Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

NIKO ORAMAA

Next-generation palomuurit ja operatiiviset teknologiat

TIETOJENKÄSITTELYN TUTKINTO-OHJELMA
2025

TIIVISTELMÄ

Oramaa, Niko: Next-generation palomuurit ja operatiiviset teknologiat
Opinnäytetyö, AMK
Tietojenkäsittely
Huhtikuu 2025
Sivumäärä: 57

Tämän opinnäytetyön tarkoituksena oli tutkia seuraavan sukupolven palomuureja, operatiivisia teknologioita sekä operatiivisten teknologioiden tietoturvan parantamista. Työssä käydään läpi vanhempien palomuurityyppien teknologiaa ja toimintatapoja, seuraavan sukupolven palomuurien ominaisuuksia, operatiivisten teknologioiden toimintatapoja ja kuinka niiden tietoturvaa on mahdollista parantaa.

Työn alussa perehdytään vanhempien palomuurityyppien toimintaan ja toiminnallisuuksiin. Seuraavassa kappaleessa perehdytään seuraavan sukupolven palomuureihin ja niiden toiminnallisuuksiin sekä kuinka seuraavan sukupolven palomuuri on ominaisuuksineen parempi vaihtoehto vanhemmille palomuurityypeille. Seuraavassa kappaleessa tutustutaan vaihtoehtoiseen seuraavan sukupolven palomuurin toteuttamiseen konttiteknologioilla. Seuraavassa kappaleessa perehdytään operatiivisiin teknologioihin, niiden tietoturvapolitiikkaan, riskienhallintaan, tietoturvastandardeihin sekä kuinka seuraavan sukupolven palomuurit ovat hyödyksi operatiivisten teknologioiden aloilla.

Loppukappaleissa oma näkemykseni tietoturvapolitiikasta, riskienhallinnasta ja kuinka seuraavan sukupolven palomuurit ovat hyödyksi operatiivisten teknologioiden aloilla sekä yhteenveto työn sisällöstä.

Avainsanat: palomuuri, seuraavan sukupolven palomuuri, ng-palomuuri, operatiivinen teknologia, tietoturva

ABSTRACT

Oramaa, Niko: Next-generation firewalls and operational technologies
Bachelor's thesis
Business information systems
April 2025
Number of pages: 57

The purpose of this thesis was to study next-generation firewalls, operational technologies and improving the information security of mentioned operational technologies. The work reviews the technology and operating methods of older firewall types, the features of next-generation firewalls, the operating methods of operational technologies, and how their information security can be improved.

At the beginning of the work, we will familiarize ourselves with the operation and functionality of older firewall types. The next section will examine next-generation firewalls and their functionalities, and how the next-generation firewall is a better alternative to older firewall types with its features. The next section will introduce an alternative implementation of a next-generation firewall using container technologies. The next section will examine operational technologies, their security policies, risk management, security standards, and how next-generation firewalls are useful in the areas of operational technologies.

The final chapters contain my own views on information security policy, risk management, and how next-generation firewalls are useful in the areas of operational technologies, as well as a summary of the work.

Keywords: firewall, next-generation firewall, ng-firewall, ngfw, operational technology, information security

SISÄLLYS

SYMBOLI- JA LYHENNELUETTELO

AVC – Application visibility and control – Käyttäjän- ja sisällöntunnistuksen hallinta
Bitti – Binary digit – Tietovuon pienin käsiteltävä osa – Kahdeksan bittiä on yksi tavu
Bottiverkko – Joukko saastuneita laitteita, joissa huomaamaton etäohjattava haittaohjelma
CI/CD – Continuous integration and continuous deployment – Jatkuva integraatio ja jatkuva käyttöönotto
DLP – Data loss prevention – Tietojen menetyksen estäminen
DMZ – Demilitarized zone – Puskurivyöhyke
DNP3 – Distributed Network Protocol3 – OT-ympäristöissä käytetty viestintäprotokolla
DPI – Deep packet inspection – Syvä pakettitarkistus
FTP – File transfer protocol – Tiedonsiirtomenetelmä
FW – Firewall – Palomuuri
Gbps – Gigabits per second – Gigabittiä sekunnissa (katso bitti)
GBps – Gigabytes per second – Gigatavua sekunnissa (katso tavu)
GDPR – General data protection regulation – Euroopan Unionin yleinen tietosuoja-asetus
HIPS – Host-based intrusion prevention system – Isäntäjärjestelmän tunkeutumisen havaitsemisjärjestelmä
HMI – Human-machine interface – Ihmisen ja koneen välinen rajapinta
HTTP – Hypertext transfer protocol – Hypertekstin siirtoprotokolla
IACS – Industrial automation and control systems – Teollisuuden automaation ja hallinnan järjestelmät
IBM – International Business Machines Corporation – Teknologiayritys
ICS – Industrial control system – Teollisuuden ohjaus/automaatiojärjestelmä
IDS – Intrusion detection system – Tunkeilijan havaitsemisjärjestelmä
IEC – International Electrotechnical Commission – Kansainvälinen sähköalan standardointijärjestö
Industry 4.0 – Teollisuus 4.0 – Neljäs teollinen vallankumous – IoT, IIoT, pilvilaskenta ja koneoppiminen

IoT – Internet of things – Esineiden internet

IIoT – Industrial internet of things – Teollinen esineiden internet

IPS – Intrusion prevention system – Murron estämisjärjestelmä

IPSec – IP security architecture – Tietoliikenneprotokollaryhmä

ISA – International Society of Automation – Kansainvälinen tekninen yhdistys

ISO – International Organization for Standardization – Kansainvälinen standardisoimisjärjestö

Kernel – (Käyttöjärjestelmän) ydin – Toimii suojatussa ytimen muistiavaruudessa

LDAP – Lightweight Directory Access Protocol – Verkkoprotokolla, jota hakemistopalvelut käyttävät

Modbus – Vanhimpia OT-ympäristöissä käytetyistä viestintäprotokollista

MTU – Maximum transmission unit – Maksimi tiedonsiirtoyksikkö

NAT – Network address translation – Osoitteenmuunnos

NGFW – Next-generation firewall – Seuraavan sukupolven palomuuri

NGIPS – Next-generation intrusion prevention system – Seuraavan sukupolven murron estämisjärjestelmä

NIS2 – Network and Information Security Directive 2 – Euroopan unionin asettama verkko- ja tietoturvadirektiivi

NIST – National Institute of Standards and Technology – Yhdysvaltain standardisointi- ja teknologiainstituutti

OS – Operating system - Käyttöjärjestelmä

OSI – Open Systems Interconnection Reference Model – Tiedonsiirtoprotokollien yhdistelmä

OT – Operational technology – Operatiiviset teknologiat

P2P – Peer to peer – Vertaisverkkoyhteys

Profibus – Process Field Bus – Siemensin kehittämä kenttäväyläprotokolla

Profinet – Process Field Net – Profibusin seuraaja, modernisoitu ethernetiä käyttävä kenttäväyläprotokolla

PLC – Programmable logic controller – Ohjelmoitava logiikkaohjain

RTU – Remote terminal unit - Etäpääteyksikkö

SCADA – Supervisory control and data acquisition – Käytönohjausjärjestelmä

SMTP – Simple mail transfer protocol – Viestien välityksen protokolla

SSH – Secure shell – Salatun tietoliikenteen protokolla

SSL – Secure socket layer – Salausprotokolla

Stuxnet – Windows-pohjainen mato – SCADA-hyökkäyksiin erikoistunut hienostunut mato

Tavu – Byte – Tallennuskapasiteetin mittayksikkö – Yksi tavu on kahdeksan bittiä

TCP – Transmission control protocol – Tietoliikenneprotokolla

TLS – Transport layer security – Kuljetustason turvallisuus

UTM – Unified threat management – Yhdistetty uhkien hallinta

VPN – Virtual private network – Virtuaalinen erillisverkko

WAN – Wide area network – Laajaverkko

1 JOHDANTO

Yritykset tavoittelevat oman tietoturvansa näkökulmasta läpinäkyvyyttä ja kontrollia sekä etulyöntiasemaa tietoverkkojensa ja datan suojauksessa. Tavoitellessaan hienostunutta ja virtaviivaistettua tietoturvaratkaisua, yritykset kääntyvät moniin erillisiin laitteisiin, joilla on vain yksi toiminto sekä ohjelmistoihin, jotka eivät pysty vastaamaan nykyaikaisiin tietoturvahaasteisiin.

Näistä monista erillisistä ratkaisuista rakentuu suuri ja monimutkainen epäkäytännöllinen ratkaisu. Monimutkainen ja epäkäytännöllinen johtaa kasvaviin kuluihin ja ongelmiin. Nämä eivät kuulu sujuvasti toimivaan organisaatioon (Miller, 2011, s.7).

Haitallisten toimijoiden toiminta- ja torjuntatavat kilpailevat toinen toistaan vastaan. Perinteiset tietoturvaratkaisut kuten palomuurit, tunkeilijan havaitsemisjärjestelmät (IDS), murron estämisjärjestelmät (IPS), virustorjunnat, yhdistetyt uhkien hallintajärjestelmät (UTM) sekä muut voivat olla toimivia ratkaisuja, on myös kehitetty nämä yhdistävä ratkaisu, next-generation palomuuri. Next-generation palomuuri (NGFW), riippuen palveluntarjoajasta tuo tietoturvaratkaisut yhtenäiseen, integroituun palveluun.

NGFW voi konseptina kuulostaa vaikealta ja ylimääräiseltä sekä turhalta työltä. Jokaisen erillisen tietoturvaratkaisun hallinnointi saattaa kuitenkin osoittautua työläämmäksi ja kalliimmaksi pitkässä juoksussa, verrattuna yhtenäistettyyn NGFW-ratkaisuun. Kaikkien tietoturvaratkaisujen tuonti yhden hallinnointijärjestelmän alaisuuteen tehostaa työn sujuvuutta ja tehokkuutta. Työn sujuvuuden ja tehokkuuden nostaminen vastapainoisesti laskee kulutettuja työtunteja ja kuluja.

2 PALOMUURIT

Termi palomuuri on monille tuttu, mutta mitä sillä tarkoitetaan? Palomuuri on nykyaikaisissa Windows -laitteissa esiasennettu ja peruskonfiguroitu ohjelmisto, joka estää sopimattomien verkkoyhteyksien pääsyn laitteeseen (F-Secure, 2022). Palomuurin tehtävänä on tutkia sisään tulevat ja ulos lähtevät paketit sekä päättää hyväksytäänkö vai hylätäänkö paketti (Liu, 2010, luku Johdanto, s.vii).

Yksinkertaistettuna perinteinen palomuuri ohjaa sekä luotetun että luottamattoman verkon liikennettä. Suurin osa perinteisistä palomuureista toimii portti- tai pakettien suodatusperusteisesti tai jonkinlaisella variaatiolla (kuten tilaton pakettisuodatus) tämäntyyppisestä palomuurista.

Nämä perinteiset palomuurit ovat yleisimpiä niiden helppokäyttöisyyden ja kustannustehokkuuden vuoksi sekä ne ovat olleet vallitseva ratkaisu jo vuosikymmeniä (Miller, 2011, s.12).

2.1 Palomuurien säännöt

Palomuurien toiminnan perustana toimivat hierarkkiset säännöt, jotka ohjaavat palomuurin toimintaa ja liikennettä. Palomuurikäytäntöjen rakentaminen oikein on vaativaa ja vaikeaa työtä, varsinkin kun sääntöjen määrä kasvaa, sääntöjen priorisointijärjestys on monimutkainen ja säännöissä on päällekkäisyyksiä. Hierarkian priorisointijärjestykseen tulee kiinnittää huomiota päällekkäisyyksien ja vakavien priorisointivirheiden vuoksi. Jos yhdenkin säännön priorisaatio on väärä, voi vaikutus ulottua moniin, ellei jopa kaikkiin muihin sääntöihin ja palomuuri saattaa päästää sisään haitallista liikennettä tai estää legitiimin liikenteen. Riippuen organisaation koosta, voi palomuurissa olla satoja, jopa tuhansia päällekkäisiä sääntöjä (Liu, Gouda, 2008, s.1). Gartnerin mukaan vuonna 2025 noin 99 % palomuurimurroista tulee johtumaan huonosti tai väärin konfiguroiduista palomuurisäännöistä (Palo Alto Networks, n.d.-a.; Panetta, 2019).

2.1.1 Tilattomat palomuurit

Tilattomat palomuurit ovat ensimmäisen sukupolven palomuureja, joiden toimintaperiaate perustuu listaan, johon on esimääritelty hyväksymis- ja kieltosääntöjä. Tilattomat palomuurit toimivat OSI-mallin kerroksilla 3 ja 4, eli verkko- ja kuljetuskerroksilla.

Palomuuri suodattaa verkkoliikennettä pakettien otsikoiden perusteella, huomioimatta pakettien tilaa tai asiayhteyttä. Tilattoman palomuurin säännöt ovat hierarkiajärjestyksessä ja sääntölista käydään läpi ylhäältä alas. Sisään tulevan IP-paketin otsikosta tarkistetaan lähtö- ja kohde-IP-osoitteet, lähtö- ja kohdeportit sekä TCP-paketti (Nurmi, 2021, s.6; Palo Alto Networks, n.d.-b).

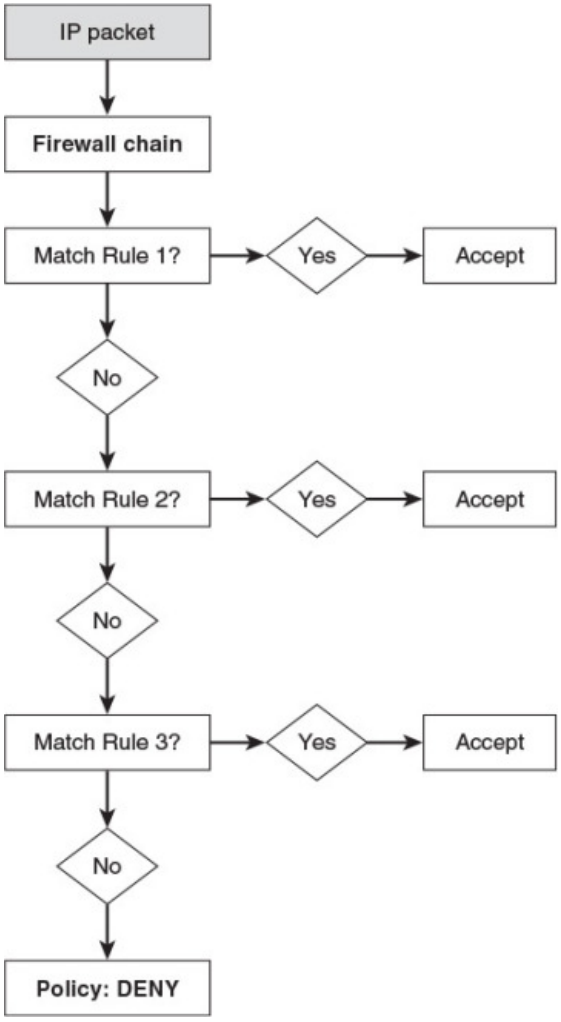
Tilattomalla palomuurilla on muutama etu verrattuna muihin palomuureihin. Tilattoman palomuurin suodatustekniikalla tehty paketin tarkistus käyttää minimaalisen määrän resursseja ja näin ollen tarjoaa todella matalan viiveen verkkoliikenteeseen (Checkpoint, 2023). Paketin tarkistuksen nopeuteen ja keveyteen vaikuttaa sääntöjen hierarkiajärjestyksessä kuvan 1 mukaan tehty tarkistus. Mitä ylempää listasta sääntö hyväksytään, sitä vahvempi se on, yliajaen alhaisemmat säännöt ja näin ollen alempia sääntöjä ei tarvitse tarkistaa, säästäen resursseja (Nurmi, 2021, s.6).

Tilattoman palomuurin keveyden ja minimaalisen resurssienkulutuksen vuoksi myös kulut ovat matalat ja skaalautuvuus suuri. Jos tilaton ja tilallinen palomuuri on asennettu samanlaisille alustoille, tilattoman palomuurin läpi kulkee nopeammin ja enemmän verkkoliikennettä verrattuna tilalliseen palomuuriin (Checkpoint, 2023).

Tilattoman palomuurin toimintaperiaatteella on myös monia haittapuolia. Koska toimintaperiaatteessa tarkistetaan vain paketin otsikko, ei palomuuri tiedä, jos paketti sisältää haitallisia tietoja ja palomuuri saattaa päästää paketin läpi. Palomuuri ei myöskään suojaa OSI-mallin 7-kerroksella, eli sovelluskerroksella tapahtuvia hyökkäyksiä vastaan. Palomuuri on myös voimaton palvelinestohyökkäyksiä vastaan. Koska palvelinestohyökkäyksissä

yleisesti käytetään bottiverkkoja, näyttää sisään tuleva liikenne legitiimiltä ja palomuuri päästää liikenteen sisälle. Hyökkäyksissä liikennettä on niin paljon, että tilattomatkin palomuurit, ja näin ollen palomuurin takana olevat palvelimet saadaan ruuhkautettua, hidastaen loppukäyttäjien kokemusta tai kaataen palvelimet (Checkpoint, 2023).

Tilattoman palomuurin konfiguroinnissa käytetään pohjana yleisesti joko salli kaikki- tai kiellä kaikki -mallia. Salli kaikki -mallilla täytyy erikseen kieltää kaikki liikenne, jota ei haluta. Kiellä kaikki -mallilla täytyy erikseen sallia kaikki liikenne, joka halutaan, mutta kieltomalli on helpompi pohja tietoturvalle (Nurmi, 2021, s.7; Suehring, 2015, s.29). Pohjana tämänlainen zero trust -käytäntö on turvallinen, kun erikseen täytyy sallia haluttu liikenne. Tosin, kuten edellä mainittu, tilaton palomuuri toimii vain OSI-mallin tasoilla 3 sekä 4, eikä tutki paketteja otsikkoa syvemmältä.



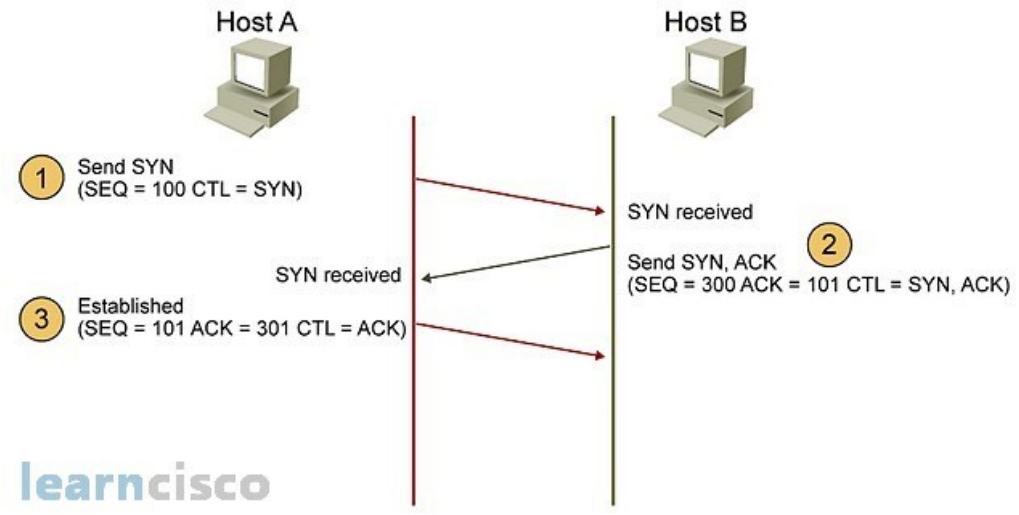
Kuva 1 – Hylkää kaikki -käytännön hierarkia (Suehring, 2015, s.29).

2.1.2 Tilalliset palomuurit

Tilalliset palomuurit ovat uudempia, toisen sukupolven palomuureja. Tilalliset palomuurit toimivat myös OSI-mallin kerroksilla 3 ja 4, eli verkko- ja kuljetuskerroksilla. Kun tilattomat palomuurit tutkivat vain paketin otsikon, tilalliset palomuurit tutkivat myös palomuurin tilaa. Tilalliset palomuurit pystyvät tarkempaan kulunvalvontaan seuraamalla sisäisen ja ulkopuolisen verkon kommunikointitilaa. Laite- ja ohjelmistotoimittajat kovakoodaavat tilan seurannan toiminnot laitteisiinsa sekä ohjelmistoihinsa ja eri toimittajilla on usein eri kovakoodausmenetelmät (Palo Alto Networks, n.d.-c.).

Kun palomuurille tulee liikennettä, tarkistetaan ensin listasta kulunvalvonnan säännöt, nähdäkseen onko halutun tyyppinen liikenne sallittua. Sallitulle liikenteelle luodaan väliaikainen merkintä palomuurin tilatauluun (state table), johon sisältyy erilaisia parametrejä kuten tulo- ja lähtö-IP-osoitteet, TCP-portit, asiaankuuluvat TCP-liput sekä SEQ- ja ACK-tiedot. Lopullisen päätöksen tekevät palvelimelta palaavat paketit, joita verrataan tilatauluun ja hyväksytään vain, jos parametrit vastaavat toisiaan (Palit, 2024).

Yksinkertaistettuna päätös liikenteen ohjauksesta perustuu kolmivaiheiseen kättelyyn. Yhteyden muodostaminen (SYN), tiedonsiirto (SYN-ACK) ja yhteyden katkaisu (ACK) (kuva 2) (Nurmi, 2021, s.8; Palit, 2024; Wilkins, 2013).

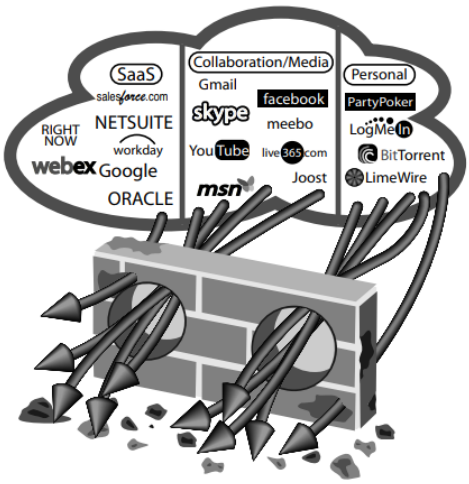


Kuva 2 – TCP kolmivaiheinen kättely (LearnCisco, 2023).

2.2 Porttiperusteiset palomuurit

Vanhat porttitasolla toimivat palomuurit ovat toimimaton ratkaisu nykyverkossa. Vuosia sitten, kun verkossa liikenne oli hyvin suoraviivaista ja yhtenäistä, portin sulkeminen oli sama asia kuin sovelluksen estäminen. Sähköposti (SMTP) käytti porttia 25, tietoliikenneprotokollaa (TCP) käyttävä tiedonsiirtomenetelmä (FTP) käytti porttia 20 ja verkkoselailu (HTTP) porttia 80. Nykyaikana suuri osa verkkoliikenteestä on kryptattua SSL-tekniikkaa portista 443 ja monet sovellukset käyttävät monia eri portteja omilla säännöillään (Miller, 2011, s.33).

Porttitason palomuurit ovat yleisesti asennettuna kriittisiin tietoverkon risteyskohtiin ja näin oletuksena näkevät kaiken liikenteen. Ongelmaksi muodostuu nimenomaan porttitason laajuus. Palomuuri näkee kaiken liikenteen, mutta ei pintaa syvemmältä. Palomuuri päättelee sovellustason palvelun porttinumerosta, joka on paketin otsikossa. Sen sijaan, että palomuurit toimisivat vaatimusten perusteella, ne luottavat yleiseen toimintatapaan, jossa annettu portti vastaa annettua palvelua (esimerkiksi FTP vastaa porttia 20) (Miller, 2011, s.33). Näin ollen, ne eivät osaa tunnistaa saman portin alla toimivia sovelluksia tai niiden liikennettä (kuva 3).



Kuva 3 – Porttitason palomuuri ei osaa suodattaa liikennettä. (Miller, 2011, s.33).

2.2.1 Intrusion detection system

IDS-järjestelmät ovat passiivisia, joko pilvi- tai paikallissovelluksia tai asennettavia laitteita. IDS tarkkailee ja tutkii esiasetettujen käytäntöjen perusteella verkon liikennettä mahdollisten käytäntö- ja liikennepoikkeavuuksien varalta. Epänormaalin liikenteen ja

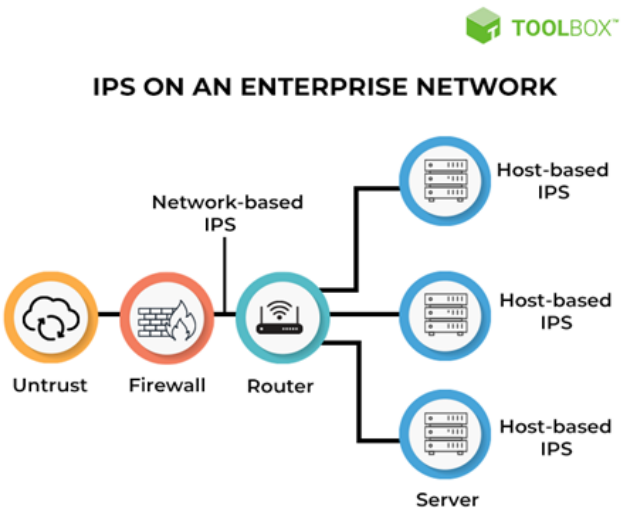
käytäntörikkomusten tiedot kerätään tapahtumalokiin ja osoitetuille käyttäjille lähetetään ilmoitus tapahtumista (IBM, 2023).

Edes jatkuvan kehityksen avulla, IDS-järjestelmät eivät aina ole tarpeeksi tehokkaita vastaamaan jatkuvasti kehittyviä uhkia nykyaikana. Päivittämättömät ja huonosti konfiguroidut IDS-järjestelmät on mahdollista ohittaa monin eri keinoin kuten pakettien pilkkomisella, koordinoidulla pienen kaistaleveyden hyökkäyksellä/skannauksella, osoitteen väärentämisellä tai jatkuvilla, lievästi muokatuilla hyökkäyksillä (IBM, 2023).

Pakettien pilkkominen tarkoittaa, että liian isot MTU:n ylittävät paketit pilkotaan lähetysvaiheessa ja vastaanottava kohde kokoaa pilkotut paketit ennen niiden välittämistä sovelluskerrokseen. Haitallisen toimijan mahdolliset hyökkäystavat koostuvat pilkottujen pakettien päällekkäisyyksistä, päällekirjoituksesta sekä aikakatkaisuista. Tämänlaiset hyökkäykset korvaavat pilkottujen pakettien tiedot muulla tiedolla, haitallisen paketin luomiseksi (Einorytė, 2024).

2.2.2 Intrusion prevention system

Toisin kuin IDS, joka vain hälyttää huomatuista murroista, IPS myös toimii murtoja vastaan. IPS-järjestelmä on tarkoitus asentaa ulko- ja sisäverkon väliin niin, että se näkee kaiken liikenteen ja voi aktiivisesti käydä murtoja vastaan (Miller, 2011, s.36). IPS-järjestelmiä on myös mahdollista asentaa loppukäyttäjän työasemalle tarkkailemaan työaseman liikennettä HIPS-mallisesti (kuva 4) (ESET, 2024).

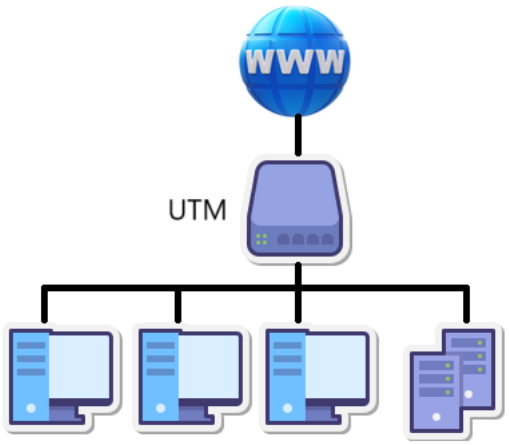


Kuva 4 - IPS yritysverkossa (Ashtari, 2022).

IPS osaa suorittaa verkkoliikenteelle reaaliaikaista syväpakettitarkastusta ja havaitessaan epäilyttäviä tai haitallisia paketteja, ryhtyy järjestelmä toimiin. IPS pystyy katkaisemaan TCP-yhteyden ja estää liikenteen haitallisesta ja haitalliseen IP-osoitteeseen. Välittömien toimenpiteiden jälkeen IPS:n on mahdollista tehdä muutoksia palomuuriin, estäen jatkossa samantyyppiset hyökkäykset (Nurmi, 2021, s.12; ForcePoint, 2019).

2.3 Unified threat management

Unified threat management jakaa samoja piirteitä sekä ominaisuuksia next-generation palomuurien kanssa, mutta nämä ovat kuitenkin eri järjestelmiä. UTM on kiinteä laite, joka asennetaan tietoverkon ulkoreunalle ja tarkoituksena on, että kaikki verkkoliikenne kulkee laitteen läpi (kuva 5).



Kuva 5 - UTM laitteen sijoitus verkossa (kuva: Niko Oramaa).

Modernit haasteet vaativat moderneja ratkaisuja. Millerin (2011, s.39) mukaan UTM-järjestelmät ovat vain yksi perinteisiin tekniikoihin perustuva lähestymistapa moderneihin haasteisiin muiden joukossa. Tietoturvaratkaisuja tarjoavat yritykset etsivät tapoja vähentää kustannuksia, ja kokeiluissaan alkoivat lisäämään IPS- sekä virustorjuntalisäosia tilallisiin palomuureihinsa säästöjen toivossa. Tietoturvajärjestelmät erillisinä ratkaisuinaan ovat pelkän tietoturvatehokkuuden mittarilla aivan yhtä päteviä kuin UTM yksinään. UTM järjestelmän suurin etulyöntiasema syntyy järjestelmien integroinnista yhdeksi laitteeksi ja näin ollen käyttöönoton sekä käytön yksinkertaistumisesta. Joka tapauksessa, lopputulos on sama erillisillä tietoturvaratkaisuilla kuin UTM:llä, puutteet ovat samankaltaisia (Miller, 2011, s.33).

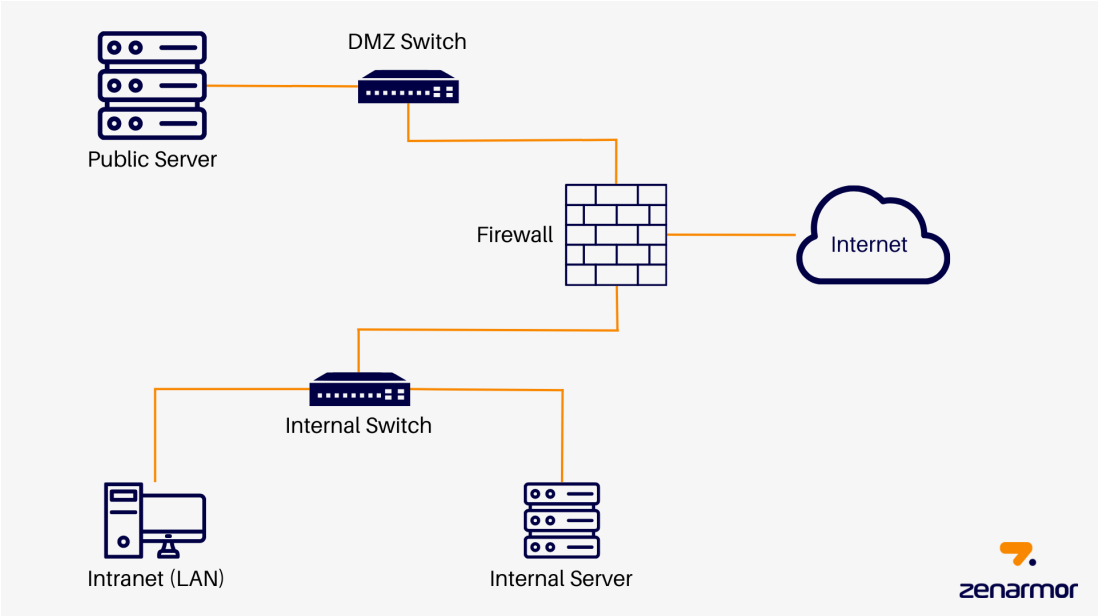
UTM-laitteeseen sisältyy yleensä, valmistajasta riippuen, roskapostin-, virus- ja vakoiluohjelmien torjunta, tietoverkon palomuuri, IDS, IPS ja sisällön suodatus. Jotkin laitteet sisältävät myös etäreititysmahdollisuuden (remote routing), tietojen menetyksen estämisen (DLP), osoitteenmuunnoksen (NAT) sekä tuen virtuaaliselle erillisverkolle (VPN). UTM on kehitetty yksinkertaistamaan tietoturvaratkaisujen laajaa kirjoa yhdeksi laitteeksi, sen sijaan, että olisi erillinen laite tai palvelu jokaiselle edellä mainitulle ratkaisulle, mahdollisesti jopa eri toimittajilta (Kaspersky, 2017).

UTM-järjestelmien huomattava etu verrattuna seuraavan sukupolven palomuureihin on niiden helppous. Verkon tietoturvaa rakennettaessa UTM:llä on mahdollista valita tietyt tarvittavat tietoturvaratkaisut tai vaihtoehtoisesti valita kerralla kaikki palvelut (Fortinet, n.d.-a; Xiaoyun, 2023).

2.4 Demilitarized zone

Demilitarized zone on alun perin sotilastermi, jolla tarkoitetaan puskurivyöhykettä. Tietoverkoissa DMZ-network on puskurivyöhyke sisäverkon ja internetin välillä, johon sijoitetaan palveluita, joiden täytyy olla saavutettavissa julkisesti internetistä, mutta joita ei haluta päästää suoraan yrityksen sisäverkkoon. Pyrkimys on lisätä ylimääräinen suojakerros yrityksen tietoverkkoon, erityisesti sisäverkon ja internetin välille.

Yrityksen tietoverkko voidaan jakaa kerroksiin, sisä-, DMZ- ja ulkoverkko. Sisäverkko on luotettu ympäristö, johon sijoitetaan palvelimet ja työntekijöiden tietokoneet. DMZ-verkko on puoliluotettu vyöhyke, jossa on julkisesti saatavilla olevia palveluita, kuten verkkosivupalvelin, sähköpostipalvelin tai VPN-yhdyskäytävä. Ulkoverkko on epäluotettu ympäristö, ulkoinen internet (Fortinet, n.d.-b; Zenarmor, 2024).



Kuva 6 - DMZ-verkon sijoitus tietoverkossa (Zenarmor, 2024).

3 NEXT-GENERATION PALOMUURIT

Suuressa osassa yrityksiä tietoverkkojen tietoturva on pirstaleista ja epäjohdonmukaista, johtaen vakaviin tietoturvariskeihin. Millerin (2011, s.39) mukaan vaikka yritysten tietoturvaa on koitettu parantaa lisäämällä bolt-on tyylisiä ratkaisuita, ovat koitokset todistetusti olleet tehottomia.

Jotta palomuurista saataisiin taas yritysten tietoturvan kulmakivi, next-generation palomuurien tavoitteena on korjata tietoturvan ydinongelmat. Kun lähdetään puhtaalta pöydältä, NGFW luokittelee verkkoliikennettä sovelluksen identiteetillä, mahdollistaakseen jokaisen sovellustyypin hallinnan.

Millerin (2011, s.42) mukaan tehokkaan next-generation palomuurin välttämättömiä toiminnallisuuksia ovat vähintään:

- Sovelluksen tunnistaminen riippumatta portista, protokollasta, välttelytekniikasta ja SSL-kryptaamisesta ennen minkään muun toiminnon suorittamista.
- Tarjota näkyvyyttä ja tarkkaa käytäntöihin perustuvaa sovellusten ja yksittäisten toimintojen hallintaa.
- Tunnistaa tarkasti käyttäjät ja soveltaa asetettuja käytäntöjä käyttäjätietojen perusteella.
- Tarjota reaaliaikaista suojausta laajaa uhkien kirjoa vastaan, mukaan lukien ne, jotka toimivat OSI-mallin 7-kerroksella eli sovelluskerroksella.
- Integroida, ei vain yhdistellä, perinteisen palomuurin toimintoja ja edellä mainittuja lisätoimintoja, kuten IPS.
- Perinteisen palomuurin toimintoja kuten pakettien suodatus, osoitteenmuunnos, tilallinen tarkistus ja tuki virtuaaliselle erillisverkolle.

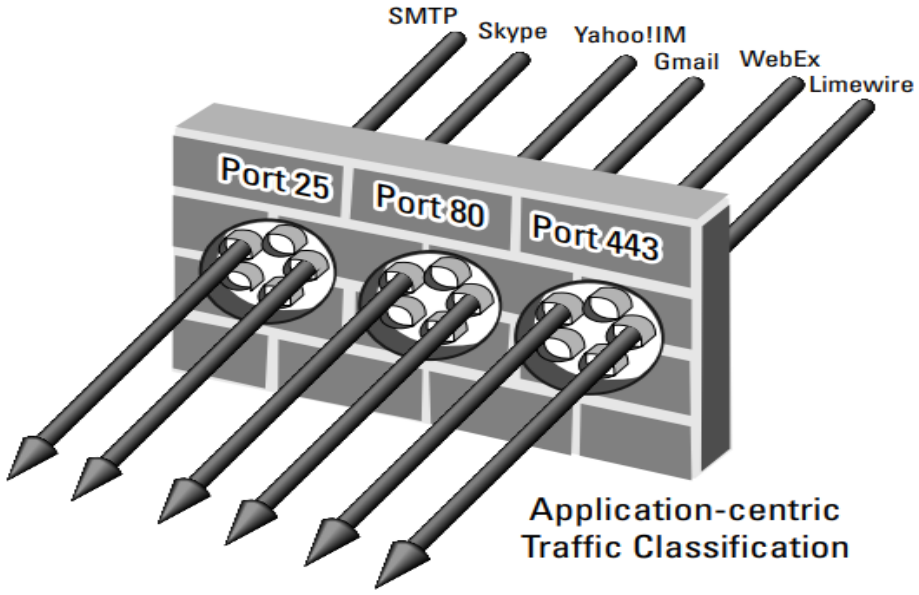
3.1 Sovellustunnistus

Sovellustunnistuksen tärkeimpiä ensiaskelia ovat portin ja protokollan vahvistaminen, mutta ne eivät ole riittäviä. Sen sijaan, että luotetaan taustalla toimivien, tunnistamattomien verkkoyhteyksien palveluihin, vankka

sovellustunnistus ja -tutkinta mahdollistavat tarkan verkkoistuntojen hallinnan palomuurin läpi kulkevien sovellusten ja pakettien perusteella (kuva 7).

Palomuuri päättelee sovelluksen protokollan ja onko salaus käytössä. Jos salaus on käytössä, se puretaan. Sovellustunnistuksen jälkeen tiedot salataan uusiksi. Palomuuri päättelee myös, onko alun perin havaittu protokolla oikea protokolla vai onko protokolla tunneloitu, piilottaen alkuperäisen protokollan.

Palomuuri myös analysoi kontekstiperusteella allekirjoituksia, uniikkeja ominaisuuksia ja tapahtumien tunnusominaisuuksia tunnistaakseen sovelluksen riippumatta portista tai protokollasta. Tähän sisältyy kyky havaita toimintoja sovellusten sisältä, kuten pikaviestipalvelun sisäinen tiedonsiirto (Miller, 2011, s.43).



Kuva 7 - Sovellustunnistus käytännössä (Miller, 2011, s.43).

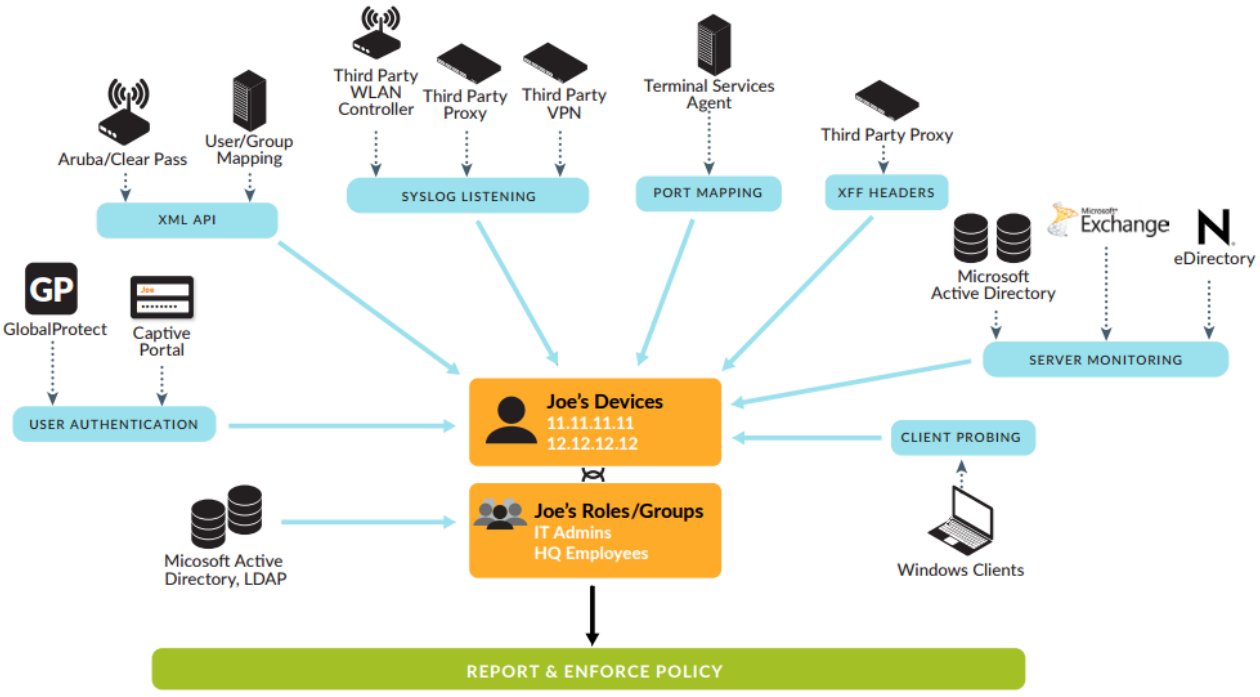
3.2 Sisällöntunnistus

Yksi suurimmista harppauksista palomuuritekniikassa on aktiivinen sisällön tunnistus ja -suodatus. NGFW pystyy itse selvittämään verkkoliikenteen sisällön tutkimalla IP-paketin tiedot OSI-mallin tasojen 2–7 väliltä, riippumatta porteista, protokollista, salauksesta (SSH/SSL) tai muista välttelytekniikoista. Erikoistapauksissa, joissa sovelluksen välttelytekniikat ovat ylitsepääsemättömiä, NGFW:n on mahdollista tunnistaa sovelluksen tarkoitus

perustuen heuristiikkaan ja/tai käyttäytymiseen (Roukka, 2015, s.8–9; Palo Alto Networks, 2025a).

3.3 Käyttäjätunnistus

Jo pidemmän aikaa internetin käytössä on ollut laaja-alainen muutos. Tämän muutoksen myötä pelkkiin IP-osoitteisiin pohjautuvat palomuurisäännöt ovat jääneet tietoturvattomiksi. Käyttäjän identiteetin tunnistus helpottaa palomuurisääntöjen rakentamista, kun loppukäyttäjä voidaan varmistaa IP-osoitteesta tai laitteesta huolimatta. Onnistuneen tunnistuksen jälkeen käyttäjän tiedot saadaan yrityksen toimialueen LDAP-hakemistosta, eli esimerkiksi Microsoftin omasta Active Directory-palvelusta. Käyttäjän tietoihin voi kuvan 8 mukaisesti sisältyä henkilön ryhmäroolit, tunnetut laitteet, henkilökohtaiset palomuurisäännöt ja sallitut sovellukset, esimerkkinä SSH- tai FTP-yhteydet. (Tuomaala, 2018, s.11; Parkki, 2019, s.15; Palo Alto Networks, 2025b).



Kuva 8 - Käyttäjätunnistuksen kaavio (Palo Alto Networks, 2025b).

3.4 Sandboxing

Sandboxing on yksi NGFW:n ominaisuuksista, joka on aktiivisten uhkien torjunnan peruspilareita. Sandboxingissa on kyse eristetystä ympäristöstä, ”hiekkalaatikosta”, jossa voidaan suorittaa ja tutkia koodia ilman uhkien leviämisen vaaraa (Fortinet, n.d.-c).

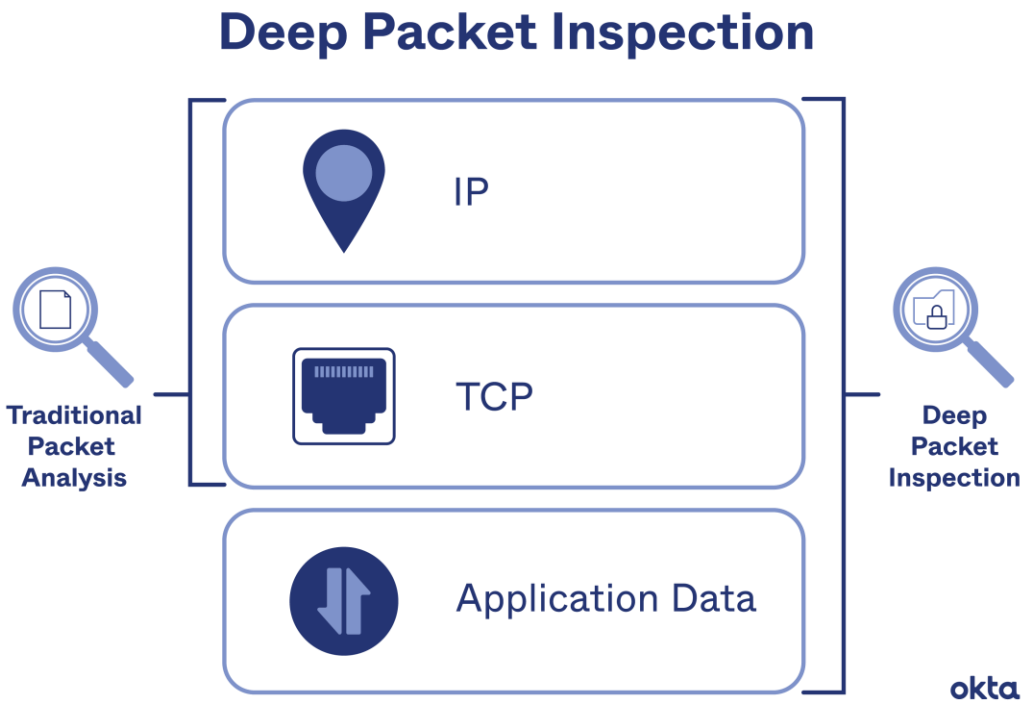
Havaitessaan entuudestaan tuntematonta verkkoliikennettä, NGFW vie liikenteen karanteeniin sandbox-ympäristöön analysoitavaksi. Karanteenissa analysoidaan sen käyttötarkoitusta ja motiiveja tutkimalla sen tietoja ja käytöstä, esimerkiksi jos tiedosto tekee muutoksia tietokoneeseen, kuten järjestelmä- tai rekisteritiedostoihin (Fortinet, n.d.-c).

Sandbox-karanteeni on tarkka, mutta siinäkin on mahdollisuus virheisiin, varsinkin jos karanteeni on lyhytaikainen. Varma analyysi voi vaatia viikkojenkin karanteenin, jos haitallinen tiedosto on rakennettu toimimaan pitkäaikaisesti tai huomattavalla viiveellä. Jos yrityksellä on BYOD-käytäntö, on mahdollista, että käyttäjä lataa ja suorittaa omassa tai julkisessa verkossa haitallisia tiedostoja. Uudempi IPv6 käyttää salattua protokollaa, jolla on myös mahdollisuus ohittaa sandbox. Myös P2P-yhteyksiä hyödyntävä verkkoliikenne, kuten tiedostojen jako (torrent-ohjelmat), pikaviestimet (Skype, WhatsApp), kryptovaluutat (Bitcoin) ja esimerkiksi jotkin VPN:ät voivat mahdollisesti ohittaa sandbox-ympäristön (Nurmi, 2021, s.15–16; Tuomaala, 2018, s.8–9; Fortinet, n.d.-c).

3.5 Paketin syvätarkistus

Paketin syvätarkistus (DPI) arvioi tarkistuspisteen läpi kulkevan IP-paketin dataa sekä otsikkoa. Näin osataan estää sopimattomat protokollat, spam-viestit, virukset, tunkeutumiset sekä muut määritetyt kriteerit täyttävät paketit kulkemasta tarkistuspistettä pidemmälle. DPI myös määrittelee, mitä tietyille paketeille tehdään. Ohjataanko paketti toiseen kohteeseen, hylätäänkö paketti vai päästetäänkö se läpi.

DPI toimii OSI-mallin sovelluskerroksella. Soveltaen määriteltyjä sääntöjä reaaliaikaisesti, DPI päättää mitä paketille tehdään (Brook, 2018).



Kuva 9 - Paketin syvätarkistus yksinkertaistettuna (Integrated Research n.d.; Okta, 2024).

3.6 Siirtymisen haasteet

Vaikka NGFW on hieno paperilla ja jopa käytännössä, on myös syitä olla vaihtamatta.

Tämän päivän tietoturvajärjestelmät ja laitteiden määrä on paisunut niin suureksi, että koko tietoturva-arkkitehtuurin uudelleenrakentaminen NGFW-alustalla tulee viemään huomattavan määrän resursseja, varsinkin jos tällaista projektia ei suunnitella etukäteen (Nurmi, 2021, s.27–28; Hagerty, 2023).

Laitteiden sekä lisälisenssien hinnat. Hinnat nousevat huomattavasti, kun palomuurin kapasiteettia nostetaan. Käytetään esimerkkinä taulukossa 1 näkyviä Ciscon Firepower 4100-sarjan 4112-, 4115- sekä 4125-laitteita. Ciscon tietolomakkeen (liite 2) mukaan 4112- sekä 4115-yksiköissä on sama laitteisto ja 4125-yksikössä on edellä mainittuihin verrattuna kaksinkertainen

määrä tallennustilaa sekä yhden 1100W virtalähteen sijaan kaksi 1100W virtalähdettä.

Taulukko 1 - Ciscon Firepower laitteiden hintoja (ITPrice, 2025).

	4112	4115	4125	Voimassaoloaika
Listahinta	$112,721	$150,297	$237,974	
Threat Protection	$63,558	$84,744	$134,174	3 vuotta
Malware Protection	$63,558	$84,744	$134,174	3 vuotta
URL Filtering	$63,558	$84,744	$134,174	3 vuotta
Pakettihinta	$140,457	$187,276	$296,525	3 vuotta

Kuten taulukosta 1 ja liitteestä 2 on nähtävissä, laitteiden hinnat nousevat huomattavasti vaikka laite ei sisäisesti muuttuisikaan. Laitteiden ohjelmistoissa on askelittaisia eroja, kuten liitteestä 1 on nähtävissä.

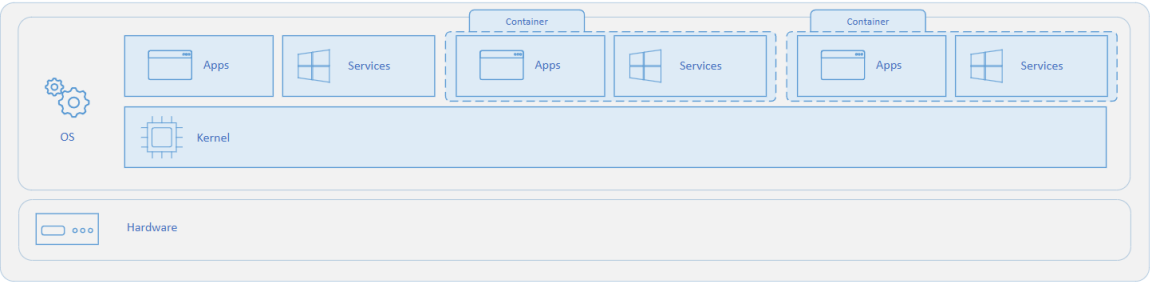
Ciscon Firepower 4100-sarja on vuonna 2016 julkaistu suurille organisaatioille ja laitoksille kuten tietokeskuksille ja suurille kampuksille suunniteltu palomuuri. Cisco on lopettanut Firepower 4100-sarjan myynnin vuonna 2021. Jälleenmyyjät jatkavat myyntiä.

4 KONTTITEKNOLOGIAT JA NGFW

4.1 Mitä konttiteknologia on

Konttiteknologiat ja kontit ovat tapa paketoida ja helpottaa eri sovellusten käyttöä monissa eri ympäristöissä ja käyttöjärjestelmissä, niin pilvessä kuin paikallisesti. Kontit tarjoavat helpotusta sovellusten käyttämiseen, kehittämiseen ja hallitsemiseen kevyiden ja eristettyjen ympäristöjen muodossa. Kontit käynnistyvät ja pysähtyvät nopeasti, tehden niistä ihanteellisia sovelluksille, joiden tulee pystyä sopeutumaan nopeasti vaihtuvaan tarpeeseen (Microsoft, 2025).

Kontti on eristetty ja kevyt järjestelmä, joka on rakennettu isäntälaitteen käyttöjärjestelmän kernelin päälle ajamaan tiettyä sovellusta tai palvelua.



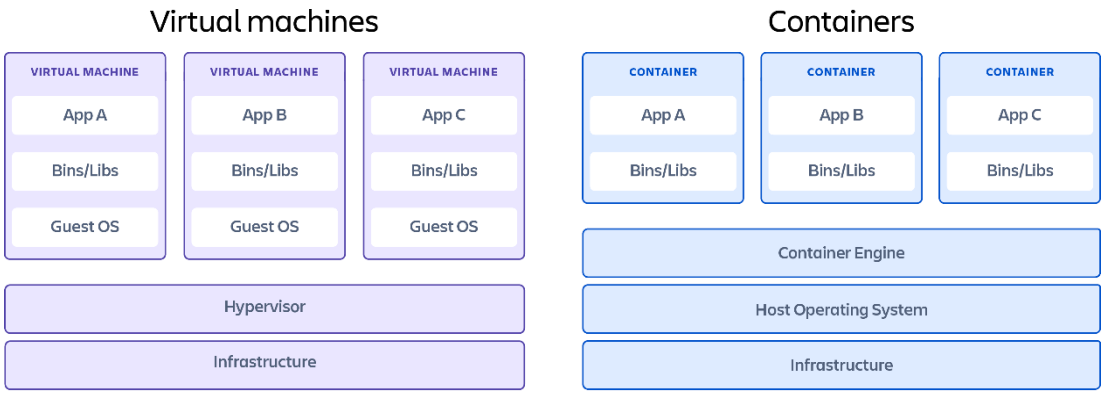
Kuva 10 - Konttiteknologian arkkitehtuuri (Microsoft, 2025).

Vaikka kontti jakaa isäntälaitteen käyttöjärjestelmän kernelin, ei kontilla ole rajoittamatonta pääsyä siihen. Yleisesti kontti saa eristetyn pääsyn ja joissain tapauksissa virtualisoidun näkymän järjestelmästä. Virtualisoidussa näkymässä kontilla on pääsy järjestelmään ja rekistereihin, mutta tehdyt muutokset vaikuttavat vain konttiin ja muutokset hylätään käytön jälkeen. Halutessa tietoja voidaan tallentaa esimerkiksi Azure Diskiin (Microsoft, 2025).

4.1.1 Konttiteknologiat ja virtuaalikoneet.

Kontit ja virtuaalikoneet ovat hyvin samankaltaisia resurssien virtualisointiratkaisuita. Näiden ratkaisuiden erottaja on virtualisointitapa. Virtuaalikoneet virtualisoivat tietokoneen komponenteista lähtien ja kontit

virtualisoivat vain käyttöjärjestelmästä syvemmälle, esimerkiksi sovelluksia. Yksi yleisimmistä toimintatavoista on käyttää virtuaalikoneen käyttöjärjestelmää pohjana kontille (Microsoft, 2025; Buchanan, n.d.).



Kuva 11 - Kontin ja virtuaalikoneen arkkitehtuurit (Buchanan, n.d.).

4.2 Konttipalomuurit

Konttipalomuuri on sovelluspohjainen versio seuraavan sukupolven palomuurista, joka on rakennettu konttiympäristöä varten. Perinteiset seuraavan sukupolven palomuurit voidaan asentaa vain konttiympäristön reunalle eivätkä näin ollen pysty kontin sisäiseen sovellustunnistukseen. Kontin sisäinen NGFW mahdollistaa tietoturvan tarkan jatkuvuuden. Konttipalomuuri on suunniteltu mahdollistamaan häiriötön CI/CD toimintamalli reaaliaikaisen palomuuritoiminnan ohella (Palo Alto Networks, n.d.-d).

Kontit ovat alttiita samoille vanhoille verkon yli tapahtuville hyökkäyksille. Samat tunnetut vaarat uhkaavat myös kontteja, vaikka kontit ovatkin uusi ja innovatiivinen tapa käyttää sovelluksia. Oli käytössä joko kiinteä laite, virtuaalikone tai kontti, käytettävät sovellukset käyttävät silti perinteistä verkkoyhteyttä ja näin ollen ovat alttiita verkon yli tapahtuville hyökkäyksille (Palo Alto Networks, n.d.-d).

5 OPERATIIVINEN TEKNOLOGIA

5.1 Tietoturvapolitiikka ja operatiiviset teknologiat

Operatiivisten teknologioiden ympäristöt eroavat tietoturvavaatimuksiltaan huomattavasti verrattuna perinteisiin tietoverkkoihin. Ennen teollisuusautomaatiota ja tuotannon hallinta- ja valvontajärjestelmiä, operatiiviset teknologiat olivat pääosin fyysisiä ja verkollisesti eristettyjä muusta IT-ympäristöstä. Nykyisin OT-järjestelmät ovat yhä useammin kytkettynä yrityksen verkkoon ja pilvipalveluihin, jotta järjestelmiä voidaan automatisoida ja kerättyä dataa voidaan hyödyntää liiketoiminnan tehostamisessa. Tämänlainen kehitys lisää tehokkuutta, mutta samalla avaa uudenlaisia riskejä (NIST, 2023, s. 28 & s. 68).

IT- ja OT-ympäristöissä on erilaiset prioriteetit tietoturvan suhteen. IT-ympäristöissä on yleisesti käytössä melkein standardiksi noussut CIA-triadi, confidentiality eli luottamuksellisuus, integrity eli eheys ja availability eli käytettävyys. OT-ympäristöissä prioriteetit ovat yleisesti käytettävyys, sekä henkilö- että materiaaliturvallisuus, eheys ja luottamuksellisuus. OT-ympäristöissä tärkeintä on, että toiminta ei keskeydy ja toiminnasta ei aiheudu vaaraa henkilöille tai materiaalille (NIST, 2023, s. 28–32).

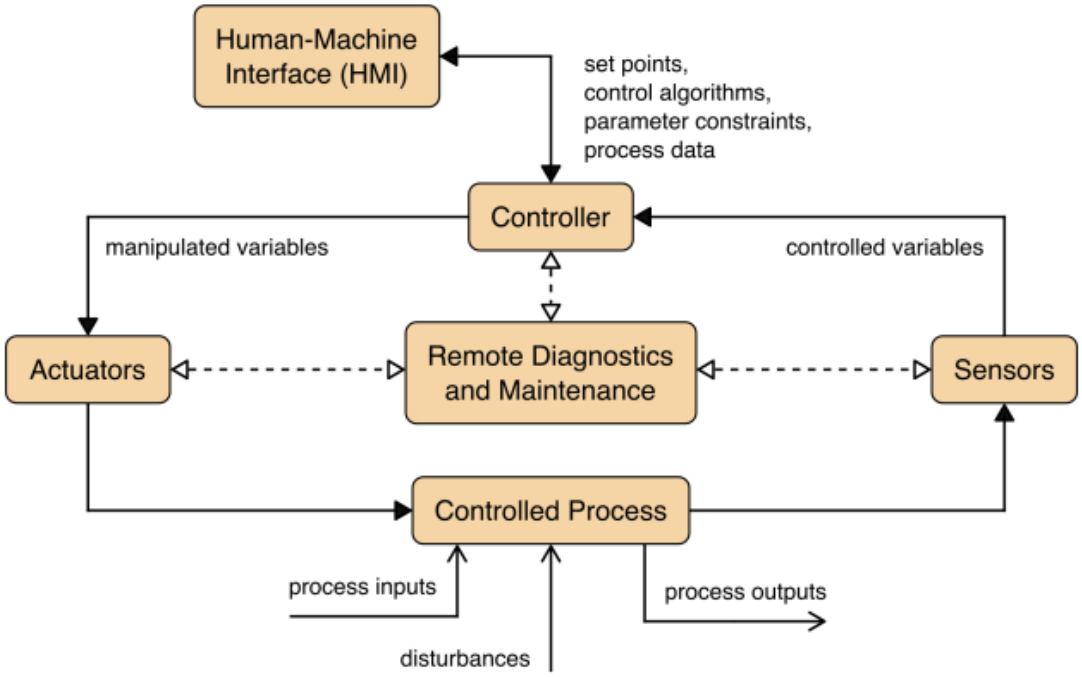
Kun OT-ympäristöt ovat verkkoyhteydessä on vaarana, että haitallinen toimija pystyy lukitsemaan hallintajärjestelmiä, vakoilla toimintaa ja varastaa prosessitietoa tai liikesalaisuuksia tai jopa manipuloida prosesseja, jolloin seurauksena voi olla toiminnan pysähtyminen tai jopa fyysiset vahingot, kuten kappaleessa 5.3.4 todetaan BlackEnergy 3:n ja Stuxnetin kaltaisilla toimilla (NIST, 2023, s. 179).

5.2 Mitä operatiivinen teknologia on

Operatiivinen teknologia on fyysisten prosessien, laitteiden ja infrastruktuurin monitorointia ja ohjausta niin sovellus- kuin laitepohjaisesti. Operatiivisten

teknologioiden järjestelmiä löytyy laaja-alaisesti eri työtehtävistä, niin kriittisen infrastruktuurin monitoroinnista kuin tehtaan kasauslinjaston robottien hallinnasta. Operatiiviset teknologiat ovat käytössä monilla eri aloilla kuten esimerkiksi valmistuksessa, lentoteollisuudessa, merenkulussa, rautateillä sekä öljy- ja kaasuteollisuudessa (Fortinet, n.d.-d).

Suurin osa moderneista operatiivisen teknologian laitteista on kehittynyt tietotekniikan lisäämisestä jo olemassa oleviin fyysisiin laitteisiin, esimerkiksi käsikäyttöiseen luistiventtiiliin on lisätty virtausmittari, venttiilin asentoanturi sekä etäohjattava sähkömoottori. Nyt valvomosta näkee virtauksen, venttiilin asennon sekä venttiiliä voi ohjata etäkäytöllä (NIST, 2023).

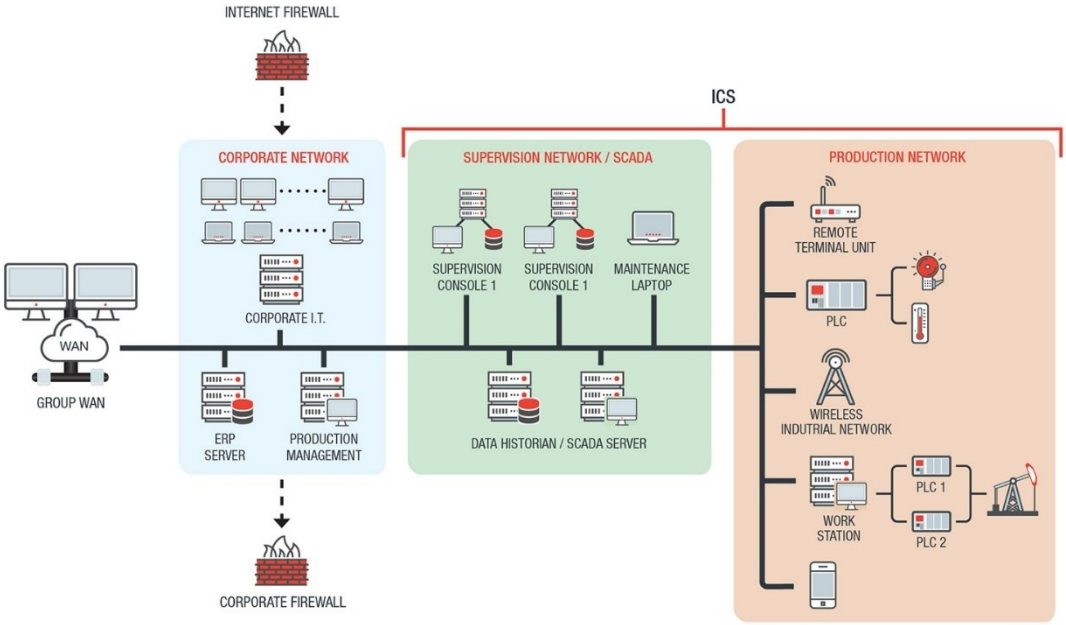


Kuva 12 - Operatiivisen teknologian tyypillinen toimintakaavio (NIST, 2023, s. 11).

5.3 Industrial control systems

Teollisuuden ohjausjärjestelmät hallitsevat, automatisoivat ja valvovat fyysisiä prosesseja teollisuuden prosesseissa. Teollisuuden ohjausjärjestelmät ohjaavat operatiivisen teknologian laitteita joko automaattisesti erilaisten parametrien perusteella tai manuaalisesti käytönohjausjärjestelmän kautta (Cisco, 2024a).

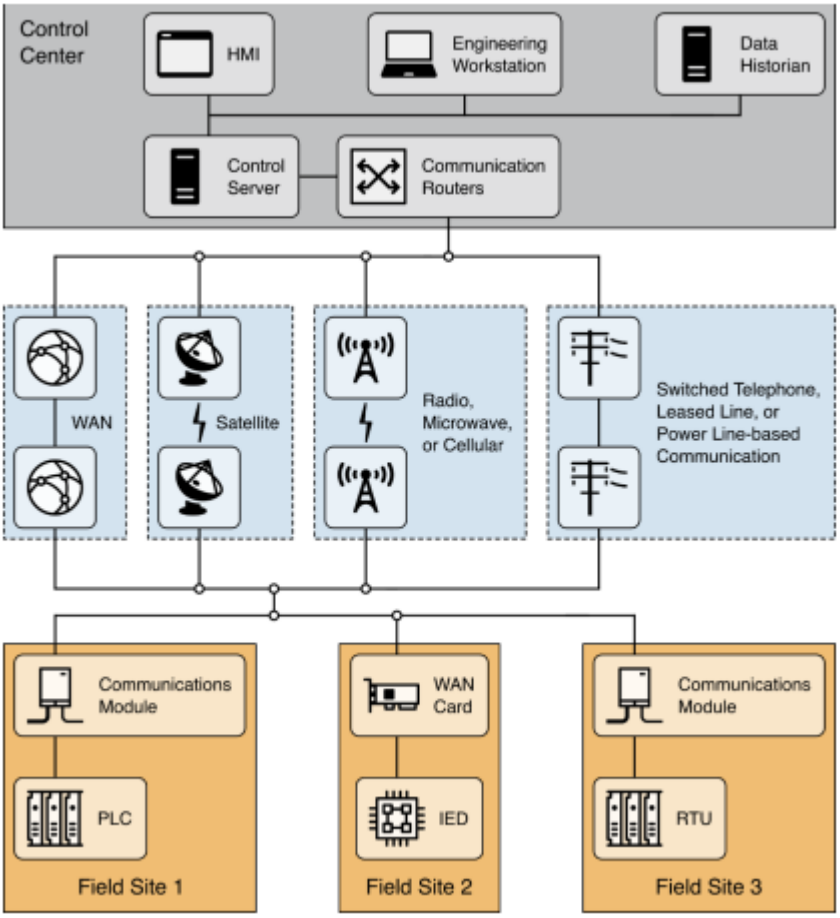
Teollisuuden ohjausjärjestelmiin tapahtuvat hyökkäykset ovat yleisesti kohdistettuja hyökkäyksiä, joilla on tarkoitus päästä syvemmälle operatiivisten teknologioiden järjestelmiin. Hyökkäyksillä voi olla eri motiiveja, kuten rahallinen hyöty, teknologioiden kopioiminen tai kehityksen hidastaminen. Yksi tunnetuimpia tapahtuneita hyökkäyksiä on tapaus Stuxnet (Trendmicro, n.d.-a).



Kuva 13 – Teollisuuden ohjausjärjestelmäkaavio (Trendmicro, n.d.-a).

5.3.1 SCADA

Käytönohjausjärjestelmiä käytetään hajautettujen laitteiden hallintaan, joille keskitetty tiedon keräys on yhtä tärkeää kuin hallinta. Näitä laitteita käytetään esimerkiksi veden jakelu- ja raideliikenteen ohjausjärjestelmissä. Käytönohjausjärjestelmät yhdistävät datan keräyksen, lähetyksen sekä ihmisen ja koneen välisen rajapinnan joko graafiseksi tai tekstipohjaiseksi käyttöliittymäksi, josta on mahdollista valvoa ja hallita prosesseja (NIST, 2023, s. 12–18).



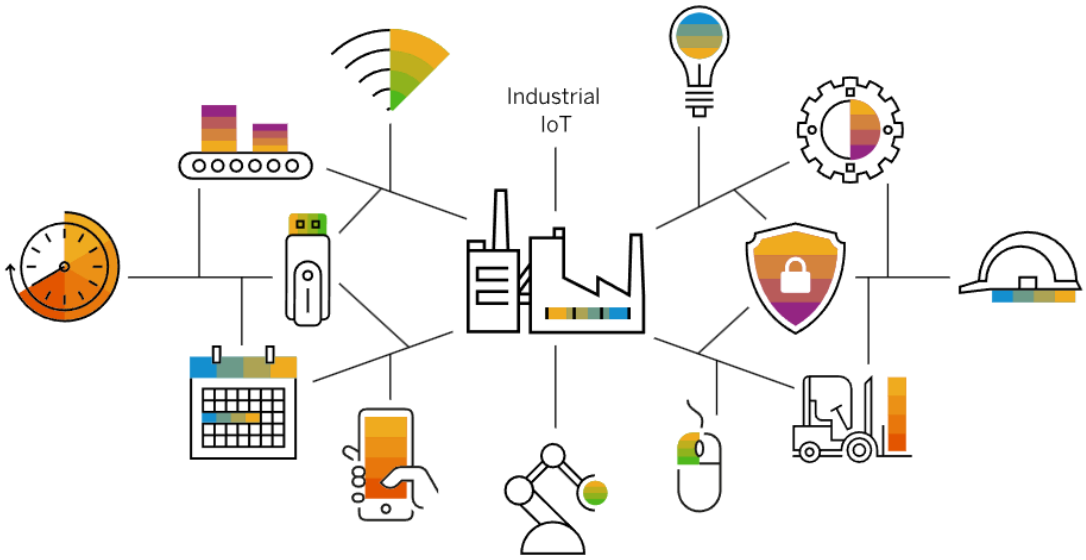
Kuva 14 - Tyypillisen SCADA-järjestelmän toimintakaavio (NIST, 2023, s.13).

5.3.2 Industrial Internet of Things

Kun IoT painottuu enemmän kuluttaja- ja pienemmän skaalan laiteverkostoihin, teollisuuden IoT painottuu enemmän suuriin tehdas- ja laitosympäristöihin sekä niiden laitteiden väliseen kommunikaatioon, big dataan ja koneoppimiseen. IIoT parantaa teollisuuden ja yritysten tehokkuutta ja prosessien luotettavuutta.

Tietotekniikan ja operatiivisen teknologian yhdistyminen tarjoaa teollisuudelle parempaa järjestelmien automaatiota, optimointia sekä parempaa näkyvyyttä logistiikkaan ja toimitusketjuihin. IIoT:n tarjoama reaaliaikainen data mahdollistaa automaation päätöksenteon sekä helpottaa manuaalisten päätösten tekoa. Jatkuva ja reaaliaikainen datan tallennus ja lähetys tarjoavat teollisuudelle ja yrityksille monia kasvumahdollisuuksia. Data mahdollistaa

virheistä oppimisen ja prosessien tehokkuuden kasvattamisen (Trendmicro, n.d.-b).



Kuva 15 - Industrial Internet of Things (SAP, n.d.).

5.3.3 IIoT ja tietoturva

Kun siirrytään IIoT-ratkaisuihin, on kolme aluetta joihin tulee kiinnittää huomiota: saatavuus, skaalautuvuus ja tietoturva. Saatavuus ja skaalautuvuus ovat helpompia hoidettavia, mutta tietoturva on alue jossa moni ei onnistu.

Monet yritykset käyttävät edelleen vanhoja sovelluksia ja järjestelmiä. Useat näistä sovelluksista ja järjestelmistä ovat vuosikymmeniä vanhoja ja joskus jopa päivittämättömiä, luoden tietoturvauhkia. Tietoturvan tärkeys nousee esille aina kun merkittäviä tietoturvan murtotapauksia esiintyy maailmalla. Jos haitalliset toimijat pääsevät murtautumaan verkkoon, on mahdollista, että koko laitoksen tuotanto joudutaan pysäyttämään niin pitkäksi aikaa, että tietotekniikan tilanne saadaan stabiiliksi.

Monet tietoturvaan liittyvät ongelmat johtuvat usein IIoT:n vajavaisista tietoturvatoimenpiteistä. Riskien määrä kasvaa jokaisesta avonaisesta portista, puutteellisesta autentikointimenetelmästä ja vanhentuneesta sovelluksesta. Kun nämä puutteet yhdistetään siihen, että laitteet saattavat olla suorassa yhteydessä ulkoverkkoon, riskien määrä ja laatu nousee

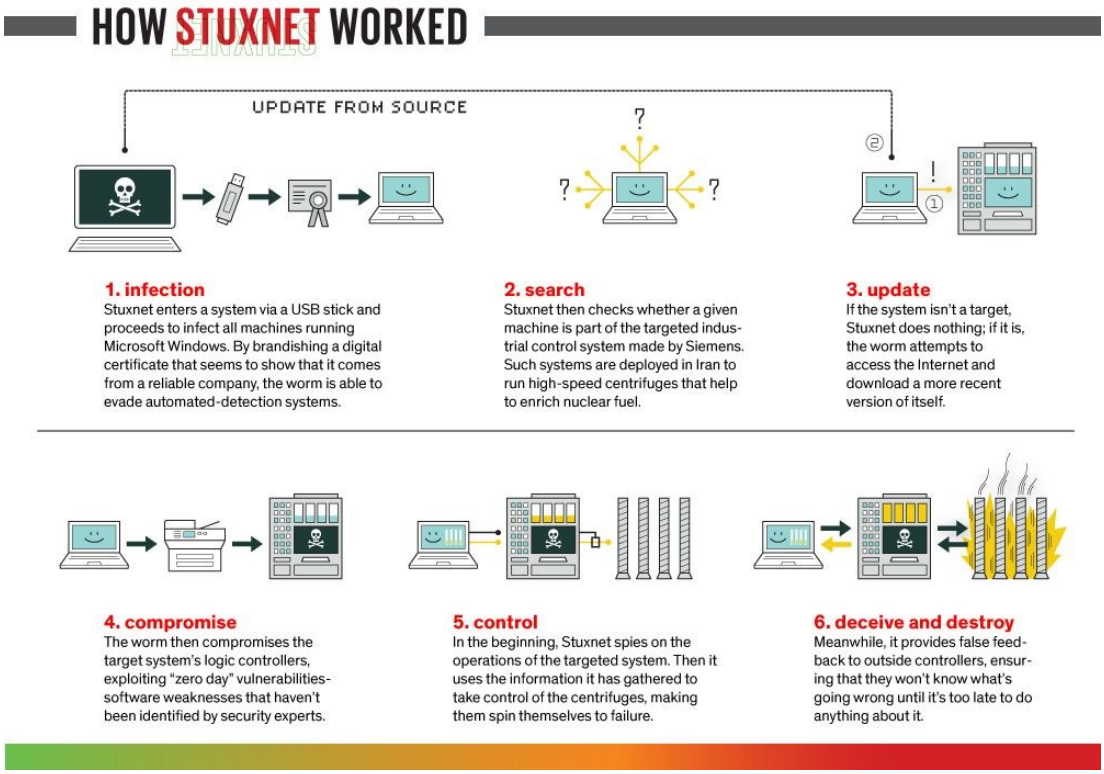
huomattavasti. Yritykset saattavat tiedostaa, että liiketoiminta voi hetkellisesti halvaantua tietomurron seurauksena. Kun tietotekniikka ja operatiivinen teknologia yhdistyy, nousee esiin huomattava uusi riski: ulkomaailman uhat, jotka voivat vaikuttaa kansalaisten jokapäiväiseen elämään (Trendmicro, n.d.-b). Ensimmäisen kerran tämä uhka realisoitui virallisesti suuressa mittakaavassa Ukrainassa vuoden 2015 joulukuussa, kun BlackEnergy 3 tuhosi sähköverkon operatiivisen teknologian järjestelmiä.

5.3.4 BlackEnergy 3 ja Stuxnet

Vuoden 2015 joulukuussa tehtyä BlackEnergy 3-hyökkäystä pidetään ensimmäisenä virallisena onnistuneena kriittiseen infrastruktuuriin kohdistuvana hyökkäyksenä. Hyökkääjät onnistuivat saamaan pääsyn kolmen eri energiayhtiön SCADA-järjestelmiin. Pääsyn aikana hyökkääjät manipuloivat laitteistoa vastoin raja-arvoja ja manipuloinnin jälkeen tuhosivat sovellusinfrastruktuuria KillDisk-ohjelmistolla. Hyökkäyksen tuloksena oli noin kuuden tunnin virtakatkos, vaikuttaen yli 230 000 ihmisen arkeen. Vaikka suurin osa SCADA-järjestelmistä oli käyttökelvottomassa kunnossa, virtakatkoksen lyhytkestoisuus johtui vain ja ainoastaan yritysten työntekijöiden syvästä kriittisen infrastruktuurin tuntemuksesta ja mahdollisuudesta käyttää sähköverkkoa manuaalisesti. (Beach-Westmoreland, Styczynski, 2016).

Stuxnetin kohde oli teollisuuden ohjausjärjestelmät, pääasiassa eräs Siemensin valmistama SCADA-järjestelmä. Stuxnetin pääasiallinen levitystapa oli USB-tikkujen kautta, jolloin mato pystyi levittäytymään myös internetistä eristettyihin ympäristöihin. Kun Stuxnet havaitsi päässeensä sisään Siemensin SCADA:an, se käytti laitteeseen kovakoodattua salasanaa saadakseen käyttöoikeudet. Stuxnetiä on löydetty maailmanlaajuisesti eri SCADA-järjestelmistä esimerkiksi Kiinasta, Intiasta, Iranista ja Indonesiasta (Rantapelkonen & Salminen, 2013, s. 213). Carrin mukaan Stuxnet on mahdollisesti syypää intialaisen INSAT4-B kommunikaatiosatelliitin osittaiseen hajoamiseen vuonna 2010 (Carr, 2010).

Hyppösen mukaan Stuxnet on yksi tärkeimmistä haittaohjelmahyökkäyksistä historiassa ja nykyisin puhutaan aikakausista ennen ja jälkeen Stuxnetiä. Stuxnet pystyi leviämään minkä tahansa asemaksi kiinnitettävän laitteen kautta, kuten USB-tikku, puhelin, muistikortti ja niin edelleen. Stuxnet piiloutuu järjestelmään ja leviää muihin samassa paikallisverkossa oleviin tietokoneisiin hyödyntäen viittä eri nollapäivän haavoittuvuutta, asentaa haitallisia ajureita varastetulla sertifikaatilla ja selvittää onko järjestelmä kytköksissä Siemensin Simatic-järjestelmään. Tämän jälkeen Stuxnet muokkaa Windowsilta PLC:lle lähteviä komentoja. Kun Stuxnet on päässyt käsiksi PLC:hen, se selvittää onko käyttöympäristö halutunlainen. Jos ympäristö on vääränlainen, Stuxnet ei ryhdy toimenpiteisiin. Jos ympäristö on oikeanlainen ja ympäristöstä löytyy tietynlaisia Vaconin tai Fararo Payan valmistamia korkeataajuusmuuntimia, Stuxnet muokkaa niiden toimintaa. Estääkseen päällekkäisyydet, Stuxnet tunnistaa jo saastuneet laitteet asettamalla rekisteriin avaimen arvolla 19790509 (Hyppönen, 2022).



Kuva 16 - Stuxnetin toimintakaavio (IEEE Spectrum, 2013).

5.4 Operatiivisen teknologian riskienhallinta

Operatiivisen teknologian tietoturvariskien lieventämistä varten organisaatioiden tulee perustaa OT-tietoturvaohjelma. Ohjelman tulee olla johdonmukainen ja integroitu jo olemassa oleviin IT-tietoturvaohjelman sovelluksiin ja käytäntöihin, mutta samalla huomioida OT:n uniikit vaatimukset ja ympäristöt (NIST, 2023, s. 33). Operatiivisen teknologian täydellisen ja tehokkaan tietoturvan perustaminen on monimutkainen prosessi, joka eroaa tyypillisistä tietoturvamenetelmistä. Lopullinen tavoite on maksimoida toiminta-aika ja minimoida tietoturvaloukkaukset (Palo Alto Networks, n.d.-e).

NIST:n operatiivisen teknologian hyvään riskienhallinnan malliin kuuluu yhdeksän askelta.

1. OT-tietoturvahallinnon perustaminen.
2. OT-tietoturvaosaston perustaminen ja koulutus.
3. OT-tietoturvastrategian määrittely.
4. OT-kohtaisten käytäntöjen ja menettelyjen määrittely.
5. OT-tietoturvastrategian koulutusohjelman perustaminen.
6. OT-riskienhallintakehyksen käyttöönotto.
7. OT-huollon seurantakyvyn kehitys.
8. OT-tapahtumien reagointikyvyn kehitys.
9. OT:n palautumis- ja palautuskyvyn kehitys.
   (NIST, 2023, s. 33–43).

5.4.1 Tietoturvahallinnon perustaminen

Tietoturvahallintoon tulisi sisältyä käytäntöjen, menettelyjen ja prosessien hallintaa varten organisaation sääntely-, laki-, riski-, ympäristö- ja toiminnalliset vaatimukset. Hallinnon tulee varmistaa, että henkilökunta ymmärtää käytännöt, menettelyt ja prosessit ja informoida johtoa OT:n tietoturvariskeistä. Jotta tehokas tietoturvahallinto on mahdollista perustaa, tulee seuraavat asiat varmistaa:

- OT:n tietoturvapolitiikka on laadittu ja asiasta on tiedotettu.

- OT:n tietoturvapolitiikan roolit ja vastuut ovat koordinoituja ja yhdenmukaisia.
- OT:n tietoturvapolitiikka on laki- ja säädösvaatimusten mukainen ja nämä vaatimukset ymmärretään.
- Tietoturvariskit integroidaan yrityksen riskienhallintaprosesseihin. (NIST, 2023, s. 38).

5.4.2 Tietoturvaosaston perustaminen ja koulutus

On välttämätöntä, että monitoimisen tietoturvaosaston jäsenet jakavat keskenään tietojaan ympäristöistään. Operatiivisten teknologioiden tietoturvaosastossa tulee olla vähintään seuraavat jäsenet eri aloilta: IT-asiantuntija, käyttöinsinööri, ohjausjärjestelmäoperaattori, tietoturva-alan asiantuntija ja yrityksen riskienhallinnan asiantuntija. Lisäksi olisi suositeltavaa, että osastoon kuuluu myös jokin tietoturvapalvelujen tarjoaja (NIST, 2023, s. 38).

Tietoturvalla on myös oma osuutensa työturvallisuudessa. Tietomurrot ovat uhka teollisuuden prosessien turvallisuudelle ja luotettavuudelle, siksi myös työturvallisuuden edustajia tulee sisällyttää OT-tietoturvaosastoon. Heidän näkemyksensä ja tietämyksensä OT:n toiminnasta ja työturvasta ovat avuksi riskienhallintaprosessien suunnittelussa (NIST, 2023, s. 39).

5.4.3 Tietoturvastrategian määrittely

Koko organisaation laajuisen riskienhallintastrategian määrittely on OT:n tietoturvastrategian kehittämisen perusta. OT:n tietoturvastrategia hyödyntää organisaation riskienhallintastrategiaa, mukaan lukien organisaatiolle määritelty riskinsietokyky, uhat, oletukset, rajoitukset, prioriteetit ja kompromissit strategian räätälöimiseksi edelleen OT:n tietoturvastrategiaan sovellettavaksi.

OT:n tietoturvastrategia:

- Täydentää organisaationlaajuisen riskienhallintastrategian ohjeita OT-kohtaisten rajoitusten ja vaatimusten osalta.
- Käsittelee OT:n tietoturvastrategian toimintamallia.
- Kaavoittaa sopivan tietoturva-arkkitehtuurin OT-ohjelman eri sijainneille.
- Määrittää OT-kohtaisen tietoturvakoulutuksen ja -tietoisuuden.

Tietoturvastrategian tulisi helpottaa organisaation riskiensietokyvyn tarkentamista, joka omalta osaltaan ohjaa OT:n tietoturvastrategian prioriteetteja. Strategian tulee myös ottaa huomioon organisaation IT:n sekä OT:n huolet ja vaatimukset. IT voi pitää datan menetystä tai järjestelmien korkeaa saatavuutta korkeampana prioriteettina, kun taas OT voi pitää järjestelmän turvallisuutta, henkilö- ja ympäristövahinkojen ennaltaehkäisyä tai tuotannon tehokkuutta korkeampana prioriteettina (NIST, 2023, s. 39–40).

5.4.4 Käytäntöjen ja menettelyjen määrittely

Käytännöt ja menettelyt ovat välttämättömiä minkä tahansa tietoturvastrategian onnistumiselle. Missä mahdollista, OT-kohtaiset tietoturvakäytännöt ja -menettelyt tulee johtaa olemassa olevista tietoturva- ja laitoksen toimintaperiaatteista sekä menettelyistä johdonmukaisuuden varmistamiseksi koko organisaation laajuisesti (NIST, 2023, s. 40).

Organisaation johto on vastuussa organisaation riskinsietotasosta, eli riskin tason, jonka organisaatio on valmis hyväksymään, kehittämisestä ja viestinnästä, jonka avulla OT:n tietoturvaosasto voi määrittää riskienhallintastrategian. Tietoturvapolitiikan kehittämisen tulee perustua riskiarviointiin, joka asettaa organisaation turvallisuusprioriteetit ja -tavoitteet. Tietoturvapolitiikan käytännöt ja menettelyt tulee dokumentoida sekä testata ja päivittää säännöllisesti (NIST, 2023, s. 40).

5.4.5 Tietoturvastrategian koulutusohjelman perustaminen

Organisaatioiden tulee varmistaa, että koko henkilöstö, joka on kosketuksissa OT-järjestelmien kanssa, mukaan lukien urakoitsijat, konsultit ja muut ulkopuoliset saavat tarpeellisen tietoturvakoulutuksen sekä tietotekniikasta että operatiivisista teknologioista (NIST, 2023, s. 41).

Tämän koulutuksen tarkoitus on tiedottaa henkilöstölle tietoturvan perusperiaatteista, opettaa ja opastaa henkilöstöä heidän omasta vaikutuksestaan turvallisuuteen ja tietoturvaan sekä kuinka toimia OT-järjestelmien kanssa. Tietoturvakoulutus tulee pitää uusille työntekijöille työsuhteen alussa sekä kaikille työntekijöille tietyin aikavälein, riippuen organisaation käytännöistä (NIST, 2023, s. 41).

5.4.6 Riskienhallintakehyksen käyttöönotto

Operatiivisten teknologioiden riskienhallintaprosessissa on neljä komponenttia. Riskien kehystys, riskien arviointi, riskiin vastaaminen sekä riskin seuranta. Nämä toiminnot ovat toisistaan riippuvaisia sekä ne tapahtuvat usein samanaikaisesti organisaatiossa. Esimerkiksi seurantakomponentin tulokset syötetään kehystyskomponenttiin. Koska ympäristö jossa organisaatiot toimivat on jatkuvassa muutoksessa, riskienhallinnan tulee olla jatkuva prosessi, jossa kaikilla komponenteilla on jatkuvaa toimintaa. On tärkeää muistaa, että nämä osat liittyvät kaikentyyppisten riskien hallintaan, kuten tietoturvaan, fyysiseen turvallisuuteen kuin myös taloudellisiin riskeihin (NIST, 2023, s. 45).

5.4.7 Huollon seurantakyvyn kehitys

Organisaatioiden tulee kehittää ja ottaa käyttöön menetelmiä ja työkaluja, joilla varmistaa OT-laitteiden rutiininomaiset ennaltaehkäisevät huolto- ja korjaustyöt suoritetaan organisaation käytäntöjen ja menettelytapojen mukaisesti. Kunnossapidollisten töiden kirjaamiseen ja seurantaan käytettyjä

työkaluja tulee valvoa ja hallita. Prosessien ja työkalujen tulee mahdollistaa kunnossapidollisten töiden aikataulutus, valtuutus ja seuranta. Jos kunnossapidollinen työ vaatii etäkäyttöä, tulee varmistaa, että etäkäyttötyökalu tukee suoritettujen huoltotoimenpiteiden kirjausta, huoltohenkilön henkilöllisyyden todentamista ja yhteyden välitöntä katkaisua huoltotoimenpiteiden jälkeen (NIST, 2023, s. 41).

5.4.8 Tapahtumien reagointikyvyn kehitys

Organisaatioiden tulee perustaa OT-tietoturvan tapahtumia varten reagointisuunnitelma, johon sisältyy suunnittelu, havainnointi, analyysi, eristäminen sekä raportointi siinä tapauksessa, että tietoturvaloukkaus on tapahtunut. Suunnitelma edellyttää useiden tietoturvaominaisuuksien perustamista, mukaan lukien tapahtumien hallinta, tekninen analyysi, haavoittuvuuksien hallinta ja vastausviestintä. Osana suunnitelmaa OT-tietoturvaosaston tulee laatia reagointimalli. Reagointimallin tarkoituksena on määrittää tietoturvahäiriöiden laajuus ja riski, reagoida tapahtumiin asianmukaisesti, viestiä tapahtumasta kaikille sidosryhmille ja vähentää ennakoivasti tulevia vaikutuksia. Tämä malli koskee koko OT:n henkilöstöä sekä verkkoja, järjestelmiä ja dataa.

Ilman tämänlaista mallia organisaation on erittäin vaikea reagoida tietoturvahäiriön sattuessa. Malliin sisältyvät henkilöstön roolit ja vastuut, poikkeamien torjuntatyönkulku, tapahtumatyypin ja vakavuuden luokittelu, kriittisten henkilöiden yhteystiedot jotka tulisi ottaa mukaan, ulkopuolisten tahojen yhteystiedot jotka voivat olla hyödyllisiä reagointimallin avustamisessa, tiedonjakopolitiikassa sekä sisäisessä että ulkoisessa viestinnässä (NIST, 2023, s. 41–42).

5.4.9 Palautumis- ja palautuskyvyn kehitys

Organisaation tulee kehittää valmiudet toipua tietoturvahäiriöistä ja palauttaa tietoturvahäiriön vaikuttamat toiminnot ja palvelut tietoturvahäiriötä edeltävään tilaan. Tämä valmius sisältää yleisesti seuraavat tehtävät:

- Määritä häiriöstä toipumisen palautumistavoitteet. Esimerkiksi palautumiskyvyn tulee asettaa etusijalle ihmisten turvallisuus ja ympäristöturvallisuus ennen tietoturvaloukkauksen heikentämän OT-toiminnan uudelleenkäynnistämistä.
- Määritä työalueen onnettomuuspalautussuunnitelma ja liiketoiminnan jatkuvuussuunnitelma, jotta organisaatio voi valmistautua reagoimaan asianmukaisesti tietoturvahäiriön aiheuttamiin toimintahäiriöihin.
- Määritä varmuuskopiojärjestelmät ja -prosessit varmuuskopioimaan asiaankuuluvien OT-järjestelmien tila, tiedot, määritystiedot ja ohjelmat säännöllisin väliajoin.
- Määritä palautusprosessit ja -menettelyt, jotka suoritetaan tietoturvahäiriöiden vaikutuksen alaisten OT-toimintojen, laitteiden ja palvelujen palauttamiseksi.
- Määritä viestintäsuunnitelmat palautustoimien koordinoimiseksi sisäisten ja ulkoisten sidosryhmien ja johtoryhmän kanssa.
- Määritä viestintäsuunnitelma julkista suhdetoimintaa varten.
- Testaa toimintasuunnitelma kohtuullisin väliajoin.
  (NIST, 2023, s. 42–43).

5.5 Tietoturvastandardit ja -direktiivit

Tietoturvastrategian vahvistamiseksi on mahdollista ottaa käyttöön esimerkiksi ISO 27001 tai ISA 62443 standardit. Euroopan unioni osittain määrittelee kyberturvallisuusdirektiivejä, joihin organisaatioiden tulee sovittaa toimintaansa.

5.5.1 ISO/IEC 27001

ISO/IEC 27001 on maksullinen tietoturvallisuuden standardisarja tietoturvan hallintajärjestelmille. Standardi määrittää vaatimukset, jotka tietoturvan hallintajärjestelmän tulee täyttää. Standardi tarjoaa kaikenkokoisille organisaatioille ohjeistuksen tietoturvan hallintajärjestelmien luomiselle, ylläpidolle sekä jatkuvalle kehitykselle. Jos organisaatiolla on ISO/IEC 27001-sertifikaatti, on organisaatiolla käytössään järjestelmä organisaation käyttämään sekä käsittelemään dataan ja organisaatio kunnioittaa kansainvälisen standardin asettamia parhaiden käytäntöjen ja periaatteiden toimintatapoja (ISO, 2022).

ISO 27001-sertifikaatin hankkiminen ei ole pakollista, mutta lain noudattaminen on. Sertifikaattia ei pakoteta hankkimaan, mutta se on usein helpoin tapa noudattaa lakeja, kuten eurooppalaista yleistä tietosuoja-asetusta (Secureframe, 2024).

ISO 27001(:2022) standardin vaatimukset:

- Systemaattinen tietoturvauhkien, mukaan lukien haavoittuvuuksien ja potentiaalisten vaikutusten tarkastelu.
- Kattavan tietoturvavalvontapaketin suunnittelu ja toteutus.
- Kattavan johtamisprosessin käyttöönotto.
- Jatkuvan tietoturvavalvonnan yhtiön tarpeiden ja turvallisuustavoitteiden mukaisesti.
- Organisaation liiketoimintatarpeiden ja riskien mukaisen tietoturvan hallintajärjestelmän käyttö.
  (IBM, n.d.).

5.5.2 ISA/IEC 62443

ISA 62443 on kansainvälinen teollisuusautomaation, kriittisen infrastruktuurin ja ohjausjärjestelmien tietoturvan standardisarja. Standardiin sisältyy ohjausjärjestelmän muodostavan teknologian lisäksi työprosessit, vastatoimet ja työntekijät. Standardi noudattaa kokonaisvaltaista lähestymistapaa, koska

kaikki riskit eivät perustu pelkkään teknologiaan. Teollisuuden automaatiosta ja ohjausjärjestelmistä vastaavalla henkilöstöllä on oltava tarvittava koulutus, tiedot ja taidot turvallisuuden takaamiseksi (IEC, 2021).

ISA 62443 on jaettu neljään pääkategoriaan, jokainen kategoria keskittyy tietoturvan eri aspekteihin.

IEC 62443-1 on yleinen johdanto, joka määrittelee ydinterminologian, käsitteet ja mallit sekä hahmottelee standardinmukaisuusmittareita, jotka koskevat kaikkia osapuolia.

IEC 62443-2 keskittyy teollisuuden automaation ja hallinnan järjestelmien turvallisuuden metodeihin ja prosesseihin. Opastaa tehokkaan tietoturvaohjelman laatimiseen käytäntöjen, menettelyiden ja johtamiskäytäntöjen avulla. Määrittelee tietoturvan hallintajärjestelmien vaatimukset loppukäyttäjälle ja laiteomistajalle.

IEC 62443-3 käsittelee järjestelmätason turvallisuusvaatimuksia turvallisen teollisuuden automaation ja hallinnan järjestelmien suunnittelussa ja toteuttamisessa. Sisältää myös riskien arvioinnin, järjestelmän suunnittelun ja tietoturvateknologioiden soveltamisen IACS-ympäristöissä.
IEC 62443-4 kuvaa järjestelmän teollisten verkkokomponenttien kehityksen elinkaarivaatimukset, tekniset toimivuus- ja turvallisuusvaatimukset. Varmistaa kehityksestä tuotteen käyttöönottoon jokaisen komponentin tietoturvastandardit (Fortinet, n.d.-e; Industrial Cyber, 2021).

IEC 62443 määrittelee viisi suojaustasoa operatiivisten teknologioiden tietoturva-arkkitehtuurissa. Suojaustasolla 0 ei vaadita erityisiä vaatimuksia tai suojausta. Suojaustasolla 1 on suojaus tahatonta tai vahingossa tapahtuvaa väärinkäyttöä vastaan. Suojaustasolla 2 on suojaus tahallista väärinkäyttöä vastaan yksinkertaisilla keinoilla, joilla on vähän resursseja tai yleisiä taitoja ja alhainen motivaatio. Suojaustasolla 3 on suojaus tahallista väärinkäyttöä vastaan kehittynein keinoin kohtuullisilla resursseilla, IACS-kohtaisella tiedolla ja kohtuullisella motivaatiolla. Suojaustasolla 4 on suojaus tahallista

väärinkäyttöä vastaan kehittyneillä keinoilla, joilla on laajat resurssit, IACS-kohtainen tietämys ja korkea motivaatio (Industrial Cyber, 2021).

Kuva 17 - IEC 62443 suojaustasot (Industrial Cyber, 2021).

5.5.3 NIS2

Network information security directive 2 on Euroopan unionin määrittelemä uusi verkko- ja tietoturvadirektiivi, joka on päivitys aiempaan NIS-direktiiviin vuodelta 2022. Se astui voimaan vuoden 2024 lokakuussa. Direktiivissä määritellään kyberturvallisuuteen sekä siihen liittyvien häiriöiden raportointia koskevia velvollisuuksia. Parsonsin mukaan direktiivi on hyödyllinen varsinkin operatiivisten teknologioiden aloilla (Parsons, 2024). NIS2-direktiivi määrittelee yhteiskunnallisesti kriittiset toimialat ja näihin kuuluvien organisaatioiden on huomioitava uudet vaatimukset. Esimerkiksi organisaatiot, niin pienet kuin suuret, jotka toimivat kriittisen infrastruktuurin parissa joko energia- tai terveysalalla, liikenteessä, julkishallinnossa tai valmistavassa teollisuudessa, kuuluvat tämän direktiivin alaisuuteen (Ikola, 2024; Euroopan parlamentin ja neuvoston direktiivi 2022/2555, 2 art.).

5.6 Operatiivinen teknologia ja NGFW

Perinteisen informaatioteknologian ja operatiivisen teknologian suurimpana erona on OT:n suora yhteys ja vaikutus ulkomaailmaan. OT:n on mahdollista häiritä yhteiskunnan normaalia toimintaa erilaisin keinoin, esimerkiksi erilaisten tuotantojen häiriöt, ympäristövahingot tai henkeen ja terveyteen kohdistuvat uhat, kuten kappaleessa 5.3.4 todetaan. Operatiivisen teknologian käyttöympäristöt saattavat toimia täysin uniikeilla sovelluksilla tai käyttöjärjestelmillä, jotka ovat epätavanomaisia tyypillisille IT-ammattilaisille (Palo Alto Networks, n.d.-e).

Tietotekniikan ja operatiivisen teknologian rajapintojen laajentuessa myös altis hyökkäyspinta laajenee. Yleisin haitallisten toimijoiden hyökkäyssuunta on internetin välityksellä. Monet HMI:t, joilla hallitaan teollisuuden ohjausjärjestelmiä, ovat myös yhteydessä ulkoverkkoon. Jokainen ulkoverkon yhteys on riski, varsinkin jos laitteella on mahdollista hallita ohjausjärjestelmiä (Palo Alto Networks, n.d.-e).

Seuraavan sukupolven palomuuri on hyödyllinen lisäosa operatiivisten teknologioiden turvaamisessa. Yrityksen IT- ja OT-verkot on mahdollista segmentoida sijoittamalla NGFW verkkojen väliin. NGFW:n avulla voidaan sallia yhteys ainoastaan hyväksyttyjen laitteiden välille ja käyttämään vain tiettyjä portteja ja OT:lle tyypillisiä protokollia, esimerkiksi DNP3, Modbus ja Profinet/Profibus. Vaikka haitallinen toimija jostakin syystä pääsisi syöttämään komentoja palomuurin läpi, voi palomuuri tunnistaa komennon poikkeavuudeksi, luokitella sen hyökkäykseksi ja pysäyttää komennon (Palo Alto Networks, 2025c). Palomuurin syväpakettitarkistus ymmärtää OT-protokollia ja tutkii, onko liikenne normaalia vai sisältääkö se poikkeuksia, esimerkiksi vääriä ohjaussignaaleja, väärin muotoiltuja komentoja tai epäilyttäviä ohjelmistopäivityksiä.

6 OMA NÄKEMYS

Yritysten digitaalinen toimintaympäristö on viime vuosina muuttunut yhä monimutkaisemmaksi, erityisesti operatiivisten teknologioiden ja informaatio- ja viestintäteknologian järjestelmien lähentyessä. Organisaation tietoturvapolitiikka muodostaa perustan järjestelmälliselle ja riskitietoiseen toimintatapaan pohjautuvalle kyberturvallisuuden hallinnalle. Nykyaikaisessa liiketoimintaympäristössä IT- ja OT-verkkojen integraatio on laajentanut hyökkäyspintaa, ja samalla asettanut uusia vaatimuksia tietoturvapolitiikan rakenteelle ja käytännön toimeenpanolle, jotta molempien ympäristöjen erityispiirteet ja suojauksen tarpeet huomioidaan. IT-ympäristöjen suojaaminen on perinteisesti perustunut hyvin standardisoituihin suojausratkaisuihin, kuten palomuureihin, käyttöoikeushallintaan ja lokitukseen, kun taas OT-ympäristöissä suojaamisen painopiste on ollut järjestelmän jatkuvuuden ja luotettavuuden varmistamisessa, usein erillään muusta tietoverkosta, kuten kappaleessa 5.3 todetaan.

Yhtenäisen tietoturvapolitiikan laatiminen edellyttää kuitenkin molempien ympäristöjen erityispiirteiden huomioimista sekä teknisellä- että organisaatiotasolla. IT-ympäristöjen tietoturva perustuu pitkälti ohjelmisto- ja päivityshallintaan, monikerroksiseen suojausmalliin ja jatkuvaan valvontaan, kun taas OT-ympäristöjen suojaamisessa korostuu verkkojen segmentointi, laitteistopohjainen turvallisuus ja protokollatason valvonta, kuten kappaleessa 5.4 todetaan.

Osana nykyaikaista tietoturvapolitiikkaa yrityksen tulisi varmistaa, että IT- ja OT-verkkojen välinen liikenne on tarkasti hallittua, ja että käytössä on modernit suojausratkaisut, kuten seuraavan sukupolven palomuurit. NGFW-teknologian avulla voidaan suojautua OT-ympäristöihin kohdistuvilta hyökkäyksiltä myös silloin, kun hyökkäys kulkee sallitun verkkoliikenteen kautta esimerkiksi poikkeuksellisten tai haitallisten komentojen muodossa (Fortinet, 2022; Palo Alto Networks, 2020). Tämänkaltaiset tekniset valmiudet tukevat tietoturvapolitiikan linjauksia, joiden tavoitteena on estää häiriötilanteet,

suojata liiketoiminnalle kriittisiä järjestelmiä ja taata tuotantoprosessien jatkuvuus.

Tietoturvapolitiikan tehokas toimeenpano edellyttää myös selkeää vastuunjakoa IT- ja OT-ympäristöjen hallinnassa, kattavaa henkilöstön koulutusta ja jatkuvaa kyberturvallisuustason arviointia. Lisäksi tietoturvapolitiikassa on tärkeää huomioida OT-järjestelmien pitkä elinkaari ja mahdollinen ohjelmistopäivitysten rajoitteellisuus, mikä lisää tarvetta verkon eristämiseen, syväpakettitarkistukseen ja monitorointiin verkko- ja sovellustasolla, kuten kappaleissa 5.4–5.4.9 todetaan.

6.1 Verkkoarkkitehtuuri ja tietoturvainfrastruktuurin sijoittaminen

Tietoturvainfrastruktuurin suunnittelu lähtee verkkojen ja järjestelmien erottelusta selkeisiin segmentoituihin turvavyöhykkeisiin ja niiden välisiin valvottuihin rajapintoihin. Teollisuusstandardi IEC 62443-3-3 määrittelee, että OT-ympäristöjen tulisi olla jaettu loogisiin ja fyysisiin turvavyöhykkeisiin, joiden välissä liikenne kulkee vain valvottujen yhdyskäytävien ja palomuurien läpi. Tämä rakenne pienentää riskiä, että mahdollinen hyökkäys leviäisi hallitsemattomasti IT-ympäristöstä OT-laitteisiin tai päinvastoin (Cisco, 2024b; IEC, 2021).

Käytännössä tietoturvainfrastruktuurin tulee rakentua seuraavista osista:

- IT- ja OT-verkkojen eriyttäminen. OT-verkkoja ei tule altistaa suoraan internet- tai toimistoverkkojen liikenteelle. Yhteys IT-verkkoon tulee sallia ainoastaan tiettyjen valvottujen ja rajoitettujen porttien ja palveluiden kautta, kuten kappaleessa 5.6 todetaan.
- Seuraavan sukupolven palomuurit. IT- ja OT-verkon välinen rajapinta tulee suojata nykyaikaisella palomuuriratkaisulla, joka kykenee syväpakettitarkistukseen OT-protokollien tasolla. Tämä mahdollistaa hyökkäyskomentojen estämisen ja komentojen väärinkäytön pysäyttämisen, kuten kappaleessa 5.6 todetaan.

- Demilitarisoitu vyöhyke. IT- ja OT-järjestelmien välinen liikenne tulisi ohjata erillisen DMZ-vyöhykkeen kautta jossa tietoliikenne voidaan eristää ja tarkistaa ennen kuin se saavuttaa kriittiset järjestelmät.
- Intrusion detection ja intrusion prevention system. OT-verkkojen sisäistä liikennettä on syytä valvoa IDS- ja IPS-järjestelmillä, jotka on konfiguroitu tunnistamaan OT-protokolliin kohdistuvat poikkeamat ja hyökkäykset kuten kappaleissa 2.2.1, 2.2.2, 3.1 ja 3.2 todetaan.
- Lokitus ja valvonta. Keskitetty lokienhallintajärjestelmä mahdollistaa sekä IT- että OT-ympäristöjen tapahtumatietojen keräämisen ja analysoinnin. Tämä mahdollistaa tietoturvapoikkeamien nopean tunnistamisen ja käsittelyn.

6.2 Tietoturvapolitiikan linjaukset ja käytännön toimeenpano

Yrityksen tietoturvapolitiikassa on tärkeää määritellä selkeästi:

- Vastuunjako: Kuka hallinnoi IT-järjestelmien ja kuka OT-järjestelmien suojausta? Selkeä roolitus vähentää inhimillisiä virheitä ja parantaa kommunikaatiota sekä valvottavuutta, kuten kappaleessa 5.4.1 todetaan (NIST, 2023, s. 38).
- Riskienhallintaprosessi: Molempien ympäristöjen jatkuva riskien arviointi ja politiikan päivittäminen uhkakuvien muuttuessa, kuten kappaleessa 5.4.6 todetaan (NIST, 2023, s. 45).
- Päivitys- ja ylläpitomalli: IT-järjestelmien laite- ja ohjelmistopäivityksiä voidaan toteuttaa säännöllisesti, mutta OT-järjestelmissä päivitykset on testattava huolellisesti ennen tuotantoon vientiä, mikä vaatii erillisen hallintaprosessin, kuten kappaleessa 5.4.7 todetaan (NIST, 2023, s. 41).
- Henkilöstön koulutus ja tietoturvakulttuuri: IT- ja OT-henkilöstölle sekä ulkopuolisille IT- ja OT-ympäristöissä toimiville henkilöille on järjestettävä säännöllistä koulutusta, jossa korostetaan molempien ympäristöjen uhkia ja turvallisuuskäytäntöjä, kuten kappaleessa 5.4.5 todetaan (NIST, 2023, s. 41).

7 YHTEENVETO

Seuraavan sukupolven palomuurit ovat keskeinen osa nykyaikaisten IT- sekä OT-ympäristöjen suojaamisessa koska ne mahdollistavat tietoliikenteen sisällön tarkan tutkimisen, uhkien torjunnan ja väärinkäytösten torjunnan verkko- ja sovellustasolla ilman, että perinteisten laitteiden turvallisuusominaisuuksia tarvitsee muuttaa.

Teollisuuden operatiiviset teknologiat ovat perinteisesti toimineet joko täysin fyysisesti tai eristyksissä tietoverkoista, mutta digitalisaation, etävalvonnan ja -käytön ja Industry 4.0 -ratkaisujen myötä nämä järjestelmät ovat yhä useammin yhteydessä verkkoon ja alttiina nykyaikaisille kyberuhille (NIST, 2023, s. 66–79). Tämän kehityksen seurauksena perinteiset reititystietoihin ja porttipohjaiseen sääntelyyn perustuvat palomuurit eivät tarjoa riittävää suojaa OT-ympäristöissä.

Seuraavan sukupolven palomuurit ovat nykyaikaisia tietoturvaratkaisuja, jotka yhdistävät syväpakettitarkastuksen, sovellustason tunnistuksen sekä tunkeutumisen estojärjestelmän. NGFW-järjestelmät eivät ainoastaan salli tai estä liikennettä portti- ja IP-tasolla, vaan ne kykenevät myös analysoimaan verkkoliikenteen sisällön ja havaitsemaan sovellus- tai protokollatason poikkeavuuksia, mukaan lukien haitalliset tai väärät komennot (Fortinet, 2022).

Operatiivisten teknologioiden ympäristössä tämä mahdollistaa esimerkiksi OT-protokollien, kuten Modbusin, DNP3:n ja Profinetin tarkastelun liikenteen sisältötasolla. NGFW voi tunnistaa ja estää haitalliset komennot, vaikka liikenne kulkisi sallitun portin kautta, kuten esimerkiksi Modbus Write Single Coil -komennon, jolla laite voidaan pysäyttää. Tämä on erityisen tärkeää OT-ympäristöissä, joissa laitteet ovat usein jopa kymmeniä vuosia vanhoja, päivittämättömiä ja suojautumiskyvyltään rajoittuneita (Palo Alto Networks, 2020).

Seuraavan sukupolven palomuurit tukevat OT-verkkojen suojaamista myös verkkoarkkitehtuurin tasolla mahdollistamalla verkon segmentoinnin IT- ja OT-verkkojen välillä, joka rajoittaa haitallisten toimijoiden liikkumisen järjestelmässä. Näin ollen seuraavan sukupolven palomuurit ovat olennainen osa nykyaikaisen OT-ympäristön kyberturvallisuusarkkitehtuuria.

LÄHTEET

Ashtari, H. (21.3.2022). Intrusion Detection System vs. Intrusion Prevention System: Key differences and similarities. Spiceworks. https://www.spiceworks.com/it-security/network-security/articles/ids-vs-ips/

Beach-Westmoreland, N., Styczynski, J. (2016). When the lights went out. Booz-Allen. Haettu 25.3.2025 osoitteesta https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Brook, C. (20.3.2018). What is Deep Packet Inspection? (And how it really works). Digital Guardian. https://www.digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more

Buchanan, I. (n.d.). Containers vs. virtual machines. Atlassian. Haettu 19.3.2025 osoitteesta https://www.atlassian.com/microservices/cloud-computing/containers-vs-vms

Carr, J. (29.9.2010). Did The Stuxnet Worm Kill India's INSAT-4B Satellite? Forbes. https://www.forbes.com/sites/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/

Checkpoint. (16.6.2023). What is a Stateless Firewall? https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-a-stateless-firewall/

Cisco. (12.9.2023). Cisco Firepower 4100 Series Data Sheet https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html

Cisco. (1.10.2024a). What is OT security? https://www.cisco.com/site/us/en/learn/topics/security/what-is-ot-security.html

Cisco. (16.8.2024b). ISA/IEC-62443-3-3: What is it and how to comply? https://www.cisco.com/c/en/us/products/collateral/security/isaiec-62443-3-3-wp.html

Einorytė, A. (22.3.2024). IP fragmentation attack: Definition, types, and prevention. NordVPN. https://nordvpn.com/fi/blog/ip-fragmentation-attack/

ESET Endpoint security. (30.4.2024). Host-based intrusion prevention system. https://help.eset.com/ees/10.1/fi-FI/idh_hips_main.html

Euroopan parlamentin ja neuvoston direktiivi 2022/2555/EU, annettu 14 päivänä joulukuuta 2022, toimenpiteistä korkean yhteisen kyberturvallisuuden saavuttamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 (NIS2-direktiivi) kumoamisesta ETA:n kannalta merkityksellinen teksti. EUVL L 333, 27.12.2022, s. 2–5. https://eur-lex.europa.eu/eli/dir/2022/2555

F-Secure. (16.11.2022). Mikä on palomuuri? https://www.f-secure.com/fi/articles/firewall

ForcePoint. (21.1.2019). What is an Intrusion Prevention System? https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips

Fortinet. (n.d.-a). What is Unified Threat Management? Haettu 28.2.2025 osoitteesta https://www.fortinet.com/resources/cyberglossary/unified-threat-management

Fortinet. (n.d.-b). DMZ Networks. Haettu 16.4.2025 osoitteesta https://www.fortinet.com/resources/cyberglossary/what-is-dmz

Fortinet. (n.d.-c). What is Sandboxing? Haettu 28.2.2025 osoitteesta https://www.fortinet.com/resources/cyberglossary/what-is-sandboxing

Fortinet. (n.d.-d). What is OT security? Haettu 20.3.2025 osoitteesta https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security

Fortinet. (n.d.-e). IEC 62443 Standard. Haettu 1.4.2025 osoitteesta https://www.fortinet.com/resources/cyberglossary/iec-62443

Fortinet. (15.4.2022). Advanced Threat Protection for Industrial Control Systems and Operational Technology. https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-advanced-threat-protection-industrial-control-systems-ot.pdf

Hagerty, M. (4.12.2023). The Pros and Cons of Next Gen Firewalls. Intellect Information Technology. https://www.intellectit.com.au/pros-and-cons-next-gen-firewalls/

Hyppönen, M. (3.8.2022). If It's Smart, It's Vulnerable. John Wiley & Sons, Incorporated. ISBN 9781119895183

IBM. (n.d.). International Business Machines Corporation. What is ISO 27001? Haettu 31.3.2025 osoitteesta https://www.ibm.com/cloud/compliance/iso-27001

IBM. (19.4.2023). International Business Machines Corporation. What is an intrusion detection system? https://www.ibm.com/think/topics/intrusion-detection-system

IEC. (26.2.2021). Internal Electrotechnical Commission. Understanding IEC 62443. https://www.iec.ch/blog/understanding-iec-62443

Ikola J. (10.4.2024). NIS2-direktiivi tiukentaa kyberturvallisuuden hallintaa – onko organisaatiosi valmis? Pinja. https://blog.pinja.com/fi/nis2-direktiivi-tiukentaa-kyberturvallisuuden-hallintaa

Industrial Cyber. (26.12.2021). The Essential Guide to the IEC 62443 industrial cybersecurity standards. https://industrialcyber.co/features/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/

Institute of Electrical and Electronics Engineers Spectrum. (26.2.2013). The real story of Stuxnet. https://spectrum.ieee.org/the-real-story-of-stuxnet

Integrated Research. (n.d.). Deep Packet Inspection: How it works and why it's important. Haettu 28.2.2025 osoitteesta https://www.ir.com/guides/deep-packet-inspection

International Organization for Standardization. (2022). ISO/IEC 27001:2022. https://www.iso.org/standard/27001

IT Price. (2025). Cisco GPL 2025. https://itprice.com/cisco-gpl/firepower

Kaspersky. (13.9.2017). What is unified threat management? https://www.kaspersky.com/resource-center/definitions/utm

LearnCisco. (1.10.2023). Understanding the TCP/IP transport layer https://www.learncisco.net/courses/icnd-1/building-a-network/tcpip-transport-layer.html

Liu, A., Gouda, M. (29.7.2008). Diverse Firewall Design. Institute of Electrical and Electronics Engineers. 19 (91). 1. https://doi.org/10.1109/TPDS.2007.70802

Liu, A. (2010). Firewall Design and Analysis. Hackensack, N.J.: World Scientific. https://doi.org/10.1142/7229

Microsoft. (22.1.2025). Windows and containers. LearnMicrosoft. https://learn.microsoft.com/en-us/virtualization/windowscontainers/about/

Miller, L. (2011). Next-Generation Firewalls for Dummies. Wiley Publishing, Incorporated. ISBN 978-0-470-93955-0

NIST. (28.9.2023). National Institute of Standards and Technology. Guide to Operation Technology Security. https://doi.org/10.6028/NIST.SP.800-82r3

Nurmi, S. (2021). Seuraavan sukupolven palomuurit. [AMK-opinnäytetyö, Satakunnan ammattikorkeakoulu]. Theseus. https://urn.fi/URN:NBN:fi:amk-202102192477

Okta. (1.9.2024). What is Deep Packet Inspection? Definition & Usage. https://www.okta.com/identity-101/deep-packet-inspection/

Palit, D. (6.11.2024). Cybersecurity Today: Cyber Attacks, Network Security, and Threat Prevention. BPB Publications. ISBN: 9789365893755

Palo Alto Networks. (n.d.-a). What is network security management? Haettu 28.2.2025 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-network-security-management

Palo Alto Networks. (n.d.-b). What is a packet filtering firewall? Haettu 4.3.2025 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-a-packet-filtering-firewall

Palo Alto Networks. (n.d.-c). What is a stateful firewall? Haettu 3.3.2025 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-a-stateful-firewall

Palo Alto Networks. (n.d.-d). What is a container firewall? Haettu 19.3.2025 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-a-container-firewall

Palo Alto Networks. (n.d.-e). What is OT security? Haettu 21.3.2025 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-ot-security

Palo Alto Networks. (3.8.2020). Security Reference Blueprint for Industrial Control Systems. https://www.paloaltonetworks.com/resources/whitepapers/industrial-control-blueprint-reference

Palo Alto Networks. (26.2.2025a). Next-Generation Firewall Docs: App-ID Overview. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/app-id/app-id-overview

Palo Alto Networks. (26.2.2025b). Next-Generation Firewall Docs: User-ID Overview. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-overview

Palo Alto Networks. (5.2.2025c). Next-Generation Firewall Docs: Forecasting and Anomaly Detection. https://docs.paloaltonetworks.com/ngfw/incidents-and-alerts/alerts/forecasting-and-anomaly-detection-ngfw

Panetta, K. (10.10.2019). Is the cloud secure? Gartner. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

Parkki, J. (2019). Palo Alto PA5060 palomuurin ominaisuudet ja käyttöönotto. [AMK-opinnäytetyö, Tampereen ammattikorkeakoulu]. Theseus. https://urn.fi/URN:NBN:fi:amk-201905067715

Parsons, D. (18.6.2024). NIS2 Compliance for OT: Strategic Implementations of ICS Controls. Sans. https://www.sans.org/blog/nis2-compliance-for-ot-strategic-implementation-of-ics-controls/

Rantapelkonen, J. & Salminen, M. (2013). The Fog of Cyber Defence. Maanpuolustuskorkeakoulu. http://urn.fi/URN:ISBN:978-951-25-2431-0

Roukka, J. (2015). Seuraavan sukupolven palomuuri. [AMK-opinnäytetyö, Satakunnan ammattikorkeakoulu]. Theseus. https://urn.fi/URN:NBN:fi:amk-2015112217125

SAP. (n.d.). What is the Industrial Internet of Things? Haettu 24.3.2025 osoitteesta https://www.sap.com/products/scm/industry-4-0/what-is-iiot.html

Secureframe. (27.7.2024). What is ISO 27001 Certification? https://secureframe.com/hub/iso-27001/what-is-iso-27001

Suehring, S. (29.1.2015). Linux Firewalls: Enhancing Security with nftables and Beyond (4). Packet-Filtering Concepts in Linux Firewalls. Addison-Wesley Professional. ISBN 9780134000022

Trendmicro. (n.d.-a). Industrial Control System. Haettu 21.3.2025 osoitteesta https://www.trendmicro.com/vinfo/fi/security/definition/industrial-control-system

Trendmicro. (n.d.-b). Industrial Internet of Things. Haettu 24.3.2025 osoitteesta https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot

Tuomaala, J. (2018). Seuraavan sukupolven palomuurin valinta. [AMK-opinnäytetyö, Lahden ammattikorkeakoulu]. Theseus. https://urn.fi/URN:NBN:fi:amk-2018082814696

Wilkins, S. (9.1.2013). Stateful Firewall Fundamentals. Pluralsight. https://www.pluralsight.com/blog/it-ops/stateful-firewall-fundamentals

Xiaoyun, C. (27.7.2023). What is UTM? Huawei IP Encyclopedia. https://info.support.huawei.com/info-finder/encyclopedia/en/UTM.html

Zenarmor. (20.6.2024). What is a DMZ (Demilitarized Zone) Network? https://www.zenarmor.com/docs/network-security-tutorials/what-is-dmz

LIITE 1: CISCO FIREPOWER 4100-SARJAN OHJELMISTOJEN EROJA (CISCO, 2023).

Features	4112	4115	4125
Throughput: FW + AVC (1024B)	19 Gbps	33 Gbps	45 Gbps
Throughput: FW + AVC + IPS (1024B)	19 Gbps	33 Gbps	45 Gbps
Maximum concurrent sessions, with AVC	10 million	15 million	25 million
Maximum new connections per second, with AVC	98K	210K	269K
TLS (Hardware Decryption)[1]	4.5 Gbps	6.5 Gbps	8.5 Gbps
Throughput: NGIPS (1024B)	19 Gbps	33 Gbps	45 Gbps
IPSec VPN Throughput (1024B TCP w/ Fastpath)	8.5 Gbps	12.5 Gbps	19 Gbps
Maximum VPN Peers	10,000	15,000	20,000

LIITE 2: CISCO FIREPOWER 4100-SERIES DATASHEET (CISCO, 2023)

Features		4112	4115	4125	4145
Dimensions (H x W x D)		1.75 x 16.89 x 29.7 in. (4.4 x 42.9 x 75.4 cm)			
Form factor (rack units)		1RU			
Supervisor		Cisco Secure Firewall 4000 Supervisor with 8 x 10 Gigabit Ethernet ports and 2 Network Module (NM) slots for I/O expansion			

Network modules		• 2 x 100 Gigabit Ethernet QSFP28 Network Module
		• 8 x 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) network modules
		  ◦ 8 x 1 Gbps Fiber or 4 x 1Gbps Copper SFP Network Module
		• 4 x 40 Gigabit Ethernet Quad SFP+ network modules
		• 8-port 1Gbps copper, FTW (fail to wire) Network Module
		  ◦ Ports that are not configured as FTW can be used as regular 1 Gb copper ports
		• 6-port 1 Gbps SX Fiber FTW (fail to wire) Network Module
		• 6-port 10Gbps SR Fiber FTW (fail to wire) Network Module
		• 6-port 10Gbps LR Fiber FTW (fail to wire) Network Module
		• 2-port 40G SR FTW (fail to wire) Network Module
		• 2-port 100Gbps Network Module			

Maximum number of interfaces		Up to 4 x 100 Gigabit Ethernet (QSFP28) interfaces, 24 x 10 Gigabit Ethernet (SFP+) interfaces; up to 8 x 40 Gigabit Ethernet (QSFP+) interfaces with 2 network modules; up to 24 x 1 Gigabit Ethernet ports(SFP) with network modules and fixed ports			
Integrated network management ports		1 Gigabit Ethernet SFP port Supports 1Gbps fiber or copper optical modules			
Serial port		1 x RJ-45 console			
USB		1 x USB 2.0			
Storage		400 GB	400 GB	800 GB	800 GB
Power supplies	Configuration	Single 1100W AC, dual optional. Single/ dual 950W DC optional[1, 2]	Single 1100W AC, dual optional. Single/ dual 950W DC optional[1, 2]	Dual 1100W AC[1]	Dual 1100W AC[1]
	AC input voltage	100 to 240V AC			
	AC maximum input current	13A			
Fans		6 hot-swappable fans			
Noise		Typical 63 dBA, max is 74 dBA			
Rack mountable		Yes, mount rails included (4-post EIA-310-D rack)			
Weight		4112/4115/4125/4145: 39.4 lb (17.87 kg) 2 x power supplies, 2 x NMs, 6 x fans; 31.4 lb (14.24 kg) no power supplies, no NMs, no fans			

[1] **Dual power supplies are hot-swappable.**