STADIA
HELSINGIN AMMATTIKORKEAKOULU

TEKNIIKAN JA LIIKENTEEN TOIMIALA

Tietotekniikka

Tietoliikennetekniikka

INSINÖÖRITYÖ

PALVELUNTOIMITTAJIEN ETÄKÄYTTÖYHTEYDET

Työn tekijä: Petri Mäkynen
Työn valvoja: Marko Uusitalo
Työn ohjaaja: Ari Silfverberg

Työ hyväksytty: __. __. 2007

Marko Uusitalo
lehtori

ALKULAUSE

Tämä insinöörityö on tehty Fingrid Oyj:lle. Haluan kiittää kaikkia työssä mukana olleita sekä työn ohjausta.

Helsingissä 31.3.2007

Petri Mäkynen

STADIA
HELSINGIN AMMATTIKORKEAKOULU

INSINÖÖRITYÖN TIIVISTELMÄ

Tekijä: Petri Mäkynen	
Työn nimi: Palveluntoimittajien etäkäyttöyhteydet	
Päivämäärä: 31.3.2007	Sivumäärä: 47 + 4 liitettä
Koulutusohjelma: Tietotekniikka	Suuntautumisvaihtoehto: Tietoliikennetekniikka
Työn valvoja: Lehtori Marko Uusitalo Työn ohjaaja: DI Ari Silfverberg	

Tässä insinöörityössä tutkittiin kolmannen osapuolen etäkäyttöyhteyksien toteuttamismahdollisuuksia. Työ tehtiin Fingrid Oyj:lle, joka vastaa Suomen päävoimansiirtoverkosta.

Työn ensimmäisessä vaiheessa opiskeltiin yksityisten virtuaaliverkkojen teoriaa. Virtuaaliverkkotekniikoiden käyttömahdollisuudet opiskeltiin käytännön kokemuksen kautta. Tämän jälkeen työssä selvitettiin SSL VPN -tekniikan teoriaa ja sen todellista toimintaa. Lisäksi tutkittiin kolmannen osapuolen yhteyksien heikkouksia ja vahvuuksia.

Tämä työ mahdollisti myös tutustumisen tietoturvastandardeihin ja käytännön SSL VPN -toteutukseen.

Työn tuloksena todettiin SSL VPN -arkkitehtuurin toiminta- ja käyttömahdollisuudet. SSL VPN todettiin tehokkaimmaksi ja joustavimmaksi tavaksi tehdä palveluntoimittajien etäkäyttöyhteydet. Lisäksi työssä on pohdittu palveluntoimittajien etäkäyttöyhteyksien ongelmien ratkaisuja. Työn ohella toteutettiin käytännön SSL VPN toteutus Fingrid Oyj:lle.

Avainsanat: SSL VPN, IPSec, etäyhteys, SSL/TLS, Cyber Security

STADIA
HELSINGIN AMMATTIKORKEAKOULU

ABSTRACT

Name: Petri Mäkynen

Title: Third Party Remote Access

Date: 31.3.2007 Number of pages: 47 + 4 appendexes

Department: Information technology Study Programme: Telecommunications

Supervisor: Marko Uusitalo, Senior Lecturer

Instructor: Ari Silfverberg, M. Sc.

The purpose of this study was to examine different possibilities to implement 3rd party remote access. This study was carried out for Fingrid Plc, which is responsible for the main transmission grid in Finland.

Some background information from Virtual Private Networks was studied first. However, a major part of this study is based on learning different ways to implement VPN techniques through practical experience. One of the main targets was to understand SSL VPN architecture and how it works. A further objective was to examine the strengths and weaknesses of 3rd party remote access.

This study also provided a possibility to gain information on security standards and a real VPN implementation.

Based on the findings of this study it seems that SSL VPN is the most effective and flexible method to implement 3rd party remote access. In addition, this study provides solutions to the problems in the 3rd party remote access system. Within this study, a real SSL VPN implementation was carried out for Fingrid Plc.

Keywords: SSL VPN, IPSec, Remote Access, SSL/TLS, Cyber Security

SISÄLLYS

LYHENTEITÄ JA MÄÄRITELMIÄ

AES	Advanced Encryption Standard; symmetrinen salausmenetelmä
AH	Authentication Header; IPSec määrittelyn mukainen salausotsikko
ARP	Address Resolution Protocol; pyytää MAC-osoitetta vastaavan IP-osoitteen verkossa
CA	Certificate Authority; Varmenneviranomainen (luotettu kolmas osapuoli)
DES	Data Encryption Standard; symmetristä salausta hyödyntävä menetelmä
3DES	TripleDES; parannettu versio DES-salauksesta, jossa DESia käytetään kolme kertaa
ESP	Encapsulation Security Payload; IPSec määrittelyn mukainen salausotsikko
FTP	File Transfer Protocol; tiedostonsiirto protokolla
HMAC	Keyed-hash Message Authentication Code; menetelmä eheys- ja todennussumman laskentaan
HTTP	Hyper Text Transfer Protocol; protokolla Internet-sivustojen näyttämiseen
HTTPS	Hyper Text Transfer Protocol; protokolla Internet-sivustojen näyttämiseen, jossa käytetään hyväksi SSL/TLS-salausta
IEC	International Electrotechnical Commission; sähköalan standardointiorganisaatio
IETF	Internet Engineering Task Force; Internetissä standardeja kehittävä organisaatio
IKE	Internet Key Exchange; salausavainten vaihtamiseen kehitetty protokolla
IP	Internet Protocol; verkkokerroksella toimiva protokolla TCP/IP-protokollaperheestä. esim. IP versio 4 tai 6
ISAKMP	Internet Security Association and Key Management Protocol; avainten-hallinta protokolla
ISO	International Standards Organization; standardointiorganisaatio
IPSec	Internet Protocol Security; tietoturva laajennus IP-protokollaan
LAN	Local Area Network; paikallisverkko

MAC	Media Access Control; käytetään laiteosoitteen yhteydessä Ethernet-verkkoissa
MAC	Message Authentication Code; kuvausfunktiolla muodostettu varmenne
MD5	Message Digest 5; eheyssumma tai tiiviste, käytetään virheiden havaitsemiseen
MPLS	Multiprotocol Label Switching; lippukytkentäinen paketinvälitys
NAT	Network Address Translation; osoitteenkäännösmenetelmä IP-verkoissa
NERC	North American Electric Reliability Council; amerikkalainen järjestö, jonka tavoitteena on huolehtia sähkönsiirron luotettavuudesta
OSI	Open Systems Interconnection; ISO:n julkaisema 7-kerroksinen viitemalli tietoliikenteelle
PVLAN	Private Virtual Local Area Network; mahdollistaa virtuaaliverkkojen jakamisen loogisiin verkkoihin
RFC	Request For Comments; IEFT:n julkaisema dokumenttisarja, joka sisältää standardeja ja määritelmiä
RSA	Rivest, Shamir, and Adleman; epäsymmetrinen salausmenetelmä
SA	Security Association; IPSec määrittelyn mukainen turvayhteys
SADB	Security Association Database; tietoturvayhteyksien tietokanta tietoliikennelaitteella
SHA	Secure Hash Algorithm; tiivistefunktio esim. SHA-1
SPI	Secure Parameters Index; parametri turvayhteyksien hallintaan
SSL	Secure Socket Layer; tietoturvaprotokolla liikenteen salaamiseen
TCP	Transmission Control Protocol; kuljetuskerroksen yhteydellinen tiedonsiirtoprotokolla
TCP/IP	Transmission Control Protocol/Internet Protocol; Internet-pohjaiseen tiedonsiirtoon kehitetty protokollaperhe
TLS	Transport Layer Security; SSL 3.0 versiosta kehitetty tietoturvaprotokolla
UDP	User Datagram Protocol; kuljetuskerroksen yhteydetön tiedonsiirtoprotokolla
X.509	IEC:n määrittely digitaaliselle sertifikaatille
VPN	Virtual Private Network; yleisesti salattu virtuaalinen yksityisverkko
WAN	Wide Area Network; etäverkko

1 JOHDANTO

Muutaman viimeisen vuoden aikana tietoliikenneyhteyksien saatavuus on merkittävästi parantunut ja samalla ovat laajakaistayhteyksien kaistanleveydet kasvaneet. Kaistanleveyksien kasvu eli yhteyksien nopeuden kasvaminen näkyy myös tietoliikenteen tehokkaana hyödyntämisenä ja tietoliikennepohjaisten sovelluksien kehittämisenä. Nykypäivänä lähes jokainen sovellus käyttää hyväksi tietoliikenneverkkoa ja asettaa myös tarpeita ohjelmien etäyhteyksille.

Yritykset antavat usein työntekijöilleen mahdollisuuden työskennellä etäyhteydellä työmatkoilla tai kotona. Yrityksen ulkoistaessa toimintoja tulee myös tarpeita rakentaa etäkäyttöyhteyksiä palveluntoimittajille. Palveluntoimittajien etäkäyttöyhteyksiä pohdittaessa suurimmaksi haasteeksi tulee tietoturvatason säilyttäminen.

Yrityksen toimiala tuo usein mukanaan erilaisia tarpeita etäkäyttöyhteyksien toteuttamiselle. Energia-alan automaatiojärjestelmät käyttävät yhä enemmän *Transmission Control Protocol/Internet Protocol* (TCP/IP) -tekniikkaan pohjautuvaa tiedonsiirtoa. TCP/IP tekee mahdolliseksi antaa oikeudet suoraan kunnossapitotiedon hakemiseen toimitetuista järjestelmistä.

Virtual Private Network (VPN) -yhteydet käsitetään yleisesti etäkäyttöyhteyksiksi. Etäkäyttöyhteyksien tarpeiden perusteella valitaan käyttöön soveltuva tekniikka. Tässä työssä tutustutaan VPN-tekniikoihin, jotka mahdollistavat etäkäyttöyhteyksien toteuttamisen. Työssä tutkitaan käytännön toteutusvaihtoehtoja ja toteutetaan käytännön toteutus. Lisäksi pohditaan amerikkalaisen standardiperheen soveltuvuutta määräämään tietoturvaehdot palveluntoimittajien etäyhteyksille.

2 TIETOTURVATAVOITTEET JA -HALLINTA

Tietoturva on käsitteenä hyvin laaja osa-alue, joka kattaa mm. verkkojen suunnittelun, laitteistot, ohjelmistot ja henkilöstön oikean asennoitumisen tietoturvan toteuttamiseen. Tietoturva ei ole ainoastaan tietoteknisten asioiden hoitamista vaan sisältää myös tiedon fyysisen turvaamisen. Tässä luvussa määritellään tietoturvan säilyttämisen merkitys, uhkakuvat ja riskeiltä suojautuminen.

2.1 Tietoturvan määrittäminen ja tavoitteet

Tietoturvaa tulee pitää yhtä tärkeänä osana kuin mitä tahansa muuta yrityksen liiketoimintoa. Tiedon saatavuuden parantuminen eli informaation verkottumisen ja yrityksien väliset yhteistyöt ovat aikaansaaneet kasvavien uhkien ja haavoittuvuuksien pelon. Tietoturva ei ole pelkästään ohjelmisto ja laitteisto haavoittuvuuksia vaan siihen sisältyy myös ihmisten toiminnasta aiheutuvia riskejä.

Tietoturvan toteuttamisen lähtökohtana on luoda tietoturvapolitiikka. Ilman tietoturvapolitiikkaa on tietoturvan toteuttaminen mahdotonta. Tietoturva voidaan saavuttaa oikealla valvonnalla, säännöillä, ohjelmistoilla ja laitteistoilla. Tämä ei kuitenkaan vielä riitä, vaan tietoturvan toteuttamiseen tarvitaan myös yrityksen johdon tuki, jotta yrityksen työntekijät ja kumppanit toimivat asetetun tietoturvapolitiikan mukaisesti.

Kasvava tiedon jakaminen ja hajautettu tietotekniikan käyttö asettaa tietoturvan saavuttamisen haasteelliseksi. Hajauttaminen vaikeuttaa järjestelmän kontrollointia ja heikentää myös keskitetyn hallinnan tehokkuutta. Suurin osa nykyisistä tietojärjestelmistä ei ole alun perin suunniteltu tietoturvallisiksi. Tällaiset järjestelmät asettavat teknisiä rajoituksia tietoturvan toteuttamiselle ja vaativat oikeanlaista hallintaa. Hallinta ja suunnittelu tulee tehdä hyvin huolellisesti ottaen yksityiskohtaiset asiat sekä järjestelmien väliset keskinäiset riippuvuudet huomioon. Lisäksi tarvitaan mahdollisesti asiantuntija-apua organisaation ulkopuolelta. [1, s. viii - ix.]

Tietoturvamääritykset

Tietoturvallisuuden tavoitteena on säilyttää tiedon luottamuksellisuus, eheys, saatavuus ja kiistämättömyys. Tavoitteet saavutetaan hallinnollisilla ja teknisillä toimenpiteillä. Luottamuksellisuudella tarkoitetaan ainoastaan asianmukaisten käyttäjien pääsyä saatavilla olevaan tietoon. Tämä varmistetaan tunnistautumisella. Tunnistautuminen yksilöi käyttäjän tai laitteen. Tunnistautuminen ei välttämättä vaadi erillistä toimintaa käyttäjältä.

Eheydellä tarkoitetaan sitä, että olemassa olevaa tietoa ei päästä muuttamaan ilman, että siitä jää jälki. Käytännössä tämä yleensä tarkoittaa sitä, että epäoikeutetut käyttäjät eivät voi muuttaa tietoa, johon heillä ei ole käyttöoikeuksia. Eheys voidaan saavuttaa todentamisella, jolla varmistetaan tunnistuksessa käytettyjen tietojen oikeellisuus. Todentamisella tarkoitetaan usein myös käyttäjän oikeuksia eli sallittuja toimenpiteitä.

Saatavuus käsittää oikeutetuille käyttäjille haluttuun tietoon pääsyn ja mahdollisuuden tiedon käsittelyyn. Kiistämättömyys on asia, jolla varmistutaan tietoverkossa, että henkilöt eivät voi kieltää toimintaansa jälkikäteen. [2.]

2.2 Riskien hallinta

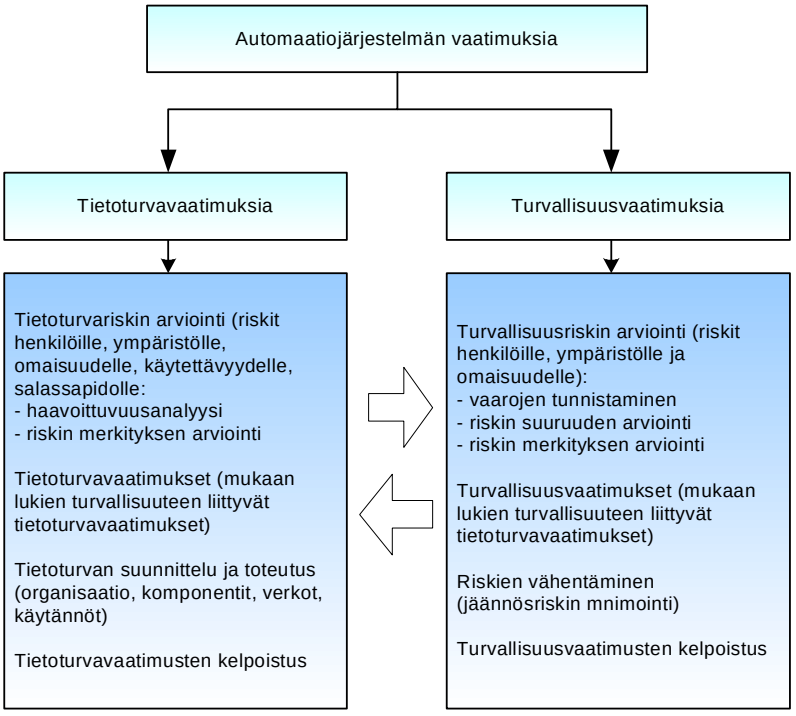
Riskien arvioinnissa määritellään suojattavan informaation menetyksen vaikutukset yrityksen toimintaan riskin toteutuessa. Yrityksien suojattava informaatio voi poiketa hyvin paljon eri yrityksien välillä, mutta tärkein asia on tunnistaa liiketoiminnan kannalta kriittinen informaatio.

Yrityksen tulisi määritellä riskien arviointi tiedon tärkeyden ja merkityksellisyyden perusteella. Riskien kartoituksen yhteydessä tulee laatia toimintaohjeet, joissa määritellään asioiden tärkeysjärjestys ja tarkka ohjeistus henkilöstön toimintaan riskin sattuessa. Tietoturvariskien kartoitus tulee sisällyttää organisaation riskien hallinnan yhteyteen. [1, s. 97.]

Automaatioympäristöissä riskillä tarkoitetaan haittaa tai muuta ei-toivottua tapahtumaa, jonka seurauksena voi aiheutua järjestelmän vaaral-

linen toiminta tai vikaantuminen, työtapaturma tai tuotannon keskeytyminen. Automaatiojärjestelmiin liittyvien tietojärjestelmien riskienhallinnan tavoitteena on, että järjestelmiin liittyvät tietoverkot ja niiden komponentit mukaan lukien sähkönsyöttö täyttävät järjestelmien käytettävyysvaatimukset. Erityisesti turvallisuuskriittisissä järjestelmissä tietoturvan vaatimustaso on korkea ja vaatii useita toimenpiteitä turvallisuuden varmistamiseksi.

Automaatioympäristöjä suunniteltaessa tietoturvavaatimukset eivät vielä välttämättä ole riittävän korkealla tasolla tai on jätetty kokonaan huomioimatta. Vaatimukset ohjaavat toimenpiteitä ja vaatimusten hallinta on avainasemassa, kun mitataan tietoturvan toteutumista järjestelmässä. Tärkeää on, että tietoturvavaatimuksia analysoidaan jo elinkaaren alkuvaiheissa, jotta asioihin pystytään reagoimaan ajoissa. Automaatiojärjestelmien tietoturvavaatimusten ja turvallisuusvaatimusten vuorovaikutus on esitetty kuvassa yksi. [3, s. 34 - 40.]



Kuva 1. Turvallisuusvaatimusten ja tietoturvavaatimusten vuorovaikutus [3, s. 36.]

3 LÄHTÖKOHDAT ETÄKÄYTTÖYHTEYKSIEN TOTEUTTAMISELLE

Etäkäyttöyhteydellä tarkoitetaan etäältä tapahtuvaa käyttöä. Etäkäyttöyhteys (VPN) muodostetaan yleisesti julkisen tietoliikenneverkon eli Internetin päälle (kuva 2). Tällaisia etäyhteyksiä kutsutaan yleisesti VPN-yhteyksiksi. VPN-yhteys voidaan muodostaa myös luotetussa verkossa varmistamaan, että tiedon eheys säilytetään. VPN-yhteyden määritelmä on hieman avoin käsite. Sen vuoksi tässä työssä VPN-yhteydellä käsitetään *Internet Protocol* (IP) -verkkoihin perustuvia VPN-yhteyksiä, joissa tiedonsiirtoon käytetään julkista Internetiä.

Muita VPN-yhteyden määritelmän täyttäviä yhteyksiä ovat mm. *Frame Relay* ja *Multiprotocol Label Switching* (MPLS) -tekniikoihin perustuvat kiinteät yhteydet. Kiinteillä yhteyksillä tarkoitetaan päästä päähän yhteyksiä, jotka ovat erotettu omiksi yhteyksiksi, joko fyysisesti tai loogisesti.

Kuva 2. Etäkäyttöyhteyden periaatekuva

Virtuaalisten yksityisverkkojen muodostuminen tapahtuu käyttämällä tunnelointiin sopivaa tietoliikenneprotokollaa. Tunnelointi tekee mahdolliseksi siirrettävän tiedon suojaamisen ja erottaa yhteyden omaksi loogiseksi yhteydeksi eli piilottaa yhteyden fyysisen topologian. Tiedon suojaamiselle on tullut tarve, koska useat tietoliikenneprotokollat kuljettavat verkossa tiedon tekstimuotoisena.

Internetin käyttäjämäärä on kasvanut räjähdysmäisesti, jonka seurauksena tietoverkkorikolliset ovat aktivoituneet. Tietoverkkorikollisilla on mahdollisuus hankkia informaatiota verkon välityksellä ja käyttää kaapattua tietoa ansiotarkoituksissa. Tärkeä asia on huomioida, että tietoverkkori-

kollisilla on suuret resurssit toiminnan organisoimiseen. Toiminta tapahtuu ympäri vuorokauden vuoden jokaisena päivänä ja asettaa haasteita tavoitteiden saavuttamiseen. [4, s. 10-20.]

Tietoverkkorikollisella on mahdollisuus lukea siirrettävän tiedon sisältö selkokielisenä tekstinä, jos yhteys ei ole toteutettu asianmukaisesti. Arkaluotoinen siirrettävä informaatio täytyy muuttaa salattuun eli kryptiseen muotoon, jotta verkossa matkalla olevaa tietoa ei ulkopuolinen pysty salakuuntelemaan. Tiedon suojaamiseen on kehitetty useita eri menetelmiä, joita tässä työssä käsitellään myöhemmin.

Etäkäyttöyhteyksien ymmärtäminen vaatii IP-verkkoihin pohjautuvan tietoliikenteen perustan tuntemuksen. Tässä luvussa käsitellään IP-verkkojen perusteita ja selvitetään tiedonvälittämistä Internetissä.

3.1 OSI-viitemalli

Tiedonsiirto vaatii sovitun tietoliikenneprotokollan, jotta haluttu yhteys voitaisiin muodostaa. Protokollaa voidaan verrata vieraaseen kieleen, jolloin kommunikointi ei ole mahdollista, jos osapuolet eivät keskustele samalla kielellä. *Open Systems Interconnection* (OSI) -malli syntyi vuonna 1983, kun *International Standards Organization* (ISO) hyväksyi tämän OSI-komitean esityksen. Tavoitteena oli luoda kerroksiin perustuva malli, jossa kerrokset tuottavat palveluita ylemmälle kerrokselle ja käyttävät hyväksi palveluita alemmalta kerrokselta. OSI-malli kuvaa tiedonlähettämisen ja vastaanottamisen vaiheet tietoliikenneverkossa siirrettävälle tiedolle. OSI-mallia käytetäänkin usein tietoliikenneprotokollan suunnittelussa. [5, s. 8.]

Käytännössä sovellukselta lähetettävä tieto kulkee OSI-mallin läpi käytettävän tietoliikenneprotokollan määrittelyn mukaisesti. Puolestaan tietoliikenneverkosta vastaanotettu tieto purkautuu sovellukselle OSI-mallin fyysiseltä kerrokselta läpi koko mallin aina sovelluskerrokselle asti (kuva 3).

Seuraavassa on esitetty OSI-mallin kerroksilla määriteltävät toiminnot:

Fyysinen kerros

Fyysinen kerros käsittää mekaanisen ja sähköisen liitännän tiedonsiirtoverkkoon tai kanavaan. Esimerkkejä fyysisen kerroksen määrittelyistä ovat valokuituliitännät ja kaapelointivaatimukset. Fyysinen kerros käsittää myös muitakin suosituksia, kuten esim. tietokoneen sarjaportin mekaaniset määritykset.

Siirtoyhteyskerros

Siirtoyhteyskerroksen tärkeimpiä tehtäviä on huolehtia yhteyden virheettömyydestä kahden pisteen välillä. Kerroksen tehtäviin kuuluu myös virheiden havaitseminen ja niistä toipuminen sekä siirrettävän tietovuon hallinta. Monessa protokollatoteutuksessa virheistä toipuminen tapahtuu myös kuljetuskerroksella, kuten IP-pohjaisessa liikenteessä. *Ethernet*-verkoissa laitteilla on fyysinen osoite, jota kutsutaan *Media Access Control* (MAC) -osoitteeksi. IP-liikenteen perusta muodostuu näiden fyysisten osoitteiden päälle.

Verkkokerros

Verkkokerroksen tunnistaa siitä, että se tarjoaa sellaisia yhteyksiä, jotka eivät ota kantaa, miten sen alapuolella siirtoyhteydet on toteutettu. IP-pohjaisessa tiedonsiirrossa verkkokerroksella muodostetaan ylemmän tason tiedoista paketti. Tämä paketti sisältää mm. tiedon lähdelaitteen ja kohdelaitteen IP-osoitteista. IP-osoitteiden avulla tiedon siirtäminen tietoverkon läpi on mahdollista.

Kuljetuskerros

Kuljetuskerros huolehtii päästä päähän tapahtuvan tietoliikenteen luotettavuudesta. Tähän sisältyy virheen havainnointia ja virheistä toipuminen. Esimerkkiprotokollia kuljetuskerroksella ovat *Transmission Control Protocol* (TCP) ja *User Datagram Protocol* (UDP). TCP-protokollan tapauksessa yhteys muodostetaan kolmivaiheisella kättelyllä. UDP-protokolla ei varmista yhteyden muodostumista vaan paketit lähetetään vastaanottajan

osoitteeseen suoraan. Kuljetuskerros huolehtii myös yhteyden toiminnasta vaihtoehtoisella reitillä.

Istuntokerros

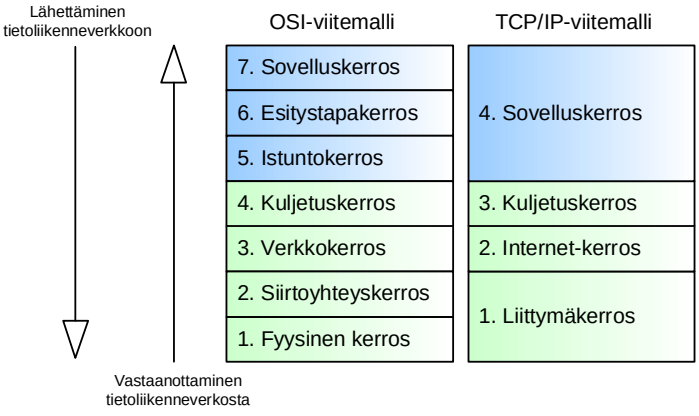
Istunto eli yhteyskerros huolehtii tiedon ryhmittelystä sovellukselle. Istuntokerroksella huolehditaan sovelluksen kanssa yhteistyössä yhteyksien hallinnasta ja tiedonsiirtoresurssien varaamisesta. Yhteyksien muodostuminen ja päättäminen tapahtuu myös istuntokerroksella.

Esitystapakerros

Esitystapakerroksella määrätään tiedon esitystapa sovellusten välillä. Tämän kerroksen ominaisuuksiin kuuluu tiedon salaus ja tiivistäminen. Esitystapakerroksella on myös mahdollista piilottaa laitteen arkkitehtuurista johtuvat riippuvaisuudet sovelluskerrokselle.

Sovelluskerros

Sovelluskerros takaa käyttäjille hajautetun informaation palvelut ja pääsyn OSI-ympäristöön. [5, s. 8-9; 6.]



Kuva 3. OSI- ja TCP/IP-viitemalli (lähdettä 6 mukaillen)

3.2 TCP/IP-viitemalli

TCP/IP-pohjaisten verkkojen historia on hyvin pitkä. Yhdysvaltojen puolustusministeriö halusi tekniikan, joka toimisi myös ydinsodan aikana. Puolustusministeriö antoi toimeksiannon tekniikan kehittämiseen ja rahoitti myös tekniikan kehittämistä. Ensimmäinen määritys TCP/IP-

protokollan määrityksestä on vuodelta 1974, mutta toimiva määritys tehtiin vasta vuonna 1978.

TCP/IP-malli on määritelty ennen OSI-mallia. OSI-malli on määritelty toimivaksi myös muissa kuin TCP/IP-pohjaisissa protokolla toteutuksissa. TCP/IP-malli toteuttaa vain IP-pohjaisten protokollien määrittelyn. TCP/IP-mallissa on neljä kerrosta ja ei ole suoraan verrattavissa OSI-malliin (kuva 3). Seuraavassa on esitelty TCP/IP-mallin kerroksien tärkeimmät ominaisuudet:

Liityntäkerros

TCP/IP-mallin alin kerros eli liityntäkerros käsittää OSI-mallin kaksi alinta kerrosta. Tämän kerroksen tehtävänä on huolehtia liitynnästä Internet-verkkoon.

Verkkokerros

Verkko- tai Internet-kerroksen tehtävänä on huolehtia IP-paketin reitittymisestä verkosta parasta mahdollista reittiä pitkin. Muodostetun yhteyden aikana ei verkkokerroksella erikseen varmisteta pakettien perille menoa.

Kuljetuskerros

Tehtävät ovat käytännössä samat kuin OSI-mallin kuljetuskerroksella, mutta TCP/IP-mallissa on vain kaksi protokollaa TCP ja UDP. TCP huolehtii päätelaitteiden välisen yhteyden luotettavuudesta ja on yhteydellinen protokolla. TCP huolehtii, että paketit saadaan vastaanottajalta oikeassa järjestyksessä ja luotettavasti. TCP:tä käytettäessä täytyy etukäteen sopia siirrettävästä tiedosta ja yhteyden päättämisestä osapuolen välillä. UDP on yhteydetön protokolla eikä edellytä erillistä yhteyden muodostamista. [5, s. 10.]

Sovelluskerroksella käytetään vastaavia protokollia kuten OSI-mallissa.

Tietoliikenneprotokollat on hyvä suunnitella OSI-mallin mukaisesti, koska TCP/IP-malli ei ota kaikkiin asioihin kantaa ja salausmenetelmissä

myös esityskerros on hyvä pitää omana osiona. OSI-mallia tulee käyttää erityisesti suunniteltaessa vaativimmissa olosuhteissa käytettäviä protokollia, kuten sähköasemien väyläprotokollia, joissa voi olla tarvetta muuttaa esim. laiteosoitemäärittelyjä.

3.3 Tiedonvälittäminen Internetissä (IPv4 ja IPv6)

Edellisessä kappaleessa on esitelty, miten TCP/IP-protokollien väliset riippuvaisuudet on toteutettu. Tämä ei kuitenkaan aivan vielä riitä siihen, että ymmärretään, miten tietoa pystytään välittämään Internetissä halutulle kohteelle halutusta lähteestä. Tässä kappaleessa tutkitaan, miten tieto välittyy ja millaisia vaihtoehtoja tiedon välittämiselle löytyy.

Internetissä jokaisella liikennöivällä laitteella on Internet-protokollaan perustuva IP-osoite. Tiedon lähettäjän tulee tietää vastaanottavan laitteen julkinen IP-osoite, jotta verkko osaa toimittaa tiedon vastaanottajalle. Lähettäjä lisää IP-pakettiin myös oman IP-osoitteen, jotta kaksisuuntaisen tietoliikenneyhteyden muodostaminen on mahdollista.

IP:n käyttäminen Internetissä välitettävään tietoon on saanut alkunsa tietokoneiden yleistymisestä. Ei ollut enää mielekästä, että kaikki laitteet liittyisivät verkkoon omilla yhteyksillä, jonka seurauksena alkoi muodostua paikallisia tietoverkkoja. Paikallisista tietoverkoista käytetään yleisesti nimeä *Local Area Network* (LAN) ja puolestaan julkiseen verkkoon liittyviä yhteyksiä kutsutaan nimellä *Wide Area Network* (WAN).

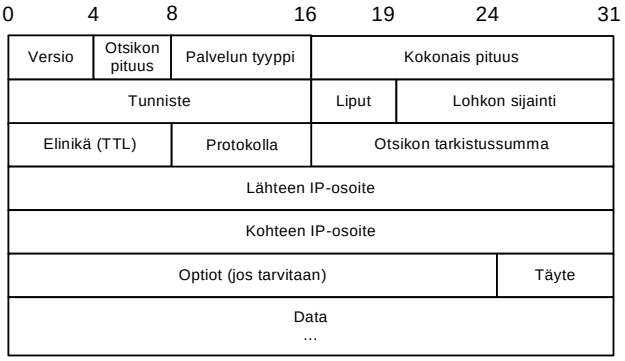
Edellä mainitut termit ovat yhä käytössä nykypäivän Internet-yhteyksillä (WAN) ja paikallisverkoissa (LAN) sekä kotona että yrityksissä. Varsinainen IP syntyi, kun WAN- ja LAN-protokollat eivät osanneet keskustella suoraan keskenään, jolloin tähän tarpeeseen kehitettiin kokonaan uusi protokolla. Tätä protokollaa alettiin kutsua Internet-protokollaksi. IP mahdollistaa, että useat eri LAN- ja WAN-protokollat kykenevät välittämään tietoa toisilleen, vaikka OSI-mallin alempien tasojen protokollat vaihdettaisiin. [7, s. 192 -199.]

Internet-protokollan versio neljä (IPv4)

IP-osoitteet määritellään käyttäen 32 bittiä eli yhteensä neljää tavua. IP-osoitteet esitetään yleensä pistemuodossa, jossa tavut erotellaan pisteillä. Yksi tavu sisältää kahdeksan bittiä ja näin ollen, jokainen tavu käsittää luvut 0...255. Isäntä IP-osoitteen visuaalinen ulkoasu on esim. *192.168.1.100*. Kullekin tietokoneelle määritellään yksikäsitteinen IP-osoite, jolla liikennöinti tietoverkossa on mahdollista.

Tietokoneelle voidaan määritellä IP-osoite, joka koostuu kahdesta IP-osoiteosasta. IP-osoiteosat ovat isäntäosa ja verkko-osa. Verkko-osa esitetään vastaavalla tavalla kuin edellä esitetty isäntäosan IP-osoite. Verkko-osoitteen tehtävänä on luokitella käytettävät IP-osoitteet omiksi ryhmiksi. Verkko-osa ja isäntä IP-osoite muodostavat yhdessä hierarkkisen osoiteavaruuden. Hierarkkinen osoiteavaruus tarvitaan, jotta Internetissä tietoa välittävät laitteet eli reitittimet pystyvät tehokkaasti siirtämään tiedon lähettäjältä vastaanottajalle. [7, s. 192 -199.]

IP-paketin otsikkorakenne on esitetty kuvassa neljä. IPv4:n mukainen otsikkorakenne on melko monikäsitteinen ja sisältää paljon parametreja. Kuvan yläreunassa olevat numerot esittävät kenttien tarvitsemia bittimääriä.



Kuva 4. IPv4-paketin otsikkorakenne [8, s. 98.]

Internet-protokollan versio kuusi (IPv6)

IPv4 määrittelyn mukaisten IP-osoitteiden määrä on suhteessa rajallinen Internet-verkkojen käyttäjämääriin. Rajallisuuden seurauksena on kehitet-

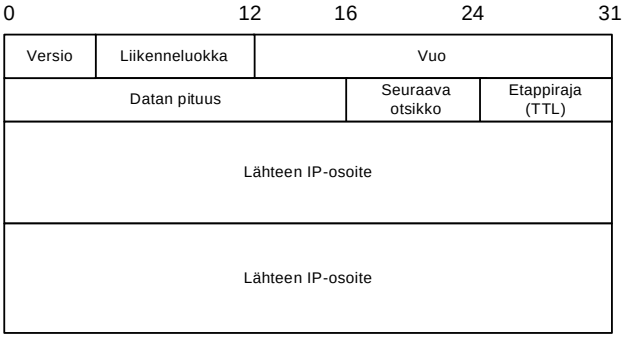
ty useita eri menetelmiä osoitemäärän kasvattamiseen. Internet on levinnyt kaikkialle maailmassa ja käyttäjien määrät jatkavat kasvuaan. Kasvun seurauksena on ollut tarvetta IP-osoitteiden määrän kasvattamiseen. 32 bitillä ilmaistujen IP-osoitteiden määrää on saatu näennäisesti kasvatettua jälkikäteen kehitetyillä menetelmillä, kuten osoitteenkäännöksellä *Network Address Translation* (NAT). IPv4-perheeseen on myös määritelty osoiteavaruuksia, joista on yleisesti sovittu, että niiden osoitteiden tietoa ei julkisessa tietoverkossa välitetä. Tällaisia osoitteita voidaan käyttää ns. sisäverkoissa (LAN) ja käyttää ainoastaan yhtä julkista IP-osoitetta kaikkien laitteiden liikennöintiin WAN-verkon suuntaan.

TCP/IP:n kehitys on hyvin sidoksissa Internetin kehittymiseen ja tarpeisiin. Tästä syystä on varauduttu IP-osoitteiden loppumiseen ja kehitetty uusi IP-protokolla, joka käyttää osoitekentässään 128 bittiä. Jokaisella bitillä voidaan ilmaista kaksi eri arvoa ja 128 bitillä ilmaistuja IP-osoitteita saadaan 2^{128} kpl. IP-osoitteiden suuri määrä mahdollistaa hyvin monelle laitteelle yksikäsitteisen IP-osoitteen. Uusittua IP-versiota kutsutaan nimellä IPv6.

IPv6-protokollaan on lisätty paljon hyviä ominaisuuksia, sillä sen kehittämisvaiheissa on jo tietoturva otettu huomioon. IPv6-protokollan merkittäviä muutoksia on osoite määrän kasvaminen, laajennettu osoitehierarkia ja joustavat otsikkorakenteet. IPv6-perusotsikko sisältää vähemmän tietoja kuin IPv4, mutta käytännössä osa IPv4:n kiinteän mittaisista otsikkokentistä on siirretty laajennusotsikoihin. IPv6-paketti sisältää aina perusotsikon, jossa kerrotaan mm. versio, lähde- ja kohdeosoite.

IPv6-osoitteiden visuaaliseen esitystapaan on lisätty heksadesimaaliluvut ja näin ollen 128 bitin IPv6-osoite voidaan ilmaista kahdeksassa 16 bitin lohkossa esim. *0:0:0:ffff:fffd:1234:56:0*. IPv6-osoitteen esitystavassa on huomattava, että jokainen neljän heksadesimaaliluvun ryhmä erotellaan kaksoispisteellä. Peräkkäisiä pelkkiä nollia sisältävät ryhmät voidaan ilmaista kahdella kaksoispisteellä. Edellinen IPv6-osoite voidaan ilmaista tiivistettynä *::ffff:fffd:1234:56:0*. [8, s. 599 - 620.]

IPv6-paketin otsikkorakenne on esitetty kuvassa viisi. IPv6-perusotsikkorakenne on huomattavasti yksinkertaisempi verrattuna aikaisempaan IPv4-otsikon määrittelyyn. Nyt palvelun tyyppi on korvattu liikenneluokalla, johon sisältyy laajennuskenttä vuo. Muita muutoksia on lähde- ja kohdeosoitteen bittimäärän kasvaminen ja elinikä lohkon muuttuminen etappirajalohkoksi. [8, s. 604.]



Kuva 5. IPv6-otsikkorakenne [8, s. 604.]

TCP- ja UDP-portit

Tiedon siirtäminen vaatii, että tiedonsiirtosovellukselle kerrotaan portti, johon lähetettävä tieto kohdistetaan vastaanottavassa sovelluksessa. Molemmissa protokollissa sekä UDP:ssä että TCP:ssä on käytössä staattisesti ja dynaamisesti määriteltyjä portteja. Staattisesti määritetyt portit on yleisesti varattu tietyn sovelluksen käyttöön. Sovellukselle kerrotaan porttinumero, jolla esim. VPN-yhteydellä käytössä oleva salausavaimien vaihtaminen suoritetaan. [7, s. 204 - 205.]

4 TIETOLIIKENTEEN SALAAMINEN

Tietoliikennettä suojatessa täytyy tuntea salaamisen tarve ja etäkäyttöyhteyksissä yleisesti käytössä olevat salausmenetelmät. Yksistään salaaminen ei riitä vaan tulee myös varmistaa, että salattu yhteys muodostetaan oikean osapuolen kanssa.

Tietoliikenteen salaamisella tarkoitetaan selkokielisen tiedon muuttamista muotoon, josta alkuperäistä tietoa ei pystytä tulkitsemaan ilman asian-

omaisten tiedossa olevaa tunnusta. Tunnus on salausavain, jolla matemaattisin keinoin muodostettu tieto pystytään avaamaan takaisin selkokielelle.

Tietoliikenteen salaaminen on tullut yhä tärkeämmäksi kasvavan arkaluontoisen tiedon jakamisen ja siirtämisen seurauksena. Ensimmäisenä julkisessa tietoverkossa on ollut tarvetta salata pankkiliikennettä ja erityisesti luottokorteilla tehtyjä ostoksia.

Tietoliikennettä pystytään salaamaan useilla erinäisillä menetelmillä, joista seuraavassa käsiteltävät menetelmät koskettavat VPN-tekniikoita ja erityisesti SSL VPN ja IPSec VPN -arkkitehtuurien yhteydessä käytettäviä menetelmiä.

4.1 Symmetrisen salauksen menetelmät

Symmetrisen salauksen menetelmät ovat yksi vanhimmista tietoliikenteessä käytetyistä salausmenetelmistä. Symmetrisen salauksen lähtökohtana on ollut sotkea alkuperäinen tieto ja salaamiseen käytettävä tieto niin hajalleen, että selvää tekstiä ei voida alkuperäisestä nähdä. Lisäksi tärkeä ominaisuus on, että pieni muutos salattavassa tiedossa aiheuttaa suuren muutoksen salattuun tietoon.

Symmetriset salausmenetelmät jaetaan kahteen eri ryhmään, jotka ovat lohko- ja jonosalaimet. Lohkosalaimet käsittelevät tekstiä määrätyn kokoisissa osalohkoissa, jotka salataan aina samalla avaimella. Lohkon pituus vaikuttaa salauksen vahvuuteen. Jonosalaimet käsittelevät tietoa pienissä yksiköissä, jotka voivat olla jopa vain yhden bitin kokoisia, mutta salausavain vaihtuu jokaisen yksittäisen osan jälkeen.

Symmetrisessä salauksessa molempien osapuolten täytyy tietää salausavain ja käytetyt salausmenetelmät, jotta salatut viestit pystytään avaamaan takaisin selkokielelle. Symmetrisen salauksen heikkouksia on, että salaus on mahdollista murtaa kokeiluhyökkäyksellä (*brute force*). Hyökkäysmahdollisuuden seurauksena salausavaimien tulisi olla riittävän

pitkiä ja vaikeita, että tietokoneella salausavaimen arvaamiseen kuluu aikaa useita vuosia.

Yleisimmät symmetrisen salauksen menetelmät ovat *Data Encyption Standard* (DES), *Triple DES* (3-DES) ja *Advanced Encyption Standard* (AES). Näistä menetelmistä turvallisimpana pidetään AES-menetelmää. Salausalgoritmien matematiikkaa ei tässä työssä esitellä. [9, s. 77 - 96; 10.]

4.2 Epäsymmetrisen salauksen menetelmät

Ongelmana symmetrisen salauksen käytössä on salausavaimien turvallinen jakaminen, jos käyttäjät ovat eripuolilla julkista tietoverkkoa. Avainta ei voida suoraan siirtää julkisen tietoverkon läpi, koska avain voisi joutua tietoverkkorikollisen käsiin. Avaimenvaihto-ongelmaan käytetään julkisen avaimen menetelmää eli epäsymmetrisen salauksen menetelmää. Epäsymmetrinen salaus vaatii suuren tietokoneen laskentakapasiteetin verrattuna symmetriseen salaukseen, jonka seurauksena se ei sovellu suurten tietomäärien salaukseen.

Epäsymmetrinen salaus käyttää salausavainparia, joka on peräisin vaikean matemaattisen prosessin tuloksena. Toinen avaimista on tehty julkiseksi avaimeksi ja toinen yksityiseksi avaimeksi. Julkista avainta ei pidetä salaisena ja se voidaan jakaa yleisesti esim. digitaalisen sertifikaatin mukana.

Yksityinen avain on tarkoitettu salassa pidettäväksi ja ainoastaan asianomaiselle osapuolelle. Avainparien tarkoitus on toimia saumattomassa yhteistyössä. Julkisella avaimella salattu tieto voidaan avata ainoastaan julkista avainta vastaavalla yksityisellä avaimella. Toiminta on päinvastainen, jos yksityistä avainta on käytetty tiedonsalaamiseen. Avainten välinen suhde mahdollistaa julkisen avaimen välittämisen verkossa. Käytännössä kuka tahansa voi salata liikenteen käyttäjän julkisella avaimella, mutta salauksen purkaminen onnistuu vain yksityisellä avaimella. Yleisin julkisen avaimen menetelmä on *Rivest, Shamir, and Adleman* (RSA).

Käytännössä tietoliikennelaitteet salaavat aina lähetetyn tiedon vastaanottajan julkisella avaimella, joten alkuperäinen lähettäjä ei pysty enää salausta avaamaan ellei alkuperäinen lähettävä tieto ole tallessa. Tällä varmistutaan, että ainoastaan oikeat vastaanottajat pystyvät tiedot avaamaan. [9, s. 131 - 155.]

4.3 Tiivistysfunktiot

Tiivistysfunktio on yksisuuntainen funktio, jonka muodostama arvojoukko (*hash*) esittää alkuperäistä tietoa. Arvojoukko lasketaan aina alkuperäiselle tiedolle eheyden varmistamiseksi tiedonsiirron aikana. Muitakin käyttökohteita tiivisteillä on, mutta etäyhteyksiä käsiteltäessä sillä varmistetaan tiedon muuttumattomuus yhteyden aikana.

Tiivistysfunktion muodostama arvojoukko on jokaiselle syötetylle tiedolle oma ja on kooltaan alkuperäistä tietoa pienempi. Tiivistysfunktion muodostama arvojoukko on myös vakiomittainen. Huomioitavaa on, että vakiomittaisuus asettaa rajoitteita tiivistyksen oikeellisuuteen, sillä kahdella erilaisella tiedolla voi olla sama arvojoukko. Tiivisteelle on mahdollista tulla sama arvo, kun kaikki eri bittivaihtoehdot on kokeiltu. Tiivistysfunktiot eivät ole yksikäsitteisiä. Tämän seurauksena tiivistystä ei voida käyttää salausmenetelmänä.

Yleisimmät tiivistysfunktiot ovat *Message Digest 5* (MD5) ja *Secure Hash Algorithm 1* (SHA-1). Näistä menetelmistä MD5 käyttää tiivistyksessä 128 bittiä, kun puolestaan SHA-1 muodostuu 160 bitistä. Käytännössä SHA-1 määrittää 2^{160} eri tiivistettä. [9, s. 107 - 127; 10.]

Avaimelliset tiivisteet

Tiivistysfunktioiden käyttö mahdollistaa myös osapuolen tiedossa olevien tunnisteiden käyttämisen. Tunnistetiivisteet muodostetaan käyttäen, joko *Message Authentication Code* (MAC) tai *Hashed Message Authentication Code* (HMAC)-menetelmää. MAC käyttää tiedon kuvausfunktiota määrittämään alkuperäisestä tiedostosta varmenteen, jota voidaan verrata digitaaliseen allekirjoitukseen. MAC-koodin ja digitaalisen allekirjoituksen

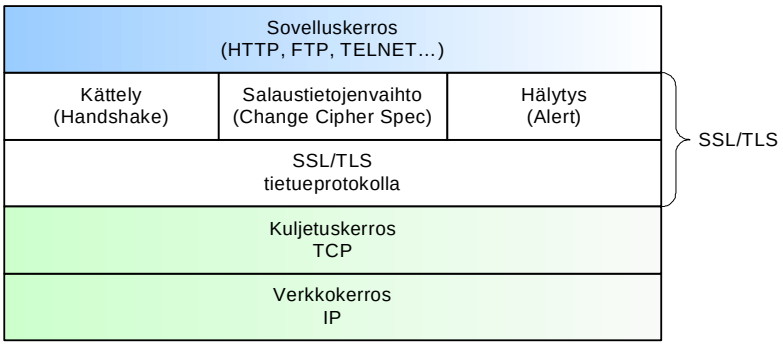
erona on, että digitaalinen allekirjoitus on samalla myös tunnistautumismenetelmä.

MAC- ja HMAC-menetelmien erona on, että HMAC käyttää myös yksityistä avainta toiminnassaan. Tiivistettävään tietoon lisätään yksityinen avain ennen tiivisteen muodostamista. Tämä tekee tiedon eheyden tarkastamisen entistä turvallisemmaksi, koska molempien osapuolien on tiedettävä myös avain, jotta tiivistyksen tulos olisi sama. Käytännössä tässä tapahtuu samalla osapuolten tunnistautuminen.

4.4 SSL/TLS

Secure Socket Layer (SSL) määrittelyn ensimmäinen versio julkaistiin vuonna 1994. Määrittelyn on tehnyt *Netscape Communications Corporation* niminen yritys, jonka tavoitteena oli luoda menetelmä turvaamaan Internet-sivustojen tietoturvaa. *Netscape* julkaisi määrityksestä päivitetyn version (SSL 3.0) vuonna 1996. Määrityksen päivityksen seurauksena *Internet Engineering Task Force* (IETF) kiinnostui SSL menetelmästä ja aloitti standardoimistyön SSL 3.0 määrittelyn pohjalta. IETF julkaisee Internet suosituksia, jotka tunnetaan nimellä *Request For Comments* (RFC). IETF:n julkaisema SSL määrittely tunnetaan nimellä *Transport Layer Security* (TLS), joka on määritelty IETF:n RFC määrittelyssä 2246 (*The TLS Protocol Version 1.0*). [6, s. 296; 11.]

SSL/TLS-protokolla sijaitsee verkkokerroksen ja sovelluskerroksen välissä, jonka seurauksena protokollalla on mahdollista turvata alemmalta kerrokselta tuleva informaatio ylemmille tasoille ja päinvastoin (kuva 6). Lisäksi tämä mahdollistaa sen, että SSL/TLS tukee useampaa sovelluskerroksella toimivaa protokollaa kuten esim. Internetin perusprotokollaa *Hypertext Transfer Protocol* (HTTP) tai tiedostonsiirtoprotokollaa *File Transfer Protocol* (FTP).



Kuva 6. SSL-protokollakerrokset (lähdettä 12 mukaillen)

SSL/TLS koostuu kahdesta päätason protokollasta, jotka ovat kättelyprotokolla (*Handshake Protocol*) ja tietueprotokolla (*Record Protocol*). Kättelyprotokolla koostuu lisäksi kolmesta alemman tason protokollasta, jotka ovat kättely (*Handshake*), salaustietojenvaihto (*Change Cipher Spec*) ja hälytys (*Alert*). Kättelyprotokollan tärkein tehtävä on huolehtia yhteyden muodostumisesta tai jatkumisesta. Tietueprotokollan tärkein tehtävä on itse tiedon salaaminen ja tiedon pilkkominen hallittaviin osasiin. [10.]

4.4.1 Kättelyprotokolla (Handshake Protocol)

Kättelyprotokollien tehtävänä on keskustella muodostettavaan yhteyteen liittyvistä ehdoista palvelimen ja asiakaspään välillä. Protokollan tärkeimpiä tehtäviä on vaihtaa tietoa tunnistus, salaus, tiedon eheys, tiedon tiivistysmenetelmistä ja hälytysviestien ilmoittamisesta.

Osapuolten tunnistautuminen perustuu digitaaliseen sertifikaattiin, joka yleensä on valtuutetun toimitsijan eli *Certification Authority* (CA) hyväksymä. CA on molempien osapuolien luotettu kolmas osapuoli, joka mm. uusii tai irtisanoo myönnetyn sertifikaatin. Sertifikaatti sisältää voimassaoloajan, julkisen avaimen, sarjanumeron ja digitaalisen allekirjoituksen. Palvelinsertifikaattina käytetään X.509-standardin mukaista digitaalista sertifikaattia.

Kättelyprotokolla (Handshake Protocol)

Alemman tason kättelyprotokollan tehtävänä on keskustella istuntoon liittyvistä asiakkaan ja palvelimen välisistä tiedoista. Kättelyprotokolla neu-

voteltavia tietoja ovat mm. istunnon tunnus, salausmenetelmät ja naapurien sertifikaatit. Kättelyprotokolla aloittaa aina istunnon neuvottelun.

Yhteyden suojaamiseen käytetään kahta eri salausmenetelmää, jotka ovat symmetrisen avaimen (yksityinen avain) ja epäsymmetrisen avaimen (julkinen avain) menetelmät. Symmetristä salausta käytetään suurten tietojen salaamiseen johtuen sen pienemmästä tietokoneen laskentakapasiteetti vaatimuksesta verrattuna epäsymmetrisen salauksen käyttöön. SSL/TLS käyttää symmetristä salausta viestien salaamiseen ja epäsymmetristä salausta käyttäjän tunnistautumiseen. Epäsymmetrisen salauksen julkista avainta käytetään myös istunnossa avaimena.

Yhteyden eheyden varmistamiseen käytetään edellisessä luvussa esitettyjä tiivistysfunktioita. SSL käyttää tiedon eheyden tarkistamiseen MAC-koodin mukaista eheydenvarmistusmenetelmää, kun puolestaan IETF:n määrittelemä TLS käyttää avainnettua tiivistysfunktiota (HMAC).

Salaustietojenvaihtoprotokolla (Change Cipher Spec Protocol)

Salaustietojenvaihtoprotokollan tärkein tehtävä on vaihtaa informaatio avainmateriaalista, jota on käytetty tiedon salaamiseen asiakaspään ja palvelimen välillä. Avainmateriaali on satunnaista dataa, jota käytetään salausavaimien luonnissa. Protokollan toiminta koostuu ainoastaan yhdestä viestistä, joka kertoo vastapäälle SSL/TLS istunnon naapurin ja kuka haluaa avaimet vaihtaa. Avain puolestaan vaihdetaan kättelyprotokollan muodostamien tietojen perusteella.

Hälytysprotokolla (Alert Protocol)

Hälytysprotokolla käyttää useita eri viestejä ilmaisemaan muodostuneen yhteyden tilaa tai virhetilannetta. Hälytysprotokollan käyttämät viestit on määritelty kokonaisuudessaan TLS-protokollan määrittelyn yhteydessä IETF:n RFC 2246:ssa. Hälytysviesti lähetetään yleensä yhteyden sulkemisen yhteydessä, kelpaamattoman paketin saapuessa tai epäonnistuneen salauksen purkamisen yhteydessä.

4.4.2 Tietueprotokolla (Record Protocol)

Toinen SSL/TLS yhteyden päätason protokollista on tietueprotokolla. Tietueprotokollan tehtäviä on pilkkoa sovellustasolta tuleva tieto salaamiseen soveltuviin osasiin. Kättelyprotokollalla neuvotelluilla salausehdoilla pilkottuihin osasiin lisätään tiedoneheyden varmistus MAC tai HMAC, jonka jälkeen osaset salataan ja siirretään kuljetuskerrokselle. Verkosta vastaanottaessa tieto puretaan kättelyprotokollan määrittelemällä tavalla. [10; 11.]

4.4.3 SSL-yhteyden muodostuminen asiakaspään ja palvelimen välillä

SSL-yhteys saa aina alkunsa kättelyssä tapahtuvien viestien vaihdolla (kuva 7). SSL mahdollistaa palvelimen tunnistautumisen asiakaspäälle edellä esitettyä julkisen avaimen menetelmää käyttäen. SSL käyttää julkisen avaimen jakamiseen digitaalista sertifikaattia.

Tässä työssä käsitellään ainoastaan SSL 3.0 ja TLS 1.0 määrittelyjen mukaista kättelyä. SSL 3.0- ja TLS 1.0-versioiden käyttö takaa parhaimman tietoturvan, kun käytetään SSL-suojaukseen perustuvia sovelluksia. SSL-istunnolla tarkoitetaan koko salatun yhteyden aikana välitettäviä viestejä ja kestoa. Seuraavassa on esitetty eri vaihteet kättelysanomien vaihdosta ja sanomien sisällöstä:

Kättelyn ensimmäisessä vaiheessa asiakas lähettää *CLIENT_HELLO*-sanoman, jonka sisältö on seuraava:

- asiakkaan tukemat SSL/TLS versiot esim. TSL 1.0 ja SSL 3.0
- listaus asiakkaan tukemista salausmenetelmistä
- istunnon tunnus (uudessa istunnossa tunnuksena nolla)
- asiakkaan satunnaisesti muodostama data (käytetään salausavainten luonnissa).

Palvelimen tulee vastata asiakkaan lähettämään *CLIENT_HELLO*-sanomaan *SERVER_HELLO*-sanomalla. Tarkoituksena on neuvotella tie-

toturvan kannalta turvallisimmat vaihtoehdot istunnolle. Palvelimen lähettämän viestin sisältö on seuraava:

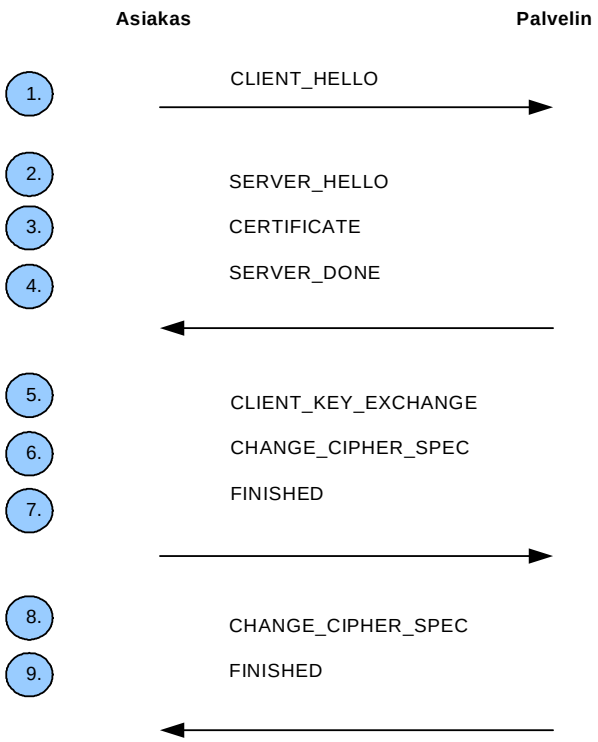
- käytettävä SSL- tai TLS-versio
- salausmenetelmät, joita käytetään istunnon aikana
- tiedon tiivistysmenetelmät
- istunnon tunnus
- palvelimen satunnaisesti muodostama data (käytetään salausavainten luonnissa).

HELLO-viestien jälkeen palvelin lähettää *CERTIFICATE*-sanoman, joka sisältää kaikki julkisen avaimen sertifikaatit aina juurivarmentajaan (CA) asti eli sertifikaattien luotettavuuspolun (*path*).

SERVER_DONE-sanomalla palvelin ilmoittaa asiakkaalle kyseisen käyttelyvaiheen olevan suoritettu.

Asiakas lähettää *CLIENT_KEY_EXCHANGE*-sanoman, joka sisältää asiakkaan salaaman viestin käyttäen palvelimen julkista salausavainta. Molemmat, sekä palvelin että asiakas muodostavat symmetriset salausavaimet käyttäen omia ns. *premaster*-avaimia ja satunaisdataa, joka on muodostettu *CLIENT_HELLO* ja *SERVER_HELLO*-sanomien yhteydessä.

Lopuksi asiakas ja palvelin lähettävät vuorotellen sanoman *CHANGE_CIPHER_SPEC*. Sanoman tarkoituksena on vahvistaa molempien osapuolten olevan valmiina aloittamaan suojattu yhteys neuvotelluilla ehdoilla. Molemmat osapuolet päättävät yhteyden *FINISHED*-sanomilla, jotka muodostuvat yhteyden aikana kertyneestä MD5- ja SHA-tiivisteistä. Osapuolet varmistavat näin sanomien olevan kunnossa ja varmistuvat tiedon eheydestä. [6, s. 298 - 300; 13.]



Kuva 7. Kättelyviestit SSL/TLS yhteyden muodostuksessa [13.]

4.5 IPSec ja salausmenetelmät

IPSec (*Internet Protocol Security*) on standardi, joka koostuu useasta eri protokollamäärittelystä. IPSec toimii OSI-mallin verkkokerroksella, jonka seurauksena IPSec mahdollistaa usean eri protokollan käyttämisen ja kryptografisen suojauksen. IPSec-standardiperheen määrittelyt on tehty IETF:n toimesta, ja kaikki määrittelyt on määritelty RFC-dokumenteissa.

IPSec-protokollien lähtötarkoituksena on ollut suojata liikenne luotettujen tietokoneiden välillä väärennyksiltä ja salakuuntelulta. Suojauksen tulee olla myös automaattista sekä suojata käytössä olevia Internet-sovelluksia.

IPSec-tekniikan ominaisuuksia ovat mm. läpinäkyvyys, jolloin sovellusohjelman ei tarvitse huomioida toiminnassaan IPSec-yhteyttä. IPSec toimii lähes kaikissa IPv4-toteutuksissa ja on osa IPv6-määrittelyä. IPSec-paketeissa tiedot ovat suojattuna IP-osoitekenttiä lukuunottamatta, sillä reitittimet tarvitset osoitteet tiedon välittämiseen. [6, s. 218 - 220.]

4.5.1 IPSecin toimintatilat

IPSec-tietoturvaprotokolla tukee kahta erilaista toimintatilaa. Toimintatiloja ovat tunneli (*tunnel mode*) ja kuljetus (*transport mode*) tilat. Tunneloinnilla tarkoitetaan kahden yhdyskäytävän välistä tilaa, jossa koko IP-paketti paketoidaan uudelleen uuden IP-paketin sisälle. Etuna tässä paketoinnissa on, että se piilottaa alkuperäisen lähettäjän ja vastaanottajan IP-paketista, jolloin liikenteen analysointi on huomattavan vaikeaa.

Kuljetustilaa voidaan käyttää ainoastaan kahden päätepisteen välillä, jolloin paketteihin lisätään ainoastaan tarvittavat salausotsikot. Kuljetustilaa ei voida käyttää kuin lopullisten pakettien vastaanottajien välillä. [14, s. 57 - 61.]

4.5.2 IPSec-otsikot eli salausotsikot

IPSec-otsikot muodostavat VPN-yhteyden tärkeimmät ominaisuudet eli näkymättömän toiminnon normaaliin tietoverkkoon nähden. Seuraavassa on esitetty salausotsikkovaihtoehdot ja niiden tärkeimmät ominaisuudet:

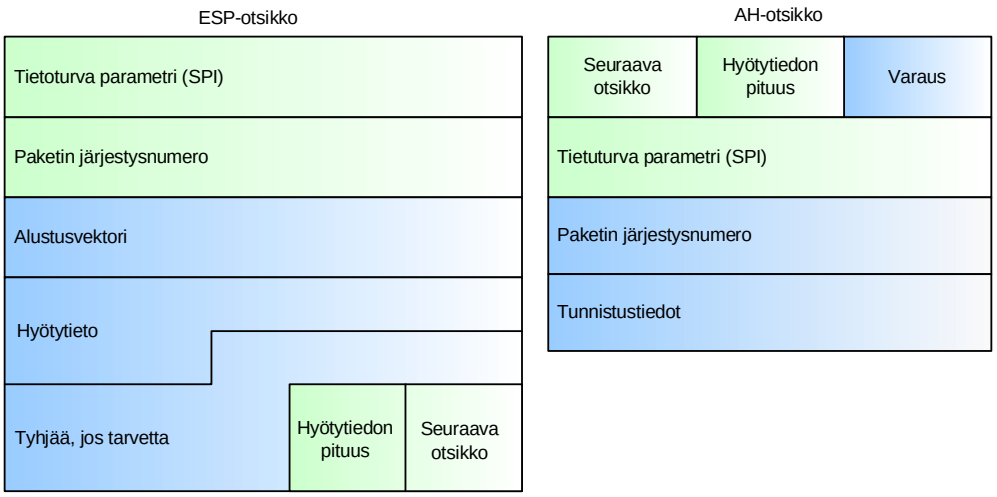
Autentikointiotsikko (Authentication Header, AH)

AH-otsikko on määritelty IETF:n RFC-dokumentissa 2402. Autentikointiotsikko sisältää eheyden tarkistustietoa, jonka tarkoituksena on ilmaista väärennykset, jos matkalla olevaa tietoa on muutettu. Autentikointiotsikko sisältää tarkistussumman, joka estää myös salakuuntelulla kaapattujen pakettien uudelleen lähettämisen. [14, s. 58.]

Hyötytiedon tietoturvaotsikko (Encapsulating Security Payload, ESP)

ESP-otsikko on määritelty IETF:n RFC-dokumentissa 2406 ja on suunniteltu tarjoamaan tietoturvapalveluita IPv4 ja IPv6 määrittelyjen mukaisille yhteyksille. Otsikkoa voidaan käyttää itsenäisesti tai vaihtoehtoisesti yhdessä edellä esitetyn AH-otsikon kanssa. ESP-otsikon suunnittelun lähtökohtana on ollut varmistaa luottamuksellisuus, tiedon alkuperän tunnistaminen, eheyden varmistaminen ja estää siirrettävien pakettien uudelleen lähettäminen. [15.]

ESP-otsikon tärkein tieto on tietoturvaparametri (*Security Parameter Index, SPI*). SPI-parametri mahdollistaa sen, että tietoliikennelaitteisto pitää kirjaa IPSec VPN -yhteydellä olevista turvayhteyksistä (*Security Association, SA*). Kuvassa kahdeksan on esitetty AH- ja ESP-otsikon rakenteet ja eroavaisuudet.



Kuva 8. Salausotsikot (lähdettä 16 mukaillen)

ESP-otsikon tehtävänä on salata IP-paketin loppuosassa oleva hyötytieto käyttäen tunnettuja salausmenetelmiä kuten 3-DES tai AES. Lisäksi VPN-yhteydellä tulee aina valita käytettävät tiedon eheyden varmistukseen käytettävät menetelmät kuten tunnistuksen mahdollistava HMAC-MD5. Salausmenetelmät valitaan kullekin yhteydelle määritettyjen ehtojen perusteella (turvayhteydet). Salausvaiheessa käytetään apuna SPI-parametriä, jolloin tietoliikennelaitteella on tiedossa yhteydellä käytettävät salausmenetelmät.

4.5.3 Turvayhteydet (Security Association, SA)

Turvayhteydet ovat IPSec VPN -yhteyden peruskomponentti. Turvayhteys esittää kahden päätepisteen välille muodostettua sopimusta. Sopimus määrää, kuinka yhteydellä on sovittu tietoturvamäärityksistä ja kuinka niitä käytetään verkon suojaamisessa. Turvayhteys sisältää kaikki tarvittavat parametrit pakettien turvalliseen siirtämiseen.

Kaksisuuntaisessa liikenteessä tarvitaan yhteyden molemmissa päissä oleville tietoliikennelaitteille kaksi turvayhteyttä, jotka määrittelevät suo-

jauksen molempiin suuntiin. Turvayhteydet ovat myös riippuvaisia käytetyistä salausotsikkorakenteista. Esimerkiksi, jos yhteydellä on sovittu käytettäväksi molempia sekä AH- että ESP-tyypin suojausta tarvitaan turvayhteyksiä yhteensä neljä kappaletta. Tietoliikennelaitteisto tallentaa turvayhteydet omaan paikalliseen tietokantaan, jota kutsutaan nimellä *Security Association Database* (SADB). [16; 17.]

4.5.4 Avaintenvaihto (Internet Key Exchange, IKE)

Avaintenvaihto tuo IPSec määrittelyyn joustavuutta ja helpottaa yhteyksien määrittämistä. Avaintenvaihto IKE on määritelty RFC-dokumentissa 2409. IKE:n toiminta perustuu *Diffie-Hellman* menetelmään. IKE tunnetaan myös ns. hybridi-protokollana, jonka osia ovat avaintenvaihdossa Oakley ja SKeme. Lisäksi IKE pohjautuu *Internet Key Exchange and Key Management Protocol* (ISAKMP) protokollaan, joka on avaintenhallintaprotokolla. ISAKMP on määritelty erikseen RFC-dokumentissa 2408.

IKE toteuttaa kaikki nämä kolme protokollaa Oakley, SKeme ja ISAKMP. IKE:n päätehtäviä on tuottaa tunnistautuminen IPSec-yhteydelle asianomaisten laitteiden välillä, keskustella salausavaimet ja turvayhteydet. IKE:n ominaisuuksia ovat:

- VPN-yhteyden kaikkia turvaparametreja ei tarvitse enää manuaalisesti määritellä.
- Turvayhteydelle voidaan määritellä erikseen elinikä. Elinikä voidaan määritellä ajan tai siirrettyjen tavujen mukaan.
- Salausavaimien vaihtaminen VPN-yhteyden aikana.
- Avaintenvaihto estää toistohyökkäyksien mahdollisuuden.
- Avaintenvaihto mahdollistaa juurivarmentajan käyttämisen yhteydellä, jolloin sertifikaattien käyttö on mahdollista.
- Avaintenvaihto mahdollistaa osapuolten dynaamisen tunnistautumisen. [16; 18.]

5 SALAUSMENETELMIEN HYÖDYNTÄMINEN VPN-YHTEYKSISSÄ

VPN-tekniikoiden lähtökohtana on ollut mahdollistaa näkymättömät yhteydet julkiseen tietoverkkoon. Internetin on mahdollista muodostaa yrityksen toimipaikkojen välisiä yhteyksiä eikä raskaita kiinteitä yhteyksiä enää välttämättä tarvita. Tässä luvussa perehdytään hieman perinteiseen IPSec-protokolalla toteutettuun VPN-arkkitehtuuriin, mutta suurempi huomio kiinnitetään haastajaan, joka on SSL/TLS-menetelmällä salattu VPN-yhteys.

5.1 VPN-topologiat

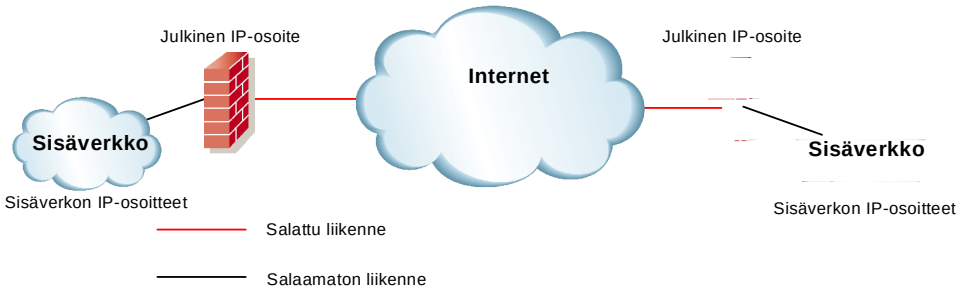
Tässä kappaleessa esitetään yleisimmät VPN-topologiat, jotka ovat päästä päähän -yhteydet ja etäkäyttömallin mukaiset etäyhteydet.

5.1.1 Päästä päähän -yhteydet (LAN-to-LAN)

Päästä päähän -yhteyksien tarkoituksena on ollut korvata kiinteitä yrityksien toimipaikkojen välisiä yhteyksiä käyttämällä olemassa olevaa julkista tietoverkkoa. Päästä päähän -yhteydet mahdollistavat verkkojen väliset verkkotason yhteydet.

Päästä päähän -yhteyksien toteuttaminen vaatii aina tietoliikennelaitteistojen välisen keskustelun. Päästä päähän -yhteyksiä voidaan toteuttaa mm. reitittimien, palomuurilaitteistojen tai erillisten VPN-päätelaitteiden välille. Salaus toimii joko etukäteen sovitulla salausavaimella tai käyttäen digitaalista sertifikaattia. Digitaalinen sertifikaatti tuo huomattavaa joustavuutta päästä päähän -mallin mukaisille yhteyksille, sillä jokaisen osapuolen kesken ei tarvitse sopia salausavainta erikseen. Päästä päähän -yhteydelle täytyy aina erikseen määritellä, mitkä verkot suojataan yhteydellä ja mitkä verkkoavaruudet menevät suoraan julkiseen tietoverkkoon ilman salausta. [16.]

Kuvasta yhdeksän nähdään päästä päähän -mallin mukainen periaatteellinen toimintamalli. Liitteessä yksi on esimerkki määrittely Juniperin Netscreen tuoteperheen palomuurille.



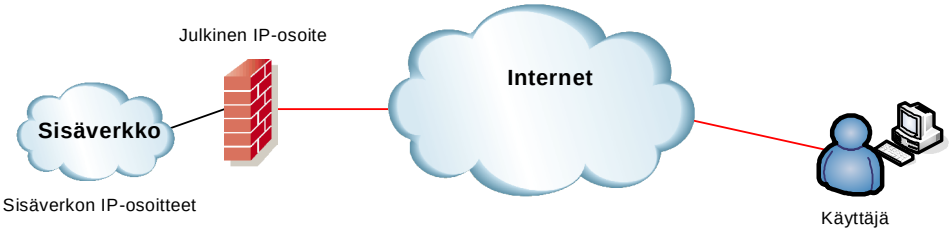
Kuva 9. Päästä päähän -VPN-yhteys

5.1.2 Etäkäyttö-VPN-yhteys (Remote access VPN)

Etäkäyttö-VPN-yhteyden lähtökohtana on ollut muodostaa yhteys yhden käyttäjän ja VPN-päätelaitteen välillä. VPN-käyttäjällä on sovellus, joka keskustelee päätelaitteen kanssa yhteyden muodostamisessa tarvittavista parametreista. Käyttäjä voidaan tunnistaa esim. etukäteen jaetulla salausavaimella (*preshared key*), digitaalisella sertifikaatilla tai vaihtoehtoisesti käyttäen erillistä tunnistuspalvelinta kuten *RADIUS* tai *TACACS+*.

RADIUS-palvelin mahdollistaa mm. kertakäyttöisten salasanojen käyttämisen, kuten *SecurID*-järjelmän käytön. *SecurID*-järjestelmässä käyttäjälle annetaan nelinumeroinen henkilökohtainen tunnus, joka on myös päätepalvelimen tiedossa. Lisäksi käyttäjällä on *SecurID*-kortti, jossa vaihtuu numerokoodi määrävälein. Kortit on synkronoitu päätepalvelimen kanssa, jotta tunnistus on mahdollista. Käyttäjän lopullinen salasana muodostuu henkilökohtaisesta tunnuksesta ja *SecurID*-kortissa vaihtuvasta numerokoodista. *SecurID*-kortti takaa vahvan tunnistuksen, jossa samaa numerokoodia ei voida käyttää kahta kertaa. [16; 19.]

Etäkäyttäjä muodostaa yhteyden yrityksen VPN-laitteiston julkiseen IP-osoitteeseen, jolloin laitteisto ja käyttäjän sovellus muodostavat yhteyden käytössä olevan tekniikan mukaisesti (kuva 10).



Kuva 10. Etäkäyttö-VPN

5.2 IPSec VPN -arkkitehtuuri

IPSec VPN on kehitetty alun perin takaamaan tietoturvapalveluita useaan erilaiseen järjestelmään, joiden liikennöinti pohjautuu IP-liikenteeseen. IPSec tukee molempia IP-osoiteperheitä eli vanhempaa IPv4-protokollaa ja uudempaa IPv6-protokollaa. IPSec määrittelee seuraavaan mukaisten kokonaisuuksien yhteistoiminnan (turvayhteys):

- tietoturvaotsikot *Authentication Header* (AH) ja *Encapsulation Security Payload* (ESP)
- turvayhteydet (SA)
- avainten hallinta (*Internet Key Exchange*, IKE)
- tunnistus ja salausmenetelmät mm. AES ja HMAC-SHA.

IPSec on IP-protokollaan lisätty tekninen menetelmä, joka mahdollistaa salatut tietoliikenneyhteydet kahden pisteen välillä. IPSec-protokollalle on tyypillistä, että yhteys muodostetaan OSI-mallin verkkokerroksella. Verkkokerroksella muodostettava yhteys joutuu itse huolehtimaan tiedonsiirron luotettavuudesta.

IPSec VPN -yhteys avaa aina verkkotason yhteydet. Etäkäyttöyhteyksiä toteutettaessa täytyy olla ehdottoman varma käytettävän tietokoneen tietoturvatasosta, jotta verkossa leviävät virukset eivät kykenisi leviämään. VPN- ja palomuurilaitteilla on mahdollista rajoittaa verkkotason yhteyksiä. Yhteyksien rajoittaminen lisää tietoturvaa.

IPSec VPN -ympäristöt mutkistuvat huomattavasti, jos verkkoihin lisätään useita päästä päähän -mallin mukaisia VPN-yhteyksiä. IPSec VPN -

arkkitehtuurin vahva puoli on päästä päähän -mallin yhteydessä mainittu julkisen avaimen menetelmä, joka mahdollistaa digitaalisella sertifikaatilla tunnistautumisen. Digitaalinen sertifikaatti tuo joustavuutta verkkoon ja yhteyksien ylläpito helpottuu, kun jokaiselle yhteydelle ei tarvitse erikseen määritellä salausavaimia. [16; 17.]

IPSec VPN -yhteys soveltuu parhaiten mm. etätoimistojen välisiin yhteyksiin, jos yhteysnopeudet ovat alle 100 Mbit/s suuruisia. Nopeassa tiedonsiirrossa salaamiseen vaadittu tietokoneen laskentakapasiteetti tarve on hyvin suuri, joka rajoittaa VPN-yhteyksien nopeutta. Nopeaan IPSec-pohjaiseen liikenteeseen vaaditaan erillinen VPN-kiihdytin. Kiihdytin mahdollistaa siirtonopeuden, jopa 1 Gbit/s asti.

IPSec VPN ei ole kustannustehokas ratkaisu, jos ollaan toteuttamassa useita eri käyttötarpeita vaativia etäkäyttöyhteyksiä. Yrityksen oman henkilöstön etäyhteyksiin IPSec VPN soveltuu hyvin, koska useat verkkolevy-yhteydet toimivat parhaiten puhtaalla verkkotason yhteydellä.

5.3 SSL VPN -arkkitehtuuri

SSL VPN ei ole yhteyksiä määrittelevä standardi vaan VPN-tekniikka, joka käyttää hyväkseen SSL/TLS-standardin mukaista suojausta. SSL VPN on uusin tekniikka suojattuihin asiakaspään yhteyksiin ja mahdollistaa toistaiseksi ainoastaan asiakaspään ja päätelaitteen välisten yhteyksien suojaamisen. SSL VPN -tekniikka ei siis tue sellaisia verkkojen välisiä VPN-yhteyksiä, joissa lähettäjää ja vastaanottajaa ei tiedetä etukäteen. SSL VPN on aina laite- tai sovellustoimittajariippuvainen johtuen SSL/TLS-protokollan monimuotoisuudesta. Monimuotoisuuden takia laitevalmistajilla on mahdollisuus käyttää protokollaa haluamallaan tavalla.

Yleisesti SSL VPN:lla käsitetään laitteistoa, joka mahdollistaa VPN-yhteyden muodostamisen käyttäen Internet-selainta tunnistautumiseen. Useat laitevalmistajat ovat lisänneet laitteisiinsa vahvoja tunnistusmenetelmiä kuten kertakäyttösalasanojen käyttämisen ja sovelluskohtaisia lisätoimintoja kuten *Citrixin* ja *Microsoft Terminal Server Clientin*.

Verkkotason yhteydet vaativat SSL VPN -laitteen tarjoamalta Internet-sivulta automaattisesti asentuvan asiakaspäänsovelluksen, jolloin sovellus neuvottelee verkkotasonyhteyden käyttäjän tietokoneelle. Sovellusta käytettäessä pystytään käyttämään Internet-selaimesta riippumattomia sovelluksia kuten etätyöpöytäyhteyksiä. SSL VPN:n etuja on helppo käyttöönottaminen, sillä laitteisto hoitaa kaikki tarvittavat yhteysmäärittelyt automaattisesti päätelaitteen ja asiakaspään välillä. Useimpiin SSL VPN päätelaitteisiin pystytään myös muodostamaan käyttäjäkohtaisia rajoituksia, jolloin välttämättä erillistä palomuuria ei tarvita rajaamaan yhteyksiä yläpäässä. [19; 20, s. 33 - 34.]

SSL VPN -laitteiston muodostamat yhteydet

SSL VPN -tekniikkaa ei ole suunniteltu käytettäväksi verkkojen välisiin yhteyksiin kuten edellä mainittiin. SSL VPN -tekniikan lähtökohtana on alun perin ollut suunnitella tekniikka, joka mahdollistaa yhteyden muodostaminen verkon resursseihin Internetiin kytketyltä tietokoneelta.

SSL VPN käyttää ilman erillisiä komponentteja ohjelmistotason yhteyksiä verkkotason yhteyksien sijasta. Syy ohjelmistotasonyhteyksien käyttöön on tietoturva ja SSL-protokollan tekniset rajoitukset. Toinen syy on, että yrityksen tietoturvapolitiikka normaalisti kieltää esim. Internet-kioskeista yhteyksien käyttämisen, jolloin verkkotason liikenteen avaaminen on viruksien kannalta erittäin vaarallista.

SSL VPN -laitteistot mahdollistavat, että käyttäjän tietokoneesta tarkistetaan luotettavuus, jolloin voidaan estää verkkotasonyhteyden muodostaminen epäluotettavilta tietokoneilta. Verkkotasonyhteys voidaan sallia ainoastaan, jos käyttäjän tietokoneesta löytyy yrityksen määrittelemä "tunnistustieto". Tunnistustieto voi olla mm. tietokoneen rekisterissä oleva ennalta määrätty arvo.

Yhdyskäytävätekniikka (Reverse Proxy Technology)

SSL VPN -laitteistojen yleisin toiminto on niiden kyky välittää uudelleen käyttäjän lähettämiä sivupyyntöjä. Laitteiston ulkoverkkoon tulevat sivu-

pyynnöt välitetään laitteiston sisäverkon puolella oleville laitteille. Tätä yhdyskäytävätyyppistä toimintaa kutsutaan nimellä *reverse proxying*. Teknisesti ottaen *reverse proxy* on palvelin, joka on ulkoisen Internet-palvelimen (laitteiston tarjoaman sivuston) ja sisäverkon välillä. Samanlaista *reverse proxying* -tekniikkaa käytetään mm. suurien Internet-sivustojen kuormanjaon yhteydessä. Kuormanjaossa varsinaiset sivupyynnöt hajautetaan useammille palvelimille toteutettavaksi. [20, s. 44 - 46.]

Sovelluksien liikenne käyttäen SSL VPN -tekniikkaa

Reverse proxy -tekniikka välittää tiedot käyttäen *Hyper Text Transfer Protocol Security* (HTTPS)- tai HTTP-liikennettä. HTTPS on suojattua Internet-liikennettä ja käyttää liikennöinnissä TCP-porttia 443, kun vastaavasti HTTP käyttää TCP-porttia 80. Sovellukset, jotka eivät pohjaudu HTTP- tai HTTPS-protokollien käyttöön valitsevat usein dynaamisesti käyttämänsä TCP tai UDP portin. Dynaamisten porttivalintojen seurauksena standardi *reverse proxy* -tekniikka ei pysty hallitsemaan sovelluksien liikennettä.

SSL VPN -laitteistojen valmistajat ovat puuttuneet porttirajoitusongelmaan ja kehittäneet ongelman kiertämiseksi erinäisiä ratkaisuja. Ratkaisuja ei ole standardoitu ja ne ovat aina laitevalmistajakohtaisia. Seuraavassa on esitelty erilaisia vakiintuneita vaihtoehtoja ohjelmistojen liikenteen toteuttamiseksi käyttäen SSL VPN -tekniikkaa:

- Porttien uudelleenohjaaminen. Tietoturvan kannalta porttien uudelleenohjaus on hyvä vaihtoehto, jos se mahdollistaa sovelluksen toiminnan.

- SSL VPN avaa dynaamisesti sovelluksien käyttämät portit. Tämä vaihtoehto on erittäin epäsuotava tietoturvan kannalta ja on vastoin SSL VPN:n perusajastusta.

- Käyttöjärjestelmiin sisältyvät komponentit, joilla voidaan ohjata yhteyksiä. Windows-käyttöjärjestelmissä esimerkiksi *Name Space*

Provider. Käyttöjärjestelmärajapintojen käyttäminen vaatii SSL VPN -laitteisto valmistajilta enemmän työtä SSL-tekniikan hyödyntämiseen. Menetelmä sitoo laitteita käyttöjärjestelmään, mutta antaa paremman kontrolloinnin yhteyksiin, joka puolestaan parantaa tietoturvaa.

- Näppäimistön, videon ja hiiren signaalien välittäminen standardissa SSL määrittelyssä. Vaihtoehto ei ole monimutkaisessa ympäristössä käyttökelpoinen.

- Verkkotasonyhteys. Toimivin ratkaisu, mutta menetelmää käytettäessä täytyy kiinnittää huomiota tietoturvaan ja käyttäjien luotettavuuteen. [20, s. 47 - 49.]

Verkkotasonyhteys ja SSL

Verkkotasonyhteydet vaativat, että käyttäjän ja VPN-laitteiston välillä on koko TCP/IP-protokolla käytössä. SSL VPN -laitteistolla on mahdollista muodostaa verkkotasonyhteys, mutta kaikilla laitteistovalmistajilla tätä ominaisuutta ei ole. SSL VPN lähettää käyttäjälle ohjelmistokoodin yleensä ActiveX-komponenttina tai Java Applettina. Ohjelmistokoodin tehtävänä on muodostaa käyttäjän tietokoneelle virtuaalinen lähiverkkosovitin. Ohjelmistokoodin huono puoli on, että se vaatii järjestelmänhallinta (*administrator*) tason käyttäjätunnuksen ensimmäisellä kirjautumiskerralla.

SSL VPN antaa virtuaaliselle lähiverkkosovittimelle IP-osoitteen laitteiston sisäverkon puolelta. Käyttäjän tietokone käyttää tätä virtuaalista lähiverkkosovitinta sisäverkon puolella olevien laitteiden kanssa kommunikointiin. Kommunikointi tapahtuu käyttämällä SSL-suojattua tunnelia sisäverkon ja etäkäyttäjän välillä. Tämä muistuttaa hyvin paljon IPSec VPN -ratkaisua, sillä virtuaalisen lähiverkkosovittimen välityksellä on mahdollista liikennöidä käyttäen protokollia kuten TCP:tä, UDP:tä ja IP:tä. Muihin sisäverkon puolella oleviin verkkoihin on mahdollista liikennöidä, jos IP-reititys on asianmukaisesti määritelty laitteiston IP-osoitteille.

SSL-tunneloinnin muotoja ovat mm. *full tunneling* ja *split tunneling*. *Full tunneling* toimintatilassa kaikki käyttäjän muodostama liikenne lähetetään SSL VPN -laitteistolle. SSL VPN -laitteisto reitittää tiedon eri verkkoihin sille määritettyjen sääntöjen mukaisesti. *Full tunneling* toiminnassa myös normaali Internet-liikenne menee tällöin SSL VPN -laitteiston kautta. *Split tunneling* -toimintatilassa puolestaan laitteiston määrityksiin liittyvä liikenne lähetetään SSL VPN -laitteistolle. Normaali Internet-liikenne kulkee suoraan käyttäjän normaalin yhdyskäytävän kautta. [20, s. 48 - 50.]

SSL VPN on arkkitehtuurina hyvin joustava ja antaa tulevaisuudessa erinomaisia mahdollisuuksia toteuttaa monimutkaisia etäyhteyksiä. SSL VPN:n erikoisuutena on, että tekniikka mahdollistaa eritasoisten verkkoyhteyksien määrittelyn sovelluksesta riippuen. Tämä on tietoturvan kannalta merkittävää ja estää hyvin esim. verkossa leviävien viruksien tarttumista.

6 KOLMANNEN OSAPUOLEN ETÄKÄYTTÖYHTEYDET

Etäkäytön tarpeet ja sovellukset vaihtelevat paljon eri yritysten välillä. Yrityksen toimiala tuo usein mukanaan erilaisia tarpeita, joista hyvänä esimerkkinä voidaan pitää energia-alaa. Fingrid Oyj (jatkossa Fingrid) on valtakunnallinen kantaverkkoyhtiö, joka vastaa Suomen päävoimansiirtoverkosta. Fingridin politiikka on käyttää palveluntoimittajia tuottamaan sähköasemien ja voimajohtojen kunnossapitoa. [21.]

Laitteet ja tekniikat ovat kehittyneet viime vuosina erittäin paljon, ja näin ollen tekniikka ei ole enää rajoitteena etäkäyttöyhteyden käyttämiseen. Etäkäyttöyhteyksien turvallinen liittäminen yrityksien tietoverkkoon asettaa usein haastavia ratkaisuja.

Tässä luvussa perehdytään palveluntoimittajille tarjottavien etäkäyttöyhteyksien taustoihin, ongelmiin ja esitetään teknisiä ratkaisuja ongelmien ratkaisemiseksi.

6.1 Palveluntoimittajien etäkäytön taustat, tarpeet ja ongelmat

Fingridillä on 105 eri puolilla Suomea sijaitsevaa sähköasemaa. Fingrid hankkii sähköasemien kunnossapidon palveluna. Palveluntoimittajat kirjaavat työnsä ja hakevat dokumentteja tarvittaessa Fingridin tietojärjestelmistä. Fingridin sisällä kunnossapidon tietojärjestelmät ovat helposti käytettävissä, mutta kolmannen osapuolen verkoista tuleville käyttäjille välitettävä tieto vaatii tietojen siirtämisen julkisen tietoverkon läpi. Tämän seurauksena on kehitettävä palveluntoimittajille soveltuva etäkäyttöyhteysmalli, joka toimisi käyttäjien omien organisaatioiden kannettavissa tietokoneissa turvallisesti.

Sähköaseman tukijärjestelmiksi on Fingridissä määritelty kaikki ne sähköaseman järjestelmät tai sovellukset, joita ei käytetä varsinaisesti ohjaamaan toimilaitteita. Tukijärjestelmät verkottuvat entistä enemmän uusien sähköasemaväylä ratkaisujen myötä ja pohjautuvat entistä enemmän TCP/IP-tekniikkaan perinteisen sarjaliikenteen sijasta. Laitteista voidaan kerätä informaatiota tiedonkeruupalvelimilla, jotka taltioivat sähköasemien laitteista kuntotietoja. Kuntotiedot parantavat vikojen ennalta havaitsemista, ja tämän seurauksena korjaustoimet voidaan aloittaa sähköverkon käytön kannalta sopivana hetkenä, jolloin käytettävyys paranee. TCP/IP-tekniikka mahdollistaa kunnossapitotietojen reitittämisen useisiin järjestelmiin ja tekee mahdolliseksi myös tietojen lukemisen etäältä. [22.]

Ongelmana toimittajien etäkäyttöyhteyksissä on niiden vaatimat rajoitustarpeet. Samalla sähköasemalla saattaa olla useiden eri palveluntoimittajien toimittamia järjestelmiä, jolloin ainoastaan IP-aliverkkotasolla tehtävät rajoitukset eivät välttämättä riitä. Yhteydet tulisi pystyä rajoittamaan niihin järjestelmiin, jotka ovat kyseisen palvelutoimittajan vastuulla.

Suurimman ongelman aiheuttaa etätyöpöytäyhteydet. Etätyöpöydän avulla on mahdollista tutkia samassa aliverkossa olevia muita laitteita, vaikka pääsy olisikin alun perin sallittu vain yhteen tietokoneeseen. Rajoitus ei estä jatkoyhteyksiä samassa aliverkossa oleville laitteille. Ongelmia eivät aiheuta järjestelmät, joista tiedot voidaan välittää suoraan yläpäähän järjestelmän omalla protokollalla tai käyttäen olemassa olevia protokollia

kuten HTTP:tä. Tietoa siirrettäessä määrätyllä tiedonsiirtoprotokollalla on mahdollista kohdistaa rajaukset käytettävään protokollaan tai protokollan käyttämään UDP- tai TCP-porttiin. Tiedonkeruupalvelimien käyttö lisäisi tietoturvaa tilanteissa, joissa sillä pystyttäisiin korvaamaan etätyöpöytäyhteyksien tarve.

Ongelma ei pelkästään rajoitu tähän vaan myös toisen toimittajan laitteiston vikaantuessa tai väärän määrityksen johdosta voi ääritapauksessa sähköaseman lähiverkko vikaantua. Väärin määritetyt tai vikaantuneet laitteet voivat verkossa lähettää virheellisiä paketteja, joihin kaikkien laitteiden täytyy verkossa vastata. Ylimääräinen liikenne voi aiheuttaa mm. paikallisen palvelunestohyökkäyksen.

6.2 Etäkäyttöyhteyksien teknisen suojautumisen vaihtoehdot

Edellisessä luvussa on esitelty kaksi pääasiallista etäkäyttöyhteys arkkitehtuuria. IPSec VPN soveltuu käytettäväksi hyvin etäkäyttömallin tai päästä päähän -mallin mukaisissa yhteyksissä. SSL VPN -arkkitehtuuri puolestaan tuottaa etäkäyttömallin mukaisia VPN-yhteyksiä.

VPN-yhteyksien muodostamisvaihtoehdot

Palveluntoimittajien yhteyksiä ajateltaessa päästä päähän -malli on usein liian raskas toteutettavaksi johtuen sen tarvitsemista tietoliikennelaitteista ja verkkotason määrittelyistä. Kunnossapitotiedon noutamiseksi päästä päähän -mallin mukaisia yhteyksiä ei tarvita ja suotavaa on toteuttaa tiedonnoutaminen käyttäen etäkäyttömallin mukaista VPN-mallia. VPN-yhteyksille usein riittää, että yhteys voidaan muodostaa käyttämällä julkista tietoverkkoa.

Etäkäyttömallia käytettäessä ongelmia voi aiheutua mm. laitteistoriippuvaisista VPN-sovelluksista. Palveluntoimittajille tulee toimittaa erillinen tietokone tai asentaa olemassa olevaan tietokoneeseen VPN-sovellus, jotta yhteyden muodostaminen on mahdollista. Palveluntoimittajan yrityksen tietokoneessa voi olla asennettuna omassa yrityksessä käytettävä VPN-sovellus, joka on eri kuin Fingridissä käytetty sovellus. Lisäksi pal-

velun toimittajilla on omat tietoturvapolitiikat, jotka vaikeuttavat sovellusten asentamista ja tuovat rajoituksia ohjelmistojen suhteen.

Toimittajan tietokoneessa oleva VPN-sovellus voi häiritä Fingridin tarjoaman VPN-sovelluksen toimintaa. Häiriöt johtuvat usein verkkojen välisistä reitityksistä ja palomuurisäännöstöistä. Ongelman yleisin aiheuttaja on laitteistovalmistajien VPN-sovelluksiin sisältyvä ohjelmistopalomuuri. Ohjelmistopalomuuri voi estää toisen valmistajan VPN-yhteyden toiminnan.

Etäkäyttömallissa palveluntarjoajalla eli tässä tapauksessa Fingridillä on tietoliikennelaitteisto, joka mahdollistaa VPN-yhteyksien neuvottelun asiakaspään ja laitteiston välillä. Palveluntoimittajalle etäkäyttömallissa tarvitaan VPN-ohjelmisto, jolla yhteydessä käytettävät yhteydenmuodostamisehdot neuvotellaan.

Vaihtoehtona etäkäyttöyhteyksien toteuttamiseksi voidaan käyttää VPN-yhteyttä, joka ei tarvitse erikseen asennettavaa VPN-ohjelmistoa. SSL VPN -arkkitehtuurissa on mahdollista saada yhteyden muodostamiseen tarvittava ohjelmisto suoraan laitteelta yhteyttä muodostettaessa. Käytännössä laitteiston muistissa on VPN-sovellus, joka asennetaan käyttäjällä ensimmäisellä yhteys kerralla. Lisää SSL VPN -toteutuksesta löytyy luvusta käytännön toteutus (luku 8).

Verkkotason rajoitukset

SSL VPN -arkkitehtuurin mukaisten laitteistojen tarjoama liikenteen rajoitusmahdollisuus ei aina riitä. Tietoturvaa mietittäessä jokainen verkossa oleva komponentti on yhtä tärkeä. Sähköasemien IP-yhteydet on toteutettu käyttäen operaattorin MPLS-verkkoa. MPLS-tekniikan käyttö muodostaa suljetut päästä päähän -yhteydet toimiston ja sähköasemien välillä. MPLS-yhteydet on erotettu julkisesta tietoverkosta omaksi loogiseksi verkoksi.

MPLS-yhteydelle voidaan samaan fyysiseen liityntään määritellä verkkoja eri käyttötarkoituksiin, mutta vaikeuksia aiheuttaa laitteet joiden tulisi

toimia kahdessa eri verkossa. Samassa verkossa voi olla laitteistoja, joihin ei toisella palveluntoimittajilla ei saa olla käyttöoikeuksia edes vahingossa. Samassa verkossa olevien laitteiden erottaminen on hankalaa ja tarvitsee tietoliikennelaitteistoilta kyvyn erotella saman verkon resursseja omiksi loogisiksi yhteyksiksi.

Edellä esitetty verkko-ongelma voitaisiin ratkaista mm. laiteriippuvaisella ratkaisulla käyttämällä kytkimiä, jotka mahdollistavat yksityisten virtuaaliverkkojen hajottamisen useampaan loogiseen virtuaaliverkkoon *Private Virtual Local Area Network* (PVLAN). Käytännössä tämä tarkoittaisi sitä, että saman virtuaaliverkon sisällä pystyttäisiin OSI-mallin siirtoyhteyskerroksella erottelemaan laitteita loogisesti eri verkkoihin. Laitteet kommunikoisivat edelleen samalla IP-osoiteavaruudella ja yhteydellä.

Samassa kytkimessä olevien laitteiden kommunikointi ei tällöin onnistu siirtoyhteyskerroksella. Kommunikointi voidaan sallia, mutta se vaatii aina verkkotasolla toimivan laitteen lisäksi. Etuja tällaisesta eristämisestä on mm. virheellisestä toiminnasta johtuvien *Address Resolution Protocol* (ARP) kyselyjen eristäminen. [23.]

Verkkotason tietoturva nousee yhä tärkeämmäksi nykypäivän tietoliikenneverkoissa, joissa siirretään reaaliaikaisesti tietoa, IP-puheluita ja videokuvaa. Verkossa täytyy olla joustavuutta määrittelemään liikenteelle erilaisia prioriteetteja, jotta tärkeimmät yhteydet toimivat aina saumattomasti.

6.3 Sopimustekniset asiat

Sopimukset esittävät erittäin tärkeää roolia, kun ollaan toteuttamassa palveluntoimittajille tarjottavia yhteyksiä. Yhteyksiä ei pidä toteuttaa ennen kuin sopijaosapuolet ovat sopineet yhteyden ehdoista ja vastuista kirjallisella sopimuksella. Sopimuksissa tulee määritellä käytettävät laitteistot ja laitteistovaatimukset ml. sallitut ohjelmistot. Sopimukset on hyvä määritellä erittäin tiukasti, koska tällöin usein vältytään yhteyksiltä, jotka eivät ole käyttäjille välttämättömiä.

Fingridissä on sopimuksen lisäksi ohje etäkäyttöyhteyden käyttämiseen. Etäkäyttöyhteysohjeessa on mukana käytettävän laitteiston tarkistamislista, joka sisältää asiat, jotka tulee olla kunnossa etäyhteyttä käytettäessä. Tarkistuslistaa täytyy ylläpitää ja päivittää jatkuvasti, jotta se vastaa tarkistushetken käsitystä tietoturva-asioiden huomioonottamisessa. Liitteessä kaksi on esitettynä Fingridin tämän hetken toimittajan kanssa läpi käytävä tarkistuslista. Lisäksi SSL VPN -laitteistoissa on mahdollisuuksia suorittaa tarkistuksia jokaisella kirjautumiskerralla, jolloin varmistutaan jatkuvasti tarkistuksen tuottamien tuloksien oikeellisuudesta. [24.]

7 CYBER SECURITY STANDARDIEN SOVELTAMINEN

Amerikkalaisen *North American Electric Realibility Council* (NERC) järjestön luomien CIP-002-009 standardien tarkoitus on määritellä kriittisten sähköjärjestelmien suojaukselle reunaehdot. Standardien määrittely kattaa ohjelmoitavat laitteet ja tietoliikenneverkkojen laitteistot, ohjelmistot ja verkossa siirrettävän tiedon. Vaatimukset koskettavat amerikkalaisia toimijoita, mutta tässä työssä on tutkittu niiden soveltuvuutta Fingridin ympäristöön.

NERC-järjestön lautakunta on hyväksynyt CIP-002...009 -standardit käytettäväksi 3. maaliskuuta 2006. CIP-002-009-standardit korvaavat aikaisemmin voimassa olleen *Urgent Action Cyber Security* -standardin. Standardi on nykyisessä muodossaan paljon kattavampi ja ottaa paremmin kantaa kohteisiin ja omaisuuteen. Lisäksi standardit ottavat paremmin huomioon eri roolit sähköverkkojen operoinnissa. [25.]

7.1 Standardien sisältö ja tavoitteet

Cyber Security -standardit muodostuvat kahdeksasta eri kokonaisuudesta. Standardeja luettaessa täytyy ymmärtää NERC-järjestön tekemät määritykset *Cyber*-termeille. Standardien määritykset pohjautuvat seuraavassa esitettyihin määritelmiin:

- *Critical Assets*; Kalustot, järjestelmät ja laitteet, jotka voivat vaikuttaa sähköverkon toimintaan tai operointiin hajotessaan tai olemalla pois käytettävistä. Esim. suojareleet ja katkaisimet.

- *Cyber Assets*; Ohjelmoitavat laitteet ja tietoliikenneverkot sisältäen laitteistot, ohjelmistot ja itse tiedon.

- *Critical Cyber Assets*; Kriittisen omaisuuden (*Critical Assets*) luotettavaan operointiin tarvittavat ohjelmistot ja tietoliikenneverkot (*Cyber Assets*). Hyvä esimerkki on käytönvalvontajärjestelmään liittyvät tietoliikenneyhteydet.

- *Cyber Security Incident*; Mikä tahansa haitallinen tai epäilyttävä toimenpide, joka vaarantaa tai haittaa kriittisen omaisuuden operointia.

Näiden määritelmien lisäksi standardeissa käsitellään fyysiset ja loogiset ympäristöt. [25.]

Standardien pääjaot pohjautuvat pääosin *International Electrotechnical Commission* (IEC) järjestön tekemään tietoturvamääritykseen 17799. Luvussa kaksi puhuttiin jo, että oikean kriittisen tiedon tunnistaminen on tärkeää ja myös *Cyber Security* -standardin ensimmäinen osa käsittää, kuinka tunnistetaan oikeat kriittiset toiminnot (*Critical Cyber Assets)*. Standardien eri osissa esitetään tarkistuslistat vaatimuksille ja kuinka vaatimukset mitataan ja valvotaan. Menetelmän tarkoituksena on asettaa palveluntoimittajille standardiin perustuvat mittarit.

Tarkistuslistassa on tarkasti kerrottu mitkä vaatimukset tulee täyttyä, jotta voidaan käyttää mm. *Critical Cyber Assets* -termiä. Esimerkkinä tästä voidaan mainita, että ohjelmoitavat laitteet (*Cyber Assets*) käyttävät ulkopuoliseen kommunikointiin reititysprotokollaa. Listaan tulisi kyllä lisätä myös staattiset reitit ykset, jotka mahdollistavat myös ulkomaailmaan kommunikoinnin.

Standardien muut osakokonaisuudet käsittävät hallinnan ja järjestelmien tietoturvan kontrolloinnin, henkilöstön kouluttamisen, fyysisten ja loogisten järjestelmien vaatimukset. Tämän lisäksi vielä yksi kokonaisuus käsittää raportoinnin. Standardien kaikkia yksityiskohtia ei tässä työssä käsitellä.

7.2 Standardien soveltuvuus kolmannelle osapuolelle

Cyber Security -standardien lähtökohtana on ollut luoda vaatimukset kriittisten järjestelmien kontrollointiin. Standardikokonaisuuksien määrittelemät vaatimuslistat ovat hyvin sovellettavia ja pystytään helposti tarkistamaan täyttyvätkö vaaditut vaatimukset. Tarkistuslistat koskettavat hyvin paljon sähköverkon eri komponentteja jopa tehorajoihin asti. Vaatimusten lisäksi tulisi ottaa vielä paremmin huomioon järjestelmien vaatimukset ja ohjelmistojen luotettavuuden määrittäminen, sillä ohjelmistovirheet ovat yleisempiä kuin itse laitteiston vikaantuminen.

Standardeissa esitetyt laatumittarit ovat peräisin Amerikasta eivätkä kaikki mittarit sovi suoraan käytettäväksi Suomalaisessa ympäristössä. Standardeista on mahdollista poimia kohtia täydentämään etäyhteys sopimuksen yhteydessä käytävää tarkistuslistaa tai yrityksen tietoturvapolitiikkaa, joka huomioi paremmin sähköverkkoliiketoiminnan. Kokonaisuudessa standardien noudattamisen valvominen on erittäin hankalaa. Standardien mittarien valvonta kaikkien palvelutoimittajien kanssa lisäisi huomattavasti työmäärää. Lisäksi mittareista suurin osa pohjautuu dokumentointiin ja dokumentoinnin valvontaan, joka ei aina välttämättä tuo haluttua tulosta.

7.3 Standardien soveltuvuus Euroopassa

Standardien tarkoitus on ottaa huomioon sähköverkkojen eri operoijat. Sähköjärjestelmien verkottuminen kehittyy hyvin nopeasti ja standardien tarkistuslistat jäävät helposti vanhoiksi. Uudet tietoturvauhat aiheuttavat standardien jatkuvan päivittämisen tarpeen. Standardien parempi lähtökohta olisi, että asiat määriteltäisiin jo eri sähköverkkojärjestelmien omissa standardeissa, joissa olisi tietoturva-asiat mietitty kuntoon tapauskoh-

taisesti. Yleisellä tasolla on hyvin vaikeaa määritellä eri sähköverkkokomponenttien tietoturvavaatimukset ja laitteiden tärkeys koko järjestelmän toiminnan kannalta.

Tämän työn tekohetkellä oli perustettu IEC-työryhmä, jonka aiheena on *Cyber Security* -standardi. Työryhmään kuuluu Ethernet-pohjaisten kenttäväylien valmistajia kuten Profibus, Fieldbus ja Modbus. Standardin lähtökohtana on kohdistaa huomiota suoraan järjestelmien ja laitteiden välisten kommunikointien tietoturvaan. Työryhmässä ei työskentele yhtään suomalaista. [26.]

8 KÄYTÄNNÖN TOTEUTUS

Palveluntoimittajien etäkäyttöyhteydet on mahdollista toteuttaa IPSec VPN -arkkitehtuuriin perustuvalla etäkäyttömallin tai päästä päähän -mallin mukaisella VPN-yhteydellä. Toinen vaihtoehto yhteyksien toteuttamiseen on käyttää SSL VPN -arkkitehtuurin mukaista etäkäyttömalliin perustuvaa etäkäyttöyhteyttä. IPSec VPN -arkkitehtuurin heikkous on sen tarvitsemat erilliset käyttäjälisenssit etäkäyttömallin mukaisissa yhteyksissä, jolloin palveluntoimittajille täytyy toimittaa omat käyttäjälisenssit VPN-sovellukseen.

Päästä päähän -mallin mukaiset etäkäyttöyhteydet eivät puolestaan sovellu käytettäväksi, koska suurin osa palveluntoimittajista työskentelee liikkuvassa työssä. Ongelmana liikkuvassa työssä on, että käyttäjät eivät ole aina paikalla omassa konttorissa, johon päästä päähän -yhteys täytyisi muodostaa. SSL VPN -arkkitehtuuri nousi parhaaksi vaihtoehdoksi johtuen sen tuomasta joustavuudesta yhteyksien määrittelyssä. Etäkäyttöpalvelun käyttäjille ei tarvitse erikseen toimittaa sovelluslisenssejä. Kokonaiskustannukset yhteyksien ylläpitämisestä kohdistuvat ainoastaan SSL VPN -laitteiston ylläpidon kustannuksiin.

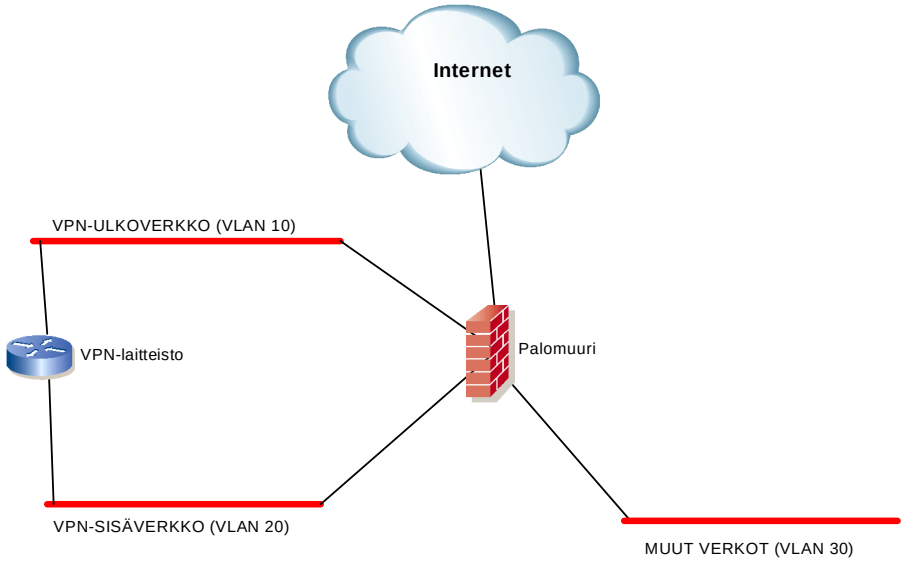
Laitteiston valintahetkellä parhaaksi SSL VPN -tuotteeksi ominaisuuksien puolesta nousi Juniperin valmistama *Secure Access* tuote. *Secure Ac-*

cess -tuotteen parhaimpia ominaisuuksia olivat hallittavuus ja joustavuus käyttäjäprofiilien määrittelyssä. Muita vaihtoehtoisia SSL VPN -tuotteiden valmistajia olivat Cisco, Nokia ja F5. F5-valmistajan tuote pärjäsi testeissä myös hyvän Citrix-tuen ansiosta, mutta ylläpidon ja kustannuksien kannalta Juniper oli tuotteena soveltuvin valinta. SSL VPN -laitteistot kehittyvät nopeaa vauhtia ja uutta ympäristöä rakennettaessa on suotavaa tarkistaa markkinoiden sen hetkinen tilanne.

Fingridille toteutettiin Juniperin SSL VPN -laitteistoon pohjautuva palveluntoimittajien etäkäyttöympäristö. Palveluntoimittajien etäkäyttöympäristöä ei käytetä Fingridin oman henkilökunnan etäkäyttöyhteyksissä vaan siihen on käytössä IPSec-tekniikkaan perustuva laitteisto.

Ympäristön suunnitteluvaihteessa palvelutoimittajien profiilit määriteltiin yrityskohtaisesti palveluihin perustuvan määrittelyjen sijasta. VPN-istuntoon voidaan profiilikohtaisesti määritellä kestoajat, tarkistusmenetelmät, IP-osoiteavaruudet ja tunnistautumismenetelmät. SSL VPN -laitteisto mahdollistaa myös Internet-pohjaiset neuvottelut. Fingridin ympäristössä käytettäviä palveluita ovat mm. etätyöpöytäyhteydet ja Internet-pohjaiset palvelut. Suunnitteluvaiheessa todettiin, että laitteiston omia etäyhteysohjelmistoja ei käytetä yhteyksien toteuttamiseen. Laitteiston tarjoamien sovellusten todettiin aiheuttavan ongelmia eri toteutuksissa. Ongelmia aiheutti mm. Telnet-istunnot, joissa tiedot eivät aina välittyneet näytölle. Erillisellä Telnet-sovelluksella ei ongelmaa havaittu.

SSL VPN -laitteistoympäristö luotiin olemassaolevaan tietoverkkoon. Internetistä muodostettu yhteys muodostetaan SSL VPN -laitteiston ulkoverkkoon, josta käyttäjälle tarjotaan Internet-sivusto tunnistautumista varten. Fingridin toteutuksessa tunnistautumismenetelmä on SecurID-tunnistus RADIUS-palvelimen kanssa. SSL VPN -laite antaa määritetylle käyttäjälle määrätyn osoiteavaruuden laitteiston sisäverkonpuoleisiin verkkoihin. Laitteiston sisäpuolella oleva verkkoympäristö täytyy ottaa hyvin huomioon ympäristön suunnitteluvaiheessa. Yhteydet muihin verkkoihin rajoitetaan erillisellä palomuurilla (kuva 11).



Kuva 11. SSL VPN -topologia

SSL VPN -laitteiston määrittely tapahtuu käyttäen Internet-selainta. SSL VPN laitteiston komentokehotteessa voidaan määritellä ainoastaan laitteiston IP-osoitteet ja salasanat. Kaikki muu laitteiston määrittely kuten käyttäjäprofiilien luonti tapahtuu graafisen selainkäyttöliittymän kautta. SSL VPN -laitteistoa ei ole mahdollista määritellä ulkoverkkoon kytketystä rajapinnasta vaan ainoastaan sisäverkon puolelta. Liitteestä kolme voidaan nähdä Juniper Networksin valmistaman *Secure Access* -laitteiston hallintaympäristö. Lisäksi palveluntoimittajalle toimitettavan yhteydenmuodostamisohjeet löytyvät liitteestä neljä.

Ympäristön suunnittelu onnistui ja osa palveluntoimittajista on siirretty uuteen etäkäyttöympäristöön. Tämän työn tekohetkellä siirretyt käyttäjät ovat olleet tyytyväisiä ympäristön toimintaan. Fingridin SSL VPN -ympäristö ei ole käyttöjärjestelmäriippuvainen vaan toimii myös Linux- ja Mac-ympäristöissä. Fingridin palveluntoimittaja oli testannut myös Linux-pohjaista versiota ja yhteys oli toiminut odotetusti. Linux-pohjainen asennuspaketti on tehty Redhat-pohjaisiin Linux-versioihin, joten palveluntoimittajan oli ensin täytynyt muuttaa asennustiedosto Debian-pohjaisiin Linux-versioihin soveltuvaksi.

Fingridin SSL VPN -ympäristö suunniteltiin tulevaisuuden tarpeita varten. Ympäristön suunnitteluhetkellä määriteltiin asetukset ympäristön kahdentamista varten. Kahdentamista varten varattiin valmiiksi IP-osoitteet ja nykyinen laite määriteltiin primääri laitteeksi. Ympäristöä ei lähdetty suoraan kahdentamaan vaan todettiin, että seurataan miten ympäristön käyttöaste nousee ja milloin kahdentaminen on tarpeellista.

9 YHTEENVETO

Työssä tutustuttiin VPN-tekniikoihin ja niiden hyödyntämiseen tietoliikenneyhteyksien rakentamisessa. Työn yhteydessä todettiin SSL VPN tekniikkaan perustuvan VPN-yhteyden olevan kustannustehokkain tapa muodostaa palveluntoimittajien etäyhteydet, koska kaikki kustannukset kohdistuvat tietoliikennelaitteisiin. SSL VPN -laitteistojen huonoja puolia olivat verkkotason yhteydellä vaaditut sovellukset, jotka vaativat tietokoneen järjestelmävalvojan tunnukset ensimmäisellä kirjautumiskerralla. Työn ohella toteutettiin Fingridille SSL VPN -tekniikkaan perustuva palveluntoimittajien etäkäyttöympäristö.

Etäyhteyslaitteistojen valmistajien tulisi kiinnittää enemmän huomiota tai antaa ehdotuksia kuinka laitteiston takana olevat verkot olisi hyvä toteuttaa. Kaikkien laitteistovalmistajien laitteistoja ei välttämättä ole mahdollista ottaa käyttöön olemassa olevassa ympäristössä.

SSL VPN -laitteiston tuomat tietoturvamäärittelyt tuovat verkkoon erittäin hyviä rajoitusmahdollisuuksia, mutta eivät yksin pysty suojaamaan etäkäyttöyhteyksiä. Huomiota tulisi kiinnittää entistä enemmän verkkotason tietoturvaan ja tietoturvahyökkäyksien havainnointiin ja estämiseen. Useat tietoturvahyökkäykset kohdistuvat verkkotason ongelmiin ja voivat jäädä kokonaan huomaamatta ilman asianmukaisia määrittelyjä ja hallintaa. Erityisen tärkeää on, että käytössä oleva tietoliikennelaitteistokanta pystyy vastaamaan tietoverkon tarpeisiin.

Lisäksi tietoturvan tarkistamiseen olisi hyvä löytää standardeihin perustuva menetelmä, jolloin voitaisiin yksiselitteisesti määritellä ehdot ja varmistaa ehtojen toteutuminen. Työssä käsitelty NERC-järjestön luoma standardi ei pysty vielä yksiselitteisesti vastamaan automaatiojärjestelmien tietoturvatarpeisiin. Panostusta tulisi siirtää enemmän järjestelmien toimittajien harteille ja yrittää muuttaa palveluntoimittajien asennetta tietoturvaa kohtaan. Tietoverkko-osaaminen tulee varmistaa, jotta tietoturvan asettamiin haasteisiin voidaan vastata.

Verkkojen monimutkaistuminen ja sovelluksien kasvava tietoliikenteen tarve aiheuttaa tulevaisuudessa suuria haasteita verkonsuunnittelulle, jossa palveluntoimittajat tulisi pystyä huomioimaan. IPv6-osoitteiden laajempi käyttö voi tuoda uusia haasteita verkkotason tietoturvan ja etäkäyttöyhteyksien toteuttamiseen.

VIITELUETTELO

[1] ISO/IEC. *International Standard 17799: Information technology — Security techniques — Code of practice for information security management* [standardi]. 2005.

[2] Viestintävirasto. *Tietoturvalliseen yhteiskuntaan* [verkkodokumentti, viitattu 20.12.2006]. Saatavissa: http://www.ficora.fi/index/palvelut/tietoturva.html.

[3] Suomen Automaatioseura ry: *Teollisuusautomaation tietoturva*. 1.painos. Helsinki: Painomerkki Oy. 2005.

[4] Perlmutter, Bruce - Zarkower, Jonathan. *Virtuaaliset yksityisverkot*. 1. painos. Helsinki: Edita. 2001.

[5] Granlund, Kaj. *Tietoliikenne*. 2. painos. Jyväskylä: Gummerus Kirjapaino Oy. 2000.

[6] Ala-Mutka, Kirsti - Rintala, Matti - Savikko, Vespe - Palviainen, Jarmo. *OSI-malli* [verkkodokumentti, viiitattu 20.12.2006]. Saatavissa: http://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html.

[7] Kerttula, Esa. *Tietoverkkojen tietoturva*. 3.painos. Helsinki: Oy Edita Ab. 2000.

[8] Douglas, E.Comer: *TCP/IP*. 1.painos. Jyväskylä: Gummerus Kirjapaino Oy. 2002.

[9] Järvinen, Petteri. *Salausmenetelmät*. 1. painos. Porvoo: WS Bookwell. 2003.

[10] Microsoft. *How TLS/SSL Works* [verkkodokumentti, viitattu 20.12.2006]. Saatavissa: http://www.microsoft.com/technet/windowsserver/.

[11] IETF. *RFC 2246: The TLS Protocol version 1.0* [standardi]. 1999. Saatavissa: http://www.ietf.org/rfc/rfc2246.txt.

[12] Microsoft. *Overview of SSL/TLS Encryption* [verkkodokumentti, viitattu 20.12.2006]. Saatavissa: http://www.microsoft.com/technet/windowsserver/.

[13] IBM. *SSL/TLS Protocol and Crypto All You Want To Know* [verkkodokumentti, viitattu 20.12.2006]. Saatavissa: http://www-1.ibm.com/support/.

[14] Heikkilä, Tommi. *Verkonhallintajärjestelmän suojaaminen IPSecin avulla* [pro gradu -tutkielma]. 2002. Saatavissa: http://tisu.it.jyu.fi/terabitti/20021028-vh-ipsec-gradu-final-2.pdf.

[15] IETF: RFC 2406: *IP Encapsulating Security Payload (ESP)* [standardi]. 1998. Saatavissa: http://www.ietf.org/rfc/rfc2406.txt.

[16] Cisco Systems Incorporation. *Network Security 2 Course Material* [verkkomateriaali, viitattu 15.1.2007]. Saatavissa: http://www.cisco.com/.

[17] IETF: RFC 2401: *Security Architecture for the Internet Protocol* [standardi]. 1998. Saatavissa: http://www.ietf.org/rfc/rfc2401.txt.

[18] Microsoft. *IPSec Architecture* [verkkodokumentti, viitattu 20.12.2006]. Saatavilla: http://www.microsoft.com/technet/network/.

[19] Juniper Networks. *Juniper Networks Secure Access: Administration Guide* [verkkodokumentti, viitattu 15.1.2007]. Saatavissa: http://www.juniper.net/.

[20] Steinberg, Joseph - Speed, Timothy. *SSL VPN - Undestanding, evaluating, and planning secure, web-based remote access*. 1. painos. Birmingham: Packt Publishing Ltd. 2005.

[21] Fingrid Oyj. *Fingrid Oyj - Suomeksi* [verkkodokumentti, viitattu 15.1.2007]. Saatavissa: http://www.fingrid.fi/.

[22] Tiesmäki, Ville. *Sähköasemien väyläratkaisujen hyödyntäminen kantaverkkoyhtiössä* [diplomityö]. 2005.

[23] Cisco Systems Incorporation. *Understanding and Configuring Private VLANs* [verkkodokumentti, viitattu 15.1.2007]. Saatavissa: http://www.cisco.com/.

[24] Pennanen, Jyrki. *Tietoturvavaatimukset toimittajille* [ei julkinen]. 2006.

[25] NERC. *Cyber Security Standards* [verkkodokumentti, viitattu 15.1.2007]. Saatavissa: ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf.

[26] IEC. Membership of WG 13: Cyber Security [verkkodokumentti, viitattu 27.1.2007]. Saatavissa: http://www.iec.ch/.

VERKKOJEN VÄLINEN VPN-YHTEYS MÄÄRITTELY JUNIPER SSG PALOMUURILLA

Seuraavassa on esitetty mallikonfiguraatio, jossa salataan 192.168.1.0/24 verkon liikenne käyttäen julkista IP-osoitetta 10.0.0.1/24. Vastapäässä salattava verkko on 192.168.2.0/24 ja julkinen IP-osoite 10.0.0.2/24. Vastapään konfiguraatio on päin vastainen mikäli käytetään Juniperin laitteistoja.

```
// Asetetaan rajapintojen määrittely ja VPN-tunnelin määrittäminen yhteydelle

set interface ethernet1 ip 192.168.1.1/24
set interface ethernet1 nat
set interface ethernet2 ip 10.0.0.1/24
set interface ethernet2 route

set interface tunnel.1 zone Untrust
set interface tunnel.1 ip unnumbered interface ethernet2
set interface tunnel.1 mtu 1500

// Määritetään laitteiston oman ulkoverkon IP-osoiteavaruus

set address "Trust" "192.168.1.0/24" 192.168.1.0 255.255.255.0

// Määritellään vastapään ulkoverkon IP-osoiteavaruus

set address "Untrust" "192.168.2.0/24" 192.168.2.0 255.255.255.0

// Määritellään salausehdot ja avaintenvaihtoprotokolla Diffie-Hellman Group2, ESP-
otsikko, symmetrinensalaus 3DES ja tiedon eheyden tarkistukseen SHA-1.

set ike p1-proposal "esp-3des-sha" preshare group2 esp 3des sha-1 minute 1440
set ike p2-proposal "esp-3des-sha" group2 esp 3des sha-1 second 28800

// Määritellään VPN-yhdyskäytävä, jossa 10.0.0.2 on vastapään julkinen IP-osoite ja vastaa-
vasti 10.0.0.1 on laitteiston julkinen IP-osoite

set ike gateway "Gateway for 192.168.2.0/24" address 10.0.0.2 id "10.0.0.2" Main local-id
"10.0.0.1" outgoing-interface "ethernet2" preshare SALAUSAVAIN proposal "esp-3des-sha"

// Liitetään yhteydelle edellä määritelty yhdyskäytävä

set vpn "VPN for 192.168.2.0/24" gateway "Gateway for 192.168.2.0/24" replay tunnel
idletime 0 sec-level compatible

// Seuraava määritys tarvitaan, jos muodostetaan VPN-yhteys muun kuin Juniperin laitteiston
kanssa esim. Cisco ASA 5500.

set vpn "VPN for 192.168.2.0/24" proxy-id local-ip 192.168.1.0/24 remote-ip 192.168.2.0/24
"ANY"

// Lisäksi liitetään vielä asetukset VPN-yhteys rajapintaan

set vpn "VPN for 192.168.2.0/24" id 1 bind interface tunnel.1
```

```
// Sallitaan palomuurille kaikilla palveluilla verkkojen välinen liikenne

set policy id 1 from "Trust" to "Untrust"  "192.168.1.0/24" "192.168.2.0/24" "ANY" permit
set policy id 1
exit

set policy id 2 from "Untrust" to "Trust"  "192.168.2.0/24" "192.168.1.0/24" "ANY" permit
set policy id 2
exit

// Lisätään reititys, jotta 192.168.2.0/24 verkkoon kohdistuvat IP-paketit menevät VPN-
tunneliin

set route 192.168.2.0/24 interface tunnel.1
```

AUDITOINTIKYSELY

Perustiedot

Tarkistettu yritys

Vastannut henkilö

Tarkastaja

Aihe

Yleistä

Onko tietoturvaohjeistus tai -politiikka käytössä?

Onko käytössä salassapitosopimus?

Miten fyysinen turvallisuus on hoidettu?

Työasema

Onko työasema henkilökohtainen?

Seurataanko työaseman käyttöä, lokien kerääminen?

Minkä tasoinen käyttäjätunnus on käytössä?

Onko salasanan suhteen vaatimuksia (pituus,vaikeus, jne)?

Onko Internet-liikenteen rajoituksia (palvelukohtaisia esim. FTP)?

Onko www-liikenteen rajoituksia (tietyt sivut tai palvelut)?

Miten hoidetaan käyttöjärjestelmien päivitykset (windowsupdate)?

Virustorjunta

Onko virustorjunta käytössä?

Käytetäänkö kaupallista tuotetta?

Miten päivitys hoidetaan?

Palomuuri

Onko palomuuri työaseman ja Internetin välissä?

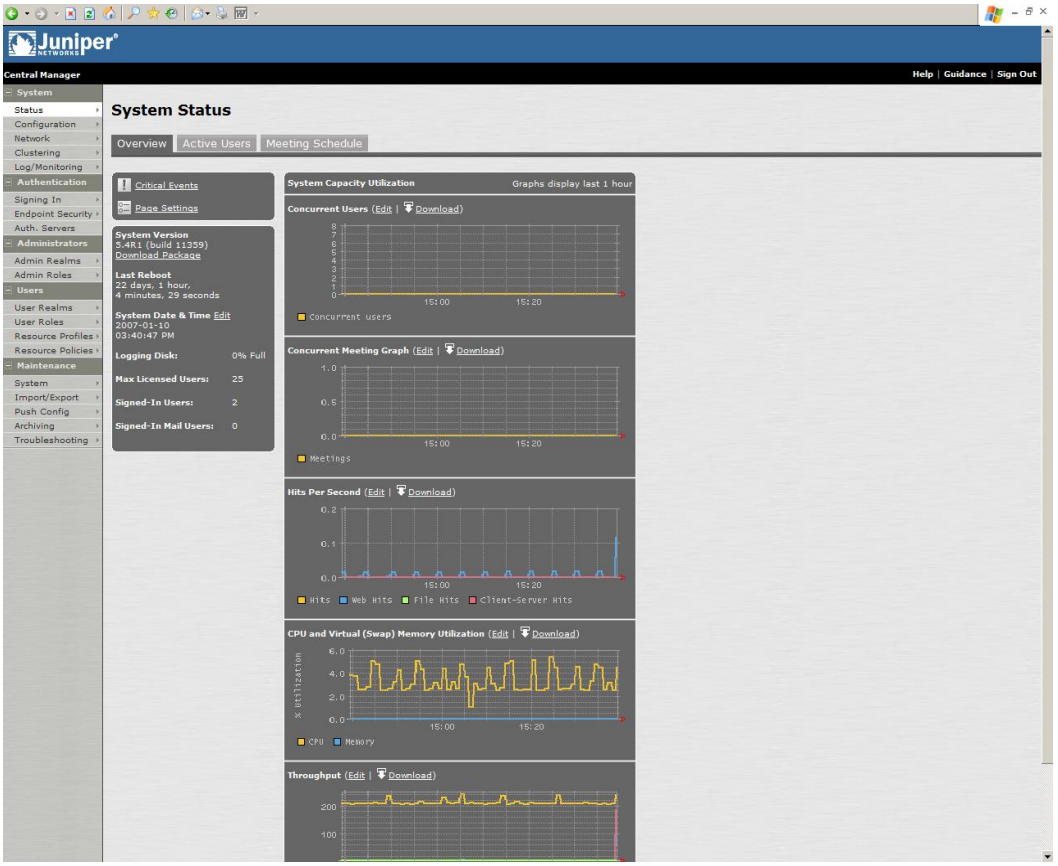
Onko se työasemassa vai onko yrityksessä erillinen ympäristö?

Miten ylläpito, oma vai ulkoinen?

Auditointi tarkistuslistan on luonut Fingrid Oyj:lle Jyrki Pennanen.

JUNIPER NETWORKS SECURE ACCESS HALLINTAYMPÄRISTÖ

Hallintaympäristöstä voidaan määritellä kaikki käyttäjäasetukset, yhteysprofiilit ja yhteyteen kuuluvat palvelut.



TOIMITTAJIEN ETÄKÄYTTÖYHTEYDEN MUODOSTAMINEN

Tämä dokumentti kuvaa kuinka palveluntoimittajien etäkäyttöyhteydet muodostetaan käyttäen Fingridin SSL VPN laitteistoa. SSL VPN perustuu SSL/TLS-tekniikalla salattuun yhteyteen, jonka lähtökohtana on muodostaa salattu yhteys Internet-selaimen avulla.

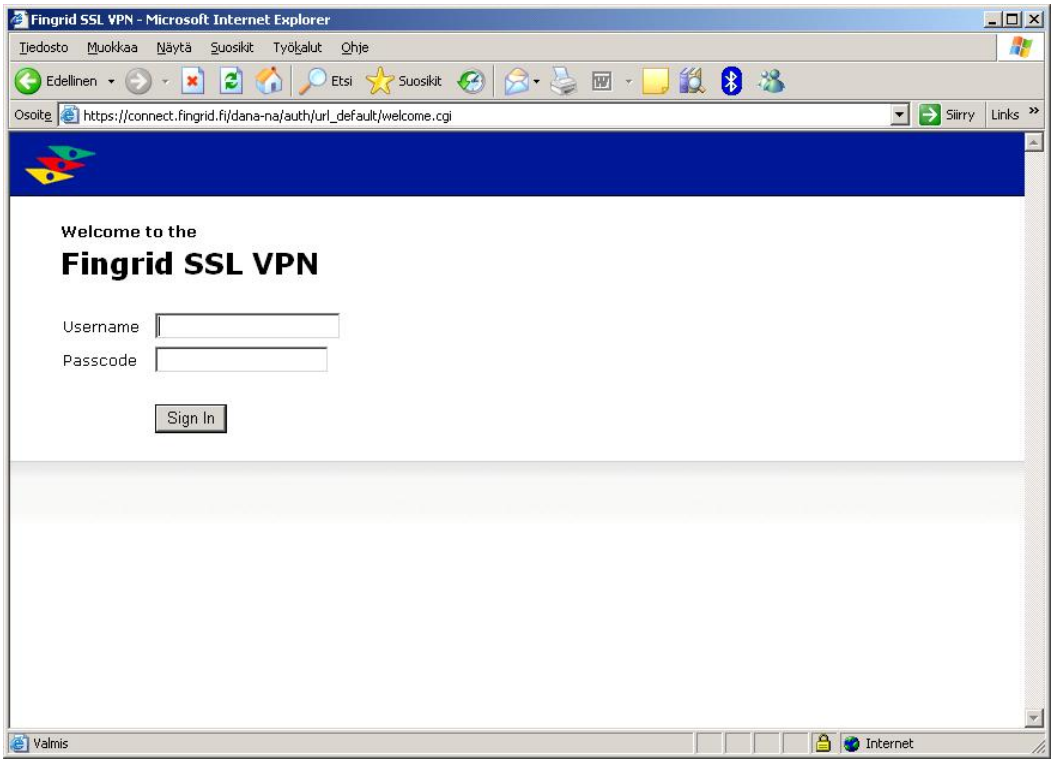
Yhteyden muodostaminen

Huomioitavaa on, että ensimmäisellä kerralla yhteyttä muodostettaessa tulee olla kirjautuneena tietokoneessa **järjestelmävalvojatason oikeuksilla**. Ensimmäisellä yhteyskerralla tietokoneeseen asentuu Juniper Networksin valmistama *Network Connect Client*, jonka tehtävänä on keskustella verkkotasonyhteys laitteiston ja tietokoneen välillä. Ensimmäisen kirjautumiskerran jälkeen järjestelmävalvojatason oikeuksia ei tarvita.

1) Yhdistetään selaimella osoitteeseen:

https://connect.fingrid.fi/

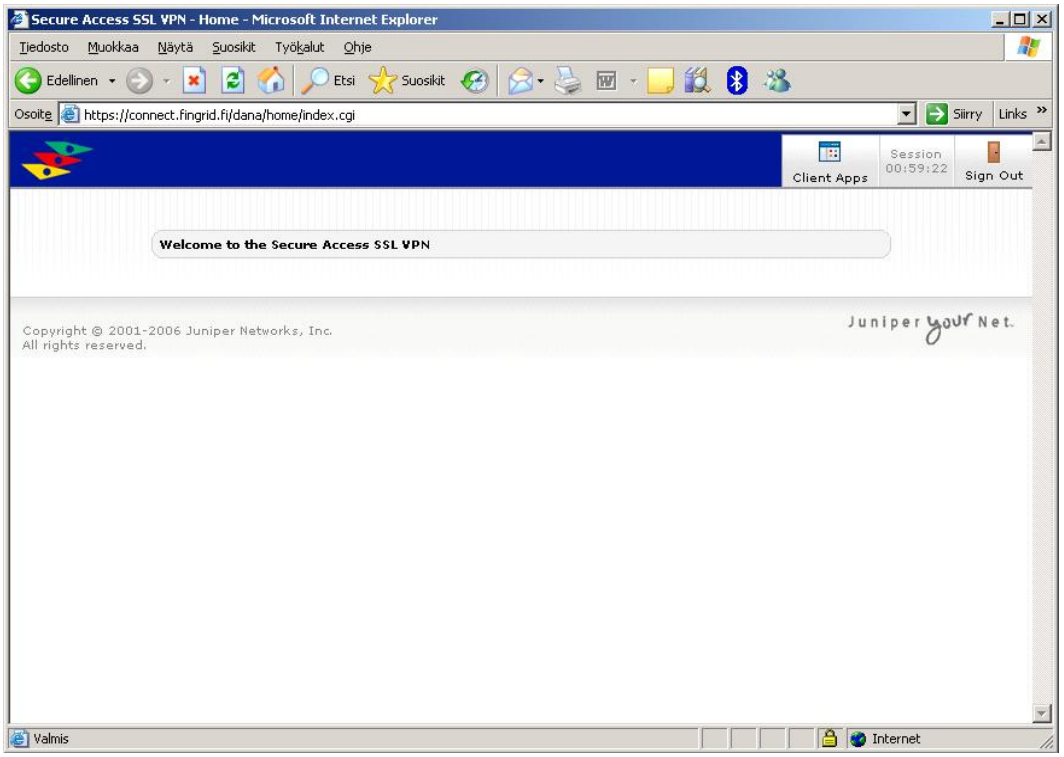
Jolloin kuvaruudulle ilmestyy kuvan yksi mukainen kuvaruutu.



Kuva 1. Kirjautumisruutu

2) Kirjautumisruutuun syötetään käyttäjätunnus (*username*) ja salasana (*passcode*) (PIN + 6 numeroa SecurID-kortista). Tämän jälkeen painetaan "*Sign In*" painiketta.

3) Kirjautumisen jälkeen nähdään kuvan kaksi mukainen selainikkuna, jolloin voidaan varmistua, että kirjautuminen on onnistunut ja salattuyhteys muodostetaan. **Selainikkuna tulee pitää auki koko suojatunyhteyden aikana.**



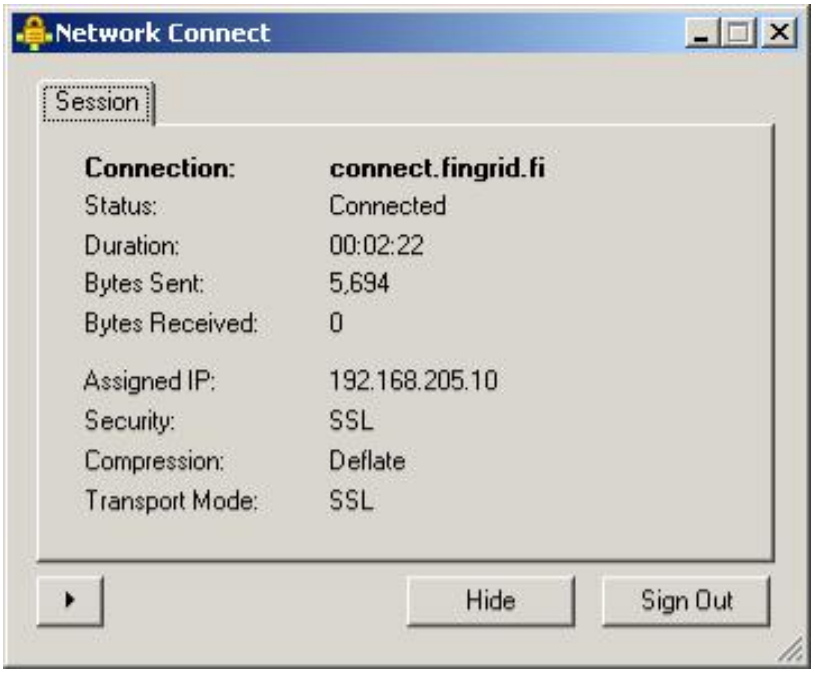
Kuva 2. Suojattuyhteys

3) Yhteys on nyt muodostunut. Yhteyden tilaa voidaan tarkastella painamalla tehtäväpalkista keltaista lukkoa hiiren oikealla painikkeella (kuva 3).

Kuva 3. Tehtäväpalkki

Hiiren oikealla painikkeella painettaessa saadaan näkyviin kuvan neljä mukainen valikko, josta "*Basic View*" vaihtoehdolla saadaan tarkemmat tiedot yhteyden tilasta (kuva 5).

Kuva 4. Valikko



Kuva 5. Yhteyden tiedot

5) **Yhteyden katkaiseminen** tapahtuu painamalla kuvan kaksi mukaisesta selainikkunasta "*Sign Out*" painiketta. Uloskirjautumisen yhteydessä tulee myös *Network Connect Client* ohjelmiston sulkeutua (keltainen lukko tehtäväpalkista).