Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2024

Kasper Jokinen

Fortinet-tuotteiden kartoitus yritykselle

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikka

2024 | 30 sivua

Kasper Jokinen

Fortinet-tuotteiden kartoitus yritykselle

Opinnäytetyön tavoitteena oli saada laajempi kuva yrityksen käyttämistä Fortinetin tietoturva- ja hallinnointituotteista ja niihin liittyvistä ominaisuuksista. Työssä selvitettiin myös Fortinetin tuotteita, joita on suunniteltu otettavan käyttöön. Nämä kaksi tuotetta ovat FortiWAF ja automatisoitu palvelinvarmenteiden provisiointi.

Fortinet on tietoturva-alan yritys, jonka tarjonnassa on monenlaisia tuotteita. Tähän työhön Fortinetin tuotteista valikoitui verkkosovelluspalomuuri (WAF), Kuormantasaus (GSLB), sovelluksentoimitusohjain (ADC) ja automatisoitu palvelinvarmenteiden provisiointi.

Raportti on teoreettinen katsaus edellä mainittuihin Fortinetin tietoturvatuotteisiin.

Asiasanat:

sovellus, varmenne, verkkoturvauhka, ohjain, palomuuri

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2024| 30 pages

Kasper Jokinen

Mapping of Fortinet products for a client company

The objective of the thesis was to acquire a comprehensive understanding of the security and management products from Fortinet utilized by the company, as well as the products associated features. The thesis also investigated Fortinet products that the company is adopting in the future. These products are FortiWAF and automated provisioning of server certificates.

Fortinet is a company specializing in cybersecurity, offering a diverse range of products. The products chosen for this thesis included a Web Application Firewall (WAF), Global Server Load Balancing (GSLB), an Application Delivery Controller (ADC), and automated provisioning of server certificates.

The report provides a theoretical review of the Fortinet security products.

Keywords:

application, certificate, web security risk, controller, firewall

Sisältö

Kuvat

Lyhenteet

ADC	Application Delivery Controller, Sovelluksen-toimitusohjain
API	Application Programming Interface, Ohjelmointirajapinta
DNS	Domain Name System, Nimipalvelujärjestelmä
GSLB	Global Server Load Balancing, Globaali kuormantasaus
IP	Internet Protocol
IPS	Intrusion Prevention System, Tunkeilijan estojärjestelmä
SQL	Structured Query Language, Standardoitu kyselykieli
SSL	Secure Sockets Layer, Salausprotokolla
TLS	Transport Layer Security, Salausprotokolla
WAF	Web Application Firewall, Verkkosovelluspalomuuri

1 Johdanto

Tässä opinnäytetyössä perehdytään tietoturvayritys Fortinetin tietoturva- ja hallintotuotteisiin. Fortinetin tuotteista käydään läpi verkkosovelluspalomuuri (WAF), kuormantasaus (GSLB), sovelluksentoimitusohjain (ADC) ja palvelinvarmenteiden automaattinen provisiointi. Työssä on Fortinet-tuotteiden tuoteselostuksia ja ominaisuuksien yksityiskohtaisempia avauksia.

Opinnäytetyön tarkoituksena on kerätä yhteen eräänlainen kokonaisuus yleisestä teoriasta ja määritelmistä sekä hieman syvemmälle menevistä Fortinetin tuotteiden selostuksista. Yleinen teoria käsittelee TLS/SSL-sertifikaatit, palomuurit ja yleisimmät verkossa olevat uhat. Pohjustus toimii kontekstina Fortinetin tuotteille. Tarkoituksena on saada kattava kuva, millaiset järjestelmät ja protokollat ovat sekä selvittää tuotteiden ominaisuuksia.

Tämä opinnäytetyö on tehty toimeksiantona suomalaiselle ICT-alan yritykselle. Yritys käyttää Fortinetin tuotteita, joista osa on jo käytössä ja osaa ollaan ottamassa käyttöön tulevaisuudessa.

Opinnäytetyön yhtenä osana on tutkia, millainen on Fortinetin automaattinen sertifikaattien provisiointi. Tämä olisi mahdollisesti hyödyllinen työkalu tulevaisuudessa, sillä nykyisin suurin osa sertifikaateista on vain vuoden voimassa kerrallaan. Jos yrityksellä on näitä paljon, aiheuttaa se paljon työtä. Tällaisen työkalun avulla saataisiin vähennettyä pakollista ns. liukuhihnatyötä.

2 Palomuuri

Palomuuri on digitaalinen tai fyysinen laite, joka valvoo sisään- ja ulosmenevää liikennettä tietoverkossa. Palomuuri toimii sille annettujen ohjeiden mukaisesti ja estää tai sallii haluttuja IP-osoitteita ja datapaketteja. Palomuureja käytetään pienissä kotiverkoissa sekä isoissa korporaatio ympäristöissä. (Yasar, 2024)

Palomuuri toimii ykköstason suojauksena ulkoisilta uhilta. Yhdistettynä IPS:n (Intrusion Prevention System) kanssa se tarjoaa suuremman suojan ulkoisilta uhilta. Palomuuri toimii porttina sisäisen tietoverkon ja ulkoisen tietoverkon välillä. Se päättää sille konfiguroitujen sääntöjen mukaan mitkä datapaketit pääsevät läpi ja mitkä eivät pääse sisälle suojattuun verkkoon. (Yasar, 2024)

Palomuureilla voidaan rajata verkkoa haluttavalla tavalla. Niitä voidaan hyödyntää lokien keräämisessä, kun halutaan selvittää esimerkiksi erilaisia käytäntömalleja. Palomuureilla voidaan estää pääsy esimerkiksi työn kannalta tarpeettomiin nettisivuihin ja täten parantaa verkkoympäristön tietoturvaa. (Yasar, 2024)

3 TLS/SSL-Sertifikaatit

Sertifikaateista käytetään nimeä digitaalinen varmenne. Varmenteen tehtävänä on salata ja todentaa verkkosivusto. SSL (Secure Sockets Layer) on suojausprotokolla, joka on nykyisin kehittynyt TLS-protokollaksi. HTTP-protokolla hyödyntää SSL:ää. Näin HTTPS-yhteydet ovat suojattuja verrattuna esim. HTTP-yhteyksiin. SSL salaa liikkuvan datan verkkosivuston ja käyttäjän välillä käyttäen salausalgoritmeja. Täten data saadaan kryptattua, eikä sitä pysty lukemaan. (Kaspersky, 2024)

SSL salauksen prosessi toimii siten, että selain yrittää muodostaa yhteyden SSL-suojattuun verkkopalvelimeen. Selain lähettää palvelimelle pyynnön tunnistautumisesta. Palvelimen tunnistauduttua se lähettää selaimelle takaisin oman SSL-varmenne kopionsa. Kun selain on saanut palvelimen varmennekopion, se tarkistaa sen luotettavuuden. Jos selain luottaa varmenteeseen, prosessi etenee ja selain ilmoittaa sen palvelimelle. Palvelin lähettää selaimelle digitaalisen allekirjoituksen ja käynnistää SSL-yhteyden. Tätä prosessia kutsutaan SSL-kättelyksi. (Kaspersky, 2024)

SSL-varmenne sisältää varsinaisen palvelunimen ja mahdolliset lisänimet. Varmenteessa näytetään sen digitaalinen allekirjoitus ja sen myöntänyt varmenneviranomainen. Varmenteesta löytyy myös sen myöntämispäivä sekä sen vanhenemispäivä. SSL-varmenteen tiedoista selviää mille taholle se on myönnetty. Taho voi olla yritys, henkilö tai laite. Viimeisenä varmenne pitää sisällään julkisen avaimen, jota se käyttää salatun yhteyden luomiseen. (Kaspersky, 2024)

4 Verkkopalveluiden hyökkäysrajapinta

Verkkoturvauhat ovat internetistä peräisin olevia kyberturvallisuusriskejä, jotka voivat altistaa käyttäjät verkossa tapahtuvalle vahingolle ja aiheuttaa ei-toivottuja toimia tai tapahtumia. Verkkoturvauhat voivat vahingoittaa vakavasti yrityksiä ja yksityishenkilöitä. (Fortinet, 2024a)

Yleisiä verkkoturvauhkia ovat tietokonevirukset, datavarkaudet ja kalasteluhyökkäykset. Tyypillisiä ongelmia ovat mm. arkaluontoisten tietojen joutuminen vääriin käsiin, henkilöiden pääsyn estäminen työasemille ja tietoverkoille ja hyökkääjän pääseminen sisälle yritysverkkoihin. (Fortinet, 2024a)

Verkkoturvauhat ja erilaiset hyökkäysmenetelmät ovat kehittyneet monimutkaisemmiksi nopeampien mobiiliverkkojen ja älylaitteiden myötä. Lisääntynyt verkon käyttö suosittujen viestintä- ja tuottavuustyökalujen sekä Internet of Things (IoT) kautta on edennyt nopeammin kuin useimpien yritysten ja loppukäyttäjien turvallisuustietoisuus. Verkkoturvauhat lisääntyvät entisestään, kun ihmiset muuttuvat yhä riippuvaisemmiksi internetistä. Tämä luo uusia haavoittuvuuksia, joita hyökkääjät voivat hyväksikäyttää. (Fortinet, 2024a)

4.1 Yleiset hyökkäysmenetelmät

Seuraavissa kappaleissa käydään läpi Fortinetin listaamat yleisimmät verkkoturvauhat, joille yritykset altistuvat. Hyökkääjien käyttämät keinot ovat lisääntyneet ja kehittyneet vuosien varrella hyvinkin edistyneiksi. Samalla puolustus tulee hieman perässä ja paikkaa hyökkääjien löytämiä aukkoja.

4.1.1 Kalastelu

Kalasteluhyökkäyksissä hyökkääjät lähestyvät käyttäjiä sähköpostitse, tekstiviesteillä tai sosiaalisen median viestisivustoilla. He esiintyvät luotettavana lähettäjänä huijatakseen käyttäjiä luovuttamaan arkaluonteisia tietoja, kuten tilinumeroita, luottokorttitietoja ja kirjautumistunnuksia. Onnistunut Kalasteluhyökkäys voi myös johtaa siihen, että kyberrikolliset saavat luvattoman pääsyn yritysverkkoihin, mahdollistaen liiketoimintadatan varastamisen. (Fortinet, 2024a)

4.1.2 Kiristysohjelmat

Kiristysohjelma on haittaohjelman muoto, jossa hyökkääjä pitää uhrinsa tietoja ja dataa panttivankina. Hyökkääjä uhkaa estää pääsyn tietoihin, tuhota ne tai julkaista tiedot, ellei uhri maksa lunnasvaatimusta. Kiristyshyökkäykset aloitetaan tyypillisesti sähköposteilla, jotka sisältävät haitallisia liitteitä tai linkkejä. Tarkoituksena on saada uhrin koneelle haittaohjelma. Ohjelma etsii salattavia tiedostoja ja lukitsee ne käyttäjiltä. (Fortinet, 2024a)

4.1.3 SQL-injektio

Structured Query Language (SQL) on tietokonekieli, jota käytetään tietokantojen hakemiseen ja kyselyihin. SQL-injektio on verkkoturvauhka, jossa hyökkääjät hyödyntävät haavoittuvuuksia sovelluskoodissa. Hyökkääjät saavuttavat tämän syöttämällä SQL-kyselyn tavallisiin verkkolomakekenttiin,

kuten verkkosivuston kirjautumislaatikoihin, jotka välitetään sovelluksen SQL-tietokantaan. SQL-injektioita on hyödynnetty jaetuissa koodikannoissa, kuten WordPress-lisäosissa. Hyökkääjät käyttävät tätä haavoittuvuutta varastaakseen mm. yrityksen arkaluonteisia tietoja. (Fortinet, 2024a)

4.1.4 Cross-site Scripting

Cross-site scripting (XSS) on verkkoturvauhka, joka mahdollistaa hyökkääjien suorittaa haitallisia skriptejä luotetuilla verkkosivustoilla. XSS-hyökkäyksessä verkkosovelluksia tai -sivuja käytetään lähettämään haitallista koodia ja vaarantamaan käyttäjävuorovaikutukset. Hyökkääjä voi sen jälkeen kaapata käyttäjän identiteetin suorittaakseen haitallista toimintaa. XSS-hyökkäyksissä käytetty skripti estää käyttäjän selaimia tunnistamasta haitallista toimintaa. Näin ollen hyökkääjä voi vapaasti selata käyttäjän evästeitä, arkaluonteisia tietoja ja sessiotokeneita, jotka on tallennettu käyttäjän selaimeen. (Fortinet, 2024a)

4.1.5 DDoS

DDoS hyökkäyksessä hyökkäävä taho aiheuttaa palvelimien jumiutumisen isolla määrällä internetliikennettä. Tarkoituksena on aiheuttaa halutulle verkolla niin iso kuorma, että palvelua ei voida käyttää tai se on hidasta. Moni näistä hyökkäyksistä on haktivistien tekemiä ja rahallisesti motivoituja. (Fortinet, 2024a)

4.1.6 Virukset ja madot

Virukset ja madot ovat haitallisia ohjelmia, jotka leviävät koneisiin ja tietoverkkoihin. Molemmat hyödyntävät haavoittuvuuksia sovelluksissa. Niitä käytetään tiedon saamiseen sekä takaovien asentamiseen. Takaovi mahdollistaa myöhemmin pääsyn koneeseen tai tietoverkkoon. Madot käyttävät erityisesti valtavia määriä tietokoneen muistia ja verkon kaistanleveyttä, mikä johtaa palvelimien, järjestelmien ja verkkojen ylikuormittumiseen ja toimintahäiriöihin. Madot voivat toimia itsenäisesti, mikä mahdollistaa leviämisen järjestelmien välillä, mutta virus tarvitsee isäntätietokoneen suorittaakseen haitallista toimintaa. (Fortinet, 2024a)

4.1.7 Vakoiluohjelmat

Vakoiluohjelma on haittaohjelman muoto, joka kerää tietoja käyttäjiltä ja heidän laitteistaan ja lähettää ne kolmansille osapuolille. Vakoiluohjelma kerää tyypillisesti arkaluonteisia tietoja ja jakaa niitä mainostajille, tiedonkeruuyrityksille ja kyberrikollisille, jotka voivat käyttää näitä tietoja hyödykseen. Vakoiluohjelman tunnistaminen voi olla vaikeaa, ja se voi aiheuttaa vakavaa vahinkoa laitteille ja verkoille. Se voi myös jättää yrityksen alttiiksi tietomurroille sekä vaikuttaa laitteen ja verkon suorituskykyyn. (Fortinet, 2024a)

5 Verkon optimointi

5.1 ADC

ADC (application delivery controller). Se on tietoverkon osa, joka hallitsee ja optimoi sitä, miten client-koneet yhdistyvät verkkoon ja yrityksen sovelluspalvelimiin. Yleisesti ottaen kontrollerilla tarkoitetaan fyysistä laitetta tai sovellusta, joka ohjaa dataliikennettä laitteiden välillä. ADC toimii kuormantasaajana palvelimien välillä ja nopeuttaa sovelluksia. (Earls, 2024)

Kuvassa 1 on yksinkertaistettuna ADC:n paikka tietoverkkoasetelmassa. ADC toimii palomuurin ja palvelimien välissä tiedonvälittäjänä ja hallintavälineenä.

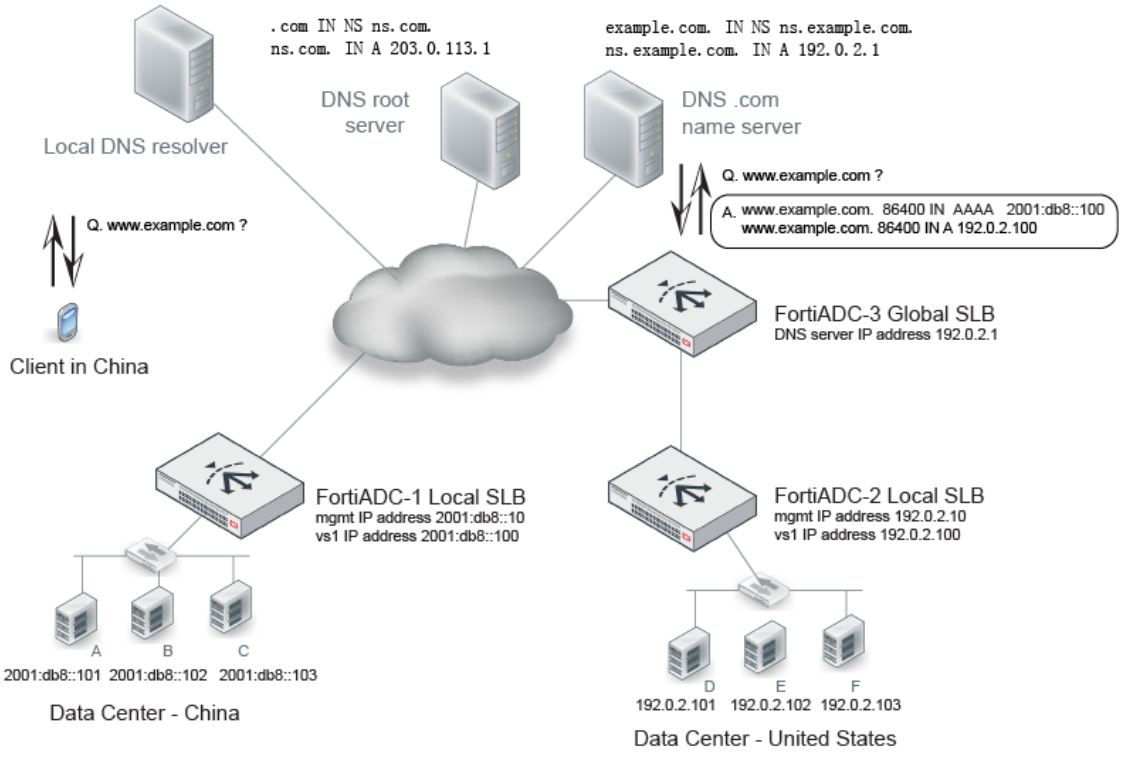
Kuva 1. Esimerkki ADC asetelmasta (Earls, 2024)

Uusimissa ADC konfiguraatioissa käytetään SSL/TLS-offloadausta, rate shapingia ja verkkosovelluspalomuureja. ADC optimoi loppukäyttäjän suorituskyvyn, luotettavuuden, datakeskuksen resurssien käytön ja turvallisuuden yrityksen sovelluksille. ADC nopeuttaa sovellusten suorituskykyä laajennetussa verkkoympäristössä toteuttamalla optimointitekniikoita, kuten sovelluksen luokittelua, pakkausta ja käänteistä välimuistitusta. Tyypillisesti ADC sijoitetaan palomuurin taakse ja yhden tai useamman sovelluspalvelimen eteen. Se toimii yhtenä hallintapisteenä, joka voi määrittää sovelluksen turvallisuustarpeet ja tarjota yksinkertaistetun tunnistuksen, autentikoinnin ja tilien hallinnan. (Earls, 2024)

5.2 GSLB

GSLB (global server load balancing). Suomeksi käytetään termiä kuormantasaus. GSLB:llä internetliikenne jaetaan globaalisti hajautettujen palvelimien kesken. GSLB:n etuja ovat mm. niiden luotettavuus ja pienet viiveet. Kuormantasaus itsessään tapahtuu kahden tai useamman palvelimen välillä. Internetliikenne jaetaan näiden palvelimien kesken, jotta yksi ei kuormitu liikaa. Kuormantasauksen voi jakaa ”tyhmiin” ja ”älykkäisiin” tekniikoihin. ”Tyhmissä” tekniikoissa kuorma jaetaan satunnaisesti, kun taas ”älykkäissä” on ominaisuuksia, jotka pystyvät päättelemään, mikä palvelin on paras käsittelemään pyynnön kyseisellä hetkellä. GSLB pystyy jakamaan liikennettä moneen eri paikkaan varmistaen sen, ettei mikään yksittäinen kohde käsittele niin montaa pyyntöä, että se aiheuttaa merkittävää viivettä. (Cloudflare, 2024b)

Kuvassa 2 on Fortinetin mallin mukainen GSLB asetelma. Kuvasta löytyy myös Fortinetin ADC-ohjaimia.



Kuva 2. Esimerkki verkkokuva GSLB (Fortinet, 2024e)

GSLB voi merkittävästi vähentää pyyntöjen ja vastausten matka-aikaa käyttäjien ja palvelimien välillä. Esimerkkinä jos käyttäjä on Los Angelesissa ja hän käyttää verkkopalvelua, jonka alkuperäispalvelin on Pariisissa, sekä pyynnöt että vastaukset joutuvat kulkemaan pitkän matkan, joka jaetaan pienempiin matkasegmentteihin, joita kutsutaan "hypyiksi". Tämä voi aiheuttaa merkittäviä viiveitä latausajassa. Käyttämällä GSLB:tä, maailmanlaajuinen palvelinallas varmistaa, että jokainen käyttäjä voi yhdistää maantieteellisesti lähellä olevaan palvelimeen, minimoiden ”hypyt” ja matka-ajan. Edellä mainitussa esimerkissä, jos Pariisissa toimiva yritys käyttäisi GSLB:tä, Los Angelesin käyttäjä voisi yhdistää palvelimeen, joka on 100 mailin säteellä hänen sijainnistaan. (Cloudflare, 2024b)

5.3 FortiADC

FortiADC on kehittynyt sovellusten toimituksen ohjain (ADC), joka tekee sovellusten käytöstä tehokkaampaa ja turvallisempaa. FortiADC toimii on-premisena tai pilvessä. Se parantaa sovellusten suorituskykyä ja varmistaa niiden turvallisuuden. FortiADC:n ominaisuuksiin kuuluu tehokas kuormantasaus tasolta 4 tasolle 7. Se sisältää myös työkaluja sisällön muokkaamiseen ja tukee edistyneitä SSL-palveluita, kuten offloadausta ja peilausta. (Fortinet, 2024c)

FortiADC nopeuttaa sovellusten toimintaa ja tarjoaa autentikointipalveluja. Se sisältää turvaominaisuuksia, kuten verkkosovelluspalomuurin, joka suojaa sovelluksia yleisimmiltä verkosta tulevilta uhilta. Palomuurin lisäksi ADC tarjoaa mm. DDoS-suojauksen ja Zero Trust Network Accessin (ZTNA). FortiADC:n voi ottaa käyttöön monella tavalla, esimerkiksi laitteistona, virtuaalikoneena, FortiFlexinä tai käyttämällä pilvipalveluiden tarjoajia. Se on myös integroitavissa Fortinetin turvaverkkoon. (Fortinet, 2024c)

Seuraavissa kappaleissa käydään läpi FortiADC:n ominaisuuksia ja sen kytköksiä muihin Fortinetin tuotteisiin.

5.3.1 Application Availability

Ominaisuus mahdollistaa monitenantti ratkaisun. Sekä VDOM että ADOM. Sovellusten suorituskyky, skaalautuvuus ja joustavuus ovat avainasemassa. (Fortinet, 2024c)

5.3.2 Web Application Protection

FortiADC WAF tuo suojaa OWASP top-10-hyökkäyksiä vastaan. Weballekirjoitukset auttavat torjumaan sekä tunnettuja että tuntemattomia hyökkäyksiä. API-turva suojaa pahantahtoisilta käyttäjiltä toteuttamalla automaattisesti turvallisuussääntöjä. Ominaisuus lisää API-turvan sujuvasti osaksi CI/CD-prosessia. (Fortinet, 2024c)

5.3.3 Application Anywhere

FortiADC:hen sisältyvä GSLB toimii on-preminä tai pilvessä. Se tekee verkosta luotettavan ja saavutettavan skaalaamalla sovellukset monien tietokeskusten kautta. Tämä siksi, että se mahdollistaa tietojen palautuksen ja parantaa sovellusten vasteaikoja. (Fortinet, 2024c)

5.3.4 Data Optimization

PageSpeed-sarjan verkkosivuston suorituskykyä parantavat työkalut voivat automaattisesti optimoida HTTP:n, CSS:n, Javascriptin ja kuvien toimituksen sovellusten käyttäjille. FortiADC mahdollistaa myös dynaamisen välimuistin, HTTP kompression ja purkamisen. (Fortinet, 2024c)

5.3.5 Application Access Management

FortiADC toimii portinvartijana offloadatakseen HTTP autentikoinnin ja valtuutuksen asiakassovelluksiin käyttäen SSO:ta, SAML:ia, LDAP:ia, RADIUS:ta, ja MFA:ta. (Fortinet, 2024c)

5.3.6 AI Security

Uhka-analytiikka on jatkuva tutkinta, joka monitoroi hyökkäyksiä verkon kohteita vastaan. Samalla se arvioi WAF- ja turvakonfiguraatiota. Näiden perusteella se pystyy tarjoamaan ehdotuksia asetusten optimoimiseen. (Fortinet, 2024c)

5.3.7 Advanced Security Services

FortiADC tarjoaa suojan monille hyökkäysvektoreille. Tietoverkkoa suojaavat IPS, virustorjunta ja IP reputaatio. Sovelluksia suojaavat DLP, testiympäristö, credential stuffing ja WAF-allekirjoitukset. (Fortinet, 2024c)

5.3.8 SSL Offloading and Visibility

FortiADC tekee suojausta ja sen purkamista käyttäen ASIC SSL:ää. Palveluun kuuluu myös SSL offloadaus ja SSL tarkastelu ja näkyvyys, joka mahdollistaa tietoliikenteen seuraamisen. (Fortinet, 2024c)

5.3.9 Scripts and DevOps Tools

Skripteillä voidaan luoda tapahtumakohtaisia sääntöjä. FortiADC:hen sisältyy kehittämistyökaluja, joihin kuuluu RestfulAPI, Declarative API, Terraform, cloud-init ja ansible. (Fortinet, 2024c)

5.3.10 Automation and Connectors

Fabric Connectors tuo avoimen API-pohjaisen integraation ja hallinnan useiden ohjelmistomääriteltyjen verkkojen (SDN), pilven, hallinnan ja kumppaniteknologioiden alustojen kanssa. Fortinet Fabric Connectors mahdollistaa avaimet käteen -periaatteella toimivan avoimen ja syvän integraation kolmansien osapuolten palveluihin, kuten K8s, AWS, OCI ja SAP. (Fortinet, 2024c)

5.3.11 Analytics and Visibility

FortiViewillä pystyy saamaan reaaliaikaisen ja historiallisen datan yhdelle näkymälle. Palvelu mahdollistaa loogisen topologian todellisista palvelimista, käyttäjien ja sovellusten tiedon analysoinnin, turvallisuusuhat ja hyökkäyskartat. FortiADC mahdollistaa useiden FortiADC-laitteiden hallinnan etänä ADC Managerin avulla. Se toimii myös Splunkin, FortiAnalyzerin ja FortiSIEMin kanssa, mikä parantaa näkyvyyttä ja tapahtumien yhteyksien ymmärtämistä. Se myös automatisoi vastauksia ongelmiin ja auttaa vastaamaan niihin. (Fortinet, 2024c)

5.4 FortiGSLB

FortiGSLB Cloud käyttää nimipalvelujärjestelmää, jonka päätavoitteena on varmistaa liiketoiminnan jatkuvuus pitämällä sovellukset toiminnassa ja käytettävissä mahdollisten ongelmien sattuessa. Palvelu hyödyntää räätälöityjä kuntotarkistuksia seuratakseen sovellusten päätepisteitä tai pilvipalveluja. Tämän Global Server Load Balancing (GSLB) ratkaisun pyrkimyksenä on tehostaa yrityssovellusten saatavuutta, käyttäjäkokemusta sekä sovellusturvallisuutta. Palvelu tarjoaa kuormantasauksen useiden tietokeskusten ja pilvisovellusten välillä GSLB Cloud -käytäntöjen, sivuston

valinnan sovelluksen tai palvelimen saatavuuden ja asiakkaan maantieteellisen sijainnin perusteella. (Fortinet, 2024d)

Seuraavissa kappaleissa käsitellään FortiGSLB:n ominaisuuksia ja kytköksiä muihin Fortinetin tuotteisiin.

5.4.1 Intelligent Traffic Management

FortiGSLB optimoi asiakaspyynnöt tietylle verkkotunnukselle (domain) jakamalla dynaamisesti työkuorman virtuaalipalvelimien, tietokeskusten ja sijaintien kesken. Liikennettä voidaan ohjata verkkoresursseihin maantieteellisen sijainnin, palvelimen suorituskyvyn, kuorman, mitatun asiakas- ja verkkosuorituskyvyn, painotettujen jakelujen ja johdonmukaisen reitityksen perusteella. (Fortinet, 2024d)

5.4.2 Advanced Health Check

FortiGSLB Cloud seuraa sovellusten päätepisteitä tai pilvipalveluja käyttäen määriteltävissä olevia kuntotarkastuksia. Kaikkia resursseja monitoroidaan taukoamatta reaaliaikaisesti. Kuntotarkastukset voidaan räätälöidä valitsemalla haluttu protokolla ja parametrit. Vaihtoehdot ulottuvat yksinkertaisesta ping-testistä aina sovellustason 7 sisällön tarkistukseen asti. (Fortinet, 2024d)

5.4.3 DNS Services

FortiGSLB tuo täydet DNS-palvelut. Niihin kuuluu DNSSEC ja standardi DNS-vyöhyke, sekä täysi tuki seuraaville resurssityypeille: A/AAAA-tietueet, CNAME, NS, MX, TXT, SRV ja PTR. (Fortinet, 2024d)

5.4.4 Synthetic Testing

Synteettinen testaus tarkistaa sovellusten saatavuuden lähettämällä kyselyjä sovelluksiin FortiGSLB-pilvestä. Sitä voidaan käyttää sovellusten verkkopalvelujen tai sovelluspäätepisteiden valvontaan eri verkkojen kerroksissa ja näiden testien tulokset voivat tarjota arvokasta tietoa sovellusten toiminta- ja katkoajoista, saatavuudesta ja alueellisista suorituskykyongelmista. (Fortinet, 2024d)

5.4.5 Fabric Connectors

FortiGSLB on osana Fortinetin turvakehikkoa. Yhteyksiä on FortiADC:lle, SD-WAN:ille ja FortiGate:lle**.** FortiGSLB:n konfiguraatiossa VIP (Virtual IP) ja SD-WAN-konfiguraatio synkronoidaan automaattisesti FortiGate- tai FortiADC-laitteilta RestAPIen kautta. (Fortinet, 2024d)

6 Verkkouhkien mitigointi

6.1 WAF

Verkkosovelluspalomuuri (WAF) auttaa suojaamaan verkkosovelluksia suodattamalla ja valvomalla HTTP-liikennettä verkkosovelluksen ja Internetin välillä. Se suojaa tyypillisesti verkkosovelluksia hyökkäyksiltä kuten cross-site forgery, cross-site-scripting (XSS), file inclusion ja SQL-injektio. (Cloudflare, 2024a)

WAF toimii OSI-mallin seitsemännellä tasolla. WAF:in päämääränä ei ole tarjota suojaa kaikenlaisia hyökkäyksiä vastaan. WAF on tyypillisesti osa laajempaa työkaluvalikoimaa, joka yhdessä muodostaa kattavan suojan useita hyökkäysvektoreita vastaan keskittyen erityisesti hyökkäysten lieventämiseen. Asentamalla verkkosovelluspalomuurin verkkosovelluksen etulinjaan luodaan suojaava kerros verkkosovelluksen ja internetin välille. Toisin kuin välityspalvelin, joka suojaa asiakaslaitteen henkilöllisyyttä käyttäen välikättä, WAF toimii käänteisenä välityspalvelimena. Se estää palvelinta tulemasta suoraan alttiiksi internetille ohjaamalla asiakasliikenteen ensin WAF:in läpi ennen kuin se saavuttaa palvelimen. (Cloudflare, 2024a)

WAF operoi tiettyjen säännöstöjen perusteella. Nämä säännöstöt pyrkivät puolustamaan uhilta suodattamalla haitallista liikennettä. WAF:in arvo perustuu osaltaan siihen, kuinka nopeasti ja helposti sen säännöstöjä voidaan muuttaa. Helppo ja nopea muokattavuus mahdollistaa nopeamman reagoinnin eri hyökkäysvektoreihin. (Cloudflare, 2024a)

6.2 FortiWAF

FortiWebin verkkosovelluspalomuuri (WAF) suojaa liiketoiminnan kannalta kriittisiä verkkosovelluksia hyökkäyksiltä, jotka kohdistuvat tunnettuihin ja tuntemattomiin haavoittuvuuksiin. FortiWeb suojaa verkkosovelluksia ja ohjelmointirajapintoja (API) OWASP Top-10 -uhilta, DDOS-hyökkäyksiltä ja haitallisten bottien hyökkäyksiltä. Edistyneet koneoppimista hyödyntävät ominaisuudet parantavat turvallisuutta ja vähentävät hallinnollista taakkaa. Ominaisuuksiin kuuluvat poikkeavuuksien havaitseminen, API:en havaitseminen ja suojaus, bottien torjunta sekä edistyneet uhka-analytiikat kriittisimpien uhkien tunnistamiseksi kaikista suojatuista sovelluksista. (Fortinet, 2024f)

Web application security estää tunnetut- ja nollapäiväuhat sovelluksissa estämättä sallittuja käyttäjiä. Käyttämällä koneoppimista kunkin sovelluksen mallintamiseen, FortiWeb tunnistaa pahantahtoiset poikkeavuudet estääkseen uhkia. (Fortinet, 2024f)

Bot defense pysäyttää haitalliset botit estämättä samalla hyödyllisiä botteja. Edistyneitä teknologioita, joita tämä työkalu hyödyntää ovat mm. botin harhautus, biometrinen tunnistus ja koneoppiminen. Nämä mahdollistavat bottiliikenteen tarkan tunnistamisen ja hallinnan. FortiWebin botin torjuntatoiminnallisuus tarjoaa tarvittavan näkyvyyden ja hallinnan ilman, että käyttäjiä hidastetaan turhilla captcha-tarkistuksilla tai muilla haasteilla. (Fortinet, 2024f)

API discovery ja protection suojaa ohjelmointirajapintoja, jotka mahdollistavat yritysten välisen viestinnän ja tukevat mobiilisovelluksia. FortiWebin API Discovery and Protection käyttää koneoppimisalgoritmeja automaattisesti löytääkseen API:t arvioimalla jatkuvasti sovellusliikennettä. (Fortinet, 2024f)

7 Fortinet-varmenneautomaatio

7.1 ACME

ACME (Automated Certificate Management Environment) on julkisen avaimen infrastruktuuri, joka käyttää X.509 (PKIX) varmenteita. Sitä käytetään moniin tarkoituksiin, joista merkittävin on verkkotunnusten (domain) todentaminen. Varmennusviranomaiset (CA) käyttäen webpki -kirjastoja luotetaan tarkistamaan, että varmenteen hakija edustaa varmenteessa mainittuja verkkotunnuksia. Tämä tarkistus suoritetaan käyttämällä ad hoc -mekanismeja. ((IETF), 2019)

7.2 Määritykset

FortiGate voidaan määrittää käyttämään varmenteita, joita hallinnoi Let's Encrypt ja muita varmenteiden hallintapalveluita, jotka käyttävät ACME-protokollaa. Palvelinvarmenteita voidaan käyttää turvalliseen administraattorin kirjautumiseen FortiGateen. FortiGatella on oltava julkinen IP-osoite ja DNS:sä oleva isäntänimi (FQDN), joka selvittää kyseiseen julkiseen IP-osoitteeseen. (Fortinet, 2024b)

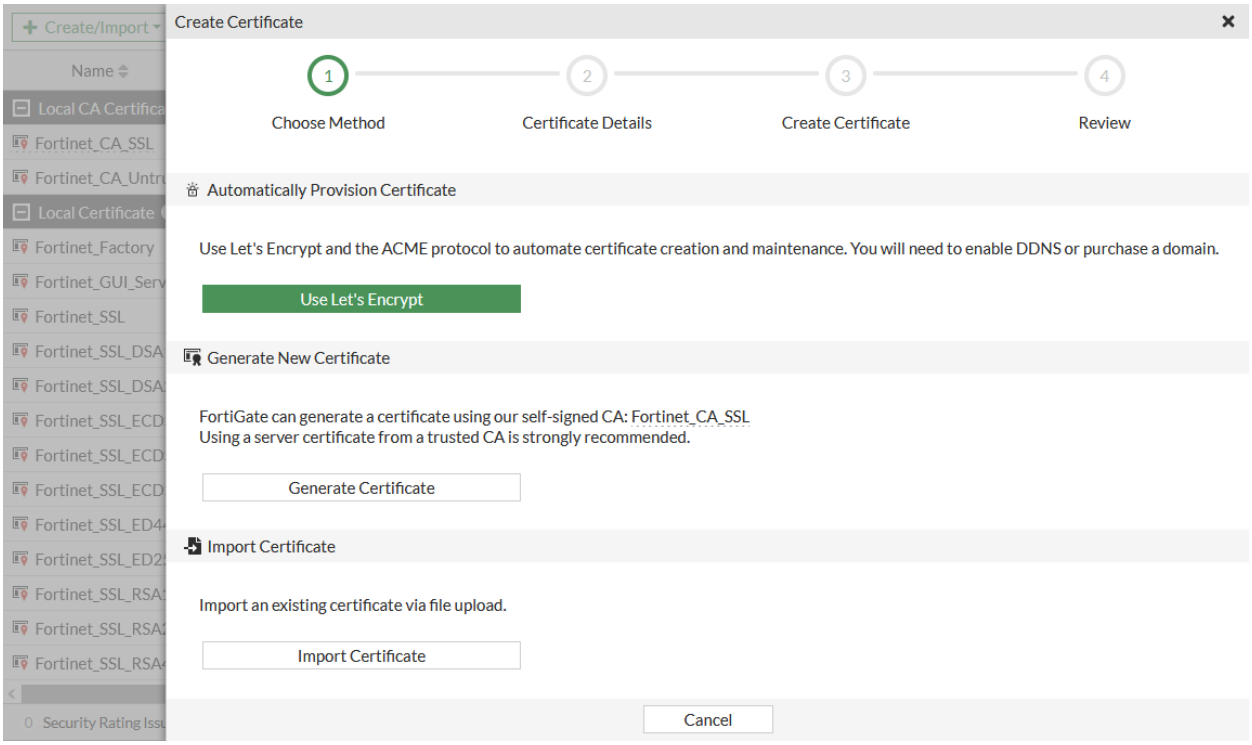
Määritetyn ACME-liittymän on oltava julkisesti saatavilla, jotta FortiGate voi kuunnella ACME-päivityspyyntöjä. Sillä ei saa olla VIP:iä (Virtual IP Address) tai portin uudelleenohjauksia portissa 80 (HTTP) tai 443 (HTTPS). Subject Alternative Name (SAN) kenttä täyttyy automaattisesti FortiGaten DNS isäntänimellä. Sitä ei pysty muokkaamaan. Wildcard-varmenteita ei voi käyttää ja monia SAN:eja ei voi lisätä. (Fortinet, 2024b)

7.3 Ohjeistus

Tässä ohjeessa käydään läpi esimerkki, miten automatisoidaan sertifikaatin luonti ACME:a käyttäen. Esimerkissä käytetään Let's Encryptin varmentamia sertifikaatteja. Ohjeistus on opinnäytetyötä kirjoittaessa uusin versio 7.4.3. Ohjeistus löytyy Fortinetin omasta dokumentaatiosta. (Fortinet, 2024b)

Kuvassa 1 mennään system-välilehdeltä create certificate kohtaan ja sieltä painetaan certificate.

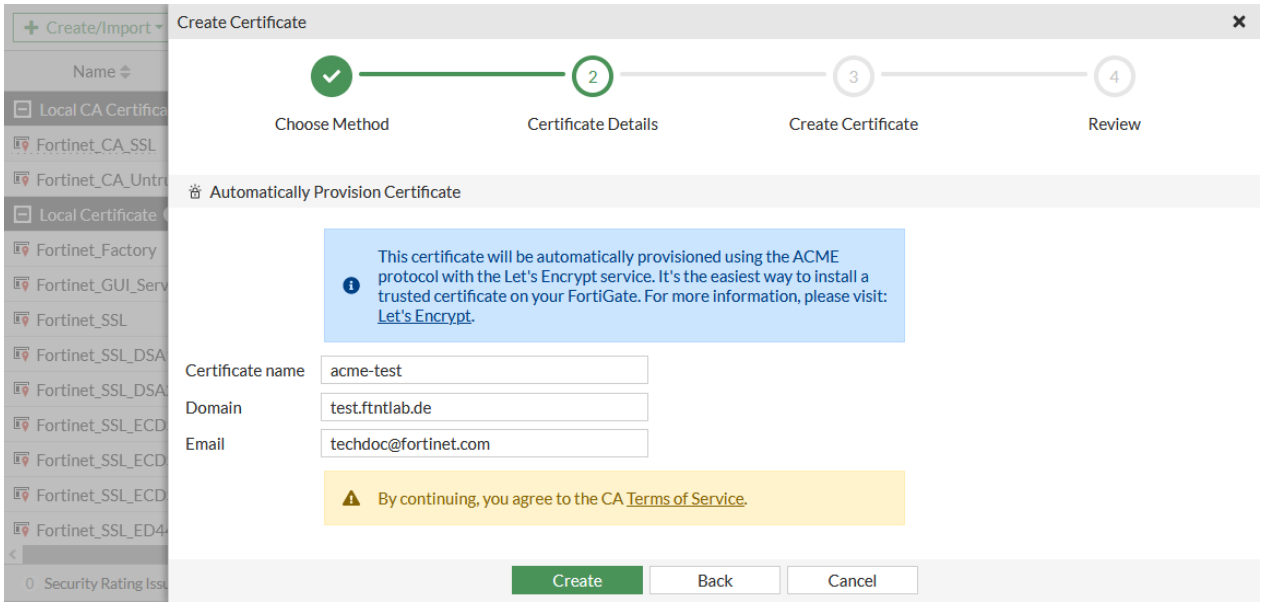
1. Klikkaa *system* > *Certificates* > *Create/import* > *Certificate.*



Kuva 3. Automaattinen sertifikaatin provisiointi ohjekuva 1 (Fortinet, 2024b)

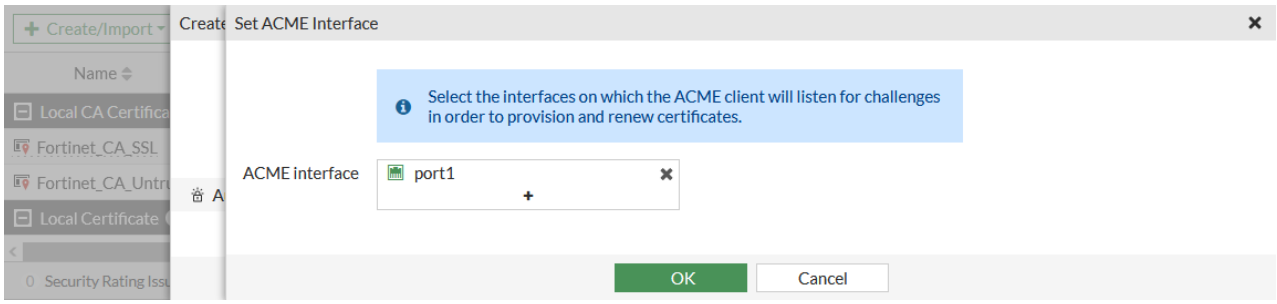
2. Klikkaa *Use Let's Encrypt.*
3. Aseta haluamasi varmenteen nimi kenttään *Certificate name.*
4. Aseta *Domain* FortiGaten julkiseen FQDN:ään.
5. Aseta *Email* kenttään haluamasi sähköpostiosoite.

Kun kaikki edeltävä on tehty kuvan 2 mukaisesti, asetetaan ACME-interface, joka näkyy kuvassa 3



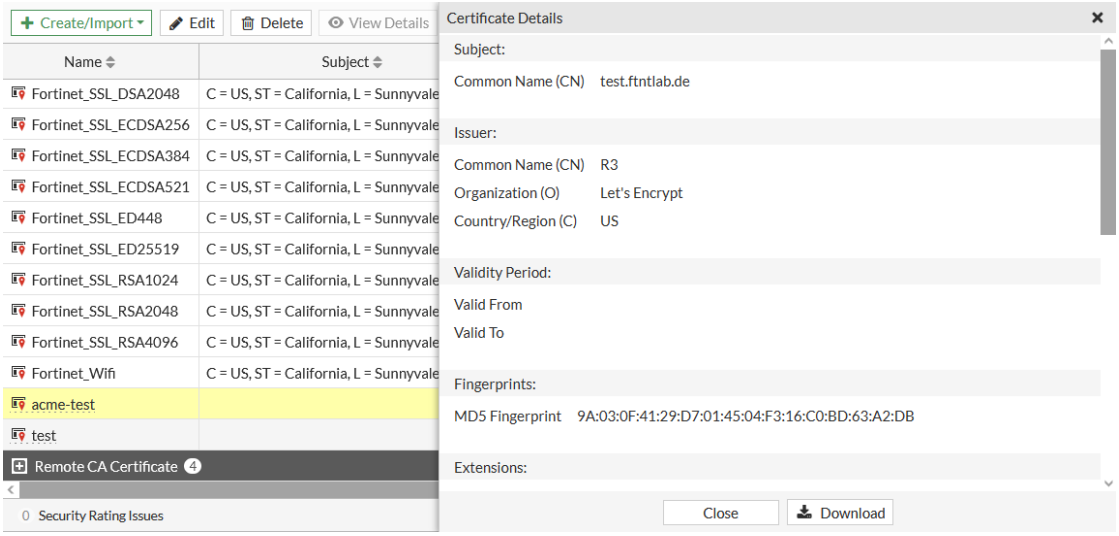
Kuva 4. Automaattinen sertifikaatin provisiointi ohjekuva 2 (Fortinet, 2024b)

6. Klikkaa *Create*.
7. Aseta *ACME interface*.



Kuva 5. Automaattinen sertifikaatin provisiointi ohjekuva 3 (Fortinet, 2024b)

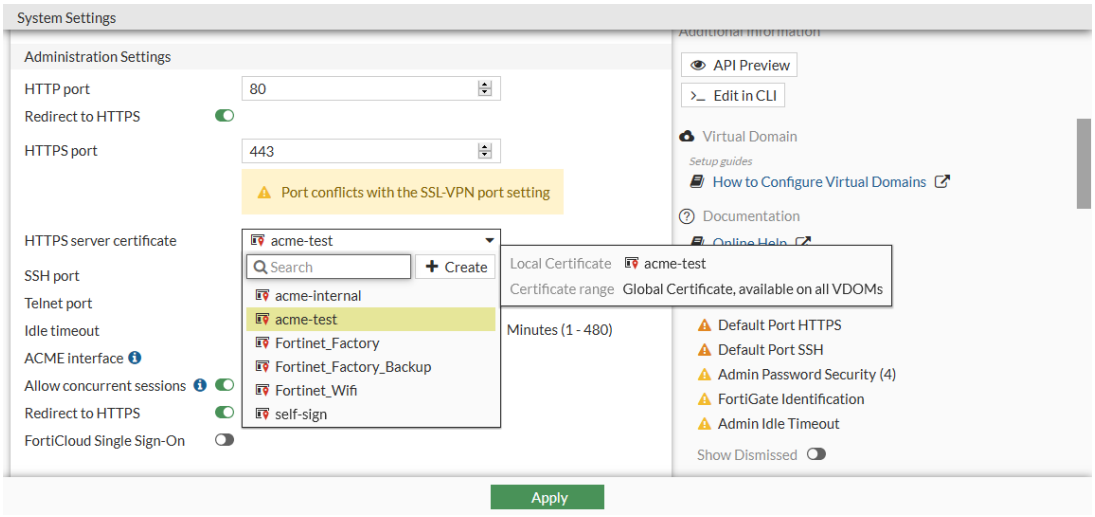
8. Klikkaa *OK*
9. Klikkaa *View Details* varmistuaksesi siitä, että FortiGaten FQDN on *Common Name (CN).*



Kuva 6. Automaattinen sertifikaatin provisiointi ohjekuva 4 (Fortinet, 2024b)

Seuraavassa vaiheessa vaihdetaan oletuksena oleva FortiGaten hallintapalvelimen varmenne uuteen julkiseen Let's Encryptin varmentamaan sertifikaattiin. Kuvassa 7 käydään seuraavat numeroidut vaiheet läpi.

1. Klikkaa *System* > *Settings.*
2. Laita *HTTPS server certificate* kenttään uusi varmenne.
3. Paina *Apply*
4. Kirjaudu FortiGateen administraattorina mistä tahansa selaimesta. Tästä ei pitäisi tulla varoituksia luottamattomista varmenteista ja varmenteen polun tulisi olla kelvollinen.



Kuva 7. Automaattinen sertifikaatin provisiointi ohjekuva 5 (Fortinet, 2024b)

8 Yhteenveto

Opinnäytetyön tavoitteena oli katsoa tarkemmin Fortinetin tuotteita: GSLB:tä, ADC:tä, WAF:ää ja palvelinvarmenteiden automaattista provisointia. Tarkoitus oli oppia lisää kyseisistä tuotteista ja niiden ominaisuuksista.

Työssä käytiin läpi yleisellä tasolla myös palomuureja, palvelinvarmenteita ja yleisiä uhkia, joille sovellukset altistuvat. Tämän tarkoituksena oli luoda pohjaa työssä käsitellyille Fortinetin tuotteille.

Työ sai nidottua yhteen halutut tuotteet ja niiden markkinoidut ominaisuudet. Työssä on suurimmaksi osaksi hyödynnetty Fortinetin omaa dokumentaatiota ja markkinointisisältöä.

Työssä ei ole hyödynnetty käytännön testausta, jolla voitaisiin todeta tuotteista yksilöllisiä tuloksia. Työ nojautuu täysin teoreettiseen tietoon tuotteista. Se antaa hyvän pohjan ymmärtää tuotteita ja auttaa erottamaan hyödyllisiä ja mahdollisesti ei tarpeellisia ominaisuuksia. Se ei kuitenkaan kerro kuinka kyseiset tuotteet toimivat toimeksiantajan ympäristöissä.

Lähteet

(IETF), I. E. 2019. *Automatic Certificate Management Environment (ACME)*. Haettu 15. 3 2024 osoitteesta Datatracker: https://datatracker.ietf.org/doc/html/rfc8555

Cloudflare. 2024a. *What is a WAF? | Web Application Firewall explained*. Haettu 7. 3 2024 osoitteesta Cloudflare: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

Cloudflare. 2024b. *What is global server load balancing (GSLB)?* Haettu 29. 2 2024 osoitteesta Cloudflare: https://www.cloudflare.com/learning/cdn/glossary/global-server-load-balancing-gslb/

Earls, E. M. 2024. *application delivery controller (ADC)*. Haettu 29. 2 2024 osoitteesta Techtarget: https://www.techtarget.com/searchnetworking/definition/Application-delivery-controller

Fortinet. 2024a. *7 Common Web Security Threats for an Enterprise*. Haettu 25. 2 2024 osoitteesta Fortinet: https://www.fortinet.com/resources/cyberglossary/web-security-threats

Fortinet. 2024b. *Automatically provision a certificate*. Haettu 15. 3 2024 osoitteesta Fortinet: https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/822087

Fortinet. 2024c. *FortiADC™ Advanced Application Delivery Controller*. Haettu 4. 3 2024 osoitteesta Fortinet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC.pdf

Fortinet. 2024d. *FortiGSLB™ Cloud*. Haettu 4. 3 2024 osoitteesta fortinet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigslb.pdf

Fortinet. 2024e. *Global load balancing basics*. Haettu 24. 3 2024 osoitteesta Fortinet: https://help.fortinet.com/fadc/4-5-1/olh/Content/FortiADC/handbook/Global_load_balancing_basics.htm

Fortinet. 2024f. *Web Application Firewall*. Haettu 7. 3 2024 osoitteesta Fortinet: https://www.fortinet.com/products/web-application-firewall/fortiweb

Kaspersky. 2024. *SSL-varmenne – määritelmä ja selitys*. Haettu 22. 2 2024 osoitteesta Kaspersky: https://www.kaspersky.fi/resource-center/definitions/what-is-a-ssl-certificate

Yasar, K. 2024. *firewall*. Haettu 22. 2 2024 osoitteesta Techtarget: https://www.techtarget.com/searchsecurity/definition/firewall