jamk

Palomuurin ja verkkosensorin asennus kybertoimintaympäristöön

Konsta Hirvikorpi

Leevi Kauranen

Opinnäytetyö, AMK
Joulukuu 2025
Insinööri (AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Hirvikorpi, Konsta & Kauranen, Leevi

Palomuurin ja verkkosensorin asennus kybertoimintaympäristöön. Tieto- ja viestintätekniikka

Jyväskylä: Jyväskylän ammattikorkeakoulu. **Joulukuu 2025**, 57 sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Tehtävänä oli toteuttaa työnantajan käytössä olevaan kybertoimintaympäristöön toiminnallisuuksien ja tietoturvan kehittämistä. Tavoitteena oli implementoida kybertoimintaympäristöön palomuuri- ja sensori ratkaisu, jossa palomuuri suojaa ympäristöä sekä lokienkäsittelijäpalvelinta, ja sensori mahdollistaa lokidatan keräämisen verkkoliikenteestä. Nämä implementoitiin yhteensopivaksi olemassa olevien laitteiden ja ratkaisuiden kanssa.

Ympäristöön asennettiin erillinen fyysinen palomuuri sekä sensori, ja lokienkäsittelijäpalvelin konfiguroitiin toimimaan näiden kanssa yhtenä kokonaisuutena. Palomuuri suodattaa lokilähteiden lähettämän liikenteen ja varmistaa, että vain määritetyt ja luotetut yhteydet ovat sallittuja. Lisäksi lokienkäsittelijäpalvelimen ja lokilähteiden välille implementoitiin TLS protokolla varmenteilla, jotta liikkuva lokitieto voidaan salata ja molempien osapuolien identiteetti varmistaa. Salaus implementoitiin, jotta verkkoliikennettä ei voida lukea tai muokata siirron aikana, kun taas sertifikaatit varmistavat, että lokienkäsittelijäpalvelin ei kommunikoi hyökkääjän operoiman lokilähteen kanssa. Tämän avulla varmistettiin sekä tiedonsiirron eheys että luottamuksellisuus.

Teknisen toteutuksen lisäksi työnantajalle tuotettiin asennusdokumentaatio, joka ohjeistaa lukijaa. Asennusdokumentaatiossa ohjeistetaan mitkä ohjelmistot ja työkalut ovat tarpeellisia ja mitkä toimenpiteet täytyy suorittaa ennen kuin toteutuksen voi aloittaa. Tämän jälkeen käydään läpi jokaisen laitteen asennus sekä laitekohtaiset konfiguraatiot. Palomuurin kohdalla ohjeistetaan verkkoporttien sekä sääntöjen konfigurointi, lokienkäsittelijäpalvelimen kohdalla ohjeistetaan TLS protokollan implementointi ja muut paikalliset konfiguraatiot.

Lopputuloksena syntyi toimiva kokonaisuus, jossa palomuuri-, lokinkeräys-, ja sensoriratkaisut on integroitu työnantajan toimintaympäristöön. Työnantajalle toimitettiin myös kattava dokumentaatio työn asennus- ja konfiguraatio vaiheista, jotta prosessin voi tarvittaessa toistaa ja ympäristön laajennus ja kehitys helpottuu.

Avainsanat (asiasanat)

Linux, kyberturvallisuus, palomuuri, sensori, virtualisointi

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Hirvikorpi, Konsta & Kauranen, Leevi

Installation of a firewall and network sensor in a cyber environment.

Jyväskylä: JAMK University of Applied Sciences, December 2025, 57 pages

Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The task was to develop the functionality and information security of the cyber environment used by the employer. The goal was to implement a firewall and sensor solution in the cyber operating environment, where the firewall protects the environment and the log handler server, and the sensor enables the collection of log data from network traffic. These were implemented to be compatible with existing devices and solutions.

A separate physical firewall and sensor were installed in the environment, and the log handler server was configured to work with them as a single whole. The firewall filters the traffic sent by log sources and ensures that only specified and trusted connections are allowed. In addition, the TLS protocol with certificates was implemented between the log handler server and the log sources to encrypt the moving log data and verify the identity of both parties. Encryption was implemented so that the network traffic cannot be read or modified during transfer, while the certificates ensure that the log handler server does not communicate with a log source operated by a malicious entity. This ensured both the integrity and confidentiality of the data transfer.

In addition to the technical implementation, installation documentation was produced for the employer to guide the reader. The installation documentation provides instructions on which software and tools are required and what steps must be taken before implementation can begin. It then goes through the installation of each device and device-specific configurations. For the firewall, it provides instructions on configuring network ports and rules, while for the log handler server, it provides instructions on implementing the TLS protocol and other local configurations.

The end result was a functional whole in which the firewall, log collection, and sensor solutions were integrated into the employer's operating environment. The employer was also provided with comprehensive documentation on the installation and configuration phases of the work so that the process can be repeated if necessary and the expansion and development of the environment can be facilitated.

Keywords/tags (subjects)

Linux, cybersecurity, firewall, sensor, virtualization

Miscellaneous (Confidential information)

-

Sisältö

Sanasto ..... Virhe. Kirjanmerkkiä ei ole määritetty.

1 Johdanto ..... Virhe. Kirjanmerkkiä ei ole määritetty.

2 Työn tavoitteet ja rajaukset ..... Virhe. Kirjanmerkkiä ei ole määritetty.

3 Kyberturvallisuuden teoria ..... Virhe. Kirjanmerkkiä ei ole määritetty.

3.1 Kyberturvallisuus ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

3.2 Tietoturvallisuus ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

3.3 Kybertoimintaympäristö ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

3.4 Hyökkäysvektorit ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

3.5 Hyökkäys pinta-ala ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

3.6 Kyberpuolustus ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

4 Tekniset ratkaisut ..... Virhe. Kirjanmerkkiä ei ole määritetty.

4.1 Palomuuri ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

4.1.1 ebtables ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

4.1.2 iptables ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

4.2 Sensori ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

4.3 Lokien hallinta ja SIEM-järjestelmät ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

4.4 Julkisen avaimen infrastruktuuri ja TLS ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

4.5 OSI-malli ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5 Toteutus ..... Virhe. Kirjanmerkkiä ei ole määritetty.

5.1 Ympäristön topologian ja fyysisten verkkoyhteyksien kuvaus **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.2 Työnantajan vaatimukset toteutetulle konfiguraatiolle ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.3 Ympäristön valmistelu ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.4 Palomuurin käyttöönotto ja konfigurointi ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.4.1 Palomuurin säännöt ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.4.2 Lokilähteiden reititys palomuurissa ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.5 Lokienkäsittelijäpalvelimen asennus ja konfigurointi **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.5.1 TLS sertifikaattien luonti ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.5.2 Lokienkäsittelyohjelmiston konfigurointi .. **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.5.3 Reitityksen ja palomuurin konfigurointi .... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.6 Sensorin käyttöönotto ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.6.1 Alustavat toimenpiteet ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.6.2 Automatiikan konfigurointi ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.6.3 Lokien lähetyksen konfigurointi ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.6.4 Ongelma TLS sertifikaattien ja avaimien konfiguroinnissa**Virhe. Kirjanmerkkiä ei ole määritetty.**

5.6.5 Reitityksen ja palomuurin konfigurointi .... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.7 Kybertoimintaympäristön testaaminen ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.7.1 Lokilähteen testaaminen ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

5.7.2 Sensorin testaaminen ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

6 Tulokset..... Virhe. Kirjanmerkkiä ei ole määritetty.

7 Pohdinta..... Virhe. Kirjanmerkkiä ei ole määritetty.

Lähteet ..... Virhe. Kirjanmerkkiä ei ole määritetty.

Liitteet ..... Virhe. Kirjanmerkkiä ei ole määritetty.

Liite 1. Liitteen otsikko ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

Liite 2. Liitteen otsikko ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

Kuviot

Kuvio 1. Ihmiset prosessit & teknologiat 8

Kuvio 2. CIA-triad 9

Kuvio 3. Fyysinen verkkotopologia 20

Kuvio 4. Palomuurin säännöt 23

Kuvio 5. TCP-palvelu joka rajoittaa portteja 24

Kuvio 6. DoS-suojaus 25

Kuvio 7. Staattinen reititys 26

Kuvio 8. DHCP-konfiguraatio lokilähteitä varten 27

Kuvio 9. Kohde- ja lähdeosoitteen muunnos 28

Kuvio 10. NAT-kohdeosoitteen muunnos 28

Kuvio 11. Esimerkki konfiguroidun palomuurin verkkoporteista 29

Kuvio 12. CA-sertifikaatin asetukset 30

Kuvio 13. Palvelimen sertifikaatin asetukset 32

Kuvio 14. Asiakaskoneen sertifikaatti asetukset 34

Kuvio 15. Esimerkki lokienkäsittelyohjelmiston konfiguraatiosta 37

Kuvio 16. Sensorin bridge 40

Kuvio 17. Sensorin lokityökalun verkkoliitäntä 40

Kuvio 18. Sensorin lokityökalun staattiset reitit 41

Kuvio 19. Sensorin lokityökalun konfiguraatio 41

Kuvio 20. Sertifikaattien korjaus skripti 42

Kuvio 21. crontab 43
Kuvio 22. Sensorin paikallinen 2- ja 3 kerroksen palomuuri 44
Kuvio 23. Iptables konfiguraatio 46
Kuvio 24. Client filebeat asetukset 47
Kuvio 25. Client filebeat testi 47
Kuvio 26. Liikennettä sensorin ja lokienkäsittelijäpalvelimen välillä. 48

Taulukot

Taulukko 1. ebtables rakenne 13
Taulukko 2. iptables rakenne 14
Taulukko 3. OSI-malli 18
Taulukko 4. Palomuurin sääntöjen hallintaelementit 23
Taulukko 5. CA-sertifikaatin asetukset 31
Taulukko 6. Palvelimen sertifikaatin asetukset 32
Taulukko 7. Esimerkki muutoksesta palvelimen sertifikaatiin 34
Taulukko 8. Asiakaslaitteen sertifikaatin asetukset 35
Taulukko 9. Ebtables konfiguraatio 44
Taulukko 10. Iptables konfiguraatio 45

Sanasto

CA	Varmenneviranomainen (engl. Certificate Authority)
CTI	Kyberuhkatieto (engl. Cyber Threat Intelligence)
EDR	Päätelaitteiden havainnointi ja reagointi (engl. Endpoint Detection & Response)
FW	Palomuuri (engl. firewall)
IDS	Tunkeutumisenhavaitsemisjärjestelmä (engl. intrusion detection system)
IOC	Vaarantumisindikaattori (engl. indicator of compromise)
MFA	Monivaiheinen tunnistautuminen (engl. Multifactor Authentication)
MISP	Haittaohjelmatietojen jakamisalusta (engl. malware information sharing platform)
NAT	Verkko-osoitteen muunnos (engl. Network Address Translation)
NGFW	Seuraavan sukupolven palomuuri (engl. Next-Generation Firewall)
OSI-model	Tietoliikenteen viitekehys, OSI-viitemalli (engl. Open Systems Interconnection Reference Model)
PKI	Julkisen avaimen järjestelmä (engl. Public key infrastructure)
SIEM	Turvallisuustietojen ja tapahtumien hallintajärjestelmä (engl. Security information and event manager)
SOC	Tietoturvavalvomo (engl. security operations center)
TCP	Siirronohjauksen yhteyskäytäntö (engl. Transmission Control Protocol)
TLS	Kuljetustason turvallisuus (engl. Transport Layer Security)

1 Johdanto

Digitalisaation kasvaessa olemme jatkuvasti enemmän riippuvaisia kybertoimintaympäristöstä ja sen toiminnasta niin yksilö-, kuin yritystasolla. Tämän vuoksi nykyajan organisaatiolle sisäiset tietoverkot ja julkinen internet ovat elintärkeä osa taloudellista toimintaa ja tätä toimintakykyä pitää kyetä suojaamaan kaiken tasoisilta uhilta. Mikäli yritys epäonnistuu tietojen ja toimintojensa suojaamisessa, saattaa sillä olla vakavia seuraamuksia kuten, toiminnan keskeytyminen, mainehaitta, kilpailukyvyn laskeminen, tietojen vuoto kilpailijalle, vakava sakkorangaistus, tai pahimmassa tapauksessa liiketoiminnan loppuminen. (Jonker, Kosinski & Lindemulder 2024)

Kaikilla organisaatioilla ei kuitenkaan ole riittäviä resursseja, osaamista, tai tahtotilaa kehittää sisäistä kyberturvallisuustoimintaa. Tällöin yritys saattaa nojautua oletukseen, etteivät itse joutuisi hyökkäyksen kohteeksi. Käytännössä kuitenkin valtaosa organisaatioista kohtaa toimintansa aikana kyberhyökkäyksiä jollain tasolla, ja ratkaiseva ero syntyy siinä, kyetäänkö ne havaitsemaan ja torjumaan vai jäävätkö ne huomaamatta. Vaihtoehtoisesti organisaatio voi hankkia ulkopuolista asiantuntemusta esimerkiksi ostamalla kyberturvallisuuspalveluita kolmannelta osapuolelta. Pienyrityksille, joilla ei ole resursseja omaan kyberpuolustukseen, ulkopuolisten kyberturvallisuuspalveluiden ja vakuutusten käyttö tarjoaa kustannustehokkaan ja luotettavan tavan vahvistaa turvallisuutta.

Organisaatioiden kyberturvallisuuden turvaamiseksi on kehitetty laajalti erilaisia työkaluja, palveluita sekä toimintaperiaatteita. Näihin kuuluvat esimerkiksi palomuurit, lokienhallintajärjestelmät, verkon ja laitteiden seurantajärjestelmät sekä tunkeutumisen havaitsemis- ja estojärjestelmät (IDS/IPS). Eri teknologiat muodostavat yhdessä kerroksellisen suojan, jossa yksittäinen ratkaisu ei yksinään ole riittävä, vaan niiden yhteistoiminta vahvistaa organisaation kykyä torjua ja havaita kyberuhkia.

Tässä opinnäytetyössä toimeksiantajan kybertoimintaympäristöä kehitetään juuri näiden teknologioiden avulla: ympäristöön asennetaan palomuuri ja verkkosensori, joiden tarkoituksena on parantaa ympäristön tietoturvallisuutta, luotettavuutta sekä seurattavuutta. Palomuuri toimii perustavanlaatuisena suojausratkaisuna, jonka avulla säädellään sisään- ja ulosmenevää verkkoliikennettä. Sen avulla pystymme estämään luvattomia yhteyksiä, sekä luomaan sääntöihin perustuvaa kontrollointia tietoliikenteen kululle. Uusimmilla NGFW-palomuureilla pystytään myös

analysoimaan liikenteen sisältöä. Sensori puolestaan täydentää suojausta mahdollistamalla liikenteen ja järjestelmien jatkuvan seurannan, sekä poikkeamien havaitsemisen. Kun kokonaisuuteen yhdistetään vielä esimerkiksi lokienhallintajärjestelmä, saadaan muodostettua kokonaisuus, jossa uhat havaitaan nopeammin ja niihin reagointi on tehokkaampaa ja helpompaa.

2 Työn tavoitteet ja rajaukset

Kehitystyön päämääränä on parantaa toimeksiantajan omistamaa kyberpuolustuksen toimintaympäristöä ja dokumentaatiota. Kehittäminen toteutetaan lisäämällä ympäristöön palomuuri suojaamaan olemassa olevia palveluita sekä työkaluja, sitä varten, kun kokonaisuus liitetään olemassa olevaan verkkoon. Tämän lisäksi asennetaan sensori, jolla voidaan kerätä dataa verkkoliikenteestä. Lokienkäsittelijäpalvelin konfiguroidaan lokien turvallista vastaanottoa varten. Laitteet ja ohjelmistot konfiguroidaan yhteensopivaksi ympäristön tämänhetkisen käyttötarkoituksen kanssa ilman että kyberturvallisuutta uhrataan tai että ympäristön toimintakyky heikkenee.

Tämän työn kontekstissa sensorilla viitataan laitteeseen, joka valvoo verkkoa tai verkon segmenttiä, ympäristön verkkoliikenne joko kulkee laitteen läpi tai se erikseen reititetään siihen. Työ käsittelee vain digitaalisia hyökkäysvektoreita ja hyökkäyspinta-alaa, joilla uhkatoimija voi vaarantaa ympäristön kiertämällä tai murtautumalla palomuurien ja muiden turvallisuustyökalujen läpi. Työ ei käsittele esimerkiksi fyysisiä hyökkäysvektoreita tai sosiaalista hyökkäyspinta-alaa. SIEM-järjestelmien tai muiden lokien analysointi- ja rikastamisohjelmistojen asennus ja konfigurointi on rajattu tämän kehitystyön ulkopuolelle. Työn sisältönä on vain palomuurin sekä sensorin asennus, lokienkäsittelijäpalvelimen konfiguraatio ja asennusdokumentaation luonti.

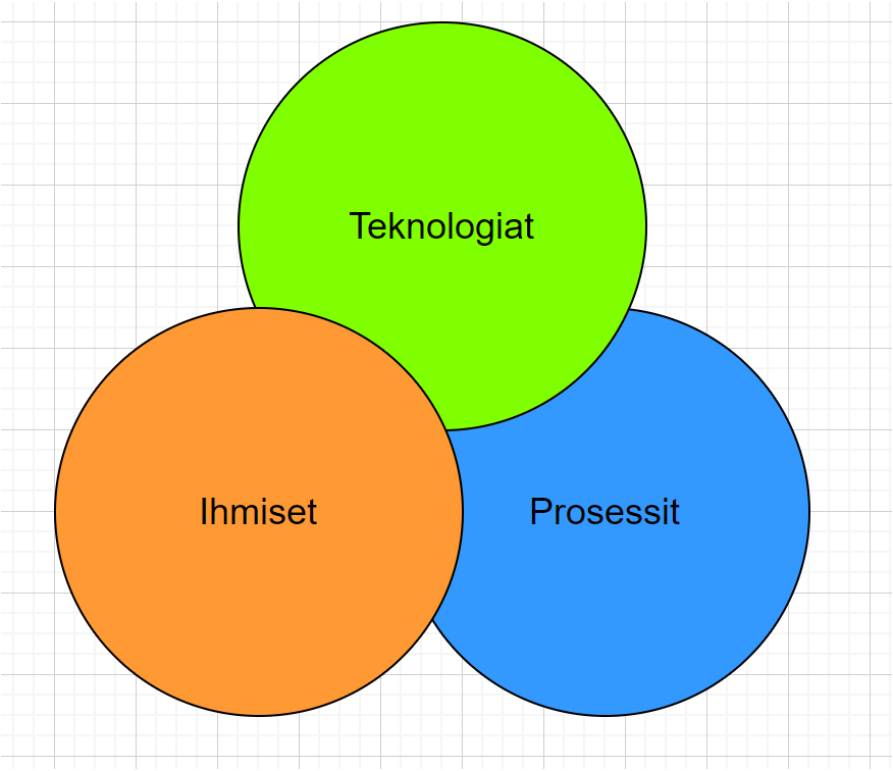
Tämä työ koostuu dokumentaatiosta, joka kuvaa palomuurin ja sensorin asennusprosessin, lokienkäsittelijäpalvelimen konfiguroinnin turvattua lokiensiirtoa varten sekä asennusdokumentaation päivityksen. Työn tuloksena toimeksiantajalle muodostuu asennusdokumentaatio ympäristön käyttöönotosta, jossa käydään läpi lokienkäsittelijäpalvelimen konfigurointi sekä sensorin ja palomuurin asennus. Työnantajalle jää myös yksi ympäristö valmiina käyttöä varten. Tekijöille kerääntyy tarvittava informatiivinen materiaali, josta tämä työ koostuu.

3 Kyberturvallisuuden teoria

3.1 Kyberturvallisuus

Kyberturvallisuus on oppiala, joka koskee kaikkia teknologioita, käytäntöjä ja politiikkoja, joilla pyritään estämään kyberuhkatekijöiden hyökkäykset tai pienentämään näiden hyökkäysten vaikutusta. Kyberturvallisuudessa pyritään suojelemaan organisaatioiden ja yksityisten henkilöiden tietokonejärjestelmät, sovellukset, laitteet, data ja taloudelliset varat kiristysohjelmilta, yleisiltä haittaohjelmilta, kalastelulta ja muilta kyberuhilta. Onnistuneilla kyberhyökkäyksillä on kyky häiritä ja tuhota organisaatioita, esimerkiksi aiheuttamalla taloudellista vahinkoa estämällä Internetistä riippuva taloudellinen toiminta tai tuhoamalla järjestelmät tai tieto, jolla organisaation toiminta toteutetaan. Taloudellisen vahingon lisäksi voidaan myös vaikuttaa mielipiteisiin esimerkiksi vähentämällä luottamusta tiettyyn organisaatioon. Yksityishenkilöihin kohdistuu myös uhkia kyberrikollisuuden kautta, kuten identiteettivarkautta tai rahastus huijauksia.

Onnistunut kybersuojaus koostuu useasta suojaus kerroksesta jaoteltuna turvattaviin laitteisiin, verkkoihin, ohjelmistoihin ja turvattavaan tietoon. Hyvän kyberturvallisuuden tason saavuttamiseksi täytyy kiinnittää huomio erityisesti ihmisiin, prosesseihin ja teknologioihin. (What is Cybersecurity? N.d.) Näitä usein kutsutaankin kyberturvallisuuden kolmeksi peruspilariksi. (Ks. Kuvio 1)



Kuvio 1. Ihmiset prosessit & teknologiat

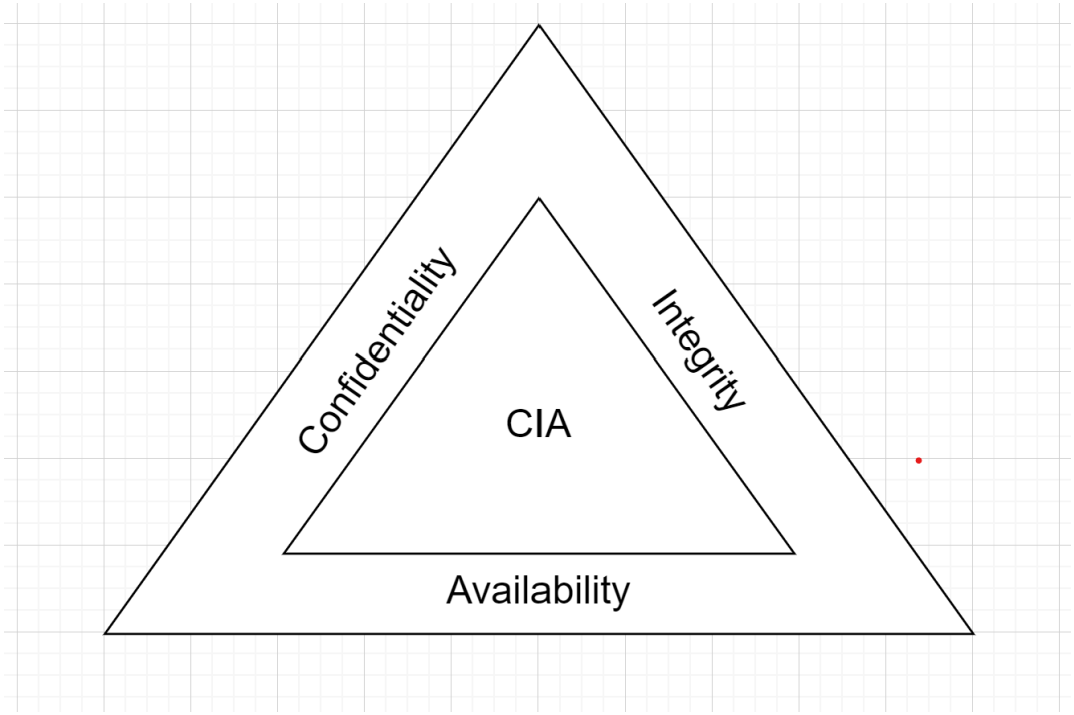
Ihminen on usein heikoin lenkki kyberturvallisuudessa, mutta oikeanlaisella osaamisella myös vahvin puolustus. Käyttäjien täytyy ymmärtää tiedon ja yksityisyyden suojaamisen periaatteet, kuten vahvojen salasanojen merkitys, kalasteluviestien tunnistaminen ja tiedon asianmukainen käsittely. Osaava ja koulutettu henkilöstö pystyy paitsi välttämään virheitä myös toimimaan ensimmäisenä suojamuurina hyökkäyksiä vastaan. Myös erikoistunut kyberturvatiimi on olennainen, sillä se kykenee tehokkaasti havaitsemaan, torjumaan ja ennaltaehkäisemään hyökkäyksiä. (Strengthening Your Cybersecurity: The power of three P’s in cybersecurity and Team Training 2023)

Prosessit ohjaavat sitä, miten turvallisuuskäytänteet otetaan käyttöön, sekä kuinka niitä valvotaan ja kehitetään. Ne luovat järjestelmällisen toimintamallin, jonka avulla uhkiin voidaan reagoida nopeasti ja johdonmukaisesti. Esimerkiksi tietoturvapoikkeamiin reagointi tulee toteuttaa ennalta määritettyjen ohjeiden mukaan, jotta toiminta ei jää sattumanvaraiseksi. Prosessien tehokkuus on kuitenkin aina riippuvainen siitä, kuinka hyvin ne on suunniteltu ja miten sitoutuneesti organisaation tiimi niitä noudattaa ja harjoittelee niiden käyttöä. (The Strengthening Your Cybersecurity: The power of three P’s in cybersecurity and Team Training 2023)

Tehokas suojaus edellyttää kehittyneiden työkalujen ja ratkaisujen hyödyntämistä. Näitä voi olla esimerkiksi IDR- ja EDR-järjestelmät, CTI-alustat, salausratkaisut ja MFA-työkalut. Tehokkaat työkalut eivät kuitenkaan itsestään takaa vahvaa puolustusta. Ilman osaavaa tiimiä ja jatkuvaa koulutusta parhaimmatkin tuotteet voivat jäädä vajaakäytölle tai jopa hyödyttömiksi. Kyberturvatiimin täytyy hallita työkalujen koko potentiaali, ja järjestelmien sekä ohjelmistojen päivitykset ja haavoittuvuudet. (Strengthening Your Cybersecurity: The power of three P's in cybersecurity and Team Training 2023)

3.2 Tietoturvallisuus

Tietoturvallisuudella tarkoitetaan tieto-omaisuuksien suojaamista kuten luottamuksellista, henkilökohtaista, arkaluonteista tai taloudellista dataa väärinkäytöltä, luvattomalta pääsyltä, muokkaukselta tai häiriöiltä. Tällaisia omaisuuksia voivat olla esimerkiksi digitaaliset tiedostot, paperi dokumentit, fyysiset tallennusvälineet tai ihmisten puhe. Tietoturvallisuus perustuu CIA-käytänteisiin, joka tulee sanoista confidentiality, integrity, availability, eli luottamuksellisuus, eheys ja saatavuus. (Holdsworth & Kosinski 2024) Näitä käytänteitä kuvataan usein CIA-kolmiolla, jota on kuvattu kuviossa 2.



Kuvio 2. CIA-triad

Luottamuksellisuus tarkoittaa sitä, että vain valtuutetut osapuolet voivat päästä käsiksi tietoihin. Luottamuksellisuus suojaa arkaluonteisia ja henkilökohtaisia tietoja paljastumiselta luvattomille henkilöille, olivatpa he organisaation jäseniä tai ulkopuolisia. Eheys tarkoittaa sen varmistamista, että tieto on täydellistä ja oikeellista. Eheys suojaa sekä tahalliselta että tahattomalta manipuloinnilta, kuten luvattomilta lisäyksiltä, muokkauksilta tai poistamisilta. Saatavuus tarkoittaa, että valtuutetuilla käyttäjillä on pääsy tarvitsemiinsa tietoihin silloin, kun he niitä tarvitsevat. Saatavuus keskittyy järjestelmien ja prosessien toimintavarmuuteen häiriöiden tai käyttökatkosten estämiseksi. (Holdsworth & Kosinski 2024)

3.3 Kybertoimintaympäristö

Kybertoimintaympäristö on digitaalinen rinnakkaistodellisuus, joka käsittää digitaaliset verkostot, joiden kautta ylläpidetään nyky-yhteiskunnan elintärkeitä toimintoja. Nämä verkostot vaikuttavat muun muassa veden- ja energiantoimitukseen, pankkijärjestelmiin, terveydenhuoltoon ja liikenteeseen. Digitalisoituneessa maailmassa kaikki nämä toiminnot ovat olennaisia hyvinvoinnillemme ja siksi ne on suojattava asianmukaisesti. (Cyber security and the cyber domain n.d.)

Kybertoimintaympäristö eroaa muista toimintaympäristöistä siten, että se ei ole maantieteellisesti rajoitettu. Esimerkiksi palvelua ylläpitävät järjestelmät saattavat sijaita toisella puolella maapalloa, kuin sen käyttäjät. Jokainen järjestelmä on esimerkki kybertoimintaympäristöstä, kuten aiemmin mainittu pankkijärjestelmä tai liikenteen ohjausjärjestelmä. Tämän vuoksi kybertoimintaympäristön turvaaminen vaatii tiivistä kansainvälistä yhteistyötä. (Cyber security and the cyber domain n.d)

3.4 Hyökkäysvektorit

Hyökkäysvektori on reitti tai menetelmä, jolla uhkatoimija pyrkii saamaan luvattoman pääsyn verkkoon tai tietokoneeseen hyödyntämällä järjestelmä- tai ympäristötason haavoittuvuuksia. Esimerkkejä hyökkäysvektoreista ovat muun muassa kalasteluviestit, haitalliset verkkosivut, haittaohjelmat (esim. virukset tai kiristysohjelmat), väärät konfiguraatiot tai haavoittuvuudet. (What Is An Attack Vector? N.d.)

Hyökkäysvektorit voi jakaa kahteen eri kategoriaan: passiivisiin vektoreihin ja aktiivisiin vektoreihin. Passiivinen hyökkäysvektori, eli passiivinen hyökkäys, on hyökkäystekniikka, jossa uhkatoimija ainoastaan tarkkailee kohdejärjestelmää eri haavoittuvuuksia, kuten avoimia portteja tai haavoittuvia ohjelmistoversioita varten. Passiivinen hyökkäys ei häiritse tai muuta järjestelmää tai sen toimintaympäristöä millään tavalla mikä tekee sen havaitsemisesta vaikeaa. (Attack Vectors: What They Are and How They Are Exploited 2025.)

Aktiivinen hyökkäysvektori, eli aktiivinen hyökkäys, on hyökkäystekniikka, joka toisin kuin passiiviset hyökkäysvektorit, muuttaa tai häiritsee kohdejärjestelmää tai sen ympäristöä. Aktiivisen hyökkäysvektorin tarkoituksena on päästä käsiksi arkaluonteisiin tietoihin tai häiritä organisaation toimintakykyä aiheuttamalla kaaosta esimerkiksi tuhoamalla laitteistoa ja / tai dataa. Aktiivisiin hyökkäysvektoreihin kuuluvat muun muassa haittaohjelmat, kiristysohjelmat, palvelunestohyökkäykset (DDoS), tietomurrot ja laitteiden fyysinen tuhoaminen. (Attack Vectors: What They Are and How They Are Exploited 2025.)

3.5 Hyökkäys pinta-ala

Hyökkäyspinta-ala konseptina liittyy hyvin läheisesti hyökkäysvektoreihin. Hyökkäyspinta-ala tarkoittaa kaikkien haavoittuvuuksien, reittien ja menetelmien kokonaisuutta, joita uhkatoimija voi hyödyntää luvatonta pääsyä varten. Hyökkäyspinta-alan voi jakaa kolmeen pääluokkaan: digitaaliseen, fyysiseen ja sosiaaliseen hyökkäyspinta-alaan. Digitaalinen pinta-ala kattaa muun muassa tekniset haavoittuvuudet, väärät asetukset ja heikot salasanat. Fyysinen pinta-ala koskee organisaation fyysisiä tiloja ja resursseja vastaan kohdistuvia uhkia, kuten laitteistovarkaus, fyysinen tunkeutuminen laitteistotiloihin tai laitteiston fyysinen tuho. Sosiaalinen pinta-ala kattaa käyttäjien manipuloinnin organisaation tietoturvan rikkomista varten. (What is an attack surface? 2022.)

3.6 Kyberpuolustus

Kyberpuolustuksella viitataan eri tietojärjestelmien, verkkojen ja datan suojaamiseen eri kyberuhkilta, luvattomalta pääsyltä ja hyökkäyksiltä. Kyberpuolustuksessa hyödynnetään erilaisia käytäntöjä, strategioita ja teknologioita kuten uhkatiedustelua, tunkeutumisen havaitsemisjärjestelmiä (IDS), palomuureja, antivirus ohjelmistoja ja toimintaohjeita (Incident Response plan, IR) uhkien havaitsemiseen, estämiseen ja torjumiseen. (Poston 2025)

Kyberpuolustuksen voi jakaa kahteen pääluokkaan, ennakoivaan ja reagoivaan. Ennakoiva kyberpuolustus tarkoittaa proaktiivisten toimenpiteiden toteuttamista uhkien torjumiseksi ennen kuin nämä uhat toteutuvat. Tämä voi sisältää esimerkiksi haavoittuvuuksien etsintää, penetraatiotestausta, uhkien metsästystä tai tietoturvakoulutusta. Reagoiva kyberpuolustus keskittyy uhkiin reagoimiseen ja vastaamiseen, kun ne ovat jo tapahtuneet. Reagoiva kyberpuolustus kattaa toimenpiteet kuten tapahtumanhallinta (Incident Response, IR), digitaalinen forensiikka ja jälkiarviointi. (Cyber defense n.d)

4 Tekniset ratkaisut

4.1 Palomuuri

Palomuuri on tietoverkon turvallisuuslaite, joka erottaa kaksi tai useampaa verkkoa toisistaan hallitsemalla, miten verkkoliikenne voi kulkea näiden verkkojen välillä. Nämä erotellut verkot voivat esimerkiksi olla luotettu sisäinen verkko ja ulkoinen ei-luotettu verkko kuten internet. Nykyään monet tahot käyttävät kahta tai useampaa palomuuria muodostaakseen hallitumman erottelun ei-luotettujen ja luotettujen verkkojen välille. Esimerkiksi julkiset palvelut, joita käytetään internetin kautta, voidaan sijoittaa kahden palomuurin välille luotuun verkkoon.

Palomuurit ovat kriittinen osa verkkojen suojausta luvattomalta käytöltä ja / tai haitalliselta toiminnalta. Palomuureja on laitteistona sekä ohjelmistona. Vaikka mikä tahansa verkkoliitännällä varustettu laite voi toimia palomuurina oikealla ohjelmistolla, eri organisaatiot mieluiten käyttävät tarkoitusta varten rakennettuja palomuuriohjelmistoja ja laitteita maksimaalista suorituskykyä ja tehoa varten sillä verkkoliikenteen skannaus suurissa määrissä vaatii paljon resursseja ja laskentakykyä laitteelta.

Palomuuri säätelee verkkoliikennettä tarkastelemalla muun muassa verkkopaketin kohdetta, lähdettä ja protokollaa. Vertaamalla näitä asetettuihin sääntöihin, laite joko antaa paketin kulkea kohteeseen tai estää sen kulun. Tämä on palomuurin perustoiminto mutta nykyajan NGFW palomuurit tarjoavat myös lisäominaisuuksia kuten verkkopakettien syvätarkistuksen, jossa tarkastellaan paketin sisältöä haitallisen datan varalta tai lokien eteenpäin lähettäminen SIEM-järjestelmälle. (What is a firewall? N.d.)

4.1.1 ebtables

Ebtables on palomuuri- ja suodatustyökalu Linux-pohjaisilla käyttöjärjestelmillä, jonka avulla pystytään luomaan ja ylläpitämään sääntöjä Ethernet-kehysten käsittelyyn ja suodatukseen. Ebtables käyttää näiden kehysten suodatukseen tauluja, jotka sisältävät ketjuja ja ne puolestaan koostuvat säännöistä. Työkalu toimii OSI-mallin tasolla 2 (siirtoyhteyskerros), ja suodattaa ethernet kehyksiä ennen kuin ne etenevät tasolle 3 (verkkokerros). (Ebtables(8) – Linux man page n.d.) Ebtablesin rakennetta ja toimintaa kuvattu lyhyesti taulukossa 1.

Taulukko 1. ebtables rakenne

Käsite	**Selitys**
Taulu (table)	Kokoelma sääntöketjuja, joilla on tietty käyttötarkoitus. Tauluja on 3 kappaletta, filter, nat, ja broute.
Ketju (chain)	Joukko sääntöjä, joita sovelletaan tietyn tyyppiseen liikenteeseen. Jokaisessa ketjussa voidaan määrittää toimintatapa, kuten DROP tai ACCEPT.
Sääntö (rule)	Yksittäinen ehto ja toiminto – tarkastetaan esimerkiksi MAC-osoite, Ethernet-tyyppi tai VLAN-tunniste ja määritetään, mitä tehdään, jos ehto täyttyy.
Kohde (target)	Toiminto, joka suoritetaan, jos sääntö täsmää (esim. ACCEPT, DROP, CONTINUE, RETURN, DNAT, BROUTED).

Esimerkiksi tilanne, jossa halutaan estää liikenne tietystä MAC-osoitteesta, luotaisiin sääntö seuraavalla komennolla:

”sudo ebtables -A INPUT -s AA:BB:CC:DD:EE:FF -j DROP”

Luotu sääntö sijoittuu FORWARD-ketjuun, joka sijaitsee suodatus (filter) taulussa. Mikäli kyseinen MAC-osoite yrittäisi lähettää kehyksen verkon yli säännön luonnin jälkeen, poistettaisiin kehys eikä sitä välitettäisi eteenpäin verkkokerrokselle.

4.1.2 iptables

Iptables-työkalulla voidaan toteuttaa palomuureja ja reititystä. Se käyttää toimintaansa Linuxin kernelistä löytyvää Netfilter-pakettisuodatinta. Iptables toimii OSI-mallin tasolla 3 (verkkokerros) käsittelemällä IP-paketteja ja hallitsemalla niiden reititystä, suodatusta sekä muokkausta. (Ellingwood 2022.) Iptablesin toiminta ja rakenne on samankaltainen kuin ebtablesilla ja sitä on kuvattu lyhyesti taulukossa 2. (ks. taulukko 2)

Taulukko 2. iptables rakenne

Käsite	**Selitys**
Taulu (table)	määrittää käsiteltävien sääntöjen tyypin. Iptablessa on useita tauluja, joista jokaisella on eri tarkoitus.
Ketju (chain)	Sisältää joukon sääntöjä, joita sovelletaan tietyssä liikennevaiheessa. Jokaisessa ketjussa voidaan määrittää oletustoiminto (policy).
Sääntö (rule)	Yksittäinen määritelmä, joka koostuu ehdosta ja toiminnosta. Ehto kertoo, millaista liikennettä tarkastellaan, ja toiminto määrittää, mitä tehdään, jos ehto täyttyy.

Ehto (match)	Tarkasteltava kriteeri, joka määrittää, mitä paketteja sääntö koskee. Ehto voi perustua IP-osoitteeseen, porttiin, protokollaan, tilaan tai muuhun kenttään.
Kohde (target)	Toimenpide, joka suoritetaan, jos sääntö täsmää. Kohde kertoo iptablesille, mitä paketille tehdään.
Policy (oletustoiminto)	Ketjun oletustoiminto, jota sovelletaan, jos yksikään sääntö ei täsmää.

4.2 Sensori

Sensori, tai anturi, viittaa tämän työn kontekstissa laitteeseen ja / tai ohjelmistoon, joka monitoroi organisaation teknistä ympäristöä, joko verkkoliikennettä tai laitteiden paikallisia operaatioita, havaitakseen normaalista poikkeavia tapahtumia. Havaitut tapahtumat kirjataan lokiin ja välitetään keskitettyyn lokien hallinta- ja analysointijärjestelmään, kuten SIEM-järjestelmään.

Yleinen sensori implementaatio on ohjelmisto asennettuna päätekäyttäjän laitteella tai palvelimella, joka monitoroi järjestelmän eri aktiviteetteja kuten tiedostomuutoksia, käyttäjän valtuutustapahtumia ja verkkoliikennettä. Sensorit keräävät tapahtumalokia jatkuvasti eikä ainoastaan silloin kuin normaalista poikkeavia tapahtumia ilmenee. Myös normaalista toiminnasta toimitetaan lokit.

4.3 Lokienhallinta ja SIEM-järjestelmät

Lokien keräämisestä käytetään yleisesti termiä lokitus, joka tarkoittaa lokitietojen tallennusta ja hyödyntämistä. Lokitietojen avulla pystytään selvittämään vastaukset kysymyksiin mitä, milloin ja miksi, kun jotakin poikkeuksellista tapahtuu. Lokilla tarkoitetaan aikajärjestyksessä kirjattuja tallenteita tapahtumista ja niihin liittyvistä tiedoista. Näitä tapahtumia on muun muassa muutokset

ja tapahtumat tietojärjestelmissä, sovelluksissa, tietoverkoissa ja tietosisällöissä. Lokitietoa syntyy esimerkiksi tietokoneen keräämästä käyttölokista, verkon tapahtumista, ohjelmistojen pääsynvalvonnasta ja virhelokista. (Näin keräät ja käytät lokitietoa 2023)

Lokinkeruussa on otettava huomioon, että väärissä käsissä lokitiedosta voidaan saada tietoa, jota pystyttäisiin käyttämään pahantahtoisesti. Liian yksityiskohtainen tapahtumien seuranta saattaa myös rikkoa yksilöiden tietosuojaa, jos se on yhdistetty henkilöiden identiteetteihin. Lokista ei pääsääntöisesti tule löytyä tietoja kuten henkilötunnukset, luottokorttinumeroita, salasanoja, käyttöavaimia tai viestiliikenteen sisältöä. (Näin keräät ja käytät lokitietoa 2023)

Pelkkä lokien keruu ei kuitenkaan ole riittävää, sillä suurissa ympäristöissä tapahtumia syntyy valtavia määriä. Tämän vuoksi tarvitaan työkaluja, jotka pystyvät kokoamaan, yhdistelemään ja analysoimaan tietoa keskitetysti. Tähän tarkoitukseen käytetään SIEM-järjestelmiä (Security information and Event Management). SIEM-järjestelmät ovat tietoturvan hallintaratkaisuja, joita käytetään keräämään lokitiedot keskitetysti yhteen paikkaan, sekä normalisoimaan ne yhtenäiseen muotoon, joka mahdollistaa niiden tehokkaan analysoinnin. Järjestelmän avulla pystytään havaitsemaan poikkeamia, luomaan hälytyksiä mahdollisista hyökkäyksistä ja tukemaan tapahtumien jälkiselvittelyä.

SIEMin keskeisiä hyötyjä ovat reaaliaikainen tilannekuva, parempi reagointikyky sekä mahdollisuus täyttää viranomaisvaatimuksia lokien säilyttämisestä ja käsittelystä. Sen avulla lokitietoja voidaan tarkastella kokonaisuutena, joka paljastaa laajempia tapahtumaketjuja ja poikkeamia. Näin SIEM toimii keskeisenä työkaluna organisaation kyberturvallisuuden hallinnassa. (Näin keräät ja käytät lokitietoa 2023)

4.4 Julkisen avaimen järjestelmä ja TLS

Julkisen avaimen järjestelmä on kokonaisuus rooleja, sääntöjä, ohjelmistoja ja laitteistoja, joiden avulla hallitaan, jaetaan, käytetään, tallennetaan ja luodaan digitaalisia sertifikaatteja sekä julkisia digitaalisia avaimia. Näitä käytetään turvalliseen kommunikaatioon julkisissa verkoissa. PKI keskit-

tyy luottamuksen rakentamiseen asiakaskoneen, palvelimen ja varmentajan (Sertifikaattiauktoriteetti, Certificate Authority, CA) välillä. Julkisen avaimen järjestelmän tärkeyttä ei voi yliarvioida, sillä se on koko nykyaikaisen tietoverkon peruskivi, joka sallii luotetun kommunikaation ei-luotetuissa verkoissa.

Kun dataa siirretään julkisissa verkoissa, halutaan varmistaa, että siirretty data on salattu luottamuksellisuutta varten ja että molemmat osapuolet ovat tunnistettavia ja luotettavia. Jos data ei ole salattu, ulkopuolinen taho asiakaskoneen ja palvelimen välissä voi kaapata liikennettä ja nähdä mitä dataa siirretään. Jos molempien osapuolien luotettavuutta ei voida varmistaa, on mahdollista, että toinen osapuolista on vihamielinen toimija.

TLS eli Transport Layer Security on kokoelma turvallisuusprotokollia, joita käytetään turvallisen yhteyden muodostamiseen hyödyntäen PKI kehikkoa. Yleinen käyttötapaus TLS protokollalle on asiakaskoneella toimivien sovelluksien ja palvelimen välisen kommunikaation salaaminen sekä yksisuuntainen tai molemminpuolinen varmennus asiakaslaitteen ja palvelimen välillä hyödyntäen sertifikaatteja. (What is TLS (Transport Layer Security)? N.d.)

Riippumatta mihin käyttötarkoitukseen TLS sertifikaatti on luotu, se sisältää aina julkisen avaimen, digitaalisen allekirjoituksen ja metadataa koskien sertifikaattiin liitettyä identiteettiä ja mahdollista sertifikaattiauktoriteettia, joka on allekirjoittanut sertifikaatin. Sertifikaattiin sisällytetty julkinen avain on osa avainparia, johon kuuluu myös sertifikaatin luojan yksityinen avain. Yksityinen avain pidetään salassa ja julkisen avaimen voi jakaa muille. (What Is an X.509 Certificate? 2025.)

Koska sertifikaatit käyttävät epäsymmetristä salausta yksityisen avaimen omistaja voi digitaalisesti allekirjoittaa sertifikaatin yksityisellä avaimellaan. Tämän allekirjoituksen voi todentaa vain yksityistä avainta vastaavalla julkisella avaimella. Kun julkinen avain vastaa allekirjoitusta, tiedetään että sertifikaatin luoja omistaa julkista avainta vastaavan yksityisen avaimen. Nyt laite voi käyttää julkista avainta siirrettävän datan salausta varten ja vastaanottaja voi purkaa salauksen omalla yksityisellä avaimellaan. (Woods 2019)

Sertifikaatti on hyvä turvallisuustoimenpide mutta se varmistaa ainoastaan yhteyden salauksen, sertifikaatin omistaja voi silti olla pahantahtoinen toimija sillä sertifikaatissa oleva julkinen avain

voi silti olla epäluotettava. Tähän ratkaisuna toimii kolmannen osapuolen toimija eli sertifikaattiauktoriteetti (Certificate Authority, CA).

Esimerkiksi palvelimen sertifikaatin omistaja voi pyytää luotettua kolmatta osapuolta, eli sertifikaattiauktoriteettia, myös allekirjoittamaan hänen sertifikaattinsa. Tässä tilanteessa kaikki asiakaskoneet, jotka ottavat yhteyden palvelimeen varmistavat ensin palvelimen sertifikaatin ja sitten varmistavat CA:n digitaalisen allekirjoituksen. Jos molemmat allekirjoitukset varmistuvat onnistuneesti asiakaskone voi luottaa, että palvelin on legitiimi ja yhteyden saa salattua. Asiakaskoneen täytyy kuitenkin omistaa sertifikaattiauktoriteetin sertifikaatti erillisenä palvelimen sertifikaatista etukäteen ja sen täytyy luottaa sertifikaattiauktoriteetin sertifikaattiin.

4.5 OSI-malli

OSI-mallilla tarkoitetaan ISO:n vuonna 1984 julkaisemaa viitekehystä, jonka avulla on määritetty standardisoitu tapa, jolla applikaatiot, laitteet, ja verkot kommunikoivat keskenään. Malli määrittää viitekehyksen tiedon liikkumisen sen lähetyksestä vastaanottoon asti verkkoratkaisujen suunnittelun helpottamiseksi. (China & Goodwin n.d). OSI-mallin 7 kerrosta on kuvattu tarkemmin taulukossa 3.

Taulukko 3. OSI-malli

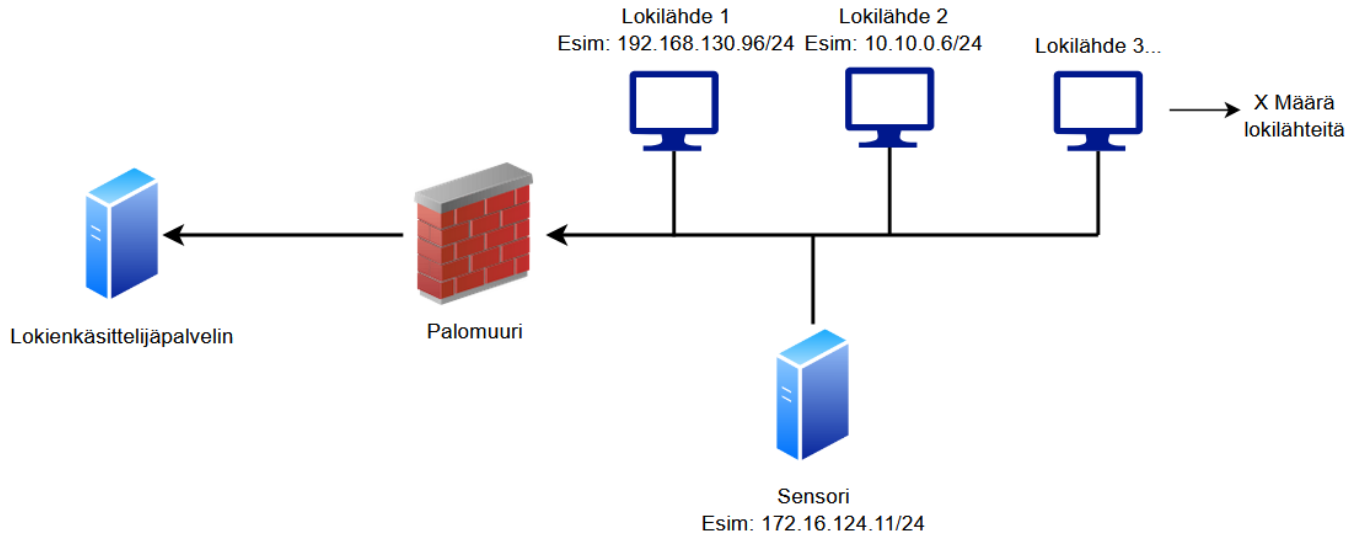
Taso	**Nimi**	**Kuvaus**	**Esimerkkejä**
7	Sovelluskerros	Rajapinta sovelluksille ja käyttäjälle. Määrittää miten ohjelmat käyttävät verkkoa ja kuinka data esitetään käyttäjälle.	HTTP, HTTPS, FTP, SMTP, DNS
6	Esityskerros	Vastaa tiedon esittämisestä, muunnoksista ja salauksesta. Huolehtii formaatin yhteensopivuudesta järjestelmien välillä.	SSL/TLS, JPEG, MPEG, ASCII

5	Istuntokerros	Vastaa yhteyden muodostamisesta, ylläpidosta ja lopettamisesta kahden laitteen välillä.	RPC, NetBIOS, SQL-istunnot
4	Kuljetuskerros	Vastaa datan siirron luotettavuudesta ja virheiden hallinnasta lähettäjän ja vastaanottajan välillä. Käytetty protokolla määrittää, kuinka yhteys muodostetaan ja miten tiedonsiirron eheys varmistetaan. TCP-protokolla varmistaa tiedon eheyden ja järjestyksen kuljetuksen aikana, kun taas UDP lähettää datan ilman yhteydenhallintaa tai virheentarkistusta.	TCP, UDP
3	Verkkokerros	Vastaa pakettien reitityksestä ja kuljetuksesta laitteiden välillä.	IP, ICMP, IPSec
2	Siirtoyhteyskerros	Vastaa tiedon siirrosta saman verkon laitteiden välillä fyysisen kerroksen yli käyttäen MAC-osoitteita.	Ethernet, kytkimet,
1	Fyysinen kerros	Määrittelee fyysisen tiedonsiirron laitteiden välillä bittitasolla käyttäen sähköisiä-, optisia-, ja radiotaajuuksia, sekä liittimiä ja kaapeleita.	Kaapelit, kuitu, verkkokortit, signaalit, bluetooth.

5 Toteutus

5.1 Ympäristön topologian ja fyysisten verkkoyhteyksien kuvaus

Kuviossa 3 esitetään kehitystyön aihetta varten toteutettava verkkotopologia. Kuvio 3 kuvaa vain rajattua osa-aluetta laajemmasta kokonaisuudesta johon työ keskittyy.



Kuvio 3. Fyysinen verkkotopologia

Lokienkäsittelijäpalvelin kerää tietoa ympäristöstä ja laitteista sille lähetettyjen lokien perusteella. Lokilähteet sekä sensori kytketään palomuuriin, jotta saadaan lisää suojausta lokienkäsittelijäpalvelimelle rajoittamalla verkkoliikennettä palvelimelle.

Palomuurin täytyy kyetä vastaanottamaan lokidataa eri lähteistä ja hyvin laajoista osoiteavaruuksista turvallisesti ja ilman että lokilähteiden yhdistäminen lokienkäsittelijäpalvelimeen on liian monimutkaista. Palomuuri toteuttaa tarvittavan reitityksen ja suojauksen.

5.2 Työnantajan vaatimukset toteutetulle konfiguraatiolle

Työnantaja asetti seuraavat geneeriset vaatimukset toteutetulle konfiguraatiolle, jotka listataan tässä.

1. Palomuuri suojaa lokienkäsittelijäpalvelinta vähentämättä muun ympäristön turvallisuutta.
2. Palomuuri reitittää lokidatan lokienkäsittelijäpalvelimelle.
3. Lokilähteitä on yksinkertaista lisätä konfiguraatioon ilman liiallista lokilähteiden tai muiden laitteiden konfigurointia.

Vaatimukset toteutetaan seuraavilla toimenpiteillä:

1. Palomuuriin konfiguroidaan vähintään säännöstö, joka estää liikenteen lokilähteiltä muualle kuin lokienkäsittelijäpalvelimeen laajemmassa kokonaisuudessa.
2. Palomuuri toimii myös reitittäjänä, lokilähteet kytketään suoraan palomuuriin.
3. Yhteys lokienkäsittelijäpalvelimen ja lokilähteiden välillä salataan ja turvataan implementoimalla TLS-protokolla. Tämä tarkoittaa sertifikaattiauktoriteetin luontia sekä yksittäisen sertifikaattien luontia lokilähteille ja palvelimelle.

5.3 Ympäristön valmistelu

Työnantajan käyttämä kybertoimintaympäristö koostuu kahdesta erillisestä laitekokonaisuudesta, joihin kuuluu muun muassa kytkimiä, sensori, palomuuri, sekä erinäisiä lokilähteitä. Ennen kuin työn aihe voidaan toteuttaa ympäristöön, tulee ympäristön fyysiset laitteet tietohuoltaa. Tämä tarkoittaa kaikkien laitteiden kiintolevyjen tietoturvallista tyhjentämistä, käyttöjärjestelmän uudelleenasennusta sekä laiteohjelmistojen päivittämistä ajan tasalle.

Tietoturvallinen muistilevyjen tyhjentäminen toteutettiin käyttämällä erillistä USB-käynnistysmediaa. Laitteet asetettiin käynnistymään USB-muistille tallennetusta käyttöjärjestelmästä, jonka avulla kiintolevyt tyhjennettiin siten, että tietojen palauttaminen ei ole mahdollista. Laiteohjelmistot päivitettiin samalla ulkoisella USB-medialla.

Ympäristön hallintaa varten otettiin käyttöön kaksi kannettavaa tietokonetta, joihin asennettiin Linux käyttöjärjestelmät. Käyttöönoton yhteydessä asennettiin myös hallinnointitehtävissä tarvittavat ohjelmistot, kuten SSH, tiedostojen pakkaamiseen ja purkamiseen käytettävä gzip, sekä muut komentorivityökalut ja apuohjelmat. Näitä laitteita käytettiin hallinnointitehtäviin työn toteutuksen ajan.

Ympäristön käyttöönoton alkuvaiheet ovat automatisoitu työnantajan käyttämän ohjelmiston avulla. Alkuvaiheen perustyöt saimme siis hoidettua suorittamalla kyseisen automatisointiohjelman, joka hoitaa muun muassa käyttäjien luonnin kohdelaitteeseen ja SSH-avaimen importoinnin. Näin varmistettiin, että hallintayhteys ympäristön laitteisiin voidaan toteuttaa turvallisesti ja toistettavasti.

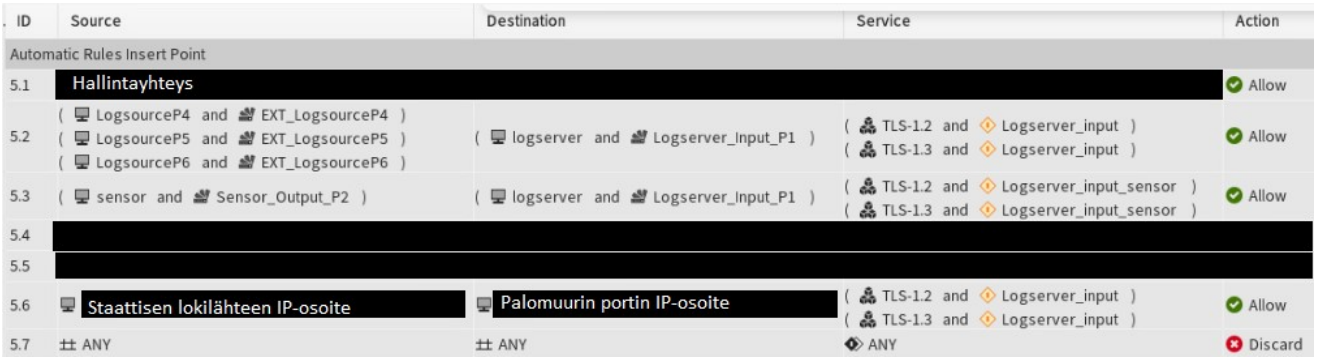
Tämän jälkeen siirryttiin yksittäisten palveluiden asentamiseen ja konfigurointiin niille varatulla palvelimella. Kun palvelut oli implementoitu, varmistettiin että palveluihin saadaan yhteys eivätkä jotkin verkkoasetukset estä yhteyttä. Kun ympäristön muut palvelut olivat valmiina ja konfiguroitu, aloitettiin tämän työn aiheen toteuttaminen ympäristössä.

5.4 Palomuurin käyttöönotto ja konfigurointi

Palomuuri asennettiin laitevalmistajan ohjeiden mukaisesti, jonka jälkeen siirryttiin kartoittamaan alustavia sääntöjä ja vaatimuksia palomuurille. Palomuurin kohdalla valmistauduttiin kahteen eri tilanteeseen koskien lokilähteitä. Voi olla tilanne, että lokilähde ei voi muuttaa IP-osoitetta tai kohdeporttia, jonne se lähettää lokia. Toisissa tilanteissa lokilähde voi muuttaa tätä lähetysosoitetta. Tämän takia luvussa 5.4.2 valmistetaan kaksi eri metodia lokien reititykseen, joita voidaan käyttää samaan aikaan tai erikseen. Lokilähteistä, jotka eivät voi muuttaa lokien kohdeosoitetta käytetään termiä **”staattinen lokilähde”**.

5.4.1 Palomuurin säännöt

Palomuurin säännöt (engl. access rules) määräävät mikä verkkoliikenne sallitaan ja minne. Päämääränä on mahdollistaa lokien vastaanottaminen ilman turvallisuusriskejä. Sääntöjä varten määriteltiin hallinnollisia elementtejä, jotka näytetään kuviossa 3 ja käsitellään tarkemmin taulukossa 4. Kuviossa 5 näytetään yhteyttä varten luotu TCP-palvelu, joka hallitsee tulevien yhteyksien kohdeportteja.

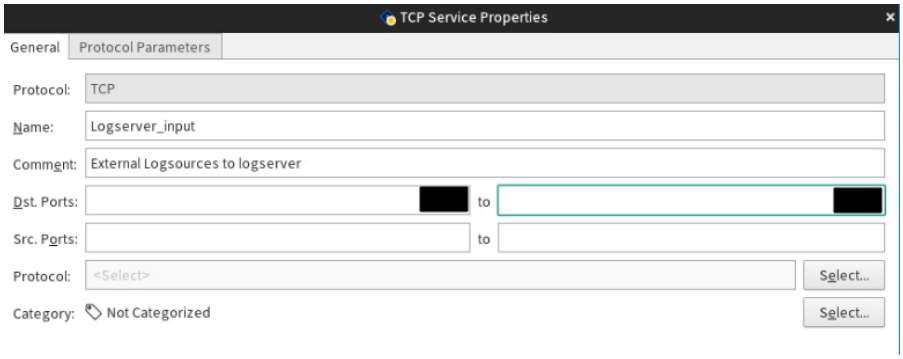


Kuvio 4. Palomuurin säännöt

Taulukko 4. Palomuurin sääntöjen hallintaelementit

LogsourcePX, esim. LogsourceP4	Elementit kuvaavat kolmea eri lokilähdettä ja jokainen elementti on yksi IP osoite.
EXT_LogsourcePX, esim EXT_LogsourceP4	Elementit hallitsevat palomuurin portteja ja niitä käytetään liikenteen hallinnassa. EXT_LogsourceP4 tarkoittaa palomuurin neljättä porttia. Sama P5 ja P6 varten.
logserver	Elementti, joka kuvaa lokienhallintapalvelinta ja sen arvo on kyseisen palvelimen IP osoite.
Logserver_input_P1	Hallinnollinen elementti, joka hallitsee palomuurin porttia 1 johon lokienkäsittelijäpalvelin on yhdistetty.

TLS-1.2 ja TLS-1.3	Suodatus elementtejä. Niillä viitataan palomuurin määritelmään TLS liikenteestä.
sensor	Hallinnollinen elementti, jonka arvo on IP-osoite. Kuvaa sensoria.
Sensor_Output_P2	Hallinnollinen elementti, jonka arvo on palomuurin portti 2.
Logserver_input, Logserver_input_sensor	Hallinnollinen elementti, jonka arvo on tietyt portit, joita lokienkäsittelijäpalvelin käyttää lokien vastaanottamiseen. Logserver input sensor on samanlainen elementti, joka sisältää sensorille varatut portit lokienhallintapalvelimella. (Ks. Kuvio 7)

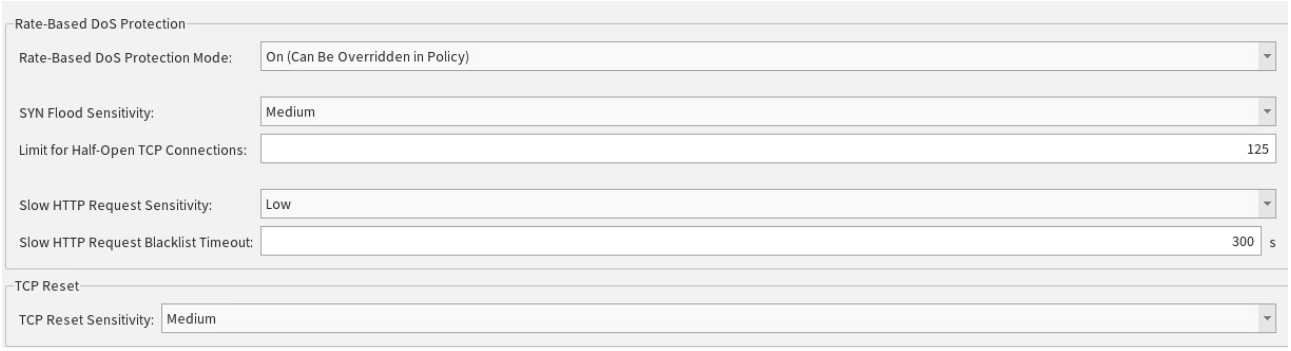


Kuvio 5. TCP-palvelu joka rajoittaa portteja

Palomuuri sallii lokilähteiden yhdistää lokienkäsittelijäpalvelimeen vain, kun lokilähde käyttää TLS protokollaa ja sen kohteena on vain tietyt portit, jotka on määritelty lokien vastaanottoa varten. Sen lisäksi liikennettä on rajoitettu porttien ja IP-osoitteiden perusteella. Esim. lokilähteen LogsourceP4 (IP-osoite) sisään tuleva verkkoliikenne sallitaan vain portista 4 (EXT_LogsourceP4). Liikenteen kohteeksi sallitaan vain porttiin 1 (Logserver_input_P1) yhdistetty lokienkäsittelijäpalvelin logserver (IP-osoite).

Sensoria koskevissa palomuurisäännöissä hyödynnettiin samaa logiikkaa. Sallitaan liikenne tietyltä IP-osoitteelta (sensorin IP) ja vain tietystä portista johon sensori on yhdistetty. Samat rajoitukset kuin muissakin lokilähteissä, vain TLS-liikenne tiettyyn IP-osoitteeseen (lokienkäsittelijäpalvelin) tietyn portin takana on sallittu.

Lopuksi estetään kaikki muu liikenne. Lähteenä ANY ja kohteena ANY. Näin estetään esim. lokilähteiden välinen kommunikointi, mahdolliset tunkeutumisyritykset hallintaverkkoon ja yleensäkin parannetaan turvallisuutta minimitoiminnallisuuden periaatteella. Samalla otettiin käyttöön palvelunestohyökkäyssuojaus. (Ks. Kuvio 6)

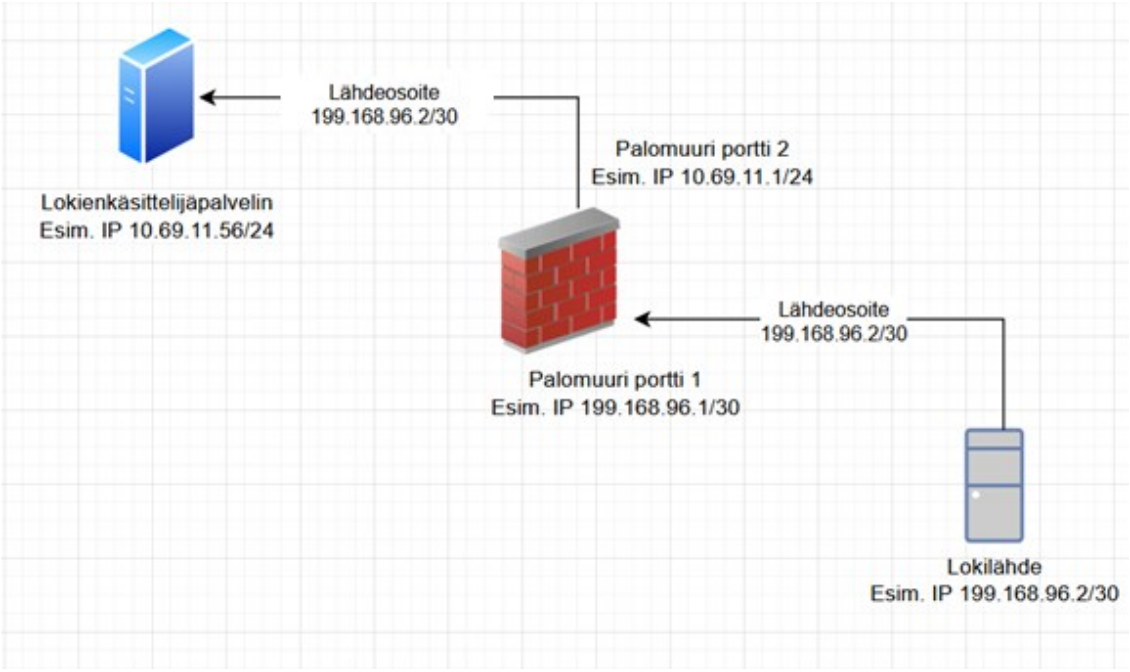


Kuvio 6. DoS-suojaus

5.4.2 Lokilähteiden reititys palomuurissa

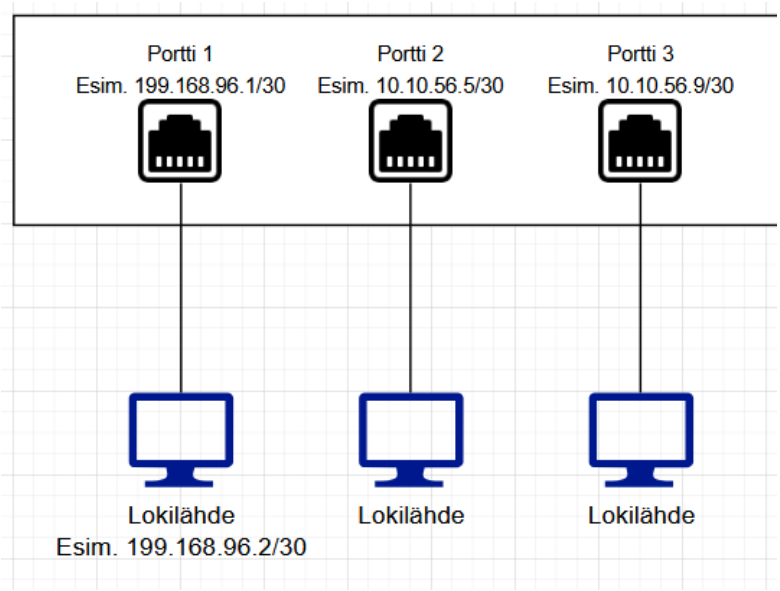
Lokien reititystä varten valmistettiin kaksi eri metodia, kuten kappaleessa 5.4 mainitaan. Molemmat metodit käyttävät staattisia reittejä mutta toinen hyödyntää NAT protokollaa. Metodi yksi perustuu siihen, että lokilähde konfiguroidaan lokienkäsittelijäpalvelimen IP-osoitteella vastaanottavaksi osoitteeksi. Toinen metodi perustuu siihen, että esim. reititys rajoitteiden vuoksi staattinen lokilähde ei voi muuttaa osoitetta, jonne se lähettää lokeja, joten palomuurin täytyy ottaa lokit vastaan. Tässä konfiguraatiossa molemmat metodit implementoidaan samaan aikaan. Edellisessä luvussa 5.4.1 määritellyt palomuurin säännöt ovat voimassa molempiin metodeihin.

Kuviossa 7 kuvataan metodia yksi, jossa palomuuri vastaanottaa verkkoliikennettä yhdistetyltä laitteelta, ja yksinkertaisesti reitittää liikenteen (jos se sallitaan sääntöjen perusteella) lokienkäsittelijäpalvelimelle. Näin yksinkertaistetaan konfiguraatiotarpeita lokienkäsittelijäpalvelimella ja ei tarvitse luoda erillistä reititystä tai muuntaa lokienkäsittelijäpalvelimen IP-osoitetta.



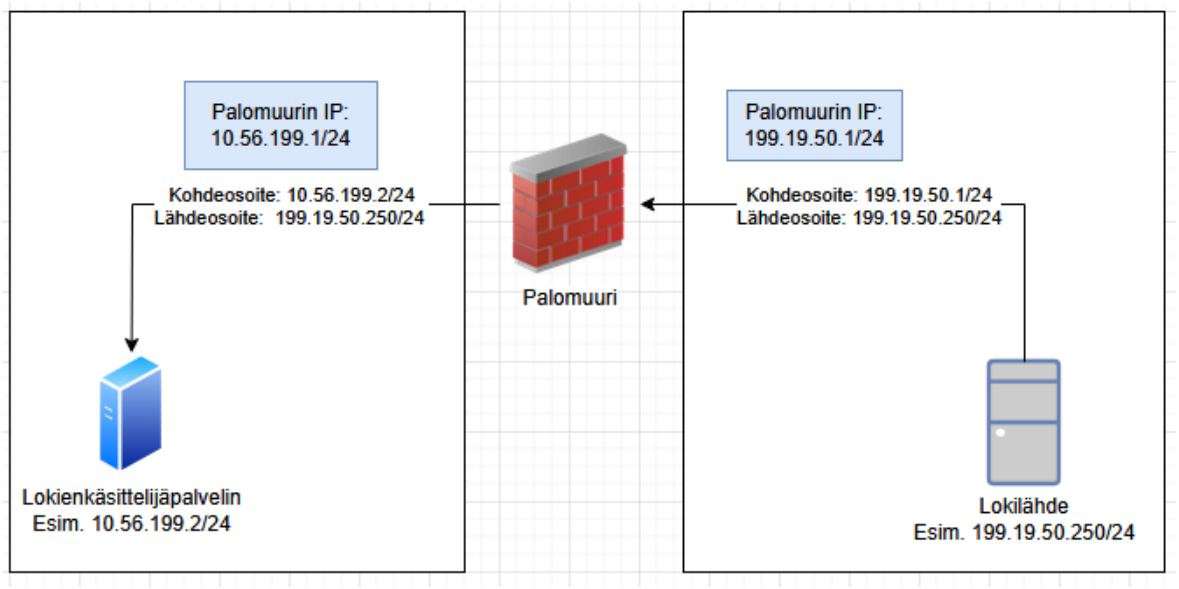
Kuvio 7. Staattinen reititys

Palomuuriin varattiin 3 porttia eri lokilähteitä varten ja näissä porteissa otettiin käyttöön DHCP-toiminnallisuus, konfiguraatio on näytetty kuviossa 8. Jokaiselle portille on määritelty tietty IP-osoite palomuurin asetuksissa ja IP-osoite, jonka se jakaa /30 aliverkosta liitetylle laitteelle. Näin vältetään mahdollisia yhteysongelmia koskien lokilähteen IP-osoitetta ja helpotetaan uusien laitteiden yhdistämistä. Lokilähteen hallitsijan tarvitsee vain joko manuaalisesti asettaa palomuurin /30 aliverkkoa vastaava IP-osoite lokilähteeseen tai antaa palomuurin jakaa osoite liitetylle laitteelle DHCP:n avulla.

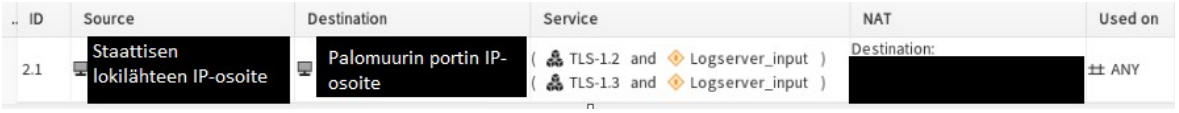


Kuvio 8. DHCP-konfiguraatio lokilähteitä varten

Metodin kaksi kohdalla staattinen lokilähde lähettää lokit tiettyyn osoitteeseen, jota ei voida muuttaa. Tässä tilanteessa lokilähde yhdistetään palomuuriin ja palomuurin verkkoportin IP osoitteeksi asetetaan se osoite, jonne staattinen lokilähde lähettää lokeja. Seuraavaksi pitää toteuttaa kohdeosoitteen reititys sillä staattisen lokilähteen näkökulmasta palomuurin pitäisi olla vastaanottava palvelin lokeja varten ja tämän takia yhteys terminoituu palomuuriin. Muuntamalla palomuurille saapuvan verkkoliikenteen kohdeosoitteen vastaanottavan portin IP-osoitteesta lokienkäsittelijäpalvelimen IP-osoitteeksi, palomuuri automaattisesti reitittää liikenteen palomuurin läpi. Kuviossa 9 näytetään esimerkki kohdeosoitteen muunnoksesta ja kuviossa 10 näytetään säännöt muunnosta varten.

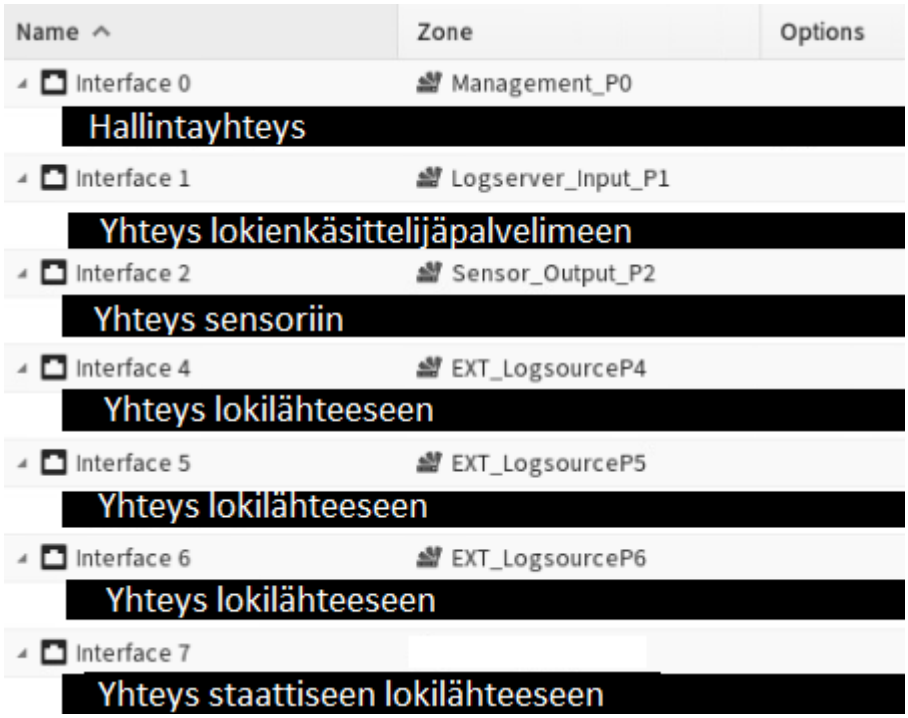


Kuvio 9. Kohde- ja lähdeosoitteen muunnos



Kuvio 10. NAT-kohdeosoitteen muunnos

Alla kuviossa 11 on vielä esimerkki täysin konfiguroidun palomuurin verkkoporteista. Normaaleihin lokilähteisiin on käytetty DHCP:tä ja staattista lokilähdettä varten porttiin on konfiguroitu staattisen lokilähteen käyttämä kohde IP-osoite.



Kuvio 11. Esimerkki konfiguroidun palomuurin verkkoporteista

5.5 Lokienkäsittelijäpalvelimen asennus ja konfigurointi

Lokienkäsittelijäpalvelimelle asennettiin Linux-pohjainen käyttöjärjestelmä sekä ohjelmisto lokien käsittelyä, vastaanottoa ja lähettämistä varten. Itse vastaanotettujen lokien käsittely hoidetaan käyttäen open-source lokienkäsittelyohjelmistoa.

Palvelimen ja lokilähteiden välinen kommunikaatio tulee salata, jotta varmistetaan ettei tietoon pääse käsiksi kuljetuksen yhteydessä, ja voidaan taata tiedon luotettavuus. Tämä toteutetaan TLS sertifikaattien avulla seuraavassa kappaleessa. Tämän jälkeen lokienkäsittelijäpalvelin konfiguroitiin vastaanottamaan tietoa vain tietyistä lähteistä palvelun konfiguraatiotiedostoa käyttäen sekä toteutettiin reititys ja paikallisen palomuurin konfigurointi.

5.5.1 TLS sertifikaattien luonti

Lokienkäsittelijäpalvelimella luotiin OpenSSL ohjelmistolla uusi sertifikaattiauktoriteetti (Certificate Authority, CA) jolla kaikki käytettävät palvelin- ja lokilähdesertifikaatit allekirjoitetaan, jotta molemmat osapuolet lokienvälityksessä voivat varmistaa toisensa identiteetit. Sertifikaatit (palvelin, asiakas, CA) ja kryptografiset avaimet rajoitetaan palvelimella vain lokien vastaanottoa varten.

Lokienkäsittelijäpalvelinta ja lokilähteitä varten luotiin omat 4096 bittiä pitkät kryptografiset avainparit ja TLS sertifikaatit varmennusta varten. Tulevat lokilähteet käyttävät omaa sertifikaattiaan sekä avainta autentikoidakseen itsensä lokienkäsittelijäpalvelimelle ja lokienkäsittelijäpalvelin autentikoi itsensä lokilähteille omalla sertifikaatillaan ja avaimella. Nämä avaimet ja sertifikaatit ovat kaikki luomamme CA:n allekirjoittamat ja näin saadaan toteutettua salattu yhteys lokidatan siirtoa varten ja identiteettien varmennus. Sertifikaattiauktoriteetin sertifikaatin asetukset ovat näytetty kuviossa 12.

```
[ req ]
distinguished_name = req_dn
x509_extensions = v3_ca
prompt = no

[ req_dn ]
CN = LogCA

[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always, issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign
```

Kuvio 12. CA-sertifikaatin asetukset

Tavoitteena oli luoda yksinkertainen sertifikaatti, joka ei tee muuta kuin allekirjoittaa muita sertifikaatteja ja todentaa itsensä, joista tärkein asetus on ”CA:true”. Asetuksien arvot ja tarkoitukset ovat kuvailtu tarkemmin taulukossa 5.

Taulukko 5. CA-sertifikaatin asetukset

Asetus	**Arvo**	**Tarkoitus**
subjectKeyIdentifier	Hash	Generoi tunnisteen julkisesta avaimesta. Tämä helpottaa sertifikaattiketjun hallintaa ja tekee tunnisteesta yksilöllisemmän.
authorityKeyIdentifier	keyid:always, issuer	Yhdistää sertifikaatin sen allekirjoittaneeseen auktoriteettiin. Mahdollistaa varmenteiden ketjutuksen.
basicConstraints	critical, CA:true	Määrittää sertifikaatin CA-varmenteeksi, jota voidaan käyttää muiden sertifikaattien allekirjoittamiseen. *Critical* tarkoittaa, että arvo täytyy vahvistaa.
keyUsage	critical, digitalSignature, cRLSign, keyCertSign	Rajoittaa, mihin sertifikaattia voidaan käyttää: allekirjoittamaan digitaalisesti, sertifikaattien revokointilistoja (CRL) sekä muita sertifikaatteja. *Critical* pakottaa tarkistuksen.

Kuviossa 13 näytetään lokienkäsittelijäpalvelimen sertifikaatin asetukset. Asetukset ovat laajalti samat kuin sertifikaattiauktoriteetin sertifikaatissa mutta muutamia asetuksia on muutettu. Sertifikaattiin lisätään DNS ja IP asetukset, joita käytetään TLS varmennuksessa. Lisätään myös ”CA:FALSE” arvo jotta sertifikaatti ei voi toimia sertifikaattiauktoriteerin sertifikaattina. Tarkemmat selitykset arvoista ja niiden tarkoituksista on taulukossa 6.

Kuvio 13. Palvelimen sertifikaatin asetukset

Taulukko 6. Palvelimen sertifikaatin asetukset

Asetus	**Arvo**	**Tarkoitus**
basicConstraints	CA: FALSE	asetuksella on määritetty, että palvelimen sertifikaatti ei saa toimia CA:na, vaan se on tarkoitettua ainoastaan varmennukseen. Tällä asetuksella estetään väärinkäyttö, jossa palvelinvarmenne allekirjoittaa muita sertifikaatteja virheellisesti.
nsCertType	server	Asetus korostaa, että sertifikaatti on palvelinkäyttöön tarkoitettu. Sisällytetty taaksepäistä yhteensopivuutta varten. Asetus on vain informaatioluontoinen.

subjectKeyIdentifier	hash	Sertifikaattiin lisätään tunniste, joka on generoitu sertifikaatin julkisesta avaimesta.
authorityKeyIdentifier	keyid,issuer:always	Linkittää sertifikaatin myöntäjään (CA). Tämä arvo tarkoittaa, että sertifikaatti sisältää CA:n tunnisteen (keyid) sekä sarjanumeron ja/tai nimen (issuer). Tämä parantaa tarkistettavuutta ja varmistaa oikean CA:n löytymisen tilanteissa, jossa on käytössä monia sertifikaatteja.
KeyUsage	critical, digitalSignature, keyEncipherment, dataEncipherment	Kentän asetukset määräävät mihin avainta voidaan käyttää. ”digitalSignature” tarkoittaa että avainta voidaan käyttää TLS-kättelytodennukseen (lyhytaikaisten avainten allekirjoittaminen, kättelyn tarkistaminen). ”keyEncipherment” arvolla mahdollistetaan RSA avainten vaihtaminen palvelimen ja asiakaslaitteen välillä suojattua yhteyttä varten. ”dataEncipherment” arvo on harvinaisempi tänä päivänä mutta sisällytetty jotta sertifikaatilla voidaan tarvittaessa salata lähetettävää dataa. ”digitalSignature” ja ”keyEncipherment” ovat tarpeellisia TLS liikennettä varten.
extendedKeyUsage	serverAuth	Ilmoitus, että varmenne on kelvollinen TLS-palvelimen todennukseen. Asiakaslaitteet tarkistavat tämän kentän varmistaakseen, että sertifikaatti voi varmentaa palvelimen.
subjectAltName	DNS, IP	Arvot DNS ja IP määrittävät sertifikaattiin palvelimen IP osoitteen sekä Fully Qualified Domain Namen (FQDN, esim. palvelin1.jamk.fi). TLS protokolla käyttää ”Subject Alternative Name” arvoja varmentamisessa, joten näin määritellään mitä osoitteita ja hostnameja varten sertifikaatti on validi.

Huomiona palvelimen sertifikaatissa on, että tilanteissa, joissa palomuuri toteuttaa kohdeosoitteen muunnoksen staattiselta lokilähteeltä tulevaan liikenteeseen, jotta se saavuttaisi lokienkäsittelijäpalvelimen, täytyy sertifikaattiin lisätä kohde IP-osoite, jota staattinen lokilähde käyttää. Koska staattinen lokilähde kuvittelee palomuurin olevan lokienkäsittelijäpalvelin, se odottaa palvelimen sertifikaatilta IP-osoitetta, jota se käyttää kohdeosoitteena mutta saa vain sertifikaattiin alun perin määritellyn lokienkäsittelijäpalvelimen oman IP-osoitteen. Korjaava toimenpide on muokata sertifikaatin asetustiedostoa, lisätä lokilähteen käyttämä IP-osoite lokienkäsittelijäpalvelinta varten ja luoda sertifikaatti uudelleen. Esimerkki tällaisesta korjauksesta on taulukossa 7.

Taulukko 7. Esimerkki muutoksesta palvelimen sertifikaatiin

[alt_names]
DNS = [FQDN]
IP.1 = [Lokienkäsittelijäpalvelimen oma IP]
IP.2 = [Staattisen lokilähteen käyttämä kohdeosoite]

Kuviossa 14 näytetään asiakassertifikaatin asetukset. Jälleen kerran, asiakaslaitteen sertifikaatti sisältää laajalti samat asetukset kuin palvelimen sertifikaatti, ainoastaan muunnettu niin että sertifikaattia voi käyttää vain TLS asiakasautentikointiin. Tämä saavutetaan extendedKeyUsage ja keyUsage arvoilla. Tarkemmat selitykset arvoista taulukossa 8.

```
basicConstraints = CA:FALSE
nsCertType = client
nsComment = "Logsource"
subjectKeyIdentifier = hash
authorityKeyIdentifier= keyid,issuer
keyUsage = critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation
extendedKeyUsage = clientAuth
```

Kuvio 14. Asiakaskoneen sertifikaatti asetukset

Taulukko 8. Asiakaslaitteen sertifikaatin asetukset

Asetus	Arvo	Tarkoitus
basicConstraints	CA: FALSE	Asetuksella rajaamme taas sertifikaatin käytön, tällä kertaa ainoastaan asiakasautentikointiin ja estämme allekirjoituksen väärinkäytön.
nsCertType	Client	Korostaa sertifikaatin tarkoitusta. Sisällytetty taaksepäistä yhteensopivuutta varten. Vain ilmoitusluontoinen.
subjectKeyIdentifier	hash	Arvo tarkoittaa, että sertifikaattiin lisätään tunniste (hash arvo), joka on generoitu sertifikaatin julkisesta avaimesta.
authorityKeyIdentifier	keyid,issuer	Toimii samalla tavalla kuin palvelimen sertifikaatissa. Se linkittää asiakas sertifikaatin sen myöntäjään (CA). Arvo sisältää CA:n avaintunnisteen (keyid) ja issuer-tiedot kuten nimi ja sarjanumero. Tämä parantaa tarkistettavuutta ja varmistaa oikean CA:n löytymisen.
keyUsage	digitalSignature, keyEncipherment, dataEncipherment, nonRepudation	Kentän asetuksilla saavutamme samat tavoitteet kuin palvelimen sertifikaatin kohdalla. ”digitalSignature” mahdollistaa TLS-käsittelyt, ”keyEncipherment” RSA avainten vaihdon ja ”dataEncipherment” sallii datan salaamisen. Uutena lisäyksenä on ”nonRepudiation” joka on

		enemmän oikeudellinen ominaisuus. Tämä arvo indikoi, että sertifikaatin haltija ei voisi kiistää allekirjoittaneensa lähetettyä viestiä. Tämä on lisätty asiakassertifikaattiin koska sen on pystyttävä todisteelliseen allekirjoitukseen ja avaintenvaihtoon.
extendedKeyUsage	clientAuth	Arvo määrittää, että sertifikaatti on tarkoitettu asiakasautentikoitiin TLS yhteydessä. Vastakohta palvelimen serverAuth arvolle. Ilman tätä arvoa palvelin ei hyväksyisi sertifikaattia asiakaslaitteen tunnistukseen.

Luomalla erillinen sertifikaattiauktoriteetti, erilliset avaimet sekä sertifikaatit rajoitetaan mahdollisen hyökkääjän kykyä aiheuttaa haittaa tilanteessa, jossa sertifikaattiauktoriteetti on hyökkääjän hallussa. Kaapattu sertifikaattiauktoriteetti mahdollistaa vain lokien lähetykseen tarkoitettujen sertifikaattien luonnin, eikä muita toimintoja varten. Lisäksi palvelin- ja lokilähde sertifikaatit ovat rajoitettu vain laitteen kyseistä roolia varten. Asiakassertifikaatit ovat rajoitettu asiakastunnistautumista varten ja palvelimen sertifikaatti on rajoitettu palvelintunnistautumista varten. Näin rajoitetaan mahdollisen kaapatun sertifikaatin käyttömahdollisuuksia, esimerkiksi palvelinsertifikaatilla ei voi tunnistautua lokienkäsittelijäpalvelimelle, joka olisi hyökkääjän kohde missä tahansa tilanteessa.

Lokienkäsittelijäpalvelimelle asennettiin myös paikallinen palomuuri tarkempaa yhteyshallintaa varten. Palvelimelle sallittiin hallintayhteys sekä tietyt IP-osoitteet ja portit, joita palvelin kuuntelee lokidataa varten. Yhteydet näihin portteihin rajoitettiin TLS-protokollaan, TCP-yhteyksiksi ja IP-osoitteet rajoitettiin tietyiksi IP-osoitteiksi, jotka ovat ennalta varattu lokilähteitä varten. Itse lokienkäsittelyohjelmisto asetettiin kuuntelemaan näitä sallittuja portteja sekä käyttämään vain TLS-

yhteyksiä, joissa molemmat osapuolet onnistuneesti autentikoivat samaa sertifikaattiauktoriteettia vastaan. Salaamattomia yhteyksiä tai lokilähteitä, jotka eivät onnistuneesti autentikoi ei sallita.

5.5.2 Lokienkäsittelyohjelmiston konfigurointi

Lokienkäsittelyohjelmisto konfiguroitiin ottamaan lokeja vastaan tietyillä porteilla ja jokaista porttia varten tehtiin oma konfiguraatio, riippuen siitä mitä formaattia tietyllä portilla odotetaan. Kuviossa 15 on esimerkki konfiguraatiosta yksittäistä porttia varten, joka ottaa vastaan ”json_lines” formaattista lokia.

```
input {
  tcp {
    port => Vastaanottava portti lokienkäsittelijäpalvelimella
    mode => "server"
    codec => "json_lines"
    proxy_protocol => false
    dns_reverse_lookup_enabled => false
    ssl_enabled => true
    ssl_certificate =>                                    server.crt"
    ssl_certificate_authorities => [                                ca.crt"]
    ##ssl_extra_chain_certs
    ssl_key =>                                  server_pkcs8.key"
    ##ssl_key_passphrase
    ssl_client_authentication => required
    ssl_supported_protocols => ["TLSv1.2", "TLSv1.3"]
    Tagit jotka lisätään vastaanotettuihin lokeihin
  }
```

Kuvio 15. Esimerkki lokienkäsittelyohjelmiston konfiguraatiosta

Konfiguraatioon määritellään kappaleessa 5.5.1 luodut palvelimen sertifikaatit sekä avaimet. Käytetään ”**ssl_client_authentication=>required**” asetusta jotta palvelin vaatii kaikkia lokilähteitä tunnistamaan itsensä sertifikaatilla. Jos kyseinen lokilähde ei onnistuneesti tunnista itseään asiakaslaitteen sertifikaatilla, yhteyttä ei muodosteta. Rajoitetaan TLS protokolla versioihin 1.2 ja 1.3 jotta vanhoja ja epäturvallisia versioita ei hyväksytä.

5.5.3 Reitityksen ja palomuurin konfigurointi

Lokilähteiden ja lokienkäsittelijäpalvelimen välinen verkkoliikenne pitää sallia paikallisessa palomuurissa ja reititys luoda manuaalisesti.

Luodaan staattiset reitit jokaiselle lokilähteelle.

- ***"[Lokilähteen aliverkko] saatavilla [Palomuurin IP-osoite samassa aliverkossa kuin lokienkäsittelijäpalvelin] verkkoportista X"***
    - ***esim. ip route add 99.99.99.0/24 via 1.1.1.1 dev ethX***

Toteutetaan palomuurin konfiguraatio myös.

- ***"Salli yhteys [Lokilähteen aliverkosta] [lokienkäsittelijäpalvelimen aliverkkoon] kun yhteys on TCP yhteys ja saapuu verkkoporttiin X"***
    - ***esim. input source 99.99.99.0/24 destination 1.1.1.0/24 protocol tcp port 1234***

Nämä toimenpiteet toteutetaan aina, oli lokilähde staattinen lokilähde tai lokilähde, jonka asetuksiin voimme vaikuttaa.

5.6 Sensorin käyttöönotto

5.6.1 Alustavat toimenpiteet

Sensori asennetaan erilliselle palvelimelle kuin lokienkäsittelijä. Tälle palvelimelle tehtiin samat toimenpiteet kuin muille eli kovalevyt tyhjennettiin, päivitettiin laiteohjelmistot ja asetettiin RAID toiminnallisuus valmiiksi.

Kovalevyjen tyhjennys toteutettiin erillisellä USB-medialla lataamalla käyttöjärjestelmä USB-laitteelta ja ylikirjoittamalla kovalevyt. Laiteohjelmiston päivittäminen toteutettiin konfiguroimalla FTP palvelu asennuskoneelle ja asettamalla palvelu isännöimään laiteohjelmistoja sisältävät kansiot. Sensorin BIOS asetuksissa määritettiin asennuskone palvelimeksi ja sieltä ladattiin laiteohjelmistot. Sensorin asennusohjelma hoiti kovalevyjen osioinnin ja virtuaalisten levyjen luonnin, joten

riittää että asetimme RAID-kontrollerin valmiiksi ja kaikki kovalevyt RAID-tilaan. Sensorin käyttöjärjestelmän asennusmediana toimii MicroSD-kortti, jonne asennus image kopioitiin Linuxin dd komennolla.

Sensorin hallintasivuna toimii sen IP osoite ***https://[sensorin IP-osoite]***

5.6.2 Automatiikan konfigurointi

Sensorin käyttöjärjestelmän asennus oli laajalti automatisoitu, joten voimme siirtyä palveluiden käyttöönottoon. Automatisointi ajetaan asennuskoneelta sensoriin ethernet yhteyden kautta.

Sensorille luotiin uusi sudo käyttäjä SSH hallintaa varten, avain kopioitiin käyttäjän sallittuihin avaimiin ssh-copy-id komennolla.

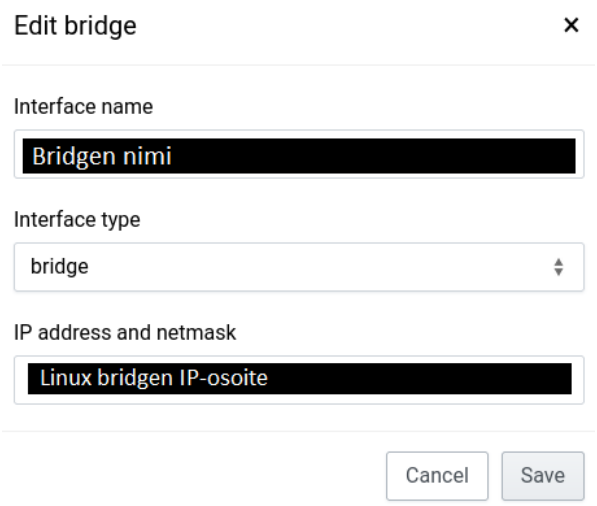
ssh-copy-id -i ~/.ssh/id_rsa.pub uusi_kayttaja@sensorin_ip

SSHD konfiguraatiosta estettiin root-käyttäjällä kirjautuminen lisäämällä rivit *PermitRootLogin* no ja PasswordAuthentication no tiedostoon /etc/ssh/sshd_config.

Työnantaja on kehittänyt automatisointia sensorin palveluiden asennusta varten, mutta nämä vaativat ensin manuaalista konfigurointia. Manuaalisesti määritettiin sensorin IP osoite ja hostname jotta automatisointi voidaan kohdistaa oikeaan laitteeseen. Seuraavaksi luotiin uusi salattu salasanaholvi, jonne tallennettiin sensoriin luodun käyttäjän salasana tunnistautumista varten sekä määritettiin yksityinen SSH avain, jonka julkinen puolisko on kopioitu sensoriin.

5.6.3 Lokien lähetyksen konfigurointi

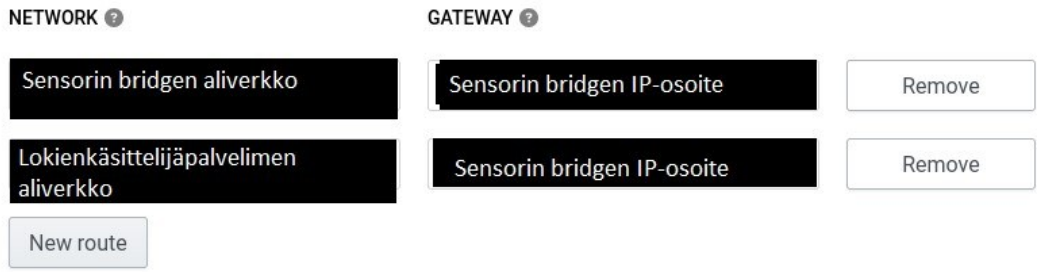
Sensorille luotiin ensin uusi virtuaalinen Linux bridge verkkoportti, jolle määritettiin IP-osoite. Lokien lähetystä varten luotiin erillinen virtuaalinen verkkoportti, joka liitettiin luotuun bridgeen. Viimeiseksi sensorin toinen fyysinen ethernet verkkoportti liitettiin juuri luotuun bridgeen. Bridgen ja sensorin lokityökalun asetukset ovat näytetty kuvioissa 16 ja 17.



Kuvio 16. Sensorin bridge

Kuvio 17. Sensorin lokityökalun verkkoliitäntä

Määritettiin myös staattinen reitti, jotta sensori osaa lähettää lokit palomuurille. Tämä täytyy tehdä, sillä lokienkäsittelijäpalvelin on eri verkossa kuin sensori ja haluamme lokien kulkevan palomuurin kautta. (Ks. Kuvio 18)



Kuvio 18. Sensorin lokityökalun staattiset reitit

Seuraavaksi määriteltiin itse kanava lokien lähettämistä varten, jonka asetukset ovat kuviossa 19. Lokityökaluun määriteltiin asiakassertifikaatti ja avain, joka luotiin kappaleessa 5.5.1. Määritellään myös sama sertifikaattiauktoriteetin sertifikaatti kuin muilla asiakaslaitteilla. Käytetään ”**ssl_verify=>true**” arvoa, jolloin sensori vaatii, että lokienkäsittelijäpalvelin autentikoi itsensä ennen lokien lähettämistä.

```
output {
  tcp {
    host => Lokienkäsittelijäpalvelimen IP osoite
    mode => "client"
    codec => "json_lines"
    port => Vastaanottava portti lokienkäsittelijäpalvelimella
    ssl_enable => true
    ssl_verify => true
    ssl_cert => [redacted]sensor.crt"
    ssl_key => [redacted]sensor.key"
    ssl_cacert => ["[redacted]ca.crt"]
  }
}
```

Kuvio 19. Sensorin lokityökalun konfiguraatio

5.6.4 Ongelma TLS sertifikaattien ja avaimien konfiguroinnissa

TLS yhteyden toteuttamiseksi sensorille tuotiin avain, sertifikaatti sekä CA sertifikaatti erillisen USB muistin kautta. Sensorin hallintasivulla määritellään, että jos halutaan lokityökalun käyttävän erillisiä tiedostoja näiden tiedostojen sisältö pitää syöttää verkkosivulle UTF-8 muodossa, josta lokityökalu tallentaa ne tiedostoiksi.

Tässä ilmeni kuitenkin ongelma. Kun verkkosivulle tallennettiin avaimet ja sertifikaatti, ne tallentuivat muistiin väärässä formaatissa, jolloin lokityökalu ei enää pystynyt lukemaan näitä tiedostoja ja kaatui.

Tämä ratkaistiin lopulta luomalla erillinen bash-skripti, joka yli kirjoittaa verkkosivulta luodut sertifikaatit ja avaimet oikein formatoiduilla versioilla. Skripti ajoitettiin suoriutumaan 5 minuutin välein. Skripti tarkastaa onko tiedosto olemassa ja vastaako sen sisältö oikein formatoitua sertifikaattia tai avainta. Skriptin sisältö on näytetty kuviossa 20.

```
#!/bin/bash
#File paths
TGT_DIR="Sensorin sertifikaattien ja avainten tallennus kansio"
SRC_DIR="Alkuperäisten settifikaattien ja avainten sijainti"

declare -A FILE_MAP=(
        ["Alkuperäisiet avaimet ja sertifikaatit"]="Kohde avaimet ja sertifikaatit"
        ["                    "]="                    "
)       Esimerkki: ["original_cert.crt"] = "korvattava.crt"

for src_name in "${!FILE_MAP[@]}"; do
    tgt_name="${FILE_MAP[$src_name]}"
    src_path="${SRC_DIR}/$src_name"
    tgt_path="${TGT_DIR}/$tgt_name"

    #if source doesn't exist, warn and skip
    if [ ! -f "$src_path" ]; then
        echo "$(date) ERROR: source file $src_path does not exist, skipping."  #>&2
        continue
    fi

    #if target doesnt exist, copy
    if [ ! -f "$tgt_path" ]; then
        echo "$(date) INFO: target $tgt_path does not exist. Copying from source."
        cp "$src_path" "$tgt_path"
        #[redacted]
        chown [redacted] "$tgt_path"
        continue
    fi

    #if target exists, check if contents differ
    #cmp is used for binary safe comparison
    if cmp -s "$src_path" "$tgt_path"; then
        #they are the same: do nothing
        :
    else
        echo "$(date) INFO: $tgt_path differs from $src_path : Overwriting"
        cp "$src_path" "$tgt_path"
    fi
done
```

Kuvio 20. Sertifikaattien korjaus skripti

Kuviossa 21 näytetään, miten skripti asetettiin ajettavaksi aina 5 minuutin välein käyttäen crontab työkalua. Skripti tuottaa lokitekstiä ”echo” komennon avulla ja tämä ohjataan /var/log/overwrite-certs.log tiedostoon jotta ohjelman toimintaa voi korjata ja seurata. Skriptin tuottamat virheviestit ohjataan samaan overwrite-certs.log tiedostoon ”2>&1” uudelleenohjauksella.

```
*/5 * * * * bash skriptin sijainti >> /var/log/overwrite-certs.log 2>&1
```

Kuvio 21. crontab

5.6.5 Reitityksen ja palomuurin konfigurointi

Luvussa 5.6.3 luotiin Linux bridge, virtuaalinen verkkoliitäntä ja staattiset reitit. Lokit saapuvat virtuaaliselle verkkoliitännälle, josta ne toimitetaan bridgeen reititystä varten, määriteltyjen staattisten reittien mukaisesti. Seuraavaksi konfiguroitiin näiden lokien reititys lokienkäsittelijäpalvelimelle. Tämä toteutettiin staattisilla reiteillä.

Sen lisäksi tehtiin erillinen paikallisen ohjelmistopalomuurin konfiguraatio koskien OSI-mallin kerroksen 2 ja 3 verkkoliikennettä. Verkkoliikenteen kulkua pyritään rajoittamaan lokityökalun virtuaalisen verkkoportin, virtuaalisen bridgen ja fyysisen verkkoportin kesken.

OSI mallin kerroksen 2 (Siirtoyhteyskerros) verkkoliikenne koostuu ethernet kehyksistä. Yleistä liikennettä tällä tasolla ovat ARP ja IPv4 protokollien liikenne. Kyseisen kerroksen liikennettä suodatamme ebtables ohjelmiston avulla. Toteutetut säännöt on selitetty taulukossa 9 ja konfiguraatio tiedosto näytetään kuviossa 22.

Taulukko 9. Ebtables konfiguraatio

Ketju	Hallitsee	Suodatus
INPUT	Itse virtuaaliselle bridge laitteelle kohdistettu liikenne.	Sallitaan liikenne sensorin fyysisestä verkkoportista ja sensorin lokityökalusta.
FORWARD	Liikenne, jota virtuaalinen bridge laite reitittää toiselle laitteelle.	Sallitaan liikenne sensorin lokityökalusta fyysiseen verkkoporttiin ja takaisin
OUTPUT	Paikallisesti generoitu liikenne, joka tulee bridge laitteesta.	Sallitaan bridge laitteen yhdistää sensorin lokityökaluun ja fyysiseen verkkoporttiin.

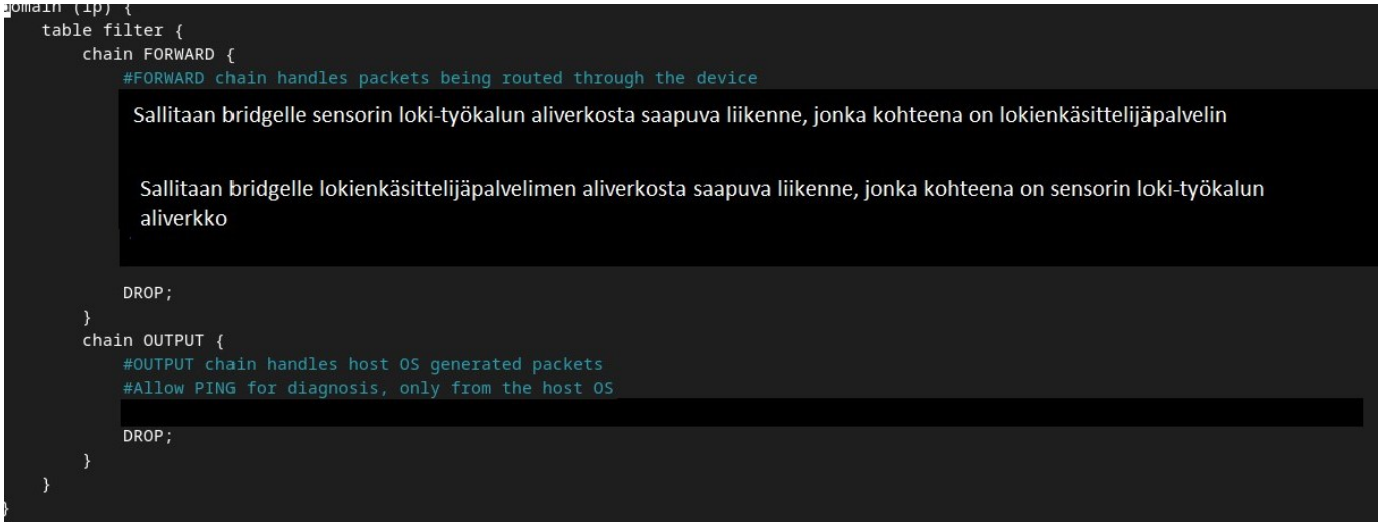
```
domain eb {
        table filter {
                chain INPUT {
                        policy DROP;
                        #input chain handles frames meant for the bridge itself.
                        Sallitaan layer-2 ethernet frame liikenne sensorin fyysisestä ethernet portista sekä sensorin loki-työkalun
                        portista itse bridgeen
                }
                chain FORWARD {
                        policy DROP;
                        #FORWARD chain handles frames forwarded by the bridge
                        Sallitaan layer-2 ethernet frame liikenne sensorin loki-työkalusta fyysiseen verkkoporttiin ja takaisin
                }
                chain OUTPUT {
                        policy DROP;
                        #OUTPUT chain handles locally generated frames. For example those created by the host OS
                        Sallitaan itse bridge laitteen yhdistää sensorin loki-työkaluun ja muihin laitteisiin jotka on yhdistetty fyysiseen
                        verkkoporttiin
                }
        }
}
```

Kuvio 22. Sensorin paikallinen 2- ja 3 kerroksen palomuuri

Iptables ohjelmiston avulla toteutettiin kolmannen kerroksen (Verkkokerros) verkkoliikenteen suodatus. Verkkokerroksessa liikenne koostuu eri protokollia noudattavista verkkopaketeista kuten IP-paketit eli toisinsanottuna sensorin lähettämät lokit. Taulukossa 10 selitetään palomuurisäännöt ja kuviossa 23 näytetään konfiguraatiotiedosto.

Taulukko 10. Iptables konfiguraatio

Ketju	**Hallitsee**	**Suodatus**
FORWARD	Verkkopaketit, jotka reitite-tään laitteen läpi.	Sallitaan sensorin lokityöka-lusta saapuva liikenne, jonka kohteena on lokienkäsittelijä-palvelin Sallitaan lokienkäsittelijäpal-velimelta saapuva liikenne, jonka kohteena on sensorin lokityökalu
OUTPUT	Paikallisesti generoidut verk-kopaketit.	Sallitaan ICMP protokollan lii-kenne Ping-toimintaa varten.



Kuvio 23. Iptables konfiguraatio

5.7 Kybertoimintaympäristön testaaminen

5.7.1 Lokilähteen testaaminen

Testilokilähteenä toimi kannettava tietokone Ubuntu 22.04 käyttöjärjestelmällä. Tietokoneelle asennettiin filebeat, joka konfiguroitiin keräämään kaikki lokit /var/log/ kansiosta ja lähettämään ne lokienkäsittelijäpalvelimelle.

Asiakaslaitteen sertifikaatit ja avaimet luotiin aikaisemmin lokienkäsittelijäpalvelimella kappaleessa 5.5.1 ja nämä avaimet ladattiin palvelimelta erilliselle USB muistitikulle, jolla ne siirrettiin kannettavaan tietokoneeseen. Filebeat asetettiin käyttämään asiakaslaitteelle tarkoitettua sertifikaattia ja avainta sekä samaa CA-sertifikaattia kuten palvelin. Filebeat konfiguraatio on kuviossa 24.

Kuvio 24. Client filebeat asetukset

Kannettava yhdistettiin palomuuriin, josta se sai IP osoitteen. TLS-yhteys testattiin komennolla *"**sudo filebeat test output**"* jonka ulostulo on näkyvillä kuviossa 25. Kun yhteys vahvistettiin toimivaksi, tarkastettiin myös lokienkäsittelijäpalvelimella lokidatan tilanne ja todettiin että lokidatan prosessointi toimii oikein.

Kuvio 25. Client filebeat testi

5.7.2 Sensorin testaaminen

Sensorin reititys testattiin Tcpdump työkalulla ja katsottiin että sensorin lokityökalu ja lokienkäsittelijäpalvelin saavat yhteyden, näytillä kuviossa 26. Kun yhteys varmistettiin toimivaksi, tarkistettiin uudelleen lokienkäsittelijäpalvelimella, että lokit vastaanotettiin ja prosessoitiin oikein.

Kuvio 26. Liikennettä sensorin ja lokienkäsittelijäpalvelimen välillä.

6 Tulokset

Kehitystyön tuloksena syntyi toimiva ja tietoturvallinen ympäristö, jossa palomuuri- ja sensori ratkaisut, salaukset sekä lokienkäsittelyratkaisut toimivat suunnitellusti. Lisäksi tuotettiin laadukas asennusdokumentaatio. Toteutettu kokonaisuus mahdollistaa verkkoliikenteen hallinnan, lokilähteiden kytkemisen ympäristöön vaivattomasti, sekä näkyvyyden parantamisen keräämällä ja keskittämällä sensorin lokit turvallisesti lokienkäsittelijäpalvelimelle. Sensorin asennus laajensi kokonaisuutta ja mahdollisti verkon tapahtumien tarkemman seurannan.

Testauksen perusteella ympäristö täytti sille asetetut tavoitteet. Verkkoliikenne kulkee hallitusti ja suodatetusti OSI-mallin 2. ja 3. kerroksissa hyödyntäen fyysistä palomuuria sekä paikallista ohjelmistopalomuuria. Luodut sertifikaatit ja avaimet toimivat oikein lokilähteiden, sensorin ja lokienkäsittelijäpalvelimen välisten yhteyksien TLS-salausta varten. Lokitietojen keruu lokilähteistä esimerkiksi Filebeat sovelluksella toimii ja näiden siirto lokienkäsittelijäpalvelimelle TLS-yhteydellä toimii. Sensori kerää verkkoliikenteestä omaa lokidataa onnistuneesti ja tämän lokidatan siirto lokienkäsittelijäpalvelimelle TLS-yhteydellä toimii. Testauksissa varmistui, että palomuurisäännöt estivät ei-toivotun liikenteen ja kaikki sallittu lokidataa sisältävä verkkoliikenne prosessoitiin lokienkäsittelijäpalvelimella oikein. Käytännön kokeiluissa ympäristön vakaus ja hallittavuus vastasivat tavoitteita, eikä merkittäviä suorituskykyongelmia ilmennyt.

Luotu asennusdokumentaatio ohjeistaa toimenpiteet, jotka on suoritettava ennen palomuurin ja sensorin asennusta sekä lokienkäsittelijäpalvelimen konfigurointia. Näihin toimenpiteisiin kuuluu

esimerkiksi laiteohjelmiston päivitys ja ympäristön muiden osien konfiguraatiota koskevat vaatimukset. Ohje sisältää laajalti samat tiedot kuin opinnäytetyö mutta tarkemmin kuvattuna, alkaen palomuurin tehdasasetusten palauttamisesta, uudelleenasentamisesta, sekä konfiguroinnista hallintaa ja lokilähteitä varten. Seuraavaksi asennusdokumentaatiossa käsitellään lokienkäsittelijäpalvelimen ohjelmiston, palomuurin ja TLS:n konfigurointi ja viimeiseksi ohjeistetaan sensorin käyttöönotto eli reitityksen, palomuurien sekä lokityökalun konfigurointi. Asennusdokumentaatio ja toteutettu ympäristö esiteltiin työnantajalle palautetta varten ja palautteen mukaiset muutokset tehtiin dokumentaatioon ja implementoitiin ympäristöön. Lopputulokseksi muodostui asennusdokumentaatio, jota on helppo seurata sekä hyödyntää. Dokumentaatiota voidaan helposti päivittää myös tulevaisuudessa, jos konfiguraatioon halutaan tehdä muutoksia.

Johtopäätöksenä voidaan todeta, että toteutettu kokonaisuus toimii hyvin kappaleen 5.7 testien mukaan ja on valmiina käyttöä varten työnantajan tarpeiden mukaisesti, sekä tarjoaa pohjan laajennettavalle kybertoimintaympäristölle.

7 Pohdinta

Opinnäytetyön aihe oli molemmille työn tekijöille hyvin mielenkiintoinen, minkä vuoksi päätimme toteuttaa työn yhdessä. Kahden henkilön toteutus toi kuitenkin mukanaan omat haasteensa, kuten työn laajuuden mitoittamisen kahden tekijän opinnäytetyölle sekä työn koordinoinnin ja vastuunjaon. Näistä syistä keskustelimme työnantajan kanssa työn laajuudesta ja päätimme laajentaa kokonaisuutta lisäämällä siihen sensorin asennuksen. Näin varmistettiin, että kokonaisuus vastasi laajuudeltaan kahden opiskelijan opinnäytetyötä ja tarjosi riittävästi sisältöä molemmille tekijöille.

Työn aihe tarkentui kesällä 2025, mutta käytännön toteutuksen aloittaminen viivästyi, ja pääsimme aloittamaan itse työn toteutuksen elokuussa. Vaikka varsinaista opinnäytetyöhön varattua laitekokonaisuutta ei saatu heti käyttöön, pystyimme hyödyntämään odotusajan tutustumalla käytettävään laitteistoon ja ohjelmistoihin muissa työpaikan projekteissa. Tämä auttoi ymmärtämään ympäristöä ja loi pohjaa varsinaisen työn toteutukselle. Laitteiston saavuttua pääsimme aloittamaan teknisen työn ja dokumentoinnin, jotka etenivät hyvässä aikataulussa. Noin kuukauden kuluttua viimeiset tekniset yksityiskohdat ja dokumentaatio olivat valmiit.

Kehitystyön toteuttaminen tarjosi hyvän mahdollisuuden soveltaa Jyväskylän Ammattikorkeakoulun opinnoissa opittuja asioita käytännössä. Työssä käsiteltiin koko laitteistokerrosta: fyysisestä kaapeloinnista ja laiteasennuksista aina palveluiden ohjelmistokonfigurointiin ja ongelmanratkaisuun saakka. Työ vahvisti erityisesti osaamista tietoverkkojen hallinnassa, tietoturvakonfiguraatioissa ja dokumentointikäytännöissä.

Opinnäytetyöprosessin aikana noudatettiin Jyväskylän ammattikorkeakoulun eettisiä ohjeita. Huolehdimme siitä, että lähteet on merkitty oikein raportointiohjeen mukaisesti ja että tekijänoikeuksia kunnioitetaan asianmukaisesti. Toimeksiantajan kanssa sovittiin, että työssä käsitellään ympäristöä yleisellä tasolla ilman sellaisia yksityiskohtia, jotka voisivat paljastaa yrityksen sisäisiä tietoja tai rakenteita.

Yhteistyö sujui kokonaisuudessaan hyvin, vaikka kahden tekijän työn yhteensovittaminen vaati säännöllistä kommunikointia ja työnjakoa. Molemmat pääsivät hyödyntämään omaa osaamistaan, ja prosessin aikana opittiin paljon myös projektinhallinnasta ja tiimityöstä. Toteutusvaiheessa suurimmat haasteet liittyivät teknisiin yksityiskohtiin, kuten laitekonfiguraatioihin, yhteensopivuusongelmiin ja palveluiden väliseen kommunikointiin. Joissain tapauksissa laitteiden ohjelmistoversiot ja rajatut käyttöoikeudet hidastivat etenemistä, mikä edellytti ongelmanratkaisukykyä ja itsenäistä selvitystyötä.

Jatkokehityksenä työlle voisi olla SOAR- ja SIEM-järjestelmien lisääminen ympäristöön, lokitiedon rikastuttaminen sekä hälytyssääntöjen luominen. Näiden avulla ympäristön tapahtumien näkyvyyttä voitaisiin parantaa ja poikkeamiin reagointia tehostaa. Lisäksi tulevaisuudessa voisi kehittää automaattisia raportointiratkaisuja, joiden avulla turvallisuustapahtumien seuranta ja analysointi olisi entistä tehokkaampaa.

Kestävä kehitys otettiin myös huomioon opinnäytetyön toteutuksessa muutamista eri näkökulmista, keskittyen teknisiin ratkaisuihin, dokumentaatioon ja fyysisiin laitteisiin. Toteutimme kestävää kehitystä käyttämällä vain olemassa olevia laitteita työn toteutuksessa, emme toteuttaneet uusien laitteiden hankintoja. Samalla näille laitteille on suunniteltu pitkä elinkaari, joka vähentää fyysisen tarvikkeen hankintoja tulevaisuudessa. Näin syntyy vähemmän SER-jätettä ja hiilijalanjälki pienenee.

Työssä hyödynnettiin myös virtualisointia, jonka avulla useita palveluita voitiin toteuttaa yhdellä fyysisellä palvelimella. Tämän avulla pystyttiin vähentämään fyysisten laitteiden tarvetta ja tekemään ympäristöstä joustavamman sekä energiatehokkaamman. Virtualisointi mahdollistaa myös järjestelmän helpon palauttamisen ja laajentamisen tulevaisuudessa, mikä tukee kestävää käyttöä ja hallittua kasvua.

Myös kyberturvallisuuden näkökulmasta työ tukee kestävää kehitystä parantamalla järjestelmien pitkäaikaista turvallisuutta. Hyvällä tietoturvan toteutuksella järjestelmän käyttöikä pitenee ja ylläpito vaatii vähemmän korjaavia toimenpiteitä. Näin resurssien kulutus vähenee ja teknologiaa voidaan hyödyntää pidempään. Lisäksi toteutuksen hyvä dokumentointi vähentää ylläpitotoimien kuluvaa aikaa ja kustannuksia.

Teknisten ratkaisuiden kohdalla hyödynnettiin paljon virtualisointia ajaakseen kehittävää kehitystä, tämä auttoi välttämään tarpeen uusille laitteille. Digitaalista kestävää kehitystä edistettiin keskittymällä vahvoihin kyberturvallisuuden ratkaisuihin, jotka tukevat yhteiskunnallista kestävyyttä tulevaisuuteen. Turvalliset tietojärjestelmät ovat välttämättömiä digitaalisessa yhteiskunnassa.

Lähteet

Attack Vectors: What They Are and How They Are Exploited. 2025. Crowdstrike. Crowdstrike verkkoartikkeli. Viitattu 06.05.2025. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/attack-vector/.

China C, Goodwin M. N.d. What is the OSI model? IBM Verkkoartikkeli. Viitattu 6.10.2025. https://www.ibm.com/think/topics/osi-model

Cyber defense. N.d. NordVPN. NordVPN:n julkaisema verkkoartikkeli. Viitattu 10.05.2025. https://nordvpn.com/fi/cybersecurity/glossary/cyber-defense/

Cyber security and the cyber domain. N.d. Ministry for Foreign Affairs of Finland. Ulkoministeriön verkkoartikkeli. Viitattu 07.05.2025. https://um.fi/cyber-security-and-the-cyber-domain.

ebtables(8) – Linux man page. N.d. linux.die.net verkkoartikkeli. Viitattu 25.10.2025. https://linux.die.net/man/8/ebtables

Ellingwood, J. 02.12.2022. How the Iptables Firewall Works. Verkkoartikkeli. Viitattu 25.10.2025. https://www.digitalocean.com/community/tutorials/how-the-iptables-firewall-works

Holdsworth, J., Kosinski M. 26.07.2024. What is information security? IBM verkkoartikkeli. Viitattu 10.05.2025. https://www.ibm.com/think/topics/information-security.

Jonker, A., Kosinski, M., Lindemulder, G. 12.08.2024. What is cybersecurity? IBM Verkkoartikkeli. Viitattu 9.6.2025. https://www.ibm.com/think/topics/cybersecurity

Näin keräät ja käytät lokitietoja. 06.03.2023. Verkkoartikkeli. Viitattu 29.08.2025. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja?toggle=Lokitus%20ja%20SIEM

Poston, H. 24.04.2025. What is cyber defense? Verkkoartikkeli, joka toimii johdantona kyber-puolustukseen. Viitattu 10.05.2025. https://cybersecurityguide.org/resources/cyber-defense/#:~:text=Cyber%20defense%20refers%20to%20the,and%20respond%20to%20cyber%20threats.

Strengthening Your Cybersecurity: The power of three P's in cybersecurity and Team Training. 24.08.2025. Verkkoartikkeli. Viitattu 29.9.2025. https://www.offsec.com/blog/the-power-of-three-ps-in-cybersecurity/

What is a firewall? N.d. Cisco. Ciscon verkkoartikkeli, jossa käsitellään palomuurien perusteita. Viitattu 05.05.2025. https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html.

What is an attack surface? 2022. IBM:n verkkoartikkeli, jossa käsitellään hyökkäyspintakonseptin yksityiskohtia. Viitattu 06.05.2025. https://www.ibm.com/think/topics/attack-surface.

What Is An Attack Vector? N.d. Fortinet. Fortinet verkkoartikkeli. Viitattu 05.05.2025. https://www.fortinet.com/resources/cyberglossary/attack-vector.

What Is an X.509 Certificate? 28.08.2025. Verkkoartikkeli. Viitattu 29.08.2025. https://www.ssl.com/faqs/what-is-an-x-509-certificate/

What is Cybersecurity?. N.d. Ciscon verkkoartikkeli. Viitattu 27.9.2025. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

What is TLS (Transport Layer Security)? N.d. Cloudflaren verkkoartikkeli. Viitattu 24.06.2025. https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

Woods, J. 21.06.2019. Understanding Public Key Infrastructure and X.509 Certificates. Verkkoartikkeli. Viitattu 10.8.2025: https://www.linuxjournal.com/content/understanding-public-key-infrastructure-and-x509-certificates