfrastruktuuria yhteisenä kuljetustienä. PPTP on PPP-protokollan laajennus, joka kapseloi PPP-kehykset IP-tietosähkeiksi IP-verkon, kuten Internetin, välityksellä tapahtuvaa tiedonsiirtoa varten. PPTP:n suunnitteli ja kehitti alunperin ryhmä insinöörejä monesta eri alan yrityksestä, kuten Microsoftilta, Ascend Communicationilta ja 3Comilta. PPTP on ollut erittäin laajalti käytössä VPN-maailmassa. (Perlmutter & Zarkower 2001: 114-115.)

PPTP käyttää TCP-protokollaa tunneleiden ylläpitoon ja se hyödyntää modifioidulla GRE-protokollalla kapseloituja PPP-kehyksiä tiedon-siirtoon.

4.3.1 PPTP toiminta

PPTP:llä on muutamia erilaisia toteuttamismalleja. PPTP käyttää palvelimelta asiakkaalle-arkkitehtuuria. Palvelimen ja asiakkaan määrittely on kuitenkin jätetty erilaisien toteutuksien varaan. Kolme yleisintä mallia PPTP:n toteuttamiseksi on asiakas-palvelin, RAS-palvelin ja palvelin-palvelin. (Perlmutter & Zarkower 2001: 116.)

PPTP käyttää muutamaa pakettia liikennöintiin. PPTP käyttää muun muassa valvontapaketteja ja datapaketteja. Datapaketit sisältävät varsinaisen käyttäjädatan. Paketit on kapseloitu käyttämällä GRE-protokollaa. Kontrolli- eli valvontapaketteja PPTP käyttää tilan-tiedusteluun ja merkinantoon. Kontrollipaketit kulkevat TCP-istunnon välityksellä, joka on luotu tunnelin päätepisteinä toimivien laitteiden välille. (Perlmutter & Zarkower 2001: 116.)

Jotta PPTP-tunneli voitaisiin aloittaa, PPTP-asiakkaan täytyy ensiksi muodostaa TCP-istunto palvelimen kanssa. Kun TCP-istunto on käynnistetty, PPTP-kontrolliviestejä voidaan lähettää palvelimen ja asiakkaan välillä. Näitä kontrolliviestejä käytetään tunnelin toiminnan eri tehtäviin. Kun tunneli on onnistuneesti aloitettu, GRE-kapseloidut datapaketit voivat kulkea kumpaankin suuntaan tämän saman palvelimen ja asiakkaan välisen tunnelin välityksellä. Kun käyttäjä on lopettanut, PPTP-asiakas lähettää kontrollipaketin palvelimelle, joka lopettaa istunnon ja purkaa PPTP-tunnelin. (Perlmutter & Zarkower 2001: 116.)

4.3.2 PPTP edut ja rajoitukset

Samoin kuin IPSec:in kohdalla, on olemassa monia tapoja toteuttaa PPTP. Koska PPTP kapseloi kokonaisen PPP-kehyksen, PPTP voi tukea useita verkkoprotokollia, joita voidaan kuljettaa PPP:n avulla. Tällä tarkoitetaan sitä, että PPTP on hyvin joustava protokolla. Tarkasteltaessa PPTP:tä hieman tarkemmin huomataan sen joustavuus myös muilla tavoin. PPTP:tä voidaan käyttää lähiverkoissa, laajan alueen verkoissa ja soittoyhteyksissä. Lisäksi PPTP:tä voidaan käyttää myös Internetissä tai missä tahansa muussa TCP/IP-pohjaisessa verkossa, huolimatta siitä onko verkko julkinen tai yksityinen. (Perlmutter & Zarkower 2001: 115-116.)

Vaikka PPTP onkin hyvin pätevä VPN-tunnelointiprotokolla, sillä on muutamia puutteita ja tiettyjä huomioitavia yleisiä asioita.

PPTP:n turvallisuusongelmat

Eräs turvallisuuskonsultti julkaisi jo kesällä 1998 raportin PPTP:n turvallisuudesta. Raportista kävi ilmi muutamia turvallisuusaukkoja

Microsoftin PPTP-versiossa. Turvallisuusaukkoja silloin oli muun muassa:

- Heikko todennus, koska PPTP-asiakkaan autentikointiin käytetään ainoastaan CHAP-protokollaa.
- Autentikoimattomat TCP-paketit, jotka jättävät VPN:n avoimeksi DoS (Denial Of Service) -hyökkäyksille.
- Huono salaus, jossa käytetään helposti murrettavia avaimia. Ongelmat perustuvat käyttäjien helposti hankittaviin salasanoihin. Myös salausalgoritmissä havaittiin puutteita.
  (Perlmutter & Zarkower 2001: 123.)

PPTP:n useisiin protokolliin liittyvät ongelmat

Vaikka PPTP tunneloi PPP:n, joka itsessään tukee monia protokollia, useimmat toteutukset eivät vielä tue kuormanaan muita kuin IPX:ää tai IP:tä. (Perlmutter & Zarkower 2001: 124.)

PPTP:n suorituskykyongelmat

PPTP:llä saattaa olla suorituskykyongelmia korkeiden saantiviiveiden verkoissa. Tähän on monia syitä. Yksi syy on esimerkiksi TCP:n käyttö PPTP:n valvontapaketeissa. Toisaalta asian liittyen on julkistettu päivityksiä, jotka ovat kasvattaneet vastaanottoon käytetyn ikkunan koon oletusarvoa ja lisänneet mahdollisuuden käyttää salausta ja pakkaamista paketti paketilta. (Perlmutter & Zarkower 2001: 122-123.)

PPTP:n laajennettavuusongelmat

Yleensä PPTP-verkkopalvelinta käytetään sekä PPTP-tunneleiden että PPP-istuntojen päättämiseen. PPP:n ja sen tarvitsemien tai käyttämien optioiden päättämiseen asettamat vaatimukset ovat huomattavat. Pelkästään PPP-istuntojen hallinnointiin verkkopalvelimilta menee niin paljon resursseja, ettei palvelimelta enää riitä resursseja hoitamaan niitä käyttäjiä, jotka vaativat samanaikaisesti yhdistettävyyttä PPTP:n välityksellä. (Perlmutter & Zarkower 2001: 123.)

4.3.3 Yhteenveto

Jos turvallisuus, suorituskyky ja laajennettavuus nähdään tietoliikenne-verkolle vähemmän tärkeinä ominaisuuksina, niin kannattaa miettiä PPTP:n valintaa VPN-protokollaksi. PPTP on valinta kun vaatimuksena on IP ja/tai IPX -liikenteen kuljettaminen. Toisaalta jos Microsoftin asema myyjänä nähdään tärkeänä ja halutaan käyttää laajalti levinnyttä ja kypsää teknologiaa, on PPTP ratkaisu VPN-protokollaksi. (Perlmutter & Zarkower 2001: 124.)

4.4 GRE

GRE-protokolla (General Routing Encapsulation) on vuonna 1994 luotu tunnelointiprotokolla. Tätä protokollaa pidetään yhtenä tunnelointiprotokollien edelläkävijöistä. GRE-protokollaa käytetään kapseloimaan toisia tunnelointiprotokollia, kuten ATMP:tä, BayDVS:ää ja PPTP:tä. GRE syntyi, koska sen tekijöiden mielestä toiset varhaiset kapselointiprotokollat olivat liian tarkkoja kyvyssään hoitaa useita erilaisia datakuormien tyyppejä. Yksi GRE-protokollan hyvä puoli oli se, että se sisälsi sisäänrakennetun kyvyn autentikoida ja tunnistaa GRE-paketin lähteen. (Perlmutter & Zarkower 2001: 134-135.)

4.5 Muita VPN-protokollia

Kiinnostavin puoli seuraavissa kolmessa esitettävässä protokollassa on se, että ne kaikki muistuttavat toisiaan ja nämä kolme protokollaa perustuvat viime kädessä, suoraan tai välillisesti, Mobile-IP:hen. Mobile-IP on protokolla, joka kehitettiin laajentamaan olemassa olevaa Internet-protokollaa siten, että mahdollistettaisiin kannettavan tietokoneen siirtäminen verkosta toiseen ilman sen IP-osoitteiden muuttamista ja ilman olemassa olevien yhteyksin purkautumista. Kaikki kolme protokollaa ovat laajentaneet Mobile-IP-protokollaa siten, että se sopisi paremmin heidän protokollansa tarpeisiin. Kaikki kolme protokollaa käyttävät RADIUS-pohjaista pakollista tunnelointia ja kyseessä olevia protokollia tavallisesti käytetään tarjoajamallisissa VPN-palveluissa. Lisäksi kaikki kolme protokollaa ovat niitä erityisesti markkinoivien tahojen yksinoikeuden piirissä. (Perlmutter & Zarkower 2001: 136/138.)

Protokollat ovat:
- VTP (Virtual Tunneling Protocol)
- ATMP (Ascend Tunnel Management Protocol)
- BayDVS (Bay Dial VPN Services)

4.5.1 VTP

VTP, virtuaalinen tunnelointiprotokolla, on Layer 3-tunnelointimenetelmä, jonka Bay Networksin ja US Roboticsin insinöörit keksivät vuonna 1996. Vaikka Bay Networks ja US Robotics yhdessä kehittivät kyseessä olevan tunnelointiprotokollan, niin vain US Robotics päätyi käyttämään sitä ja Bay Networks siirtyi kehittämään BayDVS:ää. Erot VTP:n ja BayDVS:n välillä ovat erittäin pieniä, ja aivan kuten BayDVS ja ATMP, myös VTP perustuu Mobile-IP:hen. (Perlmutter & Zarkower 2001: 139.)

4.5.2 ATMP

ATMP tunnelointiprotokollan on ainoana toteuttanut Ascend Communications. ATMP on Mobile-IP-protokollan tapainen, vaikka se käyttääkin enemmän sen terminologiaa kuin itse protokollaa. ATMP suunniteltiin alun perin palveluntarjoajien tuottamia VPN-palveluita silmällä pitäen. (Perlmutter & Zarkower 2001: 138.)

Tunnelointiprotokollana ATMP on Perlmutterin ja Zarkowerin (2001) mielestä varsin heikko, mutta se voi olla palveluntarjoajille erittäin hyödyllinen väline VPN-palveluiden valikoiman lisäämisessä. Monet palveluntarjoajat hyödyntävät jo Ascendin laitteistoa osana palveluidensa infrastruktuuria, joten joillekin ATMP on varmasti helppo valinta huolimatta sen yksinoikeudellisesta asemasta. (Perlmutter & Zarkower 2001: 138.)

4.5.3 BayDVS

BayDVS muistuttaa todella paljon ATMP:tä toiminnaltaan ja muodoltaan, vaikka näiden kahden tunnelointiprotokollan välillä on erojakin. Eroja BayDVS:än ATMP:n välillä ovat esimerkiksi termistön ja turvallisuusarkkitehtuurin välillä. Turvallisuusarkkitehtuuriin liittyen BayDVS:ssä tunnelit autentikoidaan käyttämällä MD5-sekoitteen generoimia digitaalisia allekirjoituksia, kun taas ATMP käyttää heikompaa CHAP-tyylistä menetelmää. (Perlmutter & Zarkower 2001: 138.)

Kuten ATMP, on BayDVS yksinoikeudellinen teknologia. BayDVS on kiinnostava vaihtoehto niin kauan kuin käytetään Bay Networksin tuotteita ja palveluita. Ne, jotka haluavat rakentaa VPN-palvelunsa muun kuin Bay Networksin laitteiston päälle, on etsittävä muita vaihtoehtoja. (Perlmutter & Zarkower 2001: 139.)

5 VPN-Projekti

5.1 Yritysesittely

Opinnäytetyöni ”Toimipisteiden välisen VPN-toteutuksen suunnittelu” toteutettiin käytännössä IT-alalla toimivassa keskisuuressa yrityksessä. Yrityksellä on toimipisteitä Suomessa, Ruotsissa ja Baltian maissa. Yrityksen laajentuessa ja tietojärjestelmien keskittyessä Suomeen, yrityksellä oli tarve päivittää nykyiset yhteydet tietoturvallisimmiksi tietoliikenneyhteyksiksi. Yrityksellä on selvä strategia laajentua myös tulevaisuudessa, joten tämä työssäni käsiteltävä projekti on varmasti tarpeellinen panostus yrityksen tulevaisuuttakin ajatellen.

5.2 Vaatimuksia

Vaatimuksia VPN-suunnitteluun ja käyttöön oli todella paljon. Projektin edetessä vastaan tuli koko ajan asioita, jotka tulisivat vaikuttamaan lopputulokseen. Seuraavassa muutamia esille tulleita vaatimuksia ja lähtökohtia onnistuneen VPN-ratkaisun toteuttamiseen.

Laajennettavuus

Tulevaisuuden laajentumiselle oli jätettävä mahdollisuus. Yrityksen liiketoiminnallisena strategiana on laajentuminen Euroopassa, joten on erittäin todennäköistä, että Suomeen keskitettyjä tietojärjestelmiä tullaan tulevaisuudessa hyödyntämään myös muista konsernin toimipisteistä kuin tällä hetkellä. Tehokkaan VPN-ratkaisun avulla tulevaisuuden yhteydet eivät tuota ongelmia keskitettyjen tietojärjestelmien hyödyntämisessä.

Suorituskyky

Vaikka VPN-liikenne ei merkittävästi lisääkään verkon kuormitusta pitää muistaa myös nykyisen verkon suorituskyky ulkomaailmaan. Yrityksen nykyisissä yhteyksissä riittää nopeutta monen kymmenen megabitin vauhtiin, joten kaistanleveyttä on tähän hetkeen ja tulevaisuuteen varattu riittävästi.

Turvallisuus

Turvallisuuspohdinnat tulevat aina esille vastaavanlaisten projektien yhteydessä ja asiaa ei pidä nykypäivänä mitenkään väheksyä. Yksinkertaisesti turvallisuus on niin tärkeä asia ja myös yksi tämän projektin käynnistävistä tekijöistä. Projektissa haettiin turvallisuutta tietoturvan kautta.

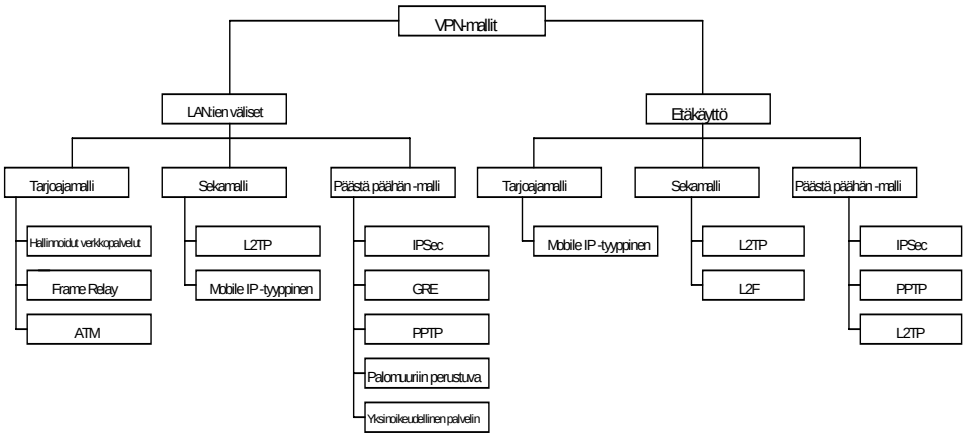
Projektin, kuten tietoturvankin, päämääriä on liikuteltavan tiedon luottamuksellisuus, eheys ja todennus. Muita mainittavia tietoturvan periaatteita ovat saatavuus, pääsynvalvonta ja kiistämättömyys. (Järvinen 2003: 29-34.)

Henkilökunta

Yrityksen IT-henkilökunnan monipuolisista ja aikaa vievistä tehtävistä johtuen VPN-toteutuksen suunnittelussa, päivittäisessä käytössä ja ylläpidossa pohdittiin mahdollisuutta ulkoistaa VPN-palvelu toteutuksen mahdolliselle tekijälle. Mahdolliseen ulkoistussopimukseen tulisi kuulumaan muun muassa asennus, hallinnointipalvelut, ongelmanratkaisu ja vianetsintä. Varsinainen loppukäyttäjätuki ja loppukäyttäjäkoulutus kuuluisi kuitenkin yrityksen omalle IT-henkilökunnalle.

VPN-malli

Olemassa olevia erilaisia VPN-malleja ovat päästä päähän -malli, palvelun tarjoaja -malli ja sekamalli. Kyseisen projektin VPN-malliksi tuli päästä päähän -malli. Ja kuten kuvasta voimme huomata, tätä mallia voidaan hyödyntää IPSec-protokollaa käyttäen niin lähiverkkojen välisiin kuin etäkäyttö-VPN:iin.



Kuva 6. VPN-mallit, -sovellukset ja -protokollat (Perlmutter & Zarkower 2001: 87)

Turvallisuusliitot

IPSec-käyttöön suunnitellussa laitteessa pitää kiinnittää huomiota myös laitteen tai sovelluksen kapasiteettiin hoitamaan IPSec-liittoja. Toiset laitteista tai sovelluksista omaavat rajoitetun kapasiteetin hoitamaan IPSec-käytössä käytettäviä avaimia ja algoritmeja. Jos laitteella on jo vaikeaa hallita sen omia IPSec-liittoja, niin laajennettavuus kyseisen laitteen avulla ei tule tulevaisuudessa onnistumaan. Suunnitteluvaiheessa yritys luonnollisesti pyrki hieman paneutumaan tarjottavien laitteiden

ominaisuuksiin ja kapasiteettiin, tosin turvallisuusliittojen määristä ei selvästi oltu mainittu minkään valmistajan laitemäärityksissä.

IPSec

IPSec-protokollaan päätymistä oli suositeltu muun muassa kolmannen osapuolen asiantuntijoiden puolesta. Alla näkyvästä kuvasta voimme myös vahvistaa kyseistä käsitystä, että protokolla on hyvin dominoivassa asemassa ja paljon käytetty protokolla.

Vendor	Product	Type	Web Address	Technology
Checkpoint	Firewall –1	Firewall	http://www.checkpoint.com	IPSec
Trusted Information Systems	Gauntlet	Firewall	http://www.tis.com	IPSec
Raptor	Eagle Mobile NT 4.0	Firewall	http://www.raptor.com	IPSec
Cisco	Layer 2 Forwarding (L2F) Products	Hardware	http://www.cisco.com	L2F
Cisco	Cisco IOS	Software	http://www.cisco.com	IPSec, L2TP
3Com	3Access VPN products	Hardware	http://www.3com.com	IPSec
Compaq-Microcom	6000 Series	Hardware	http://www.microcom.com	PPTP
Extended Systems	Extended- Net VPN	Hardware	http://www.extendsys.com	PPTP with MPPE
RedCreek Communications	Ravlin	Hardware	http://www.redcreek.com	IPSec/ISAKMP/ Oakley
Timestep	Permit System	Hardware	http://www.timestep.com	IPSec
VPNet	VPN Remote client	Hardware	http://www.vpnet.com	IPSec
Information Resource Engineering	SafeNet/ Enterprise	Multiple	http://www.ire.com	IPSec
Novell	BorderManager	NOS	http://www.novell.com	PPTP
Microsoft	NT Server 4.0 Remote Access Server / PPTP	NOS	http://www.microsoft.com	PPTP and MPPE

Kuva 7. IPSec-protokollaa tukevat laite-/ohjelmistovalmistajat (George Mason University 2005)

IKE-käytäntö – IKE-protokolla (Internet Key Exchange)

VPN-yhteyksiä suunnitellessa törmää IKE-käytäntöön. IKE-protokolla (Internet Key Exchange) on protokolla, jonka avulla osapuolet neuvottelevat yhteydenpidon turvallisuuskäytännöt. Projektissa punnittiin IPSec-protokollaperheen AH- (Authentication Header) ja ESP-protokollien (Encapsulating Security Payload) vaikutusta yhteyksien turvallisuuteen.

Huolimatta siitä, käytetäänkö ESP- vai AH-protokollaa, yhteys tarvitsee aluksi toimivaa avainten vaihtoa kommunikoivien laitteiden välillä. Kommunikointi toteutetaan sovellustason IKE-protokollalla. Turvallisuuskäytäntöjen neuvottelu noudattaa ISAKMP-määrityksiä

(Internet Security Association and Key Management Protocol). ISAKMP määrittää yleiset puitteet protokollille, joilla turvallisuuskäytäntö luodaan ja avaintenvaihto toteutetaan. Myös muutoin kuin tavallisissa IPSecin yhteyksissä. (Silván 2001.)

Käyttäjät

Käyttötarkoituksena on vain suojata kahden eri toimipisteen lähiverkkojen liikenne. Tulevaisuudessa pohdinnan alaisena on muutaman tärkeimmän asiakkaan liittäminen VPN-tunneloinnilla.

Luvun 5.2. alaluvuissa on syventäviä kysymyksiä VPN-ympäristön suunnittelijoille ja opinnäytetyön kohteena olleen yrityksen vastauksia ja ratkaisuita niihin. Opinnäytetöiden julkisuudesta ja tietoturvasyistä johtuen joitain kohtia on jätetty täyttämättä tähän raporttiin.
Luvut 5.2.1 ja 5.2.2 on kirjoitettu pääsääntöisesti siten, että asia on kirjoitettu kysymys-vastaus-tyylisesti. Kysymys on aina merkitty kursivoidusti ja vastaus on ilman mitään erityistä fonttityyliä.

5.2.1 Kartoitus

Kartoituksen alussa pitää olla pätevä suunnitelma, ajatus siitä, mitä etuja VPN-tunneloinnilla halutaan tuoda yritykselle. Onko se kustannusten aleneminen entiseen verrattuna? Esimerkiksi vanhemman ATM-Permanent Virtual Circuit -yhteyden korvaaminen VPN-ratkaisulla.

Haetaanko kustannustehokkuutta? Nopeamman yhteyden tarve tai hintavertailu mahdolliseen olemassa olevaan ratkaisuun? Yrityksen projektin päätarkoituksena oli saada lähiverkkojen välille tietoturvalliset tietoliikenneyhteydet.

Onko kysymyksessä palvelimien tietokantojen yhdistäminen tai replikointi? Suomen päätoimipisteessä tulee toimimaan yrityksen tietojärjestelmien ydin. Näin ollen VPN-yhteyksiä tullaan myös hyödyntämään toimipisteiden välillä, muun muassa palvelinten tietokantojen replikoinnissa ja yhdistämisessä.

Haetaanko pääsyä yhteiselle intranet-palvelimelle? Jokaisessa toimipaikassa toimii omat palvelimet. Varsinaista yhteistä intranet-palvelinta ei ole. Yhteinen intranet-palvelin on kyllä suunnitelmissa, mutta sen asennuksesta tai käyttöönotosta ei ole tehty tarkempia suunnitelmia. Ennen varsinaista intranet-palvelinta koekäyttöön otetaan Microsoft Share Point Portal Server. Microsoft Share Point Portal Server:in avulla voidaan tehdä intranet-palvelimen tyylisiä tehtäviä, kuten erilaisia intranet-työpöytiä, jotka sisältävät uutispalvelujen lisäksi asiakirjojen jakelu-, julkistamis- ja käsittelyominaisuudet. (Fujitsu Finland 2005).

Siirretäänkö varmistustietoja tunnelin yli? Tietojärjestelmien luonteesta johtuen varsinaisia varmistuksia ei tälläkään hetkellä ajeta verkon yli, eikä niitä aiota tulevaisuudessakaan ajaa VPN-tunnelin kautta. Tiettyjen backup-tietojen siirtäminen muista maista ja toimipisteistä tulee tapahtumaan viikonloppuisin.

5.2.2 Suunnittelu

Kartoituksen jälkeen on tiedossa vaadittavia kohtia. Kun tiedetään mitä verkkojen yhdistämiseltä halutaan, on syytä olla hyvinkin syvälle menevä suunnitelma siitä miten kaikki tullaan toteuttamaan.

Otetaan selvää eri verkkojen asetuksista.

- *IP-osoitteiden valinta? (julkinen verkko, sisäverkko)*
- *Mitä IP-aliverkkoja eri verkoissa on käytössä?*
- *Minkälaiset Internet-yhteydet eri pisteillä on käytössä?*
- *Onko käytössä julkinen kiinteä ip-osoite VPN-yhteyttä varten?*

Projektin alkaessa aliverkot selvitettiin ja koottiin suunnittelua varten. Kiinteitä IP-osoitteita yrityksellä on riittävästi, myös VPN-käyttöön jaettavaksi.

Onko olemassa olevaa palomuuriratkaisua, voidaanko sitä hyödyntää tunneloinnissa? Onko olemassa olevassa palomuurissa rajoituksia tunneloinnin toteuttamiseen? Käytössä olevaa palomuuria olisi voitu hyödyntää myös VPN-käytössä. Palomuuriin saa tarvittaessa vaadittavat VPN-ominaisuudet, mutta näin ei haluttu tehdä. Käytännössä myös tässä tapauksessa yrityksen käytössä oleva palomuuri on pakko kiertää. Tämä johtuu siitä, että palomuuri on kolmannen osapuolen hallinnoima ja ongelmatapauksissa palomuurin toimimattomuus voisi estää myös VPN-liikenteen ellei palomuuria kierrettäisi.

ISP:n (Internet Service Provider) mahdolliset rajoitukset liittymässä? Onko ISP:n puolesta palomuuria käytössä ja pitääkö pyytää muutoksia access-listoihin jotta VPN onnistuu? Internet-yhteyden palveluntarjoajan puolelta Internet-liittymässä ei ole rajoituksia mitkä vaikuttaisivat VPN-käyttöön. Internet-yhteyden palveluntarjoajan puolesta ei ole myöskään käytössä palomuuria vaan käytössä oleva palomuuri on kolmannen osapuolen ylläpitämä ja hallinnoima. Käytössä olevaan palomuuriin ja sen konfiguraatioon jouduttiin kuitenkin tekemään pieniä muutoksia, jotta VPN-liikenne saatiin toimimaan.

Kartoitetaan Internet-yhteyksien nopeudet eri toimipisteissä. Pitääkö nopeuksia nostaa sujuvan tunneloinnin takaamiseksi? Projektiin liittyvien toimipisteiden nykyiset yhteydet ovat 30Mbit/s ja 10Mbit/s. Kolmannen osapuolen asiantuntijoiden mukaan internetyhteyden nopeus on riittävä myös vaadittavaan VPN-käyttöön.

Onko liittymässä riittävästi myös Upstream-kaistaa? Tunneli on kaksisuuntainen ja Up/Downstream-nopeuksista matalampi käytännössä määrää tunnelien nopeuden. Up/Downstream-kaistaa on mittausten mukaan käytössä riittävästi.

Nopeus- ja salaustarpeiden mukaan päätetään hankittavien laitteiden ominaisuuksista. Olemassa olevan palomuurin rinnalle tai yhteyteen vain VPN-tunnelointia hoitava laite? Palomuuri ja VPN-tunneloiva yhdistelmälaite? Tässä tapauksessa olemassa olevaa palomuuria olisi voitu hyödyntää VPN-käytössä, mutta niin VPN-yhteyksien kuin palomuurin toiminnan varmemman toimivuuden kannalta päätettiin hankkia erillinen VPN-laite. Näin muun muassa vältetään laite-rikkoutumisen aiheuttamat ongelmat joko palomuurissa tai VPN-yhteyksissä. Muita mahdollisuuksia ratkaisuun olisi ollut muun muassa siten, että VPN-ominaisuus on reitittimessä, ohjelmistopohjainen, palomuurissa tai kokonaan erikseen, kuten tässä tapauksessa.

Verkon liikennemäärät? Tarkasta määrästä ei voi valitettavasti laittaa tietoa tähän työhön, mutta kaikki tietty lähiverkkojen välinen liikenne pyritään ohjaamaan käyttämään VPN-tunneleita.

Käyttäjämäärä ja etäkäyttäjien (Roaming users) määrä? Etäkäyttäjillä käytössä joku etäkäyttöohjelmisto? Yhteensä noin 30 kappaletta. Etäkäyttäjiä noin kymmenen ja vielä tällä hetkellä heillä on käytössä niin sanottu terminaali-yhteys. Lähitulevaisuudessa myös etäkäyttäjät siirtyvät VPN-käyttäjiksi ja etäkäyttäjät tulevat käyttämään palveluntarjoajan VPN Client -ohjelmistoa.

Palvelun hallinta? Hallinnan ulkoistaminen tai palvelun ostaminen SI:ltä (Service Integrator)? Jo heti projektin alusta alkaen pohdittiin VPN-palvelun hallinnan ulkoistamisesta kolmannelle osapuolelle. Yritykselle itselleen varsinainen VPN-palvelun hallinnointi ei tuo mitään lisäarvoa. Näin ollen päätettiin IT-palveluiden osassa keskittyä vain nykyiseen ydinosaamiseen ja VPN-palvelun hallinta jätettiin kolmannelle osapuolelle. Lisäksi palvelun ulkoistamiseksi saatiin loistava tarjous, joka käytännössä käsittää kaiken (konfigurointi, monitorointi, laitteet, tuki ja niin edelleen), tarjouksesta ei yrityksen edustajan mukaan voinut kieltäytyä.

VPN-palvelun hallinnointi? Palvelun laskutustapa? Koska kyseessä on ulkoistettu palvelu, ongelmatapauksissa huollon vasteaika on yksi tunti. Muina hallinnointiesimerkkeinä voidaan pitää samana arkipäivänä tapahtuvia toimenpiteitä tai kuten yleensä 24/7/365 -tyylisesti toimivaa palvelua. Näin mahdolliset ongelmatapaukset koitetaan saada ratkaistua heti kun ne ilmenevät, eli huolto toimii kellon ympäri vuoden jokaisena päivänä. Kyseessä olevan palvelun laskutustapa on kuukausipohjainen laskutus.

Yhtäaikaisten VPN-tunneleiden määrä? Palomuurin/VPN-tunneleiden nopeus, läpäisy-/salauskyky? Saman aikaisten tunneleiden määrä on tällä hetkellä maksimissaan kolmekymmentä kappaletta. Laitteiden ja VPN-tunneleiden ominaisuudet ja suorituskyky ovat erittäin riittävät projektin tarpeita varten.

Olemassa olevaa osaamista tietyn valmistajan mallistoon? Ennen projektia nykyisellä IT-henkilöstöllä ei ollut osaamista VPN-tuotteita kohtaan.

Koulutustarve laitteiden hallintaa varten? Yrityksen lähtökohta, VPN-palvelun ulkoistaminen huomioon ottaen yrityksellä ei ollut koulutustarvetta VPN-palvelua ajatellen. Tietenkin lähtökohta monella muulla yrityksellä on varmasti toinen ja valmistajan tai palvelun asentajan puolelta tuleva koulutus on varmasti hyvin tarpeen.

Riittävästi ominaisuuksia myös tulevaisuutta ajatellen? VPN-hallinnointipalvelun luonteesta johtuen yritys ei varsinaisesti omista VPN-laitteita, joten ne ovat helposti päivitettävissä tehokkaampaan kalustoon tarpeen vaatiessa.

Tarvitaanko lisää tunneleita myöhemmin tulevaisuudessa? Mitä aiotaan tunneloida? Sallitaanko vain palvelimien välinen liikenne tunnelien yli? Jo ainoastaan yrityksen strategiaa peilaten, lisää tunneleita on tulossa lähitulevaisuudessa. Tällä hetkellä vain tietty lähiverkkojen välinen liikenne tunneloidaan VPN-tunneleihin.

Yhdistetäänkö koko verkot toisiinsa vai yhdistetäänkö vain tietyt osat verkoista toisiinsa? Tässä projektissa vastaus on yksinkertainen, verkkoja ei kokonaisuudessaan yhdistetä, vain tietty liikenne kulkee VPN-tunneleiden kautta.

Onko valvonnan kannalta suositeltavaa käyttää käyttäjätunnusvarmennusta? Näin esimerkiksi varastetun kannettavan takia kaikkien roaming users -käyttäjien kannettavia ei tarvitse konfiguroida uudelleen. Pelkästään varastetun koneen käyttäjän tiedot ja tunnisteet vaihdetaan.

Varayhteys VPN-yhteyksille? Kuinka kriittinen yhteys verkkojen välillä on? Varsinaista varayhteyttä ei ole, eikä sellaista ole suunnitelmissakaan ainakaan tällä hetkellä. VPN:än laajentuessa lisää yrityksen toimipisteiden välillä, varayhteysasia tulee varmasti ajankohtaisemmaksi. Kriittisyys asteikoilla yhdestä kymmeneen, 5. Kohdeyritystä ajatellen heille tietoturva on tärkein asia mitä VPN heille tuo.

Millä tasolla olemassa olevien verkkojen tietoturva on? Projektin alkaessa toimipisteiden välisen liikenteen tietoturva ei tietystikään yltänyt VPN-liikenteen kaltaiseen tietoturvan hyödyntämiseen, mutta jo aiemmin

virustentorjunta, palomuuri, roskapostin käsittely ja käyttäjien hallinta oli sillä tasolla, ettei huonostakaan tietoturvasta voida puhua.

Virukset, madot ja muut uhkat liikkuvat VPN-tunnelien yli sujuvasti verkosta toiseen, virussuoja kunnossa? Viitaten yllämainittuihin asioihin, virusten torjunta on kunnossa. Asiaanhan tietysti myös auttaa aktiivinen ja automaattinen virussuojan päivitys.

Roaming users, onko koneissa esimerkiksi ohjelmistopalomuurit? Liikkuvien ja etäkäyttäjien koneissa on kaupallinen ohjelmistopaketti, joka sisältää muun muassa virusten torjunta- ja palomuuriohjelmat.

Päätetään käytetäänkö Roaming Users -käyttäjien tunnistamiseen ja varmentamiseen Radius-palvelinta. Voidaanko tähän hyödyntää olemassa olevaa palvelinta? Paljon liikkuvien käyttäjien, kuten esimerkiksi tuote-edustajien tunnistamiseen voidaan käyttää myös Radius-palvelinta (Remote Authentication Dial-in User Services). Radius-palvelimen avulla voidaan tehdä keskitetysti etäkäyttäjien käyttöoikeuksien valtuuttaminen, vahvistaminen ja käyttäjien tilitietojen hallinta. Jos päädytään käyttämään Radius-palvelinta, kannattaa myös punnita vaihtoehtoa, että palvelimena voisi toimia joku nykyisistä palvelimista. Näin ei tarvitsisi sijoittaa uuteen palvelimeen ja ratkaisu olisi kustannustehokas.

Päätetään salausasetuksista eri tunneleissa. Päätetään käytetäänkö VPN-laitteiden keskinäistä tunnistusta VPN-tunnelin kättelyssä? Ostetaanko kolmannelta osapuolelta varmennetut sertifikaatit tunneloinnin varmistamiseen? Vai käytetäänkö PreSharedKey menetelmää? PreSharedKey on menetelmä millä saadaan autentikointi ja salaus kohtuullisen yksinkertaiseksi ja suoraviivaiseksi. Lisäksi on mahdollista käyttää Self Signed Cerficates -varmennetta? Itse allekirjoitetulla (self-signed) varmenteella varmentaja allekirjoittaa julkisen avaimensa omalla yksityisellä avaimellaan, jolloin syntyy itse allekirjoitettu juurivarmenne. Näillä kappaleen alussa mainituilla toimenpide-esimerkeillä saadaan muun muassa yhteyden salaus, autentikointi ja paljon muuta varmistettua.

Hankitaanko tämän hetken tarpeet täyttävät laitteet vai varaudutaanko tulevaisuuteen? Kukaan meistä ei kuitenkaan varmasti tiedä tulevaisuuden tarpeita, joten monessa tapauksessa on syytä varautua myös tuleviin tulevaisuuden lisätarpeisiin, näin vältetään ainakin laitteiden osalta mahdolliset pullonkaulat tulevaisuudessa.

Tarvitaanko backup-Internet-yhteys? Varalaitteet mahdollisten laitevikojen varalle? Tarvitaanko tuplalaitteet varayhteydelle? Joillekin yrityksille VPN:n toimivuus voi olla erittäin kriittinen asia. Tietoturvallisten yhteyksien toimivuus esimerkiksi yrityksen eri toimipisteiden välillä voi olla elinehto, tietoja tarvitsee siirtää esimerkiksi

tuotekehitys- ja tuotantoyksiköiden välillä jatkuvasti ja nykyajan kiristyvässä kilpailutilanteessa yritykset haluavat varmasti tehdä tämän turvallisesti. Näin ollen tällaisessa tilanteessa olevan yrityksen on syytä miettiä myös VPN-yhteyden turvaamista erilailla ongelmien ilmaantuessa. Näitä kysymyksiä miettimällä yritys voi päättää, että hoitaako varayhteydet ja varalaitteet kuntoon. Jos heidän yhteys on toiminnan kannalta niin kriittinen, vaihtoehtoja ei juuri ole. Varalaitteiden osalta on myös huomioitava se, että käytössä olevien konfiguraatioiden aktiivinen tallennus on välttämätöntä varalaitteiden nopeaa käyttöönottoa varten.

Kustannukset ja budjetointi. Tiukka kilpailu tekee ympäristöstämme hintatietoisempaa ja välillä hankinnoissa yritetään päästä halvemmalla sieltä missä vaihtoehtoja on, vaikka kuitenkaan Ladan hinnalla ei saa ostettua Ferraria. Valitettavasti vain kaikista halvimmalla ratkaisulla harvoin pystytään toteuttamaan niitä kaikkia monipuolisia tarpeita, joita asianmukainen VPN-ratkaisu tarvitsee. Niille jotka eivät IT-alalla toimi, tämä on monesti hyvin vaikeaa ymmärtää. VPN-ratkaisua miettiessä tulisikin miettiä vaatimusten ja ratkaisun tasapainoa myös kustannuksien suhteen. Vaihtoehtoja muun muassa VPN-laitteiden suhteen kuitenkin löytyy muutamia, ensimmäiseen vastaantulevaan laitteeseen ei tarvitse tyytyä.

5.2.3 Toteutus

Koska työni tarkoituksena oli ainoastaan tehdä suunnitelma VPN-toteutusta suunnitteleville, jätän varsinaisen toteutuspuolen väliin. Tässä kappaleessa on kuitenkin muutamia kohtia varsinaista VPN-toteutusta varten.

Toteutusta aloitettaessa alkuvalmistelujen osuutta ei kannata väheksyä. Jotta työ saadaan tehtyä tehokkaasti ja nopeasti, on hyvä lähteä järjestelmällisesti liikenteeseen.

Hankitaan kaikki asennuksiin liittyvä tarpeisto valmiiksi ja testataan laitteet etukäteen. Näin saadaan esimerkiksi DOA (Defective On Arrival) -laitteet heti pois häiritsemästä varsinaista asennusta ja järjestettyä toimivat laitteet hyvissä ajoin ennen varsinaista asennusta.

Tarkastellaan IP-osoitteet, valmistellaan verkot mahdolliseen verkkotopologian muutokseen. Koska kaikki verkot pitää olla eri IP-verkoissa vaihdetaan tarvittaessa IP-aliverkot joissain yhdistettävissä verkoissa.

Asennus on pyrittävä tekemään sellaisena ajankohtana, että se tuo käyttäjille mahdollisimman vähän vaikutuksia ja katkoksia. Tosin aina ei tähän pystytä, joten tarvittaessa käyttäjille on ilmoitettava mahdollisista

katkoksista verkko- ja palvelinyhteyksissä asennuksen aikana. Asennuksen aikana konfiguroidaan VPN-tunnelit suunniteltujen asetusten mukaisesti ja laitetaan mahdollinen Radius-palvelin toimintakuntoon. Ja varsinaisen asennuksen jälkeen ei unohdeta käyttäjiä, vaan asennetaan roaming user -käyttäjien koneisiin tarvittavat ohjelmat VPN-käyttöön.

Asia, mikä monelta yritykseltä on matkan varrella unohtunut, on dokumentointi. Joten ei unohdeta dokumentoida työn eri vaiheita ja laitteisiin tehtäviä asetuksia. Dokumentoidaan myös mitä suunnitelman mukaisia toimenpiteitä suoritetaan asennuksen aikana. Tulevaisuudessa varmasti hyvä dokumentointi asennuksesta lähtien tulee auttamaan esimerkiksi myöhemmissä ongelmatapauksissa.

VPN-asennuksen onnistuminen varmistetaan testaamalla VPN-yhteyksien toimivuus ennen varsinaiseen tuotantoympäristöön kytkemistä. Samalla testataan myös roaming user -käyttäjien toimivuus ja vertaillaan suunnitelman ja toteutuksen eroja. Mitä on yhdistetty ja miten ja toimiiko kaikki niin kuin pitää.

Käyttöoikeuksien asettaminen. Verraten vaatimuksiin, suunnitelmaan ja yrityksen tarpeisiin, asetetaan käyttöoikeudet. Esimerkiksi kenellä on oikeudet käyttää palveluita tunneleiden yli ja kenellä on oikeudet tehdä muutoksia laitteiden konfiguraatioihin.

Varmistetaan, että asennuksen alusta saakka tehtyyn dokumentointiin on lisätty kaikki osavaiheet ja että kokonaisuus on asianmukaisesti dokumentoitu. Lisäksi dokumentointiin lisätään kaikkien asennettujen laitteiden asetukset liitteeksi dokumentaatiota.

Loppujen lopuksi varmistetaan vielä kerran, että kaikki toimii. Verrataan haluttujen, luvattujen ja toteutuneiden toimintojen onnistuminen ja tarvittaessa tehdään muutoksia tai ollaan tyytyväisiä lopputulokseen.

5.2.4 Jälkihoito

Projektin valmistuttua VPN-toimintoja ei voi vain jättää sivuun, vaan asia vaatii jatkuvaa tarkkailua ja kunnossapitoa. Tärkeimpänä kohtana tulee tietysti laitteiden ylläpito, mahdolliset uudet käyttäjät täytyy konfiguroida VPN-laitteeseen, ongelmatilanteiden korjaaminen ja niin edelleen.

Suunnitellaan ohjelmistopäivitykset, seurataan ohjelmistojulkaisuja. Tutkitaan onko päivitys kriittinen tietoturvan kannalta? Onko uudessa versiossa ominaisuuksia mukana, joita mahdollisesti tarvitaan asennetussa ympäristössä? Onko uudessa versiossa karsittu ominaisuuksia, jotka ovat nyt käytössä? Vaatiiko ohjelmistopäivitys

muutoksia olemassa olevaan konfiguraatioon? Yllä mainittujen seikkojen tutkiminen on aikaa vievää toimintaa ja vaatii todella paljon asiantuntemusta. Projektin vaatimuksissa ja suunnitelmassa kannattaa siis tuoda ohjelmistopäivitysten merkitys selvästi esille ja myös se, että kuka kyseisen asian hoitaa käytännössä. Jos päädytään käyttämään uusimpia ohjelmistoversiota, testataan ne ensin testiympäristössä. Lisäksi pidetään huoli, että myös mahdolliset varalaitteet päivitetään samassa tahdissa kuin tuotantolaitteet.

Projektin vaatimuksissa ja suunnitelmassa pitää tulla myös esiin kohta vikatilanteiden seuranta, valvonta ja hallinta. Kuka vastaa käytännössä vikatilanteissa vian tutkimisesta ja korjaamisesta? Näin projektin jo päätyttyä ei tarvitse huolehti vikatilanteista, vaan asia on jo ajoissa sovittu ja vikatilanteet saadaan hoidettua nopeasti pois häiritsemästä normaalia toimintaa. Lisäksi täytyy varmistaa, että mahdollinen varahenkilö tai mahdolliset varahenkilöt ovat saatavilla lomien ja/tai sairastumisten varalta. On myös muistettava varmistaa säännöllisesti, että mahdolliset varayhteydet toimivat vikatilanteiden sattuessa.

Vaikka kaikki näyttäisi sujuvan mainiosti, ei pidä unohtaa valvonnan osuutta. Ainahan kaikki ei ole niin kuin miltä se näyttää. Seurataan ja vertaillaan saatavia lokitiedostoja ja tehdään tarvittaessa toimenpiteitä niiden mukaan. Valvonnalla pidetään ylimääräinen liikenne kurissa ja tunnistetaan välittömästi mahdolliset väärinkäytökset. Väärinkäytösten sattuessa tehdään tarvittavat toimenpiteet asian korjaamiseksi.

Liikkuvien käyttäjien koneet vaativat myös jatkuvaa ylläpitoa ja tietoturvan valvontaa. Koneiden käyttäjät voivat esimerkiksi toimillaan aiheuttaa vahinkoa epähuomiossa tai tietämättömyyttään. Lisäksi koneet usein vaativat päivitystoimenpiteitä, kuten Windows XP:n Service Pack -päivitysten asentamista, mihin käyttäjällä ei välttämättä ole osaamista ja oikeuksia, joten on parempi, että ne, jotka nämä toimenpiteet hallitsevat, myös suorittavat ne.

Käyttövarmuus, laitteiden ja tunneleiden käyttöaste. Kalliita laitteita ja asennuksia ei tehdä huvin vuoksi. Varsinkin raportoinnissa pitäisi selvästi tulla esiin edellä mainitut asiat. Ulkoistetun palvelun käyttäjä ei muuten saa välttämättä mitään tietoa edellä mainituista ja saattaa vaikka maksaa aivan liikaa ominaisuuksista mitä ei edes käytä. Jos ulkoistussopimukseen on tehty erillinen SLA (Service Level Agreement), yllämainitut seikat kannattaa ehdottomasti mainita siinä. Sopimuksessa pitää ehdottomasti olla myös maininta katkosten tai vikatilanteiden aiheuttaneesta viasta ja selvitys tästä.

Raportointi, jos VPN-toiminnan hallinnointi on ulkoistettu, kuten tässä projektissa, on tehtävä selvät rajat mitä ja milloin kuuluu raportoinnin pariin. Kuinka usein ja miten raportoidaan esimerkiksi laitteiden tai tunneleiden käyttöaste ja käyttövarmuus. Kuinka pian pitää raportoida

katkosten tai vikatilanteiden sattuessa ja mitä kuuluu selvitykseen vian aiheuttajasta. Ja millainen on SLA:n toteutuminen. Lisäksi usein raportointia käytetään myös palvelun laskutuksen hyväksyntää varten..

Kun laitteet on vihdoin asennettu ja homma toimii, ei voida unohtaa tulevaisuuden kannalta elintärkeää asiaa. Pidetään huoli, että toimintaa hoitavat henkilöt ylläpitävät riittävän osaamistason asian suhteen ja kouluttavat itseään tai muuta henkilökuntaa tarpeen vaatiessa. Vastuullisten henkilöiden vastuupiiriin kuuluu myös käyttäjien ohjeistaminen ja dokumentoinnin päivitys muutosten yhteydessä

6 VPN-projektin toteutus

Projektin toteutukseen esimerkkiyritys otti selvän linjan alusta lähtien. Yritys ei itse halunnut lähteä käyttämään resurssejaan tulevaan projektiin, vaan tavoitteena oli saada luotettava partneri hoitamaan projektin varsinainen suunnittelu ja toteutus. Se, miksi yritys lähti heti etsimään kolmatta kumppania VPN-projektiin, johtui yksinkertaisesti yrityksen IT -henkilöstön rajallisista ajankäytönmahdollisuuksista ja asiantuntemuksen puutteesta tulevassa projektissa. Projektin toteuttajan vaatimuksena tuli esille myös se, että yrityksellä piti olla osaaminen koko projektin hoitamiseksi, aina suunnittelusta asennukseen ja ylläpitoon.

Projektin toteuttajien etsinnässä esimerkkiyrityksen nykyisen palomuuriratkaisun toimittaja teki parhaimman tarjouksen ja yrityksen oli helppo tehdä valinta. Esimerkkiyritys on ollut hyvin tyytyväinen palomuurin toimintaan ja sen ylläpitoon, joten yrityksen oli helppo hyödyntää alan asiantuntijaa ja syventää yhteistyötä jo entisestään tutun kumppanin kanssa.

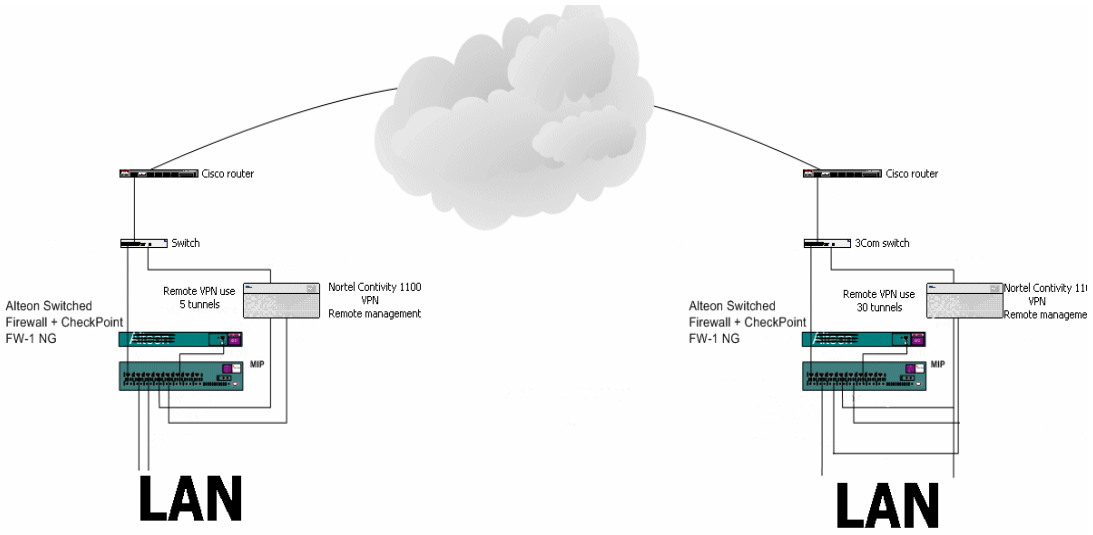
Näin ollen projekti toteutettiin yhdessä yrityksen IT-henkilöstön ja kolmannen osapuolen kanssa. Projektin varsinaisesta suunnittelusta ja toteutuksesta vastuussa oli juuri edellä mainittu kolmas osapuoli. Projektin edetessä eri vaiheiden testaus ja koekäyttö suoritettiin yhdessä yrityksen IT-henkilöstön kanssa ja samalla käytiin läpi eri vaiheiden vaatimukset ja toteutuneet ominaisuudet.

7 Projektin lopputulos

7.1 Lopullinen toteutus

Projektin päättyessä VPN-laitteeksi valittiin Nortelin Contivity 1100. Kuten mukana tulevasta liitteestä (liite 1.) voimme havaita, laitteella on mahdollista tehdä hyvin monipuoliset IPSec-asetukset. Muut liitteen kuvat ovat muita mahdollisia asetuksia ja palveluita laitteen Services-valikosta, josta myös aikaisemmin mainittu IPSec-asetukset löytyvät. Muita vertailukohtia oli muun muassa 3Com:n vastaava laite, mutta kolmannen osapuolen testien mukaan, Nortel vei voiton monipuolisella ja luotettavalla kokonaisuudellaan.

Projektin lopputulos näyttää seuraavalta:



Kuva 8. VPN-Projektin lopputulos

7.2 Pohdintaa

Yrityksen monipuolisia tarpeita oli erittäin haasteellista lähteä pohtimaan ja tuomaan esille. Tosin työ kokonaisuudessaan osoittautui todella haasteelliseksi, paljon haasteellisemmaksi kuin odotin. Tiedon saaminen asiaan liittyviltä muilta osapuolilta osoittautui aikaa myöten todella hankalaksi ja jopa mahdottomaksi. Moniin sähköposteihin ja puheluihin ei vastattu ollenkaan. Näin moni asia jäi epäselväksi ja jouduin jättämään ne työstä täysin pois. Tämä oli monessa kohdassa todella turhauttavaa ja aikaa vievää. Tämän takia työni aikataulu venähti todella paljon ja motivaatiota työn tekemiseen sai todella etsiä. Alkuperäisen suunnitelman mukaan työn valmistumisajankohta piti olla joulu 2004, joten vuoden viivästyminen on aika paljon. Monet pois jätetyistä asioista

olisivat tuoneet lisäsyvyyttä työhön ja antaneet monia lisäkohtia suunnitteluun. Aiheesta olisi siis saanut irti enemmänkin, jos aikaa olisi ollut enemmän ja olisi jatkuvasti lähettänyt kysymyksiä muille osapuolille. Tosin sain yllättäviltä, asiaan täysin kuulumattomilta tahoilta todella hyödyllistä tietoa. Tällaisena tahona mainittakoon esimerkiksi erään VPN-laitevalmistajan tekninen tuki. Näin ollen monien vaikeuksien jälkeen olen mielestäni saanut hyvän paketin kokoon, josta tosin olisi voinut saada loistavankin, jos kaikki osatekijät olisivat toimineet paremmin.

Lähdemateriaalin vähäinen määrä myös yllätti. Aiheesta on kyllä materiaalia, mutta monen materiaalin laatu on kyseenalainen. Monet artikkeleista käsittelivät vain VPN:ää yleensä ja varsinaisten tässä työssä auttaneiden tietolähteiden löytäminen oli hankalaa.

8 Lähteet

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

Jaakohuhta, Hannu 2003. IT-Ensyklopedia. Helsinki: IT Press.

Järvinen, Petteri 2003. Salausmenetelmät. Jyväskylä: Docendo Finland Oy

Silván, Markus 2001. VPN – Virtual Private Network. [Online] Viitattu 27.11.2005
http://www.cc.jyu.fi/~mape/vpn.pdf

Poonam Arora, Prem R. Vemuganti, Praveen Allani 2001. Comparison of VPN Protocols – IPSec, PPTP, and L2TP. [Online] Viitattu 19.2.2005
http://bass.gmu.edu/courses/ECE543/reportsF01/arveal.pdf

Symantec 2004. Kotisivut. [Online] Viitattu 27.11.2005
http://www.symantec.com/region/fi/resources/networks.html

BT 2005. Kotisivut. [Online] Viitattu 4.12.2005
http://www.btglobalservices.com/business/global/en/products/remote_vpn/index.html

Tekninen Korkeakoulu, tietoverkkolaboratorio 2004. Kotisivut. [Online] Viitattu 27.11.2005
http://www.netlab.hut.fi/opetus/s38192/k2002/slides/handout-08aaa.pdf

Wikipedia 2004. Kotisivut. [Online] Viitattu 27.11.2005
http://fi.wikipedia.org/wiki/L2TP

Wikipedia 2004. Kotisivut. [Online] Viitattu 27.11.2005
http://fi.wikipedia.org/wiki/GRE

Tekninen Korkeakoulu Helsinki 2004. Kotisivut. [Online] Viitattu 27.11.2005
http://www.tml.hut.fi/Opinnot/Tik-110.350/Tehtavat/rfc/2406_2.html

Helsingin Ammattikorkeakoulu Stadia 2004. Kotisivut. [Online] Viitattu 27.11.2005
http://cs.stadia.fi/~kuivanen/tietoturva/dos.php

Tekninen Korkeakoulu Helsinki 2004. Kotisivut. [Online] Viitattu 27.11.2005
http://www.tml.hut.fi/Opinnot/Tik-110.300/2000/Tehtavat/tehtava_07_-malli.html

Wikipedia 2004. Kotisivut. [Online] Viitattu 27.11.2005
http://fi.wikipedia.org/wiki/TCP/IP

Searchsecurity.com 2005. Kotisivut. [Online] Viitattu 27.11.2005
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci884946,00.html

Tampereen Teknillisen Yliopiston Tietotekniikan osasto 2005. Kotisivut. [Online] Viitattu 27.11.2005
http://www.cs.tut.fi/kurssit/8306000/2000/7a.html

Hewlett-Packard 2005. Kotisivut. [Online] Viitattu 27.11.2005
http://www.hp.fi/tuki/takuutiedot.html

Fujitsu Finland 2005. Kotisivut. [Online] Viitattu 27.11.2005
http://fi.fujitsu.com/palvelut/sovelluspalvelut/verkkotp_ratkaisut/

Karhunen, Harri 2004. Dynaaminen malli liiketoiminta sovellusten integroimiseksi. [Online] Viitattu 27.11.2005
http://66.102.9.104/search?q=cache:t3ZrnAYEihIJ:www.plugit.fi/julkaisut/15-Karhunen.pdf+Service+Integrator&hl=fi&lr=lang_fi

Microsoft 2005. Kotisivut. [Online] Viitattu 27.11.2005
http://www.microsoft.com/finland/security/professional/wirel_sec4.asp

Kuvat:

Kuva 1. Microsoft 2004. [Online] Viitattu 14.9.2004.
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/intwork/inbe_vpn_LDGG.asp

Kuva 2. Microsoft 2004. [Online] Viitattu 14.9.2004.
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/intwork/inbe_vpn_LDGG.asp

Kuva 3. Microsoft 2004. [Online] Viitattu 14.9.2004.
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/intwork/inbe_vpn_LDGG.asp

Kuva 4. Microsoft 2004. [Online] Viitattu 14.9.2004.
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/intwork/inbe_vpn_LDGG.asp

Kuva 5. Netopia 2005. [Online] Viitattua 29.10.2005
http://www.netopia.com/equipment/intl/emea/uk/ipsec.html

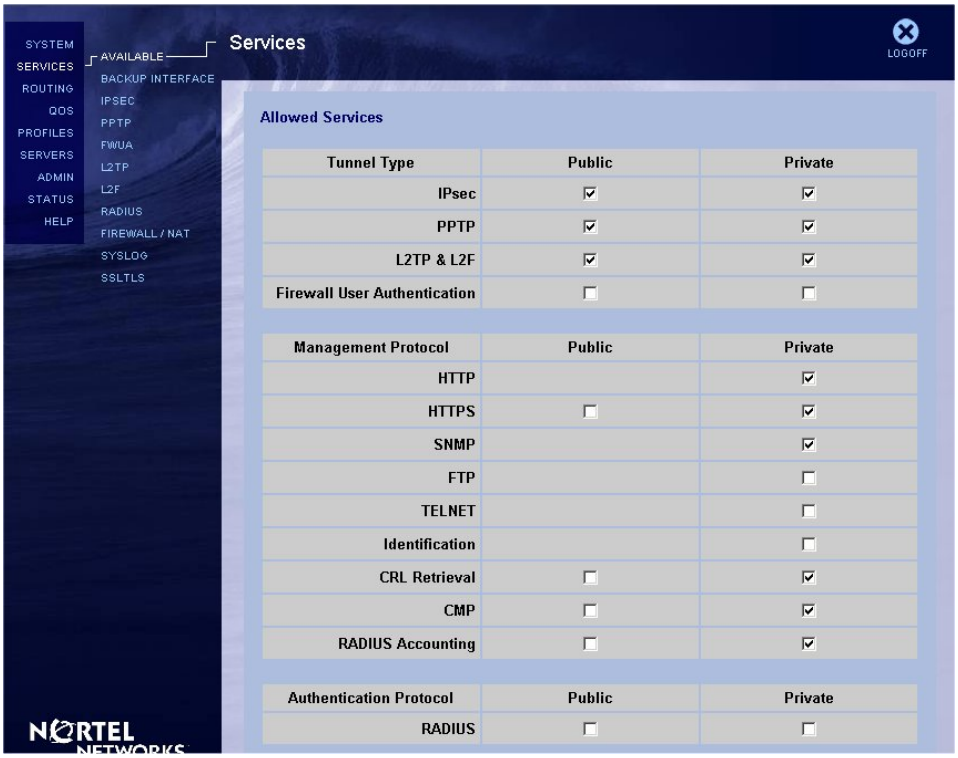
Kuva 6. Perlmutter & Zarkower 2001: 87

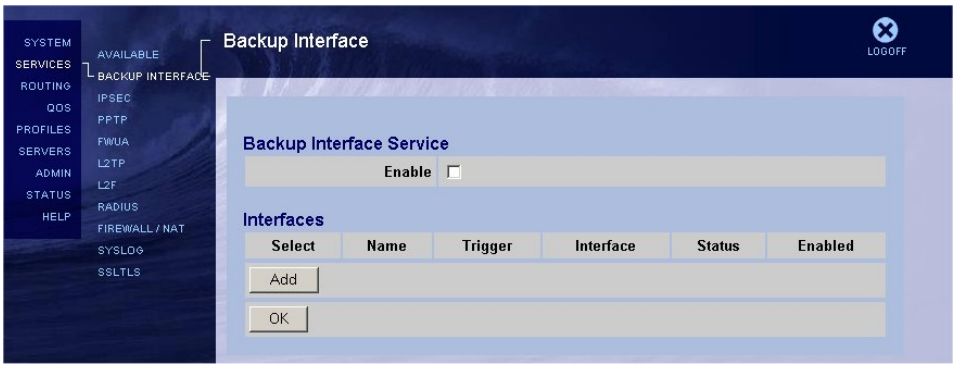
Kuva 7. George Mason University 2005. [Online Viitattu 19.2.2005].
http://bass.gmu.edu/courses/ECE543/reportsF01/arveal.pdf

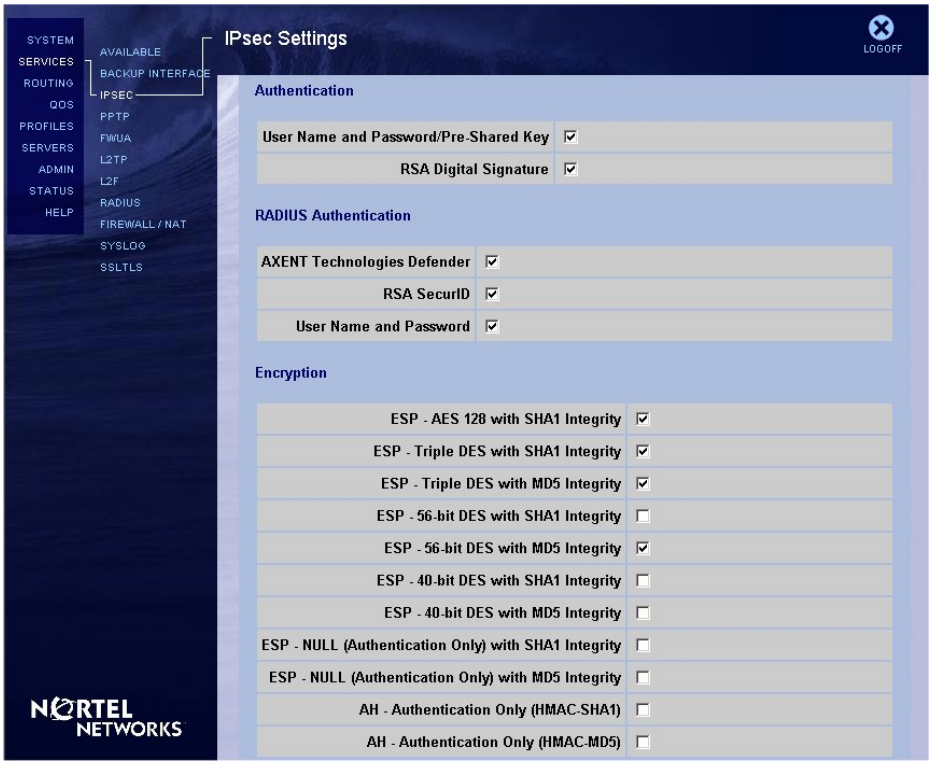
9 Liitteet

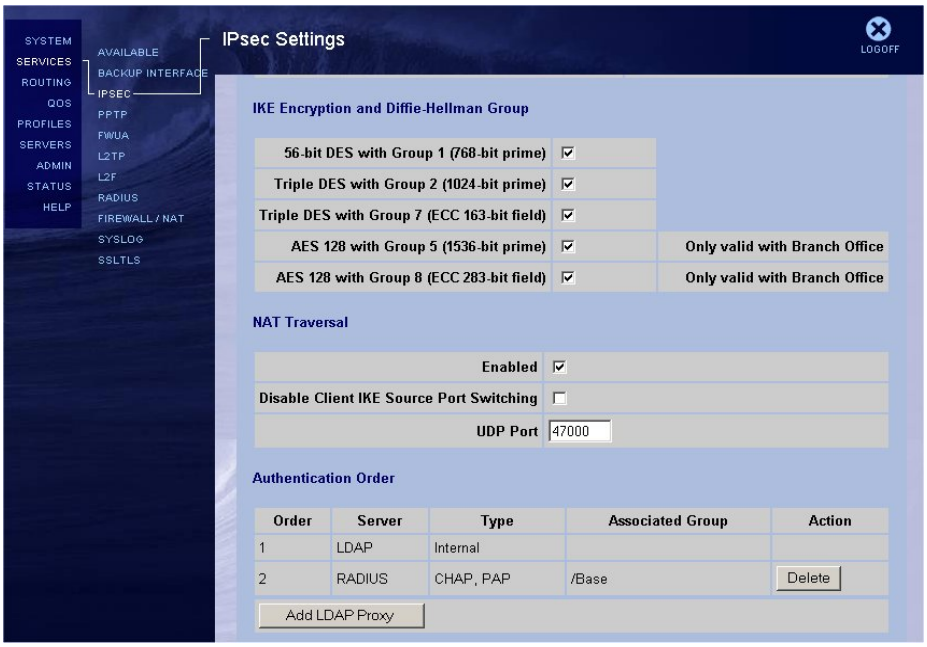
Liite 1: Esimerkkejä Nortel 1100 VPN-laitteen Services valikosta

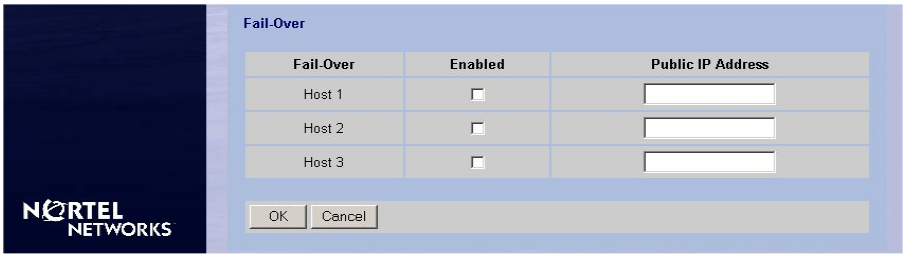
Liitteen kuvat ovat Nortel 1100 -laitteen Services-valikosta, josta halusin tuoda esille muutaman esimerkin mitä laitteen valikoissa on. Laitteesta löytyy hyvin monipuoliset ominaisuudet ja liitteen kuvista näkyy muun muassa mahdolliset salausmenetelmät, varmistusliitännän tiedot sekä Syslog-välityksen erilaiset mahdollisuudet.

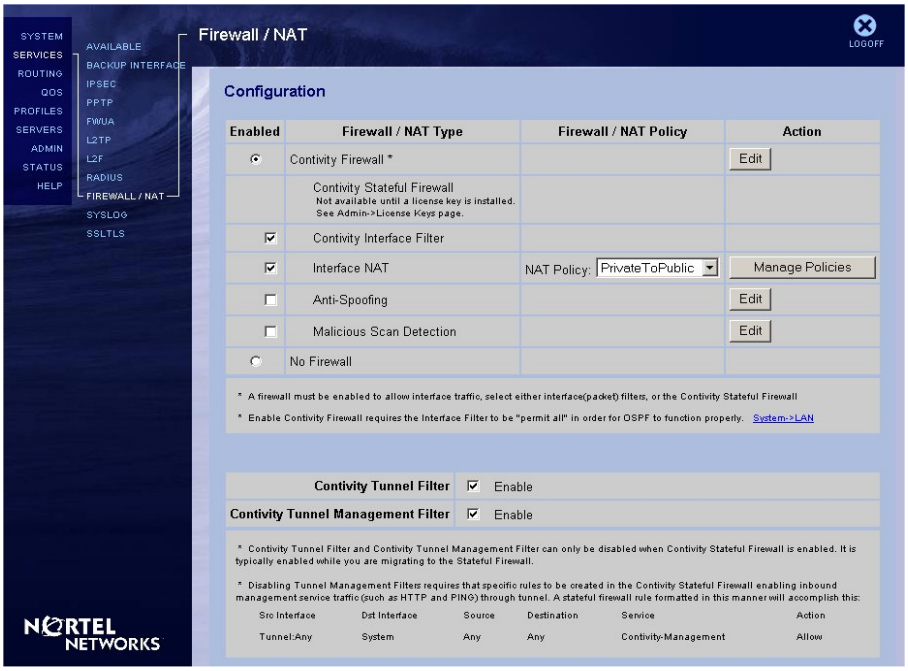


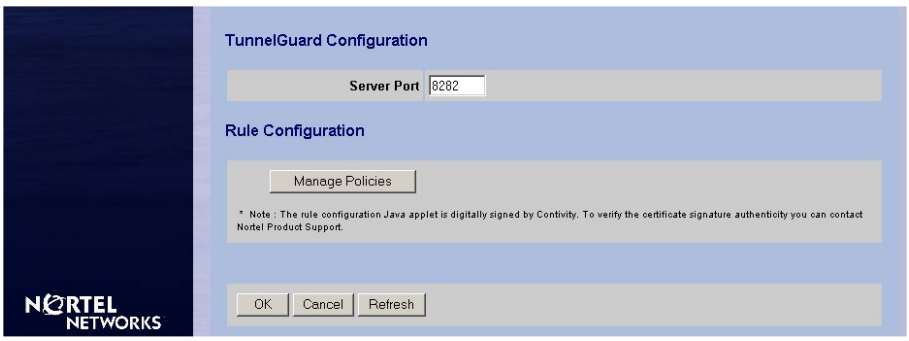


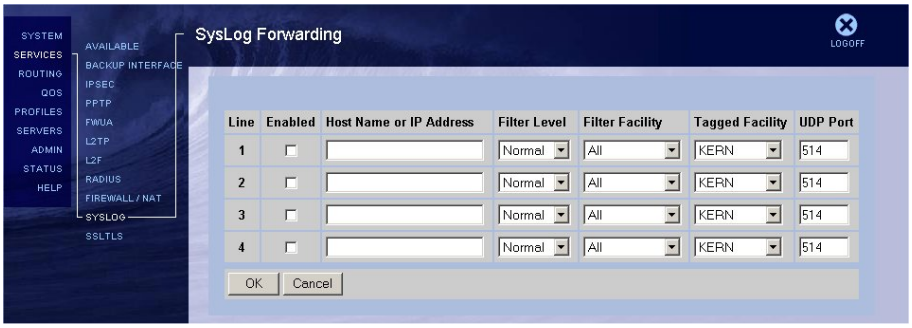

SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP
AVAILABLE
BACKUP INTERFACE
IPSEC
PPTP
FWUA
L2TP
L2F
RADIUS
FIREWALL / NAT
SYSLOG
SSLTLS
NORTEL NETWORKS
IPsec Settings
LOGOFF
Authentication
User Name and Password/Pre-Shared Key
RSA Digital Signature
RADIUS Authentication
AXENT Technologies Defender
RSA SecurID
User Name and Password
Encryption
ESP - AES 128 with SHA1 Integrity
ESP - Triple DES with SHA1 Integrity
ESP - Triple DES with MD5 Integrity
ESP - 56-bit DES with SHA1 Integrity
ESP - 56-bit DES with MD5 Integrity
ESP - 40-bit DES with SHA1 Integrity
ESP - 40-bit DES with MD5 Integrity
ESP - NULL (Authentication Only) with SHA1 Integrity
ESP - NULL (Authentication Only) with MD5 Integrity
AH - Authentication Only (HMAC-SHA1)
AH - Authentication Only (HMAC-MD5)

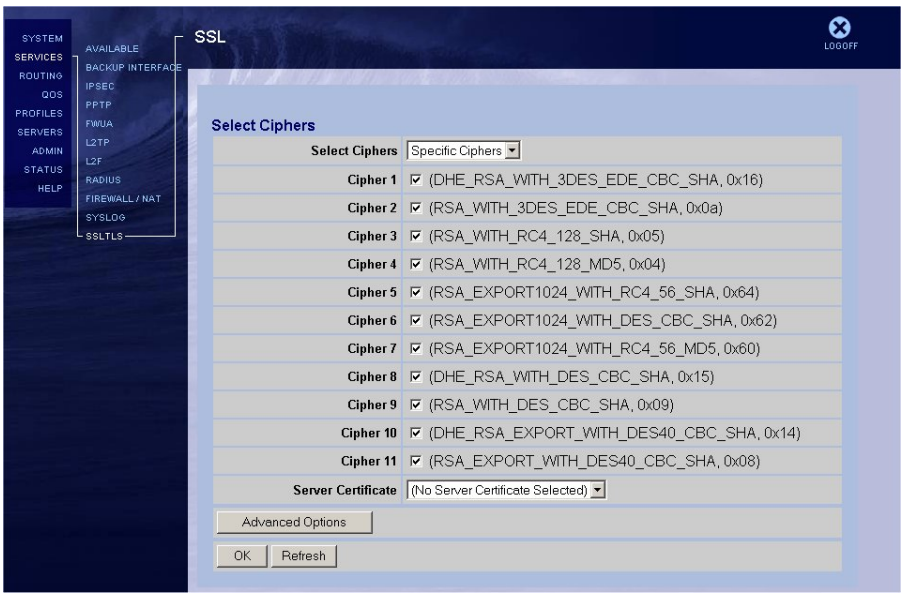

SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP
AVAILABLE
BACKUP INTERFACE
IPSEC
PPTP
FWUA
L2TP
L2F
RADIUS
FIREWALL / NAT
SYSLOG
SSLTLS
IPsec Settings
LOGOFF
IKE Encryption and Diffie-Hellman Group
56-bit DES with Group 1 (768-bit prime)
Triple DES with Group 2 (1024-bit prime)
Triple DES with Group 7 (ECC 163-bit field)
AES 128 with Group 5 (1536-bit prime)
Only valid with Branch Office
AES 128 with Group 8 (ECC 283-bit field)
Only valid with Branch Office
NAT Traversal
Enabled
Disable Client IKE Source Port Switching
UDP Port
47000
Authentication Order
Order
Server
Type
Associated Group
Action
1
LDAP
Internal
2
RADIUS
CHAP, PAP
/Base
Delete
Add LDAP Proxy


Fail-Over
Fail-Over
Enabled
Public IP Address
Host 1
Host 2
Host 3
OK
Cancel
NORTEL NETWORKS


SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP
AVAILABLE
BACKUP INTERFACE
IPSEC
PPTP
FWUA
L2TP
L2F
RADIUS
FIREWALL / NAT
SYSLOG
SSLTLS
Firewall / NAT
LOGOFF
Configuration
Enabled
Firewall / NAT Type
Firewall / NAT Policy
Action
Contivity Firewall *
Edit
Contivity Stateful Firewall
Not available until a license key is installed.
See Admin->License Keys page.
Contivity Interface Filter
Interface NAT
NAT Policy: PrivateToPublic
Manage Policies
Anti-Spoofing
Edit
Malicious Scan Detection
Edit
No Firewall
* A firewall must be enabled to allow interface traffic, select either interface(packet) filters, or the Contivity Stateful Firewall
* Enable Contivity Firewall requires the Interface Filter to be "permit all" in order for OSPF to function properly. System->LAN
Contivity Tunnel Filter
Enable
Contivity Tunnel Management Filter
Enable
* Contivity Tunnel Filter and Contivity Tunnel Management Filter can only be disabled when Contivity Stateful Firewall is enabled. It is typically enabled while you are migrating to the Stateful Firewall.
* Disabling Tunnel Management Filters requires that specific rules to be created in the Contivity Stateful Firewall enabling inbound management service traffic (such as HTTP and PING) through tunnel. A stateful firewall rule formatted in this manner will accomplish this:
Src Interface
Dst Interface
Source
Destination
Service
Action
Tunnel:Any
System
Any
Any
Contivity-Management
Allow
NORTEL NETWORKS


TunnelGuard Configuration
Server Port 8282
Rule Configuration
Manage Policies
* Note : The rule configuration Java applet is digitally signed by Contivity. To verify the certificate signature authenticity you can contact Nortel Product Support.
OK
Cancel
Refresh
NORTEL NETWORKS


SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP
AVAILABLE
BACKUP INTERFACE
IPSEC
PPTP
FWUA
L2TP
L2F
RADIUS
FIREWALL / NAT
SYSLOG
SSLTLS
SysLog Forwarding
LOGOFF
Line
Enabled
Host Name or IP Address
Filter Level
Filter Facility
Tagged Facility
UDP Port
1
2
3
4
Normal
All
KERN
514
OK
Cancel


SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP
AVAILABLE
BACKUP INTERFACE
IPSEC
PPTP
FWUA
L2TP
L2F
RADIUS
FIREWALL / NAT
SYSLOG
SSLTLS
SSL
LOGOFF
Select Ciphers
Select Ciphers
Specific Ciphers
Cipher 1
(DHE_RSA_WITH_3DES_EDE_CBC_SHA, 0x16)
Cipher 2
(RSA_WITH_3DES_EDE_CBC_SHA, 0x0a)
Cipher 3
(RSA_WITH_RC4_128_SHA, 0x05)
Cipher 4
(RSA_WITH_RC4_128_MD5, 0x04)
Cipher 5
(RSA_EXPORT1024_WITH_RC4_56_SHA, 0x64)
Cipher 6
(RSA_EXPORT1024_WITH_DES_CBC_SHA, 0x62)
Cipher 7
(RSA_EXPORT1024_WITH_RC4_56_MD5, 0x60)
Cipher 8
(DHE_RSA_WITH_DES_CBC_SHA, 0x15)
Cipher 9
(RSA_WITH_DES_CBC_SHA, 0x09)
Cipher 10
(DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, 0x14)
Cipher 11
(RSA_EXPORT_WITH_DES40_CBC_SHA, 0x08)
Server Certificate
(No Server Certificate Selected)
Advanced Options
OK
Refresh

10 Sanasto

AH-protokolla (Authentication Header)
AH (Authentication Header) on autentikointiprotokolla. AH-nimi on tullut siitä, että kyseinen protokolla laskee IPSec-paketin avaimellisen tiivisteen ja sijoittaa sen paketin otsikkokenttään. (Tampereen Teknillisen Yliopiston Tietotekniikan osasto 2005)

ATMP (Ascend Tunnel Management Protocol)
Ascend Communicationsin toteuttamana tunnelointiprotokolla. (Perlmutter & Zarkower 2001: 138)

BayDVS (Bay Dial VPN Services)
VTP-tunnelointiprotokollan suunnittelusta irrottautuneen Bay Networksin suunnittelema tunnelointiprotokolla. (Perlmutter & Zarkower 2001: 138-139)

CHAP (Challenge and Handshake Protocol)
ISDN-verkoissa soittajan tunnistukseen määritelty tunnistuskäytäntö. Tätä menettelyä käytetään useiden valmistajien ISDN-reitittimissä. (Jaakkohuhta 2003: 86)

Datagram
Tietosähke, tietoliikenneverkoissa siirrettävä tietopaketti, joka sisältää muun muassa kohteen osoitteen ja muut tarvittavat tiedot varsinaisen siirrettävän datan lisäksi. (Jaakkohuhta 2003: 126)

DOA (Defective On Arrival)
DOA-laitteilla tarkoitetaan laitteita, joissa todetaan perusteltu vika ensimmäisen käyttöönoton yhteydessä joko loppuasiakkaalla tai jälleenmyyjällä. (Hewlett-Packard 2005)

DoS (Denial Of Service)
Palvelunestohyökkäys. Tällaisella hyökkäyksellä isketään jonkun palveluntarjoajan (esim. hakukoneen) kimppuun ja estetään tätä toimimasta normaalisti. Normaali tapa tehdä tällainen operaatio on ylikuormittaa palvelin siten, ettei se ehdi enää palvella normaaleja käyttäjiä. (Helsingin Ammattikorkeakoulu Stadia 2004)

EDI (Electronic Data Interchange)
EDI tarkoittaa organisaatioiden välistä tiedonsiirtoa. Sen tavoitteena on rationalisoida hallinnon elektroninen tiedonsiirto yhtenäisillä suosituksilla. (Jaakkohuhta 2003: 167)

ESP (Encapsulating Security Payload)
ESP on turvallisuusominaisuuksia sisältävä protokolla. ESP huolehtii luottamuksellisuudesta, tiedon alkuperän todentamisesta, yhteydettömästä tiedon eheydestä ja rajoitetusti liikenteen kulun luottamuksellisuudesta. (Tekninen Korkeakoulu Helsinki 2004)

GRE (Generic Routing Encapsulation)
GRE on Ciscon kehittämä IP-tunnelointiprotokolla. GRE:n sisällä tunneloidaan tavallisesti VPN-yhteyksiä ja aivan tavallisia IP-paketteja, mutta se osaa siirtää myös multicast- ja IPv6 -liikennettä. (Wikipedia 2004)

IETF (Internet Engineering Task Force)
Järjestö, jonka tehtävänä on ylläpitää ja kehittää Internetin ja IP-teknologioiden standardointia ja julkaista suosituksia niiden käytöstä. (Jaakkohuhta 2003: 251)

IKE-protokolla (Internet Key Exchange)
IKE on turvallisuusprotokolla neuvotteluun ja autentikointiin. Sitä käytetään IPSec-protokollan yhteydessä ja IKE-protokolla on määritelty IETF (Internet Engineering Task Force) toimesta RFC:ssä (Request for Comments) 2409. (Searchsecurity.com 2005)

IP (Internet Protocol)
TCP/IP-protokollaperheen OSI-mallin verkkokerroksen reitittävä yhteydetön tietosähkepohjainen käytäntö. (Jaakkohuhta 2003: 268)

IPSec
IETF:n määrittelemä standardi IP-liikenteen suojaamiseksi pakettitasolla. (Jaakkohuhta 2003: 270)

ISAKMP (Internet Security Association and Key Management Protocol)
Aiemmin IKE-protokolla tunnettiin nimellä ISAKMP/Oakley, joka on yksi IETF:n suosimista avaintenhallintaprotokollista. ISAKMP (Internet Security Association and Key Management Protocol) on protokolla, jonka avulla IPSec-liikenteen avaintenvaihto voidaan toteuttaa erityisellä protokollalla. (Tampereen Teknillisen Yliopiston Tietotekniikan osasto 2005)

ISP (Internet Service Provider)
Internet palveluntarjoaja. Yhteisö tai yritys joka tarjoaa Internet-yhteyksiä ja / tai muita verkkopalveluita asiakkailleen. (Jaakkohuhta 2003: 274)

Istunto (Session)
Tietoliikenneyhteydessä olevien käyttäjien päätteiden välinen yhteyden-pitojakso. (Jaakkohuhta 2003: 275)

L2F (Layer 2 Forwarding)
L2F on Ciscon kehittämä nimensä mukaisesti OSI-mallin 2. tasolla toimiva protokolla, jota käytetään mm. VPN-verkkojen toteuttamiseen. L2F-protokolla keskittyy tarjoamaan standardeihin pohjautuvan tunnelointimekanismin tiedonsiirrolle. (Silván, Markus 2001)

L2TP (Layer 2 Tunneling Protocol)
Internet Engineering Task Force (IETF) määrittelemä tunnelointiprotokolla. L2TP on Ciscon ja Microsoftin kehittämä VPN-tunnelointiprotokolla joka toimii OSI-mallin 2. kerroksessa, ja siten tukee myös ei-IP-protokollia. L2TP on yhdistelmä L2F:stä ja PPTP:stä. (Jaakkohuhta 2003: 303) (Wikipedia 2004)

MD5 (Message digest 5.)
MD5 on salausmenetelmä, jota käytetään viestien autentikoimiseen. Se luo annetusta selväkielisestä tekstistä 128 bitin salatun viestin. On laskennallisesti mahdotonta löytää toista tekstiä, josta MD5:llä saisi saman tarkastussumman, joten kyseinen menetelmä yksikäsitteisesti varmentaa tekstin alkuperäisyyden. (Tekninen Korkeakoulu Helsinki 2004)

NAS (Network Access Server)
NAS-palvelimella voi toimia monessa eri tehtävässä. Sitä käytetään muun muassa reunareitittimenä, sisäänsoittopalvelimena ja tunnelointipalvelimena. (Tekninen Korkeakoulu, tietoverkkolaboratorio 2004)

NAT (Network Address Translation)
NAT on IP-verkoissa tapahtuva menettely, jossa sisäverkon yksityiset osoitteet muunnetaan liikennöitäessä julkisiin verkkoihin virallisiksi IP-osoitteiksi. NAT:in tarkoituksena on parantaa tietoturvaa yksityisissä verkoissa ja ratkaista sisäverkon ongelmat rajallisen IP-osoitemäärän suhteen. (Jaakkohuhta 2003: 365)

OVT (Organisaatioiden Välinen Tiedonsiirto)
OVT vastaan Suomessa EDI:ä. OVT sisältää mallin, jonka mukaan kehitetään OVT:n suosituksia, nämä noudattavat ja täydentävät kansainvälisiä EDI-suosituksia ja täyttävät samalla kotimaiset tarpeet. (Jaakkohuhta 2003: 398)

PPP (Point-to Point Protocol)
TCP/IP:n etäyhteysprotokolla, jota käytetään esimerkiksi lähiverkkojen reitittimien ja siltojen välillä. PPP soveltuu synkronisille ja asynkronisille yhteyksille ja on protokollariippumaton. (Jaakkohuhta 2003: 431)

PPTP (Point-to-Point Tunneling Protocol)
Microsoftin kehittämä käytäntö, jolla työasemilta voi avata virtuaaliyhteyden reititinverkon yli. Protokolla, joka tukee

moniprotokollaisia virtuaalisia yksityisverkkoja. (Jaakkohuhta 2003: 432)

QOS (Quality Of Services)
Menetelmiä, joilla pyritään takaamaan verkon palvelun laatu tietyille sovelluksille ja käyttäjille. (Jaakkohuhta 2003: 447)

RADIUS (Remote Authentication Dial-In User Service)
RADIUS protokollaa käytetään keskitetyn käyttöoikeuksien valtuuttamisen, vahvistamisen ja tilitietojen hallintaan puhelinverkkoyhteyksissä ja näennäisissä yksityisverkoissa sekä langattomassa verkkokäytössä. (Microsoft 2005)

RFC (Request for Comments)
Kommenttipyyntöjä, jotka tunnetaan TCP/IP-maailmassa. Viestit sisältävät ehdotelmia tiettyjen ominaisuuksien toteuttamiseksi. IETF:n tehtävä on julkaista suosituksia, RFC-pyyntöjä Internetin ja IP-teknologioiden standardointiin liittyen. (Jaakkohuhta 2003: 462)

SI (Service Integrator)
Palveluintegraattori, jonka tehtävänä on yhdistää eri palvelut toisiinsa ja luoda rajapinta asiakkaan ja palvelun välille. (Karhunen, Harri 2004)

TCP (Transmission Control Protocol)
OSI-mallin mukainen kuljetuskerroksen luotettava kuljetuspalvelu. (Jaakkohuhta 2003: 532)

TCP/IP (Transmission Control Protocol / Internet Protocol)
TCP/IP on usean tietoverkkoprotokollan yhdistelmä, jota käytetään Internet-liikennöinnissä. IP-protokolla on alemman tason protokolla, joka vastaa päätelaitteiden osoitteistamisesta ja pakettien reitittämisestä tietoliikenneverkossa. IP-protokollan päällä voidaan ajaa useita muita verkko- tai kuljetuskerroksen protokollia, joista TCP-protokolla on yleisin. Se vastaa kahden päätelaitteen välisestä tiedonsiirtoyhteydestä, pakettien järjestämisestä ja hukkuneiden pakettien uudelleenlähetyksestä. (Wikipedia 2004)

UDP (User Datagram Protocol)
Kuljetuskerroksen (OSI-mallin 4.kerros) tietosähkepohjainen yhteydetön kuljetusprotokolla. (Jaakkohuhta 2003: 560)

VAN (Value Added Networks)
Lisäarvoverkko. Tiedonsiirtopalveluita välittävä tietoverkko, johon saattaa liittyä erilaisia palveluita niin, että tieto sen läpi kulkiessaan saa lisäarvoa. (Jaakkohuhta 2003: 575)

VPN (Virtual Private Network)
Tietoliikennetekniikka, jolla yhdistetään yritysten eri toimipaikoissa sijaitsevia lähiverkkoja ja liikkuvia päätelaitteita käyttäen siirtotienä julkisia verkkoja. (Jaakkohuhta 2003: 589)

VTP (Virtual Tunneling Protocol)
Virtuaalinen tunnelointiprotokolla. Layer 3 -tunnelointimenetelmä, jonka Bay Networksin ja US Roboticsin insinöörit keksivät vuonna 1996. (Perlmutter & Zarkower 2001: 139)

WAN (Wide Area Network)
Laaja tietoliikenneverkko. Tälle tietoliikenneverkolle on tyypillistä laaja maantieteellinen ulottuvuus paikkakunnalta tai jopa maasta toiseen. Tällaiset laajat verkot toteutetaan yleensä yhdistelemällä erilaisia verkko-tekniikoita, kuten Frame Relay ja ATM. (Jaakkohuhta 2003: 593)