LAB University of Applied Sciences

Lähiverkot

Verkkotiedon hakeminen pääsynhallintajärjestelmän avulla

LAB-ammattikorkeakoulu
Insinööri (AMK)
2024
Janita Jyräs

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Janita Jyräs	Opinnäytetyö, AMK	2024
	Sivumäärä 36	

Työn nimi

Lähiverkot

Verkkotiedon hakeminen pääsynhallintajärjestelmän avulla

Tutkinto ja koulutusala

Insinööri (AMK), tieto- ja viestintätekniikan koulutus

Toimeksiantajaorganisaatio (jos opinnäytetyöllä on toimeksiantaja)

Yritys X

Tiivistelmä

Opinnäytetyön aiheena on laitteen paikkatiedon hakeminen pääsynhallintajärjestelmän avulla. Tavoite on rikastaa CMDB-tietokantaa integraation yli verkosta saatavien tietojen avulla reaaliajassa inventaarion ja vianselvityksen helpottamiseksi.

Lähiverkon topologioita on väylä-, rengas- ja tähtitopologiat. Lähiverkossa käytettävät aktiivilaitteet ovat kytkin, reititin, palomuuri, keskitin sekä toistin. Langaton lähiverkko voidaan rakentaa langattomien sisätukiasemien avulla. Yritysten tietoturva koostuu pääsynhallinnasta, palomuurisuodatuksesta, torjuntaohjelmista, fyysisistä suojauksista ja käyttäjäkoulutuksista.

Yritys X:llä on ennestään käytössä pääsynhallintajärjestelmä Clearpass, jonka toteutusta opinnäytetyö käsittelee. Kolmannen osapuolen vastuulla on CMDB:n ServiceNow'n toteutus ja ylläpito. Tavoitteena on laitteen liittyessä verkkoon, että API-ympäristössä toimiva Clearpass lähettää http:n POST-metodilla JSON-muotoisen viestin CMDB:lle. Viesti sisältää tiedon päätelaitteen nimestä, kytkimen tai tukiaseman nimen sekä aikaleiman verkkoon liittymisestä.

Asiasanat

tietoverkko, lähiverkko, langaton verkko, autentikointi, pääsynhallinta

Abstract

Author(s)	Type of Publication	Published
Janita Jyräs	Thesis, UAS	2024
	Number of Pages 36	

Title of Publication

Local area network

Retrieving device information from network by using access management system

Degree, Field of Study

Engineer (UAS), Information and communication technology

Organisation of the client (if the thesis work is commissioned by another party)

Company X

Abstract

The topic of the thesis is retrieving device location information by using access management system. The goal is to enrich the CMDB with real-time information obtained over the network to facilitate inventory and troubleshooting.

Local network topologies include bus, ring and star topologies. Devices that are used in local area network include switch, router, firewall, hub and repeater. A wireless network can be constructed using wireless access points. Companies' security consists of access management, firewall filtering, antivirus programs, physical protections and user training.

Company X already uses Clearpass as access management system. Thesis addresses implementation in Clearpass. The responsibility of the third party is the implementation and maintenance of CMDB in ServiceNow. The goal is that when a device connects to the network, Clearpass which operates in API environment, sends a JSON message to the CMDB using the http POST method. The message includes information about device name, switch or access point hostname and timestamp.

Keywords

network, local area network, wireless network, authentication, access management

Sisällys

SANASTO

1G, 2G, 3G, 4G, 5G = Ensimmäisen, toisen jne sukupolven matkapuhelinverkkostandardit.

Adhoc-verkko = verkko, joka muodostetaan väliaikaisesti laitteiden välille ilman aktiivilaitetta.

AP, Access Point = Langaton tukiasema, joka mahdollistaa verkkoon liittymisen langattomasti.

API = Sovellusten ohjelmointirajapinta, joka määrittelee ohjelmistojen komponenttien kommunikointitavan.

Broadcast = Verkkoliikenteen lähetystapa, jossa tieto lähetetään kaikille verkkolaitteille.

Bot, botti = Ohjelma tai skripti, joka toimii automaattisesti määritetyt toiminteet.

CI, Configuration Item = Laitekortti, joka sisältää tiedon kohteesta tai komponentista.

Client ID = Asiakastunniste, joka tunnistaa sovelluksen API-pyynnön yhteydessä.

Client Secret = Salausavain, joka varmistaa sovelluksen tunnistautumisen API-pyynnössä.

CMDB = Konfiguraatiohallinnan tietokanta, joka tallentaa organisaation IT-infrastruktuurin.

Duplex, half duplex, full duplex = Tiedonsiirron toimintatila, joka voi olla puoli- tai kaksisuuntainen laitteiden kyvykkyyden mukaan.

EAP, EAP-TLS, EAP-TTLS = Protokollat, jotka mahdollistavat langattoman verkon käyttäjien tunnistamisen ja autentikoinnin.

Endpoint = Päätelaite, joka muodostaa yhteyden verkkoon.

Endpoint context server = Palvelin, joka tallentaa ja hallinnoi endpointien tilaa ja ominaisuuksia verkossa.

Enforcement policy = Säännöstö, joka määrittää laitteiden pääsyn verkkoon ja niiden valvonnan.

Enforcement profile = Profiili, joka määrittää pääsynhallintajärjestelmässä sovelluskohtaiset asetukset ja rajoitukset.

Ethernet = Verkkoteknologia, joka mahdollistaa tiedonsiirtoyhteyden muodostamisen.

GDPR = Euroopan Unionin tietosuoja-asetus, joka määrittää yksityishenkilöiden henkilötietojen käsittelyn säännöt.

http = Protokolla tietojen siirtämiseen verkkosivujen ja selainten välillä.

HUB = Verkkolaite, jonka tehtävä on jakaa tieto eteenpäin verkonlaitteiden välillä.

IEEE = Kansainvälinen järjestö, joka kehittää standardeja sähkö- ja elektroniikkateollisuudelle.

IETF = Kansainvälinen järjestö, joka kehittää ja ylläpitää Internetin teknisiä standardeja.

IoT, Internet of Things = Asioiden Internet, laitteiden ja esineiden verkosto, joka mahdollistaa niiden viestinnän ja tiedonkeruun.

IP = Verkkoprotokolla, jota käytetään tietojen siirtämiseen Internetissä ja muissa verkoissa.

JSON = JavaScriptiin perustuva tiedonvaihtoformaatti, jota käytetään web-sovellusten ja palvelimien väliseen tiedonsiirtoon.

MAC-osoite = Laitteen ainutlaatuinen tunniste verkkokerroksella.

MAN = Laajakaistainen kaupunkialueenkattava tietoverkko.

Multicast = Verkkoliikenteen lähetystapa, jossa tieto lähetetään samanaikaisesti useammalle vastaanottajalle.

LAN = Paikallinen verkko, joka kattaa rajatun alueen, kuten rakennuksen sisätilat.

OAuth 2.0 = Open Authorization -protokollan versio 2.0, joka mahdollistaa kolmannen osapuolen sovellusten pääsyn käyttäjän tietoihin ilman erillisen salasanan jakamista.

OSI-malli = Verkon esitysmalli, joka jakaa tietoliikenne protokollat seitsemään kerrokseen.

PEAP = Turvattu laajennettu autentikointiprotokolla verkon käyttäjien tunnistamiseen.

Peer to peer = Verkkotopologia, jossa päätelaitteet muodostavat suoran yhteyden toisiinsa ilman keskitintä.

Point to point = Verkkotopologia, jossa päätelaitteet muodostavat yhteyden toisiinsa välittäjän kautta.

POST = Http-metodi, jota käytetään tiedon lähettämiseen palvelimelle.

PSK = Esijaettu avain, jota käytetään salaukseen.

RADIUS = Protokolla, jota käytetään käyttäjien tunnistamiseen ja verkkopalveluiden pääsynhallintaan.

Rootkit = Haittaohjelma, joka antaa pääsyn tietokoneen käyttöjärjestelmään.

SSID, hidden SSID = Verkkonimi, jota käytetään verkon tunnistamiseen. Piilotettu SSID on verkko, joka ei ehdota nimeä avoimesti käyttäjille.

SSO = Kertakirjautumisen järjestelmä, joka mahdollistaa käyttäjän kirjautumisen useisiin sovelluksiin yhdellä tunnistautumisella.
SSL = Verkkoprotokolla, jota käytetään salattujen tietojen siirtämiseen.

TCP = Protokolla, jota käytetään tietojen siirtämiseen verkossa varmistaen niiden luotettavan toimituksen.

TCP/IP = Protokollaperhe, joka muodostaa perustan tietoliikenteelle.

TSL = Kuljetuskerroksen protokolla, jota käytetään salattujen tietojen siirtämiseen.

Token = Tunniste, joka osoittaa käyttäjän todennetun identiteetin.

UDP = Protokolla, jota käytetään tietojen siirtämiseen ilman yhteyden varmistamista.

URL = Verkko-osoite, joka viittaa tiettyyn resurssiin Internetissä.

VLAN = Virtuaalinen paikallinen verkko, joka mahdollistaa verkon jakamisen.

VPN = Virtuaalinen yksityisverkko, joka mahdollistaa turvallisen yhteyden julkisen verkon yli.

WAN = Laaja-alainen verkko, joka kattaa laajat maantieteelliset alueet.

WEP = Langattoman verkon salaustekniikka.

Wi-Fi = Langattoman lähiverkkoteknologian kauppanimi.

WLAN = Paikallinen verkko, johon käyttäjät voivat liittyä langattomasti.

WPA, WPA2 = Langattoman verkon suojausstandardit.

WPS = Standardi langattoman verkon laitteiden turvalliseen asentamiseen.

1 Johdanto

Tietoverkkojen kehitys viime vuosikymmenten aikana on ollut nopeatempoista. Nykypäivänä länsimaisessa yhteiskunnassa internet on lähes välttämättömyys. Valtion, kuntien ja virastojen, kuten esimerkiksi pankkien, palvelut ovat siirtyneet verkkoon. Verkossa käsitellään jokaisen yksilön kohdalla koko ajan henkilökohtaisempaa tietoa.

Kehittyvä tietotekniikka vaatii huomionsa myös lähiverkoissa. Valmistajat pyrkivät koko ajan vaivattomammin mukana kulkeviin laitteisiin ja näin ollen harvassa kannettavassa tietokoneessa on enää sisäänrakennettua paikkaa Ethernet-kaapelille. Lähiverkoissa räjähdysmäisesti lisääntynyt laitteiden määrä on osaltaan vaikuttanut langattoman verkon kehittymiseen nykyiseen muotoonsa.

Lähiverkoissa vain käyttäjien ja laitteiden määrän kasvu sekä laitteiden kehittyminen ei ole ainoa haaste toimivan sisäverkon rakentamisessa. Tietoturva täytyy huomioida verkossa, ja se vaatii jatkuvaa kehittymistä ja kouluttautumista myös käyttäjiltä. Verkon kautta on mahdollista päästä hyvinkin arkaluonteisiin tietoihin käsiksi. Tietoturvan kautta pyritäänkin estämään tietojen tahallinen sekä tahaton päätyminen henkilöille, joille tieto ei kuulu.

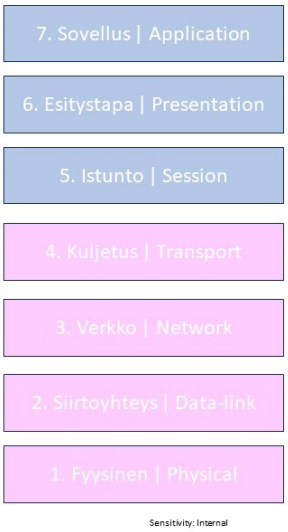
Tämä opinnäytetyö on toiminnallinen työ. Työssä tavoitteena on kuvata prosessi, jossa haetaan verkon avulla päätelaitteen paikkatieto hyödyntämällä lähiverkosta saatava tieto pääsynhallinnan avulla. Asiakkaalla on käytössään pääsynhallintajärjestelmä sekä olemassa oleva CMDB. Tässä työssä kuvataan prosessi pääsynhallinnan osuuden toteutuksesta, kun rakennetaan integraatio pääsynhallinnan ja CMDB:n välille.

Opinnäytetyön tietopohjassa käsitellään lähiverkon protokollia, rakennetta ja tietoturvaa. Alkuun käydään läpi verkon perusperiaatteita, eli OSI-mallia ja TCP/IP-protokollaa. Yleisimpien verkkotopologioiden jälkeen käsitellään lähiverkon aktiivilaitteita, sekä langattoman verkon tekniikkaa ja roolia lähiverkossa. Tietoturvaa käsitellään yleisellä tasolla. Tämän jälkeen tutustutaan toiminallisen työn järjestelmiin sekä itse työhön ja sen toteutukseen. Lopuksi käydään läpi yhteenveto.

2 Verkkoprotokollat

OSI-malli

OSI-malli tulee sanoista Open Systems Interconnection Reference Model, ja se on yksi merkittävimpiä tiedonsiirtoprotokollien yhdistelmistä. OSI-mallin alkuperäinen tarkoitus oli olla yleinen ja avoin standardi, jotta valmistajien laitteet ja ohjelmistot olisivat keskenään yhteensopivia valmistajasta riippumatta. Kilpailu valmistajien välillä on kuitenkin johtanut siihen, ettei tämä toteutunut juurikaan tuotannossa. OSI-malli vakiintui kuitenkin kuvaamaan tietoliikennejärjestelmien mukaista toimintaa. (Hakala & Vainio 2002, 126.) Kuviossa 1 näkyy OSI-malli, jossa ylemmät sovelluskerrokset on kuvattu sinisellä.



Kuvio 1. OSI-malli

OSI-mallissa on pidetty erillään palvelut, rajapinnat ja protokollat. Se on kerrosmalli, jossa alemmat kerrokset on piilotettu ylemmiltä kerroksilta. OSI-malli koostuu seitsemästä kerroksesta. Ylin kerroksista on sovelluskerros, jossa käyttäjälle näkyvät sovellukset ovat. Sovelluskerroksessa toimii muun muassa sähköposti sekä tiedostojen siirto. Tämän jälkeen on esitystapakerros, jossa tieto muutetaan käyttäjälle niin sanotusti luettavaan muotoon. Esitystapakerros siis kääntää sovelluksen datatiedon perusteella, salaa ja purkaa viestejä sekä suorittaa tiedon pakkaamisen kuljetuksen ajaksi. Istuntokerroksessa huolehditaan yhteydessä kulkevien istuntojen kanavoinnista. Käytännössä sen tehtävänä on avata, ylläpitää ja sulkea istunnot sekä synkronoida dataa lisäämällä tietovirtoihin tarkistuspisteitä. Kuljetuskerroksessa huolehditaan, että paketit kulkevat perille ja ne järjestetään oikeaan järjestykseen. Verkkokerros taas hoitaa globaalin reitityksen ja kohdekoneen löytymisen

internetistä. Siirtokerros hoitaa paikallisen lähiverkon liikennöinnin. Se tunnistaa vahingoittuneet sekä kadonneet kehykset, ja lähettää ne uudelleen. Lisäksi siirtokerros suorittaa kehystyksen, jonka tarkoituksena on jakaa verkkokerrokselta saatu data pienempiin yksiköihin ja päivittää kehysten otsikot lisäämällä otsikoihin lähettävien ja vastaanottavien päätelaitteiden MAC-osoitteet. Alimpana fyysinen kerros vastaa fyysisestä tekniikasta, synkronoi databitit, mahdollistaa moduloinnin eli signaalin muunnoksen ja määrittää tiedonsiirtonopeuden. Verkkotopologiat, eli verkon kytkennät toteutuvat fyysisessä kerroksessa, ja siinä määritetään lähetystilat, kuten esimerkiksi half duplex. OSI-mallia voidaan hyödyntää esimerkiksi vianselvityksessä rajaamalla vika tiettyyn verkkokerrokseen. (Kanade 2022.)

TCP/IP

OSI-malliin kerroksiin liittyy osaltaan TCP/IP-protokollaperhe. Verrattuna OSI-malliin, se toimii verkkokerroksesta ylöspäin. TCP/IP-protokollassa ei siis erotella tai määritellä fyysisiä kerroksia, vaan fyysiseltä kerrokselta odotetaan tiettyjä ominaisuuksia perustuen standardeihin. TCP/IP-protokollalla tarkoitetaan joukkoa protokollia, jotka rakentuvat Internet-protokollan ympärille. Siinä on viisi kerrosta: fyysinen kerros, linkkikerros, verkkokerros, kuljetuskerros ja sovelluskerros. Siirto- ja fyysistä kerrosta ei kuitenkaan ole juurikaan standardoitu IETF:n, eli Internet Engineerind Task Forcen toimesta. Useimmiten ne kuvataankin samantasoisina verkkokerroksen alla, sillä periaatteessa verkkotekniikalla ei IP-kerroksen alla ole väliä. (Kaario 2002, 21.)

TCP eli Transmissioin Control Protocol on protokolla, joka kuljettaa datapaketit verkossa ja varmistaa niiden perille pääsyn. Käytännössä se varmistaa yhteyden vastapäähän ennen kuin se lähettää datapaketteja kohteeseen. Jos vastausta ei vastaanottajalta saada, ei dataa lähetetä ollenkaan. IP eli Internet Protocol taas on tapa lähettää tietoja laitteiden välillä internetin yli. Jokaisella laitteella on verkossa yksilöllinen IP-osoite, jonka avulla laite on mahdollista tunnistaa ja näin ollen toteuttaa tiedonsiirto laitteiden välillä verkossa. IP on TCP/IP:n verkkokerroksen pääprotokolla. Sen tarkoitus on toimittaa datapaketit lähteistä kohteisiin erilaisten tunnisteiden, kuten osoitetietojen avulla. IP ja TCP eroavat toisistaan siten, että IP:n tehtävä on varmistaa tiedon kulku oikeaan osoitteeseen hakemalla ja määrittämällä IP-osoite. TCP vastaa tiedon siirtymisestä ja reitittymisestä verkon arkkitehtuurin läpi varmistaen, että tieto kulkee IP:n määrittämään kohteeseen. (Fortinet 2022.)

Kuljetuskerros hyödyntää joko TCP tai UDP protokollaa. TCP-protokollan tehtävä on huolehtia osapuolten keskustelusta, jolloin virheen todennäköisyys pienenee. UDP-protokollan erona on, ettei se tarvitse varmistusta vastapuolelta, että sitä kuunnellaan. UDP yksinkertaistettuna on valmis vastaanottamaan dataan tai lähettämään sitä saamatta varmistusta siitä, että lähetetty data on päässyt perille asti. Vaikka UDP on epäluotettava ja

yksinkertainen, on muistettava myös sen hyödyt. UDP:ta käytetäänkin monissa tarkoituksissa, joissa viestin katoaminen matkalla ei haittaa, koska UDP säästää verkon kapasiteettia. Broadcast- ja multicast-lähetyksissä TCP:n käyttö ei ole mahdollista TCP:n perustuessa kahden prosessin loogiseen yhteyteen, jolloin saman viestin lähetys useisiin osoitteisiin ei ole vaihtoehto. (Kaario 2002, 21.)

3 Lähiverkko

3.1 Lähiverkko eli LAN ja verkkotopologiat

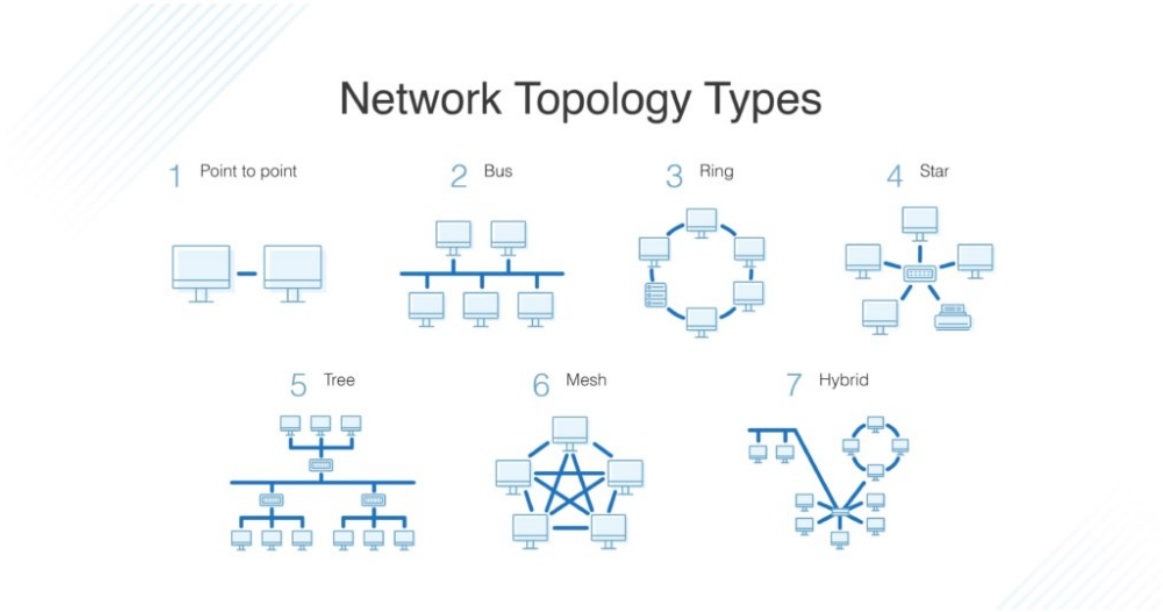
3.1.1 LAN

Lähiverkon lyhenne LAN tulee sanoista local area network. Se toimii maantieteellisesti rajoitetulla alueella. Rajattu alue on usein rakennus tai rakennusryhmä, esimerkiksi yrityksen toimistorakennus. Lähiverkon hallinta ja ylläpito on sen omistavalla taholla. Lähiverkosta puhuttaessa voidaan törmätä myös lyhenteisiin WAN (wide area network), joka tyypillisesti ulottuu ero paikkakuntien tai maiden välille. MAN (metropolitan area network) tarkoittaa kampusalue-, taajama- tai kaupunkiverkkoa. (Paananen 2005, 218.)

Lähiverkon koko vaihtelee riippuen sisäverkonlaitteista. Sisäverkosta puhuttaessa tarkoitetaan kaikkia sisäverkon komponentteja kytkimistä kaapeleihin. Yleisimmin lähiverkkoja on kahdenlaisia, palvelin lähiverkkoja ja niin sanottuja peer to peer -lähiverkkoja. Palvelinverkoissa käyttäjät liittyvät yhteiseen sisäverkon palvelimeen, johon määritetään verkonkäyttäjien pääsy ohjelmistoihin ja tietokantoihin. Palvelinlähiverkko on tyypillisin lähiverkkoratkaisu keskikokoisissa ja suuremmissa lähiverkkoratkaisuissa. Peer to peer -lähiverkko ei tarvitse keskitettyä palvelinta, ja sitä käytetäänkin pienissä lähiverkkoratkaisuissa heikon kuormansietokyvyn takia. Lähiverkkojen kehitys alkoi 1960-luvulla, kun oppilaitoksille ja yrityksille syntyi tarve saada yhteys toimipisteiden päätelaitteiden välille. (Cisco.)

3.1.2 Topologiat

Verkkotopologia tarkoittaa tapaa, jolla tietoverkko on rakennettu. Perusrakenteita lähiverkon rakentamisessa ovat väylä, rengas ja tähti -topologiat. Nimeäminen perustuu joko verkon fyysiseen rakenteeseen tai signaalin kulkuun. Perustopologioiden muunnoksia ja yhdistelmiä kutsutaan hybridirakenteiksi, tähtiverkkojen yhdistelmillä on kuitenkin vakiintunut nimi puurakenne. Väyläverkossa työasemat on kytketty rinnakkain samaan kaapeliin. Tästä seurauksena, kaikki työasemat saavat tietoonsa toisillensa tarkoitetun liikenteen. Väyläverkko oli alkuperäinen tyypillinen Ethernet-verkko. (Paananen 2005, 221.) Kuviossa 2 kuvattuna väylä (bus), rengas (ring) ja tähti (star) -topologioiden lisäksi myös puu (tree), mesh- ja hybrid-rakenteet sekä point to point -menetelmä.



Kuvio 2. Verkkotopologiatyypit (DNS Stuff 2019)

Rengastopologiassa tieto kulkee yksisuuntaisesti, ja samoin kuin väyläverkossa, tieto kulkee työasemalta toiselle vuorollaan. Rengasverkko mahdollistaa vikatilanteita varten verkon kahdennuksen. Käytössä on tällöin kaksi tiedonsiirtoreittiä, primääri ja sekundääri. Primäärirengas on ensisijaisesti käytössä, mutta vikatilanteiden ilmetessä datansiirto vaihtuu sekundäärirenkaalle. (Paananen 2005, 222.)

Rengasverkossa laitteet voivat suoraan kommunikoida vain viereisen laitteen kanssa. Viestin kulkeminen pidemmälle kuin viereisten laitteiden välillä edellyttää siis, että jokainen matkalla oleva laite saa viestin, sekä laittaa sen eteenpäin. Rengasverkon etuina onkin, että tarpeeton laite voidaan poistaa renkaasta. Tämä mahdollistaa sen, ettei laitteen vikaantuessa verkko välttämättä tarvitse uudelleen reititystä toimiakseen. (Muelander 2021.)

Tähtiverkko on verkkorakenne, jossa työasemat on kytketty keskuslaitteeseen muodostaen näin tähtimäisen kuvion. Keskuslaitteena Ethernet-verkossa toimii joko keskitin tai kytkin. Keskittimen avulla toteutettu tähtiverkko on toiminnallisesti tähtiverkko, mutta loogisesti se vastaa väyläverkkoa. Kytkimen avulla toteutetussa tähtiverkossa työasemat saadaan eroteltua toisistaan omaan linjaansa. (Paananen 2005, 223.)

Mesh-verkko on määritelmä LAN-topologian tyyppi, jossa laitteilla ei ole hierarkiaa, vaan ne ovat kytketty keskenään luoden kattavan verkon kattavuuden. Yleisimmin mesh-verkkoa hyödynnetään langattomien verkkojen toteutuksissa. Sen etuina on verkon laajentamisen lisäksi konfigurointi, sillä kun verkkoon lisätään uusi kytkentäpiste, siitä tulee automaattisesti osa verkkoa. (BasuMallick 2022.)

3.2 Lähiverkon laitteet

3.2.1 Reititin

Reititin on sisäverkon laite, joka reitittää IP-paketit kohti kohdeverkkoa. Reititin siis hallitsee IP-protokollat, eli se toimii OSI-mallin verkkokerroksessa. (Kaario 2002, 31.)

Reitittimen toimintaperiaate on muodostaa muistiinsa kuvaus verkosta. Se hyödyntää näin ollen rinnakkaisia reittejä, määrittelee varareittejä, optimoi reittejä riippuen runkoverkon kapasiteetista ja tilastoi sekä analysoi liikennettä. (Paananen 2005, 236.)

3.2.2 Kytkin

Kytkin on verkkolaite, jossa on useita liittimiä tai portteja. Kytkinportteihin voidaan yhdistää sisäverkon laitteita suoraan. Kytkin tallettaa tiedon portteihinsa kytketyistä laitteista MAC-osoitetauluun, jonka avulla se pystyy ohjaamaan paketit suoraan vastaanottavalle MAC-osoitteelle rekisteröidylle portille. Kytkin ei siis lähetä kaikkia saamiaan paketteja kaikkiin portteihinsa, vaan osaa ohjata ne oikeaan kohteeseen suoraan. (Homenet Howto 2019.)

Kytkimien käytön perusteena on useita sisäverkon koneita sisältävissä kohteissa kaistanleveyden hallinta. Kytkinten avulla saadaan luotua täysikytkentäinen verkko, jossa ei ole enää koneilla yhteistä väylää, vaan kytkin muodostaa yhteyden kehyksen lähetyksen ajaksi lähettävän ja vastaanottavan koneen välille, jolloin estetään törmäykset ja kaistanleveyden vieminen muilta käyttäjiltä. Tätä kutsutaan mikrosegmentoinniksi. (Hakala & Vainio 2002, 81–82.)

Tiedonsiirtotekniikan kehittyminen on osaltaan vaikuttanut myös kytkimien kyvykkyyksiin ja mahdollistanut keskitettyjen verkkojen hyödyntämisen. Aiemmin koaksaalikaapeleihin perustunut tiedonsiirto mahdollisti myös kytkimillä ainoastaan yhden väylän liikenteen, jolloin samanaikaisesti koneet eivät ole voineet lähettää ja vastaanottaa kehyksiä. Half duplex-liikenteessä taas on johdinparia; toinen lähettämiseen ja toinen vastaanottamiseen. Tällainen parikaapeliverkko perustuu kuitenkin keskittimiin, jolloin parit päättyvät samaan väylään, mikä estää samanaikaisen käytön. Tyypillisin liikennöintitekniikka kytkimillä on nykyisin full duplex-liikenne, joka mahdollistaa kahden koneen samanaikaisen kehysten lähettämisen ja vastaanottamisen. (Hakala & Vainio 2002, 82–83.)

Verkkokytkimet jaotellaan niin sanotusti kakkoskerroksen ja kolmoskerroksen kytkimiin riippuen siitä, millä protokollalla kytkentä toteutuu OSI-mallissa. Kakkoskerroksen kytkimet toimivat nimensä mukaan OSI-mallin toiseksi alimmalla siirtokerroksella. Sen kytkentä perustuu MAC-osoitteisiin. Kolmoskerroksen, eli verkkokerroksen kytkimissä reititys perustuu

verkko-osoitteisiin. Kehittyneemmät sovelluskytkimet toimivat OSI-mallin ylimmillä kerroksilla, jolloin kytkentä tehdään sovelluskerroksen protokollan mukaisesti. Tällaisilla tehokkailla kytkimillä on mahdollista toteuttaa myös verkkoliikenteen kuormanjakoa. (Paananen 2005, 237.)

3.2.3 Muita sisäverkon laitteita

Keskitin

Keskitin, eli HUB, on laite, joka toimii liikenteenvälittäjänä työaseman ja sisäisen väylän välillä. Erona kuitenkin kytkimeen on, että keskitin jakaa saamansa tiedon kaikkiin portteihinsa. (Paananen 2005, 236.)

Toistin

Toistin toimii OSI-mallin alimmalla, eli fyysisellä kerroksella. Se kopioi, vahvistaa ja toistaa eteenpäin vastaanottamaansa signaalia, eli toimii eräänlaisena vahvistimena. Perinteinen toistin ei ota kantaa liikenteeseen, mutta kehittyneemmillä toistimilla on mahdollista suodattaa virheliikennettä ja kuormituksen mukaan puskuroida liikennettä. Toistimen tarkoitus on vaimentaa tiedonsiirrossa syntyvää resistanssia ja kohinaa. Resistanssi on fysikaalinen ilmiö, jossa syötetty signaali vaimenee. Kohinalla taas tarkoitetaan tiedonsiirron häiriöitä. (Paananen 2005, 235.)

Silta

Siltoja voidaan verratta jossain määrin keskittimiin. Se vahvistaa vastaanotetun signaalin ja sen avulla voidaan yhdistää verkkoja sekä suodattaa yhdistettyjen verkkojen liikennettä. Silta toimii OSI-mallin siirtokerroksessa, sillä sen täytyy ymmärtää yhdistettyjen verkkojen kehysrakenteita. (Kaario 2002, 30.)

Palomuuri

Palomuuri sijaitsee yksityisen verkon ja julkisen verkon rajalla. Sen tehtävä on suodattaa liikennettä julkisesta verkosta yksityiseen verkkoon ja päinvastoin. Palomuurin tehokas toiminta perustuu siihen, miten monelta protokollapinon kerrokselta se saa tietoa. Palomuurilaitteiston vähimmäisvaatimus on kyky analysoida IP-paketteja, mutta luotettavan palomuurin on nähtävä myös muiden protokollakerroksesta saatavia tietoja. (Kaario 2002, 32.) Palomuureista lisää luvussa tietoturva.

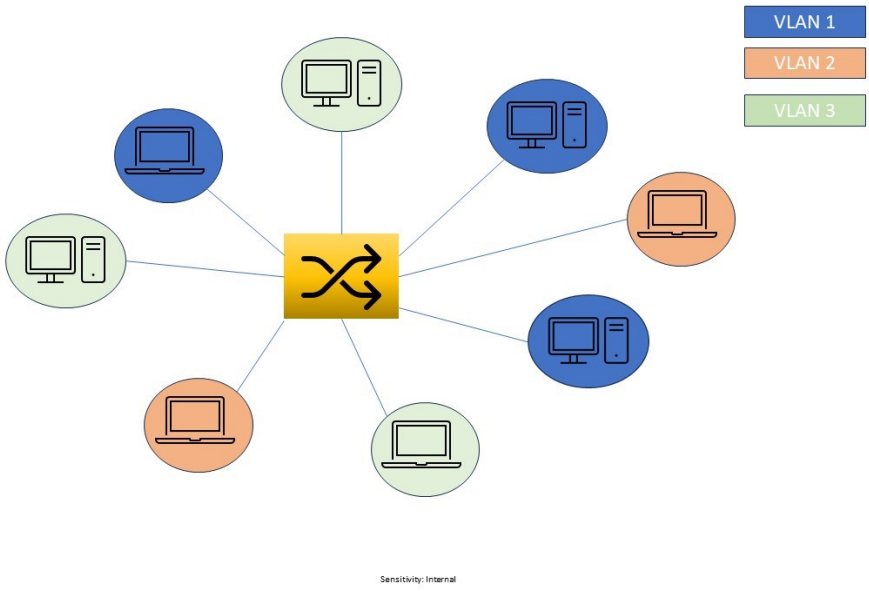
Mediamuunnin

Mediamuuntimien avulla sovitetaan erilaiset tiedonsiirtomediat toisiinsa. Yleisimmin sovitetaan parikaapeloitu Ethernet-verkko valokaapeloituun Ethernet-verkkoon. Mediamuuntimet

toimivat toistin- tai kytkentäperiaatteella. Toistinperiaatteella toimiva mediamuunnin toistaa liikenteen sellaisenaan ja toimii fyysisellä kerroksella. Kytkentäperiaatteisella mediamuuntimella olla kytkentäominaisuuksia, eli sovituksen lisäksi on mahdollisuus hyödyntää kytkevät ominaisuudet nopeuden sovituksella. (Paananen 2005, 238.)

3.3 Virtuaalinen LAN

VLAN:ia, eli virtuaalista sisäverkkoa, voidaan hyödyntää kytkinten avulla. VLAN on oma levitysalueensa, jonka avulla saadaan hallittua broadcast-liikennettä. VLAN-verkko mahdollistaa LAN-verkon fyysisten rajoitteiden kiertämisen, joka tekee siitä helpommin skaalattavan ja pienentää sen latenssia. Reitittimellä broadcast liikenne perustuu käyttäjän fyysiseen sijaintiin, jonka muuttuessa myös reitti on muutettava. Se toteutuu OSI-mallin kerroksessa 3. VLAN:in avulla voidaan erotella käyttäjät omiin ryhmiinsä riippuen heidän tarpeistaan. Yksinkertaisimmillaan VLAN voidaan konfiguroida porttikohtaisesti, jolloin porttiin kytketyt laitteet saavat VLAN:iin määritetyt oikeudet. VLAN:eja voidaan kuitenkin hallinnoida myös ohjelmistopohjaisena ja sääntöihin perustuvana, eli policy based VLAN verkkona. VLAN:ia voidaan hyödyntää yhteen rakennukseen rajoittuvan verkon ulkopuolellakin, joka helpottaa esimerkiksi yhteneväisten yritysverkkojen rakentamista toimipisteiden välillä. (Hakala & Vainio 2002, 91–93.) Kuviossa 2 näkyy keskellä kytkin, johon kytkettyjen päätelaitteiden taustavärit kuvaavat samaan VLAN:iin kuuluvia laitteita.



Kuvio 3. Virtuaalinen sisäverkko, VLAN

VLAN:ien toteutustapoja on neljä. Porttiperusteinen VLAN toteutetaan siten, että yhden tai useamman kytkimen portit jaotellaan VLAN:eiksi. Tällöin porttiin HUB:in kautta kytketyt

päätelaitteet ohjataan aina samaan verkkoon. MAC-osoitteisiin perustuvissa VLAN:issa päätelaitteen verkkokortin osoite lisätään ryhmään, josta muodostuu VLAN. Verkkokerrokseen perustuvassa VLAN:issa reititysominaisuuden omaavat kytkimet voivat muodostaa niitä aliverkkojen avulla. Sääntöperusteinen VLAN perustuu hallintaohjelmalla luotuihin sääntöihin, jonka mukaan käyttäjät ohjataan oikeaan VLAN:iin protokollien otsaketietojen avulla. (Hakala & Vainio 2002, 93–96.)

4 Langaton verkko

4.1 Yleinen langaton verkko

Langaton verkko on alun perin kehitetty tarjoamaan yleisen puhelinverkon palveluja liikkuville telepalveluiden käyttäjille. Puhelinverkko perustuu keskuspaikalla sijaitsevaan tukiasemaan, joka on jaoteltu erillisiin palveleviin alueisiin, eli soluihin. Näin mahdollistetaan laaja kattavuusalue kuormittamatta yhtä taajuuskaistaa liikaa. (Paananen 2005, 203.)

Vanhempia mobiiliverkonteknologioita ovat 3G ja 4G -verkot. Verkon nimet perustuvat sukupolveen, esimerkiksi 3G:llä tarkoitetaan verkon kolmannen sukupolven teknologiaa, eli G-kirjain tulee sanasta generation. Alun perin 1G ja 2G verkko oli suunniteltu vain puhelinliikenteen välitykseen. 3G-verkko mahdollisti myös tiedonsiirron internetin kautta yleisessä langattomassa verkossa. Tiedonsiirtonopeus 3G verkossa vaihtelee vastaanottonopeudessa 5–35 Mbit/s ja lähetysnopeus 0,1–4 Mbit/s välillä. Neljännen sukupolven, 4G-teknologian avulla taas pyrittiin siirtämään älykkyyttä päätelaitteille mahdollisimman suoralla reitillä IP-verkon yli. Nopeus 4G verkon yli tapahtuvaan tiedonsiirtoon saatiin nostettua vastaanotossa 5–300 Mbit/s ja lähetyksessä 5–30 Mbit/s välille. Myös viiveet sijoittuvat tavallisimmin 30–40 millisekunnin latenssiin, mikä tarkoittaa mahdollisuutta reaaliaikaisten tiedonsiirtopalveluiden käyttöön. (Väylävirasto 2019.)

Langattomassa verkossa on riskinä, sillä suuri käyttäjä määrä ruuhkauttaa taajuudet. Käytössä olevat taajuusalueet vaihtelevat 100 MHz:n ja 5,2 GHz:n välillä. Erilaisilla standardoinneilla pyritään yhtenäistämään taajuusalueiden käyttöä, jottei ongelmaksi muodostuisi, että käytetty taajuusalue on eri sijainnissa jo varattuna muulle käytölle. Taajuusalueen kokoon vaikuttaa kapasiteettitarve. Radiosignaalin vaimennus on taajuudesta riippuvaista, minkä takia suuret taajuusalueet tarkoittavat pienempiä soluja. Pienemmillä soluilla verkon kantavuus pienenee, joka hankaloittaa liikkumisen hallintaa. (Paananen 2005, 203.)

Langattoman verkon viides sukupolvi, eli 5G, tarjoaa käyttäjilleen edeltäjiään 3G ja 4G -verkkoa huomattavasti suurempaa tiedonsiirtokapasiteettia ja nopeampaa tiedonsiirtoa. Mobiiliverkon mahdollisuudet toimivat innovaationa monen eri osa-alueella niin yksityishenkilöiden, kuin yritysten sekä virastojen osalta. 5G:n mahdollisuuksia pyritään erityisesti hyödyntämään neljällä eri teknologian alalla, eli autoteollisuudessa, sekä terveys-, liikenne- ja energia-aloilla. (Euroopan Unioni 2022.) Kuviossa 4 on kuvattu mahdollisia käyttökohteita jokapäiväisessä arjessa.

Kuvio 4. 5G-verkon hyödyntäminen (Euroopan Unioni 2022)

Kuten edellä on kuvattu, suurimmat 5G hyödyt ovat arjen sujuvoittaminen ja turvallisuuden nostaminen. 5G mahdollistaa esimerkiksi liikkuvissa yksiköissä ajantasaisen tiedonsiirron viranomais- tai turvallisuuteen liittyvissä tehtävissä. Teollisuudessa taas energiasektori hyötyy 5G-teknologiasta automaation kehityksen kautta. Terveysteknologiaa pidetään yhtenä tärkeimpänä robotiikan ja automaation kehityksen kohteena, koska kyse on henkeen ja terveyteen liittyvästä alasta. 5G verkon viiveettömyys onkin avainasemassa tämänkaltaisessa ympäristössä. (Kauppinen 2021.)

4.2 WLAN

Langaton tukiasema on WLAN:in (wireless local area network), eli langattoman sisäverkon laite, johon käyttäjät voivat liittyä langattomasti. Sen etu on, ettei sisäverkkoon liittyviä laitteita tarvitse fyysisesti kytkeä kytkimeen tai reitittimeen kaapeleilla. Verkkolaitteet niin opiskelu, yritys kuin yksityiskäytössä ovat lisääntyneet, mikä on huomioitava oppilaitosten, yritysten sekä kodin sisäverkon suunnittelussa, joissa kaapelointi voi osoittautua haasteeksi tai ei ole mahdollista esimerkiksi mobiililaitteilla. (Hewlett Packard Enterprise 2024.)

Langaton tukiasema kytketään Ethernet-kaapelilla joko reitittimeen tai kytkimeen. Yhteyden se muuntaa joko 2,4 GHz:n tai 5 GHz:n signaaliksi. (Netgear 2022.)

Sisäverkon langattomia tukiasemia, jotka kytketään kiinteästi sisäverkon laitteisiin, kutsutaan yleisesti nimellä AP. Se on lyhenne sanasta access point. Langaton verkko voidaan toteuttaa myös työasemilla, joissa on langaton verkkosovitin. Sitä kutsutaan adhoc-verkoksi ja tällöin langaton verkko rakentuu ilman erillistä aktiivilaitetta. (Paananen 2005, 229.)

Alun perin kaikki langattomat laitteet käyttivät 2,4 GHz signaalia. 5 GHz taajuusalue on verrattain uusi signaali ja sen käyttö vaatiikin myös verkkoon liittyvältä laitteelta tuen 5 GHz signaalille. Kaksitaajuuksisten verkkojen avulla pyritäänkin hyödyntämään molempien

taajuusalueiden edut. 2,4 GHz signaalin kantama on pidempi ja yhteensopivampi vanhempien laitteiden kanssa, vaikka se onkin tiedonsiirtonopeuksissa hitaampi verrattuna 5 GHz taajuuden siirtonopeuteen. 5 GHz:n käytössä pyritäänkin hyödyntämään taajuusalueen tiedonsiirto nopeutta. Kuitenkaan kaikki sisäverkonlaitteet eivät nopeudesta erityisesti hyödy, kuten sisäverkon dataa lähettävät IoT-laitteet, on silloin matalamman taajuusalueen käyttö perustellumpaa. (Rasmussen 2021.)

Ensimmäiset saatavilla olleet WLAN-tuotteet eivät olleet yhteensopivia keskenään, jonka takia langatonta ratkaisua rakennettaessa kaikkien laitteiden tuli olla samalta toimittajalta. Sen seurauksena on kehitetty avoin standardi 802.11, jonka avulla saadaan taattua, että tuotteet ovat yhteensopivia valmistajasta riippumatta. (Paananen 2005, 210–212.)

Alkuperäiseen WLAN standardiin 802.11:sta on tehty sittemmin paranneltuja versioita, joita merkitään pienillä aakkosilla. Aakkosten päättyessä z-kirjaimeen, alettiin versioita myöhemmin merkata kahdella kirjaimella, eli aa, ab, ac ja niin edelleen. 802.11 on IEEE:n määrittämä yleinen standardi. Wi-Fi Alliance omistaa tavaramerkin Wi-Fi, jonka tarkoitus on osoittaa WLAN-tuotteiden yhteensopivuus. Wi-Fi Alliance ei ole viranomainen, vaikka se valvoo ja testaa WLAN-tuotteiden yhteensopivuutta. (Riihikallio 2017.)

Vaikka langattoman verkon hyötyjä on sisäverkossa useita, kuten kaapeloinnin puute ja edullinen ja verrattain helppo kapasiteetin kasvatus käyttäjien lisääntyessä, langattomalla verkolla ei voida korvata kokonaan fyysiseen kaapelointiin perustuvaa lähiverkkoa. Langattomassa sisäverkossa tiedonsiirron nopeus on korkeimmillaan 10 Mbps, kun taas Ethernet-yhteyksillä saavutetaan jopa tuhatkertaiset nopeudet. Langattomat yhteydet tuovat myös omat haasteensa tietoturvan näkökulmasta. (Paananen 2005, 210–212.)

5 Autentikointi ja tietoturva

5.1 Tietoturva

5.1.1 Tietoturvan määritelmä

Tietoturva koostuu hallinnollisista ja teknisistä toimista, joilla on tarkoitus varmistaa tiedon luottamuksellisuus, eheys ja käytettävyys. Luottamuksellisuudella tarkoitetaan, että tieto on vain tiedon käyttöön oikeutettujen käyttäjien nähtävissä. Eheys on sitä, että tietoa voi muuttaa vain siihen oikeutetut käyttäjät. Käytettävyydellä taas tarkoitetaan, että tietoon ja tietojärjestelmiin on pääsy vain niillä toimijoilla, joilla niiden käyttöön on oikeus. (Kyberturvallisuuskeskus 2020.)

Tietoturvallisuus voidaan jakaa osa-alueittain. Hallinnollinen turvallisuus määrittää tietoturvaa toteuttavat linjaukset, johtaa, organisoi ja jakaa vastuut. Henkilöturvallisuus on työntekijöiden ohjeistusta, kouluttamista, perehdyttämistä, taustojen tarkistusta rekrytoinnin yhteydessä sekä se kattaa salassapito- ja kilpailukieltosopimukset. Henkilöturvallisuuden suurin riski on tahattomat vahingot, sekä tarkoituksenmukaiset sabotaasit. Käyttötoimintojen turvallisuus varmistaa päätelaitteiden ja muiden verkon aktiivilaitteiden ylläpidon, huollon ja valvonnan. Tähän voidaan rinnastaa laitteistoturvallisuus, joka tarkoittaa laitteiden toiminnan varmistamista vikatilanteen, esimerkiksi sähkökatkon sattuessa. Ohjelmistoturvallisuus kattaa päätelaitteiden ohjelmistojen suojaamisen, lisenssien hallinnan, järjestelmäpäivitysten ajantasaisuuden sekä ohjelmien luvallisuuden varmistamisen. Tietoaineistoturvallisuudella tarkoitetaan tallennetun tiedon käsittelyä niin, ettei luottamuksellinen tieto pääse vääriin käsiin missään vaiheessa elinkaartaan. Tietoliikenteen turvallisuus on liikenteen jatkuvuuden, eheyden ja tiedon salaamisen varmistamista. Lisäksi osana tietoturvaa on toimitilojen fyysinen suojaus kulunvalvovannon, murtosuojausten ynnä muiden toimien avulla. Tätä kutsutaan toimitilaturvallisuudeksi. Viimeisimpänä mainittakoon yksityisyydensuoja, jolla tarkoitetaan toiminnalle välttämättömien henkilötietojen keräämistä ja suojaamista siten, että niitä käsitellään vain asianmukaisiin toimiin henkilötietosuojalakia noudattaen. (Paananen 2005, 386–387.)

5.1.2 Tietoturvasääntely ja velvollisuus laissa

Viestinnän välittäjällä, eli teleyrityksellä, yhteisötilaajalla tai muulla viestinnän välittäjällä on velvollisuus huolehtia tietoturvasta palvelujensa, viestien, välitystietojen ja sijaintitietojen osalta. Viestinnän välittäjän tehtävä on suhteuttaa toimenpiteet uhan vakavuudesta, toimenpidekustannuksista ja uhan torjunnan teknisistä mahdollisuuksista riippuen. Kyberturvallisuuskeskuksen tehtävänä on ohjata ja valvoa tietoturvavelvoitteiden noudattamista,

sekä tarkentaa laissa määritettyjä velvoitteita määräyksillään. (Kyberturvallisuuskeskus 2020.)

Pääosin velvoitteet on säädetty sähköisen viestinnän tietosuojalaissa. Lain on määrä huolehtia sähköisen viestinnän luottamuksellisuudesta, sekä taata yksityisyyden suojan toteutuminen ja edistää sähköisen viestinnän tietoturvaa. Laki velvoittaa viestinnän välittäjät huolehtimaan palvelujensa tietoturvasta, tehdä tarvittavat toimenpiteet tietoturvan toteutumiseksi ja ilmoittamaan tietoturvaan kohdistuvista uhista sekä viestintävirastolle, että tilaajalle ja käyttäjälle. (Sähköisen viestinnän tietosuojalaki 516/2004; Laki sähköisen viestinnän tietosuojalain muuttamisesta 365/2011.)

Keväällä 2018 määritettiin kaikissa EU-maissa sovellettava yleinen tietosuoja-asetus, GDPR, joka sääntelee henkilötietojen käsittelyä. GDPR on lyhenne sanoista General Data Protection Regulation. Yrityksen on noudatettava GDPR:ää mikäli se sijaitsee EU:ssa ja käsittelee henkilötietoja. Niissä tapauksissa, joissa yritys sijaitsee EU:n ulkopuolella, mutta tarjoaa tavaroita tai palveluja EU-maiden henkilöille tai seuraa näiden henkilöiden käyttäytymistä, on sen noudatettava yleistä tietosuoja-asetusta ja nimettävä EU:ssa toimiva edustaja. GDPR:n vaatimukset koskevat henkilötietojen keräämistä, säilytystä ja hallinnointia. Henkilötiedoilla tarkoitetaan henkilön yksilöiviä tietoja, kuten nimeä, osoitetta, henkilökortin tai passin numeroa, tuloja, kulttuurista profiilia, IP-osoitetta sekä sairaalan tai lääkärin hallussa olevia tietoja. Yritys ei saa käsitellä rotua tai etnistä alkuperää, sukupuolista suuntautumista, poliittisia mielipiteitä, uskonnollisia tai filosofisia vakaumuksia eikä ammattiliittoon kuulumista sisältäviä tietoja. Yritys ei myöskään saa käsitellä geneettisiä, biometrisiä tai terveydellisiä tietoja, poissulkien erityistapaukset, jolloin käsittelylle on annettu nimenomainen suostumus ja kun käsittely on tarpeellista lainsäädäntöön tai yleiseen etuun perustuen. Myös rikostuomioita ja rikkomuksia koskevia henkilötietoja ei saa käsitellä, ellei lainsäädäntö niin salli. Tietosuoja-asetus perustuu suostumukseen. Henkilön, jonka tietoja kerätään, on kyettävä ymmärtämään tietojen keruun tarkoitus ja antamaan suostumus sille. Yritys ei saa kerätä tai säilöä henkilötietoja, jotka eivät ole tietyn tarkoituksenmukaisia. Yrityksen on kyettävä antamaan henkilön pyytäessä vähintään tiedot siitä, kuka käsittelee henkilötietoja ja mistä syystä, sekä mikä käsittelyn oikeusperusta on. Henkilöllä on myös oikeus päästä tietoihinsa, siirtää ne toiseen järjestelmään ja pyytää tietojen poistoa tai korjausta. Mikäli yritys luovuttaa vahingossa tai laittomasti tietoja valtuuttamattomille vastaanottajille, on kyseessä tietoturvaloukkaus, josta on ilmoitettava tietosuojaviranomaiselle 72 tunnin sisällä loukkauksen tietoon tulemisesta. GDPR:n noudattamatta jättämisestä seuraa sakkoja, joiden suuruus tiettyjen rikkomusten kohdalla on 20 miljoonaa euroa tai 4 prosenttia yrityksen liikevaihdosta. (Your Europe 2022.)

5.1.3 Lähiverkon tietoturva

Tietoturva on kyseisen verkon tiedon turvaamista. Tietoturva mielletään usein yhdeksi tekniseksi osaksi verkkoratkaisuja, mutta kyse on ennen kaikkea laitteiden, koulutusten, ajantasaisuuden ja ihmisten toiminnan kokonaisuudesta. Tänä päivänä yrityksen tietoturvaa uhataan monin tavoin erilaisilla tietojenkalasteluyrityksillä ja muilla tietoturvahyökkäyksillä. Tietoturvassa korostuukin ennaltaehkäisy. Esimerkiksi ohjelmistojen ajantasaiset päivitykset ennaltaehkäisevät mahdollisten ohjelmistojen haavoittuvuuksien hyödyntämistä. Käyttäjien koulutus on taas avainasemassa erilaisten tietojenkalasteluviestien kohdalla. (Järvinen 2022.)

Fyysisellä tietoturvalla tarkoitetaan laitteiden suojausta. Laitteet sijoitellaan siten, että ne ovat suojassa ilkivallalta eli luvaton pääsy estetään. Sijoittelussa on huomioitava, että myös tahaton vahingoittuminen on epätodennäköistä. Sijoittelun lisäksi fyysinen suojaus tarkoittaa laiteolosuhteiden muutosten tarkkailua, kuten ympäristön lämpö- ja kosteusolosuhteiden seurantaa. (Kyberturvallisuuskeskus 2023.)

Lähiverkon tietoturvassa verkkolaitteiden turvallisuuden kannalta on huomioitava reitittimen ja kytkinten konfigurointi, vahvojen salasanojen käyttö ja tarpeettomien palveluiden poisto. Näiden lisäksi tarvitaan palomuuri. Palomuuri on järjestelmä, jonka tehtävä on suojata lähiverkkoliikenne julkiselta verkolta ja suodattaa liikennettä. Palomuuri suodattaa verkkoliikennettä IP-osoitteiden, protokollien, lähde- ja kohdeosoitteiden, verkkotunnusten, avainsanojen ja porttien tarkastelulla. Suodattimien määrittäminen on verkon ylläpitäjän vastuulla. Karkeasti voidaan puhua ohjelmistopohjaisista ja verkkopalomuureista. Ohjelmistopohjainen on päätelaitekohtainen palomuuri. Päätelaitekohtainen palomuuri suojaa vain kyseistä päätelaitetta, johon se on asennettu. Jotkin käyttöjärjestelmät tarjoavat ohjelmistopohjaisen palomuurin esiasennettuna. Lisäksi virustorjuntaohjelmat sisältävät usein ohjelmistopohjaisen palomuurin. Verkkopalomuuri suojaa koko lähiverkkoa, eli se sijaitsee julkisen verkon ja lähiverkon välissä. Sen avulla on mahdollista suojata kaikki lähiverkon laitteet. (Lorentsen 2023.)

Langaton verkko vaatii verkon suojauksessa erityishuomioita. Päätelaitteet hakevat automaattisesti parhainta signaalia langattomassa verkossa, jolloin hyökkääjän on mahdollista luoda samanniminen verkko, johon käyttäjä epähuomiossa liittyy. Mikäli langattomassa verkossa ei ole tehty verkonerottelua, voidaan jokaiselle verkkoon liittyneelle laitteelle lähettää haittaliikennettä. Langattomille radiotaajuuksille on kehitetty useita salausmenetelmiä. On kuitenkin muistettava, että vaikka radioliikenne olisi suojattu, tarvitaan suojaus vielä lähiverkon fyysisille laitteille sekä lähiverkon ja julkiverkon välille. WLAN-verkossa salakuuntelu on yleistä, jolloin verkossa kulkevien viestien salauksessa on hyödynnettävä salaisia tietoja.

Tällaisia tietoja ovat esimerkiksi salakirjoitusavaimet. Salausmenetelmistä vanhin WEP, eli Wired Equivalent Privacy, on onnistuttu murtamaan. Hieman uudempi menetelmä WPS, eli Wi-Fi Protected Setup, on suunnitteluvirheen vuoksi todettu haavoittuvaksi. Näistä kumpaakaan ei suositella käytettäväksi. Suositeltavat salausmenetelmät ovat WPA sekä sen vahvempi versio WPA2. WPA hyödyntää Advanced Encryption Standard-algoritmia, ja se yhdistettynä PSK-salasanaan on varsin turvallinen. PSK, eli Pre-Shared Key on vahva esiasetettu 20 merkkinen salasana, joka syötetään kerran verkon ensimmäisellä käyttökerralla. Mikäli hyökkääjä saa PSK:n tietoonsa on hänen mahdollista purkaa kaikki langattoman verkon liikenne. Verkko voidaan myös piilottaa muilta käyttäjiltä, josta voidaan käyttää termiä hidden SSID. Verkon piilottaminen ei kuitenkaan yksistään lisää tietoturvaa. (Kybertuvallisuuskeskus 2014.)

Verkkoliikenteen salausta IP-verkkojen yli kutsutaan SSL-salaukseksi. SSL on lyhenne sanoista Secure Sockets Layer, joka on vanhentunut protokolla, mutta terminä yleistynyt kuvaamaan liikenteen salausta. Nykyisin hyödynnetään TLS-protokollaa, eli Transport Layer Security -protokollaa. Salauksella palvelimen ja selaimen välillä pyritään suojaamaan arkaluontoisia tietoja, kuten pankkitunnuksia. Salaus tapahtuu salausavainten avulla. Salausavaimen lisäksi sivustolle tarvitaan kolmannen osapuolen myöntämä sertifikaatti, joka osoittaa yhteyden olevan oikeasti salattu. SSL-salauksella estetään muun muassa WLAN verkossa mahdollinen liikenteen salakuuntelu. (Kataja 2017.)

Verkkoliikenteen salauksessa tunnetuksi termiksi on noussut etätyön yleistymisen myötä VPN. VPN on lyhenne sanoista Virtual Private Network, eli virtuaalinen erillisverkko. Sen tarkoitus on luoda suojattu yhteys VPN-palvelimelle, jonka jälkeen se mahdollistaa suojatun selaimen käytön tai pääsyn lähiverkon dataan. VPN yhteyden avulla salataan myös käyttäjän fyysinen sijainti. VPN-palvelun käyttö ei kuitenkaan ole mahdollista samoilla verkon nopeuksilla kuin fyysisesti lähiverkossa, koska palvelimen kautta datansiirto hidastuu matkan kasvaessa. On myös huomioitava, että vaikka yhteys on suojattu vaatii se rinnalleen haittaohjelmien torjunnan sekä palomuurin kattavan tietoturvan takaamiseksi. (Solla 2017.)

Haittaohjelma on yleisnimitys haitallisille ohjelmistoille. Haittaohjelmat leviävät yleensä linkkien, mainosten tai liitteiden kautta, jotka on saastutettu. Haittaohjelmat itsessään ovat joko viruksia, matoja, mainosohjelmia, troijalaisia, kiristys- tai vakoiluohjelmia, botteja tai rootkittejä, eli piilohallintaohjelmia. Näistä jokaisella on omat toimintaperiaatteensa ja tavoitteet saastuneessa laitteessa. Viruksen ja madon tavoitteena on levitä mahdollisimman laajalle samalla aiheuttaen päätelaitteelle haittaa madot kuormittamalla tiedonsiirtokapasiteettia ja virukset tuhoamalla tiedostoja. Mato eroaa viruksesta siten, että se pystyy toimimaan saastuneessa laitteessa ilman käyttäjän toimia, esimerkiksi lähettämällä automaattisesti

käyttäjän laitteelta saastuneita sähköposteja. Sekä madot että virukset leviävät useimmiten linkkien ja sähköpostien kautta. Mainosohjelmien toimintaperiaate on avata käyttäjän laitteella erilaisia mainoksia ponnahdusikkunoina. Mainokset eivät sinänsä ole vaarallisia, mutta niiden tarkoitus on saada käyttäjä tarkoituksella tai vahingossa klikkaamaan linkkejä, mikä altistaa tietoturvariskille. Troijalaisten tarkoitus on päästä käyttäjän laitteelle ja sitä kautta sallia rikollisille pääsy laitteelle tai ladata uusia haittaohjelmia. Kiristysohjelman voi saada tietojenkalasteluyrityksen kautta tai troijalaisen mukana. Sen tarkoitus on estää käyttäjän pääsy laitteelle ja siten kiristää käyttäjältä esimerkiksi rahaa. Vakoiluohjelman tarkoitus on kerätä käyttäjästä tai organisaatiosta mahdollisimman paljon tietoa kolmannelle osapuolelle. Botit on kehitetty luvallisiin tarkoituksiin, mutta sitä voidaan hyödyntää haittaohjelmissa suorittamaan toiminteita käyttäjän laitteella. Piilohallintaohjelma pyrkii piilottamaan ja poistamaan kaikki kyberhyökkäykseen viittaavat jäljet ja sen poistaminen laitteelta on äärimmäisen haastavaa. Piilohallintaohjelmat asentuvat käyttäjän laitteelle usein toisen haittaohjelman, esimerkiksi troijalaisen yhteydessä. (Laaksoharju 2021.)

Haittaohjelmien levitessä usein linkkien ja sähköpostien kautta on käyttäjien koulutus yksi tärkeimpiä tietoturvan osia. Tämän päivän tietoturvaloukkaukset tapahtuvat usein käyttäjän huolimattomuudesta, virheestä tai osaamattomuudesta. Koulutus antaa informaation lisäksi avaimet tietoturvakulttuurin rakentamiseen. Tietoisuuden lisäksi kouluttamalla annetaan käyttäjille myös käytännön tason ratkaisuja tietoturvan parantamiseksi, kuten salasanojen hallinta. Käyttäjälähtöistä tietoturvan tärkeyttä painottaa se, että laki velvoittaa yrityksiä noudattamaan tietosuoja-asetuksia. (Perttunen 2023.)

Tietoturvauhkien ennakointi on lähiverkossa korostetussa roolissa. Vaikka tietoturvahaavojen paikkaus tapahtuisi nopealla aikataululla, tai tiedot saataisiin palautettua varmuuskopioinnin avulla, voi lyhytkestoinenkin pääsy sisäverkon tietoihin aiheuttaa mittavaa vahinkoa tiedon joutuessa vääriin käsiin. (Jokinen 2019.)

5.2 Autentikointi ja auktorisointi

5.2.1 Todennus ja kiistämättömyys

Autentikointi, eli todennus tarkoittaa menetelmiä, joiden avulla saadaan todennettua käyttäjän olevan se henkilö, joka hän väittää olevansa. Kiistämättömyydellä on tarkoitus varmistaa, ettei osapuoli voi kiistää olevansa mukana tapahtumassa. Yksinkertaisimmillaan tällä voidaan tarkoittaa esimerkiksi sähköistä allekirjoitusta asiakirjassa, joka on allekirjoitettu vahvan tunnistautumisen, kuten pankkitunnusten avulla. Tällöin kolmas osapuoli, eli pankki tunnustaa henkilön olevan se, joka hänen oletetaan olevan. (Kaario 2002, 293.)

Autentikoinnin tarkoituksena on todentaa käyttäjä, eli varmistaa hänen olevan se kuka väittää olevansa ja että hänellä on oikeus verkon tietoihin. Perinteisin esimerkki autentikoinnista on käyttäjätunnus ja salasana yhdistelmä. Tänä päivänä sitä ei voida kuitenkaan pitää tietoturvaratkaisuna parhaimpana. Kaksivaiheisen tunnistautumisen käyttö onkin yleistynyt. Kaksivaiheisen tunnistautumisen ideana on, että salasanan ja käyttäjätunnuksen lisäksi käyttäjä vahvistaa kirjautumisen mobiilivarmenteen, tekstiviestin tai token-ratkaisun avulla. Todentamisen lisäksi on todennettava käyttäjän käyttöoikeudet. Toisin sanoen käyttöoikeuksien todennus tarkoittaa palvelun käyttöoikeuksien tarkistusta. Ehdollisen pääsyn käytäntö on käyttäjälle asetettujen luottosuhteiden tarkastus. Käytännössä käyttäjällä on pääsy tiettyihin ohjelmistoihin ja sovelluksiin, mutta vain esimerkiksi sisäverkon kautta tai VPN-yhteyden yli. (Hermans 2020.)

Autentikointi voidaan toteuttaa joko kertakirjautumisena, jolloin käyttäjä tunnistautuu kerran ja pystyy käyttämään useita eri palveluita yhdellä kirjautumisella. Kertakirjautumisesta käytetään yleisesti lyhennettä SSO, joka tulee englannin kielen sanoista Single Sign On. SSO:ta hyödynnetään laajalti yritysten järjestelmissä. Sen etuina ovat työntekijän näkökulmasta vaivattomuus ja työnteon nopeutuminen, kun autentikointi kaikkiin järjestelmiin suoritetaan kerran. Vaihtoehtoisesti tunnistautumistieto voidaan siirtää palvelimelle jokaisella yhdistämiskerralla, mikä tarkoittaa käytännössä kirjautumistietojen tarkistusta jokaiseen palveluun yhdistettäessä. (Karvinen 2022.)

Identiteetin hallinnalla tarkoitetaan käyttäjälle luotua sähköistä identiteettiä. Käyttäjälle luodaan profiili, jolle käyttäjä tunnistautuu. Profiili sisältää perustiedot käyttäjästä, kuten autentikointitiedot. Kyseiselle profiilille voidaan taas määrittää pääsyt ja oikeudet sekä rooli käyttäjän mukaan. Käyttäjän rooli määrittää hänen oikeutensa järjestelmissä, kuten muokkaus- ja lukuoikeudet tiedostoihin. Yhdellä käyttäjällä voi olla useita rooleja. Yritysratkaisuissa on mahdollista myös luoda sähköiset identiteetit työntekijöiden lisäksi kumppaneille sekä asiakkaille, joille pääsy lähiverkkoon on tarpeellista. (Niemi.)

Autentikoinnissa voidaan myös salasanojen ja kaksivaiheisen tunnistautumisen lisäksi hyödyntää käyttäytymispohjaista tai biometristä autentikointia. Käyttäytymispohjainen autentikointi ei ole laajemmin käytössä, sillä se vaatii käyttäjän toiminnan analysointia ja datan keräämistä pidemmältä aikaväliltä. Pitkäaikainen tiedonkeruu ja sen analysointi vie itsessään paljon resursseja, mikä tekee käyttäytymispohjaisesta autentikoinnista haastavan toteuttaa. Biometrinen tunnistautuminen on yleistynyt nykyteknologiassa. Biometrisessa tunnistautumisessa käyttäjä kirjautuu laitteelle tai järjestelmään esimerkiksi sormenjäljen tai kasvojen tunnistamisen kautta. Käyttäjän näkökulmasta biometrisen tunnistautumisen etuina ovat vaivattomuus, kuitenkin samaan aikaan sen ollessa vahva autentikointitapa.

Biometrinen tunnistautuminen edellyttää kuitenkin korostunutta tietoturvaa tietoja säilyttävältä yritykseltä, ettei esimerkiksi käyttäjien sormenjäljet pääse leviämään rikollisten käsiin. (Gittlen & Rosencrance 2021.)

5.2.2 Pääsynhallinta

Auktorisointi eli pääsynvalvonta voidaan toteuttaa usealla eri tavalla riippuen ympäristöstä ja käyttäjän käyttöoikeuksista. Se muodostaa puitteet, jossa käyttöoikeuksia määritellään, osoitetaan sekä hallinnoidaan. Pääsääntöisesti käytetään malleja, jotka perustuvat joko roolipohjaisuuteen tai attribuutteihin. (Karvinen 2022.)

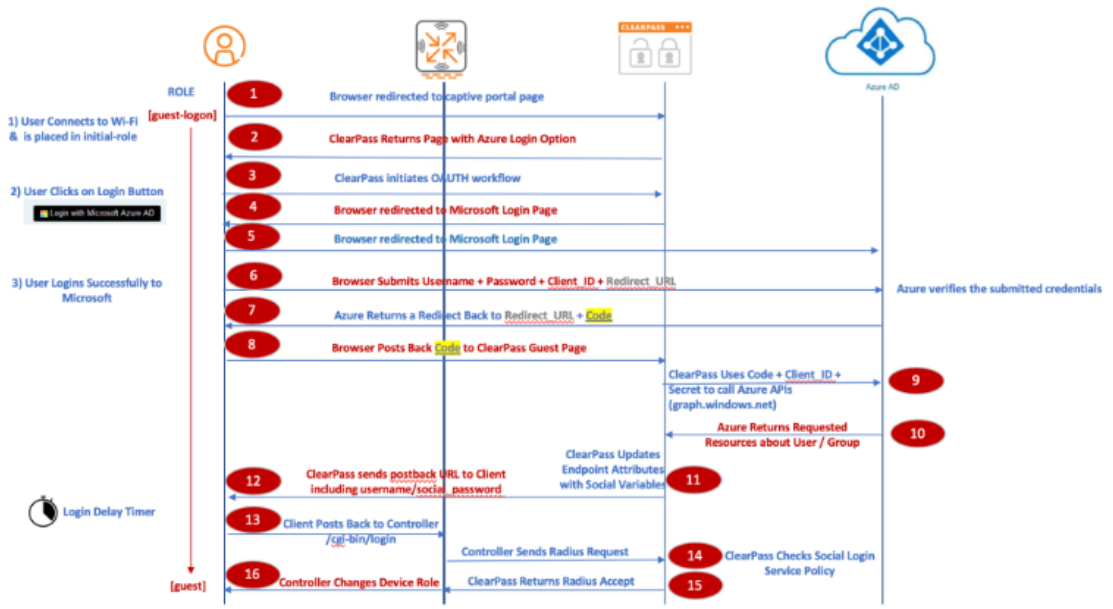
Toimiva pääsynhallintajärjestelmä tunnistaa ja tallentaa käyttäjien kirjautumistietoja, mahdollistaa käyttöoikeuksien määrittämisen ja poistamisen sekä käyttäjätunnusten tietokannan hallinnan. Pääsynhallintajärjestelmän avulla voidaan myös hallita laitteiden ja sovellusten niin sanottua digitaalista identiteettiä, eli määrittää laitteille oikeudet verkkoon pääsyyn samoin kuin käyttäjille. Toimiakseen järjestelmässä tulisi olla keskitetty hakemistopalvelu, jolla on näkyvyys kaikkiin käyttäjäkunnan osa-alueisiin. (Gittlen & Rosencrance 2021.)

6 Käytettävät järjestelmät

6.1 Pääsynhallintajärjestelmä Clearpass

Aruba Clearpass on Hewlett Packard Enterprisen tarjoama pääsynhallintaohjelma yrityskäyttöön. Laitteiden yhdistyessä verkkoon, se myöntää laitteelle käyttöoikeuden ennalta määritettyhän käyttäjäroolien, laitetyyppien ja kyberturvan perusteella. (Tablan 2022.)

Pääsyhallinnan neljä peruselementtiä on profilointi, autentikointi, valtuutus ja asento. Profiloinnin avulla ymmärretään mitä päätelaitteita verkkoon on yhdistetty. Autentikoinnin kautta tunnistetaan käyttäjä tai laite. Valtuutuksen avulla annetaan valtuudet käyttää tiettyä roolin perusteella määritettyä verkkoa tai toiminteita. Asennon muutosten avulla tunnistetaan, mikäli jo autentikoidussa ja valtuutetussa laitteessa tapahtuu odottamattomia muutoksia. Kehyksenä käytettävä 802.1X on porttipohjainen pääsynhallinta. Se sisältää kolme erilaista entiteettiä. Näitä entiteettejä ovat anoja, eli loppukäyttäjän päätelaite, autentikoija, eli verkkolaite ja autentikoiva palvelin. EAP (Extensible Authentication Protocol) on kehys usealle eri autentikointimetodille. Yleisimpiä EAP-metodeja ovat EAP-TLS, PEAP ja EAP-TTLS. RADIUS on protokolla, jota käytetään yleisesti osana autentikoinnin, valtuutuksen ja tilastointivalvonnan kommunikoinnissa. Protokollan avulla verkkolaite kommunikoi autentikointipalvelimen, eli Radius-palvelimen kanssa. Attribuutti-arvo-parit toimivat kumpaankin suuntaan viesteinä. (Hewlett Packard Enterprise 2018.) Kuviossa 4 kuvataan käyttäjän roolipohjainen autentikointi vierasverkkoon Clearpassissa.



Kuvio 4. Roolipohjainen autentikointi vierasverkkoon (Mukddam 2020)

Kuvassa 1 kuvaillun esimerkin mukaisesti käyttäjä kirjautuu verkkoon portaalin kautta, tunnistautuen esimerkin tapauksessa Microsoftin tuotteen Azure AD:n avulla. Käyttäjän painaessa kirjaudu, palvelimelle lähtee POST-pyyntö, sekä spesifioidut Client ID ja valtuutettu URL eli tapahtumankäsittelijä. Selain odottaa vastausta palvelimelta. Vastauksen saatuaan käyttäjän onnistuneesti kirjautuessa vierasverkkoon, Clearpass kerää tiedot kirjautumisesta ja käyttäjästä järjestelmään endpointiin. Tämän jälkeen Radiuksen avulla selvitetään käyttäjän oikeudet verkossa ja määritetään rooli sen mukaan. Lopuksi käyttäjä pääsee verkkoon. (Mukaddam 2020.)

6.2 Configuration Management Database

Configuration Management Database, eli CMBD on standardoitu tietokanta. Sen tarkoitus on sisällyttää yrityksen käyttämien laitteiden ja ohjelmistojen tiedot, eli yrityksen IT-infrastruktuuri. Laitteiden ja ohjelmistoja kutsutaan konfiguraatioyksiköksi, eli CI:ksi. Tietokanta konfiguraatioyksikön tiedon lisäksi myös yhdistää näiden konfiguraatioyksiköiden väliset relaatiot ja riippuvuudet. (Montgomery 2020.)

Tietokanta luo CI:t integraation, havaintotyökalujen ja manuaalisen tietojen lisäämisen avulla. Tietokannat vaativat kuitenkin aktiivista ylläpitoa ja päivittämistä. Manuaalinen tietojen lisääminen voi aiheuttaa ylimääräistä työtä ylläpidollisesta ja sen seurauksena laiterekisteriin voi syntyä kaksoiskappaleita laitekorteista, joten sitä ei suositella. (ServiceNow 2023.)

Suurimpia CMDB:n avulla saavutettavia hyötyjä on erityisesti ajantasaisen tiedon ylläpito. CMDB:n avulla voidaan hahmottaa selkeästi lintuperspektiivistä yhteyksien todelliset ja tämänhetkiset relaatiot ja keskinäiset riippuvuudet. Näin ollen selkeitä etuja on riskien arviointi, ongelmanratkaisun nopeutuminen ja taloudellinen hyöty. Sen haasteiksi voidaan katsoa muutamia seikkoja, mutta suurimpana voidaan nähdä käyttäjälähtöiset ongelmat. Lähtökohtaisesti uuden ohjelmiston käyttöönotto vaatii aina kulttuurin luomista tiimin sisällä sekä käyttäjien sitoutumista ohjelmiston käyttöön ja hyödyntämiseen. Yksi suurimpia haasteita on siis ihmisten, eli käyttäjien sitoutuminen prosesseihin ja kulttuurin muutos. Tähän liittyen CMDB:n käytöllä tulisi olla selkeä päämäärä ja tavoite, jolloin se tukee muita sisäisiä prosesseja ja sen käyttöön sitoudutaan todennäköisemmin. Tämän lisäksi haasteet keskittyvät osaltaan datan tarkka ylläpito, eli sitä päivitetään liian harvoin etsintätyökalujen tai muun automaation avulla, ja luotetaan liikaa manuaalisiin tietojen syöttöihin. (Atlassian 2024.)

7 Laitteen paikkatiedon hakeminen verkkotiedon avulla

7.1 Vaatimusmäärittely laitteen paikkatiedon hakemiselle

Yritys X:llä on tarve kartoittaa organisaationsa sisällä loppukäyttäjien päätelaitteiden sijaintitietoja. Ratkaisulla on tarkoitus rikastaa CMDB-tietokannan dataa. Käytännön hyötynä on inventaarion ja vianselvityksen helpottaminen. Lisäksi nähdään päätelaitteiden käyttöaste, kun pystytään reaaliajassa seuraamaan mihin kytkimeen tai tukiasemaan laite on milläkin aikaleimalla kytkeytynyt.

Asiakkaan sisäverkko koostuu verkkokytkimistä ja langattomista tukiasemista. Käyttäjät kytkeytyvät verkkoon liittymällä joko langattomasti tukiasemaan tai kaapelilla kytkimeen.

Asiakkaalla on käytössään Clearpass-pääsynhallintajärjestelmä, jota pyritään hyödyntämään työn toteutuksessa. Käytössä oleva CMDB on ServiceNow’n tuote. Palvelimen autentikointiin käyttöön tulee OAuth2.0.

Projektin toteutus aloitetaan aina vaatimusmäärittelyllä, jotta ymmärretään asiakkaan tarve. Vaatimusmäärittelyssä tarkastellaan lähtökohtia työn toteuttamiselle, sekä mitä projektilla on tarkoitus saavuttaa.

7.2 Suunnitelma laitteen paikkatiedon hakemiselle

Asiakkaan tiedusteltua, onko ratkaisua mahdollista toteuttaa Clearpassin kautta, selvitetään vaatimusmäärittely. Vaatimusmäärittelyn ollessa selvillä siirrytään suunnittelupalavereihin.

Suunnittelupalaverissa yhdessä asiakkaan kanssa, sekä kolmannen osapuolen, joka vastaa CMDB:stä, jaetaan vastuut, sovitaan työnkulku ja aikataulu. Kolmas osapuoli vastaa ServiseNow’n osuuden toteuttamisesta sekä CMDB:n ylläpidosta. Asiakas itse vastaa tarvittavien palomuurisääntöjen avaamisesta.

Opinnäytetyö toteutetaan Clearpass-pääsynhallinnan määritysten osuudelta. Pääsynhallinnan kautta on ennestään toteutettu autentikointi ja roolijako.

Clearpassissa Radiusta hyödyntämällä saadaan välitettyä viestin avulla useita tietoja. Suunnitelman pohjalta viestiin on tarkoitus sisällyttää laitteen nimi, aikaleima, jolloin verkkoon liitytään, sekä kytkimen tai langattoman tukiaseman nimi. Yrityksen kytkimet on nimetty niiden sijainnin perusteella. Langattomat tukiasemat on nimetty numerosarjoilla, joista on mahdollista päätellä kerros ja huone, missä tukiasema rakennuksessa sijaitsee. CMDB linkittää päätelaitteen laitekortille nimen perusteella oikean kytkimen tai langattoman tukiaseman laitekortin.

Ajallisesti työhön arvioidaan kuluvan kolme tai neljä kuukautta. Työn etenemistä seurataan yhteisillä palavereilla asiakkaan ja kolmannen osapuolen kanssa. Palavereja pidetään kaksi kertaa kuukaudessa. Yhteisten palaverien ulkopuolella vastuualueen mukaan kerätään itsenäisesti tietoa, sekä kommunikoidaan tarvittaessa sähköpostin välityksellä.

Toimintasuunnitelma pitää sisällään suunnittelun itsenäisesti vastuualueen mukaan, että palavereissa, tarvittavien tietojen keruu, testaus ja tuotantoon vienti. Lopuksi toimintaperiaate dokumentoidaan ylläpidolle.

Suunnitelman tekeminen yhdessä asiakkaan ja muiden projektin osallisten kanssa on tärkeä osa prosessia. Näin varmistetaan, että on ymmärretty asiakkaan tarve. Asiakkaan on myös tärkeä kuulla ja ymmärtää, mitä käytettävässä ympäristössä on mahdollista toteuttaa. Kolmannen osapuolen kanssa on yhdessä suunniteltava, miten projektin toteutetaan, ja mitkä ovat heidän mahdolliset vaatimuksensa ja rajoitteet. Lisäksi yhteisen aikataulun laatiminen on seurantapalaverien ja projektin toteutumisen kannalta tärkeää. Projektin suunnittelu vaatiikin jokaiselta osapuolelta hyviä kommunikointi ja vuorovaikutustaitoja, jotta kaikki osapuolet tulevat ymmärretyiksi ja projektin on mahdollista onnistua.

7.3 Määritykset ja viesti järjestelmässä laitteen paikkatiedon hakemiselle

Clearpass toimii API-rajapinnan kautta. Palvelimen autentikoinnissa käytetään OAuth2:ta. Autentikoinnissa OAuth2:n käyttö perustellaan korkeammalla tietoturvalla. Lähtökohtaisesti ei ole odotettavissa rajoitteita OAuth2:n käytölle yhdistettäessä ServiseNow’n CMDB-palvelimeen.

Palvelimen määritys tapahtuu Clearpassissa käyttöliittymän kautta. Määrityksiin vaaditaan palvelimen URL, Client ID sekä Client Secret. Nämä tiedot saadaan kolmannelta osapuolelta, joka ylläpitää ServiceNow’n CMDB:tä.

Radiusta hyödynnettäessä saadaan Clearpassissa aktivoitua viesti CMDB-palvelimelle heti, kun laite kytketään verkkoon. API-rajapinnan kautta hyödynnetään http-metodia POST. POST lähettää JSON-muotoisen viestin palvelimelle heti, kun laite liitetään verkkoon.

Viestin muoto määräytyy sen mukaan, millaisen viestin CMDB pystyy vastaanottamaan ja käsittelemään. JSON valitaan yksinkertaisuuden ja aiemman kokemuksen perusteella.

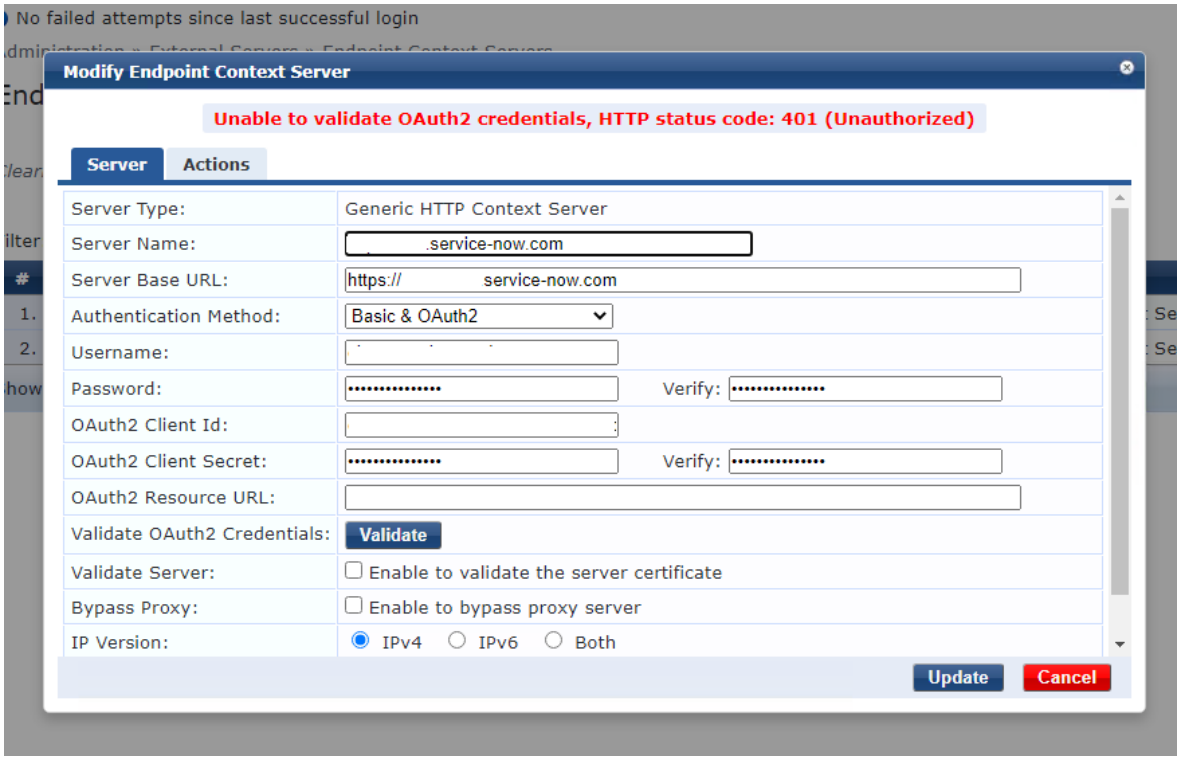
Määritykset sovitaan osana suunnitteluprosessia. Määritysten suunnittelu edellyttää, että sopijapuolet tuntevat vastuullaan olevien järjestelmien kyvykkyydet ja rajoitteet. Tässä prosessin vaiheessa on hyvä olla tiedossa, mitä tietoja vastapuolelta tarvitaan integraation toteuttamista varten.

7.4 Laitteen paikkatiedon hakemisen toteutus Clearpassissa

Toteutusprosessiin ryhdytään, kun asiakkaan sekä kolmannen osapuolen kanssa päästään yksimielisyyteen vaatimusmäärittelystä ja määrityksistä. Kolmas osapuoli lähtee toteuttamaan CMDB:n määrityksiä ServiceNow'ssa ja asiakas pitää huolen palomuurinsa osuudesta saatuaan tarvittavat tiedot IP-osoitteista ja porteista, jotka avauksessa on huomioitava.

Clearpass-järjestelmän palvelin määritysten konfiguroinnissa vaadittavat asetukset pystytään syöttämään suoraviivaisesti käyttöliittymässä. Järjestelmään syötetään kolmannen osapuolen toimittamat palvelimen URL-osoite, asiakasohjelman tunniste Client ID sekä asiakasohjelman salainen avain Client Secret.

Clearpass-järjestelmän OAuth2-autentikointimääritysten testausvaiheessa voidaan yksinkertaisesti käyttöliittymässä todeta autentikoinnin toimivuus. Validate-toiminnon avulla pystytään toteamaan, toimiiko yhteys palvelimen ja Clearpassin välillä. Tässä tapauksessa se ei kuitenkaan toimi oikein, vaan antaa virhekoodia 401, kuten nähdään kuvassa 1.



Kuva 1. Virhekoodi

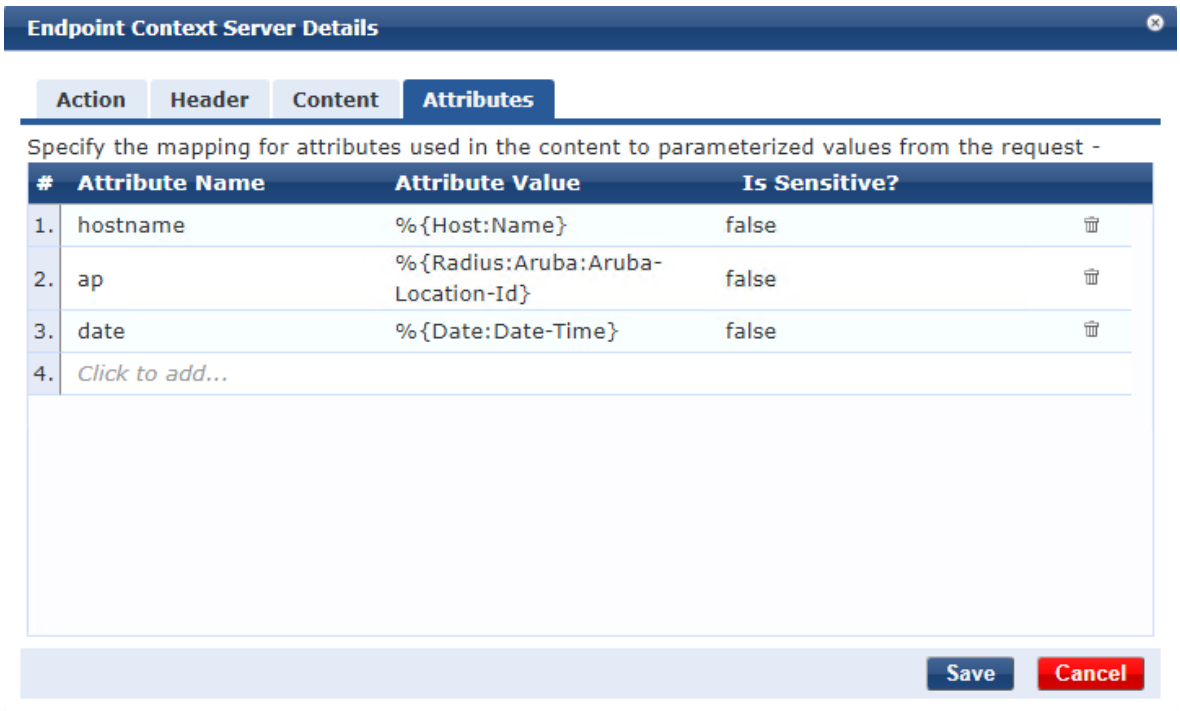
Edellä olevan kuvan mukaisesti, tässä testausvaiheessa testataan OAuth2 ja Basic yhdistelmää, saaden sama tulos kuin pelkkää OAuth 2.0 käyttämällä. Autentikointi ei siis toimi toivotulla tavalla, minkä virhekoodi kertoo. Virhekoodi 401 http-protokollassa tarkoittaa, ettei autentikointipyyntöä suoriteta loppuun, koska siitä puuttuvat pyydettyyn resurssiin

tarvittavat todennustiedot. Tässä projektissa emme kolmannen osapuolen kanssa tietojen tarkistuksesta huolimatta löytäneet syytä virhekoodille, joten asian selvitystä jatketaan yhdessä ServiceNow'n ja Clearpassin tuen kanssa. Basic on perinteisempi käyttäjätunnus ja salasana yhdistelmä.

Pääsynhallinnan kannalta on välttämätöntä määritellä säännöstö, joka selkeästi kuvailee, ketkä käyttäjät ovat oikeutettuja pääsemään verkkoon. Tämän säännöstön luominen tapahtuu käyttäen Clearpass-järjestelmän enforcement policy -toimintoja.

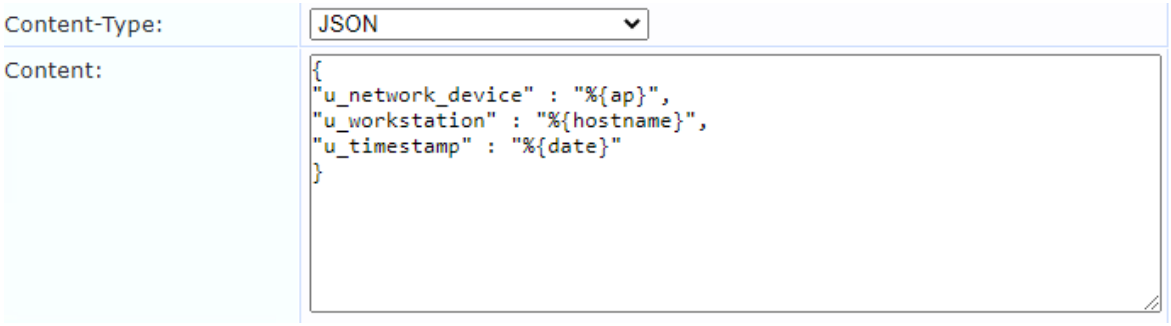
Enforcement profile -ominaisuuden avulla puolestaan määritellään tarkemmat säännöt siitä, miten verkkoon pääsy konkreettisesti tapahtuu, sekä minkälaisia lisätoimenpiteitä, kuten automaattisia ilmoituksia ServiceNow'lle, verkkoon liittymisen yhteydessä suoritetaan. Nämä määritykset varmistavat, ettei ulkopuolisilla päätelaitteilla ole mahdollista päästä verkkoon.

Palvelimelle vietävien tietojen määrittely on tehty Clearpassin käyttöjärjestelmässä yksinkertaiseksi. Clearpassiin on suoraviivaista määrittää palvelimelle vietävät tiedot. Määritykset tapahtuvat endpoint context server kohdassa. Ensin määritellään haluttu toiminne. Määrityksiin valitaan aiemmin määritelty palvelin ja autentikointimetodi. Lisäksi toiminne nimetään kuvaavasti. Tässä tapauksessa toiminne on http:n POST-metodilla viestin lähetys. Tämän jälkeen määritellään attribuutit. Kuvassa 2 on määritelty langattoman tukiaseman sijaintiedon saamiseksi toiminteelle attribuutit.



Kuva 2. Attribuutti määritykset

Attribuuttimääritykset Clearpassissa on helppo toteuttaa, koska tiedot ovat järjestelmässä valmiiksi. Käytännössä attribuutille annetaan kuvaava nimi sekä muuttujan arvo. Tämän jälkeen attribuutit sidotaan viestiin, kuten kuvassa 3.



Kuva 3. JSON-viesti

JSON-viestin rakenteeseen vaikuttaa CMDB:n kyky käsitellä viesti. Tässä tapauksessa viestin sisältämät muuttujien nimeämiset tehdään kolmannen osapuolen ilmoittamalla tavalla, jotta ServiceNow'n kyvykkyys käsitellä viestin sisältö oikein saadaan varmennettua. Vastaavat attribuuttien määritykset ja viesti tehdään myös kiinteän verkon toiminteelle, sillä kyseessä on kokonaan erillinen toiminne.

7.5 Laitteen paikkatiedon hakemisen testaus ja tuotantoon vienti

Clearpassin osalta testaus aloitetaan määrittelemällä säännöstöt yhdelle työasemalle testausta varten, jolloin se kykenee liittymään sekä langattomaan että kiinteään verkkoon käyttäen laitteen MAC-osoitetta tunnistautumiseen. Lisäksi testauksessa vaaditaan palvelin määritykset.

Testausvaiheessa tärkeää on varmistaa yhteyden toimivuus Clearpassin ja ServiceNow'n välillä. Alkuvaiheessa todettu haaste autentikoinnin suhteen vaatii järjestelmien teknisen tuen kanssa asian ratkaisua, joten tässä tapauksessa parhaaksi tavaksi todentaa yhteys testausvaiheessa on käyttää autentikointiin yksinkertaista käyttäjätunnuksen ja salasanan yhdistelmää vianrajauksen näkökulmasta, sekä aikataulullisista syistä. Näin ollen saadaan todennettua, että yhteys Clearpassin ja palvelimen välillä toimii moitteettomasti. Onnistuneesti lähetetty viesti CMDB:lle vahvistaa, että järjestelmä kykenee vastaanottamaan, käsittelemään ja tallentamaan tiedot asianmukaisesti.

Projektin toisessa testausvaiheessa luodaan tyypillinen käyttötilanne. Käyttäjä liittyy ensin kiinteään verkkoon kytkimen avulla. Tämän jälkeen käyttäjä kytkeytyy irti kiinteästä sisäverkosta ja liittyy samassa sijainnissa langattomaan verkkoon. Jonkin ajan kuluttua käyttäjä siirtyy toiseen sijaintiin, jossa hän liittyy langattomaan verkkoon.

Aluksi, kun työasema liitettään kiinteään verkkoon, kerätään tiedot liityntäpisteestä, johon laite kytketään. Tämän jälkeen, siirtyessä langattomaan verkkoon, saadaan vastaavasti tietoja tukiasemasta, johon yhteys muodostetaan. Käyttäjän myöhemmin vaihtaessa fyysistä sijaintiaan ja liittyessään jälleen langattomaan verkkoon, CMDB päivittää tiedot viimeisimmästä tukiasemasta, johon päätelaite on ollut yhteydessä viimeisimpänä. Tämä kattava testaus ja tiedonkeruu osoittivat, että pääsynhallintajärjestelmä on kykenevä seuraamaan ja tallentamaan verkkoyhteyksien tietoja reaaliaikaisesti, mikä on olennaista verkon turvallisuuden ja hallittavuuden kannalta.

Testausvaihe on tärkeä osa prosessia ennen projektin tuotantoon viemistä. Sen tarkoitus on osoittaa, että integraatio toimii toivotulla tavalla. On tärkeää pystyä toteamaan, että tieto siirtyy oikeaan paikkaan, järjestelmien välillä yhteys toimii ja järjestelmät pystyvät käsittelemään saamansa tiedot oikein. Mahdolliset virhetilanteet ovat käyttäjäystävällisemäpää, taloudellisempaa ja tietoturvallisempaa korjata ennen projektin tuotantoon vientiä. Kun virhetilanteet on korjattu tai ratkaistu muulla tavoin ja projekti todetaan testausvaiheessa toimivaksi, on se valmis tuotantoon vietäväksi. Testausvaiheessa pystytään järjestelmien toimivuuden lisäksi todentamaan, ettei verkossa oleva toimintaa rajoittavia tekijöitä, kuten esimerkiksi palomuurilla tapahtuvia rajoitteita.

Lopuksi projekti dokumentoidaan ylläpitoa ja jatkokehitystä varten. Tuotantoon viennillä tarkoitetaan käytännössä sitä, että testaukseen rakennettu, toimivaksi testattu toteutus, siirretään asiakkaan käytössä olevaan ympäristöön.

8 Yhteenveto ja pohdinta

Opinnäytetyön toteutus lähti Yritys X:n tarpeesta kartoittaa loppukäyttäjien päätelaitteiden paikkatietoja organisaatiossa. Päätavoite oli rikastaa CMDB-tietokantaa, tarkoituksena oli suoraviivaistaa päätelaitteiden inventaariota sekä verkon vianselvitystä. Lisäksi tavoitteena oli nähdä päätelaitteiden käyttöaste reaaliajassa.

Asiakkaan sisäverkko koostuu kytkimistä ja langattomista tukiasemista. Käyttäjät liittyvät sisäverkkoon kytkinten kautta kaapelilla tai langattomasti tukiasemiin. Asiakkaalla oli ennestään käytössä Clearpass-pääsynhallintajärjestelmä. CMDB:nä käyttöön tuli ServiceNow'n tuote, jonka toteutuksesta ja ylläpidosta vastaa kolmas osapuoli.

Projekti aloitettiin vaatimusmäärittelyllä ja suunnitelmalla yhdessä asiakkaan ja kolmannen osapuolen kanssa. Clearpassin kautta toteutettiin tietojen keruu. Tiedot lähetettiin palvelimelle viestinä. Kerättävät tiedot olivat päätelaitteen nimi, kytkimen tai tukiaseman nimi, johon laite on yhdistetty, sekä aikaleima. Clearpass toimii API-rajapinnassa, joten JSON-viestin lähettämiseen CMDB:lle käytettiin http:n POST-metodia laitteen yhdistyessä verkkoon. Palvelimen autentikointiin käytettiin OAuth 2.0.

Toteutusprosessi aloitettiin heti, kun vaatimusmäärittely ja suunnitelma oli tehty. Toteutus määritettiin testiympäristöön. Tavoitteena oli osoittaa palvelimen ja pääsynhallintajärjestelmän välisen yhteyden toimivuus, sekä CMDB:n kyky käsitellä viesti. Testauksessa luotiin tyypillisiä käyttötilanteita ja varmistettiin, että järjestelmä pystyy toimimaan tavoitteen mukaisesti, eli seuraamaan ja välittämään CMDB:lle päätelaitteiden verkkotietoja reaaliajassa.

Projekti vastasi tavoitteita. Päätelaitteen liittyessä verkkoon saa CMDB tiedon Clearpassista kytkimestä tai tukiasemasta, johon käyttäjä on liittynyt aikaleiman kera. Haasteena toteutuksessa oli palvelimen autentikointi, johon tarvittiin järjestelmien omien teknisten tukien selvitystä. Haasteita autentikoinnin suhteen ei osattu odottaa, ja asian selvitys hidasti projektin loppuun saattamista, eikä suunnitellussa aikataulussa pysytty.

Pääsynhallintajärjestelmän hyödyntämisellä CMDB-tietokannan rikastamiseen on organisaatioille useita hyötyjä. Laitteen paikkatietojen kartoittaminen tekee inventaarioista ja hallinnasta tehokkaampaa, koska pystytään seuraamaan päätelaitteiden todellista käyttöastetta ja sijaintia. Paikkatiedon kartoittaminen nopeuttaa vianselvitystä, mikäli ongelmia on useilla loppukäyttäjillä, nähdään aikaleimat ja sijainnit ja voidaan sitä kautta poissulkea tiettyjä vianselvityksen vaiheita, kuten yksittäisen päätelaitteen vika. Lisäksi käyttöasteen optimoinnin avulla on mahdollista nähdä verkon ruuhkaisuus tiettyinä ajankohtina, mikä helpottaa resurssien optimointia ja verkon kapasiteetin huomioimista ruuhkahuippujen aikana. Nämä laitteen paikkatiedon tallentamisen hyödyt näkyvät taloudellisena hyötynä sekä

parantuneena tietoturvallisuutena. Kustannussäästöt organisaatiolle tulevat tehokkaan inventaarion ja käyttöasteen seurannan avulla. Tällöin voidaan vähentää turhia laitehankintoja ja ylläpitokustannuksia. Parempi käyttöaste ja nopeutunut vianselvitys pienentävät liiketoiminnan häiriöitä, mikä parantaa tehokkuutta. Paikkatiedon hakeminen olemassa olevan pääsynhallintajärjestelmän parantaa turvallisuutta, kun pystytään päätelaitteen hallinnan lisäksi näkemään, milloin ja missä se on viimeksi liittynyt verkkoon. Yhteenvetona voidaankin todeta, että edellä mainittujen tekijöiden ja hyötyjen perusteella yritys voi laitteen paikkatietojen avulla parantaa toimintansa tehokkuutta, turvallisuutta ja saavuttaa kustannussäästöjä.

Yrityksille paikkatiedon ja käyttöasteen avulla saavutettu liiketoiminnan tehokkuus näkyy taloudellisena hyötynä. Maailmanlaajuisesti tarkasteltuna turhien laitehankintojen välttäminen on ympäristön kannalta tärkeää globaalien ongelmien, kuten komponenttipulan vuoksi on tärkeää. Lisäksi teknologian kehittyessä pääsynhallintajärjestelmän avulla voidaan olettaa mahdollisuuksien ja tarpeiden erilaisten tietojen reaaliaikaiselle tiedonkeruulle kasvavan. Silloin tämänkaltaiset integraatiot ovat tarpeen, jotta tieto saadaan säilöttyä asianmukaisesti. Lisäksi toteutus voidaan säilyttää samankaltaisena lisäämällä lähetettävään viestiin uusi tieto omana rivinään. Paikkatiedon reaaliaikainen tiedonkeruu pääsynhallinnan avulla tuo monia mahdollisuuksia eri aloilla kohti tehokkaampaa ja kestävämpää maailmaa.

Lähteet

Atlassian. 2024. What is a configuration management database (CMDB)? Viitattu 12.2.2024. Saatavissa https://www.atlassian.com/itsm/it-asset-management/cmdb#:~:text=CMDB%20stands%20for%20configuration%20management,%2C%20facilities%2C%20and%20even%20personnel.

BasuMallick, C. 2022. What is Mesh network? Meaning, types working, and applications in 2022. Spiceworks. Viitattu 1.4.2024. Saatavissa https://www.spiceworks.com/tech/networking/articles/what-is-mesh-network/

Cisco. 2024. What is a LAN? Viitattu 12.3.2024. Saatavissa https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html

DNS Stuff. 2019. What is network topology? Best guide to types and diagrams. Viitattu 13.4.2024. Saatavissa https://www.dnsstuff.com/what-is-network-topology

Euroopan Unioni. 2022. 5G-verkot EU:ssa: viiveitä käyttöönotossa ja ratkaisemattomia turvallisuusongelmia. Viitattu 17.3.2024. Saatavissa https://op.europa.eu/webpub/eca/special-reports/security-5g-networks-03-2022/fi/#chapter0

Fortinet. 2022. What is Trancmission Protocol Control Protocol TCP/IP? Viitattu 1.4.2024. Saatavissa https://www.fortinet.com/resources/cyberglossary/tcp-ip

Gittlen, S. & Rosencrance L. 2021. What is identity and access management? Guide to IAM. TechTarget. Viitattu 26.3.2024. Saatavissa https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

Hakala, M. & Vainio, M. 2002. Tietoverkon rakentaminen. Porvoo: Docendo Finland Oy.

Hermans, J. 2020. Moderni todentaminen (Modern Authentication) – Pelkkä käyttäjätunnus ja salasana ei enää riitä. Rauhala. Viitattu 26.3.2024. Saatavissa https://www.rauhala.fi/blog/moderni-todentaminen-modern-authentication

Hewlett Packard Enterprise. 2024. What is WLAN? Viitattu 8.1.2024. Saatavissa https://www.arubanetworks.com/faq/what-is-wlan/#:~:text=Wi%2DFi%20networks%20are%20a,that%20is%20most%20widely%20used.

Hewlett Packard Enterprise. 2018. Wired Policy Enforcement – Solution Guide, s. 6-8. Viitattu 11.11.2023. Saatavissa https://support.hpe.com/hpesc/public/docDisplay?docId=a00091135en_us

Homenet Howto. 2019. Switches. Viitattu 8.1.2024. Saatavissa https://www.homenethowto.com/switching/switches/

Jokinen, S. 2019. Mitä jokaisen toimitusjohtajan tulee tietää tietoturvasta? Triutvare. Viitattu 16.3.2024. Saatavissa https://materiaalit.triuvare.fi/artikkelit/mita-jokaisen-toimitusjohtajan-tulee-tietaa-tietoturvasta

Järvinen, P. 2022. Yrityksen tietoturvaopas. Viro: Helsingin seudun kauppakamari. Viitattu 12.3.2024. Saatavissa https://kauppakamaritieto-fi.ezproxy.saimia.fi/ammattikirjasto/teos/yrityksen-tietoturvaopas-2022#kohta:Yrityksen((20)tietoturvaopas

Kaario, K. 2002. TCP/IP-verkot. Porvoo: Docendo Finland Oy.

Karvinen, R. 2022. Autentikointi ja auktorisointi mikropalveluarkkitehtuurissa. Atostek. Viitattu 26.2.2024. Saatavissa https://atostek.com/autentikointi-ja-auktorisointi-mikropalveluarkkitehtuurissa/

Kanade, V. 2022. What is the OSI model? Definition. layers, and importance. Spiceworks. Viitattu 1.4.2024. Saatavissa https://www.spiceworks.com/tech/networking/articles/what-is-osi-model/

Kataja, J. 2017. SSL-salaus: 3 syytä miksi jokaisen sivuston tulisi käyttää salausta. Zoner. Viitattu 17.3.2024. Saatavissa https://www.zoner.fi/tietoturva/ssl-salaus/

Kauppinen, A. 2021. Uusi 5G-teknologia tekee arjesta turvallisempaa ja toimivampaa. Erillisverkot. Viitattu 26.3.2024. Saatavissa https://www.erillisverkot.fi/uusi-5g-teknologia-tekee-arjesta-turvallisempaa-ja-toimivampaa/

Kyberturvallisuuskeskus. 2014. Langattomasti, mutta turvallisesti. Viitattu 17.3.2024. Saatavissa https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Kyberturvallisuuskeskus. 2023. Ohje paikallisten matkaviestinverkkojen kyberturvallisuudesta ja riskienhallinnasta. Viitattu 16.2.2024. Saatavissa https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje%20paikallisten%20matkaviestinverkkojen%20kyberturvallisuudesta%20ja%20riskienhallinnasta_final.pdf

Kyberturvallisuuskeskus. 2020. Tietoturva. Viitattu 22.2.2024. Saatavissa https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Laaksoharju, S. 2021. Tarkastelussa 8 erilaista haittaohjelmaa. Itewiki. Viitattu 26.3.2024. Saatavissa https://www.itewiki.fi/blog/2021/02/haittaohjelmat-pahkinankuoressa-tunnistatko-erilaiset-haittaohjelmat-toisistaan/

Laki sähköisen viestinnän tietosuojalain muuttamisesta 365/2011

Lorentsen, M. 2023. Mikä on palomuuri? Kotimikro. Viitattu 17.3.2024. Saatavissa https://kotimikro.fi/tietoturva/mika-on-palomuuri

Montgomery, J. 2020. CMDB (configuration management database). TechTarget. Viitattu 21.12.2023. Saatavissa https://www.techtarget.com/searchdatacenter/definition/configuration-management-database

Muelander, J. 2021. Mitä ovat valmistajakohtaiset rengastopologiat automaatioverkoissa? DigiKey. Viitattu 4.3.2024. Saatavissa https://www.digikey.fi/fi/articles/what-are-proprietary-ring-topologies-in-automation-networks

Mukaddam, A. 2020. Clearpass tiny bite 7 – Clearpass guest social login with Azure AD (Part 1). Why-Fi++. Viitattu 1.4.2024. Saatavissa

Netgear. 2022. Mikä langaton tukiasema on? Viitattu 12.2.2024. Saatavissa https://kb.netgear.com/fi/235/Mik%C3%A4-langaton-tukiasema-on?language=fi

Niemi, Kalle. Identiteetin ja pääsynhallinta IAM. Itewiki. Viitattu 12.3.2024. Saatavissa https://www.itewiki.fi/opas/kayttajahallinta-iam/

Paananen, J. 2005. Tietotekniikan peruskirja. Porvoo: Docendo Finland Oy.

Perttunen, A. 2023. Tietoturvakoulutuksen merkitys organisaatiolle – vinkkejä ja käytännön lähestymistapoja henkilöstön tietoturvakoulutukseen. Micromagic. Viitattu 26.3.2024. Saatavissa https://micromagic.fi/story/tietoturvakoulutuksen-merkitys-organisaatioille/

Rasmussen, H. 2021. Valitse langattoman verkon taajuudeksi 2,4 tai 5 GHz. Kotimikro. Viitattu 12.2.2024. Saatavissa https://kotimikro.fi/internet/verkko/valitse-langattoman-verkon-taajuudeksi-2-4-tai-5-ghz

Riihikallio, P. 2017. WLAN, Wi-Fi vai 802.11 – mikä ero? Metis. Viitattu 4.3.2024. Saatavissa https://metis.fi/fi/2017/01/wlan-wi-fi-wifi-ero/

ServiceNow. 2023. What is a configuration management database (CMDB)? Viitattu 21.12.2023. Saatavissa https://www.servicenow.com/products/it-operations-management/what-is-cmdb.html

Solla, K. 2017. Digitreenit: Mikä ihmeen VPN? Se suojaa nettiyhteyttäsi avoimessa verkossa. Yle. Viitattu 16.3.2024. Saatavissa https://yle.fi/aihe/artikkeli/2017/09/06/digitreenit-mika-ihmeen-vpn-se-suojaa-nettiyhteyttasi-avoimessa-verkossa

Sähköisen viestinnän tietosuojalaki 516/2004

Tablan, P. 2022. What is Aruba ClearPass? How does it protect your network? Kelser. Viitattu 29.11.2023. Saatavissa https://www.kelsercorp.com/blog/what-is-aruba-clearpass-and-how-does-it-protect-your-network#:~:text=Aruba%20ClearPass%20is%20a%20policy,compliance%20with%20your%20security%20policies.

Väylävirasto. 2019. 5 G Väyläviraston toiminnassa. Väyläviraston julkaisuja 52/2019. Viitattu 4.3.2024. Saatavissa https://www.traficom.fi/sites/default/files/media/file/5g_vaylaviraston_toiminnassa.pdf

Your Europe. 2022. Yleinen tietosuoja-asetus. Viitattu 3.4.2024. Saatavissa https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm