jamk.fi

Unidirectional patch management solution to isolated network

Teemu Keso

Master's thesis
November 2018
School of Technology, Communication and Transport
Degree Program in Information Technology
Cyber Security

jamk.fi

Description

Author(s)	Type of publication	Date
Keso, Teemu	Master's thesis	17.10.2018
		Language of publication: English
	Number of pages: 57	Permission for web publication: Yes

Title of publication
Unidirectional patch management solution to isolated network

Degree programme
Master´s Degree Programme in Information Technology, Cyber Security

Supervisor(s)
Saharinen, Karo (JAMK) and Karjalainen, Mika (JAMK)

Assigned by
Mustikkamaa, Tommi

Abstract

The security of a nation's information systems is extremely important for the public security of an entire country. Various governmental networks worldwide are under constant attack from hackers and foreign state actors. Information systems are designed to be updated with security patches and newer versions of the software. If one does not apply security updates are not applied, it may compromise the system to an attack. Network isolation will achieve some information security, as the network is harder to reach by an attacker; however, this does not prevent attackers from attacking the network in some way.

The goal of the research was to identify the requirements for public authority implementing a unidirectional patch management solution to an isolated network and to develop a solution. The proposed solution, which was tested in a Proof of Concept environment that was built for this study purpose. The unidirectional patch management solution was developed with a use of an optical data diode product that transported Windows and Linux patch management files to the isolated network.

Information security audit tool for Finnish government authorities, KATAKRI 2015 was chosen for interpretation and assessment fulfilment of the requirements. Furthermore, the proposed solution was compared to publicly available information regarding a public authority's approval of unidirectional security gateway solutions.

It was not possible to conclude from the results whether all requirements were identified and implemented exactly the way a competent accreditation authority would require in order to approve a solution due to the fact that the implementation examples presented in KATAKRI 2015 itself could only be regarded as a de facto way of implementation which can in some cases achieve the required level of fulfilment.

Keywords/tags
KATAKRI, VAHTI, Data diode, Security Gateway Solutions, Patch Management

Miscellaneous

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Sukunimi, Etunimi	Opinnäytetyö, ylempi AMK	17.10.2018
	Sivumäärä 57	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: Kyllä

Työn nimi
Yksisuuntainen päivitystenhallinta suljettuun verkkoon

Tutkinto-ohjelma
Insinööri (YAMK), Kyberturvallisuus

Työn ohjaaja(t)
Saharinen, Karo (JAMK) ja Karjalainen, Mika (JAMK)

Toimeksiantaja(t)
Mustikkamaa, Tommi

Tiivistelmä

Valtiollisten tietojärjestelmien turvallisuus on kriittinen osa koko maan yleistä kokonaisturvallisuutta. Ympäri maailmaa lukuisat valtiolliset tietoverkot ovat jatkuvien hyökkäysten kohteena hakkereiden ja valtiollisten toimijoiden toimesta. Tietojärjestelmät on suunniteltu päivitettäväksi tietoturvapäivityksillä sekä uudempien ohjelmistoversioiden avulla. Jos tietojärjestelmiä ei ylläpidetä tietoturvapäivityksillä voi se vaarantaa koko tietojärjestelmän hyökkäyksille. Näiden järjestelmien eriyttämisellä suljettuun verkkoon saavutetaan joitain tietoturvaetuja, koska hyökkääjien on vaikeampi saavuttaa verkkoa, mutta eriyttäminen ei estä hyökkäyksiä kokonaan.

Opinnäytetyön tavoitteena oli tunnistaa, mitkä ovat valtiollisen toimijan toteuttamisvaatimukset yksisuuntaisen päivitysjärjestelmän toteuttamiselle suljettuun verkkoon ja toteuttaa Proof of Concept -ympäristö, missä vaatimuksien toteutuminen sekä toimivuus testataan. Yksisuuntainen päivitysjärjestelmä toteutettiin käyttämällä optista datadiodi-tuotetta, jonka avulla mahdollistettiin Windows- ja Linux-päivitystiedostojen siirtämiseen suljettuun verkkoon.

Tutkimuksen vaatimuksien identifioimiseen ja tulkintaan sekä työssä toteutetun ratkaisun arviointiin käytettiin kansallista KATAKRI 2015 tietoturvallisuuden auditointityökalua Suomen viranomaisille. KATAKRI 2015:n lisäksi tutkimuksessa toteutettua ratkaisua arviointiin käyttämällä julkisesti saatavilla olevaa tietoa arviointilaitoksen hyväksymästä yhdyskäytäväratkaisusta.

Tutkimuksen tuloksista ei voida todeta, olivatko kaikki vaatimukset yksilöity ja toteutettu täsmälleen sillä tavalla, jonka toimivaltainen viranomainen vaatisi hyväksytyltä ratkaisulta. Tämä johtuu siitä, että itse KATAKRI 2015:ssä esitettyjä toteutusesimerkkejä voidaan pitää vain de facto -mallina toteutukselle, joka voi vain tietyissä tapauksissa saavuttaa vaaditun tason, jota odotetaan hyväksytyltä mallilta.

Avainsanat
KATAKRI, VAHTI, data diodi, yhdyskäytävä ratkaisu, päivityksien hallinta

Muut tiedot

Contents

Figures

1 Introduction

In the past few years cyber and information security have become the new mainstream. As data breaches have affected up to three billion users as was the case with Yahoo (Oath 2017), and widespread ransomware epidemics that have affected all corners of society from consumers to hospital information systems. In May 2017 the national health system (NHS) of the United Kingdom was affected by the ransomware “WannaCry”. The infected computers and healthcare devices were using an unpatched or unsupported Windows operating system. (Investigation: WannaCry cyber attack and the NHS 2017, 10)

Security of a nation’s information systems is extremely important for the public security of an entire country. Various governmental networks worldwide are under constant attack from hackers and foreign state actors. The latest and most famous case in Finland has been a data leak in the Ministry of Foreign Affairs, in which the foreign actors were able to break into the Ministry's information systems and steal documents and emails from several years. (Suojelupoliisin toimintaympäristö vuosina 2015–2016, 2015, 7-8)

A typical way to import updates to an isolated network is by using a portable media that a designated person will transport from an untrusted network to a trusted network. All steps in the process are done manually. Therefore they are prone to time delays, human errors, and unintentional neglection of the transfer process. (Jones & Bowersox, 2006)

Research goals and methods

The idea for this thesis came up from a question of how to improve the thesis assigner’s Windows and Linux patch management process in an isolated network without compromising network isolation.

The solution of this thesis needs to comply with the Finnish laws, acts, regulations, and guidelines set for public authorities. In addition, the solution should speed up the whole update process, and the implementation solution should not under any circumstances allow information to leak from the isolated network.

The goal for this thesis project was to research and develop a unidirectional patch management solution that meets the aforementioned requirements. The research methodology chosen for this thesis was qualitative research that consisted of literature review, narrative analysis and a case study.

The literature review was conducted with a focus on regulations and guidelines on the subject using a narrative analysis to identify and encapsulate the requirements. A case study was designed to fulfil the design and auditing requirements. The requirement identified and implemented into the case study was compared to the limited information on successful implementation of security gateway solutions obtained from Finnish communication regulatory authority's public documents.

For this thesis, a case study was chosen because it is a well-established way to apply a theoretical concept to a real word situation. As Robison (1993, 146) states:

> *Case study is a strategy for doing a research which involves an empirical investigation of a particular contemporary phenomenon within its real-life context and using multiple sources of evidence*.

2 Theoretical background

In general, the Finnish acts do not typically define how the requirement should be fulfilled but they rather define the goals. This chapter presents some of the 'de facto' information security standards that are referred in the requirements as per acts or official guides.

The Finnish Act Decree on the Openness of Government Activities and on Good Practice in Information Management (1030/1999, 1§) requires government officials to implement a good information management processes when handling digital and physical documents. The act also states that a government authority has to investigate and assess the availability, usability, quality, and security of the information systems, as well as, security threats.

2.1 Patch management

VAHTI guide for Terminal Device Information Security Guidelines (VAHTI 5/2013) states that it is essential to keep track of the released security updates and to install them in a controlled manner but also as quickly as possible. In addition, it is important to track published vulnerabilities that affect hardware, operating systems and applications.

In 2017, a total number of 14,712 vulnerabilities were released in the Common Vulnerabilities and Exposures (CVE) vulnerability database. This is twice as much of vulnerabilities released in the previous year. For the majority of vulnerabilities, the vendor has released a fix; however, some of the vulnerabilities have been so-called zero-day vulnerabilities, in which no mitigation solutions existed during the release of the vulnerability. (Mertens 2017)

FireEye reported in 2017 that in less than a week after Microsoft released a security update, attackers were using the vulnerability in a targeted attack against a government official in the Middle East. The attacker has been suspected to be a state-run Advanced Persistent Threat (APT) group conducting a long-term cyber

espionage in nation-state interests. (Sardiwal, Londhe, Fraser, Richard, O'Leary & Cannon 2017)

Due to the fast reverse engineering and vulnerability exploitation, some government organizations have stated recommendations regarding security patching. For example, in cases where vulnerability is classified as an extreme risk, the Australian Cyber Security Centre recommends that the security patch must be applied and verified within 48 hours after its release. (Assessing Security Vulnerabilities and Applying Patches 2018, 2-3)

2.1.1 Microsoft patch management

With the release of Windows 10, Microsoft released Windows as a service model. With this model, products are not sold as a one-time license but as a service subscription offering the latest version of the product and its updates that contain new features twice a year. In this service model, Microsoft offers Windows 10 and Server 2016 with either Semi-Annual Channel or Long-Term Servicing Channel (LTSC), in which the end-user can choose how fast new features and updates will be implemented. (Overview of Windows as a service 2018)

Semi-Annual Channel is designed for end-users wanting to receive the newest features that are available for the product at the earliest opportunity. Every new release is called a feature update. New feature updates are typically published twice a year. These feature updates in practical terms new build of that operating system. Feature update is identified by four numbers that indicate the year and the month of the release. Each release is supported by Microsoft for a maximum 18 months. (Windows Server Semi-Annual Channel overview, 2017 ; Leppänen, 2017)

Long-Term Servicing Channel (LTSC) is designed for critical or specialized systems that require support, security and stability for a long period of time. A new LTSC version is released every 2-3 years. (ibid.)

Another change compared to the previous Windows versions is the new patch management model introduced with Windows 10. In this new model, different kinds of updates are not released as separate update files but as a cumulative package. A new cumulative packet is released every month. This packet includes all security,

reliability and bug fixes that are needed to patch the operating system to the latest secure version. This new monthly cumulative packet is referred to as a quality update and is typically released on the second Tuesday of every month. In October 2016, the same cumulative patch model was applied to previous Windows and Server versions that are still supported. (Mercer 2016)

The patch management files that are published for supported Windows and Server versions are digitally signed with Microsoft root certificate to determine the validity and integrity package. Each patch management file is then verified by the clients' Windows update agent to have the correct digital signature. (Windows Update Services: Client-Server Protocol, 2017)

In isolated networks, Windows Server Update Services (WSUS) is recommended by Microsoft to provide patch management. This is done with an installation of two WSUS servers. One server is connected to the Internet and the other is installed to the isolated network. The patch information is then manually exported and transferred to the isolated network. (Configure a Disconnected Network to Receive Updates 2016)

2.1.2 Linux patch management

Linux systems come in many different distributions that differ in their ability and features, which also means that there are several different ways of updating the system. Compared to Microsoft, there is no single centralized software update. Also, the support of each distribution might be different in each release. Some commercial distributions such as Red Hat offer commercial support.

Linux and Linux packet management updates are typically done by using distribution-specific tools such as yum (Yellowdog Updater, Modified), which is used in Red Hat Linux derived distributions, and APT (Advanced Package Tool) which is used in Debian derived Linux distributions. (Pulliainen 2016)

With a packet manager, it is possible to update, install and confirm dependencies of pre-compiled packages of a Linux distribution. In general, each distribution releases its own software packets to a public archive called software repository. These packages are then signed with that Linux distribution's PGP private key. With this

PGP signature, it is possible to validate the validity and integrity package that is published in a software repository. A single operating system can use several different software repositories that vary in their level of stability, trustworthiness, support and release speed. Isolated networks typically host their own repositories to enable patch management and easy distribution of custom software. (Pulliainen 2016)

2.2 Multi-Level Security in classified information systems

When handling classified information the confidentiality requirements are defined by the impact of the result from unauthorized disclosure or unauthorized use. The higher the classification level, the bigger the impact is on international relationships, government security, national defense or public interest. (VAHTI 2/2010, 2010, 52-57)

One of the best-known access control model designs to protect classified information is Bell-LaPadula (BLP). The model was created in the 1970s by Bell and La Padula to protect classified information in the U.S. Air Force. The BLP model is sometimes also referred as multilevel security (MLS) where the basic rule is that information can flow to higher levels but not lower. (Anderson 2008)

The Bell-LaPadula access control model defines user's ability to access classified information and is based on user's security clearance and need-to-know basis. The model is defined by two mandatory access rulesets as shown in Figure 1. (Schotanus, Hartog & Verkoelen 2012)

- *"No Read Up: no read access is permitted to an object with a higher classification than the clearance of the user"* (ibid.)
- *"No Write Down: no write access is permitted to an object with a lower classification than the clearance of the user."* (ibid.)

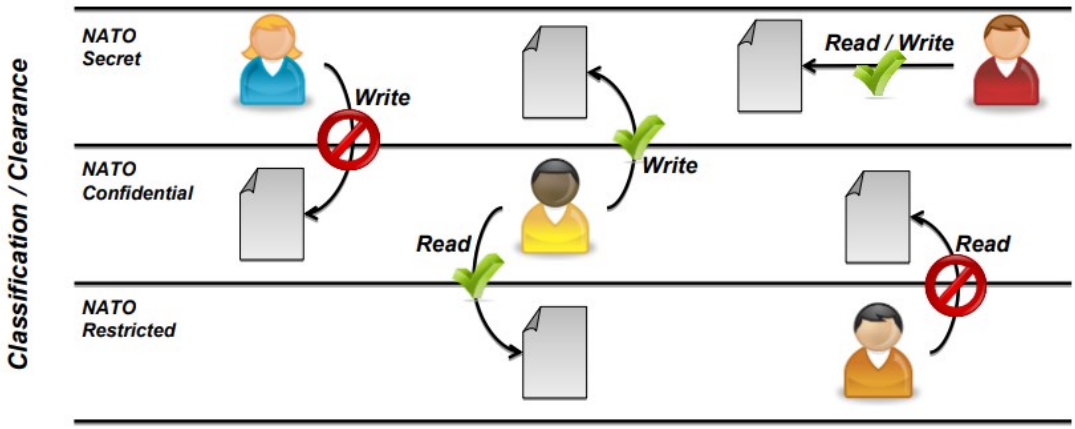

Figure 1. Bell-LaPadula access rules (Schotanus, Hartog & Verkoelen 2012)

One way to implement No-Read-Up and No-Write-Down access rules is by using network isolation. The environment is protection level set by the highest classification of information it contains resulting the enforcement of the rule No-Read-Up. The access rule No-Write-Down is enforced by the network isolation that prevents transferring information to a lower protection level. (Kiviharju 2016)

2.3 Information security requirements in the Finnish law

Information security in Finland is regulated by acts and official requirements. This subchapter presents the key requirements for governing security in a government administration. The main requirement for information security can be found in one act. The Information Security in Central Government act section 5 (Act 681/2010, 5§) contains ten basic level requirements for information security that each government authority must meet in systems that are handling government documents.

The act on Information Management Governance in Public Administration (Act 634/2011) states that the Ministry of Finance is responsible for the general guidance on the information administration of public administration authorities. The act's section 6 (ibid., 6§) states that the ministry has the right to give out norms based on the Government Information and Cyber Security Management Board (VAHTI) recommendations. These VAHTI guidelines are referred to as information management standards in a public administration to achieve the required level stated in the act 681/2010.

The Act on the Evaluation of Government Information Systems and Data Transfer Arrangements (Act 1406/2011) states that The Finnish Communications Regulatory Authority (FICORA) is responsible for ensuring the public authorities security of information and telecommunications systems. FICORA also provides certificates of accreditation and publishes official Guidance Interpretation of Criteria for Evaluation on how to interpret the criteria stated in different acts and guides (Guidance Interpretation of Criteria for Evaluation 2015).

Guidance Interpretation of Criteria for Evaluation states that a government entity can either use VAHTI guidelines for information security review or Information Security Audit Tool for Authorities (KATAKRI), or even the combination of these two. However, FICORA recommends solely to use KATARI because VAHTI and KATARI only differ in the way the guidelines are presented. The requirements are the same in both guides; however, in VAHTI guides they are divided into several different publications. (ibid.)

2.4 Information and Cyber Security Management Board (VAHTI)

The Ministry of Finance is responsible for the general development of data security and governance of information security of state administration by the act on the Governance of Data Administration in Public Administration (Act 634/2011). The Ministry of Finance has appointed Government Information Security Management Board (VAHTI) to act as the responsible party that develops and governs digital security in public administration by publishing VAHTI guidelines. These guidelines have been published since 1997 in several different areas. (Rousku 2017)

VAHTI Information Security Assessment Guide (VAHTI 2/2014, 2014) published in 2014 describes the necessary steps but also which and what VAHTI guides are necessary to be implemented in order to achieve the basic level of data security. As the VAHTI guides have not been updated after their release, FICORA has instructed in the Guide for Accredited Inspection Bodies how to implement the requirements. (Guide for accredited inspection bodies 2017)

2.5 Information Security Audit Tool for Authorities (KATAKRI)

KATAKRI is a security auditing tool for assessing the ability to protect classified information. This guide has been published by the National Security Authority (NSA) operating under the Finnish Ministry of Foreign Affairs. KATAKRI itself is not a mandatory requirement on information security by law, rather it brings together the minimum requirements in national legislation and international agreements. (KATAKRI - Information security audit tool for authorities – 2015)

The first version of KATAKRI was published in 2009 and then revised for the second version in 2011. The latest version of KATAKRI was published in 2015 and is also recognized as KATAKRI 2015. It includes significant changes in structure and can thus be regarded as a new document rather than an update. (ibid.)

KATAKRI is divided into three subdivisions that are: security management (T), physical security (F), and Information assurance (I). Each subdivision states basic level requirements needed to fulfil national and international laws but also requirements for achieving a higher level classification approval.

KATAKRI further states that in organizations or networks that handle national classified information, the requirements are divided into three classification levels: KÄYTTÖ RAJOITETTU (ST IV), LUOTTAMUKSELLINEN (ST III) and SALAINEN (ST II). These are equal to internationally recognized classification levels RESTRICTED, CONFIDENTIAL and SECRET. In official use, the only law binding a way to classify information is to use either Finnish or Swedish language classification. (ibid.)

2.6 Designing and Implementing Secure Gateway Solutions

The Finnish Communications Regulatory Authority (FICORA) has published a guide for designing and implementing secure gateway solutions (Designing and Implementing Secure Gateway Solutions 2016) that specifies the design and operational requirements stated in KATAKRI and VAHTI to establish a network connection

between two different protection levels. The first version of this guide was published in 2013 and the current third version in 2016.

The guide defines the Bell-LaPadula model rules No-Write-Down and No-Read-Up as key principles of implementation that any acceptable gateway security gateway model must follow when connecting two networks of different security classifications. (Designing and Implementing Secure Gateway Solutions 2016)

A typical way to implement the Bell-LaPadula model rules is by using either one-way data transfer device such as data diode or content filtering solutions where classified data information is detected and handled accordingly.

Designing and implementing Secure Gateway Solutions guide also describes solutions that, in principle, are not allowed to be used. However, the information owner can approve an implementation solution after assessing the risk. (ibid.)

3 Technologies and requirements in network isolation

One of the key requirements of the VAHTI guides and KATAKRI is to separate information systems by their classification. This means that network connections to untrusted networks are either limited or in higher security networks where all connections to other networks are completely disconnected.

3.1 Network Technologies in classified networks

Successfully configured corporate networks typically utilize network segmentation in order to separate different parts of the network using routers and firewalls as shown in Figure 2. Only the approved traffic is passed through from one segment to the other. Segmentation by itself does not prevent an attack but limits the availability of for example TCP/UDP ports of a given network segment. (Peterson 2016)

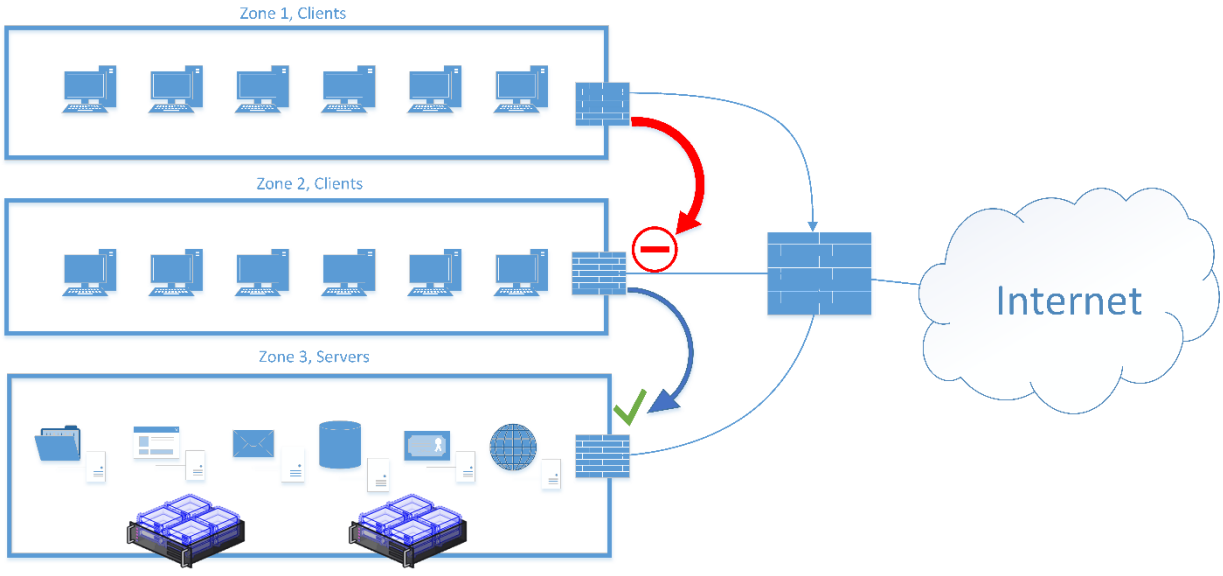

Figure 2. Network Segmentation

In highly critical networks, such as classified military networks, one of the most used security measures is to completely disconnect the network from all unsecured networks. These disconnected networks (Figure 3) are called isolated. (Petersen 2016)

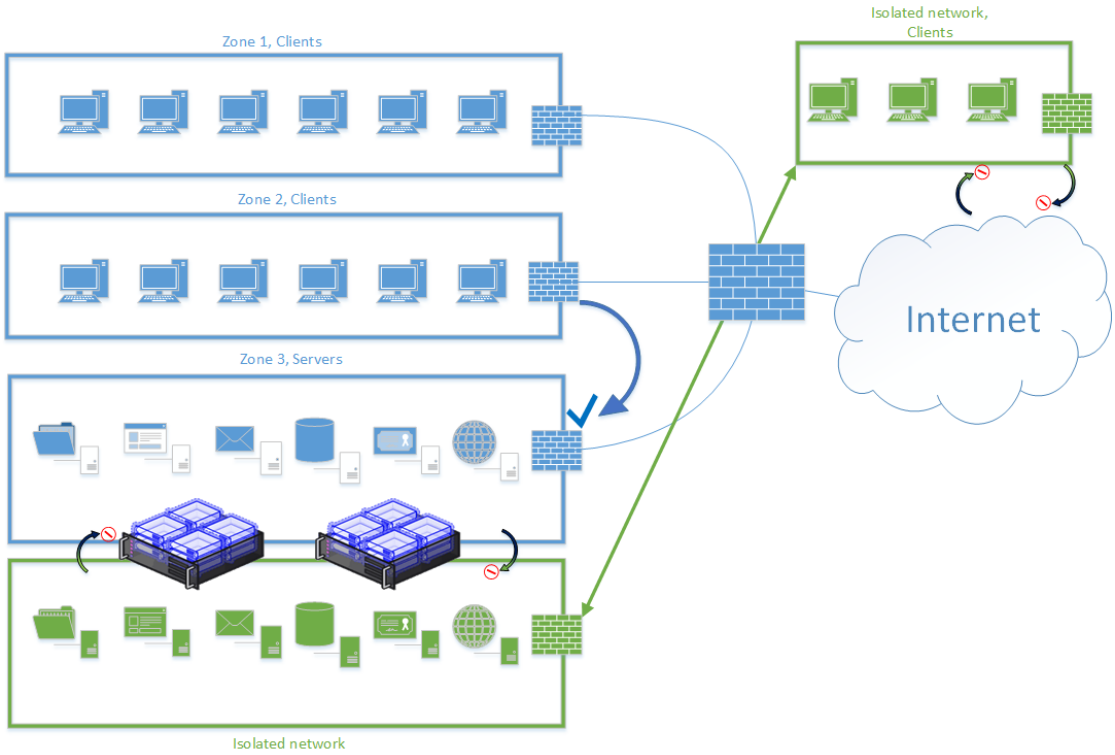

Figure 3. Isolated network

In isolated networks the separation is done on OSI layer 2. However, the network may consist of several different segments placed in separate physical locations. Isolated networks can use the same network devices and cabling with untrusted networks; however, in these cases, there are some additional requirements for the equipment and encryption.

The main difference between an isolated network and an air-gapped network is shown in Figure 4. In the air-gapped network all network devices, network cabling and end-user devices are physically separated from all untrusted networks. This separation can also be called an OSI 1 layer separation. By physically separating these networks it can be ensured that in a case of a hardware misconfiguration or a device security breach, there is no physical way the networks interconnect. (Herrero 2015)

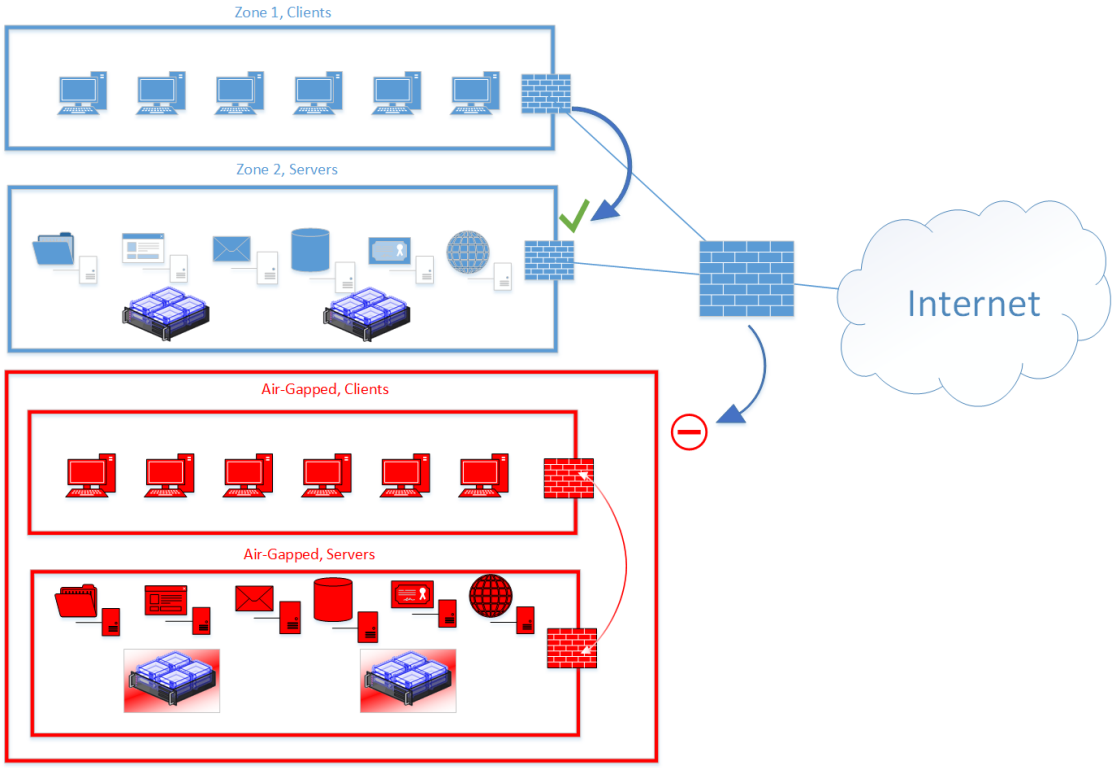

Figure 4. An air-gapped network

The practice of implementing a network isolation can be defined as security through obscurity because all information that the network holds can only be accessed within the network. All new information needs to be transferred to the isolated network manually. This can be done using portable media such as an optical media or a USB-drive. (Jones & Bowersox 2006)

This method of information transfer is also a well-known method to bypass the security that air-gapped networks provide. The most infamous example of this is the case of Stuxnet, where a USB drive was used for importing a crafted malware to an air-gapped network. The malware resulted in destruction of the centrifuges that Iran was using in their nuclear program. (Herrero 2015)

Even a perfectly implemented air-gapped installation has a vulnerability for an information breach using a side channel attack. This attack method utilizes some physical phenomena such as light, sound, vibrations or unintentional emissions of radio-frequency signals. Military standards such as TEMPEST exist to shield devices from these kinds of attacks. As TEMPEST is a classified NATO standard, there is only a very limited amount of public information available. FICORA has published a guide

for Finnish national requirements for electric emission. (Finnish Communications Regulatory Authority Instruction on EMR Protection 2013)

3.2 Data diodes and unidirectional network connections

Unidirectional network connection is a way to create a link between two networks where information is designed to only flow in one direction (Figure 5). The idea for a unidirectional network connection is not new. Some public research papers from the 1980s already refer to the subject and some publications claim that this technology has been used in high security networks already for decades. Typically, this type of a connection can be created by using data diodes or unidirectional security gateways. (Stevens & Pope 1995)

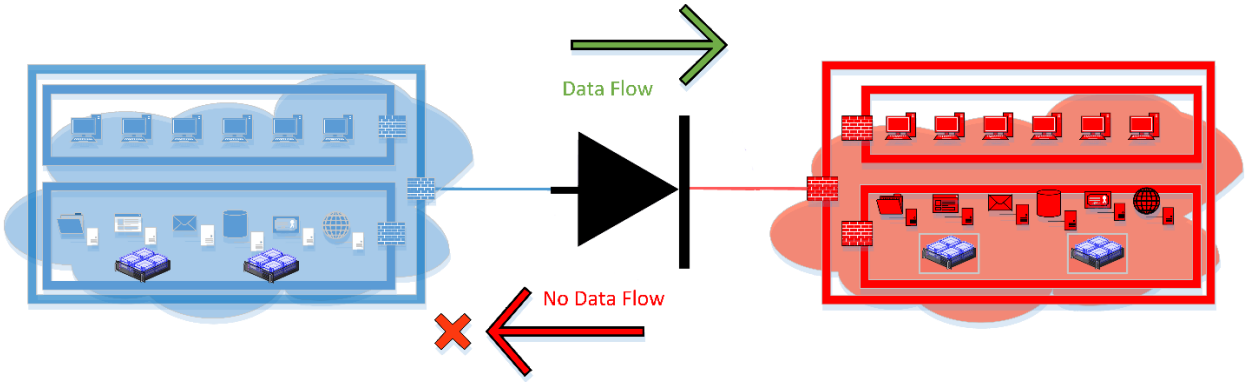

Figure 5. Unidirectional connection between two networks

3.2.1 Data Diode

The first implementations of data diodes were using physical connections with a modified RS-232 serial line. The problem with this design is that even if the transmitting wires and pins are removed from the high side in such a way that the low side can only transmit, it is still leaves the likelihood for the remaining wires to be used in a side channel attack in which case information ends up leaking from the high side. The risk of side channel attacks when using RS-232 serial lines led to the creation of optical data diodes. A U.S. patent for an optical method of a data diode implementation was issued in 1997. (Method for transferring data from an unsecured computer to a secured computer 1997)

The basic design of an optical data diode is very similar to fiber optical transmitters that use two fibers, one for transition and other for a reception. Unidirectional connection is achieved by removing one fiber connection and disabling all possible link failure identification mechanisms. Because Tx-port can only send information, it is impossible to establish a two-way connection between two networks. This type of a separation can be referred as OSI layer 1 one-way separation. (Stevens 1999)

As a data diode forces a connection to be unidirectional it also restricts the use of network transport protocols, such as TCP/IP that requires a two-way connection. There are protocols that require only a one-way connection, for example UDP, that is used for a unidirectional data transport. As UPD does not have a protocol level guarantee of message delivery when compared to TCP, a proxy server is typically implemented to both sides of a data diode. These proxy servers are responsible for acting as connection endpoints. They provide a reliable two-way connection that receives a data stream and transmits through a data diode. Proxy servers can also be used to validate and inspect information for malicious software, confidentiality and integrity. (ibid.)

3.2.2 Software unidirectional network connections

In a software unidirectional network solution the connection is established by using software rules that limit data to flow to one direction only. Depending on the manufacturer, the software may include firewalls and proxy servers or even be an all-in-one type of device.

Figure 6 demonstrates an example of a software unidirectional network solution that can be used for connecting low and high classification networks. This solution is based on using an exchange server between the two networks.

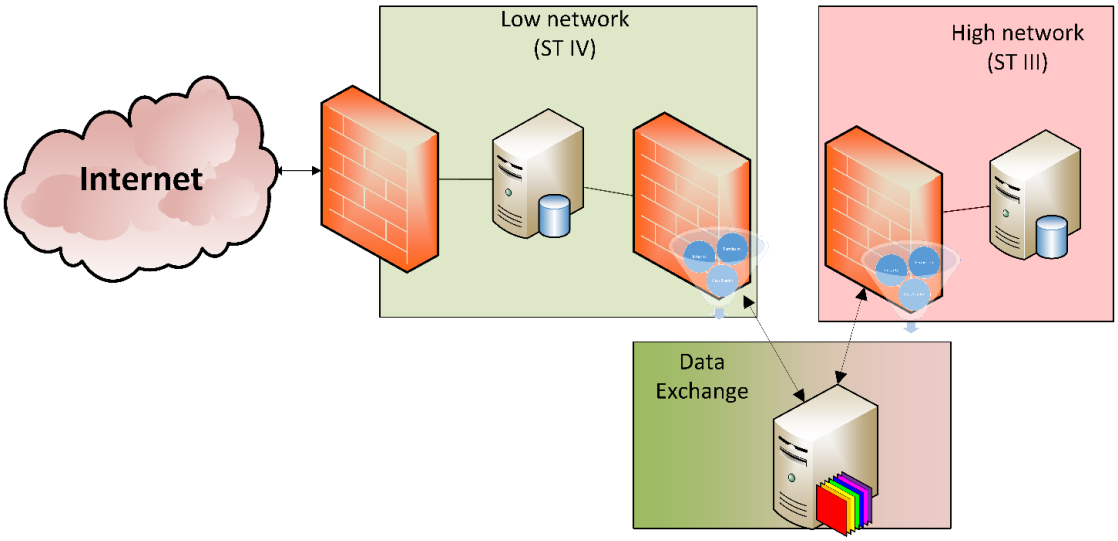

Figure 6. Software unidirectional network connections

When transmitting information from a low to a high classification network, data packets are first transmitted to an exchange server by a low classification server at a pre-defined time. Only a low classification network has access to an exchange server during this phase. A high classification server downloads a data packet from an exchange server in a pre-defined time thus completing the data packet transmission. The benefit of using this type of an implementation is that an exchange server allows the usage of standard devices and applications protocols. (Designing and Implementing Secure Gateway Solutions 2016)

4 Auditing criteria for case study

The research question for this thesis was: How to implement unidirectional patch management connection to an isolated network and what are the implementation requirements that were identified in the literature review? This chapter illustrates how a relationship between the requirements was found through the narrative analysis of the literature review (Figure 7) and how the auditing criteria were selected for the case study.

4.1 Relationship between the requirements

FICORA's guide, Guidance Interpretation of Criteria for Evaluation (2015), states that the main auditing criteria can be chosen either from VAHTI or KATAKRI. For this case study the KATARI 2015 (KATAKRI - Information security audit tool for authorities – 2015, 2016) was chosen as recommended by the FICORA guide.

KATAKRI 2015 section I1 states a specific requirement for security of a network architecture as follows:

> *The information processing environment has been separated from other respective environments" and "The connection of the information processing environment to the one(s) of another protection level requires the use of a boundary protection service approved by the competent authority for the respective level.* (ibid.)

The requirement has been presented with the following implementation example in KATAKRI 2015 section I1:

> *From protection level III onwards the connections to environments of different protection level may be done using gateway solutions approved by respective authorities. Design principles and general solution models for gateway solutions which may be approvable have been described in detail in Finnish Communications Regulatory Authority Guidelines for Gateway Solutions; "Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista"* (ibid.)

FICORA has given additional instructions for information security inspection bodies on how the requirements regarding security gateway solutions should be interpreted (Guide for accredited inspection bodies 2017, paragraph 5.4.3, subsection T8):

"In installations implemented way described in FICORA's Designing and Implementing Secure Gateway Solutions guide, installation need to be validate in corresponding the requirements stated in the guide are sufficiently implemented."

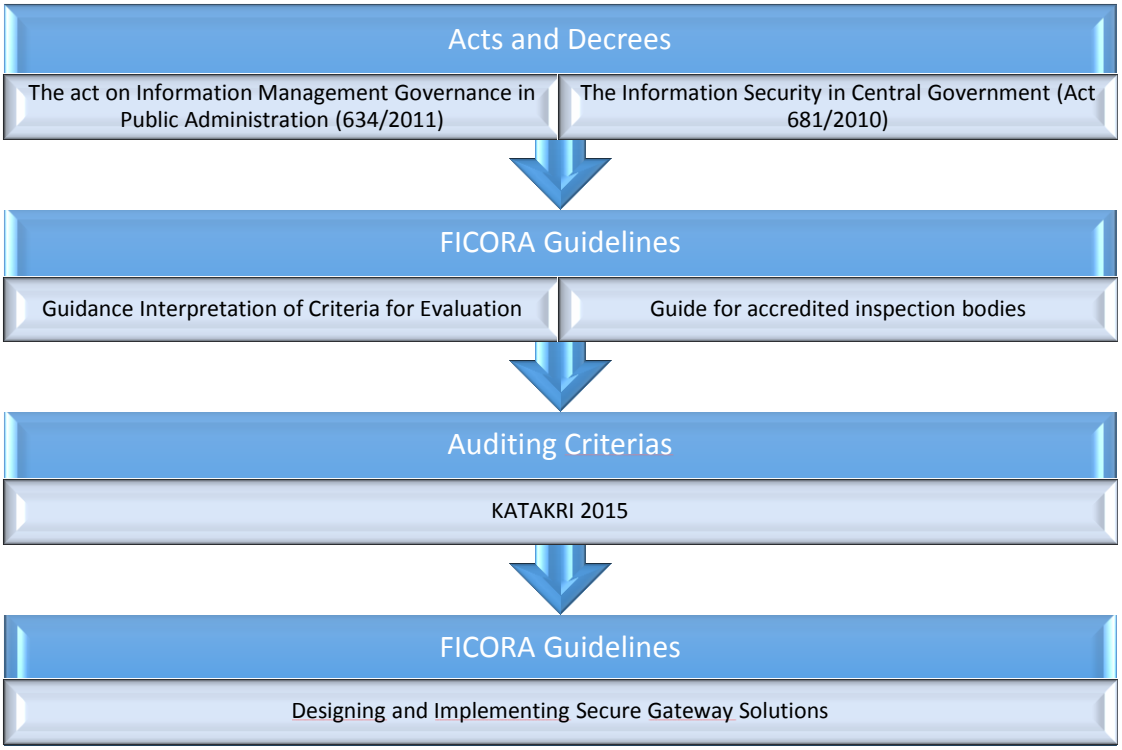

Figure 7. Auditing criteria for the case study

4.2 Secure gateway solutions' requirements for the case study

Designing and Implementing Secure Gateway Solutions (2016) describes the most common demands, examples and requirements for an acceptable gateway solution. The guide states that the general criteria for any security gateway solution is the need to implement the principles of Bell-LaPadula and the rules No-Read-Up and No-Write-Down. This means that a solution needs to prove in a reliable manner that classified information does not leak from a high classification to a lower classification network. The guide also includes examples of acceptable design solutions that rely on data diodes and software unidirectional network connections.

In addition, the guide states that the following solutions are generally expected to be taken into account in an approved design (ibid.):

- Defense in depth, fail security, fail-safe, minimum rights and minimizing vulnerability of surface design principles.

- Design needs to detect and defend risks to and from its operating environment.
- Implementing secure management and monitoring solutions.
- Typically core functionalities need to be implemented with hardened software and system solutions. Also, the security implementation design must be such that it can be reliably verified to be accurate.
- Checksums, signature validation and malware scanning are the minimum requirements.

4.3 Addressing the requirements for the case study

Security requirements identified in the Designing and Implementing Secure Gateway Solutions guide can be divided into two categories which are general criteria requirements a design needs to address and requirements that are expected to be taken into account.

General criteria requirements in the Designing and Implementing Secure Gateway Solutions guide state that both, security gateway and data diode designs are possible ways to implement a unidirectional connection to a CONFIDENTIAL (ST III) network when implementing the principles of Bell-LaPadula and the rules No-Read-Up and No-Write-Down. All approved design models require CONFIDENTIAL (ST III) network connections to originate only from RESTRICTED (ST IV) networks. Both networks need to be secured with the security classification levels presented above before implementing any interconnection.

A data diode solution was chosen for this case study because its high assurance that the connection in only unidirectional and its simple design can be easily inspected. Use of a data diode also addresses both, the thesis assigner's requirement and fail-safe requirements that unidirectional connection should, in any case, allow information to leak from a higher classification network to a lower classification network.

Designing and Implementing Secure Gateway Solutions guide does not offer detailed instructions on how the requirements that are expected to be taken into account should be implemented; it rather points to KATAKRI 2015 and VAHTI 3/2012 guides. As KATAKRI 2015 was chosen for the auditing criteria, the following KATAKRI requirements were identified to correspond the requirements stated in the Designing and Implementing Secure Gateway Solutions guide (KATAKRI - Information security audit tool for authorities, 2015, 2016):

I 01 - Secure interconnection of CIS

4) *The connection of the information processing environment to the one(s) of another protection level requires the use of a boundary protection service approved by the competent authority for the respective level*

I 02 - Secure interconnection of CIS

The segmenting of the communication network and the filtering rules has to be done following the principles of least privilege and defence-in-depth.

I 04 - Management connections

1) *Management connections have been segmented on the basis of the protection level, unless a gateway solution approved by the competent authority for the particular protection level is used.*

4) *Management connections have been limited according to the least privilege principle.*

I 08 - Principle of minimality and of least privilege

1) *Only the essential functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risks.*

2) *Organisation uses a procedure through which systems are installed and configured systematically, resulting on a hardened installation, following the configuration rules set by the organisation itself.*

3) *Configuration contains only such components, services, user and process rights which are mandatory in order to fulfil the operational as well as the security requirements*

I 09 - Protection against malware

Reliable methods for deterrence, prevention, detection, resilience and recovery measures of malware are used in the information processing environment in order to prevent unauthorised changes and other unauthorised use of the information

I 10 - Defence-in-depth - Traceability of security events

In order to detect unauthorised changes or other unauthorised or inappropriate information handling within the information processing environment, reliable methods have been taken into use for tracing the security events

I 11 - Incident detection and recovery

Reliable methods are taken into use in the information processing environment in order to detect attacks against the information processing environment, to limit the effect to a minimum amount of the information and to minimum resources of the information processing environment and to prevent other damages, as well as to restore the protected status within the information processing environment

5 How the case study was conducted

The case study was conducted in a Proof of Concept (POC) environment to implement and verify the proposed solutions for a unidirectional network connection. The decision to use a POC environment allows a quick implementation and design changes that would not be possible in an actual classified environment. The use of a POC environment also hinders the implementation possibilities when the surrounding environment does not have services that an operational network would have to offer as a network-wide as a centralized service, e.g centralized log management.

As the case study is conducted in a POC environment, some additional requirements were given by the thesis assigner:

- The patch management files that need to be transferred to a simulated isolated network are Windows 10, Windows Server 2016 and Centos 7.
- Isolated networks' security classification should be considered as confidential (ST III) in minimum.
- Implementation solution should not, in any case, allow information to leak from the higher classification network to a lower classification network.

The design of the POC environment consists of two physical proxy servers, an optical data diode device and two patch management servers, as shown in Figure 8. These patch management servers WSUS and Centos are used to download and verify the Windows and Linux patch management files. After a successful download and file verification, the files are moved to a proxy server for an additional content verification and transport. After unidirectional transportation through the data diode, the high side proxy server validates the patch management files one more time to ensure they correspond to the designed patch management files.

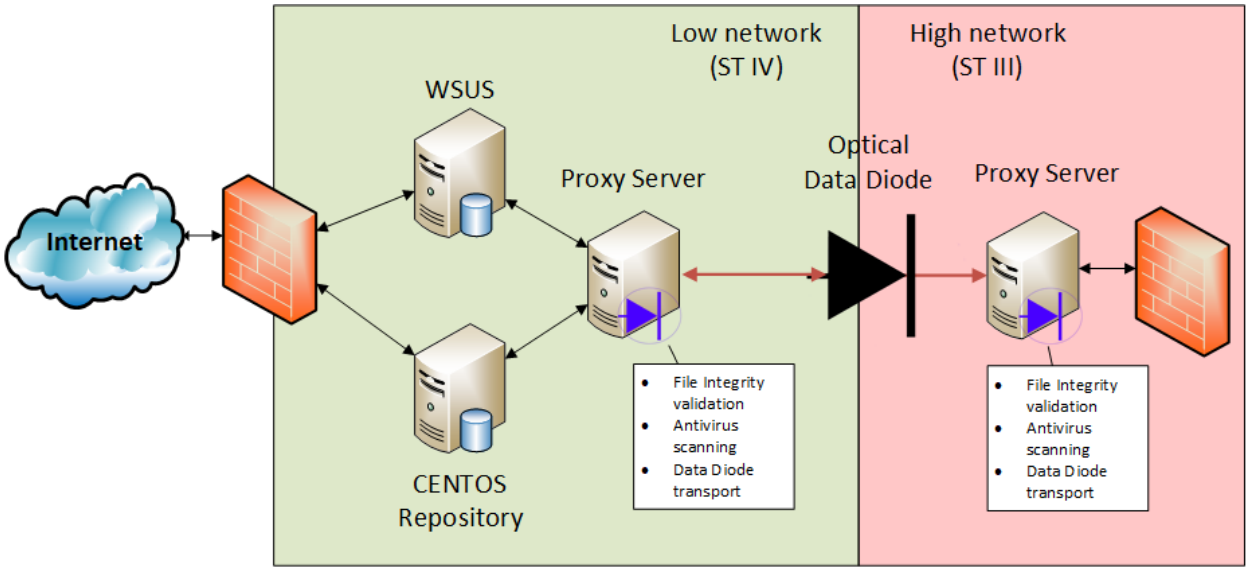

Figure 8. Proof of Concept environment design

In the Proof of Concept environment design the low networks' patch management and proxy servers are segmented with a firewall from the rest of the network as defense in depth measure. This segment would be part of the RESTRICTED (ST IV) networks that utilize network services, for example centralized log management. All the management connections would be restricted into to the segment. The patch management server would be allowed to connect to Microsoft and Centos patch management web addresses with HTTP and HTTPS connections.

The high networks proxy servers would also be segmented with a firewall that allows only a necessary connection. This segment would utilize network wide services in monitoring. The proxy server management would be limited into the segment, for example through physical management.

5.1 Windows Server Update Services (WSUS)

In the POC environment the low networks' internet connected WSUS server is configured to synchronize patch management updates for Windows 10 LTSB and Windows Server 2016 products with Critical Updates, Definition Updates and Security Updates classifications.

The WSUS service uses an HTTPS secured connection by default to obtain information about the available updates and retrieves the metadata regarding each update. This metadata includes all the information and the installation commands

regarding each update packet. The update packet itself is downloaded with a non-secured connection and after the download each update file is verified by using SHA-1 and SHA-256 digital signature information that was included in the metadata of the updates. (Windows Update Services: Client-Server Protocol 2017)

The patch management information is exported by copying first the WSUS content folder to the proxy server, then by exporting the metadata to a single cab file with WSUS tool wsusutil.exe and finally by transferring the single cab file to the proxy server.

5.2 Centos Repository

For the POC installation the Centos 7 Linux was chosen for a distribution to implement the repository mirroring. Yum packet manager, released by the CentOS project, offers by default a function that is used to verify the packages' integrity. The packet verification is done by comparing the GPG signatures of each package to the GPG keys released by the CentOS projects.

The Centos RPM packages for a base, extras and updates were downloaded as a local copy with a yum utility reposync that verifies the GPG signature of each package. The downloaded packages were then transferred to the proxy server.

5.3 Proxy servers and an optical data diode

An optical data diode was chosen for the implementation because the connection is highly assured to be unidirectional. The chosen data diode for the POC is Fox-IT 1 Gbps Data Diode – Government Edition that guarantees the connection is solely unidirectional. This data diode solution has received a classification of "*up to and including NATO SECRET, Green Scheme*" (Fox DataDiode EAL 7+ 1Gbps 2015)

The Fox-IT optical data diode is a hardware device that does not include any management console or software to configure the device; rather the device only provides a guaranteed function of unidirectional transport. All the management and configuration regarding reliability and integrity of the connection is done with Fox

DataDiode Core software that is installed to both servers. (DataDiode By Fox-IT 2018).

Data is sent through the data diode device which is controlled by the Fox DataDiode Core software that adds extra metadata to the transport stream in order to provide an additional mechanism to the high side proxy server so it can detect if any of the packets were lost during the transport. The software also includes forward error correction functionalities that can be used to help in reconstructing failed packets. More detailed information regarding these reliability and integrity settings are only available in documents that are provided to customers and are heavily restricted by copyright. (DataDiode By Fox-IT 2018)

For the POC Fox DataDiode Core software's folder and file transfer feature was chosen as the implementation option because it offers a solution to transport files and folders from pre-defined folders from the low side to the high side. As options and other features were very limited, the software was only used for providing a transport function between the networks.

Figure 9 shows how the data diode hardware and proxy servers were installed in the POC environment. The proxy servers are connected to the data diode with 1000BaseSX optic fiber network cards. The connection from the low side was done with two fibers connected as a normal two-way connection to the data diode. The high side proxy server is connected only with one fiber as the server can only receive information.

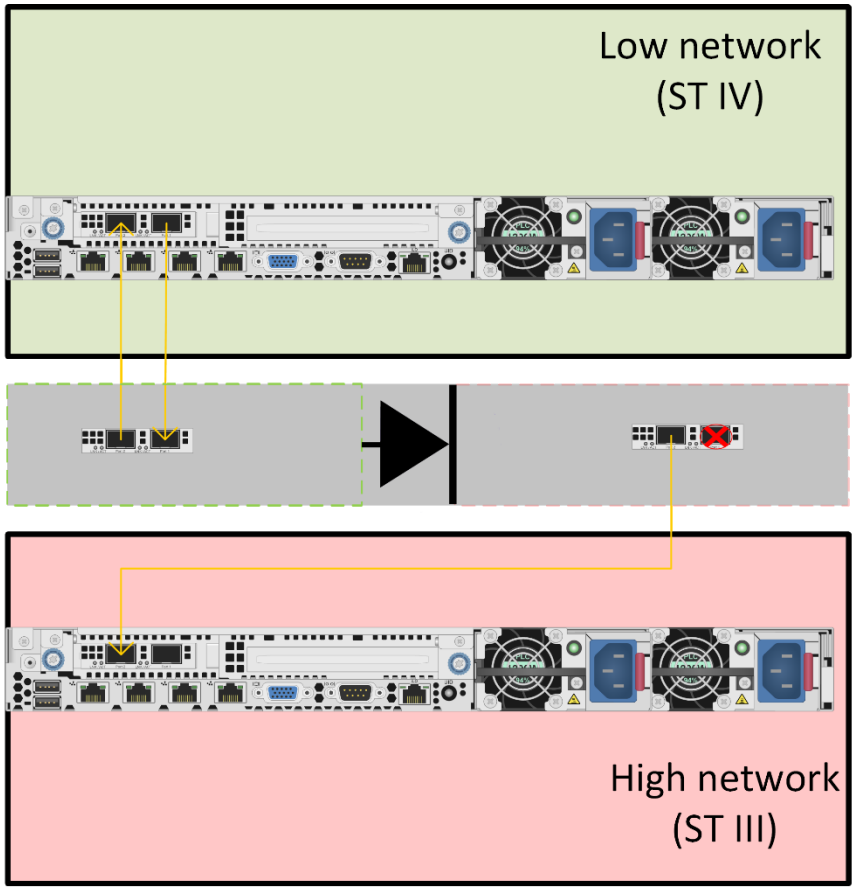

Figure 9. POC data diode installation

During the initial POC setup both Centos and Windows server operating systems were used in the proxy servers. There were some initial setup problems with the Fox DataDiode Core software when initiating the connection through the data diode. The graphical configuration interface for managing the connection was only available for Windows operating systems. For this reason, the Windows Server 2016 operating system was selected to be used as the proxy server operating system to decrease the complexity of the POC design.

5.4 Content validation

In the Designing and Implementing Secure Gateway Solutions (2016) document it is stated that checksums and signature validation as well malware scanning are required for the files that will be transported. In the POC environment an initial content validation is done during the patch download process where the downloaded file is verified to have a valid digital signature. F-Secure Security Server Premium is installed on both of the patch management servers to provide a real-time

antivirus scanning functionality. This initial content validation is only meant to be an initial process that detects all possible errors in the patch management packets as well as possible targeted attacks.

In the POC environment design the content is validated by the proxy servers on both sides of the data diode connection to confirm that only the desired patch management files are transferred. Three different content validation processes were developed to this end. The processes are shown in Figure 10 illustrating how the validation is done during the transfer.

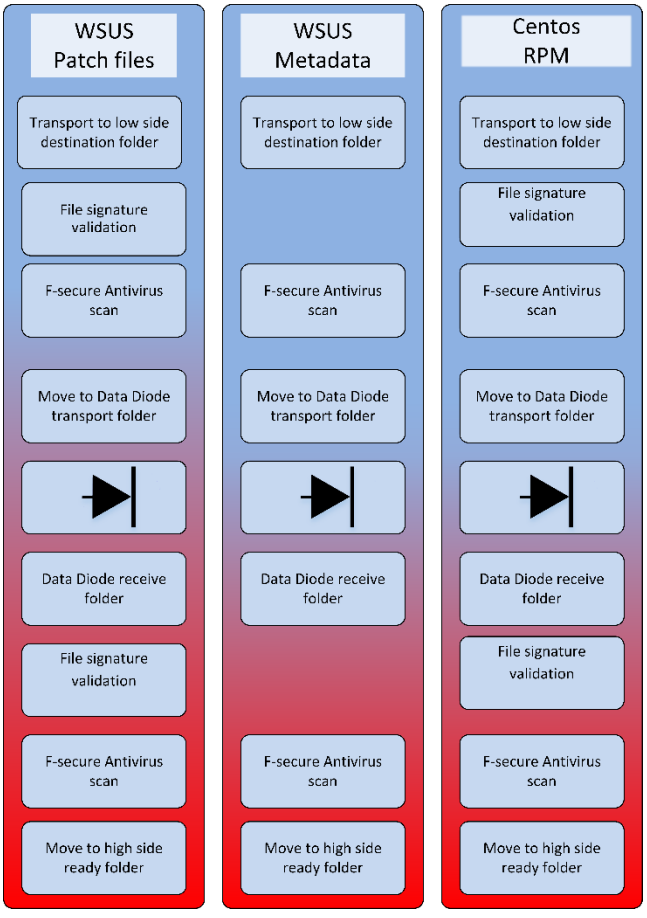

Figure 10 Proxy server content validation

WSUS patch management files

As shown in Appendix 1, a PowerShell script was developed for the validation process. PowerShell was chosen because it is prebuilt in Windows operating systems

and does not require any additional software components that would require approval in classification.

WSUS metadata

The initial design was meant to include a digital signature validation to all transported files as required. However, this was not possible to implement because the exported Windows Server Update Services (WSUS) metadata does not include any digital signature that could be validated. For this reason, the WSUS metadata only includes the F-Secure antivirus scanning.

Centos RPM

The Centos RPM file validation was done by comparing the known Centos 7 GPG signing key and the GPG signature in the RPM packages. The initial design was to utilize the GnuPG client which is available also for Windows platforms. This initial implementation design was not feasible, as the GPG signature could not be read by the GnuPG client inside the RPM packet.

The RPM file validation was implemented by using the Linux Subsystem for Windows (WSL) feature that enables the use of Linux distribution command lines and features such as RPM Package Manager (RPM). For the proxy servers, WSL was installed with Ubuntu LTS Linux Distribution. Appendix 2 shows the RPM verification bash scripts that were used for verifying the RPM packages by comparing them against the imported Centos 7 GPG key.

5.5 Scope of POC implementation

As the thesis assigner's requirements focus on unidirectional connection requirements and its auditing criteria, issues regarding KATAKRI 2015 requirements regarding organization's security management and physical security were excluded from the case study.

The implementation of the segmentation firewall and the related firewall rules could not be completed in the POC environment as there were availability problems in the firewall devices. POC environment was air gapped from any operational network to its own environment during the testing.

6 Test results of case study

The Proof of Concept environment presented in this thesis was used to test the functionality of the developed design and to identify potential issues. The test was conducted in the POC environment with Windows and Centos patch management information that was defined by the thesis assigner. An optical data diode was selected as the implementation solution to further explore what limitations might be found when using a data diode product. The implementation of a functional model of a unidirectional connection between two separated networks with content validation was a success in the POC environment.

During the implementation a limitation was found. The Fox DataDiode Core software's file and folder transport function should have been regarded as a folder mirroring process from the low to the high proxy server. This mirroring function is an outgoing process by the software, and it cannot be controlled by for example with command line in order to determine when or what folders should be transported. This can cause problems when large amounts of files are being copied to a mirroring folder and the mirroring starts before all content has been copied to the folder. This challenge was solved in the POC environment with a separate drive storage in the proxy server, where all content validation can be done. After a successful validation the content can be without any delays moved to the data diode transport folder as it is located in the same storage volume.

6.1 Comparing the requirements to the POC implementation

In chapter 4.3 the key requirements for the POC environment were identified with the KATAKRI 2015 that was used to interpret the requirements stated in the Designing and Implementing Secure Gateway Solutions guide. These requirements can be used to determine how the POC implementation compares to the necessary requirements.

6.1.1 KATAKRI 2015 I 01 - Secure interconnection of CIS

The Designing and Implementing Secure Gateway Solutions guide does not state what kind of an approval a data diode device would require. The KATAKRI I 01

requirement, however, states that the boundary protection service needs to be approved by a competent authority for the respective level.

During the literature review a press release from Advenica AB was found stating that

> *Advenica's SecuriCDS DD1000i Data Diode receives approval from FICORA(Finnish Communications Regulatory Authority) which can be used for data transfer between networks of different security levels up to the level of SALAINEN/SECRET* (Advenica Press Release 2016-04-14, 2016)

This approval was not found in FICORA's publications, rather there was a mention found in Guide for accredited inspection bodies (2017, 50) explaining that there are some data diode devices that have been approved with a special approval usage policy. More detailed information regarding approved data diode devices was not found in FICORA's publications.

However, FOX-IT data diode device does not have any known approval from The Finnish Communications Regulatory Authority (FICORA) according to the information published by the vendor. Therefore, the Fox-IT data diode solution cannot be used as an approved Secure Gateway Solution in a Finnish classified network.

6.1.2 I 02 - Secure interconnection of CIS and I 04 – Management connections

Use of an optical data diode implements a physical network rule that prevents all network connections from the CONFIDENTIAL (ST III) network to RESTRICTED (ST IV). As the data diode device itself does not have any management possibilities, all management connections are contained only to a particular network segment.

Carrying out a network segmentation allows a simple way to implement a policy that grants only the needed connection protocols, sources and ports to be used. The segmentation also allows a single point of network monitoring.

6.1.3 I 08 - Principle of minimality and of least privilege

The KATAKRI 2015 chapter I 08 presents implementation examples that include multiple security requirements for servers, workstations and equivalent devices. It is stated that following the procedure, the requirements for protection level RESTRICTED (ST IV) can be fulfilled. For the protection levels CONFIDENTIAL (ST III) and SECRET (ST II), additional implementation procedures are required.

The design of the POC environment took into account the need for minimizing the vulnerability of surface by separating all the different roles to dedicated servers. These servers were then configured to have only the necessary services and the security was hardened to allow only minimal functionality and rights.

To simulate these security requirements, Windows systems were hardened with the Microsoft Security Compliance Toolkit to provide a baseline for a security. With Centos server the Security-Enhanced Linux (SElinux) security access control was enabled and configured

In the Proof of Concept implementation the RPM file content validation was done with Windows subsystem for Linux (WSL) that has an installation requirement for Windows server 1709 or any later version of it. During the time of POC implementation the Long-Term Servicing Channel (LTSC) versions of Windows server were 1607. The presented implementation design would not be possible to conduct in an environment that are using the LTSC Windows servers. In addition it is to be noted that at the time when POC implementation was executed, Microsoft's security hardening guides did not include any security rules for WSL hardening when using Windows server 2016.

6.1.4 I 09 - Protection against malware

Designing and Implementing Secure Gateway Solutions guide chapter 4.1.1 describes what is expected from an approved data diode model. One of the requirements is that there needs to be an integrity check procedure in place. This requirement is then further explained in an example: in a patch management situation, integrity check procedure includes a validation of checksums, digital signatures and antivirus scanning of the transported files.

KATAKRI 2015 chapter I09 implementation example describes that if malware fingerprints are imported to a disconnected network manually or with approved security gateway solution, there needs to be a process for validating the integrity of the updates that by *"(source, checksums, signatures etc.)*" (KATAKRI - Information security audit tool for authorities 2015, 2016).

In the POC implementation, a content validation consisted of antivirus scanning and digital signature validation. The implemented F-Secure antivirus protection was tested with EICAR standard antivirus test file to determine the functionality of the F-Secure scanning and the validation process (EICAR Antivirus Test File 2006).

The update packet signature validation functionality was tested with digitally signed Microsoft and Centos file update packets and packets with invalid signatures. The test packets were then modified which caused them to lose signing integrity. The signature validation was also tested with packages that were signed by a third party signature but not with a valid Microsoft or Centos digital signature. In the signature validation test only valid Microsoft or Centos signed packages were proved to be able to pass the validation process.

It became clear that PowerShell has some limitations; in cases where files are dual signed with SHA-1 and SHA-256 signatures, the signature validation command Get-AuthenticodeSignature only validates the first digital signature it finds. In the case of Windows patch management files, it is the SHA 1 signature. Microsoft has stated about the SHA-1 the following:

> *"Microsoft intends to distrust SHA-1 throughout Windows in all contexts. Microsoft is closely monitoring the latest research on the feasibility of SHA-1 attacks and will use this to determine complete deprecation timelines."* (Cloutier 2017)

Signature validation was not implemented for the WSUS metadata CAB file because it does not have a digital signature by default when it is exported. It would be possible to add a separate signing task in the POC implementation to digitally sign the exported CAB file, for example with a server's certificate. This would enable proxy servers to do a signature validation. This signature could also be used as an

integrity checksum. The problem with validating the WSUS metadata will be presented in chapter 6.1.6

6.1.5 I 10 - Defence-in-depth - Traceability of security events

KATAKRI 2015 paragraphs I 10 (KATAKRI - Information security audit tool for authorities 2015, 2016) implementation examples state that a centralized log management service would be a recommended implementation method for collecting log information from all network and server devices.

In the POC implementation, a content validation process was designed to provide log information about a successful and unsuccessful validation of a digital signature or antivirus scan on the proxy server. This log information could then be transferred to, for example, the network's centralized log management, in order to provide a monitoring capability of that network's part of the security gateway solution. To prevent the use of log data as a possible side channel attack the low and high networks would need a separate centralized log management servers. Because of the scope of this thesis and limitation of the POC environment's server hardware, a centralized log management servers were not installed to the POC environment.

The Fox DataDiode Core software logs its operations using proxy server's Windows event log service. The log information includes information regarding the software's state and transferred files. Each successfully transported file is logged with a transport identifier number and with the file's full path including its filename in both of the proxy servers. During the POC implementation testing it was detected that in cases where transport failed, the high side proxy server only logged an error message that informed about a possible data loss without any file information so it was impossible to know which files were lost. In cases where possible data loss has occurred, the comparison between the proxy servers log information is the only way to identify what files have been lost.

6.1.6 Issues with WSUS metadata validation

There has been some security research done on the use of the WSUS service as an attack vector compromising a corporate network. In the Black Hat USA 2015 security conference Alex Chapman and Paul Stone (Chapman & Stone 2015) released a WSUSpect open-source tool that can be used as a man-in-the-middle (MITM) attack between WSUS server and its client. The attack utilizes a known issue: during an installation of a WSUS server, there is no requirement to implement SSL/TLS protection between the servers and clients to complete the installation.

In this attack, the connection of a WSUS server and its client could be intercepted by the MITM attacker. As the WSUS metadata had not been signed, the attacker could modify metadata for updates or replace an update file to another executable file that has a Microsoft digital signature e.g. Sysinternals PsExec. Then the WSUS client would run the attacker's modified metadata and file with system privileges as an update package.

The WSUSpect attack has limitations on implementation as it requires a WSUS server installation that uses a non-secure connection with a network where a man-in-the-middle can be executed. In cases where one of the attack requirements has been blocked, the attack will not be successful.

In 2017 Romain Coltel and Yves Le Provost presented a new WSUS attack and a tool WSUSpendu that utilizes a WSUS server as an attack vector to compromise clients and any network that utilizes its patch management information. WSUSpendu utilizes the same metadata weakness as WSUSpect but it is designed to be used on a WSUS server that an attacker has already compromised. With this tool the attacker could modify the WSUS server's metadata database in order to inject a malicious update that would get automatically approved for all the clients of that server. As the attack is part of the WSUS server's metadata and update files, it will affect all other WSUS servers that synchronize patch management information from the infected WSUS server.

There are few limitations with implementing a WSUSpendu attack. Firstly, the Windows server that is running the WSUS service should have been compromised by the attacker before implementing the attack. Secondly, if the patch management

data from the compromised server is used by another WSUS server, the malicious update needs to be approved manually by an administrator of that server or by an automatic approval rule set. A default installation of a WSUS service includes default approval settings that automatically approves new updates if they are for the WSUS service itself or new update revisions of a precisely approved update.

The WSUSpendu attack tool was tested in the POC environment's low network WSUS server. The tool was able to successfully inject a malicious update that included a command to run a PsExec management utility that is digitally signed by Microsoft. As the PSExec is an EXE file digitally signed by Microsoft, and F-secure's antivirus software does not regard it as malicious, it passed the content validation.

As the WSUSpendu attack tool was released during the time this thesis was written, the content validation design did not include any countermeasures to this attack. As the POC environment scope was set to synchronize patch management updates for Windows 10 and Windows Server 2016 products, it would be possible to implement a content validation step that would block all EXE files from the transfer. This would be possible because Microsoft releases updates as CAB files for these products. This mitigation would not remove the malicious attack command from the WSUS metadata but would prevent a command running the executable.

Microsoft releases some patch management updates as executable files, in this case, a content validation process would need to include more detailed inspection of EXE files than just a simple block. One solution would be to include more detailed verification for EXE files' digitally signed information that identifies patch management files from the digital signature and the files product name.

7 Comparison of case study to a known implementation

As stated in the Designing and Implementing Secure Gateway Solutions guide, it describes generally expected requirements and example models for the implementation of a security gateway. The Finnish Communications Regulatory Authority (FICORA) would be the competent authority organization to evaluate the POC implementation compared to the requirements. The accreditation process for the POC implementation by FICORA would not be possible to conduct because there was no implementation of the organization's security management and physical security in the case study. In order to assess the success of the case study it was compared to the information released by FICORA of a successful implementation of security gateway solutions.

The Guidance Interpretation of Criteria for accredited inspection bodies documents Annex 2 (2017, 49-50) includes an example of a report that an organization would receive from FICORA after an accreditation inspection. This example report has been added as an Appendix 3. Typically, any implementation of a security gateway solution would be implemented between two critical or classified networks. The information regarding these interconnections and its accreditation would be in most cases classified by the Act on the Openness of Government Activities (621 /1999).

The example report is presumably a redacted version of an actual accreditation inspection report for an organization. The report only includes a general description, an auditing test and the results for KATAKRI 2015 I 01 - Secure interconnection of CIS requirements. As the report includes use case scenarios, the auditing tests and results that are not redacted can be used as a technical requirement reference model to the case study implementation.

7.1 Organization O's solution

The example report presented in the previous paragraphs describes an Organization O that has successfully implemented a security gateway solution. The implementation model is the same as the one introduced in Designing and Implementing Secure Gateway Solutions guide, chapter 4.1.1. From this it can be

assumed that the unidirectional connection is between two different protection levels. As the report does not explain what the protection levels are they will be referred as low and high.

Organization O uses a data diode model that has been granted a special approval by FICORA. This special approval includes use policy requirements that are not explained in the report.

What can be detected from the report is that the security gateway solution is at least used to transport Windows and Ubuntu patch management files automatically. The files are transferred to the security gateway solution from a low networks' System Center Configuration Manager (SCCM) server and Ubuntu's patch management server. The automation process includes content validation where files are antivirus scanned and file integrities are validated. This content validation is done both in the low and high networks.

7.2 Organization O's technical inspection

What can be detected from Organizations O's report is that the following technical inspections were conducted by an accredited inspection body or FICORA:

- The configuration of low and high proxy servers was inspected. Servers' ports and vulnerabilities were scanned externally and internally
- Data diode device was inspected to correspond with a device type that has a special approval by FICORA. It was also investigated that the data diode device use policy requirements were correctly implemented
- Network connections and device installations were verified to correspond with the documentation. Network traffic was recorded for a certain period of time and analyzed.
- Management process of a security gateway solution was inspected by utilizing existing documentation and data diode logs and by interviewing and monitoring personnel.

For the content validation, the following inspections were conducted:

- Low networks SCCM and configuration of Ubuntu's patch management servers were inspected.
- Configuration of an antivirus product was investigated
- Functionality of content validation was tested with EICAR Antivirus Test File and Microsoft update files with invalid integrity.

7.3 Comparing Organization O to POC implementation

Organization O and the POC implementation have the same function of being unidirectional patch management solutions. Both implementations utilize a data diode solution in order to ensure a unidirectional connection and have content validation in proxy servers. Organization O's implementation of a data diode model received a special approval by FICORA, which is missing from the POC environment's Fox-IT data diode device.

In both implementations, the content validation includes antivirus scanning and file integrity validation. More detailed comparison in the content validation process cannot be done as there is not enough information included in Organization O's report. The content validation testing was implemented in the same way in both implementations.

The main difference between these two implementation designs is the segmentation of the patch management servers. What can be deduced from Organization O's report is that the patch management servers are presumably part of the organization O's low network management. Comparing to the case study POC environment design the patch management servers were segmented from the low network and they only downloaded the patch management information.

8 Conclusions

The goal of this thesis was to research and develop a unidirectional patch management solution that would meet the requirements identified in the literature review. The decision to use a case study as a research method was in in my opinion the right choice as the limitations that would have been difficult to identify by other means. The limitation of using a non-approved data diode device was taken into account by the thesis assigner right at the beginning of the case study.

The POC implementation successfully demonstrated the requirements that would be required from a unidirectional security gateway solution implementation. The results were then compared to other existing findings of Organization O's successful implementation of unidirectional security gateways.

Designing the operating system security hardening would have required more detailed information that could have been compared to the requirements, case study and earlier findings from a successful implementation. The content validation process was a success; however, it showed the limitations with PowerShell signature validation and Windows' subsystem for Linux hardening. The implementation options demonstrated in the POC environment might not be feasible in some classified networks due to the use of different versions or operating systems.

It is difficult to conclude whether all the identified requirements have been interpreted and implemented exactly the way a competent authority would require to approve a solution. The KATAKRI 2015 implementation examples can only be regarded as a de facto way of implementation which can in some cases achieve the required level of fulfillment. However, this means that even if an organization has interpreted the KATAKRI's requirements to the fullest, it may not lead to an approvable result. Furthermore, in an actual accreditation inspection the environment is checked as a whole, meaning that an organization's security management and physical security have an effect on technical requirements, whereas the technical implementation affects the organization's security management and physical security.

Manual patch management transfer

Information systems are designed to be updated with security patches and newer versions of a product. In the case of Windows and Linux, the product versions are supported by the vendor with feature and security updates in their lifespan. If one does not apply security updates, it may compromise the system to an attack. Network isolation or even air-gapping an information system achieve some information security, as the network is harder to reach by an attacker, however, this does not prevent all attempts as shown in attacks like Stuxnet.

As an example, in an internet connected Windows network a release of updates can be managed by synchronizing the WSUS with Microsoft's servers. In an isolated network each new update release that needs to be deployed results in a WSUS export from an internet connected network and import to isolated WSUS servers. Each export and import requires a human resource to manually transfer updates if there is no security gateway solution.

In most cases, a manual transport would require an external storage device to transfer information from an internet connected network to an isolated network. To avoid all potential information leakages from an isolated network, an external storage device needs to be erased in a reliable manner each time it is used.

Patch update information that is exported to an external storage should be inspected with a content validation and antivirus software. This can be done as recommended in KATAKRI I8 (2015) implementation example with an isolated inspection system, in which the patch management information is transferred to a different external storage as recommended. This different external storage is then used to transport patch management information to an isolated network.

When implemented ideally, the patch management transport that uses external storages can be unidirectional and secure, unless there are human errors or neglects during the transport process. The requirements and difficulties in content validation are the same as in a security gateway solution. The implementations needs to validate that only the packages that have their integrity intact and are the desirable patch management information are allowed to be transported.

As there is a risk that even the trusted internet connected classified information systems, e.g. Ministry of Foreign Affairs have a possibility be infected by foreign actors, the release of attacks like WSUSpendu introduce new risks. If the organization transports the patch management information to other networks, there is a possibility for infection of high protection level networks through the initial, compromised WSUS server.

9 Discussion

Before this thesis, I had previous knowledge that there are different requirements stated for a government entity in KATAKRI and VAHTI, however, there was very limited knowledge about the acts that govern these requirements.

During the literature review, it was surprising to find out how complex the relations are with the requirements and guidelines that describe how the requirements should be interpreted. It is not enough just to follow the requirements, but one also needs to verify how they are interpreted. For example, FICORA has instructed in the Guide for Accredited Inspection Bodies how to implement the requirements stated in VAHTI Information Security Assessment Guide. This information was only available in the FICORA's publications.

It can also be noticed that VAHTI Information Security Assessment Guide (VAHTI 2/2014, 2014) refers to the ten basic level requirements stated in the act 681/2010 in an incorrect way. The correct requirements are in the section 5§; however, the VAHTI guide states them in 4§. This same mistake was found in FICORA’s Guidance Interpretation of Criteria for Evaluation guide and Guidance Interpretation of Criteria for Accredited Inspection Bodies as they both include a citation. When I noticed these errors, I contacted FICORA and explained the situation. The error was corrected to the new version of The Guidance Interpretation of Criteria for Accredited Inspection Bodies. However, the error still remains in VAHTI document and it is highly unlikely to be fixed because these rarely are updated.

References

Act 1030/1999. Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta [The Finnish act Decree on the Openness of Government Activities and on Good Practice]. Accessed on 8.12.2017. Retrieved from https://www.finlex.fi/fi/laki/ajantasa/1999/19991030

Act 681/2010, Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa [The Information Security in Central Government]. Accessed on 8.12.2017. Retrieved from https://www.finlex.fi/fi/laki/alkup/2010/20100681

Act 634/2011. Laki julkisen hallinnon tietohallinnon ohjauksesta [The act on Information Management Governance in Public Administration]. Accessed on 8.12.2017. Retrieved from https://www.finlex.fi/fi/laki/alkup/2011/20110634

Act 1406/2011. Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista [The Act on the Evaluation of Government Information Systems and Data Transfer Arrangements]. Accessed on 10.12.2017. Retrieved from https://www.finlex.fi/fi/laki/alkup/2011/20111406

Advenica Press Release 2016-04-14 - Advenica SecuriCDS Data Diode approved for SALAINEN/SECRET level by Finnish authorities. 2016. Accessed 5.1.2018. Retrieved from Advenica AB. https://advenica.com/en/news/2016-04-14/securicds-data-diode-approved-finnish-authorities

Anderson R. 2008. Security Engineering, A Guide to Building Dependable Distributed Systems, Second Edition. Wiley Publishing Inc. Accessed on 6.1.2018.

Assessing Security Vulnerabilities and Applying Patches. 2018. Australian Cyber Security Centre. Accessed on 22.1.2018. Retrieved from https://www.asd.gov.au/publications/protect/Assessing_Security_Vulnerabilities_and_Applying_Patches.pdf

Chapman, A. & Stone, P. 2015. WSUSpect - Compromising the Windows Enterprise via Windows Update. Contextis. Accessed 4.2.2018. Retrieved from https://info.contextis.com/acton/attachment/24535/f-0252/1/-/-/-/-/WSUSpect%20-

%20Compromising%20the%20Windows%20Enterprise%20via%20Windows%20Update.pdf

Configure a Disconnected Network to Receive Updates. 2016. Microsoft Docs. Accessed on 2.2.2018. Retrieved from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd939873(v=ws.10),2.2.2018)

Coltel R., Le Provost Y. 2017. WSUSpendu. Accessed 17.2.2018. Retrieved from https://www.blackhat.com/docs/us-17/wednesday/us-17-Coltel-WSUSpendu-Use-WSUS-To-Hang-Its-Clients-wp.pdf

DataDiode By Fox-IT. 2018. Accessed on 11.6.2018. Retrieved from https://www.fox-it.com/datadiode/faq/

EICAR Antivirus Test File. 2006. Accessed 18.7.2018. Retrieved from http://www.eicar.org/anti_virus_test_file.htm

Finnish Communications Regulatory Authority Instruction on EMR Protection [Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet]. 2013. FICORA. Accessed on 5.1.2018. Retrieved from https://www.viestintavirasto.fi/attachments/Kansallinen_TEMPEST-ohje.pdf

Fox DataDiode EAL 7+ 1Gbps. 2015. Accessed on 22.1.2018. Retrieved from https://www.ia.nato.int/niapc/Product/Fox-DataDiode-EAL-7--1Gbps_250

Herrero, M. 2015. From Air Gaps to Segmentation in Industrial Control Systems. Computer Emergency Response Team for Security and Industry (CERTSI), Spain. Accessed on 11.12.2017. Retrieved from https://www.certsi.es/en/blog/airgap-en

Investigation: WannaCry cyber attack and the NHS. 2017. Web publication. National Audit Office. Accessed on 13.11.2017. Retrieved from https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

Jones, D. & Bowersox, T. 2006. Secure Data Export and Auditing using Data Diodes. Department of Computer Science, The University of Iowa, Iowa City, IA. Reference 8.11.2017. Retrieved from https://www.usenix.org/legacy/event/evt06/tech/full_papers/jones/jones.pdf

KATAKRI - Information security audit tool for authorities – 2015. 2016. Ministry of Defense. Accessed on 16.12.2017. Retrieved from http://julkaisut.valtioneuvosto.fi/handle/10024/74858

Kiviharju M. 2016. Enforcing Role-Based Access Control with Attribute-Based Cryptography in MLS Environments. Accessed on 6.12.2017. Retrieved from https://aaltodoc.aalto.fi/handle/123456789/20258#

Leppänen, T. 2017. Practical implementation of Windows end-point security controls, Master's degree programme in Information Technology, JAMK. Accessed on 24.1.2018

Leonhard, W. 2018. Perfect end to a perfect month: Yet another Win10 1709 cumulative update, KB 4058258. Computerworld. Referenced 11.8.2018. Retrieved from https://www.computerworld.com/article/3252808/microsoft-windows/perfect-end-to-a-perfect-month-yet-another-win10-1709-cumulative-update-kb-4058258.html

List of CentOS Mirrors. 2018. The CentOS Project. Accessed on 12.2.2018. Retrieved from https://www.centos.org/download/mirrors/

Mercer, N. 2016. Further simplifying servicing models for Windows 7 and Windows 8.1. Microsoft TechNet. 31.1.2018. Retrieved from https://blogs.technet.microsoft.com/windowsitpro/2016/08/15/further-simplifying-servicing-model-for-windows-7-and-windows-8-1/

Mertens, X. 2017, The Flood of CVEs. Web publication. Internet Storm Center. Accessed on 22.1.2018. Retrieved from https://isc.sans.edu/forums/diary/2017+The+Flood+of+CVEs/23173/

Method for transferring data from an unsecured computer to a secured computer. 1992. U.S Patent US5703562A. Accessed on 29.1.2018. Retrieved from https://worldwide.espacenet.com/publicationDetails/biblio?FT=D&date=19971230&DB=&locale=en_EP&CC=US&NR=5703562A&KC=A&ND=5

Ohje arviointikriteeristojen tulkinnasta [Guidance Interpretation of Criteria for Evaluation]. 2015. FICORA. Accessed on 17.12.2017. Retrieved from

https://www.viestintavirasto.fi/attachments/tietoturva/Ohje_arviointikriteeristojen_tulkinnasta.pdf

Ohje Tietoturvallisuuden Arviointilaitoksille (versio 6.0) [Guide for accredited inspection bodies]. 2017. FICORA. Accessed on 14.12.2017. Retrieved from https://www.viestintavirasto.fi/attachments/Ohje_tietoturvallisuuden_arviointilaitoksille.pdf

Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista [Designing and Implementing Secure Gateway Solutions]. 2016. FICORA. Accessed on 4.12.2017. Retrieved from https://www.viestintavirasto.fi/attachments/Yhdyskaytavaratkaisuohje.pdf

Overview of Windows as a service. 2018. Windows IT Pro Center. Accessed on 31.1.2018. Retrieved from https://docs.microsoft.com/en-gb/windows/deployment/update/waas-overview,31.1.2018

Petersen, S. 2016. Why Data Diodes Are Essential for Isolated and Classified Networks. OPSWAT Inc. Accessed on 11.12.2017 Retrieved from https://www.opswat.com/blog/why-data-diodes-are-essential-isolated-and-classified-networks

Peterson, P. 2016. Secure Network Design: Micro Segmentation. SANS Institute InfoSec Reading Room. 4.1.2018. Retrieved from https://www.sans.org/reading-room/whitepapers/bestprac/secure-network-design-micro-segmentation-36775

Pulliainen T. 2016. Linux Patch Management: Comparison of Practical Implementations. Accessed on 2.2.2018. Retrieved from http://urn.fi/URN:NBN:fi:amk-2016092314504

Rousku, K. 2017. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä; Toimintasuunnitelma vuosille 2017–2019 [The Government Information Security Management Board; Agenda 2017–2019]. Ministry of Finance. Accessed on 30.12.2017. Retrieved from http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79978/VM_21_2017.pdf?sequence=1&isAllowed=y,

Robison, C. 1993. Real World research: a resource for social scientists and practitioner-researchers. Oxford: Blackwell

Sardiwal, M. Londhe, Y. Fraser, N. Richard, N. O'Leary, J. Cannon, V. New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit. 2017. FireEye Inc. Accessed on 22.1.2018. Retrieved from https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

Schotanus, H. Hartog, T. Verkoelen C. 2012. Information Security Dept., TNO Information and Communication Technology, Delft, The Netherlands. Accessed on 6.1.2018. Retrieved from https://repository.tudelft.nl/view/tno/uuid:13bfc973-0f13-4769-a535-3385506db60a/

Stevens, M. 1999. An implication of an optical data diode. Information Technology Division Electronics and Surveillance Research Laboratory. Accessed on 24.1.2018. Retrieved from http://dspace.dsto.defence.gov.au/dspace/handle/1947/4386

Stevens, M. Pope M. 1995. Data Diodes. Information Technology Division Electronics and Surveillance Research Laboratory, Australia. Accessed on 24.1.2018. Retrieved from http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/3990/1/DSTO-TR-0209%20PR.pdf

Suojelupoliisin toimintaympäristö vuosina 2015 – 2016. 2015. [The operating environment of the security police in the years 2015-2016]. Finnish Security Intelligence Service. Accessed on 11.12.2017. Retrieved from https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/64088_Suojelupoliisin_toimintaymparisto_vuosina_2015-2016.pdf?71626e637355d488

VAHTI 2/2010, Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta [A Guide to the Implementation of the Decree on Information Security in Public Administrations]. 2010. Ministry of Finance. Accessed on 30.1.2018. Retrieved from https://www.vahtiohje.fi/web/guest/2/2010-ohje-tietoturvallisuudesta-valtionhallinnossa-annetun-asetuksen-taytantoonpanosta

Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut [Encryption solutions approved by the Finnish Communications Regulatory Authority (NCSA)] - Document diary: 1240/651/2017. 2017. The Finnish Communications Regulatory Authority (FICORA). Accessed 19.7.2018. Retrieved from https://www.viestintavirasto.fi/attachments/tietoturva/NCSA_salausratkaisut.pdf

VAHTI 5/2013, Päätelaitteiden tietoturvaohje [Terminal Device Information Security Guidelines]. 2013. Ministry of Finance. Accessed on 30.1.2018. Retrieved from https://www.vahtiohje.fi/web/guest/5/2013-paatelaitteiden-tietoturvaohje

VAHTI. 2/2014, Tietoturvallisuuden Arviointiohje [VAHTI Information Security Assessment Guide]. 2014. Ministry of Finance. Accessed on 30.12.2017. Retrieved from https://www.vahtiohje.fi/web/guest/2/2014-tietoturvallisuuden-arviointiohje

Windows Update Services: Client-Server Protocol. 2017. Developer Network. Accessed on 12.2.2018. Retrieved from https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-WUSP/[MS-WUSP].pdf

Windows Server Semi-Annual Channel Overview. 2017. Windows IT Pro Center. Accessed on 31.1.2018. Retrieved from https://docs.microsoft.com/en-gb/windows-server/get-started/semi-annual-channel-overview

Yahoo Provides Notice to Additional Users Affected by Previously. 2017. Web publication. Oath Inc. Accessed on 13.11.2017. Retrieved from https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/

Appendices

Appendix 1. Windows patch file verification PowerShell script

```
################################################################################
#By Teemu Keso
################################################################################

#Folder parametres

$sourcefolder = "E:\WSUS\WsusContent"

$destination = "c:\dest\WSUS\"

#Sigcheak parametres

$siglocation = "C:\log\Siglogfile.txt"

#F-secure parametres

#F-secure installation folder
$fsavlocation = "C:\Program Files (x86)\F-Secure\Anti-Virus\fsav.exe"

$loglocation = "C:\log\Scanlogfile.txt"

$fparametres = ("/EXT= * /ARCHIVE /NOBOOT /silent /NOBREAK
/report=$loglocation $sourcefolder ")


#Log parametres

$EndTime = Get-Date

#Before first run: New-EventLog -LogName "Update PowerShell Application" -
Source "Validation script" -ErrorAction stop

################################################################################

#Signature check Function

Function Sigcheck

{

    $items = Get-ChildItem -Recurse $sourcefolder\*.*

    ForEach($item in $items)

    {

        $validSignature = Get-AuthenticodeSignature $item | where
{($_.status -eq "Valid") -and($_.SignerCertificate.Issuer -eq "CN=Microsoft
Code Signing PCA, O=Microsoft Corporation, L=Redmond, S=Washington, C=US")}


        if($validSignature)

        {

            Write-Host "Valid filesignature in $item"

            #Poista
            #$script:sigerrorcount = 0

           }

        else

        {
```

```
            Write-Host "Signature validation not successful $item "
            Add-Content $siglocation -Value "$EndTime $item"
            #Poista
            #$script:sigerrorcount++
            return 1
        }
    }
    return 0
}
Function FCheck
{
    Write-Host "Starting F-secure antivirus scan"

#F-secure scan
    cd $sourcefolder
    #To prevent F-secure scanning the extra folders
    $fproses = Start-Process "$fsavlocation" -ArgumentList $fparametres  -
Wait -NoNewWindow -PassThru

    if ($fproses.ExitCode -eq 0)
    {
        Write-Host "F-Secure AV-scan was successful"
        #Poista
        #$script:ferrorcount = "0"
    }
    else
    {
        #Poista
        #$script:ferrorcount = "1"
        Write-Host "F-secure AV-scan was unsuccessful!"
           return 1
    }
    return 0
}
Function failure
{
    Write-Host "Problem with file validation or F-secure scanning. More
information in. More information in $siglocation and $loglocation"
    $logmessage = "Problem with file validation or F-secure scanning. More
information in $siglocation and $loglocation"

    try
    {
        New-EventLog -LogName "Update PowerShell Application" -Source
"Validation script" -ErrorAction stop
    }
```

```
    catch [System.Exception]

    {

        #to disable error message that may come

    }


    Write-EventLog -LogName "Update PowerShell Application" -Source
"Validation script" -EventID 10 -EntryType Error -Message "Problem with file
validation or F-secure scanning. More information in. More information in
$siglocation and $loglocation"

}



#Run
Write-Host "Verifying signatures from $sourcefolder folder - Start Time
$EndTime"

$sigerrorcount = Sigcheck
#Set Sigcheck function error count as a variable

If ($sigerrorcount -eq 0)

{

    $ferrorcount = FCheck
    #Set FCheck function error count as a varible

    if ($ferrorcount -eq 0)

    {

        Write-Host "Validation successful. Moving files for datadiode -
$EndTime"

        Get-ChildItem -Path $destination -Recurse | Remove-Item -force -
recurse

        Get-ChildItem -Path $sourcefolder -Recurse | Move-Item -Destination
$destination -force

    }

    else

    {

        failure

    }


}

else

{

    Failure

}
```

Appendix 2. RPM file verification bash script

```
#!/bin/bash
#RPM file location
INVALID_FILES=`find /mnt/d/Linux/*/ -type f ! -iname '*.rpm'`
for i in $INVALID_FILES;
do
        let "ERRORS=ERRORS+1"
        echo "$i: Not RPM package!"
done
if [ "$ERRORS" > 0 ]; then
        echo "Number of non RPM packages found: $ERRORS"
        exit 1
fi
#RPM file location
VALID_FILES=`find /mnt/d/Linux/*/ -type f -iname '*.rpm'`
for i in $VALID_FILES;
do
        rpm -Kv $i | grep -v OK
        if [ "$?" != "0" ]; then
                echo "Is not valid rpm!"
                exit 1
        fi
done
```

Appendix 3. Guide for accredited inspection bodies, Appendix 2

Guide for accredited inspection bodies [Ohje Tietoturvallisuuden Arviointilaitoksille (versio 6.0)], Appendix 2. Assessment report

Liite 2. Arviointiraportti

Tietoturvallisuuden arvioinnin pohjalta on laadittava arviointiraportti, jonka tulee pitää sisällään ainakin seuraavat kohdat riittävällä laajuudella perusteltuina.

- Kuvaus arvioinnin kohteesta
- Arviointityyppi
- Käytetyt kriteeristöt
- Suojattavan tiedon omistajuus ja taso
- Arvioinnin ajankohdat
- Rajaukset
- Keskeiset havainnot
- Arvioinnin tekijät
- Raportin hyväksyjät arvioinnin suorittaneessa organisaatiossa
- Tiedon siitä miten ja mistä lisätietoja raportista voi tiedustella
- Raportin jakelu (toimitetaan aina myös Viestintävirastolle)
- Vaatimuskohtainen erittely, sisältäen kuvaukset vaatimuksen toteutustavasta ja siitä, kuinka tämä on todennettu (alla ohjeellinen esimerkkitoteutustapa)

I 01 - Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen - Verkon rakenteellinen turvallisuus		**OK**
Vaatimus	**Kuinka tämä on toteutettu arviointikohteessa?**	**Arviointitulos**
Suojaustaso IV		
1) Tietojenkäsittely-ympäristö on erotettu muista ympäristöistä.	Tietojenkäsittely-ympäristö on fyysisesti muista verkoista eriytetty verkko, johon ei ulkoisia liittymiä. Poikkeuksina ovat kohdassa 4 käsitelty yhdyskäytäväratkaisu, sekä kohdassa I 09 käsitelty tiedon tuonti/vienti siirtomedialla. Fyysinen erottelu toteutettu kytkintasoa myöden, ja esimerkiksi salausratkaisuissa ja datadiodiratkaisussa toteutuu punamusta-erottelu. Huom: Arvioinnista rajattu ulos toimittajan B etähallintaratkaisu, ks. liite 1.	OK
2) Tietojenkäsittely-ympäristön kytkeminen muiden suojaustasojen ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä.	Ainoa yhteys yhdyskäytäväratkaisun kautta, ks. alakohta 4.	OK
3) Hallitun fyysisen turva-alueen ulkopuolelle menevä liikenne salataan viranomaisen ko. suojaustasolle hyväksy-	Kohteessa käytetään Viestintäviraston suojaustasolle X hyväksymää salausratkaisua (Tuotenimi, versiotiedot) tuotteen käyttöpolitiikan (xx.xx.xxxx) mukaisesti. Avaimisto tuotetaan Organisaatio O:n PKI:sta, joka sijoitettu kokonaisuudessaan ko. tietojenkäsittely-ympäristön Y sisälle. PKI:n	OK

mällä salausratkaisulla (vrt. I 12 ja I 15).	turvallisuus käsitelty tarkemmin kohdassa I 12.	
Suojaustasot III-II		
Kohtien 1 ja 3 lisäksi: 4) Tietojenkäsittely-ympäristön kytkeminen muiden suojaustasojen ympäristöihin edellyttää viranomaisen ko. suojaustasolle hyväksymän yhdyskäytäväratkaisun käyttöä.	Kohteessa käytetään Viestintäviraston yhdyskäytäväratkaisuohjeen (27.6.2017) luvussa 4.1.1 kuvatun mukaista datadiodiratkaisua. Ko. datadiodimallilla on Viestintäviraston erillishyväksyntä ko. tietojenkäsittely-ympäristöön (viite xxx).] Sisällön validointi tapahtuu AV-tuotteella sekä lähettävällä että vastaanottavalla puolella. Tuotavien asennuspakettien eheys tarkistetaan automatisoidusti (MS-tuotteet, Ubuntu-päivitykset), sekä manuaalisesti siltä osin, kuin valmistaja tarjoaa asennuspakettien tiivisteitä.	OK
Aineistot	[Dokumenttiviite a] Asiakkaan toimittama verkkokuva. [Dokumenttiviite b] Muistiinpanot asiakkaan henkilöstön haastatteluista xx.xx.xxxx ja yy.yy.yyyy. [Dokumenttiviite c] Tekninen näkymä verkkorakenteeseen. [dokumenttiviite d] Asiakkaan toimittama prosessikuvaus päivitystuonnista.	
Todennus	**Verkkorakenne** Arvioitu verkon rakennetta - asiakkaan toimittaman verkkokuvan [Dokumenttiviite a], - asiakkaan henkilöstön haastattelujen [Dokumenttiviite b], - aktiivisen rajapinta-analyysin keinoin (portti- ja haavoittuvuusskannaukset, ks. tarkempi kuvaus kohdasta I 02), - passiivisen rajapinta-analyysin keinoin (ks. tarkempi kuvaus alta), ja - verkon aktiivilaitteiden konfiguraatioiden tarkastuksella (ks. tarkempi kuvaus kohdasta I 06). Aktiivisen ja passiivisen rajapinta-analyysin perusteella rakennettu tekninen, toimitetun verkkokuvan kanssa yhtenevä näkymä verkkorakenteeseen taltioitu dokumenttiin [Dokumenttiviite c]. Passiivisessa rajapinta-analyysissä peilattu kaikki ko. ympäristössä liikkuva verkkoliikenne kahdesta runkokytkimestä, sekä puna-musta-erottelun (salauslaite- ja datadiodikytkennät) osalta myös ulkopuolen kytkimestä. Liikennettä nauhoitettu 2 vrk kussakin nauhoituspisteessä, runkokytkinten osalta samanaikaisesti. Liikennenauhoitusta on analysoitu skriptein (xxx) sekä graafisella työkalulla. **Yhdyskäytäväratkaisu** Arvioinnissa on tarkastettu UDP-liikenteen lähettävän ja vastaanottavan pään alustat konfiguraatioista, sekä portti- ja haavoittuvuusskannaamalla ne ulkoa päin. Sisääntuotavan aineiston validoinnissa (AV, eheystarkastukset) toimivuutta arvioitu tarkastamalla prosessikuvaukset, haastattelemalla henkilöstöä, AV-tuotteen konfiguraatiosta, sekä automatisoitujen osien (MS-tuotteet, Ubuntu-päivtykset) osalta SCCM:stä sekä Ubuntu-päivityspalvelimen konfiguraatiosta. Toimivuus todennettu myös lähettämällä Eicar-testivirus sekä eheydeltään rikottuja MS-päivityspaketteja diodin läpi. Verrattu yhdyskäytäväratkaisutuotteen asennusta Viestintäviraston erillishyväksynnän käyttöpolitiikkaan (viite xxx), ja todettu täyttävän politiikan vaatimukset. Tarkistettu, että laitemalli vastaa käyttöpolitiikan mallia ja versiota laitteen kyljestä ja tietolevystä silmin havainnoiden. Silmin havainnoiden ko. tuotteen kytkentäkaaviota verrattu fyysisiin kytkentöihin, ja todettu mediamuuntimen paluukanavan olevan fyysisesti irtikytkettynä. Laitekaapin pääsynhallinta ja fyysisen turvallisuus käsitelty kohdassa F xx. Datadiodituotteen hallinnointi tarkastettu kuvauksiin tutustumalla, henkilöstöä haastattelemalla sekä seuraamalla hallinnointia paikan päällä, sekä myös diodituotteen lokitietoja katselmoimalla. **Salausratkaisu** Käsitelty kohdassa I 12.	