HAMK
Hämeen ammatti-
korkeakoulu

Hyökkäyspintojen minimointi ja uhkien havainnointi verkossa

Toteutusmalli koti- ja pienyrityksen tietoverkon suojaamiseen

Ammattikorkeakoulututkinnon opinnäytetyö
Tieto- ja viestintätekniikka, Insinööri (AMK)
Syksy, 2025
Aleksi Bovellan

HAMK
Hämeen ammatti-
korkeakoulu

Tiivistelmä

Koulutus	Tieto- ja viestintätekniikan koulutus	Vuosi 2025
Tekijä	Aleksi Bovellan	
Työn nimi	Hyökkäyspintojen minimointi ja uhkien havainnointi verkossa: Toteutusmalli koti- ja pienyrityksen tietoverkon suojaamiseen	
Ohjaaja	Teemu Järvenpää	

Tämän opinnäytetyön tavoitteena oli kehittää käytännönläheinen ja kustannustehokas tietoturvamalli sovellettavaksi koti- ja pienyritysten (SoHo) tietoverkkojen turvallisuuden parantamiseksi. Työssä tarkasteltiin verkkojen ja tietoturvan perusteita, keskeisiä uhkamalleja sekä ratkaisuja, joiden avulla voidaan minimoida hyökkäyspintoja, havaita uhkia reaaliaikaisesti, ja myös torjua niitä.

Teoreettisessa osuudessa käsiteltiin muun muassa IP- ja MAC-osoitteita, verkkoprotokollia, VPN-teknologioita, salausmenetelmiä ja ajankohtaisia verkkouhkia. Käytännön toteutus perustui omaan testiverkkoon, jossa hyödynnettiin avoimen lähdekoodin ratkaisuja: OPNsense-palomuuri CrowdSec-lisäosalla, Suricata IDS/IPS, sekä Wazuh SIEM.

Tuloksena syntyi dokumentoitu malli, jota voidaan hyödyntää kotien ja pienyritysten tietoturvan kehittämisessä myös ilman syvää teknistä osaamista. Toteutus osoitti, että useilla ilmaisilla ohjelmistoilla voidaan saavuttaa korkeatasoinen suojaus. Testien perusteella suojauskerrosten yhteisvaikutus – verkkosegmentointi, uhkatunnistus, salaus ja kirjautumisen valvonta – muodosti tehokkaan puolustusratkaisun.

Avainsanat	Verkko, tietoturva, uhka, salaus, suojaus
Sivut	31 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Abstract

Information and Communication Technology Year 2025
Author Aleksi Bovellan
Subject Minimizing Attack Surface and Detecting Threats in a Network: An Implementation Model for Securing Home and Small Business Networks
Supervisor Teemu Järvenpää

The objective of this thesis was to develop a practical and cost-effective cybersecurity model for small office and home (SoHo) environments. The study explored fundamental networking and security concepts, common threat models, and technical solutions that help reduce attack surfaces, detect threats in real-time, and block them.

The theoretical section examines topics such as IP and MAC addressing, network protocols, VPN technologies, encryption mechanisms, and modern cyber threats. The practical implementation was carried out in a test environment using open-source tools, including OPNsense firewall with CrowdSec module, Suricata IDS/IPS, and Wazuh SIEM.

The outcome was a documented and applicable security model that is suitable for both home users and small businesses, even without deep technical expertise. The results demonstrated that an effective level of protection can be achieved with open-source free software and affordable hardware. Layered defense through segmentation, threat detection, encryption, and credential monitoring proved both feasible and robust.

Keywords Network, security, threat, encryption, protection
Pages 31 pages

Sisällys

Kuvat

1 Johdanto

Tietoverkkojen käyttö on levinnyt lähes kaikkiin elämän osa-alueisiin. Melkein jokaisella kotitaloudella ja pienyrityksellä on nykyään jonkinlainen verkkoinfrastruktuuri, jossa toimii useita päätelaitteita – tietokoneita, puhelimia, IoT-laitteita tai etätyöhön tarvittavia palvelimia. Tämän kehityksen rinnalla on kasvanut myös tarve ymmärtää ja hallita verkkoturvallisuutta: kodit ja pienetkin verkot voivat olla alttiita hyökkäyksille, eikä tekninen suojaus ole enää vain suuryritysten etuoikeus.

Tämän opinnäytetyön tavoitteena oli kehittää käytännöllinen, kustannustehokas ja teknisesti pätevä tietoturvamalli erityisesti koti- ja SoHo-ympäristöihin (Small Office / Home Office). Malli yhdistää teoreettisen taustan ja käytännön toteutuksen muodostaen helposti ymmärrettävän mutta vahvasti suojatun arkkitehtuurin, jota voidaan soveltaa eri ympäristöihin. Työ perustuu omaan testiverkkoon ja edullisiin sekä avoimen lähdekoodin ohjelmistoihin.

Rakenteellisesti opinnäytetyö alkaa verkkojen ja protokollien perusteista, etenee uhkakuvien ja riskien arviointiin, esittelee käytetyt tekniset ratkaisut, ja päättyy käytännön sovellukseen sekä johtopäätöksiin.

Tutkimuskysymykset:

- Miten koti- ja pienyritysverkon hyökkäyspintaa voidaan tehokkaimmin minimoida edullisilla ja avoimen lähdekoodin tietoturvaratkaisuilla?
- Kuinka avoimen lähdekoodin IDS/IPS- ja SIEM-järjestelmillä voidaan havaita ja torjua verkkouhkia koti- ja SoHo-ympäristössä reaaliaikaisesti?
- Miten monikerroksisella arkkitehtuurilla voidaan parantaa koti- ja SoHo-verkkojen tietoturvaa ilman merkittäviä kustannuksia tai syvää teknistä osaamista?

2 Tietoliikenteen perusteet

Tässä luvussa luodaan opinnäytetyön teoreettinen perusta tarkastelemalla, miten data kulkee verkossa ja missä kohdissa siihen voidaan vaikuttaa turvallisuutta parantaen.

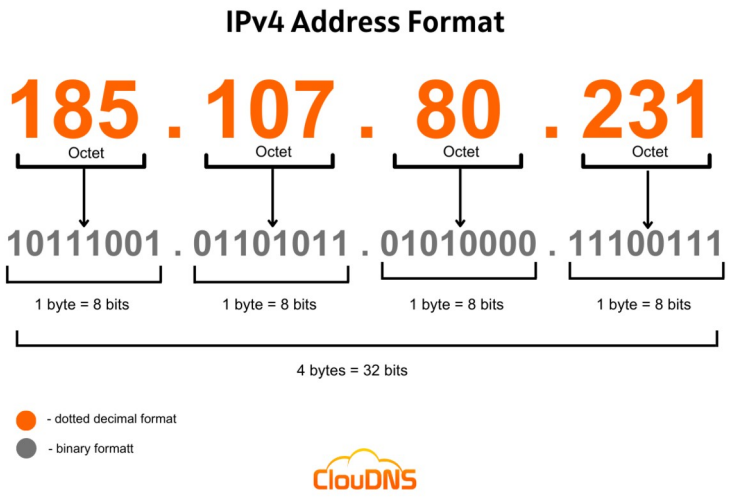
Aluksi käsitellään laitteiden yksilöinnissä käytettävät osoitteistot sekä verkkokerroksen ja kuljetuskerroksen toiminta; sen jälkeen siirrytään kerrosmalleihin ja segmentointiin. Kun nämä perusmekanismit ovat selvillä, myöhemmissä luvuissa esiteltävät uhkamallit ja suojausratkaisut asettuvat oikeaan kontekstiin.

2.1 IP- ja MAC-osoitteet

Verkkolaitteiden yksilöinti perustuu kahteen keskeiseen osoitetyyppiin: IP- ja MAC-osoitteisiin.

IPv4-osoitteet, jotka koostuvat neljästä 8-bittisestä tavusta (esim. 192.168.0.1), tarjoavat noin 4,3 miljardia eri mahdollisuutta. IPv4-osoitteen rakenne on havainnollistettu kuvassa 1. Väistämätön IPv4-osoitepula realisoitui vasta noin vuonna 2011, jolloin RIR-verkostoissa (mm. ARIN, RIPE) alettiin lähestyä osoitereservien loppumista IPv4-osoitteiden jakoprosessissa. Tästä syystä NAT (Network Address Translation) otettiin käyttöön yhdistämään sisäverkon laitteita yhden julkisen osoitteen taakse, mikä pienensi suoraan verkkoon näkyvien osoitteiden tarvetta.

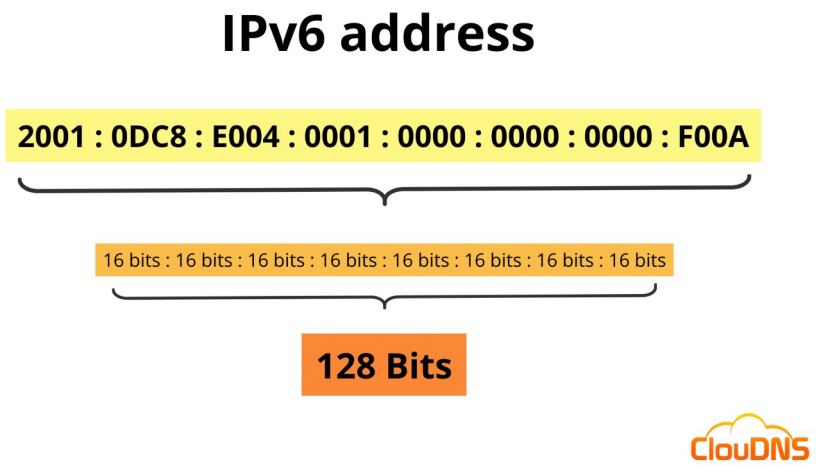
Kuva 1. IPv4-osoitteen esitystavat piste-desimaali- ja binäärimuodossa (CloudNS, 2025).



IPv6, 128-bittinen osoiterakenne (esim. 2001:0db8:85a3::8a2e:0370:7334) tarjoaa lähes rajattoman osoiteavaruuden ja palauttaa IP:n alkuperäisen end-to-end-periaatteen, parantaen myös reitityksen tehokkuutta ja turvallisuutta

(Deering & Hinden, 2017; Postel, 1981; Plummer, 1982). IPv6-osoitteen rakenne osoitetaan kuvassa 2.

Kuva 2. IPv6-osoitteen muodostuminen piste-desimaali- ja binäärimuodossa (CloudNS, 2025).



MAC-osoite, tai Media Access Control -tunniste, on verkkokortin pysyvä tunnisteformaatti, joka esitetään kuutena heksadesimaaliparina (esim. 00:1A:2B:3C:4D:5E). Koska MAC-osoite voidaan spoofata ohjelmallisesti (esim. Linux-työkaluilla), siihen ei tule turvautua luotettavana autentikointimuotona (MAC-suodatus ei yksin riitä).

2.2 TCP-, UDP- ja porttirakenne

TCP ja UDP toimivat kuljetuskerroksella (transport layer).

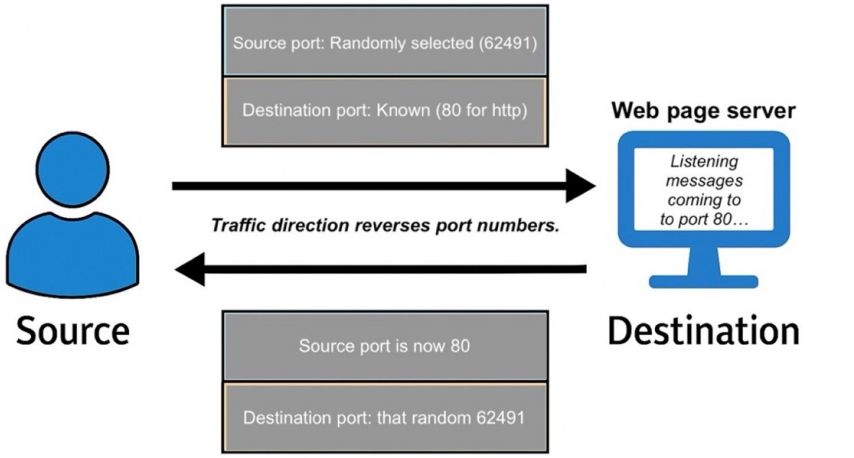
TCP käyttää kolmivaiheista SYN–SYN/ACK–ACK -kättelyä varmistamaan yhteyden luotettavan datansiirron (sisältäen järjestysnumeron, kuittaukset ja virhetarkistuksen). Yhteyden sulkeminen tapahtuu nelivaiheisella FIN/ACK-sekvenssillä, mikä mahdollistaa ennakoidun ja puhtaan sulkemisen yhteydelle.

UDP on yhteydetön ja kevyempi protokolla, jota käytetään sovelluksissa, joissa viive on kriittinen, kuten VoIP, striimaus tai DNS. UDP ei tue uudelleenlähetystä eikä

varmennusta, joten se on toimintavarma vain tilanteissa, joissa datan katoaminen on hyväksyttävää (Postel, 1980).

Kun client-pääty aloittaa yhteydenoton toiseen laitteeseen, sen käyttöjärjestelmä varaa ensin satunnaisen portin itseltään lähettäjän numeroksi (esim. 62491), ja käyttää vastaanottajan portin numerona ennalta tunnettua palvelinporttia (esim. 80 HTTP), kuten kuvassa 3 esitetään. Paluuliikenteessä taas portit vaihtuvat vastakkaisiksi, mikä mahdollistaa yhteyden ja vastauksien kohdentamisen takaisin alkuperäiseen laitteeseen ja prosessiin.

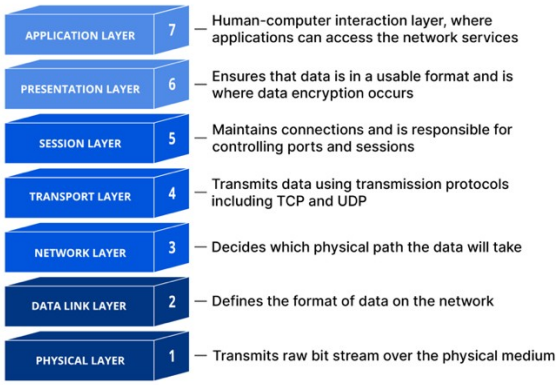
Kuva 3. Porttien valikoituminen ja liikenteen kulku.



2.3 OSI-malli ja TCP/IP-kerrokset

OSI-malli, kuvassa 4, jäsentää tietoverkon seitsemäksi eri kerrokseksi, joista tämän opinnäytetyön kannalta tärkeimmät ovat linkkikerros (link layer 2, MAC), verkkokerros (network layer 3, IP), kuljetuskerros (transport layer 4, TCP/UDP) ja sovelluskerros (application layer 7, esim. HTTP, DNS) (ISO/IEC, 1994).

Kuva 4. OSI-kerrosmalli (Cloudflare, 2025).



Tämä kerrosjako auttaa ymmärtämään, missä kohtaa järjestelmässä tietoturvariskejä voi esiintyä, jolloin niitä vastaan voidaan reagoida tehokkaammin.

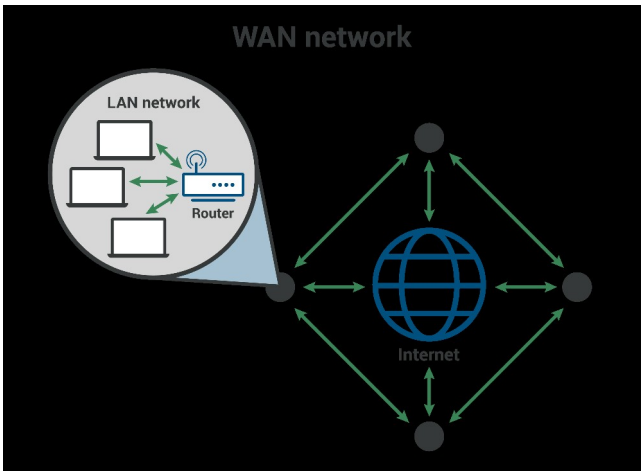
Hyökkäykset voivat kohdistua esimerkiksi:

- Sovelluskerrokseen (application layer, phishing)
- Kuljetuskerrokseen (transport layer, TCP-manipulointi)
- Verkkokerrokseen (network layer, IP-spoofing)
- Linkkikerrokseen (link layer, ARP poisoning)
- Fyysiseen kerrokseen (physical layer, USB-tikut, WIFI)

2.4 Verkkolaitteet ja segmentointi

Verkon hallintaan tarvitaan laitteita kuten kytkin (switch) lähiverkon sisäiseen liikenteen eristämiseen ja MAC-osoiteperusteiseen reititykseen, sekä reititin (router), joka yhdistää eri verkkoja ja vastaa IP-reitityksestä (Cisco Systems, 2018; IEEE, 2018). Internet koostuu käytännössä useista pienemmistä lähiverkoista, kuten kuvassa 5 on visualisoitu.

Kuva 5. Verkkorakenne tyypillisessä pienverkossa (Cloudflare, 2025).



Palomuuri yhdistetään tavallisesti reitittimen rinnalle tai sisäverkon rajapintaan, mikä mahdollistaa sääntöpohjaisen liikenteen suodatuksen, esim. OPNsense ja pfSense.

3 Uhat ja riskit

Tietoverkkojen turvallisuudessa uhkien ymmärtäminen on keskeinen osa kokonaisvaltaista suojaussuunnitelmaa. Hyökkäykset voivat kohdistua eri OSI-kerroksille, tapahtua sisältä tai ulkoa käsin, ja ne voivat olla passiivisia tai aktiivisia. Etenkin SoHo-ympäristöissä, joissa resurssit ja asiantuntemus ovat rajalliset, riskit voivat konkretisoitua nopeasti.

3.1 Verkkohyökkäysten tyypit

Tyypilliset hyökkäysmuodot voidaan jakaa karkeasti seuraaviin luokkiin:

- Palvelunestohyökkäykset (DoS/DDoS): Tarkoituksena on ylikuormittaa järjestelmä niin, ettei se pysty palvelemaan laillisia käyttäjiä.
- Man-in-the-middle (MitM): Hyökkääjä sieppaa ja mahdollisesti muokkaa kahden osapuolen välistä liikennettä.
- Porttiskannaus: Automaattinen menetelmä, jolla etsitään avoimia portteja ja niihin liittyviä palveluja mahdollisia haavoittuvuuksia varten.
- Haitalliset tiedostot, linkit ja web-sivustot: Hyökkääjä pyrkii saamaan uhrin käynnistämään haittaohjelman itse, jolloin ohjelma voi toimia vapaammin.

- Phishing ja spear-phishing: Sosiaaliseen manipulointiin perustuvat hyökkäykset, joilla yritetään saada käyttäjältä arkaluontoista tietoa.

Yhä useammin hyökkäykset ovat osa laajempaa automatisoitua infrastruktuuria, kuten botnetteja, joissa satoja tai tuhansia kaapattuja päätelaitteita käytetään koordinoituun toimintaan, kuten DDoS-hyökkäyksiin tai tietomurtoihin (Cybersecurity and Infrastructure Security Agency [CISA], 2021; European Union Agency for Cybersecurity [ENISA], 2024). SoHo-laitteet ovat usein kohteena, koska ne ovat harvoin asianmukaisesti päivitettyjä tai suojattuja (Symantec, 2018).

3.2 Protokollatason hyökkäykset

Useat hyökkäykset käyttävät hyväkseen TCP/IP-protokollan piirteitä.

Esimerkiksi TCP:n kolmitiemallin (3-way handshake) manipulointi voi mahdollistaa SYN flood -tyyppisen DoS-hyökkäyksen, jossa palvelin varaa resursseja yhteyksille, joita ei koskaan viimeistellä.

Samoin ARP spoofing voi ohjata liikennettä väärälle laitteelle lähiverkossa. Tämä mahdollistaa mm. liikenteen kuuntelun tai väärentämisen. Tällaiset hyökkäykset voivat olla erityisen tuhoisia, jos IDS/IPS-järjestelmää ei ole käytössä.

3.3 Valtiolliset uhkatoimijat ja APT-ryhmät

Advanced Persistent Threat (APT) -toimijat edustavat pitkäkestoisia ja kohdistettuja hyökkäyksiä, joissa tavoitteena on yleensä vakoilu, sabotaasi tai infrastruktuurin valvonta. Näissä tapauksissa käytetään useita eri hyökkäyskerroksia:

- Sosiaalinen manipulointi
- Haittaohjelmat
- Nollapäivän haavoittuvuudet (zero-day)

Tällaiset uhkat voivat kohdistua myös SoHo-ympäristöihin, esimerkiksi kun laite kytketään organisaation VPN-verkkoon tai pilvipalveluun. Kotiverkko voi silloin toimia

“heikkona lenkkinä”, jota pitkin voidaan murtautua organisaation sisäverkkoon (Cyberscoop, 2019).

4 Ratkaisut ja suojaustekniikat

Tietoverkkojen turvallisuuteen tähtäävässä työssä keskeistä on uhkien ennaltaehkäisy, havainnointi ja reagointi. Tämä kokonaisuus rakentuu useista eri teknisistä ja hallinnollisista suojaustasoista. SoHo-ympäristössä tehokas turvarakenne voidaan saavuttaa kustannustehokkaasti yhdistämällä edullisia ja avoimen lähdekoodin ratkaisuja sekä harkittua segmentointia.

Vaikka palomuurit ja IDS/IPS-järjestelmät valvovat verkkoliikennettä, laitteiden suojaukseen tarvitaan lisäksi ohjelmistopäivityksiä ja perinteisiä haittaohjelmien torjuntaohjelmia (antivirus). Ne toimivat tyypillisesti allekirjoituspohjaisesti vertaamalla tiedostoja ja prosesseja tunnettuun haittaohjelmatietokantaan. Useimmat moderneista antivirus-ohjelmista hyödyntävät myös heuristiikkaa ja koneoppimista tunnistaakseen uusia haittakoodeja. Suositeltavia torjuntaohjelmia ovat esimerkiksi Norton 360, AVG, BitDefender, Malwarebytes tai Windows Defender, jotka täydentävät SoHo-verkkojen tietoturvaa päätelaitetasolla.

4.1 Ohjelmistopäivitykset

Ohjelmistopäivitysten viivästyminen tai puuttuminen sähköisissä laitteissa muodostaa merkittävän haavoittuvuuden verkoille ja päätelaitteille. Julkaistuja päivityksiä ei usein asenneta välittömästi, jolloin järjestelmä jää alttiiksi tunnetuille haavoittuvuuksille – erityisesti niin kutsutuille nollapäivähaavoittuvuuksille (zero-day), joita rikolliset voivat hyödyntää ennen kuin korjaus on edes saatavilla.

Hyökkääjät käyttävät usein haavoittuvia kirjastoja, ajureita tai ohjelmistoagentteja hyväkseen saadakseen pääsyn järjestelmään ilman käyttäjän toimia. Tästä seuraa vaara myös niin sanotusta toimitusketjuhyökkäyksestä (supply chain attack), jossa päivitys tai luotettu komponentti itse sisältääkin haittakoodia. Erityisen tunnettu tapaus oli SolarWindsin Orion-alustan kautta tapahtunut maailmanlaajuinen hyökkäys, jossa haitallinen koodi levisi allekirjoitetun päivityksen mukana yli 18 000 asiakasympäristöön (CISA, 2021).

4.2 Salasanat

Salasanojen turvallisuuteen vaikuttaa keskeisesti niiden pituus, satunnaisuus ja rakenne. Vaikka vahva salausalgoritmi suojaa tiedonsiirtoa tehokkaasti, heikko salasana voi muodostaa kriittisen haavoittuvuuden – erityisesti silloin, kun se toimii ainoana pääsynhallinnan keinona.

Salasanan pituus vaikuttaa ratkaisevasti siihen, kuinka kauan sen murtaminen kestää. Nykytason laskentateholla vuonna 2025 voidaan arvioida seuraavaa: 8-merkkinen täysin satunnainen salasana voidaan murtaa harrastelijaresurssein alle tunnissa, ammattilaistasolla sekunneissa ja valtiollisin keinoin välittömästi. 12-merkkinen salasana kestää harrastelijalta kuukausia, mutta valtiotaso murtaa sen muutamassa minuutissa. Vasta 16-merkkinen satunnainen salasana tarjoaa todellista suojaa – se voi kestää harrastelijalta satoja vuosia, ammattimaiselta toimijalta kuukausia ja valtiotason hyökkääjältä useita päiviä. Yli 20-merkkiset salasanat ovat nykylaskentateholla käytännössä murtamattomia ilman haavoittuvuutta.

Turvallisuuden parantamiseksi salasanojen tulisi olla:

- vähintään 20 merkkiä pitkiä
- sisältää sekä isoja ja pieniä kirjaimia, numeroita että erikoismerkkejä
- täysin satunnaisia, ilman merkityksellisiä sanoja

Vahva salasanasuojaus edellyttää, että käyttäjät muistavat turvalliset ja pitkät salasanat. Tämän vuoksi on suositeltavaa käyttää salasanojen hallintaohjelmistoja, kuten 1Password, NordPass tai Bitwarden. Ne tallentavat kaikki käyttäjän salasanat salattuun säilöön. Säilöt ovat yleensä suojattu pääsalasanalla ja tukevat kaksivaiheista todennusta (2FA).

Uusien salasanojen turvallinen generointi voidaan toteuttaa esimerkiksi salasanasäilöjen sisäänrakennetuilla generaattoreilla, jotka tuottavat täysin satunnaisia merkkijonoja valitun pituuden ja rakenteen mukaan. Näin käyttäjä ei joudu muistamaan kuin yhden pääsalasanan – jonka tulee olla poikkeuksellisen vahva ja yksilöllinen (Hive Systems, 2023).

Mikäli salasanasäilö murretaan, hyökkääjällä on silti käytössään vain salattu tietokanta – ei suoria salasanoja. Tämän vuoksi salasananhallinnan voi nähdä yhtenä tärkeimmistä yksittäisistä suojakerroksista modernissa verkkoympäristössä (Zimmermann, 1995).

Salasanojen murtamista voidaan lähestyä useilla menetelmillä, kuten brute force -hyökkäyksillä, sanakirjahyökkäyksillä tai maskipohjaisilla generointitekniikoilla. Erityisesti mask wordlist -hyökkäykset hyödyntävät tyypillisiä käyttäytymismalleja, kuten sitä, että salasanaa muokataan hieman aiemmasta versiosta lisäämällä esimerkiksi vuosiluku tai erikoismerkki loppuun, esimerkiksi “Salasana2023” tai “Salasana2024!”. Tällaisia muunnelmia osataan ennakoida automaattisesti.

Lisäksi hyökkääjät käyttävät usein niin kutsuttuja profiilipohjaisia sanalistoja, jotka perustuvat uhrin nimeen, syntymäaikaan, harrastuksiin tai sosiaalisen median tietoihin. Tämä tekee henkilökohtaisista sanoista muodostetut salasanat erityisen alttiiksi murtamiselle.

Koska suurin osa palveluista ei ilmoita salasanavuodoista käyttäjälle automaattisesti, on suositeltavaa vaihtaa kriittisten palveluiden tunnukset säännöllisin, satunnaistetuin aikavälein. Julkisesti saatavilla olevista valvontapalveluista esimerkiksi Have I Been Pwned ja Norton 360 Identity Monitoring voivat auttaa tunnistamaan tunnettuja vuotoja.

4.3 Palomuurit ja liikenteen valvonta

Palomuuri toimii ensimmäisenä suojalinjana suodattaen liikenteen määriteltyjen sääntöjen perusteella ulkoisten ja sisäisten verkkojen välissä (Cisco Systems, 2018). Kaikissa palomuureissa on olennaista pitää sääntöjoukot ajan tasalla ja rajata liikenne minimoiden hyökkäyspinta-ala. Verkon reunalla olevien laitteiden – erityisesti palomuurien – säännöllinen päivitys ja huolellinen konfigurointi on kriittistä väärinkäytösten estämiseksi (Scarfone & Hoffman, 2009). Palomuurin rooli ei rajoitu vain porttien estämiseen: moderni palomuuri kykenee analysoimaan liikenteen sisältöä ja tunnistamaan poikkeavuuksia.

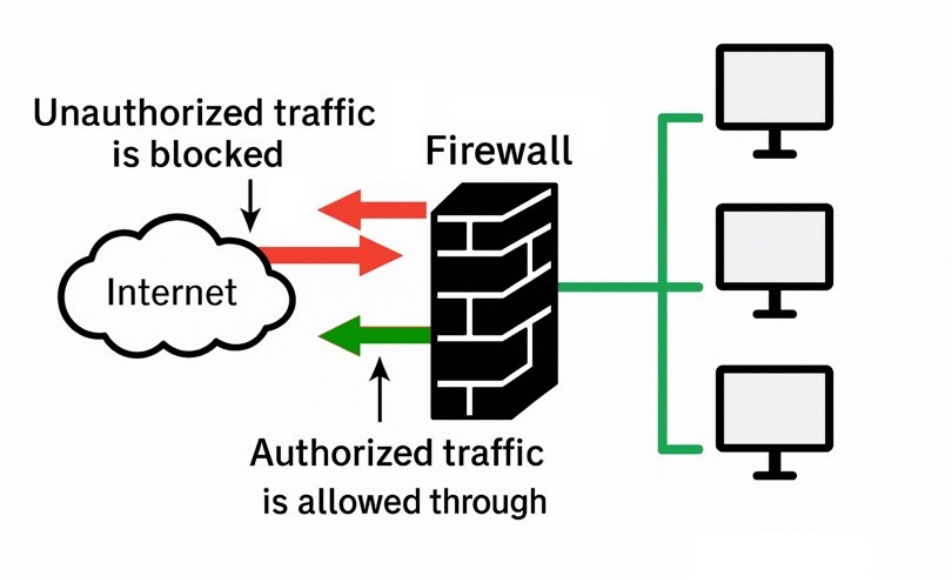
Palomuureja on useita tyyppejä, jotka voidaan luokitella esimerkiksi suojauskohteen, toteutustavan tai liikenteen suodatusmenetelmän perusteella (Palo Alto Networks, n.d.). Yleisimmät palomuurityypit voidaan kuvata seuraavasti:

- Pakettisuodatinpalomuuri: Perinteinen palomuuri tarkistaa jokaisen verkon läpi kulkevan paketin otsaketiedot (lähde- ja kohdeosoite, portit, protokolla) ja päättää sääntöjen perusteella, sallitaanko vai estetäänkö paketti. Pakettisuodattimet ovat nopeita ja yksinkertaisia, mutta eivät tutki pakettien sisältöä. Ne tarjoavat perustason suojan, mutta eivät pysty estämään monimutkaisempia hyökkäyksiä, jotka kätkeytyvät sallitun liikenteen sekaan (Scarfone & Hoffman, 2009).
- Tilallinen palomuuri: Tilatietoinen palomuuri (stateful firewall) seuraa verkkoyhteyksien tilaa ja kontekstia yksittäisiä paketteja pidemmällä aikajänteellä. Se ymmärtää esimerkiksi TCP-yhteyden avaamisen, datansiirron ja sulkemisen vaiheet. Tilallinen palomuuri osaa päästää läpi vain sallitut yhteyden muodostamisen aloitukset ja niihin kuuluvan paluuliikenteen. Tämä parantaa turvallisuutta verrattuna pelkkään pakettisuodatukseen, koska luvattomat tai odottamattomat yhteydenavaukset voidaan estää (Cisco Systems, 2020; CompTIA, 2021). Tilallinen suodatus onkin nykyaikaisten palomuurien perustoiminto.
- Sovellustason proxy-palomuuri: Sovellustason palomuuri toimii välityspalvelimena (proxy) asiakkaan ja palvelun välillä. Se vastaanottaa esim. HTTP- tai SMTP-liikenteen kokonaisuudessaan ja tarkastaa sovellustason sisältöä ennen liikenteen välittämistä eteenpäin (Scarfone & Hoffman, 2009). Tällä tavalla proxy-palomuuri voi suodattaa haitalliset sisältöhyökkäykset, kuten tiettyihin HTTP-pyyntöihin upotetut hyökkäyskoodit. Haittapuolena on usein hitaampi suorituskyky ja rajoittuminen tiettyihin protokolliin tai sovelluksiin.
- Yhdistetyn uhanhallinnan palomuuri (UTM): UTM-laitteet yhdistävät perinteisen tilallisen palomuurin toimintoihin useita muita suojamekanismeja, kuten tunkeutumisenestojärjestelmän (IPS), virustorjunnan ja sisällönsuodatuksen yhdeksi kokonaisuudeksi (Scarfone & Hoffman, 2009). UTM-palomuurit yleistyivät 2000-luvun alussa tuoden mukanaan syvällisemmän pakettitarkastuksen ja monipuoliset turvaominaisuudet yhden laitteen hallintaan. Erityisesti pienissä organisaatioissa UTM on suosittu, koska yksi laite hoitaa useita tietoturvatehtäviä keskitetysti.

- Seuraavan sukupolven palomuuri, Next Generation Firewall: NGFW laajentaa palomuurin toiminnot sovellustason tunnistukseen ja syväpakettitarkastukseen yhdistäen mukaan tunkeutumisen havainnointi/esto (IDS/IPS) -ominaisuuksia sekä esimerkiksi verkkosivujen suodatuksen ja haittaohjelmien torjunnan (Cisco Systems, 2021). NGFW kykenee tarkastelemaan liikennettä sovellustason näkymällä – esimerkiksi erottamaan Facebookin, YouTuben ja muiden sovellusten liikenteen – ja soveltamaan niihin erilaisia turvallisuuskäytäntöjä. Yhtenäistetyt politiikat ja syvä analyysi koko hyökkäyspinnalla tekevät NGFW:stä tehokkaan nykyaikaisen suojakomponentin.
- Isäntäkohtainen ohjelmistopalomuuri: Edellä mainitut ovat verkon reunalle tai liikennesolmukohtiin sijoitettavia laite- tai ohjelmistopalomuureja. Niiden lisäksi host based -palomuurit toimivat suoraan yksittäisellä tietokoneella tai palvelimella (esimerkiksi Windowsin oma palomuuri). Isäntäkohtainen palomuuri kontrolloi juuri kyseisen laitteen saapuvaa ja lähtevää liikennettä sen omien sääntöjen perusteella (Cisco Systems, 2019). Tällaiset palomuurit ovat tärkeitä viimeisenä puolustuskerroksena, etenkin kun päätelaitteet siirtyvät verkon ulkopuolelle, kuten kotikoneet tai etätyöläisten laitteet. Isäntäkohtaista palomuuria käytetään usein yhdessä verkon reunapalomuurin kanssa defence in depth -periaatteen mukaisesti, jolloin sekä verkon rajalla että jokaisessa laitteessa on suodatus (Scarfone & Hoffman, 2009).

Yllä kuvatuista tyypeistä tämä opinnäytetyö keskittyy verkon reunalle sijoitettavaan palomuuriin, joka näytetään graafisesti kuvassa 6. OPNsense on stateful eli tilallinen verkkopalomuuri, joka toimii reitittimenä ja palomuurina SoHo-verkon rajalla. Se edustaa seuraavan sukupolven palomuuria siinä mielessä, että siihen voidaan integroida IDS/IPS-toiminnallisuuksia (esim. Suricata) ja muita moduuleja (kuten CrowdSec) (CrowdSec, n.d.) parantamaan syväluotaavaa liikenteen tarkkailua. OPNsense on ohjelmistopohjainen ja avoimen lähdekoodin alusta, joten sen etuna on muokattavuus ja laaja ominaisuusvalikoima ilman lisenssikustannuksia (OPNsense, n.d.). Tässä työssä OPNsense toimi keskeisenä komponenttina, johon yhdistettiin muita ratkaisuja, joten palomuuriosuudessa keskitytään ennen kaikkea tilalliseen verkkopalomuuriin ja sen laajennuksiin.

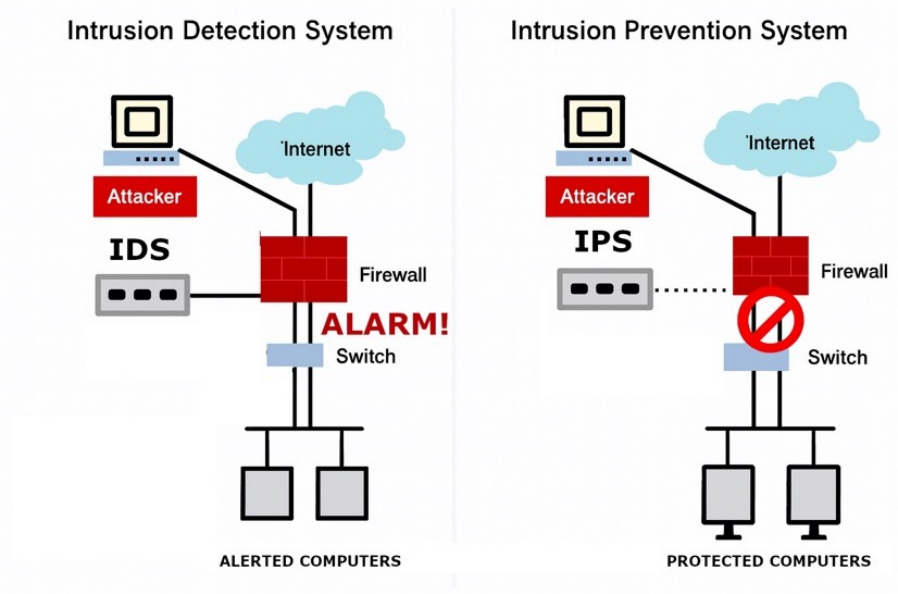
Kuva 6. Palomuurin sijoittuminen verkon rajalle.



4.4 IDS/IPS- ja SIEM-järjestelmät

Intrusion Detection Systems (IDS) ja Intrusion Prevention Systems (IPS) analysoivat verkon liikennettä etsien tunnettuja uhkia tai poikkeavaa käyttäytymistä. IDS on passiivinen — se ilmoittaa uhkista — kun taas IPS voi myös estää haitallista liikennettä reaaliajassa. IDS:n ja IPS:n väliset toiminnalliset erot näkyvät kuvassa 7.

Kuva 7. IDS/IPS-järjestelmän toiminta.



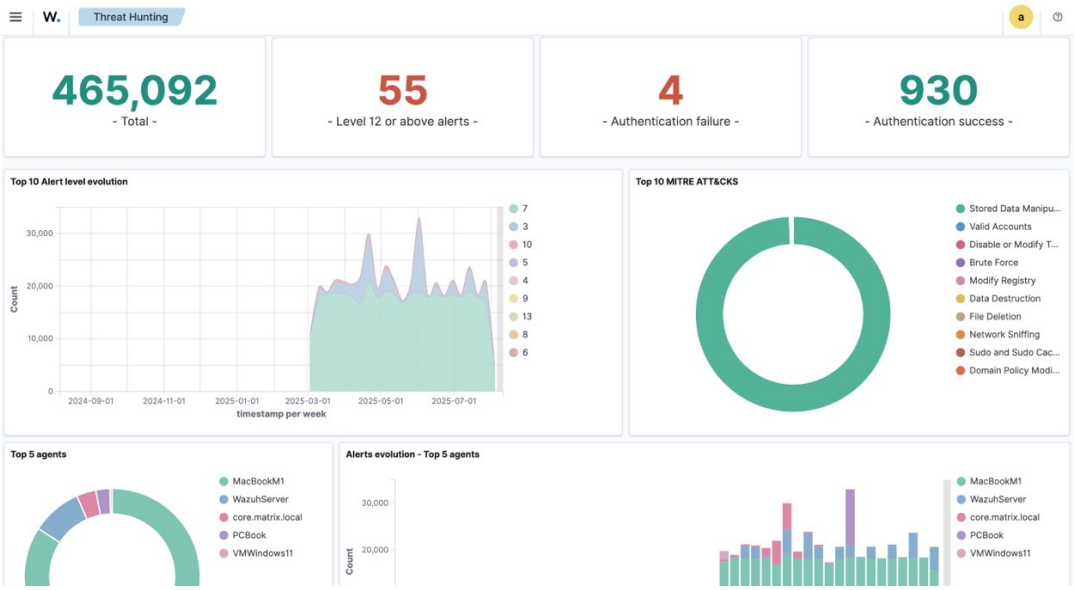
Suricata on esimerkki tehokkaasta IDS/IPS-moottorista, jota voidaan käyttää yhdessä OPNsense-alustan kanssa (Suricata, n.d.). Se mahdollistaa mm. HTTP- ja TLS-liikenteen syväanalyysin, flow-pohjaisen tilastoinnin ja reaaliaikaisen uhkalistojen käyttöönoton.

IDS/IPS-järjestelmien toiminnallisuutta voidaan merkittävästi laajentaa yhdistämällä ne reaaliaikaiseen SIEM-järjestelmään (Security Information and Event Management), joka kokoaa, analysoi ja tulkitsee päätelaitteiden sekä verkkolaitteiden tuottamaa tapahtumatietoa. Tässä opinnäytetyössä käytetyn Wazuh-järjestelmän (Wazuh, n.d.) avulla rakennettiin keskitetty valvontaympäristö, jossa eri laitteisiin – mukaan lukien langattomat päätelaitteet, OPNsense-reititin sekä Wazuh-palvelin itse – asennettiin kevyet agentit. Nämä agentit keräävät järjestelmätason lokitietoa, kuten prosessi- ja käyttäjätapahtumia, tiedostomuutoksia sekä ohjelmistoversioita, ja välittävät tiedot salatussa muodossa Wazuh-palvelimelle analysoitavaksi. Kuvassa 8 näkyy ruudunkaappaus Wazuh:n poikkeamien seurantaikkunasta.

Wazuhin analyysimoottori käyttää laajaa sääntöpohjaista mallia, joka perustuu mm. OWASP:n ja MITRE ATT&CKin kaltaisiin tunnettuja uhkia ja hyökkäystekniikoita kuvaaviin viitekehyksiin. Järjestelmä pystyy tekemään johtopäätöksiä yksittäisten havaintojen merkityksestä ja niiden mahdollisesta ketjuuntumisesta osaksi hyökkäystä, sekä seuraamaan uhkien leviämistä verkossa. Lisäksi Wazuh sisältää vahvan

auditointitoiminnallisuuden, jonka avulla voidaan keskitetysti tarkastella kaikkien valvottujen päätelaitteiden ajantasaisuutta ja suojaustasoa suhteessa tietoturvastandardeihin ja ohjelmistopäivityksiin.

Kuva 8. Wazuh-ohjelman reaaliaikainen valvontanäkymä.



Tämänkaltaisen SIEM-integraation ansiosta IDS/IPS-järjestelmä ei ole pelkkä hälytysjärjestelmä, vaan se toimii myös jatkuvan riskinarvioinnin, auditoinnin ja päätelaitteiden kokonaisturvallisuuden hallinnan välineenä – erityisesti SoHo-verkkojen kaltaisissa ympäristöissä, joissa resurssien keskittäminen yhteen näkymään on erityisen arvokasta.

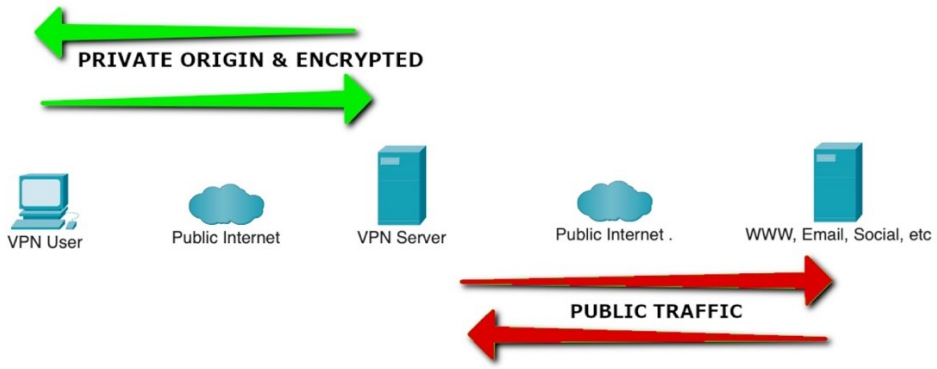
4.5 VPN-yhteydet

Virtual Private Networks (VPN) -yhteydet mahdollistavat salatun ja todennetun yhteyden päätelaitteen ja toisen verkon tai palvelimen välille, sisäverkossa tai julkisen internetin yli. Tämä estää kolmansia osapuolia lukemasta liikennettä tai jäljittämästä käyttäjän alkuperää, sillä yhteys kulkee VPN-palvelimen kautta, joten VPN:ää voidaan siksi käyttää myös etätyön turvaamiseen tai suojaamaan liikennettä esimerkiksi julkisissa verkoissa.

SoHo-ympäristöissä yleisiä teknologioita ovat IPsec/IKEv2, OpenVPN ja WireGuard; niissä asymmetrinen avaintenvaihto perustaa ensin turvallisen istunnon, jonka aikana

varsinainen datakanava salataan tehokkaalla symmetrisellä algoritmilla esim. AES-GCM (Barker ym., 2020; Kaufman ym., 2014; Kent & Seo, 2005). VPN:n toimintaperiaate havainnollistetaan kuvassa 9.

Kuva 9. VPN-yhteyden toimintaperiaate.



4.6 Salausmenetelmät

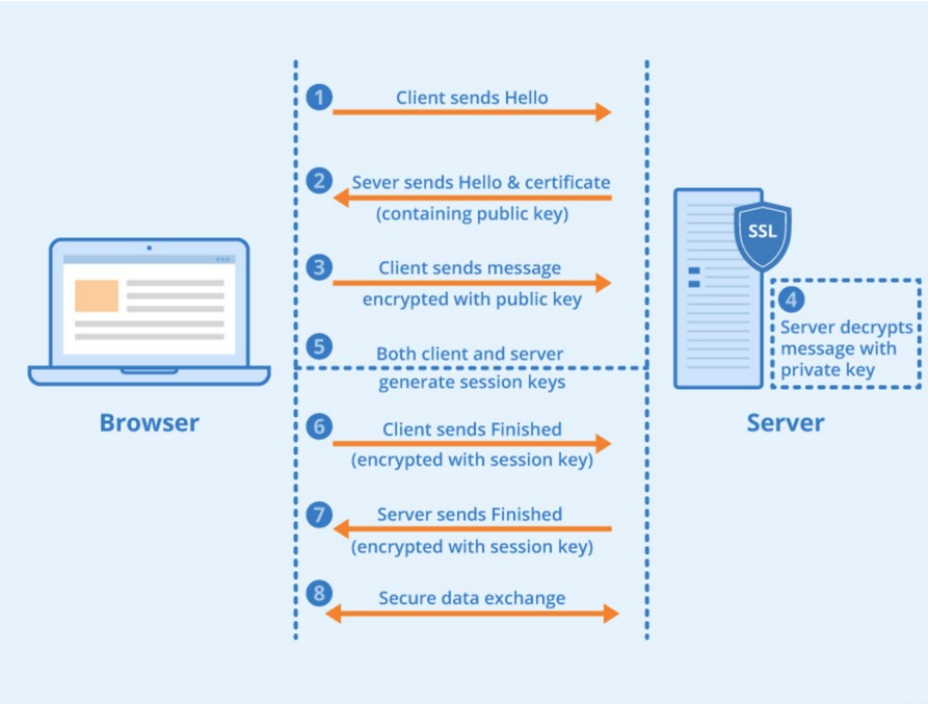
Tietoliikenteen turvaamisessa salausprotokollilla on keskeinen rooli. Niiden tarkoitus on varmistaa, että viestintä säilyy luottamuksellisena ja eheänä, eikä ulkopuoliset tahot pysty lukemaan tai muuttamaan tietoa siirron aikana. Salausmenetelmät jaetaan kahteen pääluokkaan: symmetriseen ja asymmetriseen salaukseen. Useat nykyaikaiset verkkoturvaratkaisut, kuten VPN-yhteydet, hyödyntävät näitä molempia rinnakkain.

Symmetrinen salaus (esim. AES) on nopeaa ja soveltuu suurien tietomäärien salaamiseen, mutta salausavainten jakelu vaatii luottamusta.

Asymmetrinen salaus (esim. RSA) ratkaisee tämän käyttämällä avainpareja, mutta on raskaampaa laskennallisesti.

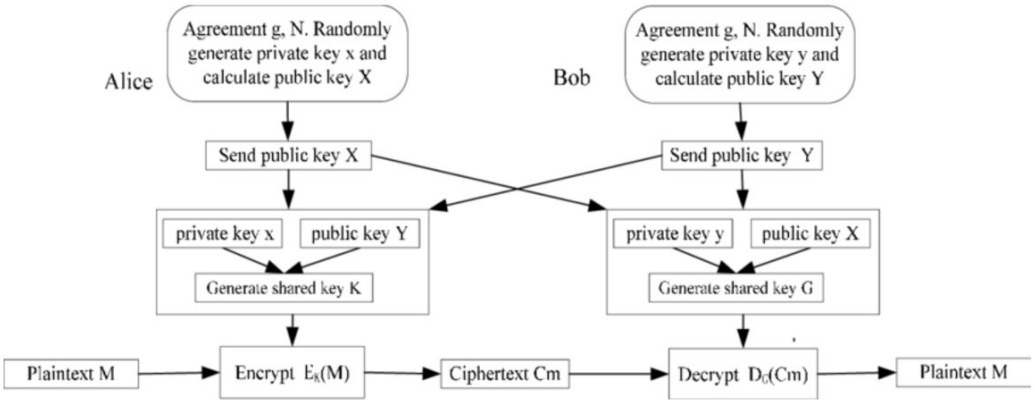
HTTPS hyödyntää TLS-salausta, jossa asymmetrinen avaintenvaihto käynnistää istunnon, ja datakanava suojataan symmetrisesti (esim. AES-GCM). Kuvassa 10 esitellään istunnon muodostamisen vaiheet. Avaintenvaihto suojaa tiedonsiirron mm. man in the middle -hyökkäyksiltä (McKay & Cooper, 2019; Rescorla, 2018).

Kuva 10. HTTPS-protokollan rakenne (Hostinger Tutorials, n.d).



Diffie-Hellman-avaimenvaihto mahdollistaa turvallisen yhteisen avaimen muodostamisen avoimen kanavan yli. DH-protokolla perustuu matemaattiseen ongelmaan nimeltä discrete logarithm problem, joka on laskennallisesti erittäin vaikea ratkaista ilman yksityisiä parametreja. Diffie-Hellman-avaintenvaihdon periaate osoitetaan kuvassa 11. Tässä menetelmässä osapuolet vaihtavat julkisia avaimia, joiden perusteella kumpikin pystyy laskemaan saman jaetun salaisuuden, vaikka mahdollinen tarkkailija ei voi palauttaa alkuperäistä avainta pelkän liikenteen perusteella (Diffie & Hellman, 1976).

Kuva 11. Diffie–Hellman-avaimenvaihto (Researchgate, n.d.).



Nykyään käytössä on myös tehokkaampi ja kevyempi versio nimeltä Elliptic Curve Diffie–Hellman (ECDH). Tämä käyttää elliptisiä käyriä julkisten avainten muodostamiseen, mikä mahdollistaa saman turvallisuustason kuin perinteinen DH, mutta pienemmällä avainkoolla ja prosessointiteholla. Esimerkiksi Curve25519 on yksi suosituimmista moderneista ECDH-implementaatioista, jota käytetään mm. OpenSSH:ssa ja WireGuard-VPN-teknologiassa (Bernstein ym., 2015).

Erityisesti VPN-tunnelin muodostus nojaa asymmetriseen salaukseen turvallisen istunnon perustamiseksi, jonka jälkeen varsinaisen tietoliikenteen salaamiseen siirrytään tehokkaampaan symmetriseen algoritmiin, kuten AES-256:een (Advanced Encryption Standard) (Stallings, 2020). Asymmetristä avaintenvaihtoa varten yleisesti käytetty protokolla on Diffie–Hellman (DH), joka mahdollistaa kahden osapuolen luoda yhteisen salaisen avaimen avoimen viestikanavan yli.

Lisäksi hash-funktioilla on keskeinen rooli tietoturvassa. Ne mahdollistavat mm. salasanojen tallennuksen ilman palautettavaa alkuarvoa (esim. SHA-256). Hash-arvot ovat yksisuuntaisia, ja niitä käytetään myös tiedostojen eheystarkastuksessa. Hashia ei voi purkaa takaisin alkuperäiseksi dataksi, ja pienikin muutos syötteessä tuottaa täysin erilaisen lopputuloksen.

Salasanojen salauksen lisäksi voidaan hyödyntää myös paikallista tiedostojen salausta, jolloin arkaluonteinen data pysyy turvassa silloinkin, kun laitteen fyysinen suojaus vaarantuu. Tyypillisiä toteutuksia ovat koko levyn salaus (esim. BitLocker, LUKS, FileVault) tai yksittäisten kansioiden salaaminen salasanalla suojattuihin arkistoihin.

5 Sovellukset ja toteutus

Tässä luvussa esitellään opinnäytetyön kokeellinen ympäristö, jonka avulla tietoturvaratkaisuja testattiin, arvioitiin ja kehitettiin. Kyseessä on pienimuotoinen mutta rakenteellisesti monikerroksinen SoHo-verkko, jonka arkkitehtuuri ja ohjelmistot simuloivat todellisen pienen yrityksen tarpeita.

5.1 Verkon suunnittelu

SoHo-testiverkko suunniteltiin kolmeen loogiseen verkkoalueeseen:

1. LAN (VLAN 1) – sisältää tärkeät päätelaitteet ja palvelimet.
2. WLAN SSID 1 (VLAN 2) – sisältää langattomat laitteet.
3. WLAN SSID 2 (VLAN 3) – eristetty vieras- ja IoT-laiteverkko.

Kaikki aliverkot eroteltiin toisistaan, ja niiden välinen liikenne reititettiin OPNsense-palomuurin kautta tiukoin säännöin.

5.2 Käytetyt laitteet ja ohjelmistot

Laitteisto:

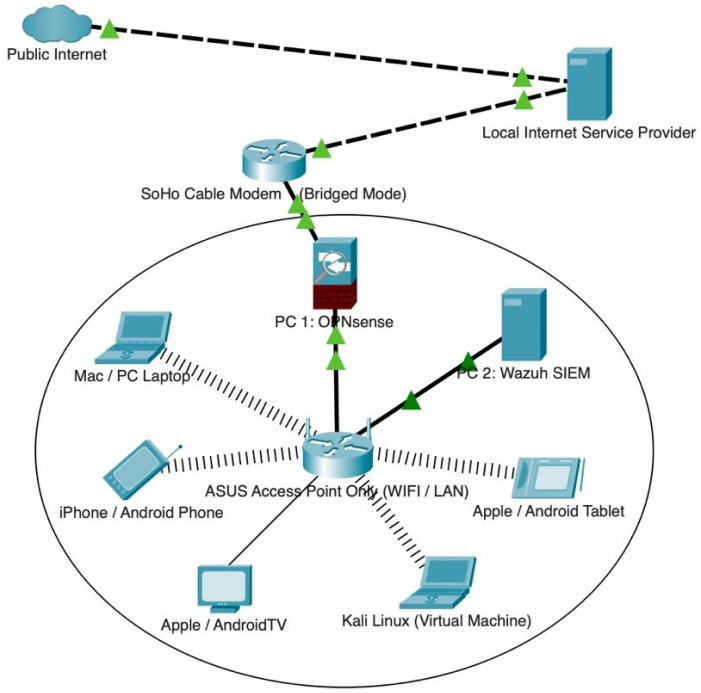
- ISP-kaapelimodeemi: Bridged mode (WAN)
- PC 1 -tietokone: OPNsense, Suricata, CrowdSec
- ASUS WIFI-tukiasema: Access Point Only mode (WIFI WPA3 / LAN)
- PC 2 -tietokone: Wazuh
- Yleiset laitteet: Mac, PC, Android, Apple, SmartTV, Wazuh-agentit ja IoT-simulaatiot

VLAN- ja IP-segmentointi:

1. VLAN 13 (Palvelimet ja LAN-laitteet): 10.43.129.0 / 29
2. VLAN 24 (Luotettu WIFI): 172.100.222.0 / 28
3. VLAN 39 (Vieras/IoT): 192.252.7.0 / 26

Visuaalinen rakennekaavio on hyödyksi verkon suunnittelussa ja rakentamisessa, josta esimerkki on kuvassa 12.

Kuva 12. Testiverkon rakenne Cisco Packet Tracer -simulaatiossa.

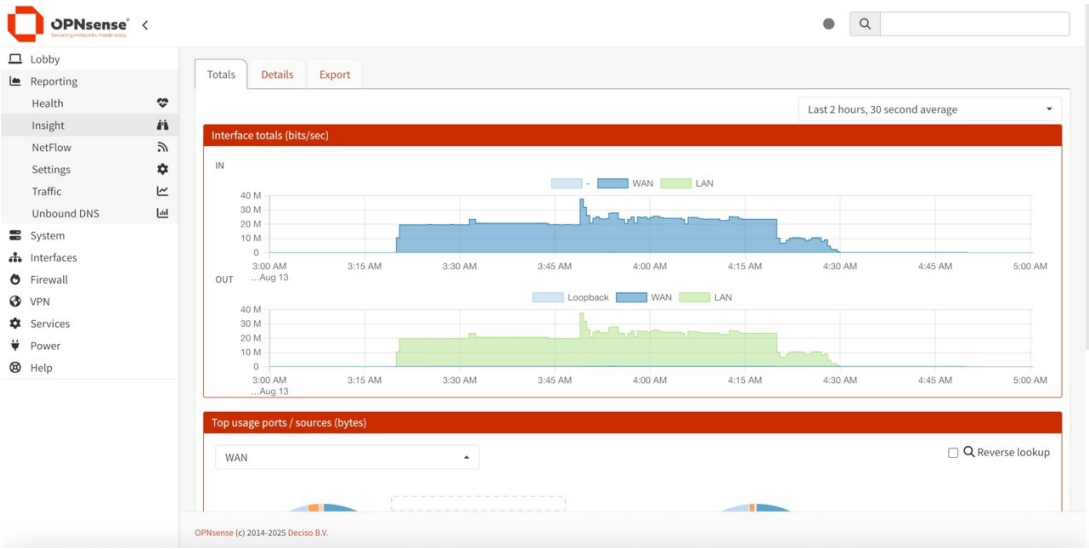


Ohjelmistot:

- OPNsense: Palomuuri, reititys, NAT, DHCP, DNS (DoT), Time, SSH, HTTPS (OPNsense, n.d.), datasiirron määrän seurantaikkuna kuvassa 13
- Suricata ja CrowdSec: IDS/IPS-tarkkailu suoraan OPNsense-alustalla (Suricata, n.d.; CrowdSec, n.d.)
- Wazuh: SIEM-lokianalysointi ja uhkatunnistus, SSH, HTTPS (Wazuh, n.d.)
- Norton 360: Päätelaitteiden viruksentorjunta
- NordPass: Salasanasuojaus
- NordVPN: Tietoliikenteen suojaus

- FileVault / BitLocker: Kiintolevyjen salaus
- Virtuaalikone: Kali Linux (hyökkäysten testaus)

Kuva 13. Dataliikennemäärän seurantaikkuna OPNsensessä.



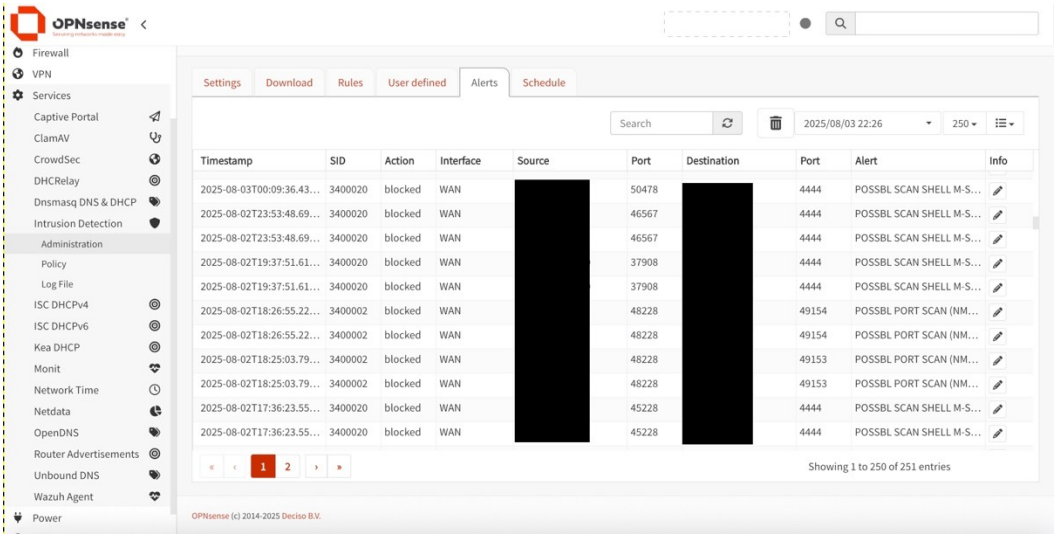
Lisäksi testiverkon reitittimenä toimivaan OPNsenseen asennettiin CrowdSec-laajennus, jonka toiminta perustuu julkiselta yhteisöltä kerättyihin uhkamalleihin ja IP-osoitelistoihin. CrowdSec valvoo samanaikaisesti myös paikallisia autentikointiyrityksiä, porttiskannauksia ja muita epänormaaleja yhteyksiä, ja pystyy automaattisesti estämään IP-osoitteita globaalien mustien listojen sekä paikallisten tapahtumien perusteella. CrowdSec täydensi tehokkaasti IDS/IPS-järjestelmän toimintaa ollessaan osana itse reititintä.

5.3 Hyökkäysten simulointi ja tunnistus

Hyökkäykset toteutettiin samassa verkossa olevalla Kali Linux -virtuaalitietokoneella, jolla testattiin useita hyökkäysskenaarioita. Näihin kuuluivat Nmap-työkalulla tehdyt porttiskannaukset laitteiden, avointen palveluiden ja haavoittuvuuksien löytämiseksi, brute force -tunkeutumisyritykset laitteisiin ja web-hallintapaneeleihin, sekä haitallisten tiedostojen luonnit, siirrot ja lataukset.

Kaikki tapahtumat rekisteröitiin ja estettiin joko OPNsense-palomuurin, Suricata IDS/IPS:n (kuvassa 14), CrowdSecin, Wazuh SIEM:n, tai antivirus-ohjelman toimesta.

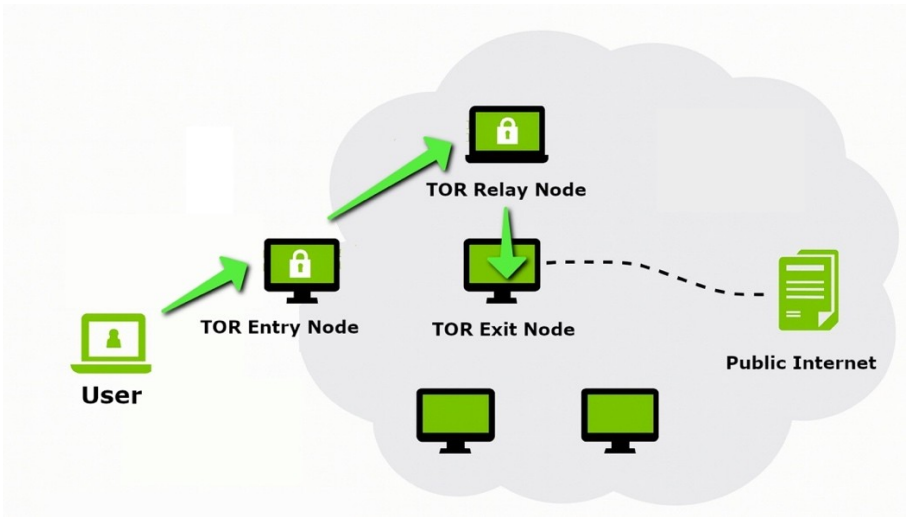
Kuva 14. Suricata IDS/IPS-ohjelman hälytysten seurantaikkuna.



5.4 Anonymiteetti ja jäljityksen vaikeus

Hyökkääjän jäljittäminen on teknisesti haastavaa, etenkin jos hyökkääjä käyttää VPN-palveluita, jotka piilottavat alkuperäisen IP-osoitteen ja salakirjoittavat liikenteen, tai TOR-verkkoa, joka näkyy kuvassa 15. TOR-verkossa liikenne kulkee usean erillisen salatun solmun läpi, muodostaen niin kutsutun sipulirakenteen.

Kuva 15. TOR-verkon reititysperiaate.



Erityisesti tutkittiin, miten TOR-verkon käyttö piilottaa hyökkäyksen alkuperän. TOR reitittää liikenteen usean salatun solmun kautta, jolloin alkuperäinen IP-osoite ja

maantieteellinen sijainti muuttuvat toisiksi. VPN:n käyttö ennen TOR-verkkoon siirtymistä antaa lisää anonymiteettiä, mutta toisaalta voi myös luoda yhdistettäviä metatietoja.

TOR:n tehokkuus perustuu siihen, että julkisessa verkossa käyttäjän yhteyden jokainen peräkkäinen reitityssolmu tuntee vain edellisen ja seuraavan solmun — ei koko ketjua. Tällöin edes verkkoa valvova taho ei näe, kuka on yhteydessä keneen (Dingledine ym., 2004). TOR-verkossa kommunikointi salataan useaan kertaan ja puretaan kerros kerrokselta, minkä vuoksi liikenne ei ole helposti yhdistettävissä lähettäjäänsä.

Kuten käsiteltiin kohdassa 3.3, myös valtiolliset toimijat voivat käyttää anonymiteettiverkkoja kuten TOR.

Yhdistämällä VPN- ja TOR-verkkojen käyttö voidaan merkittävästi vaikeuttaa käyttäjän jäljittämistä, sillä molemmat menetelmät salaavat liikennettä ja piilottavat alkuperäisen IP-osoitteen. Kuitenkin edistyneet vastatoimet, kuten datapakettien aikavälien vertaamiseen perustuva korrelaatioanalyysi, voivat mahdollistaa liikenteen yhdistämisen. Tässä menetelmässä tarkastellaan salattua VPN/TOR-liikennettä ja vertaillaan sen ajallista rytmiä muuhun havaittuun ei-salattuun datavirtaan muualla verkossa tai maailmassa: jos datapakettien ajoitukset täsmäävät keskenään, voidaan päätellä niiden liittyvän samaan käyttäjään. Myös näennäisesti pienet yksityiskohdat, kuten laitteen aikavyöhykkeen asetus, metatiedot kuten selaimen aikavyöhyke, tai DNS-pyynnöt voivat paljastaa käyttäjän maantieteellisen sijainnin. Tällaisia kehittyneitä jäljitystekniikoita hyödynnetään erityisesti valtiollisten toimijoiden, kuten kansallisten tiedusteluorganisaatioiden, toimesta (National Security Agency [NSA], n.d.).

TOR-verkko demonstroi hyvin, miten IP-osoitteen anonymisointi toimii ja miksi pelkkä verkonvalvonta ilman sisältöanalyysiä voi jäädä riittämättömäksi. SoHo-ympäristössä TOR ei välttämättä ole tavallisen käyttäjän työkalu, mutta hyökkääjän näkökulmasta se on helposti saatavilla oleva palvelu omien jälkien peittämiseen. Siksi opinnäytetyön mallissa on huomioitu, että pelkkä lähdeosoitteiden blokkaukseen perustuva suojaus (esim. IP-estolistat) ei aina riitä, vaan tarvitaan myös liikenteen sisältöjen tarkkailua ja poikkeavan käytöksen tunnistavia menetelmiä, kuten IDS/IPS ja SIEM. TOR-osuuden johtopäätös onkin, että monikerroksinen puolustus (palomuuri + IDS + SIEM) on tarpeen: vaikka TOR piilottaakin IP-osoitteen alkuperän, voidaan hyökkäyksen

tuntomerkit silti havaita muista seikoista, kuten epätavallisesta liikennemallista tai hyökkäyksen sisällöstä (esim. tietty haittakoodi liitetiedostossa).

6 Johtopäätökset ja yhteenveto

Opinnäytetyössä tutkittiin kotiverkkojen ja pienten toimistojen (SoHo) tietoturvauhkia, ja kehitettiin rakenteellinen sekä käytännön malli monikerroksisesta suojausjärjestelmästä, jonka voi toteuttaa ilman suuria kustannuksia. Työtä varten toteutettu kokonaisuus yhdisti reaktiivista palomuurisuodatusta, aktiivista IDS/IPS-valvontaa, aktiivista viruksentorjuntaa, tiedostojen ja salasanojen salausta, tiedonsiirron kryptausta, sekä keskitettyä laitteiden lokitapahtumien analysointia ja uhkailmoituksia.

Tämän työn perusteella voidaan todeta, että kotiverkko voidaan suojata kustannustehokkaasti hyödyntämällä edullisia ja avoimen lähdekoodin ratkaisuja, kuten OPNsense, Suricata ja Wazuh. Tekniset ratkaisut, kuten VPN, segmentointi ja IDS/IPS auttavat torjumaan yleisiä uhkia. Komponenttien yhteistoiminta – erityisesti reaaliaikainen valvonta ja reaktiivisuus – parantaa merkittävästi tietoturvan tasoa.

6.1 Yhteenveto toteutuksesta

Testilaboratoriossa rakennettu SoHo-verkko koostui monitasoisesta suojauksesta, ja sen perusteella voidaan tehdä useita tärkeitä johtopäätöksiä työn onnistumisesta.

Ensinnäkin verkon jakaminen segmentteihin – erottamalla esimerkiksi IoT-laitteet, työasemaverkko, vieraat, ja palvelimet omiin VLAN- tai aliverkko-osiinsa – osoittautui tehokkaaksi tavaksi parantaa tietoturvaa. Segmentointi selkiytti verkon rakennetta ja rajoitti potentiaalisten tunkeutujien liikkumavaraa: vaikka hyökkääjä olisi päässyt yhteen segmenttiin, hän ei automaattisesti päässyt käsiksi koko verkkoon. Tämä kerroksellinen eristäminen vähensi sivuttaisliikkeen riskiä merkittävästi.

OPNsense-palomuuri mahdollisti erittäin hienojakoisen sääntöpohjaisen liikenteen hallinnan. Kaikki saapuva ja lähtevä liikenne voitiin rajata tarkasti vain välttämättömään. Testit vahvistivat, että hyvin konfiguroidulla palomuurilla pystyttiin estämään ennakolta monia hyökkäyksiä: esim. tarpeettomat portit ja palvelut olivat

kiinni, jolloin automatisoidut porttiskannaukset ja triviaalit hyökkäykset eivät tuottaneet tulosta. Myös palomuurin dynaamiset estolistat (CrowdSec-lisäosan kautta) estivät tunnettuja haitallisia IP-osoitteita. Tämä osoittaa, että avoimen lähdekoodin palomuuri voi käytännössä tarjota saman tason kontrollin kuin kaupalliset laitteet, kunhan asetukset tehdään huolella.

Tunkeutumisen havainnointi ja esto toteutui onnistuneesti integroidulla Suricata IDS/IPS:llä ja CrowdSec-moottorilla. Nämä järjestelmät tunnistivat nopeasti useita testimielessä generoituja uhkia, kuten porttiskannauksia ja tunnettuja hyökkäyskuvioita, ja estivät niitä reaaliajassa. Esimerkiksi kun testiverkon palvelimelle yritettiin ajaa yleisiä haavoittuvuuksia hyödyntäviä hyökkäyksiä, IDS/IPS laukaisi hälytykset ja katkaisi epäilyttävän yhteyden ennen vahingon tapahtumista. Tämä vahvistaa ajatuksen, että syväpakettitarkastus on kriittinen osa puolustusta: siellä missä perinteinen palomuuri katsoo vain osoitteita ja portteja, IDS analysoi sisällöt ja käyttäytymisen. Yhteisvaikutuksena OPNsense + Suricata + CrowdSec muodosti tehokkaan yhdistelmän, joka reagoi uhkiin sekä tunnistus- että estotasoilla. On merkittävää, että nämäkin työkalut ovat ilmaisia ja avoimia – silti ne pystyivät havaintojen perusteella kilpailemaan kaupallisten ratkaisujen kanssa havaitsemiskyvyssä.

Wazuh SIEM tarjosi reaaliaikaisen tilanteenkuvan koko verkosta. Wazuh keräsi lokitietoa käytännössä kaikista järjestelmän osista: työasemilta, palvelimilta, reitittimeltä, palomuurilta ja jopa päätelaitteista (agenttien avulla). Tämän keskitetyn näkymän ansiosta oli mahdollista havaita korreloituja tapahtumia – esimerkiksi jos tietty päätelaite osoitti samanaikaisesti virustorjuntasignaalin ja verkon IDS hälytti kyseisen laitteen liikenteestä, voitiin ymmärtää tilanteen vakavuus paremmin. Wazuh:n analytiikka yhdisti yksittäiset hälytykset laajemmiksi tapahtumaketjuiksi, mikä auttoi tunnistamaan mahdolliset käynnissä olevat hyökkäyskampanjat. Testien perusteella Wazuh myös mahdollisti riskien arvioinnin: se automaattisesti vertasi havaintoja tietoturvaviitekehyksiin (kuten MITRE ATT&CK) ja antoi prioriteetteja hälytyksille. Tämä tarkoittaa, että SoHo-ympäristössäkin voidaan saada kokonaisvaltainen tilannekuva ilman kallista kaupallista SIEM:iä. On kuitenkin huomattava, että SIEM:n pyörittäminen rasittaa laitteistoa: runsas lokimäärä ja jatkuva analyysi vaativat tehoa ja tiedonsiirtokaistaa.

Perinteiset päätelaitesuojaukset – kuten virustorjunta ja tiedostojen salaus – osoittautuivat yhä tarpeellisiksi verkon viimeisenä puolustuskeinona. Testiverkon koneilla pyörineet virustorjuntaohjelmat (esim. Windows Defender, Norton 360 kokeiluversiona, AVG Free) havaitsivat ja estivät kaikki kokeillut haittaohjelmanäytteet, joita yritettiin ajaa tai ladata. Tämä tulos alleviivaa, että vaikka verkon reuna olisi vahvasti suojattu, tulee päätelaitteiden suojauksesta huolehtia – käyttäjän huomaamatta käynnistämä haittaohjelma voidaan pysäyttää ennen kuin se ottaa yhteyttä verkkoon, jos päätteellä on ajantasainen virustorjunta. Vastaavasti kiintolevyjen salaus (FileVault, BitLocker) ja salasanojen hallinta (NordPass) estivät testatessa asiattomia hyödyntämästä dataa, vaikka laitteeseen olisi fyysisesti päästy käsiksi tai yksittäinen salasana vuotanut.

Suojatun yhteyden muodostaminen VPN:llä osoittautui toimivaksi tavaksi sekä salaamaan liikenne että piilottamaan sen alkuperä tarvittaessa. Labraympäristössä käytetty OpenVPN-yhteys varmisti, että kaikki etäliikenne kulki salattuna tunnelina, eikä ulkopuolinen päässyt lukemaan tai muokkaamaan sitä. Samalla VPN piilotti kokeellisessa TOR-skenaariossa todellisen lähiverkon IP-osoitteen internetiin päin. Tämä opetti, että VPN-yhteyksiä kannattaa hyödyntää etenkin julkisissa verkoissa tai etätyössä, sillä ne lisäävät sekä yksityisyyttä että tietoturvaa salaamalla dataliikenteen.

Yhteenvetona voidaan todeta, että opinnäytetyössä rakennettu monikerroksinen suojausmalli onnistui tavoitteessaan: useista edullisista ja ilmaisista ohjelmistoista koottu ratkaisu saavutti tason, jossa niin verkkohyökkäysten ehkäisy, havainnointi kuin reagointikin toimivat luotettavasti. Erilaisten puolustuskerrosten yhteisvaikutus muodosti syvemmän puolustuksen, jossa kukin kerros tukee toistaan: verkon segmentointi eristää hyökkäykset, palomuuri estää luvattomat yhteydet, IDS/IPS tunnistaa poikkeavuudet, SIEM korreloi tapahtumat, ja päätelaitesuojaukset pysäyttävät viimeisetkin uhat.

Tulokset osoittavat, että jopa SoHo-ympäristössä voidaan ilman suuria investointeja saavuttaa kattava tietoturvan taso, kun hyödynnetään saatavilla olevia työkaluja oikein. Samalla projekti korosti, että järjestelmän ylläpitäjän on ymmärrettävä perusasioita (verkkoprotokollat, uhkamallit) – teknologia sinänsä on tehokasta, mutta ihmisen asiantuntemus tarvitaan sen oikeaan soveltamiseen.

6.2 Hyödyt ja rajoitteet

Suurin osa haasteista liittyi laitteiden välisiin yhteysongelmiin, erityisesti toisistaan eristettyjen verkko-osioiden konfigurointiin, NAT- sekä palomuurisääntöjen läpikäymiseen, ja IDS/IPS-järjestelmien käynnistämiseen eliminoimalla ensin väärät hälytykset oikeiden joukosta.

SIEM-lokianalysoinnin tarjoamat mahdollisuudet olivat ylivertaiset uhkien tunnistamisessa ja kokonaiskuvan tuottamisessa, mutta niiden konfigurointi vaati perehtymistä, ja eri laitteiden lokien jatkuva keräys saattaa olla kuormittavaa kevyelle laitteistolle. Tämä korostaa tarvetta tasapainottaa suojausratkaisut käytettävissä olevien resurssien mukaan.

Merkittävä oppi oli, kuinka kriittistä on ymmärtää protokollien ja tiedonsiirron toimintaperiaatteet — sillä vasta tällöin niiden liikennettä voi aidosti hallita.

6.3 Tulevaisuuden kehityskohteet

Jatkossa SoHo-verkkojen suojausta voisi kehittää edelleen seuraavilla toimenpiteillä.

SOAR-alustan (Security Orchestration, Automation and Response) käyttöönotto ja liittäminen SIEM-järjestelmään mahdollistaisi automaattisten vastatoimenpiteiden suorittamisen heti, kun SIEM havaitsee hälytyksen (Fortinet, n.d.). Käytännössä tämä nopeuttaisi reaktiota uhkiin: esimerkiksi jos Wazuh havaitsee haittaohjelmatartunnan päätelaitteella, SOAR voisi automaattisesti eristää kyseisen laitteen verkosta ja käynnistää haittaohjelman poiston. Tämä vähentäisi ihmistyön tarvetta ja toisi kohdistettua reagointikykyä, mikä on pienessä organisaatiossa arvokasta, kun omia resursseja on vähän. Automaation lisääminen toisi mukanaan myös yhdenmukaisuutta – jokainen toistuva uhkatilanne hoidettaisiin juuri suunnitellulla tavalla, nopeasti ja virheettömästi (Splunk, n.d.).

Uhkien havainnointikykyä voisi tehostaa hyödyntämällä tekoälyä ja koneoppimista. Tämä voisi tarkoittaa esimerkiksi anomaly detection -järjestelmää, joka oppii verkon normaalin käyttäytymismallin ja hälyttää poikkeamista (Kyberturvallisuuskeskus, 2022). Tekoälypohjainen valvontatyökalu osaisi havaita myös uudenlaisia uhkia, joita ei ole etukäteen kuvattu allekirjoituksina. Esimerkiksi se voisi tunnistaa, että tietty

käyttäjätili alkaa toimia epätyypillisesti (mahdollinen tilikaappaus), tai että jokin IoT-laite lähettää huomattavasti enemmän dataa kuin normaalisti (mahdollinen luvaton tiedonsiirto). Koneoppimismallit täydentäisivät nykyistä allekirjoitus- ja sääntöpohjaista IDS/IPS:ää tuomalla ennakoivan kerroksen: ne saattaisivat löytää uhan ennen kuin sille on edes julkaistu tunnistussignaalia. Tällaisen työkalun käyttöönotto lisäisi arvoa erityisesti jatkuvasti muuttuvien uhkien maailmassa, jossa aiemmin tuntemattomat hyökkäykset voivat muuten livahtaa suojauksen läpi.

Erillisen hallintaverkon (management VLAN), joka on fyysisesti ja loogisesti eristetty muista käyttäjäverkoista, rakentaminen varmistaisi, että edes sisäisessä verkossa mahdollisesti lymyävä hyökkääjä ei pääsisi käsiksi kriittisiin hallintapalveluihin. Tällä hetkellä OPNsense-palomuuri ja Wazuh-palvelin on toki suojattu palomuurisäännöin, mutta ne sijaitsevat osittain samoissa verkon osissa kuin käyttäjälaitteet. Hallinta-VLANissa kulkisi vain reitittimen, palomuurin, palvelimien ja tietoturvatyökalujen hallintaliikenne, ja siihen olisi pääsy vain valtuutetuilla ylläpitäjillä erillisestä portista tai VPN:n kautta. Tämä parantaisi turvallisuutta merkittävästi: vaikka hyökkääjä murtaisi käyttäjän päätelaitteen, hän ei pääsisi suoraan yrityksen palomuurin hallintaan, koska hallintataso on eri verkon puolella. Hallintaverkon eriyttäminen on yleinen parhaaksi katsottu käytäntö (Cisco, 2018), ja sen lisääminen SoHo-ympäristöönkin nostaisi suojauksen kypsyyttä.

Edellä mainitut kehityskohteet täydentäisivät nykyistä mallia. SOAR toisi automaattisen reagoinnin, koneoppiva analytiikka ennakoivan havaitsemisen ja hallintaverkon eriytys paremman eristysten myös sisäverkon tasolla. Jokainen näistä parannuksista vähentää inhimillisten virheiden mahdollisuutta ja vaikeuttaa hyökkääjän toimintaa entisestään, vieden rakennettua suojausmallia kohti entistä kypsempää yritystason tietoturvaa.

Lähteet

Barker, E., Dang, Q., Frankel, S., Scarfone, K., & Wouters, P. (2020). *Guide to IPsec VPNs* (SP 800-77 Rev.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-77r1

Bernstein, D. J., Lange, T., & Hamburg, M. (2015). Curve25519: New Diffie–Hellman speed records. *Lecture Notes in Computer Science*, *9215*, 207–228. https://doi.org/10.1007/978-3-662-46706-0_13

Cisco Systems. (2018). *Campus LAN and Wireless LAN Design Guide (Cisco Validated Design).* Haettu 13.8.2025, osoitteesta https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html

Cisco Systems. (2019). *Access Control Lists on ASA.* Haettu 13.8.2025, osoitteesta https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/217679-asa-access-control-list-configuration-ex.html

Cisco Systems. (2020, 15.1.). *RV Series: VPN Overview and Best Practices.* Haettu 13.8.2025, osoitteesta https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/1399-tz-best-practices-vpn.html

Cisco Systems. (2021). *Campus Switching Best Practices White Paper.* Haettu 13.8.2025, osoitteesta https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MS_Switching/Large_Campus_Switching_Best_Practices

CompTIA. (2021, 6.8.). Software vs. Hardware VPNs. Haettu 13.8.2025, osoitteesta https://www.comptia.org/en-us/blog/vpn-software-vs-hardware/

CrowdSec. (n.d.). *CrowdSec – Collaborative IPS documentation.* Haettu 13.8.2025, osoitteesta https://www.crowdsec.net/

Cyberscoop. (2019). *APT41: A dual espionage and cybercrime operation.* Haettu 13.8.2025, osoitteesta https://cyberscoop.com/apt41-fireeye-china/

Cybersecurity and Infrastructure Security Agency. (2021). *Supply chain compromise – SolarWinds.* Haettu 13.8.2025, osoitteesta https://www.cisa.gov/news-events/alerts/2021/01/07/supply-chain-compromise

Deering, S., & Hinden, R. (2017). *Internet Protocol, Version 6 (IPv6) Specification* (RFC 8200). Internet Engineering Task Force. https://doi.org/10.17487/RFC8200

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA. https://dl.acm.org/doi/proceedings/10.5555/1251375

ENISA – European Union Agency for Cybersecurity. (2024). *Threat Landscape 2024.* Haettu 13.8.2025, osoitteesta https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Hive Systems. (2023). *Password table 2023.* Haettu 13.8.2025, osoitteesta https://www.hivesystems.io/blog/are-your-passwords-in-the-green

Hostinger Tutorials. (n.d.). *What is a VPN and how does it work?* Haettu 13.8.2025, osoitteesta https://www.hostinger.com/tutorials/how-to-set-up-a-linux-vpn-server-with-openvpn

Hämeen ammattikorkeakoulu. (2023). *Tekoälyn käytön muistilista opiskelijoille*. Haettu 13.8.2025, osoitteesta https://digipedaohjeet.hamk.fi/ohje/tekoalyn-kayttajan-muistilista-opiskelijoille/

IEEE. (2018). *IEEE 802.3 Ethernet Standard.* Institute of Electrical and Electronics Engineers. https://standards.ieee.org/standard/802_3-2018.html

ISO/IEC. (1994). *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*(ISO/IEC 7498-1:1994). International Organization for Standardization.

Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., & Kivinen, T. (2014). *Internet Key Exchange Protocol Version 2 (IKEv2)* (RFC 7296). Internet Engineering Task Force. https://doi.org/10.17487/RFC7296

Kent, S., & Seo, K. (2005). *Security Architecture for the Internet Protocol* (RFC 4301). Internet Engineering Task Force. https://doi.org/10.17487/RFC4301

Kyberturvallisuuskeskus. (2022). *Tekoäly tulee muuttamaan myös kyberhyökkäyksiä.* Haettu 13.8.2025, osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tekoaly-tulee-muuttamaan-myos-kyberhyokkayksia

McKay, K., & Cooper, D. (2019). *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (SP 800-52 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-52r2

National Security Agency [NSA]. (n.d.). *Cybersecurity Guidance.* Haettu 13.8.2025, osoitteesta https://www.nsa.gov/press-room/cybersecurity-advisories-guidance/

OPNsense. (n.d.). *OPNsense documentation.* Haettu 13.8.2025, osoitteesta https://docs.opnsense.org/

Palo Alto Networks. (n.d.). *What is a next-generation firewall (NGFW)?* Haettu 13.8.2025, osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-a-next-generation-firewall-ngfw

Plummer, D. (1982). *Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware* (RFC 826). Internet Engineering Task Force. https://doi.org/10.17487/RFC0826

Postel, J. (1980). *User Datagram Protocol* (RFC 768). Internet Engineering Task Force. https://doi.org/10.17487/RFC0768

Postel, J. (1981). *Internet Protocol* (RFC 791). Internet Engineering Task Force. https://doi.org/10.17487/RFC0791

Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3* (RFC 8446). Internet Engineering Task Force. https://doi.org/10.17487/RFC8446

Scarfone, K., & Hoffman, P. (2009). *Guidelines on Firewalls and Firewall Policy* (SP 800-41 Rev.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-41r1

Splunk. (n.d.). *The Essential Guide to Security Orchestration, Automation and Response.* Haettu 13.8.2025, osoitteesta https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation.html

Stallings, W. (2020). *Cryptography and network security: Principles and practice* (8th ed.). Pearson.

Suricata. (n.d.). *Suricata – Open Source IDS/IPS/NSM engine.* Haettu 13.8.2025, osoitteesta https://suricata.io/

Symantec. (2018). *Internet Security Threat Report, Volume 23.* Haettu 13.8.2025, osoitteesta https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Wazuh. (n.d.). *Wazuh documentation.* Haettu 13.8.2025, osoitteesta https://documentation.wazuh.com/