Opinnäytetyö (AMK)

Tieto- ja viestintätekniikan koulutus

2020

Patrik Svensberg

ROOLIPERUSTAISEN VERKKOSEGMENTOINNIN SUUNNITTELU

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Insinööri, tieto- ja viestintätekniikka

Kevät 2020 | 33 sivua

Patrik Svensberg

ROOLIPERUSTAISEN VERKKOSEGMENTOINNIN SUUNNITTELU

Viime vuosina yritysmaailmassa on muodostunut trendiksi siirtää resursseja pilvipalveluihin. Nykyään pilvessä isännöidyt applikaatiot ovat syrjäyttämässä paikalliset ratkaisut, koska ne eivät onnistu tarjoamaan ohjelmistoja palveluina läheskään yhtä kätevästi. Opinnäytetyössä kartoitettiin ja suunniteltiin rooliperustainen verkkosegmentointiratkaisu, jonka tarkoitus oli yksinkertaistaa reititystä verkossa ja samalla tavoitteena oli siirtyä pois suoraviivaisista ja yleisistä tietoturva-alueista ja niiden toteutuksista. Rooliperustaiseen verkkosegmentointiin hyödynnettiin modernia verkon käyttöoikeuksien hallintaratkaisua.

Työtä lähestyttiin tutustumalla teknologioihin, joita projektissa käytettäisiin ja kartoittamalla, miten nykyinen järjestely oli toteutettu. Näiden jälkeen tutkittiin, mikä olisi paras menetelmä toteuttaa halutut tavoitteet ja mitä ne tulisivat vaatimaan. Kaikkien näiden asioiden ollessa selvillä, lähdettiin luomaan suunnitelmaa projektin toteutuksesta. Usean eri suunnitelman jälkeen päästiin lopulliseen ratkaisuun, joka tultaisiin toteuttamaan.

Lopullisessa suunnitelmassa luodaan kaksi aliverkkoa, joista toinen toimii vierasverkkona ja toinen toimistoverkkona. Vierasverkkoa muutetaan niin, että se sisältää vieraslaitteiden lisäksi ei-varmennettuja yrityslaitteita. Tämä segmentointi tullaan toteuttamaan rooliperustaisella menetelmällä, jossa käyttäjän oikeuksiin voidaan määritellä, mihin heillä on oikeus.

Työn suunnittelu antoi hyvän kuvan, mitä eri asioita kannattaa vastaavissa tehtävissä ottaa huomioon. Lopputulosta verratessa tavoitteisiin projektin alussa korostui, kuinka lähtötilanne voi muuttua, mitä enemmän eri ominaisuuksia ja vaatimuksia ilmenee.

ASIASANAT:

Verkkosegmentointi, Aruba ClearPass, VLAN, Network Access Control, Klusteri

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor's degree programme in Information and Communications Technology

Spring 2020 | 33 pages

Patrik Svensberg

DESIGNING A ROLE-BASED NETWORK SEGMENTATION

In recent years, there has been a trend in the corporate world to shift resources to cloud services. Nowadays, cloud-hosted applications are superseding local solutions because they fail to provide software as a service nearly as conveniently. The objectives of the thesis were to map out and design a role-based network segmentation solution that would simplify routing in the network and at the same time move away from linear and common information security solutions and their implementations. A modern network access control solution was utilized for role-based network segmentation.

The thesis was approached by getting to know the technologies that would be used in the project and mapping out how the current arrangement has been implemented. These were then explored as to what would be the best method of achieving the desired goals and what would be their technical requirements. After all these things were clear, the planning of the project implementation started. After a few different plans, a final solution was reached that would be implemented.

In the final plan, two subnets will be created. One subnet will serve as the guest network and the other as the office network. The guest network will be modified to include non-compliant enterprise devices in addition to guest devices. This segmentation will be implemented using a role-based method, where user rights can be defined to what they have rights to.

The planning of the thesis gave a good idea of what different things should be considered in similar tasks. When comparing the final result with the objectives at the beginning of the project, you can see how the initial situation can change the more different features and requirements appear.

KEYWORDS:

Network segmentation, Aruba ClearPass, VLAN, Network Access Control, Cluster

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET

AAA	Authentication, Authorization and Accounting protokollalla voidaan määritellä eri laitteiden ja käyttäjien pääsyä verkkoon.
AD	Active Directory on hallinnointialusta, joka autentikoi ja valtuuttaa käyttäjiä ja laitteita.
BYOD	Bring your own device on operaatiomalli, jossa esimerkiksi työntekijät käyttävät työtehtävissään omia tietokoneita yrityksen verkossa.
COA	Change of Authorization mahdollistaa AAA attribuuttien muutoksen session pystyttämisen jälkeen. [8]
CPPM	ClearPass Policy Manager hallinnoi konfiguraatioon liittyvät operaatiot ja vastaa käyttöoikeuspolitiikan täytäntöönpanosta.
DMZ	DMZ (ts. demilitarized zone) on aliverkko, joka yhdistää kontrolloidun sisäverkon isompaan ei-kontrolloituun verkkoon.
EAP	Extensible Authentication Protocol on tunnistusprotokolla, jota käytetään Asiakkaan ja Autentikaattorin välisessä autentikaatiotiedon siirrossa.
EOS/EOL	End of Support/Life tarkoittaa yleensä laitetta tai palvelua, joka ei ole enää tuettu.
HTTP	Hypertext Transfer Protocol, eli hypertekstin siirtoprotokolla, on protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon. [16]
IAM	Identity and Access Management on käyttöoikeushallintaa, joka esiintyy erilaisina menetelminä.
IDS	Intrusion Detection System pyrkii huomaamaan luvattoman toiminnan verkon reuna-alueilla.

IP	Internet Protocol (osoite), joka on määrätty laitteelle verkossa.
IPS	Intrusion Prevention System pyrkii huomaamaan ja estämään luvattoman toiminnan verkossa.
LAN	Local Area Network eli lähiverkko.
MAC	MAC-osoite on fyysinen tunniste laitteilla, jotka toimivat verkossa.
MDM	Mobile Device Management tarkoittaa erilaisten mobiililaitteiden etähallinnointia.
MSCHAPV2	Microsoftin versio Challenge-Handshake Authentication Protocol (CHAP) protokollasta, joka autentikoi käyttäjän tai laitteen autentikoivaan kokonaisuuteen. [18]
NAC	Network Access Control, eli verkon käyttöoikeuksien hallinta, suojaa verkon käyttötasoa luvattomilta laitteilta.
PEAP	Protected EAP eli suojattu EAP tunnistusprotokolla.
RADIUS	Remote Authentication Dial-In User Service, on AAA protokolla, joka määrittelee verkko-oikeuksia.
SSID	Service Set ID, joka toimii verkkotunnistautumisessa laitteen nimenä.
SSO	Single Sign-On on autentikoimistapa, jossa pyritään luomaan varmennus yhdellä tunnistautumisella niin, että ei tarvitse kirjautua useaan kertaan.
TLS	Transport Layer Security on salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne. [17]
TTLS	Tunneled Transport Layer Security eli tunneloitu TLS protokolla.
VPN	Virtual Private Network on erillinen virtuaaliverkko, joka on luotu päätelaitteen ja palvelimen välille julkisen verkon yli,

	muodostaen näennäisesti yksityisen verkon ja samalla peittäen päätelaitteen IP-osoitteen.
VRRP	Virtual Routing Redundancy Protocol mahdollistaa jokaisen laitteen toimimisen oletusyhdyskäytävänä klusterissa.
VLAN	Virtual LAN tarkoittaa virtuaalista verkkoa eli aliverkkoa.

1 JOHDANTO

Viime vuosina yritysmaailmassa on muodostunut trendiksi siirtää resursseja pilvipalveluihin. Vielä muutama vuosi sitten tavanomaiset verkkomenetelmät toimivat sujuvasti erilaisten applikaatioiden ja palveluiden tarjoamisessa. Yritykset hallinnoivat pääsääntöisesti paikallisesti omia laitteitaan ja niissä operoivia ohjelmistoja. Nykyään kuitenkin pilvessä hallinnoidut applikaatiot ovat syrjäyttämässä paikalliset ratkaisut, koska paikalliset ratkaisut eivät onnistu tarjoamaan ohjelmistoja palveluina läheskään yhtä kätevästi. Tämän lisäksi työntekijöiden ei enää ole pakko työskennellä yritysten tiloissa, vaan työtehtäviä tehdään kotoa ja muualta etänä, joten käsiteltäessä suuria määriä dataa vaaditaan joustavia verkkoratkaisuja.

Tämän opinnäytetyön tarkoituksena on kartoittaa ja suunnitella rooliperustainen verkkosegmentointiratkaisu, jolla tullaan korvaamaan jo olemassa oleva ratkaisu. Tavoitteena on suunnitella ja esitellä ratkaisu, joka yksinkertaistaa reititystä verkossa, sekä siirtyä pois suoraviivaisista ja yleisistä tietoturva-alueista ja niiden toteutuksista. Opinnäytetyö on tehty yrityksessä osana työtehtäviä. Aihe valittiin, koska se pystyttiin toteuttamaan töiden ohella ja se liittyi vahvasti opintoihin. Aiheista, joita tullaan tässä opinnäytetyössä käsittelemään, on jo hieman aikaisempaa kokemusta ja sitä voidaan tässä hyödyntää.

Opinnäytetyön keskeisimmät kysymykset, jotka projektissa tulee vastaan ovat, missä mittakaavassa työ tullaan toteuttamaan, mitä ominaisuuksia halutaan implementoida ja mitä muutoksia nykyiseen toimintamalliin tarvitsee tehdä. Suunnitellessa modernia verkkoratkaisua toteutuksen mittakaavan määrittely on hyvin keskeinen. Mitä isommassa skaalassa projekti toteutetaan, sitä paremmassa asemassa verkkoympäristö on tulevaisuutta ajatellen. Uusia ominaisuuksia mietittäessä voidaan arvioida, mitä tullaan mahdollisesti tarvitsemaan, ja tämä tukee vahvasti nykyisen toimintamallin muutosten hahmottamista.

Opinnäytetyössä käsitellään, miten yritysten sisäverkkojen tietoturvaa toteutetaan, ja toteutuksesta perehdytään verkon käyttöoikeuksien hallintaan. Opinnäytetyössä listataan keskeisimmät asiat verkon käyttöoikeuksien hallinnasta, jotka antavat taustaa ja käsitystä, mitä projektissa tullaan tekemään. Lopuksi käsitellään itse projektin etenemistä ja asioita, joita sen suunnittelussa ilmenee.

Opinnäytetyön toimeksiantajan nimi on jätetty pois työstä luottamussyistä. Työssä on myös viitattu lähteisiin, jotka ovat luottamuksellisia. Tiedot näistä lähteistä on kuitenkin muokattu suojaamaan kaikkien tahojen yksityisyyttä ja salassapitoa.

2 TIETOTURVA YRITYSVERKOISSA

Yritykset käyttävät erilaisia kanavia ja verkkoja datan kuljettamiseen ja tallentamiseen. Turvatakseen omat etunsa yritykset voivat implementoida erilaisia tietoturvaratkaisuja. Yleisimpiä tietoturvaratkaisuja verkoissa ovat palomuurit, VPN (Virtual Private Network) sekä IPS (Intrusion Prevention System), että IDS (Intrusion Detection System). Nämä menetelmät suojaavat pääasiassa verkkoja ulkopuolisilta haitoilta. Jotta yritykset voivat suojata omia etujaan sisäisesti niin, ettei luottamuksellinen informaatio ole saatavilla tahoille, joilla ei ole oikeita turvaluokituksia, niin voidaan ottaa käyttöön IAM eli Identity and Access Management. IAM:n avulla lisätään datan ja yksityisyyden turvaa.

Käyttöoikeushallinta on osa IAM:ää ja se suojaa informaation ja datan luottamuksellisuutta, eheyttä ja saatavuutta. Käyttöoikeushallinnat voivat olla joko hallinnollisia, teknisiä tai fyysisiä. Käyttöoikeushallinta, joka estää laitteiden pääsyn verkkoon tai johonkin verkon alueeseen, kutsutaan ehkäiseväksi hallinnaksi. Tällaisessa menetelmässä käytetään verkkoliityntäohjainta ja se on osa teknistä käyttöoikeushallintaa. Tekniset käyttöoikeushallinnat ovat joko fyysisiä laitteita tai ohjelmistoperäisiä. Seuraavassa kappaleessa kerrotaan, mitä tällaiset verkkoliityntäohjaimet ovat ja mitä ne sisältävät.

3 NETWORK ACCESS CONTROL

Network Access Control, jatkossa NAC, eli verkon käyttöoikeuksien hallinta, on ratkaisu, jonka tarkoitus on suojata verkon käyttötasoa luvattomilta laitteilta. Turvallisuus saavutetaan käyttämällä verkkoonpääsykytkimiä, langatonta verkkoinfrastruktuuria ja käyttöoikeuspalvelinta. Tällä tavalla NAC vahvistaa käyttöoikeuksien hallintaa verkon reunoilla.

Vanhoilla NAC-ratkaisulla ei joko ollut verkon käyttöoikeuksien hallintaratkaisua tai sitten niillä oli kyllä-ei -toimintaperiaate, joka rakentui yhden kriteerin varaan, kuten esimerkiksi, että päätelaitteella on yrityksen sertifikaatti.

Modernit NAC-ratkaisut käyttävät roolipohjaista politiikkaa saavuttaakseen dynaamisen segmentoinnin. Tämä tarkoittaa, että päätelaitteet tunnistetaan karkeammin ja niiden käyttöoikeudet voidaan määrätä aivan verkon reunalla riippuen laitteen tai käyttäjän roolista. Esimerkiksi henkilöstöhallinnon työntekijän PC:llä on erilaiset pääsyoikeudet verkossa kuin talouspuolen työntekijän PC:llä ja näillä molemmilla on erilainen pääsy verkkoon kuin tulostimilla. Modernit-NAC ratkaisut tarjoavat myös tiedon keruuta verkosta, jota voidaan käyttää tilastoihin, kapasiteetin suunnitteluun ja tapausten tutkimiseen.

3.1 Standardit ja protokollat

Nykypäivän verkot rakentuvat erilaisten standardien ja protokollien ympärille. Seuraavaksi listatut standardit ja protokollat ovat keskeisimpiä elementtejä Network Access Controllissa.

3.1.1 802.1X

802.1X on porttikohtainen todennusmenetelmä, jota käytetään lokaaleissa 802.3 lähiverkoissa ja langattomissa 802.11 verkoissa. 802.1X koostuu kolmesta kokonaisuudesta. Asiakas (engl. supplicant) eli päätelaite, kuten esimerkiksi kannettava tietokone, autentikaattori (engl. authenticator) ja AAA-palvelin, joka vastaanottaa ja vastaa verkko-oikeuspyyntöihin. [1, 2]

3.1.2 EAP

EAP (Extensible Authentication Protocol) on käyttäjientunnistusprotokolla, joka tukee useita tunnistusmenetelmiä ja on laajasti käytetty. EAP toimii osana 802.1X-toimintaympäristöä eikä vaadi Internet Protokollaa (IP). EAP-metodeja on yli 40 ja niistä käytetyimpiä ovat EAP-TLS, PEAP, EAP-TTLS ja EAP-MSCHAPv2. [3, 4]

3.1.3 EAP-TLS

EAP-TLS (EAP Transport Layer Security) on standardi verkkoautentikoinnissa ja käyttää yhtenäistä autentikaatiota palvelimen ja työaseman kanssa. EAP-TLS on yksi suojatuimmista metodeista ja sitä suositaan verkkoautentikoinnissa. [4, 5]

3.1.4 RADIUS

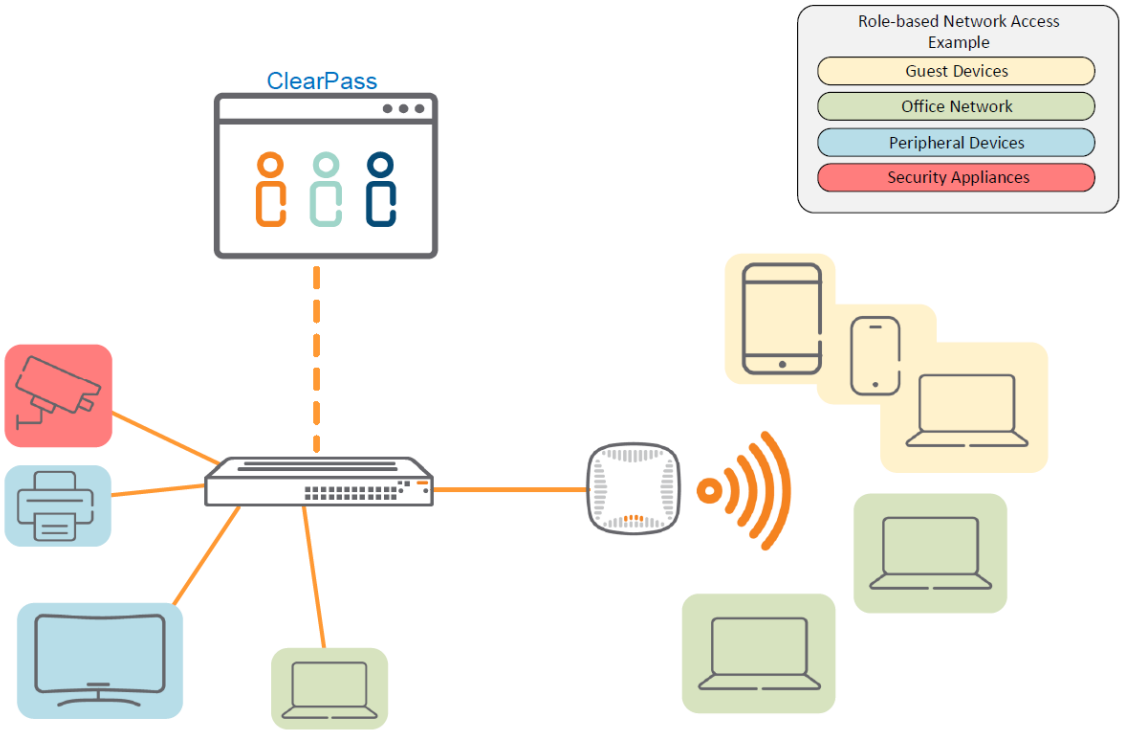
RADIUS (Remote Authentication Dial-In User Service) on AAA-protokolla, joka määrittelee verkko-oikeudet ja sitä käytetään erilaisten verkkolaitteiden väliseen kommunikaatioon. [6, 7]

3.1.5 RADIUS CoA

CoA (Change of Authorization) mahdollistaa AAA-attribuuttien muuttumisen session pystyttämisen jälkeen. CoA käytetään dynaamisesti autentikointiattribuuttien muuttamiseen sen jälkeen, kun RADIUS access-accept viesti on vastaanotettu. Tätä ominaisuutta voi verrata kytkinportin sulkemiseen tai avaamiseen. [8]

3.2 Rooliperustainen käyttöoikeus

NAC mahdollistaa useiden yhteyksien kategorioimisen. Network Access Controllerissa voidaan asettaa erilaisia attribuutteja, jotka määräävät, miten yhteyksiä avataan ja suljetaan. Vanhat NAC-menetelmät käyttävät näiden yhteyksien määrittämiseksi jonkinlaista Network Access Server palvelinta, joka toimii samalla verkkokäytäntöpalvelimena. Seuraava kuva (Kuva 1) havainnollistaa, miten rooliperustainen käyttöoikeus toteutuu.



Kuva 1. Rooliperustainen käyttöoikeus.

Kuten kuvasta 1 näkee, niin NAC mahdollistaa useiden eri laitteiden pääsyn verkkoon. NAC:hen määritellyt verkkoonpääsyroolit luokittelevat laitteet omiin aliverkkoihinsa. Ei ole väliä, onko laiteella langallinen tai langaton yhteys, jotta laite voidaan asettaa tiettyyn aliverkkoon. Aliverkoille voidaan määritellä erilaisia oikeuksia eri yhteyksille. Esimerkiksi turvallisuuslaitteille, kuten valvontakameroille ja kulunvalvonta laitteille voidaan määritellä oma aliverkko, johon voidaan esimerkiksi estää pääsy Internetistä. Aliverkkoon, johon kuuluu esimerkiksi tulostimet, voidaan antaa oikeus siten, että vain toimistotietokoneet voivat ottaa niihin yhteyden. Kuvassa 1 Aruba ClearPass toimii verkkoliityntäohjaimena, joka kategorisoi sisään tulevat yhteydet omiin erillisiin aliverkkoihinsa.

3.3 Captive Portal -tunnistautuminen

Captive portal pysäyttää HTTP pyynnöt verkkosivuille ja ohjaa käyttäjän rekisteröintisivulle. Käyttäjille voidaan antaa ohjeet, miten päätelaite tulee päivittää, jotta pääsy verkkoon voidaan antaa. Captive portal voidaan myös toteuttaa julkisissa vierasverkoissa niin, että käyttäjille annetaan väliaikaiset tunnukset, joita voidaan käyttää. [14]

3.4 Next Generation NAC -ratkaisut

Next Generation Network -ratkaisulla siirretään paikallisesti isännöityjä palveluita ja sovelluksia pilveen. Next Generation Network -ratkaisuihin kuuluvat esimerkiksi pilvessä hallitut palomuurit, käyttäjätietokannat ja verkon käyttöoikeuksien hallintapalvelut. Next Generation NAC -ratkaisut (NG-NAC) ovat tällaisia verkon käyttöoikeuksien hallintamenetelmiä, jotka ovat yleensä pilvessä isännöityjä tai toimivat ohjelmistona, joka on hankittu palveluna. Näillä ratkaisuilla voidaan vähentämään verkkoympäristöjen monimutkaisuutta, koska NG-NAC lisää keskitettyä käytönhallintaa, helppoa skaalattavuutta, verkkokuormituksen tasoittamista, sekä korkeaa suorituskykyä että saavutettavuutta. NG-NAC:llä voidaan selventää VLANien jäsentelyä, joka helpottaa uusien laitteiden käyttöönottoa. NG-NAC:n avulla voidaan kerätä enemmän tietoa, kuin vanhoissa ratkaisuissa, ja tämä lisää näkyvyyttä verkon käyttötasolle. NG-NAC -ratkaisuilla tuetaan myös kasvavaa BYOD mallia, joka on yleistymässä yhä enemmän.

4 ARUBA CLEARPASS

Aruba on kehittänyt oman Next Generation NAC -ratkaisun. Aruba ClearPass on hallinnointialusta, jolla voidaan toteuttaa dynaamista rooliperustaisen käyttöoikeuksien hallintaa ilman, että laitteisiin tarvitsee asentaa erillistä agenttia. ClearPass vahvistaa tietoturvaa ja sen avulla voidaan reakoida tietoturvarikkomuksiin sujuvammin, kuin vanhemmissa teknologioissa. Tämä toteutuu langallisissa ja langattomissa verkoissa. ClearPass mahdollistaa henkilökohtaisten ja yrityslaitteiden yhdistämisen verkkoon, joko kokonaisilla tai rajoitetuilla oikeuksilla ilman, että rikotaan yrityksen tietoturvapolitiikkaa. ClearPassin avulla pystyy tunnistamaan, mitkä laitteet ovat käytössä, kuinka moni laite on kytketty verkkoon ja mistä ne yhdistyvät. Näiden avulla saadaan laaja näkyvyys verkon jokaiseen toimintaan. ClearPass pystyy selvittämään laitteista:

- Tyypin ja mallin nimen
- MAC-osoiteen
- IP-osoiteen
- NIC-toimittajan (Network Interface Card)
- Käyttöjärjestelmän ja versionumeron
- VLANin, jossa laite toimii

[9, 10]

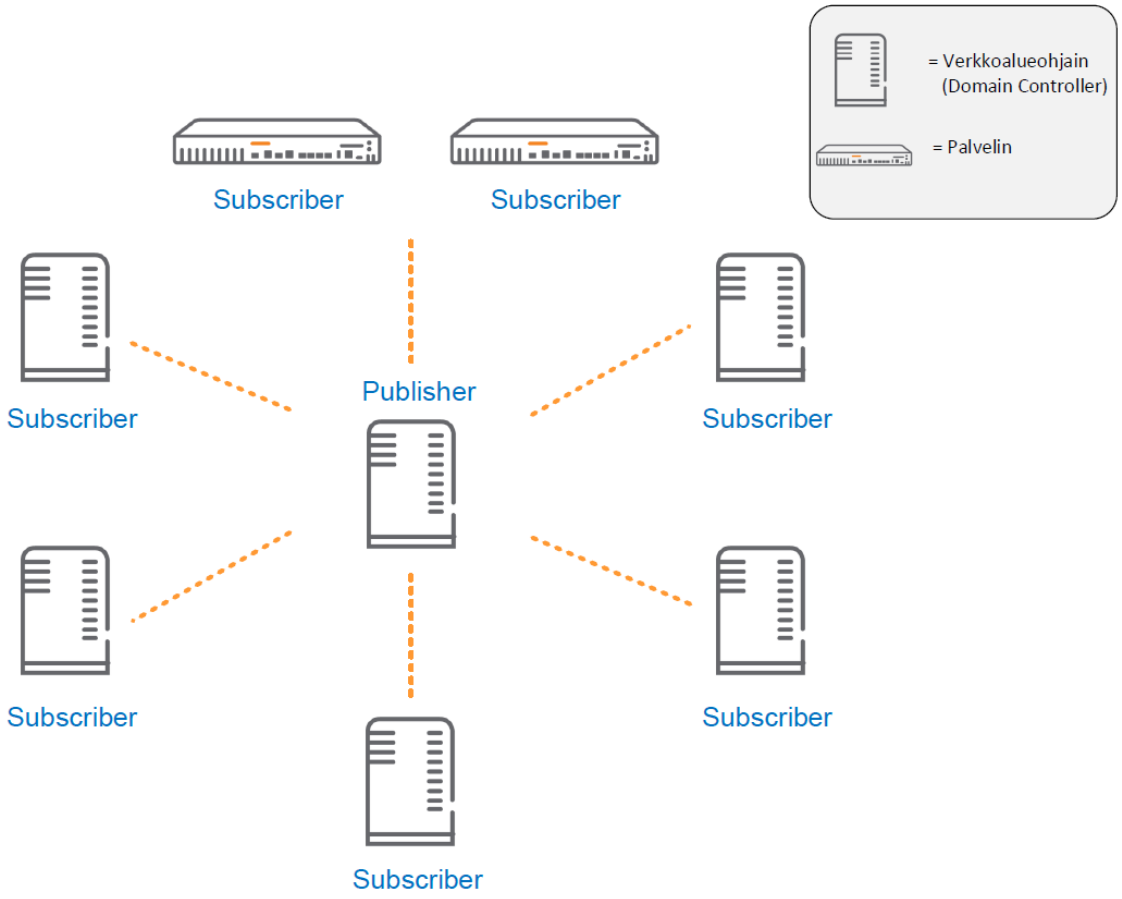
4.1 Klusteriarkkitehtuuri

Klusteri on joukko toisiinsa yhdistettyjä tietokoneita, jotka toimivat yhdessä monessa asiassa niin, että niitä voisi ajatella yhtenä laitteena. Klusterissa jokaiselle noodille on määrätty sama tehtävä, joka on ohjelmiston määrittelemä. Klusteri mahdollistaa jaetut konfiguraatiot ja tietokannat. ClearPass tukee klusteritoteutuksia ja ne voidaan toteuttaa laitteistotasolla sekä virtuaalisena. [12]

4.1.1 Publisher – Subscriber -malli

Publisher – Subscriber mallissa publisher-noodi toimii klusterin ohjaajana. Yleensä publisher-noodi vastaa muiden noodien konfiguraatioista, monitoroinnista sekä tietokantojen

replikoinnista. Publisher-noodi vastaa kaikkien tietokantojen hallinnoinnista. Publisher-noodeja voi olla vain yksi klusterissa, kun taas subscriber-noodeja voi olla määräämätön lukumäärä. Kaikki konfiguraatiot tehdään publisher-noodissa, joka sitten jakaa ne muille noodeille. Subscriber-noodit hoitavat kaikki raskaimmat työt. Kaikki AAA-tapahtumat ja RADIUS-pyynnöt ovat subscriber-noodien vastuulla. Subscriber-noodit säilyttävät paikallisen kopion konfiguraatio tietokannasta, mutta eivät pysty muokkaamaan sitä. Seuraava kuva havainnollistaa, miltä kyseinen malli näyttäisi korkealla tasolla. [11]



Kuva 2. Publisher - Subsciber -malli klusterissa.

Suurissa yrityksissä tämä on tavoiteltava malli, koska se lisää operatiivista toimintakykyä parantamalla tietoturvaa ja tietoliikenteen jatkuvuutta. Jokaiselle laitteelle kannattaa myös konfiguroida toinen laite, joka toimii varalaitteena, mikäli päälaite lopettaa toimintansa.

4.1.2 ClearPass-tietokannat

ClearPass-tietokantoihin kuuluvat konfiguraatio-, loki- ja Insight-tietokannat. Konfiguraatio-tietokannassa säilytetään lähes kaikki muokattavat ominaisuudet. Näihin kuuluvat esimerkiksi käyttäjätunnukset, roolimääritelmät, verkkolaitteet ja verkkosääntöjen profiilit. Lokitietokannassa säilytetään lokit järjestelmän käytöstä ja operaatioista. ClearPass Insight on tiedon keruu ja raportointi työkalu. Insightin avulla voi tarkastella kaavioita eri prosesseista ja luoda raportteja erilaisiin tarpeisiin. Insight-tietokanta säilyttää tiedot kaikista merkittävistä verkkotapahtumista.

Klusterissa tietokannat replikoidaan niin, että vain muutettu tieto välitetään Subscribereille. Tiedot, joita välitetään eteenpäin, sisältävät esimerkiksi konfiguraatio muutoksiin liittyvät elementit, auditointidata ja laitekohtaiset identiteettitiedot. Tietoja, joita sen sijaan ei välitetä, sisältävät esimerkiksi autentikointitulokset, sessiolokit, järjestelmätapahtumat ja monitorointidata. [11]

4.1.3 ClearPass-alueet

ClearPass-alueet kontrolloivat informaation ja Multi-Master Cachen (MMC) replikoinnin klusterissa. MMC sisältää päätelaitteiden käyntiaikaan liittyvät tiedot. MMC replikoidaan kaikille noodeille, jotka kuuluvat samaan alueeseen. Ilman ClearPassin alueita verkkoliikenne kulkee Publisherin ja kaikkien Subscribereiden välillä, joka lisää kuormitusta verkossa. [11]

Käyntiaikaan liittyvät tiedot sisältävät tiedot kaikista liitettyjen laitteiden rooleista ja asemista. Myös yhteyksien tiedot sisältyvät edellä mainittuun käyntiaikatietoihin, mikäli päätelaitteilla on OnGuard käynnissä. ClearPass OnGuard on päätelaitteisiin asennettava agentti, joka arvioi, onko laitteen turvallisuus ja yhteensopivuus riittävät, jotta laite voidaan päästää yritysverkkoon. [13]

Käyntiaikaan liittyvät tiedot sisältävät myös tiedot laitteen autentikoinnista. Nämä sisältävät esimerkiksi tiedot sessiosta, kun Change of Authorization (CoA) tapahtuu ja missä Network Access Server ja Network Access Device palvelimessa päätelaitteet ovat yhdistettyinä.

4.1.4 Kuormituksen tasaus

ClearPassin toiminnoissa autentikaatio, tietokanta ja Insight-operaatiot ovat suurimpia verkon kuormittajia. Mitä enemmän verkossa tapahtuu kuormittumista, sen epävakaammaksi verkkoliikenne muuttuu. Tämä voi aiheuttaa hidasta verkkosivujen latautumista ja pahimmassa tapauksessa verkkoympäristön kaatumista.

Kuormitusta pystytään tasoittamaan eri tavoilla ja tehokkainta on etsiä ratkaisu, joka sopii parhaiten tasoitettavaan verkkoympäristöön. Pienissä ympäristöissä Publisher voi hoitaa kaikki operaatiot, kun taas isommissa on suositeltavaa, että Subscriberit suorittavat autentikoinnit ja Publisher hoitaa tietokantojen ylläpidon ja replikaation. Myös Insight-operaatiot ovat mahdollisia Publisherille. Suurimmissa ympäristöissä ainoana muutoksena on, että pitäisi olla kaksi erillistä Insight-laitetta. Yleisesti on myös suositeltavaa, että Publisherita on kaksi, joista toinen toimii varalla, mikäli pää Publisher lopettaa toimintansa.

Jos autentikointi tuottaa liikaa kuormitusta Subscriberille, niin silloin kannattaa hankkia isommat laitteet tai lisätä Subscribereiden määrää. Jos tietokanta- tai Insight-operaatioissa alkaa näkyä liiallista kuormitusta, niin silloin ainoana vaihtoehtona on hankkia isommat laitteet.

4.2 Applikaatiot

Tässä luvussa listataan muutama applikaatio, joita ClearPass tarjoaa. Näiden applikaatioiden avulla ClearPass mahdollistaa useiden eri ominaisuuksien hallinnoinnin.

4.2.1 ClearPass Policy Manager

ClearPass Policy Manager (CPPM) hallinnoi konfiguraatioon liittyvät operaatiot ja vastaa käyttöoikeuspolitiikan täytäntöönpanosta. Myös järjestelmäasetukset on hallinnoitu CPPM:ssä. [11]

4.2.2 ClearPass Guest

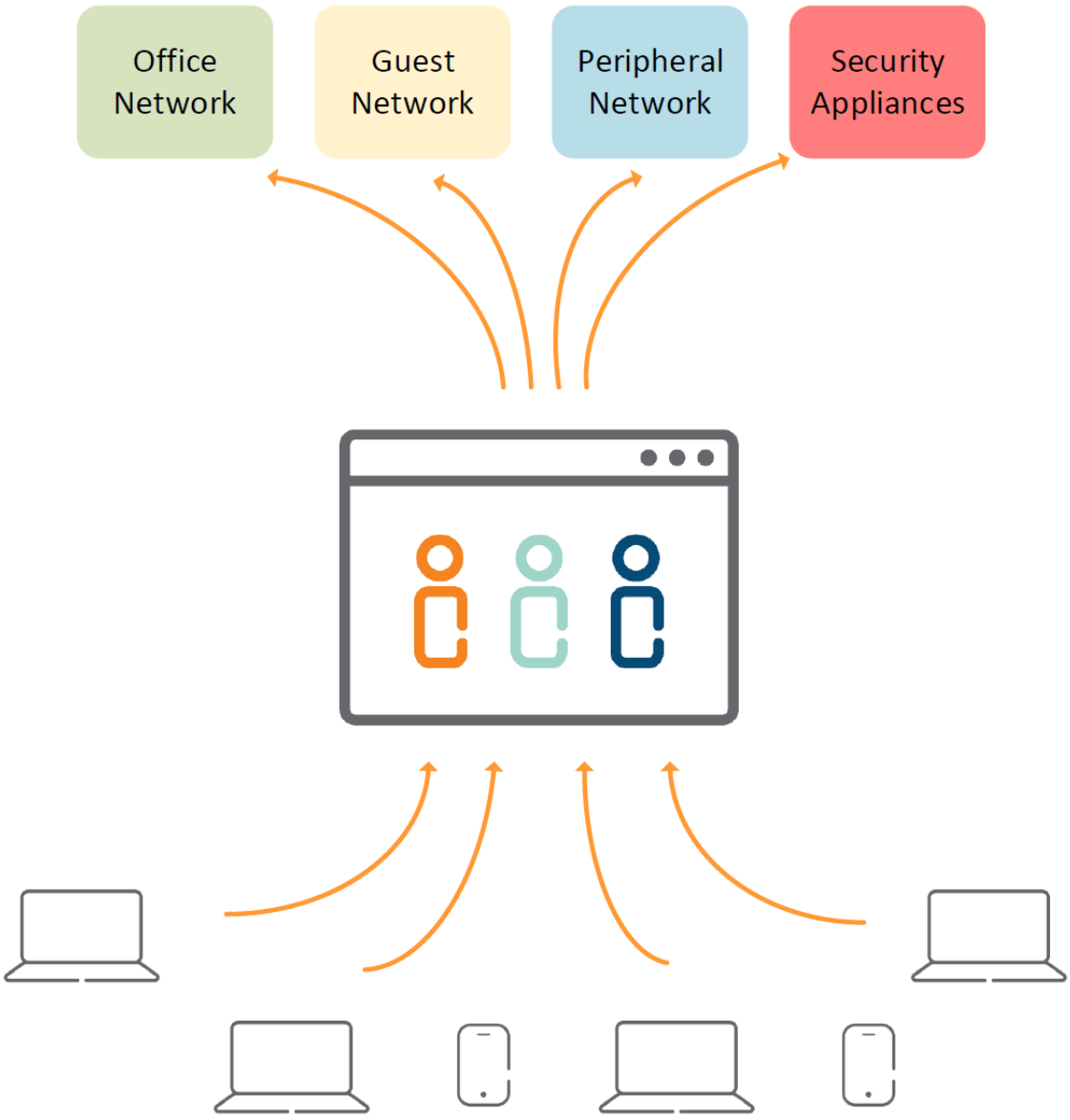
ClearPass Guest -applikaatio hallinnoi vieraskäyttäjät ja -laitteet, rekisteröintisivustot ja lomakkeet sekä käyttöoikeustasot. Guest-applikaatio hallitsee myös konfiguraatiot, jotka liittyvät ClearPass OnBoardiin. [11]

4.2.3 Insight

Insight on ClearPassiin rakennettu datan keruun ja raportoinnin työkalu. Sen avulla voi luoda erilaisia kuvioita, joista hahmottaa verkon suorituskyvyn ja kuormituksen. Insightin avulla voi myös asettaa erilaisia ilmoituksia ja tarkkailulistoja tietyille käyttäjille tai laitteille. [11]

4.3 Dynaaminen verkkosegmentointi

Aruba tarjoaa myös dynaamista verkkosegmentointia. Dynaaminen verkkosegmentointi yhdistää langalliset ja langattomat verkot yksinkertaisiksi kokonaisuuksiksi. Sen sijaan, että langallinen ja langaton toimistoverkko olisivat erillisiä, kuten esimerkiksi Toimisto LAN ja Toimisto WLAN, niin ne voidaan luokitella yhdeksi verkoksi. Aruban dynaaminen verkkosegmentointi myös mahdollistaa, että verkkoja koskevat säännöt ovat yhtenäisiä. Ainoa erotettava asia dynaamisessa verkkosegmentoinnissa on se, miten päätelaitteet ovat kytkeytyneet. Seuraava kuva (Kuva 3) havainnollistaa, miten verkkosegmentointi tapahtuu. [15]



Kuva 3. Dynaaminen verkkosegmentointi korkealla tasolla.

5 SUUNNITTELUVAIHE

Suunnitteluvaihe koostuu taustatietojen selvittämisestä, nykytilanteen hahmottamisesta ja tavoitteiden kartoittamisesta. Tässä luvussa esitetään myös, miten projekti eteni ja kuinka eri asiat muuttuivat.

5.1 Taustatiedot

Tarkoituksena on laajentaa usealle toimipisteelle seuraavan generaation verkko oikeuksien hallinnointiratkaisu. Tähän käytetään ClearPass-arkkitehtuuria, jossa toimii Publisher ja Backup Publisher. ClearPassin avulla voidaan toteuttaa myös dynaamista verkkosegmentointia. Tällä hetkellä vain yhdessä toimipisteessä on klusteritoteutus. Laajentamalla NG-NAC ratkaisua lisätään operatiivista toimintakykyä ja mahdollistetaan laajentuminen ja skaalattavuus tulevaisuudessa.

5.2 Nykyinen järjestely

Ennen kuin voi aloittaa työn suunnittelua, pitää olla ajantasainen tuntemus nykyisestä toimintamallista. Tämä helpottaa, kun varsinaisia tavoitteita aletaan listaamaan.

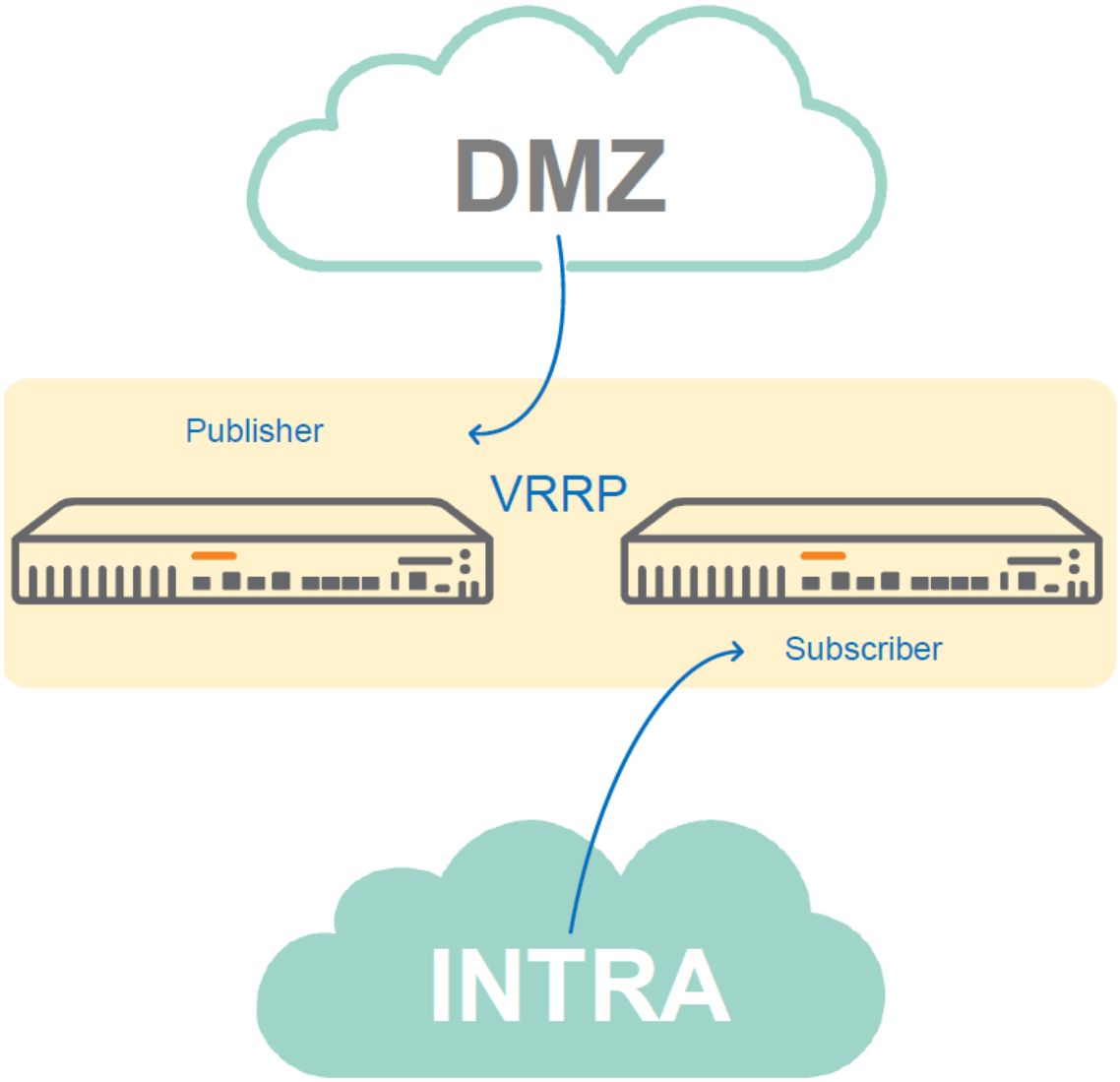
Nykyinen järjestely on hoidettu kahdella fyysisellä laitteella. Nämä laitteet muodostavat yhdessä pienitasoisen klusterin. Toinen laitteista toimii Publisherina ja toinen Subscriberina. Publisher hoitaa hallinnointitehtävät ja Subscriber hoitaa autentikoinnin. Nykyjärjestelyllä hallitaan langallisen verkon yhteydet ja langattoman verkon tuntemattomien SSID:iden yhteydet.

Langallisissa yhteyksissä käytettään 802.1X-todennusmenetelmää EAP-TLS kanssa, joka autentikoi RADIUS-palvelimelle, jossa varmuuskeinona käytetään MAC-autentikaatiota. ClearPass toimii tässä RADIUS-palvelimena.

Langattomissa yhteyksissä autentikointi riippuu laitteen SSID:stä. Varmennetut laitteet käyttävät 802.1X todennusmenetelmää EAP-TLS kanssa, joka autentikoi RADIUS-palvelimelle. Tässä sen sijaan Windows NPS toimii RADIUS-palvelimena. Tuntemattomat laitteet autentikoivat RADIUS-palvelimelle MAC-tunnisteella ja Captive Portalilla. Tässä

ClearPass toimii myös RADIUS-palvelimena. Kaikki muut SSID:t käyttävät WPA2-PSK tunnistautumista, jota hallinnoi Mobility Controller.

Jotta RADIUS toimii, niin päätelaitteiden pitää luottaa RADIUS-sertifikaattiin autentikointi palvelimella. Tulostimet ja muut oheislaitteet on konfiguroitu ohittamaan NAC. Seuraava kuva (Kuva 4) kuvaa nykyistä klusteria korkealta tasolta.



Kuva 4. Nykyinen klusteri. Muokattu viitteestä [19].

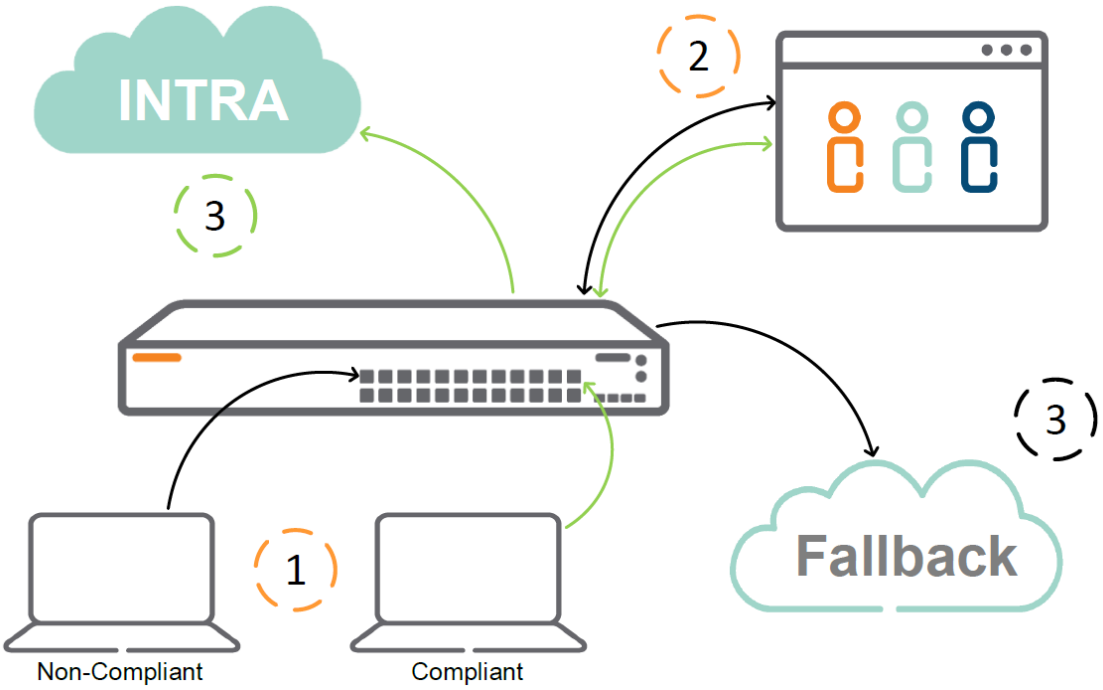
Kuten kuvasta 4 näkee, niin Subscriber vastaa sisäverkon autentikoinnista. Publisher toimii oletusyhdyskäytävänä (engl. default gateway) DMZ-aliverkkoon, mutta laitteiden välille klusterissa on konfiguroitu VRRP (Virtual Router Redundancy Protocol), joka mahdollistaa jokaisen laitteen toimimisen oletusyhdyskäytävänä. DMZ toimii erillisenä aliverkkona, joka yhdistää yritysverkon isompaan ei-kontrolloituun verkkoon, kuten esimerkiksi Internettiin.

5.3 Tavoitteet

Tavoitteiden kartoitus aloitetaan listaamalla toivotut ominaisuudet ja mitä niiden tulisi sisältää. Jatkossa käyttäjien päätelaitteiden tulisi autentikoida ClearPassilla. ClearPass hoitaa tarvittavat varmentamiset. Varmentamiseen voidaan käyttää ClearPassin tarjoamia ominaisuuksia tai MDM:ää (Mobile Device Management), joka hoitaa yhteensopivuustestit. Näitä varmennuskeinoja voi myös soveltaa toimimaan yhdessä. Windows-laitteet tulevat käyttämään laitesertifikaattia autentikoimiseen. Laitesertifikaattia käytetään autentikoitumiseen MDM:ssä, josta saadaan käyttäjäsertifikaatti, mikäli laitevaatimukset täytetään.

Uutena vaatimuksena tuli MacOS-laitteet ja jatkossa myös MacOS- sekä muille BYOD-laitteille pitää mahdollistaa tarvittaessa pääsy sisäverkon resursseihin. ClearPassin pitää pystyä antamaan erilaisia oikeuksia BYOD-laitteille, kuten esimerkiksi pääsy vain intraan. MacOS-laitteiden tulisi myös jatkossa kuulua työasemiin. MacOS-laitteiden varmennus voidaan hoitaa MDM:n avulla, jotta ne voidaan yhdistää AD:seen. AD:ta voidaan sitten käyttää apuna autentikoinnissa.

Jokaiselle toimipisteelle tulee kaksi verkkoa. Toimipisteillä tulee olla toimistoverkko ja toissijainen verkko. Toissijaisen verkon päätarkoitus on varmentaa uusia laitteita toimistoverkkoon. Seuraava kuva (Kuva 5) hahmottaa, kuinka tämä tapahtuisi. Eli yrityslaitteiden yhdistäessä verkkoon, joko langallisesti tai langattomasti, niin yhteys ohjataan ClearPassiin. ClearPass hoitaa tarvittavat tarkistukset ja mikäli laite täyttää vaatimukset, se ohjataan sisäverkkoon. Mikäli laitevaatimuksia ei täytetä, niin laite ohjataan toissijaiseen fallback-verkkoon.



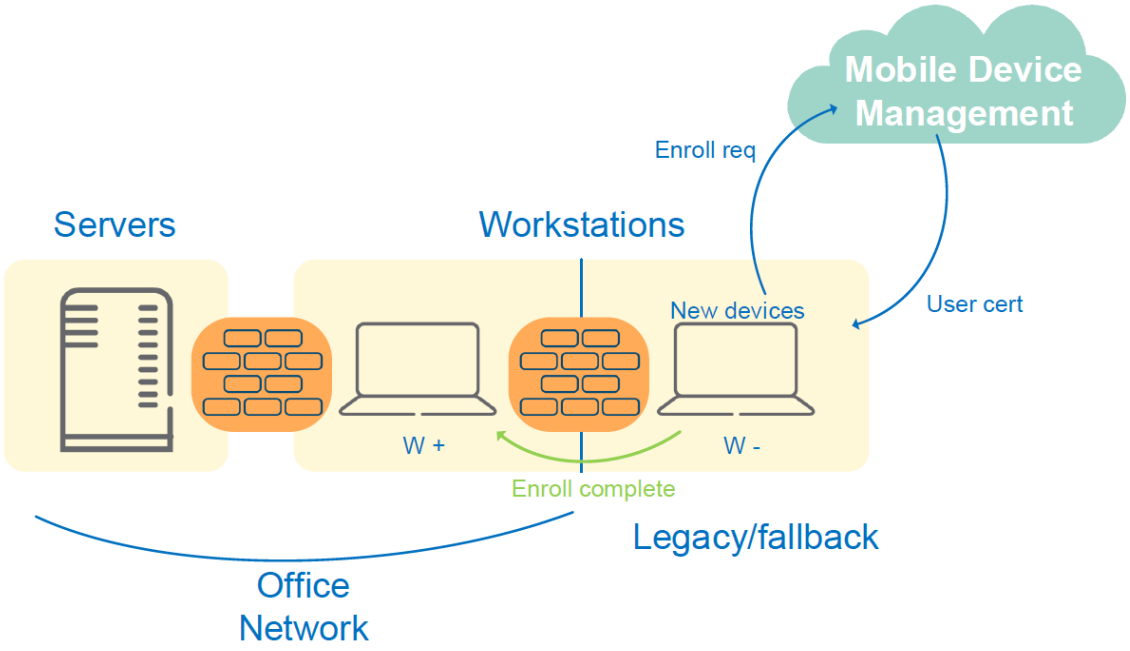
Kuva 5. ClearPass autentikaatioprosessi.

5.4 Projektin eteneminen

Tässä luvussa käsitellään projektin etenemistä. Projektia suunniteltaessa monia eri asioita tuli ilmi, jotka vaikuttivat eri määrin suunnitelman toteutukseen. Tarkoituksena on hahmottaa, millaisia asioita pitää huomioida vastaavaa toteutusta kartoittaessa ja millaisia ratkaisuja näihin voidaan tehdä. Projekti aloitettiin kartoittamalla tavoitteet ja sitä myöten tehtiin ensimmäinen luonnos.

5.4.1 Versio 1

Ensimmäinen versio pohjautui pitkälti tavoitteiden luomiin kriteereihin. Kaksi aliverkkoa tultaisiin luomaan, joista toinen toimisi pääsääntöisesti uusien laitteiden autentikointiin. Uusien laitteiden yhdistäessä verkkoon ne lähettäisivät laitesertifikaatin MDM:ään ja varmentuessa saisivat sieltä käyttäjäsertifikaatin. Kunnes koneessa on käyttäjä- ja laitesertifikaatti, se päästetään toimistoverkkoon. Tässä kohtaa ClearPassin tehtävä on tunnistaa varmennetut ja varmentamattomat yhteydet. Yhteyksien perusteella ClearPass kategorisoi yhteyden omaan aliverkkoon. Kuten seuraavasta kuvasta (Kuva 5) näkee, niin kaikki laitteet olisivat eri segmenteissään ja ne olisi suojattu palomuureilla.



Kuva 6. ClearPass konsepti korkealla tasolla.

Toimistoverkossa olisi täysi pääsy Internetiin ja sisäverkon resursseihin. Fallback verkko toimisi verkkona, josta on rajattu pääsy sisäverkon resursseihin, mutta vapaa pääsy Internettiin.

Tässä vaiheessa suunnitelmana on yhdistää MacOS-laitteet AD:seen ja varmentamisessa käytetään MDM:ää.

5.4.2 Versio 2

Kysymykset, jotka nousivat ensimmäisestä versiosta, olivat, voidaanko käyttäjäsertifikaattia käyttää vaihtoehtoisesti MacOS-laitteissa. Muita kysymyksiä olivat, miten fallback-verkko eroaa vierasverkosta ja mitkä ovat sen rajoitukset. Tietoturvan kannalta nousi myös kysymyksenä, mitä tarkastuksia ClearPass toteuttaa ja tarvitaanko ne myös fallback-verkossa. Tämän lisäksi jäi epävarmaksi, käytetäänkö ClearPassia VPN yhteyksien kanssa ja sovelletaanko ClearPassia laitteisiin, jotka ovat konfiguroitu ohittamaan NAC:n.

Edellä mainittuihin kysymyksiin vastattiin seuraavasti. Käyttäjäsertifikaattia voidaan käyttää vaihtoehtoisena ratkaisuna, mutta se ei ole suositeltavaa, koska se poistaa SSO mahdollisuuden. Fallback-verkko tultaisiin toteuttamaan vain langallisissa yhteyksissä,

kun taas vierasverkko toimii langattomassa verkossa. Fallback-verkosta olisi pääsy vain Internetiin, jotta laitteet voivat varmentua MDM:ssä. ClearPassin tulisi tarkistaa yhteensopivuus MDM:stä. MDM siis hoitaa tarkistukset, joihin kuuluu muun muassa virustorjunta, kryptaus ja palomuuriasetukset. ClearPassia ei tulla käyttämään VPN-yhteyksissä, ja ClearPassin tulee jatkossa kategorisoida laitteet, jotka ohittavat NAC:n, omaan aliverkkoon.

Tässä kohtaa projektia ilmeni myös uusi asia, joka piti huomioida. Jatkossa laitteet, joita käytetään erilaisiin kehitystarkoituksiin, tulisi päästä langalliseen verkkoon. Koska nämä kehityslaitteet eivät täytä kaikkia varmennuskriteerejä, niin ne toimivat vierasverkossa. Ratkaisuna näille laitteille tehtäisiin oma aliverkko (Dev NW).

MacOS-laitteiden kohdalla päätettiin, että niitä ei liitettäisi AD:seen, koska se tuottaisi liikaa haasteita. AD:seen liittäminen tuottaisi ongelmia muun muassa salasanojen vaihdossa ja kryptausavainten säilyttämisessä. Sen sijaan MacOS-laitteet varmennetaan MDM:ssä, joka toimii erillisenä AD:na ja joka pystyy hoitamaan tarvittavat tarkistukset. Tässä kohtaa MacOS-laitteet osittain putoavat projektista, koska ainoa asia niihin liittyen, mitä vaaditaan ClearPassilta on, että voiko se pyytää varmennustietoja MDM:stä.

5.4.3 Versio 3

Kolmannessa versiossa koitettiin vastata ongelmiin, joita tähän mennessä koottu suunnitelma sisälsi. Näitä ongelmia olivat esimerkiksi fallback-verkosta rajoittamaton pääsy Internettiin, fallbackin ja Dev NW:n luoma ylimääräinen VLAN-kuormitus ja miten tällaiset Dev NW -laitteet tultaisiin jatkossa varmentamaan tähän uuteen aliverkkoon.

Varmentamiseen ehdotettiin, että Dev NW -laitteisiin asennettaisiin joko ClearPass agentti, joka tekisi tarvittavat tarkistukset, tai että tällaisista laitteista otettaisiin MAC-osoitteet ja niiden avulla luotaisiin poikkeussäännöt verkkoon kirjautuessa. Projektin tarkoituksena oli kuitenkin yksinkertaistaa verkon toimintaa ja nämä ratkaisut eivät sitä tukeneet. MAC-osoitteita ei voida käyttää, koska jos laite on yhdistettynä telakkaan, niin niillä voi olla oma MAC-osoite. Näiden lisäksi muutama muu asia oli vielä epävarma, mutta niihin saatiin vastaukset, jotka löytyvät lopullisesta suunnitelmasta.

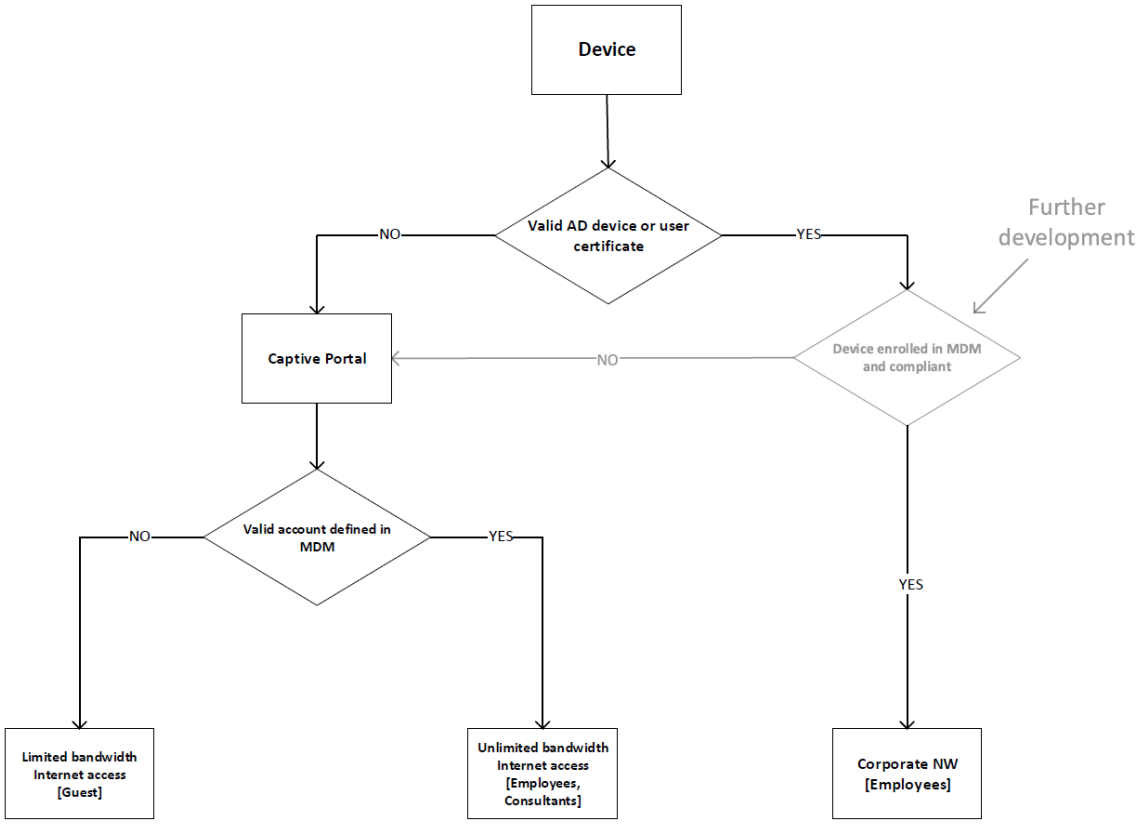
6 TOTEUTETTAVA SUUNNITELMA

Lopullinen suunnitelma jakautui kahteen osaan. Ensimmäinen osa on laajentaa nykyinen ClearPass-arkkitehtuuri kaikille toimipisteille. Toisena osana on yhdistää MDM ja ClearPass toisiinsa, jotta voidaan toteuttaa rooliperusteinen käyttöoikeusympäristö. Tässä luvussa määritellään lopullinen suunnitelma.

6.1 Suunnitelma

Viimeisessä versiossa VPN pidettiin erillään ClearPassista, päätelaitteet autentikoivat ClearPassin kautta ja ClearPass hallinnoi laitteet, jotka ovat määritelty ohittamaan verkon käyttöoikeuksien hallinnan. Windows-laitteet käyttävät laitesertifikaattia verkkoon yhdistäessä ja käyttäjäsertifikaattia käytetään toisena vaihtoehtona. MacOS-laitteita ei yhdistetä AD:seen, vaan ne varmentuvat MDM:än kautta.

Muutoksia lopulliseen versioon on luopuminen Dev NW -konseptista ja sen sijaan hyödynnetään captive portal:ia. Captive portal tukee parhaiten ei-varmennettujen laitteiden päästämistä verkkoon. Captive portal ratkaisulla voidaan ratkaista useita ongelmia ja ominaisuuksia. Sen sijaan, että luodaan useita eri aliverkkoja eri käyttäjätyypeille, niin oikeudet voidaan määritellä käyttäjäkohtaisesti. Lähtökohtaisesti on kaksi eri Internetyhteyttä, rajoittamaton työntekijöiden verkko ja rajoitettu vierasverkko. Tämä erottelu määritellään varmennusvaiheessa. Mikäli laite on varmennettu, niin se segmentoidaan yrityksen sisäverkkoon ja sillä on rajoittamaton pääsy Internettiin. Jos laite ei ole varmennettu, niin sille annetaan rajoitettu nopeus Internettiin, eikä pääsyä sisäverkon resursseihin. Seuraava kulkukaavio (Kuva 7) hahmottaa, miten segmentointi toimii.



Kuva 7. Verkkosegmentoinnin kulkukaavio.

Kuten kuvasta näkee, niin laitteen yhdistäessä verkkoon ClearPass tarkistaa, onko laite AD:ssa tai onko käyttäjäsertifikaatti voimassa. Mikäli joku näistä on kunnossa, niin laitteella pääsee sisäverkkoon. Muissa tapauksissa laite ohjataan captive portal:iin. Kun käyttäjä tunnistautuu captive portal:issa, tarkistetaan, onko käyttäjä määritelty MDM:ässä. Tämän tunnistautumisen perusteella käyttäjälle annetaan joko rajoittamaton tai rajoitettu Internettiin pääsy. Mikäli työntekijän päätelaite ei täyttäisi kaikkia vaatimuksia, niin se ohjautuisi captive portal:in kautta rajoittamattomaan verkkoon, joka toimisi fallback-verkkona. Laitteet voidaan sitten päivittää tässä verkossa, jotta ne voidaan taas yhdistää yrityksen sisäverkkoon.

Jatkossa aliverkkoja siis tulee olemaan kaksi. Toinen verkoista toimii vierasverkkona, joka sisältää myös ei-varmennettuja yrityslaitteita, ja toinen verkoista toimii yrityksen sisäverkkona, joka tulee jatkamaan normaalisti. Tässä kohtaa suunnitelma on pitkälti kartoitettu ja suurempia muutoksia ei ole tiedossa. Seuraavassa kappaleessa listataan vaatimuksia, joita projekti vaatii.

6.2 Vaatimukset

Tärkein vaatimus on laajentaa ClearPass-arkkitehtuuri jokaiselle toimipisteelle. Tämä vaatii uusia laitteita ja tietyiltä toimipisteiltä, joilla on jo joitain laitteita, pitää tarkistaa, ovatko ne enää tuettuja. Mikäli löytyy EOS- tai EOL-laitteita, niin ne pitää vaihtaa. Uudet laitteet vaativat lisenssejä, koska kyseessä on SaaS. Mahdollisten lisäpalveluiden tarve ClearPassissa pitää tarkistaa, mikäli laitteiden suorituskyky ei riitä.

Nykyinen vierasverkko pitää suunnitella uudelleen tukemaan useita eri käyttäjätyyppejä. Vierasverkko tullaan myös toteuttamaan langattomassa ja langallisissa yhteyksissä. Tämän mahdollistamiseksi, ClearPassin tulee jatkossa pystyä yhdistämään MDM:ään ja autentikoida käyttäjiä sen avulla.

6.3 Seuraava vaihe

Seuraava vaihe on aloittaa implementaatiovaiheen suunnittelu. Tämä sisältää erilaisten aspektien huomioimista ja arviointia. Ensin pitää luoda korkean tason toteutussuunnitelma, joka pohjautuu suunnitteluvaiheessa tulleisiin ratkaisuihin. Tämän perusteella luodaan lista kaikista laitteista ja lisensseistä, joita tullaan tarvitsemaan. Tästä listasta sitten luodaan kustannusselvitys. Implementaatiovaiheessa pitää myös kartoittaa, millaisia resursseja ajallisesti tullaan tarvitsemaan. Ennen kuin varsinainen implementointi voidaan aloittaa, niin tarvitaan myös testiajanjakso. Osa uusista asioista, joita tullaan implementoimaan, vaatii testaamista ennen kuin niitä voi toteuttaa tuotantoympäristössä.

6.4 Mahdolliset kehitysideat

Kuten kuvasta 7 näkee, niin tarvetta mahdolliselle kehitykselle kuitenkin jää. Projektin toteutuessa viimeisimmällä suunnitelmalla mahdollistaa, että yritysverkkoon pääsee joko AD:seen lisätyllä laitteella tai käyttäjäsertifikaatilla. Jatkossa voidaan kehittää lisävarmennus, jossa tarkistettaisiin, onko laite varmennettu MDM:ään. Mikäli ei, niin laite ohjattaisiin captive portal:iin. Toinen kehitysmahdollisuus olisi luoda yrityskoneille, jotka eivät ole varmennettu, ohjeet captive portalissa tai jossain muualla, miten kone saataisiin varmennettua, että se voidaan päästää yrityksen sisäverkkoon.

7 YHTEENVETO

Opinnäytetyön tavoitteena oli kartoittaa ja suunnitella rooliperustainen verkkosegmentointiratkaisu, joka olisi tarkoitus ottaa käyttöön jo olemassa olevassa toimintamallissa. Työ aloitettiin tutustumalla teknologioihin, joita projektissa käytettäisiin, ja kartoittamalla, miten nykyinen järjestely on toteutettu. Kun lähtötilanteesta oli selkeä kuva, alettiin listaamaan tavoiteltuja kehitysideoita. Näiden jälkeen tutkittiin, mikä olisi paras menetelmä toteuttaa halutut tavoitteet ja mitä ne tulisivat vaatimaan. Kun nämä asiat olivat selvillä, lähdettiin luomaan suunnitelmaa projektin toteutuksesta. Lopuksi laadittiin suunnitelma, joka ei vaatinut tarkentamista.

Työssä käsiteltiin, miten tietoturvaa toteutetaan yritysten sisäverkoissa, josta sitten syvennyttiin Network Access Controlliin ja tutustuttiin sen erilaisiin ominaisuuksiin sekä yleisimpiin standardeihin ja protokolliin. Tutustuttuihin ominaisuuksiin kuuluivat rooliperustainen käyttöoikeus ja captive portal, koska näitä hyödynnettiin työssä myöhemmin vastaan. Myös Next Generation NAC:sta mainittiin, koska ratkaisuna hyödynnettiin Aruba ClearPass. ClearPass on yksi suosituimmista moderneista verkon käyttöoikeuksien hallintaratkaisuista.

Projektin alussa toivottu tavoite oli myös aloittaa implementointi, mutta valitettavasti aika ei riittänyt siihen. Aikaansaatu suunnitelma valmistui kuitenkin ajallaan. Suunnitelman olisi voinut saada nopeamminkin kokoon, mutta uusien asioiden ilmetessä, sen valmistuminen venyi. Lopputulokseen oltiin kuitenkin tyytyväisiä, vaikka se muuttui hieman alkuperäisestä tavoitteesta. Tämä kuitenkin mahdollisti sen, että sai oppia paljon uusia asioita ja sai paremman käsityksen, miten projekteissa työskennellään.

Projektin edetessä implementaatiovaiheeseen ja siitä eteenpäin voi miettiä mahdollisia kehitysideoita, joita ei vielä suunnitteluvaiheessa otettu mukaan. Näihin kuuluvat esimerkiksi yrityslaitteiden varmennuksen vahvistaminen ja captive portalin kehittäminen.

LÄHTEET

[1] Wikipedia 2020. IEEE 802.1X. [Viitattu 16.3.2020] https://en.wikipedia.org/wiki/IEEE_802.1X

[2] IEEE 2020. IEEE Std 802.1X-2020. 802.1X: Port-Based Network Access Control. [Viitattu 16.3.2020] https://1.ieee802.org/security/802-1x/

[3] Wikipedia 2020. Extensible Authentication Protocol. [Viitattu 16.3.2020] https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

[4] IETF Tools 2004. Extensible Authentication Protocol (EAP). [Viitattu 16.3.2020] https://tools.ietf.org/html/rfc3748

[5] IEFT Tool 2008. The EAP-TLS Authentication Protocol. [Viitattu 16.3.2020] https://tools.ietf.org/html/rfc5216

[6] Wikipedia 2020. RADIUS. [Viitattu 16.3.2020] https://en.wikipedia.org/wiki/RADIUS

[7] IETF Tools 2000. Remote Authentication Dial In User Service. [Viitattu 16.3.2020] https://tools.ietf.org/html/rfc2865

[8] Cisco IOS Release 15SY 2019. Authentication, Authorization, and Accounting Configuration Guide, Chapter: RADIUS Change of Authorization. [Viitattu 16.3.2020] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html

[9] Aruba ClearPass 2020. Aruba ClearPass for Secure Network Access Control. [Viitattu 17.3.2020] https://www.arubanetworks.com/products/security/network-access-control/

[10] Kelser. Jonathan Stone. 2017. What is Aruba ClearPass and How Does it Protect Your Network? [Viitattu 17.3.2020] https://www.kelsercorp.com/blog/what-is-aruba-clearpass-and-how-does-it-protect-your-network

[11] ClearPass Deployment Guide 2016. Aruba ClearPass. Aruba. [Viitattu 17.3.2020] http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c05320375-1.pdf

[12] Wikipedia 2020. Computer cluster. [Viitattu 18.3.2020] https://en.wikipedia.org/wiki/Computer_cluster

[13] Aruba 2019. Data Sheet ClearPass OnGuard. [Viitattu 26.3.2020] https://www.arubanetworks.com/assets/ds/DS_ClearPass_OnGuard.pdf

[14] Wikipedia 2020. Network Access Control. Captive portals. [Viitattu 6.4.2020] https://en.wikipedia.org/wiki/Network_Access_Control

[15] Aruba 2019. Dynamic segmentation. [Viitattu 9.4.2020] https://www.arubanetworks.com/assets/so/SO_Dynamic-Segmentation.pdf

[16] Wikipedia 2019. HTTP. [Viitattu 17.4.2020] https://fi.wikipedia.org/wiki/HTTP

[17] Wikipedia 2019. TLS. [Viitattu 17.4.2020] https://fi.wikipedia.org/wiki/TLS

[18] Wikipedia 2020. Challenge-Handshake Authentication Protocol. [Viitattu 17.4.2020] https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol

[19] Luottamuksellinen toimeksiantajan dokumentti. N.d.