
Ville Vainikka

# SASE - Keskitetyn tietoliikennepohjaisen pilvinatiivin tietoturvajärjestelmän mahdollisuudet hajautetussa organisaatiossa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

4.5.2021

# Tiivistelmä


| | |
|---|---|
| Tekijä: | Ville Vainikka |
| Otsikko: | SASE - Keskitetyn tietoliikennepohjaisen pilvinatiivin tietoturvajärjestelmän käyttöönotto hajautetussa organisaatiossa |
| Sivumäärä: | 45 sivua |
| Aika: | 4.5.2021 |
| Tutkinto: | Insinööri (AMK) |
| Tutkinto-ohjelma: | Tieto- ja viestintätekniikan tutkinto-ohjelma |
| Ammatillinen pääaine: | IoT and Cloud Computing |
| Ohjaajat: | Lehtori Marko Uusitalo |


---


SASE on kaupallinen arkkitehtuurimalli, joka yhdistää tietoliikenne- ja tietoturvapilvipalvelujen markkina-alueet. Se mahdollistaa huomattavasti paremman tietoturvakontrollin aiempiin malleihin verrattuna, vaikka se sinällään ei tuo uusia ominaisuuksia. Mallia tarjotaan SaaS-palveluna, mutta onprem-ratkaisuja on myös olemassa.

Parempi tietoturva mahdollisestaan formalisoimalla ratkaisun arkkitehtuuri siten, että erilliset komponentit keskustelevat keskenään standardoidusti yhdessä pisteessä. Tällöin liikenteen käsittely on tehokkaampaa verrattuna aiempaan next-hop-malliin. Myös hallinta yksinkertaistuu, kun kaikki komponentit on hallittu yhdestä pisteestä.

SASE valikoitui internetin suojauksen malliksi valtionhallinnon TORI-ympäristössä uuden ratkaisun kehitysprojektin suunnitteluvaiheessa. Tähän sisältyi useiden eri ratkaisujen Proof-of-Value-tyylinen testaaminen. SASE:n implementoinnissa on haasteita, joista vähäisimpänä ei ole tietosuoja. Näistä kaikista selviydytään kuitenkin hyvällä suunnittelulla ja riskien ennakkoon tunnistamisella.

Arkkitehtuurimallin avulla saavutetaan aiempaan verrattuna huomattavasti turvallisempi tietojenkäsittely-ympäristö. Turvallisuuden lisäksi ratkaisu helpottaa niin loppukäyttäjien kuin ylläpidon työtä ja parantaa ympäristön tietoturvatapahtumien hallintaa huomattavasti: tarkoilla kontrolleilla ja selvillä herätteillä CSOC toiminnolle.



Avainsanat: tietoturva, kyberturvallisuus, tietoliikenne, pilvi

## Abstract


| | |
|---|---|
| Author: | Ville Vainikka |
| Title: | SASE – Centralized network based cloud native information security system deployment in decentralized organization |
| Number of Pages: | 45 pages |
| Date: | 4.5.2021 |
| Degree: | Bachelor of Engineering |
| Degree Programme: | Information and communications technology |
| Professional Major: | IoT and Cloud Computing |
| Instructors: | Marko Uusitalo, Senior Lecturer |


---


SASE is commercial architecture model, which combines networking and security cloud markets. It enables better security control compared to previous models, even though it does not bring any new features to the table. Model is offered as a SaaS service, but onprem solutions exist.

Better security is enabled by formalizing solution architecture in a way, where separate components communicate in a standardized way in a single point. This enables efficient traffic processing, compared to previous next-hop model. Administration is also simplified, when all the components are managed from a single point.

SASE was selected as internet's protection model in Finnish government's TORI-environment during new solution's development phase. This included testing multiple solutions in a Proof-of-Value style. SASE implementation is challenging, especially due to data protection aspect. However, all of the challenges are conquerable with good planning and risk recognition and management.

The final product is more secure data processing environment. On top of security, the solution eases both end user's and administration's work and improves the environment's security incident management with granular controls and clear indicators to CSOC team.



Keywords: information security, cyber security, networking, cloud

## Sisällys

## Lyhenteet

| | |
|---|---|
| AAA | Authentication, Authorization, Accounting, kirjautumisprosessi, jossa identiteetti validoidaan, sille määritetään käyttöoikeustaso ja tapahtuma lokitetaan. |
| breakout | Piste, josta tietoliikenne lähtee ulos organisaation hallusta. Esimerkiksi internetiin suunnattu liikenne monesti puhkeaa internet-palomuurilta ISP:n liittymään ja verkkoon jatkovälitettäväksi. |
| CA | Certificate Authority, varmenneauktoriteetti, myöntää allekirjoittamalla muita varmenteita, jotka ovat joko alempia CA-varmenteita tai EE-varmenteita. |
| CASB | Cloud Access Security Broker, pilvipalvelujen käytönhallinta-järjestelmä, jossa kohdepalvelun käyttöoikeus validoidaan ja käyttöä seurataan myös käytön aikana ja käyttöoikeutta voidaan muuttaa kesken käytön RBA:n perusteella. |
| CDN | Content Delivery Network, vahvasti hajautettu jakelujärjestelmä, joka välimuistaa sisältöä niin, ettei sitä tarvitse hakea kohdepalvelusta asti. |
| CSOC | Cyber Security Operations Center, eli kyberturvallisuusvalvomo, jossa valvotaan valvomohenkilökunnan toimesta yleensä 24/7-tietojenkäsittely-ympäristön tietoturvan tilaa, päätyökaluina SIEM ja SOAR. |
| CSPM | Cloud Security Posture Management, pilvipalvelun tietoturvan tason hallinta, valmiiden pilvipalveluiden tietoturvakonfiguraation tarkastuslista perustuen valmiisiin malleihin ja mahdollisuus muuttaa konfiguraatiota palvelun ulkopuolelta parempaan suuntaan keskitetysti. |
| DLP | Data Loss Prevention, tietovuotojen ehkäiseminen, jakautuu kahteen eri ratkaisuun, joko tietoliikenteen reaaliajassa läpikäynti ja siinä virtaavien tietojen tarkistaminen tai jo siirrettyjen tiedostojen tarkistaminen jälkikäteen kohdepalvelusta API:n kautta erikseen. |
| DTLS | Datagram Transport Layer Security, TLS UDP-liikenteelle. |
| EDR | Endpoint Detection and Response, päätelaitteille asennettava ohjelmisto yleensä anti-virus-ohjelmiston lisäksi, joka valvoo päätelaitteella tapahtuvia toimintoja ja pystyy tarvittaessa myös toimimaan, esimerkiksi sammuttamalla prosessin tai eristämällä työaseman. |
| EE | End-Entity, client-varmenne. |

| | |
|---|---|
| ESSO | Enterprise Single Sign-On, suuri kirjautumisjärjestelmä, johon voidaan tavalla tai toisella liittää periaatteessa kaikki organisaation kirjautumistarpeet ja IDP:t. |
| FWaaS | Firewall as a Service, palomuuri palveluna, suodatin, joka toimii yleensä L2-4-tasoilla ja tarkistaa paketteja sekä niistä muodostuvia protokollia ja sessiota. |
| GRE | General Routing Encapsulation, yleinen reititys enkapsulaatio-protokolla, jossa IP paketin päälle laitetaan toisen IP-paketin otsake, mahdollistaa VPN yhteydet mutta ei salaa |
| hop | Tietoliikenteen reitityspiste. Tietoliikenteen kulkema polku lähteestä kohteeseen muodostuu hypyistä, jotka monesti ovat fyysisiä laitteita. |
| IDP | Identity Provider, abstraktiokerros, jonka läpi haetaan ja varmistetaan käyttäjän identiteetti AAA-prosessissa. |
| IDPS | Intrusion Detection and Prevention System, tietoliikennetietoturva-järjestelmä, joka skannaa läpi tietoliikennettä reaaliajassa ja koettaa havaita sieltä uhkia ja voi halutessaan katkaista yhteyden. |
| Ipsec | Internet Protocol Security, L3-tason IP-protokolla, jolla voidaan salata liikenne (ESP) tai validoida sen muuttumattomuus (AH). |
| JA3 | Metodi TLS-clienttien sormenjäljentämiseen TLS-kättelyn tiedoista, mahdollistaa clienttien tunnistamisen ilman, että liikennettä tarvitsee purkaa. |
| mTLS | Mutual TLS authentication, yhteinen TLS tunnistus, molemmat TLS kättelyn osapuolet tunnistautuvat toisilleen eli palvelimen tunnistautumisen clientille lisäksi myös client tunnistautuu palvelimelle. |
| NaaS | Network as a Service, ostat tietoliikenne toimintaa palveluna, toteutetaan pilvestä. |
| NSaaS | Network Security as a Service, ostat tietoliikenne turvallisuutta palveluna, toteutetaan pilvestä. |
| onprem | On Premises, eli paikallisesta konesalista tarjottu palvelu, voidaan asentaa omaan konesaliin. |
| PFS | Perfect Forward Secrecy, salauksen aloituskättelyn autentikaation yhteydessä generoidaan oma sessiokohtainen yksityinen avain, eikä käytetä autentikaatioon käytetyn varmenteen omaa yksityistä avainta. Jos käytetty yksityinen avain paljastuisi, voitaisiin näillä tiedoilla purkaa tietoliikenne nauhoituksesta vain kyseinen yksittäinen sessio, eikä kaikkia miljoonia sessiota, joita palvelussa on sen varmenteen käytön aikana ollut. |

| | |
|---|---|
| pilvi | Cloud, kolmannen osapuolen linux-palvelimia suuressa keskitetyssä konesalissa, jonne ei ole pääsyä. |
| PKI | Public Key Infrastructure, julkisten avainten infra, eli varmenne-järjestelmä. Koostuu yhdestä tai useammasta CA:sta ja muista järjestelmistä, joilla pyritään takaamaan järjestelmän luottamuksellisuus. |
| PoP | Point-of-Presence, hajautetuissa pilvijärjestelmissä sama palvelu on saatavilla useasta geolokaatiosta, joiden yhteyspisteitä eli konesaleja kutsutaan popeiksi. Esimerkiksi Teamsin Suomea lähin PoP on Frankfurt am Mainissa sijaitseva konesali. |
| QoS | Quality of Service, palvelun laatu, IP pakettien headeri, johon voidaan määrittää paketin prosessointi prioriteetti, siten että tärkeämmät paketit prosessoidaan aina ensin. |
| RBA | Risk Based Access, riskipohjainen käyttöoikeusmalli, joka nojaa RBAC, mutta jatkokehittää sitä ottamalla huomioon myös muita asioita ja mahdollistaa käyttöoikeuksien dynaamisen muuttamisen kesken käytön laskennallisen riskikertoimeen perustuen. |
| RBAC | Role Based Access Control, roolipohjainen käyttöoikeusmalli, käyttöoikeudet määritetään organisaation roolin pohjalta kirjautumisen yhteydessä. |
| RBI | Remote Browser Isolation, selaimen virtualisointi proxy ratkaisulla siten, että clientille lähetetään vain kuvaa virtualisoidusta selaimesta, selattava tieto ei pääse clientille asti. |
| RTC | Real-Time Communication, yleinen termi kommunikaatiojärjestelmälle, jolla voi viestittää ja soittaa ääni- tai videopuheluita reaaliajassa. |
| SaaS | Software as a Service, ostat vain sovelluksen käyttöoikeutta palveluna, toteutetaan pilvestä. |
| SIEM | Security information and event management, tietoturvatiedon ja tapahtumien hallintajärjestelmä eli järjestelmä, jossa aggregoidaan kaikki ympäristön tietoturvakomponenteilta tulevat herätteet (lokit). |
| SOAR | Security orchestration, automation and response, automatisointityökalu SIEM:n tueksi, jossa tapahtumat voidaan käsitellä ja niihin voidaan mahdollisesti myös vastata. |

| | |
|---|---|
| SWG | Secure Web Gateway, web proxyn seuraaja, joka yleensä voi tehdä myös sisällön tarkistusta, koska se purkaa HTTPS-sessiot käsittelypisteellä ja salaa ne uudestaan käsittelyn jälkeen. |
| tenantti | "Asukas", organisaation oma asiakaskohtaisesti rajattu ympäristö pilvipalvelussa, jota voidaan räätälöidä. |
| TLS | Transport Layer Security, siirtotason suojaus, TCP-pohjainen SSL-protokollan seuraaja, jolla muodostetaan salaus esim. HTTPS-yhteyksissä. |
| TrafficShaping | Liikenteen muotoilua, liikenteelle voidaan pisteessä määrittää maksimikaista, jonka jälkeen ylimenevä liikenne joko jonotetaan maksiarvoon tai leikataan. Tällä estetään laitteen ylikuormittuminen tai valvotaan sovittua kaistan käyttöä. |
| VPN | Virtual Private Network, virtuaalinen yksityinen verkko, IP-yhteyden sisään encapsuloidaan toinen yhteys, jossa käytetään toisia IP-osoitteita, jolloin sovellus voi kommunikoida näillä virtuaalisilla osoitteilla, eikä sen tarvitse tietää, mitä välittävällä kerroksella tapahtuu. Hyvin yleisesti tämä tunneli lisäksi salataan, jolloin puhutaan esimerkiksi IPsec VPN tai SSL VPN:stä. |
| WAAPaaS | Web Application and API Protection as a Service, verkkosovelluksen ja rajapintojen suojaus palveluna, mikä tarkoittaa WAF:ia, joka kykenee molempien käyttötapauksien suojaamiseen. |
| WAF | Web Application Firewall, verkkosovelluspalomuuri, joka L2-4 sijaan toimii L7-tasolla, eli suodattaa HTTP-protokollan pyyntöjä ja sen payloadien sisältöjä. Tällä voidaan estää esim. SQL-injektioita tai muita haitallisia pyyntöjä ilman, että suojaaminen tarvitsee tehdä itse web-sovelluksessa. |
| ZTNA | Zero Trust Network Access, malli, jossa jokainen sessio autentikoidaan ja validoidaan erikseen, jatkuvasti ja yleensä vielä ennen kirjautumista itse palveluun, jolloin ennen kirjautumista ZTNA:n läpi ei kohdepalvelu ole tietoliikenteellisesti edes tavoitettavissa. |

# 1 Johdanto

Tämä dokumentti on kirjoitettu ollessani tietoturva-arkkitehtinä Valtion tieto- ja viestintätekniikkakeskus Valtorissa, jossa yhtenä työtehtävänäni on kehittää valtionhallinnon TORI-ympäristön [1] internetin käytön suojausta. Päädyimme omassa kehitystyössämme lopputulokseen, että SASE on järkevin arkkitehtuurimalli kyseiseen ympäristöön. Kipinä opinnäytetyön kirjoittamiseen tuli hieman myöhemmin. Siihen yhdistyi toive, että aiheesta opittu hyödyntäisi muitakin.

Dokumentissa on tarkoitus kuvata itse mallia ja miten sen avulla pystytään ratkaisemaan niin teknisiä kuin hallinnollisia haasteita tietoliikenteen ja tietoturvan osa-alueilla.

Dokumentin ymmärtämiseksi lukijalla oletetaan olevan hyvät perustiedot niin moderneista tietoliikenneteknologioista, kuin moderneista tietoturvaratkaisuista. Dokumentissa tullaan käsittelemään paljon teknologioita ja lyhenteitä, joita kaikkia ei opinnäytetyön laajuudessa pystytä käymään läpi, mutta tärkeimmät on pyritty avaamaan sanastossa.

# 2 Mikä SASE on

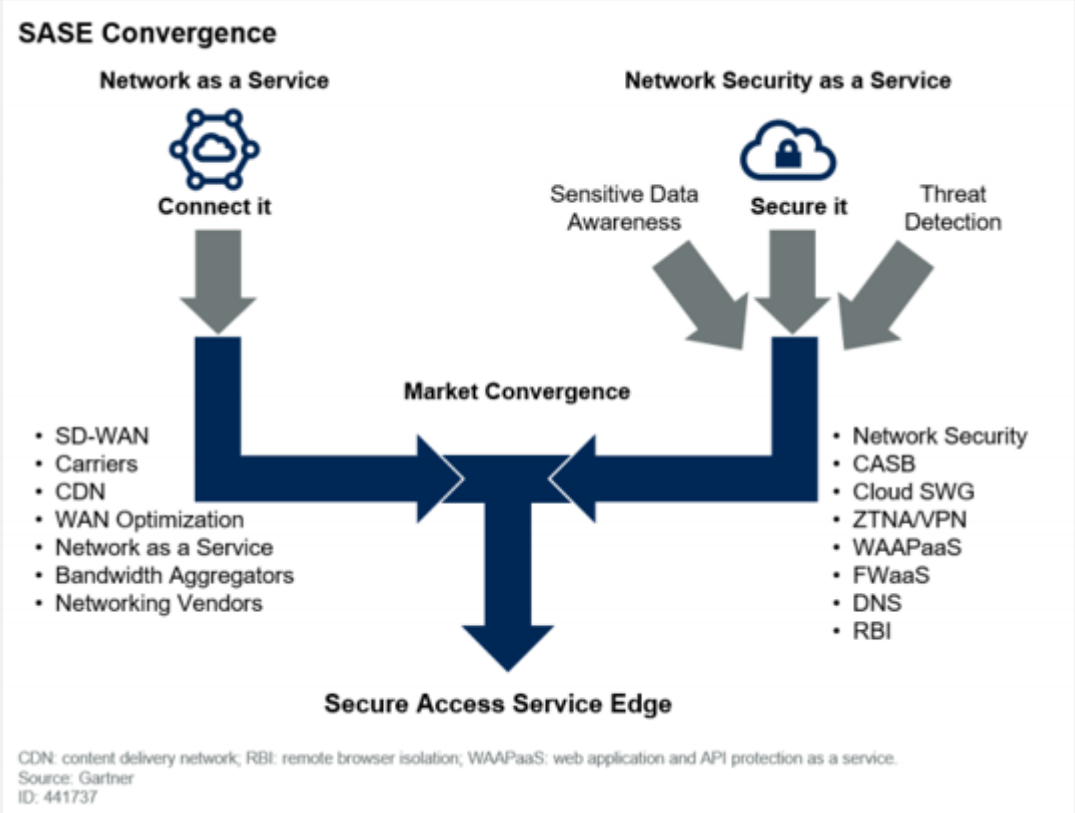
## 2.1 Alkuperä

*SASE* eli *Secure Access Service Edge* on globaalin tutkimusyrityksen Gartner Inc:n 2019 lanseeraama termi markkinatutkimuksessaan *“The Future of Network Security Is in the Cloud”* [2]. Suomeksi se voisi kääntyä esimerkiksi *Turvallinen pääsypalvelu (pilven) reunalla*.

Itse malli ei ole Gartnerin keksimä, vaan enemmänkin heidän yhteenvetonsa markkinatutkimuksesta, jonka mukaan SASE on hyvä ja toimiva malli. Ennen sitä

markkinoilla oli useita valmistajakohtaisia termejä, jotka johtivat juurensa jokaisen valmistajan omaan tuotekehityspolkuun.

Mallina SASE on yksinkertainen. Tämä on kilpailuetu markkinoilla, sillä tekninen ympäristö on hyperkompleksi. Termin lanseerauksen jälkeen valmistajat, jotka tekivät jo tätä, ottivat sen hyvin nopeasti käyttöön [3]. Myös loput valmistajat alkoivat muokkaamaan omia tuotteitaan samaan suuntaan.



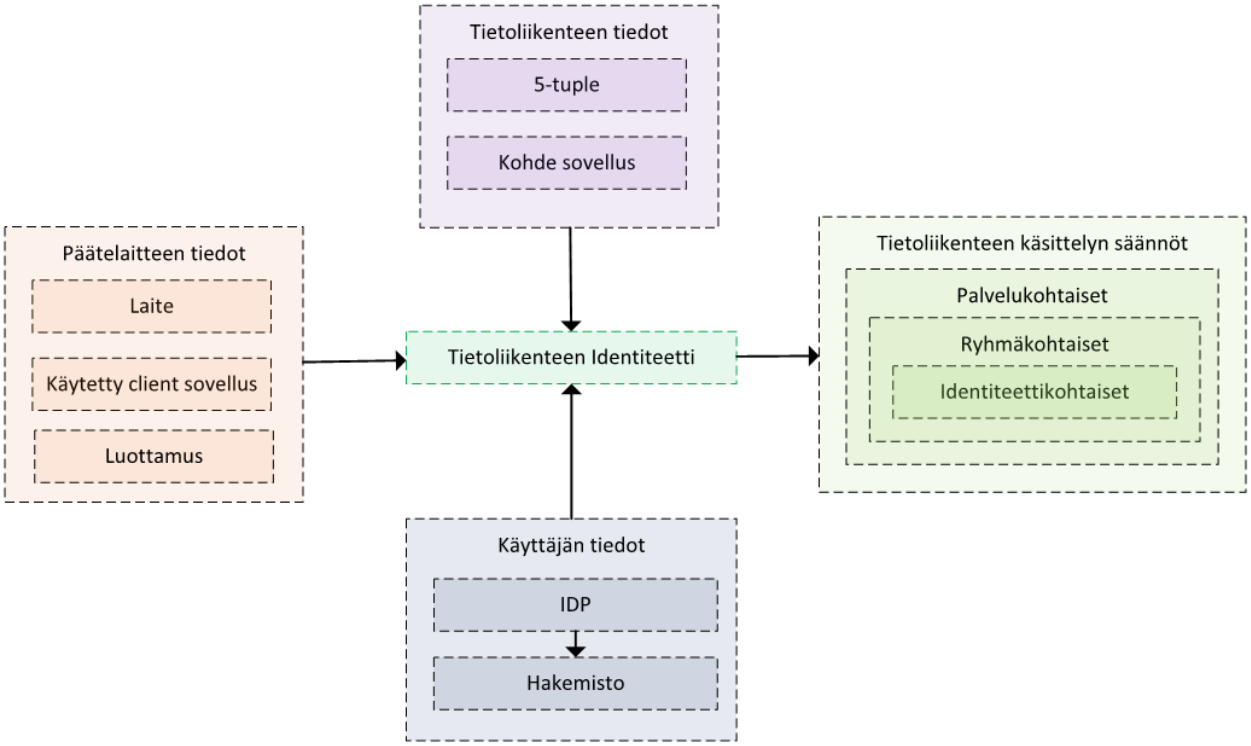

Kuva 1. Markkinoiden yhteenliittymä Gartnerin mainitusta raportista, joka kuvaa aiem-pien NaaS- ja NSaaS-markkinoiden yhdistymistä SASE:ksi.

## 2.2 Arkkitehtuurimalli

SASE on ennen kaikkea arkkitehtuurimalli, eikä se ota suoraan kantaa tarkkoihin teknologioihin tai komponentteihin, joita implementaatio pitää sisällään. Tärkeintä SASE-mallissa on siirtyminen laite- tai IP-pohjaisesta tietoliikenteen hallinnasta ja käsittelystä identiteettipohjaiseen käsittelyyn. Laite- ja IP-tieto ei sinänsä häviä

mihinkään, vaan niiden päälle on rakennettu oma identiteettiabstraktiokerros, jota käytetään liikenteen käsittelyssä.

Tämä identiteetti voi sisältää tarkentavia metatietoja, kuten IP-osoite, tietoliikennettä generoivan laitteen, sovelluksen tai käyttäjän identiteetti. Metatiedot voivat olla hankittuja eri tavoilla ja eri lähteistä.




Kuva 2. Identiteettitiedon muodostaminen yleisellä tasolla ja siinä käytetyt tiedot.

SASE on huomattava muutos vanhaan tapaan toimia, jossa verkon tietoliikenne- ja tietoturvakomponentit käsittelivät itse liikennettä yleensä sessio- tai IP-pohjaisesti. Nämä komponentit eivät useinkaan olleet synkronissa keskenään. Tämä oli ja on vieläkin ongelma tietoturvatapahtumien hallintaprosesseissa ja sitä varten on kehitetty huomattava määrä teknologioita kompensoimaan lähdetietojen vaihtelevuutta.

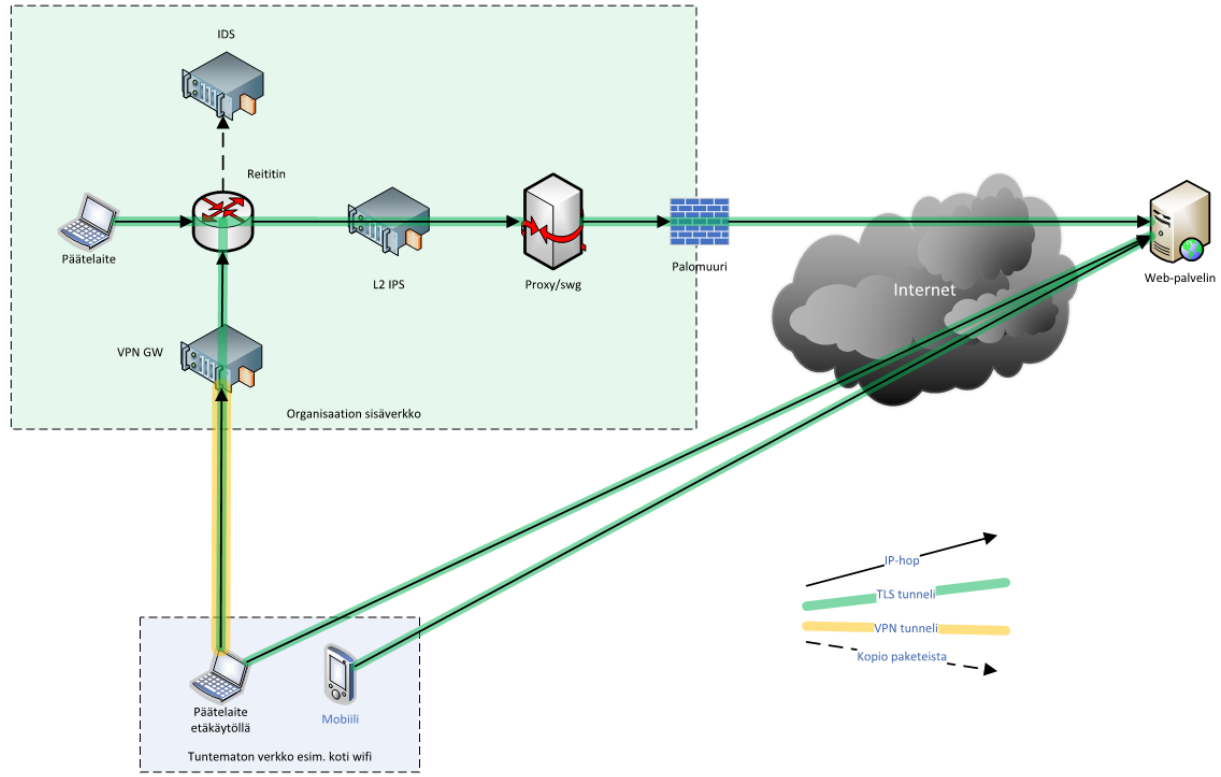
Toinen tärkeä ominaisuus SASE-mallissa on yksinkertaistettu tietoliikenteen välitysmalli, missä on vain yksi käsittelypiste tietoturvaan liittyen. Tämä helpottaa huomattavasti järjestelmän asennusta, käyttöönottoa ja ylläpitoa, sillä muutokset

voidaan kaikki tehdä yhden käyttöliittymän kautta ja pilviskenaariossa itse asennusvaihetta ei edes ole. Tämä mahdollistaa ylläpidon keskittymisen järjestelmän konfiguraation tarkentamiseen, kun aikaa ei kulu eri komponenttien yhteistoiminnan varmistamiseen.

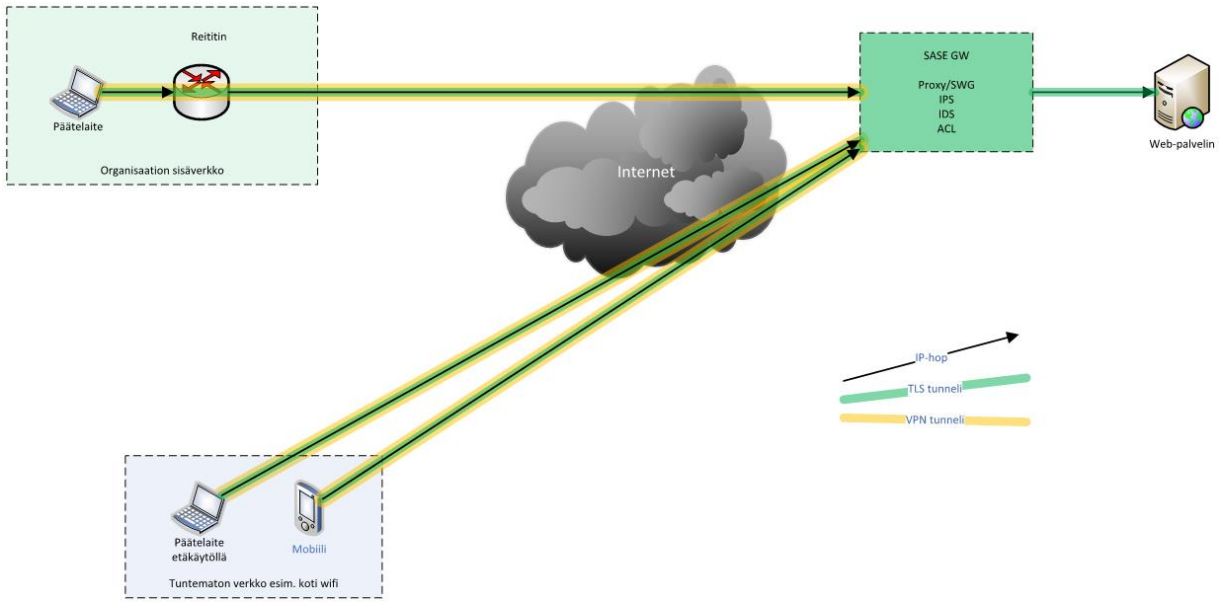
Lähes kaikki SASE-ratkaisut vaativat kuitenkin täysillä ominaisuuksilla toimiakseen päätelaitteille jonkinlaisen client-ohjelmiston, jolla liikenne voidaan valikoida ja tunneloida yhdyskäytävälle. Tunneli on tyypiltään joko D/TLS-, IPsec- tai GRE. Tunneli voidaan yleensä toteuttaa myös linjalla olevalta verkkolaitteelta, esimerkiksi palomuurilta, mutta tällöin kaikki ominaisuudet eivät yleensä ole käytettävissä.

Sovellusvaatimus johtuu tarpeesta autentikoida käyttäjä välittömästi, jotta tietoliikennettä voidaan käsitellä tarkasti ja käyttäjälle määritettyjen politiikkojen mukaisesti. Tuettuina ovat yleisimmät päätelaitteet ja käyttöjärjestelmäyhdistelmät (PC/Windows, PC/MacOS, Mobiili/Android, Mobiili/IOS). Linux-tuki on monella valmistajalla vielä tulossa tai sitä ei ole tuotteistettu, mutta se on toteutettavissa.

Client-yhteys on mahdollista muodostaa ilman loppukäyttäjän toimenpiteitä, jolloin käyttäjä ei välttämättä tiedä ratkaisusta mitään. Hyvänä ominaisuutena nämä client-sovellukset ovat yleensä hallittavissa yhdyskäytävältä eivätkä vaadi erillisen konfiguraationhallintatuotteen käyttöä niiden asetusten tai binäärien päivityksessä.




Kuva 3. Kehittyneen organisaation yleinen internetin käytön suojauksen next-hop-arkkitehtuurimalli




Kuva 4. Kehittyneen organisaation yleinen internetin käytön suojauksen SASE-arkkitehtuurimalli

Molemmissa malleissa tehdään samat turvatoimenpiteet. SASE-mallissa kaikki päätelaitetyypit ovat mukana. Lisäksi käyttäjän liikennettä voidaan arvioida käyttäjän kaikilta laitteilta yhtä aikaa, esimerkiksi riskiprofiilin muodostamiseksi. Suoja ei ole myöskään paikkariippuvainen esimerkiksi toimistoverkoista tai käyttäjän toimista sisäverkon VPN-ratkaisun päälle kytkemiseksi. Suoja on aina päällä, myöskin sisäverkossa ollessa, toisin kuin esimerkiksi client-VPN-ratkaisut.

Lisäksi tietoturvatapahtumien hallinnan näkökulmasta lokit saadaan yhdestä paikasta standardiformaatilla, eikä jokaisesta turvakontrollista tarvitse rakentaa erillistä parseria SIEM/SOAR-ratkaisuille.

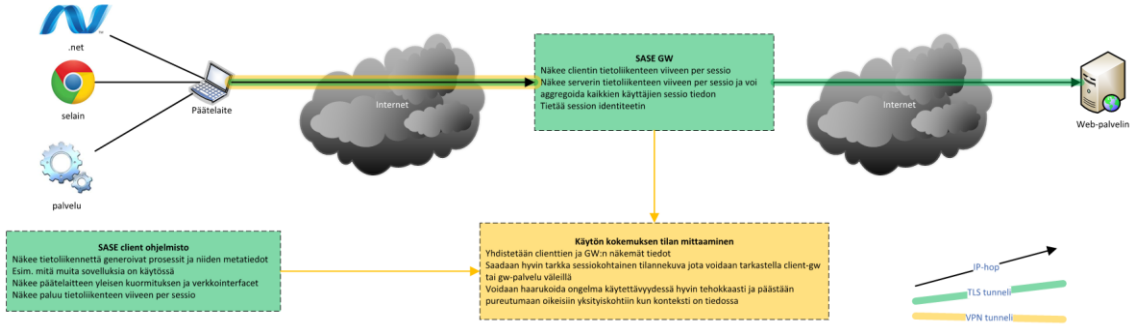
## 2.3 Tietoliikenne

Tietoliikennenäkökulmasta SASE-malli tarjoaa organisaatiolle mahdollisuuksia, etenkin jos siirtymää SDN-pohjaisiin [4] ratkaisuihin ei ole vielä tehty. Merkittävimmät ominaisuudet ovat yhden pisteen hallinta ja näkyvyys, SaaS-kiihdytys ja SDN.

Yhden pisteen hallinta mahdollistaa muun muassa tarkan konfiguroinnin kaikelle internetin suunnan liikenteelle. Tällöin osaa konfiguraatiosta ei jouduta tekemään esimerkiksi proxy-ratkaisulle, internet-muurille, VPN-yhdyskäytävälle tai mobiilihallintajärjestelmään. Määrityksiä esimerkiksi QoS/Traffic Shaping:lle voidaan tehdä kohdepalvelun, lähdekäyttäjän tai organisaation perusteella.

### 2.3.1 Näkyvyys liikenteen sisälle

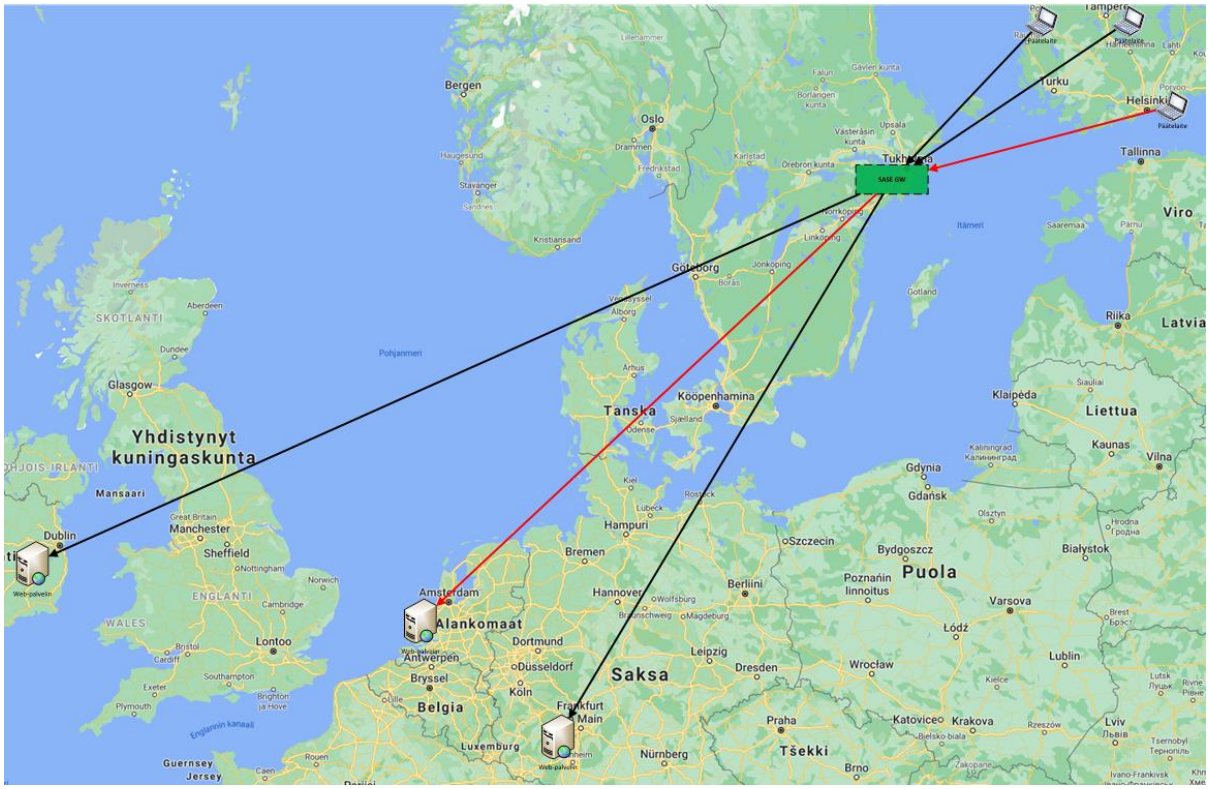
Näkyvyydessä SASE-ratkaisuilla on yleensä kolme valttikorttia: niiden sijainti reunalla päätelaitteen ja palvelun välissä, liikenteen purkukyvykkyys ja client-ohjelmisto. Nämä mahdollistavat todella tarkan metriikan ja sitä kautta diagnostiikkakuvan rakentamisen käyttötavan alusta loppuun (end-to-end).




Kuva 5. Käytön kokemuksen mittaaminen periaatetasolla.

Reunalla sijaitseminen mahdollistaa yleisen viiveen mittaamisen ja vahvan tilastotiedon muodostamisen päätelaitteen yhteyden kyvykkyydestä, sillä SASE-yhdyskäytävät sijaitsevat lähellä käyttäjää vahvojen runkoyhteyksien päässä. Yhdyskäytävällä on käytössään tuhansien päätelaitteiden sessiometriikat ja niistä muodostunut historiatieto, jolloin otannasta on helppo tehdä tilastotieteellistä analyysiä.

Reuna-konesaleissa on mittavat runkoyhteydet toisiin konesaleihin. Monet SASE-valmistajat ostavat tätä priorisoitua kaistaa tunnettuihin suuriin konesaleihin, jolloin viiveet yhdyskäytävältä voivat olla huomattavasti pienempiä tunnettuihin palveluihin kuin liikenteen reitittyessä julkisten AS:ien kautta kohdepalveluun.




Kuva 6. Käytön kokemuksen mittaaminen topologisesti. Kuvasta voidaan päätellä, että helsinkiläisellä päätelaitteella on ongelmia jo yhteydessä yhdyskäytävälle ja kaikilla päätelaitteilla on ongelmia amsterdamilaisen palvelun kanssa.

Liikenteen purkukyvykkyys mahdollistaa näkyvyyden liikenteen sisälle, mikä auttaa järjestelmää analysoimaan esimerkiksi eri HTTP-paluukoodeja. Tällöin voidaan päätellä, onko palvelun web-palvelimilla jotain tietoliikenteestä riippumatonta ongelmaa.

Client-ohjelmistolla voidaan mitata päätelaitteen konfiguraatiota ja tapahtumia. Näkyvyyttä voidaan saada esimerkiksi kotiverkosta. Esimerkiksi päätelaitteella X on aina ongelmia, kun se on kiinni Wifissä Y tai RTC-sovelluksen käyttö voi olla hidasta, koska selainprosessi vie kaiken laskentatehon, kun sillä katsotaan kryptattua videostreamia ja TLS-purku vie kaiken tehon.

### 2.3.2 SaaS-kiihdytys

Kiihdytys tässä tapauksessa tarkoittaa käyttökokemuksen parantamista optimoinnilla. Tähän on useita tapoja, joista yleisimmät ovat SASE-valmistajan ja SaaS-palvelutarjoajan tai SaaS-palvelun infran tarjoajan väliset sopimukset (SLA). Näissä luvataan runkoyhteyksille (backbone) parempaa suorituskykyä kuin julkisen internetin yli. Käytännössä tämä tarkoittaa priorisoitua kaistaa, jolloin viive palveluiden välillä saadaan mahdollisimman pieneksi, joka taas suhteessa nopeuttaa TCP-pohjaista tiedonsiirtoa [5].

Toinen yleinen tapa optimoida SaaS-palveluja on CDN-palveluiden käyttö. Niissä CDN-palvelu välimuistittaa yleisesti käytettyjä staattisia tiedostoja, jolloin niitä ei tarvitse hakea kohdepalvelusta asti. CDN-osuuksiin liittyy monesti myös SaaS-palveluiden PoP:ien määrittämisen optimointi. Palvelua pyritään käyttämään aina nopeimman yhteyden yli, joka ei välttämättä ole suoraan ole maantieteellisesti lähin PoP.

Lisäksi hyvin yleinen optimointi esimerkiksi TLS-kättelyihin on etukäteen valita käytettävät kryptoalgoritmit (cipher suite). Tunnelin muodostukseen vaaditaan, että client ja server ovat samaa mieltä valituista suitesta. Tämä on yleensä helppo toteuttaa, kunhan clientit ja kohdepalvelu tunnetaan. Optimointi jää kuitenkin monesti ylläpidolta tekemättä, koska perustoiminnallisuus, jossa client tarjoaa kymmeniä eri suiteja ja serveri voi hyväksyä kymmeniä, toimii, vaikka verraten hitaasti. Esimerkiksi Traficomin kovennusohje [6] jättää TLS1.2:lle 16 suitea mahdolliseksi, kun kättely tarvitsee vain yhden sopivan.

Esimerkkinä seuraavissa kuvissa on Metropolian hyvin toimiva oma.metropolia.fi-palvelu, josta myös löytyy optimoitavaa.

```
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 513
  Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 509
      Version: TLS 1.2 (0x0303)
    > Random: 240746f82cefbbba9719cb7e9fe4a7b143f221c9785f6f4f3a8b963196b5d46a
      Session ID Length: 32
      Session ID: a31313bf130ba76d00d3a6394cc9d291784031ea9ea7d1a95070ad41cd4a9ad5
      Cipher Suites Length: 32
    > Cipher Suites (16 suites)
        Cipher Suite: Reserved (GREASE) (0x9a9a)
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
        Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
        Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
```

Kuva 7. Windows 10 -työaseman Client Hellossa tarjoamat cipher suitet yhdistettäessä https://oma.metropolia.fi -palveluun. Kuva Wiresharkista.

```
Cipher Support
Testing 186 OpenSSL cipher suites matching "ALL:eNULL:aNULL"
  (execute "openssl ciphers 'ALL:eNULL:aNULL'" to see the list.)
--------------------
Cipher Tag                      Cipher Prot.  Key Ex.      Auth.     Encryption              MAC
ECDHE-RSA-AES256-GCM-SHA384     TLSv1.2       KX=ECDH      Au=RSA    Enc=AESGCM(256)         Mac=AEAD
DHE-RSA-AES256-GCM-SHA384       TLSv1.2       KX=DH        Au=RSA    Enc=AESGCM(256)         Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256     TLSv1.2       KX=ECDH      Au=RSA    Enc=AESGCM(128)         Mac=AEAD
DHE-RSA-AES128-GCM-SHA256       TLSv1.2       KX=DH        Au=RSA    Enc=AESGCM(128)         Mac=AEAD
ECDHE-RSA-AES256-SHA384         TLSv1.2       KX=ECDH      Au=RSA    Enc=AES(256)            Mac=SHA384
DHE-RSA-AES256-SHA256           TLSv1.2       KX=DH        Au=RSA    Enc=AES(256)            Mac=SHA256
ECDHE-RSA-AES128-SHA256         TLSv1.2       KX=ECDH      Au=RSA    Enc=AES(128)            Mac=SHA256
DHE-RSA-AES128-SHA256           TLSv1.2       KX=DH        Au=RSA    Enc=AES(128)            Mac=SHA256
ECDHE-RSA-AES256-SHA            TLSv1         KX=ECDH      Au=RSA    Enc=AES(256)            Mac=SHA1
DHE-RSA-AES256-SHA              SSLv3         KX=DH        Au=RSA    Enc=AES(256)            Mac=SHA1
DHE-RSA-CAMELLIA256-SHA         SSLv3         KX=DH        Au=RSA    Enc=Camellia(256)       Mac=SHA1
ECDHE-RSA-AES128-SHA            TLSv1         KX=ECDH      Au=RSA    Enc=AES(128)            Mac=SHA1
DHE-RSA-AES128-SHA              SSLv3         KX=DH        Au=RSA    Enc=AES(128)            Mac=SHA1
DHE-RSA-SEED-SHA                SSLv3         KX=DH        Au=RSA    Enc=SEED(128)           Mac=SHA1
DHE-RSA-CAMELLIA128-SHA         SSLv3         KX=DH        Au=RSA    Enc=Camellia(128)       Mac=SHA1
ECDHE-RSA-DES-CBC3-SHA          TLSv1         KX=ECDH      Au=RSA    Enc=3DES(168)           Mac=SHA1
DHE-RSA-DES-CBC3-SHA            SSLv3         KX=DH        Au=RSA    Enc=3DES(168)           Mac=SHA1
AES256-GCM-SHA384               TLSv1.2       KX=RSA       Au=RSA    Enc=AESGCM(256)         Mac=AEAD
AES128-GCM-SHA256               TLSv1.2       KX=RSA       Au=RSA    Enc=AESGCM(128)         Mac=AEAD
AES256-SHA256                   TLSv1.2       KX=RSA       Au=RSA    Enc=AES(256)            Mac=SHA256
AES128-SHA256                   TLSv1.2       KX=RSA       Au=RSA    Enc=AES(128)            Mac=SHA256
AES256-SHA                      SSLv3         KX=RSA       Au=RSA    Enc=AES(256)            Mac=SHA1
CAMELLIA256-SHA                 SSLv3         KX=RSA       Au=RSA    Enc=Camellia(256)       Mac=SHA1
AES128-SHA                      SSLv3         KX=RSA       Au=RSA    Enc=AES(128)            Mac=SHA1
SEED-SHA                        SSLv3         KX=RSA       Au=RSA    Enc=SEED(128)           Mac=SHA1
CAMELLIA128-SHA                 SSLv3         KX=RSA       Au=RSA    Enc=Camellia(128)       Mac=SHA1
DES-CBC3-SHA                    SSLv3         KX=RSA       Au=RSA    Enc=3DES(168)           Mac=SHA1
```

Kuva 8. https://oma.metropolia.fi-palvelun tarjoamat cipher suitet. Enumeroitu OpenSSL 1.1.1c FIPS:llä.

### 2.3.3 SDN - Software Defined Networking

Kaikki SASE-ratkaisut ovat SDN-ratkaisuja, jotka mahdollistavat tietoliikenteen manipuloinnin tarkalla tasolla ilman suoria rautapohjaisia rajoituksia. Monessa SASE-ratkaisussa on sisäänrakennettuna SD-WAN-kyvykkyyksiä. Ne vaihtelevat paljon eri tuotteiden välillä ja osassa niitä ei ole ollenkaan. SASE-kontekstissa SD-WAN tarkoittaa onprem VPN -konsentraattoria, joka voi muodostaa full mesh VPN -tunneleita niin muiden onprem-yhdyskäytävien kuin SASE:n SaaS-yhdyskäytävän kanssa.

SASE-mallin käyttöönoton jälkeen sisäverkon tarve voi vähentyä ulkoisten palveluiden käyttöön. Liikennettä ei tarvitse enää kierrättää sisäverkon tietoturvakomponenteilla, vaan se voidaan ohjata (breakout) lähimmältä hypyltä, oli se sitten itse päätelaite tai toimistoreititin, kohti SASE-yhdyskäytävää. Tällä voi olla pitkällä tähtäimellä suuria vaikutuksia. Jos onprem-palveluille ei ole enää tarvetta tai ne voidaan julkaista ZTNA:n kautta internetin yli, niin tarve suojatuille toimistoverkoille, WAN-liittymille tai runkoverkolle vähenee merkittävästi. Internetin suunnan (North-south [7]) liikenne organisaatiossa on nykyään yleensä suurin tiedonsiirto kapasiteetilla mitattuna, jos mukaan ei lasketa konesalien sisäistä (East-west) liikennettä.

Tämä mahdollistaa merkittävän organisaation tietoliikennearkkitehtuurin muutoksen, jossa sisäverkosta voidaan päätelaitteiden näkökulmasta luopua. Lisäksi tämä mahdollistaa tietoturvanäkökulmasta kaikkien verkkojen käsittelyn luottamattomina siirtomediona. Tällöin riittää, että päätelaite, käyttäjän identiteetti ja verkon yli ajettu tunneli ovat luotettuja.

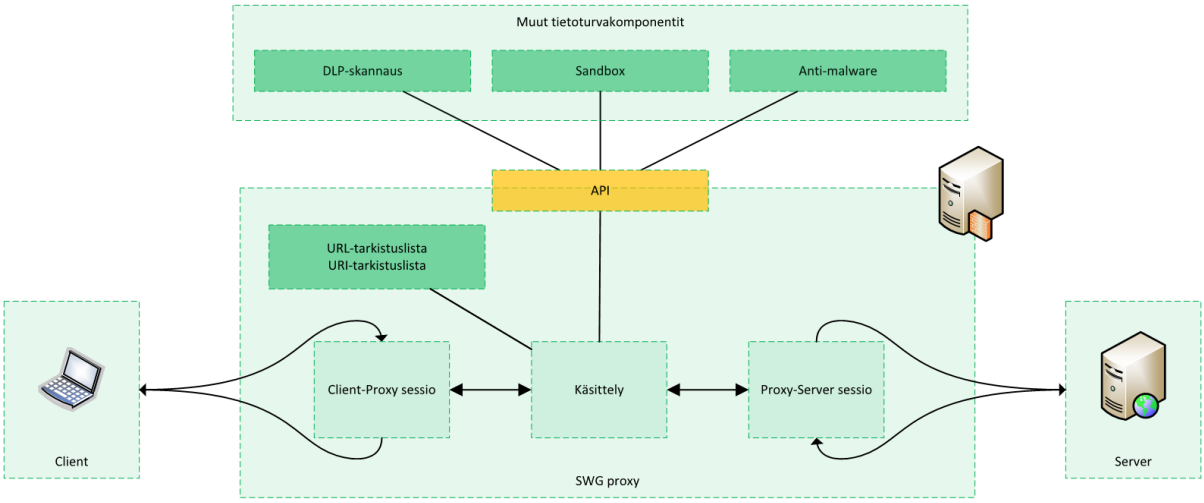
## 2.4 Tietoturvakomponentit

SASE on ensisijaisesti ohjelmistopohjainen modulaarinen tietoturvaratkaisu. Tämä tarkoittaa, että monet ominaisuudet järjestelmässä voidaan ottaa lisenssillä käyttöön tarvittaessa. Peruspalvelu sisältää vain minimin, joka yleensä tarkoittaa vain SWG-ominaisuutta.

### 2.4.1 SWG - Secure Web Gateway

SWG on SASE-mallin tärkein komponentti, koska se mahdollistaa proxy-arkkitehtuurillaan muut ominaisuudet. Tämä on seuraamus hyvin yleisestä liikenteen salaamisesta, yleisimpänä esimerkkinä HTTPS-protokollan käyttö. Jotta sisältöä voidaan käsitellä, tulee salaus purkaa (SSL decryption). Proxy-arkkitehtuurissa proxypalvelin tekee sekä transparent forward proxy- että reverse proxy -rooleja. Salauksen purku toteutetaan rakentamalla MItM-järjestely [8] clientin ja serverin väliin. Sen esivaatimuksena on, että clienteille on asennettu luotetuksi proxyn käyttämä CA.

Purku tapahtuu käytännössä siten, että proxy-palvelin ilmoittaa clientille olevansa pyydetty palvelin ja generoi reaaliajassa clientin luottaman PKI:n CA:lla pyydetyn palvelun EE-varmenteen. Tällöin client voi luotetusti muodostaa TLS-session palvelimen kanssa, kuin se olisi oikeasti pyydetty palvelu. Samaan aikaan proxy-palvelin muodostaa yhteyden kohdepalvelimelle ja esiintyy clienttinä ja muodostaa tähän oman TLS -session. Tämän jälkeen proxy-palvelin pystyy vapaasti käsittelemään kaiken clientin ja serverin välisen liikenteen olettaen, ettei sitä ole vielä erikseen salattu. SWG yleensä itse hoitaa HTTP-pohjaisen suodatuksen, eli URL, URI tai muiden HTTP request/response -koodeihin perustuvat säännöt ja niistä aiheutuvan lokituksen.




Kuva 9. Proxy-arkkitehtuuri ja miten se mahdollistaa tietoturvakomponenttien toiminnan.

### 2.4.2 IDP - Identity Provider

Identity provider on tärkeä komponentti SASE:ssa, jonka avulla saadaan identiteetti kaikelle tietoliikenteelle. Järjestelmissä on aina oma sisäinen IDP, mutta yleisesti hyvä toimintatapa on käyttää organisaation jo olemassa olevaa IDP:tä, oli se sitten pilvipohjainen ratkaisu (AAD, Okta tms) tai onprem AD.

### 2.4.3 Palomuuri – Advanced Cloud Firewall

SASE:n palomuuri mahdollistaa liikenteen tarkan suodatuksen 5-tuple- tai sovelluspohjaisesti sekä suodatuksen lokituksen. Erikseen huomioitavaa tässä kuitenkin on, että koska järjestelmän läpi menee hyvin paljon tietoliikennettä, voi tästä generoitua myös massiivinen määrä lokia.

### 2.4.4 IDPS - Intrusion Detection and Prevention System

SASE:n IDPS käy läpi liikenteen reaaliajassa ja pyrkii havaitsemaan siitä sormenjälkiä, joiden perusteella session riskiarvioita voidaan korottaa ja tarvittaessa myös estää.

### 2.4.5 Sandbox

Jos tietoliikenteestä huomataan jonkun komponentin osalta tiedostoja, joiden suorittamisesta voidaan arvioida aiheutuvan mahdollisesti uhka, voidaan tiedostosta ottaa kopio ja lähettää se Sandboxiin. Sandbox on virtualisoitu päätelaite ajossa, jonka sisään tiedosto syötetään ja suoritetaan. Suoritusta valvotaan, käyttäytyykö se oletetusti vai toimiiko se mahdollisesti epänormaalisti, jolloin voidaan tarvita jatkotoimenpiteitä.

Sandboxia käytettäessä voidaan käyttäytyminen yleensä määrittää erikseen. Esimerkiksi kun tiedosto nähdään ensimmäisen kerran, käytetään se Sandboxissa, ja sen tiiviste (hash) otetaan talteen. Seuraavalla kerralla tiedoston hashia verrataan jo tarkistettujen tiedostojen hasheihin, ja jos tiedosto on jo tarkistettu, niin

tiedostoa ei välttämättä tarvitse käyttää Sandboxissa. Sandboxiin voidaan yleensä myös määrittää, tuleeko tarkistettavan tiedoston läpimenoa viivästyttää ennen kuin se on tarkistettu, vai riittääkö mahdollinen hälytys lokille tai loppukäyttäjälle jälkikäteen.

Sandboxeista on useampia malleja eri käyttöjärjestelmille, mutta yleisimpiä ovat Windows-pohjaiset. Osalla valmistajista on myös MacOS-pohjaisia ratkaisuja. On myös yleistä, että kolmannen osapuolen Sandboxin käyttö on mahdollistettu rajapinnan (API) kautta.

### 2.4.6 DNS – Domain Name System

DNS:llä tarkoitetaan Protective DNS -ratkaisua [9], jossa DNS-proxy -ominaisuudella käydään DNS-clienttien lähettämät kyselyt ensin läpi ja verrataan listoihin tunnetuista huonoista domain-tietueista, ennen kuin vastaus clientille muodostetaan. Tätä ominaisuutta voidaan käyttää niin haittaohjelmien (malware) komentokanavia (C2) kuin aggressiivista mainostamista vastaan.

### 2.4.7 DLP - Data Loss Prevention

DLP-ratkaisun tavoite on estää tai ainakin pyrkiä hallitsemaan suojattavan tiedon exfiltraatiota organisaation hallusta. Käytännössä tätä tehdään kahdella eri tekniikalla, joko läpikäymällä tietoliikennettä reaaliajassa (Data In Transit, DIT) tai tarkastamalla se jälkikäteen (Data At Rest, DAR). Molemmissa ratkaisuissa on omat hyvät ja huonot puolensa.

DIT-ratkaisuissa reagointikyvykkyys on välitön, ja se voidaan laittaa päälle kaikelle liikenteelle. Jotta datan läpikäynnistä ei aiheudu liikaa viivettä käyttäjälle, tarvitaan paljon kallista laskentakapasiteettia ja sen lisäksi käytettyjen tarkistussääntöjen tulee olla hyvin suunniteltuja ja tarkasti kohdennettuja. DIT-ratkaisut yleensä vaativat jatkuvaa optimointia alati muuttuvan ympäristön johdosta. Jos säännöt ovat huonoja, ne eivät joko havaitse mitään tai laskentakapasiteetti ei tule riittämään niiden pyörittämiseen.

DAR-ratkaisuissa voidaan päästä lähelle reaaliaikaisuutta. Sen haaste on, että kohdepalvelun tulee olla myös hallinnan piirissä tai sillä tulee olla julkaistu API, jonka kautta skannaus voidaan suorittaa. API:n tapauksessa kohdepalvelu tulee olla otettu DLP-ratkaisun piiriin, eikä se siis toimi adhoc-tapauksiin, vaan ainoastaan erikseen rakennettuihin käyttötapauksiin.

### 2.4.8 CASB – Cloud Access Security Broker

CASB pitää tarkkaa kirjaa eri tuotteistettujen pilvipalveluiden käytöstä ja mahdollistaa organisaation SaaS-palvelujen julkaisemisen vain CASB:in kautta. Kohdepalvelut jaetaan yleensä sallittuihin (sanctioned) ja sallimattomiin (unsanctioned) ja niille voidaan tehdä sääntöjä niin palvelu-, käyttäjä-, ryhmä-, rooli- tai riskipohjaisesti. Luonteenomaista CASB-ominaisuudelle ovat vahvat valmistajan valmiiksi tuotteistamat mallit. Ylläpito voi yleensä päättää vain, miten kyseisiä palveluita arvioidaan organisaation näkökulmasta.

Erikseen mainittavaa CASB:ssa on yleensä sen vahva RBA:n käyttäminen. Käyttäjän toimien ja palveluiden maineiden perusteella määritetään jatkuvasti riskiarvoa käytölle ja sen perusteella voidaan tehdä toimenpiteitä automaattisesti (sallia, estää, hälyttää tai ilmoittaa käyttäjälle).

CASB:ia käytetään esimerkiksi rajaamaan organisaation käyttämiä tietovarantoja ja paljastamaan mahdollisesti käytössä oleva varjo-IT [10] ja sen aiheuttama riski tietojenkäsittelylle.

### 2.4.9 CSPM – Cloud Security Posture Management

CSPM perustuu malleihin tuotteistettujen pilvipalveluiden tietoturvakonfiguraatiosta, joita voidaan verrata keskitetysti käytössä oleviin konfiguraatioihin. Ajatuksena CSPM on yksinkertainen, mutta käytännössä laaja konsepti, sillä pilvipalvelut ovat teknisesti suuria ja monimutkaisia.

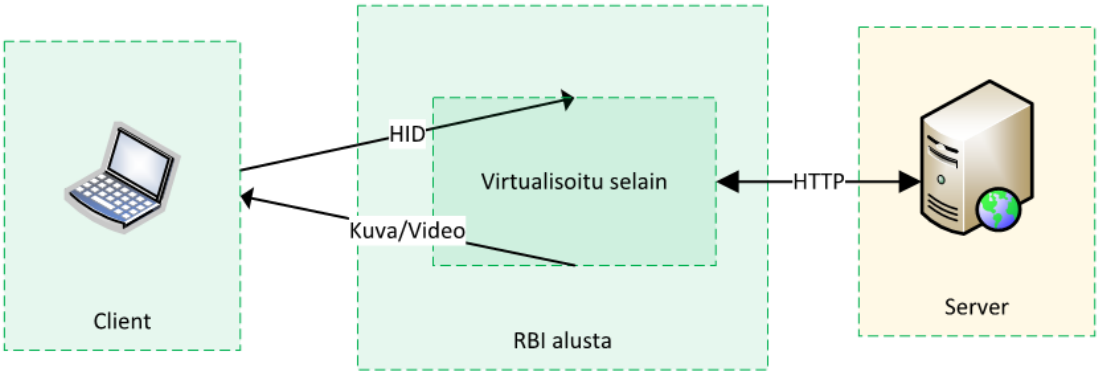
CSPM:n avulla voidaan esimerkiksi varmistaa, että kaikissa käytössä olevissa IaaS-virtuaalikoneissa hallinnan autentikaatio ja palomuurit on konfiguroitu organisaation määritysten mukaan, eikä esimerkiksi yhdessä palvelimesta tuhannessa ole jäänyt se tekemättä.

### 2.4.10 RBI – Remote Browser Isolation

RBI tarkoittaa selainistunnon virtualisointia clientin ja palvelun välissä. Tämä toteutetaan siten, että virtualisointipisteessä suoritetaan käyttäjäsessiokohtaista selainta. Se tekee HTTP-kutsut kohdepalvelulle, hakee sieltä sisällön, renderöi sen ja siirtää videokuvan siitä käyttäjälle. Kohdepalvelu ei tiedä alkuperäisestä clientistä tai käyttäjästä mitään, joten se ei voi uhata kuin virtuaalista selainistuntoa.

RBI ei ole uusi teknologia, sillä virtualisoituja työpöytiä ja sovelluksia on ollut markkinoilla jo kauan, mutta ne ovat olleet yleensä heikkoja käytettävyydeltään. Uusimmissa RBI-ratkaisuissa on päästy kuitenkin huomattavasti käytettävyydeltään parempiin ratkaisuihin: pitkälti konttiteknologian, HTML5:n ja loputtomasti skaalautuvan pilvi-infran avulla.

RBI-ratkaisut eivät ole tarkoitettuja jatkuvasti käytettäviksi, vaan ne tulisi kohdistaa joko maineeltaan huonoille sivustoille (jos niitä joutuu pakosti käyttämään) tai kriittisessä roolissa oleville henkilöille (VIP).




Kuva 10. RBI:n toimintaperiaate: Hiiri ja näppäimistö signaalit (HID, Human Interface Device) virtualisoidulle selaimelle ja video takaisin käyttäjälle.

### 2.4.11 ZTNA – Zero Trust Network Access

ZTNA [11] on yksinkertainen idea: älä luota, vaan validoi. Sillä tarkoitetaan verkkoarkkitehtuuria, jossa jokainen sovelluksen tietoliikenne yhteys autentikoidaan ja validoidaan jo verkkotasolla, ennen kuin yhteys sovellukseen teknisesti avataan.

Käytännössä tämä tarkoittaa SASE-yhdyskäytävän ja palvelun väliin rakennettavaa järjestelyä. Käyttäjän yhdyskäytävälle tehdyn autentikoinnin jälkeen tehdään vielä erillinen autentikaatio palvelua kohti, jonka jälkeen käyttäjän liikenne tunneloidaan erikseen palvelun lähellä olevaan julkaisijaan. Julkaisijasta yhteys avataan itse palveluun, jotta käyttäjä voi kirjautua sinne. Käyttäjällä ei siis ole tietoliikenneyhteyttä palveluun, ennen kuin käyttäjän käyttöoikeus palveluun on varmistettu.

### 2.4.12 Client-tunneli

SASE-ratkaisu on pohjimmiltaan client-VPN-ratkaisu, jossa suojattava tietoliikenne tunneloidaan lähtöpäästä. Normaaleista client-VPN-ratkaisuista poiketen liikenne tunneloidaan pilven SaaS-yhdyskäytävälle eikä organisaation sisäverkkoon. Monipuolisin malli on client-sovelluspohjainen tunneli, mutta voidaan käyttää myös clientitöntä versiota. Tällöin tunneli muodostetaan jostain muusta laitteesta, esimerkiksi sisäverkon toimipistereitittimestä tai palvelinten tapauksessa konesalin internet-muurilta.

Liikenteen tunnelointi estää sivustakuuntelun ja siten takaa siirrettävän tiedon luottamuksellisuuden säilymisen. Edellytyksenä on, että tunnelin muodostuksessa on käytetty riittävän luotettavaa ja vahvaa PKI:ta tunnistukseen, linjasalaus algoritmit ovat riittävän vahvoja ja avaintenvaihto on konfiguroitu oikein. Avaintenvaihdossa tulisi käyttää DHE:tä, jolloin muodostuu PFS eli jokaisella sessiolla on oma avaimensa.

Yleisin tunnelityyppi on DTLS hyvän suorituskyvyn ja yhteensopivuuden vuoksi. Sillä on yleensä varavaihtoehtona TLS. UDP:ta halutaan käyttää client-VPN-tunneloinnissa ensisijaisesti sen vuoksi, että TCP-session sisällyttäminen (encapsulation) toisen TCP-session sisään aiheuttaa suorituskykyongelmia [12]. Jotkut valmistajat käyttävät myös IPseciä tai se voidaan ottaa käyttöön. IPsec aiheuttaa aina omat haasteensa palomuurien ACL:ien kanssa, jossa sen tulee olla sallittuna. Suorituskyvyltään IPsec on verrannainen DTLS:ään siten, että DTLS on hieman vaativampi CPU:n puolesta ja IPsec puolestaan muistin [13, s.57].

Clientittömissä ratkaisuissa tunneli muodostetaan tunnelointiin kyvykkäältä verkkolaitteelta. Siihen konfiguroidaan joko encapsuloiva GRE-tunneli tai salaava IPsec-tunneli ja valitaan sinne syötettävät verkot (selector). Joissain tapauksissa käytetään IPsec-tunnelia null-encryptionilla.

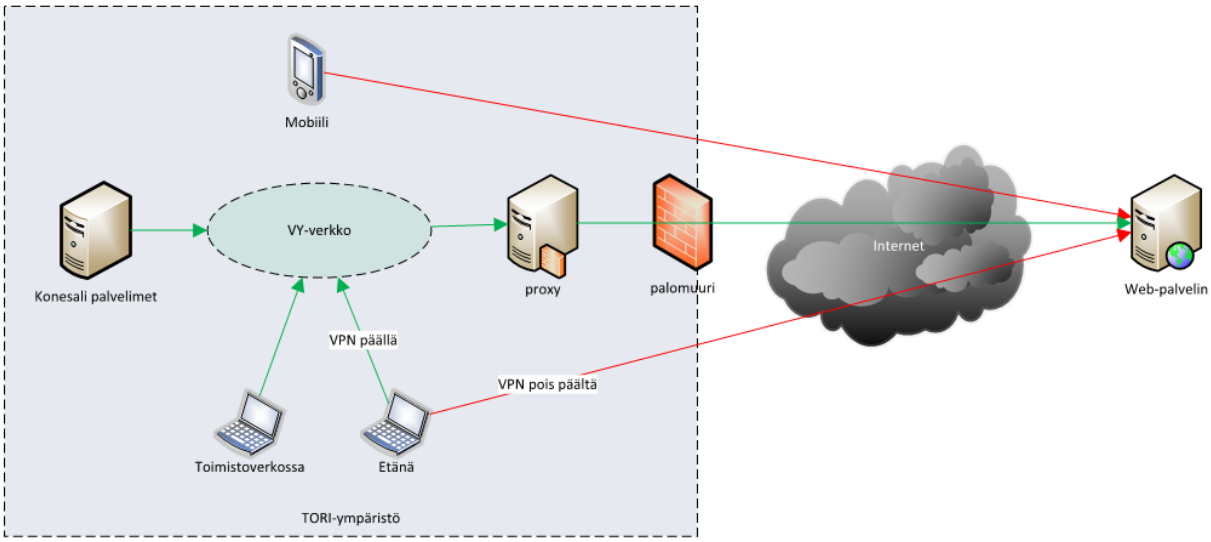
# 3 Ympäristö

Suojattava kohde on TORI-ympäristön internetin käyttö, mukaan lukien loppukäyttäjät ja laitteet. TORI-ympäristö on hajanainen hub-and-spoke-verkko, jota yhdistää yhteinen runkoverkko (hub) eli Valtion yhteinen verkko (VY-verkko) ja suuri määrä toimisto- ja konesaliverkkoja (spoke). Ympäristössä on useita omia pienempiä verkkokokonaisuuksiaan, mutta kaikkea yhdistää yhteinen runkoverkko. VY-verkko on suunniteltu täyttämään TLIV-tietojenkäsittely-ympäristön vaatimukset [14].

Verkon omistaa Valtori, mutta käytännössä suuri osa operoinnista toteutetaan sopimuspohjaisesti toimittajilla. Valtorin rooli ympäristössä on MSP-tyylinen [15] operointi, jossa suuri osa infra- ja yhteisistä palveluista on Valtorin toimittamia, mutta asiakkailla on myös omia palveluitaan. Valtorilla on noin 1400 työntekijää, joista noin 900 hoitaa TORI-ympäristöä ja loput keskittyvät TUVE eli Turvallisuus Verkko -ympäristöön.

TORI-ympäristön piirissä on yli 20 erillistä työasemaympäristöä, useita mobiililaiteympäristöjä ja kymmenisen konesalia. Toimipisteverkkoja on satoja, mutta korona-aikaan yli puolet käyttäjistä työskentelee etänä. Aktiivisia käyttäjäorganisaatioita on yli 70. Loppukäyttäjiä noin 40 000, joista lähes kaikilla on niin PC- kuin mobiililaite. Työasemista lähes kaikki ovat Windows-käyttöjärjestelmällä, mutta mukana on myös MacOS:a ja Linuxia. Mobiililaitteista suurin osa on Androideja, mutta huomattava osa on IOS-laitteita.

Ympäristön tärkeimmät yhteiset sovellukset ovat sähköposti, internetin selaus, useampi eri RTC-alusta ja ESSO-ratkaisu. Työnohjausjärjestelmät ja eri rekisterit ovat yleensä asiakaskohtaisia, mutta ristiinkäyttö on yleistä.




Kuva 11. TORI-ympäristön internetin käytön suojauksen yleisimmät käyttötapaukset.

# 4 Tarpeet

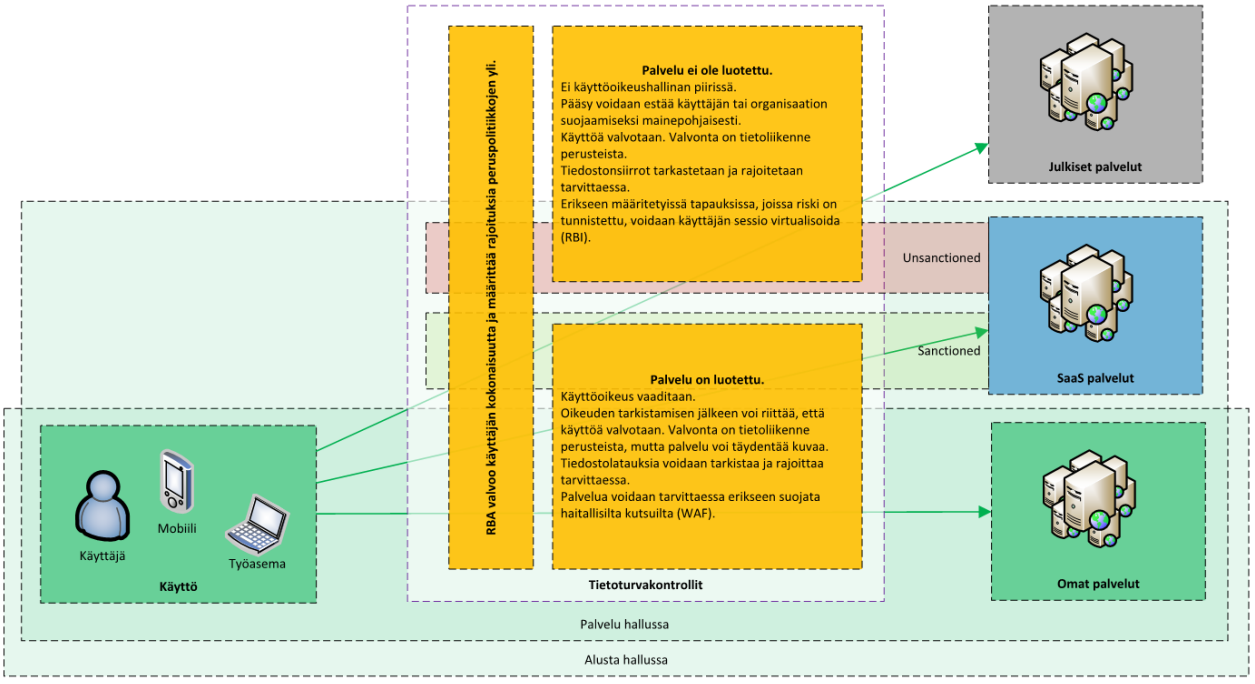
Valtorin perustarve on turvallinen internetin käyttö. Tätä toteutetaan jo nyt on-prem-ratkaisuilla, joiden keskiössä on HTTP-proxy. Tämän ratkaisuina kehitystarpeena on näkyvyyden lisääminen ja siitä johdannaisena kehittyneempien tietoturvakomponenttien hyötykäyttö.

Lisäksi Valtorilla on strateginen tarve tukea ja mahdollistaa pilvipalveluiden käyttöä, mikä käytännössä vaatii nykyarkkitehtuurin muuttamista. Käytettyjen palveluiden julkaisun suojaaminen liittyy tähän. Käytännössä se tarkoittaa jonkin tapaisen ZTNA-arkkitehtuurin rakentamista palveluiden eteen. Tällöin palvelut eivät ole suoraan avoimesti julkaistuja internetiin, vaikka ne voivatkin olla sen yli julkaistuja.

Kasvanut etätyö asettaa ympäristön suojaukselle myös omat haasteensa. Muuttunut verkkotopologian painopiste sisäverkosta päätelaitteisiin vaatii kompensoivia toimia.

## 4.1 Internetin käytön suojaus

Suojaus voidaan jakaa useampaan osaan, kuten yleiseen internetin käyttöön, tuotteistettujen pilvipalveluiden käyttöön ja omien palveluiden käyttöön, jotka sijaitsevat usein onpremissä.




Kuva 12. Internetin käytön suojattavat käyttötapaukset ja niiden tarvittavat tietoturvakontrollit.

### 4.1.1 Julkisten palveluiden käytön suojaus

Julkisten palveluiden käyttö on sähköpostin ohella suurin yksittäinen ulkoinen hyökkäysvektori [16]. Koska sivustoja on lukemattomia ja niiden kaikkien tulee olla käytettävissä, kontrollien tulee olla yleispäteviä ja suuriin massoihin sovellettavia. Nämä kontrollit voidaan jakaa kahteen eri kategoriaan, maine- ja sisältöperusteisiin.

Mainepohjaiset suojaukset perustuvat yleensä automaattisesti päivittyviin listoihin tunnetuista huonomaineisesta tai epäilyttävistä DNS-domaineista. Näitä voidaan käyttää joko HTTP-pyyntöjä käsitellessä tai jo ennen pyyntöä DNS-kyselyjen läpikäynnillä. Mainetarkistus suoritetaan aina ennen sisältötarkistusta, koska jos maine on riittävän huono, voidaan pääsy sivustolle estää eikä sisältötarkistusta tällöin tarvitse tehdä.

Tietoliikenteen sisällöntarkistus on laaja konsepti ja sitä voidaan tehdä usealla eri tavalla. Perustavalaatuinen kysymys on, onko liikenne selväkielistä vai salattua. Salatustakin liikenteestä voidaan tehdä tarkistusta itse salauksen ulkopuolelta L2-4-tasoilla pakettien ja sessioiden metatiedoista (esim. JA3). Ilman salauksen purkamista näkyvyys on hyvin rajallinen, koska ei voida olla varmoja, onko tarkastellun tunnelin sisällä mahdollisesti vielä toinen tunneli. Tällöin ulkoisen tunnelin metatiedot eivät välttämättä ole hyödyllisiä ja ne voivat olla jopa harhaanjohtavia.

Yleisimmät tavat käydä läpi salaamatonta tai purettua liikennettä ovat: analysoimalla itse paketteja (otsakkeet ja hyötykuormat erikseen), käymällä läpi pakeiteista muodostuvia protokollia ja sessiota tai kaivamalla sessiosta vielä erikseen siirrettäviä tiedostoja.

### 4.1.2 SaaS-palveluiden käytön ja julkaisun suojaus

SaaS-palvelut voidaan jakaa ilmaisiin ja maksullisiin. Lisäksi ne voidaan jakaa käytettäviin ja julkaistaviin. SaaS-palveluiden suojaamista helpottaa yleensä se,

että ne ovat selvästi tunnistettavissa, mutta suojaamista voi vaikeuttaa niiden tekninen monimutkaisuus.

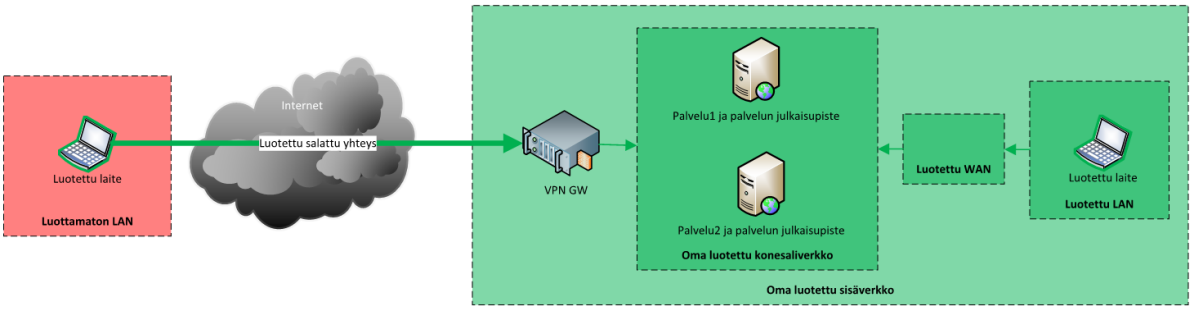
SaaS-palveluiden perussuojaus on yleensä suoraviivaista eli pääsy sinne varmistetaan ja sallitaan. Monimutkaisempaa siitä tulee, kun palvelussa tehtäviä toimia tulisi myös kyetä valvomaan. Monet valmistajat ovat kehittäneet tähän laajoja ratkaisuja, mikä helpottaa, mutta harvoin poistaa koko haastetta. Monesti palvelujen sallimisiin liittyy myös mahdollisten kilpailevien palveluiden rajoittamista, jotta organisaation tietyntyyppinen tietojenkäsittely pysyy hallitussa kokonaisuudessa. CASB- ja DLP-ominaisuudet ovat sisällönhallinnassa tärkeitä.

Palveluiden julkaisun suojaus tarkoittaa yksinkertaisimmillaan sitä, että vaikka SaaS-palvelu onkin julkaistu internetiin, ACL:llä kontrolloidaan organisaation tenantin pääsyä. Palveluun voidaan yhdistää vain etukäteen määritetyillä tavoilla, eikä kirjautumista pääse yrittämään kuka tahansa internetistä. Esimerkiksi pääsy voisi olla rajattu vain autentikoidulla ja suojatulla yhteydellä SASE-ratkaisun läpi.

### 4.1.3 Omien palveluiden käytön ja julkaisun suojaus

Vaikka etenkin uusia palveluja hankitaan ja perustetaan pilveen, on suuri osa valtionhallinnon tietojärjestelmistä edelleen onprem-ympäristöissä. Näitä palveluita julkaistaan yleensä vain sisäverkkoon ja pääsyä rajoittavat IP-pohjaiset ACL:t. Kirjautuminen tehdään itse palveluun, mutta ESSO voi olla käytössä. Palvelut sijaitsevat konesaleissa, joista on kyvykkyys julkaista palveluja suoraan internettiin, mutta näin ei yleensä tehdä tietoturvasyistä. Tämä tarkoittaa, että palveluiden käyttäminen organisaation sisäverkon ulkopuolelta vaatii VPN-ratkaisun käyttämistä. Tällöin päätelaite yhdistyy sisäverkkoon ja pääsy palveluun mahdollistuu.

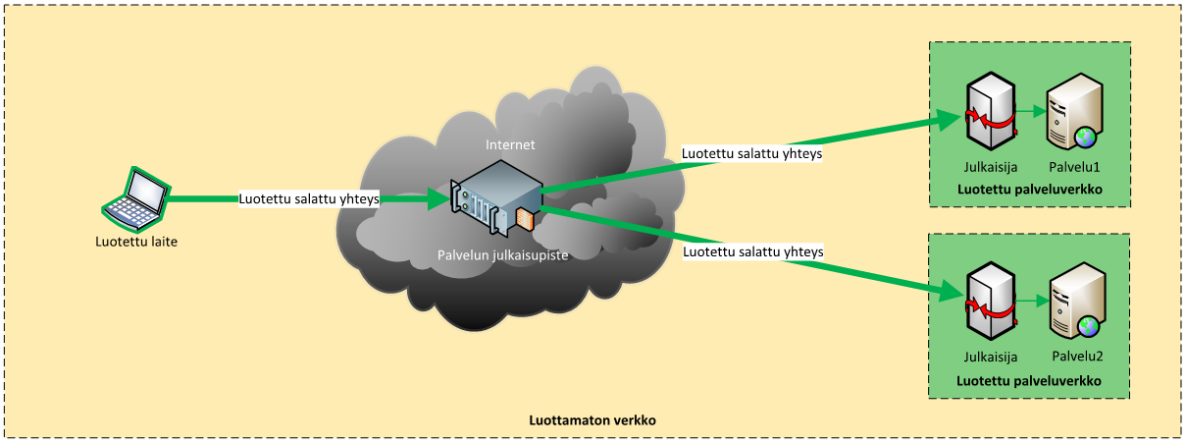
Vanha arkkitehtuurimalli, jossa käyttö tulee primääristä toimistoverkoista ja siirretään WAN-linkkien yli konesaleihin, ei enää ole järkevä, kun suuri osa käytöstä on siirtynyt toimistoverkoista etäkäytölle. Kun välittävänä kerroksena päätelaiteverkoista konesaliverkkoihin ei olekaan enää WAN vaan käyttäjän oma internetliittymä, ei ACL-pohjainen palveluiden vapaa julkaisu vain sisäverkkoon ole enää pätevä. Käytännössä internet toimii tällöin välittäjänä, jolloin organisaatio on jo hyväksynyt sen käytön, mutta ei ole vielä kenties uudistanut palvelujen julkaisun arkkitehtuuriaan.




Kuva 13. Yleinen palveluiden käyttöarkkitehtuuri, joka on suunniteltu toimistoverkko-käyttölle ja johon etäkäyttö on lisätty jälkikäteen.

Hallittu omien palveluiden julkaisu internetin yli on periaatteessa hyvin yksinkertaista. Palvelu julkaistaan julkaisupisteestä, johon käyttäjä muodostaa p2p-tunnelin luotetusta lähteestä ja autentikoituu. Sitten käyttäjä autentikoidaan uudestaan kyseistä palvelua varten ja sen onnistuessa avataan julkaisupisteeltä p2p-tunneli itse palveluun. Teknisesti tämä tarkoittaa erillisen julkaisijakomponentin lisäämistä palvelun eteen, johon p2p-tunneli muodostetaan, koska itse palvelua ei haluta muuttaa. Tämän jälkeen käyttäjä autentikoituu vielä itse palveluun.

Yksinkertaisuudessaan tämä on ZTNA-arkkitehtuuria. Muutoksena vanhaan tapaan on, että palveluita ei julkaista enää laajasti, esimerkiksi työasemaverkkoihin tai koko internetiin. Kaikki yhteyksien sallimiset ovat aina eksplisiittisiä p2p-avauksia, joissa on yleensä myös varmennepohjainen tunnistus. Tunnistus voi toimia mahdollisesti myös molemminpuolisena (mTLS). Lisäksi käytössä on oltava hyvin toimiva SSO-palvelu, sillä kirjautumisia tulee paljon, etenkin kun verkkotason kirjautumisia tullaan uusimaan julkaisupisteen toimesta jatkuvasti.




Kuva 14. Palveluiden ZTNA käyttöarkkitehtuuri, joka on suunniteltu verkon luotettavuudesta riippumattomaksi.

## 4.2 Tietoturvan modernisointi

### 4.2.1 ZTNA – Zero Trust Network Access

Tarve ZTNA:lle liittyy vahvasti etäkäytön kasvuun, mutta myös tarpeeseen pystyä validoimaan tietoturvan toteutumista ja pienentää hyökkäyspinta-alaa.

ZTNA-implementaatiot voivat olla monimutkaisia, etenkin verrattuna vanhaan tapaan pystyttää palvelu ja sallia sinne suora pääsy. Iso osa tietoturvasta jää silloin sovelluksen vastuulle. Tämä mahdollistaa monia hyökkäysvektoreita palvelua vastaan, esimerkiksi brute-force-kirjautumisyritykset, tunnusten uudelleenkäytön, palvelun enumeraatio- ja skannaustoimet, SQL-injektiot ja etenkin D/DoS-hyökkäykset. Internettiin julkaistuissa palveluissa näitä varten on tarvittu erillistä suojausta, anti-DDoS- ja WAF-toiminnallisuuksien muodossa.

Hyökkäysvektoreiden rooli vähenee huomattavasti, kun ulkopuolinen taho pääse korkeintaan yrittämään näitä toimia julkaisupistettä kohden. Julkaisupiste voidaan koventaa siten, ettei se vastaa mihinkään muuhun kuin tunnelipyyntöihin luotetuilta laitteilta. Tällöin ainoiksi ulkopuolisen toimijan hyökkäyskeinoksi palveluita vastaan jää DDoS-hyökkäys tai luotetun laitteen ja sen käyttäjän hal-

tuunotto. Suurilla SaaS-toimijoilla, jotka julkaisevat sovelluksia, on DDoS-suojaus otettu yleensä todella vakavasti, joten heidän palveluihinsa vaikuttaminen DDoS-hyökkäyksellä vaatii hyvin suurta tehoa [17] (Tbps-tasolla).

Palveluiden hyvä suojaus verkkotasolla siirtää huomion muihin hyökkäysvektoreihin, etenkin käyttäjien identiteettejä ja luotettuja päätelaitteita kohtaan. Tämä taas vuorostaan nostaa keskiöön yksinkertaisimmillaan tunnusten kalastelu-hyökkäykset (phishing) ja miksi ne ovat niin pelottavia. Millään verkkotason suojauksella ei ole väliä, jos varastetuilla tunnuksilla mennään niistä läpi.

Useat tahot ovat jatkojalostaneet ZTNA:ta. Esimerkiksi Gartner kehitti oman strategisen lähestymistapansa *CARTA:n* eli *Continous Adaptive Risk and Trust Assessment:*in [18]. Siinä verkkotason autentikaatioiden päälle on painotettu jatkuvaa uudelleenautentikointia ja käyttäjän toimien jatkuvaa seuraamista (UEBA), minkä pohjalta muodostetaan riskikerroin ja pääsyä voidaan rajata dynaamisesti (RBA).

Toinen jatkojalostus on Googlen BeyondCorp [19]. Sen perusteella yhtiö on rakentanut kaikki palvelunsa viimeisen vuosikymmen ajan ja sitä myydään nykyään myös ulospäin.

### 4.2.2 DLP – Data Loss Prevention

Kun käytetään julkisia pilvipalveluita, joihin tiedon tallentaminen on todella helppoa, tiedon exfiltraation riski kasvaa. DLP-toiminnallisuus tarjoaa tälle riskille kompensoivaa kontrollia. Tarve on mahdollistaa palveluiden käyttö, mutta silti pitää jonkinlainen kontrolli siitä, ettei käytön mukana lähde tahattomasti tai tahallaan organisaation ulkopuolelle kuulumatonta tietoa. Vanha kontrolli on ollut estää teknisesti tai kieltää hallinnollisesti tiettyjen palveluiden käyttö, mikä on haitannut normaalia työtä.

Kehittyneimmissä DLP-toiminnallisuuksissa on mahdollista myös opastaa käyttäjää toimimaan oikein. Tämä on mahdollista käyttäjä- ja kohdepalvelutiedon lisäksi tunnistamalla siirretyn tiedoston tyyppi ja kategoria. Näiden tietojen perusteella siirto voidaan väliaikaisesti keskeyttää ja näyttää käyttäjälle ilmoitus. Ilmoitus voi olla esimerkiksi ohjeistus, jossa kerrotaan organisaation Word-tiedostojen säilytyspalvelun olevan jokin toinen palvelu, kuin mihin käyttäjä on tiedostoa nyt siirtänyt. Lisäksi voidaan kysyä, onko hän varma, että haluaa jatkaa siirtoa, sillä se rikkoo organisaation tietoturvapolitiikkaa ja tapaus tullaan kirjaamaan lokiin.

### 4.2.3 CASB – Cloud Access Security Broker

Tarve kontrolloida tietoa ja teknisten kontrollien puutteellisuus on johtanut tilanteeseen, missä SaaS-palveluita ei ole voitu käyttää täysimääräisesti. Samaan tapaan kuin ennen DLP:tä on käynyt.

### 4.2.4 SSL Decrypt

Liikenteen salauksen purkamista tarvitaan, jotta liikennettä voidaan analysoida tarkasti ja siten mahdollistaa niin käyttäjien, tiedon kuin palveluidenkin hyvä suojaus. Ilman sitä suurin osa tietoturvakomponenteista on tehottomia.

### 4.2.5 Automaattiset ACL:t

Yksinkertainen, mutta hyvin tärkeä tarve suojauksessa on päästä hyötykäyttämään isojen SaaS-palveluntarjoajien automaattisesti päivittämiä ACL-listauksia tunnettujen pilvipalvelujen suhteen. IP-pohjaisten ACL:ien ylläpito manuaalisesti on hyvin työlästä ylläpidolle ja pilvipalveluissa osoitteet vaihtujat jatkuvasti. Lisäksi ACL:ien päivittymättömyys näkyy negatiivisesti loppukäyttäjille.

## 4.3 Kustannustehokkuus

Vaaditun tietoturvakyvykkyyden toteuttaminen onnistuu puhtaalla SaaS-ratkaisulla, mutta ei pelkällä onprem-ratkaisulla, sillä osa suojattavista kohteista on pilvessä. Osittain onpremissä pysyminen tarkoittaisi hybridi-ratkaisua. Tämä olisi käytännössä SaaS-ratkaisu, johon tarvitsisi lisäksi hankkia laajennukseksi onprem-laitteet ja -lisenssit. Tämä ei ole kustannustehokasta. Lisäksi TORI-ympäristön onprem-verkkoinfrastruktuuriin tehdyistä muutoksista johtuen tämä olisi huomattava investointi.

## 4.4 Käytön helppous ja ylläpidettävyys

Jotta SASE-järjestelmä saadaan laajaan käyttöön, tulee sen olla mahdollisimman näkymätön loppukäyttäjälle. Säätämistä, loppukäyttäjän toimenpiteitä tai kirjautumista vaativat sovellukset eivät ole nykypäivää. Tällainen hidastava toiminnallisuus voisi riskeerata koko palvelun käyttöönoton ja sen myötä parannukset tietoturvaan.

Valtionhallinnossa henkilöstöbudjetti on erotettu muusta budjetista, mistä johtuen henkilöstön kasvattaminen ei ole realistista. Yleensä on tultava toimeen niillä henkilöstöresursseilla, jotka ovat jo saatavilla. Tämä tarkoittaa, että ratkaisun tulee olla ylläpidettävissä kevyellä miehityksellä.

Hyvin rakennettu ja keskitetty hallinta mahdollistaa myös paremman palvelukokemuksen. Palveluun ei jää vahingossa tai kiireessä konfiguraation “häntiä”, jotka eivät tule näkymättöminä koskaan korjatuiksi, mutta voivat aiheuttaa jatkuvaa haittaa käytölle.

## 4.5 Toimintavarmuus

SASE-järjestelmän toimintavarmuus on ehdottoman kriittistä, koska sen läpi tulee virtaamaan paljon tietoa. Toimimattomuus voisi aiheuttaa merkittävää haittaa TORI-ympäristössä työskenteleville. Järjestelmän on myös vikatilanteessa mahdollistettava toiminta ilman sitä (fail-open).

SaaS-pohjaisille SASE-ratkaisulle luvataan yleensä 99,99 % SLA:ta ilmoittamattomista huoltokatkoista. Tämä tarkoittaa yhteensä noin 52 minuutin suunnittelematonta katkosta palvelussa vuosittain. Tällaiseen lukuun ei voida onprem-ratkaisulla päästä, sillä palveluita ei voida kustannussyistä rakentaa niin kestäviksi, koska käyttäjämassa ei ole riittävän suuri.

## 4.6 Vaatimukset

Kaikkien näiden mahdollisuuksien ja tarpeiden pohjalta laadittiin tekninen vaatimusmäärittely ja tarjottavan ratkaisun tulee täyttää se kaikilta kohdilta. Tämä dokumentti lisättiin Valtorin SASE-kilpailutuksen [20] dokumentaation liitteeksi. Ohessa on listaus vaatimuksista.

Taulukko 1. Kilpailutuksen tekninen vaatimusmäärittely.

| Kategoria | Kuvaus |
|---|---|
| Käytettävyys | Palvelua pitää pystyä käyttämään myös ilman client-pohjaista ratkaisua. |
| Käytettävyys | Palvelun pitää olla käytettävissä Windows, Mac, Android ja iOS:lla käyttöjärjestelmillä |
| Käytettävyys | Client -ohjelmistojen konfiguraatioiden poikkeamia pitää pystyä määrittämään hallintakäyttöliittymästä päätelaitteen käyttöjärjestelmästä riippumatta |
| Käytettävyys | Palvelun tulee toimia yhden prosessoinnin periaatteella ilman että liikennettä ohjataan erillisille komponenteille |
| Käytettävyys | Palvelun skaalautumisen ei tule aiheuttaa viiveen kasvua loppukäyttäjille |
| Käytettävyys | Palvelun politiikalla tulee pystyä ohittamaan salatun liikenteen purkaminen |
| Käytettävyys | Loppukäyttäjien autentikaation tulee tukea Azure AD SAML & SCIM toiminnallisuuksia |
| Käytettävyys | Hallinnan autentikaation tulee tukea Azure AD SAML |
| Käytettävyys | Palvelun tulee tukea useita identiteettilähteitä yhtäaikaisesti |

| | |
|---|---|
| Käytettävyys | Clientin liikennettä palveluun tulee pystyä ohjaamaan tarkasti lähde prosessi, kohde host, kohde domain tai sovellus perusteisesti |
| Käytettävyys | Client ei vaadi toimia loppukäyttäjältä lukuunottamatta asennuksen jälkeistä kirjautumista |
| Logitus | Palvelun tulee kirjoittaa yksityiskohtaista lokia loppukäyttäjien tekemistä transaktioista |
| Logitus | Palvelun lokit tulee olla integroitavissa kolmannen osapuolen SIEM järjestelmän kanssa |
| Logitus | Palvelun lokien tulee olla käytettävissä hallintakäyttöliittymän kautta |
| Logitus | Palvelun tulee lokittaa tapahtumat riippumatta niiden lopputuloksesta |
| Logitus | Palvelun politiikat, lokit ja raportointi tulee olla kohdistettavissa ryhmä- tai käyttäjätasolle |
| Logitus | Palvelun tulee tuottaa lokitietoa toiminnastaan |
| Palvelu | Asiakkaalle tarjottavan palvelun kaikkien komponenttien tulee sijaita kokonaan EU-alueen sisäpuolella |
| Palvelu | Palvelun tulee täyttää 99,99% SLA. |
| Palvelu | Ratkaisun tulee perustua tuotteisiin, jotka ovat elinkaarensa aktiivisen ylläpidon ja kehityksen vaiheessa |
| Tietoturva | Liikenne tulee olla ohjattavissa halutun Point-of-Presencen kautta |
| Tietoturva | Palvelun pitää pystyä havaitsemaan ja estämään uhkia tiedonsiirron aikana |
| Tietoturva | Palvelun tulee pystyä purkamaan kaikki sille ohjattu TLS liikenne TLS1.3 versioon asti, poislukien Certifiate Pinning poikkeamat |
| Tietoturva | Palvelun loppukäyttäjät tulee autentikoida |
| Tietoturva | Palvelun tulee sisältää kehittyneet palomuuri-ominaisuudet sisältäen: FWaaS, IDS, IPS, SSL liikenteen purku |
| Tietoturva | Palvelun tulee pystyä hallitsemaan sen läpi ladattuja tiedostotyyppejä |
| Tietoturva | Palvelun ja clientin välinen tietoliikenneyhteys tulee olla salattavissa ja purettavissa asiakkaan omilla varmenteilla |
| Tietoturva | Palvelun ja clientin välinen tietoliikenneyhteys tulee olla salattavissa vahvasti*, mutta politiikalla pitää kyetä tekemään poikkeamia. |
| Tietoturva | Clientin tulee ottaa aina yhteys automaattisesti palveluun ilman loppukäyttäjä toimenpiteitä |
| Tietoturva | Palvelun tulee pystyä häivyttämään tai piilottamaan loppukäyttäjien henkilötietoja ylläpidolta |
| Tietoturva | Liikenteen käsittelypiste saatavilla Suomessa palveluna, ilman Valtorin osallistumista |
| Tietoturva | Palvelun tulee tarjota DNS suojausta |
| Tietoturva | Palvelun tulee pystyä käsittelemään kaikkea tietoliikennettä |
| Toimittaja | Toimittajan tulee täyttää GDPR vaatimukset palvelun osalta |
| Toimittaja | Toimittajan tulee täyttää ISO/IEC 27018:2014 vaatimuset palvelun osalta |
| Toimittaja | Toimittajan tulee täyttää ISO/IEC 27001:2013 vaatimuset palvelun osalta |
| Tuki | Toimittajan on tarjottava palveluun 24/7/365 tukipalvelu |
| Tuki | Asiakkaan tulee pystyä avaamaan itse tukikeikkoja ja seuraamaan niiden tilannetta |

| | |
|---|---|
| Tuki | Tukipalvelun tulee olla saatavilla joko englanniksi tai suomeksi |
| Tuki | Palvelun dokumentaatio tulee olla saatavilla |
| Ylläpidettävyys | Palvelun clienttien tulee olla hallittavissa, päivitettävissä ja diagnosoitavissa palvelun kautta |
| Ylläpidettävyys | Palvelussa tehtyjen politiikkojen tulee voida olla kaikille käyttötavoille samat. |
| Ylläpidettävyys | Palvelussa on oma raportointinsa |
| Ylläpidettävyys | Hallintakäyttöliittymän tulee tukea roolipohjaista käyttöoikeusmallia |
| Ylläpidettävyys | Clientin tulee olla asennettavissa automaattisesti yleisten konfiguraationhallintatuotteiden kautta |
| Ylläpidettävyys | Raportointikäyttöliittymän tulee tukea roolipohjaista käyttöoikeusmallia |
| Ylläpidettävyys | Raportteja tulee pystyä tekemään käyttäjäryhmä -tasolla |
| Ylläpidettävyys | Politiikoiden tulee olla periytyviä tai kerroksellisia |
| Ylläpidettävyys | Palvelun tulee voida valvoa ja raportoida loppukäyttäjän kokemusta |

# 5 Haasteet

## 5.1 Hajautettu ympäristö

TORI-ympäristö koostuu monista osittain autonomisista ympäristöistä, mikä luo toistuvaan haasteen konfiguraationhallinnalle, yhteensopivuuksille ja testaamiselle. Vaikka SASE-clientit, niin työasemilla kuin mobiililaitteissa, ovat yhteensopivia tuettujen käyttöjärjestelmien kanssa, vaatii niiden yhteensopivuuden varmistaminen monesti konfiguraation räätälöintiä ja erillistä testaamista. Tämä on tärkeää etenkin päätelaitteiden tietoturvakomponenttien kanssa (Anti-malware ja EDR) ja mahdollisten onprem VPN-ratkaisujen kanssa. Asiakkuudet, joilla on useasti toisistaan poikkeavia vaatimuksia, aiheuttavat omat haasteensa. Ne työllistävät räätälöintien ja monimuotoisten käyttöönottojen muodossa.

TORI-ympäristössä on käytössä useiden verkkolaitevalmistajien laitteita samoissa rooleissa. Tämä tarkoittaa, että periaatteessa samat konfiguraatiot, joilla mahdollisestaan SASE:n toiminta, vaativat erilliset tekniset implementaatiot. Tämä puolestaan taas kasvattaa yhteensopivuuden varmistavan muutoksenhallinnan ja testaamisen määrää. Tämä on selvää etenkin tapauksissa, jossa tunnelointi SASE-yhdyskäytävälle halutaan tehdä esimerkiksi GRE-tunnelilla toimistoverkkojen tai konesalien reitittimiltä. Konfiguroitavia laitteita olisi satoja, ja

ne koostuisivat kymmenistä eri malleista, jolloin erilaisia tunnelikonfiguraatiota tulisi todella paljon. Lisäksi yhteistyötahoja on lukuisia ja osa muutoksista joudutaan tekemään alihankkijoiden kanssa, mikä monimutkaistaa asioita. Hyvä muutos- ja konfiguraationhallinta keventää hajautetun ympäristön työllistävää vaikutusta, mutta ei pysty sitä poistamaan.

Erillisten client-ratkaisujen asentaminen palvelimille on haastavaa, koska palvelinsovellukset eivät yleensä tue tällaista toimintaa. Suojaohjelmistojen asentaminen työasemille on normaalia toimintaa, mutta palvelimille se on enemmän poikkeus kuin sääntö. Tämän vuoksi liikenteen kaappaaminen verkkolaitteelta ja tunnelointi SASE-yhdyskäytävälle on helpoin ratkaisu. Menetettävä palvelimien identiteettitieto ei niin kriittinen kuin päätelaitteiden käyttäjä-identiteetti, sillä palvelimet toimivat kone-identiteeteillä eivätkä ne vaihdu.

Etäkäyttö aiheuttaa useita erillisiä haasteita, joista suurin osa liittyy käyttäjän lähiverkon laadun vaihteluun. Ilman loppukäyttäjän kokemuksen mittaamista, näihin laatuongelmiin on hyvin vaikea puuttua. Toinen etäkäyttöön liittyvä haaste ovat viive- tai kapasiteettivaativat sovellukset, etenkin kun käytetään jaettua VPN-kapasiteettia. Tämä ongelma korostuu ruuhka-aikaan ja on vaikea ratkaista ilman kapasiteetin yliresursointia, mikä puolestaan on kallista.

## 5.2 Lisensointimallit

Lisensointimallit vaihtelevat jonkin verran eri SASE-ratkaisujen välillä. Loppukäyttäjien määrä, riippumatta päätelaitteiden määrästä, on muodostumassa alan standardiksi.

Paljon prosessointivoimaa (DLP) tai paljon levytilaa lokien muodossa (ACFW, SWG) vaativat ominaisuudet ovat yleensä erikseen lisensoituja, ja lisensointimalli perustuu datan määrään. Sandbox-ominaisuudet ja reaaliaikaisesta liikenteestä havaittavat Advanced Anti-malware-ominaisuudet ovat yleisesti erikseen lisensoitava. Perustason IDS-toiminnallisuudet kuuluvat yleensä peruspakettiin. Sandboxeissa on yleensä mahdollisuus käyttää kolmannen osapuolen palvelua rajapinnan kautta.

DNS-ominaisuuksia ei ole kaikissa ratkaisuissa. Kehitys on kuitenkin menossa suuntaan, jossa DNS:stä on tulossa perustason ominaisuus. Lisensointi silti vaihtelee peruspaketin ja erillisen lisenssin välillä.

CASB-ominaisuus on usein erikseen lisensoitava. Samoin CSPM, mutta sen lisensointi vaikuttaa johtuvan palvelun koosta. Pienet ratkaisut kuuluvat yleensä peruspakettiin, mutta laajoissa ominaisuus on erikseen lisensoitava.

RBI-ominaisuutta ei löydy kaikilta ja se on aina erikseen lisensoitava.

ZTNA-ominaisuudet ovat yleensä kokonaan oma tuoteperheensä. Ne voivat myös olla kalliimpia kuin muut ominaisuudet yhteensä.

## 5.3 Tietosuoja ja yksityisyyden suoja

Tietosuoja ja yksityisyyden suoja ovat kaksi eri näkökulmaa henkilötietojen käsittelyyn. Tietosuojalla tarkoitetaan yleensä organisaation riskiä, jos henkilötietojen käsittely ei ole vaatimusten mukaista. Yksityisyyden suojalla tarkoitetaan yksilön riskiä, jos henkilötietojen käsittely ei ole vaatimusten mukaista. Asiaa on alettu ottamaan vakavammin GDPR:n [21] tultua voimaan vuonna 2018, ja se on muokannut koko maailman standardia henkilötietojen käsittelystä. Nykyään lähes kaikki SaaS-palveluita tarjoavat valmistajat pyrkivät olemaan GDPR-yhteensopivia. Ne tarjoavat siihen liittyen dokumentaatiota, kuinka he tekevät järjestelmissään henkilötietojen käsittelyjä.

GDPR:n keskiössä on idea, että henkilöt omistavat omat henkilötietonsa. Heille pitää kertoa, mitä tietoja heistä kerätään, millä perusteella niitä kerätään, miten niitä käsitellään ja mihin niitä käytetään. Lisäksi se määrittelee, kuinka henkilötiedostoista muodostettujen rekisterien tulee toimia kuvaamalla rekisterinpitäjien ja tiedon käsittelijöiden vastuita ja velvollisuuksia.

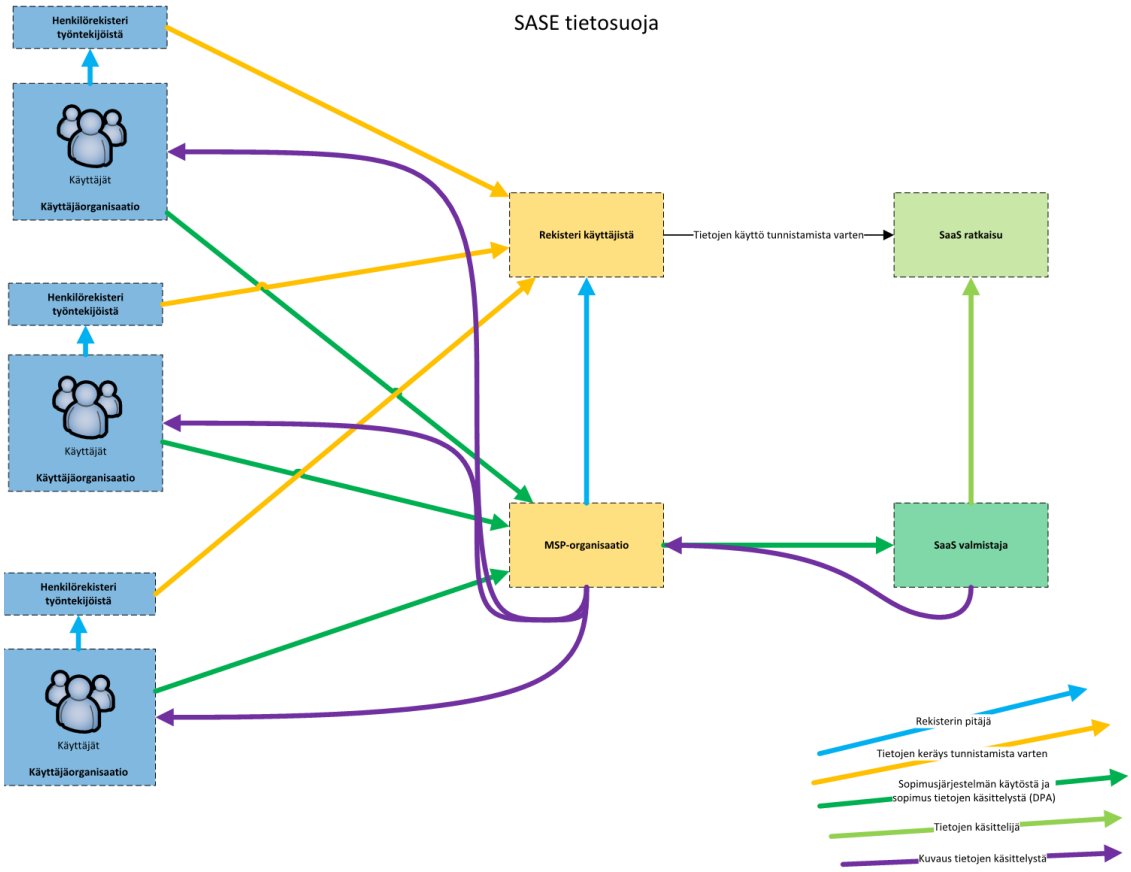
SASE-palvelun näkökulmasta tietosuojan rooli on kriittinen. Ilman sen hyväksyttävää hoitamista järjestelmä voisi olla tietosuoja-asetuksen vastainen ja siten sitä ei voisi käyttää.

SASE:n näkökulmasta tietosuoja-asetuksen mukaisessa toiminnassa on kaksi tärkeää kohtaa, artiklat 28 ja 30. Artikla 28 kuvaa, että kaikista rekisterinpitäjän (Controller) ja tiedonkäsittelijän (Processor) välisistä suhteista on sovittava sopimuksilla. Näissä sopimuksissa on kuvattava vastuut ja velvollisuudet. Yleinen yhteistyösopimus ei täytä tätä vaatimusta, vaan kyseessä tulee olla DPA (Data Processing Agreement). DPA:sta löytyvät selvät mallisopimukset, joita voidaan käyttää.

Artikla 30:n mukaan kaikki käsittelytoimet on kuvattava dokumentteihin ja itse käsittelystä on jäätävä jälki. Käsittelytoimiin lasketaan kuvaukset kerättävistä tiedoista, niiden säilytysajoista ja itse käsittelytoimenpiteistä. Jotta tämän osuuden voi kuvata, on järjestelmä tunnettava hyvin. Nämä dokumentit on pidettävä ajan tasalla, jos järjestelmään tehdään muutoksia.

Helpoimmin näiden vaatimusten täyttäminen onnistuu, kun nämä sopimukset ja määrittelyt tehdään hyvissä ajoin ennen järjestelmän käyttöönottoa tai käyttöönoton aikana. Jälkikäteen tällaisten selvitysten tekeminen voi olla hyvinkin työlästä.

GDPR myös vaatii artiklassa 35, että uusien teknologioita käyttöönottaessa on järjestelmästä tehtävä DPIA-selvitys (Data Processing Impact Assesment). DPIA:ssa käydään läpi systemaattisesti järjestelmässä käsiteltävät tiedot ja niiden kontrollit. Näin muodostuu tietosuojariskeistä tilannekuva, jonka perusteella organisaatio voi tehdä valistuneen päätöksen järjestelmän käyttöönotosta.




Kuva 15. Tietosuojan vaatimat kuvaukset ja sopimukset ovat monimutkaisia, kun SaaS-palveluita välitetään eteenpäin MSP-roolissa.

SASE-ratkaisun toimittamisen kannalta henkilötietoja tarvitaan hyvin vähän. Käytännössä tarvitaan käyttäjän tunnistamistiedot, jotka voidaan yleensä rajoittaa koostumaan vain IP-osoitteesta ja käyttäjätunnuksesta (esimerkiksi sähköpostiosoite).

On tärkeä huomioida, että käyttäjän järjestelmän läpi tekemä tietoliikenne ja siitä koostetut lokitiedot voivat sisältää henkilötietoja, joita käyttäjä on järjestelmään syöttänyt. Näitä tietoja kerätään käytönvalvontaa varten ja käytetään hyväksi tietoturvatapahtumien hallinnassa ja jälkikäteisselvittelyssä. Näitä henkilötietoja voidaan rajata järjestelmässä säännöillä. Esimerkiksi voidaan estää suurten henkilötietomassojen järjestelmän läpi vieminen DLP-ominaisuudella tai ottamalla salauksen purku pois käytöstä joihinkin palveluihin, esimerkiksi terveydenhuolto- tai pankkipalveluihin.

## 5.4 Lainsäädäntö

Lainsäädännön asettamat haasteet tekniselle järjestelmälle ovat vaativia. Tämä johtuu yleensä siitä, että lait joudutaan kirjoittamaan hyvin korkealla abstraktiotasolla, jotta ne kestävät aikaa mahdollisimman hyvin. Teknologian nopeasta kehittymisestä johtuen lainsäädäntö on usein vanhentunutta. Valtionhallinnon toiminta perustuu lakeihin, joten ne tulee ottaa huomioon kaikissa tietoteknisissä järjestelmissä.

SASE-järjestelmä on käsitetasolla aivan liian tarkka määritelmä, jotta lainsäädännössä olisi suoraa sitä koskevaa säätelyä. Kuitenkin moniin SASE:n kautta toteutettaviin toiminteisiin on laeissa otettu kantaa. Nämä lait voidaan jakaa kahteen eri kategoriaan: toimintoja puoltaviin ja rajoittaviin. Lisäksi on olemassa ohjeistuksia, jotka ovat valtionhallinnolle sitovia ja näistä on laeilla säädetty.

### 5.4.1 Käyttöä puoltavat lait

Laki sähköisen viestinnän palveluista (7.11.2014/917) [22] on laaja kokonaisuus, joka kuvaa reunaehtoja sähköiselle viestinnälle. Automaattinen tietojenkäsittely on osa sähköistä viestintää. SASE:n näkökulmasta tärkein kohta on 272 §, joka oikeuttaa viestinnän välittäjän huolehtimaan viestinnän turvallisuudesta ja osana sitä purkamaan viestinnän mahdollisen salauksen automaattista tutkintaa varten. Automaattisen tutkinnan kautta saatujen herätteiden perusteella voidaan sitten tehdä viestien (liikenteen) manipulaatiota tai siirtää viesti jatkotutkintaan. Lisäksi saman lain 138 § velvoittaa välittäjän ilmoittamaan tekemistään toimenpiteistä.

”272 § Toimenpiteet tietoturvan toteuttamiseksi:

Viestinnän välittäjällä ja lisäarvopalvelun tarjoajalla sekä niiden lukuun toimivalla on oikeus ryhtyä 2 momentissa tarkoitettuihin välttämättömiin toimiin tietoturvasta huolehtimiseksi: (18.1.2019/52)

1) viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi;

2) viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi; tai

3) viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.

Edellä 1 momentissa tarkoitetut toimet voivat käsittää:

1) viestin sisältöä koskevan automaattisen selvittämisen;

2) viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen;

3) tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä;

4) muut 1–3 kohdassa tarkoitettuihin rinnastettavat teknisluonteiset toimenpiteet.

Jos viestin tyypin, muodon tai muun vastaavan seikan perusteella on ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai käskyn eikä 2 momentin 1 kohdassa tarkoitetulla toimella pystytä turvaamaan 1 momentissa tarkoitettujen tavoitteiden toteutumista, yksittäisen viestin sisältöä saa käsitellä manuaalisesti. Manuaalisesta viestin sisällön käsittelystä on ilmoitettava viestin lähettäjälle ja vastaanottajalle, jollei ilmoittamisella todennäköisesti vaaranneta 1 momentissa tarkoitettujen tavoitteiden toteutumista.

Tässä pykälässä tarkoitetut toimenpiteet on toteutettava huolellisesti ja ne on mitoitettava suhteessa torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä 1 momentissa tarkoitettujen tavoitteiden turvaamiseksi. Toimenpiteet on lopetettava, jos niiden toteuttamiselle ei enää ole tässä pykälässä säädettyjä edellytyksiä.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä tässä pykälässä tarkoitettujen toimenpiteiden teknisestä toteuttamisesta.”

Toinen käyttöä puoltava laki on Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 [23] eli Yleinen tietosuoja-asetus (GDPR). Sen 32 artiklassa kuvataan, että rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiarvioperusteisesti turvallisuuden varmistamiseksi asianmukaisia toimia.

”32 artikla

Käsittelyn turvallisuus

1. Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten

a) henkilötietojen pseudonymisointi ja salaus;

b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;

c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;

d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

2. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

3. Jäljempänä 40 artiklassa tarkoitettujen hyväksyttyjen käytännesääntöjen tai 42 artiklassa tarkoitetun hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että tämän artiklan 1 kohdassa asetettuja vaatimuksia noudatetaan.

4. Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita.”

### 5.4.2 Käyttöä rajoittavat lait

Yleinen tietosuoja-asetus vaatii, että henkilötietoja käsitellessä on aina dokumentoitu, miten käsittelyä tehdään (30 artikla) ja käsittelystä on erikseen sovittu (28 artikla). Lisäksi kaikella henkilötietojen käsittelyllä pitää olla peruste tai siitä pitää olla sovittu (6 artikla). Tämä ei sinänsä suoraan rajoita SASE:n käyttöä, koska perusteet löytyvät ja toiminnasta voidaan sopia ja kuvata se tarkasti. On kuitenkin helpompaa pyrkiä rajoittamaan henkilötietojen käsittelyn tarvetta etukäteen, jotta ei vahingossakaan päädytä ristiriitaan käsittelyn laillisuuden suhteen.

Toinen käyttöä rajoittava laki on Laki yksityisyyden suojasta työelämässä (13.8.2004/759) [24]. Sen 21 § vaatii, että teknisistä valvontatoimista ilmoitetaan valtion virastoissa yhteistoimintamenettelyllä. Pykälä viittaa myös säädökseen Laki yhteistoiminnasta valtion virastoissa ja laitoksissa (30.12.2013/1233) [25], jonka 13 § vahvistaa käytännössä tämän vaatimuksen.

Näiden lisäksi Laki sähköisen viestinnän palveluista säädöksen 272 § viimeinen lause *”Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä tässä pykälässä tarkoitettujen toimenpiteiden teknisestä toteuttamisesta.”* asettaa suuria vaatimuksia. Se tarkoittaa käytännössä, että nykyisen Traficomin asettamat määräykset [26] ovat sitovia. Tosin tämä sama asia on käytännössä sanottu jo Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista [27] säädöksessä, jonka ydin on, että Traficom määrittää standardit, joilla tietojärjestelmien tietoturvaa arvioidaan. SASE:n kohdalla se tarkoittaa käytännössä Katakri- ja etenkin PiTuKri [28] -arviointikriteeristöjä. Nämä ovat mielestäni erinomaisia kriteeristöjä, joihin on pyritty keräämään maailmantason hyviä käytäntöjä (esimerkiksi ISO/IEC standardeista), jolla järjestelmistä pyritään saamaan riittävän tietoturvallisia. Suurimpana hallinnollisen tietoturvan haasteena

puhtaiden SaaS-palveluiden (mm. SASE) kanssa on yleensä se, että kaikkia asioita ei voida arvioida. Osa palvelun tietoturvallisuudesta perustuu aina luottamukseen, että valmistaja toimii, kuten on ilmoittanut.

# 6 Suunnitelma

Valtorissa suoritettiin tietoturvan itsearviointi vuonna 2019 CIS-kontrolleja [29] vastaan. Tämän perusteella tunnistettiin kehityskohteita, joista yksi oli nykyisen internetin käytön suojauksen ratkaisun jatkokehitys. Nykyisen ratkaisun elinkaaripäivitystä lykättiin, jotta voitiin tehdä tarkempi selvitys tarpeista ja ratkaisuvaihtoehdoista.

SASE-ratkaisun käyttöön saamiseksi laadittiin seuraava suunnitelma:

1. Tarvekartoitus
    a. Mitä tarvitaan nyt ja mitä viiden vuoden päästä?
2. Teknologiakartoitus
    a. Mitkä olisivat ratkaisuvaihtoehdot, jos ratkaisu pohjautuisi
        i. Onprem?
        ii. Cloud?
        iii. Hybridi?
3. Markkinakartoitus: SASE
    a. Mitkä ovat markkinajohtajien ratkaisumallit?
4. PoV & sisäinen viestintä
    a. Hands-on ratkaisujen testaaminen ja benchmarking
5. Vaatimusmäärittely
    a. Millainen ratkaisu tarvitaan TORI-ympäristöön?
6. Kilpailutus
    a. Lain vaatima hankintatapa valtionhallinnossa
7. Järjestelmän rakentaminen
    a. Validoidaan toimivuus ja rakennetaan perustat
    b. Ensimmäinen käyttöönotto Valtorille

8. Access osuuden käyttöönotot per ympäristö
    a. Ympäristöjä ja asiakkuuksia on paljon ja osa tarvitsee räätälöintiä
9. CASB ja DLP osuuksien käyttöönotot per asiakkuus
    a. Räätälöintiä tarvitaan, mutta vähemmän kuin Access osuudessa
10. ZTNA palveluiden rakentamisen aloittaminen
    a. Palvelut ovat perustan jälkeen pelkkää räätälöintiä ja erillisiä projekteja

Suunnitelmaa rakentaessa ja aiheeseen tutustuessa ymmärrettiin, ettei uusien tietoturvaominaisuuksien käyttöön saaminen tarkoita vain uuden järjestelmän käyttöönottoa. Osa muutoksista, jotka mahdollistavat paremman tietoturvatason, vaativat muutoksia koko ympäristön arkkitehtuurissa ja ovat siitä johtuen pidemmän ajan tavoitteita.

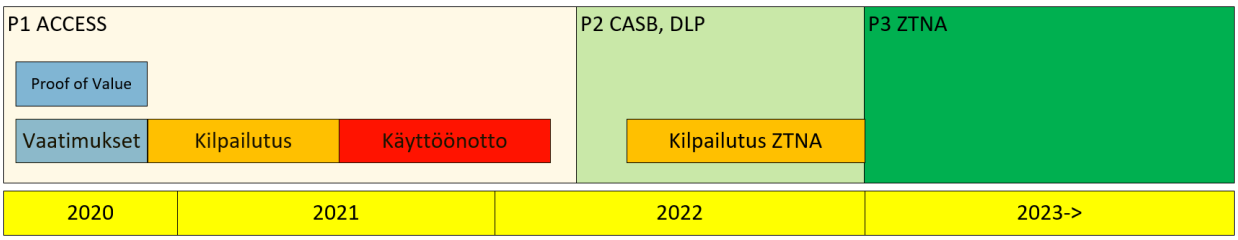
Tästä johtuen SASE:n kokonaisvaltainen käyttöönotto jaettiin kolmeen osaan:

1. Internetin käytön suojaaminen eli Access.

2. SaaS-palveluiden käytön ja julkaisun suojaus eli CASB ja DLP.

3. Omien palveluiden käytön ja julkaisun suojaus eli ZTNA.

Osat ovat toisistaan riippuvaisia siten, että seuraava osa vaatii käytännössä edellisen implementaatiota.




Kuva 16. SASE-järjestelmän vaiheittaisen käyttöönoton aikataulusuunnitelma Valtorissa vuonna 2020.

# 7 Yhteenveto

Tässä opinnäytetyössä kuvattujen asioiden perusteella pystyttiin määrittelemään TORI-ympäristöön tarvittava SASE-järjestelmä, joka mahdollisti onnistuneen kilpailutuksen. Kilpailutuksessa valittu tuote pystyy toteuttamaan tarvittavia ominaisuuksia ja sen avulla pystytään korvaamaan nykyinen järjestelmä ja samaan käyttöön uudet ominaisuudet. Pitkän tähtäimen modernisointitarpeet ja laajennettavuus on siinä myös huomioitu.

Ympäristön tietoturvavalvonnan kannalta muutos parempaan tulee olemaan huomattava, kun CSOC-toiminnolle voidaan tarjota laajaa ja syvää näkyvyyttä internetrajapintaan. Paremmat ominaisuudet tuovat käytettävyyttä käyttäjien etätyöskentelyyn ja uskottavuutta etätyöskentelyn tietoturvaan.

Järjestelmä tulee myös mahdollistamaan palveluiden suojatun julkaisemisen, mikä helpottaa niin uusien palveluiden käyttöönottoa kuin vanhojen palveluiden vaatimustenmukaisuuden täyttymistä. Samalla järjestelmän ylläpidon työtä voidaan kohdentaa paremman palvelun jatkokehittämiseen jatkuvien tuotannollisten virhetilanteiden selvittämisestä.

Tätä opinnäytetyötä voisi laajentaa kuvaamalla järjestelmän käyttöönottovaihe sekä selvittämällä lisää ZTNA-arkkitehtuurin vaikutuksia etenkin vanhojen sovellusten suojaamisessa. Suuren järjestelmän käyttöönotto on aina mielenkiintoista ja pienistäkin teknisistä yksityiskohdista voi tulla projektinhallinnallisesti merkittäviä. Isossa käyttöönotossa on aina opittavaa, etenkin jos ympäristö on näin monimuotoinen. ZTNA on parhaimmillaan, kun sovellukset on suunniteltu käyttämään sitä. Sillä voidaan kuitenkin saada helppoja voittoja vanhojen sovellusten suojauksessa, jos sovellus on siirrettävissä ainakin osittain uuteen arkkitehtuurimalliin.

# 8 Lähteet

1. 2013. Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä. Finlex. Viitattu 1.4.2021. Saatavilla: https://finlex.fi/fi/laki/ajantasa/2013/20131226

2. Neil MacDonald, Lawrence Orans, Joe Skorupa. 2019. The Future of Network Security Is in the Cloud. Gartner. Viitattu 1.4.2021. Saatavilla: https://www.gartner.com/document/3956841?ref=solrAll&refval=235882793&_ga=2.25692408.414444520.1617805682-1353706877.1617805682

3. Manoj Apte. 2019. New Report from Gartner Research: The Future of Network Security Is in the Cloud. Zscaler. Viitattu 1.4.2021. Saatavilla: https://www.zscaler.com/blogs/company-news/new-report-gartner-research-future-network-security-cloud

4. 2021. Software-Defined Networking (SDN) Definition. ONF. Viitattu 1.4.2021. Saatavilla: https://opennetworking.org/sdn-definition/

5. 2021. TCP Throughput Calculator. SWITCH. Viitattu 1.4.2021. Saatavilla: https://www.switch.ch/network/tools/tcp_throughput/

6. 2021. TLS cipher suitet turvallisuusluokille IV-III. Kyberturvallisuuskeskus. Viitattu 1.4.2021. Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TLS-cipher-suitet-turvallisuusluokille-IV-III.pdf

7. 2016. Tip of the Day: Demystifying Software Defined Networking Terms - The Cloud Compass: SDN Data Flows . Microsoft. Viitattu 1.4.2021. Saatavilla: https://docs.microsoft.com/fi-fi/archive/blogs/tip_of_the_day/tip-of-the-day-demystifying-software-defined-networking-terms-the-cloud-compass-sdn-data-flows

8. 2021. Man-in-the-Middle. enisa. Viitattu 1.4.2021. Saatavilla: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/man-in-the-middle

9. 2017. Protective DNS (PDNS). National Cyber Security Centre. Viitattu 1.4.2021. Saatavilla: https://www.ncsc.gov.uk/information/pdns

10. 2021. Tutorial: Discover and manage shadow IT in your network. Microsoft. Viitattu 1.4.2021. Saatavilla: https://docs.microsoft.com/en-us/cloud-app-security/tutorial-shadow-it

11. Scott Rose (NIST), Oliver Borchert (NIST), Stu Mitchell (Stu2Labs), Sean Connelly (DHS). 2020. Zero Trust Architecture. NIST. Viitattu 1.4.2021. Saatavilla: https://csrc.nist.gov/publications/detail/sp/800-207/final

12. Olaf Titz. 2001. Why TCP Over TCP Is A Bad Idea. inka. Viitattu 1.4.2021. Saatavilla: http://sites.inka.de/bigred/devel/tcp-tcp.html

13. Kuna Vignesh. 2017. Performance analysis of end-to-end DTLS and IPsec-based communication in IoT environments.. Digitala Vetenskapliga Arkivet. Viitattu 1.4.2021. Saatavilla: https://www.diva-portal.org/smash/get/diva2:1157047/FULLTEXT02, s. 57.

14. 2020. Katakri – tietoturvallisuuden auditointityökalu viranomaisille. Ulkoministeriö. Viitattu 1.4.2021. Saatavilla: https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

15. 2021. Managed Service Provider (MSP). Gartner. Viitattu 1.4.2021. Saatavilla: https://www.gartner.com/en/information-technology/glossary/msp-management-service-provider

16. Richard Hummel. 2021. Securing Against the Most Common Vectors of Cyber Attacks. SANS. Viitattu 1.4.2021. Saatavilla: https://www.sans.org/reading-

room/whitepapers/riskmanagement/securing-common-vectors-cyber-attacks-37995

17. 2021. Famous DDoS attacks | The largest DDoS attacks of all time. Cloudflare. Viitattu 1.4.2021. Saatavilla: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

18. Neil MacDonald. 2018. Zero Trust Is an Initial Step on the Roadmap to CARTA. Gartner. Viitattu 1.4.2021. Saatavilla: https://www.gartner.com/en/documents/3895267

19. 2021. BeyondCorp. Google. Viitattu 1.4.2021. Saatavilla: https://cloud.google.com/beyondcorp

20. 2021. Turvallinen internetyhdyskäytävä (SASE) - ohjelmistopalvelun käyttöoikeuksien jakelupalvelu sekä tuki-, asiantuntija- ja ylläpitopalvelut . Hilma. Viitattu 1.4.2021. Saatavilla: https://www.hankintailmoitukset.fi/fi/public/procurement/47879/notice/64986/overview

21. 2016. General Data Protection Regulation. GDPR. Viitattu 1.4.2021. Saatavilla: https://gdpr-info.eu/

22. 2014. Laki sähköisen viestinnän palveluista. Finlex. Viitattu 1.4.2021. Saatavilla: https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

23. 2016. EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679,. Euroopan unionin virallinen lehti. Viitattu 1.4.2021. Saatavilla: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&qid=1510823720498&from=EN

24. 2004. Laki yksityisyyden suojasta työelämässä (13.8.2004/759). Finlex. Viitattu 1.4.2021. Saatavilla: https://www.finlex.fi/fi/laki/ajantasa/2004/20040759

25. 2013. Laki yhteistoiminnasta valtion virastoissa ja laitoksissa. Finlex. Viitattu 1.4.2021. Saatavilla: https://www.finlex.fi/fi/laki/ajantasa/2013/20131233

26. 2021. Säädökset ja määräykset. Traficom. Viitattu 1.4.2021. Saatavilla: https://www.traficom.fi/fi/saadokset?group=kyberturvallisuus

27. 2011. Lakiviranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista. Finlex. Viitattu 1.4.2021. Saatavilla: https://www.finlex.fi/fi/laki/alkup/2011/20111406

28. 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Traficom. Viitattu 1.4.2021. Saatavilla: https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri

29. 2021. CIS Controls. Center for Internet Security. Viitattu 1.4.2021. Saatavilla: https://www.cisecurity.org/controls