VAASAN YLIOPISTO

TEKNILLINEN TIEDEKUNTA

TIETOLIIKENNETEKNIIKKA

Jussi Itämäki

TIETOTURVALLISET TIETOLIIKENNEYHTEYDET YRITYSYMPÄRISTÖSSÄ

ABB Oy:n ja kolmansien osapuolien tietojärjestelmien väliset tietoliikenneyhteydet

Diplomityö, joka on jätetty tarkastettavaksi diplomi-insinöörin tutkintoa varten

Vaasassa 29.6.2010

Työn valvoja	Matti Linna
Työn ohjaaja	Reino Virrankoski

ALKULAUSE

Diplomityön aihe tuli vastaan hieman sattumalta kesätöiden yhteydessä vuonna 2009. Runsaan puolen vuoden kypsyttelyn jälkeen aiheidea jalostui diplomityöprojektiksi.

Diplomityöprojekti eteni varsin perinteiseen tapaan alun ihmettelystä lopun kiireeseen. Ehkä sitä seuraavaa opinnäytetyötä kirjoittaessa osaa jakaa ajankäytön paremmin.

Projektin läpiviennin kannalta varsin tärkeiksi osoittautuivat diplomityön ohjaukseen osallistuneiden tahojen kommentit sekä Kimmo Svinhufvudin vuonna 2009 julkaistu Gradutakuu-kirja.

Kiitokset työn oikolukijalle, ohjaajille, ohjausryhmälle ja muille projektiin osallistuneille tahoille.

Vaasassa 29.6.2010
Jussi Itämäki

SISÄLLYSLUETTELO **sivu**

LYHENNELUETTELO

3DES	Triple Data Encryption Standard
AD	Active Directory
ADAM	Active Directory Application Mode
AD LDS	Active Directory Lightweight Directory Service
AES	Advanced Encryption Standard
AH	Authentication Header
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
CA	Certificate Authority
CBC	Cipher Block Chaining
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
ECB	Electronic Codebook
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAG	Intelligent Application Gateway
ICMP	Internet Control Messaging Protocol
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IIS	Internet Information Services

IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
ISA	Internet Security & Acceleration Server
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MAC	Message Authentication Code
MD5	Message-Digest 5
MIT	Massachusetts Institute of Technology
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NBA	Network Behavior Analysis
OSI	Open Systems Interconnection
PKI	Public Key Infrastructure
RDP	Remote Desktop Protocol
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SA	Security Association
SCP	Secure Copy
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SNA	Systems Network Architecture
SOAP	Simple Object Access Protocol
SRA	Secure Remote Access
SSH	Secure Shell

SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
Telnet	Telecommunication Network
TLS	Transport Layer Security
UAG	Unified Access Gateway
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VPN	Virtual Private Network
VSE	Virtual Support Engineer
WSS	Windows SharePoint Services
WWW	World Wide Web
XML	eXtensible Markup Language

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Jussi Itämäki
Erikoistyön nimi: Tietoturvalliset tietoliikenneyhteydet yritysympäristössä
Valvojan nimi: Matti Linna
Ohjaajan nimi: Reino Virrankoski
Tutkinto: Diplomi-insinööri
Yksikkö: Tieto- ja tietoliikennetekniikan yksikkö
Koulutusohjelma: Tietotekniikan koulutusohjelma
Suunta: Tietoliikennetekniikka
Opintojen aloitusvuosi: 2001
Erikoistyön valmistumisvuosi: 2010 **Sivumäärä:** 176

TIIVISTELMÄ

Diplomityössä käsitellään tietoliikenneverkkojen ja -yhteyksien tietoturvallisuutta yritysympäristössä. Aihealuetta tarkastellaan esimerkkiyrityksenä olevan ABB Oy:n näkökulmasta.

Tutkimuksen tavoitteena on luoda yleinen konsepti tietoturvallisten tietoliikenneyhteyksien luomiseen ABB Oy:n ja kolmansien osapuolien tietojärjestelmien välille. Konsepti kattaa liiketoimintayksiköiden merkittävimmät käyttötarpeet sekä noudattaa ABB:n yhtymänlaajuisia tietoturvavaatimuksia.

Tutkimuksessa käytettävä aineisto koostuu yhtymän tietoturvavaatimuksista, aihealueesta aiemmin tehdyistä selvityksistä ja tutkimuksista sekä yrityksessä tehtävästä tarvekartoituksesta. Tarvekartoitus toteutetaan haastattelututkimuksena ja sen tavoitteena on tunnistaa liiketoimintayksiköiden olemassa olevat käyttötarpeet.

Työn lopputuloksena laadittiin asetetut tavoitteet täyttänyt yleinen malli tietoliikenneyhteyksien muodostamiseen yhtiön ja kolmansien osapuolien välille. Luodun mallin ja siinä määriteltyjen palvelukonseptien avulla voidaan saavuttaa merkittäviä resurssisäästöjä ja parannuksia tietoliikenneverkon tietoturvaan.

AVAINSANAT: Tietoturva, tietoliikenneverkot, etäkäyttö, TCP/IP

UNIVERSITY OF VAASA
Faculty of Technology
Author: Jussi Itämäki
Topic of the Thesis: Secure Network Connections in Enterprises
Supervisor: Matti Linna
Instructor: Reino Virrankoski
Degree: Master of Science in Technology
Department: Department of Computer Science
Degree Programme: Degree Programme in Computer Science
Major of Subject: Telecommunications Engineering
Year of Entering the University: 2001
Year of Completing the Thesis: 2010 **Pages:** 176

ABSTRACT

This master's thesis deals with corporate telecommunication networks security and the topic is studied from an example of a company ABB Oy's point of view.

The objective of the research is to create a general model for creating secure telecommunication connections between ABB's and third party's information systems. The general model must cover most significant demands of business units and it must also fulfil ABB Group's security requirements.

The research material consists of the ABB Group's security requirements, the previously carried out studies and researches in the field as well as the needs assessment which is done in the company. Needs assessment is carried out by interviews whose objective is to identify the existing needs of the business units.

As a result, the defined general model fulfils the original objectives of research. The developed general model and included service concepts can be used to achieve significant resource savings and improvements to network security.

KEYWORDS: Security, networks, remote access, TCP/IP

1. JOHDANTO

Tietojärjestelmien merkitys yrityksille on erittäin suuri, koska käytännössä kaikki niiden toiminnot ovat riippuvaisia tietojärjestelmien avulla toteutetuista palveluista. Järjestelmiä käytetään tiedon tallentamiseen, käsittelyyn ja esittämiseen. Käyttötarkoitusten monimuotoisuudesta johtuen myös tietojärjestelmiä on useita eri tyyppejä ja niitä voidaan luokitella monella tapaa. Järjestelmät voidaan esimerkiksi jakaa hajautettuihin ja keskitettyihin tietojärjestelmiin. Yhteistä pääosalle tietojärjestelmistä on kuitenkin se, että niiden käyttöön tarvitaan tietoliikenneyhteyksiä.

Yritysten koko, rakenne, toimiala ja toimintakulttuuri asettavat tietojärjestelmille sekä niiden välisille tietoliikenneyhteyksille omia vaatimuksiaan. Tietoliikenneyhteyksiä voidaan tarvita esimerkiksi yrityksen eri toimipisteiden, alihankkijoiden ja tehtaiden tai asiakkaiden ja tuotetuen välille. Tietoliikenneyhteyksille asetetut vaatimukset liittyvät yleisesti yhteyksien luotettavuuteen, kustannuksiin, kapasiteettiin, vasteaikoihin sekä turvallisuuteen.

Diplomityössä esimerkkiyrityksenä olevan ABB Oy:n käytössä on huomattava määrä erityyppisiä tietojärjestelmiä. Tutkimuksen tavoitteena on määritellä ABB Oy:lle yleinen tietoturvallinen konsepti tietoliikenneyhteyksien muodostamiseen yhtiön ja kolmansien osapuolien tietojärjestelmien välille. Konseptin tulee kattaa liiketoimintayksiköiden merkittävimmät käyttötarpeet ja ABB:n yhtymänlaajuiset tietoturva- ja käytettävyysvaatimukset. Työn yhteydessä kolmansilla osapuolilla tarkoitetaan yhtiön asiakkaita, alihankkijoita ja kumppaneita.

Huolimatta siitä, että useat eri liiketoimintayksiköt ovat jo pitkään tarvinneet erityyppisiä etäyhteyksiä ja muita palveluita, joiden avulla voidaan muun muassa hallita asiakkaille myytyjä tuotteita tai tarjota alihankkijoille pääsy yhtiön sisäverkossa oleviin tiettyihin tietojärjestelmiin, ABB Oy:llä ei ole olemassa yleistä konseptia yhtiön ja kolmansien osapuolien välisten tietoliikenneyhteyksien muodostamiseen. Yleisen mallin puuttuminen on johtanut siihen, että eri yksiköt ovat luoneet omia yksittäisiä ratkaisuja olemassa olevien tarpeiden täyttämiseksi.

Ratkaisuja on luotu varsin tapauskohtaisesti ilman laajempaa suunnittelua. Seurauksena on muodostunut huomattava määrä erityyppisiä ratkaisuja, jotka pahimmassa tapauksessa ovat yhteensopimattomia jopa saman liiketoimintayksikön muiden olemassa olevien ratkaisujen kanssa. Ongelma korostuu entisestään, kun eri liiketoimintayksiköiden ratkaisuja vertaillaan keskenään.

Merkittävä osa tutkimuksen tavoitteiden saavuttamisessa ja yleisen mallin rakentamisessa on liiketoimintayksiköiden nykyisten ja tulevien tarpeiden selvittämisellä sekä analysoinnilla. Tarpeiden tunnistamisen lisäksi tarkastellaan yksiköiden nykyisin käyttämiä sekä vielä kehityksen alla olevia yhteysratkaisuja.

Liiketoimintayksiköiden nykyisiä ja tulevia käyttötarpeita sekä ratkaisuja selvitetään liiketoimintayksiköissä tehtävien haastattelujen avulla. Tarvekartoituksen pääpaino on niissä liiketoimintayksiköissä, jotka käyttävät nykytilanteessa eniten erityyppisiä etäyhteyksiä.

Haastattelujen avulla löydettyjä tarpeita analysoidaan ABB Oy:n tietohallinnon edustajista koostuvan ohjausryhmän sekä liiketoimintayksiköiden tietohallinto- ja palvelujohtajien kanssa. Analysoinnin tavoitteena on tunnistaa liiketoiminnan kannalta tärkeimmät tarpeet.

Työn lopputuloksena luodaan yleinen malli, jonka avulla liiketoimintayksiköiden olennaisimmat nykytarpeet voidaan toteuttaa. Mallissa määritellään miten tietoliikenneyhteydet muodostetaan kolmansien osapuolien ja ABB Oy:n tietoliikenneverkkojen välille sekä mitä palveluita yhteyksien yli voidaan käyttää.

Yleisen mallin rakentamisen kannalta on olennaista liiketoimintayksiköiden todellisten tarpeiden tunnistaminen sekä niiden onnistunut rajaaminen. Olemassa olevien tarpeiden suuri määrä tekee tehtävästä varsin haasteellisen. Epäonnistunut rajaus voi johtaa malliin, josta saatava liiketoimintahyöty on käytännössä mitätön. Konsepti otetaan liiketoimintayksiköissä täysimittaisesti käyttöön vain siinä tapauksessa, että yksiköt kokevat saavansa sen myötä merkittävää lisäarvoa.

Lopputuloksena saatua yleistä mallia tarkastellaan lopuksi erityisesti tietoturvanäkökulmasta. Tietoturvallisuuden lisäksi on arvioitava myös sen taloudellisuutta, tarkoituksenmukaisuutta sekä soveltuvuutta ja kehityspotentiaalia konseptin ulkopuolelle jääneiden yksittäisten tarpeiden suhteen. Yleistä mallia verrataan myös aiemmin käytössä olleisiin yksittäisiin ratkaisuihin.

2. TAVOITTEET JA YMPÄRISTÖ

Tutkimuksen tavoitteena määritellä yleinen tietoturvallinen malli tietoliikenneyhteyksien muodostamiseen ABB Oy:n ja kolmansien osapuolien välille. Mallissa määritellään käytettävän tietoliikenneverkon looginen rakenne, tietoliikenneyhteydet ja tarjottavat palvelut.

Diplomityö laaditaan ABB Oy:n tietohallintopalveluiden tilauksesta. Tutkimusympäristönä on yrityksen Suomessa toimivat liiketoimintayksiköt sekä tukipalvelut.

2.1. Yrityksen ja yksiköiden esittely

ABB Ltd on yksi maailman suurimpia teollisuuskonserneja ja se toimii nykyisin yli sadassa maassa. ABB on markkinajohtaja useilla sähkö- ja automaatiotekniikan osa-alueilla. Toimipaikkoja konsernilla oli vuonna 2009 87 maassa ja työntekijöitä yhteensä noin 117 000. Yhtiön pääkonttori on Zürichissä ja se on listattuna Zürichin (*SIX Swiss Exchange*), Tukholman (*OMX Stockholm*) ja New Yorkin (*New York Stock Exchange*) pörsseissä. (ABB 2010a.)

ABB Oy on konsernin Suomessa toimiva yksikkö, jolla on toimintaa yli 40 paikkakunnalla ja työntekijöitä yhteensä noin 6 000. ABB Oy kuuluu konsernin NEU (*Northern Europe*) -alueeseen. Suomen organisaatio on jaettu viiteen divisioonaan sekä tukitoimintoihin. Divisioonia ovat Sähkökäytöt ja kappaletavara-automaatio (*Discrete Automation and Motion*), Pienjännitetuotteet (*Low Voltage Products*), Prosessiautomaatio (*Process Automation*), Sähkövoimajärjestelmät (*Power Systems*) ja Sähkövoimatuotteet (*Power Products)*. (ABB 2010b.)

Sähkökäytöt ja kappaletavara-automaatio -divisioona koostuu Drives, MV Drives, Sähkökoneet (*Machines*), Motors ja Robotit (*Robotics*) -yksiköistä. Edellä mainituista yksiköistä Drives vastaa sähkökäyttöjen kehittämisestä ja valmistuksesta. MV Drives -yksikön vastuulla on sähkökäyttöprojektien markkinointi, suunnittelu ja toteuttaminen. Sähkökoneet-yksikkö vastaa suurjännitteisten vaihtovirtamoottorien ja -generaattorien suunnittelusta,

valmistuksesta ja myynnistä. Motors-yksikkö sen sijaan valmistaa ja myy pienjännitteisiä vaihtovirtamoottoreita ja -generaattoreita. Robotit-yksikön vastuulle kuuluu robottien suunnittelu ja valmistaminen. (ABB 2010b.)

Pienjännitetuotteet-divisioona koostuu Pienjännitekojeet (*Low Voltage Switches*), Pienjännitejärjestelmät (*Low Voltage Systems*) ja Asennustuotteet (*Wiring Accessories*) -yksiköistä. Yksiköiden vastuut jakautuvat siten, että Pienjännitekojeet-yksikkö kehittää, valmistaa ja markkinoi pienjännitekojeita, Pienjännitejärjestelmät-yksikkö kehittää, valmistaa ja myy pienjännitekojeistoja sekä -keskuksia ja Asennustuotteet-yksikkö keskittyy rakentamisen sähköistystarvikkeiden ja -kalusteiden kehittämiseen, valmistamiseen sekä markkinointiin. (ABB 2010b.)

Prosessiautomaatio-divisioona jakautuu Prosessiteollisuus (*Process Industry*), Marine ja Turboahtimet (*Turbocharging*) -yksiköihin. Prosessiteollisuus-yksikön vastuulle kuuluu sähkö- ja automaatiojärjestelmien sekä niihin liittyvien palveluiden kehittäminen ja markkinoiminen prosessiteollisuudelle. Marine- ja Turboahtimet-yksiköt vastaavat laivojen sähköistyksistä ja automaatiosta. (ABB 2010b.)

Sähkövoimajärjestelmät-divisioonaan kuuluu Sähkönsiirto- ja jakelujärjestelmät (*Substations*) sekä Voimantuotannon järjestelmät (*Power Generation*) -yksiköt. Ensin mainitun vastuulla on standardoitujen automaatioratkaisujen toimittaminen sähkönjakeluyhtiöille ja voimalaitosasiakkaille. Jälkimmäisen tehtävänä on sähkön siirto- ja jakelujärjestelmien suunnittelu, valmistaminen ja markkinointi. (ABB 2010b.)

Sähkövoimatuotteet-divisioona on jaettu kolmeen yksikköön. Sähkönjakeluautomaatio (*Distribution Automation*) -yksikön tehtävänä on sähköverkon suojareleiden, hälytyslaitteiden, paikallisautomaatio- ja kaukokäyttöjärjestelmien kehittäminen ja valmistaminen. Keskijännitekojeet ja -kojeistot (*Medium Voltage Apparatus and Switchgear*) -yksikkö valmistaa kojeistoja ja kytkimiä. Muuntajat (*Transformers*) -yksikkö kehittää ja valmistaa erikoismuuntajia, reaktoreita sekä suurmuuntajia sähköntuotantoon ja siirtoon. (ABB 2010b.)

Divisiooniin kuulumattomia yksiköitä on Suomessa Service, Product Support, Kotimaan myynti (*Domestic Sales*) ja Toiminnot ja palvelut (*Functions and Services*) -yksiköt. Service-yksikön tehtävänä on tuotantotehokkuutta parantavien ratkaisujen ja palveluiden kehittäminen ja toimittaminen sopimuskumppaneille. Product Support -yksikkö tarjoaa tuotteen elinkaaripalveluita. Kotimaan myynti vastaa nimensä mukaisesti kotimaan markkinoiden tuotemyynnistä. Toiminnot ja palvelut -yksikön tehtävänä on tukipalveluiden tarjoaminen liiketoimintayksiköille. (ABB 2010b.)

2.2. Ratkaisumallia ohjaavat vaatimukset

Yhtiön ja kolmansien osapuolien välisiä tietoliikenneyhteyksiä määritellään yrityksen sisäiseen käyttöön julkaistussa Dillardin, Stephansonin, Bouleyn & Wiesendangerin (2003) laatimassa External Connectivity Baseline Policies -dokumentissa.

Dokumentissa määritellään yleisellä tasolla tietoverkkojen tietoturvakonsepti, sallitut yhteydet ja niiden muodostamistavat sekä ulkoverkkoon tarjottavien palveluiden toteuttaminen. (Dillard ym. 2003.)

Ratkaisumallin määrittelyä ohjaa lisäksi yrityksen standardoimat järjestelmäratkaisut sekä käytössä oleva tietojärjestelmäarkkitehtuuri.

2.2.1. Tietoturvakonsepti

Dokumentissa määritellään, että ulkoiset yhteydet tulee erottaa palomuurilla yhtiön sisäverkosta yhteyden muodostustavasta riippumatta. Palomuureissa käytettävien palomuurisääntöjen tulee noudattaa yhtiön tietoturvavaatimuksia ja -käytäntöjä. Palomuureja käytetään lisäksi yhtiön verkon segmentointiin eri verkkoalueisiin. Tavoitteena on rajoittaa tietoturvariskien laajuutta eristämällä mahdollinen hyökkääjä vain yhteen verkkoalueeseen. Verkkoalueita, joihin voidaan muodostaa yhteys sekä yhtiön sisäverkosta että ulkoverkosta kutsutaan Demilitarized Zone (DMZ) -alueiksi. (Dillard ym. 2003.)

Verkon segmentointia käsitellään kattavammin kappaleessa 6.1.

External Connectivity Baseline Policies (Dillard ym. 2003) -dokumentissa määritellään, että DMZ-alueella sijaitsevan yhtiön omistaman tai hallinnoiman verkkosolmun tulee läpäistä yhtiön tiukennettu tietoturvatestaus. Verkkosolmu tulee määritellä siten, että vain tietyillä käyttäjillä on pääsy kyseiseen solmuun ja sen tulee myös ylläpitää lokia käyttöyrityksistä sekä sitä vastaan kohdennetuista hyökkäyksistä. Verkkosolmussa tulee lisäksi käyttää vahvoja ja usein vaihtuvia salasanoja, sen käyttöjärjestelmästä tulee karsia tarpeettomat palvelut, etähallinta tulee sallia vain tietyistä Internet Protocol (IP) -osoitteista ja verkkoalueista, verkkosolmun käyttämien tietoliikenneyhteyksien tulee olla suojattuja ja solmun tarjoamien palveluiden käyttäminen tulee sallia vain erikseen määritellylle asiakasjoukolle. (Dillard ym. 2003.)

DMZ-alueella ja muissa kriittisissä verkkosegmenteissä tulee käyttää Intrusion Detection System (IDS) -sovelluksia, jotka kykenevät tunnistamaan sovelluksissa tapahtuneita muutoksia ja tarkkailemaan epänormaalia verkkoliikennettä. Teknologian avulla kerättyä tietoa pyritään hyödyntämään hyökkäysten tunnistamiseen, todisteiden keräämiseen ja hyökkäysten selvittämiseen. Ulkoverkkoon näkyvien verkkosolmujen lisäsuojana tulee käyttää erikoistuneita Intrusion Prevention System (IPS) -ohjelmistoja. (Dillard ym. 2003.)

IPS-ohjelmistot täydentävät edellä mainittuja verkkoliikenteen tarkkailuun tarkoitettuja sovelluksia sillä, että ne kykenevät hyökkäyksen tunnistamisen lisäksi toimimaan aktiivisesti niitä vastaan (Scarfone & Mell 2007: 15). IDS- ja IPS-sovelluksia käsitellään laajemmin kappaleessa 6.3.

Myös virustorjuntaan tulee kiinnittää huomiota. Tietoliikenneyhteyksiä voidaan muodostaa vain niiden kolmansien osapuolien kanssa, jotka voivat osoittaa käyttävänsä asianmukaista virustorjuntaa. (Dillard ym. 2003.)

2.2.2. Tietoliikenneyhteydet

External Connectivity Baseline Policies (Dillard ym. 2003) -dokumentin mukaan yhteydet yrityksen ja kolmansien osapuolien tietojärjestelmien välille voidaan muodostaa Internet-palveluntarjoajan tarjoaman yleisen tietoverkon yli tai vaihtoehtoisesti voidaan käyttää yksityisiä linjoja ja verkkoja. Yleisen

tietoverkon tapauksessa käytettävää yhteystekniikkaa ei ole tarkemmin määritelty, vaan se voidaan valita tarpeen mukaan. (Dillard ym. 2003.)

Yhtiön tietoturvaohjeistuksen mukaan yleisen tietoverkon yli ei saa missään tapauksessa siirtää luottamuksellista tietoa suojaamattoman tietoliikenneyhteyden välityksellä. Sen sijaan yhteyden osapuolten välille tulee muodostaa erillinen tunneloitu yhteys. Tunneloinnissa osapuolten välille muodostetaan erillinen suojattu looginen tietoliikenneyhteys suojaamattoman tietoliikenneverkon yli (VPN Consortium 2008). Suojatun yhteyden avulla voidaan pienentää yhteyden kaappaamisen ja salakuuntelun riskiä. External Connectivity Baseline Policies -dokumentissa suositellaan käyttämään tunnelointiin Virtual Private Network (VPN) -tekniikkaa. Yhteyden salaukseen tulisi käyttää joka tilanteessa mahdollisimman vahvaa salausta. Dokumentissa suositellaan käyttämään 168-bittistä Triple Data Encryption Standard (3DES) -salausta. (Dillard ym. 2003.)

Yhtiön omat työntekijät ja valitut kolmannet osapuolet voivat muodostaa yhteyden yrityksen sisäverkkoon käyttäen ABB:n Secure Remote Access (SRA) -palvelua. Palvelussa tietoliikenneyhteydet osapuolten välille muodostetaan IPsec VPN -tekniikalla. Yhteys voidaan muodostaa ainoastaan ABB:n omistamilta tai valtuuttamilta työasemilta. Mikäli yhteyden toinen osapuoli on yhtiön ulkopuolinen toimija, tarjolla tulee olla vain tietyt palvelut. (Dillard ym. 2003; Vitorino 2009.)

VPN-yhteyksiä voidaan soveltaa myös ABB:n eri toimipisteiden välisten yhteyksien muodostamiseen. Toimipisteiden tietoverkot yhdistetään toisiinsa julkisen tietoverkon yli käyttäen VPN-tekniikkaa. External Connectivity Baseline Policies -dokumentissa VPN-yhteyksiä suositellaan käyttämään myös tilanteissa, joissa ABB:n sisäverkosta tulee muodostaa yhteys kolmannen osapuolen tietoliikenneverkkoon. (Dillard ym. 2003.)

Mikäli tietoliikenneyhteys muodostetaan yksityisen yhteyden välityksellä, External Connectivity Baseline Policies -dokumentissa korostetaan ABB:n vastuuta varmistaa, että myös toinen osapuoli suhtautuu tietoturvaan vakavasti ja täyttää yleiset vaatimukset. Tietoturvavaatimuksiin kuuluu riittävä virustorjunta, kunnolliset palomuurikäytännöt ja säännölliset

tietoturvapäivitykset. Yksityiset yhteydet tulee muodostaa siten, että ne päättyvät DMZ-alueelle ja niiden kautta pääsee käsiksi vain tiettyihin palveluihin ja resursseihin. Kolmannen osapuolen verkko-osoitteita ei saa reitittää ABB:n verkon kautta. Sama pätee myös toisin päin, liikennettä ABB:n verkko-osoitteisiin ei saa reitittää kolmannen osapuolen verkon kautta. Mikäli jostain syystä edellä mainittuun reititykseen on tarvetta, tulee käyttää Network Address Translation (NAT) -tekniikkaa osoitteen muuntamiseksi. (Dillard ym. 2003.)

2.2.3. Ulkoverkkoon tarjottavat palvelut

External Connectivity Baseline Policies -dokumentin mukaan ulkoverkkoon palveluita tarjoavat palvelimet tulee sijoittaa DMZ-alueelle ja suojata palomuurilla. Palvelimien tietoturvaan tulee kiinnittää erityistä huomiota. (Dillard ym. 2003.)

Palvelimien tietoturva-asetukset määritellään mahdollisimman vahvoiksi ja tietoturvapäivitykset otetaan käyttöön heti julkaisun jälkeen. Palvelimet ylläpitävät kattavia lokitietoja ja lisäksi niissä suoritettavien ohjelmistojen tulee läpäistä tietoturvakatselmointi. Suoritettavien ohjelmistojen joukossa on IPS-ohjelmisto ja sekä tietoliikenneyhteyksissä että tiedon tallennuksessa käytetään salausta. Palvelimien ja suoritettavien ohjelmistojen toimintaa katselmoidaan säännöllisesti. Lisäksi palvelimista on erilliset kopiot testauskäyttöön. Testiympäristön palvelimet eristetään tuotantokäytössä olevista palvelimista palomuurilla. (Dillard ym. 2003.)

2.3. Tutkimuksen tarve

Liiketoimintayksiköiden tarpeista huolimatta, ABB:llä ei ole yleistä yhtymän, alueen tai maatason konseptia yhtiön ja kolmansien osapuolien välisten tietoliikenneyhteyksien muodostamiseen.

Liiketoimintayksiköiden käyttötarpeet liittyvät erityyppisiin etäyhteyksiin ja muihin palveluihin, joiden avulla voidaan muun muassa hallita asiakkaille myytyjä tuotteita tai tarjota alihankkijoille pääsy yhtiön sisäverkossa oleviin

tietojärjestelmiin. Yleisen mallin puuttuminen on johtanut siihen, että eri yksiköt ovat luoneet omia yksittäisiä ratkaisuja tunnistettujen käyttötarpeiden täyttämiseksi.

Ratkaisuja on luotu varsin tapauskohtaisesti ilman laajempaa suunnittelua sekä toteutuksen asianmukaista katselmointia ja hyväksyttämistä. Seurauksena on muodostunut huomattava määrä erityyppisiä käytäntöjä, jotka pahimmassa tapauksessa ovat yhteensopimattomia jopa saman liiketoimintayksikön muiden ratkaisujen kanssa. Ongelma korostuu entisestään, kun eri liiketoimintayksiköiden olemassa olevia ratkaisuja vertaillaan keskenään.

Suunnittelemattomuus on tarkoittanut myös jossain tapauksissa puutteellista testausta ja dokumentointia, mikä tekee kyseisten palveluiden ylläpidosta erittäin hankalaa.

Useiden rinnakkaisten käytäntöjen ja palveluiden olemassa olo monimutkaistaa merkittävästi tietoverkkojen ja niiden tarjoamien palveluiden ylläpitoa sekä kehittämistä. Lisäongelmia tuottaa jo edellä mainittu ratkaisujen puutteellinen tai vanhentunut dokumentaatio. Tietoverkosta poistetun näennäisesti tarpeettoman palvelun todellinen tärkeys voikin selvitä pahimmillaan vasta vuosien kuluttua.

Rinnakkaiset ratkaisut tarjoavat myös laajemman hyökkäyspinta-alan ja siten ne lisäävät huomattavasti potentiaalisia tietoturvauhkia. Ratkaisujen suuri määrä hidastaa myös mahdollisten tietoturvapäivitysten käyttöönottoa ja testausta sekä hankaloittaa merkittävästi verkonvalvontaa.

Tapauskohtaisten ratkaisujen kehittäminen johtaa myös päällekkäisen työn tekemiseen yhtiössä, mikäli jo olemassa olevia ratkaisuja ei hyödynnetä täysipainoisesti. Iso osa kehittämispanoksesta menee tällaisissa tapauksissa usein jo aiemmin ratkaistujen ongelmien ja virheiden selvittämiseen.

Rinnakkaisten ratkaisujen olemassaolo lisää kustannuksia monella tasolla. Edellä mainituissa ongelmissa merkittävimmät kustannukset aiheutuvat henkilöstö-, laite- ja sovellusresurssien sitomisesta.

Yleisen konseptin puuttuminen aiheuttaa ongelmia myös tuotteiden ja palveluiden myynnissä. Nykyisellään asiakkaalle ei voida esimerkiksi osoittaa suoraan tapaa, miten yhtiö hallinnoi myymiään tuotteita mahdollisissa vikatilanteissa tai miten asiakas voi hakea ohjelmistopäivityksiä hankkimalleen laitteelle.

Tarve yhtiön ja kolmansien osapuolien yhteyksille tulee todennäköisesti lisääntymään tulevaisuudessa merkittävästi. Samaan aikaan yhteystarpeet muuttuvat jatkuvasti maailmanlaajuisemmiksi. Muutokseen voidaan vastata tehokkaimmin mahdollisimman yhtenäisillä käytännöillä ja ratkaisuilla.

2.4. Tutkimuksen tavoitteet

Tutkimuksen tavoitteena on muodostaa ABB Oy:lle yleinen tietoturvallinen malli tietoliikenneyhteyksien muodostamiseen yrityksen ja kolmansien osapuolien tietojärjestelmien välille. Määritellyn mallin ensisijaisena tavoitteena on yrityksen liiketoimintayksiköiden olennaisten liiketoimintatarpeiden toteuttaminen yhtymän tietoturvapolitiikkaa noudattaen.

Toissijaisina tavoitteina ovat yhteensopivuus olemassa olevien palveluiden ja järjestelmien kanssa, yksittäisten ratkaisujen korvaaminen yleisillä vakioiduilla ratkaisuilla, mallin ja ratkaisujen yksinkertaisuus sekä läpinäkyvyys. Ratkaisujen tulee olla luotettavia ja käytettävyydeltään riittävän hyviä.

Mallin tulee myös soveltua mahdollisimman hyvin yksiköiden jo olemassa olevien että lähitulevaisuuden käyttötarpeiden toteuttamiseen.

Yleinen malli määrittelee yhteyksien muodostamisen sekä ulkoverkosta ABB:n sisäverkkoon että ABB:n sisäverkosta ulkoverkkoon. Mallissa otetaan kantaa käytettäviin tietoliikenneyhteyksiin, tarjottaviin palveluihin, tietoliikenneverkon loogiseen rakenteeseen, käyttäjien ja laitteiden tunnistamiseen, yhteyksien suojausprotokolliin ja tarvittaviin palomuuriavauksiin sekä palveluiden käytön valvontaan.

Yleiselle mallille määriteltyjen tavoitteiden täyttäminen on tärkeää, koska niiden myötä voidaan nopeuttaa ja yksinkertaistaa tietoliikenneyhteyksien luomista yhtiön ja kolmansien osapuolien välille, parantaa kokonaistietoturvaa, vähentää rinnakkaisten yhteysratkaisujen lukumäärää, helpottaa olemassa olevien yhteyksien ylläpitoa sekä tarjota kolmansille osapuolille läpinäkyviä ja joustavia yhteysratkaisuja.

Toiminnan tehostumisen myötä yritys voi käyttää vapautuvat resurssit ydintoimintaansa ja ulkopuoliset tahot kykenevät osallistumaan kattavammin ja nopeammin yrityksen arvoketjuun. Toiminnan tehostuminen mahdollistaa myös liiketoiminnan kasvun sekä tuottavuuden parantumisen ja siten liikevaihdon ja liikevoiton lisääntymisen. (Porter 1988; Haverila, Uusi-Rauva, Kouri & Miettinen 2009: 357–358.)

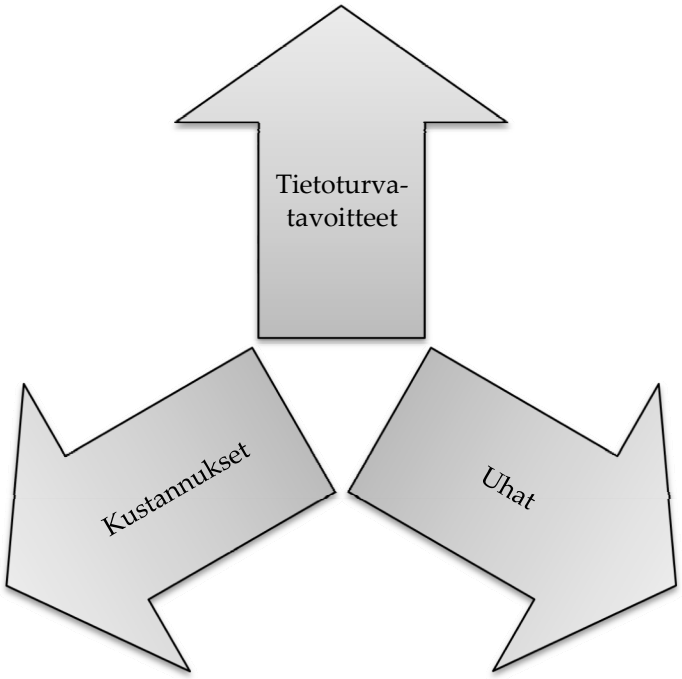
3. TIETOTURVA

Sähköisen viestinnän tietosuojalain (17.3.2006/198) mukaan tietoturvalla tarkoitetaan ”hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä”.

Kerttula (1998: 84) mainitsee tietoturvallisuuteen kuuluvan ”koko se tietojen synnyttämiseen, käyttämiseen, säilyttämiseen ja hävittämiseen liittyvien laitteiden, ohjelmistojen ja menetelmien sekä henkilöstön turvakysymysten joukko, mitä tuon turvallisuuden tavoitetilan saavuttamiseen vaaditaan”.

Tietoturvan yhteydessä käytetään kolmea peruskäsitettä, joita ovat haavoittuvuus, uhka ja kontrolli. Tietoturvahaavoittuvuudella tarkoitetaan tietojärjestelmässä olevaa heikkoutta, jonka kautta tietojärjestelmälle voi aiheutua vahinkoa. Tietoturvauhka on sitä vastoin tilanne tai tapahtumasarja, joka voi johtaa haavoittuvuuden toteutumiseen. Tietoturvauhkia ovat esimerkiksi tietojärjestelmän haavoittuvuuksiin kohdistuvat hyökkäykset. Tietoturvakontrollit ovat toimenpiteitä, laitteita, käytäntöjä tai tekniikoita, joiden avulla tietoturvahaavoittuvuuksia voidaan poistaa tai vähentää. (Pfleeger & Pfleeger 2006.)

Tietojärjestelmän tietoturvallisuus on aina käytännössä kompromissi tietoturvatavoitteiden, tietoturvauhkien ja kustannusten välillä (kuva 1). (Kerttula 1998: 206.)



Kuva 1. Käytännön tietoturvallisuuteen vaikuttavat tekijät (Kerttula 1998: 207).

3.1. Tietoturvan osa-alueet

Tietojärjestelmien tietoturvallisuus on monimutkainen ja moniulotteinen kokonaisuus, jonka systemaattinen tarkastelu ja ylläpitäminen vaativat kokonaisuuden jakamista mahdollisimman yksinkertaisiin itsenäisiin osa-alueisiin (Kerttula 1998: 85).

Valtionvarainministeriö (1999) jakaa tietoturvallisuuden seuraaviin osa-alueisiin:

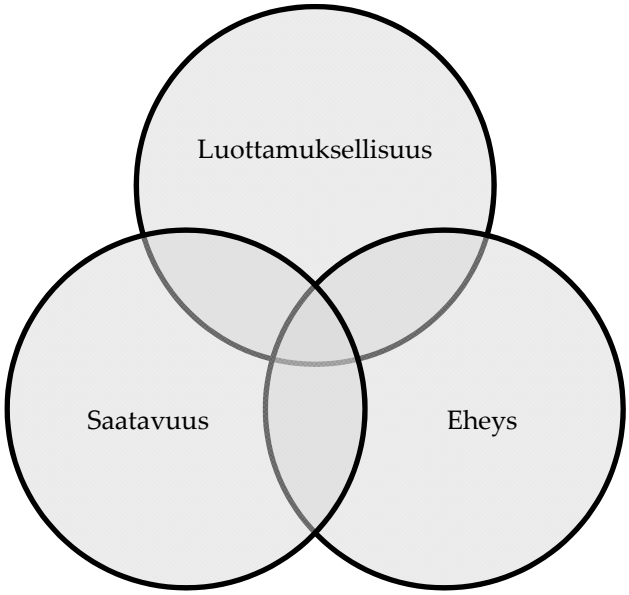
- Hallinnollinen tietoturvallisuus
- Henkilöstöturvallisuus
- Fyysinen turvallisuus

- Tietoliikenneturvallisuus
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Käyttöturvallisuus

Tässä työssä keskitytään tietoliikenteen turvallisuuteen.

3.2. Tietoturvavaatimukset

Tietoturvaan liittyy olennaisesti vaatimus tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta. Lisäksi usein korostetaan vielä vaatimusta osapuolten todentamisesta ja tapahtumien kiistämättömyydestä (Stallings 2009: 703; Kerttula 1998: 84; Valtionvarainministeriö 1999; Pfleeger ym. 2006).



Kuva 2. Tietoturvan perusvaatimusten välinen riippuvuus (Pfleeger ym. 2006).

Tietoturvan perusvaatimusten välinen riippuvuus on esitetty kuvassa 2. Vaatimukset ovat tasapainossa alueella, jossa kaikki kolme ympyrää leikkaavat toisensa.

Vaatimus luottamuksellisuudesta täyttyy, kun tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen tahojen käytettävissä. Eheydellä tarkoitetaan, että tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa ulkopuolisten toimien seurauksena. Saatavuudella vaaditaan tiedon ja järjestelmien olevan siihen oikeutettujen tahojen käytettävissä määritellyssä vasteajassa. Todentaminen tarkoittaa viestinnän osapuolten luotettavaa tunnistamista. Todentamisesta käytetään myös nimitystä autentikointi. Tapahtuman kiistämättömyys vaatii, että tapahtuma voidaan todistaa jälkeenpäin ja sillä on tällöin juridinen sitovuus, jolloin toinen osapuoli ei voi kiistää toimintaansa jälkeenpäin. (Stallings 2009: 703; Kerttula 1998: 84, 93–97; Valtionvarainministeriö 1999; Pfleeger ym. 2006.)

Edellä mainittuja vaatimuksia käsitellään tarkemmin kappaleessa 3.3.5.

3.3. Peruskomponentit

Kerttula (1998: 86) jakaa tietoturvallisuuden viiteen hierarkkiseen peruskomponenttiin, joita ovat hyökkäykset, kryptografiset primitiivit, tietoturvaprotokollat ja -mekanismit, tietoturvafunktiot sekä -palvelut.

3.3.1. Hyökkäykset

Shireyn (2000: 12) mukaan hyökkäyksellä tarkoitetaan tietojärjestelmien yhteydessä tahallista tekoa, joka on suunnattu järjestelmää vastaan ja sen tarkoituksena on esimerkiksi ohittaa järjestelmän suojaukset. Yleisesti hyökkäykset kohdistuvat johonkin tietojärjestelmän tietoturvapalveluun ja ne on suunnattu tiedon salausta tai tiettyä tietoturvaprotokollaa vastaan. Hyökkäyksien taustalla olevat syyt ja tavoitteet ovat usein varsin monimuotoisia. Yleisesti voidaan sanoa, että suojatulla tiedolla, jolla on

strategista arvoa omistajalle, on strategista arvoa myös hyökkääjälle. (Kerttula 1998: 87; Pfleeger ym. 2006.)

Pfleeger ym. (2006) mainitsee kolme hyökkääjältä vaadittavaa ominaisuutta. Hyökkääjällä tulee olla hyökkäykseen vaadittavat taidot, tiedot ja työkalut, riittävästi aikaa ja pääsy tietojärjestelmään sekä jokin syy hyökkäykseen. Vaadittavat ominaisuudet ovat siis menetelmä, mahdollisuus ja motiivi. (Pfleeger ym. 2006.)

Kerttula (1998: 89) ja Pfleeger & Pfleeger (2006) jakavat tietoturvahyökkäykset neljään perustyyppiin, joita ovat keskeytys, sieppaaminen, muuntaminen ja väärentäminen. Keskeytyshyökkäys kohdistuu tietojärjestelmän resursseja vastaan ja sen tavoitteena on estää tietyn tai tiettyjen resurssien käyttäminen ja siten saattaa tieto saavuttamattomiin. Sieppauksessa on kyse tietojärjestelmään tunkeutumisesta ja informaation varastamisesta. Sieppaushyökkäys loukkaa tiedon luottamuksellisuutta. Muuntamishyökkäyksessä hyökkääjän tavoitteena on muokata tietojärjestelmässä välitettävää informaatiota ja siten rikkoa tiedon eheyttä. Väärentämisessä hyökkääjä sekä tunkeutuu kohdetietojärjestelmään että muuttaa järjestelmän sisältämään informaatiota. Hyökkäys loukkaa tiedon luottamuksellisuutta ja eheyttä. (Kerttula 1998: 89–90; Pfleeger ym. 2006.)

Hyökkäykset jaetaan edellä mainitun jaottelun lisäksi niiden luonteen perusteella passiivisiin ja aktiivisiin hyökkäyksiin. Aktiivisella hyökkäyksellä pyritään muuttamaan ja häiritsemään kohdejärjestelmän toimintaa. Passiivisessa hyökkäyksessä sitä vastoin pyritään vain vakoilemaan kohdejärjestelmää sen toimintaan varsinaisesti puuttumatta. (Shirey 2000: 12; Stallings 2009: 703; Kerttula 1998: 90.)

Aktiiviset hyökkäykset voidaan jakaa neljään perustyyppiin hyökkäystavan perusteella. Hyökkääjä pyrkii vaikuttamaan kohdejärjestelmään esiintymällä jonain toisena osapuolena, toistamalla aiemmin kaapattua dataa, muokkaamalla järjestelmän lähettämiä viestejä tai ylikuormittamalla tiettyjä palveluita. Aktiivisten hyökkäysten luonteesta johtuen ne ovat helposti havaittavissa. Hyökkäyksien estäminen on sitä vastoin varsin hankalaa, ja yleisesti tyydytäänkin vain niiden tunnistamiseen ja vahingoista palautumiseen. (Stallings 2009: 704–705; Kerttula 1998: 90.)

Passiivisessa hyökkäystavassa hyökkääjä tavallisesti pyrkii joko analysoimaan tai kaappaamaan kohdejärjestelmän tietoliikennettä. Tietoliikenteen analysoinnissa on ajatuksena selvittää ja seurata vain hyökkääjän kannalta olennaisia yksityiskohtia, kun taas kaappaamisessa on kyse kaiken informaation läpikäynnistä. Passiivisia hyökkäyksiä on useissa tapauksissa hyvin hankala havaita. Sen sijaan estäminen tai ainakin vaikeuttaminen on huomattavasti helpompaa. Passiivisia hyökkäyksiä vastaan voidaan suojautua varsin tehokkaasti erilaisten salausmenetelmien avulla. (Stallings 2009: 704; Kerttula 1998: 90.)

Hyökkäykset voivat kohdistua suoraan salausjärjestelmää tai tietoturvaprotokollia vastaan. Ensin mainitut hyökkäykset perustuvat salauksen purkamiseen systemaattisesti vaihtoehtoja läpikäymällä. Lopputuloksena pyritään selvittämään joko pelkästään alkuperäinen viesti tai vaihtoehtoisesti käytössä oleva salausavain. Tietoturvaprotokollia vastaan tehtävissä hyökkäyksissä hyökkääjä pyrkii selvittämään miten tietojärjestelmässä käytetään kryptografisia primitiivejä. (Kerttula 1998: 90–91.)

Tietoturvahyökkäykset alkavat yleisesti kohteen tarkkailulla ja tiedustelulla. Hyökkääjän tavoitteena on kerätä mahdollisimman paljon tietoa kohteesta ja siten tunnistaa mahdollisia haavoittuvuuksia. Seuraavassa vaiheessa hyökkääjä valitsee haavoittuvuudet, joita vastaan varsinainen hyökkäys kohdistetaan ja laatii hyökkäyssuunnitelman. (Pfleeger ym. 2006.)

Tiedon keräämiseen on olemassa useita toisiaan täydentäviä menetelmiä, joista tavallisimmat ovat porttiskannaus (*Port Scanning*), sosiaalinen manipulointi (*Social Engineering*), tiedustelu (*Intelligence*) sekä käyttöjärjestelmän ja ohjelmistojen tunnistetietojen selvittäminen (*Operating System and Application Fingerprinting*). (Pfleeger ym. 2006.)

Lisäinformaatiota kohteesta saadaan myös siihen liittyvästä julkisesta dokumentaatiosta (Pfleeger ym. 2006.)

Kun hyökkääjä on saanut kerättyä kohteesta riittävästi informaatiota ja suunnitellut hyökkäyksen, aloitetaan varsinainen hyökkäys. Hyökkäykset kohdistetaan yleisesti joko kohdejärjestelmän ohjelmistojen sisältämiä

tietoturvahaavoittuvuuksia, autentikointipalvelua, tiedon luottamuksellisuutta, tiedon eheyttä tai tiedon saatavuutta vastaan. (Pfleeger ym. 2006.)

3.3.2. Kryptografiset primitiivit

Kryptografiset primitiivit ovat matemaattisia menetelmiä informaation salaamiseen ja muuntamiseen. Kryptografisia primitiivejä ovat kryptografiset algoritmit ja muunnokset. (Kerttula 1998: 91; Pfleeger ym. 2006.)

Kryptografiset algoritmit ja muunnokset ovat ennalta sovittuja, usein erittäin monimutkaisia, epälineaarisia ja yksisuuntaisia matemaattisia tai algoritmien ohjaamia operaatioita, joiden avulla salataan tietojärjestelmässä välitettäviä sanomia. Kryptografisten algoritmien ja muunnosten vahvuuden määrittämiseen on luotu useita erilaisia malleja. (Kerttula 1998: 70–71; Pfleeger ym. 2006.)

Primitiiveihin kuuluvat muun muassa tiedon salaus- ja allekirjoitusmenetelmät sekä hash-funktiot. Kryptografiset menetelmät jaetaan yleisesti salaisen ja julkisen avaimen menetelmiin. (Kerttula 1998: 23; Pfleeger ym. 2006; Stallings 2003: 20; Stallings, Brown, Bauer & Howard 2008: 42.)

Kryptografisia algoritmeja ja muunnoksia käsitellään kattavammin luvussa neljä.

3.3.3. Tietoturvaprotokollat ja -mekanismit

Tietoturvaprotokollat ja -mekanismit ovat joukko ennalta määriteltyjä toimenpiteitä, joiden tehtävänä on hyökkäysten tunnistaminen, estäminen tai vaikutusten minimoiminen (Kerttula 1998: 86, 91).

Tietoturvaprotokollien avulla voidaan siirtää informaatiota viestinnän osapuolten välillä tietoturvallisesti. Tietoturvaprotokollat, joista käytetään myös nimitystä kryptografiset protokollat, rakentuvat kryptografisista primitiiveistä. Protokollia käytetään muun muassa salausavainten jakamiseen ja hallintaan, pääsynhallintaan sekä viestinnän osapuolten tunnistamiseen. (Kerttula 1998: 92, 145–146.)

Tietoturvamekanismi koostuu yhdestä tai useammasta tietoturvaprotokollasta, kryptografisesta algoritmista tai muunnoksesta sekä ei-kryptografisista tekniikoista. Tietoturvamekanismista käytetään myös nimitystä kryptomekanismi. (Kerttula 1998: 92.)

Tietoverkkojen tietoturvamekanismit ovat usein erittäin monimutkaisia johtuen verkkoihin kohdistuvista lukuisista vaatimuksista. Lisäksi mekanismien rakenteessa on varauduttava odottamattomiin vikatilanteisiin ja hyökkäysmenetelmiin. (Kerttula 1998: 23–24.)

Mahdollisten tietoturvauhkien monimuotoisuus hankaloittaa tietoturvamekanismien kehittämistä merkittävästi. Mahdollisten ongelmien määrän kasvaessa kokonaisuuden hahmottaminen vaikeutuu, ja kehittäjän on vaikea arvioida yksittäisten tietoturvaratkaisujen vaikutusta kokonaisuuteen. Mekanismien suunnittelun jälkeen on vielä päätettävä, missä niitä loogisesti ja fyysisesti tietoverkossa hyödynnetään. Tietoturvamekanismien kehitystä ohjaavat myös käytettävissä olevat tietoturva- ja verkkoprotokollat. Lisäksi on huomioitava mekanismissa mahdollisesti käytettävän salaisen informaation hallinnointi ja suojaaminen. (Kerttula 1998: 24–25.)

3.3.4. Tietoturvafunktiot

Tietoturvaprotokollat ja -mekanismit muodostavat yhdessä kryptografisten primitiivien kanssa kokonaisuuksia, joita kutsutaan tietoturvafunktioiksi. Tietoturvafunktio on itsenäinen toiminnallinen kokonaisuus, jolla ratkaistaan jokin tietty tietoturvatavoite. (Kerttula 1998: 86, 92.)

Simmonsin (1992: 5) mukaan tietoturvafunktioita ovat muun muassa tunnistaminen, allekirjoittaminen, kuittaus, autentikointi, äänestäminen ja sertifikaatin todentaminen.

3.3.5. Tietoturvapalvelut

Tietoturvapalvelut koostuvat yhdestä tai useammasta tietoturvafunktiosta ja ne näkyvät käyttäjille konkreettisina tietoturvatavoitteina. Palvelut voidaan jakaa neljään geneeriseen tietoturvapalveluun, joita ovat luottamuksellisuus

(*Confidentiality*), eheys (*Integrity*), kiistämättömyys (*Non-repudiation*) ja oikeellisuus (*Authentication*). Tietoturvan perustavoitteisiin luetaan lisäksi yleisesti pääsynvalvonta (*Access Control*) ja saatavuus (*Availability*), vaikka ne ovatkin johdettavissa edellä mainituista neljästä geneerisestä perustavoitteesta. (Kerttula 1998: 86, 93–95.)

Tietojärjestelmässä oleva tai sinne siirretty tieto on luottamuksellista, kun se on vain sen käyttöön oikeutettujen tahojen saatavilla. Luottamuksellisuus vaatii tiedon ja tietoliikenteen suojaamista sivullisilta ja täten se suojaa passiivisilta hyökkäyksiltä. (Kerttula 1998: 93–95; Valtionvarainministeriö 1999; Stallings 2007: 703; Pfleeger 2006.)

Tiedon ja tietojärjestelmän eheys vaatii, että tieto ja tietojärjestelmä ovat luotettavia, oikeita ja ajantasaisia. Vaatimuksena on lisäksi, että niihin voivat tehdä muutoksia ainoastaan muutoksiin oikeutetut tahot. Myöskään mahdolliset laite- ja ohjelmistoviat tai luonnontapahtumat eivät saa aiheuttaa muutoksia tietoihin. Tietojen ja järjestelmien eheyttä vastaan voidaan hyökätä aiemmin mainituilla aktiivisilla hyökkäyksillä. (Kerttula 1998: 93–96; Valtionvarainministeriö 1999; Stallings 2007: 703; Pfleeger 2006.)

Tiedon ja tietojärjestelmän oikeellisuuden varmistamiseen liittyy sekä tiedon että tietoa käsittelevän olion autentikointi. Autentikoinnissa on kyse alkuperäisen tiedon, henkilön tai olion tunnistamisesta ja identiteetin todistamisesta. Viestinnän osapuolten tulisikin autentikoida sekä toisensa että vastaanottamansa informaation. Autentikoinnin avulla voidaan suojautua ennen kaikkea useilta aktiivisilta hyökkäystavoilta. (Kerttula 1998: 93–96; Valtionvarainministeriö 1999; Stallings 2007: 703.)

Tieto on kiistämätöntä, kun kaikki tietoa koskevat tapahtumat ja niissä mukana olleet osapuolet voidaan tarkastaa jälkeenpäin. Kiistämättömyys takaa, että viestinnän osapuolet voivat varmistua tiedon siirtyneen toisilleen. Tiedonsiirron kiistämättömyys on yksi suojautumiskeino tiettyjä aktiivisia hyökkäyksiä vastaan. (Kerttula 1998: 96–97; Valtionvarainministeriö 1999; Stallings 2007: 703.)

Pääsynvalvonnassa kohdejärjestelmä hallitsee järjestelmän ja sen sisältämien tietojen käyttämistä. Pääsynvalvonta kontrolloi sitä, millä oliolla on oikeus tiettyihin tietoihin ja järjestelmiin sekä mitä kyseinen olio järjestelmässä voi tehdä. Pääsynvalvonta vaatii olioiden autentikointia. (Kerttula 1998: 96–97.)

Saatavuudessa on kyse siitä, että tieto tai tietojärjestelmä on käytettävissä tietyssä vasteajassa. Tietojärjestelmän ja sen sisältämien tietojen tulee palautua ja olla käytettävissä hyökkäyksen jälkeenkin. (Kerttula 1998: 97; Valtionvarainministeriö 1999; Pfleeger 2006.)

3.4. Tietoliikenneverkkojen tietoturva

Tietoliikenneverkkojen suojaamisessa käytettävät kryptomekanismit sijoitetaan johonkin verkkokerrokseen tai niiden väliin. Tietoturvasuunnittelussa verkkoa tuleekin tarkastella kerroksittain. (Kerttula 1998: 191.)

Tietoliikenneverkkojen tietoturvan yhteydessä on olennaista erottaa toisistaan verkon avulla välitettävät sanomat ja verkossa siirrettävät paketit. Sanomalla tarkoitetaan kokonaista viestiä, joka siirretään lähettäjältä vastaanottajalle ja se voi koostua useasta tietoliikennepaketista. Verkossa käytettävien laitteiden ja protokollien vastuulla on sanomien jakaminen paketteihin, pakettien siirtäminen tietoliikenneverkossa ja pakettien kokoaminen takaisin alkuperäisiksi sanomiksi. (Kerttula 1998: 189–190.)

Tietoliikenneyhteyksien suojaamisen perustavoitteena on Kerttulan (1998: 206) mukaan saavuttaa riittävän suuri varmuus siitä, että ulkopuoliset eivät pysty lukemaan tai muuttamaan verkossa välitettäviä sanomia. Huomioitavaa tietoturvassa on suhteellisuuden periaate. Esimerkiksi maksuliikenneinformaation siirtäminen verkossa vaatii huomattavasti kehittyneemmän suojausmenetelmän kuin markkinointimateriaalin siirtäminen. (Kerttula 1998: 206.)

Merkittävimmät erot eristetyn tietojärjestelmän ja tietoliikenneverkkoon kytketyn välillä voidaan jakaa Pfleeger ym. (2006) mukaan kuuteen osa-alueeseen.

Tietoliikenneverkkojen yhteydessä käyttäjät voivat toimia anonyymisti, jolloin myös hyökkääjä voi suorittaa hyökkäyksensä anonyyminä. Hyökkääjä voi peittää jälkensä ohjaamalla hyökkäyksen kulkemaan useiden ulkopuolisten tietojärjestelmien kautta. Lisäksi erityisesti julkisiin tietoverkkoihin kytkettyjen järjestelmien kohdalla hyökkääjän maantieteellisen sijainnin merkitys vähenee. (Pfleeger ym. 2006; Kerttula 1998: 206.)

Tietoliikenneverkko koostuu useista yksittäisistä laitteista ja tällöin myös tietoliikenne kulkee useiden eri laitteiden kautta. Verkkosolmujen lukumäärän kasvaminen lisää mahdollisia hyökkäyskohteita ja -lähteitä huomattavasti. Lisäongelmia aiheuttaa laitteiden heterogeenisyys esimerkiksi tietoturva-asetusten suhteen. (Pfleeger ym. 2006.)

Tietoliikenneverkot mahdollistavat resurssien ja kuormituksen jakamisen sekä laitteiden että käyttäjien välillä. Luonnollinen seuraus ominaisuudesta on väärinkäytösmahdollisuuksien lisääntyminen. (Pfleeger ym. 2006.)

Tietoliikenneverkkoa käyttävä tietojärjestelmä on lähtökohtaisesti monimutkaisempi kuin tietoliikenneyhteyksiä käyttämätön tietojärjestelmä. Tietojärjestelmän monimutkaistuminen vaikuttaa kokonaisuuteen kahdella tasolla; toisaalta lisäämällä hyökkäyspinta-alaa ja toisaalta vaikeuttamalla järjestelmän toiminnan seuraamista. (Pfleeger ym. 2006.)

Tietoliikenneverkkojen laajennettavuus johtaa epäselvyyteen verkon rajoista ja siihen kuuluvista solmuista. Vapaan laajennettavuuden myötä verkkoon liittyvä solmu voi yhdistää useita verkkoja yhteen. Tällöin tietoturvasääntöjen ylläpitäminen on erittäin monimutkaista verkon jatkuvasti muuttaessa muotoaan. (Pfleeger ym. 2006.)

Tietoliikenteen reititykseen verkossa käytetään hyvin harvoin kiinteitä reittejä, jolloin tietoliikennepakettien reiteistä ei voida olla varmoja pakettien lähetyksen yhteydessä. Kiinteiden reittien puuttuminen voi johtaa pakettien kulkemisen vihamielisten tai suojaamattomien verkkosolmujen kautta viestinnän alkuperäisten osapuolten siitä tietämättä. (Pfleeger ym. 2006.)

Parziale, Britt, Davis, Forrester, Liu, Matthews ja Rosselot (2006: 772) luettelevat seitsemän yleistä tietoverkkoja vastaan tehtävää hyökkäysmenetelmää:

- tietoliikennepakettien kaappaaminen
- identiteetin väärentäminen
- palvelunestohyökkäys
- tietoliikenteen väärentäminen
- salausavainten murtaminen
- virukset ja madot
- porttiskannaus

Tietoliikennepakettien kaappaamisessa on tavoitteena päästä käsiksi salaamattomaan arkaluonteiseen informaatioon. Identiteetin väärentämisessä hyökkääjä pyrkii esiintymään sallittuna käyttäjänä ja pääsemään näin käsiksi arkaluonteiseen tietoon tai lähettämään viestejä toisen henkilön nimissä kolmansille osapuolille. Palvelunestohyökkäyksessä tietoverkko tai jokin sen osa pyritään saattamaan pois käytöstä ylikuormittamalla tietoverkkoa. Tietoliikenteen väärentämisessä hyökkääjä kaappaa ja muokkaa kohteena olevan tietoliikenneyhteyden yli siirrettävää informaatiota. Salausavainten murtamisessa hyökkääjä pyrkii murtamaan tai arvaamaan kohteena olevan tietoliikenneyhteyden salaamiseen käytettävät salausavaimet. Virusten ja matojen avulla hyökkääjä pyrkii vahingoittamaan tietoverkon laitteita ja tuhomaan välitettävää informaatiota. Porttiskannauksessa tavoitteena on kerätä informaatiota tietoverkon mahdollisista hyökkäyskohteista. (Parziale ym. 2006: 772.)

3.5. Tietoturvariskien hallinta

Tietoturvauhkien hallintaan on olemassa useita menetelmiä ja kontrolleja. Osa menetelmistä kykenee täysin torjumaan tiettyjä uhkia, osa lieventämään seurauksia ja osa vain tunnistamaan toteutuneita hyökkäyksiä. (Pfleeger ym. 2006.)

Tietoturvavahinko tapahtuu, kun jokin tietoturvauhka realisoituu. Tietoturvavahingoilta voidaan suojautua poistamalla mahdolliset tietoturvahaavoittuvuudet tai -uhat. Mahdollisesti toteutuvaa tietoturvavahinkoa kutsutaan tietoturvariskiksi. (Pfleeger ym. 2006.)

Tietoturvariskien hallintaan on olemassa viisi perusstrategiaa. Tietoturvariski voidaan estää täysin *(Prevent)*, estää osittain *(Deter)*, siirtää *(Deflect)*, tunnistaa *(Detect)* tai siitä voidaan palautua *(Recover)*. Käytännössä yleisesti käytetään useamman perusstrategian kombinaatioita. (Pfleeger ym. 2006.)

Riski voidaan täysin estää joko poistamalla riskiin liittyvä tietoturvahaavoittuvuus tai torjumalla siihen kohdistuvat hyökkäykset. Riskin osittaisessa estämisessä riskiin liittyvän haavoittuvuuden hyödyntämistä vaikeutetaan olennaisesti hyökkääjän näkökulmasta. Riskin siirtämisessä on ajatuksena tehdä jostain toisesta riskistä hyökkääjän näkökulmasta alkuperäistä riskiä kiinnostavampi. Riskin tunnistamisessa tyydytään vain tarkkailemaan riskin mahdollista toteutumista. Palautumisstrategiassa on kyse siitä, että riskin toteutuessa järjestelmä palautetaan hyökkäystä edeltäneeseen tilaan. (Pfleeger ym. 2006.)

Tietoturvariskejä kontrolloidaan salausmenetelmillä, ohjelmisto- ja laitteistopohjaisilla kontrolleilla, tietoturvapoliitikoilla ja -käytännöillä sekä fyysisillä kontrolleilla. (Pfleeger ym. 2006.)

Viestinnän salaamisella on erittäin suuri merkitys tietojärjestelmän tietoturvallisuuteen, mutta se ei yksistään riitä. On myös tärkeää käyttää riittävän vahvoja salausmenetelmiä oikeissa kohteissa. Liian heikko salausmenetelmä saattaa johtaa väärään turvallisuuden tunteeseen ja jopa heikentää järjestelmän kokonaistietoturvaa. Liian vahva salausmenetelmä sitä

vastoin voi aiheuttaa tietojärjestelmän suorituskyvyn merkittävää heikentymistä, erityisesti mikäli menetelmää käytetään järjestelmässä väärin. (Pfleeger ym. 2006.)

Ohjelmistopohjaisia kontrolleja ovat ohjelmistojen sisäiset tietoturvakontrollit, itsenäiset tietoturvaohjelmistot sekä ohjelmistojen kehitystyökalujen tietoturvakontrollit (Pfleeger ym. 2006).

Laitteistopohjaisilla kontrolleilla tarkoitetaan erillisiä tietoturvalaitteita. Laitteistopohjaisia kontrollilaitteita ovat muun muassa palomuurit, IPS-laitteet, VPN-reitittimet sekä erilaiset älykortit. (Pfleeger ym. 2006.)

Tietoturvapolitiikkoihin ja -käytäntöihin kuuluu esimerkiksi pakotetut säännölliset salasanan vaihtamiset ja tietojärjestelmän käyttösäännöt. Fyysisiä kontrolleja ovat muun muassa kulunvalvonnalla valvotut suljetut tilat ja varmuuskopioiden säilyttäminen useassa paikassa. (Pfleeger ym. 2006.)

Pfleeger ym. (2006) määrittelee tietoturvakontrolleille ja niiden käyttämiselle neljä periaatetta:

- kontrollien tulee olla tehokkaita, helppokäyttöisiä ja sopivia
- paras tietoturva saadaan käyttämällä useita toisiaan tukevia kontrolleja
- kontrolleja tulee kehittää jatkuvasti
- järjestelmän kokonaistietoturva on aina yhtä vahva kuin sen heikoin tietoturvakontrolli

4. KRYPTOGRAFISET MENETELMÄT

Tietoturvan teknisten tavoitteiden toteuttamiseen liittyy olennaisesti kryptografia, joka on informaation salaukseen liittyvien matemaattisten menetelmien tutkimusta (Kerttula 1998: 23). Edellä mainittuja matemaattisia menetelmiä kutsutaan kryptografisiksi algoritmeiksi ja muunnoksiksi (Kerttula 1998: 70–71; Pfleeger ym. 2006).

Kryptografiaan liittyy olennaisesti informaation salaaminen ja salauksen purkaminen. Informaation salauksessa alkuperäinen selväkielinen informaatio salataan jonkin kryptografisen algoritmin eli salausmenetelmän avulla. Salauksen purkamisessa on kyse päinvastaisesta operaatiosta. Salattu viesti muunnetaan takaisin selväkieliseksi tietyn kryptografisen algoritmin avulla. (Parziale ym. 2006: 777; Kaufman, Perlman & Speciner 2002: 41.)

Salaukseen käytetään yleisesti salausmenetelmiä, joissa sekä informaation salaukseen että salauksen purkamiseen käytetään salausavainta ja jotain tiettyä salausalgoritmia. Salauksen vahvuus riippuu ensisijaisesti käytetystä salausavaimesta, joka voidaan valita salausmenetelmästä riippuvasta joukosta vaihtoehtoja. Lähtökohtaisesti mitä enemmän on vaihtoehtoja, sitä vahvempi salaus on mahdollista saavuttaa. (Parziale ym. 2006: 778.)

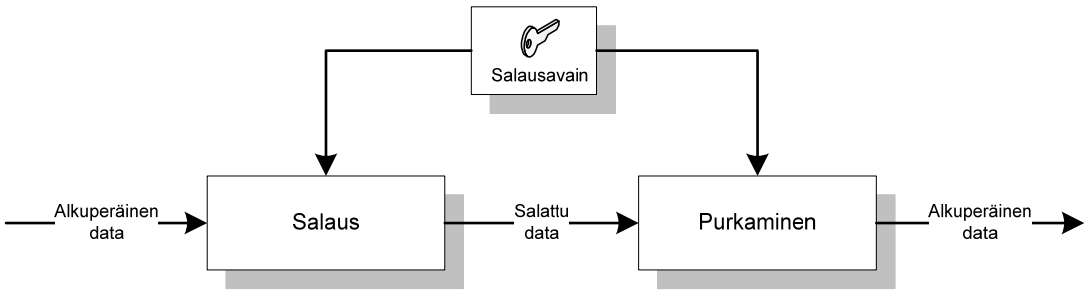
Salauksen avulla voidaan varmistaa viestinnän luottamuksellisuus, autentikoida viestinnän osapuolet, valvoa viestinnän eheyttä ja taata viestinnän kiistämättömyys (Parziale ym. 2006: 779).

Kryptografiset menetelmät voidaan jakaa salausmenetelmiin ja tiivistefunktioihin. Salausmenetelmät voidaan edelleen jakaa julkisen ja salaisen avaimen menetelmiin. (Kaufman ym. 2002: 47; Lehtonen 2004: 11–12.)

4.1. Salaisen avaimen menetelmä

Salaisen avaimen menetelmästä käytetään myös nimeä symmetrinen salaus. Menetelmässä sekä informaation salaukseen että salauksen purkamiseen käytetään samaa salausavainta. Viestinnän osapuolten tulee sopia käytettävästä

salausavaimesta ennen salauksen käyttöönottoa. Kuvassa 3 on esitetty periaatekuva symmetrisestä salauksesta. (Parziale ym. 2006: 779; Stallings 2003: 24–25; Lehtonen 2004: 11.)



Kuva 3. Symmetrisen salauksen periaatekuva (Pfleeger ym. 2006).

Symmetrisiä salausmenetelmiä on kahta tyyppiä, lohko- ja jonosalausalgoritmeja. Lähdeinformaatiota käsitellään lohkosalauksessa useamman bitin lohkoina ja jonosalauksessa bitti kerrallaan. (Parziale ym. 2006: 779; Stallings ym. 2008: 44–49.)

Lohkosalausalgoritmeja käytetään useassa eri tilassa. Yksinkertaisin tiloista on Electronic Codebook (ECB), jossa jokainen lähdeinformaation bittilohko salataan itsenäisesti. ECB:n ongelmana on, että hyökkääjän on mahdollista muodostaa koodikirja, jolla salaus voidaan murtaa, mikäli hyökkääjä saa selvitettyä riittävän määrän viestipareja (alkuperäinen ja sitä vastaava salattu viesti). Ongelma voidaan kiertää yleisesti käytetyllä Cipher Block Chaining (CBC) -tilalla, jossa lohkon salaus riippuu lähdeinformaatiolohkon lisäksi edellisestä salatusta lohkosta. (Parziale ym. 2006: 779.)

Lohkosalausalgoritmit käyttävät usein alkuarvovektoreita. Alkuarvovektorit ovat riippumattomia salausavaimista ja ne sopivat siten algoritmien alkuarvojen määrittämiseen. (Parziale ym. 2006: 779.)

Tunnettuja lohkosalausmenetelmiä ovat muun muassa Data Encryption Standard (DES) ja sen muunnos Triple-DES (3DES), Advanced Encryption Standard (AES) sekä International Data Encryption Algorithm (IDEA). (Parziale ym. 2006: 779–780.)

Data Encryption Standard (DES) on menetelmistä vanhin, ja sitä ei enää pidetä turvallisena. Menetelmässä lohkon koko on 64 bittiä. Salausavain on 56 bittinen luku, joka usein esitetään pariteettibitit mukaan lukien 64 bittisenä lukuna ja se jaetaan algoritmissa käytettäviin 16 aliavaimeen. Salausmenetelmässä käytetään täysin samaa algoritmia sekä viestien salaamiseen että salauksen purkamiseen ja salaus- ja purkamisprosessit eroavat toisistaan ainoastaan aliavainten käytön suhteen. Menetelmällä salattu viesti sisältää yhtä monta merkkiä kuin alkuperäinen viesti. (Parziale ym. 2006: 779–780; Stallings ym. 2008: 44–45.)

DES-menetelmän merkittävin haavoittuvuus liittyy salausavaimen heikkouteen. 56 bittinen avain on murrettavissa kaikkien mahdollisten avainten läpikäyntiin perustuvalla Brute force -menetelmällä varsin nopeasti. Menetelmän uudemmat muunnokset kuten 3DES suorittaa DES-menetelmässä käytetyn salausalgoritmin kolmeen kertaan käyttäen kahta tai kolmea joko 112 tai 168 bittistä salausavainta. (Parziale ym. 2006: 780; Stallings ym. 2008: 45–46.)

3DES-menetelmän merkittävinä etuina ovat salausalgoritmin yhteensopivuus DES-menetelmässä käytetyn algoritmin kanssa ja vahvat salausavaimet, jotka kestävät erityisesti 168 bittisinä Brute force -menetelmällä tehtäviä hyökkäyksiä varsin hyvin. 3DES-menetelmän heikkouksina voidaan mainita salausalgoritmin ohjelmistototeutuksen hankaluus ja tehottomuus sekä vain 64 bittinen lohkokoko. (Stallings ym. 2008: 46.)

Advanced Encryption Standard (AES) -menetelmä on suunniteltu DES- ja 3DES-menetelmien korvaajaksi ja se perustuu Rijndael-lohkosalausalgoritmiin. Algoritmissa lohkon koko on 128 bittiä ja salausavain voi olla joko 128, 192 tai 256 bittinen. (Parziale ym. 2006: 780; Stallings ym. 2008: 47.)

Toinen DES-menetelmän korvaajaksi tarkoitettu lohkosalausmenetelmä on International Data Encryption Algorithm (IDEA), joka käyttää 64 bittisiä lohkoja ja 128 bittistä salausavainta. IDEA on DES-menetelmään verrattuna nopeampi ja vahvempi. (Parziale ym. 2006: 780.)

Jonosalausmenetelmistä tunnetuin on A5, jota käytetään GSM-standardissa. Jonosalausalgoritmit ovat periaatteessa yhtä turvallisia kuin lohkosalausalgoritmit, mikäli käytettävät salausavaimet ovat pituudeltaan

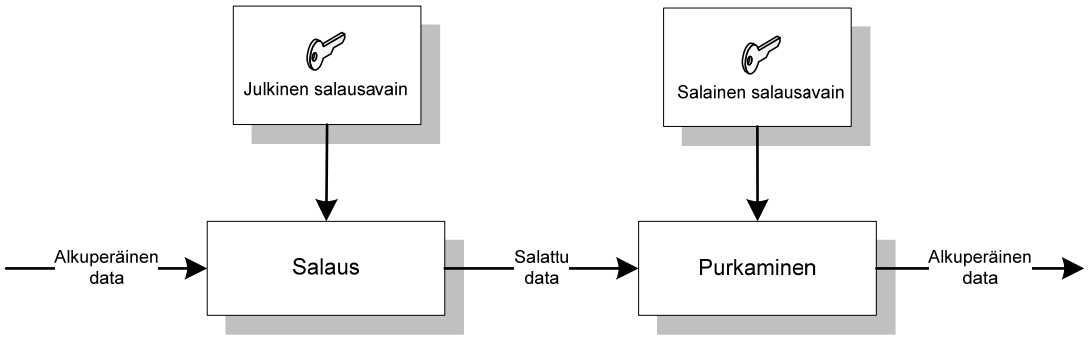
vastaavia ja jonosalausalgoritmin satunnaislukugeneraattori on oikein suunniteltu. (Parziale ym. 2006: 780; Stallings ym. 2008: 47–48.)

Jonosalausalgoritmien merkittävimmät edut lohkosalausmenetelmiin verrattuna ovat nopeus ja toteutuksen yksinkertaisuus. Lohkosalausmenetelmien eräänä merkittävänä etuna voidaan mainita mahdollisuus käyttää samoja salausavaimia. (Stallings ym. 2008: 48.)

Symmetristen salausmenetelmien merkittävin etu liittyy niiden tehokkuuteen. Menetelmät on myös helppo toteuttaa laitteistopohjaisina. Merkittävin heikkous liittyy avainten hallintaan. Menetelmien hyödyntäminen vaatii turvallisen tavan salausavainten siirtämiseen viestinnän osapuolten välillä. (Parziale ym. 2006: 780.)

4.2. Julkisen avaimen menetelmä

Julkisen avaimen menetelmää kutsutaan myös epäsymmetriseksi salaukseksi. Menetelmässä käytetään salausavainparia informaation salaukseen ja salauksen purkamiseen. Avainparin toinen avain on julkinen ja toinen yksityinen salainen avain. Menetelmässä on tärkeää, että yksityistä avainta ei voida johtaa julkisesta avaimesta. Epäsymmetrisen salauksen toimintaperiaate on esitetty kuvassa 4. (Parziale ym. 2006: 780; Stallings ym. 2008: 56–59; Lehtonen 2004: 11.)



Kuva 4. Epäsymmetrisen salauksen periaatekuva (Pfleeger ym. 2006).

Epäsymmetrisessä salauksessa informaatio, joka on salattu julkisella avaimella, voidaan purkaa ainoastaan käyttämällä saman avainparin yksityistä avainta. Vastaavasti yksityisellä avaimella salatun informaation purkaminen vaatii saman avainparin julkisen avaimen. (Parziale ym. 2006: 780–781; Stallings ym. 2008: 57–59.)

Epäsymmetrisessä salauksessa avainten hallinta on yksinkertaista, sillä viestinnän osapuolet tarvitsevat vain toistensa julkiset avaimet informaation salaukseen. Avainten vaihtoon ei tarvita salaisen avaimen salausmenetelmissä vaadittavaa suojattua yhteyttä, koska pelkkien julkisten avaimien joutuminen kolmansien osapuolien käsiin ei vaaranna salausta. (Parziale ym. 2006: 780–781; Stallings ym. 2008: 56–59.)

Parziale ym. (2006: 782) mainitsee Rivest Shamir Adleman (RSA) -algoritmin olevan yleisin epäsymmetrinen salausmenetelmä. RSA-menetelmä on lohkosalausalgoritmi ja se perustuu suurten alkulukujen tulon tekijöihin jaon ongelmallisuuteen. Algoritmissa käytettävät julkiset ja yksityiset avaimet muodostetaan kertomalla kaksi erittäin suurta alkulukua toisillaan. (Parziale ym. 2006: 782; Stallings ym. 2008: 60.)

RSA-algoritmilla salattu viesti on periaatteessa purettavissa, mikäli hyökkääjällä on käytettävissään salatun viestin lisäksi salaukseen käytetty julkinen avain ja hyökkääjä kykenee jakamaan julkisen avaimen tekijöihin. Tekijöihin jakaminen vaikeutuu merkittävästi avaimen koon kasvaessa, ja Stallings ym. (2008: 60) toteaa 1024 bittisten salausavaimien riittävän käytännössä kaikkiin tarkoituksiin.

Toinen yleinen epäsymmetrinen salausmenetelmä on Diffie-Hellman-avaintenvaihtoalgoritmi, joka on tarkoitettu salaisen tiedon välittämiseen suojaamattoman tietoliikenneyhteyden yli. Algoritmi perustuu suurten lukujen diskreettien logaritmien laskemisen vaikeuteen. Menetelmässä viestinnän osapuolet valitsevat ja laskevat joukon lukuja, joista osa on julkisia ja osa salaisia. Osapuolet lähettävät toisilleen julkiset luvut ja johtavat julkisten sekä salaisten lukujen perusteella viestinnän salauksessa käytettävät salausavaimet. Salausavaimia ei voida määrittää yhteyden yli siirretyn informaation

perusteella, mikäli valitut ja siten myös lasketut luvut ovat riittävän suuria. (Parziale ym. 2006: 783.)

Diffie-Hellman-menetelmä sopii hyvin symmetristen salausmenetelmien vaatimien suojattujen avaintenvaihtoyhteyksien luomiseen. Algoritmin merkittävin ongelma on sen rajoittuneisuus, se kykenee ainoastaan välittämään salauksessa käytettävät salausavaimet osapuolten välillä. Menetelmä ei kykene esimerkiksi autentikoimaan osapuolia, vaan siihen joudutaan käyttämään jotain toista menetelmää. (Parziale ym. 2006: 783; Stallings ym. 2008: 61.)

Symmetrisiin salausmenetelmiin verrattuna epäsymmetristen salausmenetelmien merkittävimmät heikkoudet liittyvät niiden monimutkaisuuteen. Monimutkaisuuden myötä ne kuluttavat runsaasti laskentatehoa ja niiden toteuttaminen laitteistopohjaisena on vaikeaa. Epäsymmetriset salausmenetelmät eivät siten sovellu suurten informaatiomassojen salaukseen. (Parziale ym. 2006: 783.)

Julkisen avaimen salausmenetelmiä käytetään sen sijaan symmetristen salausmenetelmien salausavaimien jakamiseen ja salaamiseen sekä digitaaliseen allekirjoittamiseen (Stallings ym. 2008: 59, 61). Hyvässä kryptografisessa järjestelmässä käytetäänkin sekä symmetrisiä että epäsymmetrisiä salausmenetelmiä (Parziale ym. 2006: 783).

4.3. Tiivistefunktiot

Tiivistefunktio on matemaattinen funktio, joka tuottaa muuttuvamittaisesta syötteestä kiinteämittaisen tiivisteen. Tiiviste on ikään kuin alkuperäisen syötteen sormenjälki. (Parziale ym. 2006: 785; Stallings ym. 2008: 52–55; Lehtonen 2004: 12.)

Kryptografiassa käyttökelpoisimpia ovat yksisuuntaiset tiivistefunktiot. Yksisuuntaiselta tiivistefunktiolta vaaditaan, että sen avulla voidaan laskea alkuperäisestä viestistä nopeasti sellainen tiiviste, jonka muuntaminen takaisin alkuperäiseksi viestiksi on erittäin hankalaa. Hyvän tiivistefunktion tulee lisäksi tuottaa mahdollisimman ainutkertaisia tiivisteitä eli todennäköisyys sille, että

on olemassa kaksi erilaista syötettä, joilla on sama tiiviste, tulee olla mahdollisimman pieni. (Parziale ym. 2006: 785; Stallings ym. 2008: 54–55.)

Tiiviste, jonka laskemisessa tiivistefunktio käyttää syötteenä annetun alkuperäisen datan lisäksi salausavainta, kutsutaan Message Authentication Code (MAC) -tiivisteeksi. Tiivistefunktio voi hyödyntää joko symmetristä tai epäsymmetristä salausalgoritmia MAC-tiivisteen luomisessa. (Parziale ym. 2006: 786.)

Tiivistefunktioita käytetään yleisesti viestien eheyden tarkastamiseen ja viestinnän osapuolten tunnistamiseen (Parziale ym. 2006: 786).

Viestin eheys tarkastetaan siten, että lähettäjä laskee alkuperäiselle viestille tiivisteen ja lähettää sekä tiivisteen että alkuperäisen viestin vastaanottajalle. Seuraavaksi viestin vastaanottaja laskee vastaanotetulle viestille tiivisteen samalla tiivistefunktiolla ja vertaa sitä lähettäjän laskemaan tiivisteeseen. Mikäli tiivisteet täsmäävät, vastaanottaja olettaa viestin olevan alkuperäinen. (Parziale ym. 2006: 786.)

Viestinnän toinen osapuoli voidaan autentikoida käyttämällä tavallisten tiivisteiden sijaan MAC-tiivisteitä. Mikäli vastaanotettu MAC-tiiviste voidaan purkaa tietyllä salausavaimella, vastaanottaja voi varmistua lähettäjästä. (Parziale ym. 2006: 786.)

Yleisesti käytettyjä tiivistefunktioita ovat Message-Digest 5 (MD5) ja sen korvaajaksi tarkoitettu Secure Hash Algorithm (SHA). MD5 luo 128 bittisiä tiivisteitä ja SHA-funktion 1. versio (SHA-1) 160 bittisiä tiivisteitä. Molemmat funktiot tallettavat tiivisteeseen tiedon alkuperäisen syötteen pituudesta, mutta kumpikaan ei osaa ottaa syötteenä salausavainta. (Parziale ym. 2006: 788.)

Hash-based Message Authentication Code (HMAC) on menetelmä, jonka avulla voidaan luoda niin sanottuja avainnettuja MAC-tiivisteitä käyttäen mitä tahansa kryptografista tiivistefunktiota, kuten esimerkiksi edellä esitettyjä MD5- ja SHA-1-funktioita. Menetelmä perustuu syötteen salaamiseen ennen varsinaisen tiivistefunktion suorittamista. Koska HMAC-menetelmässä tiiviste lasketaan kahdesti, myös syöte salataan kahdesti käsittelijän salaisella

avaimella. (Krawczyk, Bellare & Canetti 1997; Diersk ym. 2008: 14; Stallings ym. 2008: 632–634.)

4.3.1. Digitaalinen allekirjoittaminen

Digitaalista allekirjoittamista voidaan käyttää olioiden autentikointiin ja viestinnän kiistämättömyyden varmistamiseen. On kuitenkin huomattava, että digitaalisen allekirjoittamisen avulla ei voida taata viestinnän luottamuksellisuutta, koska kuka vain voi purkaa salatun viestin käyttämällä lähettäjän julkista avainta. (Parziale ym. 2006: 781–782, 787; Stallings ym. 2008: 62.)

Digitaalinen allekirjoittaminen toteutetaan epäsymmetrisellä salausmenetelmällä siten, että viestinnän lähettävä osapuoli luo yksityisellä avaimellaan salatun MAC-tiivisteen ja lähettää sen alkuperäisen viestin mukana vastaanottajalle. Mikäli vastaanottaja kykenee avaamaan MAC-tiivisteen lähettäjän julkisella avaimella ja se täsmää vastaanotetusta viestistä lasketun tiivisteen kanssa, vastaanottaja voi varmistua viestin lähettäjän henkilöllisyydestä. (Parziale ym. 2006: 781–782, 787; Stallings ym. 2008: 62.)

4.3.2. Digitaalinen kirjekuori

Digitaalisen kirjekuoren avulla voidaan lähettää salaista informaatiota suojaamattoman tietoliikenneyhteyden yli. Menetelmää käytetään yleisesti symmetristen salausmenetelmien salausavaimien jakamiseen. (Parziale ym. 2006: 787; Stallings ym. 2008: 64.)

Digitaalinen kirjekuori luodaan salaamalla alkuperäinen viesti kertakäyttöisellä salausavaimella. Seuraavaksi kertakäyttöinen salausavain salataan vastaanottajan julkisella avaimella ja lähetetään tiivisteenä salatun viestin yhteydessä vastaanottajalle. Vastaanottaja purkaa yksityisellä salausavaimella viestin tiivisteenä lähetetyn kertakäyttöisen salasanan ja purkaa sillä varsinaisen viestin. (Stallings ym. 2008: 64.)

4.4. Digitaaliset sertifikaatit

Julkisen avaimen salauksen eräs merkittävä tietoturvaongelma liittyy julkisen avaimen jakamiseen ja olioiden autentikointiin. Hyökkääjän on mahdollista korvata viestinnän toisen tai molempien osapuolien julkiset avaimet omalla julkisella avaimellaan ja näin päästä käsiksi yhteyden yli lähetettyyn salattuun informaatioon. (Parziale ym. 2006: 791; Stallings ym. 2008: 62.)

Ongelma voidaan ratkaista käyttämällä digitaalisia sertifikaatteja. Digitaaliset sertifikaatit ovat tiedostoja, jotka sitovat julkisen avaimen ja sen omistajan identiteetin yhteen. Sidoksen vahvistamisesta vastaa luotettava kolmas osapuoli, jota kutsutaan varmentajaksi. Varmentajasta käytetään usein englanninkielistä nimeä Certification Authority (CA). (Parziale ym. 2006: 791; Stallings ym. 2008: 62; Pfleeger ym. 2006.)

Varmentaja salaa digitaalisen sertifikaatin omalla salaisella salausavaimellaan, jolloin varmentaja voidaan identifioida purkamalla sertifikaatti varmentajan julkisella avaimella. Yleisesti digitaalinen sertifikaatti sisältää omistajan julkisen avaimen ja identiteetti-informaation lisäksi tietoa sertifikaatin myöntämis- ja päättymisajankohdasta. (Parziale ym. 2006: 791–792; Stallings ym. 2008: 62.)

Koska varmentajia voi olla useita, tarvitaan tapa, jolla voidaan varmistua varmentajan luotettavuudesta. Varmentajat muodostavat hierarkkisen luottamusketjun (*Trust Chain*), jossa hierarkiassa ylemmällä tasolla oleva varmentaja takaa alemman tason luotettavuuden. Luotettavuuden takaamiseen käytetään digitaalisia sertifikaatteja. Luottamusketjun tietoturvan tulee luonnollisesti olla erittäin vahva ja sen tulee vahvistua hierarkiassa ylöspäin mentäessä. (Parziale ym. 2006: 792.)

4.5. Satunnaisluvut

Satunnaislukugeneraattorit ovat merkittävässä roolissa useissa kryptografisissa järjestelmissä. Satunnaislukuja käytetään muun muassa salausalgoritmien alkuarvoina. (Parziale ym. 2006: 792–793.)

Hyvän satunnaislukugeneraattorin tulee tuottaa mahdollisimman ennalta arvaamattomia lukuja, joita ei voida laskea, vaikka generaattorin toimintalogiikka olisi tiedossa. Tehtävä on vaikea, koska tietokoneet, joilla satunnaisluvut yleisesti määritellään, perustuvat säännöllisten laskutoimitusten tekemiseen ja satunnaisluvut joudutaankin aina jollain tasolla laskemaan jonkin algoritmin perusteella. (Parziale ym. 2006: 793.)

5. TCP/IP-ARKKITEHTUURI

TCP/IP-protokollapino koostuu useista tietoliikenneverkoissa käytettävistä protokollista. Viralliselta nimeltään protokollapino on Internet Protocol Suite. Virallisen nimen sijaan protokollapinosta käytetään yleisesti nimeä TCP/IP, joka viittaa protokollapinon alkuperäisiin ydinprotokolliin, Transmission Control Protocol (TCP) ja Internet Protocol (IP) -protokolliin. Protokollapinon kehittämisestä vastaa nykyisin Internet Engineering Task Force (IETF). (Stewart 2009; Parziale ym. 2006: 1–4.)

TCP/IP-arkkitehtuuri pohjautuu kerroksittaiseen malliin, jossa protokollat sijoittuvat eri kerroksille niiden käyttötarkoituksen ja toiminnallisuuden mukaan. Kerrosmalliin perustuva arkkitehtuuri tarjoaa useita etuja yksitasoiseen arkkitehtuuriin verrattuna. (Parziale ym. 2006: 6.)

Kerrosmallin merkittävin etu on siinä, että se yksinkertaistaa kokonaisuuden ymmärtämistä ja sovellusten sekä protokollien suunnittelua. Sovelluskehittäjän ja -suunnittelijan kannalta oleellista on ainoastaan, että standardin määrittelemät rajapinnat toteutetaan. Varsinaisella toteutustavalla ei ole merkitystä. Modulaarinen rakenne nopeuttaa myös kehitystyötä ja toteutusta. (Anttila 2001: 30–31; Stallings 2009: 44.)

TCP/IP-mallin lisäksi tietoliikenneverkoissa käytetään muun muassa Systems Network Architecture (SNA) ja Open System Interconnection (OSI) -kerrosmalleja. Eri mallit eroavat toisistaan huomattavasti muun muassa kerrosten lukumäärän ja niillä toteutettavien toiminnallisuuksien suhteen. (Parziale ym. 2006: 6.)

5.1. OSI-malli

Anttilan (2001: 30–31) mukaan kaikki verkkotekniikat on mallinnettavissa OSI-mallin avulla. Malli on kehitetty 80-luvun alussa kansainvälisen International Organization for Standardization (ISO) -standardointitoimiston yleiseksi verkkoarkkitehtuuriksi ja sen päätavoitteena oli vähentää verkkotekniikoiden yhteensopivuusongelmia. OSI-mallia kehitettäessä pohjalla ei ollut mitään

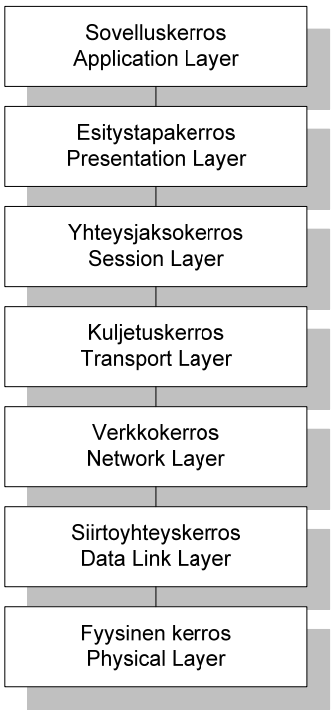
olemassa olevaa mallia ja se sekä sen sisältämät standardiprotokollat ovat läpikäyneet vaativan virallisen hyväksymisprosessin toisin kuin esimerkiksi TCP/IP-malli ja suuri osa siihen kuuluvista protokollista. (Anttila 2001: 30–31; Parziale ym. 2006: 6, 20–21.)

OSI-mallia ei ole kuitenkaan otettu käyttöön alun perin suunnitellussa laajuudessa (Anttila 2001: 30–31). Anttila (2001: 30–31) mainitsee erääksi syyksi sen, että OSI-mallin määrittelemät standardit ovat monimutkaisia sekä käyttää että toteuttaa. ISO-standardien tiukka muodollinen hyväksymisprosessi on lisäksi hidastanut mallissa määriteltyjen standardien jatkokehitystä (Parziale ym. 2006: 21). Eräs merkittävä syy on myös ollut se, että kilpailevan TCP/IP-arkkitehtuurin tärkeimmät protokollat olivat jo koeteltuja ja kypsiä samaan aikaan, kun OSI-mallia vasta kehitettiin (Stallings 2009: 43).

OSI-mallin käytännön ongelmat ovat johtaneet siihen, että mallista on muotoutunut niin sanottu referenssimalli (Anttila 2001: 30–31; Stallings 2009: 44).

5.1.1. OSI-mallin kerrokset

OSI-malli koostuu seitsemästä itsenäisestä kerroksesta, jotka ovat sovelluskerros (*Application Layer*), esitystapakerros (*Presentation Layer*), yhteysjaksokerros (*Session Layer*), kuljetuskerros (*Transport Layer*), verkkokerros (*Network Layer*), siirtoyhteyskerros (*Data Link Layer*) ja fyysinen kerros (*Physical Layer*). Kerrosten keskinäinen järjestys on esitetty kuvassa 5. (Anttila 2001: 30–31.)



Kuva 5. OSI-mallin kerrokset.

Sovelluskerros on OSI-mallin kerroksista lähimpänä käyttäjää. Kerros tarjoaa sovelluksille verkkopalveluita. (Anttila 2001: 32.)

Esitystapakerros määrittelee välitettävän informaation muodon eli koodaustavan. Kerroksen tehtävänä on myös toimia tulkkina, ja sen avulla voidaan esimerkiksi muuttaa merkkejä merkistöstä toiseen. (Anttila 2001: 33.)

Yhteysjaksokerros koordinoi sovellusten eri toimintoja laitteiden välillä. Kerros vastaa siirrettävän informaation välittämisestä oikeassa järjestyksessä. (Anttila 2001: 33.)

Kuljetuskerros vastaa ylemmiltä kerroksilta tulevan informaation pilkkomisesta segmentteihin ja välittämisestä vastaanottajalle. Kerroksen toimintaperiaate voi olla yhteydellinen tai yhteydetön. (Anttila 2001: 34.)

Verkkokerros pakkaa kuljetuskerrokselta vastaanotetut segmentit käytettävän verkon vaatimusten mukaisiin paketteihin ja välittää ne vastaanottajalle. Kerros

vastaa myös pakettien reitityksestä; paketit lähetetään vastaanottajan verkkokerroksen osoitteen perusteella vastaanottajalle. (Anttila 2001: 34.)

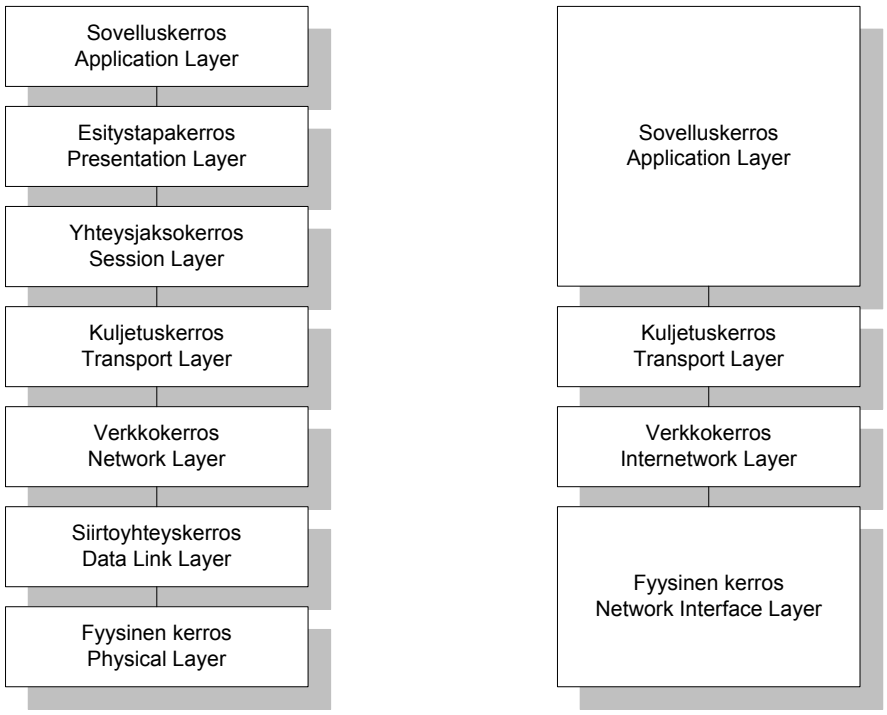
Siirtoyhteyskerros vastaa lähetettävän datakehyksen rakentamisesta. Datakehys pitää sisällään muun muassa verkkokerrokselta saadut paketit. Kerroksessa kehykseen lisätään tarvittavat otsikkotiedot. (Anttila 2001: 34.)

Fyysinen kerros on nimensä mukaisesti lähimpänä laitteistotasoa. Kerroksessa määritellään miten bittien välitys toteutetaan käytössä olevalla tekniikalla. Määrittelyt pitävät sisällään muun muassa käytettävät koodausmenetelmät ja jännitetasot. (Anttila 2001: 34.)

5.2. TCP/IP-kerrosmalli

Vaikka TCP/IP-tekniikka on kehitetty ennen OSI-mallia, niin siitä huolimatta TCP/IP-pinon kerrokset vastaavat pääsääntöisesti OSI-mallin kerroksia (Anttila 2001: 35.)

TCP/IP-malli on jaettu sovelluskerrokseen (*Application Layer*), kuljetuskerrokseen (*Transport Layer*), verkkokerrokseen (*Internetwork Layer*) ja fyysiseen kerrokseen (*Network Interface Layer*). TCP/IP-kerrosmallia on verrattu OSI-malliin kuvassa 6. (Anttila 2001: 35; Parziale ym. 2006: 7–8.)



Kuva 6. OSI-mallin ja TCP/IP-pinon kerrosten vastaavuus.

Sovelluskerroksen tehtävänä on tarjota rajapinta TCP/IP-tekniikkaa käyttäville sovelluksille. Osa kerroksen protokollista voi olla suoraan käyttäjän hallittavissa, kuten esimerkiksi File Transfer Protocol (FTP). Yleinen sovelluskerrokselle sijoittuva protokolla on edellä mainitun FTP:n lisäksi Hypertext Transfer Protocol (HTTP) -protokolla. (Parziale ym. 2006: 7; Black 1998: 10.)

Kuljetuskerros mahdollistaa päätelaitteiden väliset tiedonsiirtoyhteydet ja se tukee useita samanaikaisia yhteyksiä. Merkittäviä kuljetuskerroksen protokollia ovat Transmission Control Protocol (TCP) ja User Datagram Protocol (UDP). (Parziale ym. 2006: 7–9; Black 1998: 10.)

Kuljetuskerroksen protokollat käyttävät pakettien välitykseen alla olevan verkkokerroksen protokollia (Anttila 2001: 133). Kuljetuskerroksen protokollat tarjoavat toiminnallisuuksia muun muassa luotettavaan tiedonsiirtoon sekä ruuhkan- ja vuonhallintaan. (Parziale ym. 2006: 143.)

Verkkokerros sisältää toiminnallisuudet, joiden avulla useita verkkoja voidaan liittää toisiinsa. Verkkokerroksesta käytetään joissakin yhteyksissä nimeä Internet-kerros. Sen tehtävänä on piilottaa fyysisen tason yhteydet ylemmiltä verkkokerroksilta. Verkkokerroksen protokollat vastaavat tietoliikennepakettien reitittämisestä ja siirtämisestä. Lisäksi kerroksen protokollia käytetään dynaamiseen osoitteen määrittämiseen ja selvittämiseen verkkokerroksen ja fyysisen kerroksen välillä. Kerroksen tärkein protokolla on Internet Protocol (IP). (Parziale ym. 2006: 8, 67; Black 1998: 9–10.)

Muita verkkokerroksen merkittäviä protokollia ovat Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), Address Resolution Protocol (ARP) ja Dynamic Host Configuration Protocol (DHCP). Vaikka ICMPv4- ja IGMPv3-protokollat toimivat IPv4-protokollan päällä, ne sijoittuvat kuitenkin arkkitehtuurisesti samalle kerrokselle. (Parziale ym. 2006: 8, 67; Black 1998: 9–10.)

Fyysinen kerros on TCP/IP-mallin alin verkkokerros. Kerros sisältää nimensä mukaisesti varsinaiset fyysiset tiedonsiirtoyhteydet. Lähtökohtaisesti ainoa fyysisen kerroksen komponenteille asetettu vaatimus on, että niiden tulee tarjota verkkokerroksen protokollille standardoitu rajapinta komponenttien käyttämiseen. Fyysisen kerroksen laitteet ja yhteydet voivat perustua esimerkiksi X.25-, Asynchronous Transfer Mode (ATM) tai General Packet Radio Service (GPRS) -teknologiaan. (Parziale ym. 2006: 8; Black 1998: 9.)

5.3. Ydinprotokollat

5.3.1. Internet Protocol (IP)

Internet Protocol on IETF:n virallinen standardi numero viisi (IETF STD 5). Standardiin kuuluu IP:n lisäksi ICMP- ja IGMP-protokollat. IP-protokolla on määritelty protokollaksi, joka tulee toteuttaa kaikissa TCP/IP-tekniikkaa hyväksikäyttävissä sovelluksissa. (Parziale ym. 2006: 68.)

IP-protokolla on määritelty RFC-dokumenteissa RFC 950, RFC 919, RFC 922, RFC 3260, RFC 3168 ja RFC 1349 (Parziale ym. 2006: 68). Protokollasta on

käytössä tällä hetkellä kaksi versiota; versiot neljä (IPv4) ja kuusi (IPv6). Valtaosa Internetin verkkoliikenteestä käyttää edelleen IPv4-protokollaa. (Anttila 2001: 113.)

IPv4-protokollan tehtävänä on välittää tietoliikennepaketteja. Pakettien välitystä varten protokolla luo eräänlaisen virtuaalisen verkon, jonka avulla alla oleva fyysinen kerros piilotetaan ylemmän tason kerroksilta. IPv4-protokolla vastaa ylemmiltä kerroksilta tulevien tietoliikennepakettien osioimisesta ja reitityksestä. (Anttila 2001: 114.)

IPv4-protokolla ei ylläpidä tietoja muodostetuista yhteyksistä eli se on toimintaperiaatteeltaan yhteydetön protokolla. IPv4 ei sisällä toiminnallisuuksia verkkoliikenteen määrän hallintaan (*vuonohjaus*) eikä virheenkorjaukseen. Edellä mainittujen ominaisuuksien karsimisella protokollasta on saatu yksinkertainen, suorituskykyinen ja vikasietoinen. (Anttila 2001: 114; Parziale ym. 2006: 68.)

IPv4-protokollan reititysalgoritmi reitittää jokaisen tietoliikennepaketin itsenäisesti aiemmista paketeista välittämättä. Käytännössä reitit ovat kuitenkin varsin pysyviä, ja ne muuttuvat lähinnä vain poikkeustilanteissa. (Anttila 2001: 114–115.)

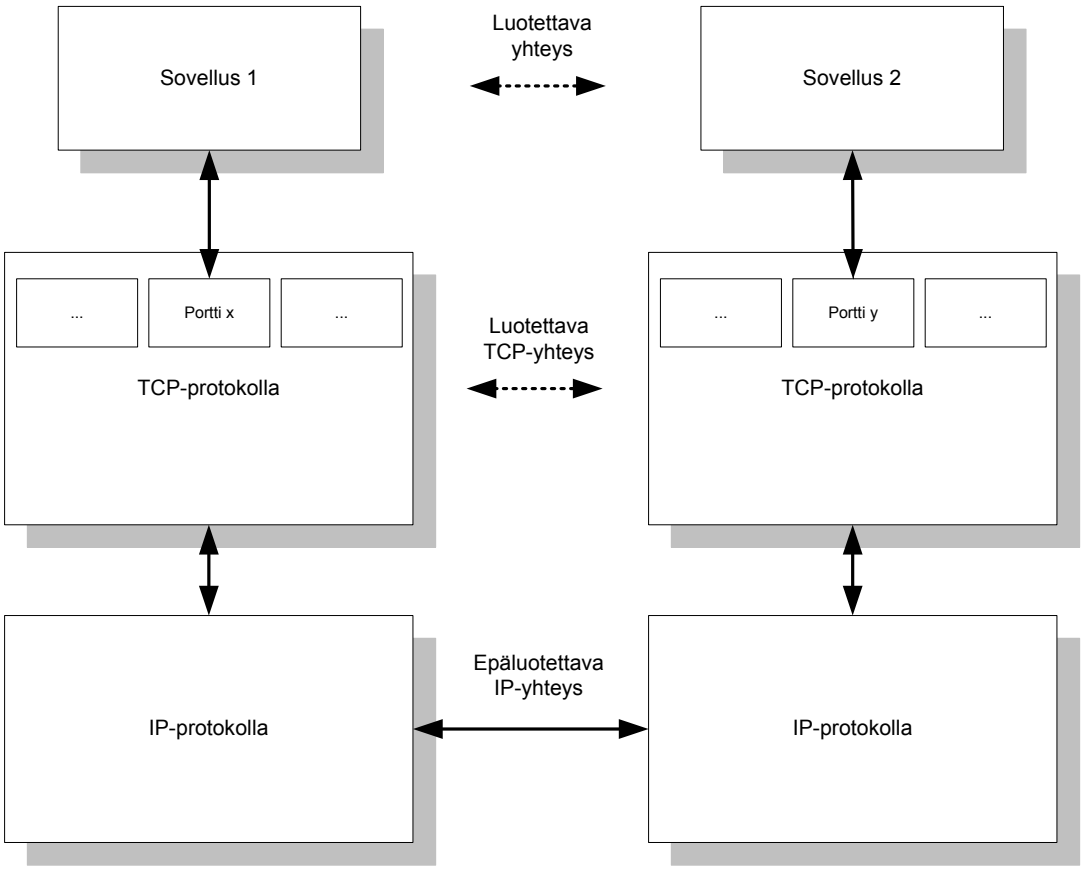
IPv4-pakettien reitityksen kannalta olennaiselle IP-osoitteelle on varattu 32-bittiä IPv4-standardissa. Standardi on tarkemmin määritelty RFC 1166 -dokumentissa. Osoite koostuu verkko-osoitteesta (*Network Number*) ja laiteosoitteesta (*Host Number*). IPv4-protokollaa käyttävissä tietoliikenneverkoissa jokaisella verkkoon liitetyllä laitteella on vähintään yksi yksilöllinen IPv4-osoite. Osoitteita käytetään laitteiden tunnistamiseen sekä verkkoliikenteen reitittämiseen. (Anttila 2001: 84–85; Parziale ym. 2006 68–69.)

IPv4-osoitteiden tehokkaaseen hyödyntämiseen käytetään menetelmää nimeltä aliverkotus (*Subnetting*). Menetelmässä verkko jaetaan sisäisesti useampaan aliverkkoon siten, että ulospäin verkko näyttää yhtenäiseltä. Aliverkotus toteutetaan pääsääntöisesti reitittimillä. (Anttila 2001: 97; Parziale ym. 2006: 72.)

Aliverkkojen muodostamismenetelmiä on useita. Yleisimmin käytössä on menetelmä, jossa aliverkko luodaan erillisen aliverkonpeitteen (*Subnet Mask*) avulla. Menetelmässä IPv4-osoitteen laiteosa jaetaan verkko- ja laiteosoitteisiin niin sanotun aliverkonpeitteen avulla. (Anttila 2001: 99–100; Parziale ym. 2006: 73.)

5.3.2. Transmission Control Protocol (TCP)

Transmission Control Protocol on IETF:n standardi numero seitsemän (IETF STD 7) ja se on kuvattu RFC 793 -dokumentissa. Protokollasta on yleisesti käytössä versio neljä (TCPv4). TCPv4-protokolla on luotettava yhteydellinen protokolla, joka sisältää vuonhallinnan, multipleksoinnin ja datan kapseloinnin. Protokollan tehtävänä on tarjota kahden päätelaitteen välille luotettava yhteydellinen tiedonsiirtokanava alemman kerroksen protokollan ominaisuuksista riippumatta. (Anttila 2001: 133–135; Parziale ym. 2006: 149–151.)



Kuva 7. TCPv4-yhteyden periaatekuva (Parziale ym. 2006: 150).

TCPv4-protokolla vastaanottaa ylempien verkkokerroksien protokollilta informaatiota ja paketoi sen itsenäisesti sopivan kokoisiin TCPv4-segmentteihin, jotka protokolla toimittaa alemmalle verkkokerrokselle edelleen käsiteltäväksi. Paketoinnin yhteydessä protokolla numeroi jokaisen paketoimansa oktetin. TCPv4-yhteyden toimintaperiaate on esitetty kuvassa 7. TCPv4-protokolla on vuorovaikutuksessa ylempien verkkokerrosten kanssa TCP-porttien välityksellä. (Anttila 2001: 134; Parziale ym. 2006: 150–151.)

Jokaisella TCPv4-segmentillä on järjestysnumero, joka määräytyy sen sisältämän ensimmäisen oktetin perusteella. Protokolla lähettää jokaisen segmentin mukana tiedon sen järjestysnumerosta ja pyytää vastaanottajalta kuittauksen (ACK). Vastaanottaja kuittaa lähetyksen lähettämällä ACK-viestin, joka sisältää tiedon vastaanottajan odottaman seuraavan segmentin järjestysnumerosta. Segmentti lähetetään uudestaan, mikäli vastaanottaja ei lähetä kuittausta ennalta määrätyssä ajassa. Uudelleenlähetyskäytäntö riippuu

TCPv4-protokollan toteutuksesta; jossain tapauksissa uudelleen lähetetään vain viimeisimmässä ACK-viestissä ilmaistu segmentti ja joissain sekä ilmaistu segmentti että kaikki sen jälkeen lähetetyt kuittaamattomat segmentit. Vastaanottaja järjestää segmentit järjestysnumeroiden perusteella ja poistaa tarvittaessa päällekkäisen informaation. (Anttila 2001: 134; Parziale ym. 2006: 151, 161–162.)

Multipleksointi toteutetaan TCPv4-protokollassa TCP-porttien avulla. Yksittäinen TCPv4-pino kykenee hallitsemaan useita samanaikaisia yhteyksiä erottelemalla yhteydet eri portteihin. Porttinumeroita on käytettävissä 2^{16} kappaletta. (Anttila 2001: 135, 139; Parziale ym. 2006: 151.)

TCPv4-yhteyttä muodostettaessa molemmat osapuolet neuvottelevat muun muassa käytettävistä porttinumeroista ja oktettien järjestysnumeroinnista ennen varsinaista tiedonsiirtoa. Osapuolten välille muodostuu looginen yhteys, joka puretaan tiedonsiirron päätyttyä molemminpuolisesti. Yhteydet yksilöidään käytettävien porttinumeroiden ja IPv4-osoitteiden perusteella. (Anttila 2001: 135; Parziale ym. 2006: 151.)

Porttinumero muodostaa yhdessä IPv4-osoitteen ja käytetyn protokollan kanssa niin sanotun Socket-rajapinnan, joiden avulla yhteydet voidaan yksilöidä tilanteissa, joissa tietyn päätelaitteen tiettyyn sovellukseen on useita samanaikaisia yhteyksiä useammalta asiakaslaitteelta (Anttila 2001: 141–143; Parziale ym. 2006: 145–146).

Edellä kuvatusta yhteyden muodostumisperiaatteesta johtuen TCPv4-protokolla on niin sanottu yhteydellinen protokolla (Anttila 2001: 135). TCPv4-protokolla toimii Full Duplex -periaatteella, joten dataa voidaan siirtää molempiin suuntiin samanaikaisesti (Parziale ym. 2006: 151).

5.3.3. User Datagram Protocol (UDP)

User Datagram Protocol on IETF:n standardi numero kuusi (IETF STD 6) ja se on määritelty RFC 768 -dokumentissa. UDP-protokollan perustehtävä on informaation välittäminen ja se on yleinen TCP/IP-toteutuksissa, joissa siirretään pieniä tietoliikennepaketteja tai siirrettävän informaation satunnaiset

virheet eivät ole merkityksellisiä. UDP-protokollasta on käytössä sen ensimmäinen versio (UDPv1). (Parziale ym. 2006: 146.)

UDPv1 on hyvin yksinkertainen protokolla ja se on periaatteessa vain sovellusrajapinta IPv4-protokollalle. Yksinkertainen rakenne tekee protokollasta hyvin tehokkaan. Protokolla täydentää IPv4-protokollan tarjoamia palveluita lisäämällä multipleksauksen, joka on toteutettu TCPv4-protokollan tapaan porttien (*UDP-portit*) avulla. (Anttila 2001: 167; Parziale ym. 2006: 147.)

5.4. TCP/IP-protokollapinon haavoittuvuudet

TCP/IP-verkkojen tietoturvaongelmien taustalla on Keaninin (2005: 13) mukaan pääsääntöisesti sekä itse TCP/IP-protokollapinoon että sitä käyttäviin ohjelmistoihin liittyvät ongelmat.

Protokollapinon tietoturvaongelmat johtuvat suurilta osin siitä, että TCP/IP-protokollapinoa ei ole suunniteltu alun perin tarjoamaan tietoturvapalveluita, vaan ajatuksena on ollut, että tietoturvaratkaisut toteutetaan verkkoa käyttävissä sovelluksissa ja päätelaitteissa (Harris & Hunt 1999: 896; Keanini 2005: 13).

Ohjelmistojen osalta ongelmia tuottaa sovellusten jatkuva monimutkaistuminen, joka kasvattaa suoraan potentiaalisten suunnittelu-, toteutus- sekä määrittelyvirheiden lukumäärää (Harris ym. 1999: 897; Keanini 2005: 13).

TCP/IP-arkkitehtuurin haavoittuvuuksia voidaan hahmotella varsin hyvin käyttämällä kerroksittaista lähestymistapaa. Tarkoitukseen sopii OSI-mallin mukainen kerrosjako, koska sen avulla voidaan kohdentaa haavoittuvuudet hieman TCP/IP-mallin omaa kerrosjakoa yksityiskohtaisemmin. (Reed 2003.)

TCP/IP-protokollapinon tietoturvahaavoittuvuuksia on käsitelty OSI-mallin mukaisilla kerroksilla liitteessä 1.

6. TIETOLIIKENNEVERKKOJEN SUOJAUSMENETELMIÄ

Tietoliikenneverkkojen tietoturvaan voidaan vaikuttaa merkittävästi verkon arkkitehtuurilla, käytettävillä verkkolaitteilla ja -protokollilla. Tässä luvussa esitellään joitakin tietoturvaa parantavia suojausmenetelmiä.

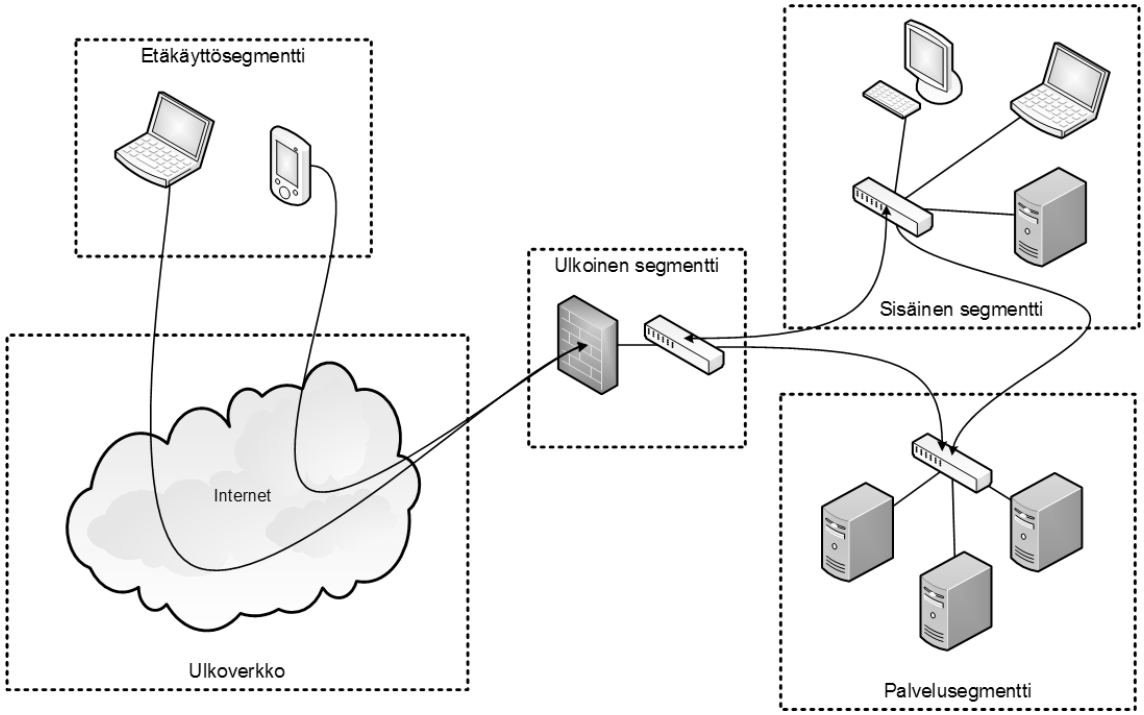
6.1. Verkon arkkitehtuuri

6.1.1. Verkon segmentointi

Verkon segmentoinnilla voidaan vaikuttaa merkittävästi tietoverkon kokonaistietoturvaan. Segmentoinnilla voidaan vähentää tietoturvauhkien kokonaismäärää ja rajata yksittäisten haavoittuvuuksien vaikutusta. Segmentoinnin ajatuksena on jakaa verkko useisiin pienempiin osiin, ryhmitellä verkon palvelut loogisesti eri segmentteihin ja kontrolloida segmenttien välisiä yhteyksiä. Yleisperiaate verkon jakamisessa ja palveluiden ryhmittelyssä on sijoittaa kaikki palvelut ja järjestelmät, joilla on erilaiset tietoturva- ja liikennöintivaatimukset omiin verkkosegmentteihin. (Pfleeger ym. 2006; Young 2001; Maley 2001: 6–7; CCNA Notes 2010; LINFO 2005; Laaksonen, Nevasalo & Tomula 2006: 182.)

Alateeq (2005) käsittelee pienten organisaatioiden verkkojen segmentointia ja toteaa optimaaliseksi verkon jakamisen neljään segmenttiin. Hänen mukaansa verkko tulee jakaa ulkoiseen segmenttiin, palvelusegmenttiin, sisäiseen segmenttiin ja etäkäyttäjille tarkoitettuun verkkosegmenttiin (Alateeq 2005).

Palvelusegmentistä käytetään yleisesti nimeä DMZ-alue ja se muodostaa Alteeqin mallissa yhdessä sisäisen segmentin kanssa organisaation sisäverkon. Sisä- ja ulkoverkko on yhdistetty toisiinsa ulkoisen segmentin avulla. Etäkäyttösegmentti sijoittuu mallissa sisäverkon ulkopuolelle ja yhteydet sieltä sisäverkkoon kulkevat ulkoisen segmentin kautta. Alateeqin malli on esitetty kuvassa 8.



Kuva 8. Verkon jakaminen segmentteihin (Alateeq 2005).

Alateeqin mallissa ulkoinen segmentti sisältää laitteet, jotka ovat suorassa yhteydessä julkiseen verkkoon. Palvelusegmenttiin sijoitetaan verkkopalvelut, joihin tulee saada yhteys julkisesta verkosta ja muista verkkosegmenteistä. Sisäinen segmentti sen sijaan sisältää organisaation työasemat ja sisäiseen käyttöön tarkoitetut verkkopalvelut. Etäkäyttösegmentti on mallissa varattu etäkäyttäjien yhteyspisteille. (Alateeq 2005.)

Mallissa tietoliikenne eri segmenttien välillä on tarkasti rajattua ja kontrolloitua. Ensimmäinen ja ehkä merkittävin kontrollipiste on ulko- ja sisäverkon rajalla. Ulkoisessa segmentissä olevien verkkolaitteiden vastuulla on sallia vain erikseen määritelty liikenne ulko- ja sisäverkon välillä. Palvelusegmenttiin sallitaan liikenne kaikista verkkosegmenteistä, mutta vain määrättyihin palveluihin. Tietoliikenne palvelusegmentistä ulospäin on pääsääntöisesti estetty. Sisäinen segmentti on mallissa kaikkein tarkimmin eristetty muista ja sinne sallitaan vain tarkasti määritelty liikenne, jota on esimerkiksi tietty ulkoisen segmentin kautta tuleva suojattu etäyhteysliikenne. Sisäisestä segmentistä sallitaan ulospäin vain määritelty liikenne palvelusegmenttiin ja ulkoiseen segmenttiin. Etäyhteyssegmenttiin sallitaan tuleva liikenne vain

ulkoverkosta ja sieltä sallitaan vain suojattu lähtevä liikenne ulkoisen segmentin kautta sisäiseen segmenttiin. (Alateeq 2005.)

Yleisesti organisaation koon kasvaessa myös sen tietoliikenneverkko laajenee ja monimutkaistuu, jolloin myös verkkosegmenttien optimaalinen lukumäärä kasvaa yli neljän varsin nopeasti. Tietoturvanäkökulmasta laajassa tietoverkossa on tärkeää sijoittaa esimerkiksi verkkolaitteet omaan verkkosegmenttiinsä (Laaksonen ym. 2006: 183). Vaikka Alateeqin malli on laadittu erityisesti pienille organisaatioille ja yksinkertaisiin tietoliikenneverkkoihin, sen perusperiaatteet ovat sovellettavissa myös suurten organisaatioiden monimutkaisiin tietoverkkoihin.

Verkko voidaan segmentoida sekä fyysisellä että loogisella tasolla. Fyysisen tason segmentoinnissa verkko jaetaan fyysisiin segmentteihin siten, että kaikki segmenttiin kuuluvat solmut ovat fyysisesti yhteydessä toisiinsa. Loogisen tason segmentointi ei sen sijaan vaadi segmentin solmujen välille fyysistä yhteyttä. Loogisen tason verkkosegmenttejä kutsutaan yleisesti virtuaalisiksi lähiverkoiksi eli Virtual Local Area Network (VLAN) -verkoiksi. (Laaksonen ym. 2006: 183; IEEE 802.1Q 2003.)

Teknisesti verkon fyysinen segmentointi voidaan toteuttaa reitittimillä, kytkimillä, silloilla, keskittimillä tai toistimilla. Vaativampi loogisen tason segmentointi toteutetaan pääosin reitittimillä ja osittain kytkimillä. (CCNA Notes 2010; LINFO 2005.)

Yksinkertaisimmillaan verkko voidaan segmentoida OSI-mallin fyysisellä kerroksella käyttäen keskittimiä tai toistimia. Fyysisellä kerroksella tehdyn segmentoinnin avulla voidaan hallita ja vähentää verkkoon kohdistuvia fyysisen tason tietoturvauhkia ja -haavoittuvuuksia. (CCNA Notes 2010.)

Kehittyneempi vaihtoehto on segmentoida verkko OSI-mallin siirtoyhteyskerroksella kytkimien tai siltojen avulla. Siirtoyhteyskerroksella verkkoliikennettä ja siten myös tietoturvauhkia sekä -haavoittuvuuksia voidaan hallita huomattavasti fyysistä kerrosta monipuolisemmin. Kytkimet ja sillat kykenevät ohjaamaan tietoliikennettä kohde- ja lähdeosoitteiden (*MAC*-

osoitteet) perusteella, jolloin verkkoliikenne on mahdollista ohjata sallittuihin segmentteihin tai hylätä kokonaan. (CCNA Notes 2010.)

Verkko voidaan segmentoida myös verkkokerroksella reitittimien avulla. Koska reititin toimii kytkimiä ja siltaa korkeammalla verkkokerroksella, se tarjoaa niitä monipuolisempia mahdollisuuksia verkkoliikenteen hallintaan. Tietoliikennettä voidaan hallita muun muassa MAC-osoitteiden lisäksi IP-osoitteiden avulla. Segmenttien hallintaan käytettäviä reitittimiä nimitetään yleisesti palomuureiksi. (CCNA Notes 2010.)

6.1.2. Tärkeiden palveluiden toisintaminen

Pfleeger ym. (2006) mukaan tietoliikenneverkon ja organisaation toiminnan kannalta tärkeitä palveluita tarjoavat verkkosolmut tulee toisintaa. Toisintaminen voidaan toteuttaa joko pitämällä ensisijaisen solmun rinnalla toissijaista verkkosolmua, joka otetaan käyttöön ensisijaisen solmun vikaantuessa tai kahdella rinnakkaisella verkkosolmulla, joista toisen vikaantuessa palveluvastuu siirtyy toiselle. Tietoturvanäkökulmasta toisintamisen avulla voidaan rajata tietoturvauhkien ja -haavoittuvuuksien vaikutusta ja parantaa tiedon saatavuutta. (Pfleeger ym. 2006.)

6.2. Palomuuri

Bellovin & Cheswick (1994) määrittelevät palomuurin olevan useista yksittäisistä komponenteista koostuva järjestelmä, joka on sijoitettu kahden tietoliikenneverkon väliin. Verkkojen välinen liikenne ohjataan palomuurin kautta ja sen tehtävänä on päästää läpi vain tietty sallittu tietoliikenne. Palomuurin tulee lisäksi olla mahdollisimman immuuni tietoturvahyökkäyksille. (Bellovin ym. 1994.)

Parziale ym. (2006: 795) mainitsee palomuurin olevan komponentti, jonka avulla verkko voidaan jakaa kahteen tai useampaan tietoturvaltaan eritasoiseen verkkoon.

Palomuurit käyttävät yleisesti neljää perusmenetelmää tietoliikenteen kontrollointiin. Palveluvalvonnan (*Service Control*) avulla määrätään, mitkä palvelut ovat sallittuja, yhteyssuunnan valvonta (*Direction Control*) määrää, mistä suunnasta tulevat palvelupyynnöt hyväksytään, käyttäjävalvonnan (*User Control*) avulla hallitaan, kuka mitäkin palvelua voi käyttää ja sisällönvalvonta (*Behavior Control*) määrittelee, miten palveluita voidaan käyttää. (Smith 1997; Kerttula 1998: 249.)

Palomuurin kaksi perustehtävää ovat pääsynvalvonnan suorittaminen ja tapahtumien seuranta. Muihin palomuurin tehtäviin voivat kuulua muun muassa Network Address Translation (NAT) -tekniikalla toteutetut osoitteenmuunnostoiminnot ja VPN-toiminnot. (Kerttula 1998: 244; Stallings ym. 2008: 275–276.)

Pääsynvalvonnassa on kyse tietoliikenteen valvomisesta ja kontrolloinnista. Palomuuri tarkkailee tietoliikennepaketteja sekä avoimia yhteyksiä, vertaa kerättyä informaatiota palomuurille asetettuihin sääntöihin ja päättää, mitkä tietoliikennepaketit sallitaan, ja mitkä estetään. Palomuuri selvittää ainakin paketin lähde- ja kohdeosoitteet, käytetyn protokollan sekä lähde- ja kohdeporttien numerot. (Kerttula 1998: 244–245; Stallings ym. 2008: 276.)

Tapahtumien seurannassa palomuuri kerää ja ylläpitää informaatiota sen kautta kulkeneesta sekä sallitusta että estetystä tietoliikenteestä. Tiedon avulla voidaan selvittää mahdollisia tietoturvahyökkäyksiä. (Kerttula 1998: 246.)

Palomuurit jaetaan toimintaperiaatteen perusteella yleisesti neljään ryhmään, joita ovat tilattomat pakettisuodatinpalomuurit (*Packet Filtering Firewall*), tilalliset pakettisuodatinpalomuurit (*Stateful Inspection Firewall*), sovellustason yhdyskäytävät (*Application-level Gateway*) ja piiritason yhdyskäytävät (*Circuit-level Gateway*). (Stallings ym. 2008: 276–283.)

6.2.1. Tilattomat pakettisuodatinpalomuurit

Tilaton pakettisuodatinpalomuuri toimii verkkokerroksella ja se suodattaa tietoliikennepaketteja pakettien otsikoiden sisältämien tietojen perusteella. (Stallings ym. 2008: 276–277; Kerttula 1998: 251–253.)

Tilaton pakettisuodatinpalomuuri ei säilytä yhteyksien tilatietoja, joten se on nimensä mukaisesti tilaton kontrollijärjestelmä. Pakettien suodatus tehdään pelkkien suodatussääntöjen perusteella aiemmista tapahtumista riippumatta eli suodatussäännöt ovat yhteydestä riippumattomia. Suodatusmenetelmää kutsutaan staattiseksi suodatukseksi. (Stallings ym. 2008: 278–280; Pfleeger ym. 2006; Lucas, Henmi, Singh & Cantrell 2006: 105–107.)

Pakettisuodatinpalomuurien merkittävinä etuina Stallings ym. (2008: 279) mainitsee rakenteen yksinkertaisuuden, suodatuksen läpinäkyvyyden ja nopeuden. Palomuurityypin merkittävimmät ongelmat liittyvät palomuurin toimintaperiaatteeseen tarkastella vain alempia verkkokerroksia. Ominaisuudesta seuraa muun muassa se, että palomuurin keräämien lokitietojen analysointi on usein varsin vaikeaa. Tilaton pakettisuodatinpalomuuri ei kykene havaitsemaan verkko-osoitteiden väärentämistä. Lisäksi palomuurin suodatussääntöjen laatiminen on varsin työlästä. (Stallings ym. 2008: 279–280.)

6.2.2. Tilallinen pakettisuodatinpalomuuri

Tilallinen pakettisuodatinpalomuuri käyttää dynaamista suodatusmenetelmää pakettien suodattamiseen eli suodatussäännöt ovat yhteydestä riippuvia. Palomuuri tarkastelee tietoliikennepakettien otsikkotietojen lisäksi kuljetuskerroksen tilatietoja. (Stallings ym. 2008: 280–281; Lucas ym. 2006: 107–108; Pfleeger ym. 2006.)

Tilallisen pakettisuodatinpalomuurin merkittävinä etuina ovat tilattomaan pakettisuodatinpalomuuriin verrattuna muun muassa se, että se tukee olioiden autentikointia ja kykenee havaitsemaan myös ylemmille verkkokerroksille kohdistettuja hyökkäyksiä. (Stallings ym. 2008: 281; Pfleeger ym. 2006.)

6.2.3. Piiritason yhdyskäytävä

Piiritason yhdyskäytävä toimii kuljetuskerroksella ja se on sovelluksesta riippumaton (Stallings ym. 2008: 282; Parziale ym. 2006: 803–804). Piiritason yhdyskäytävästä käytetään myös nimeä Piiritason proxy-palvelin (Stallings ym. 2008: 282).

Yhdyskäytävän toimintalogiikka eroaa huomattavasti pakettisuodatinpalomuureista. Yksinkertaistettuna toiminta voidaan jakaa neljään vaiheeseen. Ensimmäisessä vaiheessa yhdyskäytävä ottaa vastaan asiakkaan yhteyspyynnön, toisessa vaiheessa asiakas autentikoidaan ja asiakkaan valtuudet tarkastetaan, kolmannessa vaiheessa yhteyspyyntö joko hyväksytään tai hylätään. Mikäli yhteys hyväksytään, yhdyskäytävä avaa yhteyden asiakkaan tavoittelemaan kohdepalvelimeen. Kun yhteys kohdepalvelimeen on avattu, siirrytään neljänteen vaiheeseen, jossa yhdyskäytävä toimii datan välittäjänä asiakkaan ja kohdepalvelimen välillä. Yhdyskäytävä ei muokkaa välittämäänsä dataa. (Stallings ym. 2008: 282; Parziale ym. 2006: 798–804.)

Yhdyskäytävä voi autentikoida asiakkaan esimerkiksi salasanan tai verkko-osoitteen avulla. Yhdyskäytävä voi myös suorittaa kryptografisen autentikoinnin. (Parziale ym. 2006: 800.)

Piiritason yhdyskäytävällä on useita merkittäviä etuja muihin palomuuriratkaisuihin verrattuna. Yhdyskäytävä kykenee autentikoimaan sekä käyttäjän että asiakaslaitteen, kontrolloimaan yhteyttä, ylläpitämään kattavaa tapahtumalokia, tarjoamaan välimuistin tietoliikennepaketeille ja hyvän suojauksen heikoille tai viallisille verkkotason toteutuksille. (Stallings ym. 2008: 282–283; Parziale ym. 2006: 803–804; Kerttula 1998: 255–258.)

Eräs merkittävä piiritason yhdyskäytävän heikkous on se, että sen käyttöönotto vaatii usein muutoksia organisaation verkkoympäristöön. Toinen merkittävä heikkous liittyy resurssien käyttöön. Piiritason yhdyskäytävä kuormittaa pakettisuodatinpalomuureja enemmän tietoliikenneverkkoa. (Stallings ym. 2008: 282–283; Parziale ym. 2006: 803–804; Kerttula 1998: 255–258.)

6.2.4. Sovellustason yhdyskäytävä

Sovellustason yhdyskäytävän merkittävin ero piiritason yhdyskäytävään verrattuna on siinä, että sovellustason yhdyskäytävä toimii nimensä mukaisesti sovelluskerroksella ja on täten sovellusriippuvainen. Sovellusriippuvuudesta seuraa, että jokaista sovellusta varten on oltava oma yhdyskäytävä. (Stallings ym. 2008: 282; Parziale ym. 2006: 798–799.)

Yhdyskäytävä toimii siten, että asiakkaan ottaessa yhteyttä se pyytää asiakkaalta autentikointitietoja. Autentikointi voidaan tehdä usealla tavalla. Esimerkiksi etäautentikointina tai pelkällä käyttäjätunnus-salasana-parilla. Autentikoinnin onnistuessa yhdyskäytävä avaa yhteyden asiakkaan pyytämään kohdepalvelimeen. Yhteyden muodostuttua yhdyskäytävä hallitsee kokonaisvaltaisesti tietoliikenneyhteyttä asiakkaan ja kohdekoneen välillä. (Stallings ym. 2008: 282; Parziale ym. 2006: 799.)

Sovellustason yhdyskäytävää kutsutaan joissain yhteyksissä myös Sovellustason proxy-palvelimeksi (Stallings ym. 2008: 282).

Sovellustason yhdyskäytävä sallii vain tukemaansa sovellusta koskevan liikenteen, poimii tietoliikennevirrasta vain sallimansa paketit ja komennot sekä hallitsee tietoliikennevirtaa molempiin liikennöintisuuntiin. (Stallings ym. 2008: 282; Parziale ym. 2006: 799–800.)

Sovellustason yhdyskäytävä tarjoaa piiritason yhdyskäytävään verrattuna lisäetuna tiettyjen sovellusprotokollien kontrolloinnin. Edun vastapainona sovellustason yhdyskäytävän tulee tukea erikseen jokaista sovellusprotokollaa. (Parziale ym. 2006: 801.)

6.3. IDS- ja IPS-järjestelmät

Intrusion Detection System (IDS) -järjestelmät ovat ohjelmistoja, joiden päätehtävänä on analysoida tietoverkon liikennettä ja tunnistaa verkon tietoturvaa, käyttösääntöjä tai sovittuja käytäntöjä uhkaavia tapahtumia. Uhkaaviin tapahtumiin voidaan lukea muun muassa ulkopuolisten tahojen suorittamat hyökkäykset tietoverkon palveluita vastaan ja sallittujen käyttäjien vahingossa tai tahallaan tekemät väärinkäytökset. Ohjelmistot kykenevät ylläpitämään kattavaa lokia havaitsemastaan epätavallisesta tietoliikenteestä ja informoimaan siitä tietoverkon vastuuhenkilöitä. (Scarfone ym. 2007: 21; Pfleeger ym. 2006.)

Intrusion Prevention System (IPS) -järjestelmät ovat ohjelmistoja, jotka toimivat IDS-järjestelmien tapaan, mutta ne pyrkivät pelkän uhkaavien tapahtumien

tunnistamisen lisäksi suorittamaan vastatoimia. Uhkaa voidaan pyrkiä torjumaan useilla eri tavoilla, esimerkiksi muuttamalla automaattisesti tietoverkon tietoturvamäärityksiä tai katkaisemalla olemassa olevia yhteyksiä. (Scarfone ym. 2007: 21–22).

IDS- ja IPS-järjestelmiä on olemassa useita eri tyyppejä eri käyttötarkoituksia varten. Järjestelmät eroavat toisistaan ensisijaisesti siinä minkä tyyppisiä uhkaavia tapahtumia ne kykenevät tunnistamaan ja miten tunnistus tehdään. (Scarfone ym. 2007: 21; Pfleeger ym. 2006.)

Scarfone ym. (2007: 21) esittelee neljä IDS- ja IPS-järjestelmien perustyyppiä. Ensimmäinen perustyyppi valvoo tiettyä tietoverkon segmenttiä tai tiettyjä verkkosolmuja ja analysoi verkko- ja sovellusprotokollien tuottamaa verkkoliikennettä. Toinen perustyyppi on tarkoitettu langattomiin verkkoihin ja se tarkkailee langattoman verkon verkkoprotokollien tuottamaa verkkoliikennettä. Kolmas perustyyppi valvoo koko verkon liikennettä ja pyrkii havaitsemaan epänormaaleja verkkoliikennemääriä sekä niiden taustalla olevia tekijöitä. Scarfone ym. (2007: 21) käyttää kolmannesta perustyypistä nimeä Network Behavior Analysis (NBA). Neljäs perustyyppi on solmupohjainen ja se valvoo yksittäistä verkkolaitetta tai -solmua. (Scarfone ym. 2007: 21.)

Uhkaavien tapahtumien tunnistamismenetelmät voidaan jakaa kolmeen ryhmään. Menetelmät pohjautuvat joko tunnistetietojen etsimiseen, tilalliseen protokollien analysointiin tai poikkeuksien tunnistamiseen. (Scarfone ym. 2007: 22.)

Tunnistetietoihin pohjautuvassa menetelmässä uhkaavia tapahtumia etsitään hakemalla tietoverkon tietoliikenteestä järjestelmän tiedossa olevien uhkien tunnistetietoja. Menetelmän suurin heikkous on siinä, että järjestelmä kykenee havaitsemaan ainoastaan jo aiemmin tunnistettuja hyökkäyksiä ja uhkia. (Scarfone ym. 2007: 22; Pfleeger ym. 2006.)

Poikkeuksien tunnistamiseen pohjautuvassa menetelmässä verkkoliikenteelle määritetään raja-arvot, joiden sisällä verkkoliikenteen katsotaan olevan normaalia. Raja-arvoja rikkovan tapahtuman päätellään olevan tietoturvauhka. Poikkeuksien tunnistamiseen pohjautuva menetelmä voi olla hyvin tehokas

havaitsemaan aiemmin tunnistamattomia uhkia. Menetelmän käytön kannalta merkittävin haaste on verkkoliikenteen raja-arvojen luotettava määrittely. Liian tiukat raja-arvot johtavat väärien hälytysten runsaaseen määrään ja liian löysät rajat todellisten uhkien havaitsemattomuuteen. (Scarfone ym. 2007: 22; Pfleeger ym. 2006.)

Tilalliseen protokollien analysointiin pohjautuvassa menetelmässä käytetään hyväksi yleisesti määriteltyä informaatiota verkkoprotokollien tietoturvallisesta ja kielletystä käytöstä. Informaatiota verrataan toteutuneeseen verkkoliikenteeseen ja pyritään sen perusteella tunnistamaan uhkaavia tapahtumia. Menetelmän ongelmat liittyvät verkkoprotokollien turvallisen käytön määrittelyn vaikeuteen ja laiteresurssien huomattavaan kulutukseen. Kolmas merkittävä ongelma on, että menetelmän avulla ei voida tunnistaa hyökkäyksiä, joissa verkkoprotokollia käytetään sallitulla tavalla, mutta vahingoittamistarkoituksessa. (Scarfone ym. 2007: 22.)

6.4. Julkisen avaimen infrastruktuuri (PKI)

Julkisen avaimen infrastruktuuri koostuu politiikoista, palveluista ja proseduureista. Politiikat määrittelevät säännöt, joiden mukaan kryptografisen järjestelmän tulee toimia ja erityisesti miten salausavaimista sekä muusta arvokkaasta informaatiosta huolehditaan. Proseduurit määräävät miten salausavaimia luodaan, hallitaan ja käytetään. Palvelut sen sijaan toteuttavat proseduureissa ja politiikoissa määritellyt toiminnot. (Pfleeger ym. 2006.)

Julkisen avaimen infrastruktuurista käytetään usein englanninkielistä nimeä Public Key Infrastructure (PKI). Kerttulan (1998: 357) mukaan PKI:n sovelluksia ovat salaus, digitaalinen allekirjoitus ja avaintenhallinta. Julkisen avaimen infrastruktuurin päätarkoituksena on huolehtia salausavaimista ja sertifikaateista (Kerttula 1998: 357).

Julkisen avaimen infrastruktuuriin kuuluu muun muassa julkisen avaimen sertifikaatit, varmentajat, sertifikaattien säilytyspaikka, sertifikaattien kumoaminen, salausavainten varmuuskopiointi ja tarvittaessa palauttaminen, tuki digitaalisten allekirjoitusten kiistämättömyydelle, automaattinen

avainparien ja sertifikaattien päivitys, avainhistorian ylläpito, tuki ristiinvarmennukselle sekä varmenteiden välittäminen. (Kerttula 1998: 357–358.)

Kerttula (1998: 357) mainitsee PKI:n tärkeimpänä ominaisuutena läpinäkyvyyden. Läpinäkyvyydellä tarkoitetaan, että järjestelmä operoi salausavaimia ja sertifikaatteja informaation salauksessa ja digitaalisessa allekirjoituksessa käyttäjältä näkymättömissä. (Kerttula 1998: 357.)

Eräs julkisen avaimen infrastruktuuri on International Telecommunication Union (ITU) -järjestön tietoliikennealan standardointisektorin (ITU-T) määrittelemä X.509, joka on myös ISO-standardi 9594-8. Standardi määrittelee viitekehyksen yksinkertaiselle ja vahvalle autentikoinnille sekä julkisen avaimen sertifikaateille ja attribuuttisertifikaateille. Attribuuttisertifikaatti on varmenne, joka liittää yhteen identiteetin ja identiteettiin liittyvät ominaisuudet. Standardin uusin versio on X.509 v3. (ITU-T X.509 2006; Chokhani, Ford, Sabett, Merrill & Wu 2003: 3–4.)

6.5. Tietoliikenneyhteyksien salaaminen

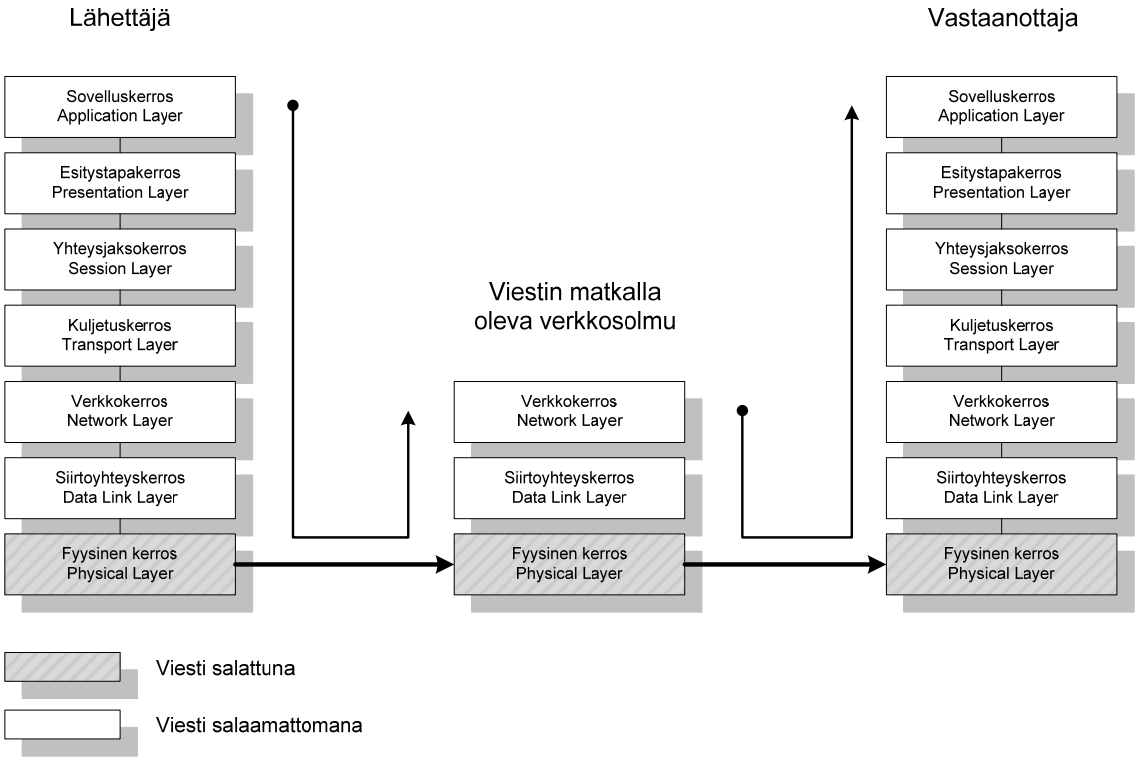
Tietoliikenneyhteyksien salaaminen parantaa oikein käytettynä tietoverkkojen tietoturvaa merkittävästi. On kuitenkin huomattava, ettei paraskaan salausmenetelmä välttämättä paranna kokonaistietoturvaa, mikäli verkon perusrakenteessa on olennaisia tietoturvahaavoittuvuuksia tai -puutteita. Toinen huomioitava asia on, että salausta käytettäessä merkittävimmät haavoittuvuudet liittyvät tiedon käsittelyyn sekä ennen salausta että salauksen purkamisen jälkeen. Kolmas huomio liittyy salausavaimien hallintaan; salausmenetelmien heikoin lenkki on yleisesti salausavaimet ja ennen kaikkea niiden hallinta. Heikko salausavain tekee kehittyneestäkin salausmenetelmästä helposti haavoittuvan. (Pfleeger ym. 2006.)

Tietoliikenneverkoissa salausta voidaan käyttää joko kahden verkkosolmun välisen yhteyden salaamiseen tai niissä suoritettavien ohjelmistojen välisien yhteyksien suojaamiseen (Pfleeger ym. 2006). Ensin mainitusta tapauksesta

Pfleeger ym. (2006) käyttää nimeä Link Encryption (*linkkitason salaus*) ja jälkimmäisestä End-to-end Encryption (*sovellustason salaus*).

6.5.1. Linkkitason salaus -menetelmä

Linkkitason salaus -menetelmässä tietoliikenne salataan ja puretaan siirtoyhteys- tai verkkokerroksella (Pfleeger ym. 2006). Kuvassa 9 on esitetty periaatekuva menetelmästä.



Kuva 9. Periaatekuva linkkitason salaus -menetelmästä (Pfleeger ym. 2006).

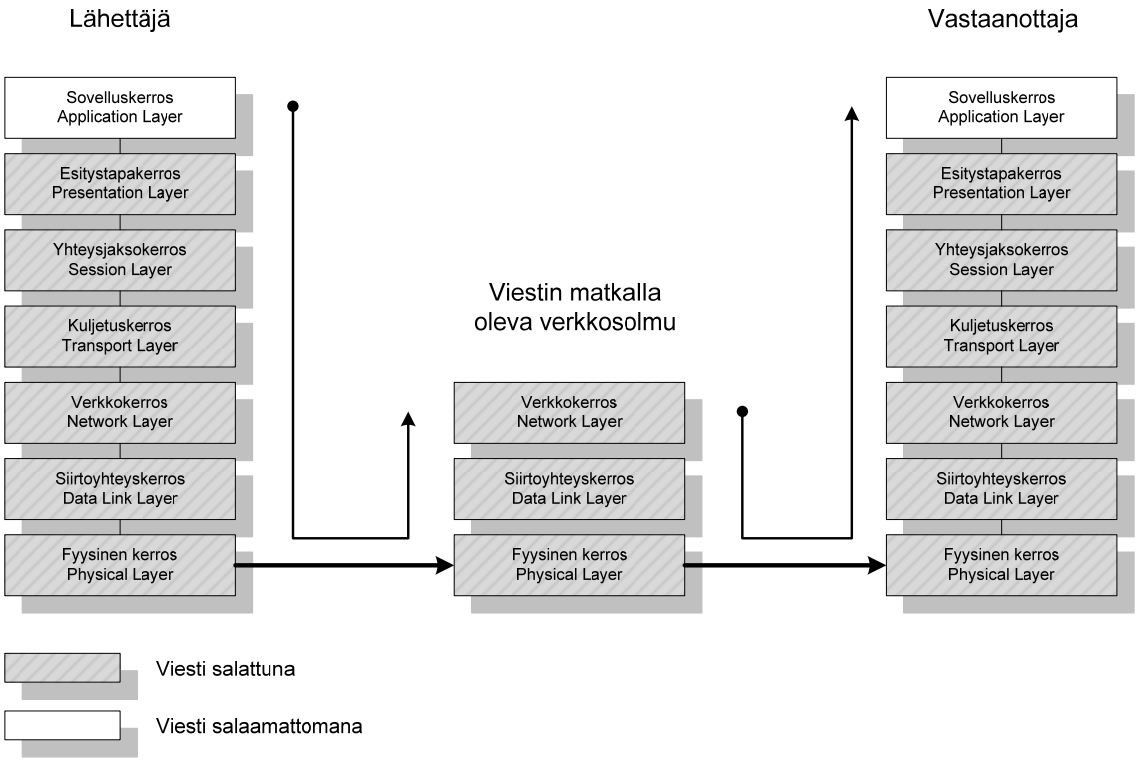
Kuvasta voidaan havaita, että menetelmässä suojataan data vain tiedonsiirron osalta. Informaatio näkyy suojaamattomana fyysisen kerroksen tai siirtoyhteyskerroksen yläpuolisissa verkkokerroksissa. Hyökkääjän onkin mahdollista päästä käsiksi suojaamattomaan informaatioon varsin yksinkertaisesti esimerkiksi ohjaamalla tietoliikenne vihamielisen solmun kautta. (Pfleeger ym. 2006.)

Linkkitason salaus on käyttäjän, ja mikäli käytetään laitteistopohjaista salausta myös operaattorin sekä käyttöjärjestelmän näkökulmasta näkymätöntä. Kun salaus ja purku suoritetaan siirtoyhteyskerroksella, siirrettävät tietoliikennepaketit salataan kokonaisuudessaan joitakin siirtokerroksen otsikkotietoja lukuun ottamatta. Mikäli salaus ja purkaminen suoritetaan verkkokerroksella, siirrettävät tietoliikennepaketit salataan kokonaisuudessa siirtoyhteyskerroksen otsikkotietoja ja joitakin verkkokerroksen otsikkotietoja lukuun ottamatta. Linkkitason salaus sopii erityisesti tilanteisiin, joissa tietoverkko on tiedonsiirtokanavaa lukuun ottamatta turvallinen. (Pfleeger ym. 2006.)

Mikäli linkkitason salausta käyttävällä solmulla on vain yksi liityntäpiste tietoverkkoon, se joutuu salaamaan kaiken solmusta lähtevän tietoliikenteen. Seurauksena myös vastaanottavan solmunkin tai liikennettä edelleen välittävän solmun on tuettava samaa salausmenetelmää purkaakseen vastaanotetun paketin tai toimittaakseen sen eteenpäin. Ellei vastaanottava tai välittävä verkkosolmu tue käytettyä salausmenetelmää, paketti joudutaan joko lähettämään uudelleen salaamattomana tai hylkäämään. (Pfleeger ym. 2006.)

6.5.2. Sovellustason salaus -menetelmä

Sovellustason salaus -menetelmässä tietoliikenne salataan jo sovelluskerroksella (Pfleeger ym. 2006). Kuvassa 10 on esitetty periaatekuva sovellustason salauksesta.



Kuva 10. Periaatekuva sovellustason salaus -menetelmästä (Pfleeger ym. 2006).

Menetelmässä lähettävän ja vastaanottavan sovelluksen väliin muodostuu salattu looginen yhteys, jonka yli kulkeva informaatio puretaan vasta vastaanottavassa sovelluksessa. Informaatio kulkee siis koko matkan suojattuna. (Pfleeger ym. 2006.)

Menetelmää käytettäessä solmujen välillä siirrettävät tietoliikennepaketit salataan ainoastaan varsinaisen datan osalta. Paketin otsikkokenttiä ei salata. (Pfleeger ym. 2006.)

Sovellustason salaus antaa korkeantason suojan hyökkäyksiä vastaan. Hyökkääjä voi päästä käsiksi salaamattomaan tietoon ainoastaan seuraamalla kohdesolmun sovelluskerroksella kulkevaa dataa, mikäli oletetaan, että käytössä olevaa salausta ei voida purkaa. Sovelluskerroksen informaation kaappaaminen vaatii käytännössä vihamielisen koodin suorittamista kohdesolmussa.

Koska End-to-end Encryption -menetelmässä tietoliikennepaketin otsikkokenttiä ei salata eikä varsinaista viestiä pureta ennen vastaanottavaa verkkosolmua, niin paketin reitillä olevien solmujen ei tarvitse tukea paketin salaukseen käytettyä salausmenetelmää (Pfleeger ym. 2006).

Sovellustasolla tehtävä salaus voidaan toteuttaa joko ohjelmisto- tai laitteistopohjaisena. Ohjelmistopohjaisen salauksen merkittävin etu laitteistopohjaiseen salaukseen nähden on, että se antaa huomattavasti enemmän liikkumavaraa sen suhteen, missä tapauksissa ja mihin paketteihin salausta käytetään. (Pfleeger ym. 2006.)

Sovellustasolla tehtävän salauksen olennainen etu linkkitason salaukseen nähden on siinä, että sitä käytettäessä kaikkea lähtevää liikennettä ei tarvitse salata. Merkittävin heikkous liittyy salausavaimiin. Sovellustason salauksessa jokaisen käyttäjäparin välille muodostetaan looginen yhteys, ja uniikkeja salausavaimia pitää tällöin olla vähintään yksi käyttäjää kohden, kun linkkitason salauksessa avaimia tarvitaan vain yksi solmuparia kohden. (Pfleeger ym. 2006.)

Sovellustason salausta voidaan Pfleeger ym. (2006) mukaan haluttaessa täydentää linkkitason salauksella.

6.5.3. Virtuaalinen yksityisverkko (VPN)

Linkkitason tai sovellustason salausta ja autentikointia hyödyntämällä voidaan luoda niin sanottuja virtuaalisia yksityisverkkoja (*Virtual Private Network*). Virtuaalisista yksityisverkoista käytetään yleisesti nimeä VPN-verkko. VPN-tekniikan perusajatuksena on muodostaa suojattu looginen yhteys kahden luotetun verkkosolmun välille epäluotettavan tietoverkon yli. (Pfleeger ym. 2006; Kerttula 1998: 228–229; Parziale ym. 2006: 862–863; Lucas ym. 2006: 212–213; Stallings ym. 2008: 288.)

Muodostettua loogista yhteyttä nimitetään usein VPN-tunneliksi. VPN-verkkojen yhteydessä puhutaan usein myös datan tunneloinnista, jolla tarkoitetaan datan siirtämistä VPN-tunnelin yli. (Kerttula 1998: 233–234.)

VPN-tekniikan avulla voidaan yhdistää yksittäisten verkkosolmujen lisäksi kokonaisia tietoverkkoja toisiinsa. Tekniikan avulla alla olevan tietoliikenneverkon rakenne voidaan piilottaa VPN-verkon osapuolilta. VPN-verkon solmut kokevatkin kuuluvansa samaan fyysiseen verkkoon, vaikka solmujen välinen liikenne voi todellisuudessa kiertää useiden ulkopuolisten tietoliikenneverkkojen kautta. (Pfleeger ym. 2006; Kerttula 1998: 228–229; Lucas ym. 2006: 212.)

VPN-tekniikan merkittävimpinä etuina perinteisiin kiinteisiin yhteyksiin verrattuna Lucas ym. (2006: 213) mainitsee joustavuuden ja alhaisemmat kokonaiskustannukset. Lisäetuna Kerttula (1998: 232) nostaa esiin VPN-tekniikan mahdollistavan yhtenäisemmän verkkoarkkitehtuurin. Kustannussäästöt voivat olla jopa 30–80 prosenttia kiinteisiin yhteyksiin verrattuna, kun yhteydet muodostetaan VPN-tekniikalla julkisen tietoliikenneverkon yli (Lucas ym. 2006: 213). Tekniikan joustavuuden myötä muun muassa uusien yhteyksien luominen ja vanhojen sulkeminen on huomattavasti nopeampaa ja helpompaa kiinteisiin yhteyksiin verrattuna.

VPN-verkko voidaan rakentaa useilla eri tavoilla. Verkon yhteydet voidaan toteuttaa esimerkiksi erillisillä yleiskäyttöisillä palomuureilla, erikoistuneilla VPN-reitittimillä tai tavallisissa palvelimissa suoritettavilla VPN-ohjelmistoilla. Myös yhteyksien tunnelointiprotokollaksi on useita vaihtoehtoja. Protokollasta riippuen tunnelointi voidaan tehdä esimerkiksi siirtoyhteys-, verkko- tai esitystapakerroksella. (Lucas ym. 2006: 213–214; Stallings ym. 2008: 288–289.)

Edellä mainittujen tekijöiden lisäksi VPN-yhteyden terminointipisteet ovat miltei vapaasti valittavissa. Terminointipisteellä tarkoitetaan paikkaa, jossa VPN-tunneli päättyy ja tunneloitu data puretaan. Terminointipiste voi sijaita esimerkiksi käyttäjän työasemassa tai VPN-reitittimessä. (Lucas ym. 2006: 213–214; Kerttula 1998: 233.)

7. TIETOLIIKENNEYHTEYKSIEN SUOJAUSPROTOKOLLIA

Yleisesti käytössä olevia tietoliikenneyhteyksien suojausprotokollia ovat Secure Sockets Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPsec) ja Secure Shell (SSH).

7.1. Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) -protokolla on Netscape Communications Corporation -yrityksen kehittämä tietoturvaprotokolla. SSL-protokollan versio 1.0 valmistui vuonna 1994, mutta sitä ei virallisesti julkaistu. Virallisia julkaisuja sen sijaan olivat versio 2.0 vuonna 1995 ja versio 3.0 vuonna 1996. (Kaufman ym. 2002: 477–478.)

Myöhemmin SSL-protokollan kehitys- ja standardointivastuu on siirtynyt IETF:lle. Ensimmäinen julkaisu tapahtui vuonna 1999, jolloin IETF julkaisi SSL-protokollan 3. version pohjalta luodun Transport Layer Security (TLS) -protokollan version 1.0, joka on esitelty RFC 2246 -dokumentissa. (Dierks & Allen 1999.)

Koska SSL- ja TLS-protokollat ovat pääperiaatteiltaan samanlaisia, tässä tutkielmassa käydään tarkemmin läpi vain TLS-protokolla.

7.2. Transport Layer Security (TLS)

Transport Layer Security (TLS) -protokolla on IETF:n kehittämä tietoturvaprotokolla. TLS-protokollan uusin versio on 1.2 ja se on esitelty Dierksin ja Rescorlan vuonna 2008 julkaisemassa RFC 5246 -dokumentissa. TLS-protokolla 1.2 on lähtökohtaisesti alaspäin yhteensopiva TLS-protokollan versioiden 1.0 ja 1.1 sekä SSL-protokollan versioiden 2.0 ja 3.0 kanssa. (Stallings ym. 2008: 652; Diersk & Rescorla 2008: 1.)

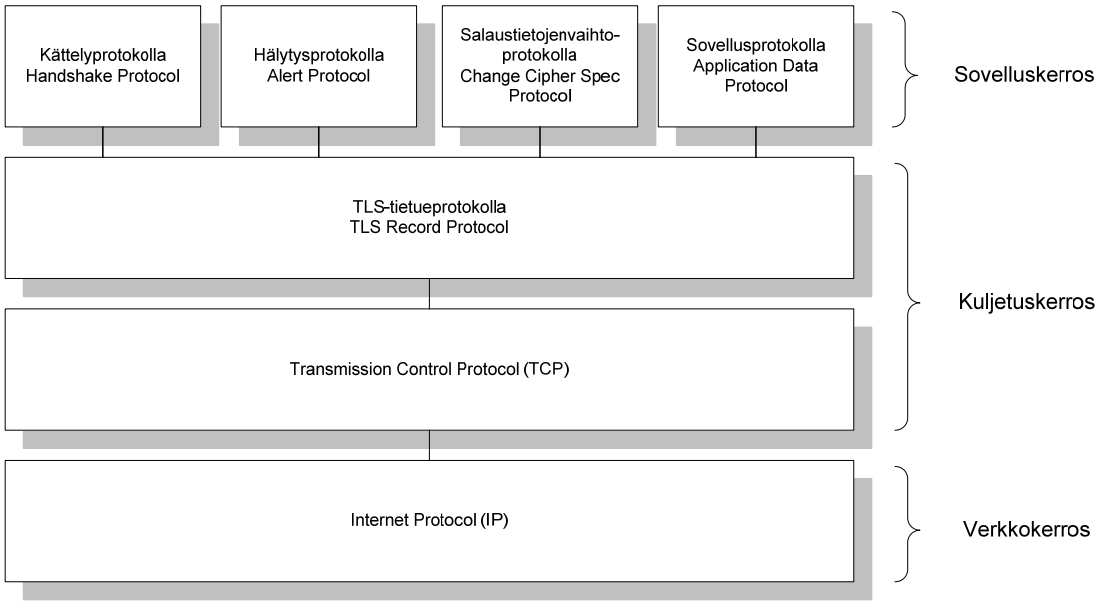
TLS-protokolla toimii TCP/IP-mallin sovellus- ja kuljetuskerroksella (*OSI-mallin yhteysjakso- ja kuljetuskerroksella*). Protokolla kykenee myös paketoimaan dataa OSI-mallin sovellus- ja esitystapakerroksilla. (Lucas ym. 2006: 237–238; Steinberg & Speed 2005).

TLS-protokolla on yleiskäyttöinen kuljetuskerroksen protokollia tiedonsiirtoon käyttävä tietoturvaprotokolla. TLS-protokolla voidaan toteuttaa joko osana taustalla olevaa protokollapinoa tai erillisenä johonkin tiettyyn ohjelmistoon esimerkiksi Internet-selaimeen kuuluvana osana. Ensin mainitulla tavalla toteutettuna TLS-protokolla on sovelluksille läpinäkyvä. TLS-standardi jättää sen yläpuolella toimiville protokollille melko paljon liikkumatilaa. Standardissa ei esimerkiksi määritellä, missä tilanteessa kättelyprotokolla (*Handshake Protocol*) suoritetaan tai kuinka autentikointisertifikaatteja vaihdetaan. (Stallings ym. 2008: 652; Diersk ym. 2008: 3–4.)

Transport Layer Security -protokollan tärkein tehtävä on turvata kahden sovelluksen välinen tiedonsiirtoyhteys. TLS-protokolla jaetaan sisäisesti tietue- ja kättelykerrokseen. (Stallings ym. 2008: 652; Diersk ym. 2008: 3–4; Parziale ym. 2006: 854.)

Tietuekerroksella käytetään TLS-tietueprotokollaa (*TLS Record Protocol*). Ylemmälle kättelykerrokselle sijoittuvat kättelyprotokolla (*Handshake Protocol*), hälytysprotokolla (*Alert Protocol*), salaustietojenvaihtoprotokolla (*Change Cipher Spec Protocol*) sekä sovellusprotokolla (*Application Data Protocol*). Ylemmän tason protokollat käyttävät informaation siirtämiseen alemman tason tietueprotokollaa. (Diersk ym. 2008: 3, 14; Stallings ym. 2008: 652–656; Mäkynen 2007: 18.)

TLS-protokollapino on esitetty kuvassa 11. Kuvassa protokollapino on sijoitettu TCP/IP-mallin mukaisille verkkokerroksille.



Kuva 11. Transport Layer Security -protokollapino (Stallings ym. 2008: 653).

TLS-protokollaan liittyy kaksi olennaista käsitettä, TLS-yhteys ja TLS-istunto. TLS-yhteydet ovat sovellusten välisiä läpinäkyviä tiedonsiirtoyhteyksiä. Jokainen TLS-yhteys on yhdistetty johonkin tiettyyn TLS-istuntoon, joka on yhteys asiakkaan ja palvelimen välillä. TLS-istunnot luodaan kättelyprotokollan avulla, ja niiden avulla määritellään TLS-yhteydessä käytettävät tietoturvaparametrit. Yhteen TLS-istuntoon voidaan yhdistää useita TLS-yhteyksiä, jolloin yhteyksissä käytettävät tietoturvaparametrit voidaan määritellä keskitetysti. (Stallings ym. 2008: 652; Diersk ym. 2008: 15, 80.)

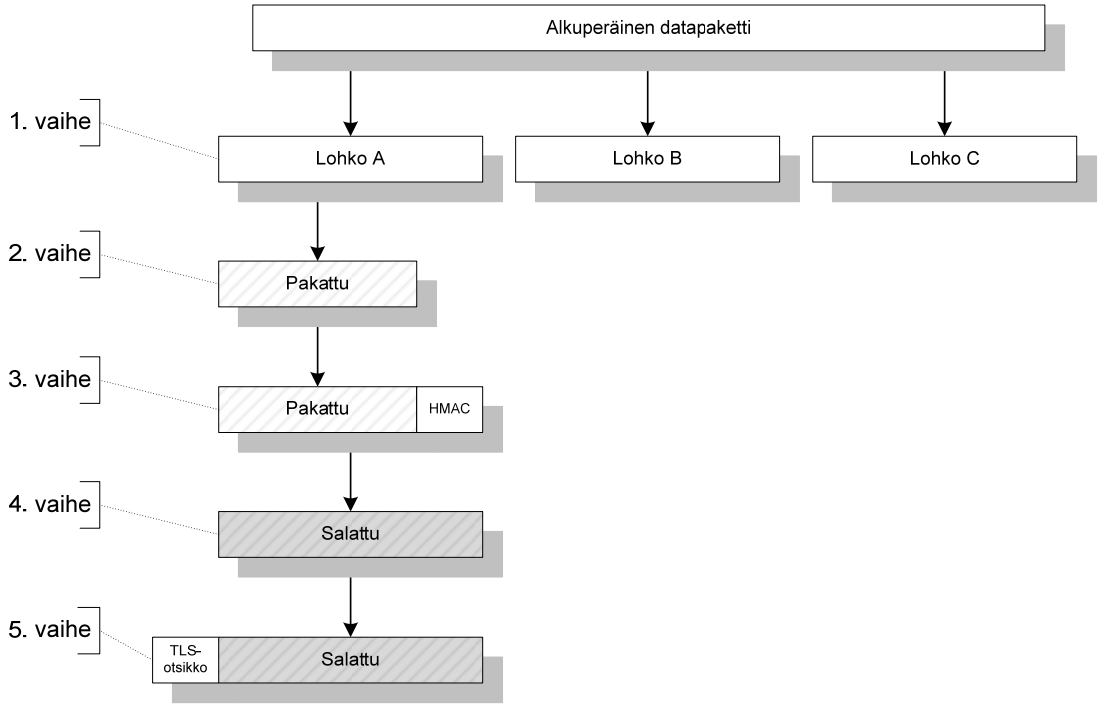
7.2.1. Tietuekerros

Tietuekerroksen TLS-tietueprotokolla toimii jonkin kuljetuskerroksen luotettavan tiedonsiirtoprotokollan päällä ja tarjoaa ylemmän kerroksen protokollille viestinnän salaus- ja autentikointipalveluita, joiden avulla varmistetaan tietoliikenneyhteyden luottamuksellisuus ja eheys. (Stallings ym. 2008: 652; Diersk ym. 2008: 3–4; Parziale ym. 2006: 854.)

Yhteyden luottamuksellisuus varmistetaan salaamalla yhteys symmetrisellä salausmenetelmällä ja eheys käyttämällä HMAC-tiivisteitä. Jokaista yhteyttä varten generoidaan uniikit salausavaimet sekä symmetristä salausta että

HMAC-tiivisteiden laskemista varten. Käytettävät salausavaimet neuvotellaan TLS-kättelyprotokollan avulla. Tietueprotokollaa voidaan käyttää myös ilman salausta ja HMAC-tiivisteitä. (Diersk ym. 2008: 3; Stallings ym. 2008: 653.)

Kuvassa 12 on esitetty tietueprotokollan toiminta vaiheittain dataa lähetettäessä.



Kuva 12. TLS-tietueprotokollan toiminta vaiheittain (Stallings ym. 2008: 653).

Ensimmäisessä vaiheessa sovelluskerrokselta tuleva data pilkotaan maksimissaan 2^{14} tavun lohkoihin. Toisessa vaiheessa lohkot voidaan haluttaessa pakata ja kolmantena vaiheena lohkoille lasketaan HMAC-tiiviste. Neljännessä vaiheessa lohko ja tiiviste salataan symmetrisellä salausmenetelmällä. Viidentenä vaiheena on TLS-otsikon muodostaminen ja lisääminen neljännessä vaiheessa muodostettuun pakettiin. Otsikkotietoina ilmoitetaan muun muassa ylemmän tason protokolla, jolta data on tullut tietueprotokollalle, TLS-protokollan versio ja lohkon koko tavuina. Viimeisessä vaiheessa paketti lähetetään jotain kuljetuskerroksen luotettavaa protokollaa käyttäen. (Diersk ym. 2008: 14–21; Stallings ym. 2008: 653–654.)

Vastaanottaja suorittaa edellä esitetyt vaiheet käänteisessä järjestyksessä; paketin salaus avataan, tiivistefunktiolla laskettua tiivistettä verrataan paketin mukana toimitettuun tiivisteeseen, puretaan mahdollinen pakkaus, yhdistetään lohkot ja lopulta toimitetaan data ylemmän kerroksen protokollalle. (Stallings ym. 2008: 654.)

7.2.2. Kättelykerros

Kättelykerroksen protokollien avulla palvelin ja asiakas neuvottelevat ennen tiedonsiirron aloittamista muun muassa käytettävistä tiivistefunktioista, salausalgoritmeista sekä -avaimista. Lisäksi kättelykerroksen protokollia voidaan käyttää palvelimen ja asiakkaan autentikointiin. Autentikointi voidaan tehdä joko molemminpuolisesti tai siten, että vain toinen osapuoli todennetaan. Diersk ym. 2008: 3.)

Protokollilta vaaditaan kolme perusominaisuutta (Diersk ym. 2008: 3):

- viestinnän osapuolet todennetaan epäsymmetrisen salausmenetelmän avulla
- neuvotteluyhteyden yli siirrettävä salainen tieto ei näy kolmansille osapuolille
- kolmas osapuoli ei voi muokata neuvotteluyhteydessä siirrettävää informaatiota alkuperäisten osapuolien huomaamatta

Salaustietojenvaihtoprotokolla (*Change Cipher Spec Protocol*) on yksinkertaisin kättelykerroksen protokollista. Sen ainoana tehtävänä on informoida yhteyden toista osapuolta siitä, että viestin lähettäjä on valmis ottamaan käyttöön sovitun symmetrisen salausmenetelmän ja istuntoavaimen. (Stallings ym. 2008: 654; Diersk ym. 2008: 26–27.)

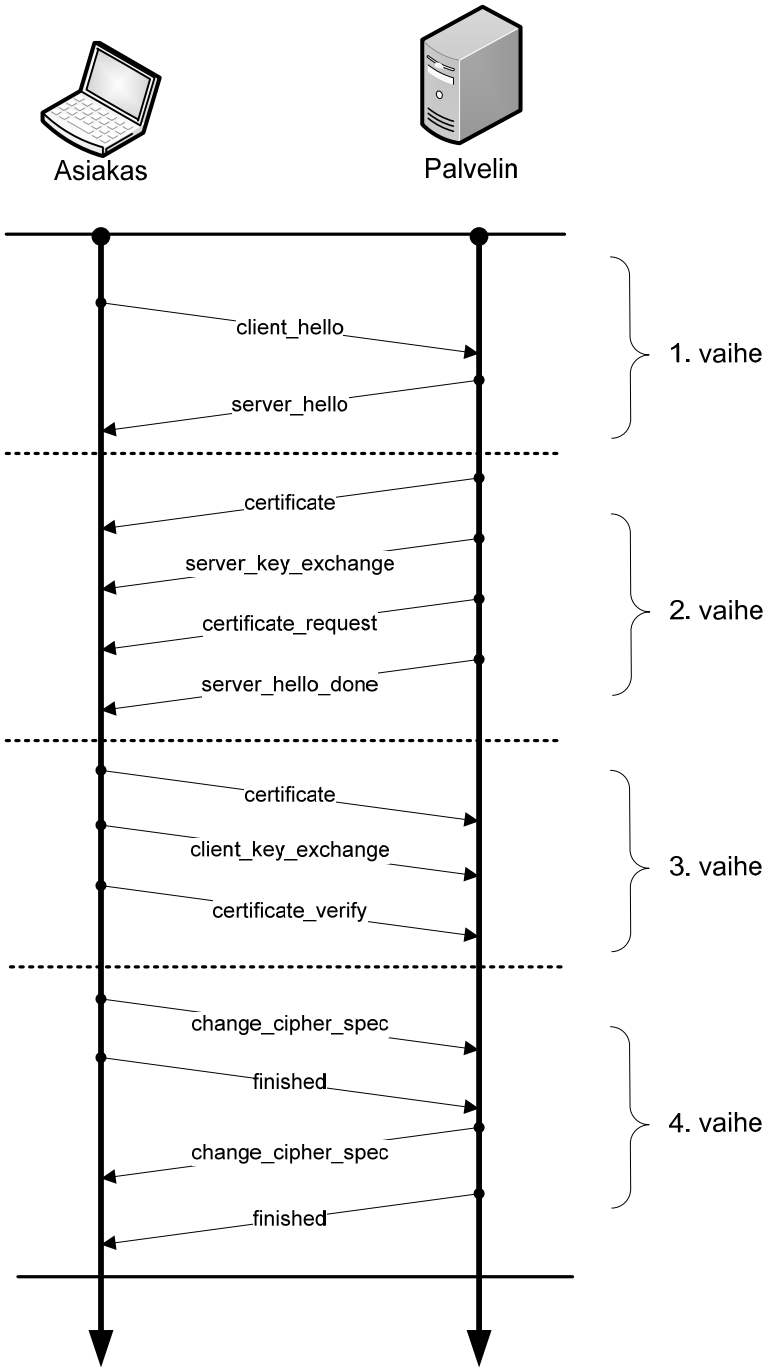
Hälytysprotokollan (*Alert Protocol*) tehtävänä on informoida yhteyden toista osapuolta mahdollisista virhetilanteista. Protokollan lähettämät viestit sisältävät virheen kuvauksen ja arvion sen vakavuudesta kaksiportaisella

asteikolla. Mikäli vastaanotettu viesti on luokiteltu vakavaksi, yhteys suljetaan välittömästi. (Stallings ym. 2008: 654; Diersk ym. 2008: 27.)

Sovellusprotokolla (*Application Data Protocol*) on sovelluskerroksen protokolla, joka käyttää TLS-protokollan tarjoamia palveluita. Yleinen TLS- tai SSL-protokollaa tiedon salaukseen hyödyntävä protokolla on Hypertext Transfer Protocol Secure (HTTPS) -protokolla. HTTPS-protokolla on määritelty RFC 2818 -dokumentissa. (Rescorla 2000.)

Kättelyprotokolla (*Handshake Protocol*) on monimutkaisin kättelykerroksen protokollista. Kättelyssä palvelin ja asiakas sopivat käytettävästä TLS- tai SSL-protokollasta, valitsevat käytettävät salausmenetelmät, mahdollisesti autentikoivat toisensa ja vaihtavat salaista informaatiota käyttäen julkisen avaimen salausmenetelmiä. Yhteyden yli ei voida siirtää dataa ennen kuin kättelyprotokolla on saanut kättelyn suoritettua. (Stallings ym. 2008: 654; Diersk ym. 2008: 32–33.)

Kättelyprotokollan toiminta on esitetty kuvassa 13.



Kuva 13. Kättelyprotokollan toiminta vaiheittain (Stallings ym. 2008: 655).

Protokollan toiminta perustuu viestien välitykseen asiakkaan ja palvelimen välillä. Loogisen yhteyden luonti voidaan jakaa neljään vaiheeseen. (Stallings ym. 2008: 654.)

Ensimmäisessä vaiheessa alustetaan looginen yhteys ja vaihdetaan tietoa tuetuista tietoturvapalveluista. Aloitteen tekee asiakas lähettämällä client_hello-viestin. Viestin mukana toimitetaan istuntotunniste, satunnaisluku, joka koostuu 32 bittisestä aikaleimasta ja 28 tavun mittaisesta satunnaisluvusta, tieto uusimmasta asiakkaan tukemasta TLS- tai SSL-protokollan versiosta sekä tiedot asiakkaan tukemista salaus- ja pakkausmenetelmistä. Viestiin voidaan liitää mukaan myös informaatiota mahdollisesti tarvittavista laajennuksista. Viestin lähettämisen jälkeen asiakas jää odottamaan palvelimelta samat edellä mainitut parametrit sisältävää server_hello-viestiä. Mikäli yhteyden asetuksista ei päästä yksimielisyyteen, palvelin lähettää handshake_failure-viestin ja katkaisee yhteyden. (Stallings ym. 2008: 655–656; Diersk ym. 2008: 33–43.)

Toinen vaihe riippuu käytettävästä epäsymmetrisestä salausmenetelmästä. Kuvan 13 esimerkissä palvelin lähettää asiakkaalle digitaalisen sertifikaattinsa, informaatiota symmetrisen istuntoavaimen luontia varten sekä pyytää asiakasta lähettämään oman sertifikaattinsa. Sertifikaatteina käytetään yleisesti X.509 v3 -standardin mukaisia digitaalisia sertifikaatteja. Vaihe päättyy aina palvelimen lähettämään server_hello_done-viestiin. (Stallings ym. 2008: 656; Diersk ym. 2008: 47–55.)

Kolmas vaihe alkaa asiakkaan vastaanotettua server_hello_done-viestin. Aluksi asiakas tarkastaa aiemmin vastaanotetun server_hello-viestin parametrit ja palvelimen mahdollisesti lähettämän sertifikaatin oikeellisuuden. Mikäli sertifikaatti ja parametrit ovat kelvollisia, jatketaan eteenpäin ja generoidaan varsinaisessa yhteydessä käytettävä istuntoavain. Istuntoavain salataan yleisesti palvelimen sertifikaatin mukana toimitetulla julkisella RSA-avaimella. Asiakas lähettää istuntoavaimen palvelimelle client_key_exchange-viestissä. (Stallings ym. 2008: 656; Diersk ym. 2008: 55–62.)

Muut vaiheessa tehtävät toimet riippuvat käytettävästä salausmenetelmästä. Esimerkissä asiakas lähettää palvelimelle sertifikaattinsa ennen client_key_exchange-viestiä. Vaiheen viimeisenä viestinä asiakas lähettää certificate_verify-viestin, jonka avulla palvelin autentikoi asiakkaan. (Stallings ym. 2008: 656; Diersk ym. 2008: 55–62.)

Neljännessä vaiheessa asiakas lähettää salaustietojenvaihtoprotokollan avulla ensin change_cipher_spec-viestin ja heti sen jälkeen finished-viestin käyttäen aiemmissa vaiheissa sovittua salausalgoritmia, avaimia ja muita ominaisuuksia. Palvelin vastaa lähettämällä change_cipher_spec- ja finished-viestit. Kättely on nyt suoritettu ja symmetrisellä salauksella suojattu looginen yhteys on valmiina käytettäväksi. (Stallings ym. 2008: 656; Diersk ym. 2008: 63–64.)

7.2.3. SSL/TLS VPN

TLS-protokollaa ja sen edeltäjää SSL-protokollaa voidaan käyttää VPN-yhteyksien luomiseen. Protokollien avulla luoduista VPN-yhteyksistä käytetään yleisesti nimitystä SSL/TLS VPN -yhteys. Protokollat huolehtivat viestintäosapuolien autentikoinnista sekä tietoliikenteen salauksesta ja siirtämisestä osapuolten välillä. SSL/TLS VPN -yhteyksien muodostaminen edellyttää viestintäosapuolten välillä tehtävää kättelyä, jonka eteneminen on kuvattu kappaleessa 7.2.2. SSL/TLS VPN -yhteydet suojaavat datan TCP/IP-mallin sovelluskerroksella ja ne käyttävät tiedonsiirtoon sovelluskerroksen HTTPS-protokollaa. (Lucas ym. 2006: 237–238, 243; Steinberg ym. 2005; Rowan 2007.)

SSL/TLS VPN -yhteyksien merkittävin etu liittyy HTTPS-protokollan käyttämiseen. Protokollan myötä VPN-yhteyksien luomiseen riittää pelkkä Internet-selain. Lisäksi, koska HTTPS-protokolla on yleisesti käytetty ja siten myös useissa verkoissa sallittu protokolla, VPN-yhteys voidaan muodostaa miltei mistä vain. SSL/TLS VPN -yhteyksissä tehtävä käyttäjien autentikointi mahdollistaa käyttöoikeuksien joustavan hallitsemisen. Autentikointiin voidaan käyttää lukuisia autentikointimenetelmiä ja -protokollia. (Lucas ym. 2006: 242–243; Stanton 2005; Rowan 2007.)

SSL/TLS VPN -tekniikalla on etujen vastapainoksi joitakin heikkouksia. SSL- tai TLS-protokollia käyttävät VPN-yhteydet kuormittavat runsaasti laiteresursseja, koska sovelluskerroksella tehtävä datan salaaminen joudutaan usein suorittamaan ohjelmistopohjaisena laitteistopohjaisen salauksen sijaan ja väärin muotoillut tai rikkonaiset tietoliikennepaketit joudutaan käsittelemään sovelluskerroksella sen sijaan, että ne hylättäisiin jo alemmilla verkkokerroksilla. Toinen merkittävä ongelma liittyy tekniikan joustavuuteen.

Koska VPN-yhteys voidaan muodostaa miltei miltä tahansa laitteelta ja mistä tahansa verkosta, laitteiden tietoturvasta ei ole mitään takeita. (Lucas ym. 2006: 243–244; Stanton 2005.)

7.3. Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) on IETF:n standardoima IP-protokollan laajennus, joka on osa IP-protokollan 6. versiota (IPv6). IPsec on joukko yleiskäyttöisiä verkkokerroksella toimivia protokollia, joita käytetään IP-liikenteen suojaukseen. IPsec-protokollia voidaan käyttää myös IP-protokollan 4. version yhteydessä (IPv4). IPsec on määritelty RFC 4301 -dokumentissa. (Kent & Seo 2005: 1–5; Pfleeger 2006; Stallings ym. 2008: 656–657; Parziale ym. 2006: 809–810.)

IPsec mahdollistaa viestinnän osapuolten autentikoinnin, viestinnän luottamuksellisuuden ja salausavainten hallinnan vaatimatta merkittäviä muutoksia ylempien tai alempien verkkokerrosten protokolliin. IPsec-protokollat ovat riippumattomia käytettävistä salausprotokollista ja ne antavat TLS- ja SSL-protokollien tapaan viestinnän osapuolten neuvotella käytettävistä salausmenetelmistä sekä muista yhteyden yksityiskohdista. (Pfleeger ym. 2006; Stallings ym. 2008: 657.)

IPsec on käyttäjille ja sovelluksille läpinäkyvä, ja sen avulla voidaan suojata yksittäisiä käyttäjiä tai vaihtoehtoisesti koko verkossa kulkevaa liikennettä käyttämällä IPseciä esimerkiksi verkon reitittimissä tai palvelimilla. IPsec-protokollien avulla voidaan suojata verkkoliikenteen lisäksi epäsuorasti myös verkkolaitteita. (Markham 1997.)

IPseciä voidaan hyödyntää myös verkkojen välisessä reitityksessä. IPsec-protokollat voivat esimerkiksi taata reitittimille tulevan reititysinformaation oikeellisuuden. (Huitema 1998.)

IPsec käyttää tietoliikenteen turvaamiseen Authentication Header (AH) ja Encapsulated Security Payload (ESP) -mekanismeja. Kolmas IPseciin

olennaisesti liittyvä mekanismi on Internet Key Exchange (IKE) -protokolla. (Kent ym. 2005: 9; Stallings ym. 2008: 658; Parziale ym. 2006: 809.)

Authentication Header (AH) -mekanismin avulla voidaan varmistaa datan eheys sekä toteuttaa osapuolten valtuuttaminen ja autentikointi. Encapsulated Security Payload (ESP) sen sijaan mahdollistaa AH:n tarjoamien palveluiden lisäksi datan luottamuksellisuuden. Molemmat turvamekanismit voivat lisäksi toimia kuljetus- tai tunnelointitilassa. (Kent ym. 2005: 9–10.)

Kuljetustilaa käytetään yleisesti tilanteissa, joissa tarvitaan tietoturvallinen yhteys kahden päätepisteen välille. Kuljetustilassa IP-paketti suojataan otsikkotietoja lukuun ottamatta ja tarvittavat IPsec-otsikot lisätään heti alkuperäisten IP-otsikoiden perään. (Kent ym. 2005: 14–15.)

Tunnelointitilassa tietoturvallinen yhteys muodostetaan kahden yhdyskäytävän välille. Tilassa alkuperäiset IP-paketit suojataan kokonaisuudessaan ja paketoidaan uusien IP-pakettien sisälle. IPsec-otsikot lisätään uuden paketin IP-otsikoiden perään ennen alkuperäisen paketin otsikoita. (Kent ym. 2005: 15–16.)

Kuljetus- ja tunnelointitilaa on havainnollistettu kuvissa 14 ja 16.

7.3.1. Turvayhteys (SA)

Kent ym. (2005: 11–12) mainitsevat turvayhteyksien (*Security Association*) olevan IPsecissä olennaisia. Turvayhteys (SA) on yksisuuntainen lähettäjän ja vastaanottajan välinen linkki, joka tarjoaa tietoturvapalveluita linkin yli siirrettävälle tietoliikenteelle. Kaksisuuntaista suojattua tiedonsiirtoa varten tarvitaan kaksi turvayhteyttä. Yksittäisen linkin tietoturvapalvelut toteutetaan joko AH:n ja tai ESP:n avulla. IKE-protokollan tärkein tehtävä liittyy turvayhteyksien luomiseen ja ylläpitämiseen. (Kent ym. 2005: 11–12; Stallings ym. 2008: 659.)

Turvayhteys määrittelee käytettävän salausalgoritmin ja tilan, salausavaimen ja -parametrit, autentikointiprotokollan ja -avaimen, yhteyden keston, yhteyden

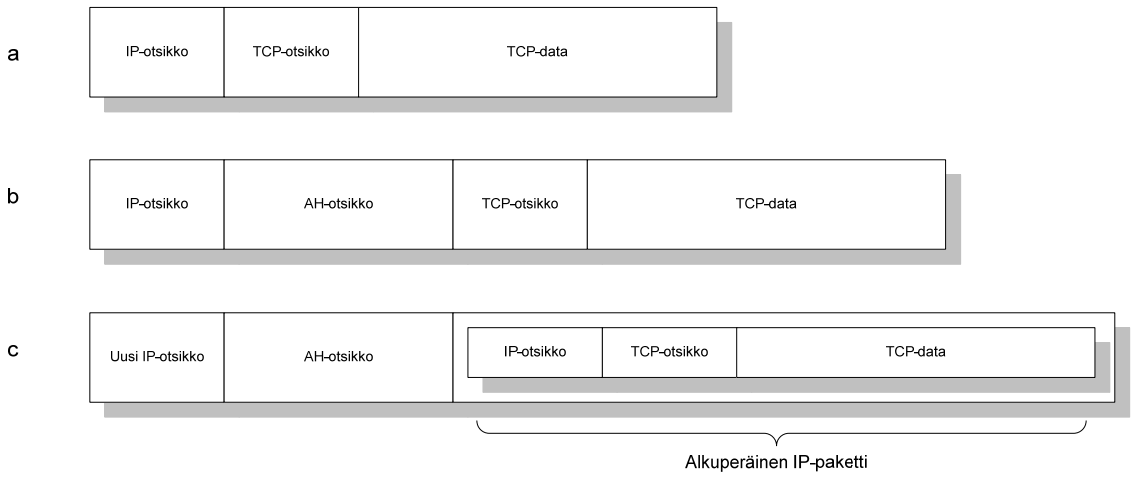
toisen osapuolen IP-osoitteen sekä siirrettävän datan luottamuksellisuuden. (Pfleeger ym. 2006; Kerttula 1998: 222.)

Turvayhteydet voidaan tunnistaa yksiselitteisesti yhteystunnuksen (*Security Parameter Index*), kohteen IP-osoitteen ja käytössä olevan turvaprotokollan avulla. Yhteystunnus (SPI) on tiettyyn turvayhteyteen liitetty tunniste, jolla on ainoastaan paikallinen merkitys. (Stallings ym. 2008: 659; Comer 2000: 585–586.)

7.3.2. Authentication Header (AH)

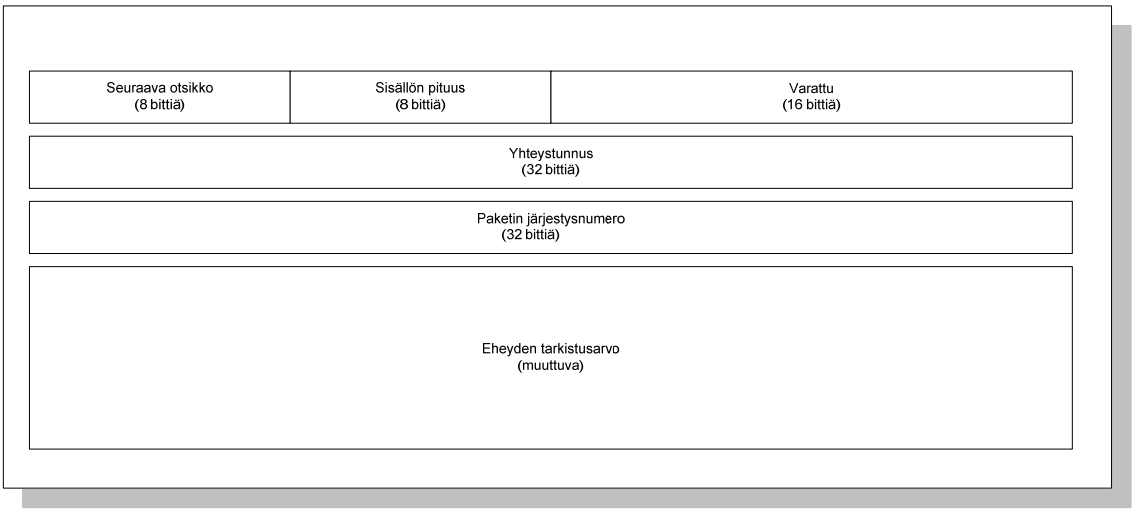
Kerttula (1998: 221) käyttää Authentication Header (AH) -mekanismista suomenkielistä nimitystä autentikointiotsikko. Mekanismin toiminta perustuu alkuperäiseen IP-pakettiin lisättävään AH-otsikkoon, jonka avulla paketin lähettäjä voidaan tunnistaa ja paketin eheys tarkistaa. AH-mekanismi on esitetty IETF:n RFC 4302 -dokumentissa. (Kent 2005a: 2; Stallings ym. 2008: 660.)

Kuvassa 14 on esitetty kolme yksinkertaistettua mallia IPv4-paketista. Ylin (a) kuvaa tavallista pakettia, ja kaksi alempaa paketteja, joihin on lisätty autentikointiotsikko. AH-otsikolla varustetuista paketeista ylempi (b) on kuljetustilassa ja alempi (c) tunnelointitilassa.



Kuva 14. IPv4-paketti autentikointiotsikolla (Comer 2000: 584, 588).

AH-otsikko on esitetty kuvassa 15 ja otsikkokenttien kuvaukset taulukossa 1.



Kuva 15. AH-otsikko (Stallings ym. 2008: 661).

Taulukko 1. AH-otsikoiden kuvaukset (Kent 2005a: 5–9).

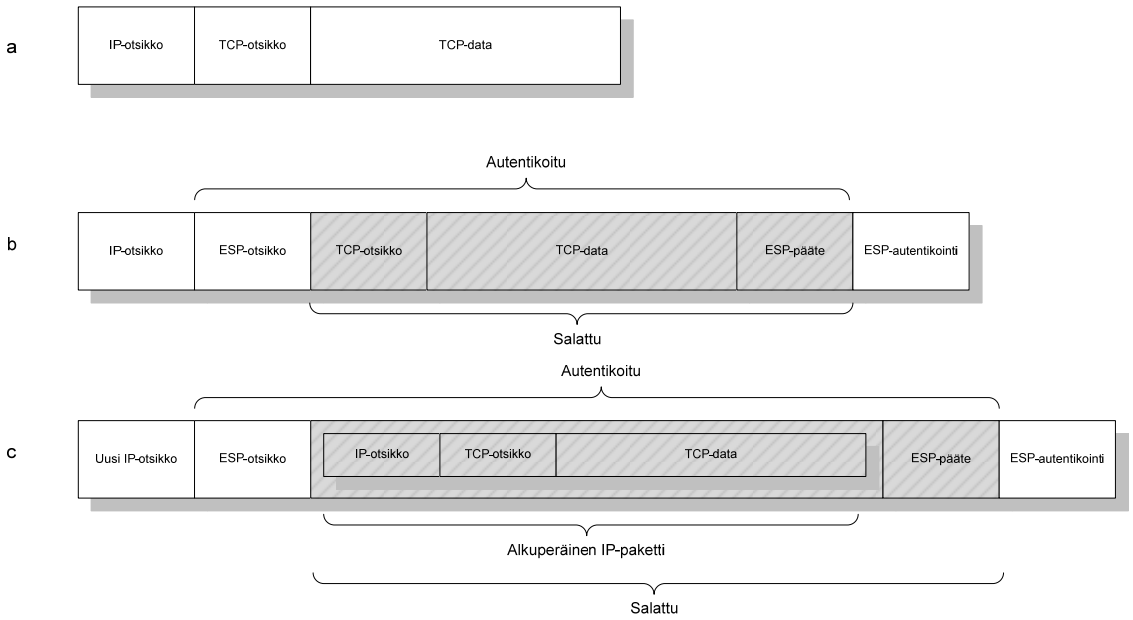
Kenttä	**Koko**	**Kuvaus**
Seuraava otsikko (*Next Header*)	8 bittiä	Osoittaa vastaanottajalle kuljetuskerroksen protokollan otsikkokentän sijainnin paketissa.
Sisällön pituus (*Payload Length*)	8 bittiä	AH-otsikon pituus.
Varattu (*Reserved*)	16 bittiä	Varattu tulevaisuuden käyttöä varten.
Yhteystunnus (*Security Parameter Index*)	32 bittiä	Turvayhteyden tunniste, johon paketti on liitetty.
Paketin järjestysnumero (*Sequence Number*)	32 bittiä	Juokseva paketin järjestysnumero. Voidaan käyttää toistohyökkäysten torjuntaan.
Eheyden tarkistusarvo (*Integrity Check Value*)	Muuttuva	Sisältää ICV-arvon paketin eheyden tarkastamista varten.

7.3.3. Encapsulating Security Payload (ESP)

Kerttula (1998: 221) kutsuu Encapsulating Security Payload (ESP) -mekanismia suomenkielisellä termillä koteloitu salattu data. Mekanismin toiminta perustuu AH:n tapaan IP-pakettiin lisättävään otsikkoon. ESP mahdollistaa myös datan salauksen. ESP-mekanismia voidaan käyttää joko itsenäisesti tai yhdessä AH-

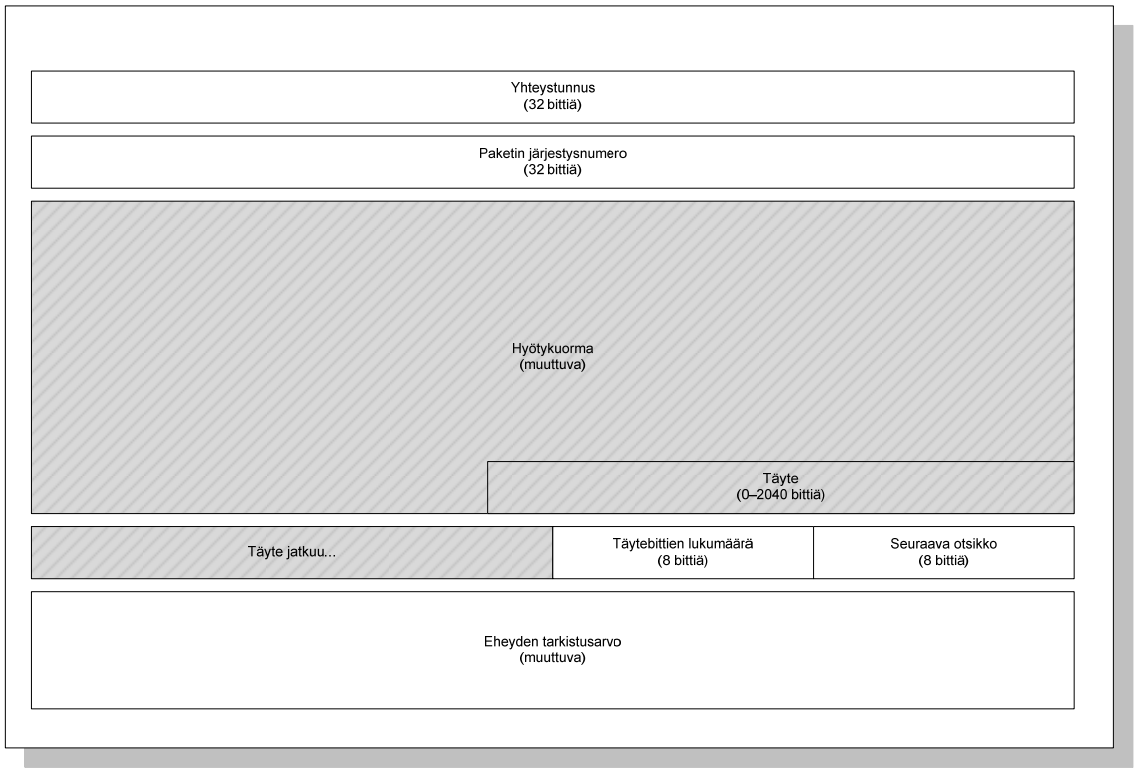
mekanismin kanssa. ESP on esitetty IETF:n RFC 4303 -dokumentissa. (Kent 2005b: 1–4; Parziale ym. 2006: 817–818.)

Kuvassa 16 on esitetty kolme yksinkertaistettua mallia IPv4-paketista. Ylin (a) kuvaa tavallista pakettia ja kaksi seuraavaa paketteja, joihin on lisätty ESP-otsikko. ESP-otsikolla varustetuista paketeista ylempi (b) on kuljetustilassa ja alempi (c) tunnelointitilassa.



Kuva 16. IPv4-paketti ESP-otsikolla (Comer 2000: 586, 588).

ESP-otsikko on esitetty kuvassa 17 ja otsikkokentät on kuvattu tarkemmin taulukossa 2.



Kuva 17. ESP-otsikko (Stallings ym. 2008: 661).

Kuvassa tummennettuna esitetyt osat paketista voidaan salata.

Taulukko 2. ESP-otsikoiden kuvaukset (Kent 2005b: 4–17).

Kenttä	**Koko**	**Kuvaus**
Yhteystunnus (*Security Parameter Index*)	32 bittiä	Turvayhteyden tunniste, johon paketti on liitetty.
Paketin järjestysnumero (*Sequence Number*)	32 bittiä	Juokseva paketin järjestysnumero. Voidaan käyttää toistohyökkäysten torjuntaan.
Hyötykuorma (*Payload Data*)	Muuttuva	Kuljetuskerrokselta tullut paketti. Voidaan salata.
Täyte	0–2040 bittiä	Täytebitit, joilla salattava paketti saadaan käytettävälle salausalgoritmille oikean kokoiseksi tai ylittämään 32 bitin vähimmäisrajan.
Täytebittien lukumäärä (*Pad Length*)	8 bittiä	Käytettyjen täytebittien lukumäärä.
Seuraava otsikko (*Next Header*)	8 bittiä	Kertoo hyötykuormana olevan paketin ensimmäisen otsikon tyypin.
Eheyden tarkistusarvo (*Integrity Check Value*)	Muuttuva	Sisältää ICV-arvon paketin eheyden tarkistamista varten.

7.3.4. Internet Key Exchange (IKE)

IPsec protokolla käyttää avaintenhallintaan yleisesti Diffie-Hellman-menetelmään pohjautuvaa Internet Key Exchange (IKE) -protokollaa. IKE-protokollan 2. versio (IKEv2) on määritelty RFC 4306 -dokumentissa. (Kaufman 2005: 1.)

IKE-protokolla on protokollien Internet Security Association and Key Management Protocol (ISAKMP), Oakley ja SKEME yhdistelmä. IKE tukee turvayhteyksien automaattista neuvottelua sekä avainten päivittämistä ja generointia. (Parziale ym. 2006: 829–830.)

IKE-protokolla autentikoi yhteyden molemmat osapuolet ja luo suojatun turvayhteyden. Viestinnän osapuolet kykenevät vaihtamaan luodun turvayhteyden yli informaatiota ja neuvottelemaan käytettävistä kryptografisista algoritmeista sekä luomaan AH- ja ESP-turvayhteyksiä. (Kaufman 2005: 3–4.)

7.3.5. IPsec VPN

IPsec-protokollia voidaan käyttää VPN-yhteyksien luomiseen. Protokollien vastuulla on tietoliikenteen salaaminen ja siirtäminen. IPsec VPN -yhteyksissä tietoliikenne suojataan verkkokerroksella. IPsec-protokollien avulla voidaan muodostaa verkkojen tai yksittäisten laitteiden välisiä VPN-yhteyksiä. (Rowan 2007; Stanton 2005.)

IPsec VPN -yhteyksien merkittävin etu on riippumattomuus ylemmistä verkkokerroksista. Yhteyden yli voidaan siirtää mitä vain ylemmiltä kerroksilta tulevaa dataa. Toinen merkittävä etu on siinä, että IPsec antaa mahdollisuuden valita käytettävät eheyden varmistus-, salaus- ja autentikointiprotokollat. (Rowan 2007; Stanton 2005; Lucas ym. 2006: 234–235.)

Eräs IPsec VPN -tekniikan heikkouksista on, että VPN-yhteyden käyttäminen vaatii erillisen sovelluksen tai laitteen. Lisäongelmia tuottaa se, että eri laite- ja sovellusvalmistajien tuotteet eivät tavallisesti ole yhteensopivia. Lisäksi IPsec VPN -yhteydet vaativat muutoksia tietoliikenneverkkojen reititys- ja palomuurisääntöihin. (Rowan 2007; Stanton 2005; Lucas ym. 2006: 235–236.)

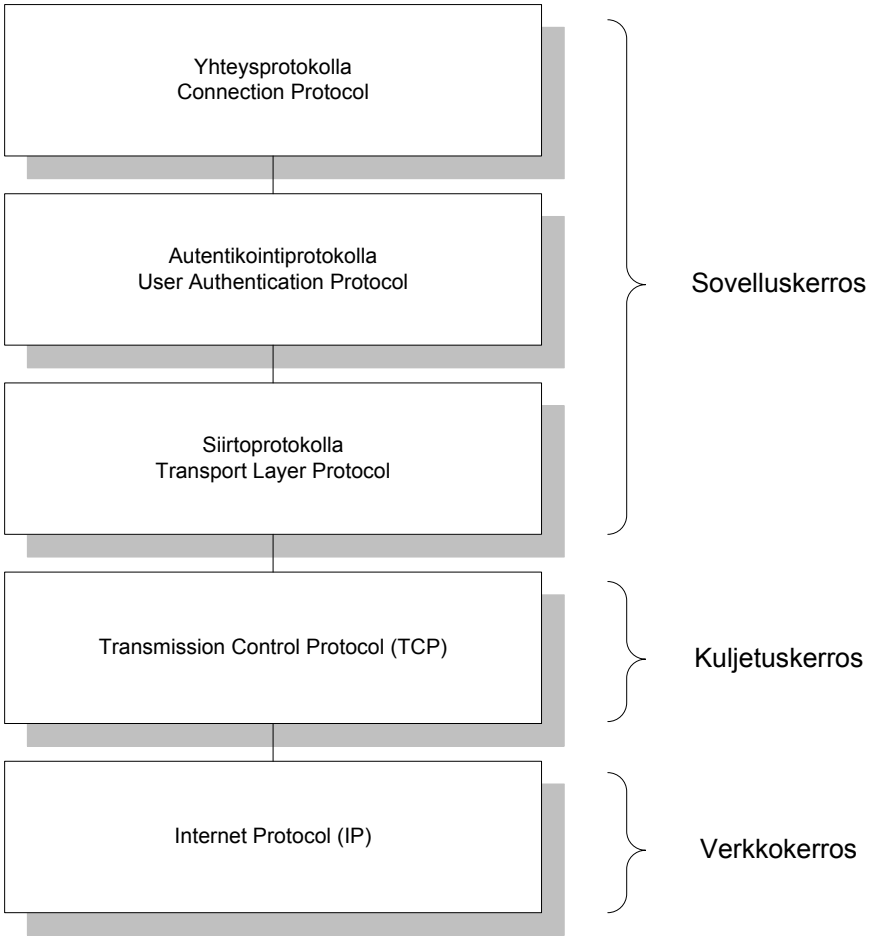
Lisäongelmana Lucas ym. (2005: 236) nostaa esiin IPsec VPN -tekniikan yhteensopimattomuuden NAT-tekniikan kanssa. Rowan (2007) sen sijaan mainitsee IPsecin tunnelointimekanismin tuottavan runsaasti ylimääräistä verkkoliikennettä.

7.4. Secure Shell (SSH)

Secure Shell (SSH) on sovelluskerrokselle sijoittuva protokolla, jonka avulla on mahdollista muodostaa sovelluskerroksella suojattu tietoliikenneyhteys kahden osapuolen välille. SSH on alun perin suunniteltu etäkäyttöprotokollaksi. Protokollan uusin ja yleisimmin käytetty versio on vuonna 1996 julkaistu versio 2.0 (SSH-2). SSH-protokollaa käytetään yleisesti TCP/IP-yhteyksien päällä. (Ylönen & Lonvick 2006: 3–5; Kerttula 1998: 302–303.)

SSH-protokolla koostuu kolmesta pääkomponentista. Siirtoprotokollan (*Transport Layer Protocol*) tehtävänä on palvelimen autentikointi sekä yhteyden luottamuksellisuuden ja eheyden takaaminen. Autentikointiprotokolla (*User Authentication Protocol*) sijoittuu siirtoprotokollan päälle ja sen tehtävänä on työaseman autentikointi palvelimelle. Kolmas pääkomponentti on autentikointiprotokollan päälle sijoittuva yhteysprotokolla (*Connection Protocol*), ja sen tehtävänä on multipleksoida suojattu tunneli useisiin loogisiin kanaviin. (Ylönen ym. 2006: 2; Kerttula 1998: 303.)

Protokollan komponentit ja niiden sijoittuminen TCP/IP-mallin verkkokerroksille on esitetty kuvassa 18.



Kuva 18. SSH-protokollan pääkomponentit (Ylönen ym. 2006).

SSH-protokollaa voidaan käyttää muun muassa suojattujen etähallintayhteyksien muodostamiseen ja tietoliikenteen tunnelointiin. Protokollaa voidaan myös hyödyntää muiden protokollien yhteydessä. Esimerkiksi tiedostojen siirtoon tarkoitetut SSH File Transfer Protocol (SFTP) ja Secure Copy (SCP) -protokollat käyttävät SSH-protokollaa tietoliikenneyhteyksien suojaamiseen. (Kerttula 1998: 302–303.)

8. NYKYTILANTEEN KARTOITUS

8.1. Tutkimusmenetelmä

Tutkimus aloitettiin tunnistamalla ABB Oy:n liiketoimintayksiköt, joilla oli käytössä eniten tietoliikenneyhteyksiä kolmansien osapuolien tietojärjestelmiin tai jotka tarjosivat eniten palveluita kolmansille osapuolille. Käyttötapausten lukumäärää arvioitiin karkeasti diplomityön ohjausryhmän tiedossa olleiden tapausten perusteella. Diplomityön ohjausryhmä koostui ABB Oy:n tietohallintopalveluiden edustajista. Ohjausryhmän kokoonpano on esitetty liitteessä 2.

Tarvekartoitukseen valittiin alustavasti mukaan neljä liiketoimintayksikköä. Valitut yksiköt olivat Drives, Service, Prosessiteollisuus ja Sähkönjakeluautomaatio. Muillekin ABB Oy:n liiketoimintayksiköille varattiin mahdollisuus osallistua tarvekartoitukseen, mutta kartoitukseen mukaan pääsy vaati kyseisiltä yksiköiltä oma-aloitteisuutta.

Tarvekartoituksessa liiketoimintayksiköiden olemassa olevia ja tulevia tarpeita pyrittiin tunnistamaan haastattelemalla ensisijaisesti yksiköiden tietohallintopäälliköitä. Keskusteluissa esiin nousseita liiketoimintatarpeita ja jo olemassa olevia ratkaisuja selvitettiin laajemmin jatkohaastattelujen avulla, jotka kohdistettiin käyttötapauksista vastuussa oleviin työntekijöihin. Drives- ja Sähkönjakeluautomaatio-yksiköiden osalta jatkohaastatteluja käytiin tietohallinnon lisäksi tuotekehityksen edustajien kanssa.

Haastattelujen myötä kartoituksessa mukana olleiden liiketoimintayksiköiden määrä kasvoi kahdella. Mukaan otettiin aiemmin mainittujen yksiköiden lisäksi Motors- ja Sähkökoneet-yksiköt. Varsinaisen tarvekartoituksen jälkeen haastatteluja käytiin myös Muuntajat-yksikön tietohallintopäällikön kanssa.

Haastattelumenetelmänä käytettiin teemahaastattelua, joka sopi joustavana haastattelumenetelmänä hyvin vaikeastikin tunnistettavien tarpeiden kartoittamiseen. Hirsjärvi, Remes & Sajavaara (2008: 200–201) mainitsevat teemahaastattelun etuina, että sen avulla voidaan joustavasti huomioida

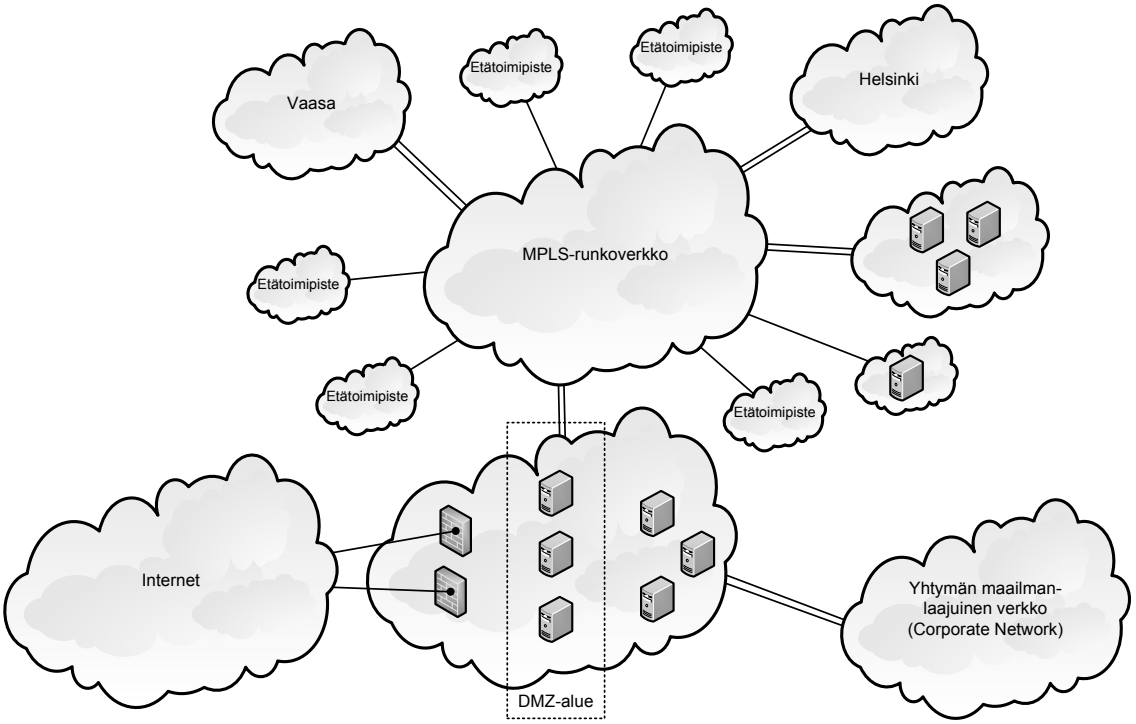
haastateltavat, kerätä informaatiota useissa eri tilanteissa sekä innostaa haastateltavat mukaan haastatteluun. Haastattelumenetelmä antaa lisäksi mahdollisuuden muuttaa haastatteluaiheiden järjestystä ja tehdä tulkintoja (Hirsjärvi ym. 2008: 200–201). Teemahaastatteluissa käsitellyt aihealueet on esitetty liitteessä 3.

Osa haastatteluista tehtiin yksilö- ja osa ryhmähaastatteluina. Pääosa yksilöhaastatteluista ja osa ryhmähaastatteluista toteutettiin puhelinhaastatteluina.

Haastattelujen pohjalta tehtyjen tulkintojen ja tunnistettujen tarpeiden oikeellisuuden varmistamiseksi liiketoimintayksiköille ja haastatelluille henkilöille annettiin mahdollisuus tarkastella ja kommentoida tuloksia ennen niiden jatkokäsittelyä.

8.2. Olemassa olevan tietoliikenneverkon rakenne

ABB Oy:n tietoliikenneverkko koostuu kahdesta pääkampuksesta, muutamasta ulkopuolisesta palveluntarjoajasta sekä noin viidestäkymmenestä etätoimipisteestä. Pääkampukset Vaasassa ja Helsingissä sekä tärkeimmät palveluntarjoajat on kytketty runkoverkkoon kahdennetuilla yhteyksillä. Kuvassa 19 on esitetty yksinkertaistettu kuva yrityksen verkosta. (Taimisto 2010.)



Kuva 19. Periaatekuva ABB Oy:n tietoliikenneverkosta (Taimisto 2010).

Yhteydet Internetiin ja yhtymän maailmanlaajuiseen verkkoon (*Corporate Network*) on toteutettu yhtymälle infrapalveluita tuottavan yhteistyökumppanin kautta. Internet-yhteys on kahdennettu ja suojattu palomuureilla. Lisäksi käytetään NAT-tekniikkaa verkko-osoitteiden muuntamiseen. Sisäverkon tietoliikenne Internetiin kulkee lisäksi sovellustason yhdyskäytävän kautta. Yhteys yhtymän maailmanlaajuiseen verkkoon on kahdennettu. (Taimisto 2010.)

Yhteydet kolmansien osapuolien tietojärjestelmiin on muodostettu Internetin yli. Pysyvämmät yhteydet eli niin sanotut LAN-to-LAN-yhteydet on rakennettu yleisesti yhdyskäytävien välisillä IPsec-protokollia tunnelointiin käyttävillä VPN-yhteyksillä. (Taimisto 2010.)

ABB Oy:n runkoverkko on toteutettu Multiprotocol Label Switching (MPLS) -tekniikalla ja sen hallinta on ulkoistettu ulkopuoliselle palveluntarjoajalle. (Taimisto 2010.)

MPLS-tekniikan avulla voidaan luoda suorituskykyisiä, hyvin skaalautuvia sekä protokollariippumattomia runkoverkkoja. MPLS sijoittuu arkkitehtuurisesti OSI-mallin siirtoyhteyskerroksen ja verkkokerroksen väliin. Tekniikan kantavana ajatuksena on tehostaa tietoliikennepakettien reititystä käyttämällä paketin otsikoiden sijaan niin sanottuja nimilappuja (*Label*). Menetelmässä runkoverkkoon saapuvan paketin otsikkotiedot tarkastetaan ja tietojen pohjalta paketille annetaan nimilappu, jossa määritetään paketin määränpää runkoverkossa ja osittainen tai täydellinen kulkureitti. Paketin saapuessa määränpäähän nimilappu poistetaan ja paketti välitetään runkoverkon ulkopuolelle. MPLS-tekniikan avulla loogisten tunneloitujen yhteyksien luominen on varsin yksinkertaista. (Rosen, Viswanathan & Callon 2001.)

Verkko on segmentoitu kolmeen osa-alueeseen, yhteen DMZ-alueeseen, sisäverkkoon ja ulkoverkkoon. Sisäverkkona käsitellään runkoverkkoon kytkettyjä tietoverkkoja ja yhtymän maailmanlaajuista verkkoa. Ulkoverkkoa ovat kaikki sisäverkon ja DMZ-alueen ulkopuolelle jäävät verkkoalueet. DMZ-alue sijaitsee loogisesti Internetin ja infrapalveluita tarjoavan yhteistyökumppanin tietoverkon rajalla. Palveluntarjoajan hallussa olevien palvelimien lisäksi DMZ-alueeseen voidaan kytkeä myös yksittäisissä toimipisteissä olevia palvelimia. (Taimisto 2010.)

8.3. Tutkimukseen liittyvät riskit ja ongelmat

Merkittävä tutkimukseen liittyvä riski on, että tarvekartoituksessa jää joukko liiketoiminnan kannalta merkittäviä käyttötarpeita tunnistamatta. Riskin toteutuessa työn lopputuloksena saatava ratkaisumalli voi osoittautua jo käyttöönoton yhteydessä perustaltaan puutteelliseksi.

Toinen merkittävä riski liittyy tunnistettujen tarpeiden luokitteluun. Tarpeiden arviointi joudutaan tekemään suurilta osin karkeiden arvioiden ja liiketoimintayksiköistä lähtöisin olevan osittain puolueellisen informaation pohjalta ilman laskettavissa tai muuten tarkasti määritettävissä olevaa vaikutusta yrityksen liiketoimintaan.

8.4. Tunnistetut käyttötarpeet

Tarvekartoituksessa tunnistettiin yhteensä 64 käyttötarvetta, jotka jakaantuivat epätasaisesti kartoituksessa mukana olleiden yksiköiden kesken. Tarpeista 21 kappaletta nousi esiin Sähkönjakeluautomaatio-yksikössä, 4 Motors-yksikössä, 5 Sähkökoneet-yksikössä, 7 Prosessiteollisuus-yksikössä, 19 Drives-yksikössä ja 8 Services-yksikössä. Tunnistetut yksittäiset käyttötarpeet on esitetty liitteessä 4.

Sähkönjakeluautomaatio-yksikön tarpeista viisitoista liittyi ABB:n sisäverkosta alihankkijoille ja asiakkaille tarjottaviin palveluihin. Tarpeita, joihin liittyi yhteyksiä ABB:n sisäverkosta kolmansien osapuolien tietojärjestelmiin, tunnistettiin viisi kappaletta. Yksi tunnistetuista tarpeista vaati yhteyksiä molempiin suuntiin.

Tarvekartoituksessa tunnistetut tarpeet liittyivät Sähkönjakeluautomaatio-yksikön osalta muun muassa hajautetun tuotekehityksen vaatimuksiin, tuotteiden ylläpitoon, komponenttien valmistamiseen, tukipalveluiden tuottamiseen, tuotepäivityksiin, ulkopuolisten konsulttien käyttämiseen sekä asiakkaille tarjottaviin lisäpalveluihin.

Kaikki Motors-yksikön neljä tunnistettua käyttötarvetta liittyivät alihankkijoille tarjottaviin yhteyksiin ABB:n sisäverkon palveluihin. Tunnistetut tarpeet koostuivat alihankkijoille ulkoistetuista tuotannon tuki- ja ylläpitopalveluista.

Sähkökoneet-yksikön viidestä tunnistetusta tarpeesta neljä vaati tietoliikenneyhteyksiä ulkoverkosta ABB:n sisäverkkoon ja yksi vaati yhteyksiä molempiin suuntiin. Tunnistetut käyttötarpeet liittyivät alihankkijoiden kanssa yhteisen työryhmäsovelluksen käyttämiseen, tiedonjakamiseen alihankkijoille ja asiakkaille sekä alihankkijoiden yhteyksiin yksikön väistymässä olevaan toiminnanohjausjärjestelmään.

Prosessiteollisuus-yksikön tarpeista viisi kappaletta liittyi ABB:n sisäverkosta asiakkaiden tietojärjestelmiin muodostettaviin etäyhteyksiin. Tarpeita, joihin liittyi kolmansien osapuolien yhteyksiä ABB:n sisäverkkoon, tunnistettiin kaksi

kappaletta. Tarpeet liittyivät yksikön osalta asiakkaiden käytössä olevien automaatiojärjestelmien tuki- ja ylläpitopalveluihin.

Drives-yksikön tunnistetuista käyttötarpeista kymmenen liittyi asiakkaiden ja alihankkijoiden hallussa olevien tietojärjestelmien käyttämiseen. Kahdeksan käyttötarvetta sitä vastoin liittyi alihankkijoille ja asiakkaille tarjottaviin ABB:n sisäverkon palveluihin. Yksi tarve vaati yhteyksiä molempiin suuntiin. Yksikön tunnistetut tarpeet liittyivät muun muassa hajautettuun tuotekehitykseen, asiakkaalle toimitettujen tuotteiden ylläpitoon, ulkoistettuun komponenttituotantoon sekä ulkopuolisten konsulttien käyttöön.

Service-yksikön tunnistetut yhteystarpeet jakaantuivat liikennöintisuunnan suhteen siten, että viisi yksittäistä tarvetta koski ulkoverkkoon muodostettavia tietoliikenneyhteyksiä ja kolme ABB:n sisäverkkoon avattavia yhteyksiä. Yksikön tarpeet liittyivät asiakkaan tietojärjestelmien etähallintaan ja -valvontaan sekä tiedonsiirtoon asiakkaiden ja alihankkijoiden välillä.

9. AINEISTON RAJAAMINEN

Kaikki tarvekartoituksessa tunnistetut tarpeet kattavan ratkaisun luominen on erittäin monimutkaista ja aikaa vievää. Tutkimukselle on kuitenkin varattu vain rajallinen aikamäärä, joten työssä käsiteltävien tarpeiden joukkoa jouduttiin rajaamaan ja valitsemaan liiketoiminnan kannalta merkittävimmät tarpeet.

Vastuu olennaisten tarpeiden tunnistamisesta ja valinnasta oli ABB Oy:n tietohallinnon johtoryhmällä (*Country IS Board*). Country IS Board on toimielin, joka käyttää korkeinta maatason päätäntävaltaa tietohallintoon liittyvissä asioissa ja se koostuu pääsääntöisesti divisioonatason tietohallintopäälliköistä.

9.1. Rajausprosessi

Rajausprosessin aluksi kaikki tarvekartoituksessa tunnistetut käyttötarpeet yhdistettiin ja niitä tarkasteltiin kokonaisuutena. Seuraavassa vaiheessa samantyyppiset tarpeet ryhmiteltiin tarvekokonaisuuksiksi.

Tarpeiden ryhmittelyssä kiinnitettiin huomiota varsinaisen tarpeen lisäksi siihen liittyviin käyttötapauksiin, yhteyden kohteeseen ja tarvitsijaan sekä liikennöintisuuntaan. Luokittelussa huomioitiin eräänä kriteerinä myös kyseisen tarpeen mahdollinen ratkaisumalli.

Edellä kuvatun luokittelun suurimpana ongelmana oli käyttötarpeiden takana olevien todellisten tarpeiden tunnistaminen. Ongelmia tuotti lisäksi esiin nousseiden tarpeiden laajuus ja samankaltaisuus. Ongelmista johtuen yksiselitteisen ryhmittelyn tekeminen käytettävissä olleessa ajassa osoittautui mahdottomaksi ja luokittelun suhteen jouduttiin tekemään kompromisseja. Täydellisen ja yksiselitteisen ryhmittelyn sijaan tavoitteena oli ryhmitellä tarpeet suuripiirteisesti loogisiin tarvekokonaisuuksiin.

Ryhmittelyn lopputuloksena saatiin 22 tarvekokonaisuutta, joista 15 piti sisällään yhteystarpeita ABB:n sisäverkkoon, viisi ryhmää koostui yhteystarpeista ulkoverkkoon ja kaksi ryhmä piti sisällään tarpeita, jotka

vaativat yhteyksiä sekä sisä- että ulkoverkkoon. Tarvekokonaisuuksiin kuuluvat yksittäiset tarpeet on esitetty liitteessä 4.

Yksiköittäin tarvekokonaisuuksia tarkasteltaessa huomataan Drives- ja Sähkönjakeluautomaatio-yksiköiden tarpeiden muistuttavan pääsääntöisesti toisiaan. Toinen selkeä pari on Service- ja Prosessiteollisuus-yksiköt. Sähkökoneet- ja Motors-yksiköt sen sijaan erottuvat sekä muista että toisistaan selvästi. Diplomityön ohjausryhmän kanssa käytyjen keskustelujen pohjalta voidaan arvioida kartoituksen ulkopuolelle jääneiden yksiköiden muistuttavan joko Motors- tai Sähkökoneet-yksiköitä kolmansien osapuolien yhteyksiin liittyvien tarpeiden osalta.

Sähkönjakeluautomaatio-yksikön tunnistetut tarpeet luokiteltiin kuuluvan 13 eri tarvekokonaisuusryhmään ja Drives-yksikön tarpeiden 12 eri tarvekokonaisuusryhmään. Prosessiteollisuus-yksikön tarpeet kuuluivat viiteen eri ryhmään ja Service-yksikön tarpeet seitsemään tarvekokonaisuusryhmään. Motors-yksikön tarpeet luokiteltiin sisältyvän kolmeen ryhmään ja Sähkökoneet-yksikön tarpeet seitsemään tarvekokonaisuusryhmään.

Muodostetut tarvekokonaisuudet ja niihin kuuluvien yksittäisten tarpeiden esiintyminen eri liiketoimintayksiköissä on esitetty taulukossa 3. Taulukossa yksiköt on merkitty seuraavilla lyhenteillä: Sähkönjakeluautomaatio (DA), Motors (MO), Sähkökoneet (MA), Prosessiteollisuus (PI), Drives (DR) ja Service (SE).

Taulukko 3. Tarvekokonaisuudet ja niihin kuuluvien yksittäisten tarpeiden esiintyminen eri liiketoimintayksiköissä.

Kohde	**Tarvekokonaisuus**	**DA**	**MO**	**MA**	**PI**	**DR**	**SE**
Sisäverkko	Etäyhteydet ABB:n hallussa oleviin laitteisiin tai järjestelmiin		X				
Sisäverkko	Alihankkijoiden yhteydet sisäverkon dokumentti- ja materiaalipankkeihin	X	X	X	X	X	X
Sisäverkko	Asiakkaiden yhteydet sisäverkon dokumentti- ja materiaalipankkeihin	X		X	X	X	X
Sisäverkko	Tuotepäivitysten tarjoaminen asiakkaille	X			X		

Sisäverkko	Alihankkijoiden yhteydet sisäverkon tuotekehitysjärjestelmiin	X				X	
Sisäverkko	Varastojen ja tuotetoimitusten seuranta		X			X	
Sisäverkko	Asiakkaiden yhteydet tilausten seurantajärjestelmään	X				X	
Sisäverkko	Ulkoisten konsulttien tarvitsemat yhteydet					X	
Sisäverkko	Extranet-palvelut asiakkaille ja alihankkijoille			X			
Sisäverkko	Asiakkaiden yhteydet tuoteräätälöinti- ja verkkokauppapalveluihin	X					
Sisäverkko	Tuotetukipalveluiden tarjoaminen asiakkaille	X					
Sisäverkko	Alihankkijoiden ja asiakkaiden käytössä olevien ABB:n tuotteiden lisenssien hallinta ja tarkastaminen	X		X			
Sisäverkko	Tiedonsiirto asiakkaan järjestelmästä ABB:n toiminnanohjausjärjestelmään (Maximo)						X
Sisäverkko	Alihankkijoiden yhteydet ABB:n toiminnanohjausjärjestelmään (DG)			X			
Sisäverkko	ABB:n ja kolmansien osapuolien tietojärjestelmien käyttäminen mobiililaitteilla					X	
Ulkoverkko	Sisäverkossa estettyjen palveluiden tai protokollien käyttäminen	X					X
Ulkoverkko	Etähallintayhteydet asiakkaan hallussa oleviin laitteisiin tai järjestelmiin	X			X	X	X
Ulkoverkko	Etävalvontayhteydet asiakkaan hallussa oleviin laitteisiin tai järjestelmiin	X			X	X	X
Ulkoverkko	Tiedonsiirto asiakkaan ja alihankkijan välillä						X
Ulkoverkko	Yhteydet alihankkijoiden dokumentti- ja materiaalipankkeihin					X	
Ulkoverkko	Yhteydet asiakkaiden dokumentti- ja materiaalipankkeihin						X
Sisäverkko ja ulkoverkko	Tietokantojen synkronointi alihankkijan verkossa olevien tietokantojen kanssa	X		X		X	

Seuraavassa vaiheessa tarvekokonaisuuksia arvioitiin diplomityön ohjausryhmän kanssa. Tavoitteena oli tunnistaa ja valita joukosta akuuteimmat ja merkittävimmät kokonaisuudet. Tarvekokonaisuuksien arvioinnin yhteydessä selvitettiin voidaanko kyseisiä tarpeita ratkaista olemassa olevilla yleisillä ratkaisuilla. Lisäksi selvitettiin, onko tarpeita sivuavia projekteja tai kehityshankkeita käynnissä yhtiössä yhtymän tasolla. Eräänä olennaisena mittarina käytettiin tarvekokonaisuuteen liittyvien tarpeiden esiintymislaajuutta kartoituksessa mukana olleiden liiketoimintayksiköiden piirissä. Arvioinnissa pyrittiin huomioimaan lisäksi eri tarvekokonaisuuksien keskinäisiä riippuvuuksia.

Tarvekokonaisuuksien analyyttisen tarkastelun pohjalta nousi esiin kuusi tarvekokonaisuutta, joista kaksi koostui sisäverkkoon tulevista yhteystarpeista, kolme ulkoverkkoon suuntautuvista yhteyksistä ja yksi molempiin suuntiin yhteyksiä vaativista tarpeista. Merkittävimmiksi tarvekokonaisuuksiksi tunnistetut kuusi kokonaisuutta luokiteltiin vielä ensisijaisiin ja toissijaisiin tarvekokonaisuuksiin. Ensisijaisiksi luokiteltiin neljä kokonaisuutta ja toissijaisiksi kaksi.

Viimeisessä vaiheessa tarvekartoituksessa esiin tulleet tarpeet, määritellyt tarvekokonaisuudet ja arvioinnin lopputulokset esiteltiin tietohallinnon johtoryhmälle. Johtoryhmän tehtävänä oli tunnistaa ja valita jatkokäsittelyyn otettavat tarvekokonaisuudet esityksen pohjalta.

9.2. Olennaiset tarpeet

Liiketoiminnan kannalta olennaisiksi tarvekokonaisuuksiksi valittiin kuusi kokonaisuutta. Ensisijaisia tarpeita ovat alihankkijoiden ja asiakkaiden yhteydet ABB:n sisäverkon dokumentti- ja materiaalipankkeihin (*tarvekokonaisuudet 1 ja 2*) sekä etävalvonta- ja etähallintayhteydet asiakkaan hallussa oleviin laitteisiin tai järjestelmiin (*tarvekokonaisuudet 3 ja 4*). Toissijaisia tarpeita ovat tietokantojen synkronointi alihankkijan verkossa olevien tietokantojen kanssa (*tarvekokonaisuus 5*) sekä tiedonsiirto asiakkaan ja alihankkijan välillä (*tarvekokonaisuus 6*).

9.2.1. Alihankkijoiden yhteydet materiaalipankkeihin

Alihankkijoiden yhteydet ABB:n sisäverkon dokumentti- ja materiaalipankkeihin -tarvekokonaisuus sisältää yksitoista yksittäistä tarvetta, joista neljä on lähtöisin Sähkönjakeluautomaatio-yksiköstä ja kolme Drives-yksiköstä. Muista neljästä yksiköstä löytyi jokaisesta yksi yksittäinen tarvekokonaisuuteen luokiteltu tarve.

Kokonaisuuteen kuuluvat yksittäiset tarpeet liittyvät hajautettuun ohjelmistokehitykseen, komponenttien valmistukseen, tiedonjakamiseen alihankkijoille, markkinointimateriaalin tuottamiseen, materiaalien hankintaan ja varastologistiikkaan, järjestelmien ylläpitoon ja käyttöönottoon sekä testausdatan siirtämiseen.

9.2.2. Asiakkaiden yhteydet materiaalipankkeihin

Asiakkaiden yhteydet ABB:n sisäverkon dokumentti- ja materiaalipankkeihin -tarvekokonaisuus koostuu viidestä yksittäisestä tarpeesta. Jokaisesta kartoituksessa mukana olleesta yksiköstä pois lukien Motors, löytyi yksi yksittäinen kokonaisuuteen luokiteltu tarve tai käyttötapaus.

Yksittäiset tarpeet liittyvät järjestelmien ylläpitoon ja käyttöönottoon sekä tuotetestien tulosten tai muun materiaalin jakamiseen asiakkaille.

9.2.3. Asiakasjärjestelmien etävalvontayhteydet

Etävalvontayhteydet asiakkaan hallussa oleviin laitteisiin tai järjestelmiin -kokonaisuuteen liittyen tunnistettiin seitsemän yksittäistä tarvetta, joista neljä nousi esiin Drives-yksiköstä. Loput kolme jakaantuivat tasan Service-, Prosessiteollisuus- ja Sähkönjakeluautomaatio-yksiköiden kesken. Kaikki yhteystarpeet liittyvät asiakkaan hallussa olevien tuotteiden ja järjestelmien ylläpitoon.

9.2.4. Asiakasjärjestelmien etähallintayhteydet

Etähallintayhteydet asiakkaan hallussa oleviin laitteisiin tai järjestelmiin -kokonaisuuteen luokiteltiin kuuluvan kaksitoista yksittäistä tarvetta. Tarpeista viisi on lähtöisin Drives-yksiköstä, neljä Prosessiteollisuus-yksiköstä, kaksi Sähkönjakeluautomaatio-yksiköstä ja yksi Service-yksiköstä. Kokonaisuuteen kuuluvat tarpeet liittyvät asiakkaan hallussa olevien tuotteiden ja järjestelmien ylläpitoon.

9.2.5. Tietokantojen synkronointi

Sähkökoneet-, Drives- ja Sähkönjakeluautomaatio-yksiköissä esiintyi jokaisessa yksi yksittäinen tietokantojen synkronointi alihankkijan verkossa olevien tietokantojen kanssa -tarvekokonaisuuteen luokiteltu tarve. Tunnistetut tarpeet liittyivät ryhmätyösovellusten käyttämiseen ja testausinformaation siirtämiseen.

9.2.6. Tiedonsiirto alihankkijan ja asiakkaan välillä

Tarvekartoituksessa mukana olleista yksiköistä Service nosti esiin tarpeen välittää informaatiota suoraan asiakkaan ja alihankkijan välillä. Tarpeen taustalla on se, että osa Service-yksikön käyttämistä alihankkijoista on varsin pieniä ja niillä ei välttämättä ole resursseja ottaa käyttöön informaation sähköiseen jakamiseen tarkoitettuja ja ABB:n tietoturvavaatimukset täyttäviä palveluita.

10. OLENNAISTEN TARPEIDEN TOTEUTTAMINEN

Luvussa käsitellään jatkokäsittelyyn valittuja tarvekokonaisuuksia, niiden sisältämiä yksittäisiä tarpeita sekä olemassa olevia ratkaisuja. Lisäksi hahmotellaan ja tarkastellaan mahdollisia yleisiä ratkaisumalleja.

10.1. Alihankkijoiden yhteydet materiaalipankkeihin

Liiketoimintayksiköiden ulkoistaessaan toimintojaan on syntynyt tarve tarjota alihankkijoille pääsy yrityksen sisäverkon materiaali- ja dokumenttipankkeihin. Suorilla yhteyksillä tavoitellaan erityisesti toiminnan tehostumista ja parempaa tietoturvaa verrattuna manuaaliseen materiaalin jakamiseen esimerkiksi sähköpostin avulla.

Materiaalin jakamisen merkittävin ongelma liittyy käytössä olevien taustajärjestelmien monimuotoisuuteen. Eri liiketoimintayksiköt käyttävät useita erityyppisiä tietojärjestelmiä dokumenttien sekä muun materiaalin hallintaan ja jakamiseen. Monimuotoisuus on johtanut resurssien pirstoutumisen ja ongelmiin erityisesti kokonaisuuden hallinnan suhteen.

Tarvekartoituksessa mukana olleet yksiköt käyttävät dokumenttien ja muun materiaalin hallintaan IBM:n Lotus Notes -tietokantoja, Microsoftin SharePoint -sisällönhallintajärjestelmää sekä erinäisiä World Wide Web -pohjaisia sisällönhallintajärjestelmiä. Lisäksi käytetään perinteisiä levyjakoja.

10.1.1. Olemassa olevat käyttötapaukset

Olemassa olevissa ratkaisuissa alihankkijoiden yhteydet on toteutettu Microsoftin Internet Security & Acceleration (ISA) tai IBM:n Lotus Domino Web Access -yhdyskäytävien avulla, VPN-yhteyksinä, File Transfer Protocol (FTP) tai SSH File Transfer Protocol (SFTP) -palvelimien avulla tai joidenkin edellä mainittujen menetelmien yhdistelminä.

Käytetyt ratkaisut tarjoavat useita vaihtoehtoja käyttäjien tunnistamiseen, autentikointiin ja valtuuttamiseen. Esimerkiksi ISA-yhdyskäytävän yhteydessä

käytetään Microsoftin Active Directory Application Mode (ADAM) -palvelimen tarjoamia palveluita.

Ratkaisuista ongelmallisin on tietoturvamielessä FTP-palvelimen ja suoran palomuuriavauksen avulla toteutettu käytäntö, koska tällöin kaikki tietoliikenne on salaamatonta (Lucas ym. 2006: 105). Suojatut tietoliikenneyhteydet voidaan toteuttaa ISA-yhdyskäytävän, VPN-yhteyksien, SFTP-palvelimen sekä Lotus Domino Web Access -yhdyskäytävän avulla (Lucas ym. 2006: 105, 193, 212; Milza & Rogers 2005.)

10.1.2. Yhtenäinen sisällönhallintajärjestelmä

Ensimmäisenä askeleena kohti yhtenäistä ratkaisua on materiaalin hallinnan yhtenäistäminen. Yhtenäisen ratkaisun käyttöönottoon on useita perusteita. Eräs merkittävä etu on, että kaikki tuki- ja hallinnointiresurssit voidaan keskittää yhden järjestelmän ympärille. Keskittäminen johtaa toiminnan tehostumiseen ja siten myös mahdollisiin kustannussäästöihin (Porter 1988; Haverila ym. 2009: 357–358). Tietoturvanäkökulmasta yhteen järjestelmään siirtyminen rajaa hyökkäyspinta-alaa, jolloin tietoturvariskien analysointi ja havainnointi tehostuu (Alateeq 2005; Maley 2001: 4–5). Muutoksen myötä tietoturvariskien hallinta voi muuttua reaktiivisesta ongelmien paikkailusta proaktiiviseksi tietoturvan aidoksi kehittämiseksi (Keanini 2005: 2–3).

ABB on standardoinut yhtymänlaajuiseksi työryhmäsovellusalustaksi Microsoft SharePoint-sovelluksen. Päätöksen myötä yhtymä on sitoutunut järjestelmän käyttämiseen myös tulevaisuudessa ja varannut resursseja järjestelmän käyttöönottoon ja palveluiden kehittämiseen. (ABB 2010c.)

SharePoint on monipuolinen erityisesti yrityskäyttöön suunnattu sisällönhallintajärjestelmä ja sovellusalusta. Järjestelmä on suunniteltu ensisijaisesti Internet-selaimella käytettäväksi ryhmätyöalustaksi ja se tarjoaa muun muassa monipuoliset mahdollisuudet käyttöoikeuksien määrittelyyn. SharePoint-alusta sopii hyvin sekä staattiseen että dynaamiseen dokumenttien jakamiseen ja se käyttää tiedonsiirtoon sovelluskerroksella HTTP- ja HTTPS-protokollia. SharePoint-alustan pohjalla on Microsoft SharePoint Foundation

-teknologia, joka tunnettiin aiemmin nimellä Microsoft Windows SharePoint Services (WSS). (Zachry & McCollum 2007; Microsoft 2010a.)

SharePoint on jo laajamittaisessa käytössä useissa ABB Oy:n yksiköissä, joten käyttöönottokynnys on kattavien käyttökokemusten myötä kilpailevia järjestelmiä alempi. Lisäksi SharePoint-alustan merkittävänä etuna on hyvä yhteensopivuus ABB Oy:n käyttämien muiden Microsoft-tuotteiden kanssa (Zachry ym. 2007; Microsoft 2010a). Esimerkkinä mainittakoon työasemissa käytössä oleva Microsoft Office -toimisto-ohjelmisto. Huomionarvoista on myös se, että joustavan käyttöoikeuksien määrittelyn myötä SharePoint-alustan avulla voidaan antaa tarvittaessa tietyille alihankkijoille muokkaus- ja lisäysoikeudet tiettyihin verkkopalveluihin.

Edellä mainittujen perusteiden myötä SharePoint on suositeltavin valinta yhtenäiseksi sisällönhallintajärjestelmäksi.

SharePoint-verkkopalvelut vaativat toimiakseen Microsoft Windows -palvelinympäristön, jossa on käytettävissä SharePoint Foundation, Internet Information Services (IIS) -WWW-palvelinohjelmisto sekä Microsoftin SQL -tietokantapalvelinohjelmisto. Lisäksi ympäristön tulee tukea .NET ja ADO.NET -ohjelmointirajapintoja. (Microsoft 2010a; Microsoft 2010b.)

SharePoint-alusta mahdollistaa useita erilaisia tapoja ja menetelmiä, joiden avulla alustan päällä toimivat verkkopalvelut voidaan julkaista yrityksen sisäverkon ulkopuolelle. Yksinkertaisimmillaan voidaan käyttää SharePoint-sovelluksen vakiotoiminnallisuuksia ja jakaa vapaasti kaikki verkkopalvelun informaatio suojaamattomana ulospäin. Toisena ääripäänä voidaan mainita erilliseen sovellusyhdyskäytävään perustuva ratkaisu, jossa verkkopalvelun sisältämän informaation käyttöoikeudet on tarkoin määritelty, käyttäjien tunnistaminen, autentikointi ja valtuuttaminen sekä yhteyden suojaaminen toteutetaan sovellusyhdyskäytävän avulla. (Microsoft 2009.)

10.1.3. Materiaalin jakoa koskevia vaatimuksia

Tarkasteltavassa tarvekokonaisuudessa alihankkijoiden kanssa jaettava materiaali on pääsääntöisesti arkaluontoista ja sen suojaukseen tulee kiinnittää

erityistä huomiota. Materiaali tulee suojata siten, että se on ainoastaan sen käyttöön oikeutettujen tahojen saatavissa. Suojauksen tulee ulottua sekä sisällönhallintajärjestelmään että järjestelmän ja alihankkijan välille muodostettuihin tietoliikenneyhteyksiin.

Käsiteltävän materiaalin arkaluontoisuuden lisäksi kokonaisuuteen kuuluvia tarpeita yhdistää se, että yhtäaikaisten yhteyksien lukumäärä on melko pieni ja niiden yli siirrettävät datamassat vähäisiä. Taustalla on se, että yksittäiseen käyttötapaukseen liittyvien alihankkijoiden lukumäärä on kohtuullisen pieni (*maksimissaan kymmeniä*), siirrettävä materiaali koostuu pääasiassa yksittäisistä pienehköistä tiedostoista eikä yhteyksien viiveillä tai kaistanleveydellä ei ole suurta merkitystä.

Siirrettävien datamassojen koosta, yhtäaikaisten yhteyksien lukumäärästä, siirrettävän materiaalin arkaluontoisuudesta sekä yhteyksien viiveille asetuista vaatimuksista johtuen, sopivin menetelmä tietoliikenneyhteyksien suojaamiseen on SSL- tai TLS-protokolla.

SSL- ja TLS-protokollien avulla voidaan varmistaa tietoliikenneyhteyksien korkean tason luottamuksellisuus sekä riittävän tason käytettävyys. Yhteyden yli siirrettävän datamäärän pysyessä kohtuullisena, protokollan käytöstä aiheutuva tietoliikenneverkon ja palvelinten ylikuormitus ei nouse merkittäväksi ongelmaksi. (Beltran, Guitart, Carrera, Torres, Ayguadé & Labarta 2004.)

Koska materiaali on suojattava myös sisällönhallintajärjestelmässä, siinä on oltava mekanismi käyttäjien tunnistamiseen, autentikointiin ja valtuuttamiseen. Alihankkijoiden pienehkö lukumäärä antaa mahdollisuuden hyödyntää lukuisia erilaisia menetelmiä. Yksinkertaisin ja monessa mielessä mielekkäin ratkaisu on käyttää ABB:n yhtymänlaajuista jo olemassa olevaa autentikointipalvelua käyttäjien todentamiseen.

Yhtymän autentikointipalvelun avulla voidaan autentikoida ja valtuuttaa sekä yrityksen työntekijät että ulkopuoliset yhtymänlaajuisesta käyttäjätietokannasta löytyvät käyttäjät. Palvelu on toteutettu Microsoftin Lightweight Directory Access Protocol (LDAP) -hakemistopalveluprotokollaan ja Kerberos-

autentikointiprotokollaan perustuvilla Active Directory (AD) -palveluilla. Käyttäjätietokantana on yhtymänlaajuinen Active Directory -hakemisto ja sitä käytetään LDAP-rajapinnan tarjoavien Active Directory Application Mode (ADAM) -palvelimien kautta. Kaikki palveluun tulevat, lähtevät ja sisäiset yhteydet suojataan sovellustasolla SSL- tai TLS-protokollalla. (Jäggli & Khylenko 2009.)

Windows Server 2008 myötä ADAM on uudelleen nimetty Active Directory Lightweight Directory Services (AD LDS) -palveluksi (Microsoft 2010e).

10.1.4. Vaihtoehtoiset ratkaisumallit

SSL- tai TLS-protokollan avulla suojatut tietoliikenneyhteydet tarjoava ja yhtymän ADAM-autentikointipalvelua käyttävä sisällönhallintapalvelu voidaan toteuttaa SharePoint-alustan omilla komponenteilla. Toinen vaihtoehto on käyttää mallia, jossa yhteyksien suojaaminen tehdään SSL- tai TLS-protokollaa käyttävällä VPN-ratkaisulla ja käyttäjien tunnistaminen, autentikointi sekä valtuuttaminen SharePoint-sovelluksella. Kolmantena vaihtoehtona on käyttää SSL- tai TLS-protokollaa sekä ADAM-autentikointipalvelua tukevaa sovellusyhdyskäytävää, joista esimerkkinä mainittakoon Microsoftin ISA-yhdyskäytävän korvannut Forefront Unified Access Gateway (UAG) -sovellus. Kolmannessa mallissa pääsynvalvonta sekä käyttäjien tunnistaminen, autentikointi ja valtuuttaminen tehdään sovellusyhdyskäytävän avulla, ja tiedot todennuksesta sekä käyttäjän valtuuksista välitetään SharePoint-alustalle. Mallissa sovellusyhdyskäytävä huolehtii yhteyksien suojaamisesta.

Ensimmäisen mallin etuna on ratkaisun yksinkertaisuus; mallissa ei tarvita SharePointin lisäksi muita sovelluksia. Yksinkertaisuus tarkoittaa yleisesti myös edullisia lisenssi- ja laitekustannuksia. Lisäksi erityisesti käyttäjänäkökulmasta etuna on, että palvelun käyttöön riittää pelkkä Internet-selain.

Ratkaisun merkittävimmät heikkoudet liittyvät siihen, että mallissa SharePoint-alustan päällä suoritettavat verkkopalvelut näkyvät suoraan ulkoverkkoon. Palveluiden käyttäjien näkökulmasta ongelmana on se, että jokaiseen palveluun tulee kirjautua eri verkko-osoitteesta. Tietoturvamielessä ongelmallista on

SharePoint-alustassa mahdollisesti piilevät tietoturvaongelmat, joiden vakavuutta korostaa se, ettei mallissa ole raja-aitoja SharePoint-alustan ja ulkoverkon välillä (Wilson 2009).

Toisessa ratkaisumallissa käyttäjät autentikoidaan ja valtuutetaan kahdesti; ensin VPN-yhteyttä muodostettaessa ja sen jälkeen SharePoint-palveluun kirjauduttaessa. Ensimmäiseen malliin verrattuna etuna on, että palvelut eivät näy suoraan ulkoverkkoon vaan välissä on ainakin VPN-yhdyskäytävä.

VPN-yhteyksiin pohjautuvan ratkaisumallin merkittävimmät heikkoudet liittyvät järjestelmän monimutkaistumiseen. Lisäkustannuksia seuraa muun muassa mallin vaatimien VPN-yhteyksien toteuttamisesta. Käyttäjänäkökulmasta ratkaisu on ensimmäistä vaihtoehtoa epämiellyttävämpi. Käyttäjä joutuu erillisten verkko-osoitteiden muistamisen lisäksi käyttämään verkkoselaimen lisäksi erillistä VPN-ohjelmistoa tai -laitetta ja mahdollisesti jopa kirjautumaan yhteyttä muodostettaessa kahteen kertaan.

Sovellusyhdyskäytävään perustuvan ratkaisumallin merkittävin etu on siinä, että ulkoverkkoon näkyy vain yksi ainoa yhteyspiste, jonka kautta käyttäjät ohjataan yksittäisiin verkkopalveluihin. Koska käyttäjien tunnistaminen, autentikointi ja valtuuttaminen sekä yhteyden suojaaminen toteutetaan yhdyskäytävässä, käyttäjät eivät tarvitse palvelun käyttöön pääsääntöisesti kuin Internet-selaimen ja yhden käyttäjätunnus-salasana-parin. (Microsoft 2009.)

Tietoturvanäkökulmasta yhden yhteyspisteen valvonta ja hallinta on sekä yksinkertaisempaa että tehokkaampaa kuin useamman yhteyspisteen. Lisäksi sovellusyhdyskäytävät tarjoavat yleisesti ottaen monipuolisemmat työkalut tietoturvan hallintaan ja valvontaan kuin SharePoint. Eräs erityisesti SSL- ja TLS-protokollien yhteydessä merkittävä useimmista sovellusyhdyskäytäväratkaisuista löytyvä tietoturvan hallintaan liittyvä ominaisuus on tietoliikenneyhteyden muodostamisen yhteydessä tehtävä käyttäjän työaseman tietoturvatarkastus. (Microsoft 2009.)

Mikäli sovellusyhdyskäytävä käyttää tiedonsiirtoon sovelluskerroksella HTTPS-protokollaa, tietoliikenneyhteyksien muodostaminen

sovellusyhdyskäytävään yksinkertaistuu huomattavasti. HTTPS-protokollan merkittävä etu on siinä, että valtaosa käytössä olevista tietoliikenneverkoista ja verkkolaitteista on määritelty sallimaan HTTPS-liikenne jo valmiiksi. (Rowan 2007; Lucas ym. 2006: 243.)

Ratkaisumallin merkittävimmät ongelmat liittyvät VPN-yhteyttä käyttävän mallin tapaan kokonaisuuden monimutkaistumiseen. Sovellusyhdyskäytävän hankinta, käyttäminen ja ylläpito tuovat jonkin verran lisäkustannuksia pelkkään SharePoint-sovelluksen vakiokomponentteja käyttävään malliin verrattuna. Toisaalta valitusta sovellusyhdyskäytäväratkaisusta riippuen sen avulla voidaan mahdollisesti tarjota ulkoverkkoon muitakin palveluita kuin SharePoint-alustan päälle rakennettuja.

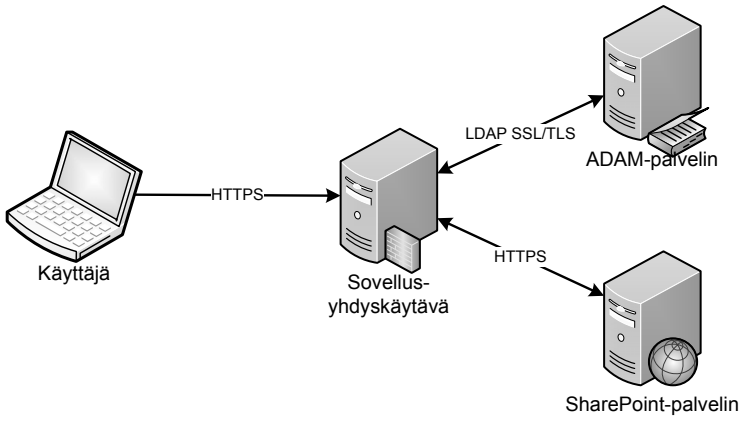
Edellä mainittu Microsoftin Forefront Unified Access Gateway (UAG) on esimerkki sovellusyhdyskäytävästä, jonka avulla voidaan julkaista organisaation sisäverkon palveluita ja resursseja ulkoverkkoon. UAG toimii verkkojen välissä etäkäyttäjien yhteyspisteenä, ja sen päätehtävinä on tietoliikenneyhteyden salaaminen, käyttäjien tunnistaminen, autentikointi ja valtuuttaminen sekä tietoliikenteen välittäminen käyttäjän ja sisäverkon palvelun välillä. UAG:n tarjoaman yhteyspisteen kautta etäkäyttäjät voivat käyttää sisäverkon palveluita Internet-selaimen avulla. (Microsoft 2010c.)

Vuonna 2010 julkaistu Forefront Unified Access Gateway 2010 -sovellus on Microsoftin Forefront -tietoturvatuoteperheen osa ja se korvaa Intelligent Application Gateway (IAG) -sovelluksen ja osittain myös ISA-tuotteet. UAG-yhdyskäytävä on pohjimmiltaan SSL- ja TLS-protokollia käyttävä VPN-yhdyskäytävä, joka sisältää joitakin sovellustason palomuurin ominaisuuksia. Tiedonsiirtoyhteydet yhdyskäytävän ja etäkäyttäjien välillä toteutetaan HTTPS-protokollalla. UAG:n valtti on hyvä yhteensopivuus erityisesti Microsoftin yritystuotteiden kanssa. (Snyder 2010.)

ABB Oy:n tapauksessa kokonaisuutena toimivimmaksi ratkaisuksi nousee SharePoint-alustaan ja sovellusyhdyskäytävään perustuva ratkaisumalli. Järjestelmän monimutkaistumisen ja mahdollisten lisäkustannusten vastapainoksi ratkaisumallin avulla voidaan tarjota liiketoimintayksiköille suoraviivainen, mutta kuitenkin monipuolinen menetelmä materiaalin

jakamiseen alihankkijoille. Ratkaisu tarjoaa lisäksi tietohallinnolle kattavat mahdollisuudet yhteyksien valvontaan ja hallintaan. Ratkaisumallin merkittävä etu VPN-yhteyksiä käyttävään ratkaisuun verrattuna on sen yksinkertaisuus käyttäjänäkökulmasta.

Periaatekuva ratkaisumallista on esitetty kuvassa 20.



Kuva 20. SharePoint-alustaan ja sovellusyhdyskäytävään perustuva ratkaisumalli.

10.2. Asiakkaiden yhteydet materiaalipankkeihin

Asiakkaiden yhteydet sisäverkon dokumentti- ja materiaalipankkeihin -kokonaisuuden yksittäiset tarpeet liittyvät pääsääntöisesti tiedostojen jakamiseen olemassa oleville asiakkaille. Jaettavat tiedostot ovat muun muassa testisertifikaatteja, tuotepäivityksiä sekä tuote- tai tuotantoinformaatiota sisältäviä dokumentteja.

Merkittävimmät erot kappaleessa 10.1. käsiteltyyn alihankkijoiden yhteydet sisäverkon dokumentti- ja materiaalipankkeihin -kokonaisuuteen ovat siinä, että asiakkaiden yhteydet sisäverkon dokumentti- ja materiaalipankkeihin -kokonaisuudessa yksittäisiin tarpeisiin liittyvien asiakkaiden lukumäärä on pääsääntöisesti merkittävästi suurempi kuin alihankkijoiden määrä kappaleessa

10.1. käsitellyissä tarpeissa ja asiakkaille ei tarvitse antaa jaettaviin dokumentteihin muokkaus- tai kirjoitusoikeuksia.

Materiaalia jaetaan asiakkaille olemassa olevissa käyttötapauksissa muun muassa ulkoverkkoon jaettujen Lotus Notes -tietokantojen, SharePoint-alustan ja sähköpostin avulla. Ratkaisujen monimuotoisuus vaikeuttaa kokonaisuuden hallintaa ja tällä on negatiivisia vaikutuksia muun muassa tietoturvaan sekä palveluiden käytettävyyteen. Negatiivisia vaikutuksia on käyty tarkemmin läpi kappaleessa 10.1.

Kokonaisuuteen kuuluvat yksittäiset tarpeet eroavat toisistaan jaettavien tiedostojen kokoluokan ja yhteyden tarvitsijoiden lukumäärän (*kymmenistä satoihin*) suhteen. Edellä mainitusta seuraa huomattavia eroja myös kokonaisliikennöintimääriin ja siten tarvittavaan tiedonsiirtokapasiteettiin. Lisäksi jaettavan materiaalin luonteessa on merkittäviä eroja; osa materiaalista on hyvin asiakaskohtaista ja osa varsin yleistä.

Asiakkaille tarjottavien yhteyksien tulee olla asiakkaan näkökulmasta mahdollisimman suoraviivaisia. Lähtökohta on, että materiaali on saatavissa helposti ilman erikoisohjelmistoja tai -laitteita. Vaatimuksen seurauksena materiaalin tulee käytännössä olla saatavissa Internet-selaimella ja käytettävien tietoliikenneyhteyksien tulee käyttää sovelluskerroksella joko HTTP- tai HTTPS-protokollaa (Rowan 2007; Lucas ym. 2006: 243). Lisäksi yhteyksien ja palveluiden tietoturvan tulee olla tarkoituksenmukaisella tasolla. Luottamuksellisen materiaalin siirtoon tulee käyttää SSL- tai TLS-protokollalla suojattuja tietoliikenneyhteyksiä (Steinberg ym. 2005).

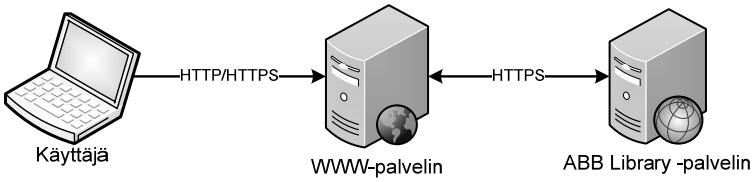
10.2.1. Eri tilanteiden ratkaisumallit

Kappaleessa 10.1.4. esitelty SharePoint-alustaan ja sovellusyhdyskäytävään perustuva ratkaisumalli on käyttökelpoinen myös materiaalin jakamiseen asiakkaille sellaisten tarpeiden kohdalla, joissa materiaali on luottamuksellista, sen tarvitsijoiden lukumäärä on kohtuullinen ja käyttäjät tarvitsevat pidempiaikaista pääsyä palveluun.

Mikäli SharePoint-alustan ja sovellusyhdyskäytävän yhteydessä käytetään kertakäyttöisiä salasanoja ja niiden hallinnointiin sopivaa järjestelmää, voidaan mallilla täyttää tarpeita, joissa yhteydet ovat kertaluonteisia ja jaettava materiaali luottamuksellista. Ratkaisumallin kohdalla yhteyksien tarvitsijoiden lukumäärällä ei ole huomattavaa merkitystä. Esimerkiksi UAG-sovellusyhdyskäytävä tukee kertakäyttöisiä salasanoja SharePoint-palveluiden yhteydessä (Microsoft 2010d).

Haastavin tilanne on tarpeiden kohdalla, joissa jaettava materiaali on luottamuksellista, materiaalin tarvitsijoiden lukumäärä on suuri ja yksittäiset käyttäjät tarvitsevat pidempiaikaista pääsyä palveluun. Teknisesti edellä kuvatut tarpeet voidaan toteuttaa melko yksinkertaisesti SharePoint-alustan ja sovellusyhdyskäytävän avulla, mutta ongelmallisimpaan osa-alueeseen eli käyttäjätunnusten luomiseen ei ole riittävän luotettavaa automaattista ratkaisua vaan tunnukset joudutaan luomaan pääosin manuaalisesti.

Materiaalin ollessa luonteeltaan yleistä sen jakaminen voidaan toteuttaa olemassa olevan ABB Library -palvelun avulla. Yksinkertaistettu kuva ABB Library -palvelusta on esitetty kuvassa 21.



Kuva 21. ABB Library -palvelun komponentit ja yhteydet.

ABB Library on sisällönhallintajärjestelmä, jonka avulla yhtiön verkkosivuilla voidaan julkaista dokumentteja. Järjestelmän avulla dokumenttien näkyvyyttä voidaan rajoittaa tarvittaessa. Dokumentit voidaan jakaa esimerkiksi vain sisäverkkoon, tietyille käyttäjille tai käyttäjäryhmille. Järjestelmä on yhtymän standardoima ja ylläpitämä. (ABB 2010d.)

ABB Library -palvelu tukee suojattuja HTTPS-yhteyksiä ja käyttää yhtymän ADAM-autentikointipalvelua (Kulakowski 2008).

ABB Library -palvelun hyvänä puolena on tiivis integrointi yhtiön Internet-sivuihin. Integroinnin myötä materiaalin jakaminen asiakkaille onnistuu yksinkertaisesti ja loogisesti suoraan verkkosivujen kautta (ABB 2010d). Palvelun heikkoutena on hieman epäselvä tulevaisuus, erityisesti yhtymänlaajuisesti käyttöönotettavien SharePoint-palveluiden myötä.

10.3. Asiakasjärjestelmien etävalvontayhteydet

ABB Oy:n valmistamat tuotteet hyödyntävät koko ajan laajamittaisemmin tietotekniikkaa ja eräs sen mukanaan tuoma mahdollisuus on tuotteiden etävalvonta. Etävalvonnan myötä asiakkaiden on mahdollista valvoa käytössä olevia laitteita ja järjestelmiä keskitetysti, ja samalla vähentää valvontaan sitoutuvia resursseja. Etävalvonta antaa asiakkaalle myös mahdollisuuden ulkoistaa järjestelmän valvonta ulkopuoliselle palveluntarjoajalle. Edellä mainittujen mahdollisuuksien lisäksi etävalvontaa voidaan hyödyntää tuotekehitysinformaation keräämiseen.

Etävalvontayhteydet asiakkaan hallussa oleviin laitteisiin tai järjestelmiin -tarvekokonaisuus koostuu yksittäisten tuotteiden, kokonaisten automaatio- sekä asiakasjärjestelmien ylläpitoon liittyvistä tarpeista. Tavoitteena on kerätä tarkkailtavasta järjestelmästä säännöllisesti tietoa, jonka perusteella voidaan seurata järjestelmän toimintatilaa ja ratkaista tai ennaltaehkäistä mahdollisia ongelmatilanteita.

Yksiselitteisen ja kaikkiin tilanteisiin sopivan etävalvontayhteysmallin rakentaminen on haastavaa erityisesti kahdesta syystä. Ensinnäkin järjestelmien toteutuksessa käytetty perustekniikka ja siten myös laskentaresurssit vaihtelevat huomattavasti (Sjöblom 2008). Toiseksi järjestelmien yhteydessä käytetyt tietoliikenneyhteydet julkiseen verkkoon eroavat toisistaan merkittävästi muun muassa kapasiteetin ja käyttökustannusten suhteen. Esimerkiksi hissikuiluun sijoitettu ja GPRS-yhteyttä käyttävä taajuusmuuttaja asettaa hyvin erilaiset vaatimukset käytettävälle etävalvontaratkaisulle kuin kiinteällä yhteydellä Internetiin kytketty teollisuus-PC.

Etävalvontayhteyksissä sovelluskerroksella käytettävien protokollien merkitys korostuu entisestään. Valvottavat laitteet tai järjestelmät voivat olla hyvinkin syvällä asiakkaan tietoverkossa, jolloin niistä lähtevä ja niihin tuleva verkkoliikenne on tarkoin rajattua. Lisäksi liikenne kulkee todennäköisesti useiden liikennettä ohjaavien ja rajaavien verkkolaitteiden kautta, jolloin erityisesti tulevan liikenteen reitittäminen on monimutkaista. Myös lähtevän liikenteen reititys- ja suodatussääntöjä joudutaan muuttamaan, mikäli esimerkiksi käytetään jotain verkossa aiemmin estettyä sovellusprotokollaa.

Yleisesti ottaen varmimmin sallittua on HTTP- tai HTTPS-protokollaa käyttävä verkkoliikenne, mutta valitettavasti kyseiset protokollat sopivat sellaisenaan varsin heikosti etävalvontainformaation välittämiseen. Niiden rinnalla onkin syytä käyttää esimerkiksi Simple Object Access Protocol (SOAP) -protokollaa, joka mahdollistaa etäproseduurikutsut (*Remote Procedure Call*) eXtensible Markup Language (XML) -merkintäkieltä hyväksikäyttäen. (Sjöblom 2008.)

10.3.1. Etävalvonnan toteutustavat

Etävalvontaan on yksinkertaistettuna kaksi tapaa, järjestelmät joko lähettävät tilatietoja itsenäisesti ulkoiseen tietojärjestelmään tai varastoivat tilatiedot omaan muistiinsa, josta ne käydään manuaalisesti lukemassa (Sjöblom 2008). Olemassa olevissa käyttötapauksissa käytetään molempia edellä mainittuja tapoja.

Jos etävalvonta toteutetaan siten, että tilainformaatio tallennetaan asiakkaan verkossa olevaan laitteeseen, joudutaan todennäköisesti tekemään muutoksia asiakkaan verkon reititysmäärityksiin ja palomuurisääntöihin (Sjöblom 2008). Tarvittavat muutokset voivat olla erittäin laajoja erityisesti, jos tilainformaatiota joudutaan hakemaan suoraan valvottavasta laitteesta tai yhteysprotokollana käytetään jotain muuta kuin HTTP- tai HTTPS-protokollaa. Huomattavaa on, että muutokset joudutaan tekemään jokaisen asiakkaan kohdalla erikseen, joka luonnollisesti lisää tuotteen tai palvelun käyttöönottoon liittyviä kustannuksia. Menetelmän käyttäminen voi olla perusteltua suurten yksittäisten järjestelmien etävalvontaratkaisuissa, mutta ei sarjatuotantona tehtävien tuotteiden kohdalla.

Käytännössä etävalvontaratkaisun valintaan vaikuttaa useita muuttujia. Vaikuttavina tekijöinä ovat muun muassa valvottavan tuotteen tai järjestelmän laskentaresurssit, käytettävissä olevat tietoliikenneyhteydet ja ulossaatava tilainformaatio sekä ennen kaikkea asiakkaiden vaatimukset ja olemassa olevat järjestelmät. Esimerkiksi jo pelkkä tiedonsiirtoprotokolla määräytyy käytettävissä olevan laskentatehon ja tietoliikenneyhteyden sekä siirrettävän tilainformaation määrän perusteella.

10.3.2. Olemassa olevat käyttötapaukset

Itsenäiseen informaation siirtämiseen käytetään olemassa olevissa ratkaisuissa suojattuja SSH File Transfer Protocol (SFTP) tai Secure Copy (SCP) -protokollia. Varsinainen tietoliikenne voidaan edellä mainittujen protokollien yhteydessä kuljettaa julkisen verkon yli sellaisenaan tai sitten salatussa VPN-tunnelissa. Eräs Suomessa vielä kokeiluvaiheessa oleva etävalvontaratkaisu on ABB:n Remote Access Platform (RAP) -konsepti.

RAP-konsepti on Puolan MV Drives -yksikössä kehitetty etävalvonta- ja etähallintaratkaisu. Konsepti perustuu ABB:n verkkoon sijoitettaviin viestintä- ja tietokantapalvelimiin sekä kohdejärjestelmässä ajettavaan etäsovellukseen. Ratkaisu perustuu NextNine Ltd:n NextNine Service Automation -tuotteeseen. Konsepti on yhtymän tukema, ja sen avulla on mahdollista integroida etävalvonta ABB:n käyttämiin järjestelmiin. Esimerkiksi varaosatilaukset voidaan automatisoida etävalvontasovellukselta saatavan informaation perusteella. (Wnek 2009.)

Kuvassa 23 on esitetty periaatekuva RAP-konseptista.

NextNine Service Automation -tuote koostuu etäjärjestelmässä ajettavasta alustariippumattomasta NextNine Virtual Support Engineer (VSE) -Java-sovelluksesta sekä VSE-sovelluksen hallintaan ja sen keräämän valvontainformaation tallennukseen käytettävistä NextNine Service Center ja NextNine Communications -palvelimista. (NextNine 2007.)

Yksi Service Center -palvelin kykenee hallinnoimaan useita VSE-sovelluksia NextNine Communication -palvelimen avulla. Etäsovelluksen ja

hallinnointipalvelimien väliset yhteydet ovat SSL- tai TLS-protokollalla suojattuja HTTPS-yhteyksiä. Vastaavasti yksittäinen VSE-sovellus voi valvoa useita samassa asiakasverkossa olevia laitteita ja järjestelmiä. Valvontainformaatiota voidaan siirtää useilla eri protokollilla VSE:n ja valvottavan laitteen tai järjestelmän välillä. (NextNine 2007.)

Menetelmissä, joissa tilainformaatio luetaan suoraan valvottavasta järjestelmästä, käytetään yleisesti erilaisia etätyöpöytäsovelluksia ja -protokollia, joista esimerkkinä mainittakoon Microsoftin Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), Xremote ja Vector Networksin PC-Duo. Etätyöpöytäsovellusten ja -protokollien kohdalla varsinainen alla oleva tietoliikenneyhteys on yleisesti olemassa olevissa ratkaisuissa IPsec-, SSL- tai TLS-protokollaa hyödyntävä VPN-yhteys.

Käytettyjen VPN-ratkaisujen merkittävä ongelma on niiden keskinäinen yhteensopimattomuus, joka on johtanut siihen, että asiakkaasta riippuen etävalvontayhteyksiin joudutaan käyttämään jotain tiettyä VPN-sovellusta tai -laitetta (Rowan 2007; Stanton 2005). VPN-yhteyksien lisäksi käytetään myös SSH-yhteyksiä sekä yhteyden tunnelointiin että varsinaiseen etävalvontaan.

Nykyisessä käytännössä sisäverkosta ulkoverkkoon suuntautuvissa etäyhteyksissä jokaiselle yhteydelle määritetään lähtöpisteeksi jokin tietty sisäverkon työasema. Sisäverkon palomuuri- ja reititysmääritykset tehdään siten, että vain lähtöpisteeksi valitusta työasemasta voidaan muodostaa yhteys tiettyyn ulkoverkon verkko-osoitteeseen käyttäen tiettyjä sovellus- ja tietoliikenneprotokollia. Mikäli lähtöpisteeksi on valittu fyysinen työasema virtualisoidun sijaan, ratkaisu voi johtaa työasema- ja ohjelmistoresurssien vajaakäyttöön tapauksissa, joissa esimerkiksi valmistajakohtaisia VPN-sovelluksia ei voida käyttää samassa työasemassa (Crosby & Brown 2006: 6).

Nykyisessä ABB Oy:n käyttämässä verkkomallissa sisä- ja ulkoverkon rajalla tehdään osoitteenmuunnos NAT-tekniikalla. Seurauksena osoitteenmuunnoksesta on, että kohdejärjestelmä ei näe lähtöpisteen oikeaa verkko-osoitetta. Kohdejärjestelmä näkee sen sijaan sen verkkosolmun osoitteen, jossa osoitteenmuunnos on viimeiseksi tehty (osoitetta nimitetään julkiseksi verkko-osoitteeksi) ja käyttää tätä osoitetta etävalvontayhteyden

tunnistamiseen. Mikäli lähtöpisteen verkkoliikenne reititetään jostain syystä kulkemaan jonkin toisen julkisen verkkosolmun kautta, yhteyttä asiakasjärjestelmään ei voida muodostaa ilman kohdejärjestelmään tehtäviä muutoksia. Edellä mainittu ongelma voi toteutua, jos tiedonkulussa liiketoimintayksiköiden ja yhtiön tietohallinnon välillä on katkoksia.

10.3.3. Etävalvontayhteyksien ongelmia ja vaatimuksia

Eräs merkittävimmistä ongelmista etävalvontayhteyksien luonnissa liittyy jo aiemmin mainittuihin reitityssääntöihin. Asiakasverkko, johon yhteys otetaan, on usein varsin monimutkainen. Verkko koostuu lukuisista palomuureista sekä muista tietoliikennevirtoja kontrolloivista verkkosolmuista, joiden avulla rajataan erityisesti verkkoon tulevaa tietoliikennettä. Etäyhteyksiä rakennettaessa joudutaan jokainen matkalla oleva verkkosolmu määrittämään siten, että haluttu tietoliikenne pääsee valvottavaan järjestelmään asti. Määritysten tekeminen on yleisesti varsin monimutkaista ja aikaa vievää. Lisäksi määrityksiä joudutaan jatkuvasti tarkastelemaan sekä lähde- että kohdeverkoissa tapahtuvien muutosten myötä. (Sjöblom 2008.)

Ongelmaa voidaan kompensoida käyttämällä etävalvontaan menetelmää, jossa aloite yhteyden luomiseen tulee valvottavalta järjestelmältä tai laitteelta ja yhteys muodostetaan ABB Oy:n DMZ-alueella olevaan palvelimeen (Sjöblom 2008). Menetelmän tehokkuus perustuu siihen, että yleisesti tietoliikenneverkot määritetään sallimaan lähtevää liikennettä huomattavasti saapuvaa liikennettä vapaammin (Sjöblom 2008). Mikäli jostain syystä ei voida käyttää tilainformaation itsenäiseen siirtämiseen perustuvaa valvontamenetelmää, ongelmaa voidaan vähentää käyttämällä SSL- tai TLS-protokollaa hyödyntäviä VPN-yhteyksiä. Kun VPN-yhteydet terminoidaan mahdollisimman lähelle valvottavaa järjestelmää, voidaan minimoida matkalla oleviin verkkosolmuihin tehtäviä muutoksia (Stanton 2005; Rowan 2007). Riittää, että solmut määritetään sallimaan HTTPS-liikenne yhteyden terminointipisteeseen saakka (Stanton 2005; Rowan 2007).

Mikäli etävalvontayhteyden yli lähetetään luottamuksellista informaatioita, yhteyden tulee olla suojattu sovelluskerroksella. Suositeltavimmat

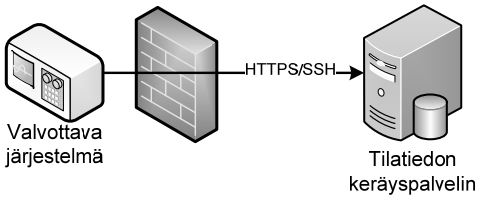
suojausprotokollat ovat SSL- ja TLS-protokollat, mutta myös SSH-protokolla on varsin käyttökelpoinen useissa tapauksissa.

Siirrettävän tilainformaation ollessa vähemmän arkaluontoista voidaan sovelluskerroksella käyttää suojaamattomia protokollia. Yhteyden tulisi silti olla ainakin verkkokerroksella suojattua, jotta viestinnän osapuolet voidaan tunnistaa luotettavasti. Suojaukseen voidaan käyttää IPsec-protokollia.

Etävalvontayhteysratkaisuissa on huomioitava myös riittävän kattavien lokitietojen ylläpitäminen ja huolehdittava siitä, että valvottavan järjestelmän tilainformaatio on vain siihen oikeutettujen tahojen saatavilla.

10.3.4. Ratkaisumallit

Lähtökohtaisesti suositeltavin tapa toteuttaa järjestelmien tai laitteiden etävalvonta on käyttää menetelmää, jossa valvottavat järjestelmät siirtävät itsenäisesti tilainformaatiota ABB Oy:n verkossa olevaan palvelimeen (Sjöblom 2008). Menetelmä on yksinkertainen erityisesti asiakkaan näkökulmasta (Sjöblom 2008). Periaatekuva ratkaisumallista on esitetty kuvassa 22.



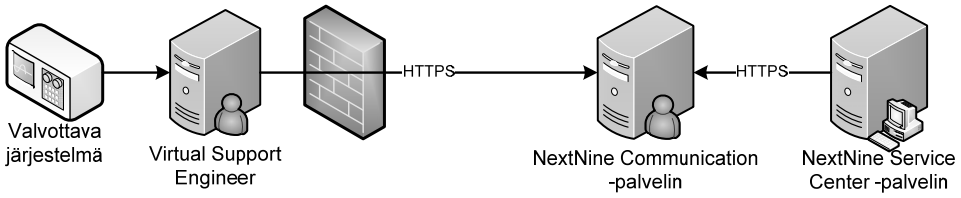
Kuva 22. Etävalvontainformaation tallentaminen palvelimeen.

Palvelimen ja valvottavan järjestelmän välisen tietoliikenneyhteyden tulee olla vähintään verkkokerroksella suojattu. Suositeltavin sovelluskerroksella käytettävä protokolla on SSL- ja TLS-protokollia hyödyntävä HTTPS, mutta muun muassa valvottavan järjestelmän laskentaresursseista ja tietoliikenneyhteyksien ominaisuuksista riippuen voidaan käyttää myös muita protokollia ja yhteyden suojausmenetelmiä. On huomattava, että myös palvelimelle tallennettava tilainformaatio tulee suojata asianmukaisesti.

Etävalvonnan kokonaistietoturvan kannalta on olennaista varmistaa tapahtumien jäljitettävyys ylläpitämällä kattavaa tapahtumalokia.

Eräs etävalvontaan soveltuva menetelmä on yhtymän RAP-konsepti. RAP vaatii valvottavalta järjestelmältä melko paljon laskentatehoa, joten se sopii sellaisiin järjestelmiin, joissa valvontaan käytetään esimerkiksi PC-työasemia. Useimmille sulautetuille järjestelmille konseptin resurssivaatimukset ovat jo selkeästi liikaa.

Yksinkertaistettu malli RAP-konseptista on esitetty kuvassa 23.

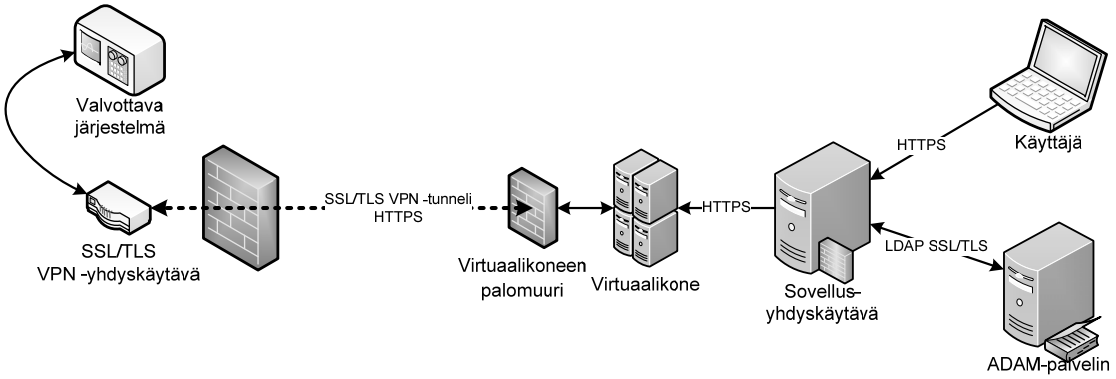


Kuva 23. RAP-konseptin komponentit ja yhteydet.

Mikäli järjestelmien tai laitteiden etävalvontaan joudutaan syystä tai toisesta käyttämään menetelmää, jossa valvontainformaatio luetaan suoraan valvottavasta järjestelmästä joko graafisen tai tekstipohjaisen etäkäyttöyhteyden yli, niin yhteydet on muodostettava SSL/TLS VPN -tekniikalla. Verkkoympäristössä tapahtuvien muutosten vaikutusten minimoimiseksi on tärkeää, että VPN-yhteys terminoidaan loogisesti mahdollisimman lähelle valvottavaa järjestelmää (Stanton 2005; Rowan 2007). Lisäksi VPN-yhteys on rakennettava siten, että verkkoliikenne ohjataan liikennettä valvovan palomuurin kautta lähdeverkosta VPN-tunneliin.

ABB:n verkon osalta VPN-yhteydet terminoidaan omaan erilliseen verkkoalueeseensa, johon voidaan muodostaa SSL- tai TLS-protokollalla suojattu yhteys miltä tahansa sisäverkon työasemalta sovellusyhdyskäytävän kautta. Yhteyttä muodostettaessa käyttäjät autentikoidaan sovellusyhdyskäytävässä ja vain etävalvonta- ja etähallintayhteyksien käyttöön oikeutetut käyttäjät päästetään käyttämään verkkoalueen palveluita. Ideaalitilanteessa kaikkia verkkoalueen palveluita voidaan käyttää myös

pelkällä Internet-selaimella ilman apuohjelmia sekä sisä- että ulkoverkosta. Periaatekuva ratkaisumallista on esitetty kuvassa 24.



Kuva 24. SSL/TLS VPN -yhteyttä käyttävät suorat etävalvontayhteydet.

Edellä mainittu verkkoalue sisältää kaikki etävalvonta- ja etähallintayhteyksien käyttöön sekä valvontaan tarvittavat laite- ja sovellusresurssit. Laite- ja sovellusresurssit voidaan tarjota esimerkiksi virtualisoituna. Verkkoalue sisältää myös tarvittavat mekanismit kattavien lokitietojen ylläpitoon.

Eräs toimiva tapa SSL/TLS VPN -yhteyden luomiseen etävalvontayhteyksien kohdalla on käyttää niin sanottua Reverse Proxy -tekniikkaa, jossa VPN-palvelin toimii eräänlaisena yhdyskäytävänä. Menetelmässä palvelin sijoitetaan sisäverkkoon ja se määritellään näkymään ulkoverkkoon. Palvelin vastaa ulkoverkosta tuleviin yhteyspyyntöihin, tunnistaa, autentikoi ja valtuuttaa käyttäjän, muodostaa SSL- tai TLS-protokollalla suojatun VPN-yhteyden palvelimen ja käyttäjän välille sekä toimii välittäjänä käyttäjän ja sisäverkon palveluiden välillä. Kappaleissa 10.1. ja 10.2. käsitellyt sovellusyhdyskäytävät pohjautuvat yleisesti Reverse Proxy -tekniikkaan. (Steinberg ym. 2005; Harding 2003.)

Tekniikan avulla SSL/TLS VPN -yhteys voidaan rakentaa varsin kustannustehokkaasti sijoittamalla yksittäinen VPN-palvelin valvottavan järjestelmän yhteyteen ja määrittämällä kohdejärjestelmän reitityssäännöt siten, että ulkoverkosta voidaan ottaa yhteys VPN-palvelimeen. Prosessia nopeuttaa muun muassa se, että palvelimissa voidaan käyttää jo ennen laitteen asiakasverkkoon kytkemistä tehtyjä ja suurilta osin vakioituja asetuksia.

Molemmat edellä esitetyt ratkaisumallit sisältävät joitakin hyviä ja huonoja ominaisuuksia. Vaikka ensimmäinen malli onkin lähtökohtaisesti suositeltavampi, niin lopullinen valinta riippuu valvottavasta järjestelmästä ja asiakkaan tarpeista.

Ensimmäisen mallin merkittävimmät edut liittyvät yhteyksien rakentamisen ja ylläpidon yksinkertaisuuteen sekä kevyisiin resurssivaatimuksiin. Mikäli menetelmässä käytetään tiedonsiirtoon yleisesti käytössä olevia protokollia, asiakasverkon reititys- ja suodatussääntöihin ei tarvitse tavallisesti tehdä suuria muutoksia käyttöönoton yhteydessä. Lisäksi ratkaisu on varsin tunteeton verkossa käyttöönoton jälkeen tapahtuville muutoksille. Ratkaisumallin yhteydessä voidaankin käyttää pitkälle vakioituja menetelmiä ja siten saavuttaa kustannussäästöjä. Kevyet resurssivaatimukset mahdollistavat mallin hyödyntämisen myös sellaisten järjestelmien yhteydessä, joissa on rajoituksia laskentaresurssien tai tietoliikenneyhteyksien kapasiteetin suhteen.

Ensimmäisen mallin merkittävin ongelma on implementoinnin vaikeus erityisesti olemassa oleviin järjestelmiin. Toinen merkittävä puute on, että mahdollisesti tarvittava etähallintayhteys tulee rakentaa erikseen.

Ratkaisumallin, jossa tilatiedot luetaan suoraan valvottavasta järjestelmästä, etuina voidaan mainita mallin käyttöönoton helppous useiden olemassa olevien järjestelmien kohdalla ja rakennetun yhteyden sopiminen myös etähallintaan.

Mallin heikkouksia ovat yleisesti korkeammat laite- ja lisenssikustannukset, korkeat resurssivaatimukset sekä yhteyksien rakentamiseen ja ylläpitoon liittyvät ongelmat. Korkeat resurssivaatimukset ovat pääosin seurausta etävalvontaan käytettävistä graafisista etäkäyttösovelluksista. Tekstipohjaiset etäkäyttösovellukset ovatkin huomattavasti kevyempiä sekä laskentaresurssien että tietoliikenneyhteyksien kuormituksen suhteen. Yhteyksien rakentaminen ja ylläpitäminen on hankalaa, koska tietoliikenteen suunta on asiakasverkossa ulkoverkosta sisäverkkoon.

Yhteenvetona voidaan todeta menetelmän, jossa valvottavat järjestelmät siirtävät tilatietoa itsenäisesti ABB:n verkossa olevaan palvelimeen sopivan erityisen hyvin sellaisten tarpeiden toteuttamiseen, joissa etävalvonnan

yksinkertaisuus, luotettavuus ja taloudellisuus ovat ensiarvoisen tärkeitä tai laite- ja tiedonsiirtoresurssit ovat rajalliset. Malli, jossa tiedot luetaan suoraan valvottavasta järjestelmästä, sopii sen sijaan tarpeisiin, joissa järjestelmän etähallinta on vähintään yhtä tärkeää kuin etävalvonta tai joissa aiemmin esitellyn etävalvontamallin implementoiminen valvottavaan järjestelmään on erittäin työlästä.

10.4. Asiakasjärjestelmien etähallintayhteydet

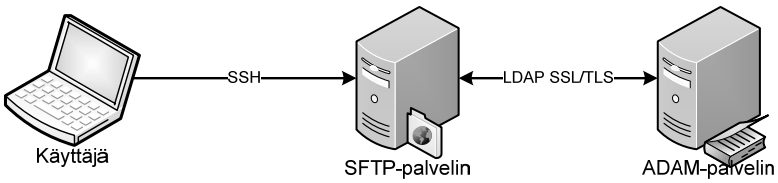
Asiakasjärjestelmien etähallintayhteydet -kokonaisuuteen kuuluneet yksittäiset tarpeet liittyvät läheisesti kappaleessa 10.3. läpikäytyihin etävalvontakokonaisuuden tarpeisiin. Yksittäiset tarpeet liittyvät pääosin laitteiden tai järjestelmien ylläpitoon, mutta joukossa on myös tiedonsiirtoon ja tukipalveluiden tuottamiseen liittyviä tarpeita.

Suositeltava tapa ylläpitoon tai tukipalveluiden tuottamiseen tarvittavien etähallintayhteyksien toteuttamiseen on kappaleessa 10.3.4. esitelty ratkaisumalli, jossa käytettiin SSL- tai TLS-protokollalla suojattuja VPN-yhteyksiä ja erillistä yhdyskäytäväverkkoa.

Etähallintayhteyksiä käytetään tiedonsiirtoon erityisesti etäjärjestelmän varmuuskopioinnin yhteydessä. Etähallintayhteyksien sopiminen tiedonsiirtoon riippuu huomattavasti käytettävästä etäkäyttöprotokollasta ja -sovelluksesta. Yleisesti ottaen etäkäyttöprotokollia ei ole suunniteltu suurten tietomassojen luotettavaan siirtämiseen, ja tämä näkyy muun muassa siinä, että yhteyden katketessa tiedonsiirto joudutaan useissa tapauksissa aloittamaan alusta.

Parempi tapa suurten datamassojen siirtämiseen on SSH-protokollaa tietoliikenneyhteyden suojaukseen käyttävä SFTP-protokolla (Galbraith & Saarenmaa 2006). SFTP-protokolla on erityisesti tiedonsiirtoon ja -hallintaan suunniteltu protokolla (Galbraith ym. 2006). Periaatekuva ratkaisumallista on esitetty kuvassa 25.

Protokollan merkittävinä etuina on sen tietoturva, yleisyys ja suhteellinen tehokkuus. Heikkouksina voidaan mainita se, että se vaatii sitä tukevan palvelimen lisäksi erillisen asiakasohjelman. Toisaalta tarjolla on hyvinkin kehittyneitä asiakasohjelmia, jotka kykenevät muun muassa jatkamaan yhteyden katketessa kesken jääneitä tiedonsiirtoyhteyksiä. (WinSCP 2010.)



Kuva 25. Tiedostojen tallentaminen SFTP-palvelimeen.

SFTP-protokollan joustavaa käyttöä varten ABB:n DMZ-alueella tulee olla LDAP-autentikointia tukeva SFTP-palvelin. Palvelimen pitää luonnollisesti ylläpitää riittävää tapahtumalokia, valvoa tulevia ja lähteviä tietoliikenneyhteyksiä sekä taata luotettava pääsynvalvonta. SFTP-palvelin käyttää käyttäjien autentikointiin olemassa olevien ADAM-palvelimien tarjoamia autentikointipalveluita.

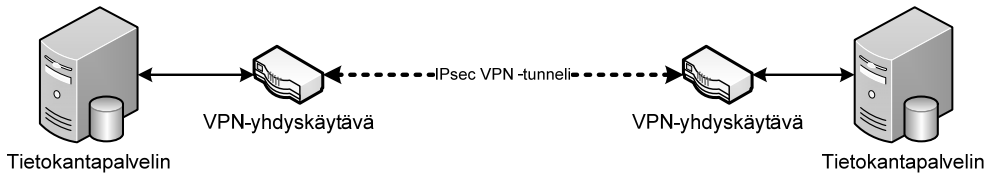
Toinen yhtenäisen mallin kannalta periaatteessa hyvä vaihtoehto olisi käyttää datan siirtämiseen ja tallentamiseen SharePoint-sovellusta. Valitettavasti edes uusin SharePoint 2010 -alusta ei tue yksittäisten yli kahden gigatavun tiedostojen tallentamista ja ei sen vuoksi sovi suurten datamassojen säilyttämiseen. (Microsoft 2010f.)

10.5. Tietokantojen synkronointi

Tietokantojen synkronointi alihankkijan verkossa olevien tietokantojen kanssa -kokonaisuuteen kuuluvat yksittäiset tarpeet liittyvät testausinformaation ja testiasemaparametrien keskitettyyn siirtämiseen sekä ryhmätyösovelluksen sisältämän informaation synkronointiin alihankkijan ja ABB:n verkoissa olevien tietokantojen välillä.

Tietokantojen synkronoinnissa on yksinkertaistettuna kyse siitä, että yhteen tietokantaan tehdyt muutokset tehdään myös muihin samaa tietoa sisältäviin tietokantoihin. Mikäli tietokannat on hajautettu eri tietokantapalvelimille, synkronointiin joudutaan käyttämään tietoliikenneyhteyksiä. (Özsu & Valduriez 1991: 1–9.)

Olemassa olevissa käyttötapauksissa tietokantapalvelimien väliset tietoliikenneyhteydet ovat niin sanottuja LAN-to-LAN-yhteyksiä, jotka ovat ABB Oy:n ja alihankkijoiden verkkojen välille muodostettuja pysyviä loogisia yhteyksiä. LAN-to-LAN-yhteydet on toteutettu IPsec-protokollaa käyttävillä VPN-yhteyksillä. Tietokantapalvelimina käytetään Microsoftin SQL Server -tuotteita. Myös synkronointi tehdään SQL Server -palvelimen omilla työkaluilla. Käytössä oleva malli on esitetty kuvassa 26.



Kuva 26. Tietokantojen synkronointi.

Nykyisissä käyttötapauksissa merkittävänä ongelmana on yhteyksien heikko luotettavuus ja sen myötä vaihtelevat vasteajat. Ongelmaa korostaa entisestään se, että Microsoftin SQL Server -palvelimen synkronointityökalut on suunniteltu alun perin käytettäväksi nopeissa ja luotettavissa lähiverkoissa.

Koska tietojen synkronointi tehdään julkisen tietoliikenneverkon yli, yhteyden luotettavuuden ja ennen kaikkea vasteaikojen parantaminen on erittäin vaikeaa ja kallista (Pfleeger ym. 2006; Forte 2009). Taloudellisesti mielekkäin vaihtoehto on käyttää Microsoftin tai kolmansien osapuolien tarjoamia vikasietoisempia replikointimenetelmiä ja -sovelluksia tietokantojen synkronointiin.

Tietoturvamielessä nykyisten ratkaisujen ongelma on, että ne käyttävät vain verkkokerroksella suojattuja tietoliikenneyhteyksiä. Mikäli synkronoitava data on luottamuksellista, yhteydet tulisi suojata sovelluskerroksella. Suojaukseen ja datan tunnelointiin on suositeltavaa käyttää SSL- tai TLS-protokollaa.

10.6. Tiedonsiirto alihankkijan ja asiakkaan välillä

Tarvekartoituksessa nousi esiin tarve välittää informaatiota ABB Oy:n käyttämiltä alihankkijoilta ABB:n asiakkaille. Nykyisin ABB toimii tiedon välittäjänä erityisesti tapauksissa, joissa pienillä alihankkijoilla ei ole resursseja ottaa käyttöön materiaalin jakamiseen soveltuvia järjestelmiä.

Huomionarvoista on, että jaettava informaatio on usein ABB:n näkökulmasta luottamuksellista materiaalia, jolloin sen hallintaan käytettäville järjestelmille kohdistuu lukuisia tietoturvavaatimuksia. Materiaalin tulee olla suojattua ja ainoastaan sen käyttöön oikeutettujen tahojen käytettävissä. Lisäksi tietoliikenneyhteydet tulee suojata riittävällä tasolla. Mikäli tieto on arkaluonteista, yhteys tulee suojata sovelluskerroksella SSL- tai TLS-protokollalla.

Tarpeen luonteesta riippuen voidaan käyttää useita erilaisia ratkaisuja. Mikäli tarve on luonteen sellainen, että yhteydet ovat melko pysyviä, voidaan soveltaa kappaleessa 10.2.1. esitettyjä SharePoint-alustaan ja sovellusyhdyskäytävään perustuvia ratkaisumalleja. Kantavana ajatuksena on, että ABB tarjoaa alihankkijalle tai asiakkaalle perusinfrastruktuurin materiaalin jakamiseen.

Ei kuitenkaan ole tarkoituksenmukaista, että ABB Oy tarjoaisi edellä kuvattuja palveluita laajamittaisesti ja pysyvästi. Palveluita tarjotaan ainoastaan valikoiduissa yksittäisissä tapauksissa. Pidemmän aikavälin tavoitteena on ohjata alihankkija tai asiakas ottamaan käyttöön oma ABB:n tietoturvakriteerit täyttävä materiaalin jakojärjestelmä.

11. YLEINEN MALLI

Edellisessä luvussa tarkasteltiin mahdollisia ratkaisumalleja, joiden avulla voidaan toteuttaa tiettyjä tarvekartoituksessa esiin nousseista yksittäisistä käyttötarpeista muodostettuja tarvekokonaisuuksia. Huomattavaa on, että osa tarvekokonaisuuksista koostuu tarpeista, jotka vaativat tietoliikenneyhteyksiä ABB Oy:n sisäverkosta kolmansien osapuolien verkkoihin ja osa vastaavasti yhteyksiä kolmansien osapuolien verkoista ABB Oy:n sisäverkkoon.

Viimeisenä vaiheena esitellyt ratkaisumallit yhdistetään yhdeksi kattavaksi konseptiksi. Konseptissa määritellään palvelut, joiden avulla voidaan tarjota alihankkijoille ja asiakkaille pääsy ABB Oy:n dokumentti- ja materiaalipankkeihin, muodostaa etävalvonta- ja etähallintayhteyksiä asiakkaiden tietoliikenneverkoissa oleviin laitteisiin ja järjestelmiin sekä välittää materiaalia alihankkijoilta asiakkaille. Lisäksi tarkastellaan tietokantojen synkronointia julkisen verkon yli.

Konseptin määrittelyssä tulee lisäksi huomioida mallin skaalautuminen jatkokäsittelyn ulkopuolelle jääneiden ja tarvekartoituksessa tunnistamattomien tarpeiden vaatimuksiin.

11.1. Verkon looginen rakenne

Luvussa 10 määriteltyjen ratkaisumallien käyttöönotto vaatii muutoksia yhtiön tietoliikenneverkon loogiseen rakenteeseen. Nykyinen laaja DMZ-alue jaetaan ulkoiseen ja sisäiseen DMZ-alueeseen. Lisäksi verkkoon luodaan kaksi uutta verkkosegmenttiä, joita käytetään ABB Oy:n ja kolmansien osapuolien välille muodostettavien loogisten tietoliikenneyhteyksien terminointipisteinä.

Toinen uusi segmentti toimii asiakasverkkoon avattavien etävalvonta- ja etähallintayhteyksien terminointipisteenä ja sisäverkon käyttäjien etäyhteysyhdyskäytävänä. Segmenttiä kutsutaan tässä mallissa etäkäyttösegmentiksi.

Toinen uusi segmentti on sen sijaan varattu muille loogisille yhteyksille, kuten esimerkiksi LAN-to-LAN-yhteyksille ja siitä käytetään nimeä etäyhteyssegmentti.

Merkittävin ero segmenttien välillä on se, että etäkäyttösegmenttiin terminoidaan suorat etävalvonta- ja etähallintayhteydet, jotka ovat luonteeltaan väliaikaisia eli ne avataan vain tarvittaessa ja aloite niiden muodostamiseen tehdään ABB Oy:n verkosta. Etäyhteyssegmenttiin terminoitavat loogiset yhteydet ovat sen sijaan luonteeltaan pysyviä eli ne ovat jatkuvasti avoinna, eikä niitä tarvitse erikseen tiedonsiirtoa aloitettaessa muodostaa.

Malli konseptin mukaisen tietoliikenneverkon loogisesta rakenteesta on esitetty kuvassa 27.

Muutoksien avulla verkosta saadaan joustavampi ja tietoturvallisempi. Tietoturvan parantuminen perustuu siihen, että muutoksen myötä ulko- ja sisäverkon välissä on useampia rajamuureja. Lisäksi muutos mahdollistaa palveluiden tietoturvan kannalta loogisemman sijoittelun. Esimerkiksi useita aiemmin sisäverkossa tai ulospäin näkyneellä DMZ-alueella olleita palveluita voidaan sijoittaa muutoksen myötä sisäiselle DMZ-alueelle. (Pfleeger ym. 2006; Laaksonen ym. 2006: 182; Young 2001; Maley 2001: 6–7.)

11.2. Verkkosegmenttien väliset yhteydet

Verkkosegmentit luokitellaan luottamuksellisuustasoihin, joista sisäverkon segmenteistä alimpana on ulkoinen DMZ-alue. Yhtä tasoa ylempänä ovat sisäinen DMZ-alue, etäkäyttö- ja etäyhteyssegmentit. Muut sisäverkon verkkosegmentit luokitellaan edellä mainittuja segmenttejä korkeampiin luottamuksellisuustasoihin. Tietoliikenne alemmilta tasoilta ylemmille on pääsääntöisesti estetty, mutta niissä poikkeustapauksissa, joissa se on sallittua, yhteydet tulee suojata vähintään verkkokerroksella. Sen sijaan yhteydet ylemmiltä tasoilta alemmille on yleisesti sallittu.

Verkkosegmenttien väliseen ja sisäiseen tietoliikenteeseen tulee kiinnittää erityistä huomiota. Esimerkiksi tietoliikenneyhteydet, joiden yli siirretään

luottamuksellista tietoa, suojataan aina sovelluskerroksella. Verkkosegmentit erotetaan toisistaan palomuureilla, joiden tehtävänä on valvoa ja kontrolloida segmenttien välistä tietoliikennettä.

Ulkoinen DMZ-alue vastaa hyvin pitkälti nykyistä DMZ-aluetta, ja sinne voidaan muodostaa yhteyksiä sekä ulko- että sisäverkosta. Ulkoiselta DMZ-alueelta voidaan muodostaa yhteyksiä vain sisäiselle DMZ-alueelle. Yhteyksien tulee olla aina suojattu sovelluskerroksella. Merkittävä osa tulevasta ja verkkosegmentin sisäisestä tietoliikenteestä on suojaamatonta.

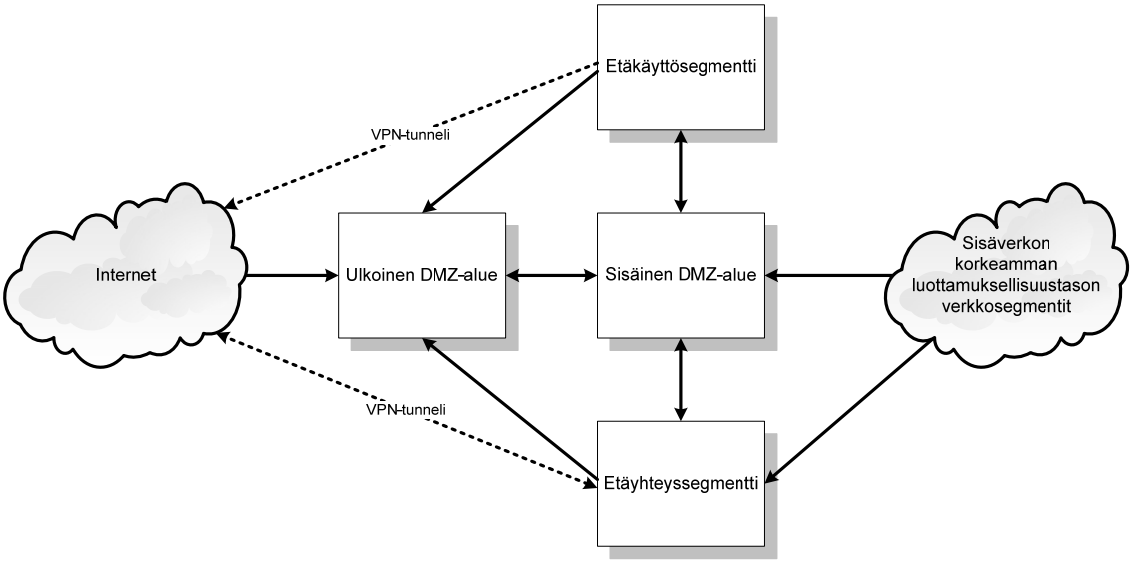
Sisäinen DMZ-alue näkyy sisäverkkoon, ja sieltä voidaan muodostaa yhteyksiä ulkoiselle DMZ-alueelle, etäkäyttö- ja etäyhteyssegmentteihin. Tietoliikenneyhteydet etäkäyttö- ja etäyhteyssegmentteihin tulee aina suojata sovelluskerroksella.

Tietoliikenneyhteyksien etäkäyttö- ja etäyhteyssegmenttiin tulee aina olla suojattuja.

Etäkäyttösegmenttiin voidaan muodostaa yhteys sisäiseltä DMZ-alueelta. Toiseen suuntaan yhteyksiä voidaan muodostaa ulkoverkkoon sekä ulkoiselle ja sisäiselle DMZ-alueelle. Tietoliikenneyhteydet segmenttiin ja segmentistä ulos tulee aina suojata sovelluskerroksella.

Etäyhteyssegmenttiin on mahdollista muodostaa tietoliikenneyhteyksiä sisäiseltä DMZ-alueelta ja sisäverkon korkeamman luottamuksellisuustason verkkosegmenteistä. Segmentistä voidaan vastaavasti muodostaa yhteyksiä ulkoverkkoon, ulkoiselle ja sisäiselle DMZ-alueelle sekä joissakin erikoistapauksissa sisäverkon korkeamman luottamuksellisuustason verkkoalueisiin. Segmenttiin tulevien ja sieltä lähtevien tietoliikenneyhteyksien tulee aina olla suojattuja.

Yksinkertaistettu malli verkkosegmenttien välisistä tietoliikenneyhteyksistä on esitetty kuvassa 27.



Kuva 27. Tietoliikenneverkon looginen rakenne ja segmenttien väliset yhteydet.

11.3. Palvelukonseptit

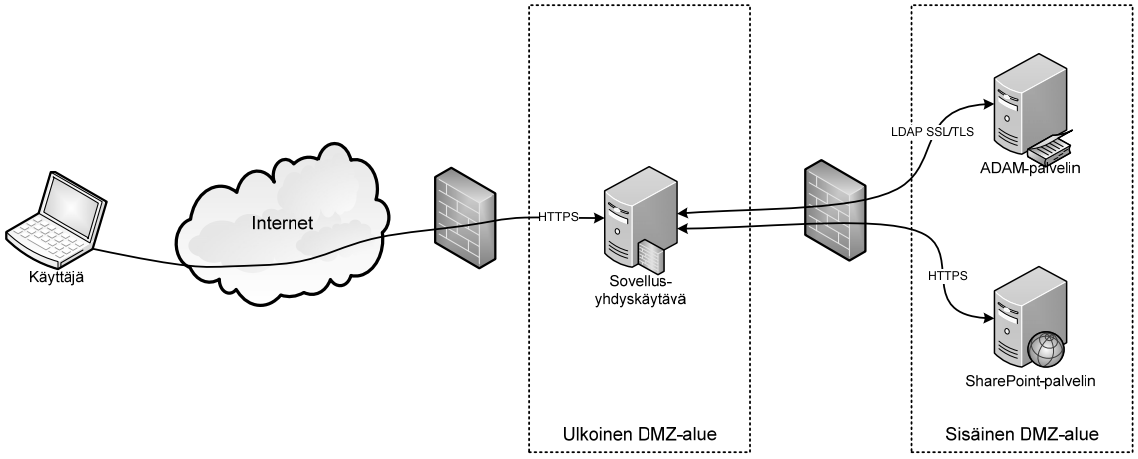
Kaikki palvelut, joihin tulee saada muodostettua suoria yhteyksiä sekä sisä- että ulkoverkosta, sijoitetaan ulkoiselle DMZ-alueelle. Sen sijaan sisäiselle DMZ-alueelle sijoitetaan palvelut, joiden käytön tulee onnistua ulkoiselta DMZ-alueelta ja sisäverkon verkkosegmenteistä.

Etäkäyttösegmenttiin sijoitetaan palvelut, jotka tarvitaan etävalvonta- ja etähallintayhteyksien muodostamiseen ja käyttämiseen. Etäyhteyssegmentille sijoitetaan palvelut, joihin tulee saada muodostettua yhteyksiä muiden loogisten yhteyksien yli.

11.3.1. Materiaalin jakaminen alihankkijoille

Materiaalin jakaminen alihankkijoille toteutetaan SharePoint-palveluiden avulla, joihin muodostetaan SSL- tai TLS-protokollalla suojatut yhteydet ulkoverkosta ulkoisella DMZ-alueella olevan sovellusyhdyskäytävän kautta. Varsinaiset SharePoint-palvelimet sijoitetaan sisäiselle DMZ-alueelle. Sovellusyhdyskäytävä vastaa pääsynvalvonnasta, muodostaa suojatun

yhteyden käyttäjän haluamaan sisäisellä DMZ-alueella olevaan SharePoint-palveluun, toimii yhteyden välittäjänä ja viestinnän päätyttyä purkaa käytetyn yhteyden. Sovellusyhdyskäytävä käyttää käyttäjien autentikointiin ja valtuuttamiseen sisäisellä DMZ-alueella olevan ADAM-palvelimen tarjoamia autentikointipalveluita. Tarvittavat palvelimet ja niiden väliset yhteydet on esitetty kuvassa 28.



Kuva 28. Yhteys SharePoint-palveluihin sovellusyhdyskäytävän kautta.

Palomuurisäännöt tulee määrittää siten, että ulkoisella DMZ-alueella olevaan sovellusyhdyskäytävään sallitaan HTTPS-protokollaa käyttävät tietoliikenneyhteydet ja sisäisellä DMZ-alueella olevaan SharePoint-palvelimeen sallitaan sovellusyhdyskäytävältä tulevat HTTPS-yhteydet. Lisäksi sisäisen DMZ-alueen ADAM-palvelimeen sallitaan sovellusyhdyskäytävältä tulevat SSL- tai TLS-protokollalla suojatut LDAP-yhteydet.

Materiaalin jakamisen yhteydessä tapahtumalokiin kirjataan sovellusyhdyskäytävään tulleet yhteyspyynnöt, onnistuneet ja epäonnistuneet autentikoinnit sekä käytetyt SharePoint-palvelut ja niissä tehdyt toimet.

11.3.2. Materiaalin jakaminen asiakkaille

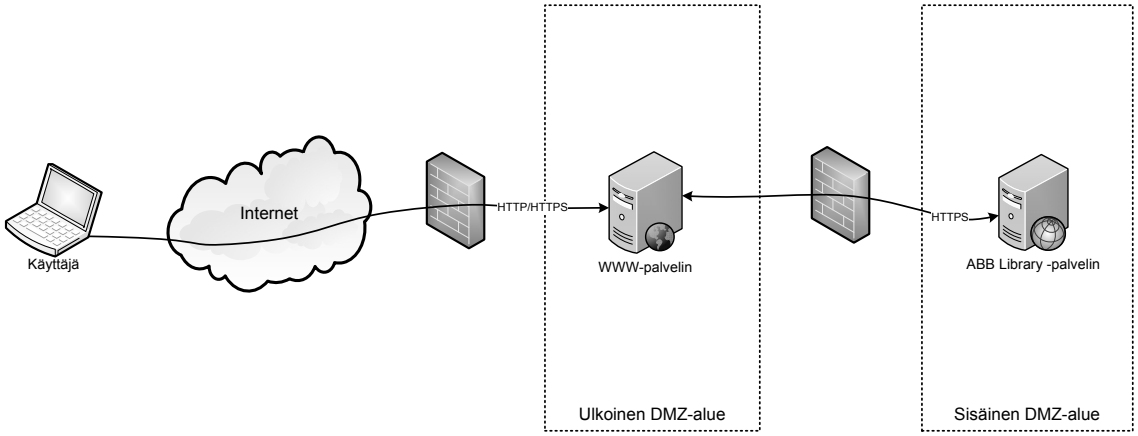
Materiaalin jakamiseen asiakkaille on käytössä kaksi eri mallia. Jaettavan materiaalin ollessa luottamuksellista käytetään sisäisellä DMZ-alueella olevaa SharePoint-alustaa ja ulkoisella DMZ-alueella olevaa SSL- tai TLS-protokollaa

yhteyksien suojaamiseen käyttävää sovellusyhdyskäytävää. Sovellusyhdyskäytävä vastaa käyttäjien tunnistamisesta, autentikoinnista ja valtuuttamisesta. Sovellusyhdyskäytävä käyttää käyttäjien autentikointiin ja valtuuttamiseen sisäisellä DMZ-alueella sijaitsevia autentikointipalvelimia. Autentikointi voidaan tehdä joko ADAM-palvelimen tarjoamien autentikointipalveluiden kautta tai vaihtoehtoisesti kertakäyttösalasanoja tukevan palvelimen kautta.

Mikäli jaettava materiaali on luonteeltaan yleistä, materiaalin jakamiseen käytetään yhtymän tarjoamaa ABB Library -palvelua. Palvelua käytetään ulkoiselle DMZ-alueelle sijoitettujen WWW-palvelimien kautta.

Kun materiaalia jaetaan asiakkaille SharePoint-palveluiden avulla, verkon palomuurisäännöt ovat samat kuin kappaleessa 11.3.1. esitetyt. Mikäli käytetään ABB Library -palvelua, ulkoisella DMZ-alueella sijaitsevaan WWW-palvelimeen tulee sallia HTTP- ja HTTPS-yhteydet. Lisäksi tulee sallia HTTPS-yhteydet WWW-palvelimesta sisäisen DMZ-alueen ABB Library -palvelimeen.

Kuvassa 29 on esitetty yksinkertaistettu malli ABB Library -palvelun käyttämistä yhteyksistä ja palvelimista.



Kuva 29. Yhteydet ABB Library -palveluun.

Jos materiaalin jakamiseen käytetään SharePoint-alustaa ja sovellusyhdyskäytävää, tapahtumalokiin kirjataan sovellusyhdyskäytävään tulleet yhteyspyynnöt, onnistuneet ja epäonnistuneet autentikoinnit sekä

käytetyt SharePoint-palvelut ja niissä tehdyt toimet. ABB Library -palvelun tapauksessa tapahtumalokiin kirjataan palveluun tulleet yhteyspyynnöt, onnistuneet ja epäonnistuneet autentikoinnit sekä palvelussa tehdyt toimet.

11.3.3. Etävalvontainformaatio kerääminen palvelimeen

Suositeltava tapa toteuttaa laitteiden ja järjestelmien etävalvonta on käyttää menetelmää, jossa valvottava järjestelmä tai laite lähettää tilainformaatiota itsenäisesti ABB Oy:n ulkoisella DMZ-alueella sijaitsevaan palvelimeen. Tapauksissa, joissa käytetään tai on mahdollista käyttää valvottavan järjestelmän yhteydessä PC-työasemia, voidaan etävalvontayhteydet toteuttaa yhtymän RAP-konseptin mukaisesti.

Palomuurisäännöt tulee määritellä siten, että ulkoisella DMZ-alueella olevaan valvontainformaation keräämiseen tarkoitettuun palvelimeen sallitaan asiakasverkosta tulevat tilainformaation siirtoon tarkoitetut tietoliikenneyhteydet. Lisäksi etävalvontatietojen lukemista varten sallitaan sisäverkosta tulevat palvelimeen kohdistuvat HTTPS- ja SSH-yhteydet. Asiakasverkon palomuurit ja reitittimet tulee määritellä niin, että etävalvontainformaation siirtoon käytettävät yhteydet sallitaan ABB Oy:n ulkoisella DMZ-alueella olevaan palvelimeen.

Kuvassa 30 on esitetty periaatekuva etävalvontainformaation keräämisestä. Edellä kuvattu menetelmä on käytössä asiakasverkko A:n kohdalla.

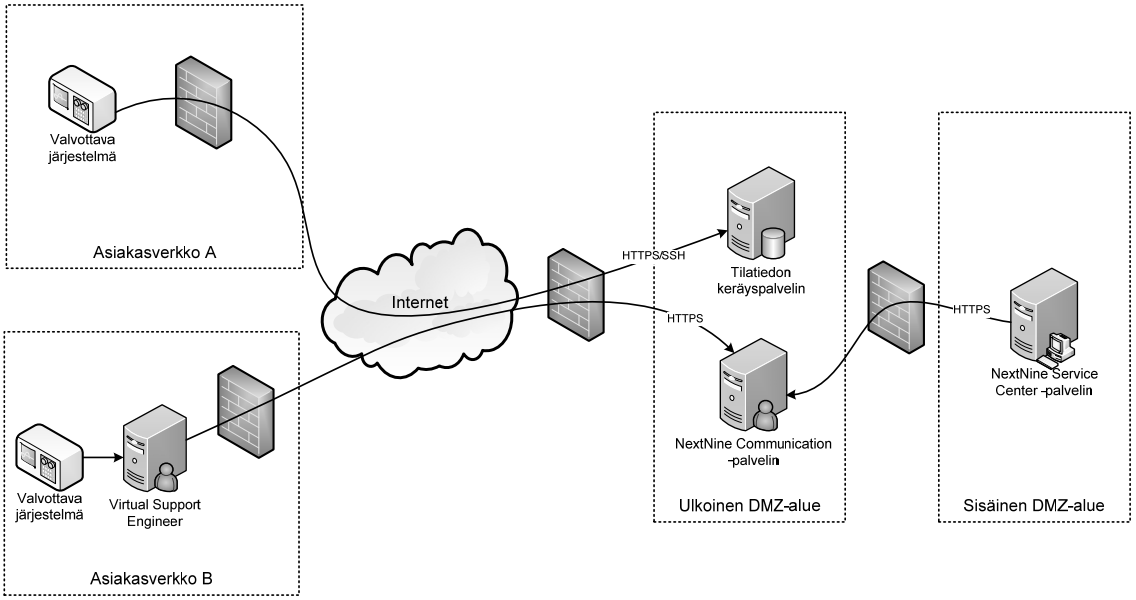
Tapahtumalokiin kirjataan palvelimeen sisä- ja ulkoverkosta tulleet hyväksytyt ja hylätyt yhteyspyynnöt sekä niiden yksityiskohdat.

Mikäli etävalvontainformaation keräämiseen käytetään RAP-konseptia, ulkoiselle DMZ-alueelle sijoitetaan NextNine Communications -palvelin ja sisäiselle DMZ-alueelle NextNine Service Center -palvelin (Wnek 2009).

Palomuuriasetukset tulee tehdä siten, että ulkoisella DMZ-alueella olevaan NextNine Communication -palvelimeen sallitaan asiakasverkon VSE-sovellukselta ja sisäisen DMZ-alueen NextNine Service Center -palvelimelta tulevat HTTPS-yhteydet. Lisäksi NextNine Service Center -palvelimeen

sallitaan sisäverkon ylemmän luottamuksellisuustason verkkosegmenteistä tulevat HTTPS-yhteydet.

Kuvassa 30 käytetään asiakasverkko B:n tapauksessa RAP-konseptia.



Kuva 30. Etävalvontainformaation kerääminen palvelimeen.

RAP-konseptia käytettäessä tapahtumalokiin kirjataan palvelimiin sisä- ja ulkoverkosta tulleet hyväksytyt ja hylätyt yhteyspyynnöt sekä niiden yksityiskohdat.

11.3.4. Suorat etävalvonta- ja etähallintayhteydet

Mikäli valvottava laite tai järjestelmä ei kykene itsenäisesti välittämään valvontainformaatiota, tilatiedot on luettava suoraan valvottavasta järjestelmästä etäkäyttöyhteyden yli. Informaation lukemiseen käytettäviä etäkäyttöyhteyksiä voidaan useissa tapauksissa käyttää myös järjestelmien etähallintaan.

Etäkäyttöyhteydet asiakkaan verkkoon toteutetaan SSL- tai TLS-protokollaa käyttävinä VPN-yhteyksinä. VPN-yhteyden terminointipiste sijoitetaan asiakasverkossa loogisesti mahdollisimman lähelle valvottavaa järjestelmää tai

laitetta ja ABB:n verkossa etäkäyttösegmenttiin. Etäkäyttösegmentissä VPN-tunneliin menevä ja tunnelista tuleva tietoliikenne suodatetaan palomuurin läpi ennen reitittämistä muualle verkkosegmenttiin. SSL/TLS VPN -yhteydet luodaan käyttämällä niin sanottua Reverse Proxy -tekniikkaa sijoittamalla fyysinen SSL/TLS VPN -yhdyskäytävä asiakkaan verkkoon.

Varsinainen etävalvonta- tai etähallintayhteys muodostetaan VPN-yhteyden päälle käyttämällä etäkäyttösegmentin tarjoamia sovellus- ja laiteresursseja. Etäkäyttösegmenttiin sijoitetaan palvelimia, joissa ajetaan tietyille etäkäyttöyhteyksille varattuja virtuaalikoneita, joihin on asennettu kyseisessä etäkäyttöyhteydessä tarvittavat sovellukset ja protokollat sekä ohjelmistopalomuuri VPN-liikenteen suodattamiseen.

SSL- tai TLS-protokollalla suojatut yhteydet virtuaalikoneille muodostetaan sisäiselle DMZ-alueelle sijoitetun sovellusyhdyskäytävän avulla. Käytettävä sovellusyhdyskäytävä vastaa käyttäjien tunnistamisesta, autentikoinnista ja valtuuttamisesta, muodostaa suojatun yhteyden käyttäjän haluamaan virtuaalikoneeseen, toimii yhteyden välittäjänä ja viestinnän päätyttyä purkaa käytetyn yhteyden. Sovellusyhdyskäytävä käyttää käyttäjien autentikointiin ja valtuuttamiseen sisäisellä DMZ-alueella olevaa ADAM-autentikointipalvelua. Sisäisen DMZ-alueen sovellusyhdyskäytävän avulla voidaan sallia myös ulkoisen DMZ-alueen sovellusyhdyskäytävällä autentikoidun ja valtuutetun käyttäjän pääsy etäkäyttösegmenttiin.

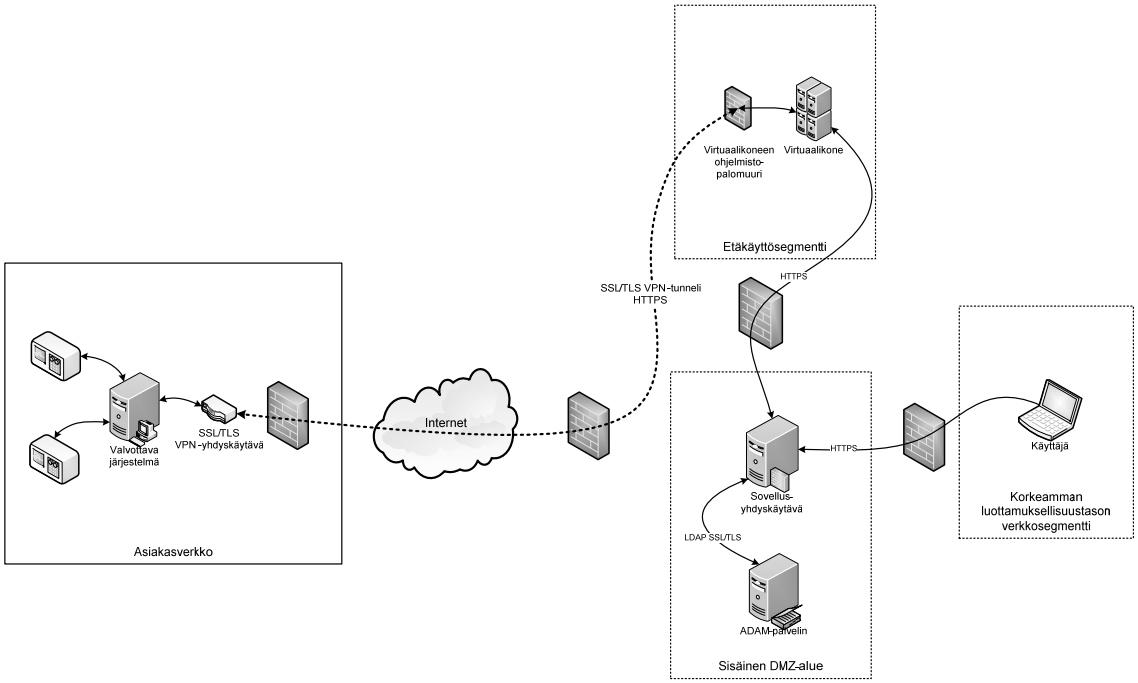
Sisäverkosta tuleva käyttäjä voi etäkäyttää virtuaalikonetta sovellusyhdyskäytävän tarjoamalla selainpohjaisella etäkäyttösovelluksella. Toisena vaihtoehtona on käyttää erillistä etähallintasovellusta. Ulkoverkosta tulleet käyttäjät voivat sen sijaan käyttää vain selainpohjaista etäkäyttösovellusta.

Asiakasverkon palomuurit on määritettävä sallimaan ABB Oy:n etäkäyttösegmentistä tulevat HTTPS-yhteydet verkkoon sijoitettuun SSL- tai TLS-yhdyskäytävään.

ABB:n verkon palomuurisäännöt asetetaan sallimaan virtuaalikoneilta lähtevät HTTPS-yhteydet asiakasverkkoon, virtuaalikoneille sisäisen DMZ-alueen

sovellusyhdyskäytävältä tulevat HTTPS-yhteydet sekä ylemmän luottamuksellisuustason verkkosegmenteistä sisäisen DMZ-alueen sovellusyhdyskäytävään tulevat HTTPS-yhteydet. Lisäksi virtuaalikoneiden ohjelmistopalomuurit määritetään sallimaan sovellusyhdyskäytävältä tuleva ja etävalvottavaan tai -hallittavaan järjestelmään lähtevä tiettyä etäkäyttöprotokollaa käyttävä tietoliikenne.

Kuvassa 31 on esitetty periaatekuva etähallintayhteyksien muodostaminen.



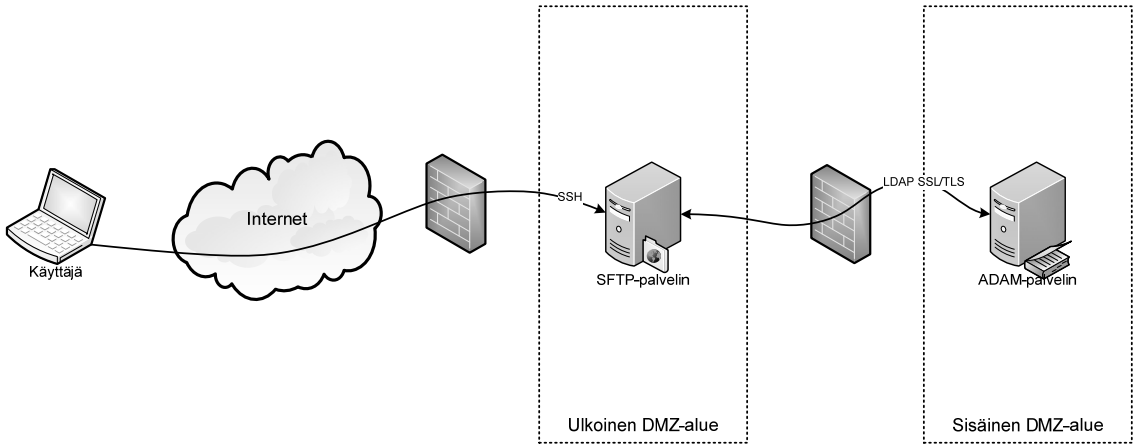
Kuva 31. Suorat etävalvonta- ja etähallintayhteydet asiakasverkkoon.

Tapahtumalokiin kirjataan sisäisen DMZ-alueen sovellusyhdyskäytävään, etäkäyttösegmentin virtuaalikoneisiin ja asiakasverkon VPN-yhdyskäytävään tulleet yhteyspyynnöt sekä onnistuneet että epäonnistuneet autentikoinnit.

11.3.5. Suurten tiedostojen siirtäminen

Suurten tiedostojen ja tietomassojen kuten varmuuskopioiden siirtoa varten ulkoiselle DMZ-alueelle sijoitetaan SFTP-palvelin, joka vastaa tiedonsiirron lisäksi tiedon säilytyksestä sekä käyttäjien tunnistamisesta, autentikoinnista ja valtuuttamisesta. Palvelin käyttää käyttäjien autentikointiin ja valtuuttamiseen

sisäisen DMZ-alueen ADAM-palvelimen tarjoamia autentikointipalveluita. Tarvittavat palvelimet ja niiden väliset yhteydet on esitetty kuvassa 32.



Kuva 32. Yhteydet SFTP-palvelimeen.

Palvelimen käyttöä varten ulkoiselle DMZ-alueelle sallitaan ulko- ja sisäverkosta SFTP-palvelimelle tulevat SSH-yhteydet. Lisäksi sallitaan autentikoinnissa tarvittavat SSL- tai TLS-protokollalla suojatut LDAP-yhteydet palvelimen ja sisäisellä DMZ-alueella olevan autentikointipalvelun välillä.

SFTP-palvelimen yhteydessä tapahtumalokiin kirjataan palvelimeen sisä- ja ulkoverkosta tulleet yhteyspyynnöt sekä onnistuneet ja epäonnistuneet autentikoinnit.

11.3.6. Materiaalin välittäminen alihankkijoilta asiakkaille

Materiaalin välittämiseen alihankkijoilta asiakkaille käytetään kappaleissa 11.3.1. ja 11.3.2. mainittuja SharePoint- ja sovellusyhdyskäytäväpalveluita.

11.3.7. Tietokantojen synkronointi

Tietokantojen synkronointi julkisen verkon yli toteutetaan etäyhteyssegmenttiin sijoitettujen palveluiden kautta. Etäyhteyssegmenttiin sijoitetaan tietokantapalvelin, jonka sisältämä tietokanta tai tietokannat synkronoidaan alihankkijan verkossa olevan tietokannan kanssa.

Etäyhteyssegmentillä oleva tietokanta on kopio sisäverkon tietyllä korkeamman luottamuksellisuustason verkkosegmentillä olevasta tietokannasta. Kopio ja alkuperäinen kanta synkronoidaan ylemmän tason tietokantapalvelimen aloitteesta. Kopio sisältää vain synkronoitavaksi tarkoitetun datan.

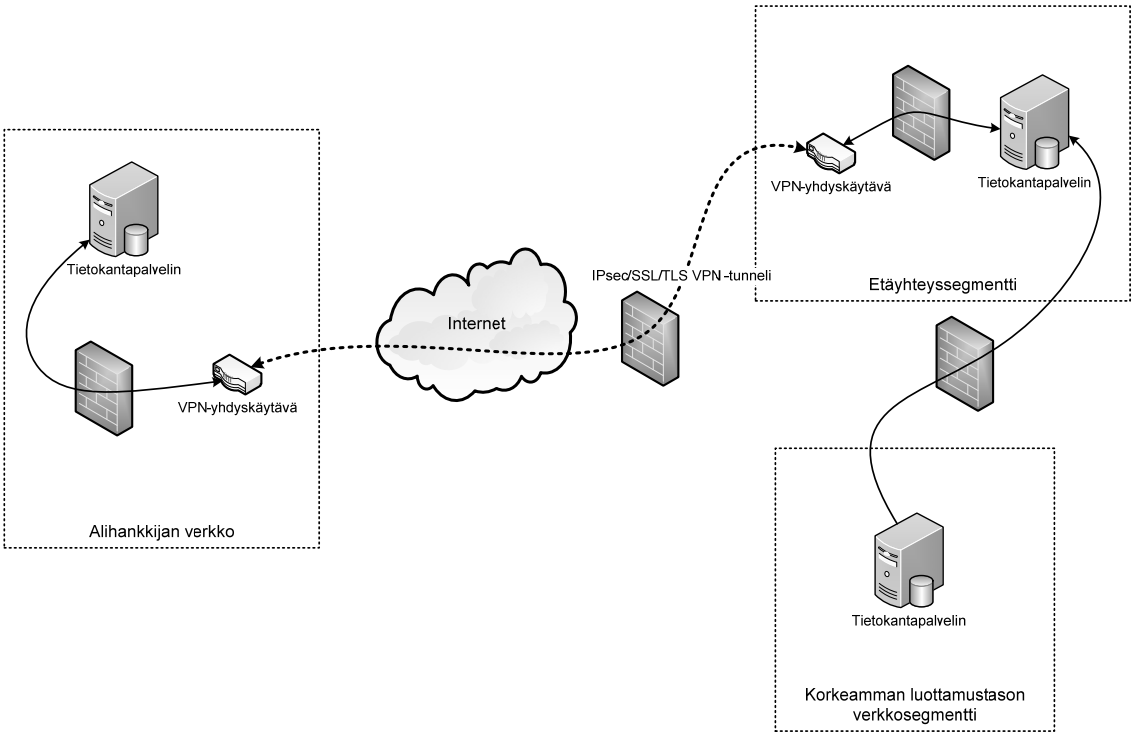
Synkronointi alihankkijan tietokannan kanssa tehdään alihankkijan ja ABB Oy:n verkon välille muodostetun IPsec tai SSL/TLS VPN -yhteyden yli. VPN-yhteys terminoidaan alihankkijan verkossa mahdollisimman lähelle tietokantapalvelinta ja ABB:n verkossa etäyhteyssegmentille sijoitettuun VPN-yhdyskäytävään. VPN-tunneliin menevä ja tunnelista tuleva tietoliikenne suodatetaan etäyhteyssegmentissä VPN-yhdyskäytävän ja tietokantapalvelimen väliin sijoitetulla palomuurilla.

Synkronointia varten tulee sallia etäyhteyssegmentillä ja alihankkijan verkossa olevien VPN-yhdyskäytävien välinen VPN-liikenne. Lisäksi etäyhteyssegmentin tietokantapalvelimeen sallitaan tietoliikenneyhteydet korkeamman tason verkkosegmenttien tietokantapalvelimista.

Etäyhteyssegmentillä oleva VPN-yhdyskäytävän ja tietokantapalvelimen välistä tietoliikennettä valvova palomuuri asetetaan sallimaan ainoastaan synkronoitavien tietokantojen välinen tietoliikenne.

Myös alihankkijan verkossa on sallittava ABB Oy:n etäyhteyssegmentiltä tuleva VPN-yhdyskäytävään kohdistuva VPN-liikenne. Lisäksi on sallittava synkronoitavaan tietokantapalvelimeen kohdistuva etäyhteyssegmentin tietokantapalvelimelta tuleva tietoliikenne.

Kuvassa 33 on esitetty tietokantojen synkronoinnissa tarvittavat palvelimet ja yhteydet.



Kuva 33. Tietokantojen synkronoinnissa tarvittavat yhteydet.

Tietokantojen synkronoinnin yhteydessä tapahtumalokiin kirjataan etäyhteyssegmentin tietokantapalvelimeen kohdistuneet ja siitä lähteneet synkronointipyynnöt sekä sisä- että ulkoverkon osalta. Lisäksi lokiin tulee kirjata tieto synkronoinnin yhteydessä muutetuista tiedoista.

11.4. Muiden tunnistettujen tarpeiden toteuttaminen

Määriteltyjä palvelukonsepteja voidaan soveltaa lisäksi useiden jatkokäsittelyn ulkopuolelle jääneiden yksittäisten tarpeiden toteuttamiseen.

Etävalvontainformaation kerääminen palvelimeen -palvelukonseptissa laadittua perusmallia, jossa julkisesta verkosta sallitaan suojatut yhteydet ABB Oy:n ulkoisella DMZ-alueella olevaan palvelimeen, voidaan hyödyntää useissa tuotepäivitysten tarkastamiseen ja lataamiseen, tilausten seurantaan, lisenssien tarkastamiseen, tuoteräätälöintiin sekä -myyntiin liittyvissä tarpeissa.

Materiaalin jakaminen asiakkaille -konseptissa esitellyllä ABB Library -palvelulla voidaan toteuttaa joitakin tuotetukipalveluihin liittyviä tarpeita.

Materiaalin jakamiseen alihankkijoille -palvelukonseptissa käytettävä SharePoint soveltuu myös tuotekehitystyökalujen alustaksi, joten konseptia voidaan hyödyntää myös hajautetun tuotekehityksen joidenkin tarpeiden toteuttamiseen.

Palvelukonsepti, jossa määritellään suorien etävalvonta- ja etähallintayhteyksien rakentaminen asiakasverkkoon, on VPN-yhteyksien muodostamisen osalta sovellettavissa tarpeisiin, joissa vaaditaan sovelluskerroksella suojattuja yhteyksiä kolmansien osapuolien verkkojen sisältämiin palveluihin. Esimerkkinä mainittakoon tarpeet, joissa tarvitaan yhteyksiä asiakkaan tai alihankkijan verkossa sijaitseviin materiaalipankkeihin.

Tarvekartoituksessa esiin nousseet tarpeet alihankkijoiden yhteyksistä toiminnanohjausjärjestelmiin, konsulttien yhteyksistä tiettyihin sisäverkon palveluihin, ABB:n verkossa olevien laitteiden ja järjestelmien etävalvontayhteydet sekä kaksisuuntaiset yhteydet alihankkijan verkossa oleviin järjestelmiin voidaan pääosin toteuttaa tietokantojen synkronointi -konseptissa määritellyin perusratkaisuin.

11.5. Vertailu lähtötilanteeseen

Määritelty yleinen malli tuo useita etuja aiemmin käytettyihin yksikkökohtaisiin ratkaisuihin verrattuna.

Yleisessä mallissa määritelty ABB Oy:n tietoliikenneverkon looginen rakenne lisää merkittävästi verkon joustavuutta aiempaan rakenteeseen verrattuna. Uudet ulko- ja sisäverkon rajalle luodut verkkosegmentit antavat mahdollisuuden sijoittaa verkkopalveluita tarkoituksenmukaisemmin. Joustavuuden lisäksi muutos parantaa verkon tietoturvaa rajaamalla mahdolliset tietoturvaongelmat ja -hyökkäykset aiempaa pienemmälle alueelle. (Pfleeger ym. 2006; Laaksonen ym. 2006: 182; Young 2001; Maley 2001: 6–7.)

Toinen tietoturvan kannalta merkittävä asia on luottamuksellisen informaation siirtoon käytettävien tietoliikenneyhteyksien suojaaminen sovelluskerroksella. Aiempiin suojaamattomiin tai vain verkkokerroksella suojattuihin yhteyksiin nähden, sovellustason suojaus takaa viestinnälle korkeamman tason luottamuksellisuuden (Pfleeger ym. 2006). Vaikka sovelluskerroksella tehtävä suojaus kuluttaakin verkkokerroksella tehtävää suojausta enemmän laskentaresursseja, se ei tarkastelluissa tapauksissa muodostu merkittäväksi ongelmaksi nykyisillä laiteresursseilla (Beltran ym. 2004).

Tietoturvanäkökulmasta kolmas merkittävä etu aiempaan nähden on kerättävälle loki-informaatiolle mallissa määritellyt kriteerit. Kattavien tapahtumalokien avulla voidaan muun muassa palautua mahdollisista tiemurroista ja murtoyrityksistä. (Lucas ym. 2006: 344.)

Yleinen malli ja siinä määritellyt palvelukonseptit yksinkertaistavat tietoliikenneyhteyksien hallintaa ja valvontaa sekä vähentävät hyökkäyspinta-alaa korvaamalla useita rinnakkaisia ratkaisuja yhteisillä vakioiduilla ratkaisuilla (Alateeq 2005). Rinnakkaisten ratkaisujen vähentämisellä voidaan myös vähentää sitoutuvia laite- ja sovellusresursseja, ja siten saavuttaa mahdollisia kustannussäästöjä (Porter 1988; Haverila ym. 2009: 357–358).

Sitoutuvia laiteresursseja voidaan vähentää merkittävästi käyttämällä virtualisointitekniikoita etähallinta- ja etävalvontayhteyksien yhteydessä (Crosby ym. 2006: 6).

Yleinen malli mahdollistaa myös palveluiden ylläpidon laajamittaisemman ja tehokkaamman keskittämisen, jonka avulla voidaan saavuttaa huomattavia kustannussäästöjä (Porter 1988; Haverila ym. 2009: 357–358).

Yhteyksien ja palveluiden tietoturvaa parantaa myös se, että palvelukonsepteissa pyritään käyttämään mahdollisimman laajamittaisesti hyödyksi olemassa olevia luotettavia autentikointipalveluita. Autentikointi-informaation keskittämisellä yksinkertaistetaan palveluiden ylläpitoa merkittävästi aiempiin yksittäisiin yksikkökohtaisiin ratkaisuihin verrattuna. (Ojaluoma 2008: 8.)

Liiketoimintayksiköiden näkökulmasta yleisen mallin ja siinä määriteltyjen palvelukonseptien käyttöönotto yksinkertaistaa tietoliikenneyhteyksien muodostamista kolmansien osapuolien kanssa. Mallin avulla yksiköt voivat muodostaa yhteyksiä huomattavasti aiempaa nopeammin ja edullisemmin. Myös mallin rakennusvaiheessa huomiotta jääneiden tarpeiden ratkaiseminen on aiempaa yksinkertaisempaa, koska niiden ratkaisemiseen voidaan soveltaa palvelukonsepteissa määriteltyjä perusperiaatteita ja käytäntöjä.

Yleisen mallin mukanaan tuoma ristiriitainen muutos on byrokratian lisääntyminen. Muutos on liiketoimintayksiköiden näkökulmasta heikkous, mutta tietohallinnon ja tietoturvan näkökulmasta etu. Byrokratian avulla voidaan osaltaan varmistaa, että luotavat yhteydet ja käyttöönotettavat palvelut ovat oikeasti tarpeellisia, täyttävät tietyt tietoturvakriteerit ja ovat kaikkien osapuolien tiedossa (Laaksonen ym. 2006: 146–155). Ero nykyiseen käytäntöön, jossa yksiköt ovat voineet tehdä käyttämiinsä yhteyksiin ja palveluihin muutoksia varsin vapaasti, on huomattava. Muutoksia on voitu tehdä jopa tietohallinnon niistä mitään tietämättä.

Käyttäjänäkökulmasta yleinen malli ja siinä määritellyt palvelukonseptit tuovat joustavuutta ja suoraviivaisuutta palveluiden käyttöön. Määriteltyjen konseptien myötä esimerkiksi palveluiden käyttöön tarvittavien salasanojen lukumäärä vähenee ja yhä useampaa palvelua voidaan käyttää ilman erikoissovelluksia tai -laitteita. Salasanojen lukumäärän vähentämisellä on positiivinen vaikutus käytettävyyden lisäksi myös tietoturvaan (Johnston, Eloff & Labuschagne 2003: 3; Tiwari & Joshi 2009: 1). Palvelut ovat myös saavutettavissa entistä helpommin ja työntekijät voivat esimerkiksi ottaa tiettyihin palveluihin yhteyttä suoraan ulkoverkosta ilman monimutkaisia IPsec VPN -yhteyksiä.

11.6. Mallin käyttöönotto

Yleisen mallin käyttöönotto aloitetaan tekemällä tietoliikenneverkkoon mallissa määritellyt muutokset. Loogisen rakenteen muuttaminen vaatii muutoksia verkon reititys- ja palomuurisääntöihin sekä joidenkin palveluiden uudelleensijoittamista. Uudelleensijoittamisen yhteydessä joudutaan

todennäköisesti tekemään myös joitakin muutoksia siirrettyjä palveluita käyttäviin järjestelmiin.

Kun verkon looginen rakenne vastaa mallissa määriteltyä, voidaan aloittaa palvelukonsepteissa määriteltyjen palveluiden ja tarvittavien yhteyksien rakentaminen. Verkon loogisen rakenteen muokkaaminen ja määriteltyjen palveluiden toteuttaminen tehdään tietohallinnon johdolla.

Käyttöönoton seuraava vaihe aloitetaan, kun palvelukonsepteissa määritellyt palvelut ovat valmiina. Kolmannessa vaiheessa olemassa olevat rinnakkaiset ratkaisut korvataan vaiheittain konseptissa määritellyillä yleisillä ratkaisuilla. Olemassa olevien ratkaisujen korvaaminen aiheuttaa luonnollisesti lisätyötä myös liiketoimintayksiköissä.

Jotta määritetystä yleisestä mallista saadaan kaikki hyöty irti, käyttöönoton yhteydessä on tärkeää keskittää palveluiden ylläpitoa tietohallinnolle. Keskittämisen yhteydessä on kuitenkin huomioitava, ettei byrokratiaa lisätä tarpeettomasti. Yhteiset ratkaisut pysyvät yhteisinä ratkaisuina vain, jos yksiköt kokevat saavansa lisääntyvän byrokratian vastapainoksi merkittäviä etuja.

Kolmannen vaiheen jälkeen siirrytään ylläpito- ja kehittämisvaiheeseen, jossa on tärkeää säilyttää tiivis yhteys liiketoimintayksiköihin ja kehittää olemassa olevia palveluita vastaamaan entistä paremmin yksiköiden toiveita. Ylläpito- ja kehittämisvaiheessa on kartoitettava proaktiivisesti liiketoimintayksiköiden uusia käyttötarpeita. Tunnistettuihin käyttötarpeisiin tulee myös reagoida.

12. YHTEENVETO

Nykyisin yritysten tietoliikenneverkoille kohdistuu varsin monenlaisia vaatimuksia. Verkkojen on kyettävä mukautumaan muun muassa niitä hyödyntävien tietojärjestelmien laajenemiseen, uusiin käyttötarpeisiin ja jatkuvasti lisääntyviin liikennemääriin. Verkkojen odotetaan toimivan taustalla läpinäkyvästi ja ennen kaikkea tietoturvallisesti.

Tietoliikenneverkon tietoturvallisuus muodostuu lukuisista toisiinsa vaikuttavista teknisistä ja hallinnollisista elementeistä. Huomattavaa on, että verkon kokonaistietoturva määräytyy aina tietoturvaltaan heikoimman yksittäisen elementin perusteella.

Tutkimuksessa keskityttiin TCP/IP-protokollapinoa käyttävien yritysverkkojen tietoturvallisuuteen, jota tarkasteltiin lähinnä teknillisellä tasolla. Aihealuetta lähestyttiin esimerkkiyrityksenä toimineen ABB Oy:n näkökulmasta.

Tutkimuksen tavoitteena oli määrittää yleinen tietoturvallinen malli tietoliikenneyhteyksien muodostamiseen ABB Oy:n ja kolmansien osapuolien tietojärjestelmien välille. Mallin tuli kattaa merkittävimmät liiketoiminnan käyttötarpeet.

Eräs osa tutkimusta olikin eri liiketoimintayksiköiden olemassa olevien käyttötarpeiden kartoittaminen ja olennaisten tarpeiden tunnistaminen.

Tutkimuksen lopputuloksena luotu yleinen malli täyttää sille asetetut tavoitteet ainakin teoreettisella tasolla. Varsinaisen toteutuksen suhteen malli määrittelee lähinnä ääriviivat tarpeiden ratkaisemiseksi ja antaa siten varsinaiselle toteutukselle jonkin verran liikkumavaraa.

Mallissa määriteltyjen palvelukonseptien avulla voidaan toteuttaa liiketoiminnan kannalta olennaisiksi valitut käyttötarpeet yhtymän virallista tietoturvapolitiikkaa noudattaen. Luotu malli ylittää joiltakin osin virallisen tietoturvapolitiikan vaatimukset. Esimerkkinä mainittakoon tietoliikenneyhteyksien suojaaminen sovelluskerroksella verkkokerroksen sijaan, mikäli yhteyden yli siirretään luottamuksellista informaatiota. Lisäksi

yleisessä mallissa määritellyt palvelukonseptit hyödyntävät mahdollisimman laajalti olemassa olevia ratkaisuja ja palveluita.

Mallia rakennettaessa kiinnitettiin erityistä huomiota valittujen ratkaisujen monikäyttöisyyteen, mukautumiseen mahdollisiin tuleviin tarpeisiin sekä käytettävyyteen ja läpinäkyvyyteen käyttäjänäkökulmasta. Tuleviin tarpeisiin on varauduttu suunnittelemalla verkon looginen rakenne joustavaksi, käyttämällä palvelukonsepteissa monikäyttöisiä ratkaisuja sekä sijoittamalla palvelut eri verkkosegmentteihin joustavasti. Palvelukonseptien yhteydessä määritellyt perusperiaatteet soveltuvat pikaisen tarkastelun perusteella myös jatkokäsittelyn ulkopuolelle jääneiden tarpeiden toteuttamiseen.

Ratkaisujen luotettavuutta on tavoiteltu käyttämällä mahdollisimman suoria tietoliikenneyhteyksiä sekä tarkoituksenmukaisia, mutta kuitenkin yleisiä protokollia.

Palvelukonsepteissa käytetyt ratkaisut on laadittu siten, että niiden käyttäminen on mahdollisimman yksinkertaista. Suunnittelussa tavoitteena on ollut, että käyttäjien tarvitsee kirjautua palveluita käyttääkseen vain yhteen järjestelmään ja, että käyttöön ei tarvita erikoisohjelmistoja tai -laitteita.

Yleisen mallin käyttöönotto on melko laaja operaatio, mutta verkon loogiseen rakenteeseen tehtäviä muutoksia lukuun ottamatta se voidaan tehdä suurilta osin häiritsemättä nykyisiä käytössä olevia järjestelmiä. Työmäärästä huolimatta, malli kannattaa ehdottomasti ottaa käyttöön erityisesti sen tarjoamien tietoturvaparannusten ja resurssisäästöjen vuoksi.

Luotu yleinen malli parantaa tietoverkon tietoturvaa muun muassa jakamalla verkon tarkemmin määriteltyihin verkkosegmentteihin, käyttämällä yleisesti sovellustasolla suojattuja yhteyksiä aiempien käytettyjen suojaamattomien tai vain verkkotasolla suojattujen yhteyksien sijaan, yksinkertaistamalla yhteyksien valvontaa ja hallintaa sekä vähentämällä hyökkäyspinta-alaa karsimalla rinnakkaisia ratkaisuja. Rinnakkaisten ratkaisujen karsiminen vähentää myös niiden kehittämiseen ja ylläpitämiseen kuluvia resursseja sekä mahdollistaa toimintojen laajamittaisemman keskittämisen.

Vaikka laadittu malli täyttää tutkimukselle asetetut tavoitteet, siinä on vielä selkeästi parantamisen varaa. Toteutettavuuden kannalta olisi tärkeää rajata tarkemmin eri tarpeiden ratkaisemiseen käytettävissä olevia sovelluksia ja protokollia. Lisäksi mallissa pitäisi määritellä myös hallinnollisen tason tietoturvakäytännöt ja käydä läpi kaikki ABB Oy:n sisäverkon verkkosegmentit sekä määritellä niiden väliset yhteydet.

Eräs yksittäinen lisäselvitystä vaativa aihealue on käyttäjätunnusten hallinta. Riittävän tietoturvatason saavuttaminen vaatii käytössä olevien järjestelmien kohdalla runsaasti käsityötä. Manuaalisen työn runsas määrä on ongelma sellaisten tarpeiden kohdalla, joissa yhteyksien tarvitsijoiden lukumäärä on suuri. Tilalle tarvittaisiin menetelmä, joka tunnistaisi ja todentaisi käyttäjät riittävän luotettavasti ja kykenisi luomaan käyttäjätunnukset mahdollisimman automaattisesti järjestelmään.

Toinen lisätyötä vaativa osa-alue on ABB:n tietoliikenneverkkojen loogisen rakenteen dokumentointi. Erityisesti yhtymänlaajuisten verkkopalveluiden dokumentaatiossa esiintyi runsaasti ristiriitaisuuksia verkon loogisen rakenteen suhteen.

LÄHDELUETTELO

ABB (2010a). *ABB Group* [online]. ABB Ltd:n Internet-sivut [siteerattu 25.3.2010]. Saatavana World Wide Webistä: <URL: http://www.abb.com/>.

ABB (2010b). *ABB* [online]. ABB Oy:n Internet-sivut [siteerattu 25.3.2010]. Saatavana World Wide Webistä: <URL: http://www.abb.fi/>.

ABB (2010c). *Shared SharePoint Infrastructure – ABB Collaboration Program* [online]. ABB Groupin Intranet-sivut [siteerattu 7.6.2010]. Saatavana World Wide Webistä: <URL: http://inside.abb.com/cawp/gad00138/5f0b86fc84d95368c12576a400368ef3.aspx>.

ABB (2010d). *ABB Library* [online]. ABB Groupin Intranet-sivut [siteerattu 7.6.2010]. Saatavana World Wide Webistä: <URL: http://fi.inside.abb.com/library>.

Alateeq, Ibrahim N. (2005). *Design Secure Network Segmentation Approach*. SANS Institute. 25 s. Saatavana World Wide Webistä: <URL: http://www.sans.org/reading_room/whitepapers/hsoffice/design-secure-network-segmentation-approach_1645>.

Anttila, Aki (2001). *TCP/IP-tekniikka*. 2. painos. Juva: WS Bookwell. 471 s. ISBN 951-832-061-6.

Bellovin, Steven M. & William R. Cheswick (1994). Network Firewalls. *IEEE Communications Magazine* 32: 9, 50–57.

Beltran, Vicenç, Jordi Guitart, David Carrera, Jordi Torres, Eduard Ayguadé & Jesus Labarta (2004). Performance Impact of Using SSL on Dynamic Web Applications. 6 s. *XV Jornadas De Paralelismo*. Barcelona: European Center for Parallelism of Barcelona. 6 s.

Black, Uyless D. (1998). *TCP/IP and related protocols*. 3. painos. New York etc.: McGraw-Hill Inc. 402 s. ISBN 0-07-913282-0.

CCNA Notes (2010). *LAN Segmentation* [online]. [siteerattu 18.5.2010]. Saatavana World Wide Webistä: <URL: http://netcert.tripod.com/ccna/internetworking/lanseg.html>.

Chokhani, Santosh, Warwick Ford, Randy V. Sabett, Charles R. Merrill & Stephen S. Wu (2003). *Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework*. IETF RFC 3647. 94 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc3647.txt>.

Comer, Douglas E. (2000). *Internetworking with TCP/IP: Principles, Protocols, and Architectures*. 4. painos. New Jersey: Prentice-Hall Inc. 750 s. ISBN 0-13-018380-6.

Crosby, Simon & David Brown (2006). The Virtualization Reality. *ACM Queue* 4: 10, 34–41.

Dierks, Tim & Eric Rescorla (2008). *The Transport Layer Security (TLS) Protocol Version 1.2*. IETF RFC 5246. 104 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc5246.txt>.

Dierks, Tim & Christopher Allen (1999). *The TLS Protocol Version 1.0*. IETF RFC 2246. 80 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc2246.txt>.

Dillard, Clayton, Mia Stephanson, Gene Bouley & Bill Wiesendanger (2003). *External Connectivity Baseline Policies*. 13 s. ABB Group Processes 9AAD103843. Julkaistu sisäiseen käyttöön.

Forte, Dario (2009). *SSL VPN and Return on Investment: A Possible Combination*. Network Security 2009: 10, 17–19.

Galbraith, Joseph & Oskari Saarenmaa (2006). *SSH File Transfer Protocol*. IETF Internet-Draft. 60 s. Saatavana World Wide Webistä: <URL: http://tools.ietf.org/id/draft-ietf-secsh-filexfer-13.txt>.

Harding, Andrew (2003). SSL Virtual Private Networks. *Computers & Security* 22: 5, 416–420.

Harris, Brendon & Ray Hunt (1999). TCP/IP Security Threats and Attack Methods. *Computer Communications* 22: 10, 885–897.

Haverila, Matti J., Erkki Uusi-Rauva, Ilkka Kouri & Asko Miettinen (2009). *Teollisuustalous*. 6. painos. Tampere: Hämeen kirjapaino Oy. ISBN 978-951-96765-6-2.

Hirsjärvi, Sirkka, Pirkko Remes & Paula Sajavaara (2008). *Tutki ja kirjoita*. 13–14. osin uudistettu painos. Helsinki: Tammi Oy. ISBN 951-26-5635-6.

Huitema, Christian (1998). *IPv6: The New Internet Protocol*. 2. painos. New Jersey: Prentice Hall Inc. 247 s. ISBN 978-0-13-850505-5.

IEEE 802.1Q (2003). *IEEE Standards for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks*. New York: IEEE. 327 s. ISBN 0-7381-3662-X.

IETF STD. *IETF Internet Standards* [online]. [siteerattu 27.5.2010]. Saatavana World Wide Webistä: <URL: http://www.apps.ietf.org/rfc/stdlist.html>.

ITU-T X.509 (2006). *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*. Geneve: International Telecommunication Union. 174 s.

Johnston, J., J. H. P. Eloff & L. Labuschagne (2003). Security and Human Computer Interfaces. *Computers & Security* 22: 8, 675–684.

Jäggli, Christian & Anatoliy Khylenko (2009). *Application Integration Steps: Global DMZ Authentication Service: Identity Service Solution*. 21 s. ABB Group 9AAD112328. Julkaistu sisäiseen käyttöön.

Kaufman, Charlie (2005). *Internet Key Exchange (IKEv2) Protocol*. IETF RFC 4306. 99 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc4306.txt>.

Kaufman, Charlie, Radia Perlman & Mike Speciner (2002). *Network Security: Private Communication in a Public World*. 2. painos. New Jersey: Prentice Hall Inc. 713 s. ISBN 0-13-046019-2.

Keanini, Tim (2005). Protecting TCP/IP. *Network Security* 2005: 11, 13–16.

Kent, Stephen (2005a). *IP Authentication Header*. IETF RFC 4302. 34 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc4302.txt>.

Kent, Stephen (2005b). *IP Encapsulating Security Payload (ESP)* [online]. IETF RFC 4303. 44 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc4303.txt>.

Kent, Stephen & Karen Seo (2005). *Security Architecture for the Internet Protocol*. IETF RFC 4301. 101 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc4301.txt>.

Kerttula, Esa (1998). *Tietoverkkojen tietoturva*. 1. painos. Helsinki: Oy Edita Ab. 510 s. ISBN 951-37-2672-X.

Krawczyk, Hugo, Mihir Bellare & Ran Canetti (1997). *HMAC: Keyed-Hashing for Message Authentication*. IETF RFC 2104. 11 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc2104.txt>.

Kulakowski, Andrzej (2008). *Short Update on the ABB Library*. ABB Group 9AKK101130D8111. Sisäiseen käyttöön julkaistu PowerPoint-esitys.

Laaksonen, Mika, Terho Nevasalo & Karri Tomula (2006). *Yrityksen tietoturvakäsikirja*. 1. painos. Helsinki: Edita Publishing Oy. 324 s. ISBN 951-37-4701-8.

Lehtonen, Satu (2004). *Turvallisuuden hallinta yrityksen langattomissa lähiverkoissa*. Diplomityö. Teknillinen korkeakoulu. 105 s.

LINFO (2005). *Network Segment Definition* [online]. [siteerattu 18.5.2010]. Saatavana World Wide Webistä: <URL: http://www.linfo.org/network_segment.html>.

Lucas, Mark, Anne Henmi, Abhishek Singh & Chris Cantrell (2006). *Firewall Policies and VPN Configurations*. 1. painos. Rockland: Syngress Publishing Inc. 482 s. ISBN 1-59749-088-1.

Maley, Brent (2001). *Network and System Planning – How to Reduce Risk on a Compromised System*. SANS Institute. 10 s. Saatavana World Wide Webistä: <URL: http://www.sans.org/reading_room/whitepapers/malicious/network-system-planning-reduce-risk-comprimised-system_89>.

Markham, Tom (1997). *Internet Security Protocol* [online]. Dr. Dobb's Journal [siteerattu 29.5.2010]. Saatavana World Wide Webistä: <URL: http://www.drdobbs.com/184410213>.

Microsoft (2009). *Design Extranet Farm Topology (Office SharePoint Server)* [online]. Microsoft TechNet [siteerattu 6.6.2010]. Saatavana World Wide Webistä: <URL: http://technet.microsoft.com/en-us/library/cc263513(office.12).aspx>.

Microsoft (2010a). *Microsoft SharePoint 2010 IT Professional Evaluation Guide*. Microsoft Whitepaper. 49 s. Saatavana World Wide Webistä: <URL: http://go.microsoft.com/fwlink/?LinkId=167123>.

Microsoft (2010b). *Hardware and Software Requirement (SharePoint Foundation 2010)* [online]. Microsoft TechNet [siteerattu 6.6.2010]. Saatavana World Wide Webistä: <URL: http://technet.microsoft.com/en-us/library/cc288751.aspx>.

Microsoft (2010c). *Overview of Forefront UAG Features* [online]. Microsoft TechNet [siteerattu 6.6.2010]. Saatavana World Wide Webistä: <URL: http://technet.microsoft.com/en-us/library/dd857382.aspx>.

Microsoft (2010d). *Why Enable SharePoint Extranet Access With Forefront UAG?* [online]. Microsoft TechNet [siteerattu 6.6.2010]. Saatavana World Wide Webistä: <URL: http://technet.microsoft.com/en-us/library/dd861393.aspx>.

Microsoft (2010e). *Active Directory* [online]. [siteerattu 16.6.2010]. Saatavana World Wide Webistä: <URL: http://www.microsoft.com/windowsserver2008/en/us/ad-main.aspx>.

Microsoft (2010f). *SharePoint Server 2010 Capacity Management: Software Boundaries and Limits* [online]. Microsoft TechNet [siteerattu 16.6.2010]. Saatavana World Wide Webistä: <URL: http://technet.microsoft.com/en-us/library/cc262787.aspx>.

Milza, Matthew & Scott Rogers (2005). *Securing a Lotus Domino Web Server* [online]. IBM Technical Library [siteerattu 19.6.2010]. Saatavana World Wide Webistä: <URL: http://www.ibm.com/developerworks/lotus/library/dominowebserver-security/>.

Mäkynen, Petri (2007). *Palveluntoimittajien etäkäyttöyhteydet*. Insinöörityö. Helsingin ammattikorkeakoulu. 62 s.

NextNine (2007). *NextNine Service Automation – System Overview*. NextNine Ltd. 37 s.

Ojaluoma, Juha (2008). *Mobiilitunnistamisen hyödyt ja mahdollisuudet Helsingin yliopistossa*. Pro Gradu -tutkielma. Helsingin yliopisto. 89 s.

Parziale, Lydia, David T. Britt, Chuck Davis, Jason Forrester, Wei Liu, Carolyn Matthews & Nicolas Rosselot (2006). *TCP/IP Tutorial and Technical Overview*. 8. painos. IBM Redbooks. 998 s. ISBN 0-7384-9468-2.

Pfleeger, Charles P. & Shari Lawrence Pfleeger (2006). *Security in Computing*. 4. painos. New Jersey: Prentice Hall. 880 s. Sähköinen kirja. ISBN 978-0-13-239077-4.

Porter, Michael E. (1988). *Kilpailuetu: Miten ylivoimainen osaaminen luodaan ja säilytetään.* 2. painos. Espoo: Weilin+Göös. ISBN 951-35-3548-7.

Reed, Damon (2003). *Applying the OSI Seven Layer Network Model to Information Security*. SANS Institute. 31 s. Saatavana World Wide Webistä: <URL: http://www.sans.org/reading_room/papers/index.php?id=1309>.

Rescorla, Eric (2000). *HTTP Over TLS*. IETF RFC 2818. 7 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc2818.txt>.

Rosen, Eric C., Arun Viswanathan & Ross Callon (2001). *Multiprotocol Label Switching Architecture*. IETF RFC 3031. 61 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc3031.txt>.

Rowan, Tom (2007). VPN Technology: IPsec vs. SSL. *Network Security* 2007: 12, 13–17.

Scarfone, Karen & Peter Mell (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. National Institute of Standards and Technology. 127 s. NIST Special Publication 800-94.

Shirey, R. (2000*). Internet Security Glossary*. IETF RFC 2828. 212 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc2828.txt>.

Simmons, Gustavus J. (1992). *Contemporary Cryptology: The Science of Information Integrity*. New York: IEEE Press. 640 s. ISBN 978-0-87-942277-6.

Sjöblom, Markus (2008). *Remote Monitoring of Industrial Frequency Converters*. Diplomityö. Vaasan yliopisto. 69 s.

Smith, Richard E. (1997). *Internet Cryptography*. 1. painos. Boston: Addison-Wesley Longman Publishing Co., Inc. 356 s. ISBN 0-201-92480-3.

Snyder, Joel (2010). *Forefront Unified Access Gateway 2010 Review* [online]. Techworld.com [siteerattu 6.6.2010]. Saatavana World Wide Webistä: <URL: http://review.techworld.com/encryption/3214550/forefront-unified-access-gateway-2010-review/>.

Stallings, William (2003). *Cryptography and Network Security: Principles and Practices*. 3. painos. New Jersey: Pearson Education Inc. 681 s. ISBN 0-13-111502-2.

Stallings, William (2007). *Data and Computer Communications*. 8. painos. New Jersey: Pearson Education Inc. 878 s. ISBN 0-13-243310-9.

Stallings, William, Lawrie Brown, Mick Bauer & Michael Howard (2008). *Computer Security: Principles and Practices*. 1. painos. New Jersey: Pearson Education Inc. 798 s. ISBN 978-0-13-513711-6.

Stanton, Ray (2005). Securing VPNs: Comparing SSL and IPsec. *Computer Fraud & Security* 2005: 9, 17–19.

Steinberg, Joseph & Tim Speed (2005). *SSL VPN: Understanding, Evaluating and Planning Secure, Web-based Remote Access: A Comprehensive Overview of SSL VPN Technologies and Design Strategies*. 1. painos. Packt Publishing. 212 s. Sähköinen kirja. ISBN 978-1-90-481107-7.

Stewart, William (2009). *Living Internet* [online]. [siteerattu 18.6.2010]. Saatavana World Wide Webistä: <URL: http://www.livinginternet.com/>.

Sähköisen viestinnän tietosuojalaki 17.3.2006/198.

Taimisto, Hannu (2010). *Periaatepiirrokset ABB Oy:n tietoliikenneverkon rakenteesta*. 2 s. Julkaisematon.

Tiwari, Paras B. & Shashidhar R. Joshi (2009). Single Sign-on with One Time Password. *Asian Himalayas Regional IEEE/IFIP International Conference on Internet 2009, 1–4*. Kathmandu: IEEE International. ISBN 978-1-4244-4569-1.

Valtiovarainministeriö (1999). *Valtioneuvoston periaatepäätös valtiohallinnon tietoturvallisuudesta*. Helsinki: Valtiovarainministeriö. Saatavana World Wide Webistä: <URL: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/6294_fi.pdf>.

Vitorino, Ivo (2009). *SRAnext Service – Architecture Design*. 15 s. ABB Group Reference Architecture 9AAD112346. Julkaistu sisäiseen käyttöön.

VPN Consortium (2008). *VPN Technologies: Definitions and Requirements* [online]. [siteerattu 27.3.2010]. Saatavana World Wide Webistä: <URL: http://www.vpnc.org/vpn-technologies.html>.

Wilson, Tim (2009). *Microsoft SharePoint: A Weak Link In Enterprise Security?* [online]. DarkReading.com [siteerattu 6.6.2010]. Saatavana World Wide Webistä: <URL: http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=212903345>.

WinSCP (2010). *Supported Transfer Protocols* [online]. WinSCP-sovelluksen dokumentaatio [siteerattu 20.6.2010]. Saatavana World Wide Webistä: <URL: http://winscp.net/eng/docs/protocols#sftp>.

Wnek, Maciej (2009). *Global ABB Remote Access Platform*. Sisäiseen käyttöön julkaistu PowerPoint-esitys.

Ylönen, Tatu & Chris Lonvick (2006). *The Secure Shell (SSH) Protocol Architecture*. IETF RFC 4251. 30 s. Saatavana World Wide Webistä: <URL: http://www.ietf.org/rfc/rfc4251.txt>.

Young, Scott (2001). *Designing a DMZ*. SANS Institute. 8 s. Saatavana World Wide Webistä: <URL: http://www.sans.org/reading_room/whitepapers/firewalls/designing-dmz_950>.

Zachry, Tiffany & Brian A. McCollum (2007). Constructing Online Workspaces for Collaboration: An Experience with Two Cases of Contrasting Systems. *Professional Communication Conference 2007*, 1–6. Seattle: IEEE International. ISBN 978-1-4244-1242-6.

Özsu, M. Tamer & Patrick Valduriez (1991). *Principles of Distributed Database Systems*. 2. painos. New Jersey: Prentice-Hall Inc. 666 s. ISBN 0-13-659707-6.

LIITTEET

LIITE 1. TCP/IP-protokollapinon haavoittuvuudet kerroksittain

1.1. Fyysinen kerros

Reed (2003: 5) toteaa fyysisen kerroksen olevan kaikkein haavoittuvin ympäristön muutoksille, ja pienetkin muutokset voivat aiheuttaa suuria tuhoja koko tietoverkossa. Vahingollinen muutos voi olla yksinkertaisimmillaan vahingossa irrotettu sähköjohto. Lisäongelmia tuottaa se, että fyysisellä kerroksella toimivien järjestelmien sekä laitteiden valvonta ja suojaaminen on sekä vaikeaa että kallista. Ongelma korostuu, koska häirintään ja tietoliikenteen kaappaamiseen soveltuvat järjestelmät sekä ohjelmistot ovat usein varsin yksinkertaisia ja siten myös edullisia. (Reed 2003: 5.)

Fyysinen kerros erottuu muista kerroksista konkreettisuudellaan; kerros koostuu lähinnä fyysisistä laitteista. Fyysisten laitteiden suojaus ja valvonta toteutetaan varsin perinteisin menetelmin esimerkiksi valvontakameroilla. Abstraktimmalla tasolla sovelletaan erilaisia salausmenetelmiä. (Reed 2003: 6; Pfleeger ym. 2006.)

Reed (2003: 6) ja Pfleeger ym. (2006) luettelevat fyysisen kerroksen haavoittuvuuksiksi virtakatkot, ympäristön muutokset, laitteiden varkaudet, laitteiden ja tiedon tuhoutumisen tai vahingoittumisen, toimintaympäristön luvattomat muutokset, tietoliikenteen häirinnän ja kaappaamisen sekä fyysisten siirtoyhteyksien vahingoittumisen. Mahdollisina kontrollointitapoina Reed (2003: 6) ja Pfleeger ym. (2006) mainitsevat suljetut kulunvalvonnan piirissä olevat tilat, kuva- ja äänivalvonnan, tiedon salauksen sekä elektromagneettisen suojauksen.

1.2. Siirtoyhteyskerros

Siirtoyhteyskerroksen suurin heikkous liittyy kerroksen tehtävään taata yhteensopivuus fyysisen kerroksen ja ylempien kerrosten välillä. Tehtävästä tekee haastavan fyysisen kerroksen laitteiden monimuotoisuus. Yhteensopivuuden saavuttamiseksi kerroksella joudutaan tukemaan myös heikosti suunniteltuja ja joissain tapauksissa myös vanhentuneita standardeja. (Reed 2003: 7.)

Reed (2003: 7) mainitsee siirtoyhteyskerrokselle sijoittuvan ARP-protokollan erityisen ongelmalliseksi. Hyökkääjä voi ARP-protokollan haavoittuvuuksien avulla väärentää IP- ja MAC-osoitepareja (*ARP Spoofing*). Väärentämisen myötä verkkosolmujen välinen liikenne voidaan ohjata kulkemaan halutun solmun kautta ja näin seurata tietoliikennettä. Hyökkäystapaa kutsutaan Man in the Middle -hyökkäykseksi. Kerroksen toinen varsin ongelmallinen osa-alue ovat aliverkot. (Reed 2003: 7–8.)

Siirtoyhteyskerroksen tietoturvaa voidaan parantaa käyttämällä suojattuja protokollia, joiden avulla voidaan tunnistaa käyttäjät ja salata yhteyden yli kulkeva tieto. Tietoturvaa voidaan parantaa myös niin sanotulla laitteistotason suodatuksella (*MAC Address Filtering*), jossa laitteet tunnistetaan yksilöivän MAC-osoitteen perusteella. (Reed 2003: 7–8.)

Reed (2003: 8) mainitsee siirtoyhteyskerroksen haavoittuvuuksiksi MAC-osoitteen väärentämisen, aliverkkojen kiertämisen, reititystietojen väärentämisen sekä erityisesti langattomien verkkojen heikon salauksen ja käytönvalvonnan. Kerroksen tietoturvan hallintakeinoina Reed (2003: 8) nostaa esiin laitetason suodatuksen, aliverkkojen hallinnan ja langattomien verkkojen tapauksessa vahvan salauksen ja pääsynvalvonnan sekä kantoalueen suunnittelun.

1.3. Verkkokerros

Verkkokerroksen rooli tekee siitä houkuttelevan kohteen hyökkäyksille. Hyökkääjän näkökulmasta kiinnostavia ovat kerroksen reitityksestä ja

resurssien yksilöimisestä sekä tunnistamisesta vastaavat protokollat. Mielenkiintoa lisää myös useiden verkkokerroksen protokollien sisältämät ryhmälähetysmekanismit. (Reed 2003: 9.)

Reed (2003: 9) toteaa useiden reititysprotokollien olevan tietoturvamielessä varsin alkeellisia. Vaikka päätelaitteet kykenevät pääsääntöisesti neuvottelemaan reitityksestä suojattujen protokollien avulla, niin niillä ei kuitenkaan ole keinoja varsinaisen reitin turvallisuuden määrittämiseen. Resurssien tunnistamisesta vastaavien protokollien ongelmana on yleisesti lähettäjän autentikointi. Valtaosa protokollista ei kykene luotettavasti autentikoimaan lähettäjää ja ne joutuvatkin luottamaan suurilta osin siihen mitä lähettäjä itse itsestään kertoo. Kolmas merkittävä ongelma on protokollien ryhmälähetysmekanismien väärinkäyttö; hyökkääjä voi mekanismeja hyväksikäyttämällä ylikuormittaa verkkoresursseja. Hyökkäystapaa kutsutaan palvelunestohyökkäykseksi (*Denial of Service Attack*). (Reed 2003: 9.)

Verkkokerroksen haavoittuvuuksia vastaan voidaan yksinkertaisimmillaan suojautua oikein määritellyllä palomuurilla. Lisäksi turvallisuutta voidaan parantaa merkittävästi tehokkailla salaus- ja autentikointimenetelmillä. Kolmas osa-alue on reitityksen turvaaminen. Reitityksen luotettavuutta voidaan parantaa esimerkiksi oikein määritellyin reitittimin. (Reed 2003: 10.)

Yksittäisistä haavoittuvuuksista Reed (2003: 10) nostaa esiin reitityksen ja IP-osoitteen väärentämisen. Merkittäviä keinoja, joiden avulla uhkia voidaan vähentää, ovat Reedin (2003: 10) mukaan tiukat reititys- ja palomuurisäännöt, ryhmälähetysten valvontatyökalut sekä tietoturvallisten sovellusten ja protokollien suosiminen.

1.4. Kuljetuskerros

Kuljetuskerroksen protokollien merkittävimmät haavoittuvuudet liittyvät Reedin (2003: 11–12) mukaan virheiden ja vikatilojen käsittelyyn, porttien kierrättämiseen sekä suorituskyvyn korostamiseen.

Useiden protokollien kohdalla on suunnitteluvaiheessa lähdetty oletuksesta, että protokollien toimintaympäristö on luotettava ja turvallinen. Lähtöoletus on johtanut siihen, että protokollat käyttäytyvät usein poikkeustilanteissa ennalta arvaamattomasti. Hyökkääjä voi käyttää virhetilanteiden puutteellista käsittelyä hyväkseen ja saada protokollan tekemään haluamiaan toimia. (Reed 2003: 11.)

Yleinen käytäntö ylikuormittaa kuljetuskerroksen mekanismeja vaikeuttaa tietoliikenteen suodattamista ja hallinnointia. Tämä koskee erityisesti sovellusten tunnistamiseen käytettäviä portteja. Samoja portteja käytetään yleisesti useiden itsenäisten toimintojen ja sovellutusten hyödyntämiseen. Porttien kierrättäminen lisää myös mahdollisten tietoturvahaavoittuvuuksien lukumäärää, kun niihin joudutaan sallimaan lukuisia erityyppisiä tietoliikenneyhteyksiä. (Reed 2003: 11–12.)

Valtaosalle kuljetuskerroksen protokollista on ominaista pyrkimys mahdollisimman suureen suorituskykyyn ja käytettävyyteen. Tavoitteiden saavuttaminen on useissa tapauksissa vaatinut kompromisseja tietoturvan suhteen. Merkittävimmät ongelmat liittyvät lähettäjän autentikointiin ja tietoliikenneyhteyksien eheyteen. (Reed 2003: 12.)

Verkkokerroksen tapaan kuljetuskerroksen protokollien haavoittuvuuksia vastaan voidaan suojautua kehittyneiden palomuurien avulla. Verkon eri rakenteellisilla tasoilla toimivien palomuurien suodatussääntöjen tulee olla mahdollisimman tiukkoja ja yksityiskohtaisia. Sääntöjen tulisi ulottua protokolla ja porttitasolle asti. Uhkia voidaan vähentää myös käyttämällä mahdollisimman turvallisia tietoliikenneprotokollia. (Reed 2003: 12–13.)

Reed (2003: 13) listaa kuljetuskerroksen tietoturvaongelmiksi poikkeustilanteiden puutteellisen käsittelyn, protokollien toteutuserot, kuljetuskerroksen mekanismien ylikuormittamisen sekä tietoliikenteen väärentämisen. Torjuntakeinoina Reed (2003: 13) mainitsee tiukat ja yksityiskohtaiset palomuurisäännöt, suojatut yhteydet ja autentikointimekanismit sekä älykkäät palomuuriratkaisut.

1.5. Yhteysjaksokerros

Yhteysjaksokerroksen tietoturvariskit keskittyvät olioiden autentikointiin ja pääsynvalvontaan. Kerroksella toimivien protokollien on ensiarvoisen tärkeää käyttää turvallisia mekanismeja yhteyksien luomiseen ja hallintaan. Erityisesti olioiden autentikoinnin tulee olla mahdollisimman suojattu tapahtuma ja sen yhteydessä protokollan ei saa lähettää ylimääräistä tietoa. Vaatimuksista huolimatta useat käytössä olevat protokollat sisältävät kuitenkin vakavia puutteita autentikoinnin suhteen. Osa protokollista jopa lähettää yhteyttä muodostettaessa kaikki tiedot suojaamattomina tai käyttää vain heikkoja salausmenetelmiä. (Reed 2003: 14–15.)

Protokollien käyttämien heikkojen salausalgoritmien lisäksi, ongelmia tuottavat myös käyttäjien liian heikot salasanat, jotka murentavat vahvankin salauksen hyödyt nopeasti. Toinen salasanoihin läheisesti liittyvä asia on pääsynvalvonta. Heikot salasanat yhdessä puutteellisen pääsynvalvonnan kanssa antavat hyökkääjälle mahdollisuuden käyttää erilaisia hyökkäystapoja salasanojen selvittämiseksi. Salasanoja voidaan yrittää ratkaista päättelemällä tai käymällä kaikki mahdolliset merkkiyhdistelmät läpi. Jälkimmäistä tapaa kutsutaan Brute force -menetelmäksi. (Reed 2003: 15.)

Yhteysjaksokerroksen tietoturvaongelmia voidaan Reedin (2003: 15) mukaan parhaiten torjua vahvoilla salausmenetelmillä, joilla suojataan koko viestintäketjua salasanojen tallennuksesta tiedonsiirtoon. Kokonaisuuteen kuuluu lisäksi käytössä olevien salasanojen ja tunnisteiden säännöllinen uusiminen sekä toimiva pääsynvalvonta (Reed 2003: 15–16).

Kerroksen vakavimpina haavoittuvuuksina Reed (2003: 16) mainitsee puutteelliset autentikointimekanismit, pääsynvalvonnan sekä arkaluonteisen tiedon vuotamisen. Uhkien torjuntakeinoja ovat salasanojen suojattu säilyttäminen ja välittäminen, toimiva pääsynvalvonta sekä suojatut yhteydet (Reed 2003: 16).

1.6. Esitystapakerros

Esitystapakerroksen haavoittuvuudet liittyvät pääsääntöisesti kerroksen toimintojen toteutukseen tai salausmenetelmiin. Kerroksen joidenkin protokollien arvaamaton tapa käsitellä virheellisesti muotoiltua syötettä muodostaa useissa tapauksissa merkittäviä tietoturvaongelmia. Puutteet syötteiden tarkastuksessa saattavat pahimmillaan mahdollistaa hyökkääjän pääsyn järjestelmään. (Reed 2003: 17–18.)

Esitystapakerroksella käytettävien salausmenetelmien ongelmat liittyvät yleisesti joko puutteelliseen toteutukseen tai arkkitehtuuriin. Lisähaasteita tuovat salaus- ja purkumenetelmien nopea kehitys sekä laskentatehon voimakas kasvu. (Reed 2003: 18.)

Kerroksen tietoturvauhkia voidaan vähentää käytettävien salausmenetelmien jatkuvalla päivittämisellä sekä toiminnallisuuksien huolellisemmalla toteuttamisella. Käytössä olevia salausmenetelmiä ja -mekanismeja tulisi arvioida, päivittää ja tarvittaessa vaihtaa turvallisempiin riittävän usein. Esitystapakerroksen toiminnallisuudet tulisi toteuttaa siten, että kaikki protokollille tuleva syöte tarkastetaan huolellisesti. (Reed 2003: 18.)

Reedin (2003: 18) mukaan esitystapakerroksen merkittäviä haavoittuvuuksia ovat virheellisen syötteen puutteellinen hallinta ja salausmenetelmien ongelmat. Haavoittuvuuksien hallintakeinoina Reed (2003: 18) mainitsee syötteiden huolellisen tarkastamisen ja hallinnan sekä protokollien eriyttämisen ja salausmenetelmien jatkuvan tarkastelun.

1.7. Sovelluskerros

Sovelluskerros on luonteeltaan ylimmäisenä kerroksena varsin joustava. Valtaosa kerroksen haavoittuvuuksista liittyykin juuri joustavuuden mukanaan tuomaan avoimuuteen. (Reed 2003: 19.)

Kerroksen yksi merkittävä tietoturvaongelma on sovelluskerrokselle sijoittuvat sovellusprotokollat, jotka on suunniteltu tietoturvan suhteen puutteellisesti.

Kyseiset protokollat eivät suojaa tallennettuja tietoja, niissä voi olla sisäänrakennettuja mekanismeja, joilla suojaukset voidaan ohittaa tai ne eivät käytä tarkoituksenmukaista käyttäjän tunnistusta. Protokollat saattavat lisäksi käsitellä syötteitä puutteellisesti, vaativat tarpeettoman vahvat oikeudet toimiakseen tai niiden monimutkaiset käyttäjänhallintamekanismit on toteutettu huolimattomasti tai väärin. (Reed 2003: 19–20.)

Sovelluskerroksen haavoittuvuuksia voidaan vähentää tehokkaasti sovellusprotokollien ja niitä käyttävien sovellusten huolellisella suunnittelulla sekä toteuttamisella. Sovellusten ja sovellusprotokollien tulisi hyödyntää alempien kerrosten tarjoamia tietoturvapalveluita, tarkastaa huolellisesti saatavat syötteet ja lähtevät viestit sekä käyttää vahvoja salaus- ja autentikointimenetelmiä. Muiden kerrosten tietoturvapalveluiden lisäksi ohjelmistojen on syytä toteuttaa myös omia tietoturvakontrolleja, joiden avulla voidaan hallita resurssien käyttöoikeuksia. Kontrollien tulee olla joustavia, tehokkaita ja suoraviivaisia. Lisäksi sovelluksen on syytä pitää yllä tarkkaa lokia sekä sisältää auditointiominaisuuksia. (Reed 2003: 20.)

Sovellusten suunnittelun ja toteutuksen ohella on tärkeää myös kunnollinen testaus ja katselmointi. Tietoturvaa voidaan parantaa myös kehittyneillä palomuureilla, joiden avulla hallita ja rajata sovellusten verkkoliikennettä. Laitteistotasolla haavoittuvuuksia voidaan kontrolloida käyttämällä IDS- ja IPS-järjestelmiä, joita käsitellään tarkemmin kappaleessa 6.3. (Reed 2003: 20.)

LIITE 2. Diplomityön ohjausryhmän kokoonpano

Diplomityön ohjausryhmä koostui ABB Oy:n tietohallintopalveluiden edustajista ja siihen kuului kolme jäsentä. Ohjausryhmän toimintaan osallistui diplomityöprojektin edetessä myös muita tietohallintopalveluiden työntekijöitä.

Ohjausryhmä jäsenet:

- Hannu Taimisto
  Service Manager, Telecommunication & Voice

- Raimo Villikka
  Security Manager

- Pasi Tolkki
  Service Manager, Collaboration & Groupware

Ohjausryhmän toimintaan osallistuneet muut henkilöt:

- Esa Pigg
  IS Service Desk Manager

- Matti Muilu
  System Manager

LIITE 3. Tarvekartoituksen toteutus

3.1. Haastattelut

Tarvekartoitus tehtiin haastattelututkimuksena. Haastattelumenetelmänä käytettiin teemahaastattelua ja haastateltavat olivat pääsääntöisesti yksiköiden tietohallinnon henkilökuntaa.

Sähkönjakeluautomaatio

23.2.2010 Puhelinhaastattelu, Allan Örn ja Lucas Nyberg
3.3.2010 Haastattelu, Allan Örn ja Markus Maier

Prosessiteollisuus

19.2.2010 Puhelinhaastattelu, Anders Gästgifvars
12.3.2010 Puhelinhaastattelu, Kim Lampola
18.3.2010 Puhelinhaastattelu, Riku Hyttinen
25.3.2010 Puhelinhaastattelu, Pertti Rönkkö

Sähkökoneet

4.3.2010 Puhelinhaastattelu, Harri Malen

Drives

4.3.2010 Puhelinhaastattelu, Tuomo Pigg
4.3.2010 Puhelinhaastattelu, Taito Ilmonen
22.3.2010 Puhelinhaastattelu, Juha Kestilä
31.3.2010 Puhelinhaastattelu, Teemu T. Heikkilä ja Tapio Loponen

Motors

11.3.2010 Puhelinhaastattelu, Hannu Ojajärvi
18.3.2010 Haastattelu, Hannu Ojajärvi ja Eija Jukkanen

Service

12.3.2010 Puhelinhaastattelu, Tomi Hämäläinen
19.3.2010 Haastattelu, Kai Kulmala
7.4.2010 Puhelinhaastattelu, Tomi Hämäläinen

Muuntajat

26.4.2010 Puhelinhaastattelu, Leena Rautakoski

3.2. Haastatteluissa käsitellyt aihealueet

Koska haastattelut toteutettiin teemahaastatteluina, ne olivat varsin vapaamuotoisia, eikä niissä käytetty etukäteen laadittuja yksityiskohtaisia kysymyslistoja. Haastatteluissa käsiteltiin seuraavia aihealueita:

- Yksiköiden nykyisin käyttämät palvelut ja järjestelmät, joihin asiakkaiden tai alihankkijoiden tulee saada yhteys ulkoverkosta.

- Alihankkijoiden tai asiakkaiden tarjoamat palvelut, joihin tulee saada yhteys ABB:n sisäverkosta.

- Alihankkijoiden tai asiakkaiden käytössä olevat järjestelmät, joihin tulee saada etäyhteys ABB:n sisäverkosta.

- Yksikön käyttämät tai vielä kehitteillä olevat ratkaisut tunnistettuihin käyttötarpeisiin.

LIITE 4. Tunnistetut tarpeet

Taulukko 1. Etäyhteydet ABB:n hallussa oleviin laitteisiin tai järjestelmiin.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Automaattivarastojen hallinta	Etävalvonta ja -hallinta	Alihankkijat	Sisäverkko
Uunien etävalvonta	Etävalvonta ja -hallinta	Alihankkijat	Sisäverkko

Taulukko 2. Alihankkijoiden yhteydet sisäverkon dokumentti- ja materiaalipankkeihin.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Järjestelmien ylläpito ja konfigurointi	Yhteys dokumentti- ja materiaalipankkeihin	Alihankkijat, omat työntekijät	Sisäverkko
Tiedonjakaminen	Yhteys dokumentti- ja materiaalipankkeihin	Alihankkijat	Sisäverkko
Hajautettu ohjelmistokehitys	Yhteys dokumenttipankkiin	Alihankkijat	Sisäverkko
Tuotteiden arvokilpien teettäminen	Yhteys dokumenttipankkiin	Alihankkijat	Sisäverkko
Moottoreiden arvokilpien teettäminen	Yhteys dokumenttipankkiin	Alihankkijat	Sisäverkko
Markkinointimateriaalin tuottaminen	Yhteys materiaalipankkiin	Alihankkijat	Sisäverkko
Komponenttien valmistus	Yhteys tuotantodokumentteihin	Alihankkijat	Sisäverkko
Materiaalien hankinta ja varastologiikka	Yhteydet materiaalien hankinta- ja varastologiikan järjestelmiin	Alihankkijat, asiakkaat	Sisäverkko

Taulukko 3. Asiakkaiden yhteydet sisäverkon dokumentti- ja materiaalipankkeihin.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Testitulosten jakaminen	Yhteys materiaalipankkiin	Asiakkaat	Sisäverkko
Tiedonjakaminen	Yhteys dokumentti- ja materiaalipankkeihin	Asiakkaat	Sisäverkko
Järjestelmien ylläpito ja konfigurointi	Yhteys dokumentti- ja materiaalipankkeihin	Asiakkaat	Sisäverkko

Taulukko 4. Tuotepäivitysten tarjoaminen asiakkaille.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Tuotepäivitykset	Yhteys päivityspalvelimeen	Asiakkaat	Sisäverkko

Taulukko 5. Alihankkijoiden yhteydet sisäverkon tuotekehitysjärjestelmiin.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Hajautettu tuotekehitys	Yhteys versionhallintajärjestelmiin	Alihankkijat	Sisäverkko
Hajautettu tuotekehitys	Yhteys pakettienhallintajärjestelmiin	Alihankkijat	Sisäverkko
Hajautettu tuotekehitys	Yhteys ohjelmistovirheiden raportointijärjestelmiin	Alihankkijat	Sisäverkko
Komponenttien valmistus	Yhteys laaturaportointityökaluihin	Alihankkijat	Sisäverkko

Taulukko 6. Varastojen ja tuotetoimitusten seuranta.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Varastoinventaario	Viivakoodien lukupäätteiden yhteydet	Alihankkijat	Sisäverkko
Tuote- ja tilausseuranta	Viivakoodien lukupäätteiden yhteydet	Asiakkaat	Sisäverkko

Taulukko 7. Asiakkaiden yhteydet tilausten seurantajärjestelmään.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Tilausten seuranta	Yhteys tilaustenseurantajärjestelmään	Asiakkaat	Sisäverkko
Tuote- ja tilausseuranta	Yhteys tilaustenseurantajärjestelmään	Asiakkaat	Sisäverkko

Taulukko 8. Ulkoisten konsulttien tarvitsemat yhteydet.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Ulkoisten konsulttien yhteydet ABB:n järjestelmiin	Yhteydet ABB:n järjestelmiin	Alihankkijat	Sisäverkko

Taulukko 9. Extranet-palvelut asiakkaille ja alihankkijoille.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Tiedonjakaminen	Extranet-palvelut	Alihankkijat, asiakkaat	Sisäverkko

Taulukko 10. Asiakkaiden yhteydet tuoteräätälöinti- ja verkkokauppapalveluihin.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Tuoteräätälöintipalvelut	Yhteys räätälöintipalveluihin	Asiakkaat	Sisäverkko
Tuotepäivitykset	Yhteys verkkokauppaan	Asiakkaat	Sisäverkko

Taulukko 11. Tuotetukipalveluiden tarjoaminen asiakkaille.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Tukipalveluiden tuottaminen	Yhteys tukimateriaaliin	Asiakkaat	Sisäverkko
Tukipalveluiden tuottaminen	Ruudunkaappausten siirtäminen	Asiakkaat	Sisäverkko

Taulukko 12. Alihankkijoiden ja asiakkaiden käytössä olevien ABB:n tuotteiden lisenssien hallinta ja tarkastaminen.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Tuotteiden ylläpito	Lisenssien hallinta ja aktivointi	Asiakkaat	Sisäverkko
Ryhmätyösovelluksen käyttäminen	Lisenssien tarkastaminen	Alihankkijat	Sisäverkko

Taulukko 13. Tiedonsiirto asiakkaan järjestelmästä ABB:n toiminnanohjausjärjestelmään (Maximo).

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Tiedonsiirto asiakkaan järjestelmistä	Datan siirto Maximoon	Asiakkaat	Sisäverkko

Taulukko 14. Alihankkijoiden yhteydet ABB:n toiminnanohjausjärjestelmään (DG).

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Yhteydet toiminnanohjausjärjestelmään	Yhteys DG-järjestelmään	Alihankkijat	Sisäverkko

Taulukko 15. ABB:n ja kolmansien osapuolien tietojärjestelmien käyttäminen mobiililaitteilla.

Tarve	**Käyttötapaus**	**Tarvitsija**	**Suunta**
Järjestelmien käyttäminen mobiililaitteilla	Yhteys mobiililaitteilla	Omat työntekijät	Sisäverkko

Taulukko 16. Sisäverkossa nykyisin estettyjen palveluiden tai protokollien käyttäminen.

Tarve	**Käyttötapaus**	**Kohde/tarvitsija**	**Suunta**
Pikaviestinyhteydet	ABB:n verkossa estettyjen palveluiden käyttäminen	Asiakkaat, alihankkijat, omat työntekijät	Ulkoverkko
Konsulttien yhteydet omiin järjestelmiinsä	Konsulttien tarvitsemat ABB:n verkossa estetyt protokollat	Alihankkijat	Ulkoverkko
Suojaamattomat tiedonsiirtoyhteydet	Suojaamattomat yhteydet tiettyihin järjestelmiin ja laitteisiin	Alihankkijat, asiakkaat	Ulkoverkko

Taulukko 17. Etähallintayhteydet asiakkaan hallussa oleviin laitteisiin tai järjestelmiin.

Tarve	**Käyttötapaus**	**Kohde**	**Suunta**
Tuotteiden ylläpito	Etähallinta	Asiakkaat	Ulkoverkko
Etäyhteydet automaatiojärjestelmiin	Tukipalvelut	Asiakkaat	Ulkoverkko
Etäyhteydet automaatiojärjestelmiin	Tiedonsiirto	Asiakkaat	Ulkoverkko
Etäyhteydet automaatiojärjestelmiin	Käyttöönottotuki	Asiakkaat	Ulkoverkko
Tuotepäivitykset	Etäyhteys asiakkaan päivityspalvelimeen	Asiakkaat	Ulkoverkko
Tuotteiden ylläpito	Tuotepäivitykset	Asiakkaat	Ulkoverkko

Taulukko 18. Etävalvontayhteydet asiakkaan hallussa oleviin laitteisiin tai järjestelmiin.

Tarve	**Käyttötapaus**	**Kohde**	**Suunta**
Tuotteiden ylläpito	Etävalvonta	Asiakkaat	Ulkoverkko
Etäyhteydet asiakasjärjestelmiin	Etävalvonta	Asiakkaat	Ulkoverkko
Mittaustiedon kerääminen	Datan siirto ABB:n palvelimeen	Asiakkaat	Sisäverkko

Taulukko 19. Tiedonsiirto asiakkaan ja alihankkijan välillä.

Tarve	**Käyttötapaus**	**Kohde/tarvitsija**	**Suunta**
Tiedonsiirto	Tiedonsiirto asiakkaan ja alihankkijan välillä	Alihankkijat, asiakkaat	Ulkoverkko, sisäverkko

Taulukko 20. Yhteydet alihankkijoiden dokumentti- ja materiaalipankkeihin.

Tarve	**Käyttötapaus**	**Kohde**	**Suunta**
Yhteydet ulkoisiin suunnittelutoimistoihin	Yhteydet ulkoisiin suunnittelutoimistoihin	Alihankkijat	Ulkoverkko
Yhteydet testausjärjestelmiin	Yhteydet alihankkijan testausjärjestelmiin	Alihankkijat	Ulkoverkko

Taulukko 21. Yhteydet asiakkaiden dokumentti- ja materiaalipankkeihin.

Tarve	**Käyttötapaus**	**Kohde**	**Suunta**
Tiedonsiirto	Yhteys asiakkaan materiaali- ja dokumenttipankkeihin	Asiakkaat	Ulkoverkko

Taulukko 22. Tietokantojen synkronointi alihankkijan verkossa olevien tietokantojen kanssa.

Tarve	**Käyttötapaus**	**Kohde/tarvitsija**	**Suunta**
Testiasemaparametrien muuttaminen	Tietokantasynkronointi	Alihankkijat	Ulkoverkko, sisäverkko
Ryhmätyösovelluksen käyttäminen	Tietokantasynkronointi	Alihankkijat	Ulkoverkko, sisäverkko
Testausdatan siirtäminen	Tietokantasynkronointi	Alihankkijat	Ulkoverkko, sisäverkko