jamk.fi

VLAN-verkkojen automatisointi

Juho Tauriainen

Opinnäytetyö
Toukokuu 2021
Tekniikan ala
Tieto- ja viestintätekniikka, insinööri (AMK)

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Tauriainen Juho	Opinnäytetyö, AMK	toukokuu 2021
	Sivumäärä 41	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
VLAN-verkkojen automatisointi

Tutkinto-ohjelma
Tieto- ja viestintätekniikka, insinööri (AMK)

Työn ohjaaja(t)
Sampo Kotikoski, Jarmo Nevala

Toimeksiantaja(t)
Jyväskylän kaupunki, Tietohallinto

Tiivistelmä

Organisaatioiden ja yritysten tietoverkon jatkuvassa kasvussa nähdään haasteita kyberturvallisuuden ja laitteiden ylläpidon hallinnoinnissa. Verkon täytyy olla jatkuvasti saatavilla ja sen täytyy vastata nopeasti, sekä olla jatkuvasti valmis muutoksille. Tätä varten markkinoilla on lukuisia järjestelmiä ylläpitämään verkon toimivuutta. Tämän opinnäytetyön toimeksiantajana toimi Jyväskylän kaupungin Tietohallinto. Jyväskylän kaupungin Tietohallinnolla on vastuullaan tuhansia laitteita ja näiden hallintaan vaaditaan monenlaisia työkaluja. Aruba ClearPass-järjestelmän käyttöönotolla ja testauksella haluttiin helpottaa ja automatisoida kohdeverkon kytkimien konfigurointia ja parantaa kyberturvallisuutta. Aruba ClearPass-järjestelmä otettiin käyttöön kaupungin virtuaalipalvelimelle askel kerrallaan Aruban, työkavereiden ja verkon ohjeiden mukaan. Käyttöönoton aikana päädyttiin monen tavan tarjonnasta laitekohtaiseen tunnistukseen. ClearPass-järjestelmässä määritettiin käytäntöjä, joiden mukaan se tunnisti laitteet ja ohjasi ne oikeaan verkkoon. AD:hen lisättiin tietokoneille koneryhmät, jonka avulla koneet päätyvät oikeaan verkkoon tunnistauduttuaan ClearPass-järjestelmässä.

Työn tavoitteet testauksen aikana toteutui suunnitellulla tavalla. Kannettavat päätyivät oikeaan verkkoon koneryhmän mukaan ja vieras laite päätyi asiakasverkkoon. Tämä säästää tietohallinnon työntekijöiltä paljon aikaa, kun ei tarvitse enää konfiguroida kytkimiä uudelleen laitteiden vaihtaessa paikkaa.

Tietoverkon toiminnan automatisointi on nykyaikaista ja se tulee tulevaisuudessa olemaan yleisempää sen järjestelmällisyyden ja monipuolisuuden takia. Verkot kasvavat niin suuriksi ja niiden ylläpito tulee olemaan aina vain hankalampaa, jos tämän kaltaisia järjestelmiä ei olisi olemassa.

Avainsanat (asiasanat)
Aruba ClearPass, IEEE 802.1X, VLAN

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Tauriainen Juho	Bachelor's thesis	April 2021
		Language of publication: Finnish
	Number of pages: 41	Permission for web publication: x

Title of publication
Automatization of VLANs

Degree programme
Bachelor of engineering, information technology

Supervisor(s)
Kotikoski Sampo, Jarmo Nevala

Assigned by
City of Jyväskylä, Tietohallinto

Abstract

The continuous growth of the data network of organizations and companies sees challenges in managing cybersecurity and equipment maintenance. The network must be constantly available and responsive all the time as well as be constantly ready for change. Because of this there are numerous systems on the market to maintain network functionality. Thesis was assigned by City of Jyväskylä's Tietohallinto. The City of Jyväskylä's Tietohallinto is responsible for thousands of devices and a variety of tools are required to manage them. The implementation and testing of the Aruba ClearPass system was intended to facilitate and automate the configuration of the switches in the target network and to improve information security. The Aruba ClearPass system was deployed to the city's virtual server step by step according to Aruba, co-workers, and network research instructions. During deployment, many options were available, but device-specific identification was concluded. Policies were assigned to ClearPass in order to identify devices and route them to the correct network. Computer groups were added to the AD, allowing the machines to end up on the right network after being authenticated in ClearPass.

The objectives of the work during the testing were achieved as planned. The laptops ended up on the right network according to the machine group and the foreign device ended up on the guest network. This saves time from Tietohallinto's employees when they no longer have to reconfigure switches when devices change locations.

The automation of the operation of a data network is modern and it will be more common in the future due to its systematicity and versatility. Networks will grow so large that they will be more difficult to maintain if such systems like ClearPass do not exist.

Keywords/tags (subjects)
Aruba ClearPass, IEEE 802.1X, VLAN

Miscellaneous (Confidential information)

Sisältö

Kuviot

Lyhenteet

AAA	Authentication, Authorization ja Accounting. Protokolla käyttäjien todentamiseen, valtuutusten antamiseen ja käytön seurantaan tietoverkossa.
ACL	Access Control List. Pääsylista, jolla määritellään, päästetäänkö paketti läpi vai ei.
ADSL	Asymmetric Digital Subscriber Line. Verkkokytkentätekniikka
API	Application Programming Interface. Ohjelmointirajapinta, jonka avulla eri ohjelmat voivat vaihtaa tietoja keskenään.
EAP	Extensible Authentication Protocol. Käyttäjien tunnistusportokolla.
GUI	Graphical User Interface. Graafinen käyttöliittymä.
HP	Hewlett Packard Enterprise. Yritys, joka tarjoaa muille yrityksille palvelimia, tallennusjärjestelmiä, verkkolaitteita sekä ohjelmistoja ja palveluja.
IP	Internet Protocol. Yleinen protokolla, joka kuljettaa IP-tietoliikennepaketteja.
LAN	Local Area Network. Lähiverkko.
LDAP	Lightweight Directory Access Protocol. Protokolla hakemistopalveluiden käyttöön.
MPLS	Multiprotocol Label Switching. IP-pakettien kuljetusmenetelmä, jossa paketit kuljetetaan määriteltyjen yhteyksien ylitse nopean runkoverkon solmujen kautta.

QoS	Quality of Service. Tietoliikenteen luokittelu ja priorisointi termi.
TLS	Transport Layer Security. Protokolla, jonka avulla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.
VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko.
VMWare	Ohjelmisto virtuaalitietokoneiden luontiin ja ajamiseen.
VoIP	Voice over Internet Protocol. Tekniikka, jonka avulla ääntä voidaan siirtää reaaliaikaisesti Internetin avulla.
WLAN	Wireless Local Area Network. Langaton Lähiverkko.

1 Johdanto

Tietoverkkojen toimivuus ja nopeus nousevat jatkuvasti huomion kohteeksi, kun verkot jatkuvasti kasvavat ja tuottavat lisää työtä siitä vastaaville organisaatioille ja yrityksille. Päätelaitteita lisääntyy ja niitä tulee koko ajan uusia ja erilaisia, tämä tuo myös lisää haasteita tieto- ja kyberturvallisuuteen ja laitteiden yhteensopivuuksiin. Kehittynyt tekniikka tuo myös mukanaan erilaisia ratkaisuja, joiden avulla on helpompi ylläpitää tätä jatkuvasti kasvavaa ympäristöä.

Tämän opinnäytetyön tarkoituksena oli helpottaa kohdeverkon reunakytkimien konfigurointia ja parantaa tietoturvaa sekä kyberturvallisuutta yhdessä Aruba ClearPass-järjestelmän kanssa. Opinnäytetyö pitää sisällään ClearPass-järjestelmän käyttöönoton ja sen asettamista verkkoon. Opinnäytteen toimeksiantajana toimi Jyväskylän kaupungin Tietohallinto, joka vastaa kaupungin toimipisteiden päätelaitteiden ja verkkojen toimivuudesta. Jyväskylän kaupungin toimipisteitä ovat esimerkiksi sosiaali- ja terveyspalvelut, koulut ja päiväkodit.

1.1 Tutkimusasetelma

Tässä opinnäytetyössä käytettiin kvalitatiivista tutkimusotetta ja tutkimusmenetelmä oli konstruktiivinen. Kvalitatiivisella eli laadullisella tutkimuksella haetaan pääsääntöisesti laadullisia tuloksia, jossa pohjaudutaan eri näkökulmiin tutkimuksen toteutuksessa. Laadullisessa tutkimuksessa tärkeimpänä tekijänä on tehdä ilmiöstä ymmärrettävä, eli kokonaiskuva ja syvempi käsitys ilmiöstä täytyy olla selvillä. (Weselius, H. 2017.)

Konstruktiivinen tutkimusmenetelmä kulkee hyvin yhdessä laadullisen tutkimuksen kanssa, koska konstruktiivisessa menetelmässä haetaan suunnittelua, käsitteellistä mallintamista, mallien toteutusta ja testaamista. Sillä haetaan reaalimaailman ongelmaan ratkaisua suoraviivaisesti, tutkimalla teoriaa syvällisesti käytännöllistä tietoa hankkimalla kehittämisen kohteesta. Teorian tutkimisen jälkeen laaditaan ratkaisuja,

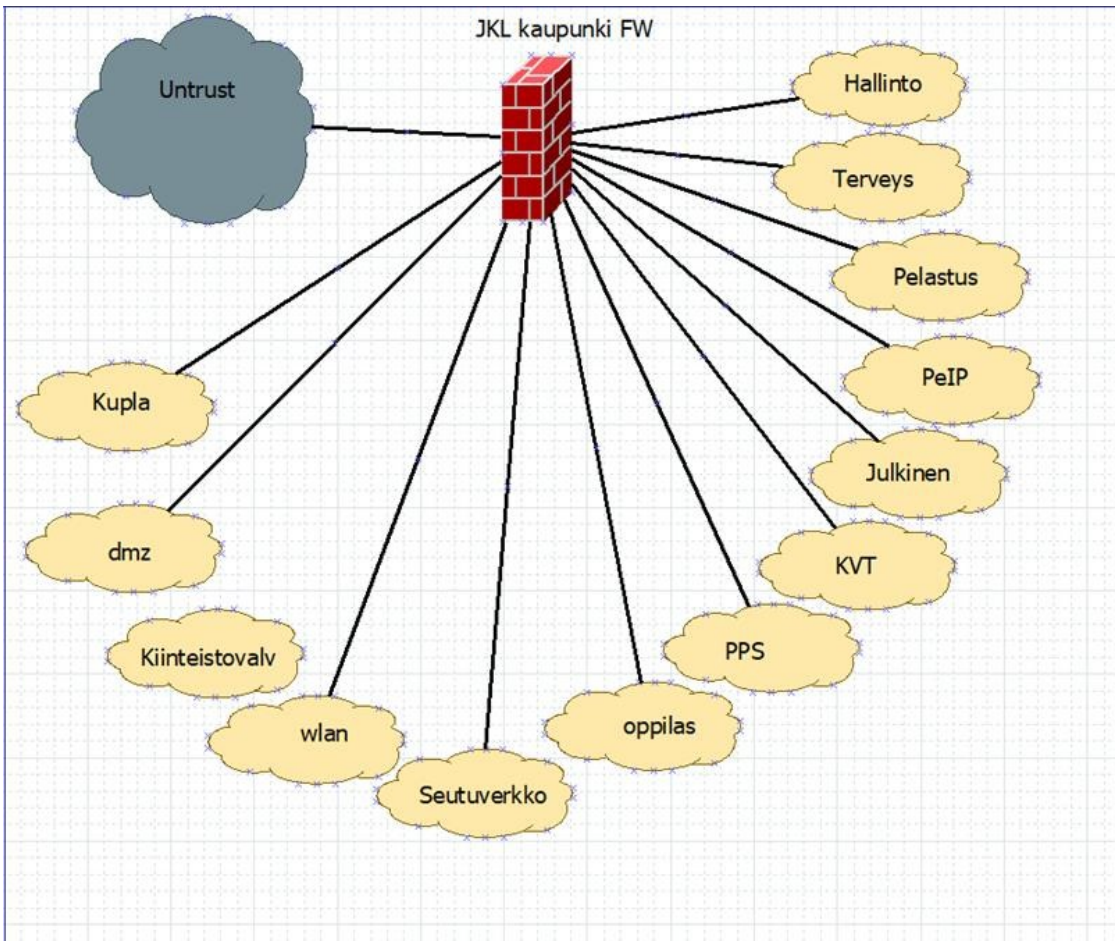
niitä testataan ja esitetään ongelma ratkaistuksi. (Lukka, K. 2001.) Opinnäytetyön tarkoituksesta saatiin kehitettyä tutkimuskysymys, joka on: Voidaanko kohdeverkon reunakytkimien konfigurointia ja kyberturvallisuutta parantaa Aruba ClearPass-järjestelmän avulla?

2 Ympäristön nykytilanne ja ongelmat

Jyväskylän Tietohallinto vastaa kaupungin kiinteiden ja langattomien verkkojen suunnittelusta ja ylläpidosta. Eri toimipaikkojen kiinteät verkot tarjoavat pääsyn kaupungin verkkoon ja sen palveluihin. Toimipaikkojen verkkonopeudet vaihtelevat työasemien ja laitteiden/kuidun saatavuuden mukaan 10Mb/s ADSL-liittymistä 10GB/s kuituliittymiin. Jossain paikoissa saattaa olla vielä kahden ja neljän Mb/s liittymiä käytössä kiinteistöpuolen laitteille kuten rikoshälytin tms. Kaupungin konesalin yhteys on kahdennettu kahta kautta kahteen konesaliin, josta menee kaksi kuitua konesalien välillä 10GB/s yhteydellä.

Verkkoyhteydet toimipisteisiin tilataan tietohallinnon kautta, jolloin operaattori toimittaa verkkoyhteyden toimipisteisiin. Operaattorin osuus rajoittuu verkko-operaattorin reitittimeen ja toimipisteen kytkimistä vastaa Tietohallinto. Verkkoyhteys toimipisteessä toteutetaan MPLS-verkkona, eli toimipisteeseen tuodaan asiakkaiden tarvitsemat VLAN:it.

Kaupungilla on käytössä 13 eri VLAN:ia, jotka ovat palomuurissa ja ne ovat Hallinto, Terveys, Pelastus, PeIP, Julkinen, KVT, PPS, Oppilas, Seutuverkko, Wlan, Kiineistövalvonta, dmz ja Kupla. Konesaleissa on myös lisänä muita VLAN:ja, jotka on paikallisesti laitettu tai sitten VLAN-reititettyjä. (Kuvio 1)



Kuvio 1 Eri VLAN:it

2.1 Ongelmat

Nykytilanteessa uusien laitteiden lisääminen verkkoon tuottaa paljon työtä minkä pystyisi juuri tämän Aruba ClearPass järjestelmän avulla ohittamaan. Esimerkiksi, kun halutaan lisätä uusi tietokone verkkoon täytyy se portti kytkimestä konfiguroida käsin oikeaan VLAN:iin mihin verkkoon kone halutaan liittää. Konfigurointi lisää paljon työtä varsinkin verkkopuolella, kun esimerkiksi uusia kouluja, päiväkoteja ja sairaaloita valmistuu. Konfiguraation automatisointi ClearPassin avulla helpottaisi myös sitä, kun työntekijät muuttavat/vaihtavat huoneita, paikkoja tai toimipisteitä keskenään niin IT-tukea ei tarvitsisi, kun jokainen portti käy kaikille laitteille. Jyväskylän Kaupungin verkossa on tällä hetkellä käytössä Ciscon langattomia tukiasemia, seka LAN-verkossa HP:n ja Ciscon kytkimiä ja reitittimiä.

Verkon jatkuva kasvaminen ja laitteiden lisääntyminen vaikeuttaa verkon hallintaa, koska esimerkiksi policyjen määrittäminen fyysisiin portteihin ja eri VLAN verkkojen hallinta liikenteen tyypin mukaan on työlästä. Verkon kasvamisen takia IP-aliverkot ovat lisääntyneet ja sen myötä on tullut valtavasti eri VLAN:ja, sekä pääsylistojen (ACL) ylläpitö on haastavaa pitää tasaisena VLAN rajapinnoissa. Haastavan siitä tekee se, kun yhtä policyä muutetaan johtaa se siihen, että muitakin policyjä pitää mahdollisesti muuttaa odottamattomien syiden takia.

Tavoitteena onkin päästä eroon fyysiestä tavasta, jossa policyjä sidotaan VLAN rajapintoihin ja portteihin. Tavoitellaan käyttäjä- ja laitekeskeistä mallia, jossa policyt seuraavat käyttäjiä riippumatta siitä miten he yhteyden verkkoon muodostavat. Tämä auttaa siinä, että ei ole enään tarvetta konfiguroida ennalta VLAN:ja, pääsylistoja ja QoS:seja tiettyihin portteihin vaan, kun käyttäjät yhdistävät laitteensa verkkoon niin policyt ladataan verkon liityntäkerrokselle ja siitä käyttäjät saavat oikeat oikeudet itselleen.

3 Pääsynhallinta

NAC eli Network Access Control on ratkaisu verkon käyttöoikeuksien hallintaan, jonka ideana on suojata verkkoa luvattomilta laitteilta ja käyttäjiltä. Suojaus toteutetaan yleensä verkon reunakytkimillä ja käyttöoikeuspalvelimilla, jotka vahvistavat verkon käyttöoikeudet verkon reunalla. (Network Access Control. N.d.)

Tällä hetkellä laitteille annetaan sertifikaatit, jotta ne saadaan liitettyä kaupungin verkkoon, joka ei ole niin moderni tapa. Modernit NAC-ratkaisut ovat taas monipuolisempia ja helpompia, kun ne käyttävät roolipohjaista politiikkaa, jolla saadaan käyttöön dynaaminen segmentointi. Dynaaminen segmentointi tarkoittaa siis sitä, että asiakkaiden laitteet voidaan tunnistaa karkeammin ja paremmin jo verkon reunoilla, jossa niille voidaan samalla määrittää käyttöoikeudet välittämättä käyttäjän tai laitteiden rooleista. (Configuring NAC. N.d) Modernina NAC-ratkaisuna toimii esimerkiksi Aruba ClearPass, joka tuo myös lisänä verkon tarkastelua, eli se kerää tietoa verkosta, missä ja miten laitteet ja käyttäjät kirjautuvat verkkoon. Moderni NAC kerää

myös reaaliaikaista tietoa verkosta ja sen käyttäjistä, jos käyttäjät tekevät epänormaaleja muutoksia, esimerkiksi koittavat kirjautuvat monelle eri palvelimelle tai lataavat palvelimilta paljon tietoa itselleen. Tiedon keruun avulla voidaan tilastoida verkon toimintaa, suunnitella kapasiteetteja eri tilanteita varten ja tutkia epänormaaleja tapauksia. Modernit NAC ratkaisut myös lisäävät verkon tieto- ja kyberturvallisuutta monella tasolla. Esimerkiksi meillä tietohallinnon työntekijöillä on erilaiset oikeudet tietokoneilla ja käyttäjillä, kun taas rakennuspuolen tietokoneilla ja käyttäjillä. Sitten taas tulostimillakin on omat oikeutensa verkkoon. (About the ClearPass Access Management System. N.d)

3.1 Aruba ClearPass (Roolipohjainen pääsynhallinta)

Aruba ClearPass on roolipohjainen pääsynhallinta alusta, jonka avulla tunnistetaan kuka, millä ja mistä laitteella verkkoon koitetaan muodostaa yhteyttä, sekä mitkä laitteet ovat käytössä. Vain valtuutetuille ja todennetuille käyttäjille ja laitteille sallitaan yhteys verkkoon. Järjestelmän avulla voidaan suorittaa päätelaitteiden eli esimerkiksi tietokoneen RADIUS-todennus tai IEEE 802.1X-standardin mukainen porttikohtainen todennus. (Data sheet Aruba Clearpass Policy Manager. 2021.)

ClearPass ei vaadi laitteille asennettavaa sovellusta ja se tuo myös ison muutoksen kyberturvallisuuteen, koska se seuraa ja reagoi tietoturvarikkomuksiin langallisissa ja langattomissa verkoissa. ClearPass tuo myös tuen omien laitteiden liittämisessä yrityksen verkkoon, joko täysin tai rajoitetuin oikeuksin ilman, että yrityksen tietoturvapolitiikkaa rikotaan. ClearPassin avulla laitteesta saadaan kerättyä seuraavat tiedot:

- Laite tyyppi ja malli
- IP-osoite
- MAC-osoite
- Network Interface Card(NIC)-toimittajan
- Käyttöjärjestelmä ja sen versio
- VLAN:in

(Stone 2017.)

3.2 AAA-palvelu

AAA-protokolla eli Authentication/todentaminen, Authorization/valtuutus ja Accounting/tilastointi. Protokollan avulla voidaan varmistaa laitteen/käyttäjän identiteetti, antaa pääsy käyttäjälle/laitteelle tai seurata käyttäjän/laitteen toimintaa verkossa. AAA-protokollia yleisimmin käytössä olevat on RADIUS, DIAMETER ja TACACS+. DIAMETER ja TACACS+ ovat uudempia, mutta työssä käytetään RADIUS-protokollaa. (Configuring AAA. 2013.)

Todentaminen tarkoittaa käyttäjän tai laitteen tunnistamista verkkoon kirjautuessa. Tunnistamiseen on käytössä monia tapoja, mutta yleisin näistä on käyttäjätunnus salasana yhdistelmä tai laitteissa sertifikaatti/MAC-osoite. Käyttäjätunnus salasana yhdistelmän heikkous on liian helpot salasanat, jonka takia on kehitetty varmempia menetelmiä kuten vaihtuvat salasana, eli samantapaiset kuin pankkien avainlukulistat tai sitten vaihtoehtoisena tapana on käyttää normaalia salasanaa sekä sen jälkeen tuota vaihtuvaa salasanaa vielä vahvistuksena. Vaihtuvalle salasanalle on tullut vielä avainlukulistojen lisäksi sovelluksia, jotka päivittävät kuusinumeroista lukua, jolla pääsee kirjautumaan sisään esimerkiksi Microsoftin ja Googlen Authenticator sovellus, joita kutsutaan myös kaksivaiheiseksi tunnistautumiseksi. (Configuring AAA. 2013.)

Valtuutuksen tarkoitus on antaa käyttäjälle verkko-oikeudet, jotka hänen profiilinsa on ennalta määritetty, esimerkiksi pääsy oikeille verkkolevyille, sivuille ja sovelluksiin. Valtuutus tehdään todentamisen jälkeen, kun käyttäjä on onnistuneesti kirjautunut verkkoon. Valtuutusta käytetään yleensä WLAN-verkoissa siten, että samasta tukiasemasta ulkopuoliset käyttäjät pääsevät internettiin, mutta ei yrityksen verkkolevyille tai muihin yrityksen palveluihin, kun taas yrityksen työntekijät pääsevät samoista tukiasemista omiin palveluihinsa. (Configuring AAA. 2013.)

Tilastoinnin tarkoitus on kerätä tietoa käyttäjän toimista kuten: mistä ja milloin käyttäjä kirjautuu, mitä palveluita käyttäjä on käyttänyt, verkkolevyjen muokkauk-

sesta/käytöstä ja käyttäjän toimista esimerkiksi verkkolaitteiden asetuksien muokkauksesta. Näiden tietojen avulla voidaan vikatilanteissa selvittää milloin ja missä ongelma on syntynyt. (Configuring AAA. 2013.)

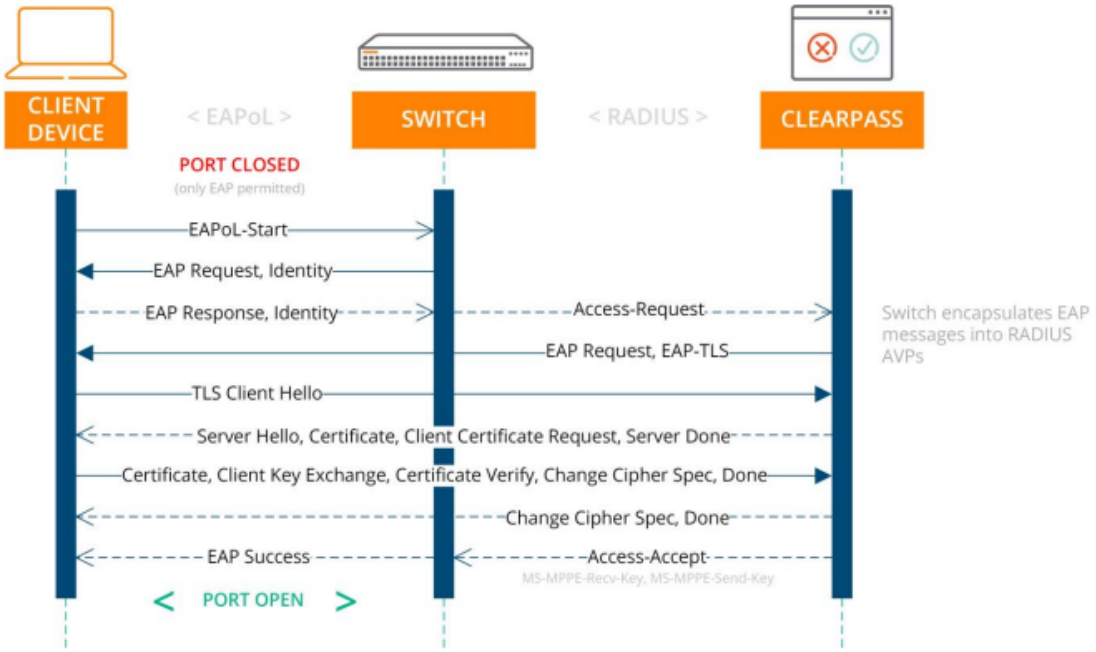
3.3 IEEE 802.1X

IEEE 802.1X standardi on porttikohtainen todennusmenetelmä langattomaan ja langalliseen verkkoon. Porttikohtaista todennusmenetelmää käytetään estämään luvattomien laitteiden pääsy verkkoon, joka parantaa verkon kyberturvallisuutta. 802.1X perustuu EAP-protokollaan.

Todennusmenetelmä pitää sisällään kolme eri osapuolta, jotka ovat asiakas eli laite esimerkiksi tietokone, autentikointipalvelin, joka on yleensä RADIUS-palvelin ja autentikoija eli verkon liityntäpiste, joka on yleensä kytkin. (802.1X: Port-Based Network Access Control 2020.)

3.3.1 Protokollat

IEEE 802.1X käyttää useita eri protokollia tiedon siirtämiseen ja tiedon salaamiseen. Yleisimmin käytettyjä protokolla on EAP, RADIUS ja EAPOL. EAPOL-protokollaa käytetään asiakkaan ja liityntäpisteen välillä, kun taas RADIUS-protokollaa NAS-liityntäpisteen eli kytkimen ja autentikointipalvelimen väliseen liikenteeseen. (Catalyst 6500 Release 12.2SX Software Configuration Guide. 2016.)



Kuvio 2 EAPOL todennus, ClearPass palvelimen kanssa (Wired Policy Enfrocement ClearPass. 2018.)

EAP eli Extensible Authentication Protocol on käyttäjien tunnistusprotokolla, joka kehitettiin alun perin Point-to-Point (PPP) protokollalle, mutta nykyään se tukee useita todennusmenetelmiä kuten IEEE 802, eikä se vaadi IP:tä. EAP toimii suoraan siirtoyhteyskerroksella ja sen isoimpia etuja on sen joustavuus. Eli EAP:ia käytetään yleensä tietyn todennusmenetelmän valitsemiseen sen jälkeen, kun autentikointipalvelin kysyy tarkennettuja tietoja mitä todennusmenetelmää halutaan käyttää. (Aboba ym. 2004, 3.)

PEAP eli Protected Extensible Authentication Protocol on sama kuin EAP-protokolla, mutta se on suunniteltu tarjoamaan turvallisempi todennus 802.11 langattomille verkoille, jotka tukevat 802.1X porttikohtaista todennusta. PEAP todentaa palvelimen julkisen avaimen varmenteella ja suorittaa todennuksen suojatussa TLS-istunnossa, jonka avulla WLAN-käyttäjät, WLAN-asemat ja todennuspalvelin voivat todentaa itsensä. (Rouse N.d.)

Erona EAP-protokollaan PEAP tuo turvallisen kuljetuksen todennettuun tietoon, lisäämällä tunneloinnin PEAP asiakkaan ja todentamispalvelimen välille, eli liikenne salataan. Sillä estetään esimerkiksi salasanojen kaappaaminen.

LDAP eli Lightweight Directory Access Protocol on protokolla, joka toimii yhdessä 802.1X:n todennuksen yhteydessä, mutta valtuutus tapahtuu LDAP:n avulla. LDAP on hakemistopalvelujen pääsykortti, joka pääsääntöisesti tarkistaa käyttäjän kirjautuessa koneelle, tämän henkilön attribuutit kuten sukunimen, etunimen, ryhmäkäytännöt, puhelinnumerot ja niin edelleen. Tiedot saadaan, kun tunnistautuminen on onnistunut ja ClearPassin Policy Manager etsii tiedot käyttäjän tunnuksen avulla AD:sta LDAP:n avulla. (Adding Active Directory as an Authentication Source to Policy Manager. N.d.)

3.4 RADIUS

RADIUS eli Remote Authentication Dial-In User Service on AAA-protokolla, jonka avulla määritellään AAA-mallin mukainen tunnistautuminen, valtuutus ja tilastointipalvelu, sekä kommunikointi päätelaitteiden ja tunnistautumispalvelimen välillä. RADIUS-protokollaa on käytetty sisäänsoittopalveluihin tarjoamaan käyttäjien tunnistusta, mutta nykyään RADIUS on enemmän käytössä yritysten sisäisissä verkoissa. RADIUS-protokollan kehitti Livingston yhtiö. (RADIUS Protocol and Components 2012.)

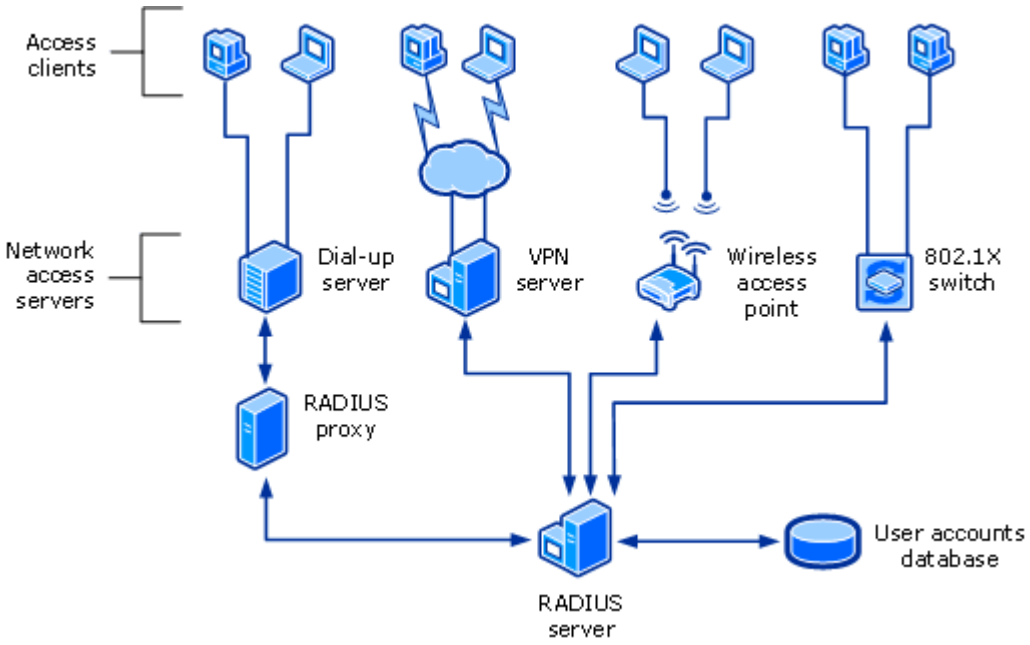
3.4.1 RADIUS-komponentit ja protokollan toiminta

RADIUS komponentteja on viisi erilaista:

- Asiakkaan laite (Tietokone)
- NAS-liityntäpiste (Kytkin)
- RADIUS-välityspalvelin (Proxy)
- RADIUS-palvelin (Serveri)
- Käyttäjätietokanta (AD)

Asiakkaan laite esimerkiksi tietokone tai kannettava, joka haluaa pääsyn verkkoon lähettää pyynnön NAS-liityntäpisteelle eli kytkimelle. Liityntäpiste kysyy tunnistetietoja käyttäjältä, jotka ovat yleensä käyttäjätunnus ja salasana. Seuraavaksi liityntäpiste tai välityspalvelin välittää käyttäjän tunnistetiedot eteenpäin RADIUS-palvelimelle, joka tarkastaa ne käytössä olevasta käyttäjätietokannasta.

Tunnistetietojen olevan oikeat RADIUS-palvelin tunnistaa käyttäjän ja antaa käyttäjälle valtuutuksen. (RADIUS Protocol and Components 2012.)



Kuvio 3 RADIUS-komponentit (RADIUS Protocol and Components. 2012.)

4 Hallintajärjestelmän asennus virtuaaliympäristöön

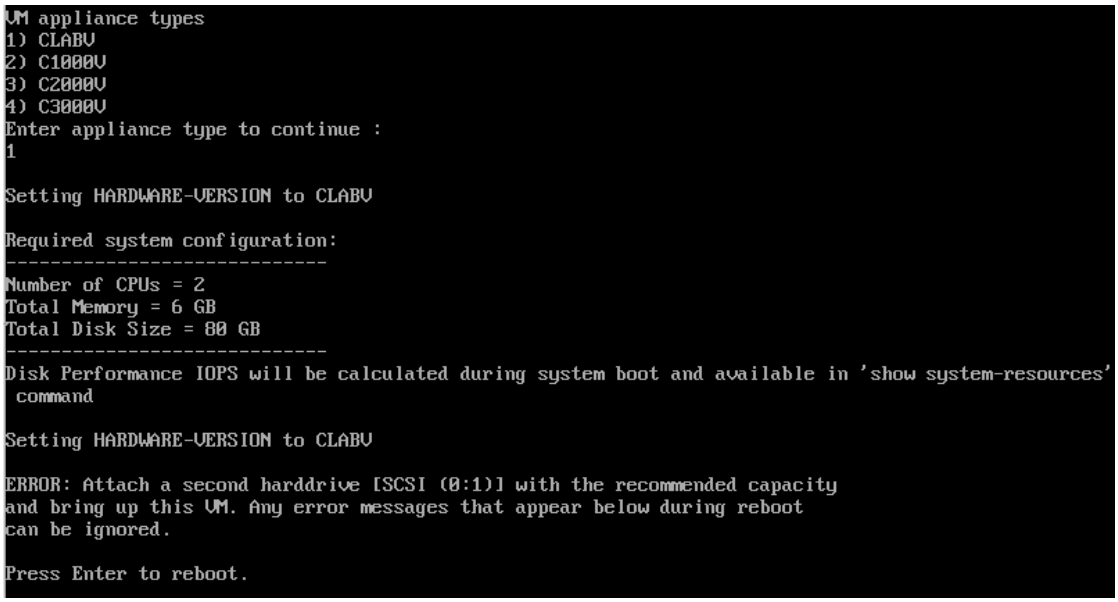
Saimme HP:lta Jyväskylän kaupungille virtuaaliympäristöön asennettavan ClearPass Policy Manager imagen ja lisenssit, jonka avulla pystymme testaamaan ClearPassin asennusta ja sen toiminnallisuuksia. ClearPassin virtuaaliympäristö liitetään kaupungin Hallinto VLAN:iin, joka on VLAN 801 ja Data portti tietoihin syötettiin DHCP palvelimen IP-osoitteet.

4.1 Palvelimen määrittäminen

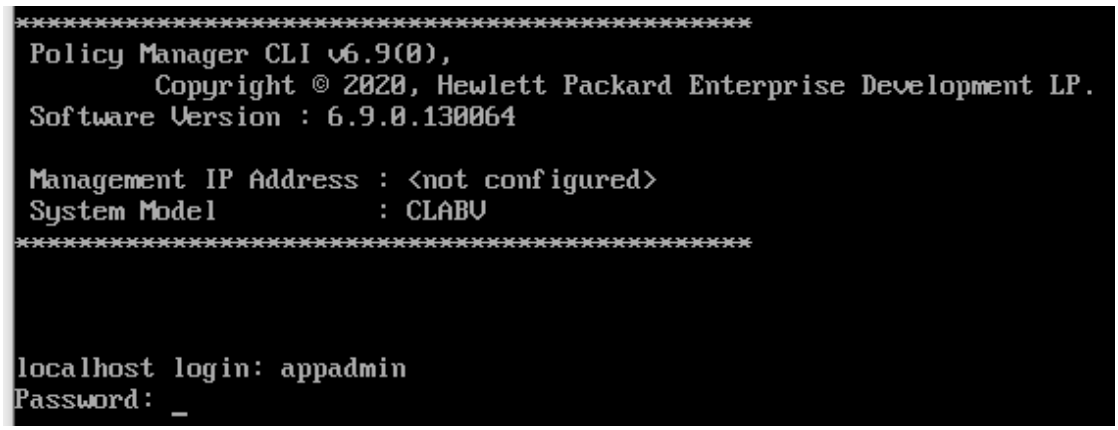
Ensin OVF-päätteinen image tiedosto ladataan vSphere Clientin kautta kaupungin virtuaaliympäristöön VMWareen. VMWaresta käynnistäessä asennus kysyy ensimmäisenä mikä virtuaalikone versio valitaan, neljästä vaihtoehdosta, joissa jokaisessa on erilaiset vaatimukset palvelimelta, joita on:

- käyttäjien määrä
- prosessorien ja keskusmuistin määrä
- kovalevyn tila
- verkkoporttien nopeus ja määrä
- IOP tason eli levyn kirjotusnopeuden mukaan

Sen jälkeen piti lisätä toinen kovalevy kooltaan 80GB, jotta asennus lähti kulkemaan eteenpäin, kun valitsimme CLABV version eli se vaatii kaksi varattua virtuaaliprosessoria, 6GB keskusmuistia ja 80GB kovalevytilaa kuten kuviosta 4 nähdään. Tämän jälkeen päästään kirjautumisikkunaan, jossa tunnukset ovat ennalta määritetty ClearPassin asennusohjeissa. (Kuvio 5) (VMware vSphere Hypervisor (ESXi) Requirements. N.d.)

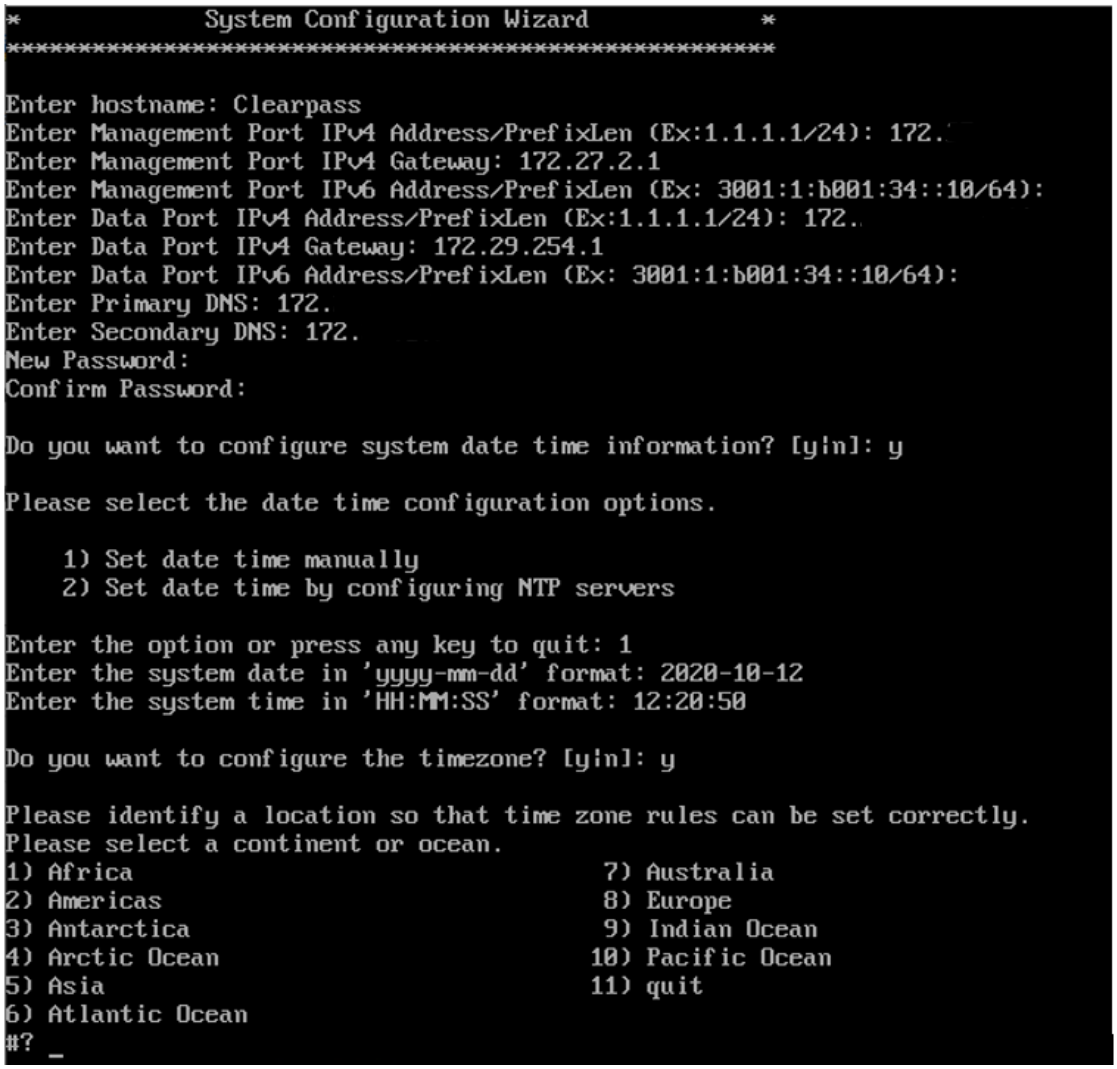


Kuvio 4 Palvelimen konfigurointi 1



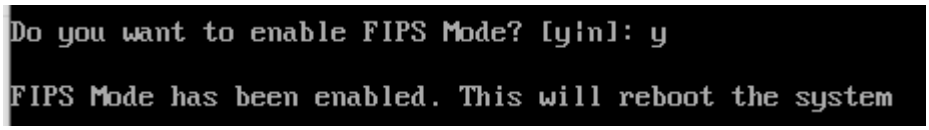
Kuvio 5 Palvelimen konfigurointi 2

Kirjautumisen jälkeen palvelin aloittaa asennustyökalun, jossa määritellään hallinta portin, data portin ja DNS palvelimen IP-osoitteet. Seuraavaksi asetetaan salasana, jonka avulla seuraava kirjautuminen onnistuu. Tämän jälkeen päivitetään vielä aika ja maantieteellinen alue sekä otetaanko FIPS tila käyttöön. (Kuvio 6&7&8) (Using VMware vSphere Web Client to Install ClearPass on a Virtual Machine. N.d.)



Kuvio 6 Palvelimen konfigurointi 3

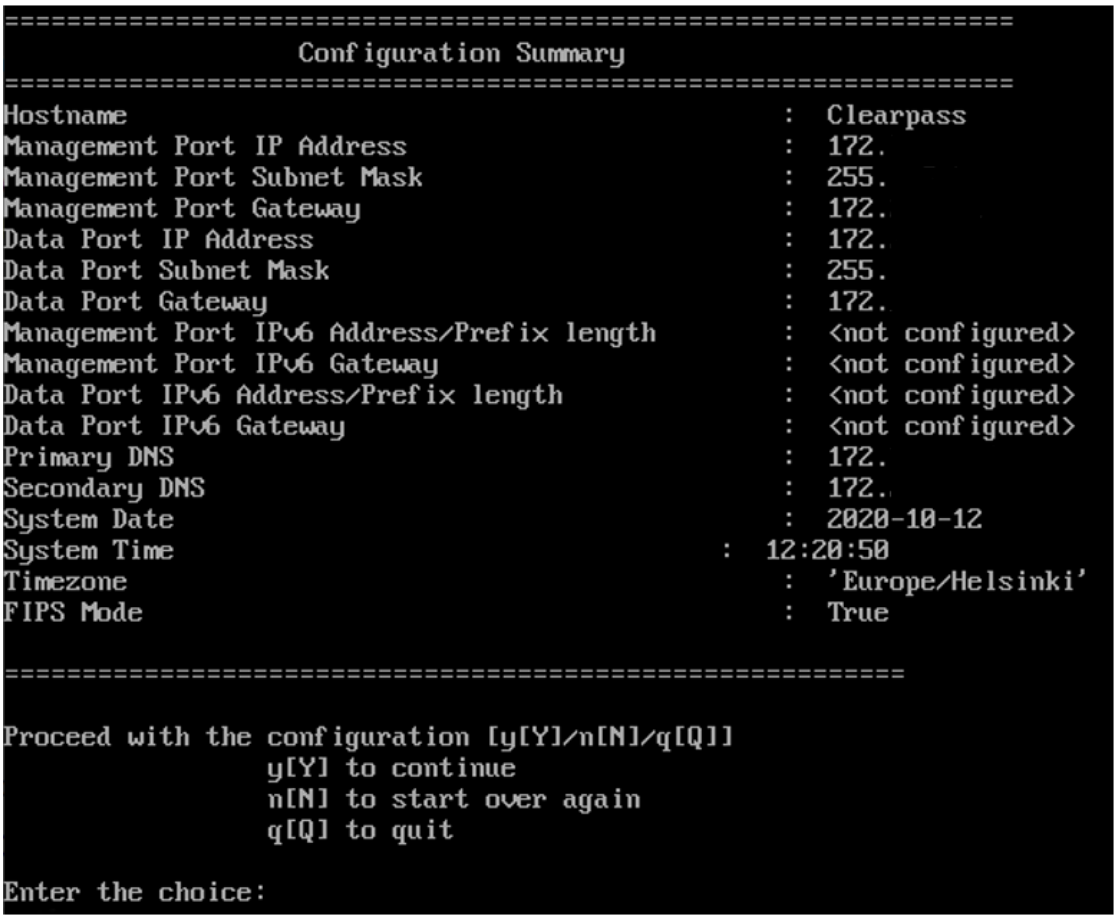
Kuvio 7 Palvelimen konfigurointi 4



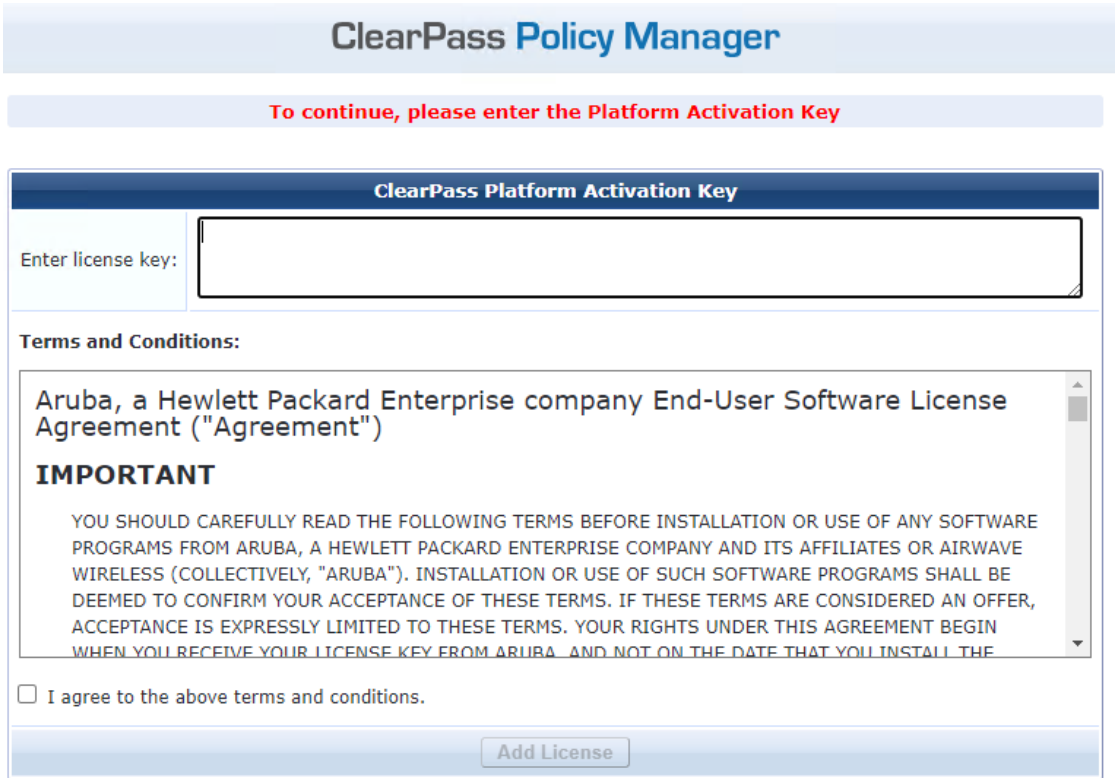
Kuvio 8 Palvelimen konfigurointi 5

Palvelimen asetusten määrittämisen lopussa tulee yhteenveto määritetyistä asetuksista ja ne voi hyväksyä, aloittaa alusta tai lähteä pois määrittämisestä, jonka jälkeen palvelin käynnistyy uudelleen. Tämän jälkeen hallinta portin IP-osoitteella pääsee selaimen kautta ClearPass Policy Manager palvelimen GUI-ikkunaan, joka kysyy ensimmäisenä lisenssiä ja hyväksymistä ehtoihin ja sääntöihin. (Kuvio 9 & 10) Lisenssin laittamisen ja ehtojen hyväksymisen jälkeen kirjaudutaan sisään hallintaportaaliin tunnuksella admin ja aikaisemmassa kohdassa määritellyllä salasanalla, jonka jälkeen

hallintaportaali aukeaa. (Using VMware vSphere Web Client to Install ClearPass on a Virtual Machine. N.d.)



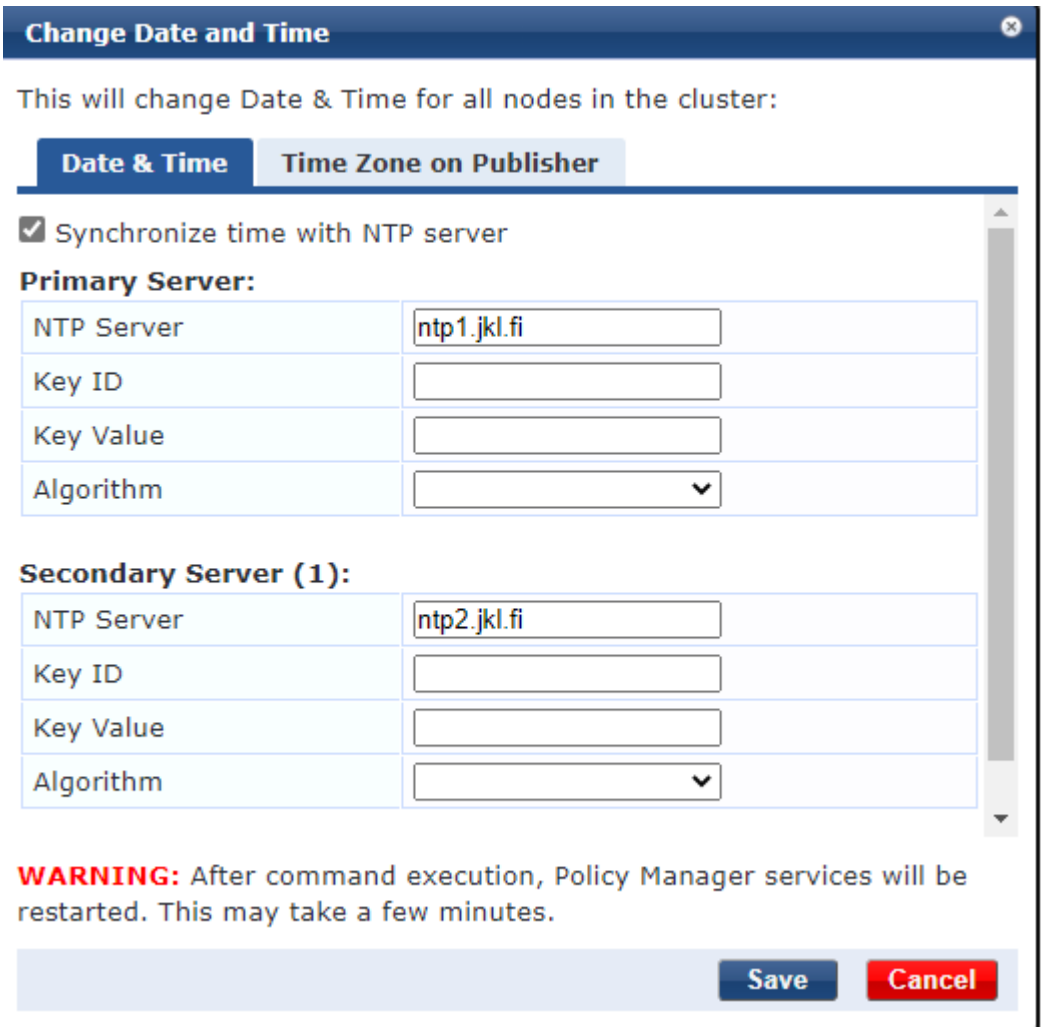
Kuvio 9 Yhteenveto palvelimeen konfiguroiduista asetuksista



Kuvio 10 ClearPass GUI

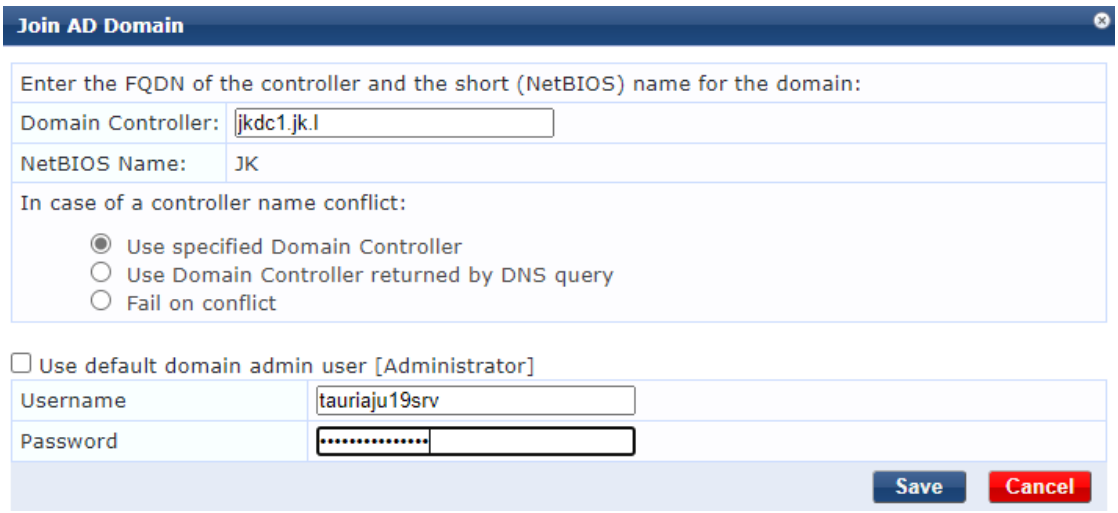
4.2 Domainin ja AD:n yhdistäminen

ClearPass Policy Manager hallintaikkunaan päästyä, halutaan ClearPass yhdistää Jyväskylän kaupungin domainiin. Ensin kuitenkin pitää määrittää palvelimen aika samaksi kaupungin NTP-palvelimen kanssa, joten NTP palvelimet vain lisätään ClearPass palvelimen hallinnan kautta. (Kuvio 11) (Joining a Policy Manager Server to an Active Directory Domain. N.d.)



Kuvio 11 NTP-palvelimen lisäys

ClearPassiin lisättiin asiakas, cygnet ja jk.l domainit, jotka ovat jokainen erikseen toimivia domaineja eikä niillä ole luottosuhteita. Kuvioissa 12 ja 13 nähdään, miten domain lisätään ja miten se näkyy hallintapaneelissa. Domainien liittyessä ClearPassiin se luo tilin Policy Manager nodelle AD:n tietokantaan. Palvelimen konfiguraatio asetuksista määritetään myös RADIUS-palvelimen parametrien alta ” Log Accounting Interim-Update Packets” päälle, joka liittyy AAA-protokollan tilastointiin, kun palvelimet keskustelevat radiuksen kanssa. Tämän avulla pystytään seuraamaan, kuinka paljon kaistaa käytetään yhteyden aikana ja kauan yhteys on kestänyt. (Joining a Policy Manager Server to an Active Directory Domain. N.d.)



Kuvio 12 Domainin lisäys

	Domain Controller	NetBIOS Name
1.	ASIAKAS.JYVASKYLA.FI	ASIAKAS
2.	CYGNNET.FI	CYGNNET
3.	JK.L	JK

Kuvio 13 Domainit ClearPassissa

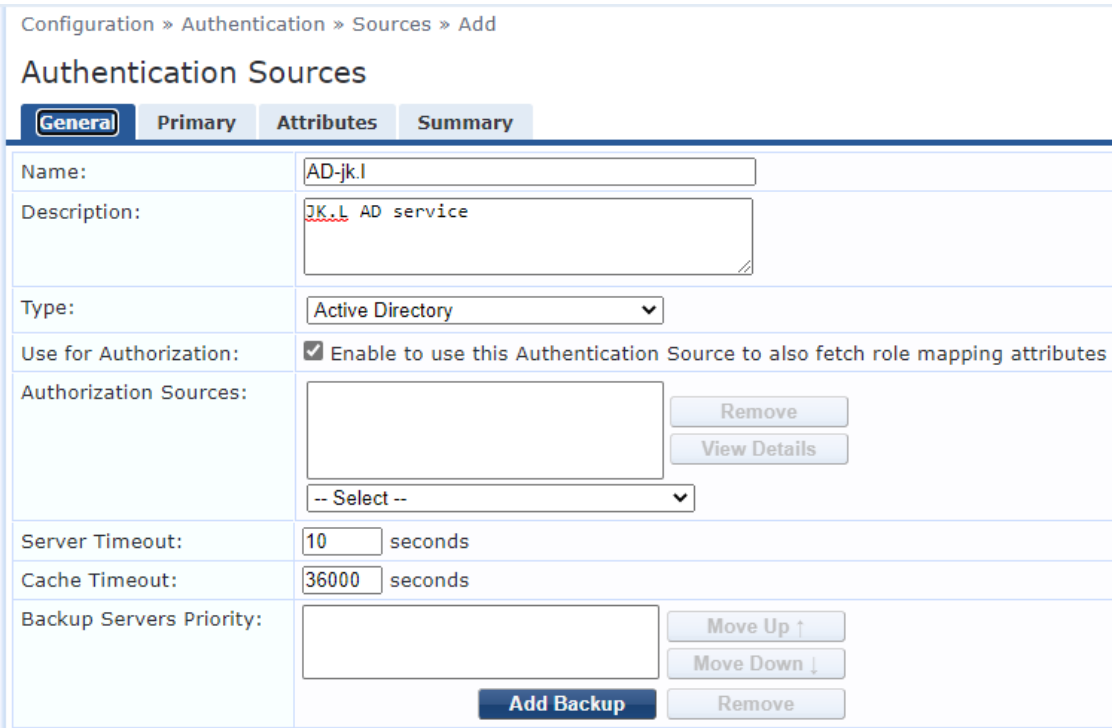
4.3 AD:n lisääminen Policy Managerin todentamisen lähteeksi

Kun policy manager on liitetty kaupungin domainiin voidaan AD lisätä policy manageriin todentamisen lähteeksi. AD:n lisääminen on pakollista, jotta policy manager saa oikeudet käyttäjien tietoihin, jotka on tallennettu AD:n tietokantaan. Valtuuttaminen policy managerin ja AD:n välillä toteutetaan LDAP-protokollalla, joka tarjoaa keinoja tietojen hakemiseen, palauttamiseen, sisällön käsittelyyn ja pääsyn monipuolisiin suojaustoimintoihin. Sen avulla saadaan mahdollisuus paikallistaa organisaatio, henkilöitä ja muita resursseja, kuten tiedostoja ja laitteita verkosta, joko internetistä tai yrityksen omasta intranetistä. (Adding Active Directory as an Authentication Source to Policy Manager. N.d.)

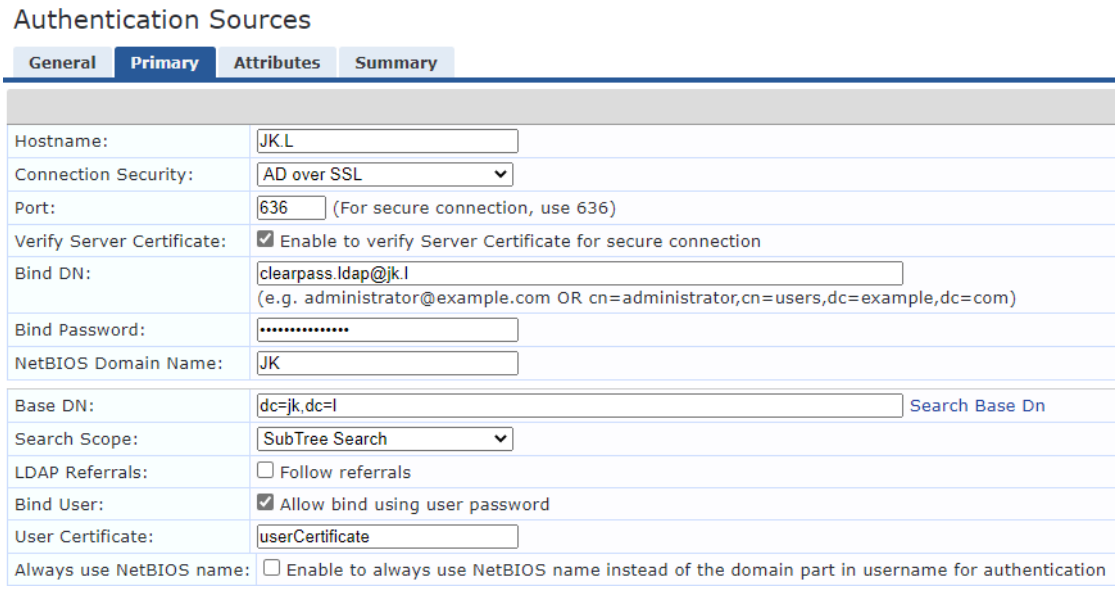
Ennen todentamista ClearPassin kanssa täytyi luoda ns. ”palvelukäyttäjä” AD:hen jolla on normaali Domain oikeus, joka nimettiin clearpass.ldap@jk.l. Se ei ole mikään normaali tunnus vaan pelkästään luotu tunnus ClearPassin ja AD:n väliseen keskuste-

luun. Tunnus täytyy olla sellainen missä ei salasana vanhene ikinä eikä tunnus vanhene koskaan, koska muute salasanan tai tunnuksen vanhetessa ClearPass ei voi noutaa tietoja AD:sta. Se nimettiin tuon nimiseksi, että ymmärretään mihin sitä käytetään. Bind DN tarkoittaa bind toimintoa, joka tarkoittaa todentamista LDAP-palvelimelle, mikä AD:n on tehtävä ennen kuin se voi suorittaa kyselyitä LDAP-palvelinta vastaan. Clearpass.ldap tunnus on nyt tuo bind tunnus, jonka avulla AD todistaa LDAP-palvelimelle, että sillä on oikeus tehdä kyselyjä sitä vasten. (Adding Active Directory as an Authentication Source to Policy Manager. N.d.)

Todennuksen alussa valitaan tyyppi millä todennus halutaan tehdä ja tässä tapauksessa se on Active Directory, niin kuin kuviossa 14 näkyy. Syötettiin myös todennukselle nimi ja lisätiedot. Kuviossa 15 yhdistetään AD SSL:n yli, eli salauksen kanssa, mikä käyttää porttia 636. (Adding Active Directory as an Authentication Source to Policy Manager. N.d.)

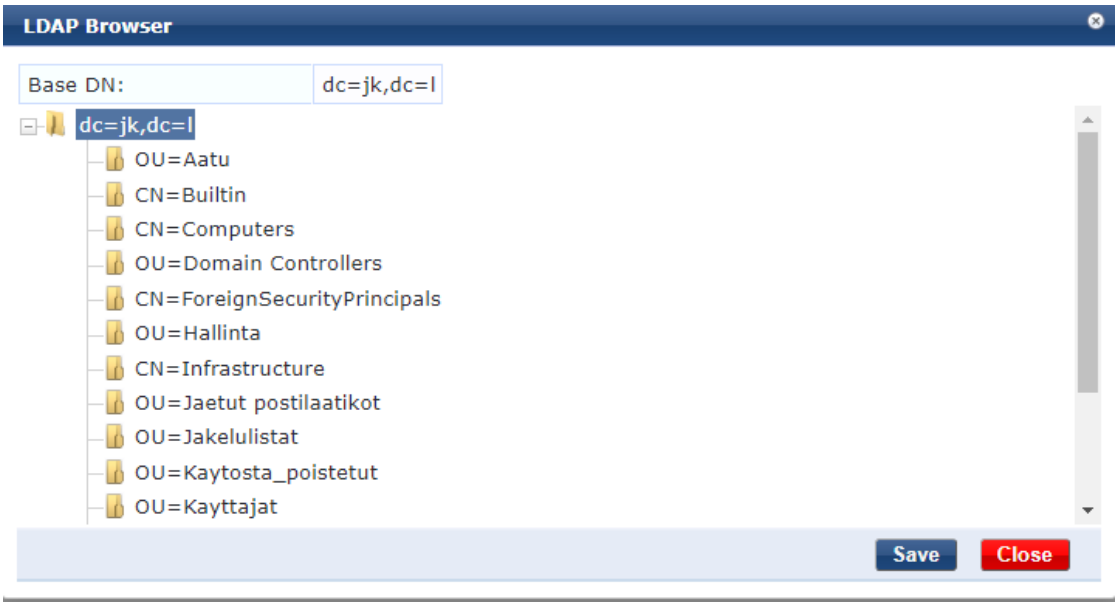


Kuvio 14 Todenamisen tyypin valitseminen



Kuvio 15 Yhdistäminen SSL-salauksen kanssa

Syötetään clearpass.ldap tunnuksen tunnus ja salasana ja painetaan ”Search Base Dn”, jolla testataan, että yhteys AD:hen muodostaa. Kuviosta 16 nähdään AD-yhteyden muodostuneen, kun nähdään AD:n rakenne. (Adding Active Directory as an Authentication Source to Policy Manager. N.d.)

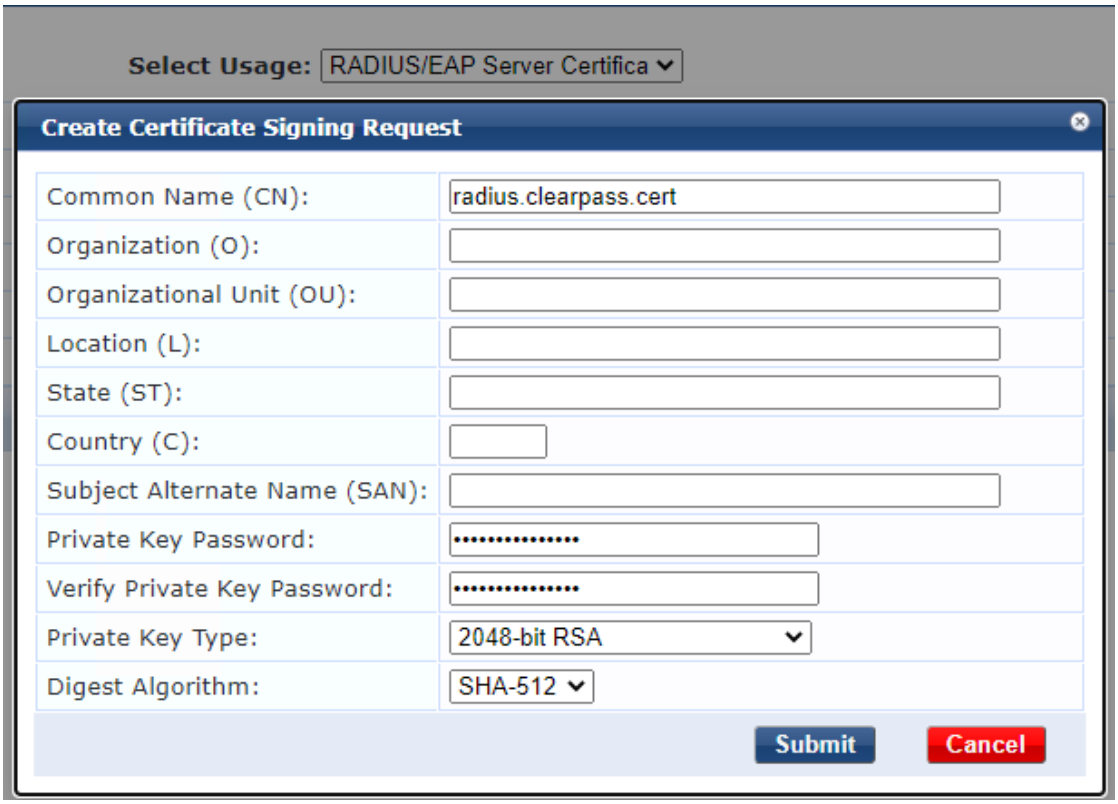


Kuvio 16 Yhteys AD:hen

4.4 RADIUS-sertifikaatin asennus

ClearPassiin täytyy asentaa RADIUS-palvelimen sertifikaatti, jotta tunnistautuminen voidaan tehdä laitteiden ja ClearPassin välillä.

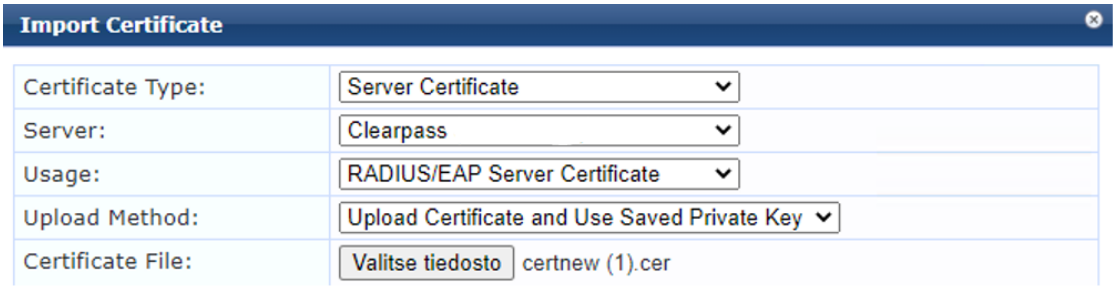
Asennus aloitetaan luomalla ClearPassin päässä sertifikaatin allekirjoituspyyntö, joka luo sertifikaattipyynnön, csr-tiedoston ja yksityisen avaimen, mikä tallentuu ClearPassiin. Luodessa sertifikaattia ei tarvitse kuin nimetä se fiksusti ja laittaa yksityisen avaimen salasana ja muistaa se, jotta voit tuoda sertifikaatin, kun olet luonut sen (Kuvio 17). (Robers 2017.)



Kuvio 17 RADIUS sertifikaatin tiedot

Tämän jälkeen Jyväskylän kaupungin sertifikaatti palvelimelle luodaan uusi sertifikaatti. Palvelimen kautta ladataan juurisertifikaatti Base 64 muodossa ja sen jälkeen pyydetään palvelimelta sertifikaattia syöttämällä sertifikaatti pyyntö koodi kenttään. Sertifikaatin muodoksi valitaan web server, koska se on sama asia kuin RADIUS-palvelimen sertifikaatti. (Robers 2017.)

Ennen sertifikaatin lisäystä täytyy ClearPassiin käydä lisäämässä juurisertifikaatti luotettujen sertifikaattien listaan. Tämän jälkeen luodun sertifikaatin lisääminen onnistuu ClearPassiin, koska se tietää mistä sertifikaatti tulee. Ennen piti syöttää yksityisen avaimen tiedosto ja salasana, mutta nykyään sen tekeminen ei ole tarpeellista, kun avaimen salasana tallentuu ClearPassin järjestelmään automaattisesti (Kuvio 19). (Robers 2017a.)



Kuvio 18 Radius sertifikaatin lisäys

5 Verkon konfiguraation automatisointi

Opinnäytetyössä halutaan automatisoida VLAN:ien konfigurointia kytkimissä. Ei tarvitsisi jokaista porttia konfiguroida käsin oikeaan VLAN:iin vaan kytkimen portit menisivät automaattisesti oikeaan VLAN:iin kytkettävän laitteen mukaan. Automatisointi aloitetaan konfiguroimalla kytkin, jotta se voidaan lisätä ClearPassiin samalla kun lisätään 802.1X langallinen palvelu ja sen ominaisuudet.

5.1 Kytkimen konfigurointi

Käytössä on HPE Aruba 2530 sarjan 24 porttinen kytkin, jolle aluksi varataan IP-osoite DHCP-palvelimelta hallinto VLAN:iin ja sen jälkeen määritellään kytkimelle konsoli portin avulla IP-osoite, oletusyhdyskäytävä ja aliverkon peite. Kytkimelle lisätään myös VLAN:it joita on kuusi kappaletta sekä vakio VLAN. IP-osoitteen määrittämisen jälkeen kytkimeen on mahdollista muodostaa telnet-yhteys etähallintaa varten.

Seuraavaksi kytkimelle määritellään RADIUS-palvelimeksi ClearPass-palvelin, jossa ensimmäisellä komennolla määritetään ClearPass palvelin IP-osoitteella ja Pre-shared avaimen avulla se RADIUS-palvelimeksi. Toisella komennolla otetaan käyttöön RADIUS CoA-toiminallisuus. Kolmas komento sallii kytkimen vastaanottaa CoA-viestejä milloin tahansa. (Configure 802.1X Authentication. 2017.)

```
radius-server host x.x.x.x key "yyyyyyyy"

radius-server host x.x.x.x dyn-authorization

radius-server host x.x.x.x time-window 0
```

Kytkimelle pitää vielä konfiguroida seuraavilla kahdella komennoilla porttikohtainen 802.1X todentaminen, sekä aktivoida 802.1X. Kolmas ja neljäs komento sen sijaan ottaa käyttöön RADIUS Accounting-toiminnon 3 minuutin päivitysajalla. (Configure 802.1X Authentication. 2017.)

```
aaa authentication port-access eap-radius

aaa port-access authenticator active


aaa accounting network start-stop radius


aaa accounting update periodic 3
```

Viimeinen vaihe kytkimen konfiguroinnissa on ottaa käyttöön 802.1X todentaminen porttitasolla. Portit, joilla testaus suoritetaan ovat 1 ja 2 portit. Sallitaan porteissa vain yksi todennettu käyttäjä, sekä laitetaan EAP-paketeille 30 sekunnin aikaikkuna, jossa ne sallitaan. Tämän avulla portissa olevalla laitteella on tarpeeksi aikaa tunnistautua, sekä estetään laitetta saamasta väärää IP-osoitetta DHCP-palvelimelta väärästä VLAN:ista tunnistusprosessin aikana. Kolmantena komentona lisätään vielä porteille MAC-pohjainen todennus, eli jos laite ei tue 802.1X autentikointi, voidaan laite tunnistaa kuitenkin MAC-osoitteen avulla. Kaksi viimeistä komentoa asettaa portin oletus VLAN:iin, jos laite ei läpäise MAC-pohjaista tunnistautumista. Oletus VLAN on tässä tapauksessa julkinen 886 VLAN. (Configure 802.1X Authentication. 2017.)

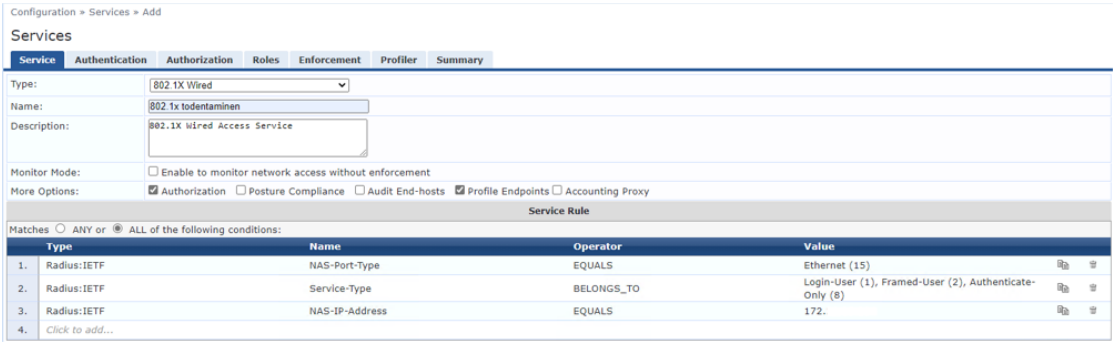
```
aaa port-access authenticator 1-2

aaa port-access authenticator 1-2 client-limit 1

aaa port-access authenticator 1-2 unauth-period 30

aaa port-access mac-based 1-2

aaa port-access mac-based 1 unauth-vid 886

aaa port-access mac-based 1 unauth-vid 886
```

5.2 802.1X langallinen palvelu

ClearPass policy managerissa on erilaisia palveluita, joiden avulla todennus ja valtuutus tehdään. Policy managerissa on valmiina monenlaisia pohjia palveluille, jotka helpottavat luomaan omaan tarpeeseen oikean palvelun. Palveluita pystyy luomaan myös manuaalisesti, jos valmista pohjaa ei ole saatavilla tai palvelu velhon kanssa, joka neuvoo eri vaiheitten läpi. Yleisimmät palvelut, joita käytetään ovat Aruba 802.1X langaton, 802.1X langaton ja 802.1X langallinen. (Services N.d.)

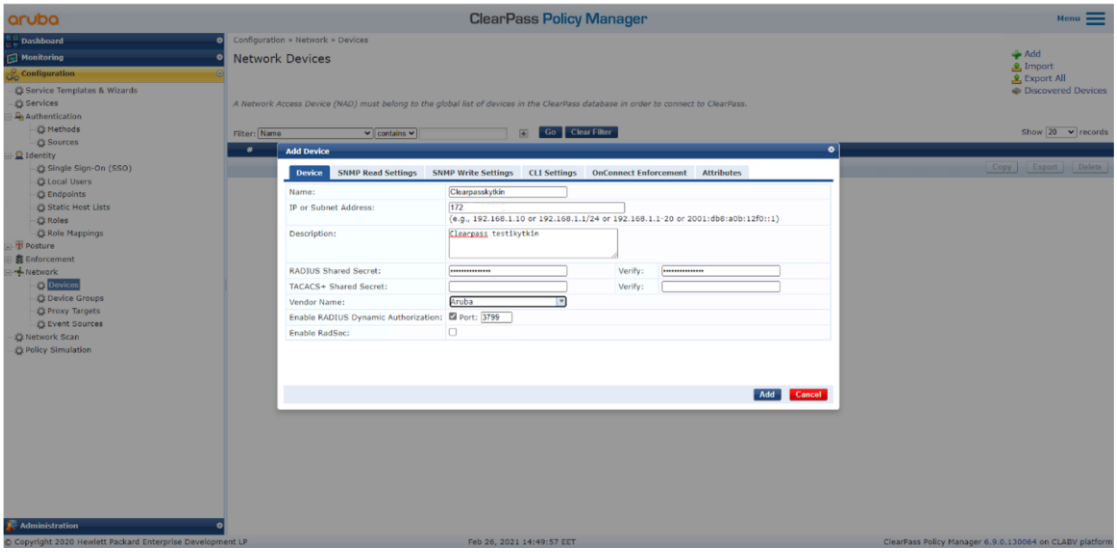
5.2.1 802.1X langallisen palvelun lisäys

Opinnäytetyössä halutaan toteuttaa 802.1X todennus langallisessa verkossa, joten palveluksi valitaan 802.1X langallinen, joka todentaa ja valtuuttaa laitteita ethernet/lan verkon läpi. Kuviosta 20 havaittiin, että palvelua luodessa valitaan ensin tyyppi, annetaan sille nimi ja kuvaus sekä nähdään säännöt, jotka ovat valmiiksi määritetty langalliselle palvelulle. Lisätään sääntöihin kuitenkin kytkimen IP-osoite, jotta ClearPass käyttää vain testikäytössä olevaa kytkintä RADIUS-pyyntöihin. Tällöin ei häiritä myöskään muuta verkon liikennettä. Otetaan käyttöön myös laitteiden profilointi, jonka avulla voidaan tunnistaa laite automaattisesti esimerkiksi kannettavan ja tulostimen välillä. (Robers, H. 2017b.)



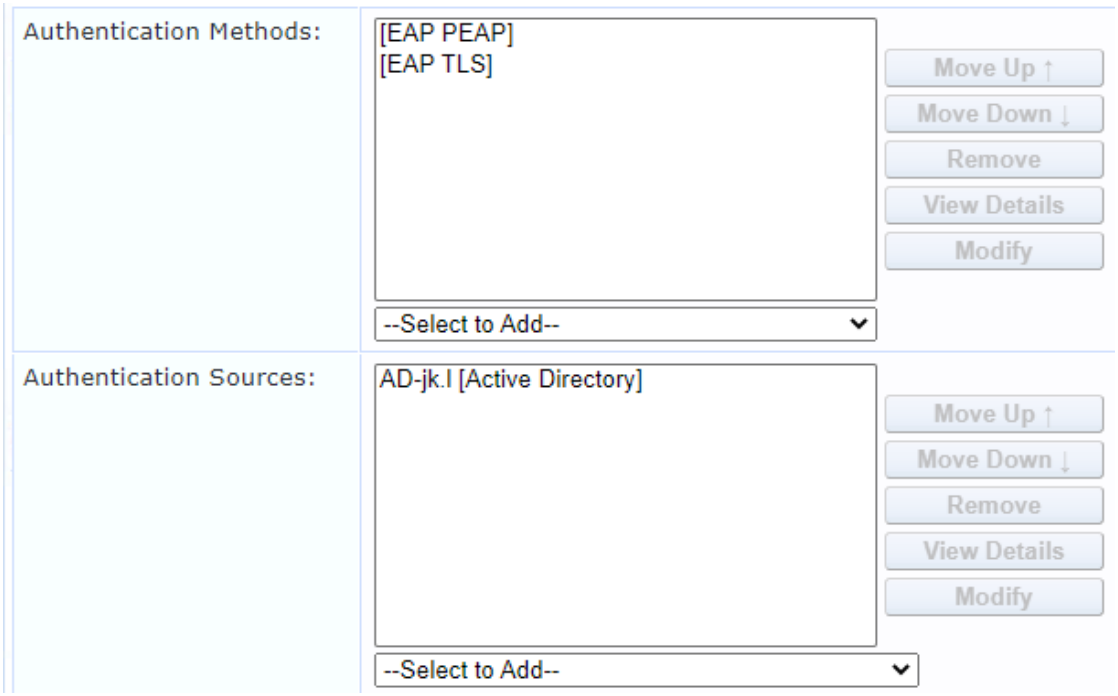
Kuvio 19 802.1X langallinen palvelu

Langallisen palvelun lisäyksessä täytyy huomioida, että kytkin, jota halutaan käyttää testauksessa, täytyy ensin lisätä ClearPassin laite välilehteen kuten kuviossa 21. Tässä tapauksessa lisätään testikytkin, jota aikaisemmassa kappaleessa konfiguroitiin, antamalla kytkimen etähallinta IP-osoite, nimi, RADIUS-server komennossa määritetty Pre-shared key ja laitetaan päälle radiuksen dynaaminen valtuutus vakio portilla 3799. (ClearPass Deployment Guide. 2017.)



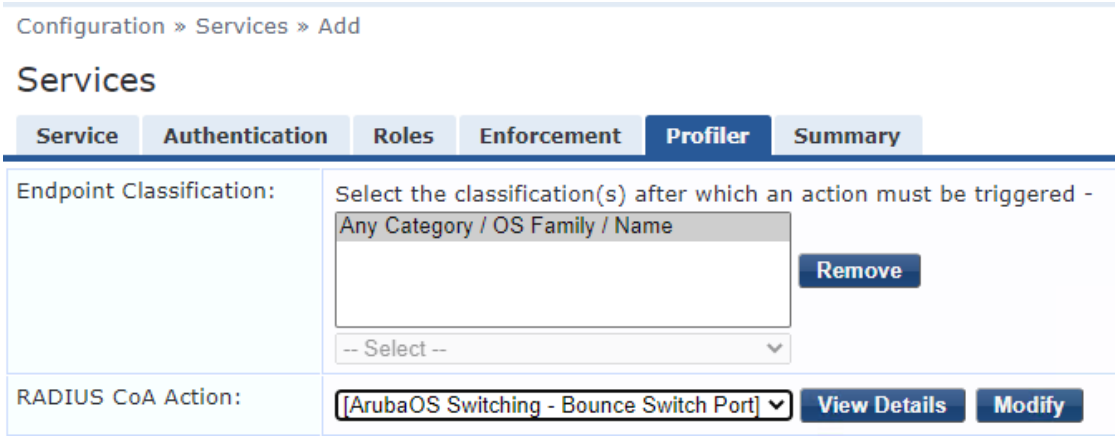
Kuvio 20 Kytkimen lisäys ClearPassiin

Kuviossa 22 todennus menetelmiksi valitaan EAP PEAP sekä EAP TLS, jotka toteuttavat todennuksen salauksen käyttäjän kirjautuessa laitteelle. Todennus lähteeksi valitaan kaupungin AD. (Robers, H. 2017b.)



Kuvio 21 Todennus käytännöt

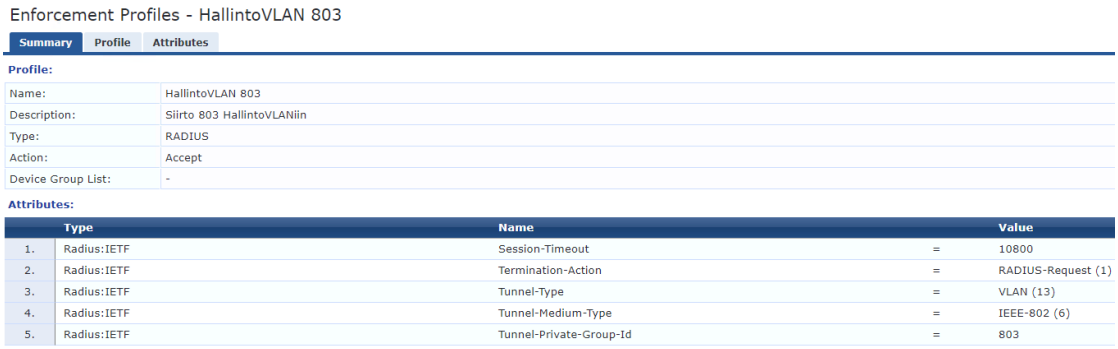
Kuviossa 23 valitaan profilointia varten Bounce Switch port-toiminto, joka aiheuttaa kytkimen portin alustuksen uuden laitteen kytkeytyessä, eli esimerkiksi jos portissa on ollut kannettava ja sen jälkeen siihen kytketään tulostin, osaa se hakea oikeasta DHCP-poolista tulostimelle IP-osoitteen. (Robers, H. 2017b.)



Kuvio 22 Profilointi

Profilointia varten täytyy myös lisätä toimeenpano profiileita, johon lisätään verkossa olevat VLAN tunnisteet. Toimeenpano profiileita on lisätty hallinto, terveys ja julki-

selle VLAN:ille kuvion 24 mukaisesti. Toimeenpano määrittää mihin VLAN:iin laite lisätään riippuen siitä mikä koneryhmä laitteelle on määritetty. (Wired Policy Enfrocement ClearPass. 2018.)



Kuvio 23 Toimeenpano HallintoVLAN

Toimeenpano saadaan toimimaan lisäämällä ClearPassiin rooleja, jotka ovat nimetty cg_Clearpass_Hallinto_TESTI sekä cg_Clearpass_terveys_testi (Kuvio 25). Samannimiset koneryhmät on lisätty AD:seen, jonka avulla ClearPass tarkastaa kumpaan koneryhmään laite kuuluu. (Robers, H. 2017b.)

Kuvio 24 Roolit

Kuviosta 26 nähdään, että toimeenpano tarkastaa roolien avulla mihin koneryhmään laite kuuluu ja toimeenpano profiili määrittää sitten mihin VLAN:iin laite laitetaan. Machine Authenticated vain tarkistaa, että laite on AD:ssa ja näin laite saa päivitykset, siihen saa etäyhteyden ja uusi käyttäjä voi kirjautua koneelle. (Wired Policy Enfrocement ClearPass. 2018.)

Kuvio 25 Toimeenpano

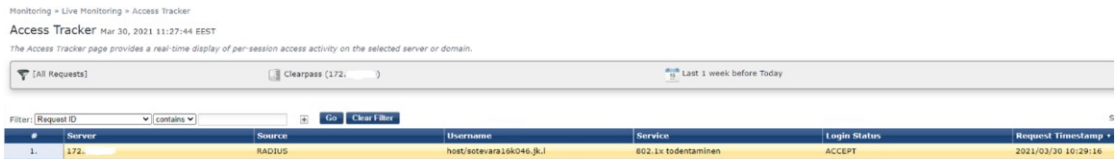
6 Testaus

ClearPassin toiminta testataan kahdella HP EliteBook 820 G3 kannettavalla, joista toinen on asennettu kaupungin windows imagella ja konetili löytyy AD:sta, sekä sille on määritetty koneryhmä hallinto tai terveys verkkoon. Toisella kannettavista ei ole konetiliä AD:ssa, eli kone toimii vieraana laitteena.

6.1 HallintoVLAN

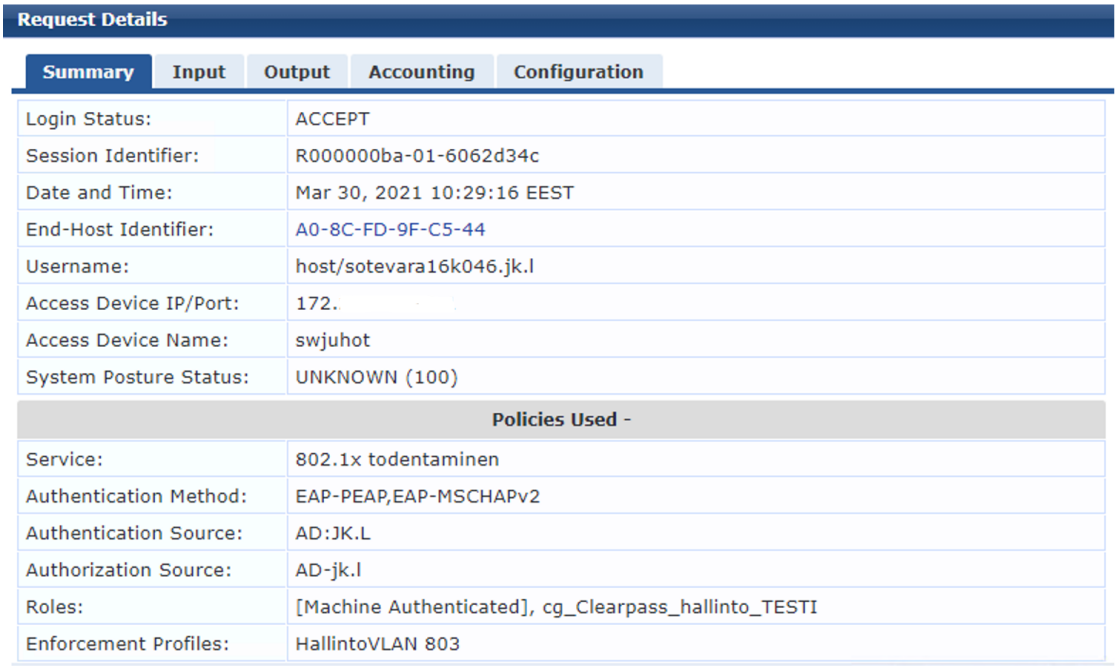
Kannettavalle on määritetty koneryhmä cg_Clearpass_Hallinto_TESTI, palveluasetuksista laitettu automaattinen lankaverkon määrittäminen päälle sekä verkkosovittimen asetuksista otettu 802.1X-todennus käyttöön ja valittu pisa sertifikaatit varmenteiden myöntäjiksi, jotta kannettava osaa yhdistää verkkoon 802.1X palvelun avulla. (Robers, H. 2017b.)

Kannettava kytketkään kytkimen portti numeroon yksi ja katsotaan ClearPassin päästä Access Tracker-välilehdeltä, että kannettava on tunnistautunut 802.1x todentaminen-palvelun avulla (kuvio 27).



Kuvio 26 Access Tracker

Kuviosta 28 nähdään ClearPassin saaneen RADIUS-pyynnön. Kuviosta nähdään myös ClearPassin hyväksyneen koneen, saaneen sen MAC-osoitteen, verkkonimen, todennustavan, todennus ja valtuutus lähteen sekä tarkastanut mihin koneryhmään kannettava kuuluu, ja sen mukaan antanut laitteelle HallintoVLAN 803 toimeenpano profiilin.



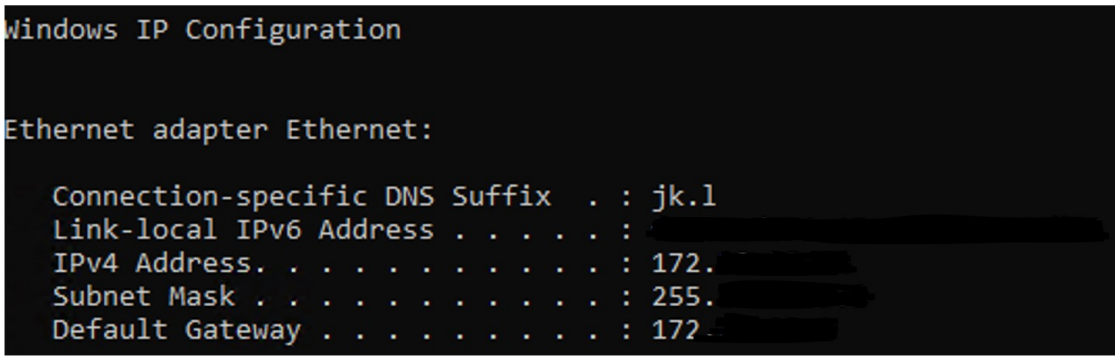
Request Details

Summary | Input | Output | Accounting | Configuration

Login Status:	ACCEPT
Session Identifier:	R000000ba-01-6062d34c
Date and Time:	Mar 30, 2021 10:29:16 EEST
End-Host Identifier:	A0-8C-FD-9F-C5-44
Username:	host/sotevara16k046.jk.l
Access Device IP/Port:	172.
Access Device Name:	swjuhot
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	802.1x todentaminen
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:JK.L
Authorization Source:	AD-jk.l
Roles:	[Machine Authenticated], cg_Clearpass_hallinto_TESTI
Enforcement Profiles:	HallintoVLAN 803

Kuvio 27 HallintoVLAN RADIUS pyyntö

Kuvion 29 mukaan nähdään kannettavan saaneen oikeasta DHCP-poolista IP-osoitteen.



```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : jk.l
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 172.[redacted]
   Subnet Mask . . . . . . . . . . . : 255.[redacted]
   Default Gateway . . . . . . . . . : 172.[redacted]
```

Kuvio 28 HallintoVLAN IP-osoite

6.2 TerveysVLAN

Kannetavan koneryhmän vaihtuessa cg_Clearpass_terveys_TESTI ryhmään, nähdään kuvioista 30 ja 31 TerveysVLAN RADIUS-pyyntö sekä IP-osoitteen vaihtuneen eri DHCP-pooliin.

Request Details

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R000000ff-01-606c3a54
Date and Time:	Apr 06, 2021 13:39:16 EEST
End-Host Identifier:	A0-8C-FD-9F-C5-44
Username:	host/sotevara16k046.jk.l
Access Device IP/Port:	172.
Access Device Name:	swjuhot
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	802.1x todentaminen
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:JK.L
Authorization Source:	AD-jk.l
Roles:	[Machine Authenticated], cg_Clearpass_terveys_TESTI
Enforcement Profiles:	TerveysVLAN 889

Kuvio 29 TerveysVLAN RADIUS pyyntö

```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : jk.l
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 10.[redacted]
   Subnet Mask . . . . . . . . . . . : 255.[redacted]
   Default Gateway . . . . . . . . . : 10.[redacted]
```

Kuvio 30 TerveysVLAN IP-osoite

6.3 Vieras laite

Vieraan laitteen kytkeytyessä verkkoon, on kytkimen porttiin määritetty sen menevän asiakas VLAN:iin. Kuviosta 32 nähdään näin tapahtuvan, kun kannettava kytketään verkkoon RADIUS-pyyntö ei mene läpi ja kannettavan liittyminen verkkoon estetään. Kuviossa 33 nähdään koneen saavan IP-osoitteen asiakas VLAN:ista ja näin rajoitetaan kannettavan oikeuksia verkossa.

Request Details

Summary | Input | Output | Alerts

Login Status:	REJECT
Session Identifier:	R00000102-01-606c4593
Date and Time:	Apr 06, 2021 14:27:15 EEST
End-Host Identifier:	98-E7-F4-F6-59-4C
Username:	host/sotevara16k023.jk.l
Access Device IP/Port:	172
Access Device Name:	swjuhot
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	802.1x todentaminen
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	None
Authorization Source:	-
Roles:	[Other]
Enforcement Profiles:	[Deny Access Profile]

Kuvio 31 AsiakasVLAN RADIUS pyyntö

```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : asiakas.jyvaskyla.fi
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 10.[redacted]
   Subnet Mask . . . . . . . . . . . : 255.[redacted]
   Default Gateway . . . . . . . . . : 10.[redacted]
```

Kuvio 32 AsiakasVLAN IP-osoite

7 Pohdinta

Opinnäytetyön tavoitteena oli helpottaa kohdeverkon reunakytkimien konfiguraatiota, sekä ottaa käyttöön ja testata Aruba ClearPass-järjestelmän toimivuutta langallisessa verkossa. Päätelaitteiden vaihtaessa paikkaa tai tarvetta päästä toiseen verkkoon oli kytkimen portti konfiguroitava käsin uudelleen, joka lisäsi paljon työtä. Oli myös mahdollista laittaa tuntematon laite porttiin ja saada kyseisen portin VLAN:ista IP-osoite, mikä aiheuttaa tieto- ja kyberturvallisuus riskin.

Aruba ClearPass-järjestelmä saatiin asennettua virtuaalipalvelimelle ja konfiguroitua testikytkin käyttöön, jonka kanssa testattiin järjestelmän toimivuutta. ClearPass-järjestelmään määritettiin palvelu, joka toimii vain testikytkimen kanssa eikä häiritse muuta verkkoa. Järjestelmää testattiin yhden testikytkimen ja kolmen eri Windows kannettavan kanssa. Kahdelle kannettavalle annettiin kaksi eri koneryhmää, joista toinen menee hallinto VLAN:iin ja toinen terveys VLAN:iin. Kolmas kone toimi niin sanottuna vieraana laitteena.

Opinnäytetyön tutkimuskysymys oli, voidaanko kohdeverkon reunakytkimien konfigurointia ja kyberturvallisuutta parantaa Aruba ClearPass-järjestelmän avulla. Työssä päästiin haluttuun tavoitteeseen ja järjestelmää testatessa se toimi niin kuin sen pitikin. Kannettavien liittyessä kytkimeen ethernet kaapelin avulla ja ClearPassin tekemien tarkistuksien jälkeen, saivat ne oikeat IP-osoitteet oikeasta VLAN:ista koneryhmän mukaan. Vieras laite taas päätyi asiakas VLAN:iin, koska sitä ei tunnistettu. Järjestelmän automaatio säästää tietohallinnon työntekijöiden aikaa, kun pelkkä koneryhmän muuttaminen siirtää koneen oikeaan verkkoon eikä työntekijöiden tarvitse enää muuttaa kytkimen konfiguraatiota.

Järjestelmä on mahdollista ottaa laajempaan käyttöön suurimmassa osassa Jyväskylän kaupungin toimipisteitä, joista tuettuja kytkimiä löytyy. Osassa toimipisteitä saattaa olla vielä niin vanhoja kytkimiä, että käyttöönotto ei ole niihin vielä mahdollista ja se vaatii laajempaa selvitystä. Kytkimien täytyy tukea IEEE 802.1X-standardia, jonka vuoksi yleistettävyys on rajallista, eikä testautulosta voida verrata suoraan isompaan testiympäristöön viennistä. Testauksessa ei kuitenkaan

kohdattua ongelmia, etteikö järjestelmää voisi viedä isompaan ympäristöön. Järjestelmä toimii myös muiden, kuin HP:n ja Aruban laitteilla, jonka vuoksi testauksen vieminen isompaan ympäristöön on helpompaa.

Järjestelmään voidaan tulevaisuudessa lisätä myös muita ominaisuuksia, kuten laitteiden profilointia ja laitteiden käyttäytymistä verkossa voidaan valvoa tarkemmin. Järjestelmään voidaan lisätä tarkistus metodeja, esimerkiksi tarkistamaan onko laitteessa palomuuri kunnossa, käyttöjärjestelmän päivitykset ajantasalla ja mitä laitteita tietokoneeseen on liitetty. Laitteessa kaikkien metodien ollessa kunnossa myönnetään pääsy verkkoon. ClearPass-järjestelmän toimintaa voidaan laajentaa myös muihin laitteisiin vaikka ne eivät tukisikaan 802.1X-standardia esimerkiksi kiinteistövalvonta, tulostimet ja VoIP-puhelimet, jolloin laitteen autentikointi voidaan hoitaa MAC-osoitteen perusteella.

Lähteet

802.1X: Port-Based Network Access Control. 2020. IEEE verkkosivut. Viitattu 11.9.2020. https://1.ieee802.org/security/802-1x/

Aboba, B., Microsoft., Blunk, L., Merit Network, INC., Vollbrecht, J., Collbrecth Consulting LLC., Carlson, J., Sun. & Levkowetz, H. 2004. Extensible Authentication Protocol (EAP). IETF Tools -nettisivu. Viitattu 1.10.2020. https://tools.ietf.org/html/rfc3748#page-3

About the ClearPass Access Management System. N.d. Aruba network verkkosivut. Viitattu 19.10.2020. https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Default.htm#About%20ClearPass/About_ClearPass.htm%3FTocPath%3DAbout%2520ClearPass%7C_____2

Adding Active Directory as an Authentication Source to Policy Manager. N.d. Aruba networks verkkosivut. Viitattu 22.10.2020 https://www.arubanetworks.com/techdocs/ClearPass/6.9/Aruba_DeloyGd_HTML/Content/Active%20Directory/AD_auth_source_adding.htm?tocpath=Preparing%20ClearPass%20for%20Active%20Directory%20Authentication%7C_____2#Authorization

Catalyst 6500 Release 12.2SX Software Configuration Guide. 2016. Cisco verkkosivut. Viitattu 2.10.2020. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html

ClearPass Deployment Guide. 2017. PDF-dokumentti. Aruba a Hewlett Packard Enterprise company. Viitattu 29.3.2021.

Configure 802.1X Authentication. 2017. PDF-dokumentti. Aruba. Viitattu 29.3.2021.

Configuring AAA. 2013. Ciscon verkkosivut. Viitattu 18.9.2020. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_aaa.html#wp1259589

Configuring NAC. N.d. Ciscon verkkosivut. Viitattu 19.10.2020. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_nac.html#wp1382989

Data sheet Aruba Clearpass Policy Manager. 2021. PDF-dokumentti. Aruba a Hewlett Packard Enterprise company. Viitattu 20.10.2020.

Geier, J. 2008. Implementing 802.1X Security Solutions of Wired and Wireless Networks. Indianapolis: Wiley Publishing cop.

Joining a Policy Manager Server to an Active Directory Domain. N.d. Aruba networks verkkosivut. Viitattu 16.9.2020. https://www.arubanetworks.com/techdocs/ClearPass/6.8/Aruba_DeployGd_HTML/Content/Active%20Directory/Joining_AD_domain.htm

Lukka, K. 2001. Konstruktiivinen tutkimusote. Viitattu 16.4.2021. https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

Network Access Control. N.d. Vmwaren verkkosivut. Viitattu 23.9.2020. https://www.vmware.com/topics/glossary/content/network-access-control

Rouse, M. N.d. PEAP (Protected Extensible Authentication Protocol). Techtraget verkkosivut. Viitattu 2.10.2020. https://searchsecurity.techtarget.com/definition/PEAP-Protected-Extensible-Authentication-Protocol

RADIUS Protocol and Components. 2012. Microsoftin verkkosivut. Viitattu 11.9.2020. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc726017(v=ws.10)?redirectedfrom=MSDN

Robers, H. 2017a. Aruba ClearPass Workshop - Wireless #2 - Installing the ClearPass RADIUS certificate. Youtube-videopalvelu. Julkaistu 22.5.2017. Viitattu 22.10.2020. https://www.youtube.com/watch?v=G7I2JyF8z7w&list=PLsYGHuNuBZcb0xD05v9zdwv7NlUG_8oJS&index=6

Robers, H. 2017b. Aruba ClearPass Workshop - Wired #1 - Wired 802.1X with ArubaOS switch. Youtube-videopalvelu. Julkaistu 12.5.2017. Viitattu 22.10.2020. https://www.youtube.com/watch?v=GWgfHCk-DHMM&list=PLsYGHuNuBZcb0xD05v9zdwv7NlUG_8oJS&index=14

Services. N.d. Aruba network verkkosivut. Viitattu 4.2.2021. https://www.arubanetworks.com/techdocs/ClearPass/6.9/PolicyManager/Content/CPPM_UserGuide/Services/Intro_Services.htm

Soveltavasta tutkimuksesta. N.d. Viitattu 15.4.2021. https://oppimateriaalit.jamk.fi/yamk-kasikirja/soveltavat-tutkimusmenetelmat/

Stone, J. 2017. What is Aruba ClearPass and How Does it Protect Your Network? Kelserin verkkosivut. Viitattu 16.9.2020. https://www.kelsercorp.com/blog/what-is-aruba-clearpass-and-how-does-it-protect-your-network

Using VMware vSphere Web Client to Install ClearPass on a Virtual Machine. N.d. Aruba networks verkkosivut. Viitattu 19.10.2020. https://www.arubanetworks.com/techdocs/ClearPass/6.8/CPPM_GettingStarted/Content/Get_Start_Guide/Virtual%20Appliances/ESX_virtual_applicance.htm#Launch

VMware vSphere Hypervisor (ESXi) Requirements. N.d. Aruba networks verkkosivut. Viitattu 19.10.2020. https://www.arubanetworks.com/techdocs/ClearPass/CP_ReleaseNotes_6.7.0/Content/SystemRequirements/ESXiRequirements.htm

Weselius, H. 2017. Laadullisen tutkimuksen perusteet. Verkkodokumentti. Viitattu 16.4.2021.

Wired Policy Enfrocement ClearPass. 2018. PDF-dokumentti. Aruba a Hewlett Packard Enterprise company. Viitattu 29.3.2021