jamk

WatchGuard-palomuurin lokitus

Topi Niinijärvi

Opinnäytetyö, AMK
Joulukuu 2021
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Niinijärvi, Topi

WatchGuard-palomuurin lokitus

Jyväskylä: Jyväskylän ammattikorkeakoulu. Helmikuu 2021, 49 sivua.

Tekniikan ala. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Toimeksiantajana toimiva Isoweli Oy on ICT-alan yritys, joka toimittaa yrityksille kattavia ICT-palveluita.

Isoweli Oy tarvitsee käyttöönsä palomuurille tarkoitetun lokitusratkaisun. Yrityksen käytössä oleva ja jälleenmyyty WatchGuard-tuotemerkin Firebox nimeä kantava palomuurijärjestelmä tuottaa merkittävän määrän lokitietoa, jota ei käytetä hyödyksi.

Lokitietojen säilytyksessä tulee ottaa huomioon tiedon arkuus ja siihen liitetyt mahdolliset seikat. Lokitietojen siirtämiseen, käsittelyyn ja säilömiseen tarkoitetut palvelut ja kokonaisuudet tutkittiin kehittämistutkimuksen muodossa. Kyseinen kehittämistutkimus aloitettiin täysin puhtaalta pöydältä luomalla kaksi erilaista järjestelmää. Näiden kahden järjestelmän kesken vertailtiin niiden eroavaisuuksia ylläpidon, hallinnan ja ominaisuuksien muokattavuuden perusteella. Keskeisessä osassa on myös järjestelmien tarjoamien palveluiden peilaaminen tietoturvan eri osa-alueisiin.

Lopputuloksena saatiin vertailtua kahta erilaista palvelukokonaisuutta ja niiden tarjoamia ominaisuuksia. Lopputulosten perusteella saatiin ehdotettua toimeksiantajalle järjestelmistä koostuvaa kokonaisuutta, joka on mahdollinen toteuttaa heidän käyttämäänsä tuotantoympäristöön.

Avainsanat (asiasanat)

lokitiedostot, palomuurit, tietoturva

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Niinijärvi, Topi

WatchGuard firewall logging

Jyväskylä: JAMK University of Applied Sciences, February 2021, 49 pages.

Information and Communications Technology. Degree Programme in Information and Communications Technology. Bachelor's thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

Assigner of the thesis is Isoweli Oy. Isoweli Oy is an ICT company that provides comprehensive ICT services to companies.

Isoweli Oy needs a logging solution for a firewall. Isoweli is using and reselling WatchGuard Firebox firewalls. These firewalls generate significant amount of log information that is not utilized.

When storing log data, the sensitivity of the data must be considered carefully. Services and entities for the transfer, processing and storage of log data were studied in the form of a development study. The development study was started from a scratch by creating two different systems. The differences between the two systems were compared in terms of maintenance, management, and customizability of features. Mirroring the services provided by the systems to different aspects of cybersecurity is also a key part.

As a result, two different systems were created and compared between. Based on the results, a system was proposed to the client, which can be implemented in the production environment they use.

Keywords/tags (subjects)

log files, firewalls, cyber security

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenteet

AD	Active Directory
API	Application Programming Interface
EU	Euroopan unioni (European Union)
FTP	File Transfer Protocol
GB	Gigabyte
GDPR	General Data Protection Regulation
IP	Internet Protocol
JSON	JavaScript Object Notation
Katakri	Kansallinen turvallisuusauditointikriteeristö
LTS	Long Term Support
MB	Megabyte
REST	Representational State Transfer
SSH	Secure Shell
SSL	Secure Sockets Layer
VPN	Virtual Private Network
WAN	Wide Area Network

1 Johdanto

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi Isoweli Oy. Isoweli Oy on vuonna 1999 perustettu yritys, joka toimii ICT-alalla. Yritys työllistää reilut 50 henkilöä ja yrityksen päätoimipaikkana toimii Jyväskylä sekä Keski-Suomi. Sivutoimipisteet löytyvät myös Tuusulasta sekä Saarijärveltä.

Isoweli Oy tarjoaa asiakkaille kaikenkattavia ICT-ratkaisuja, jotka rakennetaan asiakkaan tarpeiden ja vaatimusten mukaisesti (Isoweli Oy n.d.)

1.2 Toimeksianto ja tavoitteet

WatchGuard-palomuurilaitteisto tarjoaa kattavaa lokitusta, jota voidaan hyödyntää tehokkaammin erillisen lokituspalvelimen avulla. Omien erilaisten suodattimien luomisella ja muokattavalla graafisella käyttöliittymällä on tiedon seuraaminen, tutkiminen ja analysointi käyttäjäystävällisempää. Lokituspalvelimen avulla pystytään myös helpommin kontrolloimaan lokitietojen säilytystä.

Toimeksianto suoritetaan Isoweli Oy:n suljetussa testiympäristössä. Testiympäristö on rakennettu Vmware ESXi -alustalle.

Toimeksiannon tavoitteina on selkeä sekä tehokas tapa kerätä lokitietoa Watchguard-palvelusta, säilöä tätä tietoa tietoturvallisesti ja tarvittaessa palauttaa tietoa 12 kuukauden ajalta. Lokitietojen tietoturvallisessa säilömisessä tulee ottaa huomioon GDPR:n (General Data Protection Regulation) asettamat säännökset. Toimeksiantaja on myös ottanut esille, että järjestelmien hallintaan liittyen tulee olla tarkkana. Erilaiset hallintaan liittyvät ominaisuudet järjestelmissä ovat kriittisiä, jotta järjestelmien käyttöä pystytään kontrolloimaan tehokkaasti.

2 Tutkimusasetelma

Opinnäytetyön tarkoituksena on rakentaa WatchGuardin tarjoamalle Firebox-palomuuriratkaisulle lokituspalvelin. WatchGuard tarjoaa omaa lokituspalvelinratkaisua, joka kantaa nimeä

WatchGuard Dimension. Firebox-palomuurit keräävät normaaliin tapaan lokitietoa, jonka lähettäminen edelleen myös toisenlaiseen, niin sanottuun avoimen lähdekoodin ratkaisuun on toteutettavissa.

Opinnäytetyö toteutettiin kehittämistutkimuksena. Työssä verrataan kahta erilaista ratkaisumallia toteutukselle, jotka kumpikin valmiina tuotteena tuovat yrityksen käyttöön uusia erilaisia työkaluja ja -menetelmiä työn helpottamiseksi.

Keskeisiä tutkimuskysymyksiä kahden erilaisen palvelun vertaamiselle olivat:

1. Kuinka palvelut eroavat eri osa-alueilla? (Ylläpito, hallinta, muokattavuus.)
2. Palveluiden peilaaminen Katakrissa (Katakri, Kansallinen turvallisuusauditointikriteeristö) määritettyihin vaatimuksiin

Kehittämistutkimuksen alkuvaiheissa pyritään rajaaman kehittämisen kohteena olevan asian muutostarpeet. Kohteen muutostarpeet ovat voineet tulla tietoon esimerkiksi kehitettävän tuotteen loppukäyttäjiltä. Kun erilaiset muutostarpeet tuotteelle on saatu rajattua, voidaan muutoksen mahdollistavat erilaiset vaihtoehdot rajata. Näiden vaihtoehtojen pohjalta rajataan taas haasteet, joita muutokset tuovat mukanaan. (Pernaa 2013).

Opinnäytetyön pohjana on, että yrityksellä ei ole käytössä erillistä lokipalvelinta tai -palvelua, josta voitaisiin käyttäjäystävällisesti erillisen portaalin kautta tutkia palomuurilla tapahtuneita lokitietoja. Nykyisellään lokitietojen tutkiminen vaatii erillisen kirjautumisen palomuurille ja lokitietojen raakadatan tutkimisen.

Kehittämiskohteena tuleva palvelu edesauttaa tiedon tulkintaa ja säästää näin myös työntekijöiden työaikaa, kun tieto on helpommin saatavilla.

3 Lokitus

3.1 Lokitus yleisesti

Lokituksella tarkoitetaan erilaisten lokitietojen tallentamista, näiden käsittelyä sekä hyödyntämistä. Toimenpiteen tarkoituksena on tuoda tukea tietoturvaan tarjoamalla mahdollisuutta tarkastella sekä tutkia erilaisia tapahtumia. Myös erinäisten virheilmoitusten lokittaminen helpottaa ongelmanratkontaa. Lokitietoja voidaan kategorisoida erilaisiin ryhmiin, kuten esimerkiksi ylläpito-, muutos-, virhe- ja käyttöloki. Edellä mainitut kategoriat ovat yleisimmät, mutta lokitietoja on mahdollista kategorisoida myös kerätyn tiedon luonteen ja laadun perusteella melko vapaasti. Lokitiedon muodosta, keräämistavasta tai laadusta huolimatta tulee erinäisiä lokitietoja käsitellä samalla periaatteella. (VAHTI 3/2009 Lokiohje.)

Lokitiedot sisältävät poikkeuksetta sellaista informaatiota, joka luokitellaan henkilötiedoiksi, on tällöin lokitietojen käsittelyssä ja säilömisessä noudatettava EU:n (Euroopan unioni, European Union) tietosuoja-asetusta. Esimerkiksi IP-osoite (Internet Protocol) on tietosuojalautakunnan vuonna 2006 antaman päätöksen mukaan pääsääntöisesti luokiteltavissa henkilötiedoksi. Kyseessä oli laaja tekijänoikeusrikkomuksiin liittyvä tapaus, jossa henkilöitä oli yhdistetty tapahtuneisiin tekijänoikeusrikkomuksiin saatujen IP-osoitteiden avulla. (Finlex 2006.)

Lokitietojen oikeaa määrää on vaikea hahmottaa ja kirjata etukäteen paperille. Lokituksen oikean tahdin ja määrän saa selville helpoiten, kun aloittaa lokituksen ja tarkkailee alussa tarkemmin lokituksen määrää ja tiedon laatua. Testausvaiheessa muutokset on helpompi tehdä järjestelmään, jolloin oikeaa ja tärkeää lokitietoa ei jää vahingossa puuttumaan muutosten takia. Testausvaiheessa on myös hyvä muistaa, että lokitustahtia ei ole syytä laittaa liian voimakkaaksi ensimmäisenä. Liian voimakkaalla lokituksella on mahdollista saada lokipalvelu tukkoon nopeasti.

Lokitietojen säilytyksestä ei ole laissa määritetty tarkkaa aikajaksoa, vaan säilytyksessä tulee huomioida säilytyksen kohteena olevan tiedon laatu ja sisältö. Näiden tietojen perusteella määritellään usein säilytysaika kuuden ja 24 kuukauden väliltä. Henkilötietoja tulisi säilyttää vain se aika, kun niiden käyttö on tarpeellista ja perusteltua. (Traficom 2020.) Lokitietojen säilytyksessä tulisi myös huomioida kyberuhkiin ja -hyökkäyksiin liittyvät lakiseikat. Esimerkiksi tietojärjestelmien häirintään liittyvä syyteoikeuden vanhentumisaika on viisi vuotta, kun taas törkeän tietojärjestelmän

häirinnän syyteoikeuden vanhentumisaika on 10 vuotta. (Viemerö, M. 2017.) Tällöin tiettyjen lokitietojen säilytykseen olisi hyvä varata paljon kapasiteettia ja resursseja, jolloin tietoja voidaan tarvittaessa kaivaa melkein kymmenen vuoden takaa vielä esille. Säilytykseen liittyviä resursseja tulee laskelmoida ja tarkkailla tarkasti, jotta kriittistä ja välttämätöntä dataa ei pääse inhimillisen virheiden takia katoamaan lainkaan.

3.2 Lokityypit

Lokityypit voidaan jakaa sisällön perusteella erilaisiin kategorioihin, ja ne voidaan tällä tavalla luokitella erilaisiksi lokityypeiksi. Lajittelun perusteella voidaan lokitietoja käsitellä eri tavalla, joka edesauttaa lokien selkeyttämisessä ja tulkitsemisessa.

Opinnäytetyössä käytettävä WatchGuard Firebox -sarjan palomuurilaitteisto luokittelee lokitiedot seuraaviin kategorioihin: palomuuri-, tietoverkko-, välityspalvelukäytäntö-, ylläpito- ja turvallisuuslokit. Myös laitteen omista palveluista pidetään lokia. Aiemmin mainitut kategoriat auttavat käyttäjää etsimään ja tutkimaan oikean aihealueen lokitietoja. Näiden otsikkotasojen alta löytyvät kyseiseen aihealueeseen liittyvät tarkemmat lokitiedot, joita on voitu rajata esimerkiksi liikenne-, hälytys-, tapahtuma-, virheenkorjaus- ja tilastolokeihin. (Log Message Catalog 2020).

Palomuuriloki on Firebox-laitteen itse tuottamaa lokia, jonka sisältä voi löytää esimerkiksi hälytyksiä kyberhyökkäyksiin liittyen. Tietoverkkolokit muodostuvat, kun palomuurin läpi kulkee liikennettä. Esimerkkinä tietyn rajapinnan läpi kulkeva liikenne generoituu tietoverkkolokien alle. Mikäli laitteelle on määritetty välityspalvelinkäytänteitä ja niiden perusteella liikennettä ohjataan, muodostuu siitä lokitietoja kyseiseen kategoriaan. Ylläpitoloki pitää sisällään laitteeseen itsessään liittyvät lokitiedot, joissa näkyvät käyttäjän kirjautumiset hallintaportaaleihin sekä näihin tehdyt muutokset.

4 Toteutuksen suunnitelmavaihe

4.1 Yleistä

Opinnäytetyö toteutetaan Isoweli Oy:n omassa suljetussa ympäristössä. Ympäristö on rakennettu VMware ESXi -virtuaalialustalle. Ympäristö on suljettu kokonaisuus, jonne on opinnäytetyön tekijälle myönnetty oikeudet pystyttää virtuaalisia palvelimia sekä päätelaitteita. Ympäristöstä on pääsy ulkoverkkoon erillisen virtuaaliverkon kautta, jotta ohjelmistojen lataaminen sekä päivittäminen onnistuu ilman, että näitä tulisi erikseen siirtää suljettuun ympäristöön.

4.2 WatchGuard

Opinnäytetyö pohjautuu Isoweli Oy:n käyttämiin ja jälleenmyytyihin WatchGuard Firebox-palomuureihin. Suljetussa toteutusympäristössä on käytössä WatchGuard Firebox-sarjan laite, jota ei täsmennetä tarkemmin opinnäytetyöhön.

WatchGuard on vuonna 1996 perustettu yhtiö, joka tarjoaa asiakkaillensa verkkoturvallisuuteen liittyviä ratkaisuja ja tuotteita. Yhtiön tarjoamat ratkaisut pitävät sisällään heidän omia fyysisiä tuotteitansa. Nämä fyysiset tuotteet pitävät sisällään erilaisia kokonaisuuksia, mutta näiden lisäksi tarjotaan laitteen rinnalle myös erinäisiä palveluita ja kokonaisuuksia. Yhtiön päämaja on Seattlessa, Yhdysvalloissa, ja se työllistää yli 1200 henkilöä. Yhtiön tarjoamat fyysiset palomuuriratkaisut kantavat tuotenimeä Firebox. (WatchGuard 2020.)

Palomuurilaitteistolta on tarkoitus ohjata lokitiedot erilliselle lokipalvelimelle, jossa tiedon luokittelu ja tutkiminen tapahtuu. Ratkaisut on kuvattu kappaleessa 4.3 Palvelut.

WatchGuard mahdollistaa lokien siirtämisen joko heidän omalle Dimension-alustallensa tai ulkopuoliselle lokipalvelimelle. Dimension-palvelusta enemmän otsikossa 4.3.2.

4.3 Palvelut

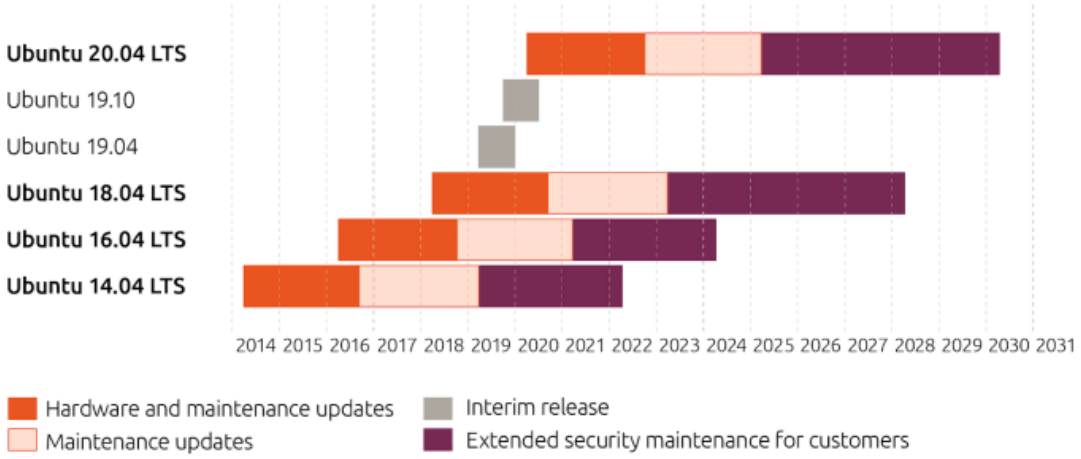
Lokipalvelimet toteutetaan erillisille Linux-palvelimille. Palvelinvalinnassa Windows-pohjainen ratkaisu ei tullut kysymykseen, koska tämä vaatisi erillisen lisenssin toimiakseen. Palvelut, joita toteu-

tuksessa on suunniteltu käytettäväksi, ovat rakennettu toimimaan Linux-pohjaisissa käyttöjärjestelmissä. Linux-palvelin vaatii myös virtuaaliympäristöstä annettavilta resursseilta huomattavasti vähemmän, kuin vastaava Windows-palvelin. Myöskään graafiselle käyttöliittymälle ei ole tarvetta. Käytettävä Linux-ratkaisu on lisensoitu GNU General Public License:llä, joka takaa käytön kaikille. Myös lähdekoodin kopiointi, muokkaus ja jakaminen on sallittu tällä lisenssityypillä. (GNU Operating System, 2020.)

Isoweli Oy:n testiympäristöön rakennettavassa ratkaisussa on tarkoitus kuvastaa kuitenkin aitoa tuotantoympäristöä, jolloin palvelut rakennetaan ja suunnitellaan sellaisiksi, kuin ne olisivat oikeassa käytössä tuotantoympäristössä. Palvelut rakennetaan tietoturvallisiksi ja niiden pystyttämisessä ja konfiguroinnissa otetaan huomioon ylläpito, kustannustehokkuus ja käytettävyys. Virtuaalialustan käyttö palvelimille takaa helpomman kustannustehokkuuden hallinnan, kun laitteille annettuja resursseja voidaan helposti muokata keskeytyksettä ilman, että oikeaa fyysistä palvelinrautaa joudutaan vaihtamaan.

4.3.1 Open source -ratkaisu

Palvelu rakennetaan Ubuntu Server 18.04 LTS -version (Long Term Support) päälle. Versio 18.04 on tuettu käyttöjärjestelmäpäivitysten osalta lähes vuoteen 2023 asti. Palvelun käyttöä on myös mahdollista jatkaa jatketulla tuella vuoteen 2028 asti. Versio 18.04 LTS takaa kuitenkin vielä hyvän tuen päivityksille, vaikka versionumeron korotus saattaa tulla ajankohtaiseksi nopeallakin aikataululla. Eri versioiden tukeen liittyvät tiedot katsottavissa Kuvio 1. (Ubuntu, 2021.)



Kuvio 1 Ubuntu Server -tuotteidein tuki (What is Ubuntu LTS release? 2020).

Ubuntu, eli Debian-pohjainen ratkaisu todettiin valinnaksi, koska opinnäytetyön tekijällä on aikaisempaa kokemusta kyseisestä käyttöjärjestelmästä aikaisempien kurssitoteutuksien muodossa. Vaihtoehtoinen valinta olisi ollut CentOS-pohjainen Linux-järjestelmä. Kyseisestä järjestelmästä ei tekijällä ole kuitenkaan yhtä kattavaa kokemusta ja tietoa, kuin Debian-pohjaisesta ratkaisusta.

Linux-palvelimelle otetaan käyttöön Fail2Ban-niminen ohjelmisto. Ohjelmisto tarkkailee palvelimen omia lokitiedostoja poikkeamien varalta. Mikäli ohjelmisto havaitsee haitaksi luokiteltavia epäonnistuneita kirjautumisyrityksiä, luo ohjelmisto palomuurisäännön kyseistä hyökkääjää kohtaan ja estää tämän pääsyn palvelimelle. Ohjelmisto on hyvin muokattavissa ja luo lisäturvaa palvelimelle. (Fail2Ban, 2016.)

Palvelinta pyritään myös koventamaan mahdollisimman paljon. Palvelimelta poistetaan turhat ohjelmistot sekä estetään palvelimen palomuurilta ei-tarvittavat yhteydet. Tarvittavat palomuurisäännöt voidaan toteuttaa myös käytettävältä WatchGuard-laitteelta. Linux-palvelimille rajataan pääsy pelkästään sisäverkosta SSH-yhteyttä (Secure Shell) käyttäen sekä vahvaa tunnistautumista hyödyntäen.

Linux-palvelimia pystytetään kaksi samaan verkkoon. Toisella palvelimella ajetaan avoimeen lähdekoodiin perustavaa Elastic-yrityksen ELK Stack -ohjelmistoa, ja toiselle palvelimelle pystytetään WatchGuard Dimension.

ELK Stack tulee sanoista Elasticsearch, Logstash ja Kibana. Nämä kolme muodostavat yhdessä ELK Stack -kokonaisuuden. Elasticsearch pohjautuu Apache Lucene -kirjastoon ja on hakukoneohjelmisto. Ohjelmiston ensimmäinen versio on julkaistu vuonna 2010. Elastic kuvailee ohjelmansa olevan tunnettu nopeuden, skaalautuvuuden ja yksinkertaisen REST (Representational State Transfer) API:n (Application Programming Interface) takia. (Elastic 2021.) Elasticsearch on DB-Engines-sivuston hakukoneohjelmistojen listauksessa sijalla yksi. (DB-Engines, 2021.) Logstash on osa ELK-kokonaisuutta, joka mahdollistaa datan keräämisen ja siirtämisen. Ohjelman avulla data kulkeutuu Elasticsearch-ohjelmaan. Kibana takaa visuaalisen kokonaisuuden, johon on mahdollista aiempien ohjelmien syöttämän datan pohjalta luoda erilaisia visualisointeja.

4.3.2 WatchGuard Dimension

Toiselle palvelimelle pystytetään WatchGuardin tarjoama Dimension, joka on suoraan ladattavissa heidän omilta sivuiltaan. Dimension vaatimuksena on, että se pyörii täysin virtuaalisella alustalla. Ohjelmistokokonaisuuden lataaminen ei vaadi kirjautumista tai tarkempaa lisenssin ostamista, mutta lokitietoja lähettävästä palomuurilaitteistosta on löydyttävä aktiivinen ”Support”-tason tilaus. Tilauksen tason Dimension saa selville hakemalla tiedon erilliseltä services.watchguard.com-sivustolta. Ohjelmaa ei saa ladattua erillisenä, vaan se tulee kokonaisuutena käyttöjärjestelmän kanssa. Dimension on mahdollista asentaa VMware- sekä Hyper-V-alustoille.

Dimension koostuu neljästä pääkomponentista, jotka ovat lokien kerääjä, palvelin, lokien tietokanta sekä web-palvelu. Lokien kerääjä vastaanottaa erilaiset lokiviestit eri WatchGuard-tuoteperheen tuotteilta ja koostaa näistä tietoa web-palveluun sekä erilaisiin raportteihin. Palvelin tarjoaa järjestelmälle hallintasovelluksen sekä rajapinnan lokitiedoille. Tietokanta on sisäänrakennettuna järjestelmässä ja se on PostgreSQL-pohjainen tietokanta. Dimensionjärjestelmässä on myös mahdollista siirtää lokitietojen kopiot erilliselle PostgreSQL-pohjaiselle tietokannalle. Dimension mahdollistaa myös lokitietojen varmuuskopioinnin, mutta vaihtoehdot ovat melko suppeat, eikä niihin saa täyttä kontrollia ja kiertoa. Web-palvelu on järjestelmän tarjoama web-pohjainen graafinen käyttöliittymä, joka mahdollistaa palvelun hallinnoinnin sekä lokitietojen selaamisen.

4.3.3 Palveluiden suojaaminen

Järjestelmien ja palveluiden käytössä ja hallinnoinnissa on käytetty pohjana yrityksen omia arvoja. Näitä arvoja kuitenkin on verrattu esimerkiksi Katakriin, tietoturvallisuuden auditointityökaluun viranomaiselle. Katakri, koko nimeltään kansallinen turvallisuusauditointikriteeristö, on hallituksen turvallisuuteen liittyvä ohjelmisto. Ensimmäinen versio Katakrista on julkaistu vuonna 2009, ja se on valmistunut puolustusministeriön johdosta. Ensimmäisen version jälkeen on Katakrin päivittämisestä ollut vastuussa sisäministeriö, mutta vuoden 2014 jälkeen vastuussa on ollut ulkoministeriössä toimiva Kansallinen turvallisuusviranomainen. (Katakri, 2020.)

Katakrin osa-alueen I: teknisen tietoturvallisuuden alaisuudesta löytyvistä vaatimustasoista saadaan muodostettua kattava pohja opinnäytetyössä käytössä oleville palveluille. Opinnäytetyössä toteutetaan kaksi erilaista palvelua, joiden kesken verrataan paljolti Kataktrin antamia vaatimuksia. Näitä vertailuja tekemällä saadaan Isoweli Oy:lle varmistettua tietoturvallinen ja toimiva palvelukokonaisuus.

Tärkeinä pääpiirteinä on palveluissa esimerkiksi käyttäjille annettavat rajoitukset. Palveluissa käytössä olevat liialliset käyttöoikeudet eivät ole tarpeellisia, mikäli käyttötarkoitus palvelussa on esimerkiksi pelkästään tiedon lukeminen. Tällöin tunnuksella ei ole tarvetta tehdä muutoksia itse palveluun ja siihen liitettyihin palveluihin. Katakri ”I-06 Vähimpien oikeuksien periaate – pääsyoikeuksien hallinnointi” -kohdan toteutusesimerkkejä voidaan pitää hyvänä pohjana käyttäjiin kohdistuvissa käyttöoikeusmenetelmissä (Katakri, 2020).

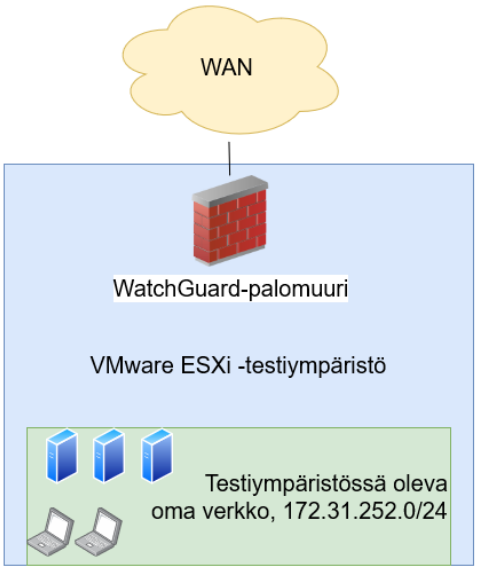
Myös palveluiden alustana toimivina palvelinratkaisuissa tulisi hyvä ottaa huomioon Katakrin kohta ”I-08 Vähimmäistoimintojen ja vähimpien oikeuksien periaate – järjestelmäkovennus”. Palvelualustoissa ei tulisi pyöriä erinäisiä palveluita, mikäli niiden käytölle ei ole esimääritettyä tarvetta. Ylimääräiset palvelut luovat järjestelmään enemmän uhkia ja mahdollisia tietoturva-aukkoja. Näiden eliminointi asennusvaiheessa on suotavaa, mikäli tarvetta käytölle ei ole. Käytettyjen palveluiden auditointi ja koventaminen on tarpeen niille osa-aluille, mitkä jätetään käyttöön. (Katakri, 2020).

Isoweli Oy:lle tuotetussa opinnäytetyössä palvelut rakennetaan suojattuun ympäristöön, johon ei ole pääsyä ulkoverkosta ilman käyttäjään kohdentuvaa autentikointia SSL (Secure Sockets Layer)

VPN-yhteyden (Virtual Private Network) avulla. Tämä ei kuitenkaan poista järjestelmien osalta auditointia palveluille, jotka ovat alttiita ulkomaailmasta tuleville hyökkäyksille. Palvelu toteutetaan niin, että sen käyttö ja ylläpito on täysin tietoturvallista palvelun ollessa saatavilla ulkoverkosta käsin.

5 Tekninen toteutus

Teknisen toteutuksen pohjaksi on opinnäytetyön tekijälle luotu erilliseen VMware-ympäristöön tunnukset, jotka mahdollistavat virtuaalikoneiden luonnin sekä hallinnoinnin. Testiympäristö on suljettu kokonaisuus, joka koostuu virtuaalialustasta, ympäristön omasta palomuurista ja virtuaalialustalla pyörivistä virtuaalilaitteista. Testiympäristön palomuurille on myös luotu työtä varten oma aliverkko 172.31.252.0/24. WatchGuard Firebox -palomuurilaitteisto löytyy aliverkon IP-osoitteesta 172.31.252.1. VMware-ympäristössä on määritetty pääsy kyseiseen verkkoon virtuaalisen kytkimen kautta ja kyseinen aliverkko kantaa verkkolaitteiden adaptereissa nimeä ”IW_TopiN_NW”. Verkosta on sallittu liikenne ulkomaailmaan, mutta ulkomaailmasta ei ole pääsyä ympäristössä oleviin laitteisiin ilman SSL VPN -yhteyttä. Opinnäytetyötä varten on palomuurille luotu myös SSL VPN -yhteyttä varten tunnukset. WatchGuard-palomuurille on luotuna myös erilliset katselu- sekä konfigurointitunnukset. Testiympäristön palomuurille on luotu sääntö, joka sallii Firebox-laitteesta lokitietojen lähettämisen. Testiympäristöä havainnollistava kuva nähtävissä Kuvio 2.



Kuvio 2 Käytettävä testiympäristö (WAN, Wide Area Network)

Lokitiedot kertyvät ja lähtevät Firebox-laitteesta sen perusteella, onko käytössä oleviin palomuurikäytäntöihin määritetty lokitus päälle. Testiympäristön Firebox-laitteelle on määritetty tiettyihin käytänteisiin lokitukset päälle, jotta opinnäytetyötä varten saadaan kerättyä lokitietoja. Vaikka kyseessä on testiympäristö, ei opinnäytetyötä varten haluta käyttää kaikkia palomuurin verkkoliitäntöjä ja käytänteitä datan kertymistä varten.

Dimension-järjestelmä vaatii myös erilliset käyttäjätunnukset palomuurille. Tätä varten palomuurille on luotu erilliset tunnukset, jotka liitetään Dimension-järjestelmään.

5.1 Dimension-järjestelmä

5.1.1 Palvelun pystytys

Toteutushetkellä Dimension-järjestelmä kantaa versionumeroa 2.2 ja se on julkaistu kesäkuun 2. päivä. Järjestelmän pystytystä varten on WatchGuard ilmoittanut asennusohjeiden ohella, kuinka määrittää riittävä määrä muistia kyseiselle palvelulle, katso Taulukko 1.

Taulukko 1 Dimension-järjestelmän muistin määritys (Install WatchGuard Dimension, 2021.)

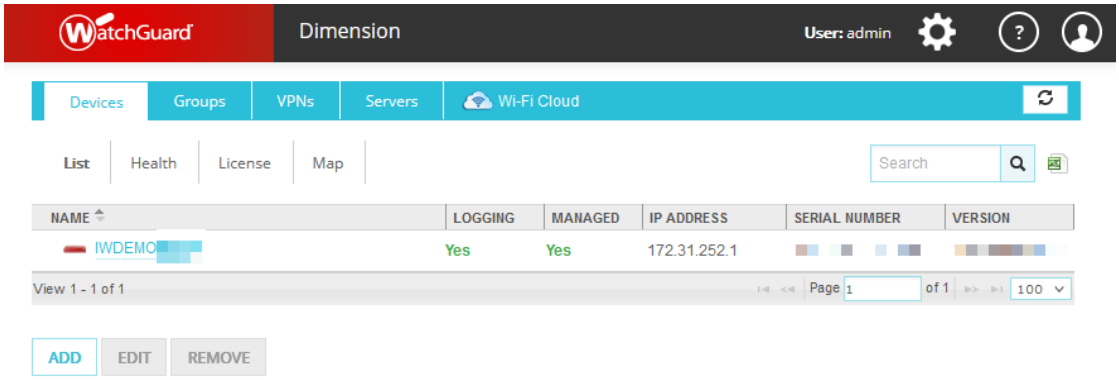
Laitemäärä	Järjestelmän muisti (sisäisellä tietokannalla)	Järjestelmän muisti (ulkoinen tietokanta)
100	1200 MB (Megabyte)	600 MB
200	2400 MB	1200 MB
400	4800 MB	2400 MB
500	6000 MB	3000 MB

Vaikka testiympäristön kone- ja liikennemäärä eivät vastaa minimilaitemäärää, pystytetään palvelu testiympäristöön käyttäen 2048 MB muistia. Testiympäristössä käytettävien resurssien puolesta kyseinen ylilyönti resurssien suhteen on mahdollista, mutta todellisessa tuotantoympäristössä tulisi mahdolliset käytettävät resurssit laskelmoida tarkasti, jotta vältytään ylimääräisiltä kustannuksilta. Virtuaaliympäristössä pystytettävään palveluun on mahdollista vaivattomasti, ja ilman suuria lisäkustannuksia, lisätä resursseja myös jäljestä, jolloin resurssit saadaan mitoitettua tarkasti. Dimension-palvelimelle asetetaan levytilaa 40 GB (Gigabyte) ja se yhdistetään VMware-ympäristössä ”IW_TopiN_NW” verkkoadapteriin. Asennusvaiheessa palvelulle määritetään kiinteä IP-osoite 172.31.252.100.

Dimension-palveluun määritetään aiemmin Firebox-palomuurille luotu uusi käyttäjätunnus, joka mahdollistaa ylläpitoyhteyden palvelun ja palomuurin välille. Ylläpitoyhteyden avulla palvelut keskustelevat keskenään ja ylläpitoyhteys mahdollistaa esimerkiksi erilaisten toimintojen käyttämisen suoraan Dimension-järjestelmän kautta.

Dimension-palvelun asennus on suoraviivainen ja ei tarjoa kustomointivaihtoehtoja lainkaan. WatchGuard on myös rajannut käyttäjien pääsyä käyttöjärjestelmän asetuksiin ja muutoksiin. Käyttöjärjestelmässä on pääkäyttäjätunnuksen käyttöä rajattu, eikä käyttäjällä ole oikeuksia tai tunnuksia tehdä muutoksia järjestelmään. Rajaus estää palvelimelle tehtävät muutokset. WatchGuard:n tarjoamista dokumentaatioista ei selviä mahdollisia tunnuksia, joilla järjestelmään pystyisi tekemään muutoksia. Palvelun ainoat muutosmahdollisuudet löytyvät web-pohjaisesta käyttöliittymästä, jotka kohdistuvat kuitenkin itse Dimension-palveluun, eikä Linux-pohjaiseen käyttöjärjestelmään.

Dimension-järjestelmän web-pohjaiseen hallintaan kirjaudutaan selaimen kautta suoraan palvelimelle määrätyllä IP-osoitteella, 172.31.252.100. Pystytyksen yhteydessä luodut tunnukset syötetään ja päästään aloitussivustolle, jossa näkyy kaikki Dimension-järjestelmään liitetyt laitteet sekä palvelut, katso Kuvio 3.

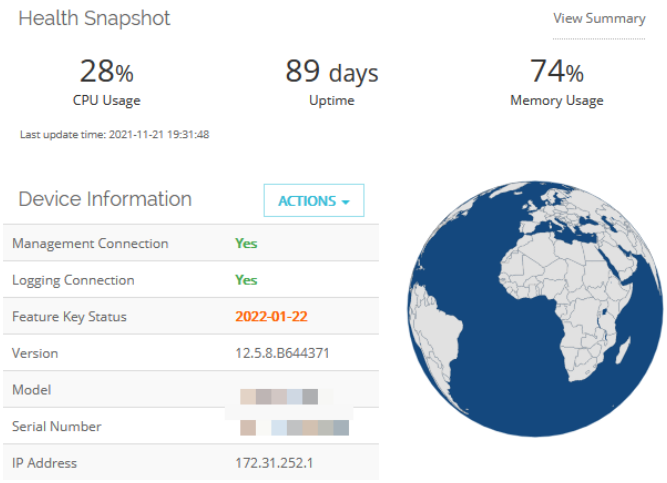


Kuvio 3 Dimension-järjestelmän näkymä.

Testiympäristössä käytössä ei ole muita palveluita tai laitteita, joita olisi mahdollista liittää Dimension-järjestelmään.

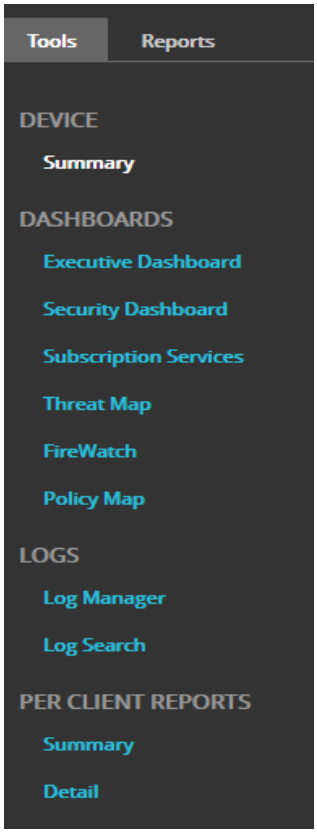
5.1.2 Palvelun toiminta

Aiemmin mainitun Kuvio 3 palvelunäkymän kautta päästään palomuurille tarkoitetulle hallintasivustolle. Kyseinen sivusto kertoo aloitussivustollaan heti laitteen prosessorin käyttöasteen, palomuurilaitteen käynnissä olon päivinä sekä laitteen muistin käyttöasteen, katso Kuvio 4.



Kuvio 4 Palomuurihallinnan näkymä.

Palvelun käyttöliittymästä löytyy selkeä luettelo järjestelmän tarjoamista ominaisuuksista, katso Kuvio 5.

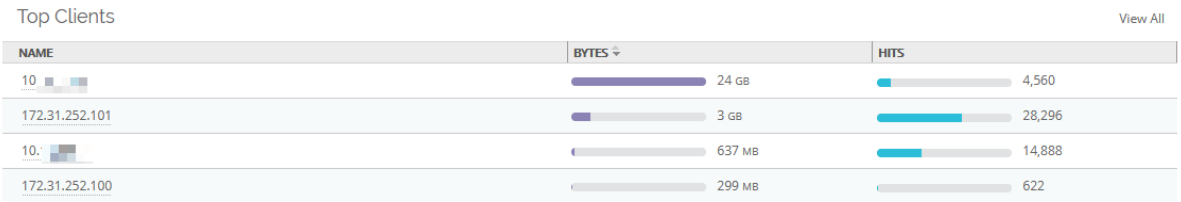


Kuvio 5 WatchGuard Dimension Web UI -palvelut.

Summary-sivustolta löytyy aiemmin mainitun Kuvio 4:n näkymä. Näkymästä löytyy myös aktiivisimmat palomuurin sääntökäytännöt, joista ilmenee kyseisen käytännön läpi kulkema datamäärä ja osumien määrä. Kyseinen näkymä on nähtävissä tarkemmin ”Policy Map”-kohdan alta. Summary-sivuston alkunäkymää ei ole mahdollista muuttaa, vaan järjestelmään on asetettu näkymään kyseiset datatiedot. Erilaisen yleisnäkymän luominen aloitussivustolle olisi hyvä lisä palveluun, mutta ei kuitenkaan välttämätön.

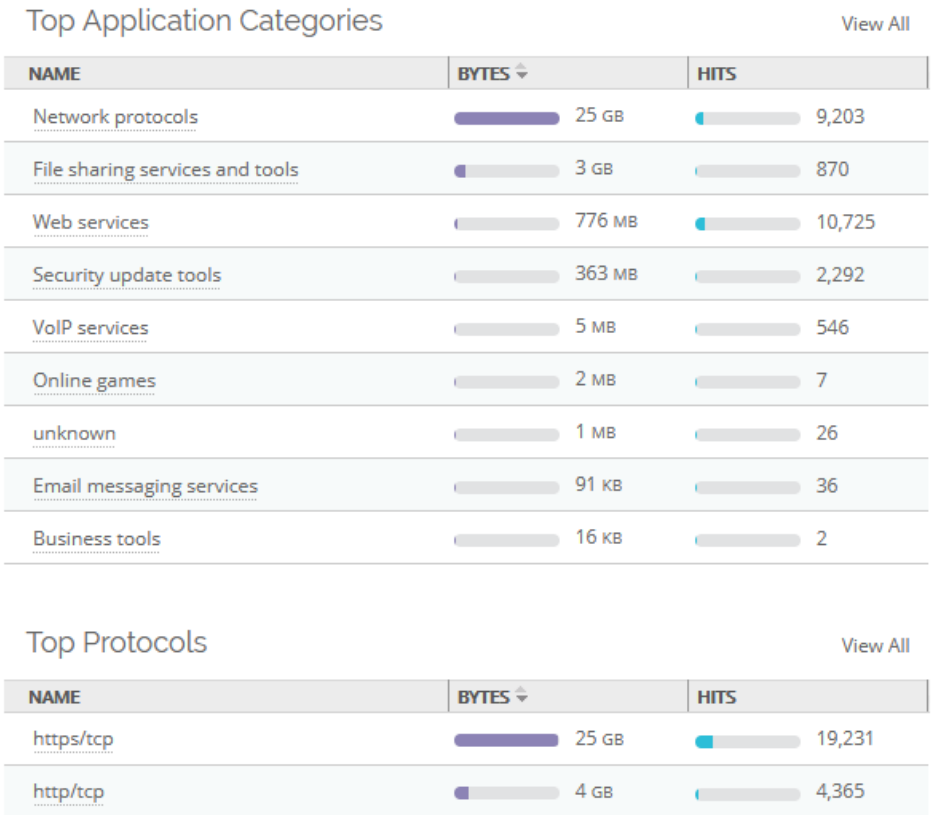
Executive Dashboard -sivuston kautta nähdään lokitietojen valossa tarkempaa dataa liikenteestä. Sivuston kautta nähdään tarkempaa liikennettä kuvattuna eri osa-alueilla, joka kuvastaa selkeästi liikenteen kulun. Top Clients -otsikon alta näkee palomuurin takana olevien laitteiden datamäärät,

katso Kuvio 6. IP-osoitteella näkyvät laitteet 172.31.252.101 on opinnäytetyön tekijän tekemä ylimääräinen palvelin, joka kehittää liikennettä. Toinen kuviossa näkyvä laite IP-osoitteella 172.31.252.100 on itse WatchGuard Dimension -palvelin.



Kuvio 6 Top Clients -otsikon dataliikenne kuvattuna.

Samanlainen kuvaava otsikko löytyy myös nimellä ”Top Destinations”, joka kertoo liikenteen kohteen. Liikenne on myös eroteltu esimerkiksi käytetyn applikaation ja protokollan mukaan, katso Kuvio 7.

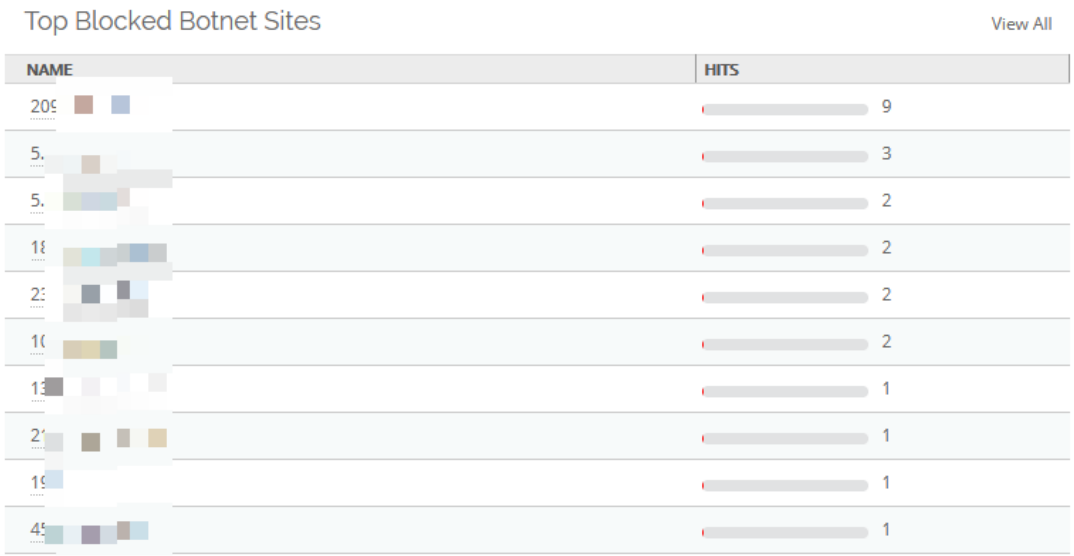


Kuvio 7 Applikaation ja protokollan mukaan luokiteltu liikenne.

Seuraavan alavalikon kautta, Security Dashboard, pystytään tarkkailemaan tietoturvan näkökulmasta erilaisia tapahtumia. Dimension kerää tapahtumia erilaisista uhkiin liittyvistä tapahtumista. Tietoturvauhkiin liittyvät tiedot ovat osittain sidoksissa Firebox-laitteeseen liitettyyn lisenssiin ja sen tasoon. WatchGuard kertoo sivuillaan erilaisten näkymien olevan seuraavanlaisia:

- Top Blocked Advanced Malware (APT)
- Top Blocked Botnet Sites
- Top Blocked Clients
- Top Blocked Mobile Devices
- Top Blocked Destinations
- Top Blocked URL Categories
- Top Blocked Applications
- Top Blocked Application Categories
- Top Blocked Protocols
- Top Blocked Attacks

Kyseiset otsikot näkyvät sivustolla vain, mikäli kyseiseen kategoriaan liittyviä tapahtumia on ollut havaittavissa. Testiympäristön laitteella saatiin näkyviin otsikot Top Blocked Clients, Top Blocked Botnet Sites, Top Blocked Destinations, Top Blocked Protocols ja Top Blocked Attacks. Kuvio 8 näh-dään, kuinka testiympäristön palomuuri on torjunut osittain tiettyjä osoitteita. (WatchGuard, 2021).

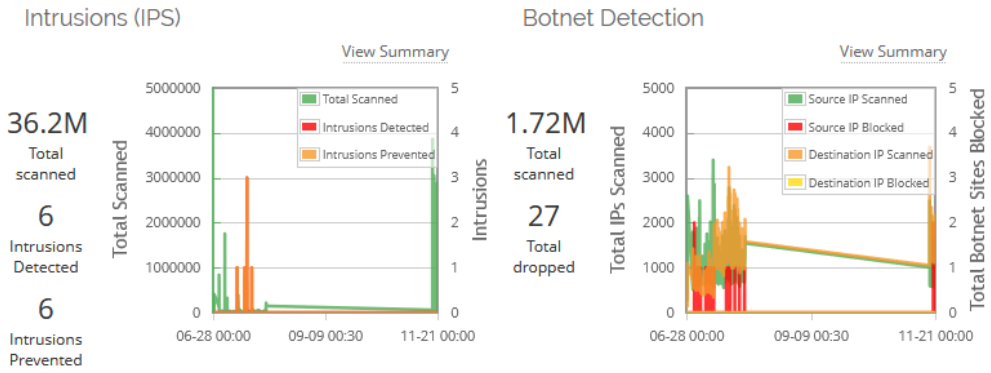


Kuvio 8 Blocked Botnet Sites Security Dashboard -näkymässä.

Top Blocked Attacks -otsikon alta on nähtävissä ”SSH Brute Force Login” hyökkäyksiä, katso Kuvio 9.

Kuvio 9 SSH Brute Force Login Security Dashboard -näkymässä.

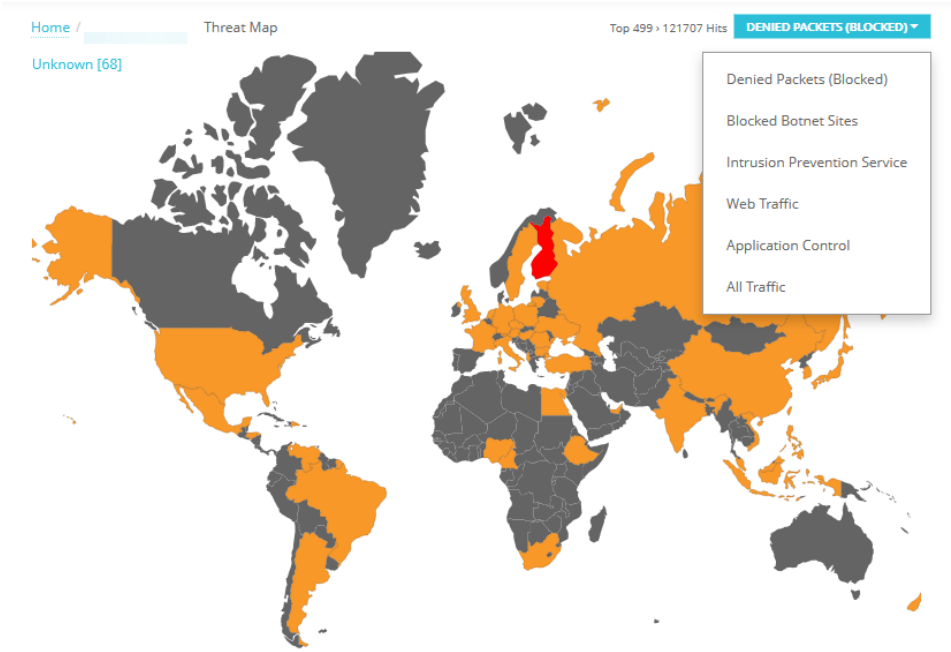
Erilaiset lisensseihin liittyvät tapahtumat ovat nähtävillä myös seuraavalla sivustolla ”Subscription Services”. Sivu kertoo suoraan skannauksien määrän, huomatut tunkeutumiset ja kuinka monta tunkeutumista se on pystynyt estämään. Myös skannattut ”Botnet Detection” tilastot ovat nähtävillä, katso Kuvio 10.



Kuvio 10 Subscription Services -näkymän tilastot.

Threat Map -osiosta on nähtävillä karttakuvan avulla, minne kaikki palomuurilla tapahtuvat tapahtumat sijoittuvat geologisesti. Karttanäkymässä on mahdollista vaihtaa kartalla näkyviä tapahtumia esimerkiksi estettyjen pakettien, estettyjen bottiverkkojen tai kaiken liikenteen mukaan. Kuvio 11 nähdään kaikki mahdolliset rajausvaihtoehdot karttanäkymään. Karttanäkymässä voi tiettyä maata painamalla nähdä tarkennetun tapahtumatietueen kyseiseen maahan liittyvistä tapahtumista. Näkymä näyttää myös protokollan ja mahdollisen kaupungin, mikäli se on saatu IP-

osoitteesta selville, IP-osoitteen sekä kuinka monesti kyseinen tapahtuma on esiintynyt lokitiedoissa.



Kuvio 11 Dimension-järjestelmän tarjoama karttanäkymä tapahtumista.

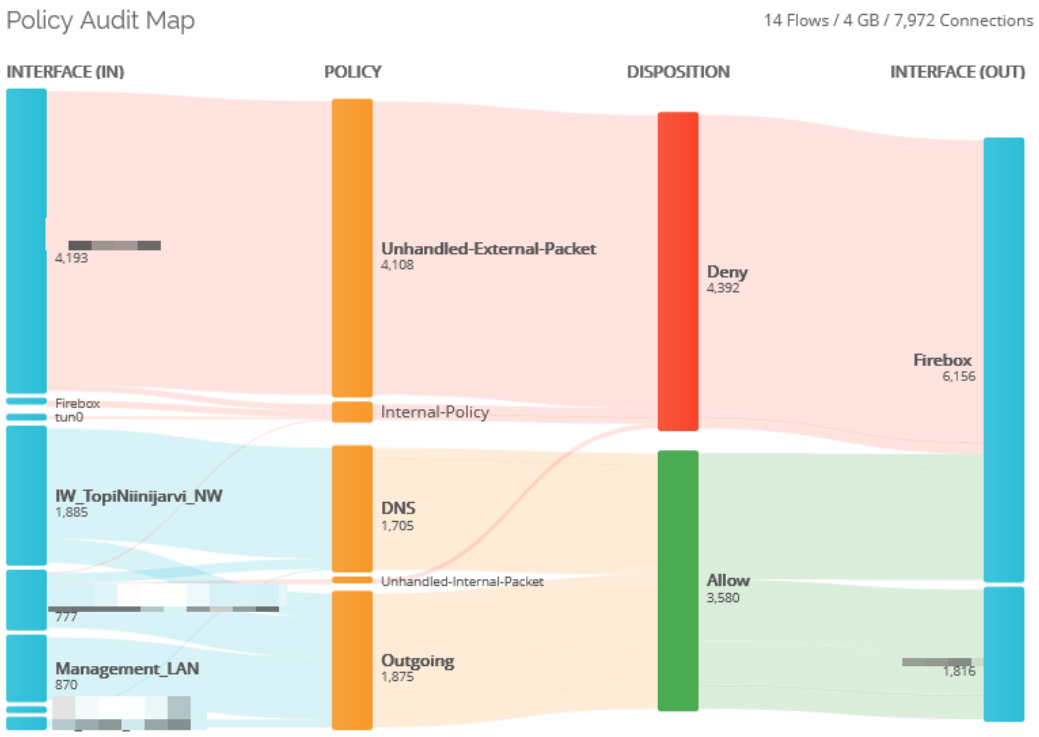
Järjestelmä ei kerro suoraan sivustolla eri värikoodien merkityksiä, mutta värikoodit ovat selitetty Dimension-järjestelmän ohjeistuksessa. Värikoodit ovat merkattuina melko järkevästi ja helposti tulkittavissa: punainen osoittaa korkeaa ja suurinta määrää estetyille tapahtumille, oranssi on keskiverto määrä estettyjä tapahtumia ja keltainen pienehkö määrä estettyjä tapahtumia. Kirkkaan vihreällä värikoodilla kerrotaan, että sallittuja tapahtumia on suurehko tai suurin määrä, vaalean vihreällä värillä sallittuja tapahtumia on keskiverto määrä ja harmaalla värillä osoitetaan, että tapahtumia ei ole lainkaan.

Karttakuvassa on myös ilmaisin ”Unknown”, jonka takaa saa listauksen tapahtumista ja IP-osoitteista, joita ei ole voitu määrittää kartalle.

Karttanäkymästä saa myös tarkemman tapahtuman selville, kun on ensin valinnut haluamansa maan ja tämän jälkeen valitsee listalta IP-osoitteen. Tuleva listaus esittää kaikki tapahtumat kronologisessa järjestyksessä kyseiselle IP-osoitteelle. (WatchGuard 2021.)

Firewatch-näkymä antaa interaktiivisen raportointityökalunäkymän, joka muodostaa palomuuri-laitteiston läpi kulkevasta liikenteestä laatikkomaisia elementtejä, joita pystyy tarkkailemaan. Näkymä tarjoaa tiedot ”Source”, ”Destination”, ”Domains”, ”Application”, ”Web Audit” ja “Protocol” tapahtumista. Testiympäristön tarjoama lokitieto on kuitenkin painottunut vahvasti muutamaan tiettyyn IP-osoitteeseen, jolloin näkymä ei vielä tarjoa kattavaa lisäarvoa. Tuotantoympäristössä näkymä tarjoaa paremmin statistiikkaa yhteyksistä ja niihin liittyvistä asioista.

Niin sanotuista kojelautanäkymistä viimeisenä Dimension-järjestelmä tarjoaa vielä palomuurille luotujen käytäntöjen mukaan tapahtuvan liikenteen. Näkymä kertoo, minkä palomuurikäytännön läpi liikenne on mennyt ja kuinka sille on lopulta käynyt, katso Kuvio 12.



Kuvio 12 Policy Map -näkymä Dimension-järjestelmässä.

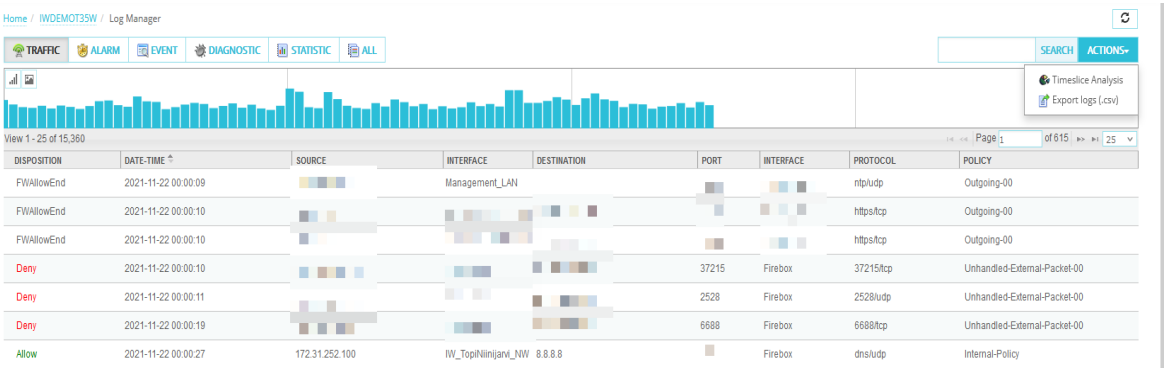
Policy Map -näkymässä pystyy hiiren osoittimella katsomaan tarkemmin liikenteen jakautumista ja osoittimen painalluksilla saamaan lisätietoja.

Dimension-järjestelmän lokitietojen manuaalista selaamista pystytään harjoittamaan järjestelmän tarjoamalla ”Log Manager” sekä ”Log Search” -työkaluilla. Log Manager -työkalu tarjoaa lokitiedot

kronologisessa järjestyksessä. Kaikki aiemmin esitellyt näkymät ja toiminnot pohjautuvat täysin puhtaaseen lokitekstiin, jota pystytään selaamaan erilaisten rajausten avulla. WatchGuard luokittelee lokitiedot viiteen erilaiseen kategorialuokkaan, jotka ovat:

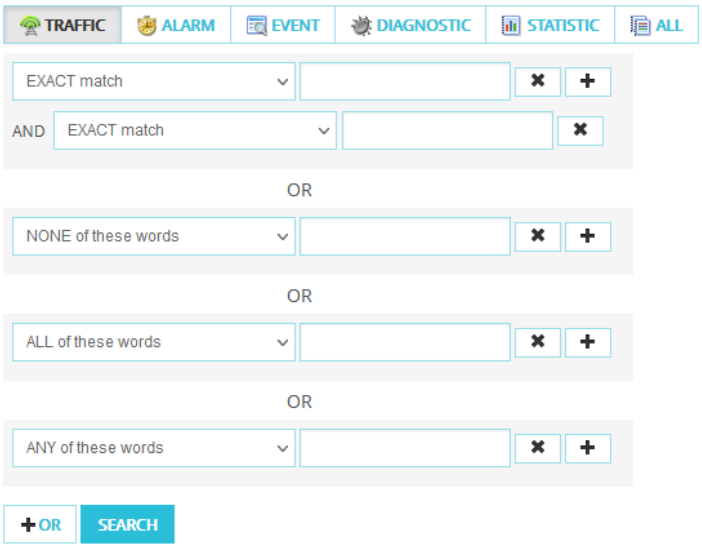
- Traffic
- Alarm
- Event
- Diagnostic
- Statistic

Lokitietoja voidaan selata aikajaksojen perusteella, lokitiedoista voidaan muodostaa erillinen .csv-tiedosto ladattavaksi ja lokitiedoista voidaan muodostaa piirakkagraafeja, katso Kuvio 13.



Kuvio 13 Lokitietojen selaus Dimension-järjestelmässä.

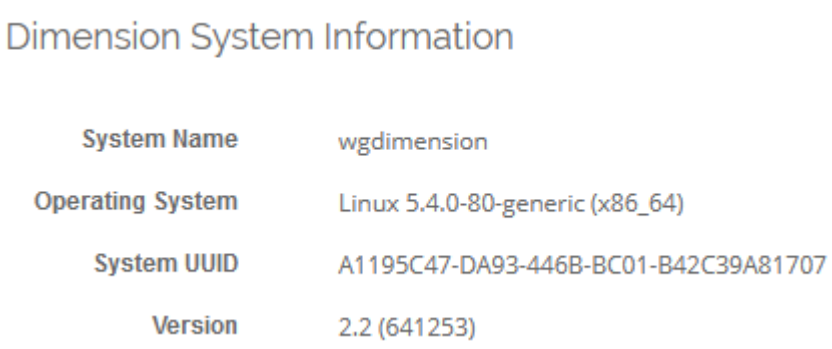
Lokitietojen hakutoiminnolla voidaan määritellä hakukenttään erilaisia arvoja ja hakuehdoiksi täsmentää ANY, ALL, EXACT tai NONE. Hakuehtoja voidaan putkittaa OR-lausetta hyödyntäen. Haut voidaan rajata tiettyyn lokikategoriaan tai hakea kaikista saatavilla olevista lokitiedoista, katso Kuvio 14.



Kuvio 14 Dimension-järjestelmän lokitietojen hakukone.

5.1.3 Dimension-järjestelmän muokattavuus ja hallinnointi

Dimension-järjestelmä on muokattuvuuden kannalta valitettavan suljettu kokonaisuus, joka ei tarjoa loppukäyttäjille mahdollisuutta tehdä muutoksia. Tämä johtuu siitä, että Dimension-järjestelmä ei ole vapaan lähdekoodin järjestelmä, vaan täysin WatchGuardin lisensoima palvelu. Käytettävä käyttöjärjestelmä ei myöskään ole GNU-lisenssiin perustava, vaan käytössä on WatchGuard:n oma tuote. Käyttöjärjestelmään viitataan palvelun sisäisessä informaatiossa ”Linux Generic”, katso Kuvio 15.



Kuvio 15 WatchGuard Dimension -järjestelmän käyttöjärjestelmäkuvaus.

Järjestelmässä on kuitenkin kattavasti saatavilla eritasoisia käyttöoikeuksia käyttäjätunnuksille. Tämä ominaisuus takaa sen, että järjestelmään voidaan luoda pelkkiä katselutunnuksia, jolloin vaarana ei ole sitä, että lokitietoja vahingossa poistettaisiin. Korkean tason admin-tunnuksia ei tulisi ikinä käyttää normaaliin lokitietojen katseluun, vaan siihen tarkoitettuja erilaisia tunnuksia. Dimension-järjestelmässä on myös mahdollista ottaa käyttöön Active Directory Authentication, joka hakee verkosta löytyvältä Windows-palvelimelta AD-käyttäjätiedot (Active Directory). Kyseinen ominaisuus osoittautuu tärkeäksi toimeksiantajan kohdalla, koska yrityksen käytössä on AD-ratkaisu. Integraation toteutus ei kuitenkaan ole mahdollinen testiympäristössä, kun erillisen Windows-palvelimen rakentaminen ei ole osana opinnäytetyötä. Yrityksen WatchGuard-spesialistien mukaan aiemmin käytetyt ja testatut AD-integraatiot WatchGuard-sarjan tuotteilla ovat olleet onnistuneita ja toimivia. Tällöin mahdollisessa todellisessa tuotantoympäristöön kohdistuvassa toteutuksessa Active Directory authentication -ominaisuus otetaan käyttöön. Ominaisuuden käytöllä saadaan rajattua pois paljon manuaalista työtä, joka kohdistuu käyttäjätunnuksiin ja niiden hallinnointiin. Erilaisin roolein voidaan AD-ympäristössä rajata käyttäjiä Dimension-palvelun käyttöön.

Dimension-järjestelmä mahdollistaa pääsyn estämisen palveluun muista osoitteista tai verkoista, kuin mitä järjestelmään on syötetty. Oletuksena palvelu sallii yhteydet kaikista osoitteista. Tätä on kuitenkin rajattu opinnäytetyön kohdalla jo palomuurin puolelta, koska ympäristöön ei ole vapaata pääsyä. Ominaisuus on kuitenkin hyvä tiedostaa, mikäli palvelua pystytettäisiin suoraan julkiverkkoon. Järjestelmä tarjoaa myös eräänlaisen käyttäjätileihin kohdistuvan lukituksen, joka lukitsee käyttäjätilejä epäonnistuneiden kirjautumisien jälkeen.

Järjestelmän tarjoamat liitokset erillisen AD-palvelimen kanssa tarjoavat suurta hyötyä. Erilaiset pakotetut salasanakäytänteet ja käyttäjähallintamuutokset voidaan suorittaa suoraan erilliseltä palvelimelta, jolloin käyttäjien luomis- ja poistoprosesseihin saadaan tehokkuutta.

Dimension-järjestelmä saa isoja päivityksiä noin kahdesti vuodessa, joissa on yleisiä korjauksia löytyneisiin ongelmiin. Päivitykset ovat sisältäneet myös erilaisia tietoturvapäivityksiä. Järjestelmän päivittäminen tapahtuu uuden versiopäivityksen lataamisella, jonka jälkeen se ajetaan Dimension-järjestelmään Upgrade-painikkeen kautta. (WatchGuard, 2020.)

Lokitietojen varmuuskopiointia varten Dimension-järjestelmään on mahdollista luoda rinnalle erillinen PostgreSQL-tietokantapalvelin, jonne varmuuskopiot voidaan ajaa. Erillisten varmuuskopioiden ajaminen toiselle palvelimelle tapahtuu liittämällä palvelin Dimension-järjestelmään SSH FTP –(File Transfer Protocol) palvelimena. Lokitietojen varmuuskopiointia ei saada käyttöön, ellei SSH FTP -yhteyttä ole muodostettu palvelinten välille. Palvelujen välinen autentikointi tapahtuu käyttäjätunnuksella sekä julkisella SSH-avaimella. Dimension-järjestelmä on automaattisesti luonut avaimen, joka lisätään FTP-palvelimelle.

Dimension-järjestelmän omat lokitiedot ovat saatavilla erillisellä auditointityökalulla, joka näyttää käyttäjien kirjautumiset ja erilliset tapahtuvat muutokset järjestelmissä, katso Kuvio 16.

Kuvio 16 Dimension-järjestelmän omat lokitiedot, tekijän tekemiä muutoksia palvelussa.

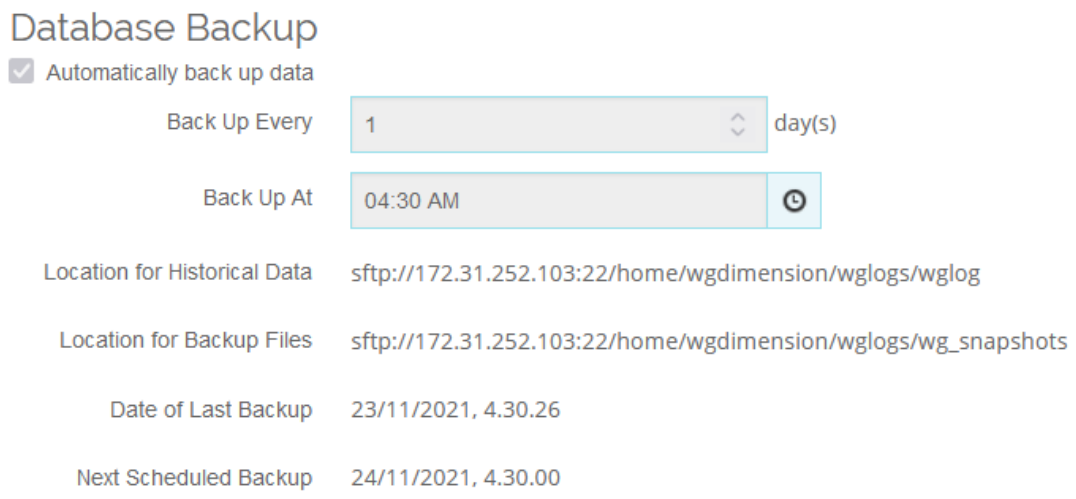
Dimension-järjestelmään otettiin käyttöön lokitietojen tallennus ulkoiselle Linux-palvelimelle käyttäen aiemmin mainittua SSH FTP -yhteyttä. Yhteyttä varten pystytettiin uusi Linux Ubuntu 18.04 -version palvelin. Palvelin sai IP-osoitteen 172.31.252.103. Palvelimelle luotiin uusi admin-tason käyttäjä wgdimension. Käyttäjän kotikansioon luotiin polkuun ”~/.ssh/” -niminen kansio, jonka sisälle tiedosto ”authorized_keys”. Merkki ”~”-kansiorakenteessa kuvastaa nykyisen käyttäjän omaa kotikansiota. Tiedostoon tallennettiin Dimension-palvelimelta saatu julkinen avain. Palvelimella otettiin myös käyttöön openSSH-ohjelmisto, jotta SSH-yhteyden muodostaminen onnistuu. Aiemmin luodun kansion ja siellä olevan tiedoston kannalta kriittiseksi asiaksi osoittautui näille annetut oikeudet. Kansiolla ”ssh” tuli olla tarkalleen määritettynä käyttöoikeudet komennolla ”chmod 700”, joka antaa kansion omistajalle täydet oikeudet. Tiedostolla ”authorized_keys” tulee olla annettuna oikeudet ”chmod 600”, joka antaa tiedoston omistajalle luku- ja kirjoitusoikeuden. Myös

käyttäjän kotikansiolla polussa /home/wgdimension tulee olla määritetty oikeudet oikein. Kyseiseen kansioon on annettava oikeudet ”chmod 755”, joka antaa omistajalle täydet oikeudet, ryhmälle luku- ja suoritusoikeudet ja yleisesti samat luku- ja suoritusoikeudet. Yhteyden muodostaminen ei onnistunut ennen kuin nämä oikeudet oli määritetty oikein. Testiympäristöstä syntyvien lokien lähettäminen erilliselle palvelimelle kuormittaa palvelinta lokitietojen koon puolesta noin yhden megatavun verran. Lokitiedot muodostuvat erilliselle palvelimelle pakatussa muodossa, katso Kuvio 17

```
iwtopi@topi-01sv003:/home/wgdimension/wglogs/wglog$ ls -l
total 1884
-rw-r--r-- 1 wgdimension wgdimension 988241 Nov 23 02:30 20211121.zip
-rw-r--r-- 1 wgdimension wgdimension 935948 Nov 23 02:31 20211122.zip
```

Kuvio 17 Dimension-järjestelmän lähettämä pakattu lokitieto erillisellä palvelimella.

Dimension-järjestelmä mahdollistaa lokitietojen varmuuskopioinnin minimissään kerran päivässä. Muut vaihtoehdot varmuuskopioinnin luomiseksi on vain määritetty kellonaika tapahtumalle, katso Kuvio 18.



Kuvio 18 Dimension-järjestelmän mahdollistama varmuuskopiointi lokitiedoille ja palvelun asetuksille.

Lokitietojen tuominen takaisin varmuuskopioinnin sijainnista on myös mahdollista. Itse Dimension-järjestelmän tietokantaan voi määrittää asetuksen, joka poistaa tietyn päivärajan ylitettyä vanhat tiedot. Oletuksena asetus ei ole päällä, jolloin vanhoja lokitietoja ei poisteta.

5.1.4 Yhteenveto

Dimension-järjestelmä tarjoaa kattavan kokonaisuuden erilaisille WatchGuard-sarjan tuotteille. Keskittämällä erinäisiä palveluita WatchGuard-tuotesarjaan, pystyy Dimension-järjestelmästä saamaan paljon irti. Kattavat valmiit näkymät, mahdollisuus web-näkymän ja lokitietojen perusteella muodostuvasta karttanäkymästä luoda suoria sääntöjä palomuuriin antavat erinomaiset valmiudet myös kokemattomalle käyttäjälle luoda erilaisia sääntöjä nopeasti. WatchGuard:n tarjoamat päivityspaketit tuovat lisäturvaa ja korjauksia ominaisuuksiin. Käyttäjienhallinnan ominaisuudet ovat riittävät ja valmius AD-palvelimen yhdistämiselle auttavat yrityksen palveluiden yhdistämisessä.

Dimension-järjestelmän käyttöjärjestelmän suljettu kokonaisuus osoittautui kuitenkin järjestelmän isoimmaksi haitaksi. Suljetun lähdekoodin palvelujen kovennuksesta ei voida olla täysin varmoja ilman erillisiä penetraatiotestauksia. Kuitenkin palvelun pystyttämisellä suljettuun ympäristöön ja tekemällä rajauksia sekä kovennuksia palomuuritasolla voidaan varmistua palvelun tietoturvasta. Erillisen varmuuskopiointipalvelun liittämisestä Dimension-järjestelmän rinnalle saadaan palvelulle lisäarvoa, jolloin lokitietojen oikeaoppisesta ja lakisääteisestä säilytyksestä voidaan varmistua. Palveluiden pyöriessä virtuaalialustalla voidaan varmuuskopioinnista varmistua vielä alustan erillisillä varmuuskopiointiratkaisuilla. Kahdentaminen takaa palveluiden jatkuvuuden ja mahdollisissa katastrofitilanteissa voidaan varmistua tiedon eheydestä.

WatchGuard Dimension takaa kattavasti hyvät ominaisuudet verkkoliikenteen seuraamiseen, tietoturvapoikkeamien havaitsemiseen ja lokitietojen oikeaoppiseen säilömiseen. Lisäarvoa tuovat Windows Active Directory -liitäntä, joka helpottaa käyttäjienhallintaa.

5.2 Avoimen lähdekoodin ratkaisu

5.2.1 Palvelun pystytys

Avoimeen lähdekoodiin perustava ratkaisu pystytettiin Ubuntu Linux 18.04 LTS -version päälle. Palvelin pystytettiin Dimension-järjestelmän tavoin VMware-virtuaalialustalle. Palvelimelle asetettiin keskusmuistia 2 GB ja kovalevytilaa 4 GB. Palvelimelle asetettiin kiinteä IP-osoite 172.31.252.200.

Ubuntu-palvelimen pystytys on myös melko suoraviivainen tapahtuma ja asennusvaiheen aikana ei palvelimelle tehty paljoa muutoksia. Muutokset tehtiin vain näppäimistöasetuksiin, ja palvelimelle luotiin paikallinen tili. Tätä samaa tiliä käytetään palvelimelle kirjautumiseen ja asennuksien toteuttamiseen.

Palvelimelle sallittiin SSH-yhteyden muodostaminen, jotta hallintayhteys voidaan muodostaa virtuaalialustan tarjoaman yhteyden sijaan erillisellä ohjelmistolla, PuTTy. PuTTy on ohjelmisto, jota käytetään SSH-palvelimien käyttämiseen. (PuTTy, n.d.).

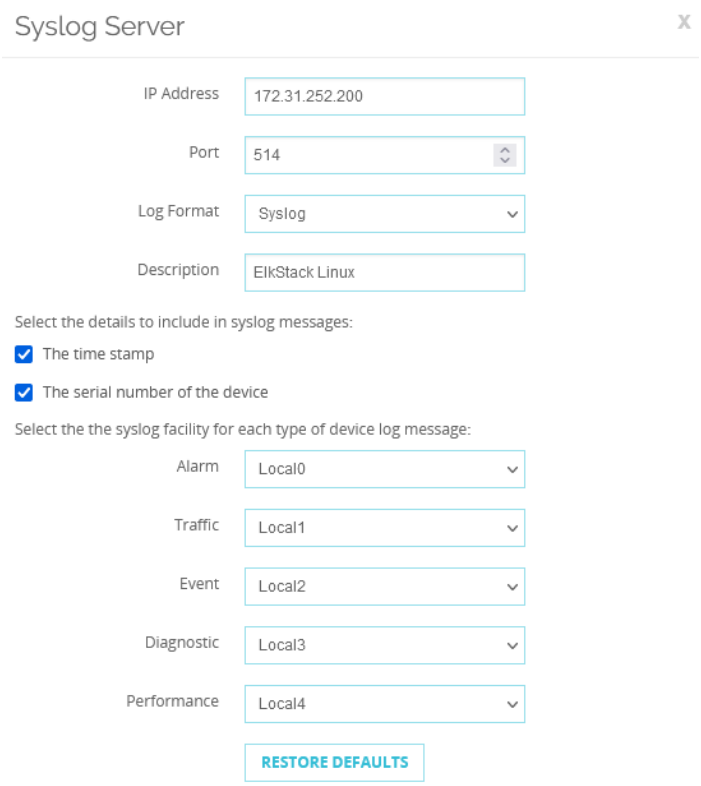
Palvelimelle asennettiin ELK-Stack-kokonaisuus, joka kattaa Elasticsearch, Logstash ja Kibana -ohjelmistot. Ohjelmien asentaminen onnistuu suoraan ELK-Stackin tarjoamasta arkistosta.

Ohjelmien konfigurointi aloitettiin määrittämällä Elasticsearch-ohjelmaan IP-asetukset. Ohjelman asetuksissa on vakiona määritteet, että palvelu löytyy osoitteesta ”localhost”. Tämän määrityksen sijaan käytetään mielummin kiinteästi määritettyjä IP-osoitteita, joten tiedostoon ”etc/elasticsearch.elasticsearch.yml” -muokattiin määrite ”network.host: 172.31.252.200”. Palvelussa on oletuksena käytössä http-kuuntelua varten portti 9200, tähän ei tehdä muutoksia. Myöskään muihin tiedoston asetuksiin ei tehdä muutoksia.

Seuraavana konfiguroidaan Kibanan asetuksia, joka on web-käyttöliittymä palvelulle. Kyseinen moduuli tarjoaa graafisen käyttöliittymän, jonka kautta voidaan tulkita järjestelmään lähetettyjä indeksoituja tietoja. Kibanan konfiguraatiotiedosto löytyy polusta /etc/kibana/kibana.yml. Tiedostoon määritetään palvelun käyttämä portti, oletuksena portti 5601, jota ei muuteta. Palveluun määritetään ”server.host: ”172.31.252.200”” ja Elasticsearch-palvelun sijainti ”elasticsearch.hosts: [”http://172.31.252.200:9200”]”, muita muutoksia konfiguraatioon ei tehdä.

Filebeat-järjestelmä toimii tiedonvälittäjänä, joka välittää valitut tiedot Kibana-järjestelmään. Filebeat-ohjelman konfiguraatiotiedosto löytyy polusta /etc/filebeat/filebeat.yml. Kyseiseen tiedostoon määritetään esimerkiksi lokien alkuperäinen kansio, josta ne noudetaan. Firebox-palomuurin lokitietoja varten on luotu hakemistoon ”/var/log/” firewall-logs-niminen kansio, jonka sisälle lokitiedot vastaanotetaan. Kyseinen polku määritetään filebeat.yml-tiedostoon.

WatchGuard Firebox-palomuurista tiedostojen siirtäminen Linux-palvelimelle aloitetaan konfiguroimalla palomuurin ”Logging”-asetuksia. Ulkoisen ja muun kuin Dimension-palvelun käyttö vaatii, että palvelin lisätään järjestelmään Syslog-serverinä. Lokitietojen formaatiksi voi valita joko Syslog tai IBM LEEF. Lokipalvelin määritetään palomuurille Kuvio 19 mukaisesti. Käytämme tässä syslog-pohjaista lokitietoa. IBM LEEF -muodossa lähtevissä lokitiedoissa ei ole lainkaan suorituskykyyn liittyviä lokitietoja.



Kuvio 19 WatchGuard Firebox -palomuurin Syslog serverin määritykset.

Kuviossa näkyvät ”Local0-4” -määritykset tietyn tyyppisille lokitiedoille avataan WatchGuard Dimension -ohjeistuksessa. Kuvio 19 näkyvä pienemmällä numerolla varustettu nostattaa kyseisen

lokitiedon prioriteettiä, jolloin Local0-määritys asettaa hälytykseksi luokiteltavan lokitiedon korkeimmalle tasolle. Testiympäristön kokeilua varten käytämme vakiona olevia tietoja ja asetamme palomuurin lähettämään kaikki saatavilla olevat lokitiedot, eli hälytykset, liikenteen, tapahtumat, diagnostiikan sekä suorituskykyyn liittyvät tiedot. (WatchGuard, 2021).

Porttivalinnaksi valitaan 514, joka on lokien vastaanottamiseen tarkoitetun rsyslog-ohjelmiston oletusportti. Rsyslog-ohjelmisto tulee sanoista “The rocket-fast system for log processing”. Ohjelmisto on tarkoitettu tiedon kuljettamiseen erilaisten palveluiden välillä. Ohjelmisto pystyy kuljettamaan jopa miljoona viestiä sekunnissa (rsyslog, 2020). Rsyslog-ohjelmisto asennetaan vastaanottavalle Linux-palvelimelle ja sinne tehdään Liite 1 mukaiset konfiguraatiot. Konfiguraatiossa kerrotaan, että mikäli lähettävän palvelimen nimi vastaa testiympäristön palomuurilaitteiston nimeen, se kirjoittaa lokitietoa tietyssä kansiossa olevaan tekstitiedostoon. Palvelu käynnistetään uudelleen ja toimivuus voidaan taata.

Kehittyneestä lokitiedostosta voidaan tutkia ja nähdä esimerkkirivi, minkälaisena syötteenä palomuuri lähettää lokitietoa:

Nov 23 08:26:14 IWDEMOxxxx serial (2021-11-23T06:26:14) firewall: msg_id="3000-0148" Allow IW_TopiNiinijarvi_NW Firebox 82 udp 20 64 172.31.252.100 8.8.8.8 55125 53 geo_dst="USA" msg="DNS Forwarding" record_type="PTR" question="2.255.255.10.in-addr.arpa" (Internal Policy)

Lokitieto koostuu monesta osiosta, joista ensimmäisen alkuun on liitetty aikaleima. Ensimmäinen aikaleima on todellinen ja sama kuin palomuurille asetetussa aikavyöhykkeessä. Päivämäärän formatointi on selkeästi normaalista poikkeava, kun merkitsemisessä käytetään kuukauden kolmea ensimmäistä kirjainta, jonka jälkeen on merkittynä kuukauden päivämäärä ja tämän jälkeen kellonaika käyttäen formaattia tunti:minuutti:sekunti. Seuraavassa tietueessa on palomuurilaitteistolle asetettu nimi, josta on pyyhitty tarkempi mallimerkintä. Nimitietueen jälkeen kerrotaan laitteiston sarjanumero. Sulkujen sisälle on asetettu aikaleima +0 vyöhykkeeltä. Saadussa viestissä oleva ”msg_id” kertoo numerosarjan, jotka ovat avattuna WatchGuardin omassa katalogissa. ’Allow’ kertoo, että kyseinen liikenne on hyväksytty. IW_TopiNiinijärvi_NW kertoo palomuurille asetetun rajapinnan nimen, jota seuraa kohteen nimi, tässä tilanteessa Firebox. Numero 82 kertoo toisen

lähteen mukaan paketin koon (Meier, 2016), mutta WatchGuardin oma ohjeistus ei tarjoa informaatiota lainkaan kyseiselle kohdalle lokitietoa (WatchGuard, 05/2020). UDP kertoo käytettävän protokollan. Protokollan jälkeen on kaksi numerosarjaa, jotka WatchGuard-katalogin mukaan ovat arvot tiedoille paketin koko ja TTL (time to live). Maierin mukaan toinen arvoista on TTL, toiselle ei löydy tietoa. (Maier, 2016). Näitä tietoja seuraa tieto lähteestä, josta paketti on lähtenyt liikkeelle, 172.31.252.100. Tätä seuraa tieto kohteesta, 8.8.8.8. IP-osoitteiden jälkeen kerrotaan lähtöportti ja kohdeportti. Viestissä on mukana myös geolokaatio, paketin oma viesti, tyyppi ja kysymys.

WatchGuard:n tarjoama katalogin esimerkkiviestit eivät täsmänneet täysin saamaamme viestiin, vaan viestissä olevien arvojen paikat vaihtelivat. Maier (Maier, 2016) oli luonut vuonna 2016 lokitietoviestin perusteella erillisen Grok-kuvion, jonka pohjalta opinnäytetyön tekijä tulkitsi mahdollista lokiviestiä. Maier ei ollut artikkelissaan tuonut esille alkuperäistä lokitietoviestiä. Maierin kirjoittama artikkeli on vuodelta 2016, jolloin vuosien saatossa WatchGuard Firebox -laitteesta lähetettävä lokitieto on saattanut muuttaa muotoaan myös. (Maier, 2016).

Lokiviestissä mainittu ”msg_id” kertoo WatchGuard-katalogin mukaan tarkemmin viestin sisällöstä ja aihealueesta. Erilaisia ID-sarjoja on useita satoja, ellei jopa tuhansia. Katalogin pituus on 257 sivua ja sivuilla on vaihtelevasti yhdestä kahdeksaan ID-sarjaa avattuna. Kuvio 20 on esimerkkinä turvapalveluihin (Security Services) liittyvästä tapahtuma (Event) ID:sta ja niiden tarkemmista selityksistä.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
1F000001	ERROR	Security Services / Gateway Anti-Virus	Process failed to start	Cannot start ScanD	ScanD -- Process failed to start	Cannot start ScanD	—
1F010015	INFO	Security Services / Gateway Anti-Virus	Ready for service	ScanD ready	ScanD -- Ready for service	ScanD ready	—
2E000005	ERROR	Security Services / Signature Update	Process exiting	SIGD shutting down	SIGD -- Process exiting	SIGD shutting down	—

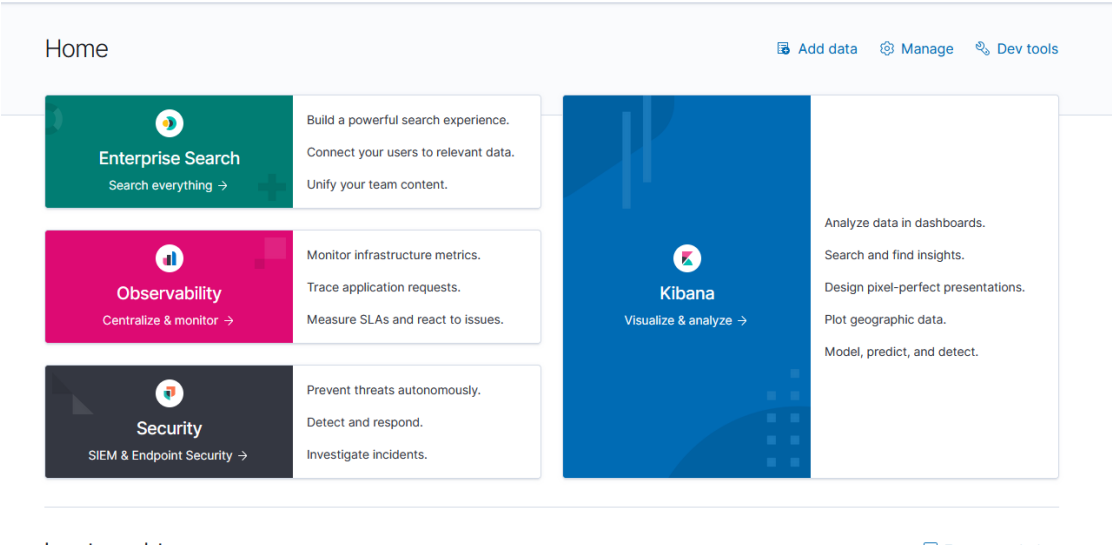
Kuvio 20 WatchGuard Log Message Catalog esimerkki (WatchGuard, 05/2020).

Mainittu Grok on työkalu, joka mahdollistaa lokitietojen parsimisen. Grok-kuvio muodostaa annetusta datasta kuvion avulla ymmärrettävää dataa, jota pystytään hallinnoimaan esimerkiksi Elasticsearch-ohjelmiston avulla. Ohjelmisto ei osaa tunnistaa automaattisesti esimerkiksi Firebox-laitteen lähettämää lokitietoviestiä, vaan Grok-kuvion avulla on kerrottava, mitä mikäkin kohta

viestistä tarkoittaa. Kun järjestelmä tunnistaa annetut viestit ja niiden arvot, voidaan niiden pohjalta muodostaa tarkempaa tietoa. (Elastic, 2021).

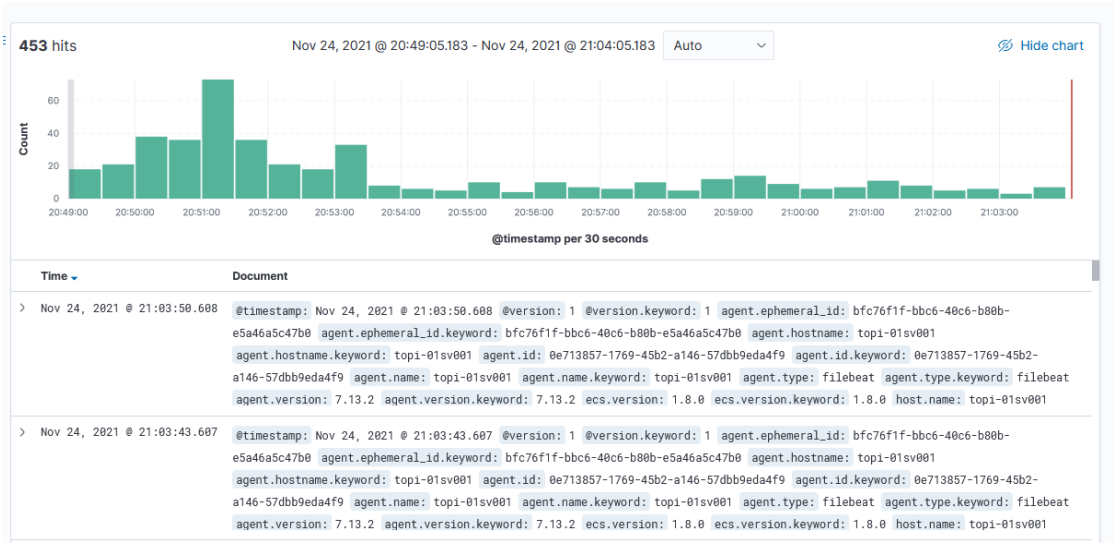
Annettujen tietojen perusteella on mahdollista lähteä rakentamaan Grok-kuviota, jolla viestistä saadaan eroteltua tärkeitä elementtejä ja luotua statistiikkaa näiden pohjalta. Grok-kuvioiden konfiguraatiot luodaan polkuun */etc/logstash/conf.d/*. Polkuun luotiin tiedosto nimeltä */etc/logstash/conf.d/grok-example.conf*. Konfiguraatioon lisättiin tiedot input-arvolle, mistä alkuperäinen lokitiedosto löytyy ja mistä kohtaa lokitietoa tiedoston luku aloitetaan. Konfiguraation perään lisättiin tieto, mihinkä tiedostot lähetään, eli kerrottiin Elasticsearch-järjestelmän osoite ja lisättiin index-nimi tuleville tiedoille, demo-grok. Ennen viestien parsimista tarkastetaan, että palvelut välittävät viestin web-käyttöliittymään oikein ja lokitiedot saadaan tarkastettua ymmärrettävässä muodossa.

Kibana-palveluun, jossa lokitietoja voidaan selata graafisen käyttöliittymän kautta, aukaistaan web-pohjaisessa käyttöliittymässä siirtymälle osoitteiseen 172.31.252.200:5601, katso Kuvio 21.



Kuvio 21 Kibana-palvelun pääsivu palvelimella 172.31.252.200.

Sivustolla siirrytään Kibana-näkymään ja siirrytään Discover-työkaluun. Vasemmalla löytyvästä valikosta voidaan valita ”Index Pattern”, josta valitsemme konfiguraatioon määritetyn ”demo-grok indexin. Tämän jälkeen Kibana näyttää siirrettyjen lokitietojen tiedot, katso Kuvio 22.



Kuvio 22 Kibana-palvelun näkymä lokitietojen siirron jälkeen.

Annetuista tiedoista näkee kuitenkin, että alkuperäiseen lokitietoon on lisättynä paljon ylimääräistä tietoa. Viestiin on lisätty tietoja palveluun lähettävästä palvelimesta tietoja, eli kyseessä olevasta Linux-palvelimesta. Tämä tieto häiritsee alkuperäisen viestin tulkitsemista ja tiedon hakemista. Palvelu osaa tulkita itse lisäämiensä tietojen otsikot, jolloin näiden perusteella pystytään tekemään rajauksia. Kuitenkin WatchGuard Firebox -palomuurin oikeaa ”message”-tietoa järjestelmä ei ole osannut automaattisesti tulkita. Järjestelmä on tunnistanut tiedon vain otsikkona ”message”, mutta ei mitään sen sisältöä, katso Kuvio 23.

Kuvio 23 Alkuperäisen lokitiedon ympärille lisättyjä ylimääräisiä tietoja.

Ylimääräisten tietojen poistamisella voidaan helpottaa tulevaa filtteröintiä, jolloin alkuperäistä viestiä lukemalla saadaan helpompi käsitys viestin sisällöstä.

Elastic:n omista dokumentaatioista löydettiin ohjesivusto, joka kertoo, kuinka tietyt tiedot voidaan pudottaa tiedon lähetyksestä. Määritykseen on mahdollista antaa tietty ehto, jolloin tieto tiputetaan pois. Mikäli ehtoa ei määritetä, jätetään tieto aina pois. Myöskään kaikkea niin kutsuttua metatietoa ei pysty viestistä poistamaan. Tutkimalla lokitiedosta löytyvää ylimääräistä dataa voidaan päätellä pudotettavat arvot ja syöttää ne konfiguraatiotietoihin, katso Liite 2. (Elastic, n.d.).

Konfiguraatiomuutoksen jälkeen viestin sisältöä on saatu siistittyä, katso Kuvio 24.

Kuvio 24 Kibana-palvelun näkymä lokitiedosta ylimääräisten tietojen poiston jälkeen.

Ennen lokitiedon parsimista Grok-kuviolla, suoritettiin lokitietojen osalta niiden säilömisen kannalta testaaminen. Lokitietojen kiertämiseen käytetään logrotate-nimistä ohjelmistoa. Logrotate-ohjelmisto tarjoaa ratkaisua järjestelmille, jotka käsittelevät paljon lokitietoja. Se tarjoaa ympäristön ylläpitäjälle mahdollisuuden kierrättää automatisoidusti lokitietoja talteen (Troan, E., Brown, P., Kaluza, J. n.D.).

Logrotate mahdollistaa lokitietojen pitkäaikaisenkin säilytyksen tehokkaasti, kun ohjelmiston kiertoon suunnatussa konfiguraatiossa on myös mahdollista asettaa lokitietojen pakkaaminen kiertoon päälle. Konfiguraatiotiedostossa voidaan määrittää lokitiedostot, joihin kierto toteutetaan, joko yksittäisenä tiedostona tai kokonaisena hakemistona.

Logrotate-ohjelmalla on konfiguraatiotiedostoja useassa paikassa. */etc/logrotate.conf*-tiedostossa on määritys, joka lukee kansiosta */etc/logrotate.d* olevat konfiguraatiot. Kyseisestä kansiosta löytyy oletuksena tiedosto ”rsyslog”, jonka sisään muutokset tehdään. Tiedostoon on jo määritettynä vakiona olevia määrityksiä tietyille lokitiedostoille, joihin ei tehdä muutoksia. Tiedostoon lisätään omat määritykset, jotka koskevat lokitiedostoa, johon Firebox-palomuurijärjestelmä lähettää lokitiedot suoraan.

Konfiguraatio aloitetaan määrittämällä joko hakemisto tai tiedosto, jonka perään syötetään halutut määritykset. Konfiguraatio on nähtävissä Liitteessä 3. Konfiguraatioon on määritettynä haluttu kiertomäärä lokitiedostolle, 14 kertaa. Käytännössä tämä tarkoittaa, että lokitiedostoa kierrätetään 14 kertaa, ennen kuin se poistetaan tai mahdollisesti postitetaan sähköpostin välityksellä. Tämä tieto yksinään ei riitä määritykselle. Halutun kiertomäärän jälkeen järjestelmälle ilmoitetaan, milloin kierto tehdään. Esimerkkikonfiguraatiossa tämä tehdään päivittäin. Muita mahdollisia määrityksiä ovat viikottain, kuukausittain tai vuosittain. Näiden tietojen avulla kerätään testiympäristössä lokitietoa kahden viikon ajalta, jonka jälkeen data poistetaan. Jokainen lokitiedosto on yhden päivän ajalta. Seuraava määritys ”*copytruncate*” kertoo järjestelmälle, että alkuperäistä lokitiedostoa ei siirretä tai poisteta, vaan tästä luodaan kopio. Kyseinen komento on välttämätön tilanteissa, jossa jokin muu järjestelmän sovellus käyttää tiedostoa. Kyseinen tiedosto on jatkuvasti käytössä, koska tiedostoon tulee lokitietoa jatkuvasti ja Elastic-kokonaisuus lähettää kyseisestä tiedostosta dataa web-pohjaiseen näkymään luettavaksi. Jotta aikaisempi ”*copytruncate*” -määritys toimii, tulee tälle määrittää sijainti, johon tieto siirretään. Halutut vanhat lokitiedot siirretään alkuperäisen lokitiedoston sijaintiin luotuun kansioon ”*rotate*”. Ilman erillistä määritystä aiemmat lokitiedot tallenetaan numerojärjestyksessä ilman muuta indikaattoria. Päivämäärän ilmoittaminen vanhaan lokitietoon on saatavuuden kannalta äärimmäisen tärkeää, joten tämä tieto lisätään määrityksellä ”*dateext*”. Määritys lisää tiedoston nimen perään päivämäärän muodossa VVVVKKPP, eli vuosiluku, kuukausi, päiväys. Päivämäärän muotoa on mahdollista muokata myös määrityksellä ”*dateformat*”, mutta tälle ei ole käytännön merkitystä vielä testiympäristön kohdalla.

Lokitietojen säilytyksen kannalta on tärkeää tiedostaa, että pitkäaikainen säilytys lokitiedolle saattaa syödä resursseja huomattavasti. Logrotate-järjestelmä tukee suoraan vanhojen lokitietojen pakkaamista, jolloin säilytettävä data voidaan säilöä tietoteknisesti tehokkaammin. Vanhan datan pakkaaminen vaikeuttaa kuitenkin tiedon saatavuutta, mutta ei tee tästä kuitenkaan mahdotonta. On kuitenkin otettava huomioon, että mikäli lokitietoa säilytetään esimerkiksi kymmenen vuoden ajalta, on tämä erittäin suuri määrä tietoa. Testiympäristön lokitietomäärällä yhden päivän lokitiedoston tiedostokoko on pakkaamattomana noin 7 MB. Logrotaten pakkaamisen jälkeen kyseinen päivittäinen lokitiedosto on kuitenkin enää vain 0,5 MB kokoinen. Pakkausmenetelmä on tehokas, joka takaa huomattavaa resurssien säästämistä järjestelmälle. Konfiguraatioon on tehty määritys ”*compress*”, joka päivittäin pakkaa vanhan lokitiedon. Järjestelmä käyttää pakkaamiseen oletuksena ilman erillista määritystä ”*gzip*”-ohjelmistoa. Konfiguraation viimeisenä määrityksenä on ”*delaycompress*”. Kyseinen määritys käskee järjestelmää viivyttämään pakkauksen seuraavaan sykliin,

eli esimerkkikonfiguraatiossa seuraavaan päivään. Esimerkiksi viikoittaista sykliä käyttäessä olisi mahdollista jättää lokitieto Elastic-järjestelmälle luettavaan muotoon viikon ajaksi. Tällöin Elastic-järjestelmälle tulisi kertoa vanhan lokitiedoston sijainti. Vaikka tiedostolla on muuttuva nimi päivämäärän lisäyksen takia, olisi tiedosto silti mahdollista saada luettua järjestelmään. Logrotaten luomia vanhoja lokitiedostoja nähtävissä Kuvio 25.

```
iwtopi@topi-01sv001:/var/log/firewall-logs/rotate$ ls -la
total 12768
drwxr-xr-x 2 syslog syslog    4096 Nov 27 06:25 .
drwxr-xr-x 3 syslog syslog    4096 Nov 23 17:58 ..
-rw-r----- 1 syslog adm     340255 Nov 15 06:25 WatchGuard-XTM.log-20211115.gz
-rw-r----- 1 syslog adm     350532 Nov 16 06:25 WatchGuard-XTM.log-20211116.gz
-rw-r----- 1 syslog adm     361227 Nov 17 06:25 WatchGuard-XTM.log-20211117.gz
-rw-r----- 1 syslog adm     471819 Nov 18 06:25 WatchGuard-XTM.log-20211118.gz
-rw-r----- 1 syslog adm     491902 Nov 19 06:25 WatchGuard-XTM.log-20211119.gz
-rw-r----- 1 syslog adm     475133 Nov 20 06:25 WatchGuard-XTM.log-20211120.gz
-rw-r----- 1 syslog adm     502373 Nov 21 06:25 WatchGuard-XTM.log-20211121.gz
-rw-r----- 1 syslog adm     518293 Nov 22 06:25 WatchGuard-XTM.log-20211122.gz
-rw-r----- 1 syslog adm     499223 Nov 23 06:25 WatchGuard-XTM.log-20211123.gz
-rw-r----- 1 syslog adm     550747 Nov 24 06:25 WatchGuard-XTM.log-20211124.gz
-rw-r----- 1 syslog adm     496898 Nov 25 06:25 WatchGuard-XTM.log-20211125.gz
-rw-r----- 1 syslog adm     499314 Nov 26 06:25 WatchGuard-XTM.log-20211126.gz
-rw-r----- 1 syslog adm    7482385 Nov 27 06:25 WatchGuard-XTM.log-20211127
```

Kuvio 25 Logrotate-ohjelmiston luomia pakattuja vanhoja lokitiedostoja.

Järjestelmään saapuvien lokitietojen graafiksi muodostamisen edellytyksenä on saada aikaan toimiva Grok-kuvio, joka osaa alkuperäisestä palomuurin viestistä poimia tarvittavat tiedot. Kuitenkin useiden erilaisten testaamisten ja kokeilujen jälkeen viestin sisältöä ei onnistuttu parsimaan. Grok-kuviointi osoittautui haastavaksi kokonaisuudeksi osana WatchGuard Firebox-järjestelmän palomuuriviestiä, joka on sisällöltään ja rakenteeltaan hyvin erikoinen. Esimerkkinä mahdollinen vaihtuva ID-numerointi, joka pitää sisällään monta sataa erilaista vaihtoehtoa. Jotta järjestelmä osaisi kertoa erilaisen numerosarjan perusteella tapahtuman tietoa, tulisi järjestelmään luoda ja syöttää monta sataa erilaista WatchGuard tietuetta. WatchGuard ei tarjoa aiemmin mainittuja ID-numeroinnin takana olevia tietoja suoraan muuten kuin katalogissaan, joka on PDF-muotoinen tiedosto (WatchGuard, 2021).

Grok-kuviointiin liittyvät testaukset toteutettiin aluksi suoraan palvelimella ja tuloksia pyrittiin seuraamaan web-näkymästä. Testausta hidasti huomattavasti palvelujen käynnistäminen uudelleen

aina muutosten jälkeen. Tästä syystä testausvaiheessa käytettiin erillistä virheen korjaajasovellusta, Grok Debuggeria. Sovellukseen voidaan syöttää haluttu lokitieto ja Grok-kuvio, jonka jälkeen sovellus näyttää parsitun lopputuloksen. (Grok Debugger, n.d.).

Grok-kuvion anteeksiantamattomuus hidasti myös testausta. Parsimiseen liittyvässä koodissa oleviin virheisiin järjestelmä antaa virheilmoituksen ”Compile ERROR”, joka ei viittaa mihinkään tiettyyn kohtaan. Virheen sattuessa mitään kohtaa parsimisesta ei suoriteta. Ristiriitaisuudet WatchGuard:n tarjoamassa katalogissa ja saadussa lokitiedossa luovat lisähaastetta oikeanlaisen parsimiskonfiguraation luomiseen. Myös tiedon nykyhetken epävarmuus luo lisää epävarmuutta siihen, että tulevaisuudessa muutoksia lokitiedon pohjarakenteeseen voisi tapahtua. Tällöin rakennettu avoimen lähdekoodin lokitietopalvelin muuttuisi hetkessä toimimattomaksi lokien selaamisen ja tutkimisen osalta. Tämä taas vaarantaa tietoturvan peruskäsitteen saatavuuden, koska lokitietojen nopeaa tutkimista on estetty tai häiritty. Saatujen tulosten perusteella palvelun kehittämiseen käytettävää aika käytettiin Dimension-järjestelmän tutkimiseen. Opinnäytetyön tekijä sekä toimeksiantaja olivat yhteisymmärryksessä asian suhteen, että avoimeen lähdekoodiin perustuvan ratkaisun toteuttaminen täysin toimivana ratkaisuna edellyttäisi vahvaa spesifiä osaamista tietyiltä osa-alueilta. Näiden osa-alueiden tutkimiseen ja opetteluun käytettyä aikaa ei pidetty järkevänä. Tärkeämpänä pidettiin saatua tutkimustulosta ja sitä, kuinka avoimen lähdekoodin lokien säilömiseen käytettyä rsyslog-palvelua voitaisiin mahdollisesti käyttää Dimension-järjestelmän kanssa.

5.2.2 Yhteenveto

Opinnäytetyön tekijän olettamuksena oli, että avoimeen lähdekoodiin perustava ratkaisu saataisiin täysin vertailukelposeksi kokonaisuudeksi. Kuitenkin aiemmin esitetyt haasteet palvelun pystyttämisessä ja lopullisen kunnollisen palvelun toteutuksessa estivät kaikkien osa-alueiden vertailun. Esimerkiksi erilaisia näkymiä pohjautuen lokitietoihin ei saatu toteutettua. Kuitenkin pystytettyjä palveluita ja siihen kuuluvia osia pyritään vertaamaan ja ottamaan niiden tulokset mukaan tutkimustuloksiin.

6 Tutkimustulokset

Opinnäytetyö suoritettiin kehittämistutkimuksena, jonka valossa opinnäytetyön eri osa-alueita vertailtiin. Kehittämistutkimus aloitettiin molempien järjestelmien kohdalla täysin nollasta, koska olemassa olevia järjestelmiä ja palveluita ei ollut olemassa. Pernaa (Pernaa, 2013) kertoo, että kehittämisprosessin osana on välttämätöntä olla autenttisissa olosuhteissa tapahtuvaa testausta. (Pernaa, 2013). Opinnäytetyö toteutettiin täysin ympäristössä, joka pyrki osittain kuvastamaan oikeaa tuotantoympäristöä. Tuotantoympäristön mukaista täydellistä ja oikeaa tietoverkkoliikennettä ei kuitenkaan täysin voida toteuttaa testiympäristöön tarkoitetulla alustalla, mutta tiettyjä oikeita elementtejä pystytään tuomaan testiympäristön tarjoamasta alustasta esille. Tärkeimpänä puuttuvana osana on selkeästi eri laitteiden tuottama oikea tietoverkkoliikenne, josta muodostuva lokitieto kuormittaa WatchGuard-palomuurilaitteistoa ja siihen liitettyjä lokipalvelimia erilaisella kuormalla. Kuorma on osittain laskettavissa tarjolla olevista ennakkotiedoista, mutta kuorman laskeminen voi osoittautua haasteelliseksi. Tällöin on käytettävä seurantaa palvelujen pystytys- ja alkuvaiheilla, mikä takaa palvelujen osalta tärkeää informaatiota. Pystytysvaiheessa saatavan tiedon perusteella pystytään takaamaan palveluille tarpeellinen resurssimäärä.

Tutkimustulokset puoltavat vahvasti sitä, että WatchGuard on pyrkinyt ulkoisen, avoimeen lähdekoodiin perustuvan ratkaisun olevan haasteellinen rakentaa toimivaksi kokonaisuudeksi. Saatavilla olevien dokumentaation ristiriitaisuus todelliseen tietoon, esimerkiksi lokitiedon sisällön rakenteeseen liittyen, luo epäluotettavaa kuvaa yrityksestä ja heidän tarkoitusperistään.

Vastapainoksi haasteelliselle avoimen lähdekoodin ratkaisulle WatchGuard tarjoaa kuitenkin erittäin kattavan ja monipuolisen oman Dimension-järjestelmän lokitietojen tutkimiseen, seurantaan ja säilömiseen. Saatavilla olevat erilaiset valmiit ratkaisut järjestelmän parantamiseen takaavat, että järjestelmistä on mahdollista rakentaa tietoturvallinen kokonaisuus. WatchGuard:n tarjoamat ohjeistukset oman palvelunsa kehittämiseksi ovat kattavat. Erillisen lokien säilöntään tarkoitetun palvelimen liittäminen Dimension-järjestelmään on tärkeä lisä palvelulle. Palvelun käytön rajaaminen virtuaalialustalle on jokseenkin rajoittava tekijä tietynlaisissa tuotantoympäristöissä, jotka voisivat käyttää WatchGuard:n tuotteita, mutta eivät pystyisi resursoimaan itselleen virtuaalialustaa käyttöön.

Asetettujen kriteerien pohjalta WatchGuard Dimension -järjestelmä ja avoimen lähdekoodin ratkaisu eroavat tietyillä osa-alueilla, mutta eivät kriittisesti. Suurimpana erona erottuu selkeästi järjestelmien pystytykseen vaadittavat taitotasot erilaisista järjestelmistä. Dimension-järjestelmän pystytys ja käyttöönotto on selkeä ja suoraviivainen, kun taas avoimen lähdekoodin ratkaisu vaatii paljon erilaisten järjestelmien tuntemusta, osaamista ja konfigurointia.

Molemmat järjestelmät pystyvät takaamaan käyttäjien autentikointiin ja ylläpitämiseen erinomaiset työkalut. Tällöin järjestelmään annettavien käyttöoikeuksien avulla pystytään helposti kontrolloimaan, että tiedon luottamuksellisuus ja eheys pysyvät kunnossa. Saatavuuteen liittyvät asiat ovat myös osittain käyttöoikeuksien takana, mutta suurimmalta osalta saatavuuteen liittyvät järjestelmien tarjoamat palvelut ja kuinka ne toteutetaan. Molemmat palvelut takaavat yritykselle olennaisen palvelun, eli Windows Active Directory -pohjaisen käyttäjien saatavuuden.

Järjestelmien palveluiden tarjoamien mahdollisuuksien avulla lokitiedon saatavuus pystytään takaamaan myös vuosien takaa. Palveluiden pystyttämisen yhteydessä saatujen tietojen avulla pystytään myös tiettyjä palveluita yhdistämään, jolloin tiedon oikeaoppista säilömistä voidaan harjoittaa entistä paremmin. Avoimen lähdekoodin ratkaisussa toteutettu logrotate-ohjelmiston tarjoama kokonaisuus lokitietojen kierrättämiseen takaa sen, että Dimension-järjestelmästä varmuuskopioidut lokitiedot voidaan säilöä pakatussa muodossa. Tämä taas takaa pienemmän resurssitarpeen, mikä tuo säästöjä palvelun kustannuksiin.

Palveluiden tietoturvaa voidaan parantaa huomattavasti pelkästään toteuttamalla ne suoraan palomuurin taakse. Tällöin palomuurille voidaan suoraan luoda säännöstö, joka estää palveluiden käytön suoraan ulkoverkosta. Palveluita pystyttäisiin tällöin hyödyntämään ilman fyysistä läsnäoloa käyttämällä suojattua etäyhteyttä. Dimension-järjestelmän suljetun lähdekoodin takia kyseisen palvelun käyttämää palvelinta ei pystytä erillisillä ohjelmilla ja muutoksilla itse koventamaan. Tällöin on luotettava täysin WatchGuard:n tekemiin ratkaisuihin palvelinalustan suhteen. Avoimen lähdekoodin ratkaisussa jokainen kovennus on täysin itse päätettävissä ja kontrolloitavissa. WatchGuard tarjoaa kuitenkin Dimension-järjestelmälle jatkuvia päivityksiä, jotka pystytään ajamaan järjestelmään helposti käyttöliittymän kautta. Avoimen lähdekoodin ratkaisussa tulisi ylläpi-

totoimet huolehtia täysin itse. Automatisointi usean palvelun alustalla ei ole suotavaa, koska järjestelmiin tulevat päivitykset voivat rikkoa kokonaisuuden toiminnan esimerkiksi ohjelmistovirheen vuoksi.

Avoimen lähdekoodin palvelusta ei onnistuttu rakentamaan täydellistä kokonaisuutta, jolloin pystyttäisiin vertailemaan itse palvelun tarjoamia palveluita lokitietojen tutkimiseen. Käytetty avoimen lähdekoodin alusta tarjoaa kuitenkin mahdollisuuden kyseisille ominaisuuksille täysin, mikäli lokitieto olisi saatu järjestelmään sen ymmärtämässä muodossa. On kuitenkin myös ymmärrettävä, että tämän rakentaminen olisi syönyt myös huomattavasti resursseja. Avoimen lähdekoodin järjestelmän vaikeuksien kautta voidaan myös päätellä, että mahdollisesti saman palvelun ylläpito ja kehittäminen olisivat saattaneet osoittautua yhtä vaikeiksi projekteiksi. Palvelun tarkoituksena ei ole olla työntekijöille jatkuva kehityskohde ja aikaa syövä kokonaisuus. Palvelun on tarkoituksena antaa yritykselle ja sen työntekijöille lisäarvoa ympäristön hallintaan ja tietoturvan tarkkailuun.

Opinnäytetyön tarjoama palvelukokonaisuus tuo toimeksiantajalle paljon lisäarvoa, mutta tekniikan alan näkökulmasta katsoen järjestelmäkokonaisuus ei ole merkittävä tai uusia toimintoja tarjoava. Työn tarkoituksena ei luoda yleisesti mitään mullistavaa, vaan tarjota toimeksiantajalle näkökulmia eri palveluiden tarjoamille ominaisuuksille. Opinnäytetyön rajoittuvuus tietyn merkkiseen palomuurilaitteistoon on osana työtä, koska palomuuriratkaisut eivät tarjoa lokitietoa niin sanotussa yleispätevässä muodossa, vaan ovat aina merkkikohtaisia. Tämän takia lokitusratkaisuja ei pysty suoraan koskaan käyttämään eri valmistajan laitteissa, vaan ne vaativat aina ammattilaisen tekemiä muutoksia järjestelmiin.

7 Johtopäätökset

Tutkimustulosten perusteella voidaan todeta, että järjestelmien pystyttämiseen käytettävät resurssit eroavat valtavasti. Avoimeen lähdekoodiin perustuvan ratkaisun kanssa on myös taisteltava paljon erilaisten ongelmien kanssa, joidenka ratkaiseminen vaatii paljon erilaisten järjestelmien tuntemusta ja oppimista. Vaikka tietotekniikan alalla palveluiden ylläpito ja kehittäminen ovat aina osana työtä ja erilaisia järjestelmiä, ei näistä haluttu kehittää liikaa ylimääräistä kuormaa opinnäytetyön toimeksiantajalle.

Saatujen tulosten perusteella toimeksiantajalle ehdotetaan Dimension-järjestelmän pystytystä yhdistäen avoimen lähdekoodin ratkaisusta saatua toteutusta lokitietojen kierrättämiseen. Yhdistämällä näin kahdesta palvelusta parhaat puolet saadaan toimeksiantajalle tarjottua käyttäjäystävällinen käyttöliittymä, helposti kehitettävä ja ylläpidettävä ympäristö, jonka taustalla olevat järjestelmät ovat tietoturvallisia. Myös lokitietojen säilytys pystytään toteuttamaan yrityksen antamilla määritteillä ja takaamaan tiedon saatavuus aina. Järjestelmän kehittämistyössä ja ylläpitoon liittyvissä toimissa pystytään myös antamaan näkökulmat. Järjestelmän kannalta on myös oleellista, että pystytysvaiheessa on mukana vähintään yksi toinen ammattilainen, jolloin järjestelmään liittyvät kriittiset osa-alueet pystytään selkeästi kuvaamaan toiselle taholle. Järjestelmän oikeaoppinen dokumentointi on myös osana sen perustamista, jolloin järjestelmän kokonaiskuva on otettu huomioon myös yrityksen jatkuvuussuunnitelmassa.

8 Pohdinta

Opinnäytetyön edetessä on opittu käsittelemään lokitietoa asiankuuluvasti ja käyttämään säilömiseen tietoturvan perusteita, luotettavuutta, eheyttä ja saatavuutta. Palvelujen pystyttämiseen vaadittavien resurssien ja taitotason vaihtelevuus tuli opinnäytetyön tekijälle yllätyksenä. Työn tekijällä oli vahva käsitys, että molemmat palvelut saataisiin huomattavasti vertailukelpoisempaan asemaan, jolloin palvelujen tarjoamia käyttöliittymiä olisi pystytty vertaamaan. Toteutetuilla järjestelmillä on valtavasti potentiaalia antaa yritykselle lisäarvoa lokitietojen säilytyksen, selaamisen ja tarkkailun kannalta.

Suurimpana haasteena opinnäytetyössä tekijä pitää ehdottomasti avoimen lähdekoodin ratkaisussa olevaa lokitiedon tulkintaa ja siihen liittyviä haasteita. Lokitietoviesti oli vaihteleva kokonaisuus, johon liittyvät dokumentaatiot eivät täsmänneet täysin todellisuuteen. Myös lokitietoviestin parsiminen aiheutti työn tekijälle paljon hankaluuksia, jotka koituivat lopulta toisen järjestelmän vajaavaisuuteen.

Työn tekijän osallistuminen lopullisen tuotantoympäristöön pystytettävän ratkaisun rakentamiseen edesauttaa palvelun oikeaoppista käyttöä ja hallinnointia. Järjestelmien pystytykseen liittyvissä asioissa voidaan varmistua, että lokitiedot tullaan säilömään oikeaoppisesti ja vaadituilla määritteillä. Myös aiemmassa kappaleessa mainitun jatkuvuussuunnitelman kannalta toteutettu dokumentaatio järjestelmistä takaa erilaisissa häiriötilanteissa palveluiden jatkumisen.

Lähteet

DB-Engines Ranking of Search Engines. 2021. DB-Engines-sivuston listaus hakukoneohjelmistojen kuuluisuden ja käytön mukaan. Viitattu 5.4.2021. https://db-engines.com/en/ranking/search+engine

Elastic. N.d. Drop fields from events. https://www.elastic.co/guide/en/beats/filebeat/current/drop-fields.html

Elastic. Grok filter plugin. 2021. Viitattu 23.11.2021. https://www.elastic.co/guide/en/logstash/current/plugins-filters-grok.html

Elastic. What is Elasticsearch? 2021. Kuvaus Elasticsearch-ohjelmasta. Viitattu 5.4.2021. https://www.elastic.co/what-is/elasticsearch

Finlex. Henkilötieto – Arkaluonteinen henkilötieto. 4.4.2006. Viitattu 21.3.2021. https://finlex.fi/fi/viranomaiset/ftie/2006/20060001

GNU Operating System. 2020. GNU lisenssin informaatiosivusto. Viitattu 28.3.2021. https://www.gnu.org/licenses/gpl-3.0.html

Grok Debugger. n.d. Grok-kuvion testaukseen suunnattu työkalu. Viitattu 27.11.2021. http://grokdebug.herokuapp.com/

Isoweli Oy. N.d. Yrityskuvaus verkkosivuilla. Viitattu 8.2.2021. https://isoweli.fi/

Katakri 2020. Kansallinen turvallisuusviranomainen. Tietoturvallisuuden auditointityökalu viranomaiselle. Viitattu 20.11.2021. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Troan, E., Brown, P., Kaluza, J. n.D. Logrotate(8) – Linux man page. https://linux.die.net/man/8/logrotate

Pernaa, J. 2013. Kehittämistutkimus tutkimusmenetelmänä. Viitattu 21.3.2021. https://helda.helsinki.fi/bitstream/handle/10138/317958/2013_Pernaa_KT_tutkimusmenetelmana_KT_kirja.pdf

PuTTy. n.d. SSH-asiakasohjelma. Viitattu 22.11.2021. https://www.putty.org/

Log Message Catalog, WatchGuard. Päivitetty 5/2020. Firebox-laitteen lokiviestien katalogi. Viitattu 21.3.2021. https://www.watchguard.com/help/docs/fireware/12/en-US/log_catalog/Log-Catalog_v12_6.pdf

Lokien keräys ja käyttö. 2016. Viestintävirasto. Viestintäviraston ohjeistus lokitietojen tallentamiseen ja käyttöön. Viitattu 5.4.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitusohje.pdf

Maier, W. 29.11.2016. Erweiterte Log-Auswertung mit graylog. Viitattu 23.11.2021. https://www.boc.de/watchguard-info-portal/2016/11/erweiterte-log-auswertung-mit-graylog/

rsyslog. 2020. Ohjelmiston kuvaus verkkosivuilla. Viitattu 23.11.2021. https://www.rsyslog.com/

Traficom. Näin keräät ja käytät lokitietoja. 21.7.2020. Ohjeistus lokitietojen keräämiseen ja käyttämiseen. Viitattu 5.4.2021. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

Ubuntu. 2021. Ubuntu Server lataussivusto ja tietoa uusimmasta versiosta. Viitattu 28.3.2021. https://ubuntu.com/download/server#releases

Ubuntu. 2020. What is an Ubuntu LTS release? Blogi-kirjoitus Ubuntun versionhallintaan liittyen. Viitattu 28.3.2021. https://ubuntu.com/blog/what-is-an-ubuntu-lts-release

VAHTI 3/2009 Lokiohje. Päivitetty 9.6.2020. Valtiovarainministeriön ohjeistus lokitukseen. Viitattu 28.2.2021. https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-32009-lokiohje

Viemerö, M. 2017. Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet – Työpaja #2 – 18.8.2017. Valtiovarainministeriön yhteishankkeiden työpajamateriaali. Viitattu 5.4.2021. https://vm.fi/documents/10623/4914009/JUHTA+tietosuoja+lokitus+180817/14baba1f-98e5-4887-b3e4-65a98f465e75

WatchGuard. 2021. Configure Syslog Server Settings. Viitattu 23.11.2021. https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/logging/send_logs_to_syslog_c.html

WatchGuard. 2021. Install WatchGuard Dimension. Viitattu 20.11.2021. https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/dimension/install_dimension_d.html

WatchGuard. 5/2020. Fireware v12.6. Log Message Catalog. Viitattu 23.11.2021. https://www.watchguard.com/help/docs/fireware/12/en-US/log_catalog/Log-Catalog_v12_6.pdf

WatchGuard. 2021. Security Dashboard (Dimension). Viitattu 21.11.2021. https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/dimension/dashboard_security_d.html

WatchGuard. 2021. Set Up & Administer Dimension. Viitattu 18.11.2021. https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/dimension/about-dimension_d.html?tocpath=Fireware%7CDimension%7C_____0

WatchGuard. 2021. Threat Map. Viitattu 21.11.2021. http://www.watchguard.com/help/docs/fireware/12/en-us/Content/en-US/dimension/threat_map_d.html

WatchGuard. 2020. Yrityskuvaus verkkosivuilla. Viitattu 6.3.2021. https://www.watchguard.com/wgrd-resource-center/docs/watchguard-brochure

WatchGuard, 2020. WatchGuard Dimension v2.1.2 Update 4 Release Notes. Viitattu 22.11.2021. https://www.watchguard.com/support/release-notes/fireware/12/en-US/EN_ReleaseNotes_Dimension_v2_1_2/index.html

Liitteet

Liite 1. Rsyslog 10-custom.conf tiedostoon tehdyt muutokset

```
if $hostname == 'IWdemoXXX' then {

/var/log/firewall-logs/WatchGuard-XTM.log

~

}
```

Liite 2. /etc/filebeat/filebeat.yml tehdyt muutokset

processors:

- drop_fields:

fields: ["message.keyword", "fileset.name", "event.timezone.keyword", "tags", "_score", "agent.ephemeral_id", "agent.name", "host.name", "host.name.keyword", "version", "version.keyword", "agent.hostname", "agent.id", "agent.type", "agent.version", "ecs.version", "input.type", "log.offset", "version"]

Liite 3. /etc/logrotate.d/rsyslog -konfiguraatiotiedosto

```
/var/log/firewall-logs/WatchGuard-XTM.log

{

rotate 14

daily

copytruncate

olddir /var/log/firewall-logs/rotate

dateext

compress

delaycompress




}
```