Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista

Muutoshistoria

Päivämäärä	Kuvaus
4.11.2013	Ensimmäinen julkaisuversio.
23.9.2015	Täsmennetty sisältösuodatusratkaisun kuvausta taulukossa 3.
27.6.2016	Pieniä täsmennyksiä lukuun 3. Täsmennyksiä ja täydennyksiä lukuihin 4 ja 5.
20.12.2018	Pieniä täsmennyksiä kuvauksiin. Lisätty luvut 5.3, 5.4 ja 5.5.
2.12.2021	Täydennetty kuvauksia lukuihin 4.1.1, 5.3, ja 5.5. Pieniä termistötäsmennyksiä ja ajantasaistuksia.

Sisällys

1 Johdanto

Kansainvälisistä tietoturvallisuusvelvoitteista, turvallisuusselvityksistä sekä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annettujen lakien[1] mukaan Liikenne- ja viestintävirasto Traficomin tehtäviin kuuluvat erilaiset tietojärjestelmien turvallisuusarvioinnit ja -hyväksynnät. Traficomin suorittamissa tietojärjestelmäarvioinneissa eräs arvioitava kohde on yhdyskäytäväratkaisut eri turvallisuusluokkien ympäristöjen välillä. Tässä ohjeessa kuvataan yleisimmät edellytykset hyväksyttävissä oleville yhdyskäytäväratkaisuille sekä esitetään esimerkkejä ratkaisumalleista.

2 Määritelmät

"Hyväksyttävällä yhdyskäytäväratkaisulla" tarkoitetaan tässä ohjeessa toteutusta, joka mahdollistaa eri turvallisuusluokkien ympäristöjen[2] liittämisen siten, että luotettavasti estetään ylemmän turvallisuusluokan tiedon kulkeutuminen matalamman turvallisuusluokan ympäristöön.

"Yksisuuntaisella suodatusratkaisulla" tarkoitetaan tässä ohjeessa toteutusta, joka rajaa liikennöinnin yksisuuntaiseksi.

"Datadiodilla" tarkoitetaan tässä ohjeessa yksisuuntaista suodatusratkaisua, joka rajaa liikennöinnin yksisuuntaiseksi OSI-mallin[3] fyysisellä kerroksella.

3 Yhdyskäytäväratkaisujen yleiset suunnitteluperiaatteet

Hyväksyttävien yhdyskäytäväratkaisujen yleisenä suunnitteluperiaatteena on toteuttaa Bell-LaPadula-mallin[4] säännöt "No Read Up" ja "No Write Down". Hyväksyttävän yhdyskäytäväratkaisun tulee toisin sanoen luotettavasti estää ylemmän turvallisuusluokan tiedon kulkeutuminen[5] matalamman turvallisuusluokan ympäristöön.

Bell-LaPadula -mallin toteuttamiseksi käytetään usein menetelminä

- yksisuuntaisia suodatusratkaisuja, joissa sallitaan yksisuuntainen liikennöinti matalamman luokan ympäristöstä ylemmän luokan ympäristöön, sekä
- sisältösuodatusratkaisuja, joissa tieto tunnistetaan ylemmän luokan ympäristössä, ja sallitaan vain matalamman luokan tiedon siirtyminen ylemmän luokan ympäristöstä matalamman luokan ympäristöön.

Hyväksyttävältä toteutukselta edellytetään yleisesti myös monikerrossuojaamisen[6], vikaturvallisuuden[7], vähimpien oikeuksien ja haavoittuvuusavaruuden minimoinnin periaatteiden täyttämistä. Keskeiset suodatustoiminnallisuudet tulee toteuttaa luotetun ohjelmisto- ja rauta-alustan päällä. On myös huomioitava, että yhdyskäytäväratkaisun tulee pystyä suojaamaan itseään käyttöympäristönsä uhkia vastaan, ja että turvallisuustoteutuksen oikeellisen toiminnan tulee olla luotettavasti todennettavissa. Yhdyskäytäväratkaisulle edellytetään luotettavaa toteutusta myös turvallisuuden hallinnoinnille sekä valvonnalle, mukaan lukien hyökkäysten havainnointikyky yhdyskäytäväratkaisua ja/tai sen suojaamaa ympäristöä vastaan.

---

[1] Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). Turvallisuusselvityslaki (726/2014). Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011).
[2] Ympäristöjen oletetaan lähtökohtaisesti olevan toisilleen ei-luotettuja myös tilanteissa, joissa yhdistetään eri organisaatioiden hallinnoimia ympäristöjä toisiinsa.
[3] International Organization for Standardization. 1994. ISO/IEC 7498-1:1994. Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model.
[4] Bell, D & LaPadula, L. 1973. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, Volume I & II.
[5] Kattaen kaikki tiedon välitystavat, sisältäen esimerkiksi tiedon kopioimisen, tiedon näyttämisen ja tiedon soittamisen.
[6] Engl. ”defence in depth”.
[7] Engl. ”fail secure” ja ”fail safe”. Huomioitava muun muassa virtualisoinnissa, jossa isäntäkoneen (host) vikaantuminen voi vaikuttaa useamman virtuaalikoneen (guest) toiminnallisuuteen. Toisaalta esimerkiksi yhdyskäytäväratkaisun tietoliikennelaitteiden tulee vikatilanteessa päätyä lähtökohtaisesti liikennöinnin estävään (fail closed) tilaan.

Yhdyskäytäväratkaisuun ja sen komponentteihin liittyvät lokitiedot tulee suojata lähtökohtaisesti yhdyskäytäväratkaisun ylemmän puolen luokituksen mukaisesti[8].

4 Yleisimmät yhdyskäytäväratkaisutyypit

Yleisimmät hyväksyttävät yhdyskäytäväratkaisut jakautuvat yksisuuntaisiin suodatusratkaisuihin ja alkiotunnistuksen sisältösuodatusratkaisuihin. Yksisuuntaiset suodatusratkaisut jakautuvat edelleen datadiodiratkaisuihin ja muihin yksisuuntaisiin suodatusratkaisuihin. Tässä luvussa kuvataan eri yhdyskäytäväratkaisutyyppien keskeiset ominaispiirteet sekä esitetään viitteellisiä esimerkkitoteutuksia.

4.1 Yksisuuntaiset suodatusratkaisut

4.1.1 Datadiodiratkaisut

Datadiodiratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 1.

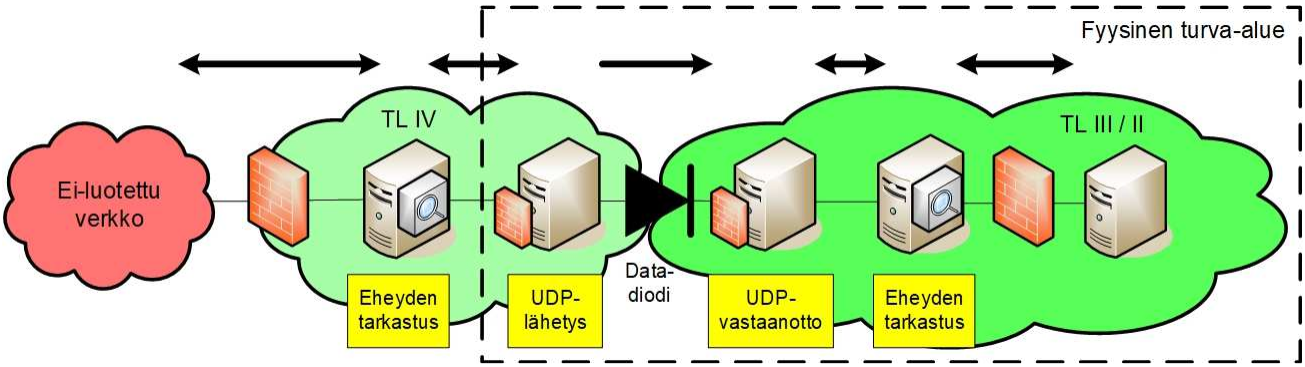
Taulukko 1. Datadiodiratkaisujen ominaispiirteitä.

Tiedonsiirron suunta	Matalamman luokan ympäristöstä ylemmän luokan ympäristöön.
Kuvaus	OSI-mallin fyysisen kerroksen tasolla tapahtuva vain yhteen suuntaan tiedonsiirron mahdollistava toteutus[9]. Hyväksyttävässä toteutuksessa yhdyskäytäväratkaisun tuottama yksisuuntaisuus tulee olla toteutettuna muusta yhdyskäytäväratkaisun toiminnallisuudesta luotettavasti eriytettynä[10]. Hyväksyttävä toteutus edellyttää tyypillisesti myös kovennetuille käyttöjärjestelmäalustoille rakennettuja UDP-liikennettä välittäviä lähetys- ja vastaanottopalvelimia, sekä siirretyn aineiston eheyden tarkastavaa menettelyä[11]. Jotkin lähetys- ja vastaanottopalvelinten ohjelmistot tukevat myös kaksisuuntaisen protokollan jäljittelyä (emulointia). Vaikka tiedonsiirto eri turvallisuusluokkien välillä toteutuu yksisuuntaisena, jäljittely voi yksinkertaistaa lähetys- tai vastaanottopalvelimen liittämistä kyseisen turvallisuusluokan ympäristön muihin palveluihin. Jäljittely voi yksinkertaistaa tiedonsiirtoa esimerkiksi silloin, kun matalamman luokan ympäristöstä on tarve siirtää ylemmän luokan ympäristöön reaaliaikaista videokuvaa, JSON-muotoista sovellusliikennettä tai SMTP-muotoista sähköpostiliikennettä. Tuki eri protokollien jäljittelyyn on tuotekohtaista. Tällä tarkoitetaan sitä, että eri valmistajien tuotteet ja tuotemallit voivat erota merkittävästi tukemiensa protokollien ja niiden toiminnallisuuksien osalta.
Sovelluskohteita	Turvapäivitysten tuonti turvallisuusluokan III tai II ympäristöihin. Matalamman luokan tiedon tuonti tilannekuvatiedon tarkkuuden parantamiseksi (esimerkiksi paikkatiedon, hälytysten, sensoritiedon tai kameravalvontatiedon välittäminen keskusvalvomoon / tilannekeskukseen). Matalamman turvallisuusluokan ympäristön sähköpostien välitys ylemmän luokan ympäristöön.

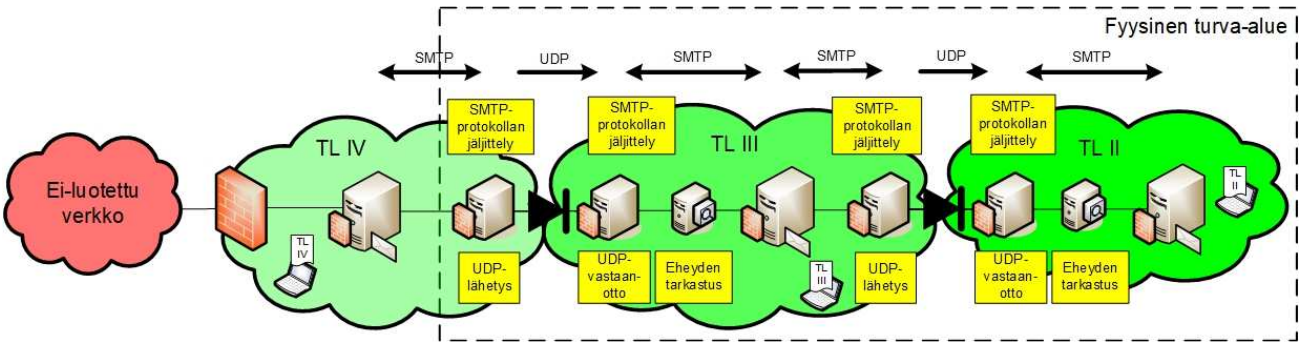
[8] Luokittelun perusteena hyökkäystyypit, joissa yhdyskäytäväratkaisun lokitietoja käytetään piilokanavana (engl. "covert channel") ylemmän turvallisuusluokan tietojen siirtämiseen matalamman turvallisuusluokan ympäristöön.
[9] Esimerkiksi yksisuuntainen valokuituyhteys.
[10] Eriyttäminen tulee toteuttaa siten, että käyttäjän tai ylläpitäjän toimilla, tai millään järjestelmässä suoritettavalla ohjelmakoodilla ei voida vaikuttaa yhdyskäytäväratkaisun toteuttamaan yksisuuntaisuuteen. Tämä kattaa muun muassa yhdyskäytäväratkaisuun kytkettävät laitteisto- ja ohjelmistokomponentit sekä laitteen laiteohjelmiston.
[11] Sisältäen esimerkiksi päivitysten tuonnissa vähintään siirrettyjen tiedostojen tarkistussummien ja allekirjoitusten tarkistamisen, sekä haittaohjelmaskannauksen.

Soveltuvuus turvallisuus-luokittain	Hyväksyttävissä yhden tai useamman turvallisuusluokan ylittävänä yhdyskäytäväratkaisuna välillä TL IV → TL III, TL III → TL II, TL IV → TL II ja moniportaisena toteutuksena erityisehdoin myös TL II → TL I.

Viitteellisiä esimerkkitoteutuksia on esitetty kuvissa 1 ja 2.



Kuva 1. Viitteellinen esimerkkitoteutus datadiodiratkaisusta.



Kuva 2. Viitteellinen esimerkkitoteutus datadiodiratkaisusta.

4.1.2 Muut yksisuuntaiset suodatusratkaisut

Muiden yksisuuntaisten suodatusratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 2.

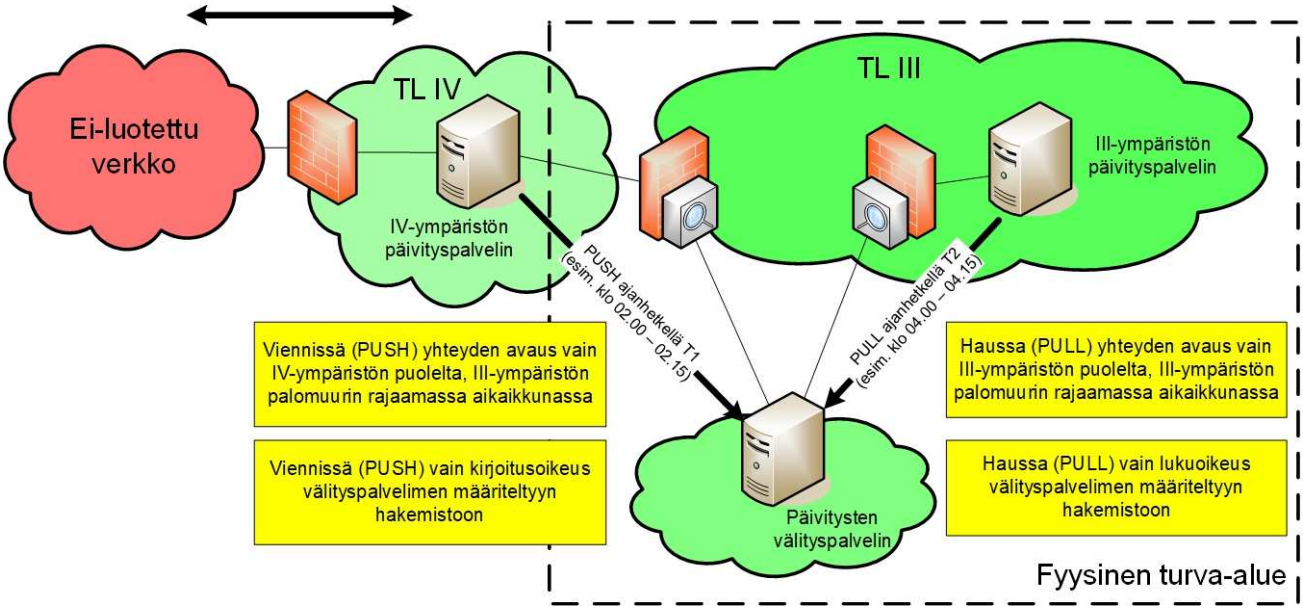
Taulukko 2. Muiden yksisuuntaisten suodatusratkaisujen ominaispiirteitä.

Tiedonsiirron suunta	Matalamman luokan ympäristöstä ylemmän luokan ympäristöön.
Kuvaus	Tyypillisesti OSI-mallin verkko- ja sovelluskerroksen tasoilla toteutettava vain yhteen suuntaan tiedonsiirron mahdollistava ratkaisu. Ratkaisu voi sisältää ajastettujen palomuurisääntöjen avulla eristetyn vyöhykkeen eri turvallisuusluokkien ympäristöjen välillä, mikä rajaa tiedonsiirron vyöhykkeiden välillä tapahtuvaksi vain yhteen suuntaan kerrallaan, ja sallii vain tunnistetut liikennetyypit. Toteutuksissa tulee huomioida erityisesti, että määritetyn aikaikkunan aikana avattujen yhteyksien päättymisestä varmistutaan[12] aikaikkunan sulkeutuessa. Turvallisuusluokkien välisen vyöhykkeen hallinnoinnin eriyttäminen ympäröivien turvallisuusluokkien hallintaratkaisuista tuo lisäsuojaa erityisesti tilanteisiin, joissa hyökkääjällä on pääsy[13] ylemmän tai alemman turvallisuusluokan ympäristön hallintaratkaisuihin. Erityisesti

[12] Varmistumisessa voidaan hyödyntää esimerkiksi tilataulun tyhjennystä (flush) tai vastaavaa menetelmää.
[13] Esimerkiksi haittaohjelman avulla.

	tulee huomioida, että välityspalvelimen lokitietoja ei tule siirtää matalamman turvallisuusluokan ympäristöön (piilokanava, vrt. alaviite 8).
Sovelluskohteita	Turvapäivitysten tuonti turvallisuusluokan III ympäristöihin. Matalamman luokan tiedon tuonti tilannekuvatiedon tarkkuuden parantamiseksi.
Soveltuvuus turvallisuus-luokittain	Hyväksyttävissä yhden turvallisuusluokan ylittävänä yhdyskäytäväratkaisuna välillä TL IV → TL III.

Viitteellinen esimerkkitoteutus on esitetty kuvassa 3.



Kuva 3. Viitteellinen esimerkkitoteutus yksisuuntaisesta suodatusratkaisusta.

4.2 Alkiotunnistuksen sisältösuodatusratkaisut

Alkiotunnistuksen sisältösuodatusratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 3.

Taulukko 3. Alkiotunnistuksen sisältösuodatusratkaisujen ominaispiirteitä.

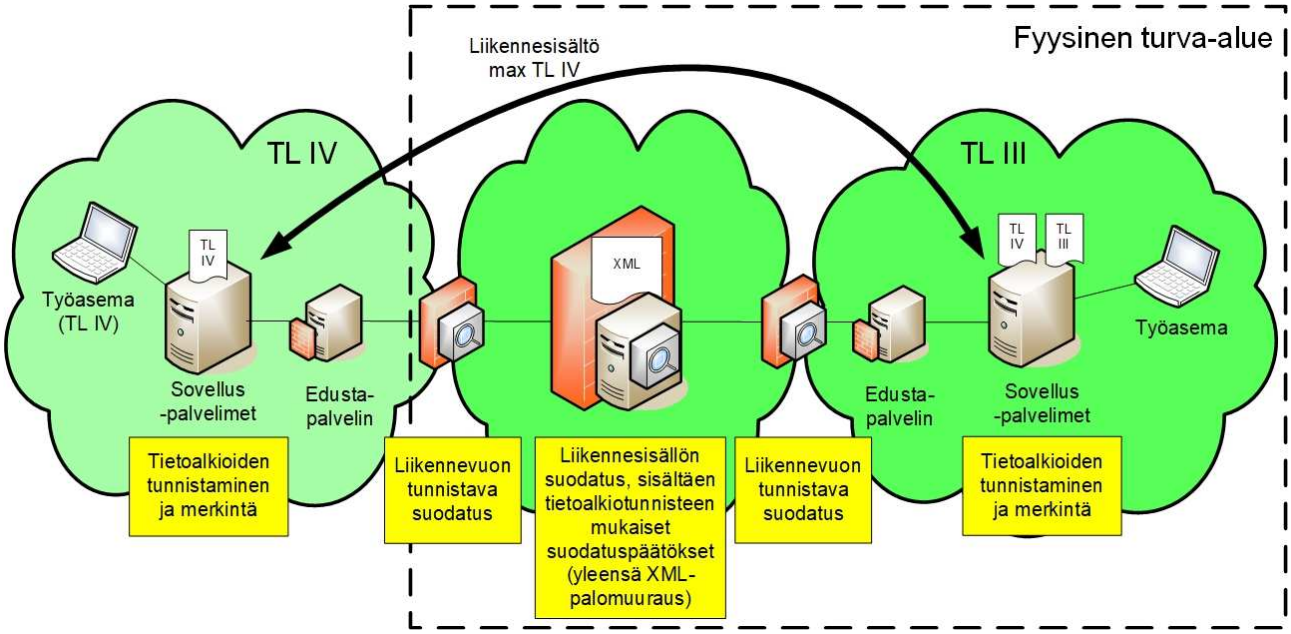
Tiedonsiirron suunta	Ylemmän luokan ympäristöstä matalamman luokan ympäristöön, matalamman luokan ympäristöstä ylemmän luokan ympäristöön, edellisten yhdistelmä tai/ja saman turvallisuusluokan ympäristöstä toiseen saman turvallisuusluokan ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan yksi tai useampi seuraavista käyttötapauksista: A. Ylemmän luokan ympäristöstä matalamman luokan tiedon siirto matalamman luokan ympäristöön. B. Matalamman luokan ympäristöstä ylemmän luokan ympäristöön suuntautuva tiedonsiirto. C. Tietojen siirto kahden järjestelmän välillä siten, että siirto rajataan vain tarkasti määriteltyihin tietoihin (esimerkiksi kahden eri organisaation hallinnoimien turvallisuusluokan III järjestelmien välinen tiedonvaihto[14]). Käyttötapauksiin A, B ja C hyväksyttäviltä toteutuksilta edellytetään seuraavien ehtojen täyttymistä:

[14] Tässä ohjeessa ei käsitellä eri organisaatioiden välisiä luottosuhteita tai menetelmiä, joilla organisaatiot varmistuvat toistensa tiedonsuojauskyvyn riittävyydestä ennen tietojen luovuttamis-/vaihtopäätöksiä.

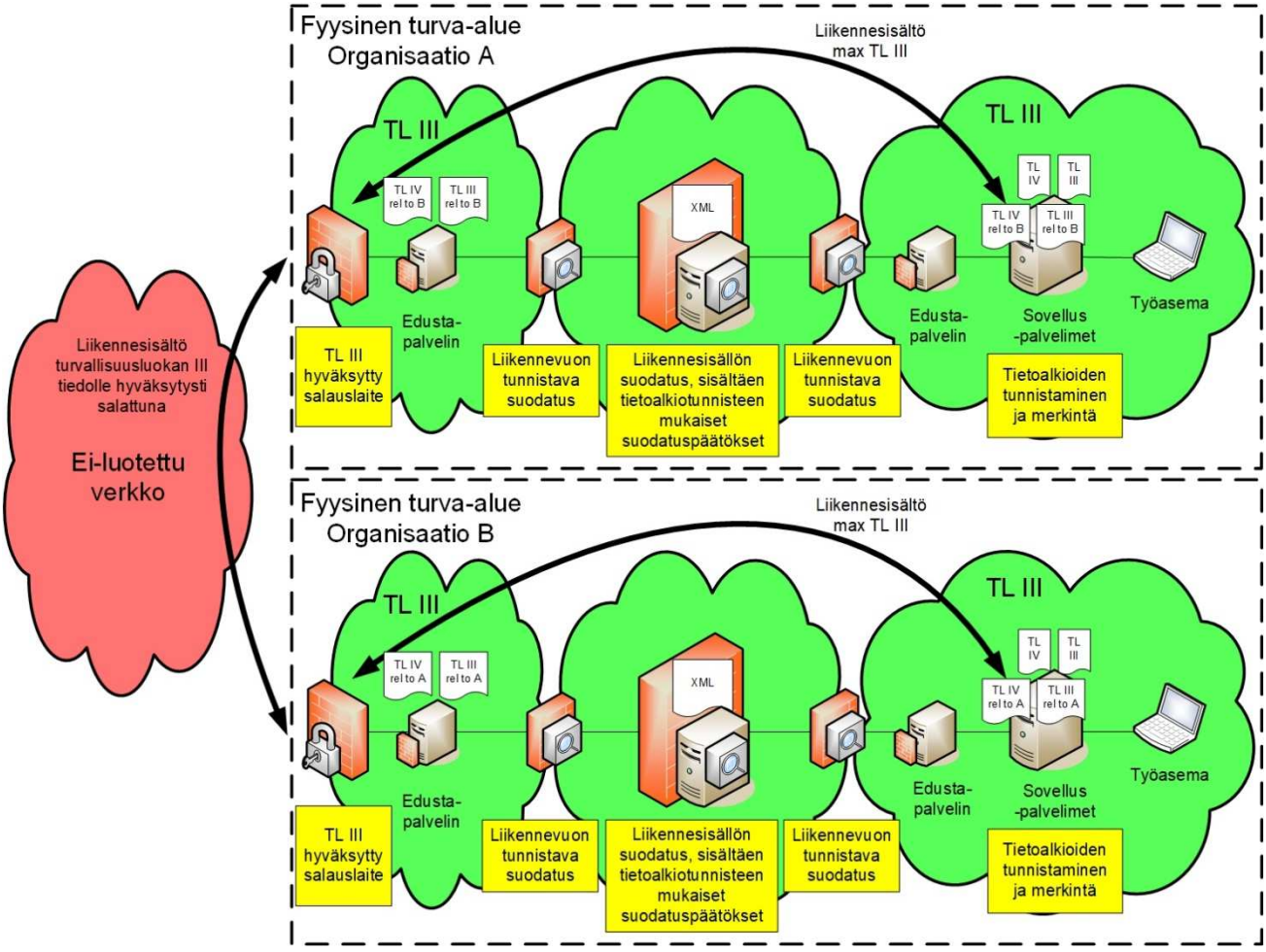
	1) Tieto tunnistetaan ja merkitään[15] oikeellisesti. 2) Sovellustason sanomamuoto on täsmällisesti määritetty. 3) Määritetyn sanomamuodon noudattaminen tarkistetaan. 4) Sovellustason suodatus toimii luotettavasti oikein merkittyjen, sekä myös virheellisten syötteiden tapauksessa. 5) Sovellustason suodatustoiminnallisuus on eriytetty muusta sovellustoiminnallisuudesta. 6) Suodatustoiminnallisuuden haavoittuvuusavaruus on minimoitu[16] ja suodatus toteutetaan useassa kerroksessa[17]. Liikennesisällön suodatus on toteutettava sekä verkkoteknisesti (IP-portti-rajaukset) että sovelluskerroksen tasolla (esimerkiksi tietotyyppien, pituuksien ja syntaksin tarkastaminen ennen käsittelyä). Useissa hyväksyttävissä olevissa toteutuksissa suodatusta tuetaan lisäksi liikennevuon tunnistavalla suodatuksella (vrt. luku 5.1). Erityisesti sovelluskerroksen tason suodatuksessa tarkastuksen kohteen on pystyttävä osoittamaan, miten suodatusalustan haavoittuvuuksilta on pyritty suojautumaan ja miten suodatusratkaisussa (esimerkiksi XML-palomuurissa) varmistutaan siitä, että datan (esimerkiksi XML-dokumentin) jossain kentässä ei kuljeteta ylemmän turvallisuusluokan tietoa matalamman turvallisuusluokan ympäristöön. Suodatusalustan eheydestä on myös pystyttävä varmistumaan (huomioitava erityisesti sitominen luotettuun rauta-alustaan ja eheystarkastukset). Liikennesisällön koneellinen suodatus voi joissain yksisuuntaista suodatusratkaisua hyödyntävissä käyttötapauksissa olla osin korvattavissa suppeammilla, esimerkiksi henkilöstön toteuttamaan dokumenttisuodatukseen pohjautuvilla menetelmillä. Tällainen käyttötapaus voi ilmetä esimerkiksi tilanteissa, joissa turvallisuusluokan III ympäristössä laaditaan turvallisuusluokan IV dokumentti, joka siirretään datadiodin läpi turvallisuusluokan IV ympäristöön (vrt. kuva 5). Alkiotunnistuksen sisältösuodatusratkaisuja käytetään usein myös täydentävinä suojauksina osana muita yhdyskäytäväratkaisuja[18].
Sovelluskohteita	Turvallisuusluokan III järjestelmät, joista tarve siirtää turvallisuusluokan IV tietoa turvallisuusluokan IV järjestelmään (esimerkiksi turvallisuusluokan III tilannekuvajärjestelmistä siirrettävä turvallisuusluokan IV paikkatieto). Turvallisuusluokan IV järjestelmät, joista tarve siirtää turvallisuusluokan IV tietoa turvallisuusluokan III järjestelmään. Organisaation hallinnoima järjestelmä, josta tarve siirtää ja johon tarve vastaanottaa määriteltyjä tietoja (esimerkiksi vain paikkatietoa) toisen organisaation järjestelmään/järjestelmästä.
Soveltuvuus turvallisuus-luokittain	Hyväksyttävissä yhden turvallisuusluokan ylittävänä yhdyskäytäväratkaisuna välillä TL IV ←→ TL III. Käyttötapauksen A toteutus datadiodiin yhdistettynä (vrt. kuva 5) hyväksyttävissä myös välillä TL II → TL III ja TL II → TL IV.

Viitteellisiä esimerkkitoteutuksia on esitetty kuvissa 4, 5 ja 6.

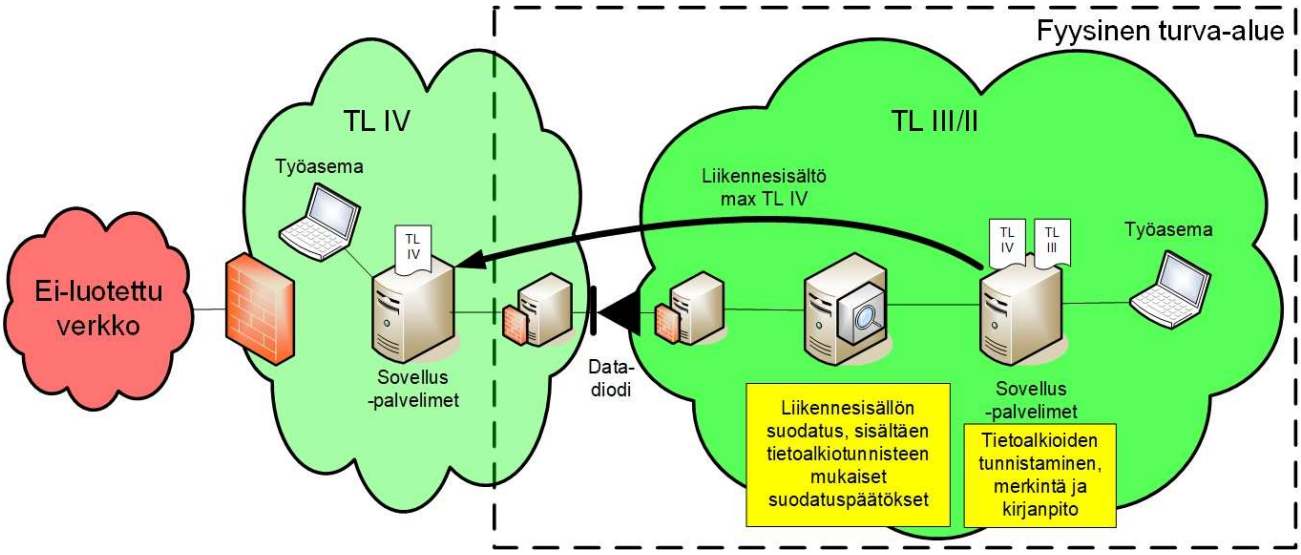
[15] Merkinnät voivat sisältää turvallisuusluokan lisäksi tiedot esimerkiksi omistajasta, salassapitoajasta ja jakelusta.
[16] Kattaen muun muassa käyttöjärjestelmä-, sovellusohjelmisto- ja verkkokerroksen. Sovellusohjelmistotason käytännön toteutukset edellyttävät usein haavoittuvuusavaruuden rajaamista vain tiukasti määriteltyä toiminnallisuutta tarjoavan edustapalvelimen avulla. Joissain järjestelmissä yhdyskäytävän suuntaan tarjottava sovellustoiminnallisuus saattaa olla rajattavissa myös suoraan taustajärjestelmässä.
[17] Esimerkiksi suodatus palomuurein ja IPS-järjestelmin IP-osoitteen ja portin, ja sovellussuodattimilla esimerkiksi XML-skeeman ja XML-kenttien sisällön osalta. Lisäksi usein IPS-järjestelmin myös liikennöintiprotokollan osalta.
[18] Esimerkiksi datadiodin tai muun yksisuuntaisen suodatusratkaisun läpi siirretyn aineiston validointi.



Kuva 4. Viitteellinen esimerkkitoteutus alkiotunnistuksen sisältösuodatusratkaisusta.



Kuva 5. Viitteellinen esimerkkitoteutus alkiotunnistuksen sisältösuodatusratkaisusta.



Kuva 6. Viitteellinen esimerkkitoteutus alkiotunnistuksen sisältösuodatusratkaisusta.

5 Muita ratkaisumalleja

Tässä luvussa kuvattavien ratkaisumallien turvallisuudessa on tiettyjä tunnistettuja heikkouksia, mistä johtuen ne eivät lähtökohtaisesti ole Traficomin NCSA-toiminnon yleisesti hyväksyttävissä. Tietyissä järjestelmissä ei ole kuitenkaan mahdollista käyttää luvun 4 malleja esimerkiksi käyttöympäristön poikkeavasta luonteesta johtuen[19]. Tiedon omistaja voi tällaisissa tilanteissa riskienarviointinsa perusteella mahdollisesti hyväksyä näitä ratkaisumalleja omien tietojensa suojaamiseen.

5.1 Liikennevuon sisältösuodatusratkaisut

Liikennevuon sisältösuodatusratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 4.

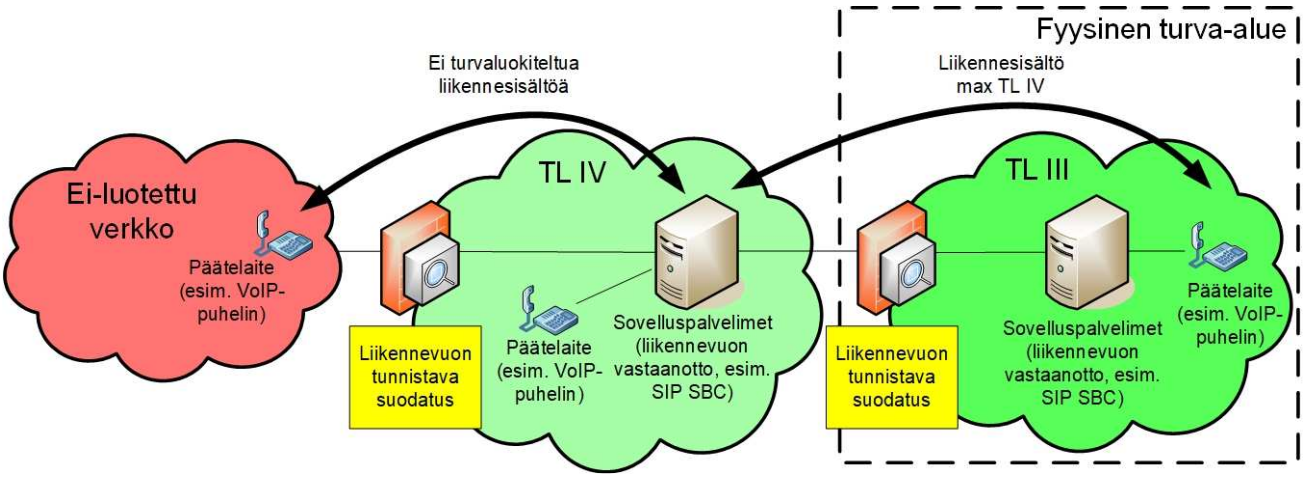
Taulukko 4. Liikennevuon sisältösuodatusratkaisujen keskeiset ominaispiirteet.

Tiedonsiirron suunta	Matalamman luokan ympäristöstä ylemmän luokan ympäristöön tai/ja ylemmän luokan ympäristöstä matalamman luokan ympäristöön tai/ja saman turvallisuusluokan ympäristöstä toiseen saman turvallisuusluokan ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan yksi tai useampi seuraavista käyttötapauksista: A. Matalamman luokan ympäristöstä ylemmän luokan ympäristöön suuntautuva tiedonsiirto. B. Ylemmän luokan ympäristöstä matalamman luokan tiedon siirto matalamman luokan ympäristöön. Toteutuksissa täyttyvät tyypillisesti seuraavat yleisperiaatteet: 1) Liikennevuo on täsmällisesti määritetty. 2) Liikennevuomäärityksen noudattaminen tarkistetaan. 3) Suodatus toimii luotettavasti oikeiden, sekä myös virheellisten syötteiden tapauksessa. 4) Suodatustoiminnallisuus on eriytetty sovelluspalvelun toiminnallisuudesta.

[19] Esimerkiksi tietyt viranomaisoperaatiot, joissa käsiteltävän turvallisuusluokan III tiedon salassapitoaika on lyhyt, ja joissa käytettävien kulkuneuvojen fyysiset ominaisuudet eivät mahdollista useamman päätelaitteen asennusta.

	5) Suodatustoiminnallisuuden haavoittuvuusavaruus on minimoitu[20] ja suodatus toteutetaan useassa kerroksessa[21]. Liikennevuon sisältösuodatus toteutetaan sekä verkkoteknisesti (IP-portti-rajaukset), että liikennevuon tunnistavalla suodatuksella (esimerkiksi sallimalla kyseisestä portista liikennöinnin vain tunnistetun ja hyväksytyn protokollan avulla). Liikennevuon suodatuksella tarkastetaan esimerkiksi pakettien kehystyksen oikeellisuus (täsmääkö määrityksiin, onko muodollisesti oikeaa liikennettä), pakettien kehysten kenttien maksimi-/minimipituudet (tiettyjen puskuriylivuotohyökkäysten suodatus) sekä pakettien kehysten kenttien sisällön muodollinen kelpoisuus (onko esimerkiksi sekvenssinumeroa kuvaavan kentän sisältö numeerinen). Liikennevuon sisältösuodatus sallii vain muodollisesti oikeelliseksi tunnistetut liikennevuot (allowlisting). Liikennevuon sisältösuodatuksen suodatusalustan eheydestä pyritään varmistumaan (erityisesti sitominen luotettuun rauta-alustaan ja eheystarkastukset). Yhteyksien avaaminen rajataan yleensä mahdolliseksi vain ylemmän turvallisuusluokan ympäristöstä käsin. Liikennevuon sisältösuodatusratkaisuja käytetään usein täydentävinä suojauksina osana muita yhdyskäytäväratkaisuja[22].
Sovelluskohteita	Turvallisuusluokan IV tai III järjestelmä, johon on tarve tuoda matalamman turvallisuusluokan tietosisältöä siirtävä liikennevuo (esimerkiksi VoIP-puheluliikenne) matalamman turvallisuusluokan ympäristöstä.
Soveltuvuus turvallisuus-luokittain	Tiedon omistajalle tai sen valtuuttamalle taholle saattaa olla mahdollista hyväksyä ratkaisuja riskienarviointinsa perusteella omistamiensa tietojen suojaamiseen, lähtökohtaisesti välillä Internet → TL IV tai/ja Internet → TL III.

Viitteellinen esimerkkitoteutus on esitetty kuvassa 7.



Kuva 7. Viitteellinen esimerkkitoteutus liikennevuon sisältösuodatusratkaisusta.

[20] Kattaen muun muassa käyttöjärjestelmä-, sovellusohjelmisto- ja verkkokerroksen.
[21] Esimerkiksi suodatus palomuurein IP-osoitteen ja portin, sekä IPS-järjestelmin liikennöintiprotokollan osalta.
[22] Esimerkiksi alkiotunnistuksen sisältösuodatusratkaisun tukeminen liikennevuon sisältösuodatuksella.

5.2 Virtualisointiratkaisut

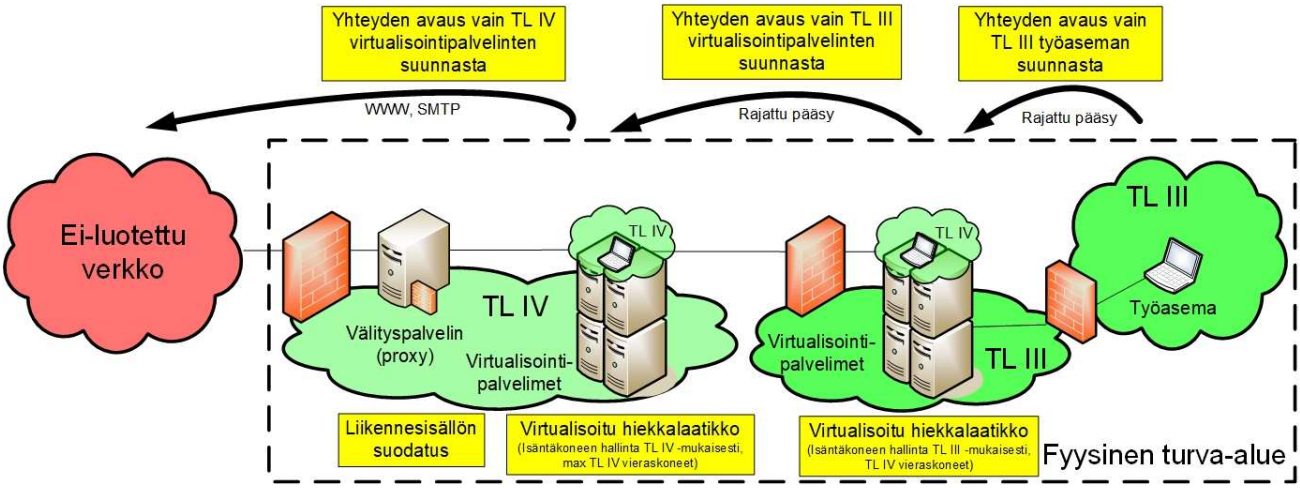
Virtualisointiratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 5.

Taulukko 5. Virtualisointiratkaisujen ominaispiirteitä.

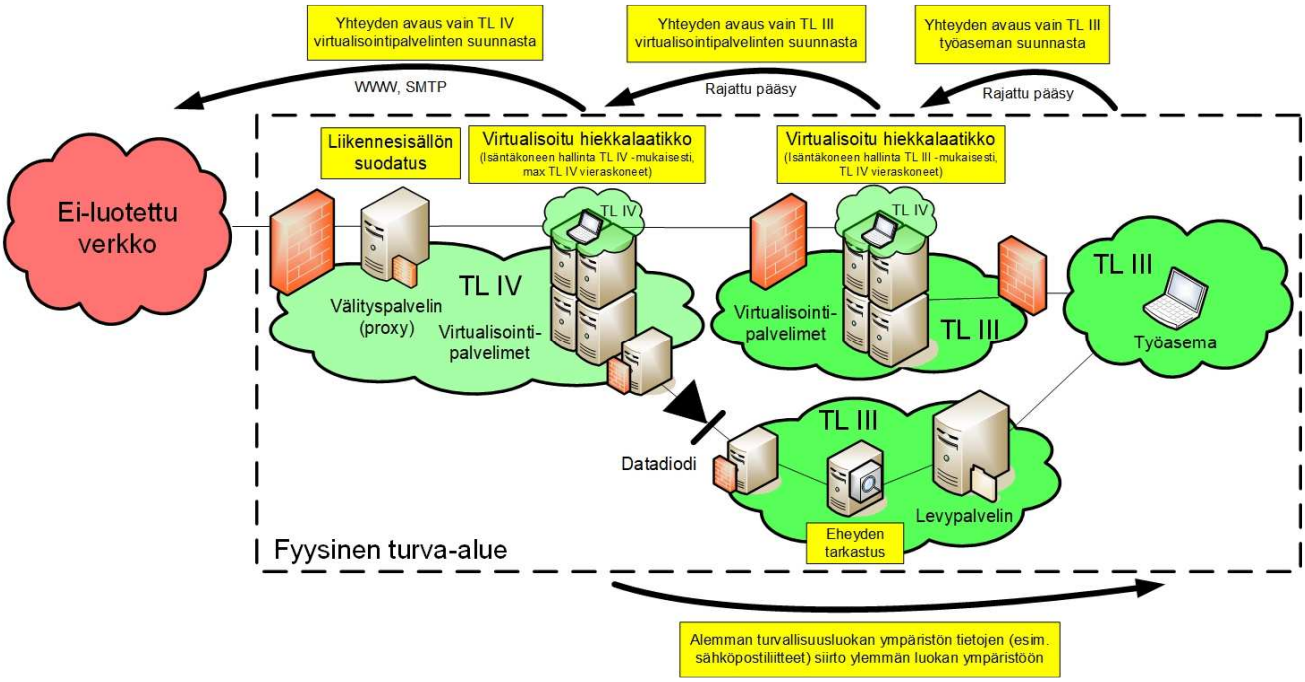
Tiedonsiirron suunta	Matalamman luokan ympäristöstä ylemmän luokan ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan matalamman luokan ympäristön käyttö ylemmän luokan ympäristöstä käsin. Tyypillisiä toteutusmalleja ovat esimerkiksi web-selailun ja sähköpostipalvelujen virtualisointiratkaisut. Virtualisointiratkaisuissa turvallisuusluokkien erottelussa nojataan usein käytettyjen virtualisointiohjelmistojen tarjoamaan suojaukseen isäntäkoneen ("host") ja vieraskoneen ("guest") erottelussa[23]. Joidenkin hyökkäysmenetelmien riskejä voidaan pienentää käyttämällä ketjutettuna useampaa eri virtualisointiratkaisutuotetta. Useissa ratkaisuissa turvallisuusluokkien erottelua tuetaan erillisellä ohjelmistoratkaisulla, jolla ylemmän luokan ympäristöön tarjotaan matalamman turvallisuusluokan vieraskoneesta vain peruskäsittelyrajapinta (näyttö, näppäimistö, hiiri) ilman esimerkiksi leikepöytä- tai levykäyttörajapintoja. Tässä mallissa isäntäkoneen hallinta- ja valvontaratkaisut tulee toteuttaa aina ylemmän turvallisuusluokan mukaisesti, ja yhteyksien avaaminen rajataan mahdolliseksi vain ylemmän turvallisuusluokan ympäristöstä käsin. Esimerkiksi web-selailun virtualisointiratkaisuissa huomioidaan tyypillisesti myös vieraskoneiden säännöllinen uudelleenalustus luotettavasta lähteestä, vieraskoneiden looginen erottelu toisistaan (esimerkiksi VLAN-erottelu) sekä vieraskoneiden ja ei-luotetun verkon välisen liikenteen suodatus tunnettujen haitallisten sisältöjen osalta välityspalvelimen ("proxy") avulla.
Sovelluskohteita	Web-selailun tai Internetissä reitittyvän sähköpostipalvelun käyttö turvallisuusluokan III ympäristöstä.
Soveltuvuus turvallisuus-luokittain	Tiedon omistajalle tai sen valtuuttamalle taholle saattaa olla mahdollista hyväksyä ratkaisuja riskienarviointinsa perusteella omistamiensa tietojen suojaamiseen, lähtökohtaisesti välillä Internet → TL IV tai/ja Internet → TL III.

Viitteellisiä esimerkkitoteutuksia on esitetty kuvissa 8, 9 ja 10.

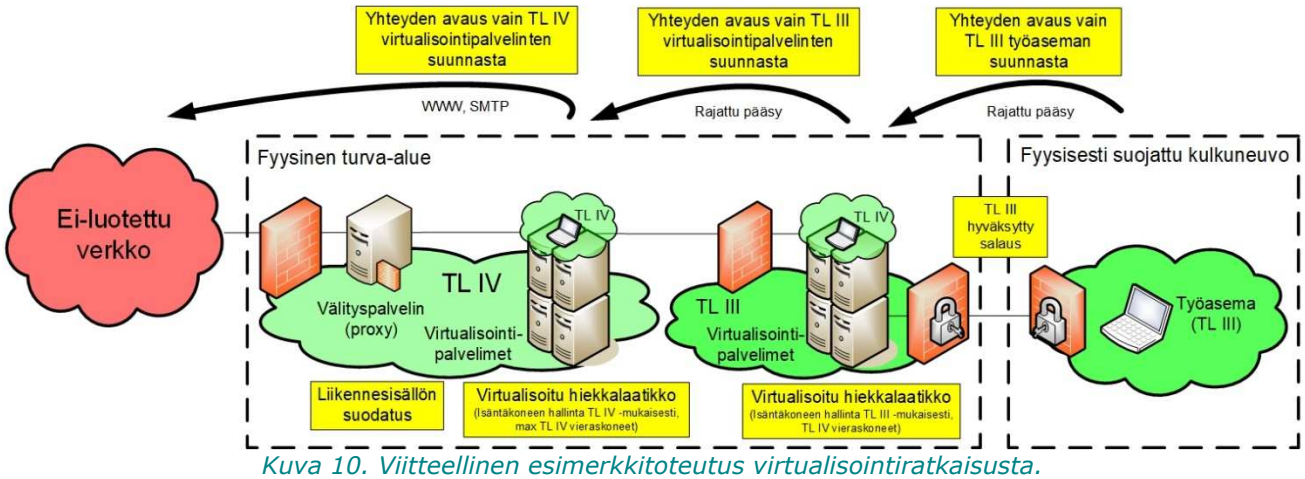
[23] Erottelusta käytetään usein käsitettä "hiekkalaatikointi" (sandboxing).



Kuva 8. Viitteellinen esimerkkitoteutus virtualisointiratkaisusta.



Kuva 9. Viitteellinen esimerkkitoteutus virtualisointiratkaisusta.



Kuva 10. Viitteellinen esimerkkitoteutus virtualisointiratkaisusta.

5.3 KVM-ratkaisut

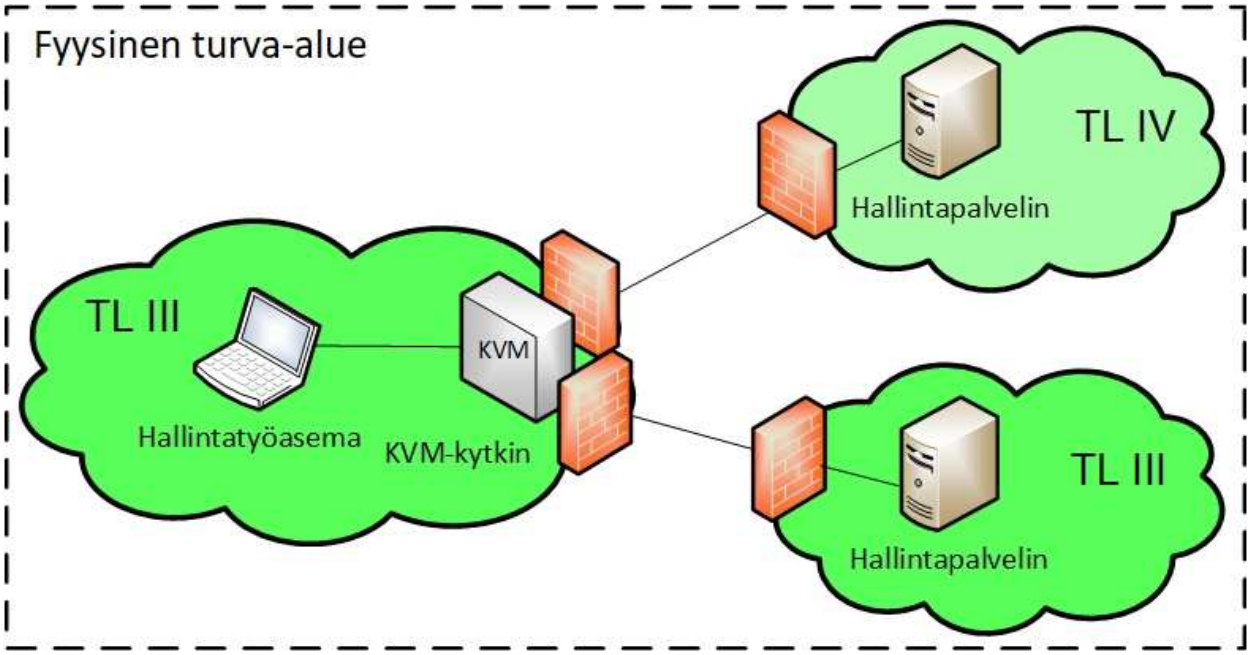
KVM-ratkaisujen (engl. "Keyboard, Video, Mouse") keskeiset ominaispiirteet on kuvattu taulukossa 6.

Taulukko 6. KVM-ratkaisujen ominaispiirteitä.

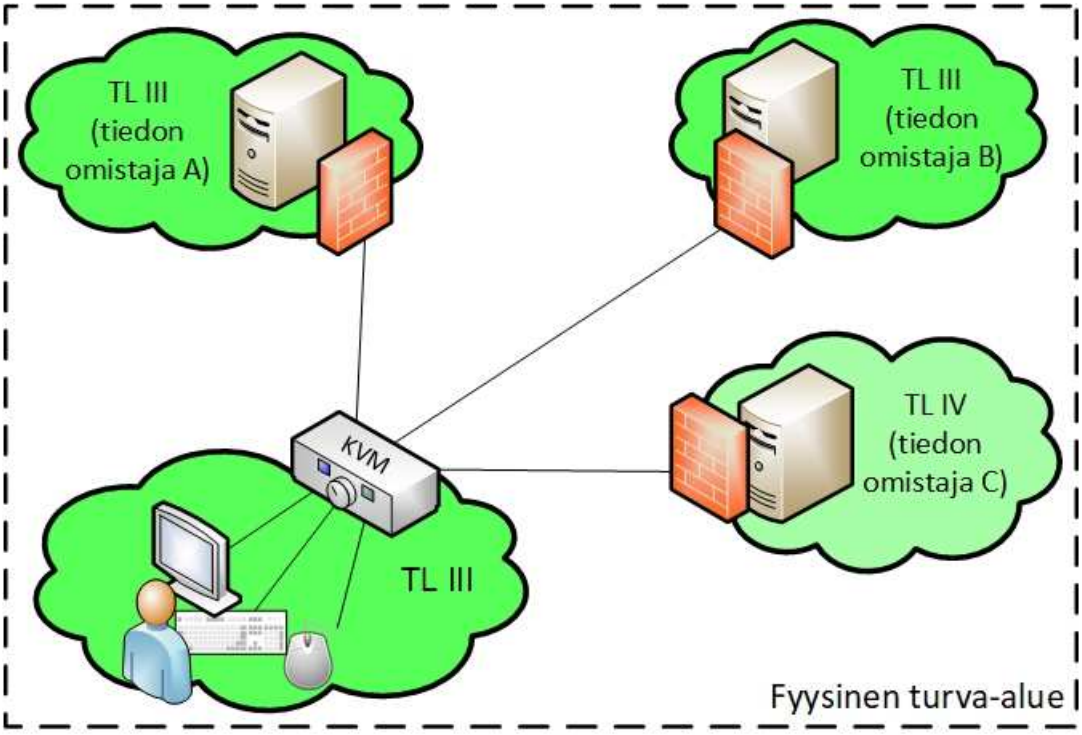
Tiedonsiirron suunta	Matalamman luokan ympäristöstä ylemmän luokan ympäristöön, ylemmän luokan ympäristöstä matalamman luokan ympäristöön, tai/ja saman turvallisuusluokan ympäristöstä toiseen saman turvallisuusluokan ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan yksi tai useampi seuraavista käyttötapauksista: A. Matalamman luokan ympäristön hallinta ylemmän luokan ympäristöstä käsin. B. Yhden näppäimistön, näytön ja hiiren sisältävän työpisteen liittäminen eri turvallisuusluokkien tai eri tiedon omistajien ympäristöihin. Yleisimpien KVM-ratkaisujen turvallisuus perustuu KVM-kytkimen kykyyn rajata liikennöinti vain näppäimistön, näytön ja hiiren toiminnallisuuksiin. Toteutustavat vaihtelevat mekaanisiin kytkimiin perustuvasta fyysisestä eriytyksestä aina monitasoiseen ohjelmistopohjaiseen loogiseen eriyttämiseen. KVM-kytkimen toimintatapaa ei voi luotettavasti päätellä vain laitteen pintapuolisella tarkastelulla. Erityisesti ohjelmistopohjaiseen eriyttämiseen nojaavista KVM-ratkaisuista tulee huomioida, että kyseiset ratkaisut koostuvat yleensä laitteistosta ja ohjelmistoista, minkä toiminnallisuudet ja riskit ovat monin paikoin yhteneviä perinteisten tietokoneiden kanssa. Useat KVM-kytkimet pystyvät esimerkiksi tarkastelemaan kaikkea niiden läpi kulkevaa tietoa, tallentamaan tiedosta itseensä kopioita tai lähettämään tiedot edelleen muille itseensä kytketyille laitteille. Useiden KVM-kytkinten laitteistoon ja ohjelmistoon voi olla haastavaa saada luotettavaa näkyvyyttä, ja myös niiden hallintaan ja valvontaan voi käyttäjäorganisaatioilla olla vain rajatut mahdollisuudet. KVM-ratkaisujen turvallisuutta yhdistää tuotekohtaisuus. Tällä tarkoitetaan sitä, että eri valmistajien tuotteet ja tuotemallit, kuten myös saman valmistajan eri tuotteet, voivat erota merkittävästi luotettavuudeltaan. Useat tuotevalmistajat pyrkivät osoittamaan tuotteensa luotettavuutta esimerkiksi eri maiden viranomaisten tuotehyväksymisprosessien kautta[24]. KVM-ratkaisuja yhdistää tyypillisesti myös se, että ne eivät pysty estämään ylemmän turvallisuusluokan tiedon kulkeutumista matalamman turvallisuusluokan ympäristöön tilanteissa, joissa esimerkiksi haittaohjelma pystyy käyttämään ylemmän turvallisuusluokan ympäristön näppäimistöä.
Sovelluskohteita	Turvallisuusluokan III hallintatyöasemalta käsin tapahtuva turvallisuusluokan IV ympäristön ylläpito/hallinta. Käyttäjän pääsy työpisteeltään, samaa näppäimistöä, näyttöä ja hiirtä käyttäen, eri turvallisuusluokkien tai eri tiedon omistajien ympäristöihin.
Soveltuvuus turvallisuus-luokittain	Tiedon omistajalle tai sen valtuuttamalle taholle saattaa olla mahdollista hyväksyä riskienarviointinsa perusteella täydentävillä suojauksilla varustettuja tuotteita, lähtökohtaisesti välillä TL IV → TL III, Internet → TL IV tai/ja saman turvallisuusluokan sisällä (eri tiedon omistajat).

[24] Joidenkin maiden joihinkin käyttötapauksiin hyväksymiä tuotteita on listattu osoitteessa http://www.ia.nato.int/niapc.

Viitteellisiä esimerkkitoteutuksia on esitetty kuvissa 11 ja 12.



Kuva 11. Viitteellinen esimerkkitoteutus KVM-ratkaisusta.



Kuva 12. Viitteellinen esimerkkitoteutus KVM-ratkaisusta.

5.4 Ohutpääteratkaisut

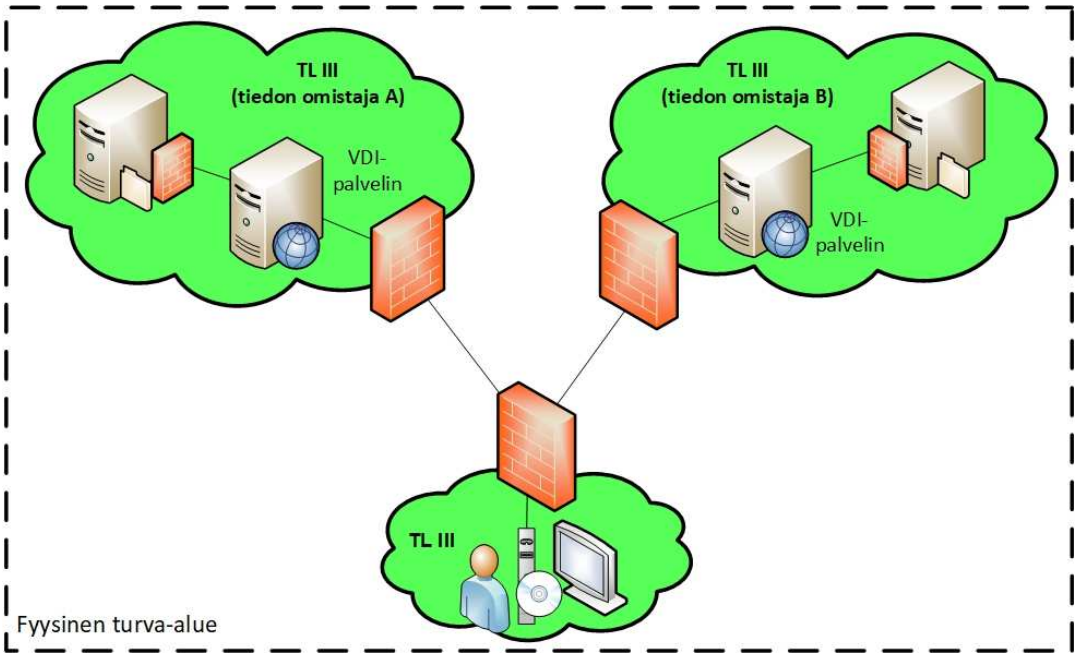
Ohutpääteratkaisujen (engl. "thin/zero client") keskeiset ominaispiirteet on kuvattu taulukossa 7.

Taulukko 7. Ohutpääteratkaisujen ominaispiirteitä.

Tiedonsiirron suunta	Matalamman luokan ympäristöstä ylemmän luokan ympäristöön, ylemmän luokan ympäristöstä matalamman luokan ympäristöön, tai/ja saman turvallisuusluokan ympäristöstä toiseen saman turvallisuusluokan ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan yksi tai useampi seuraavista käyttötapauksista: A. Eri turvallisuusluokkien ympäristöjen käyttö yhdellä päätelaitteella. B. Eri tiedon omistajien ympäristöjen käyttö yhdellä päätelaitteella. Yleisimpien ohutpääteratkaisujen turvallisuus perustuu siihen, että päätelaite alustetaan jokaisen käyttökerran alussa luotetusta lähteestä ja tyhjennetään aina käyttökerran päätyttyä. Tyypillisiä alustamiseen käytettyjä menetelmiä ovat käynnistäminen kirjoitussuojatulta medialta[25] tai fyysisesti suojatusta verkkokytkennästä. Erityisesti luotettava tyhjentäminen on haaste, johon tyypillisesti pyritään vastaamaan minimoimalla päätelaitteen ohjelmallisesti muokattavat laitteisto-osat ja toiminnallisuudet[26], sekä tarjoamalla päätelaitteelle suojattavat tiedot vain virtuaalityöpöytäratkaisuilla[27]. Ohutpääteratkaisut eivät tyypillisesti kykene estämään suojattavan tiedon kulkeutumista[28] päätelaitteelle. Päätelaite tuleekin suojata aina korkeimman sillä käsiteltävän tiedon turvallisuusluokan mukaisesti. Erityisiä riskejä liittyy tilanteisiin, joissa päätelaitteelle tarjotaan samanaikaisesti eri turvallisuusluokkien tai eri tiedon omistajien tietoja. Useimmissa ratkaisuissa on mahdollisuus pyrkiä ohjelmallisesti estämään tiedon välittyminen, esimerkiksi leikepöydän kautta, eri virtuaalityöpöytäistuntojen välillä. Näissä tilanteissa tietojen erottelu nojaa usein vain virtuaalityöpöytäratkaisun ohjelmistototeutuksen luotettavuuteen.
Sovelluskohteita	Samalla päätelaitteella tapahtuva eri turvallisuusluokan tai/ja eri tiedon omistajien ympäristöjen käyttö.
Soveltuvuus turvallisuus-luokittain	Tiedon omistajalle tai sen valtuuttamalle taholle saattaa olla mahdollista hyväksyä ratkaisuja riskienarviointinsa perusteella, lähtökohtaisesti välillä TL IV → TL III, Internet → TL IV tai/ja saman turvallisuusluokan sisällä (eri tiedon omistajat).

Viitteellinen esimerkkitoteutus on esitetty kuvassa 13.

[25] Esimerkiksi CD-ROM-levy.
[26] Esimerkiksi käyttämällä päätelaitetta, jossa pysyvämmän tiedontallennuksen mahdollistavat muistialueet (muun muassa laiteohjelmisto, engl. firmware) on pyritty lukitsemaan muutoksilta.
[27] Engl. Virtual desktop infrastructure, VDI.
[28] Tieto välittyy tyypillisesti ainakin kuvana.



Kuva 13. Viitteellinen esimerkki ohutpääteratkaisusta.

5.5 Monitasopääteratkaisut

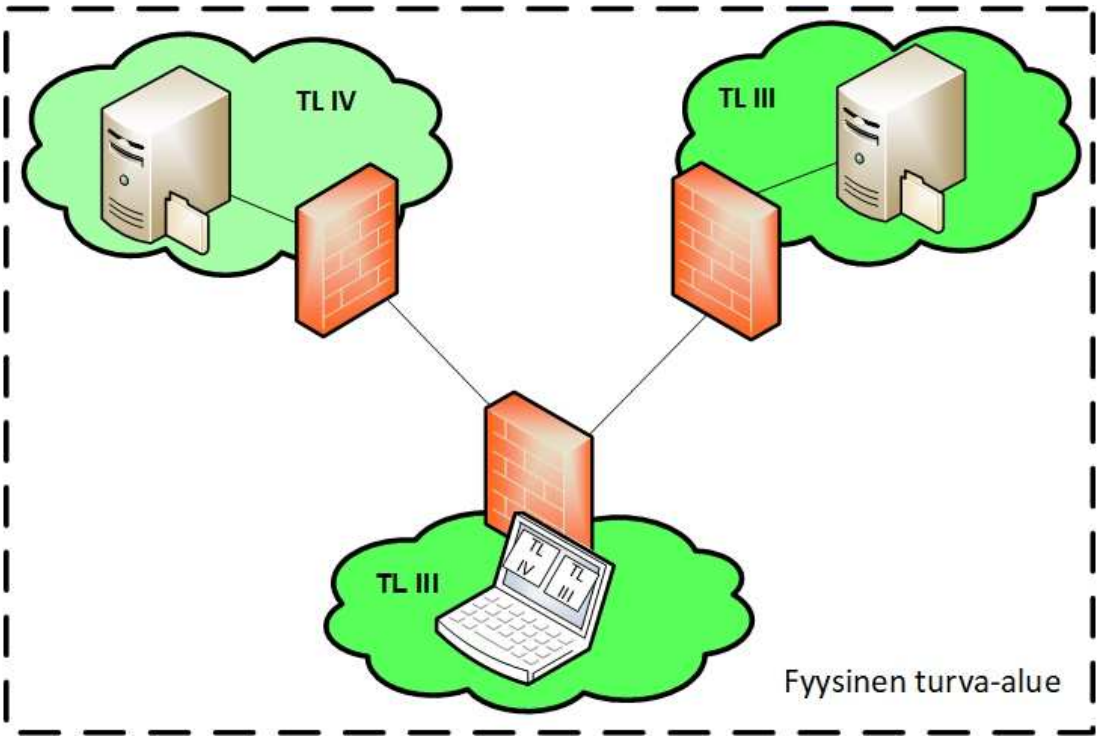
Monitasopääteratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 8.

Tiedonsiirron suunta	Matalamman luokan ympäristöstä ylemmän luokan ympäristöön, ylemmän luokan ympäristöstä matalamman luokan ympäristöön, tai/ja saman turvallisuusluokan ympäristöstä toiseen saman turvallisuusluokan ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan eri turvallisuusluokkien ympäristöjen käyttö yhdellä erikoisvalmisteisella päätelaitteella. Monitasopääteratkaisujen turvallisuus perustuu päätelaitteen laitteisto- tai/ja ohjelmistotasolla toteutettavaan turvallisuusluokkien erotteluun. Erottelu on tuotteesta riippuen toteutettu joko A) täysin ohjelmistolla, B) osin ohjelmistolla ja osin laitteistolla, tai C) täysin laitteistolla. Mallin A ratkaisuissa laitteistoalustan päällä ajetaan räätälöityä käyttöjärjestelmäalustaa, jonka pääasialliset tehtävät ovat tarjota laitteistoalustan käyttämiseen välttämättömät rajapinnat, sekä virtualisointiratkaisu, jonka päällä varsinaiset eri turvallisuusluokkien tietoa sisältävät virtuaalikoneet ajetaan. Tällaisille ratkaisuille on tyypillistä, että räätälöity käyttöjärjestelmäalusta on huomattavasti suppeampi kuin yleiset saatavilla olevat käyttöjärjestelmät, ja suppeampi koodimäärä on pyritty toteuttamaan mahdollisimman virheettömästi. Tällaisten ratkaisujen tarjoama turvallisuusluokkien erottelu nojaa erityisesti räätälöidyn käyttöjärjestelmäalustan luotettavuuteen. Mallin B ratkaisuissa suojaus nojaa osin ohjelmisto- ja osin laitteistotason erotteluun. Tyypillinen ratkaisumalli on, että eri turvallisuusluokan ympäristöt asennetaan fyysisesti erillisille kiintolevyille, mutta hyödyntävät esimerkiksi samoja fyysisiä verkkoportteja. Mallin C ratkaisuissa erottelu on pyritty toteuttamaan mahdollisimman pitkälti fyysisellä tasolla. Tyypillinen ratkaisumalli on, että keskeinen eri

	turvallisuusluokille yhteinen laitteisto on näyttö, mutta että lähes kaikki muut laitteistot on kahdennettu päätelaitteen ulkokuoren sisällä. Erityisesti täysin ohjelmistolla toteutettavaan erotteluun nojaavista monitasopääteratkaisuista tulee huomioida virtuaalikoneiden käyttämiin jaettuihin resursseihin[29] liittyvät riskit. Jaettujen resurssien kautta on yleensä mahdollista muodostaa sivukanava tiedonsiirtoa varten eri virtuaalikoneiden välille, mikä voi mahdollistaa esimerkiksi ylemmän turvallisuusluokan tiedon oikeudettoman siirtämisen matalamman turvallisuusluokan ympäristöön. Sivukanavan hyödyntämisen edellytyksenä on tyypillisesti se, että hyökkääjän hallinnoima ohjelmakoodi saatetaan suoritettavaksi laitetta hallinnoivaan virtualisointialustaan (hypervisor) tai sen ajuriin, laitteistoläheisempään ohjelmistoon[30] tai esimerkiksi prosessorin, näytönohjaimen tai vastaavan komponentin mikrokoodiin. Sivukanavan hyödyntäminen on yleensä mahdollista myös tilanteissa, joissa hyökkääjän hallinnoima ohjelmakoodi saatetaan suoritettavaksi ylemmän ja matalamman turvallisuusluokan virtuaalikoneisiin. Aika ajoin havaitaan myös sellaisia sivukanavien hyödyntämistapoja, joissa virtualisoidusta matalamman luokan ympäristöstä käsin voidaan tehdä päätelmiä prosessorin ja muistin muusta toiminnasta tai muissa virtuaalikoneissa käsiteltävistä tiedoista. Sivukanavan hyödyntämiseen liittyviä riskejä voidaan merkittävästi pienentää toteuttamalla monitasopääteratkaisu niin sanottuna monikäynnistyksellisenä (multi-boot). Tällä tarkoitetaan ratkaisumallia, jossa eri virtuaalikoneet ovat omissa, eri avaimistoilla salatuissa konteissaan ja jossa vain yhden virtuaalikoneen käynnistäminen kerrallaan on mahdollista. Monitasopäätelaitteiden turvallisuutta yhdistää tuotekohtaisuus. Tällä tarkoitetaan sitä, että eri valmistajien tuotteet, kuten myös saman valmistajan eri tuotteet, voivat olla luotettavuudeltaan merkittävästi eroavia. Useat tuotevalmistajat pyrkivät osoittamaan tuotteensa luotettavuutta esimerkiksi eri maiden viranomaisten tuotehyväksymisprosessien kautta[31]. Monitasopäätelaitteita yhdistää myös se, että niitä ei ole tyypillisesti suunniteltu tilanteisiin, joissa eri tiedon omistajat varaavat teknisen tarkastusoikeuden tietojensa käsittely-ympäristöihin.
Sovelluskohteita	Samalla päätelaitteella tapahtuva eri turvallisuusluokan ympäristöjen käyttö.
Soveltuvuus turvallisuus-luokittain	Tiedon omistajalle tai sen valtuuttamalle taholle saattaa olla mahdollista hyväksyä ratkaisuja riskienarviointinsa perusteella, lähtökohtaisesti välillä TL IV → TL III tai Internet → TL IV.

Viitteellinen esimerkkitoteutus on esitetty kuvassa 14.

[29] Esimerkiksi virtalähde, prosessori, muisti, näytönohjain, massamuisti, äänikortti, näppäimistö ja hiiri.
[30] Yleensä BIOS tai UEFI.
[31] Joidenkin maiden joihinkin käyttötapauksiin hyväksymiä tuotteita on listattu osoitteessa http://www.ia.nato.int/niapc.



Kuva 14. Viitteellinen esimerkki monitasopääteratkaisusta.

6 Lisätietoa

1. Bell, D & LaPadula, L. 1973. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, Volume I & II.
2. Euroopan unionin neuvosto. 2013. Neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi (2013/488/EU). URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:274:0001:0050:FI:PDF.
3. International Organization for Standardization. 1994. ISO/IEC 7498-1:1994. Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model.
4. Jones, D & Bowersox, T. 2006. Secure data export and auditing using data diodes. In *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop* (EVT'06). URL: http://homepage.cs.uiowa.edu/~jones/voting/diode/evt06paper.pdf.
5. Kang, M, Moskowitz, I & Chincheck, S. 2005. The Pump: A Decade of Covert Fun. In *Proceedings of the 21st Annual Computer Security Applications Conference* (ACSAC '05). URL: http://www.acsac.org/2005/papers/Kang.pdf.
6. Kansallinen turvallisuusviranomainen. 2020. Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille. URL: https://um.fi/documents/35732/0/Katakri-2020_201218.pdf.
7. NIST. 2004. NIST Special Publication 800-27 Rev A: Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A. URL: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
8. Okhravi, H & Sheldon, F. 2010. Data Diodes in Support of Trustworthy Cyber Infrastructure. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10). URL: http://web.mit.edu/ha22286/www/papers/CSIIRW10.pdf.
9. Stevens, M. 1995. An Implementation of an Optical Data Diode. DSTO-TR-0785. URL: https://apps.dtic.mil/sti/pdfs/ADA365579.pdf.
10. Tiedonhallintalautakunta. 2021. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM2021:05). URL: http://urn.fi/URN:ISBN:978-952-367-500-1.