

Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2021

Matti Saastamoinen

# ETÄTYÖSKENTELYN VPN- JA ZERO TRUST -SELVITYS

Matti Saastamoinen

# ETÄTYÖSKENTELEN VPN- JA ZERO TRUST - SELVITYS

Etätyöskentely on kasvava trendi yrityksissä nykyaikana. Tämän opinnäytetyön tutkimuksissa tutkittiin etätyössä käytettäviä sovelluksia. Tutkimuksissa löytyi sovelluksia, jotka vaativat yhteyden yrityksen sisäiseen verkkoon. Sovelluksille selvitettiin vaihtoehtoja, joilla sovellukset voidaan toteuttaa Zero Trust -arkkitehtuurin mukaisesti käyttämällä mahdollisimman vähän VPN-yhteyksiä.

Tutkimuksessa selvitettiin ensin Zero Trust -arkkitehtuuria ja tämän jälkeen palveluita, joilla arkkitehtuuria voidaan toteuttaa. Tutkimuksessa löytyi muutama vaihtoehto palveluista, jotka soveltuvat yritykselle sovellusten etäkäyttöön Zero Trust -arkkitehtuurin mukaisesti.

Zero Trust -arkkitehtuuriin siirtyminen on suuri prosessi, joka vaatii valtavasti tutkimusta sovelluksista ja omasta verkosta. Tässä opinnäytetyössä tehtiin alustava tutkimus, jonka pohjalta yritys voi jatkaa omaa tutkimustyötään arkkitehtuurin toteuttamiseksi myöhemmin. Opinnäytetyön tutkimustyön jälkeen jää vielä paljon selvitettävää palveluista, sovelluksista ja niiden toteutuksesta.

## ASIASANAT:

zero trust, etäkäyttö, etätyö, tietoturva, tietoliikenne.

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and communication technology

2021 | 30 pages

Matti Saastamoinen

# REMOTE WORK VPN AND ZERO TRUST RESEARCH

Telecommuting is a growing trend in companies. This thesis was a preliminary research on applications used while working remotely. Several applications were found that required a connection to the inside network of the company. Research was done to find options for deploying the software for users according to the Zero Trust architecture.

In the study Zero Trust architecture was first studied and after this services that could be used to deploy the software according to the architecture. A few alternatives were found that could be used by the company.

The transition to a Zero Trust architecture is a huge process that requires extensive research of the applications and network. This thesis was a preliminary research that can be used as a basis for more research by the company to carry out deploying a Zero Trust architecture-based network. After this thesis there is still research to be done by the company.

## KEYWORDS:

zero trust, remote work, cybersecurity, data communications

# SISÄLTÖ

<b>KÄYTETYT LYHENTEET TAI SANASTO</b>	<b>6</b>
<b>1 JOHDANTO</b>	<b>7</b>
<b>2 ZERO TRUST -ARKKITEHTUURI</b>	<b>8</b>
2.1 Zero Trust -termin määrittäminen	8
2.2 Zero Trust -arkkitehtuurin periaatteet	8
<b>3 OSI-MALLI</b>	<b>10</b>
<b>4 ZERO TRUST MALLIIN SIIRTYMINEN</b>	<b>13</b>
4.1 Alustava tutkimus	13
4.2 Kipling-metodi	14
<b>5 TYÖNTEKIJÖIDEN ETÄTYÖSKENTELY</b>	<b>15</b>
5.1 Käytössä oleva laitteisto	15
5.2 VPN ongelmat	15
5.3 Etätyöskentely	15
<b>6 AZURE AD APPLICATION PROXY -PALVELU</b>	<b>16</b>
6.1 Tietoturvallisuus	16
6.2 Toiminta	17
6.3 Vaatimukset	18
<b>7 CITRIX VIRTUAL APPS AND DESKTOPS JA WORKSPACE -PALVELU</b>	<b>19</b>
7.1 Toiminta	19
7.2 Zero Trust -arkkitehtuuri Citrixillä	20
<b>8 MICROSOFT UNIVERSAL PRINT -PALVELU</b>	<b>23</b>
<b>9 ZERO TRUST NETWORK ACCESS</b>	<b>25</b>
9.1 Toiminta	25
9.2 Fortinet	25
<b>10 POHDINTA</b>	<b>28</b>
<b>LÄHTEET</b>	<b>29</b>

# KUVAT

Kuva 1 OSI-mallin kerrokset, ja kuvaus tietoliikenteestä verkossa.	10
Kuva 2 Application proxyn toiminta (Microsoft 2021)	17
Kuva 3 Citrix palveluiden yhteydet Zero Trust toteutuksessa. (Citrix 2021)	22

## KÄYTETYT LYHENTEET TAI SANASTO

AD	Active Directory
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPSec	Internet Protocol Security
LLC	Logical Link Controller
MAC	Media Access Control
OSI	Open Systems Interconnection
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SSL	Secure Socket Layer
VPN	Virtual Private Network
ZT	Zero Trust
ZTA	Zero Trust Access
ZTNA	Zero Trust Network Access

# 1 JOHDANTO

Etätyöskentely on kasvava työskentelyn muoto yrityksissä. Perinteisesti etätyöskentely hoidetaan VPN (Virtual Private Network) -yhteyksillä. VPN-yhteydet aiheuttavat mahdollisia tietoturvauhkia yrityksille, joita minimoimaan on kehitetty Zero Trust -arkkitehtuuri verkon rakentamiseksi.

Opinnäytetyön tarkoituksena on tutkia yrityksen vakioidulla päätelaitteella etätyöskentelyssä käytettäviä verkkoyhteyksiä sekä selvittää mahdollinen siirtyminen Zero Trust -malliin VPN-yhteyksien käytössä. Etätyö tarkoittaa tässä tapauksessa työpaikan ulkopuolella tehtävää työtä [1]. Zero Trust -malli pyrkii poistamaan luontaisen luottamuksen sisäverkosta ja samalla rakentamaan luottamusta lukuisten pyyntöjen kautta. Tämä voidaan saavuttaa luomalla kontekstia vahvan tunnistautumisen, käyttöoikeuksien, laitteen tilan ja haettavan tiedon arvon perusteella. [2]

Työn aikana tutkitaan, mitä yhteyksiä käytettävät järjestelmät ja ohjelmat vaativat työskentelyn mahdollistamiseksi ja mitkä näistä yhteyksistä pystyttäisiin toteuttamaan VPN-tunnelin ulkopuolella internetin yli. VPN-tunneli on salattu yhteys tietokoneen tai mobiililaitteen ja ulkoisen verkon välillä. Salattu yhteys auttaa varmistamaan, että arkaluonteiset tiedot lähetetään turvallisesti. Se myös estää ulkopuolisten ihmisten salakuuntelemasta tietoliikennettä mahdollistaen turvallisen etätyöskentelyn. [3] Opinnäytetyössä tutkitaan vaihtoehtoja, joilla voidaan toteuttaa Zero Trust -arkkitehtuurin mukainen verkkorakenne järjestelmille ja sovelluksille, joita käytetään etätöissä. Zero Trust -mallista selvitetään, mitä malliin siirtyminen vaatii etätyöskentelyssä ja myös riskien arviointi.

Tutkimus etätyöskentelyn yhteyksistä on ajankohtainen, sillä nykyinen COVID-19-pandemiatilanne on ajanut työntekijöitä enenevässä määrin etätöihin hallituksen suositusten vuoksi. [4] Tutkimus antaa myös kuvan yrityksen verkon toiminnasta ja käytännöistä ja sen avulla voidaan tehdä muutoksia tai parannuksia yrityksen sisäiseen verkkoon. Zero Trust -malleista ja VPN-yhteyksien käyttöönotoista on tehty aikaisemmin useampia opinnäytetöitä, esimerkiksi Terva P, Zero Trust -arkkitehtuuri [5] ja Oksanen E, VPN-erillisverkon käyttöönotto yrityksessä. [6]

## 2 ZERO TRUST -ARKKITEHTUURI

### 2.1 Zero Trust -termin määrittäminen

Zero Trust on tietoturva-alan puhutuimpia aiheita tällä hetkellä. Arkkitehtuurin tarkoituksena on vähentää tietoturvamurtoja yrityksen verkkoihin ja pienentää onnistuneiden murtojen vaikutusta poistamalla mahdollisuuksia verkossa liikkumiseen. Zero Trust -arkkitehtuurin periaatteena on lause ”Never trust, always verify”, joka ilmaisee luottamuksen eliminointia verkossa. [7]

Arkkitehtuurin on kehittänyt John Kindervag työskennellessään Forrester Research yhtiöllä. Kehitys alkoi, kun Kindervag pohti tavallista tapaa turvata yrityksen verkkoa, jossa ajateltiin, että uhka ei voi tulla verkon sisäpuolelta ja jokainen käyttäjä toimii verkossa vastuullisesti. Perinteisessä verkossa sisään päästyään hyökkääjä voi yleensä liikkua verkossa vapaasti ja päästä käsiksi haluamiinsa resursseihin, sillä turvaaminen loppuu yleensä verkon ulkorajaan. Zero Trust mallissa tämän kaltaista luottamusta sisäverkon käyttäjiin pidetään uhkana ja se pyritään eliminoimaan. [7]

### 2.2 Zero Trust -arkkitehtuurin periaatteet

Zero Trust -malli perustuu luottamuskäytäntöihin ja sen yksi tärkeimpiä toimia on estää tietomurtoja ja sivuttaisliikettä yrityksen sisäverkossa. Käyttäjille ja laitteille ei myönnetä luottamusta ehdottomasti verkkoon pääsyn jälkeen, vaan niitä arvioidaan ja tarkkaillaan jatkuvasti. Lähtökohtaisesti käyttäjille tulisi luovuttaa käyttöoikeuksia mahdollisimman vähän, joita he tarvitsevat työnsä suorittamiseen. Käyttöoikeuksien minimimäärän myöntäminen vähentää väärinkäytön riskejä verkossa. [8]

Mallin käyttöönottoon on monenlaisia vaihtoehtoja, mutta perustana on mallille yleisesti ajatellut perusperiaatteet:

1. Jokainen datalähde, sovellus tai palvelu luokitellaan resurssiksi. Yritysten verkot eroavat toisistaan hyvin paljon käytetyn laitteiston ja sovellusten kannalta. Verkossa saattaa olla myös tietokantoja, palveluna toimitettavia sovelluksia (Software as a Service, SaaS) sekä lukuisia muita järjestelmiä.

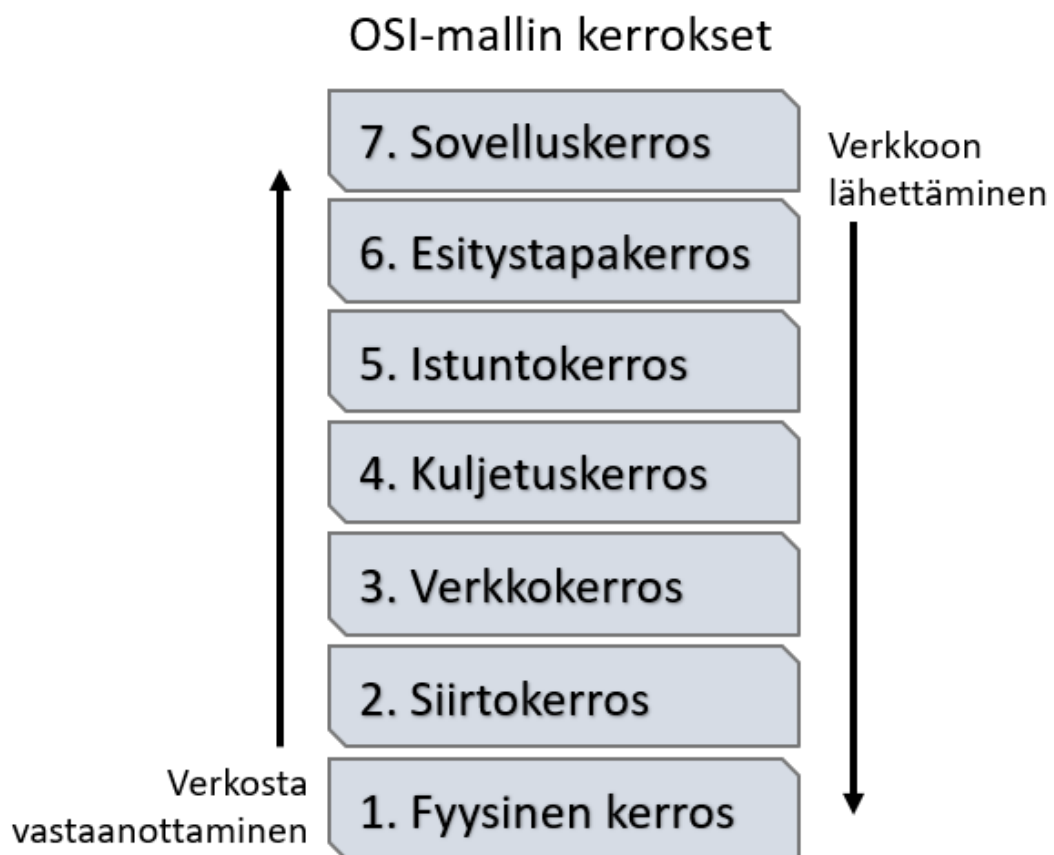


2. Kaikki tietoliikenne suojataan riippumatta sijainnista verkossa. Laitteiden sijainti yrityksen omassa verkossa ei saisi taata itsessään luottamusta kyseiseen laitteeseen. Oman tietoverkon sisältä saapuva liikenne tulisi tarkistaa ja turvata samalla tavalla kuin yrityksen verkon ulkopuolelta saapuva liikenne.
3. Käyttöoikeus resursseihin myönnetään kertaluontoisesti. Palvelua tai sovellusta käyttämään pyytävän käyttäjän oikeus tulisi arvioida joka kerta kun sovellukseen tai palveluun halutaan pääsy. Käyttöoikeuksia tulisi myös myöntää käyttäjille mahdollisimman vähän, kumminkin niin että suoritettavan tehtävän tekeminen onnistuu. Esimerkiksi jos tarvitaan tietyn kansion tiedostoihin pelkkä lukuoikeus, niin muokkausoikeuksia tiedostoihin ei tulisi myöntää. Käyttöoikeuksia pitäisi myös rajata mahdollisimman pieneen määrään resursseja kerralla.
4. Käyttöoikeudet resursseihin päätetään dynaamisilla politiikoilla. Yritys suojaa resurssejaan identifioimalla resurssinsa, käyttäjät ja käyttöoikeuksien tarpeen resursseihin. Dynaamisissa politiikoissa arvioidaan niin resurssia, käyttäjää ja laitetta jolta käyttöoikeuspyyntö saapuu. Käyttäjän identiteettiin voi kuulua käyttäjätunnus ja muut siihen lisätyt yksilöivät tiedot. Laitteen tila voidaan arvioida käyttäen useita erilaisia kriteereitä, kuten ohjelmistoversioita, laitteen sijaintia verkossa, saapuvan pyynnön ajankohtaa, aikaisempaa toimintaa verkossa sekä laitteelle asennettuja valtuustietoja.
5. Yrityksen resurssien suojauksen ja eheyden jatkuva valvonta. Edes yrityksen resursseja ei tulisi luokitella luotetuiksi ilman jatkuvaa valvontaa. Zero Trust -mallia käyttöönottaessa tulisi resursseille luoda myös oma valvonta. Valvonnalla voidaan varmistaa, että resurssit ovat turvallisia ja ohjelmistojen päivitykset ovat ajan tasalla.
6. Resurssien käyttöoikeuksien autentikoinnin ja auktorisoinnin valvonta tulee olla jatkuvaa. Käyttöoikeuksia pitää jatkuvasti valvoa ja pyytää autentikointia, kun sovelluksiin tai palveluihin pyydetään pääsyä. Autentikointi ja auktorisointi voidaan suorittaa esimerkiksi kaksivaiheisella tunnistautumisella (Multi Factor Authentication, MFA)
7. Yritys kerää mahdollisimman paljon informaatiota omista resursseistaan, verkkorakenteesta sekä tietoliikenteestä laitteiden välillä parantaakseen verkon tietoturvallisuutta.

Luetellut peruseriaatteet ovat tarkoituksella mahdollisimman riippumattomia eri teknologioista, jotta yritykset voivat käyttää niitä ohjenuorana omassa toiminnassaan käytettäville laitteille tai sovelluksille. [8]

### 3 OSI-MALLI

OSI-malli (Open Systems Interconnection Model) on yleinen viitekehys, jossa verkon toiminnot jaetaan eri käsitteellisiin kerroksiin, joilla voidaan kuvailla eri toimintoja. Mallissa verkon toiminnot jaetaan 7 eri kerrokseen. Kerrokset ovat fyysinen, siirto-, verkko-, kuljetus-, istunto-, esitystapa- ja sovelluskerros. Kuvassa 1 on perinteinen esitystapa OSI-mallista ja kuvaus, kuinka liikenne kulkee verkosta käyttäjille. [10]



Kuva 1 OSI-mallin kerrokset, ja kuvaus tietoliikenteestä verkossa.

#### Fyysinen kerros

OSI-mallin alin kerros sisältää tietoliikenteen lähettämisen ja vastaanottamisen verkossa. Fyysisestä kerroksesta löytyy fyysisiä laitteita, kuten reitittimiä, kytkimiä, kaapelointia, modeemeja ja verkkosovittimia. Data, joka muunnetaan fyysisessä kerroksessa

biteiksi, voidaan näiden laitteiden välillä lähettää sähköisesti, optisesti tai radiosignaaleilla.[10]

### **Siirtokerros**

Siirtokerroksessa toisiinsa suoraan kytketyt yhteyspisteet hoitavat verkon tietoliikennettä ja korjaavat virheitä, jotka ovat saattaneet tapahtua fyysisessä kerroksessa. Siirtokerroksessa on kaksi omaa alakerrostaan. MAC (Media Access Control) hoitaa tietoliikenteen ohjausta ja kanavointia laitteen lähettämille paketeille verkossa. LLC (Logical Link Control) tarjoaa liikenteen ja virreehallintaa sekä tunnistaa yhteyksien protokollat. [10]

### **Verkkokerros**

Verkkokerroksessa vastaanotetaan paketit siirtokerroksesta ja toimitetaan ne oikeille vastaanottajille pakettiin liitettyjen osoitetietojen mukaisesti. Verkkokerros selvittää vastaanottajan käyttäen loogisia osoitteita, kuten IP-osoitteita. Tässä kerroksessa reitittimet ovat kriittinen osa, jotka reitittävät liikennettä verkkojen kesken. [10]

### **Kuljetus**

Kuljetuskerros hallinnoi datapakettien toimituksia ja virheidentarkistusta. Kuljetuskerros hallinnoi myös datapakettien kokoa, sekvensointia ja yleisesti tiedonsiirtoa järjestelmien ja isäntien välillä. Esimerkiksi TCP, eli Transmission Control Protocol on kuljetuskerros. [10]

### **Istunterkerros**

Istunterkerros hallinnoi keskustelua eri tietokoneiden välillä. Istunto tai yhteys luodaan laitteiden välille ja sitä hallinnoidaan, se myös lopetetaan istunterkerroksessa. Istunterkerroksen toiminnoissa on myös autentikointia ja yhteyden uudelleenmuodostamista. [10]

## **Esitystapakerros**

Esitystapakerros muotoilee ja kääntää dataa sovelluskerrokselle syntaksin perusteella, jota sovellus hyväksyy. Joissain tapauksissa esitystapakerrosta kutsutaan syntaksikerrokseksi. Esitystapakerros voi myös hoitaa sovelluskerroksen vaatimaa salausta ja salauksen purkua. [10]

## **Sovelluskerros**

Sovelluskerroksessa käyttäjä ja sovelluskerros vuorovaikuttavat ohjelmistosovelluksien kanssa. Tämä kerros havaitsee verkkopalvelut, joita myönnetään sovelluksille, kuten verkkoselaimille. Sovelluskerros tunnistaa keskustelukumppanit, resurssien käytettävyyden sekä synkronoi viestinnän. [10]

## 4 ZERO TRUST MALLIIN SIIRTYMINEN

Zero Trust -arkkitehtuuriin siirtyminen ei ole järkevää toteuttaa kerralla koko verkolle, ellei kyseessä ole täysin uuden verkon rakentaminen. Zero Trust käytännöt kannattaa toteuttaa olemassa olevaan verkkoon osittain. Yrityksen verkko on hyvä segmentoida osiin ja pohtia mitkä kohteet halutaan siirtää ensimmäisenä Zero Trust -malliin. Työn pohjana on hyvä olla yrityksen verkon modernisoinnin suunnitelma, joka helpottaa kehitystyön jakamista pienempiin osiin. Monet yritykset toimivat vuosia niin sanotussa verkon hybridimallissa toteuttaen osittain Zero Trust periaatteita ja osittain vanhempaa verkon rajansuojauksen periaatteita. [8]

### 4.1 Alustava tutkimus

Zero Trust -arkkitehtuurissa ensimmäisenä toimenä on selvittää suojattava rajapinta. Rajapinta pitää sisällään yrityksen suojattavia kohteita, kuten dataa, omaisuutta, sovelluksia tai palveluita. Englanniksi näistä käytetään lyhennettä DAAS (data, assets, applications, services). [7]

Esimerkkejä DAASeista ovat

- Data: Luottokorttitiedot, potilastiedot, yksilöivät henkilötiedot, immateriaalioikeudet
- Applications: Käytettävät sovellukset
- Assets: Päätelaitteet, Internet of Things (IoT) laitteet, valmistuslaitteisto
- Services: DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), Active Directory [11]

Kun suojattavat rajapinnat on selvitetty, tulee seuraavaksi tarkkailla verkon liikennettä. Verkon käyttäjien, laitteiden ja sovellusten ja niiden välille tarvittavien yhteyksien identifiointi on elintärkeää oikeanlaisen Zero Trust -politiikan luomiseksi. [7]

Tämän jälkeen kannattaa tehdä Zero Trust -mallisen verkon suunnittelu. ZT (Zero Trust) verkot ovat täysin mukautettuja, yrityksen omien resurssien ja verkkoliikenteen mukaan suunniteltuja. Yleisesti Zero Trust -verkkoja toteutettaessa käytetään toisen sukupolven palomureja. Näitä palomureja käytetään segmentointi yhdyskäytävinä ja niillä voidaan muodostaa mikrokehä suojattavien kohteiden ympärille. Segmentaatiolla voidaan

toteuttaa valvontaa ja käyttövaltuushallintaa kaikelle, joka yrittää käyttää suojattua resurssia. [11]

#### 4.2 Kipling-metodi

Zero Trust -politiikan muodostamiseen voidaan käyttää Kipling-metodia, joka määrittää politiikan avainsanojen mukaan kuka, mitä, missä, milloin, minne, miksi ja miten. Zero Trust -politiikkoja voidaan toteuttaa ainoastaan OSI-mallin 7. kerroksessa. [7]

Politiikat ovat kokoelma sääntöjä ja käytäntöjä, joita käytetään esimerkiksi valtuuttamaan käyttöoikeus tietyille ihmisille yksittäiseen sovellukseen. Politiikkoja voidaan käyttää verkon liikenteen ohjaamiseen ja rajoittamiseen käyttäjiltä sekä laitteilta. [9]

Kipling metodilla voidaan määrittää politiikkaan seuraavat asiat:

- **Kuka** tarvitsee pääsyn suojattuun resurssiin?
- **Mikä** sovellus on käytössä suojattavassa resurssissa?
- **Milloin** resurssia käytetään?
- **Missä** on datapaketin saapumiskohde?
- **Miksi** datapaketti yrittää saada pääsyn suojattavaan resurssiin?
- **Miten** datapaketti saa yhteyden sovelluksen kautta?

Kun politiikat määritellään hyvin tarkasti, varmistutaan siitä, että dataliikenne suojattuihin resursseihin on sallittua. [11]

Kun Zero Trust -politiikka on asetettu käyttöön ja resurssia suojataan, tulee sitä myös jatkuvasti valvoa ja ylläpitää. Valvontaa varten tulee asettaa lokien muodostaminen suojatun resurssin käytöstä. Lokeihin kirjattu valvontadata tulee ylettyä OSI-mallin 7. kerrokseen asti, jotta resurssin käytöstä saadaan mahdollisimman realistinen kuva. Tällä tavoin voidaan resurssia suojata tehokkaasti ja saadaan kuva, kuinka paljon resursseja käytetään. [11]

## 5 TYÖNTEKIJÖIDEN ETÄTYÖSKENTELY

Suuri osa yrityksen työntekijöistä työskentelee tällä hetkellä etänä nykyisen pandemiatilanteen vuoksi. Työntekijöille on annettu kehoitus tehdä etätöitä, jos omat työtehtävät tämän sallivat. Etätyöskentelyssä yrityksen työntekijät käyttävät VPN-sovellusta muodostaakseen suojatun yhteyden yrityksen sisäverkkoon yrityksen ulkopuolelta.

### 5.1 Käytössä oleva laitteisto

Yrityksen työntekijät käyttävät pääasiassa yrityksen toimittamia työasemia etätyöskentelyyn. Työasemiin on asennettu vakiosovellukset, sekä eri työtehtävissä tarvittavia sovelluksia. Vakiosovelluksiin kuuluu myös VPN-ohjelma turvatun yhteyden muodostamiseen yrityksen verkkoon.

### 5.2 VPN ongelmat

Työntekijöille ilmaantui VPN-yhteyksissä erilaisia ongelmia. On ilmaantunut reititysongelmia, jotka estävät yhteyksiä toimimasta. VPN-yhteyden luotettavuudessa on myös ollut ongelmia. Yhteydet ovat saattaneet yllättäen katketa kesken työnteon ja kestää jonkin aikaa, että yhteys palaa takaisin. Käyttäjät ovat myös raportoineet yhteyksien nopeuksien hidastumisesta, kun VPN-yhteyttä on käytetty. Ongelmien takia on yrityksen sisällä alettu pohtimaan vaihtoehtoja VPN yhteyksille ja Zero Trust -arkkitehtuuri todettiin parhaaksi tavaksi poistamaan liikennettä VPN tunneleista internetin yli käytäväksi. Verkon uudistaminen päätettiin aloittaa etätyöstä.

### 5.3 Etätyöskentely

Tutkittaessa työasemille asennettavia sovelluksia paljastui muutamia sovelluksia, jotka vaativat yhteyden yrityksen sisäverkkoon. Näiden sovellusten siirtäminen toteutuksiin, joissa ei tarvita VPN-yhteyttä parantaisi yrityksen tietoturvaa. Etätyöskentelyssä tarvitaan myös yhteyttä yrityksen sisäverkossa sijaitseviin levyosioihin sekä mahdollisuutta tulostaa yrityksen omiin tulostimiin ja monitoimilaitteisiin verkon yli. Näille kaikille on pyritty löytämään vaihtoehtot, jotka voidaan toteuttaa Zero Trust -periaatteella.

## 6 AZURE AD APPLICATION PROXY -PALVELU

Azure AD (Active Directory) Application Proxy mahdollistaa sisäverkon web-sovellusten julkaisemisen ulkoverkkoon. Etäkäyttäjät, jotka tarvitsevat pääsyä yrityksen sisäverkossa sijaitseviin sovelluksiin voivat päästä käyttämään sovelluksia turvallisesti Azure AD Application Proxyn kautta. Azure AD Application Proxyn avulla on mahdollista päästää etätyöntekijät käyttämään sovelluksia jopa omilla laitteillaan ilman VPN yhteyttä käyttäen yhtä Azure AD kirjautumista. [12]

### 6.1 Tietoturvallisuus

Azure AD Application Proxy tarjoaa myös monia tietoturvaluushyötyjä. Azure ADta käyttäen voidaan päästää ainoastaan hyväksytyt yhteydet läpi omaan sisäverkkoon. Sallimalla pelkästään hyväksytyt yhteydet estävät suuren määrän anonyymejä hyökkäyksiä, sillä ainoastaan autentikoidut tunnukset pääsevät käsiksi sovelluksiin. [13]

Application Proxyssa on myös mahdollista määrittää sovelluksia käyttävät henkilöt. Muodostamalla politiikkoja voidaan määrittää ehtoja, jotka mahdollistavat pääsyn sovellukseen. Ehdot voivat perustua useampaan vaihtoehtoon, kuten sijaintiin, josta kirjautuminen tapahtuu, autentikoinnin vahvuuteen ja riskiprofiiliin. Ehdollisessa pääsyssä voidaan myös käyttää kaksivaiheista tunnistautumista, lisäten yhden tietoturvaluuskerroksen käyttäjien autentikointiin ja Microsoft Cloud App Securitylla voidaan tarkkailla sovelluksia reaaliaikaisesti. [13]

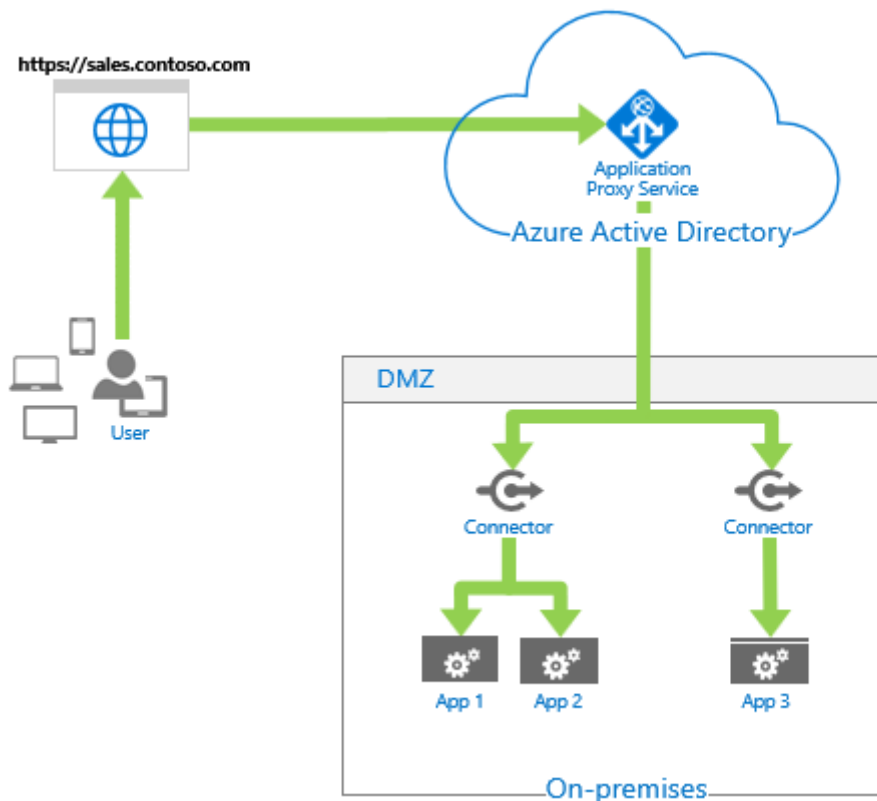
Kaikki liikenne Application Proxyssa päättyy pilveen, koska Azure AD Application Proxy on käänteinen välityspalvelin. Tästä konfiguraatiosta johtuen palvelimiin ei koskaan muodosteta suoraa HTTP-yhteyttä ja palvelimet on paremmin turvattu tähdätyiltä hyökkäyksiltä. [13] Azure AD Application Proxy on myös rakennettu niin, että sisäverkkoon ei tarvitse avata saapuville yhteyksille portteja. Application Proxyn liittimet käyttävät vain ulospäin suuntautuvia yhteyksiä, ja kaikki yhteydet ovat suojattuja.[13]



## 6.2 Toiminta

Application Proxy on Azure AD palvelu, joka konfiguroidaan Azuren omassa portaalissa. Application Proxyn kautta on mahdollista julkaista julkinen HTTP/HTTPS-osoite Azuren pilvessä, joka yhdistyy sisäverkossa sijaitsevan sovelluspalvelimen osoitteeseen. Tämän toiminnon avulla käyttäjät pääsevät käsiksi sisäisiin web-sovelluksiin samalla tavalla kuten he pääsevät käsiksi esimerkiksi Microsoft 365:een. [12]

Palvelun komponentteihin kuuluvat Application Proxy -palvelu, joka toimii pilvessä, Application Proxy -liitin, agentti, joka on käynnissä sisäverkon palvelimella ja liittää Application Proxy -palvelun ja käytettävän sovelluksen, sekä Azure AD, joka toimittaa ja tarkastaa käyttäjien identiteetit. Kirjautumisen jälkeen käyttäjät pystyvät käyttämään web-sovelluksia joko tutulla URL-osoitteella tai My Apps -sovelluksen kautta. Application Proxyn kautta on mahdollista valtuuttaa pääsy esimerkiksi Remote Desktopiin, SharePoint sivustoille sekä Outlookin verkkoversioon. [12] Kuvassa 2 on yksinkertaisesti selitettynä Application Proxyn komponenttien liittyminen toisiinsa.



Kuva 2 Application proxyn toiminta (Microsoft 2021)

### 6.3 Vaatimukset

Jotta voi toteuttaa AD Application Proxyn omassa verkossa, tulee ensin täyttää palvelun vaatimukset. Azure AD:sta pitää olla verkossa asennettuna Premium versio, jotta Application Proxy voidaan ottaa käyttöön. Toimiakseen AD Application Proxy vaatii, että verkkoon on asennettu liittimiä. Liittimet toimivat agentteina, jotka yhdistävät käyttäjät soveluksiin sisäverkossa. Liittimet voidaan asentaa palvelimille, virtuaalikoneelle, jossa on hypervisor, tai virtuaalikoneelle, joka on asennettu Azure palveluun. Liittimen kautta voidaan muodostaa ulospäin suuntautuva yhteys Application Proxy palvelua varten. Laitteet, joille liitin asennetaan, tulee olla TLS (Transport Layer Security) 1.2 versio käytössä. Jos toteutus on mahdollista, liittimet kannattaa asentaa samaan verkkoon ja segmenttiin kuin liittimiä käyttävät web-sovellukset. Application Proxy liittimet yhdistävät HTTPS:n ja HTTP:n kautta, joten portteihin 443 ja 80 tulee avata ulospäin suuntautuva liikenne. [14]

Application Proxyn liittimet tarvitsevat myös pääsyn useisiin verkko-osoitteisiin rekisteröintiä ja verifiointia varten. Osoitteet ovat luoteltuna lähteessä [15] kohdassa Allow access to URLs. Näihin osoitteisiin tulee sallia pääsy yrityksen palomuurista, jotta palvelu toimii. [15]

## 7 CITRIX VIRTUAL APPS AND DESKTOPS JA WORKSPACE -PALVELU

Citrix Virtual Apps and Desktop -palvelun avulla voi turvallisesti toimittaa käyttäjille virtuaalisia sovelluksia tai työpöytiä mille tahansa laitteelle. Palvelu tarjoaa käyttäjille pääsyn Windows- ja Linux-sovelluksiin tai virtuaalisiin työpöytiin keskitetysti ja turvallisesti riippumatta käyttäjän sijainnista tai käyttämästään käyttöjärjestelmästä. [16]

Citrixin Workspace-sovellus antaa käyttäjille keskitetyn pääsyn virtuaalisiin sovelluksiin, -työpöytiin, web-sovelluksiin sekä SaaS:iin (Software as a Service). Sovellus voidaan asentaa koneelle tai sitä voidaan käyttää selaimella yrityksen tarjoamasta internet-osoitteesta. [17]

### 7.1 Toiminta

Citrix Virtual Apps and Desktops -palvelu mahdollistaa virtualisointiratkaisuja, jotka tarjoavat yrityksen IT:lle hallinnoinnin virtuaalikoneista, -sovelluksista ja tietoturvasta tarjoten samalla pääsyn käyttäjille riippumatta sijainnista tai laitteesta. Palvelun avulla toimittavien sovellusten ja virtuaalikoneiden asennus, konfigurointi, päivitykset ja monitorointi jää Citrixille. Yritykselle jää täysi kontrolli sovelluksien, politiikkojen ja käyttäjien hallinnoinnista. [18]

Yrityksen resurssit yhdistetään Citrix Cloud Connectoriin, joka toimii yhdyskäytävänä yrityksen resurssien ja Citrix Cloudin välillä. Cloud Connector mahdollistaa pilven hallinnoinnin ilman VPN yhteyksiä. Resurssit sisältävät Cloud Connectorit sekä laitteistot tai muut resurssit, joita käytetään toimittamaan ohjelmat ja virtuaalikoneet käyttäjille. [18]

Citrix Cloudissa tehdään konfiguraatiot sovellusten ja virtuaalityöpöytien toimittamisesta käyttäjille. Citrix Cloudissa määritellään myös URL-osoite, mistä käyttäjät pääsevät Citrix Workspaceen sekä käyttäjien tunnistautumistapa, esimerkiksi Active Directory. Citrix Cloudissa pääsee myös määrittämään ulkoisia yhteyksiä käytettyjen resurssien sijainneille. [18]

Käyttäjät voivat asentaa Citrix Workspace-sovelluksen omalle päätelaitteelleen. Workspace-sovelluksen kautta käyttäjät pääsevät turvallisesti käyttämään heille

luvitettuja ohjelmia, dokumentteja, työpöytiä. Workspace-sovellusta voidaan käyttää tietokoneilla, älypuhelimilla tai tableteilla. Jos laitteelle ei voida asentaa Workspace-sovellusta, niin Workspacea pääsee käyttämään myös selaimella. [18]

Citrix Virtual Apps and Desktops -palvelusta löytyy monia erilaisia tapoja toimittaa sovelluksia käyttäjille.

- Asennettu sovellus: Sovellus, joka asennetaan osana järjestelmäasennusta virtuaalisille koneille.
- Streamed app (Microsoft App-V): Sovellus toimitetaan käyttäjille verkon yli pyynnöstä. Sovellus ja sen rekisteriasetukset on eristetty virtuaalisella työasemalla käyttöjärjestelmästä. Toiminto auttaa ratkaisemaan yhteensopivuusongelmia sovelluksen ja käyttöjärjestelmän välillä.
- Layered app (Citrix App Layering): Jokaisessa kerroksessa on määriteltynä yksi sovellus, agentti tai käyttöjärjestelmä. Layered appia käyttäen järjestelmänvalvoja pystyy helposti luomaan toimitettavia näköistiedostoja sovelluksista. Kun yksi kerros päivitetään, päivittyy se kaikkiin näköistiedostoihin, jotka käyttävät kyseistä kerrosta.
- Hosted Windows App: Sovellus on asennettu useamman käyttäjän Citrix Virtual Apps -isännälle ja toimitetaan sovelluksena käyttäjille. Käyttäjät pääsevät helposti käyttämään sovellusta, vaikka sovellus toimitetaan etäältä.
- Tietokoneen etäkäyttö: Etäkäyttö mahdollistaa käyttäjän oman työpaikalla sijaitsevan työaseman käyttämisen etänä. Työasemalta käyttäjät pääsevät käyttämään sovelluksia ja resurssejaan ongelmitta. [19]

## 7.2 Zero Trust -arkkitehtuuri Citrixillä

Citrix Virtual Apps and Desktops ja Workspace -palveluiden avulla on mahdollista rakentaa Zero Trust -toteutuksella pääsy sisäverkon resursseihin käyttäjille. Workspace toimii pisteenä, jossa valvotaan pääsyä sovelluksiin ja tietoihin. Pääsyn käsittely alkaa vakiolla ”default deny”-säännöllä, joka estää pääsyn. Pääsy annetaan vasta kun oikeus on varmistettu käyttäjän ja laitteen tunnistetiedoilla, sekä muilla tiedoilla, mukaan lukien aika, sijainti. [20]

Citrix Gateway -palvelulla voidaan hoitaa tietoturvaa joustavasti. Palvelussa voi konfiguroida useita todennusvaiheita luottamuksellisen datan pääsyyn, jotka voivat pohjautua

käyttäjään, rooliin, sijaintiin, laitteiston tilaan sekä moniin muihin. Citrixin identiteettilähtöinen todentamistapa mahdollistaa yrityksen omien identiteettisovellusten säilyttämisen, kuten kaksivaiheinen todentaminen. Se tukee muun muassa LDAP, RADIUS-, TACACS-, Diameter- ja SAML2.0 -autentikointia. [20]

Citrix Gateway -palvelulla voidaan toteuttaa myös SmartAccess ja SmartControl politiikkoja, jotka tarjoavat joustavuutta käyttöoikeuden myöntämiseen. SmartAccess skannauksen tuloksen perusteella käyttäjälle voidaan myöntää täysi pääsy, osittainen pääsy, karanteeni tai yhteyksien esto. Esimerkkinä, jos käyttäjän laite ei läpäise yhteneväisyysvaatimuksia, käyttäjälle voidaan myöntää vähennettyjä oikeuksia sovelluksiin tai resursseihin. SmartControl keskittää politiikkojen hallinnoinnin Citrix Gatewayhin. [20]

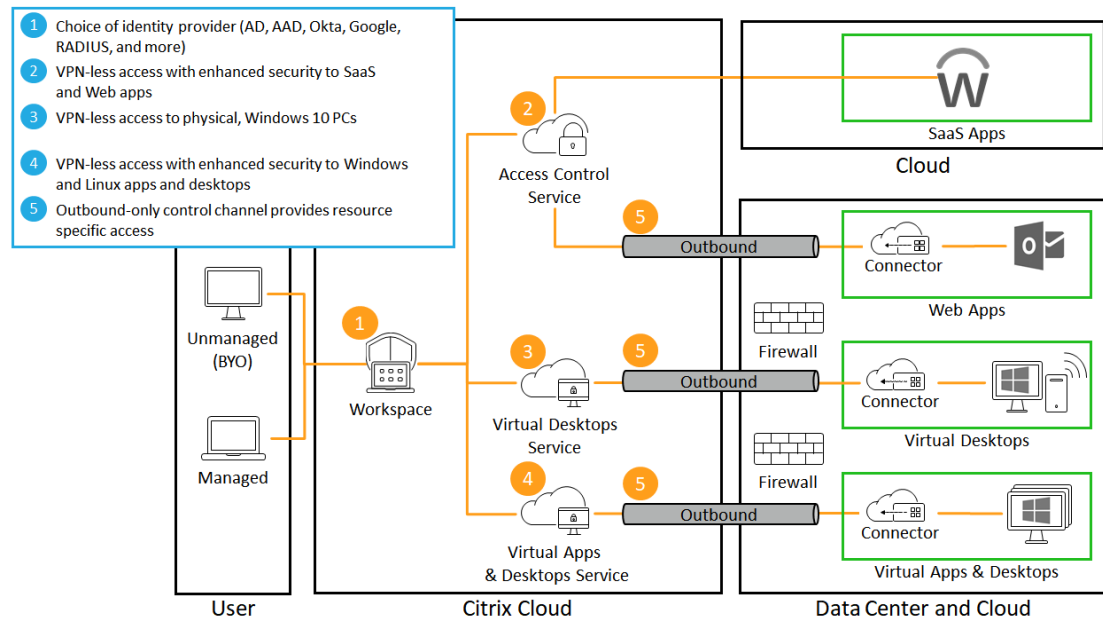
Secure Workspace Access keskittyy suojaamaan käyttäjän työtilan yrityksen hallinnoituilla laitteilla ja myös käyttäjien omilla laitteilla. Käyttäjien tiedot ovat aina suojattuja. Citrix Secure Workspace Access mahdollistaa URL-osoitteiden suodatusta ja integroidun selaimen eristyspalvelun. Työkalut tarjoavat järjestelmänvalvojalle mahdollisuuden sallia tai estää pääsy URL-osoitteisiin eristetyssä tilassa. Perinteinen URL-suodatus luottaa sokeasti osoitteisiin sallittujen osoitteiden listalla. Secure Workspace Access ei lähtökohtaisesti luota osoitteisiin sallittujen listalla, sillä sivustoilla saattaa olla haitallisia linkkejä. Secure Workspace Access testaa myös linkit sallittujen osoitteiden sisällä. [20]

Citrix Security Analytics valvoo verkkoa ja tarjoaa riskien arviointia Zero Trust -arkkitehtuurin perustalla. Security Analytics kokoaa yhteen tapahtumia kaikista Citrix palveluista. Palvelu auttaa visualisoimaan ja kartoittamaan luottamussuhteita. Se korreloi tapahtumia ja toimia tunnistaakseen poikkeamien tunnistamiseksi. [20]

Citrix Security Analytics -palvelulla voidaan suorittaa jatkuvaa seuranta verkko sivujen käytöstä. Valvotut toimet sisältävät vierailun haitallisilla, vaarallisilla tai tuntemattomilla verkkosivuilla, käytetyn verkon kaistan määrän sekä vaaralliset tiedoston siirrot. Jos käyttäjä lataa suuria määriä tiedostoja, voidaan häneltä kysyä selitystä toiminnalle ja vastauksen perusteella tehdä jatkotoimia. Sääntöjä voidaan konfiguroida aktivoitumaan tietyistä toimista arvioimalla jatkuvasti riskejä. Esimerkiksi Citrix Workspace -istunto voidaan katkaista, jos tarkkailtu riski pistemäärän muuttuessa. [20]

Järjestelmänvalvojat voivat sallia pääsyn palveluihin, kun riski tasot ovat sallitulla tasolla. Nämä ominaisuudet aktivoituvat erilaisten tekijöiden perusteella kirjautumisen aikana tai jatkuvassa valvonnassa Citrix Security Analyticsilla. Se seuraa jatkuvasti tapahtumia ja riski-indikaattoreita Citrix-palveluista ja kolmannen osapuolen tietoturvatkaisuista

kuten Azure AD. Kuvassa 3 on kaavio, miten Citrixin omat palvelut yhdistyvät toisiinsa Zero Trust -arkkitehtuurissa. [20]



Kuva 3 Citrix palveluiden yhteydet Zero Trust toteutuksessa. (Citrix 2021)

## 8 MICROSOFT UNIVERSAL PRINT -PALVELU

Microsoft Universal Print mahdollistaa paikallisten verkkotulostuspalvelimien siirtämisen pilveen. Universal Print toimii täysin Microsoft Azurella. Kun palvelu otetaan käyttöön yhteensopivilla tulostimilla, se ei vaadi yrityksiltä paikallista infrastruktuuria. Universal Print on Microsoft 365 tilauspohjainen palvelu, jonka kautta yritykset voivat keskittää tulostimiensa hallinnoinnin. Palvelu on täysin integroitu Azure AD:n kanssa ja tukee kertakirjautumista. Universal Print -palvelua voidaan käyttää myös ei-tuettujen tulostimien kanssa, käyttäen Universal Print liitinohjelmistoa. [21]

Universal Print toimii yhteistyössä monien tulostussovellusten ja laitteistojen valmistajien kanssa. Moni valmistaja onkin tehnyt valmiiksi toteutuksia, jotka integroituvat helposti Universal Print -palvelun kanssa. Tähän listaan kuuluvat muun muassa Brother, Canon, HP, Lexmark, PaperCut, Printix, Toshiba, Xerox sekä monia muita. [22]

Universal Print on uusi ratkaisu markkinoilla, joten vielä ei ole paljon laitteita, jotka integroituvat suoraan palveluun. Tämän kaltaisissa tapauksissa tulostimet yhdistetään Universal Print liitintä sovelluksen avulla. Tulostimet rekisteröidään palveluun tämän avulla, jonka jälkeen tulostimia voidaan tuoda käyttöön. Universal Print liitin asennetaan laitteelle, joka täyttää seuraavat vaatimukset:

- Käynnissä ympäri vuorokauden (lepo-/horrostila otettu pois päältä)
- On jatkuvasti yhteydessä internettiin
- Pääsee yhdistämään seuraaviin osoiteisiin
  - \*.print.microsoft.com
  - \*.microsoftonline.com
  - \*.azure.com
  - \*.msftauth.net
  - go.microsoft.com
  - aka.ms [23]

Kun tulostimet on rekisteröity palveluun liitintäsovelluksen kanssa, voidaan tulostimia jakaa käytettäväksi käyttäjille. Tulostimien jakaminen onnistuu Azure -portaalin kautta, jossa tulostimille voidaan asettaa nimet sekä määrittää käyttäjät, jotka pääsevät käyttämään tulostinta. Tulostimien jakamiselle on asetus, josta tulostin voidaan jakaa kaikille

organisaation käyttäjille kerralla, tai määrittää pienempi käyttäjäryhmä kyseiselle tulostimelle. [24]

Universal Print -palvelu toimii pilvessä, mikä mahdollistaa tulostimien käytön mistä tahansa. Tarvitaan internet yhteys ja mahdollisuus autentikoida Azure AD:n kanssa. Universal Print poistaa myös tulostinajurien asennusvaatimuksen tulostavilta laitteilta. Käyttäjät pystyvät palvelusta etsimään itsellensä lähimmän tulostimen helposti ja tulostamaan vaivattomasti. Tulostimien käyttöoikeuksien määrittäminen Azure AD:n kautta parantaa tietoturvaa ja kaikki yhteydet ovat suojattuja HTTPS-yhteyksillä. [25]



## 9 ZERO TRUST NETWORK ACCESS

Zero Trust Network Access (ZTNA) on kategoria teknologioita, jotka mahdollistavat turvatun etäyhteyden sovelluksiin ja palveluihin perustuen kulunvalvontapolitiikkoihin. Toisin kuin VPN-yhteydet, jotka myöntävät täydellisen pääsyn sisäverkkoon, ZTNA-ratkaisulla voidaan sallia yhteydet vain tiettyihin resursseihin ja oletusarvoisesti kieltää pääsy muihin resursseihin. [26]

### 9.1 Toiminta

ZTNA:lla pääsy resursseihin sallitaan käyttäjän autentikoinnin jälkeen ZTNA-palvelussa. ZTNA-palvelu antaa pääsyn resurssiin turvatun kryptatun tunnelin kautta. Tämä tarjoaa lisäkerroksen tietoturvaa yrityksen sovelluksille suojaten muuten julkisesti näkyvän IP-osoitteen. [26]

ZTNA käyttää hyväksi niin sanottua Dark Cloud -konseptia, estäen käyttäjiä näkemästä ja käyttämästä sovelluksia ja palveluita, joihin heillä ei ole käyttöoikeuksia. Tämä ehkäisee mahdollista sivuttaisliikettä verkossa, missä vaarantunut tunnus tai päätelaite voisi skannata sisäverkon. [26]

ZTNA-palvelussa kulunvalvonta voidaan toteuttaa identiteettipohjaisilla järjestelmillä, vaihtoehtona IP-osoite pohjaisille konfiguraatioille VPN-palveluissa. ZTNA mahdollistaa myös sijainti- tai laitekohtaisen kulunvalvonnan, estäen esimerkiksi päivittämättömiä tai haavoittuneita laitteita yhdistämästä yrityksen palveluihin. [26]

### 9.2 Fortinet

Fortinetin palveluilla on mahdollista toteuttaa ZTNA-palvelu yrityksen etätyöntekijöille. Fortinetin Zero Trust Access (ZTA) -viitekehys käyttää hyväksi integroituja tietoturvaratkaisuja, jotka mahdollistavat käyttäjien ja laitteiden tunnistamisen ja luokittelun niiden yrittäessä yhdistää verkkoon. Niiden yhteensopivuus yrityksen omiin politiikkoihin voidaan arvioida sekä seurata niitä jatkuvasti verkossa. [27]

FortiAuthenticator toimii keskitettynä paikkana käyttäjien tunnistautumiselle, valtuuttamiselle, kirjanpidolle, käyttöoikeuksien hallinnoinnille ja kertakirjautumiselle. Se varmentaa

käyttäjän identiteetin muun muassa käyttäjätunnuksen, varmenteiden ja monivaiheisen tunnistautumisen kanssa. FortiAuthenticator jakaa nämä tiedot roolipohjaisen kulunvalvontapalvelun kanssa myöntääkseen käyttäjälle räätälöidyn pääsyn sovelluksiin ja palveluihin. FortiAuthenticator tukee myös Security Assertion Markup Language (SAML) -toteutuksia, mahdollistaen turvallisen pääsyn SaaS-ratkaisuihin, kuten Microsoft 365. [27]

FortiToken mahdollistaa kaksivaiheisen tunnistautumisen FortiAuthenticatorille, joko fyysisellä avaimella tai mobiiliratkaisuna. Mobiiliratkaisu on Open Authorization (OAuth) -yhteensopiva kertakäyttöinen salasananageneraattori Android tai iOS laitteille, joka tukee aika- tai tapahtumapohjaisia avaimia. [27]

FortiNAC, verkon kulunvalvontaratkaisu havaitsee ja tunnistaa verkossa olevat tai siihen pääsyä hakevat laitteet. FortiNAC skannaa ne varmistaakseen, että laitteet eivät ole vaarantuneet ja luokittelee ne roolin ja toiminnan mukaisesti. Se voi hyödyntää olemassa olevia agentteja hakeakseen laitteiden tietoja. [27]

FortiNAC voi tehdä dynaamista verkon mikrosegmentointia, vaikka verkossa olisi useamman valmistajan laitteistoja. Se tukee yli 170 valmistajaa ja 2400 laitetta, ja toimii vuorovaikutuksessa niiden kanssa pitääkseen ne omissa segmenteissään. FortiNAC voi myös integroitua FortiGate toisen sukupolven palomuurin kanssa tarjotakseen aiempohjaista segmentointia. Aiempohjaisella segmentoinnilla voidaan merkitä resursseja yhteensopivuusvaatimuksilla, esimerkiksi GDPR, ja FortiGate-palomuuuri pitää vaatimukset voimassa riippumatta siitä mihin resurssi siirtyy verkossa. [27]

ZTA toimintamalli olettaa, että luottamus laiteeseen on muuttuvaa. Laite saattaa olla luotettu, ja sen jälkeen saastua, tai sovellukset laitteessa saattavat paljastua haavoittuviksi. Pitääkseen luottamukset ajan tasalla FortiNAC valvoo verkkoa jatkuvasti. Huomatesaan epänormaalia laitetoimintaa FortiNAC voi toteuttaa vastatoimia, kuten sijoittaa laitteen karanteenialueelle, jotta laitteisto ei voi toimia hyökkäysalustana verkkoon, tai siirtää laitteita korjaussegmenttiin, jotta käyttäjä voi ratkaista havaitun ongelman. [27]

FortiClient-sovelluksella voidaan toteuttaa joustavia VPN-yhteys mahdollisuuksia päätelaitteille. Se tukee Secure Socket Layer (SSL) -yhteyksiä sekä Internet Protocol security (IPSec) -yhteyksiä. Sovelluksella on mahdollista tehdä jaettua tunnelointia SSL-yhteyksillä, jotta käyttäjien kaikki internet liikenne ei mene yrityksen VPN-päätteen läpi parantaen VPN-yhteyden käyttömukavuutta. Samalla FortiClient-sovelluksessa on suojauksia, että internet-pohjainen liikenne ei voi päätyä VPN-yhteyteen ja vaarantaa sitä. [27]

Käyttäjien yhdistäessä yrityksen sisäverkkoon FortiClient Fabric Agent jakaa päätelaitteen turvallisuus telemetria dataa, kuten käyttöjärjestelmän, sovellukset, tunnetut heikoudet, päivitykset ja tietoturvallisuus tilan FortiGaten toisen sukupolven palomuurin kanssa. Tämä mahdollistaa Fortinetin ZTA-työkalujen parantaa käyttöikeuden politiikkoja laitteille. [27]

## 10 POHDINTA

Opinnäytetyön pääasiallinen tavoite oli tehdä alustavaa tutkimusta yrityksen etätyöskentelijöiden VPN-yhteyksien vähentämiseen. Työn ensimmäisenä vaiheena oli tehdä tutkimusta, mihin kaikkeen etätyöskentelijät tarvitsevat yhteyttä yrityksen sisäverkkoon. Tutkimuksessa paljastui ohjelmistoja, jotka eivät toimi ilman sisäverkon yhteyttä. Tämän jälkeen tutkimus suuntautui etsimään vaihtoehtoja näiden sovellusten toteutukselle paikallisen asennuksen sijaan.

Harmillisesti ajallisesti lyhyen tutkimuksen takia ei yrityksen verkosta ehditty tehdä kattavampaa tutkimusta, ja tutkimus keskittyi Zero Trust -arkkitehtuuria noudattavien vaihtoehtojen etsimiseen yritykselle. Yrityksen tarpeisiin soveltuvia vaihtoehtoja löytyi muutama, joita lähdettiin tutkimaan opinnäytetyössä enemmän. Nämä vaihtoehdot vaativat lisätutkimusta vielä yrityksen omien sovellusten ja järjestelmien kanssa, ennen kuin niitä voidaan alkaa toteuttamaan yrityksessä.

Jatkossa yrityksen tietoliikenteen, palvelinten ja kyberturvan henkilöstön tulee tutkia tarkemmin sovelluksia ja niiden vaatimuksia sekä mahdollista toteutusta. Yrityksellä on jo käytössään osittain palveluita Citrixiltä, joten mielestäni helpoin ratkaisu suurimmalle osalle yhteyksien Zero Trust -toteutuksesta onnistuisi Citrix Virtual Apps and Desktops -palveluiden kautta. Tämä vaatii toki lisätutkimusta siitä, miten toteutus jatkossa tehtäisiin.

## LÄHTEET

- [1] Akava 2019. Etätyö. Viitattu 6.2.2021 <https://akava.fi/tietoa-tyosta/etatyo/>
- [2] National Cyber Security Centre 2020 Mobile Device Guidance. Viitattu 6.2.2021 <https://www.ncsc.gov.uk/collection/mobile-device-guidance/infrastructure/network-architectures-for-remote-access#zero>
- [3] Cisco What is a VPN – Virtual Private Network. Viitattu 6. Helmikuu 2021 [https://www.cisco.com/c/en\\_uk/products/security/vpn-endpoint-security-clients/what-is-vpn.html](https://www.cisco.com/c/en_uk/products/security/vpn-endpoint-security-clients/what-is-vpn.html)
- [4] Valtioneuvoston viestintäosasto 2020. Viitattu 6. Helmikuu 2021 <https://valtioneuvosto.fi/-/10616/hallitus-teki-periaatepaatokset-maskisuosituksesta-ja-etatyosta>
- [5] Terva, P. 2020. *Zero Trust -arkkitehtuuri*. Insinöörityö. Kaakkois-Suomen ammattikorkeakoulu, Kouvola. 38s.
- [6] Oksanen E. *VPN-erillisverkon käyttöönotto yrityksessä*. Insinöörityö. Turun ammattikorkeakoulu, Turku. 2019. 31s.
- [7] Palo Alto Networks. What is a Zero Trust Architecture. Viitattu 28.2.2021 <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>
- [8] Rose S. – Borchert O. – Mitchell S. – Connelly S. National Institute of Standards and Technology 2020. Zero Trust Architecture. Viitattu 8.3.2021 <https://csrc.nist.gov/publications/detail/sp/800-207/final>
- [9] Cisco. What is a network policy. Viitattu 8.3.2021 <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-policy.html>
- [10] Forcepoint. The OSI Model Defined. Viitattu 10.3.2021 <https://www.forcepoint.com/cyber-edu/osi-model>
- [11] Palo Alto Networks. Implementing Zero Trust Using the Five-Step Methodology. Viitattu 14.3.2021 <https://www.paloaltonetworks.com/cyberpedia/zero-trust-5-step-methodology>
- [12] Microsoft 2020. Using Azure AD Application Proxy to publish on-premises apps for remote users. Viitattu 1.4.2021 <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-proxy>
- [13] Microsoft 2020. Security considerations for accessing apps remotely with Azure AD Application Proxy. Viitattu 1.4.2021 <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-security>
- [14] Microsoft 2020. Plan an Azure AD Application Proxy deployment. Viitattu 5.4.2021 <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-deployment-plan>
- [15] Microsoft 2021. Tutorial: Add an on-premises application for remote access through Application Proxy in Azure Active Directory. Viitattu 5.4.2021 <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-add-on-premises-application>
- [16] Citrix, Ruiz A. 2020. Citrix Virtual Apps and Desktop service. Viitattu 11.4.2021 <https://docs.citrix.com/en-us/tech-zone/learn/tech-briefs/cvads.html>
- [17] Citrix, Feller D. 2020. Workspace App. Viitattu 11.4.2021 <https://docs.citrix.com/en-us/tech-zone/learn/tech-briefs/workspace-app.html>

- [18] Citrix 2021. Citrix Virtual Apps and Desktops service. Viitattu 12.4.2021 <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops-service.html>
- [19] Citrix 2021. Citrix Virtual Apps and Desktops service Delivery Methods. Viitattu 13.4.2021 <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops-service/delivery-methods.html>
- [20] Citrix, Lazurca F. 2021. Zero Trust Architecture Viitattu 17.4.2021 <https://docs.citrix.com/en-us/tech-zone/learn/tech-briefs/zero-trust.html#citrix-zero-trust-architecture>
- [21] Microsoft 2020. What is Universal Print. Viitattu 18.4.2021 <https://docs.microsoft.com/en-us/universal-print/fundamentals/universal-print-what-is>
- [22] Microsoft 2021. Universal Print, Partner Integrations. Viitattu 18.4.2021 <https://docs.microsoft.com/en-us/universal-print/fundamentals/universal-print-partner-integrations>
- [23] Microsoft 2020. Install Universal Print Connector on Windows. Viitattu 18.4.2021 <https://docs.microsoft.com/en-us/universal-print/fundamentals/universal-print-connector-installation>
- [24] Microsoft 2020. Universal Print, Share Printers. Viitattu 18.4.2021 <https://docs.microsoft.com/en-us/universal-print/portal/share-printers>
- [25] Microsoft. Universal Print. Viitattu 18.4.2021 <https://www.microsoft.com/en-us/microsoft-365/windows/universal-print>
- [26] Palo Alto. What is Zero Trust Network Access. Viitattu 21.4.2021 <https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access>
- [27] Fortinet. Zero-Trust Access for Comprehensive Visibility and Control. Viitattu 21.4.2021 <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-zero-trust-network-access-for-visibility-and-control.pdf>