jamk.fi

IDS-palvelun kartoitus

Alexander Puhakka

Opinnäytetyö
Huhtikuu 2021
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), Tieto- ja viestintätekniikan tutkinto-ohjelma

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Puhakka Alexander	Opinnäytetyö, AMK	Huhtikuu 2021
	Sivumäärä 51	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
IDS-palvelun kartoitus

Tutkinto-ohjelma
Tieto- ja viestintätekniikka

Työn ohjaaja(t)
Kotikoski Sampo, Häkkinen Antti

Toimeksiantaja(t)
YSP Oy

Intrusion Detection System (IDS) on tietoliikenteen valvontaan käytettävä järjestelmä. IDS analysoi läpikulkevaa datan paketteja syvällisemmin perinteisen palomuurin lisäksi muodostaen hälytyksiä havainnoista, jotka tunnistetaan joko tunnisteiden tai poikkeamien avulla, tuoden älykkäämpää valvontaa järjestelmiin. IDS on yleistynyt roimasti viime vuosikymmenien aikana, jopa niin paljon, että tänä päivänä useat palveluntarjoajat ovat valmiiksi integroineet IDS:n heidän palomuuri-järjestelmiinsä.

Tarkoituksena oli selvittää, onko IDS tarpeellinen ja soveltuva toimeksiantajan ympäristöön. Selvitys tehtäisiin kartoittamalla vaatimukset ja tarvittavat ominaisuudet, joita IDS:ltä odotetaan, ja etsittäisiin niiden pohjalta sopivat palvelu- ja ohjelmistovaihtoehdot.

IDS-palvelun kartoitus toteutettiin YSP Oy:lle. Kartoitettavana ympäristönä toimi heidän tarjoamansa Traffic Gateway -palvelu, joka on asiakkaille keskitetty yhteyksien hallintaan keskittyvä palvelu. Järjestelmään oltiin toivottu saavan tietoliikenteeseen lisää näkyvyyttä kasvaneen käyttäjä- sekä datamäärän vuoksi, jonka vuoksi IDS-järjestelmän ominaisuuksien korkeampi havainnointi ja lokitus järjestelmässä alkoi kiinnostamaan.

Kartoitus toteutettiin tutustumalla ensin lähemmin IDS-järjestelmän toimintaan ja eri ominaisuuksiin sekä kohdeympäristöön. Toimeksiantajan kanssa käytiin läpi vaatimuksia palvelulle, jonka avulla pystyttiin tunnistamaan ympäristöön mahdollisesti sopivat palvelumuodot ja ohjelmistovaihtoehdot. Sopivin vaihtoehto pyrittiin löytämään vertailemalla vaihtoehtoja keskenään.

Lopputuloksena tehtiin hankintasuositus kahdesta eri palvelumuodosta, jotka koettiin sopivan Traffic Gateway -palveluun. Toinen loisti halpojen kustannuksien vuoksi toisen ollessa ominaisuuksiltaan kattavampi. Molemmilla etuna oli helppo käyttöönotto.

Avainsanat (asiasanat)
Tietoliikenne, IDS, Palomuuri, Snort, Suricata, Kartoitus

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Puhakka Alexander	Bachelor's thesis	April 2021
		Language of publication: Finnish
	Number of pages: 51	Permission for web publication: x

Title of publication
Mapping of IDS service

Degree programme
Communication and information technologies

Supervisor(s)
Kotikoski Sampo, Häkkinen Antti

Assigned by
YSP Oy

Intrusion Detection System (IDS) is a network-monitoring system with a purpose to deeply analyze incoming network traffic and making alerts of its discoveries, bringing smarter monitoring to the network besides the traditional firewall. IDS uses fingerprints or anomalies to discover harmful activity in the network. In recent decades, IDS has grown in popularity and today many of the leading service providers implement IDS systems inside their firewall services.

The object was to research if an IDS-system is necessary and functional in the clients environment. This was done by mapping out the requirements for the service such as the necessary features. Based on the results a couple of different Service and software options would then be chosen for more in depth review.

Mapping was made for YSP Oy and their traffic Gateway -service, that they offer for clients. Traffic Gateway Is an environment, focused on giving the customer a carefree maintenance over their connections to their devices. Because of rising amount of users and traffic in the network, YSP wanted more awareness in the network side. IDS focused on these kinds of features, which raised interest for the system.

First part in the mapping was to study IDS and the target network about its features and capabilities. Requirements were gone through with the client, which were then used to identify possibly suitable IDS-services and software. The best choice was going to be picked by comparing the candidates with each other.

At the end a purchase proposal was made about two different service formats, which were seen as good candidates for the target network. The first ones assets were low costs whereas the other ones assets was its amount of features. Both shined with their easy deployment

Keywords/tags (subjects)
Networking, IDS, Firewall, Snort, Suricata, Mapping

Miscellaneous (Confidential information)

Sisältö

Sisältö **1**

1 Johdanto **4**

1.1 Tutkimusmenetelmä ja kysymykset 5

1.2 Tarve 5

1.3 Tavoitteet 6

1.4 Toimeksiantaja 7

2 Intrusion Detection System (IDS) **9**

2.1 Aktiivinen ja Passiivinen valvonta 9

2.2 Säännöt (Signature based- and anomaly based detection) 10

2.3 Suodatus 12

2.4 Sensoreiden sijoittelu 13

3 Traffic Gateway **15**

3.1 Ympäristö 16

3.2 Valvonta 18

3.3 Palomuuri 18

3.3.1 Tiedonsiirto Traffic Gateway -palvelussa 20

4 Yrityksen vaatimukset IDS-palvelulle **21**

4.1 Yleiset vaatimukset 21

4.2 IDS-palvelun vaikutus havaittuihin riskeihin 23

5 IDS-palveluiden vertailu **26**

5.1 Palveluvaihtoehdot 26

5.1.1 Snort ja Suricata -ohjelmistot 26

5.1.2 Pfsensen paketti vai itsenäinen palvelin 28

5.1.3 Palveluntarjoajan palvelut 29

5.2 Ohjelmisto/palvelu vertailu 30

5.3 Palvelun resurssivaatimukset 32

5.3.1 Testaus 35

5.4 Kustannukset 41

6 Pohdinta 45

6.1 Johtopäätökset 45

6.2 Hankintasuositus 47

6.2.1 Pfsense paketti 47

6.2.2 VaultSec-palvelu 48

Lähteet 49

Kuviot

Kuvio 1. YSP Oy Tiivistelmä (YSP Oy n.d.) 7

Kuvio 2. Network based intrusion detection system esimerkki 14

Kuvio 3. Host based intrusion detection system esimerkki 15

Kuvio 4. Traffic Gateway ympäristökuvaus 16

Kuvio 5. Pfsense dashboard 20

Kuvio 6. Palomuurin resurssit ennen aktiivista IDS-valvontaa 33

Kuvio 7. Palomuurin resurssit aktiivisen IDS-valvonnan aikana 34

Kuvio 8. Snort Global settings 36

Kuvio 9. Snort rajapinta asetukset 37

Kuvio 10. IDS-hälytykset osa1 39

Kuvio 11. IDS-hälytykset osa2 39

Kuvio 12. Palomuurin muistin käyttö viikon ajalta 40

Kuvio 13. Palomuurin prosessorin käyttö viikon ajalta 40

Taulukot

Taulukko 1. Protokollat Traffic Gateway -palvelussa 22

Taulukko 2. Riskianalyysi 24

Taulukko 3. VaultSec palvelutasot 29

Taulukko 4. Pfsense paketti palvelumuodon kustannusarvio 42

Taulukko 5. Itsenäinen palvelin palvelumuodon kustannuasrvio 43

Taulukko 6. VaultSec Enterprise palvelumuodon kustannusarvio 44

Lyhenteet

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
VPN	Virtual Private Network
IPSec	Internet Protocol Security
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
SNMP	Simple Network Management Protocol
LIVA	Liikennevalo järjestelmä
MPOJ	Muuttuva pysäköinninopastus järjestelmä
NGFW	Next Generation Firewall
CPU	Central Processing Unit, prosessori
RAM	Random Access Memory, Keskusmuisti
TLS	Transport Layer Security
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network

1 Johdanto

Opinnäytetyössä käsitellään tietoliikenteen valvontaan käytettäviä IDS, eli Intrusion Detection System -järjestelmiä. Työssä selvitettiin eri IDS-järjestelmien ominaisuuksia ja toimintatapoja vahvistaa verkon turvallisuutta. Selvitys tehtiin pääasiassa etsimällä tietoa erilaisista IDS toteutuksista netistä, sekä selaillen ihmisten kokemuksia eri foorumeilta. Tiedonkeruun avulla kohdistettiin palvelun tyyppi yrityksen tarpeisiin ja vaatimuksiin, minkä jälkeen palvelu vaihtoehtoja vertailtiin keskenään ja tuotiin esille jokaisen palveluvaihtoehdon vahvuudet. Sen jälkeen lähdettiin testaamaan palveluntarjoajan avustuksella, miten palvelu vaikuttaisi nykyiseen järjestelmään sekä minkälaista dataa järjestelmä tuottaisi. Testeissä hyödynnettiin palveluntarjoajan tarjoamaa palvelua. Testeistä kerättyä dataa analysoitiin kokouksessa palveluntarjoajan kehittämän dokumentin avulla, jonka jälkeen arvioitiin palvelun kannattavuus yritykselle.

Toimeksiantajana opinnäytetyölle toimii YSP Oy. YSP on suomalainen ICT-yritys, joka on erikoistunut älykkään liikenteen erilaisiin toteutuksiin. Yritys tarjoaa Traffic Gateway nimistä palvelua, jonka yhteyksiä hallitaan palomuurin voimin. Vahvemmalle tietoturva järjestelmälle oli ollut kysyntää kasvavan asiakasmäärän ja datan vuoksi, minkä seurauksena palvelua lähdettiin työstämään. Sen lisäksi yhteyksien päässä kenttälaitteiden fyysinen turvallisuus ei ollut YSP:n hallittavissa, joten haluttiin varautua omassa päässä mahdollisimman hyvin tilanteisiin, jossa mahdollinen laitekaappaus tai luvaton verkkoon kytkeytyminen ja sen kautta tehtävä hyökkäys voitaisiin havaita ja parhaimmassa tapauksessa myös estää. Yritys toivoi IDS-palvelun auttavan valvomaan käyttäjien tekemiä toimenpiteitä sekä parantamaan tietoliikenteen datan monitorointia ja sen hallintaa, jonka jälkeen IDS-palvelua voisi mahdollisesti tarjota eteenpäin asiakkaille.

1.1 Tutkimusmenetelmä ja kysymykset

Tutkimuskysymyksiä lähdettiin selvittämään käyttämällä tutkimusmenetelmänä soveltavaa tutkimusta. Soveltavassa tutkimuksessa käytetään jo olemassa olevaa informaatiota ja sovelletaan sitä paikantamaan ratkaisut kohdistettuihin ongelmiin. Tämän työn tapauksessa kartoitetaan IDS-palvelun tarve Traffic Gateway -palvelussa hyödyntäen toimeksiantajalta saatuja dokumentaatioita. Lisäksi yritetään miettiä ratkaisut havaittuihin ongelmiin ottaen huomioon IDS-järjestelmän tuomat ominaisuudet. (Tuomi, S. & Latvala, E N.d.)

Työssä rajataan toimeksiantajan kanssa palvelukohtaiset vaatimukset ja kehityskohteet, joita toivotaan IDS-palvelun avulla parantaa, peilaten näitä Traffic Gateway -palveluun. Vaatimuksien ja kehityskohteiden pohjalta esitellään eri työkaluja ja tekniikoita, joita vertaillaan toisiinsa. Vaihtoehtojen parista valitaan palvelu, joka parhaiten sopisi yrityksen tarkoituksiin.

Kartoitettava palvelu tulee osaksi olemassa olevaa palvelua, jonka vuoksi tutkimuskysymykset mietittiin huomioiden nykyisen palvelun kehityksen. Tutkimuskysymykset ovat lueteltuna alla olevassa listassa, joka koostuu yhdestä pääkysymyksestä, sekä useasta tarkentavasta kysymyksestä.

- Onko IDS-palvelun lisääminen Traffic Gateway -palvelun yhteyteen järkevää tietoturvan kannalta
    - Vahvistaako IDS-palvelu yleistä tietoturvaa palvelussa
    - Mitkä toiminnallisuudet IDS-järjestelmään tarvitaan?
    - Mikä IDS-toteutus olisi käytännöllisin yritykselle?
    - Onko IDS-palvelun lisääminen nykyiseen palveluun taloudellisesti kannattavaa?
    - Vaikuttaako IDS negatiivisesti verkon toimintaan?

1.2 Tarve

Yrityksellä on tällä hetkellä palvelussa OSI-mallin L4-tasolla toimiva palomuurisääntöpohjainen kahdennettu palomuuri käytössä, jolla hallitaan tulevaa ja lähtevää liikennettä. Palomuuri estää vain sen liikenteen, mikä ei täytä sääntöjen kriteerejä. Kriteerit koostuvat lähde ja kohde osoitteesta, liikenteen käyttämästä protokollasta sekä

lähde ja kohde portista, eikä täten osaa analysoida sääntöjen läpi pääsevää liikennettä syvällisemmin. Palomuurisäännöissä on sallittu laajasti yleisesti käytössä olevia protokollia, joiden kautta osaava hyökkääjä osaisi naamioida itsensä muun liikenteen joukkoon. Palomuurin takana olevissa verkoissa on yritykselle kriittisiä palvelimia, joista yhteyksiä voi olla julkisilta alueilta löytyviin laitteisiin kuten liikennevaloihin tai ilmoitustauluihin. Kentällä olevien laitteiden tietoturvaa on vaikeata nostaa, koska laitteet ovat asiakkaiden omistamia ja ylläpitämiä. Sen seurauksena toimeksiantaja halusi lähteä vahvistamaan palomuurin rajapintojen tietoturvaa syvemmällä tietoliikenteen analyysillä.

1.3 Tavoitteet

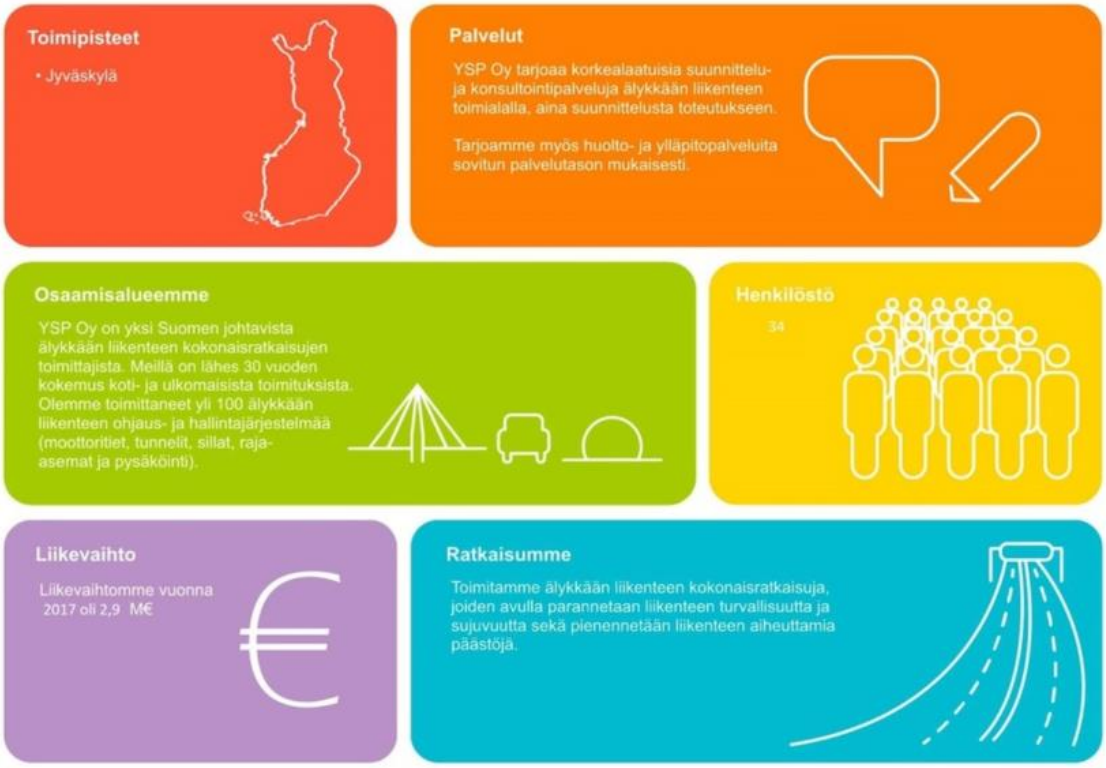
Päätavoitteena yleisesti on kartoittaa ja valita yritykselle sopiva IDS-järjestelmä, joka vahvistaisi tietoturvaa yrityksen kriittisissä palveluissa. Vahvempi tietoturva mahdollistaisi paremman perustan tarjota palveluita asiakkaille aiempaa korkeammalla tietoturvatasolla. Tähän liittyen laajan IDS palvelutarjonnan takia tavoitteena on löytää yrityksen tarpeisiin sopivin vaihtoehto. Palvelun tulisi olla sellainen, joka olisi helppo yhdistää olemassa olevien järjestelmien kanssa, sekä sisältäisi ominaisuuksia, joista yritys voisi hyötyä nyt ja myös kehittää jatkossa.

IDS-palvelut mahdollistavat kattavan datan seurannan ja talletuksen, joka yleisen tietoturvan lisäksi mahdollistaisi yrityksen paremmin monitoroimaan verkossa liikkuvaa liikennettä, erityisesti julkisiin portteihin tulevaa liikennettä. Tavoitteena on tällä tavoin pystyä jatkossa tunnistamaan turhaa ja ei haluttua liikennettä verkossa sekä estämään mahdolliset uhkatekijät. Näin vältyttäisiin turhilta kaistan kuormituksilta, ja mahdollistettaisiin nopeat yhteydet asiakkaille.

IDS-järjestelmän tullessa jo olemassa olevan palvelun yhteyteen, on tärkeää huomioida, miten IDS:n lisäys palvelun rakenteeseen vaikuttaa kustannuksissa ja toiminnallisuudessa. Siksi tavoitteena on löytää kustannustehokas IDS-ratkaisu, joka sisältää tarpeeksi ominaisuuksia, mutta ei vaikuta muuhun ympäristön toimintaan negatiivisesti.

1.4 Toimeksiantaja

YSP Oy on Suomalainen tekniikan yritys, joka on erikoistunut tarjoamaan älykkään liikenteen ratkaisuja asiakkaille yli 30 vuoden ammattitaidolla. YSP on alkuisin Jyväskylästä, jossa toimisto sijaitsee tänä päivänäkin. Yritys on suhteellisen pieni, työllistäen vähän yli 30 henkeä. Henkilökunnan osaaminen kattaa sähkö-, automaatio- ja ICT-puolen tehtävät, joiden avulla yritys voi tarjota korkealaatuisia suunnittelu ja konsultaatio palveluja asiakkaille(kts. Kuvio 1).(YSP Oy n.d.)



Kuvio 1. YSP Oy Tiivistelmä (YSP Oy n.d.)

YSP on osana Dynniq konsernia, joka kuuluu kansainvälisesti johtaviin älykkään liikenteen toteuttajiin ja työllistää kaiken kaikkiaan jopa 1600 henkeä 13:sta eri maassa. Suomen konserni on jaettu kahteen osaan, jotka kuuluvat Dynniq Finland Holding Oy:n alle, joka on osa Dynniq Nordic -yksikköä. Toinen Dynniq Finland Holdingin alla toimivia yhtiö on Dynniq Finland, jonka kanssa YSP Oy tekee läheistä yhteistyötä. Dynniq Finland Oy:n tuorein julkinen liikevaihto on julkaistu vuoden 2019 lopussa,

jolloin liikevaihto oli 10,6 miljoonaa euroa. YSP:n oma liikevaihto vuoden 2019 lopussa oli 2,7 miljoonaa euroa.(YSP Oy n.d.)

YSP perustettiin vuonna 1984 Jyväskylässä. Tällöin Yritys tunnettiin nimellä Yleinen Sähköpalvelu Oy, joka on nykypäivänä lyhennetty vain alkukirjaimiin. Yritys tarjosi alun perin sähkö- ja automaatiojärjestelmien suunnittelua, mutta tekniikan kehittyessä yritys laajensi osaamistaan ICT-puolelle, minkä jälkeen pystyttiin tarjoamaan älykkäämpiä ratkaisuja tieliikenteessä toimiviin järjestelmiin. Vuonna 2010 Imtech (Nykyinen Dynniq) osti YSP Oy:n sen aikaisen liiketoiminnan.(YSP Oy n.d.)

Tänä päivänä YSP jatkaa osana Dynniq-konsernia tarjoten älykkäitä tietoliikenneratkaisuja tieliikenne järjestelmiin ympäri Suomen. Asiakkaille tarjotaan asiantuntija-, suunnittelu-, konfigurointi-, käyttöönotto- ja huoltopalveluja asiakkaan toiveet ja vaatimukset huomioon ottaen. 30 vuoden asiantuntemuksen ja kokemuksen jälkeen YSP on toteuttanut yli 100 eri älykkään liikenteen ratkaisua ympäri Suomen. YSP:llä on sertifioitu laatujärjestelmä ISO 9001:2015 standardin mukaan, jota noudattaen varmistetaan korkeatasoinen projekti- ja palvelutoiminta.(YSP Oy n.d.)

YSP:n toiminta tällä hetkellä kohdistuu Suomen sisällä tapahtuviin projekteihin. Palveluiden kohdistuessa tieliikenteen älykkäisiin ratkaisuihin, ovat asiakkaat usein valtion alaisia, kuten Fintraffic, joka vastaa Suomen maanteiden tieliikenteen hallinnasta sekä useat kaupungit ympäri suomen. Suurimmassa osasta projekteista toimitaan alihankkijoina, mutta YSP tarjoaa myös suoraan omia palveluita kuten huolto- ja ylläpitoa jo olemassa oleviin järjestelmiin.

2 Intrusion Detection System (IDS)

Intrusion Detection System on tietoliikenteen valvomiseen käytetty järjestelmä, joka toimii lisäturvana palomuurin lisäksi. IDS valvoo verkkoa jatkuvasti tallettaen läpimenevää dataa ja haluttaessa ilmoittaa havainnoistaan ylläpidolle. Halutessa ohjelman voi laittaa suorittamaan aktiivisia liikenteen estotoimenpiteitä, jolloin voidaan puhua Intrusion Prevention System ohjelmistoista (Lutkevich 2020).

IDS-järjestelmiä on ollut olemassa jo viimeisen 40 vuoden aikana. Älykkäämpi liikenteen valvonta nousi aiheelliseksi internetin suuren käyttäjämäärän kasvun myötä, mikä toi myös mukanaan suuren kasvun liikkuvassa datassa. Ensimmäinen dokumentoitu IDS-järjestelmä on vuodelta 1984, jolloin tätä kutsuttiin nimellä Intrusion Detection Expert System (IDES). 1990-luvulla yleistyivät työssäkin käsiteltävät kaksi IDS:n perus valvontatekniikkaa, Network Intrusion Detection (NIDS) sekä Host Based Intruison Detection (HIDS) ja ovat sieltä lähtien pysyneet yleisimpinä valvontamuotoina. IDS-järjestelmien suosio kasvoi 1990-luvun loppu puolella, jolloin vuoden 1998 ja 2002 välillä käyttömäärä nousi jopa 25% ja on jatkanut nousuaan IDS:n ollessa vuonna 2010 seitsemänneksi käytetyin tietoturva järjestelmä.(Pathan 2014)

Nykypäivänä IDS-järjestelmät koetaan olevan pakollinen lisä verkoissa kasvavien uhkien myötä. Siksi nähdäänkin suurien verkkolaite- ja palveluvalmistajien kuten Ciscon tai McAfeen myös sijoittavan paljon resursseja IDS/IPS-järjestelmien kehittämiseen (Guercio 2021). Useat laitetoimittajat, kuten Palo-alto tarjoavat myös nykyisin IDS-järjestelmiä, jotka ovat valmiiksi sisäänrakennettuina heidän palomuuriratkaisuihinsa.

2.1 Aktiivinen ja Passiivinen valvonta

IDS palvelujen suosion suurin syy on palvelujen monipuolisuus ja kyky muovautua juuri käyttäjän haluamiin rajoihin. Järjestelmistä on kehitetty kaksi päätyyppiä, aktiivinen- (IDS) ja passiivinen (IPS) valvonta (Keary 2020.) Passiivinen valvontatyyppi mo-

nitoroi kohdetta toimien enemmän valvonta työkaluna, josta voi helposti käydä tutkimassa järjestelmässä havaittuja hälytyksiä (alerts). Passiivisen valvonnan aikana järjestelmä ei tee mitään konkreettisia vastatoimenpiteitä kuten lähde-IP:n estämistä estääkseen uhkatekijöitä. Sen sijaan, kun ohjelma havaitsee uhan joko ulko- tai sisäverkosta, siitä luodaan hälytys, jonka kautta ylläpito voi aloittaa vastatoimet (Yadav 2020).

Aktiivinen valvonta tunnetaan paremmin nimellä Intrusion Prevention System, eli IPS. Tässä valvontatyypissä perustoiminnot pysyvät samana kuin IDS:n kanssa, mutta suurin ero on uhkatilanteissa, missä aktiivinen valvonta tekee sille annettujen ohjeiden mukaan toimenpiteet estääkseen uhkatekijän. Tämä voi olla lähde IP-osoitteen estäminen tai portin sulkeminen (Keary 2020).

Teoriassa IPS:n toimintojen pitäisi päihittää IDS: ominaisuudet, sillä IPS omaa paljon enemmän ominaisuuksia. Tilanne ei aina kuitenkaan ole näin. Kummatkin Valvontatyypit noudattavat tiettyjä parametreja valvonnan suorittamiseen. Jos parametrit ovat huolimattomasti määritelty, voi järjestelmä alkaa tekemään niin sanottuja ”false positive”, eli virheellisiä havaintoja, estäen kohteita ja samalla yhteyksiä, jotka eivät oikeasti ole uhkia verkolle. Tästä syystä molempien valvonta tyylien konfiguroiminen kestää hyvin pitkään (Lutkevich 2020). Voidaankin todeta, että vaikka aikomuksena olisi ottaa aktiivinen valvonta käyttöön, on valvonta parempi aloittaa passiivisella valvonnalla ja rajata säännöt sille tasolle, että voidaan todeta hälytyksien olevan vain aiheellisia, jonka jälkeen aktiiviset ominaisuudet voidaan kytkeä päälle.

2.2 Säännöt (Signature based- and anomaly based detection)

Säännöillä tehdään IDS:lle määritykset siitä, mitä rajapinnoilla halutaan valvoa. Sääntöjä voidaan luoda kahdella eri tavalla, käyttäen tunnistetietokantoja (Signature based detection) ja luoden omat tunnisteparametrit (Anomaly based detection). Yleisimpänä tapana käytetään tunnistetietokantoja, sillä tietokannat sisältävät aiemmin havaittujen uhkatekijöiden, kuten virusten tai troijalaisten tunnisteita, joita IDS vertaa tulevan ja menevän liikenteen sisältöön. Kumpaakin tapaa voidaan myös hyödyntää samanaikaisesti (Keary 2020).

Kantoja ylläpitää jokin tietoturvayhteisö kuten Talos, jotka analysoivat ja päivittävät omia kantojaan aina uhan havaittaessa. Kannat ovat kattavia ja ryhmiteltynä esimerkiksi kohde palveluun kohdistettujen uhkien mukaan, joka helpottaa sääntöjen suodatusta. Tietokantoja on sekä ilmaisia että maksullisia, mutta ilmaisella versiolla on heikkoutensa. Ilmaiset kannat eivät välttämättä ole yhtä kattavia kuin maksulliset, tarkoittaen että ilmaisia kantoja päivitetään rajoitetusti. Maksullisia kantoja päivitetään aina uusia uhkia havaittaessa. Ilmaisten tietokantojen joukosta löytyvät myös yhteisöjen tunnistekannat, jotka sisältävät itse käyttäjien tekemiä sääntöjä. Yhteisökantoja saa päivittää kuka vain yhteisöön kuuluva jäsen, mikä tarkoittaa, että päivitykset eivät noudata tiettyjä intervalleja. Sen sijaan uusia sääntöjä ilmestyy sitä mukaa, kun niitä lisätään. Käyttäjät saavat halutessaan lähettää kannan haltijoille heidän itse tekemiään sääntöjä, jotka arvion jälkeen lisätään kantaan ja ovat ilmaiseksi ladattavissa kenelle vain.(What are the differences in the rule sets? N.d.)

Tunnistekannat ovat muiden luomia parametreja ja ovat alkuvaiheessa helpoin tapa saada nopeasti dataa ulos verkoista, eikä kohdejärjestelmässä välttämättä muuta tulla tarvitsemaankaan. Vaihtoehtona kuitenkin on myös enemmän työtä vaativat itse laaditut säännöt, eli poikkeaman tunnistusparametrit (Anomaly based detection).

Anomaly ased detection tarkoittaa, että verkon normaalin liikenteen määrän, tyylin tai muun ominaisuuden mukaan luodaan staattiset hälytysrajapinnat, joita rikkoessa luodaan hälytys. Tunnistustyylissä pakettien sisältöä ei niinkään analysoida valmiiden tunnisteiden tavalla. IDS:lle voidaan antaa esimerkiksi maksimi tiedonsiirto tietyllä rajapinnalla, jota ei saa ylittää. Rajat yleensä generoidaan tunnistamalla, mikä on normaalia verkossa. Siksi konfiguroimiseen vaaditaan paljon tietämystä kohdeverkosta ja sen toimintatavoista.(Pathan 2014)

Itse tehdyillä tunnisteparametreilla on isompi mahdollisuus tuottaa ”false positive” hälytyksiä (Open Source IDS Tools: Comparing Suricata, Snort, Bro (Zeek), Linux 2020.) Tuotettu data on kuitenkin hyödyllistä selvittäessä, onko palomuurin säännöissä joitain aukkoja. Käytetään esimerkkinä tilannetta toimeksiantajan verkossa ta-

pahtuvasta skenaariosta. Asiakkailla on omat palvelimet omissa rajatuissa verkoissaan. Asiakkaiden käyttäjillä on staattisesti sidotut IP-osoitteet, mikä tarkoittaa, että heidän liikkeitään pystytään valvomaan. Asiakas yrittääkin tavoittaa jonkin toisen asiakkaan palvelinta ja onnistuu. Koska tämä ei ole normaalia liikennettä kyseiselle käyttäjälle, nostetaan tilanteesta hälytys.

Säännöissä piilee myös ongelmansa. Virukset ja muut verkkoa uhkaavat tekijät kehittyvät nykyään niin nopealla tahdilla, että tunnisteet eivät välttämättä tunnista uutta kehittynyttä haittaohjelmaa. Näissä tilanteissa vaarana ovat ”false negatives” tilanteet, joissa IDS päästää läpi ilman hälytystä paketin, joka sisälsikin haittaohjelman ja järjestelmä vaarantuu ilman että ylläpito sitä huomaa. Voidaankin todeta, että IDS-järjestelmien ja tunnistekantojen ylläpidon tehtävänä on pitkälti reagoida mahdollisimman nopeasti uusiin uhkiin, sillä ennakointi on lähes mahdotonta (Lutkevich 2020).

2.3 Suodatus

IDS-järjestelmät eivät tee mitään ilman erillistä käskyä. Siksi palvelu kuuluu opettaa tunnistamaan mitä kuuluu päästää läpi ja mitä ei. Tämä koskee sekä käyttäessä tunnistekantoja, että poikkeamia hälytystunnisteina. Järjestelmän opettaminen on hidasta ja työlästä etenkin, jos tekijällä ei ole mitään ymmärrystä kohdeverkosta. Siksi suositellaan aina tekemään alustavaa taustatutkimusta, jotta osataan tunnistaa mahdolliset uhkavektorit kohdeverkossa. Suodatusesimerkkinä voidaan käyttää palvelin verkkoa, jossa on vain Linux pohjaisia käyttöjärjestelmiä. Rajapinnalle on turhaa laittaa Windows-järjestelmien haavoittuvuuksia valvovia parametreja, koska näitä ei koskaan tule sattumaan. Alustavan tiedustelun avulla pienennetään palvelun alussa tapahtuvan kuorman määrää, jolloin saavutetaan nopeammin optimaalinen lopputulos.

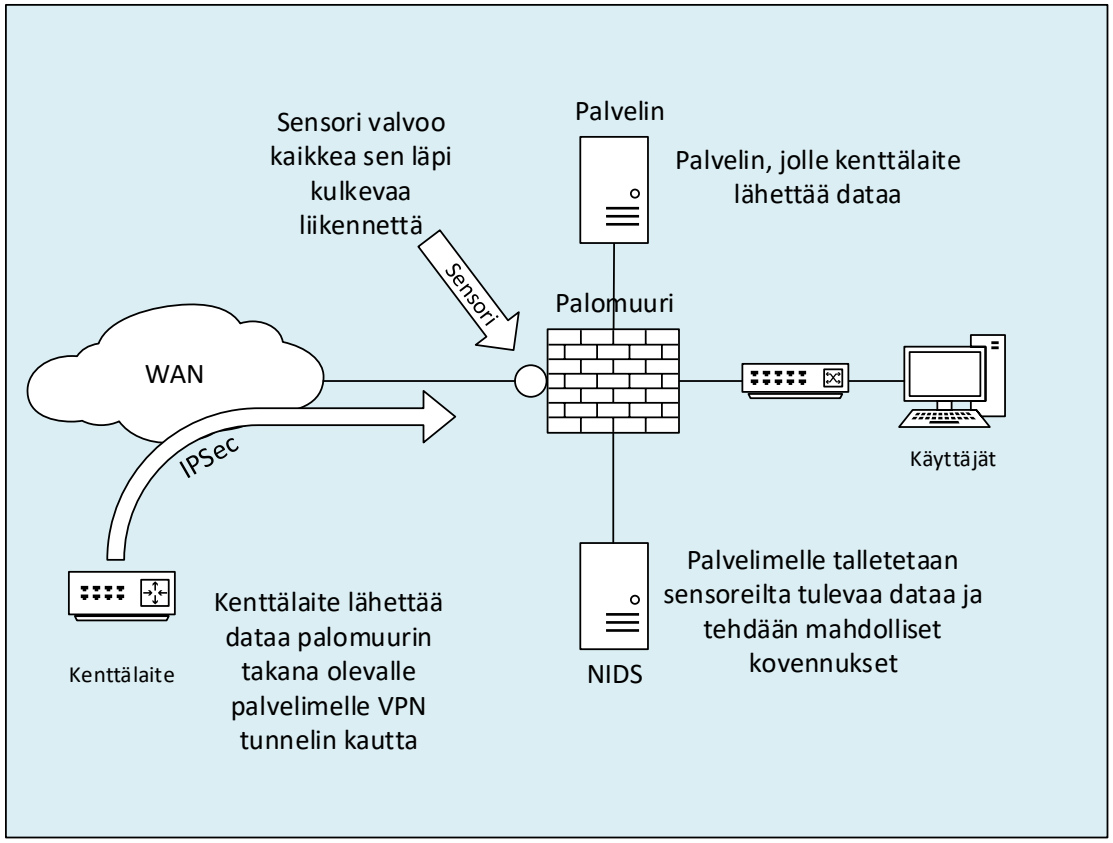
Tunnistekantoja on helpompi suodattaa, sillä kannat ovat jo valmiiksi kategorisoitu jonkin verkkoaspektin, kuten käyttöjärjestelmän mukaan. Poikkeamien havaitsemiseen ei oikoteitä ole ja on siksi työläämpi. Pitkän opettamisen takia yrityksien on useimmiten paras aloittaa pelkillä IDS:n ominaisuuksilla, eli palvelu ei tee havaintojen

perusteella mitään toimenpiteitä, sen sijaan IDS merkitsee havainnon ja ilmoittaa ylläpidolle haluttaessa.

2.4 Sensoreiden sijoittelu

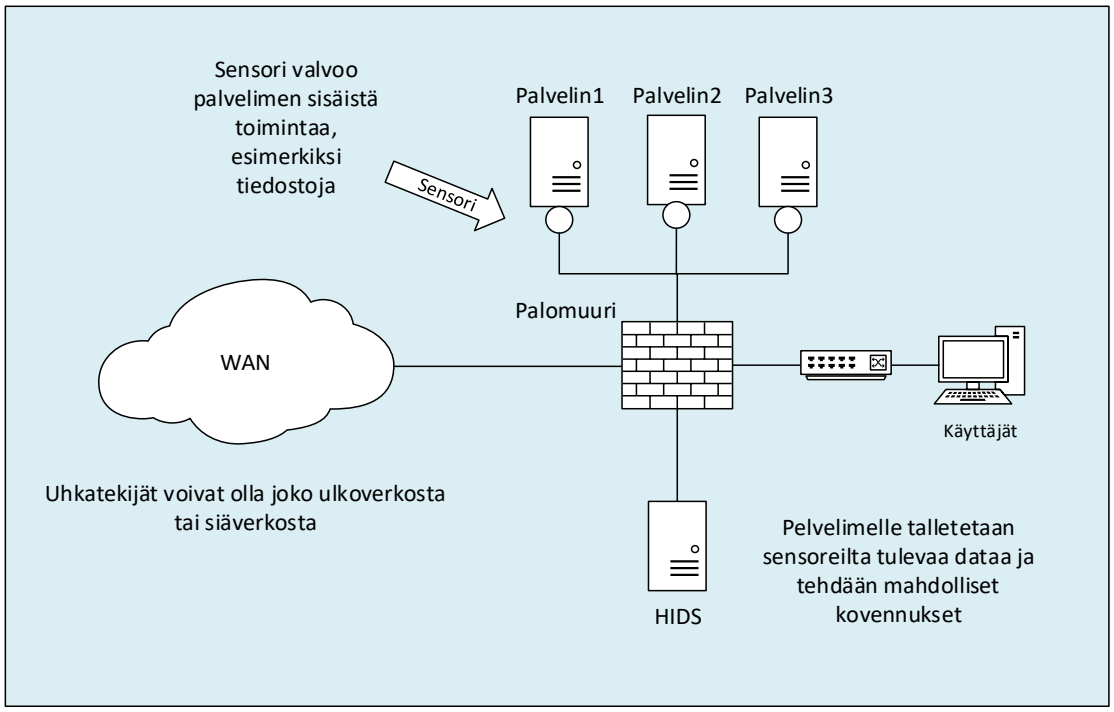
IDS-järjestelmän valvontaan kuuluu sijoittaa valvovat sensorit sellaisiin kohtiin verkossa, josta liikenne saadaan kulkemaan läpi. Sensorit voidaan sijoittaa joko verkkotasolle (NIDS) tai suoraan valvottavaan laitteeseen (HIDS).

Network Based Intrusion Detection System, eli NIDS on verkkoliikenteen valvontaan käytettävä tekniikka. Sensorit sijoitetaan haluttujen rajapintojen juurelle, jossa toimivat välikätenä tulevalle liikenteelle, kuten proxy ja tarkistavat kaikki sisään tai ulos kulkevat paketit pakettitasolla palomuurin IP-tason lisäksi (kts. Kuvio 2). Tämä tarkoittaa, että liikenteestä saadaan valvottaessa enemmän tietoa irti kuin vain palomuurin tapaan IP-osoitteita, protokolleja ja portteja analysoimalla (Yadav 2020). NIDS-toiminnallisuus perustuu siihen, että liikenteen on kuljettava IDS:n läpi, jolloin Traffic Gateway -palvelun tilanteessa, jossa on useita rajapintoja, on IDS paras sijoittaa palomuurin yhteyteen.



Kuvio 2. Network based intrusion detection system esimerkki

Host Based Intrusion Detection System, eli HIDS on IDS:n muoto, jossa valvontaa ei suoriteta verkon rajapinnalla, vaan suoraan laitteen sisällä, johon liikenne kohdistuu. Kohdelaitteelle istutetaan agentti, joka omaa virustorjunta ohjelman piirteitä valvoen mitä laitteella tehdään, skannaa sen sisältöä ja kirjoittaa lokeihin(kts. Kuvio 3). HIDS hyödyntää valvonnassa NIDS:n tavoin tunnisteita, jotka se itse luo kohdelaitteen tiedostojen ja ohjelmien HASH-arvoista. HIDS-järjestelmän heikkous on, että valvonta suoritetaan suoraan kohdelaitteella, eikä sitä edeltävällä rajapinnalla. Tämä tarkoittaa, että uhkatilanne mahdollisesti havaitaan vasta kun vahinko on jo tehty. HIDS-valvonta on myös työläämpää ylläpitää, sillä jokaiselle kohdelaitteelle on asetettava oma agentti(Pathan 2014). Työn aikana tullaan enemmän keskittymään NIDS-valvonnan ominaisuuksiin, sillä implementointi tulee huomattavasti helpommaksi ja halvemmaksi keskitetymmällä valvonnalla. Sen lisäksi tarkoituksena on parantaa rajapinnoille kohdistuvan liikenteen monitorointia.



Kuvio 3. Host based intrusion detection system esimerkki

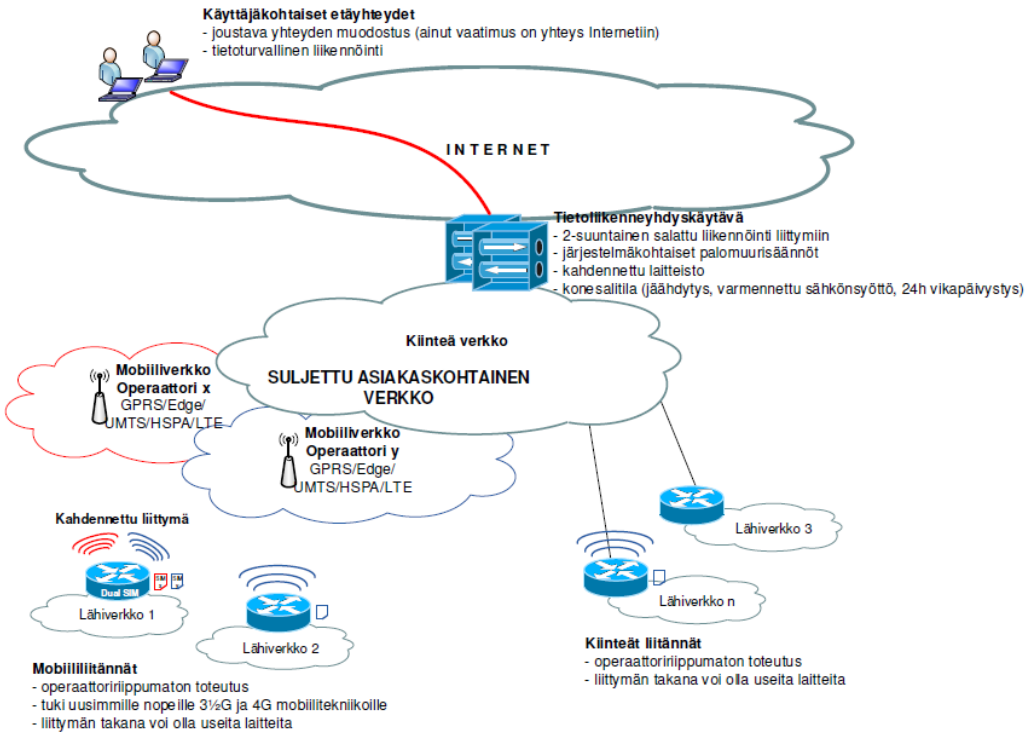
3 Traffic Gateway

IDS-palvelu tullaan toteuttamaan toimeksiantajan Traffic Gateway -palvelun yhteyteen, joka on yksi palveluista, joita tarjotaan asiakkaille. Traffic Gateway -palvelun tavoitteena on tarjota asiakkaille huoleton, tietoturvallinen, operaattoririippumaton ja mahdollisimman helposti hoidettava prosessi uutta verkkoa rakentaessa. Palvelu kattaa suunnittelun, laitteiden hankinnan, käyttöönoton sekä verkon että dokumentoinnin ajantasaisen ylläpidon. Palvelu vapauttaa asiakkaan huolen hankkia omia konesalipalveluita ja laitteistoa koska kaikki yhteydet kulkevat keskitetysti toimeksiantajan hallitseman palomuurin kautta.

Asiakkaille tarjotaan tietoturvallinen ja paikasta riippumaton käyttäjäyhteys, jolla hallinnoida omia järjestelmiään. Turvallinen yhteys on toteutettu käyttäen OpenVPN-ohjelmistoa käyttäjille ja IPSec VPN-protokollaa kenttälaitteiden tietoliikenneyhdyskäytäville. Käyttäjien luominen ja hallinnointi kuuluu myös palvelunsisältöön.

3.1 Ympäristö

Traffic Gateway -ympäristö on kokonaisuutena kokoelma verkkoja, jotka keskustelevat keskenään muilta suljetussa ympäristössä (kts. Kuvio 4). Ympäristö koostuu asiakkaiden käyttäjistä, palvelimista ja muista verkkoihin liittyvistä laitteista, kuten erityyppisistä reitittimistä. Palvelun verkoissa ei ole tavanomaista käyttäjäverkkoa, sen sijaan kaikki käyttäjäliikenne on toteutettu VPN-protokollia käyttäen. Traffic Gateway -palvelu on toteutettu pilvipalveluna, joka pyörii TNNet Oy:n konesalissa. Vaikka fyysinen rauta ja ohjelmisto ei ole toimeksiantajan omistamaa on palvelun toiminta ja hallinnointi täysin heidän hallinnassa. Tällä tavoin on pystytty säilyttämään pienen yrityksen ketterän toiminta sekä samalla toteuttamaan skaalautuvan, luotettavan sekä nopeasti ja laajasti kustomoitavan ympäristön, pienentäen samalla kustannuksia.



Kuvio 4. Traffic Gateway ympäristökuvaus

Palvelimien ohjelmistot ovat erilaisia tieliikenteen ohjaukseen tai valvontaan liittyviä ohjelmistoja, jotka hyödyntävät perinteisten protokollien lisäksi myös omia tarkoituk-

seen räätälöityjä protokollatoteutuksia. Tietoliikenteen suodatus hoidetaan sekä palvelimen sisäänrakennetun muurin että Traffic Gateway -palvelun palomuurin avulla. Palvelinympäristö on pilkottu omiin pienempiin segmentteihin, joka mahdollistaa paremman liikenteenvalvonnan ja käyttäjien satavuuden rajaamisen. Uhkatilanteissa pystytään myös paremmin välttymään tilanteista, joissa yksi saastunut kone voisi saastuttaa muitakin ympäristön koneita. Ympäristön resursseja valvotaan erillisellä valvontapalvelimella, joka hoitaa kyselyt käyttäen SNMP-protokollaa. Valvonnan avulla pystytään valvomaan ylhäällä olevia VPN yhteyksiä, sekä palvelimien fyysisiä resursseja, kuten muistia ja levytilaa.

Palvelimien ja kentällä olevien laiteverkkojen yhteydet on luotu käyttäen site-to-site VPN tekniikkaa joko kiinteää- tai langatonta verkkoa hyödyntäen. Kiinteän verkon toteutuksissa kenttäverkot ovat yleensä yhden päätelaitteen takana, joka voi olla joko reititin tai toinen palomuuri, jonka kautta yhteydet haarautuvat useisiin aliverkkoihin. Langattomat verkot koostuvat useista mobiilireitittimistä kentällä, joiden takaa löytyy yleensä pienempi osa aliverkkoa. Laitteiden keskustelu keskenään tapahtuu tässä tilanteessa palomuurin kautta. Vaikka yhteyksiä tulee useasta eri osoitteesta palomuurille päin, on liikenne pystytty rajaamaan käyttäen Virtuaalisia IP-osoitteita. Virtuaali IP:n avulla IPSec-konfiguraatiot on voitu pitää samanlaisina eri kohteissa, mikä helpottaa ja nopeuttaa ylläpitoa. Jokaiselle asiakkaalle on määritetty oma Virtuaali IP, johon heidän kenttälaitteensa muodostavat yhteyden. Näin estetään tilanteet, joissa yksi paljastunut pre-shared key ei vaaranna muiden asiakkaiden toimintaa.

Kenttäympäristöt pääasiassa koostuvat kahdesta eri laitekokoonpanosta, jotka kummatkin liittyvät tieliikenteen ohjaukseen tai opastukseen. Ensimmäisenä on Liikennevalo järjestelmät (LIVA), jotka koostuvat tievarsilaitteista, kuten liikennevaloista. Toisena on muuttuvat pysäköinninopastusjärjestelmät (MPOJ), jotka koostuvat opasteista, joissa on käytössä älykkäämpää pysäköinninopastusta. Tarkoituksena on opastaa autoilevat tienkäyttäjät parkkitiloihin, joissa on tilaa. Muitakin ympäristöjä on, jotka pohjautuvat tarjoamaan etäyhteyksiä kentällä oleville verkkolaitteille, eivätkä sen kummemmin vaadi palvelinyhteyksiä.

3.2 Valvonta

Traffic Gateway -palvelussa kenttälaitteiden ja palvelimien resurssien valvontaan hyödynnetään Centreon valvontapalvelinta. Centreon ohjelmistosta on käytössä ilmainen versio, jonka avulla valvonta suoritetaan hyödyntäen SNMP-protokollaa. Kenttälaitteiden kohdalla valvotaan kohdelaitteen ylhäällä oloa sekä langattomien reitittimien signaalivahvuuksia tuettujen laitteiden kohdalla. Palvelimilta haetaan SNMP-protokollalla tietoja fyysisistä resursseista, kuten käytössä olevasta muistista, levytilasta yms. Kirjoitushetkellä valvonta palvelu on vielä kehitysvaiheessa.

3.3 Palomuuri

Palomuuri toimii sisäverkon ja ulkoverkon erottajana valvoen näiden kahden alueen välillä liikkuvaa tietoliikennettä. Yksinkertaisella palomuurilla valvonta suoritetaan Osi-mallin layer 4-tasolla tarkoittaen, että suodatus tehdään IP-osoitteiden ja protokollien perusteella määritetyillä säännöillä. Säännöt koostuvat lähde- ja kohde IP-osoitteesta, tulevan liikenteen protokollasta ja siihen määritellystä porttiavaruudesta. Näin pystytään suurimmalta osin estämään uhkatekijöiden pääsy yrityksen kriittisiin palveluihin, kun väylinä toimivat vain tarvittavat portit.(Anicas 2015)

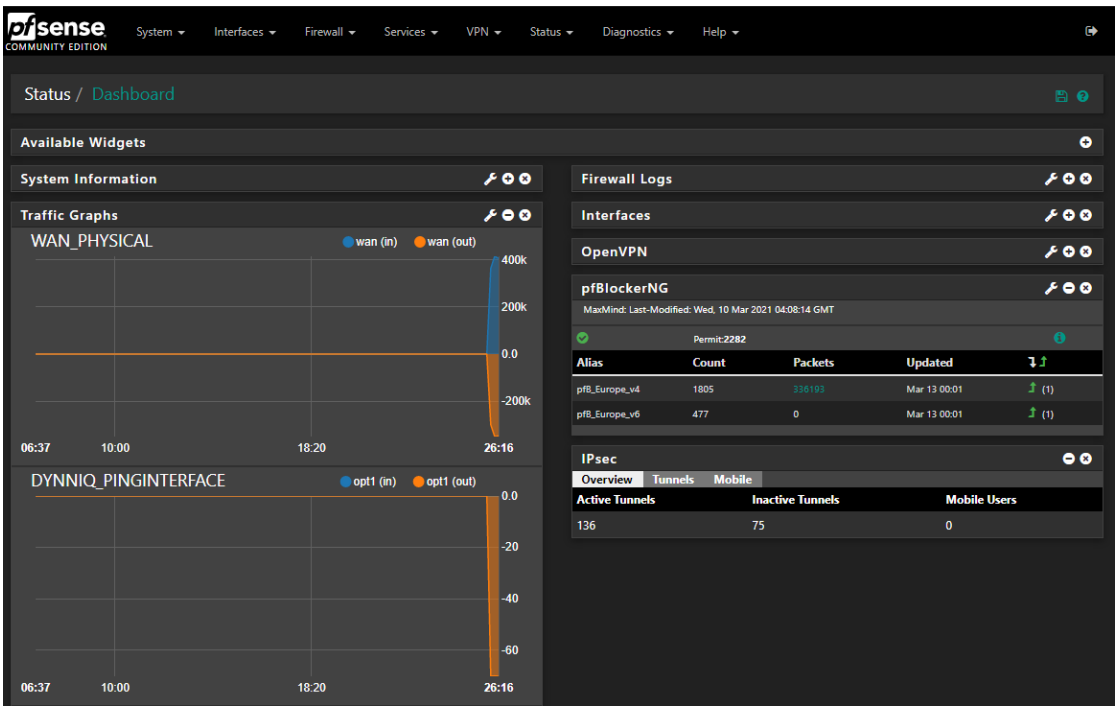
Yksinkertainen palomuuri ei pysty itse generoimaan sääntöjä analysoimalla liikkuvaa liikennettä, koska ei ole mitään mahdollisuutta tietää, mikä kuuluu haluttuun liikenteeseen ja mikä ei. Siksi säännöt on manuaalisesti määritettävä halutuille rajapinnoille. Nykypäivänä jos palomuurilta halutaan saada enemmänkin irti kuin vain yksinkertaista liikenteen suodatusta, voidaan hankkia niin sanottu ”Next Generation Firewall” (NGFW). NGFW tarkoituksena on tuoda älykkäämpää turvaa verkon hallintaan. Tämä tarkoittaa, että samasta paketista löytää kaikki tarvittavat ominaisuudet verkon ylläpitoon, kuten käyttäjien hallinnan ja virustorjunnan. Perinteisen palomuurauksen lisäksi liikenteen suodatusmahdollisuuksia on laajennettu toimimaan muullakin kuin vain IP- ja porttitasolla, joihin myös työn aihe IDS/IPS palvelut sijoittuvat. Toimeksiantajan ympäristössä käytössä on Netgaten kehittämä Pfsense-palomuuriohjelmisto, joka tuo mukanaan juuri NGFW:ltä odotettuja ominaisuuksia.(What is a Next Generation Firewall (NGFW)?. n.d.)

Pfsense on avoimen lähdekoodin palomuuriohjelmisto, jonka pohjana on käytetty FreeBSD käyttöjärjestelmää(Pfsense n.d.) Ohjelmiston takana on Texasista lähtöisin oleva yritys Netgate, joka aloitti Pfsense-projektin vuonna 2012. Heidän tavoitteenaan on tarjota paras mahdollinen avoimen lähdekoodin palomuuriohjelmisto, joka pystyisi haastamaan muiden valmistajien palomuuriohjelmistot.(About Netgate. n.d.)

Pfsense-ohjelmiston tarkoituksena on tuoda kaikki perusominaisuudet, mitä palomuurilta voi odottaa, kuten palomuuraus, nattaus, reitittäminen ja datan lokitus. Sen lisäksi ohjelmisto on laajasti muokattavissa omanlaiseksi suuren lisäosakirjaston vuoksi. Lisäosakirjastot koostuvat kolmannen osapuolen ohjelmistoista, jotka ovat räätälöity toimimaan saumattomasti Pfsensen ohjelmiston kanssa. Paketteja on tarjolla esimerkiksi Proxy ja VPN palveluihin sekä myös työtä käsitteleviin IDS-palveluihin. Laajan kirjaston avulla ohjelmistolla pystytään toteuttamaan samoja NGFW:ltä odotettavia ominaisuuksia ilman pelkoa, että resurssit kuluisivat turhiin ominaisuuksiin.(Pfsense, getting started. n.d.)

Konfiguraatiot voidaan tehdä joko komentolinjalta tai selainpohjaisen graafisen käyttöliittymän kautta, mikä tekee hallinnasta hyvin käyttäjäystävällisen. Käyttöliittymä on siististi tehty ja toimii kaiken kokoisilla näytöillä ja laitteilla. Käyttöliittymää on helppo opetella käyttämään ja käytettävyyttä helpottaa muokattava etusivu, johon voi lisätä omiin tarpeisiin liittyviä widgettejä (kts. Kuvio 5). Laajan lisäosakirjaston lisäksi, Pfsensellä on hyvin aktiivinen käyttäjäyhteisö, mikä mahdollistaa nopeiden päivitysten tekemisen uhkia havaittaessa sekä laajan ja osaavan avun lähteen ongelmatilanteissa.

Tällä hetkellä Traffic Gateway -palvelussa hyödynnetään Pfsensen palomuurauksen ja nattauksen lisäksi IPSec sekä OpenVPN -palveluja, joista IPSec hoitaa tunneloinnin kentällä oleville laitteilla ja OpenVPN käyttäjien etäyhteydet. Lisäksi asiakkaiden käyttäjien hallinta on keskitetty palomuurille, mikä tarkoittaa, ettei yrityksellä tarvitse erikseen olla Active Directoryn tapaista keskitettyä palvelinta. Toimeksiantajalla ei ole suoraa tukisopimusta Netgaten kanssa, mutta virtuaaliympäristön ylläpitäjällä on, jonka kautta bugi-ilmoituksia ja muita ongelmia pystytään hoitamaan.



Kuvio 5. Pfsense dashboard

3.3.1 Tiedonsiirto Traffic Gateway -palvelussa

Kenttälaitteiden ja hallintapalvelimien yhteydet Traffic Gateway -palvelussa on toteutettu käyttäen Internet Protocol Security VPN-protokollaa. IPSec on layer 3-tason protokolla, jonka avulla tiedonsiirto Traffic Gateway -palvelussa pystytään toteuttamaan kenttälaitteiden, käyttäjien ja palvelimien välillä turvallisesti julkisen verkon yli. Toimiakseen, kummallakin osapuolella kuuluu olla identtiset konfiguraatiot, jotta yhteys voidaan muodostaa. Yhteyksissä käytetään IPSec:n Main moodia Aggressive moodin sijaan. Main moodi luo alkuun suojatun tunnelin, jonka sisällä suoritetaan sitten loppuun algoritmien valinnat ja avainten vaihdot. Aggressive moodissa algoritmit ja avaimet kulkisivat ilman salausta.(Loshin, P. 2018)

Käyttäjien etäyhteyksiin hyödynnetään OpenVPN-ohjelmaa. OpenVPN on avoimen lähdekoodin ohjelma, joka hyödyntää yhteyksissään Transport Layer Security- (TLS) ja Secure Socket Layer (SSL) -protokollia salatakseen liikenteen (What Is OpenVPN & How Does OpenVPN Work? n.d.) Traffic Gateway -palvelun palomuurilla Pfsensellä on tarjolla valmis sisäänrakennettu OpenVPN-paketti, jonka avulla voidaan hyödyntää muurin käyttäjänhallintaa ja VPN-ohjelmaa samanaikaisesti. Jokaiselle asiakkaalle tehdään oma VPN-palvelin, johon määritetään yhteyden asetukset, kuten tunnelissa

käytettävät IP-osoitteet, salausalgoritmit ja sallitut verkot. Asiakkaille ladataan oma henkilökohtainen asennuspaketti, joka sisältää OpenVPN GUI -ohjelman, joka on yhteisön kehittämä käyttöliittymä, sekä omat konfiguraatiot. Valmiin paketin pystyy lataamaan suoraan palomuurilta. Asennuspaketti toimitetaan asiakkaalle, joka ohjelman avulla kirjautua omilla tunnuksillaan palvelimelle.

4 Yrityksen vaatimukset IDS-palvelulle

4.1 Yleiset vaatimukset

Toimeksiantajan vaatimukset IDS-palvelua kohtaan käytiin läpi suunnittelukokouksessa. Kokouksesta ei laadittu muistiota, sen sijaan vaatimukset otettiin ylös ranskalaisin viivoin ja selitetään auki tässä tarkemmin. Vaatimusten pohjalta räätälöitiin myös tutkimuskysymykset, jotka esiteltiin työn ensimmäisessä kappaleessa.

Ensimmäisenä ja yhtenä tärkeimmistä vaatimuksista, palvelun pitää olla kustannustehokas. Palvelun tulee tuottaa niin paljon tarpeellista dataa, että se on aiheuttamiensa kustannusten kannalta kannattavaa. Koska suurin osa Traffic Gateway -palvelun tietoliikenteestä on toteutettu privaatin verkon ylitse, ei verkossa pystytä hyödyntämään IDS:n ominaisuuksia täysivaltaisesti. IDS-ominaisuudet painottuvat havaitsemaan julkisen rajapinnan kautta tulevia hyökkäyksiä, joita ympäristössä ei paljon kirjoitushetkellä ole. Siksi Kustannuksissakin on tunnistettava nämä seikat ja osattava miettiä, riittääkö hyödylliset ominaisuudet korvaamaan siitä koostuvat kustannukset. Jotta kustannukset pysyisivät matalina, ollaan vaihtoehdoiksi valittu vain ilmaisia ohjelmistoja, joissa kulut keskittyisivät itse palvelun kehittämiseen.

Traffic Gateway -palvelun data on pääosin staattista, sillä kentällä olevat kojeet lähettävät tarkoin väliajoin dataa palvelimille, eikä tähän tapahdu muutoksia muuta kuin huolto- tai ongelmatilanteissa. Tästä syystä oletettu data on kentällä olevien kojeitten lähettämää jaksottaista dataa, mutta ylläpidon osalta ei tällä hetkellä ole mahdollisuutta tietää, onko joku muu mahdollisesti kaapannut kentällä olevan laitteen ja

käyttää laitteen käyttämää kaistaa hyökkäysvektorina. Jotta tällaiset tilanteet voitaisiin estää, halutaan IDS-palvelun valvovan laitteilta tulevaa dataa palomuurin IP- j porttitason lisäksi pakettitasolla. Dataa pitäisi pystyä palomuurin tavoin valvomaan reaaliaikaisesti, sen lisäksi kaikki epäilyttävä data pitäisi pystyä tallettamaan jatkotutkimuksia varten. Uhkahavainnoista pitäisi tulla hälytys ylläpidolle välittömästi, kun poikkeama havaitaan.

Kenttäkojeissa on paljon variaatiota, jonka takia kojeisiin käytetään laajasti eri protokollia. Kojeisiin on yleisesti auki hallintayhteydet, jotka voivat olla SSH, tai selainpohjainen HTTP/HTTPS yhteys. Sen lisäksi kojeet lähettävät ohjauspalvelimille staattista dataa, joihin on käytössä omat palveluun liittyvät räätälöidyt portit. Data kulkee kuitenkin pääosin TCP-protokollan avulla ja kaikki yhteydet ovat suojattuna IPSec-protokollaa käyttäen. Jotta palvelu olisi yritykselle kannattava, on sen pystyttävä analysoimaan laajasti eri protokollien paketteja. Vähimmäisvaatimuksena on taulukossa luetellut protokollat, joita tällä hetkellä käytetään yrityksen datansiirrossa (kts. Taulukko 1).

Protokollat verkossa
TCP/UDP
ICMP
DNS
SSH
RDP
NTP
IPSec
TLS
SSL
FTP
IKE
SNMP

Taulukko 1. Protokollat Traffic Gateway -palvelussa

Laajan protokollakirjaston lisäksi ympäristössä on useita kriittisiä rajapintoja, joiden tarkempi monitorointi on suuri prioriteetti yritykselle. Siksi palvelun pitäisi pystyä valvomaan samanaikaisesti useita eri rajapintoja ilman, että se negatiivisesti vaikuttaisi verkon sulavuuteen, kuten kaistan nopeuteen tai muun raudan ylikuormitukseen.

Pakollisten vaatimusten lisäksi olisi toivottua, että palvelua olisi mahdollisuus kehittää ja laajentaa tulevaisuudessa. Tämä tarkoittaa, että palvelu ei saa olla käyttöönottovaiheessa jo resursseiltaan käytetty. käyttöönottovaiheessa palvelun halutaan tuovan IDS-tason ominaisuuksia, mutta palvelun toivotaan tukevan myös IPS-palvelun toimintoja, joita voitaisiin tulevaisuudessa implementoida.

4.2 IDS-palvelun vaikutus havaittuihin riskeihin

Vaatimusten lisäksi IDS-palvelun hyötyjä arvioitiin myös riskianalyysin kautta. Riskianalyysistä pystytään havaitsemaan IDS-palvelulta saatavia parannuksia jo tiedostettujen riskien kautta. Samalla pystyttäisiin havaitsemaan uusia riskejä ympäristössä. Riskianalyysiä oli aikaisemmin päivitetty Traffic Gateway -palvelun suhteen vuonna 2018, jolloin käytössä oli vielä vanha palomuuri. Riskianalyysiä päätettiin käydä läpi kokouksessa, johon osallistui muita palvelun ylläpitäjiä. Kokouksen aikana käytiin läpi olemassa olevat riskit, niiden tämän hetkinen tila sekä mietittiin uusia riskejä. Omana tehtävänä oli miettiä, miten IDS:llä pystytään estämään tai havaitsemaan tunnistettuja riskejä. Tätä työtä varten koostettiin riskianalyysistä suppeampi versio, johon koottiin ne riskit, joihin pystyimme toteamaan IDS:n tuovan jonkin tasoista parannusta. Taulukkoon koottiin yhteensä 5 riskiä, joista jokainen painottuu eri tilanteisiin (kts. Taulukko 2).

Riskianalyysi koostuu riskin kuvauksesta, jossa pyritään esittämään havaittu riski mahdollisimman hyvin. Riskin todennäköisyys ja vakavuus määritetään arvolla, joka on 1-4 välillä, isomman arvon ollessa vakavampi. Todennäköisyydellä kerrotaan kuinka usein kyseinen riski voi sattua, kun taas vaikuttavuudella pyritään arvioimaan riskin aiheuttamia kustannuksia. Riskin merkittävyys mitataan kertomalla yhteen todennäköisyyden ja vaikuttavuuden. Riski käsitellään vakavana, jos merkittävyyden arvo on yli 6.

Traffic Gateway Riskianalyysi					
#	Riski	Todennäköisyys	Vaikuttavuus	Merkittävyys	IDS vaikutus
1	Vanhentuneet/heikot salaukset yhteyksissä	2	4	8	Havaitsee yritykset murtaa salauksia. Havaitsee heikot salaukset.
2	Liian väljät ja vaikeasti tulkittavat palomuurisäännöt eivät tarpeeksi tarkasti suodata liikennettä.	2	2	4	Havaitsee muutokset liikenteen määrässä/kohteessa. Tunnisteet havaitsevat tunnetut skannaukset.
3	Asiakkaiden tai henkilökunnan päätelaitteiden aiheuttamat uhat kuten virukset, madot yms.	2	3	6	Havaitsee tunnisteiden avulla tunnetut haittaohjelmat. Havaitsee muutokset liikenteen määrässä/kohteessa.
4	Osalla palvelimista haavoittuvia ohjelmistoversioita ja osassa yhteys julkisesta verkosta.	3	3	9	Havaitsee jos yritetään murtaa tunnettuja haavoittuvuuksia. Havaitsee muutokset liikenteen määrässä/kohteessa. Havaitsee skannaukset.
5	Palomuuriin tai muuhun palveluun kohdistettu DDOS-hyökkäys.	2	2	4	Havaitsee jos äkillinen kasvu liikenteessä tapahtuu. IPS-ominaisuudet estäisivät suoraan yritykset.

Taulukko 2. Riskianalyysi

Havaituissa riskeissä pääpiirteenä on jokin uhkatekijä, joka yrittää hyödyntää havaittua heikkoutta järjestelmässä. Haavoittuvuus voi johtua esimerkiksi ylläpitäjän huolimattomuudesta liian väljissä palomuurisäännöissä tai sitten vanhoista salausalgoritmeista tai ohjelmistoista. Jokaiseen kohtaan löydettiin kuitenkin jokin tapa, miten näitä voitaisiin havaita ja mahdollisesti estää käyttäen IDS:n ominaisuuksia.

Hyökkääjän käyttäessä tiedossa olevia haavoittuvuuksia, kuten taulukon 2 kohdissa 1 ja 4, IDS havaitsee nämä joko käyttäen valmiita tunnisteita tai määritettyjä rajapintoja. Tällaisissa tilanteissa on tunnisteilla kuitenkin todennäköisempi varmuus havaita uhka. Tunnisteet voisivat esimerkiksi hälyttää bruteforce yrityksistä tai niinkin yksinkertaisista asioista, kuin havaituista heikoista salauksista. Palvelimien kohdalla, varsinkin niillä, jotka ovat tavoitettavissa suoraan internetistä, bruteforce on suuri turvallisuusriski ja siksi olisi hyvä olla IDS:n kaltaista lisäturvaa valvomassa sille kohdistettua liikennettä.

Kohdat 2 ja 3 liittyvät enemmän henkilön tekemään tai aiheuttamaan virheeseen, jonka takia hyökkääjälle aukeaa väylä päästä sisään sisäverkon järjestelmiin. Riskeiksi

oli tunnistettu haavoittuneet päätelaitteet ja liian väljät palomuurisäännöt, jotka molemmat liittyvät henkilön huolimattomuuteen joko oman työpisteensä huolehtimisessa tai itse ylläpitotyön tekemisessä. IDS auttaa kuitenkin tehokkaasti tunnistamaan mainittuja uhkatekijöitä. Tunnisteiden avulla suurin osatunnetuista haittaohjelmista tunnistetaan. Tunnistus ei kuitenkaan tapahdu suoraan päätelaitteelta, jos käytössä ei ole HIDS-järjestelmä. Kun käytössä on NIDS-järjestelmä, uhka tunnistetaan vain, jos haittaohjelma yrittää jollekin sisäverkon rajapinnalle. Tunnisteet tai asetetut data-rajapinnat auttavat myös tunnistamaan liian väljien sääntöjen kohdalla, jos muutoksia tapahtuu, esimerkiksi palvelinta yritetään saavuttaa tarkoituksesta poikkeavaan porttiin. IDS:lle kaikki liikenne on oletuksena epäilyttävää ja siksi ohjelmalle on opetettava luotettavat lähteet, jotta voidaan tunnistaa oikeat uhkatekijät.

Distributed Denial of Service (DDoS), eli palvelunestohyökkäys on yksi yleisimmistä hyökkäyksistä, joita yritysverkot kohtaavat. Yrityksien tietoturvaan keskittyvä yritys Netscout Systems raportoi, että vuoden 2020 ensimmäisenä puoliskona havaittiin jopa 4,8 miljoonaa palvelunestohyökkäystä (Netscout Threat Intelligence Report 2020). Uhka ei siis ole vähäteltyä ja pitäisi löytyä jokaisen yrityksen riskianalyysistä, joilla on tarjota julkisia palveluita. Palvelunestohyökkäyksien ollessa hyvin yleisiä, on niiden varalle myös kehitetty vastatoimia, jotka myös IDS omaa. Hyökkäyksen sattuessa IDS havaitsee tunnisteiden tai omien staattisten hälytysrajapintojen avulla, jos palveluestohyökkäyksien peruspiirteitä, kuten normaalia isompia paketteja kohdistuu tiettyyn kohteeseen. Hälytyksiin sisältyy aina lähde-IP, jonka estämällä pystytään tyrehdyttämään hyökkäystä. IDS ei tee estoa itse, jos tätä ei erikseen ole sallittu. Onneksi suurin osa IDS-toteutuksista pystyvät nykypäivänä toimimaan IPS-järjestelmän tavoin ja automaattisesti aloittaa liikenteen estot. Tärkeintä kuitenkin on, että IDS auttaa havaitsemaan uhan, jotta järjestelmän ylläpito pystyy mahdollisimman nopeasti aloittamaan vastatoimet.

5 IDS-palveluiden vertailu

5.1 Palveluvaihtoehdot

Toimeksiantajalle on tärkeää pystyä itse hallinnoimaan omia järjestelmiään. Siksi IDS-palvelua ei haluta erottaa toisen operaattorin konesaliin. Nykyisen palvelun koon ja aiemman IDS kokemuksen puutteen takia myös suuret kaupalliset IDS-palvelut on jätetty pois vertailusta. Vaihtoehdoiksi valikoitui palomuurille tarjolla olevat valmiiksi integroidut IDS-paketit Snort ja Suricata sekä konesalipalveluntarjoajan tarjoama palvelu, joka hyödyntää Snort-ohjelmistoa.

Pfsense-palomuurilla on laaja kirjasto paketteja, jotka ovat valmiiksi räätälöity toimimaan palomuurin ohjelmiston kanssa. Paketit ovat Netgaten yhteisön tekemiä avoimen lähdekoodin ohjelmistoja, joita kuka vain voi hyödyntää ilman kustannuksia. Kirjastosta voidaan valita kahdesta valmiiksi integroidusta IDS/IPS palvelusta. Vaihtoehtoina ovat Snort ja Suricata -ohjelmistot. Kummatkin ohjelmistot ovat Pfsensen versioina liikenteen valvontaan tarkoitettuja ohjelmistoja (NIDS). Ohjelmistot ovat perusominaisuuksiltaan samankaltaisia ja siksi työssä vertailu pyritään hoitamaan tuomalla kummankin ohjelmiston vahvuudet sekä heikkoudet esille, tiivistämällä opitut asiat vertailutaulukossa.

Kahden itse rakennetun palvelun lisäksi vertailuun on otettu myös mukaan toimeksiantajan konesalipalveluntarjoajan palvelu, jotta saataisiin myös valmiin palvelumuodon ominaisuuksia esiteltyä. Palvelu on rakennettu IDS-järjestelmän ympärille, tuoden lisänä laajempaakin valvontaa asiakkaan koko järjestelmästä keräten lokeja halutuista kohteista.

5.1.1 Snort ja Suricata -ohjelmistot

Snort on Martin Roeschin vuonna 1998 perustettu avoimen lähdekoodin ohjelmisto, joka on nykyisin Ciscon omistama. Cisco osti vuonna 2013 Sourcefire-yhtiön, joka oli silloinen Snort-ohjelmiston omistanut yritys. Vaikka Ciscolla ohjelmistoa hyödynnetään kehittämään heidän omia IDS-toteutuksiaan, on ohjelmisto pysynyt avoimen

lähdekoodin -ohjelmistona ja noudattaa GPLv2 (General public license version 2) mukaista sopimusta (White, Fitzsimmons & Matthews 2013).

Snort on oletuksena komentolinjalta konfiguroitava ohjelma, mutta laajan käytön vuoksi ohjelmistosta on olemassa graafisia käyttöliittymiä kuten Pfsensen versio käyttömukavuuden parantamiseksi. Snort on NIDS-järjestelmä, jonka voi konfiguroida kolmeen eri toimintatapaan:

- Sniffer
- Lokien keräys
- Passiivinen / Aktiivinen valvonta

(What can I do with Snort? n.d.)

Sniffer analysoi läpi kulkevaa dataa tekemättä sen kummemmin liikenteelle mitään, kun taas loki toiminnolla talletetaan liikennettä myöhempää analyysiä varten. Kolmantena on IDS ominaisuudet, jolloin kaksi aikaisempaa toiminnallisuutta yhdistetään ja tuodaan vielä hälytykset mukaan.

Suricata on toinen hyvin laajasti käytössä oleva avoimen lähdekoodin IDS -ohjelmisto, jonka omistaa Open Information Security Foundation (OISF), joka on Yhdysvaltain turvallisuusviraston rahoittama yritys (OISF. n.d.) Se on Snortin tapaan myös pääasiassa NIDS-järjestelmä, kun ohjelmiston IDS- tai IPS ominaisuuksia käytetään. Näiden lisäksi ohjelmistolle on lueteltuna viisi muuta perustoimintoa:

- Verkon turvallisuuden valvonta (Network Security Monitoring, NSM)
- Yhteydetön PCAP tiedoston analyysityökalu
- Liikenteen talletus PCAP-lokitus työkalulla
- ”Unix Socket mode” automatisoituun PCAP-tiedostojen käsittelyyn
- Linux Netfilter palomuuri integraatio
- Instrusion Detection System, IDS
- Intrusion Prevention System, IPS

(Suricata, Complete list of Suricata Features n.d.)

Suricata on myös Snortin tapaan komentolinjalta konfiguroitava ohjelma, mutta on laajasti tarjolla itselle sopivalle käyttöjärjestelmälle ja ohjelmiston pohjalta on olemassa graafisia käyttöliittymiä, joista tässä työssä käsitellään Pfsenseltä löytyvää versiota. Kumpikin ohjelmisto hyödyntää pääasiassa tunnisteita valvonnan suorittamiseen ja samat kannat ovat tarjolla kummallekin. Tunnisteiden lisäksi kummallakin ohjelmistolla on mahdollisuus luoda omia staattisia hälytysrajapintoja ja kirjoittaa omia tunnisteita.

5.1.2 Pfsensen paketti vai itsenäinen palvelin

Snort ja Suricata -ohjelmistot ovat saatavilla Pfsenselle räätälöityinä sekä erillisinä ohjelmistoina. Ominaisuuksiltaan ohjelmistot ovat samanlaiset, mutta eroja huomaa käytettävyydessä, sekä kustannuksissa. Suurin ero voidaan todeta hinnassa. Itse ohjelmistot ovat kummassakin ilmaisia, mutta erillinen ohjelmisto vaatii täysin uuden alustan, jolla toimia. Palvelimen osto ei ole kovinkaan kallista, kun puhutaan virtuaaliympäristöstä, mutta kustannuksia tulisi paljon käyttöönotossa. Kustannukset käsitellään tarkemmin kappaleessa 5.4.

Pfsensen paketti käyttää hyödykseen jo ylläpidolle tuttua palomuuriympäristöä, mikä helpottaa käyttöönottoa. Käytössä on graafinen käyttöliittymä, mitä ei ole omassa IDS-palvelimessa. IDS:n ollessa muurilla on myös kaikki valvontaan tarvittavat parametrit, kuten rajapinnat ja aliakset (osoiteryhmät) valmiiksi käytettävissä palomuurin resursseista. Analysoitu data pystytään suoraan lokittamaan esimerkiksi palomuurin järjestelmä lokeihin, josta data pystytään siirtämään halutessa erilliselle lokipalvelimelle laajempaa analyysiä varten. Erillinen lokipalvelin olisi mahdollisesti tarpeen sillä Pfsense integraation heikkoutena on rautaresurssit ja vähäinen tallennustila, joka ei mahdollista laajempaa loki analyysiä. Jos data talletetaan vain palomuurille on hälytyksiä valvottava aktiivisesti, jotta ne ehditään huomata. Erillinen lokipalvelin helpottaisi taakkaa järjestelmän ylläpitäjillä, kun dataa ei tarvitse olla jatkuvasti valvomassa.

Itsenäisen palvelimen ratkaisu on paremmin dokumentoitu kummankin ohjelmiston kohdalla. Ongelmia tuo Traffic Gateway -palvelun useat rajapinnat. Jotta valvonta

pystyttäisiin suorittamaan kaikilla rajapinnoilla, pitäisi IDS-palvelin sijaita joko jokaisella rajapinnalla, että liikenne kulkisi sen läpi, tai sitten hakea kopioita liikenteestä. Tässä tilanteessa palomuurilta, jossa jokainen rajapinta sijaitsee. Tämä poistaisi paljon ominaisuuksia, kuten tulevaisuuden IPS-ominaisuudet kokonaan sekä mahdollisuuden tehdä suoraan estoja hälytyksien perusteella liikenteeseen. Sen sijaan estot olisi tehtävä palomuurin säännöillä tai IP-osoitteiden estolistoilla. Erillisen palvelimen toteuttaminen olisi aivan liian kompleksi kohdeverkossa ja siksi palomuurin tarjoamat integroidut IDS versiot olisivat käytettävyydeltään parempi valinta.

5.1.3 Palveluntarjoajan palvelut

Yrityksen Traffic Gateway -palvelun järjestelmät toimivat kaikki TNNetin hallinnoimassa pilvipalvelussa, jonka takia päätettiin kolmantena vaihtoehtona ottaa vertailuun mukaan myös heidän tarjoamat IDS-ratkaisut. Asiasta käytiin ensiksi sähköpostikeskustelu, jonka kautta selvisi, että tarjolla olisi palvelu nimeltään VaultSec, joka on heidän itse kokoama IDS-kokonaisuus. Palvelussa on mukana itse IDS-valvonnan lisäksi laajempia valvontamahdollisuuksia, kuten lokien keräämistä palomuurilta tai muilta järjestelmän laitteista hyödyntäen eri datankeruu ominaisuuksia (Syslog, netflow, ipfix). Palvelua tarjotaan kahtena eri palvelumallina, jotka on tiivistetysti kuvattuna alla olevassa taulukossa (kts. Taulukko 3). Kirjoitushetkellä Traffic Gateway -palvelun yhteydessä on aktiivisena n.20 rajapintaa, jonka perusteella päädyttiin olemaan huomioimatta perustason palvelua palveluvaihtoehtojen vertailussa. Kuukausihinta perustuu rajapintojen määrään, jolloin hinta nousisi jo Enterprise palvelun yli.

VaultSec	Perustaso	Enterprise
Kuvaus	Pienille yrityksille. Multi-tenant ympäristö (jaettu ympäristö)	Isommille yrityksille Oma palvelin Enemmän vapautta kustomoida dataa omanlaiseksi.
Ominaisuudet	TNNetin ylläpitämä Geneerinen raportti joka kuukausi Halpa ratkaisu jos ei ole useita VLAN-verkkoja	Mahdollisuus Luoda joka VLANista oma näkymä. Pystytään logittamaan muutakin kuin vain palomuurilta tulevaa dataa. Helpottaa luomaan hälytysrajapintoja kattavan logituksen ansiosta
Hinta	30e/kk/VLAN Lisäpalveluina kattavempia raportteja	500e/kk Lisäpalveluina apuja logi-rajauksiin ja lisäraportteja. Palomuurin resurssi-lisäykset kuuluvat hintaan muurin ollessa TNNetin konesalissa. Ei ole määrällisesti rajattu.

Taulukko 3. VaultSec palvelutasot

Palvelu käyttää Snort IDS-ohjelmistoa hyväkseen, joka pystyttäisiin sulauttamaan järjestelmiin joko erillisenä Snortin pyöriessä omalla palvelimella, tai sitten hyödyntäen Pfsenseltä löytyvää versiota, josta data siirrettäisiin sitten erilliselle loki-palvelimelle. Palvelimella data jalostettaisiin hyödyntäen Elastic-search -ohjelmaa ja siihen saatavia lisätyökaluja.

5.2 Ohjelmisto/palvelu vertailu

Snort ja Suricata -ohjelmistot ovat hyvin samankaltaisia eivätkä eroa toisistaan radikaalilla tavalla. Kummatkin ovat ilmaisia ohjelmistoja ja sopivat siksi hyvin toimeksiantajalle, jonka järjestelmissä ei ole aikaisemmin ollut IDS-palvelua, eikä siksi aikaisempaa kokemusta ole. Ilmaisilla ohjelmistoilla saadaan kustannukset pidettyä alhaisina, jolloin ne keskittyvät ainoastaan työn määrään ja valinnaisiin maksullisiin tunnisteisiin. Kumpikin ohjelmisto on NIDS-järjestelmä, joka toimii tietoliikenteen analysoijana ja pystyy haluttaessa muuttumaan IPS järjestelmäksi. Kummassakin ohjelmistossa on tuki usealle käyttöjärjestelmälle, mukaan lukien Windows, joka on toimeksiantajalle tutuin ympäristö.

Dokumentaatiota on tarjolla paljon kummastakin ohjelmistosta. Kummankin ohjelmiston kotisivuilla on tarjolla kaikki dokumentaatio, mitä voi tarvita asennuksesta sääntöjen tekoon. Ohjeet keskittyvät komentolinjalta tehtyihin konfiguraatioihin, mikä voi vaikeuttaa konfiguraatiota Pfsense-versioiden kohdalla. Pfsensen Snort-versiolle on kuitenkin myös olemassa oma käyttöohje, jonka voi löytää Netgaten dokumentaatiosta. Suricatan käyttöliittymä muistuttaa hyvin pitkälle Snort-versiota, joten käyttöohjetta voi osittain hyödyntää, mutta ei voi olettaa kaiken pitävän paikkansa kummankin kohdalla.

Kummatkin ohjelmistot ilmoittavat pystyvänsä analysoimaan tietoliikenteessä nähtyjä yleisimpiä protokollia kuten TCP, UDP, ICMP ja IP ja kattavat myös muut Taulukossa 1 ilmoitetut protokollat, jotka esiintyvät Traffic Gateway -palvelussa. Suricatalla on huomattavasti enemmän lueteltuna valvottavia protokollia kuin Snortilla, joista IKEv2 on yksi toimeksiantajan kohdalla huomioitava protokolla. IKEv2 on IPSec-protokollassa käytettävä liikenteen salaukseen käytettävä protokolla (What is IKEv2 n.d.)

Koska Traffic Gateway -palvelun suurin osa liikenteestä kulkee IPSec-tunnelien kautta, on hyvä, jos liikenteen kättelyitä pystytään valvomaan. On hyvä mainita, että Snort tarjoaa mahdollisuuden sovellustason valvontaan hyödyntäen OpenApp ID lisäosaa ja siihen tarkoitettua tunnistekantaa. Käyttöä kyseiselle ominaisuudelle ei kuitenkaan todennäköisesti verkosta löydy, sillä palvelimilla toimivat palvelut ovat asiakkaiden itse räätälöimiä, eivätkä siksi tunnisteisiin osu.

Tunnisteissa Snortilla on etu, sillä Talosin tarjoamissa tunnistekannoissa hyödynnetään Snortin syntaksia, jolloin Snort pystyy kokonaisvaltaisesti hyödyntämään kantojen sisältöä. Muiden käyttökokemuksia lukiessa foorumeilla raportoidaan, että Suricatalla vuorostaan on havaittu ongelmia pystyä hyödyntämään kaikkia Talosin tarjoamia sääntöjä. Siksi Suricatalla ei välttämättä tule olemaan yhtä laajaa tunnistekirjastoa kuin Snortilla. Yhteensopivuusongelma ei ole kuitenkaan vakava ja samat sekä Talosin että Emergin Threats:n valmistamat tunnistekannat ovat saatavilla kummallekin ohjelmistolle, lukuun ottamatta aiemmin mainittua OpenAPP ID tunnisteita, jotka löytyvät vain Snortilta.

Suurin ero kahden ohjelmiston välillä on miten kumpikin prosessoi läpi kulkevaa dataa. Snort hyödyntää singlethread-ominaisuutta, joka tarkoittaa, että se pystyy ajamaan yhden prosessin kerrallaan ohjelman sisällä, kun taas Suricata hyödyntää multithreading-ominaisuutta, joka suorittaa useita prosesseja samanaikaisesti. Multithreading on tietoliikenteen analyysissäkin haluttu ominaisuus, sillä se hyödyntää tehokkaammin järjestelmän resursseja.

Asiaa on tutkittu Yhdysvalloissa Clarksonin korkeakoulussa, jossa verrattiin miten Suricatan multithreading-ominaisuudet pärjäisivät Snortin singlethread ominaisuuksille. Korkeakoulussa testissä tehtiin jopa 8600 eri kokeilua, jotka koostuivat 10:stä eri prosessorin ydin määrästä 24 ytimeen asti sekä sekä 10:stä eri datamäärästä, jotka syötettiin kummallekin ohjelmistolle. Snort:sta oli testeissä mukana sekä yksi että moni-instanssinen (useita rinnakkain) järjestelmä, jotta saataisiin lisää vertailukohteita. Tuloksista selvisi, että Suricata päihitti Snortin kaikissa ydin määrissä, joista 6-ytiminen

järjestelmä osoittautui suurimmaksi eroksi. Korkeakoulun testi todisti, että multithreading-ominaisuuksilla on väliä, jonka takia voidaan todeta Suricatan olevan parempi valinta suorituskyvyn suhteen (White, Fitzsimmons & Matthews 2013).

Huomioitavaa on, että ero on olemassa vain Pfsensen tarjoamissa versioissa, joissa Snortista on käytössä kirjoitushetkellä versio 2. Snort 3 tukee multithreading-ominaisuuksia ja voidaan olettaa olevan yhtä suorituskykyinen kuin Suricata. Päivitykselle ei kuitenkaan ole päivämäärää tiedossa. Toisena huomioitavana asiana on datan määrä järjestelmissä. Palveluntarjoajan kautta saatiin selville, että järjestelmän keskimääräinen datan käyttö IPSec-rajapintaa kohden, jossa pääasiassa liikenne liikkuu, on hyvinkin pieni (muutama kb/s). Tämä tarkoittaa, että datan analysointi ei vaadi paljon prosessointi tehoa, eikä siksi single- tai multithreading-ominaisuuksilla ole suurta väliä. Toki koska multithreading on tarjolla ja ominaisuus tuo vain plussia mukanaan, ei sitä kannata sivuuttaa.

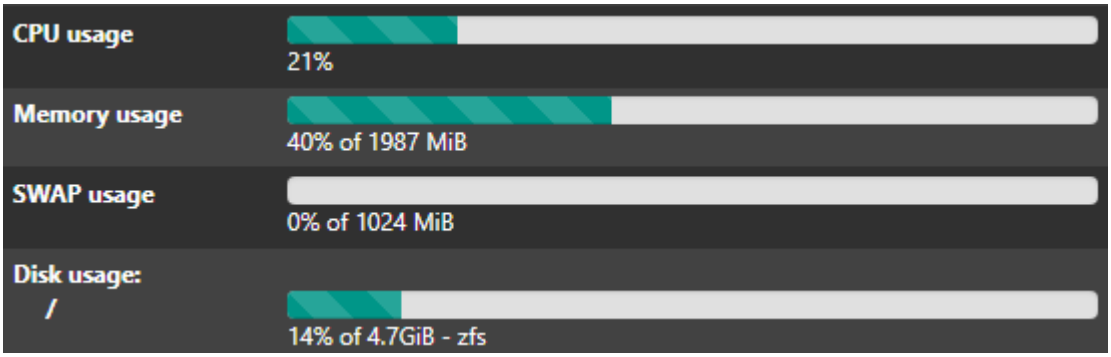
Snortin heikkoudet piilevätkin sen vanhassa versiossa, joka on käytössä Pfsensen tarjoamassa paketissa. Multithreading-ominaisuuden lisäksi Snort 3 on kooditasolta lähtien kirjoitettu uusiksi, jonka seurauksena ohjelmisto on paremmin optimoitu kuin edeltäjänsä (Snort 3 n.d.) Koska päivitykselle ei ole päivämääräkään tiedossa, on kirjoitushetkellä Suricata oletettavasti paremmin optimoitu kuin Snort sillä Suricata on alusta alkaen ollut multithreading-ominaisuuksia hyödyntävä ohjelmisto. Suricatallakaan ei kirjoitushetkellä ole tarjota uusinta versiota Pfsenselle. Tämän hetkinen versio 5.0.4 ei eroa Snortin versioiden lailla suuresti päivitetystä 6.0.1. Suricata 5 on myös edelleen tuettu versio, joka saa päivityksiä myös tarpeen tullen. Versio 6 on myös tulossa Pfsenselle sillä Netgaten foorumeilta selviää, että Suricata 6 on ollut tarjolla vuoden 2020 lopussa Pfsensen repositoriossa, mutta palautettiin versionumeroon 5.0.4 suurien bugimäärien takia.

5.3 Palvelun resurssivaatimukset

Vaikkei IDS-palvelun asennus vaadi paljon alustalta, on kuitenkin hyvä kartoittaa mahdolliset resurssivaatimukset. Resurssivaatimuksia tutkiessa otetaan huomioon sekä muurin yhteydessä toimiva palvelu, että erillinen palvelin. Huomioitavia asioita

ovat vaadittava prosessointi, muisti, levytila ja kaistanopeus tiedonsiirrolle rajapintaa kohden, jolloin saadaan samalla selville palvelun alkutilanteeseen sekä tulevaisuuden laajentamiseen vaadittavat resurssit.

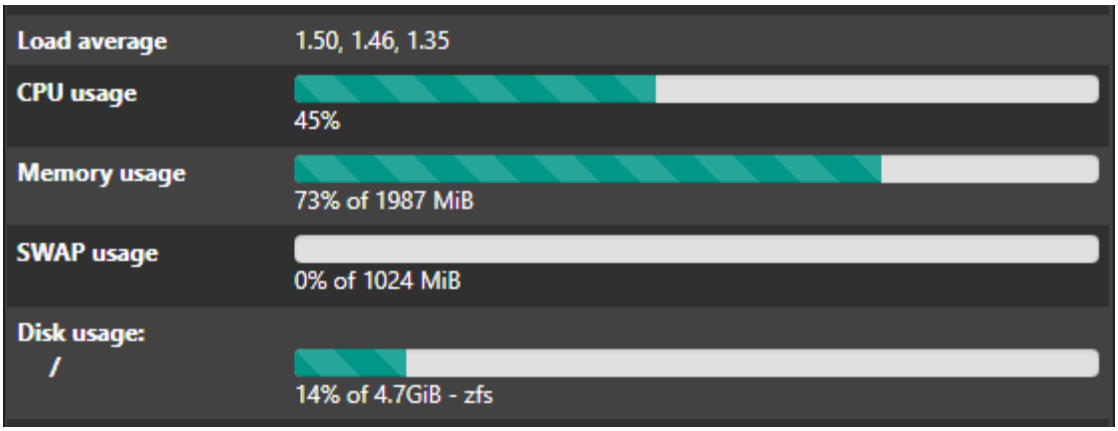
Muuri on jatkuvassa käytössä ja suurimmaksi osaksi liikenteen normit ovat helposti tunnistettavissa ilman suurempia poikkeamia. Pieniä poikkeamia esiintyy etäyhteyksien takana olevien käyttäjien yhteydenotoissa, mutta muutos ei ole suuri. Muurin normaali tila voidaan siis huomata suhteellisen helposti. Kuvio 7 on otettu palomuurin etusivulta, joka esittää reaaliaikaisesti palomuurin resurssien käyttöä (kts. Kuvio 7). Kuvion otto hetkellä Kaikki järjestelmän rajapinnat olivat aktiivisina, aktiivisia käyttäjiä oli vajaa 10 ja VPN-tunneleita oli 137.



Kuvio 6. Palomuurin resurssit ennen aktiivista IDS-valvontaa

Sekä muistin että tallennustilan arvot pysyvät normaali käytössä kuvion mukaisissa arvoissa kummankin heiton ollessa +/- 1%. Muisti on hyvin tärkeä ottaa huomioon, sillä IDS vaatii oman osansa käynnistyäkseen ja valvomiseen. Myös tunnisteiden lataaminen kuluttaa muistia, joka voidaan huomata palveluntarjoajan kanssa tehdyssä demossa luvussa 5.3.1. Tallennustilalle ei tule muutoksia tapahtumaan, sillä IDS ei automaattisesti luo loki-tiedostoja, vaan taltioi lyhyeltä ajalta hälytyksiä. Tallennustilan lisäystä tiedusteltiin myös palveluntarjoajalta, mutta sitä he eivät suositelleet. Demossakin lokit talletettiin erilliselle palvelimelle, jolloin palomuurin tallennustila pysyi koskemattomana. Fyysisten resurssien testejä ei suoritettu erillisellä IDS-palvelimella, mutta voidaan olettaa kuormituksien olevan liki samat omalla palvelimella pyörivälle IDS:lle, kuin palomuurilla olevalle.

Kirjoitus hetkellä palomuurilla on käytössä 2 ytiminen prosessori, jonka käyttöarvot vaihtelevat 20-80% arvoissa 25% ollessa keskimääräinen käyttö. Demon aikana prosessoinnin kohdallakin saatiin hyvin testattua paljonko normaali IDS-valvonta vaatisi resursseja rajapintaa kohden. Tulokseksi saatiin n. 10% rajapintaa kohden, joka tarkoittaisi, että prosessorin ytimiäkin pitäisi lisätä nykyisestä kahdesta ytimestä ainakin neljään, jotta muuri jaksaisi pyörittää kaikkia lähemmäs 20:tä rajapintaa. Alla olevassa kuviossa on esitettynä resurssit kahden aktiivisen rajapinnan jälkeen ja miten ne vaikuttavat palomuurin resursseihin (kts. Kuvio 7).



Kuvio 7. Palomuurin resurssit aktiivisen IDS-valvonnan aikana

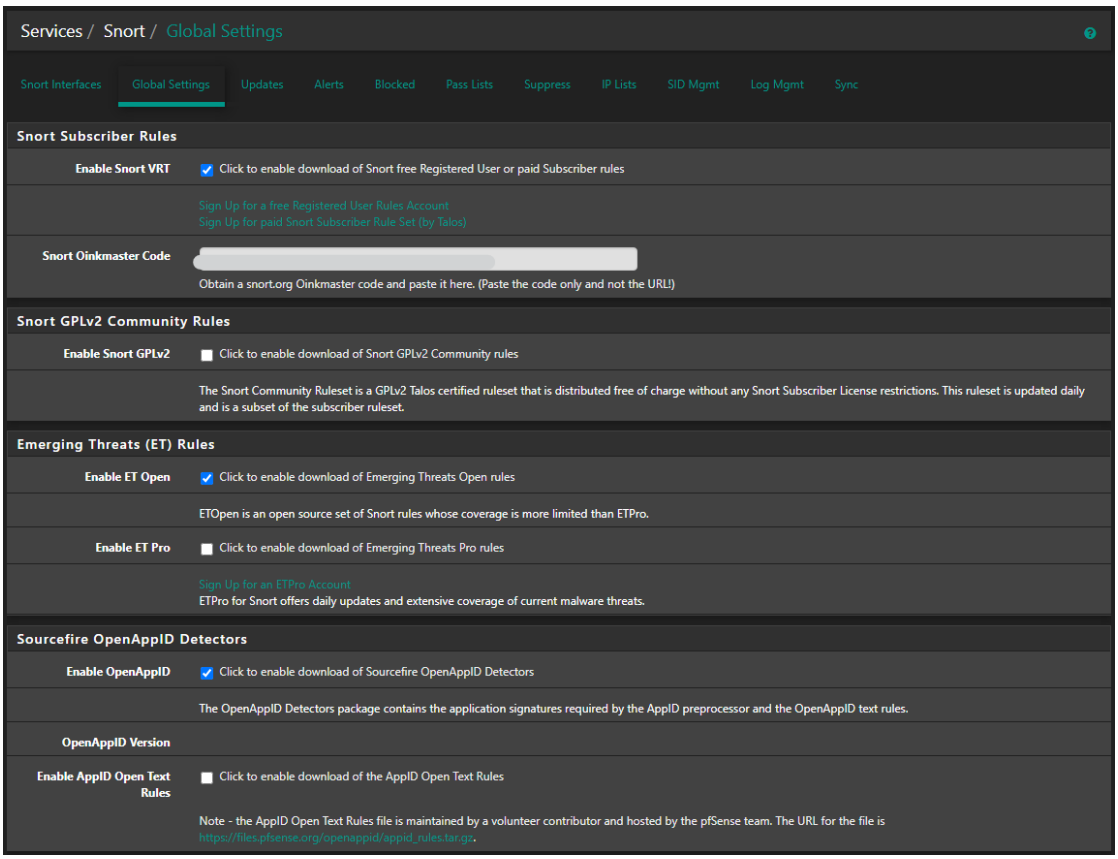
Kuvioiden arvot perustuvat Snort IDS:n tuloksiin, joka käyttää Singlethread teknologiaa. Aiemmin todettiin Suricatan olevan multithreading-ominaisuuksiensa ansiosta tehokkaampi, joten voidaan olettaa esitettyjen kuormituksien olevan maksimit ja Suricatan tapauksessa kuormitus oletettavasti on hieman pienempi prosessoinnin suhteen.

Voidaan todeta, että resurssien lisääminen on aiheellista, jos IDS laitettaisiin pyörimään palomuurin yhteyteen. Tässä pilvipalveluiden vahvuudet tulevat esiin. Pilvessä pyörivään palveluun on helppo lisätä rautaresursseja kuten muistia, ilman että tarvitsisi itse käydä fyysisesti muuttamassa mitään. Raudan lisäys ei vaadi pitkiä katkoksia, mikä on myös iso vahvuus järjestelmässä, jonka pitäisi olla käytössä vuorokauden ympäri. Erillisen palvelimenkin kohdalla palveluntarjoaja on informoinut, että resurssien suhteen on helpompi aloittaa vähällä ja nostaa kun sille on tarvetta sen sijaan, että virtuaalikoneen resursseja lähtisi pienentämään.

5.3.1 Testaus

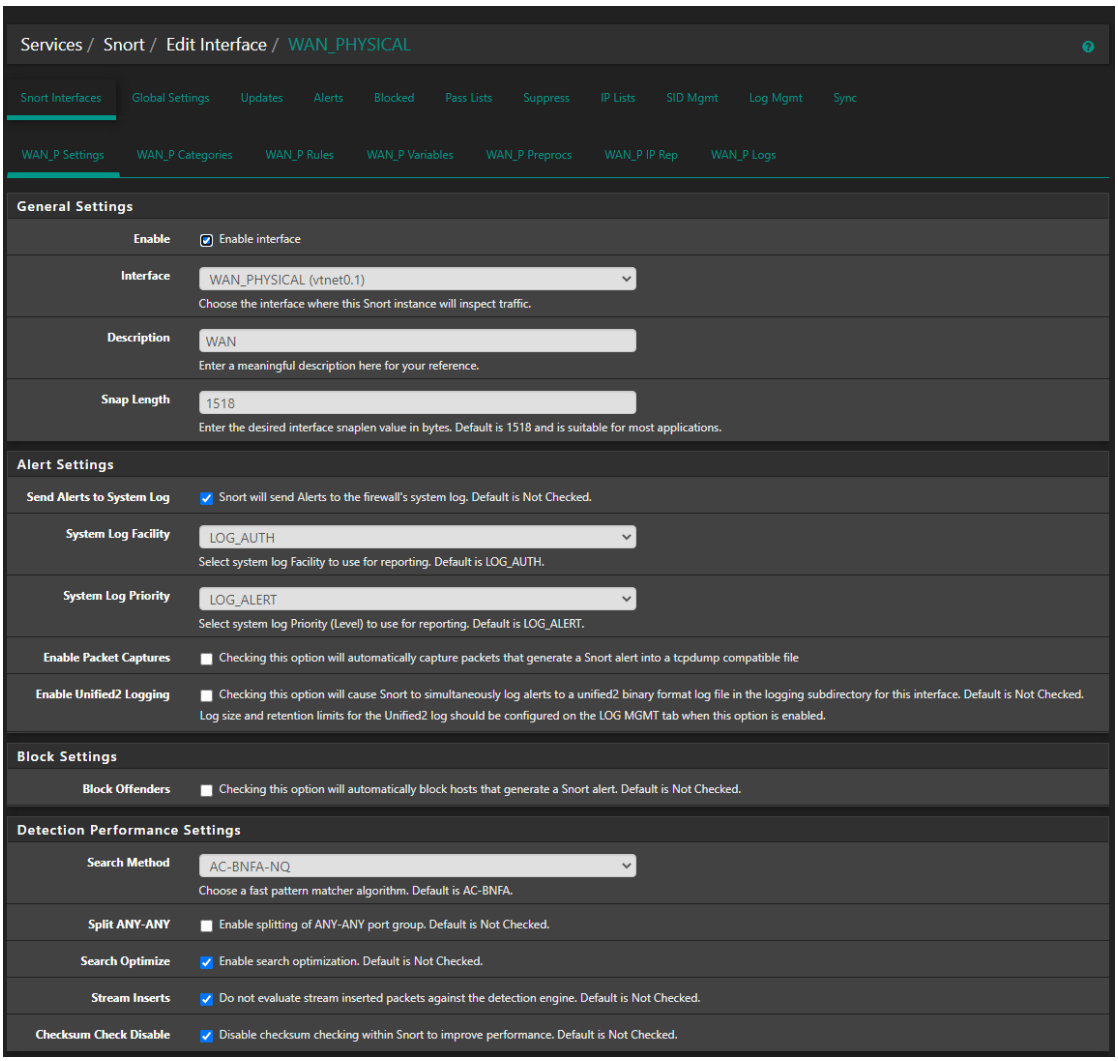
Koska palveluntarjoajalla oli jo valmiiksi suunniteltuna hyvä raportointi IDS-datalle, pyysimme heiltä demoa omasta palvelustaan. Demo tulisi pyörimään kuukauden ajan valvoen kahta rajapintaa, sillä testihetkellä ei muurin resurssit riittäneet enempään. Data lähetettäisiin palomuurilta erilliselle loki-palvelimelle, josta data koostettaisiin raportiksi. Rajapinnoiksi valittiin julkinen (WAN) ja yksi sisäinen palvelinverkko. Kuukauden aikana tunnistekantana toimi Talosin tarjoama maksullinen kanta, jossa kaikki säännöt olivat aktiivisena. IDS:n tuottamiin hälytyksiin ei reagoitu millään tavalla demon aikana, jotta saataisiin mahdollisimman paljon dataa kerättyä.

Kuvio 8 on otettu palomuurin Snort ”global settings” -välilehdeltä. Sivulla määritetään tunnistekannat, joita tullaan käyttämään sekä päivitys intervalli tunnisteille. Demon aikana tunnisteista oli valittuna Talosin maksullinen ”Snort VRT” sekä ”ET Open” tunnistekanta. GPLv2 tunnisteita ei tarvinnut erikseen valita, sillä tunnisteet sisältyivät Snort VRT tunnisteisiin. Muut yleiset Snort asetukset pysyivät oletusasetuksilla.



Kuvio 8. Snort Global settings

Seuraavana määritettiin kummankin rajapinnan asetukset. Kuviossa 9 on esiteltynä WAN rajapinnan asetukset, jotka kopioitiin suoraan sisäisen rajapinnan asetuksiin (kts. Kuvio 9). Demossa data siirrettiin erilliselle loki-palvelimelle hyödyntäen ”Send Alerts To System Log” -asetusta, joka luo hälytyksistä järjestelmän lokeihin myös merkinnän, josta palveluntarjoaja pystyi datan hakemaan käyttäen Syslog-protokollaa. Aktivoitaessa ”Block offenders” -asetus valvonta muuttuu passiivisesta aktiiviseksi, mutta koska hälytyksiin ei haluta reagoida, eikä minkäänlaista suodatusta ole tehty, olisi aktiivisesta valvonnasta vain harmia. ”Detection Performance Settings” osioon oli valittuna asetukset parhaan suorituskyvyn mukaan.



Kuvio 9. Snort rajapinta asetukset

Demon avulla tavoitteena oli pystyä arvioimaan datan määrän ja ominaisuuksien perusteella, onko IDS:n tuottama data oikeasti tarpeellista parantamaan nykyisen palvelun tietoturvaa. Demon tuloksissa painoarvo olisi seuraavissa asioissa:

- Datan määrä
- Hälytyksien vakavuus
- Järjestelmä kuormitus

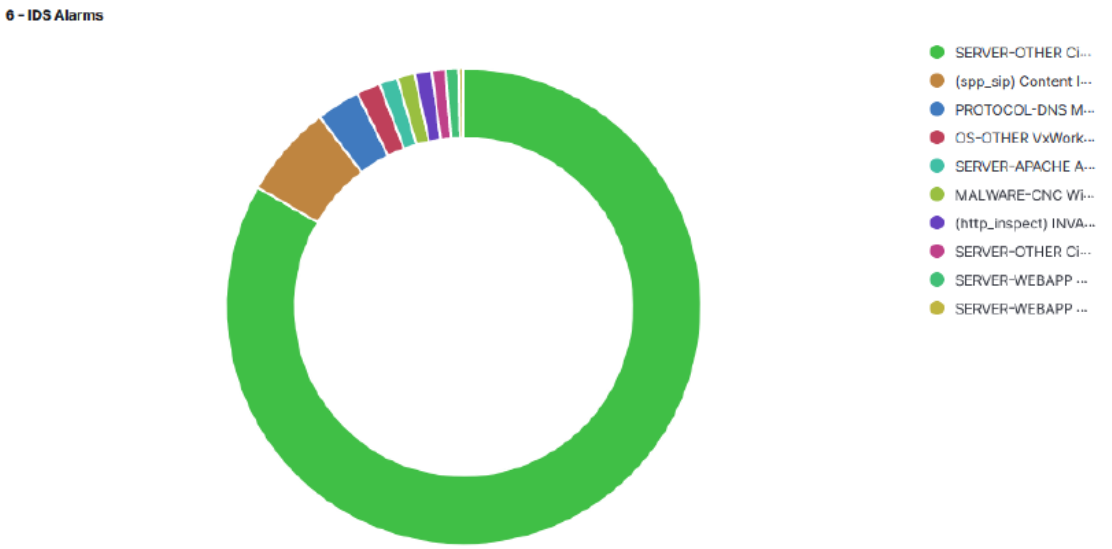
Kuukauden jälkeen kerättyä dataa käytiin läpi palaverissa, jossa palveluntarjoajan edustaja esitteli heidän raportointimalliaan. Raporttimalliin oli kerätty palomuurilta kerättyä syslog dataa, joka oli visualisoitu kaavioilla ja taulukoilla. Sen perusteella pystyttiin näkemään, paljonko liikennettä oli milläkin rajapinnalla siirtynyt kuukauden aikana ja mistä. Data on hyvin hyödyllistä niille yrityksille, jotka eivät aktiivisesti valvo

palomuurilla kulkevaa liikennettä. Snortin havainnoista oli oma kaavionsa, jossa esiteltiin ohjelmiston itse generoima kuvaus havainnosta, lähde osoite sekä kohdeosoite (kts. Kuviot 8 ja 9). Hälytyksiä ei ollut generoitunut kuukauden aikana kovinkaan paljon verrattuna käyttäjä- tai DMZ-verkkoon, mikä oli odotettavissa liikenteen ollessa staattista järjestelmässä. Suurin määrä hälytyksistä liittyi IPSec-protokollan haavoittuvuuteen, jossa yritettäisiin aiheuttaa DOS-hyökkäys IKEv2-kyselyiden avulla. Palomuurin suuren VPN-yhteyksien määrän vuoksi hälytys oli aiheellinen, mutta kuten kuviossa 12 voidaan nähdä, olivat hälytykset kahdesta eri osoitteesta, jotka voitiin todeta olevan asiakkaiden osoitteita. Hälytyksen avulla pystyttiin paikantamaan ongelma IPSec-yhteyden kättelyssä ja korjaamaan ongelma kyseisessä yhteydessä. Muut kuviossa 12 nähdyt hälytykset olivat aiheettomia niiden jäädessä WAN-rajapinnalle. Vaikka hälytykset olivat aiheettomia, toi raportti esille mitkä hyökkäykset olisivat mahdollisia järjestelmässä.

Huomioitavaa tässä on IDS-palvelun yksi heikkous. WAN-rajapinnan valvonta ei ole suotavaa koska IDS ei ymmärrä olla analysoimatta palomuurin jo estämiä paketteja ja kuormitusta tulee siksi turhaan. Näin kuitenkin tehtiin, jotta saataisiin mahdollisimman paljon dataa irti kuukauden ajalta ja saataisiin paremmin selvitettyä myös kuormitus vaatimuksia. Toisena WAN-rajapinnalle kohdistuva liikenne ei suurella todennäköisyydellä koskaan ole itse julkiselle rajapinnalle tarkoitettu, vaan sen takana olevalle palvelinverkolle. Toisin sanoen todenmukaisempia uhkaskenaarioita voidaan paremmin valvoa sisäverkon rajapinnoista. Tällöin tiedetään paremmin mihin palveluun uhka kohdistuu, sillä WAN-rajapinnalle jääneet paketit eivät ole vielä kerenneet mennä nattauksen läpi. Siksi lopullinen kohdeosoite voi olla vaikea tunnistaa. Miinuksena on, että uhka on jo päässyt läpi kyseiselle rajapinnalle ja mahdollisesti haavoittanut jo järjestelmiä.

Kaiken kaikkiaan demo kuvasti hyvin palvelun laajuutta ja mahdollisuuksia tuoda uutta näkökulmaa Traffic Gateway -palvelunkin liikenteen kulkuun. Raportti oli helposti luettava ja sisälsi tarpeellista informaatio, jota pystyi myös suodattamaan haluttuihin arvoihin. Demo korosti palveluntarjoajan palvelun vahvuuksia myös IDS-

rintamalla. Datankeruu on korkeammalla tasolla kuin pelkän IDS-järjestelmän tarjoamassa kokonaisuudessa, joka mahdollistaa paremman näkyvyyden verkossa ja auttaa staattisten valvontaparametrien luomisessa.



Kuvio 10. IDS-hälytykset osa1

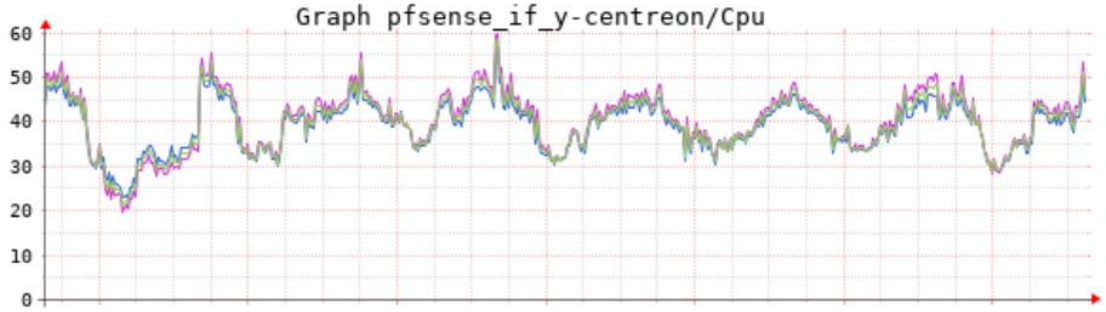
6 - Datasheet

Alarm	Alarm ID	Source IP	Destination IP	Count
SERVER-OTHER Cisco ASA IKEv2 denial of service attempt	32111			1,023
SERVER-OTHER Cisco ASA IKEv2 denial of service attempt	32113			316
(spp_sip) Content length mismatch	18			1
PROTOCOL-DNS Multiple vendor DNS message decompression denial of service attempt	23039			1
OS-OTHER VxWorks TCP URG memory corruption attempt	51111			4
SERVER-APACHE Apache Struts remote code execution attempt	41818			13
SERVER-APACHE Apache Struts remote code execution attempt	49376			13
MALWARE-CNC Win.Trojan.ZeroAccess inbound connection	31136			2
(http_inspect) INVALID CHUNK SIZE OR CHUNK SIZE FOLLOWED BY JUNK CHARACTERS	28			9
SERVER-OTHER Cisco IOS invalid IKE fragment length memory corruption or exhaustion attempt	37875			10

Kuvio 11. IDS-hälytykset osa2

Raporttiin kerätyn datan lisäksi seurattiin itse myös miten paljon IDS kuluttaisi palomuurilla resursseja sekä prosessoinnissa, muistissa että tallennustilassa. Suurin kuormitus arvioitiin näkyvän muistissa ja prosessoinnissa, mutta ei niinkään tallennustilassa sillä dataa talletettiin erilliselle palvelimelle. Kuvio 11 esittää muistin- ja kuvio 12 prosessorin käyttömäärän viikon ajalta (kts. Kuviot 11 ja 12).

Kuvio 12. Palomuurin muistin käyttö viikon ajalta



Kuvio 13. Palomuurin prosessorin käyttö viikon ajalta

Prosessointiin ei isoja piikkejä tai ylikuormituksia ollut huomattavissa viikon käytön aikana keskimääräisen kuormituksen ollessa n. 40%. Prosessoinnin kasvu oli n. 10% rajapintaa kohden. Voidaan siis todeta, että kahden prosessorin järjestelmä pystyi hyvin valvomaan kahta rajapintaa kaiken muun palomuurin tehtävien ohessa, mutta ei riitä kaikkien rajapintojen valvontaan.

Muistissa pystyttiin havaitsemaan säännöllisiä kuormituspiikkejä. Piikit tapahtuivat keskiyöllä ja kestivät noin 2 tuntia. Syyksi voidaan olettaa olevan tunnisteiden päivitys ja niiden uudelleen lataaminen, joka järjestelmää kuormittaa. Sen lisäksi järjestelmässä käynnistetään IPSec-tunnelit uudestaan joka yö klo. 2:00, joka voi myös olla syynä kuormitukselle. Piikkejä lukuun ottamatta muisti tuntui riittävän hyvin kahden rajapinnan kohdalla. Jos siis kolmas rajapinta olisi demoon lisätty, olisi normaalisti järjestelmä jaksanut ylläpitää IDS:n valvontaa kaiken muun ohessa. Mutta piikkien kohdilla kahdellakin rajapinnalla kuormituksen ollessa korkeimmillaan yli 90%, voi olla, että järjestelmän muisti olisi ylittynyt ja pidempi hidastuminen tai katkos voisi olla tuloksena.

5.4 Kustannukset

Työn yhtenä tavoitteena on löytää toimeksiantajalle IDS-palvelu, joka olisi kustannuksiltaan pieni, mutta sisältäisi kuitenkin yritykselle tärkeät ominaisuudet. Koska kumpikin IDS-ohjelmisto on ilmainen, mietitään kustannuksia palvelumuotojen mukaan. Jokaisesta palvelumuodosta on koottu taulukko, jossa on lyhyt kuvaus palvelusta sekä arvioidut kustannukset, jotka siitä seuraa. Virtuaalikoneiden ja rauta lisäysten kustannukset ovat palveluntarjoajan VaultCloud-hinnaston mukaan tehty 24kk:n määräaikaisella sopimuksella (www.tnnet.fi/tuotteet/vaultcloud/). Arvioidut vaadittavat työtunnit ovat myös lueteltuna taulukkoon, mutta ei ole huomioitu laskuissa.

Pfsensen paketti palvelumuoto on esiteltynä taulukossa 4 (kts. Taulukko 4). Tässä palvelumuodossa IDS-ohjelmisto olisi integroituna palomuurille, jolloin se hyödyntäisi palomuurin resursseja. Aiemmin tutkittujen resurssivaatimusten ansiosta tiedetään, etteivät nykyiset palomuurin resurssit riitä valvomaan Traffic Gateway -palvelun kaikkia rajapintoja. Siksi Arvioituihin kustannuksiin on laskettu mukaan prosessori määrän lisäys joko yhdellä tai kahdella prosessorilla, sekä muistin lisäys, joka olisi n. 0,4GB rajapintaa kohden, jotta järjestelmässä sattuvat piikit eivät aiheuttaisi haittoja muuhun toimintaan. Lisäkustannuksina palvelumuotoon tuottaa valinnainen lokien parantaminen, joka vaatisi erillisen lokipalvelimen, koska levytilan kasvattaminen ei ole suositeltua palomuurilla. Arvioidut kustannukset ilman erillistä loki-palvelinta tulisivat olemaan pienimmät vaihtoehtojen välillä.

Työtunteja on arvioitu olevan vähän kyseisen palvelumuodon parissa, sillä käyttöliittymä on valmiiksi tuttu tehdyn demon sekä ylläpitäjien palomuuri käyttöliittymän tuntemuksen ansiosta. Käyttöönotto on helppoa ja nopeata, mutta suurin osa tunneista tulee olemaan itse tunnisteiden suodatusvaiheen valvonnassa. Palomuurin vähäisten lokien keruu mahdollisuuksien takia valvontaa joudutaan suorittamaan aktiivisesti, vieden enemmän tunteja kuin valmiin palvelun kohdalla, jossa dataa voidaan isommissa kokonaisuuksissa katsoa läpi. Koulutukseen kuluvat työtunnit ovat samat jokaisen palvelumuodon kohdalla, koostuen koulutuksen laatimisesta, sekä kaikkien koulutukseen osallistuvien henkilöiden työtunneista.

Palvelumuoto	Pfsensen paketti
Kuvaus	Pfsenseen valmiiksi integroitu Snort/Suricata -paketti. Lisätään palomuurin resursseja tarpeiden mukaan
Kustannukset	Ohjelmisto ilmainen Muistia: n. 0,4GB/VLAN Prosessoreita: 3 - 4 kpl (Nykyinen 2kpl) Prosessori: 14€/kk/kpl Muisti: 9€/kk/GB Kustannukset lisättäisiin nykyiseen muurin kuukausi hintaan: 68 - 82€/kk
Työmäärä	Käyttöönotto: 1 työpäivä Suodatus vaihe: 2h/vrk kuukauden ajan Ylläpito: 1h/vko tai hälytyksen sattuessa Koulutukset: 3 työpäivää
HUOM	Maksullinen tunnistekanta jätetty laskuista. Pfsense vaatii vain yhden sensorin/yksi maksullinen sopimus valvomaan kaikkia rajapintoja Valinnainen lokipalvelin: 1CPU, 4GB RAM, 20GB SSD/500GB HDD - 55,30€ 2CPU, 8GB RAM, 20GB SSD/500GB HDD – 82,60€

Taulukko 4. Pfsense paketti palvelumuodon kustannusarvio

Itsenäisen palvelimen palvelumuoto on esiteltynä taulukossa 5 (kts. Taulukko 5). Tässä palvelumuodossa IDS-järjestelmä sijoitettaisiin omalle palvelimelle palomuurin taakse ja data kerättäisiin suoraan palvelimelle. Itsenäisen palvelimen kohdalla Kustannukset kasvavat uuden virtuaalipalvelimen hankinnan sekä käyttöönoton myötä, aiemman käyttökokemuksen ja käyttöönoton monimutkaisuuden takia.

Virtuaalikoneille palvelumuodolle on lueteltuna kolme eri versiota. Aiemmin tehdyissä testeissä todettiin, ettei 2 prosessoria riitä valvomaan kaikkia rajapintoja. Tuloksiin vaikutti palomuurin muut toimenpiteet, jotka veivät resursseja. Uudella palvelimella IDS olisi ainut ohjelma ja saisi siksi hyödyntää koko palvelimen resursseja. Siksi mahdollisuus on aloittaa ja kokeilla 2 prosessorin palvelimella. Virtuaalipalvelimelle tehoja pystyttäisiin helposti nostamaan myöhemmin tarpeen tullessa.

Kustannukset tulevat olemaan korkeammat tässä palvelumuodossa, sillä itse käyttöönottoon voidaan laskea menevän huomattavasti enemmän aikaa kuin kahteen muuhun palvelumuotoon. Ympäristö ei ole tuttu ylläpitäjille yrityksessä, sekä kaikki konfiguraatiot pitäisi tehdä alusta loppuun itse.

Palvelumuoto	**Itsenäinen palvelin**
Kuvaus	Uusi palvelin, johon asennetaan Snort/Suricata. Lähdetään testaamaan halvimmalla mahdollisella virtuaalikoneella. Palvelimen resursseja lisätään tarpeen mukaan
Kustannukset	Ohjelmisto ilmainen Virtuaalipalvelin vaihtoehdot (Linux): 2CPU, 8GB RAM, 20GB SSD/500GB HDD - 82,60€/kk 3CPU, 12GB RAM, 20GB SSD/500GB HDD - 109,90€/kk 4CPU, 16GB RAM, 20GB SSD/500GB HDD - 137,20€/kk
Työmäärä	Käyttöönotto: 3 työpäivää Suodatus vaihe: 2h/vrk kuukauden ajan Ylläpito: 1h/vko tai hälytyksen sattuessa Koulutukset: 3 työpäivää
HUOM	Maksulliset tunnistekannat nostaisivat paljon hinnastoa jokaisen rajapinnan tarvitessa oman sensorin.

Taulukko 5. Itsenäinen palvelin palvelumuodon kustannuasrvio

Viimeisessä taulukossa on esiteltynä palveluntarjoajan VaultSec-palvelun Enterprise versio (kts. Taulukko 6). Palvelu on kuukausihinnaltaan kalliimpi kuin aiemmat palvelumuodot, mutta tuo mukanaan jo valmiiksi viilatun palvelukokonaisuuden ja sitä kautta huolettomamman käyttöönoton. Palvelun mukana ei tarvitse huolehtia Virtuaalikoneiden tai palomuurin resurssien lisäyksistä, sillä tämä kuuluisi palvelun hintaan. Rajapintojen valvonta on rajaton ja konfigurointiin on tarjolla asiantuntevaa apua.

Työtunnit olisivat alhaisimmat tässä palvelumuodossa, jos verrataan muihin vaihtoehtoihin. Käyttöönoton suorittaa palveluntarjoaja, mikä helpottaa ja nopeuttaa prosessia toimeksiantajan puolella. Apua olisi myös tarjolla alkuvaiheen suodatuksissa, mikä tarkoittaa, että päästään nopeammin vaiheeseen, jossa ylläpitäjän ei tarvitse aktiivisesti joka päivä valvoa järjestelmää. Myös laajemmat lokit auttavat siirtymään

nopeammin ajoittaisiin ylläpitäjän tarkistuksiin, sillä dataa voidaan tutkia enemmän kerrallaan.

Palvelu hyödyntää myös Talosin maksullista tunnistekantaa. Tiedetään, että maksulliset tunnistekannat ovat kattavampia ja paremmin ylläpidettyjä kuin ilmaiset, mikä on suuri plussa palvelun kohdalla. Kantojen hinnastoja ei kuitenkaan ole otettu mukaan laskuihin kahden muun palvelumuodon kanssa kantojen kalliin hinnan vuoksi. Talosin maksullinen kanta, joka on halvin tarjolla oleva maksaa 399$ (n. 330€) sensoria kohden vuodessa (Rule Subscriptions n.d.) Proofpoint, joka ylläpitää Emerging Threats Pro Ruleset tunnistekantaa ei virallisesti ilmoita kannan hinnastoa sivuillaan ilman erillistä tarjouspyyntöä, mutta foorumeilta ja joidenkin verkkokauppojen sivuilta selviää, että yhden vuoden lisenssi voisi maksaa 400–800€. Jos hinnat laskettaisiin mukaan kahteen aikaisempaan palvelumuotoon, olisi Pfsensen paketti edelleen huomattavasti halvempi vaihtoehto Pfsensen pystyessä hyödyntämään yhtä maksullista kantaa kaikkiin rajapintoihin. Sen sijaan erillisessä palvelussa joka rajapinnalle pitäisi ostaa erillinen sensori/kanta, joka nostaisi hinnan roimasti yli kummankin muun palvelumuodon, korostaen palvelumuodon sopimattomuutta Traffic gateway -palvelun järjestelmään.

Palvelumuoto	**VaultSec Enterprise**
Kuvaus	Palveluntarjoajan keskikokoisille ja isoille yrityksille tarkoitettu IDS- ja loki-palvelu. Oma palvelin, jossa IDS ja Lokien keräys/jalostus Rajaton resurssien ja VLANien määrä tukipalvelut
Kustannukset	Palvelu: 500€/kk Lisäpalveluna Kuukausiraportti 160€/kk
Työmäärä	Käyttöönotto: 1 työpäivä Suodatus vaihe: 2-3h/vko kuukauden ajan Ylläpito: 1h/vko tai hälytyksen sattuessa Koulutukset: 3 työpäivää
HUOM	Talosin tarjoama maksullinen Snort VRT Tunnistekanta kuuluu hintaan

Taulukko 6. VaultSec Enterprise palvelumuodon kustannusarvio

6 Pohdinta

6.1 Johtopäätökset

Työn tavoitteena oli kartoittaa IDS-järjestelmän tarve Traffic Gateway -palvelussa ja selvittää olisiko IDS-järjestelmän lisäys järkevää palvelun kannalta huomioiden tutkimuskysymykset. Ensimmäisenä selvitettiin yrityksen vaatimukset IDS-järjestelmälle, jossa nousi esille seuraavat asiat:

- Kustannustehokkuus
- reaaliaikainen valvonta
- laaja protokolla kirjasto
- Pystyä suorittamaan valvontaa usealla rajapinnalla samanaikaisesti
- Mahdollisuus kehittää

Vaatimuksien perusteella koottiin myös tutkimuskysymykset. Kysymyksissä esiteltiin yksi pääkysymys sekä useilla tarkentavilla kysymyksillä. tutkimuskysymykset olivat:

- Onko IDS-palvelun lisääminen Traffic Gateway -palvelun yhteyteen järkevää tietoturvan kannalta
    - Vahvistaako IDS-palvelu yleistä tietoturvaa palvelussa
    - Mitkä toiminnallisuudet IDS-järjestelmään tarvitaan?
    - Mikä IDS-toteutus olisi käytännöllisin yritykselle?
    - Onko IDS-palvelun lisääminen nykyiseen palveluun taloudellisesti kannattavaa?
    - Vaikuttaako IDS negatiivisesti verkon toimintaan?

Kartoituksen aikana kaksi palvelumuotoa (Pfsense paketti ja VaultSec) toivat laajasti mukanaan toivottuja ominaisuuksia, erillisen palvelimen ollessa huomattavasti heikoin valinta Traffic Gateway -palvelussa. Vaatimuksien lisäksi käytiin läpi Traffic Gateway -palvelun riskianalyysissä havaitut uhat ja peilattiin IDS:n ominaisuuksia vaikuttaa niihin. Riskeistä paikannettiin 5 kpl uhkia, joihin IDS:n ominaisuuksilla olisi pystynyt vaikuttamaan.

Seuraavana vertailtiin itse IDS-ohjelmistoja, joihin valittiin kaksi avoimen lähdekoodin ohjelmaa, Snort ja Suricata. Valintakriteereinä toimivat Pfsensen integraatio mahdollisuus, hinta sekä kummankin laaja dokumentointi ja hyvin aktiiviset yhteisöfoorumit. Ohjelmistoja lähdettiin vertailemaan tuomalla kummankin vahvuudet esille ja sitä kautta etsittiin eroavaisuuksia ohjelmistojen välillä. Vertailukohteet osoittautuivat hyvin samankaltaisiksi ominaisuuksiltaan. Suurimmaksi eroavaisuudeksi korostui Suricatan multihreading-ominaisuus, jota ei Snortin Pfsense-integraatiossa käytettävä versio hyödyntänyt.

Kummatkin IDS-ohjelmistot kattoivat ominaisuuksiltaan järjestelmälle aiemmin määritetyt vaatimukset koostuen alhaisista kustannuksista, laajasta protokollien valvonta kirjastosta sekä kattavasta usean rajapinnan reaaliaikaisesta valvonnasta. Vaatimuksien lisäksi ohjelmistot toivat mukanaan kehitysmahdollisuuksia sekä valvonnan että yleisen lokituksen kannalla. Kehitysmahdollisuuksina korostui omien tunnisteiden tekomahdollisuus, mahdollisuus siirtyä aktiiviseen valvontaan ja laajemman lokituksen toteutus. Ottaen huomioon kaikki aiemmin mainitut seikat, voidaan todeta IDS-palvelun parantavan Traffic Gateway -palvelussa tietoturvaa ja yleistä havainnointia.

Palvelumuodoista sekä Pfsensen paketti että palveluntarjoajan palvelu todettiin sopivaksi Traffic Gateway -palvelussa. Erillinen itse rakennettu IDS-palvelin ei sopinut vaihtoehdoksi Traffic Gateway -palveluun usean syyn vuoksi. Suurimpana syynä oli ympäristön monimutkainen usean rajapinnan rakenne. Erillinen IDS:n sisältävä laite pitäisi lisätä jokaiselle rajapinnalle, jotta valvonta toimisi, tai data pitäisi kopioida erilliselle yksittäiselle IDS-palvelimelle, jolloin jouduttaisiin luopumaan ominaisuuksista, kuten suoraan hälytyksistä generoitavista estosäännöistä ja aktiivisesta valvonnasta.

Pfsensen paketin vahvuudet olivat tuttu ja helppokäyttöinen käyttöliittymä sekä alhaiset kustannukset, joissa kulut koostuivat palomuurin resurssien lisäämisestä sekä ylläpidon käyttöönotto ja valvonta kustannuksista. Valmiin palvelun vahvuudet olivat sen monipuolisuudessa, palvelun tuodessa pelkän IDS-järjestelmän lisäksi laajempaa lokien keräystä. Palveluun kuului myös asiantunteva tuki ja valvontaa parantava Talosin maksullinen Snort VRT -tunnistekanta. Miinuksena oli palvelun korkeahko hinta

(500€/kk) verraten toisiin vaihtoehotihin. Kaiken oppiman jälkeen pystyttiin vastaamaan tutkimuskysymyksien pääkysymykseen ja todeta IDS-järjestelmän olevan soveltuva Traffic Gateway -palvelussa. Tulosta korosti IDS:n monipuolisuus, alhainen käyttöönotto kynnys sekä tulevaisuuden hyödyt.

6.2 Hankintasuositus

Sekä palveluntarjoajan palvelu että Pfsensen integraatio on todettu toimivaksi tehdyssä demossa, jossa hyödynnettiin kumpaakin palvelumuotoa. Valmiin palvelun raportti toi paljon hyödyllistä dataa esille näyttäen hyvin mitä mahdollisuuksia laajempi lokitus toisi järjestelmässä kun taas Pfsensen integraatio loisti sen alhaisten kustannuksien kohdalla. Kumpikin tuo omat vahvuutensa esille eikä kumpikaan ole huono vaihtoehto kohdepalvelulle. Siksi hankintasuositus on tehty kumpaankin palvelumuotoon peilaten.

6.2.1 Pfsense paketti

Pfsensen paketti oli kaikista halvin ja helpoin käyttöönottaa tutun ympäristön ja valmiiden konfiguraatioparametrien saatavuuden ansiosta. Käyttöliittymässä on mahdollisuus suoraan selailla ja vaikuttaa havaittuihin hälytyksiin ja hälytyksien kohdalta on suora linkki tarkempaan kuvaukseen havaituista uhista lisäten monitorointia verkossa. Integraatiossa ei menetetä ominaisuuksia itsenäisen versioon verrattuna, joten haittapuolia ei ole muuta kuin palomuurin nykyiset resurssimäärät, joita jouduttaisiin lisäämään. Ohjelmistovaihtoehtoina oli Snort ja Suricata, joista Suricata olisi tällä hetkellä parempi vaihtoehto. Suricata on käytettävyydeltään ja vaadittavilta ominaisuuksiltaan liki identtinen Snortin kanssa, tuoden samalla enemmän yritykselle hyödyllisiä ominaisuuksia ja ennen kaikkea prosessointi tehoa.

Suricata on myös tehokkaampi ohjelmisto kuin Snort multithreading-ominaisuuden avulla, jonka avulla järjestelmän prosessointitehoja pystytään hyödyntämään tehokkaammin. Vaikutus korostuu mitä enemmän rajapintoja lisätään. Suricatalla on myös tarjolla sama tunnistekirjasto kuin Snortilla sekä valvontaan laajempi kirjasto protokollia kuten IKev2-protokolla, joka voisi olla hyödyksi Traffic Gateway -järjestelmässä.

Suricatan omat viralliset dokumentaatiot ovat hyvin kattavat siistillä ja selvällä rakenteella, mikä auttaa ongelmien selvityksessä. Sen lisäksi Pfsensen versiosta löytyy paljon videoita esimerkiksi Youtubesta, joita pystytään myös hyödyntämään tarpeen tullessa. Suricatan nykyinen versio 5 on edelleen ylläpidetty versio. Suricata 6 julkaisu oli elokuussa 2020, mutta Pfsensen versio on vielä työn alla.

6.2.2 VaultSec-palvelu

Palvelu oli hintaluokaltaan hieman kalliimpi kuin itse rakennettu, mutta on valmis kokonaisuus, joka helpottaisi käyttöönottoa ja suoraan parantaisi näkyvyyttä järjestelmässä. Traffic Gateway -ympäristö on palomuurin osalta tuttu palveluntarjoajalle, josta on myös apua käyttöönotossa. Lisäksi palveluntarjoajalta on saatavilla apua koko palvelun elinkaarelle ja on mahdollisuus myös järjestää koulutuksia IDS:n tai lokipalvelimen käyttöön liittyen tai tilata lisäpalveluna heidän tekemiään kuukausiraportteja jotka olisivat demossa esitetyssä muodossa.

Lokeja pystyttäisiin keräämään erilliselle lokipalvelimelle palomuurin lisäksi muistakin järjestelmään kuuluvista laitteista kuten palvelimilta. Lokipalvelimella on myös lupa itse luoda omia kuvioita tai trendejä halutuista resursseista. IDS:n valvontadataakin olisi helpompaa käsitellä ja staattisia hälytysrajapintoja olisi helpompi tehdä. Palvelussa käytettäisiin myös maksullista tunnistekantaa, mikä jo itsessään lisäisi havaittavuutta suuremman tunnistemäärän ansiosta.

Palvelu pystytään toteuttamaan erillisenä tai Pfsensen integroidun IDS:n tavoin, joista integraatio on todennäköisin aiemmin mainitun rajapintalukumäärän vuoksi. Sitä ajatellen palvelu kattaa palomuurille vaadittavat IDS:n aiheuttamat lisäresurssien kustannukset.

Lähteet

Anicas, M. 2015. What is a Firewall and How Does It Work?. Verkkojulkaisu. Viitattu 15.7.2020. https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work.

About Netgate. n.d. Netgate kotisivut. Viitattu 15.7.2020. https://www.net-gate.com/company/about-us.html.

Guercio, K. 2021. Best Intrusion Detection and Prevention Systems for 2021: Guide to IDPS. Verkkojulkaisu. Viitattu 15.1.2021. https://www.esecurityplanet.com/products/intrusion-detection-and-prevention-systems/.

Keary, T. 2020. IDS vs IPS. Verkkojulkaisu. Viitattu 23.6.2020. https://www.comparitech.com/net-admin/ids-vs-ips/.

Loshin, P. 2018. IPsec (Internet Protocol Security). Verkkojulkaisu. Viitattu 24.6.2020. https://searchsecurity.techtarget.com/definition/IPsec-Internet-Protocol-Security.

Lutkevich, B. 2020. Intrusion Detection System (IDS). Verkkojulkaisu. Viitattu 1.7.2020. https://searchsecurity.techtarget.com/definition/intrusion-detection-system.

Netscout Threat Intelligence Report. 2020. Netscout kyberuhkaraportti. Viitattu 22.10.2020. https://www.netscout.com/threatreport.

OISF. n.d. Suricata verkkojulkaisu Open Information Security Foundation järjestöstä. Viitattu 11.1.2021. https://suricata-ids.org/about/oisf/

Open Source IDS Tools: Comparing Suricata, Snort, Bro (Zeek), Linux. 2020. Blogi. Viitattu 8.1.2021. https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview.

Pathan, A. 2014, The state of the art in intrusion prevention and detection, E-kirja, Boca Raton/ Florida: CRC Press/Taylor & Francis Group, Viitattu 2.2.2021.

Pfsense, Getting started. n.d. Pfsense esittely sivu. Viitattu 15.7.2020. https://www.pfsense.org/getting-started/.

Pfsense. n.d. Netgaten Pfsense esittelysivu. Viitattu 15.7.2020. https://www.net-gate.com/solutions/pfsense/#applications

Rule Subscriptions. n.d. Snort tunnistekantojen hinnasto. Viitattu 23.6.2020. https://www.snort.org/products#rule_subscriptions.

Snort 3. n.d. Snort versio 3 esittelysivu. Viitattu 26.1.2021. https://www.snort.org/snort3.

Suricata, Complete list of Suricata features. n.d. Suricata ominaisuuksien listaus. Viitattu 26.1.2021. https://suricata-ids.org/features/all-features/.

Tuomi, S. & Latvala, E. N.d. Opinnäytetyön ohjaajan käsikirja. Jyväskylän ammattikorkeakoulun avoimet oppimateriaalit. Viitattu 5.2.2020. https://oppimateriaalit.jamk.fi/yamk-kasikirja/.

What are the differences in the rule sets?. N.d. Snort usein kysytyt kysymykset sivu. Viitattu 24.6.2020. https://www.snort.org/faq/what-are-the-differences-in-the-rule-sets.

What can I do with Snort?. n.d. Snort FAQ. Viitattu 26.1.2021. https://www.snort.org/faq/what-can-i-do-with-snort.

What is a Next Generation Firewall (NGFW)?. n.d. Check pointin verkkojulkaisu. Viitattu 15.7.2020. https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/#.

What Is IKEv2?. n.d. CactusVPN esittely IKEv2 toimintaan. Viitattu 11.1.2021. https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-ikev2/#definition.

What Is OpenVPN & How Does OpenVPN Work?. n.d. CactusVPN esittely OpenVPN toimintaan. Viitattu 11.1.2021. https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-openvpn/#definition.

White, J. Fitzsimmons, T & Matthews, J. 2013. Quantitative Analysis of Intrusion Detection Systems: Snort and Suricata. Clarkson yliopiston tekemä tutkielma. Viitattu 9.11.2020. https://people.clarkson.edu/~jmatthew/publications/SPIE_SnortSuricata_2013.pdf.

Yadav, A. 2020. Network design: Firewall, IDS/IPS. Verkkojulkaisu. Viitattu 16.8.2020. https://resources.infosecinstitute.com/topic/network-design-firewall-idsips/#gref.

YSP Oy. n.d. YSP kotisivut. Viitattu 8.6.2020. https://www.ysp.fi/ysp/