Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2021

Topi Ketola

IDENTITEETTIPOHJAISEN PÄÄSYNHALLINNAN TOTEUTTAMINEN TIETOVERKOSSA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2021 | 54 sivua

Topi Ketola

IDENTITEETTIPOHJAISEN PÄÄSYNHALLINAN TOTEUTTAMINEN TIETOVERKOSSA

Nykyaikaisissa tietoverkoissa erilaisten laite- ja käyttäjäryhmien määrä kasvaa kasvamistaan, jolloin perinteiset tavat tietoverkon suojaamiseksi eivät riitä. Yrityksen tietoverkon resurssien ja verkkoon yhdistettyjen laitteiden sekä käyttäjien suojaamiseksi on käytettävä nykyaikaisia ratkaisuja, kuten identiteettiin pohjautuvaa pääsynhallintaa.

Opinnäytetyön toimeksiantajana on laivanrakennukseen erikoistunut yritys, Meyer Turku Oy. Varmatoimiset ja turvalliset tietoliikenneyhteydet ovat tärkeässä roolissa kohdeyrityksen ydintehtävän, laivanrakennuksen, mahdollistamisessa.

Opinnäytetyön tavoitteena oli tutustua IEEE 802.1X -standardiin pohjautuvan porttikohtaisen todennuksen käyttämiin protokolliin sekä Cisco Identity Services Engine -pääsynhallintaohjelmiston profilointiominaisuuksiin sekä sen ympärillä oleviin komponentteihin. Identiteettipohjaisen pääsynhallinnan teoriaan perehtymisen jälkeen käsitellään Cisco ISE:n profiloinnin testausta ja käyttöönottoa kohdeyrityksessä. Porttikohtaisen todennuksen ja päätelaitteiden profiloinnin käyttö parantaa yritysverkon tietoturvaa, luo näkyvyyttä tietoverkossa olevien laitteiden ja käyttäjien toimintoihin sekä helpottaa tietoverkon hallintaa.

Työn toteutus alkoi yrityksen tietoverkossa olevien laiteryhmien kartoituksella, minkä jälkeen profiloinnin testaus aloitettiin luomalla profilointipolitiikat testilaitteille. Testausvaiheen tuloksia tarkkailtiin ja tehtiin tarvittavia muutoksia, minkä jälkeen oli mahdollista suorittaa profilointi muille yrityksen tietoverkossa oleville laiteryhmille.

Cisco ISE:n käyttöönotto vahvisti yrityksen tietoverkon turvallisuutta ja vähensi verkon ylläpitäjiltä vaadittavia toimenpiteitä uusien laitteiden kytkeytyessä verkkoon. Profilointisääntöjä on mahdollista hioa vielä yksityiskohtaisemmiksi tulevaisuudessa, jolloin tietoturva paranee entisestään.

ASIASANAT:

ISE, profilointi, pääsynhallinta, tietoverkot

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and communication technology

2021 | 54 pages

Topi Ketola

IMPLEMENTATION OF IDENTITY-BASED NETWORK ACCESS CONTROL IN DATA NETWORK

In modern data networks, the number of different groups of devices and users is growing, leaving traditional ways of protecting a data network insufficient. Therefore, modern solutions, like identity-based network access control is required.

This thesis was assigned by Meyer Turku Oy, a company which specializes in building cruise ships. Many critical functions in shipbuilding rely extensively in data network connections, thus making these connections reliable and secure is important.

Goal of this thesis was to learn theory of IEEE 802.1X port-based network access control and get familiar with Cisco Identity Services Engine security policy management platform's profiling options. Implementation and reporting phase of Cisco ISE profiling follows the theory part.

Implementation of the work began with the mapping of device groups on the company's data network, after which profiling policies were assigned to few test devices which are part of company's device inventory. After successfully profiling the test devices and tweaking the authentication and authorization rules the policies were assigned to all remaining device groups.

The implementation of Cisco ISE strengthened the security of the company's data network and reduced the measures required of network administrators when new devices connected to the network. It is possible to hone the profiling policies into even more detail in the future, with further improvement in security.

KEYWORDS:

access control, data networks, ISE, profiling

SISÄLTÖ

KUVAT

TAULUKOT

KÄYTETYT LYHENTEET

AAA	Authentication, Authorization and Accounting. AAA-malli koostuu protokollista, jotka ovat vastuussa pääsynhallinnassa todennuksesta, valtuutuksesta sekä tilastoinnista.
BOOTP	Bootstrap Protocol. IP-osoitteen automaattiseen jakoon käytetty protokolla.
CDP	Cisco Discovery Protocol. Siirtoyhteyskerroksella toimiva Ciscon yksityisomisteinen tiedonkeräysprotokolla.
Cisco ISE	Cisco Identity Services Engine. Identiteettipohjainen pääsynhallintaohjelmisto.
DHCP	Dynamic Host Configuration Protocol. Jakaa verkon laitteille dynaamisesti konfiguraatioparametreja, muun muassa IP-osoitteen ja oletusyhdyskäytävän.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka yhdistää verkkotunnukset IP-osoitteisiin.
EAP	Extensible Authentication Protocol. Porttikohtaisessa todennuksessa käytettävä viitekehys.
EAP-TLS	EAP with Transport Layer Security. EAP-metodi, joka käyttää todennusmenetelmänä varmenteita.
HTTP	Hypertext Transfer Protocol. Hypertekstin siirtoprotokolla.
IBNS	Identity Based Networking Services. Viitekehys, jota voidaan käyttää erilaisiin todennus- ja valtuutuskeinoihin.
IEEE 802.1X	IEEE:n (Institute of Electrical and Electronics Engineers) ylläpitämä ja kehittämä 802.1X-porttikohtaisen todennuksen standardi.
IP	Internet Protocol. Protokolla, jonka avulla datapaketit reitittyvät oikeisiin kohteisiin.

LAN	Local Area Network. Fyysisesti yhdessä maantieteellisessä sijainnissa sijaitseva pääte- ja verkkolaitteiden muodostama tiedonsiirtoverkko.
LLC	Logical Link Control. Siirtoyhteyskerroksen alikerros.
LLDP	Link Layer Discovery Protocol. Siirtoyhteyskerroksella toimiva tiedonkeräysprotokolla.
MAB	MAC Authentication Bypass. Vaihtoehtoinen todennustapa laitteille, jotka eivät tue 802.1X-todennusta.
MAC	Media Access Control. Ethernet-verkossa olevan laitteen fyysinen osoite, joka toimii yksilöivänä tunnisteena.
MPLS	Multi-Protocol Label Switching. Moniprotokollainen leimakytkentä.
MS-CHAPv2	Microsoftin toinen versio CHAP (Challenge-Handshake Authentication Protocol) -protokollasta. Salasanapohjainen todennusmenetelmä.
NetFlow	Ciscon yksityisomisteinen protokolla tietoverkon liikenteen analysointiin.
OSI	Open Systems Interconnection. ISO:n (International Organization for Standardization) kehittämä malli tietoliikennejärjestelmien suunnitteluun.
OUI	Organizationally unique identifier. MAC-osoitteen ensimmäiset 24 bittiä muodostuvat tästä organisaation yksilöivästä tunnisteesta.
PEAP	Protected Extensible Authentication Protocol. Ciscon, Microsoftin ja RSA Securityn kehittämä EAP-metodi.
RADIUS	Remote Authentication Dial-In User Service. Protokolla, joka huolehtii käyttäjän todennukseen, valtuutukseen ja tilastointiin liittyvän tiedon välittämisestä autentikaattorin ja autentikaatiopalvelimen välillä.

SNMP	Simple Network Management Protocol. Tietoverkkojen hallintaan käytettävä protokolla.
TACACS+	Terminal Access Controller Access-Control System Plus. AAA-mallia hyödyntävä Ciscon yksityisomisteinen protokolla.
TCP	Transmission Control Protocol. Kuljetuskerroksella toimiva yhteydellinen tiedonsiirtoprotokolla.
UDP	User Datagram Protocol. Kuljetuskerroksella toimiva yhteydetön tiedonsiirtoprotokolla.
VLAN	Virtual Local Area Network. Lähiverkon segmentointiin käytettävä verkkotekniikka.

JOHDANTO

Moderneissa tietoverkoissa on kytkettynä paljon erilaisia laitteita ja käyttäjäryhmiä, joille on määritettävä eritasoisia oikeuksia verkon resursseihin tietoturvan säilyttämiseksi. Perinteiset tunnistautumis- ja hallintamenetelmät vaativat runsaasti manuaalista työtä, joten nykyaikaiset verkot vaativat uudenlaista lähestymistapaa asiaan. Identiteettiin pohjautuva pääsynhallinta on oiva keino määrittää, mitkä laitteet pystyvät yhdistämään yrityksen verkkoon ja mihin verkon resursseihin pääsy sallitaan.

Tämän opinnäytetyön aiheena on identiteettipohjaisen pääsynhallinnan toteuttaminen kohdeyrityksen tietoverkossa. Opinnäytetyön toimeksiantajana on Meyer Turku Oy. Aihe valikoitui yrityksessä käynnistyneen projektin myötä, jossa on tarkoituksena ottaa käyttöön Cisco Identity Services Engine -pääsynhallintaohjelmisto. Cisco ISE:n käyttöönotto kokonaisuudessaan olisi ollut liian laaja aihe opinnäytetyötä varten, joten koin sopivaksi valita Cisco ISE:n profilointiosion suunnittelun, testauksen ja käyttöönoton opinnäytetyöni aiheeksi.

Opinnäytetyön tavoitteena on tutustua identiteettipohjaisen pääsynhallinnan toteuttamiseen tietoverkossa, kartoittaa yrityksen verkkoon yhdistetyt laiteryhmät sekä määrittää, miten eri laiteryhmien identiteetti profiloidaan Cisco Identity Services Engine -pääsynhallintaohjelmistossa ja mitkä ovat parhaat tavat laitteiden todennuksessa sekä valtuutuksessa niiden yhdistäessä yrityksen tietoverkon resursseihin.

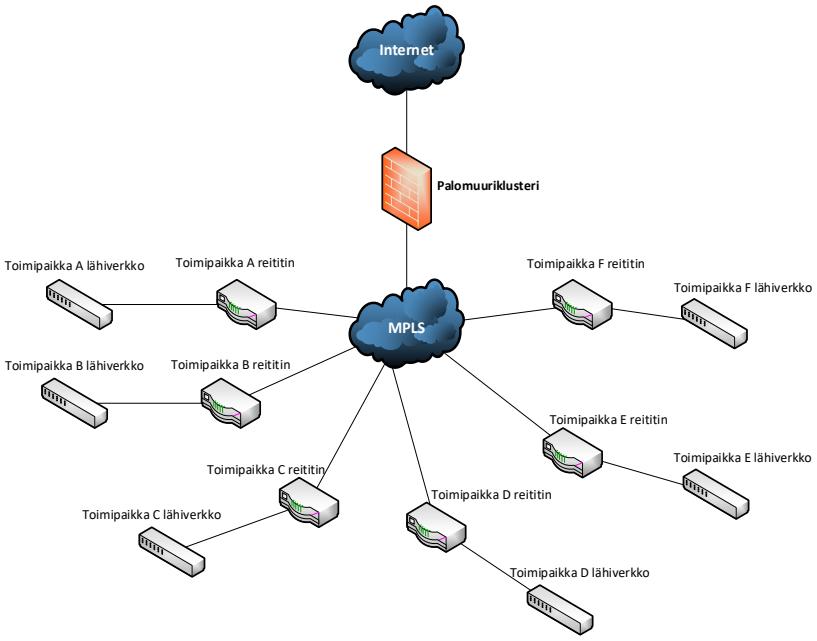
Opinnäytetyö koostuu toimeksiantajana toimivan yrityksen ja sen tietoverkkoarkkitehtuurin esittelystä, teoriaosuudesta, työn toteutuksen osuudesta sekä pohdinnasta. Teoriaosuudessa käsitellään identiteettipohjaisen pääsynhallinnan käyttämiä protokollia ja Cisco ISE:n sekä sen profilointipalvelun ympäröivien komponenttien toimintaa. Toteutusosuudessa käsitellään tarkemmin Cisco ISE:n profiloinnin suunnittelua, testausta ja käyttöönottoa kohdeyrityksessä.

TOIMEKSIANTAJA

Opinnäytetyön toimeksiantaja on Meyer Turku Oy. Yritys on laivanrakennuksen edelläkävijä, joka on erikoistunut rakentamaan risteilyaluksia. Meyer Turku tytäryhtiöineen ja kattavan alihankkijaverkostonsa avustuksella hoitaa risteilyalustensa suunnittelun, rakennuksen ja varustelun. Yritys on tärkeä työllistäjä Varsinais-Suomen alueella ja työllistää yli 2 000 työntekijää. Näin suuressa yrityksessä on tärkeää huolehtia siitä, että yrityksen tietoverkko on segmentoitu järkevästi pienempiin osiin, jotta kaikki verkkoon yhdistetyt laitteet ja käyttäjät eivät voi keskustella keskenään. Turvalliset ja varmatoimiset tietoliikenneyhteydet ovat tärkeä osa onnistunutta laivanrakennuksen kokonaisuutta. (Meyer Turku 2021.)

Meyerillä on kuusi toimipistettä Suomessa, kun lasketaan mukaan tytäryhtiöiden toimipisteet. Tämä opinnäytetyö käsittelee Cisco ISE:n profiloinnin testausta langallisen verkon osalta Meyer Turun telakalla. Päätoimipisteellä suoritetun onnistuneen käyttöönoton jälkeen samat toimenpiteet suoritetaan muilla toimipisteillä, mutta se ei kuulu tähän opinnäytetyöhön.

Toimipisteiden verkot on yhdistetty toisiinsa MPLS (Multi-Protocol Label Switching) -verkkotekniikkaa käyttäen. Kuvassa 1 on yrityksen tietoverkon topologia yksinkertaistettuna.



Kuva 1. Kokonaiskuva toimipisteiden verkkoarkkitehtuurista

TEORIATAUSTA

Cisco ISE eli Identity Services Engine -ohjelmiston toiminnallisuus perustuu usean tietoliikenneprotokollan ja tekniikan hyödyntämiseen. Tässä osiossa kerrotaan perustiedot opinnäytetyöhön liittyvistä protokollista ja tekniikoista.

3.1 OSI-malli

OSI-viitemalli (Open Systems Interconnection Reference Model) on ISO:n (International Organization for Standardization) kehittämä malli tietoliikennejärjestelmien suunnitteluun. Tästä viitemallista pyrittiin luomaan standardi, jonka avulla kaikkien eri laitevalmistajien ja ohjelmistotuottajien tuotteet olisivat sopineet yhteen. Näin ei kuitenkaan tapahtunut eri toimijoiden välisen kilpailun takia ja OSI-mallin mukaisia järjestelmiä ei otettu käyttöön laajalti. (Hakala & Vainio 2005, 126.)

OSI-malli koostuu seitsemästä kerroksesta, joista kukin toimii yhteistyössä yhtä alemman ja ylemmän kerroksen kanssa. OSI-mallin kerrokset ja niiden toiminta selitettynä alimmasta ylimpään:

3.1.1 Fyysinen kerros

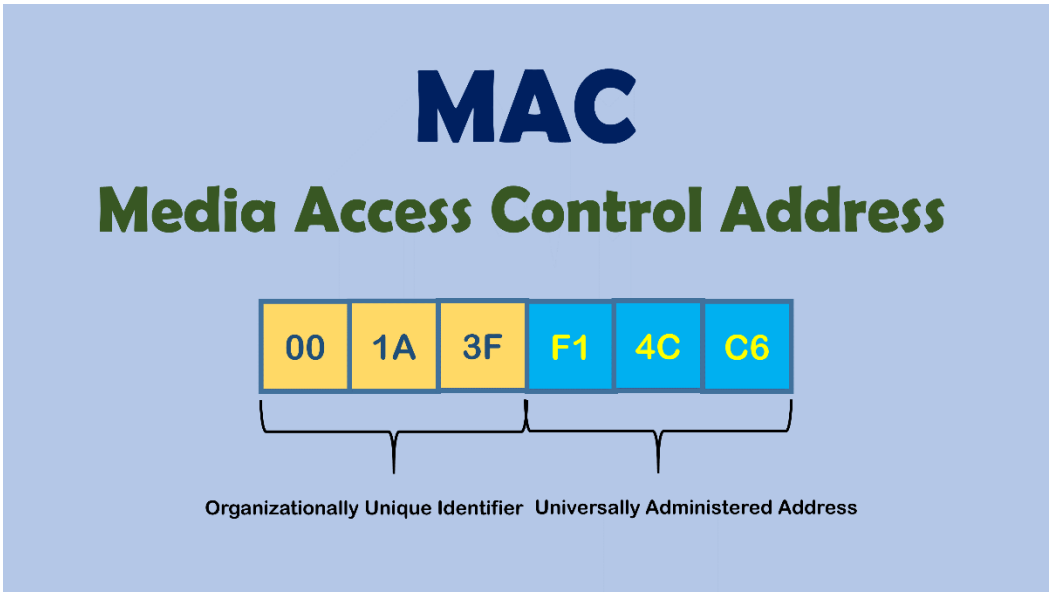
Fyysisen kerroksen tehtävänä on määritellä tiedonsiirron käyttämien sähkösignaalien jännitetasot, liitin- ja kaapelityypit, fyysiset mediat ja hoitaa funktiot, joiden avulla tiedonsiirron fyysinen osuus tapahtuu yhdistettyjen laitteiden välillä. Tämä kerros tarjoaa fyysiset valmiudet tiedon lähettämiselle ja vastaanottamiselle. Tässä kerroksessa toimivia laitteita ovat keskittimet, toistimet ja mediamuuntimet. (Hakala & Vainio 2005, 139; Kaario 2002, 19–20.)

3.1.2 Siirtoyhteyskerros

Siirtoyhteyskerros luo tiedonsiirtoyhteyden verkkokerrokselle ja huolehtii fyysisen kerroksen siirtovirheiden korjauksesta. Tämän kerroksen tehtävänä on myös säännöstellä fyysiselle kerrokselle kulkeutuvan datan määrää tai määritellä etuoikeuksia siirtotien

käyttöön yhdistettyjen laitteiden välillä. Siirtoyhteyskerroksen on mahdollista käyttää useampaa kuin yhtä fyysistä yhteyttä laitteiden välillä. (Kaario 2002, 20.)

Siirtoyhteyskerros voidaan jakaa kahteen alikerrokseen: LLC (Logical Link Control) ja MAC (Media Access Control). LLC-alikerros huolehtii verkkokerroksen protokollien tunnistamisesta ja kapseloinnista sekä siirtovirheiden korjauksesta. MAC-alikerroksen tehtävänä on yksilöidä kaikki Ethernet-verkkoon liitettävät laitteet ja määrittää oikeudet näille laitteille. MAC-osoite koostuu kuudesta kaksinumeroisesta heksadesimaaliluvusta, muodostaen 48-bittisen kokonaisuuden. Näistä 24 ensimmäistä bittiä muodostavat laitevalmistajan uniikin tunnisteen eli OUI:n (Organizational Unique Identifier) ja viimeiset 24 bittiä ovat laitteen juokseva sarjanumero. Kuvassa 2 esitellään MAC-osoitteen rakenne. (Kaario 2002, 20.)



Kuva 2. Esimerkki MAC-osoitteesta. (Medium 2019.)

Tämän kerroksen käytössä olevia protokollia ovat muun muassa Ethernet ja PPP (Point-to-Point Protocol). (Kaario 2002, 20.)

3.1.3 Verkkokerros

Verkkokerroksen tehtävänä on tarjota luotettava tiedonsiirto, riippumatta verkon rakenteesta. Tämän kerroksen vastuulla on valita reitti tietoverkon sisällä kulkeville paketeille

ja priorisoida eri liikennöintimuodot. Edellä mainitun lisäksi tämä kerros voi hoitaa vuonvalvontaa sekä tarkkailla laatuvaatimuksia. Tämän kerroksen käytössä olevia protokollia ovat muun muassa IPv4, IPv6 ja ICMP. (Hakala & Vainio 2005, 139; Kaario 2002, 20.)

3.1.4 Kuljetuskerros

Kuljetusprotokollat huolehtivat tämän kerroksen vastuulla olevista tehtävistä, kuten sovellusten lähettämän datavirran pilkkomisesta osiksi eli segmenteiksi, yhteyden muodostamisesta ja purkamisesta asiakas- ja palvelinohjelmistojen välillä sekä datan perille saapumisesta sopivalla kuittausmenettelyllä. (Hakala & Vainio 2005, 139–140.)

Osa kuljetuskerroksen protokollista ovat kehittyneempiä kuin toiset. Kehittyneemmät protokollat kykenevät tarkkailemaan dataa vastaanottavan laitteen kuormitustilannetta ja ilmoittavat dataa lähettävälle laitteelle kuinka paljon dataa toinen osapuoli voi ottaa vastaan. Jos protokolla suorittaa edellä mainitut toimenpiteet, on se yhteydellinen protokolla, kuten TCP (Transmission Control Protocol). (Hakala & Vainio 2005, 139–140.)

Yhteydellisen protokollan vastakohta on yhteydetön protokolla. Tällainen protokolla suorittaa vain osan toimenpiteistä, jotka yhteydellinen protokolla suorittaa kokonaan. Esimerkkinä toimii UDP (User Datagram Protocol), joka huolehtii vain datavirran pilkkomisesta osiksi. (Hakala & Vainio 2005, 140.)

3.1.5 Istuntokerros

Yhteysjakso- eli istuntokerroksen vastuulla on käyttöoikeuksien tarkistaminen ja järjestelmän suojauksiin liittyvät toimenpiteet. Tässä kerroksessa toimivat ohjelmistot huolehtivat muun muassa vaadittavien kirjautumismetodien sekä salausmenetelmien tarjoamisesta. Nykyaikaisissa järjestelmissä pääosin käyttöjärjestelmä vastaa edellä mainituista tehtävistä. (Hakala & Vainio 2005, 140.)

3.1.6 Esitystapakerros

Tämän kerroksen tehtävänä on määritellä asiakkaan ja palvelimen välillä tapahtuvan sanomaliikenteen muoto. Erilaiset koodausjärjestelmät toimivat esitystapakerroksessa ja tiedonsiirto näiden järjestelmien välillä toteutetaan binäärimerkkijonoina. Tiedonsiirrossa

käytetään vain yhtä tietotyyppiä, joten on määriteltävä kuinka alkuperäiset tietotyypit koodataan binäärimerkkijonoksi ja dekoodataan alkuperäisiksi tietotyypeiksi vastaanottavan sovelluksen päässä. (Hakala & Vainio 2005, 140.)

Esimerkkejä tämän kerroksen määrityksistä ovat eri merkkikoodistot, tietotyyppien esitystavat ja binäärimuotoisen datan käsittelykuvaukset. Nykyaikana käyttöjärjestelmä huolehtii tämän kerroksen tehtävistä. (Hakala & Vainio 2005, 140.)

3.1.7 Sovelluskerros

Sovelluskerroksen vastuulla on hoitaa määrittely kaikille sovellusten ja käyttöjärjestelmien osille, joita ei alemmilla kerroksilla ole määritelty. Nykyaikaisissa lähiverkkojen käyttöjärjestelmissä ja sovelluksissa ei ole mahdollista erotella istunto-, esitystapa- ja sovelluskerrosta, joten ne mielletään yhdeksi kokonaisuudeksi. (Hakala & Vainio 2005, 140–141.)

3.2 TCP/IP-protokollaperhe

TCP/IP-protokollaperhe on liitoksissa kaikkiin OSI-mallin kerroksiin. TCP/IP-protokollaperheessä ei määritellä OSI-mallin kahden alimman kerroksen, siirto- ja fyysisen kerroksen toimintoja, vaan on mahdollista käyttää mitä tahansa näillä kerroksilla toimivaa verkkotekniikkaa. Käytännössä siis TCP/IP-protokollien toiminnallisuus sijoittuu verkkokerroksesta ylöspäin. (Kaario 2002, 22.)

TCP/IP-protokollaperhe tarkoittaa protokollia Internet-protokollan (IP) ympärillä. Tässä protokollaperheessä on viisi kerrosta: fyysinen kerros, siirtokerros, verkkokerros, kuljetuskerros ja sovelluskerros.

Kuvassa 3 esitetään TCP/IP-protokollapino suhteutettuna OSI-malliin. (Kaario 2002, 22.)

Kuva 3. TCP/IP-protokollapino suhteutettuna OSI-malliin. (Kaario 2002, 22.)

3.3 IEEE 802 -standardi

Institute of Electrical and Electronics Engineers (IEEE) on mailman suurin tekniikan alan ammattilaisjärjestö, joka tunnetaan laadukkaista tiedejulkaisuista ja standardien määrittelyistä tekniikan eri osa-alueilla.

IEEE 802 on on ryhmä standardeja, jotka käsittävät fyysisen ja siirtoyhteyskerroksen OSI (Open Systems Interconnection) -mallista. Jokaiselle tämän ryhmän standardille on oma työryhmänsä, joka keskittyy kehittämään ja ylläpitämään kyseistä standardia.

Merkittävimmät IEEE 802 -työryhmän standardeista ovat IEEE 802.1, IEEE 802.3 ja IEEE 802.11. IEEE 802.1 määrittelee arkkitehtuurin lähiverkkoyhteyksille, hallinnalle sekä tietoturvalle. Tärkeä osa tätä standardia on 802.1Q, joka lisää tuen virtuaalilähiverkoille (VLAN), joiden avulla voidaan jakaa fyysinen tietoverkko loogisiin osiin. Tähän standardiin kuuluu myös 802.1X, jota hyödynnetään identiteettiin pohjautuvan pääsynhallinnan toteuttamisessa. IEEE 802.3 määrittää toimintaperiaatteita Ethernet-pohjaisille verkoille. Ethernet-verkkotekniikkaa käytetään enimmäkseen lähiverkoissa, mutta myös kaupunkiverkoissa (MAN) sekä laajaverkoissa (WAN). IEEE 802.11 on langattomien lähiverkkojen (WLAN) kehittämisen standardi. (Kaario 2002, 143–146; Geier 2008, 22.)

3.4 AAA-malli

AAA-malli jakautuu kolmeen eri alueeseen; tietoverkon resursseihin pyrkivän käyttäjän identiteetin todentamiseen eli autentikointiin (engl. authentication), valtuutukseen eli autorisointiin (engl. authorization) jolla määritetään mitkä resurssit ja toimenpiteet käyttäjältä sallitaan, sekä tilastointiin (engl. accounting) verkon resurssien käytöstä. Esimerkkejä AAA-mallia hyödyntävistä protokollista ovat Remote Authentication Dial-in User Service (RADIUS) ja Ciscon yksityisomistuksellinen Terminal Access Controller Access-Control System Plus (TACACS+). (Techopedia.)

3.5 Virtuaalilähiverkko

Lähiverkko (LAN) on pääte- ja verkkolaitteiden muodostama tiedonsiirtoverkko, joka on fyysisesti yhdessä maantieteellisessä sijainnissa. Yrityksen lähiverkko voi koostua esimerkiksi työasemista, verkkotulostimista, palvelimista sekä verkkolaitteista, kuten kytkimistä ja reitittimistä. (Cisco 2018.)

Virtuaalilähiverkkojen (VLAN) avulla fyysinen tietoverkko voidaan jakaa loogisiin osiin. On suositeltavaa, että lähiverkon eri tyyppiset päätelaitteet eritellään omiin virtuaalilähiverkkoihin, jolloin samassa virtuaalilähiverkossa olevat laitteet voivat kommunikoida keskenään, mutta liikennöinti muihin virtuaalilähiverkkoihin ei onnistu, ellei sitä ole erikseen määritelty. Näillä toimenpiteillä parannetaan lähiverkon tietoturvaa sekä pienetään yleislähetysten toimialuetta (broadcast domain). (Cisco 2018.)

3.6 DHCP -protokolla

DHCP (Dynamic Host Configuration Protocol) on protokolla, jota käytetään erilaisten määritysten jakamiseen palvelimelta asiakkaalle. Yleisimpiä DHCP:n käyttötarkoituksia ovat päätelaitteille IP-osoitteen, oletusyhdyskäytävän ja DNS (Domain Name System) -palvelimen osoitteen jakaminen. DHCP:llä voidaan määritellä myös muita parametreja, kuten kellon synkronointiin tarkoitetun aikapalvelimen (Network Time Protocol Server) tai sähköpostipalvelimen (Simple Mail Transfer Protocol Server) IP-osoitteiden jakamisen päätelaitteille. (RFC 2131, RFC 2132).

3.7 DNS-järjestelmä

DNS (Domain Name System) on nimipalvelujärjestelmä, jonka tarkoituksena on yhdistää verkkotunnukset IP-osoitteisiin. Verkkotunnukset ovat ihmisille helpompia muistaa, kuin numeerisessa muodossa olevat IP-osoitteet, joita käytetään verkon laitteiden välisessä kommunikoinnissa. Nimipalvelujärjestelmiä on julkisia ja yksityisiä. Nimipalvelujärjestelmän IP-osoite voidaan tarjota päätelaitteelle esimerkiksi DHCP:tä käyttäen. (RFC 1035, 1987.)

3.8 802.1X-standardi

802.1X on standardi lähiverkossa suoritettavalle porttikohtaiselle todennukselle. Nykyaikana yrityksen tietoverkkoihin yhdistävät muutkin kuin yrityksen omat työntekijät, esimerkiksi alihankkijat, konsultit ja yritysvieraat. Tämän vuoksi on äärimmäisen tärkeää suojata liityntäpisteet, joista päätelaitteet yhdistävät verkkoon. Porttikohtainen todennus on oiva työkalu tähän tehtävään. (Cisco 2011.)

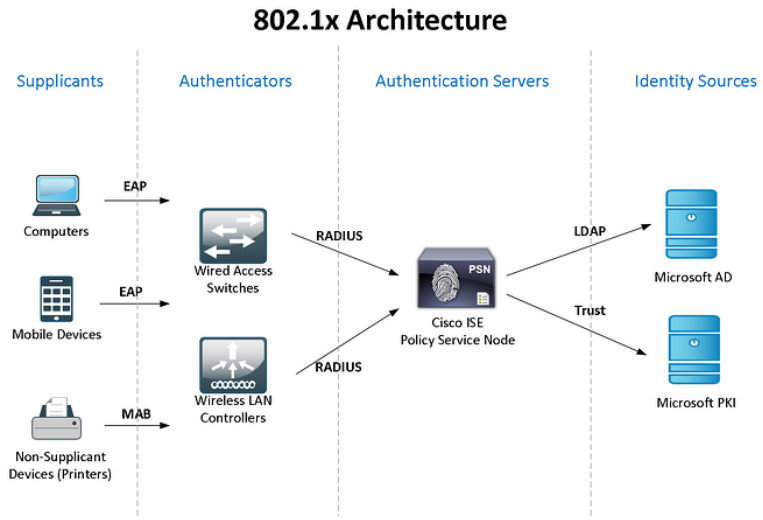
802.1X-standardi toimii OSI-mallin siirtoyhteyskerroksella ja pystyy joko sallimaan tai kieltämään pääsyn päätelaitteelta verkon resursseihin, riippuen käyttäjän tai laitteen identiteetistä. Porttikohtaisen todennuksen ollessa käytössä, verkkokytkin tai langaton tukiasema päästää läpi pelkästään EAPoL (Extensible Authentication Protocol over LAN) liikennettä, jonka avulla todennetaan verkon resursseihin pyrkivä tahon identiteetti. Jos identiteetti todennetaan onnistuneesti, niin autentikaattori sallii muunkin verkkoliikenteen kyseisestä liityntäpisteestä. (Cisco 2011.)

802.1X porttikohtainen todentaminen koostuu kolmesta komponentista:

1. Asiakas (Supplicant): Päätelaitteella suoritettava asiakasohjelma, joka varmistaa loppukäyttäjän identiteetin ja välittää tunnistetiedot autentikaattorille todennusta varten. Windows 10 -käyttöjärjestelmä tukee 802.1X-standardin määrittämistä ilman kolmannen osapuolen ohjelmistoa.
2. Autentikaattori (Authenticator): Laite, joka toimii verkon liityntäpisteenä, yleensä verkkokytkin tai langaton tukiasema. Autentikaattori toimii tiedon välittäjänä asiakkaan ja autentikointipalvelimen välillä.

3. Autentikointipalvelin (Authentication server): Palvelin, joka tarkastaa autentikaattorin välittämät tunnistetiedot ja määrittää asiakkaalle oikeuksiensa mukaisen pääsyn verkon resursseihin.

Porttikohtaiseen todentamiseen on mahdollista integroida erillinen lähde, josta autentikointipalvelin tarkistaa asiakkaan identiteetin oikeellisuuden. Tämä toteutus on usein käytössä nykyaikaisissa identiteettiin pohjautuvissa pääsynhallintajärjestelmissä ja identiteetin lähteenä toimii usein Microsoftin AD (Active Directory), joka on Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu. Kuvassa 4 on esitelty 802.1X-todennuksen arkkitehtuuri. (Lookingpoint 2018.)



Kuva 4. 802.1X:n perusarkkitehtuuri ja erillinen identiteettilähde. (Lookingpoint 2018.)

Seuraavissa alaluvuissa käsitellään 802.1X-standardin mukaisen porttikohtaisen todennuksen käyttämiä protokollia sekä vaihtoehtoisia todennusmenetelmiä, jota käytetään laitteilla, jotka eivät tue 802.1X-standardin mukaista todennusta.

3.8.1 EAP-viitekehys

EAP (Extensible Authentication Protocol) on viitekehys, jota käytetään laajalti porttikohtaisessa todennuksessa. EAP:n arkkitehtuuri luo pohjan todennukselle, jota on helppo muokata omaan käyttöön sopivaksi. EAP toimii OSI-mallin siirtoyhteyskerroksella ja sitä on käytetty paljon PPP-yhteyksissä (Point-to-Point). Tällä kerroksella toimiessaan EAP ei vaadi olemassaolevaa IP-yhteyttä. (Richter & Wood 2015, 40)

EAP-viestien liikennöintiin asiakkaan ja autentikaattorin välillä on käytössä paketointiprotokolla EAPoL (Extensible Authentication Procotol over LAN). Autentikaattorin ja autentikointipalvelimen väliseen liikennöintiin käytetään RADIUS (Remote Authentication Dial-In User Service) -protokollaa. EAP-viitekehyksen mukaisessa todennuksessa varsinainen todennusmenetelmä määritetään vasta silloin, kun autentikaattori pyytää asiakkaalta lisätietoa. Yleisimpiä käytössä olevia EAP-metodeja ovat PEAP, MS-CHAPv2 sekä EAP-TLS. (Richter & Wood 2015, 40)

3.8.2 PEAP-protokolla

PEAP (Protected Extensible Authentication Protocol) on Ciscon, Microsoftin ja RSA Securityn kehittämä EAP-todennustapa, joka parantaa todennuksen turvallisuutta luomalla suojatun tunnelin tietoliikenteelle käyttäen TLS (Transport Layer Security) –protokollaa.

Kyseinen suojattu tunneli muodostetaan suojausvarmenteen avulla, jonka lähettämällä autentikointipalvelin todistaa asiakkaalle luotettavuutensa. PEAP ei vaadi asiakkaan puolelta asiakasvarmennetta, vaan tunnelin määritykseen riittää palvelinvarmenne ja asiakaslaitteelle asennettu juurivarmenne (root certificate), joka on saman varmentajan allekirjoittama, kuin autentikointipalvelimelle asennettu palvelinvarmenne. (Cisco 2011.)

3.8.3 MS-CHAPv2-protokolla

MS-CHAPv2 on Microsoftin toinen versio CHAP (Challenge-Handshake Authentication Protocol) -protokollasta. MS-CHAPv2-todennusta käytetään usein PEAP:n kanssa, jolloin asiakkaan ja autentikointipalvelimen välinen liikenne on salattua. Ilman PEAP:n käyttöä MS-CHAPv2-todennus on alttiina niin kutsutuille sanakirjahyökkäyksille, joissa hyökkääjä yrittää arvata salasanan käymällä kaikki sanakirjan sanat läpi komentosarjan avulla. MS-CHAPv2 on salasanapohjainen todennusmenetelmä, joka tukee sekä asiakkaan, että palvelimen todentamista. PEAP-MSCHAPv2-yhdistelmää käytetään pääosin Microsoftin Active Directory -ympäristöissä. (Cisco 2011.)

3.8.4 EAP-TLS-protokolla

EAP-TLS (EAP with Transport Layer Security) käyttää todennusmenetelmänä varmenteita. Tämä vaatii asiakaslaitteelle asennetun asiakasvarmenteen ja autentikointipalvelimelle asennetun palvelinvarmenteen. EAP-TLS on hyvin tuettu eri valmistajien keskuudessa, joten EAP-TLS tuki löytyy esimerkiksi Ciscon ja Microsoftin RADIUS-palvelimilta. (Geier 2008, 109–110.)

3.8.5 RADIUS-protokolla

RADIUS (Remote Authentication Dial-In User Service) on protokolla, joka huolehtii käyttäjän todennukseen, valtuutukseen ja tilastointiin liittyvän tiedon välittämisestä autentikaattorin (Network Access Server) ja autentikaatiopalvelimen (RADIUS Server) välillä käyttäen UDP-protokollan portteja 1812 ja 1813. (Cisco 2006.)

RADIUS-protokollan prosessissa on mukana todennettava käyttäjä, autentikaattori, autentikointipalvelin ja käyttäjätietokanta. Autentikaattorina voi toimia esimerkiksi verkkokytkin tai langaton tukiasema. Tässä opinnäytetyössä RADIUS-palvelimena toimii Cisco ISE, joka on integroitu kohdeyrityksen Active Directory -palveluun. (Cisco 2006.)

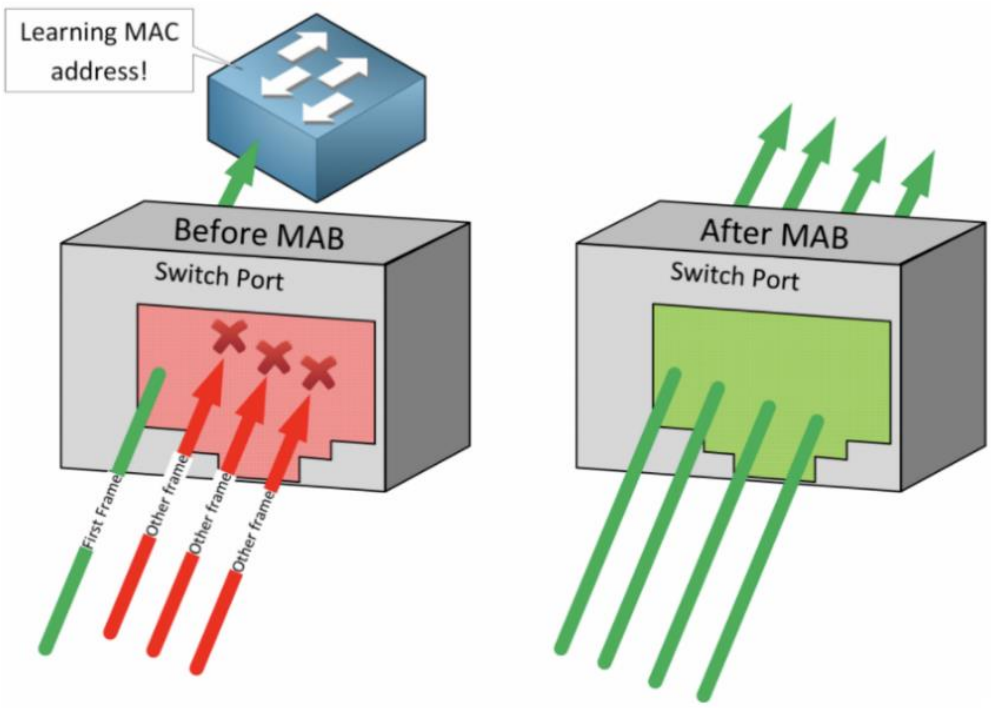
Cisco ISE hyödyntää RADIUS-protokollan CoA (Change of Authorization) -ominaisuutta suorittaessaan laitteiden automaattista profilointia. Kyseinen ominaisuus tarkoittaa, että ISE:n eli RADIUS-palvelimen oppiessa päätelaitteesta lisätietoa sen on mahdollista dynaamisesti muuttaa laitteen oikeuksia verkon resursseihin. (Cisco 2019.)

3.8.6 MAB-todennus

Yleinen tapa tehdä yrityksen tietoverkosta turvallinen on käyttää 802.1X-standardin mukaista porttikohtaista todennusta, mutta kaikkien laitteiden kanssa tämä ei ole mahdollista. Esimerkiksi monet verkkotulostimet, valvontakamerat sekä verkkoon kytkettävät elektroniset sensorit eivät tue 802.1X-protokollaa, jolloin on käytettävä vaihtoehtoista tapaa laitteiden tunnistamiseksi.

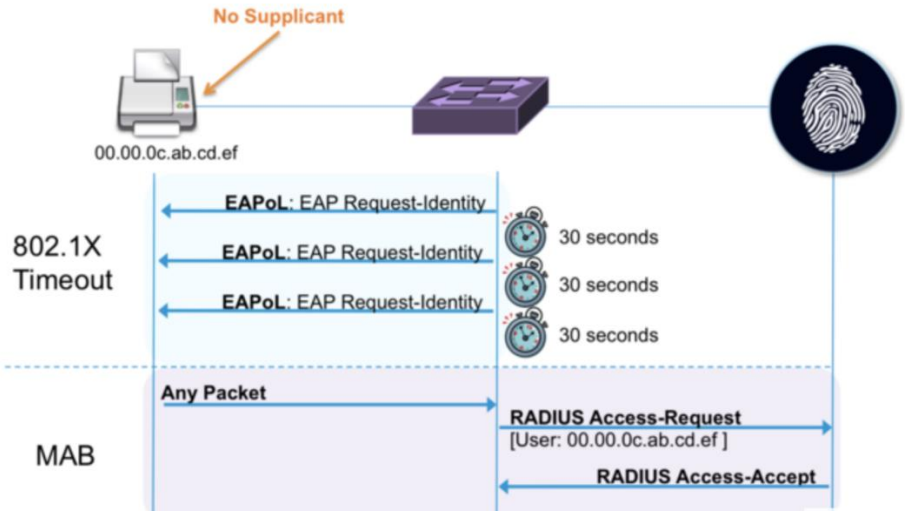
MAB (MAC Authentication Bypass) on hyvä vaihtoehto edellä mainittujen laitetyyppien tunnistukseen. MABin toimintaperiaate on yksinkertainen ja turvallinen. Kun päätelaite

yhdistetään kytkinporttiin ensimmäistä kertaa, MAB sallii vain ensimmäisen kehyksen saadakseen päätelaitteen MAC-osoitteen. Tämän jälkeen MAC-osoite välitetään autentikointipalvelimelle ja tarkistetaan onko kyseisestä osoitteesta liikennöinti sallittu. Jos osoite on sallittujen listalla, niin kytkin päästää muutkin kehykset läpi ja liikennöinti voi alkaa. Kuvassa 5 on visualisoitu MABin toimintaperiaate. (Cisco 2011.)



Kuva 5. MAC Authentication Bypass –toimintaperiaate. (LinkedIn 2019.)

MAB voidaan konfiguroida kahdella eri tavalla. Standalone-määrityksessä käytetään vain MAB-autentikointia päätelaitteen todentamiseen. Fallback-määrityksessä päätelaite pyritään todentamaan ensin 802.1X:n mukaisesti ja tämän epäonnistuessa käytetään MAB-autentikointia laitteen todentamiseksi. Kuva 6 havainnollistaa onnistunutta MAB-autentikointia Fallback-tilassa. (Cisco 2011.)



Kuva 6. Onnistunut MAB-autentikointi. (LinkedIn 2019.)

Oletusasetuksella MAB sallii vain yhden päätelaitteen per kytkinportti ja aiheuttaa turvallisuusrikkomuksen havaitessaan useamman kuin yhden MAC-osoitteen. MAB voidaan määrittää toimimaan erilailla, sillä tietyissä tilanteissa on tarpeen muuttaa tätä toiminnallisuutta, esimerkiksi kun kytkinporttiin on yhdistetty hallitsematon kytkin tai VoIP-puhelin, joka on yhdistetty tietokoneeseen.

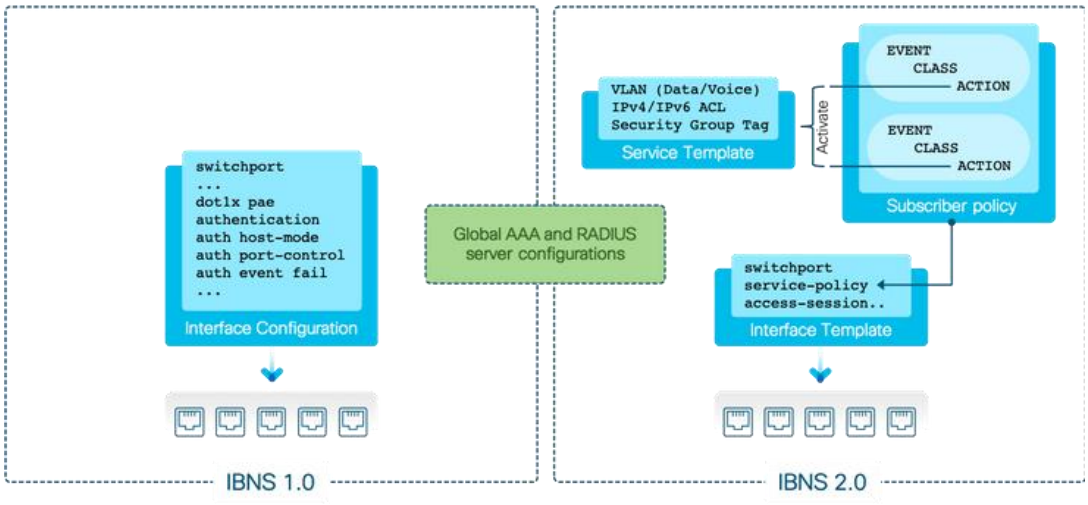
MAB-todennuksessa on useita asetuksia eri skenaarioille. Single-host mode -asetus on käytössä oletuksena, jolloin sallitaan vain yksi MAC-osoite jokaista kytkinporttia kohden. Multi-domain authentication host mode -asetus sallii kaksi MAC-osoitetta jokaista kytkinporttia kohden. Yksi äänensiirtoon tarkoitettuun virtuaalilähiverkkoon (Voice VLAN) ja toinen tiedonsiirtoon tarkoitettuun virtuaalilähiverkkoon (Data VLAN). Tätä asetusta suositellaan käytettäväksi, kun samaan kytkinporttiin on yhdistetty VoIP-puhelin ja tietokone. Multi-authentication host mode -asetuksessa sallitaan lukuisia MAC-osoitteita kytkinporttia kohden ja jokainen MAC-osoite todennetaan yksitellen. Tätä asetusta suositellaan käytettäväksi, kun kytkinporttiin on yhdistetty toinen kytkin. Multi-host mode -asetus sallii lukuisia MAC-osotteita jokaista kytkinporttia kohden, mutta vain ensimmäinen MAC-osoite todennetaan ja kaikki muut sallitaan. (Cisco 2011.)

3.9 IBNS 2.0 -malli

Cisco IBNS 2.0 (Identity Based Networking Services) on moderni ratkaisu yrityksen tietoverkon käyttäjien todennuksen ja pääsynhallinnan konfigurointiin. Yrityksen tietoverkkoon yhdistää nykyaikana monia eri käyttäjiä yrityksen omien työntekijöiden lisäksi, kuten alihankkijoita, ja työntekijätkin mahdollisesti työskentelevät etäyhteyksien kautta, jonka vuoksi on tärkeää pystyä määrittämään käyttäjän identiteettiin pohjautuva pääsy tietoverkon resursseihin. IEEE 802.1X-standardin mukainen porttikohtainen todennus on hyvä lähtökohta edellä mainitun kaltaiselle tietoverkkoarkkitehtuurille, mutta silti tarvitaan paremmin skaalautuva ja joustavampi ratkaisu tietoturvan ylläpitämiseksi. Cisco IBNS 2.0:n avulla tietoverkon ylläpitäjän on helppo konfiguroida verkon aktiivilaitteille erilaisia pääsynhallintapolitiikkoja. Verkon aktiivilaitteilla suoritettava käyttäjien pääsynhallinta on mahdollista toteuttaa IEEE 802.1X-standardin, MABin tai verkkoselainpohjaisen autentikoinnin avulla. (Cisco 2014.)

Cisco IBNS:n avulla on mahdollista määrittää verkkokytkimen portteihin konfiguraatiomalli (template), jolloin porttiin yhdistävälle käyttäjälle voidaan muun muassa osoittaa pääsy johonkin tiettyyn VLANiin tai tarvittaessa sulkea kaikki portista kulkeva liikenne.

Cisco IBNS 2.0 on uudistettu versio IBNS 1.0:sta. Merkittävimmät uudistukset IBNS 2.0:ssa on mahdollisuus määrittää käytettäväksi useita AAA-palvelimia, keskitetty pääsynhallintakonfiguraatioiden määrittely kytkimellä, verraten IBNS 1.0:n porttikohtaiseen määrittelyyn. Kuvassa 7 visualisoidaan näiden versioiden erot. (Cisco 2014.)



Kuva 7. Erot IBNS 1.0 ja IBNS 2.0 välillä (Cisco Community 2021.)

3.10 Dynamic VLAN Assignment

Dynamic VLAN Assignment -ominaisuus tarjoaa mahdollisuuden siirtää loppukäyttäjä tiettyyn virtuaalilähiverkkoon dynaamisesti. Virtuaalilähiverkko, johon käyttäjä siirretään, riippuu ISE:ssä tehdyistä valtuutuspolitiikoista, jotka määrittävät ohjauksen tiettyyn verkkosegmenttiin riippuen loppukäyttäjän tarjoamasta identiteetistä todennusvaiheessa. (Integrating IT 2018.)

3.11 Cisco Identity Services Engine (ISE) -pääsynhallinta-alusta

Cisco Identity Services Engine on identiteettitietoinen pääsynhallinta-alusta, johon verkon ylläpitäjä voi luoda kattavia pääsynhallinta- ja turvallisuuskäytäntöjä. Cisco ISE:n arkkitehtuurin avulla voidaan määrittää eritasoiset oikeudet kaikille erilaisille laite- ja käyttäjäryhmille, jotka yhdistävät yrityksen tietoverkkoon. Tämän lisäksi ISE kerää reaaliaikaista tietoa verkon tapahtumista. Toisin sanoen Cisco ISE yhdistää kaikki AAA-mallin palvelut samalle alustalle. (Cisco Identity Services Engine Administrator Guide 2021.)

Cisco ISE on skaalautuvuutensa ansiosta pätevä pääsynhallintaratkaisu kaiken kokoisiin yrityksiin ja tietoverkkoihin. Cisco ISE on saatavilla fyysisenä palvelimena sekä virtuaalikoneena. Verkon aktiivilaitteet toimivat tiiviissä yhteistyössä ISE:n kanssa ja tämän synergian avulla verkkoon pyrkivien tahojen identiteetti voidaan varmistaa tarkasti ja täten myöntää pääsy kyseiselle identiteettiryhmälle tarkoitettuihin resursseihin. Tämän myötä onnistutaan parantamaan yrityksen verkon tietoturvaa ja tehostamaan palveluiden tuottamista. (Cisco Identity Services Engine Administrator Guide 2021.)

Seuraavaksi on selitetty Cisco ISE -pääsynhallinta-alustan tärkeimmät ominaisuudet.

Verkon aktiivilaitteiden hallinta. ISE käyttää TACACS+-protokollaa verkon aktiivilaitteiden konfiguraation valvontaan ja tarkasteluun. Täten voidaan tarkasti määritellä, kenellä on pääsy verkkolaitteiden hallintaan ja minkä tasoiset oikeudet käyttäjällä on. (Cisco Identity Services Engine Administrator Guide 2021.)

Turvallinen langaton verkkoyhteys vieraille. Cisco ISE mahdollistaa muiden kuin yrityksen työntekijöiden, kuten vieraiden, alihankkijoiden, konsulttien ja asiakkaiden tunnistamisen yrityksen verkkoon liityttäessä ja täten voidaan määrittää kullekin sopivat oikeudet

verkon resursseihin, riskeeraamatta tietoturvallisuutta. Tässä tapauksessa käyttäjän todentaminen tapahtuu yleensä selainpohjaisella todennuksella, jota kutsutaan WebAuth-menetelmäksi. (Cisco Identity Services Engine Administrator Guide 2021.)

Verkon läpinäkyvyys. Cisco ISE luo läpinäkyvyyttä verkossa oleviin laitteisiin ja helpottaa eritasoisten pääsyjen sallimista. ISE:n toiminta kattaa kaikki yhteystyypit, oli se sitten langaton, langallinen tai VPN (Virtual Private Network) -yhteys. Cisco ISE käyttää monenlaisia sensoreita kerätäkseen tietoa verkkoon liitetyistä päätelaitteista. Protokollia, joita ISE:n sensorit käyttävät hyödykseen ovat muun muassa DHCP, HTTP, NetFlow sekä RADIUS. Päätelaitteista kerättäviä tietoja ovat muun muassa IP-osoite, MAC-osoite, laitemerkki ja käyttöjärjestelmän tyyppi. (Cisco Identity Services Engine Administrator Guide 2021.)

Langallisen verkon turvallisuus. ISE:n yhteensopivuus usean eri autentikointiprotokollan kanssa mahdollistaa turvallisen verkkoyhteyden myös langallisesti. Langallinen verkkoyhteys turvataaan usein määrittelemällä ISE käyttämään esimerkiksi 802.1x-, RADIUS- tai MAB-protokollaa. (Cisco Identity Services Engine Administrator Guide 2021.)

Verkon segmentointi. Cisco ISE kerää paljon tietoa verkkoon yhdistävistä laitteista, jota voidaan käyttää hyödyksi verkon segmentoinnissa ja laitteiden automaattisessa siirtämisessä oikeaan virtuaalilähiverkkoon. (Cisco Identity Services Engine Administrator Guide 2021.)

Uhkien rajoittaminen. Cisco ISE tarkkailee jatkuvasti verkkoon yhdistettyjen laitteiden toimintaa ja kykenee dynaamisesti muokkaamaan laitteelle myönnettyjä oikeuksia, jos laite on saastunut esimerkiksi haittaohjelman myötä. (Cisco Identity Services Engine Administrator Guide 2021.)

Turvallisuuden ekosysteemin integraatiot. Cisco ISE voidaan määrittää käyttämään pxGrid-ominaisuutta, joka mahdollistaa oleellisen tiedon välittämisen muille verkonhallintaohjelmistoille. (Cisco Identity Services Engine Administrator Guide 2021.)

Cisco ISE:n käyttöönoton toteutukseen on eri tapoja. ISE voidaan ottaa käyttöön yksittäisenä (standalone deployment) tai hajautettuna (distributed deployment) toteutuksena. ISE:n toiminta koostuu hallinnasta (administration), politiikkapalvelusta (policy service), valvonnasta (monitoring) sekä haluttaessa verkon hallinnallisen tiedon välityksestä eri verkonhallintaohjelmistojen välillä käyttäen pxGrid-protokollan viitekehystä. Yksittäisessä toteutuksessa sama noodi hoitaa kaikki edellä mainitut toiminnot. Hajautetussa

toteutuksessa toimintojen työkuormaa voidaan jakaa eri noodien välillä, jolloin myös vikasietoisuus paranee. (Cisco Identity Services Engine Administrator Guide 2021.)

Seuraavaksi on selitetty tarkemmin eri noodien toiminnot. Policy Administration (PAN) -noodi käsittelee kaikki AAA-mallin palvelut eli todennuksen, valtuutuksen ja tilastoinnin. Lisäksi sen kautta hoidetaan kaikki ISE:n hallintaan liittyvät toimenpiteet. Hajautetussa toteutuksessa voi olla korkeintaan kaksi PAN-tilassa olevaa noodia, toisen ollessa ensisijainen ja toisen toissijainen. (Cisco Identity Services Engine Administrator Guide 2021.)

Policy Service (PSN) -noodi myöntää käytännössä pääsyn verkkoon, tarkistaa päätelaitteiden kunnon (posture) ja muita tärkeitä attribuutteja, määrittää vieraskäytön ja profilointipalvelut. Hajautetussa toteutuksessa ainakin yhden noodin on oltava politiikkapalvelu-tilassa. Jos useita noodeja on tässä tilassa, niistä on mahdollista muodostaa noodiryhmä, joka parantaa toteutuksen vikasietoisuutta. (Cisco Identity Services Engine Administrator Guide 2021.)

Monitoring Node (MnT) -noodi vastaa edellä mainittujen noodien tapahtumien ja toimenpiteiden ylöskirjaamisesta lokiin ja tarjoaa lisäksi edistyksellisiä työkaluja verkon valvontaan ja vianselvitykseen. Tämä noodi yhdistää kaiken keräämänsä datan ja muodostaa siitä selkeästi ymmärrettäviä raportteja. Yhden noodin pitäisi aina olla MnT-tilassa ja korkeintaan kaksi noodia voi olla tässä tilassa yhtäaikaisesti, jolloin ne ovat ensi- ja toissijaisessa muodossa, joka parantaa vikasietoisuutta. Ciscon suositus on, että yksi noodi ei ole vastuussa politiikkapalvelusta sekä valvonnasta. (Cisco Identity Services Engine Administrator Guide 2021.)

pxGrid-noodi mahdollistaa verkonhallintaa koskevan datan välittämisen Cisco ISE:n ja muiden verkonhallintaohjelmistojen välillä, huolimatta siitä ovatko ne muiden valmistajien vai Ciscon omia ohjelmistoja. Cisco pxGrid sallii myös muiden valmistajien ohjelmistojen suorittaa toimenpiteitä, kuten laitteen tai käyttäjän asettaminen karanteeniin havaitessaan tietoturvapoikkeamia verkossa. Hajautetussa toteutuksessa on mahdollista olla useampi pxGrid-noodi käytössä, jolloin parannetaan toteutuksen vikasietoisuutta. (Cisco Identity Services Engine Administrator Guide 2021.)

3.11.1 Profiling Service

Cisco ISE:n profilointipalvelu (Profiling Service) tarjoaa dynaamisen tavan tunnistaa ja luokitella kaikki verkkoon liitetyt laitteet. ISE:n anturit (ISE probes) keräävät tietoa kaikista verkon laitteista, jonka avulla ISE luo sisäisen tietokannan eri laiteryhmien profiileista. Cisco ISE:ssä on sisäänrakennettuja politiikkoja, joiden perusteella laitteet voidaan jakaa erilaisiin ryhmiin laitteen tyypistä riippuen. Näiden sisäänrakennettujen politiikkojen lisäksi on suotavaa luoda uusia, juuri omaan tietoverkkoon ja sen laitekantaan sopivia politiikkoja. Cisco ISE:n käyttömahdollisuudet eivät rajoitu pelkästään toimistoverkkoihin, joissa on verkon aktiivilaitteiden lisäksi vain työasemia, matkapuhelimia, palvelimia ja verkkotulostimia. Sen avulla on mahdollista tunnistaa kattavasti erilaisia IoT (Internet of Things) -laitteita, kuten valvontakameroita, lämmityksen, ilmanvaihdon ja ilmastoinnin hallintalaitteita (HVAC) sekä valaistuksen hallintaan käytettäviä laitteita.

Laitteen profiilin tunnistamisen jälkeen on mahdollista joko myöntää pääsy juuri oikeisiin verkon resursseihin, riippuen oikeuksista jotka kyseiselle laiteryhmälle on määritetty tai vaihtoehtoisesti evätä pääsy verkon resursseihin kokonaan. Esimerkiksi, jos päätelaite profiloidaan verkkotulostimeksi, se voidaan automaattisesti siirtää verkkotulostimille tarkoitettuun virtuaalilähiverkkoon. On myös mahdollista määrittää työntekijälle eri tasoisia oikeuksia verkon resursseihin, riippuen siitä millä laitteella työntekijä yhdistää verkkoon. Voidaan esimerkiksi myöntää täydet oikeudet verkon resursseihin, kun työntekijä yhdistää verkkoon yrityksen toimialueeseen liitetyllä työasemalla ja rajata pääsyä, kun yhdistäminen tapahtuu henkilökohtaisella matkapuhelimella. Politiikkapalvelu-noodi (PSN) suorittaa edellä mainitut toimenpiteet. (Cisco Community 2021.)

3.11.2 ISE Probes

ISE:n probeja eli antureita on mahdollista määrittää keräämään dataa päätelaitteista monella eri tavalla. ISE:n profilointipalvelun tukemien anturien toiminta on selitetty seuraavaksi.

RADIUS probe kerää ja koostaa asiakkaiden RADIUS-palvelimelle lähettämää dataa ja kerää tästä oleellisia atribuutteja profilointia varten. Esimerkkejä RADIUS proben keräämästä datasta ovat MAC- ja IP-osoite, päätelaitteen tyyppi, autentikoivan laitteen tunniste ja portti, johon päätelaite on kytketty. (Cisco Community 2021.)

Laitesensori (Device Sensor) kerää päätelaitteista tietoa muun muassa CDP, LLDP, DHCP ja HTTP –protokollien avulla ja välittää nämä tiedot AV (Attribute-Value) -pareina RADIUS-protokollan tilastointipakettien sisällä ISE:n politiikkapalvelunoodille. ISE:n profilointipalvelun on mahdollista kerätä ja jäsennellä nämä AV-parit ainoastaan RADIUS-anturia käyttämällä, joten laitesensorin käyttö vaatii RADIUS proben olevan määritettynä. Laitesensori on tuettu ominaisuus useissa Cisco Catalyst -sarjan kytkimissä ja langattoman verkon kontrollereissa. (Cisco Community 2021.)

SNMP (Simple Network Monitoring Protocol) Trap probea käytetään ilmoittamaan ISE:lle päätelaitteen yhdistämisestä verkkoon tai yhteyden katkeamisesta ja laukaisemaan SNMP Query proben toiminnan. SNMP Trap proben toiminta vaatii määrityksen kytkimelle tai langattoman verkon kontrollerille, jotta kyseiset ilmoitukset välitetään ISE:n politiikkapalvelunoodille. SNMP Trap probea ei ole tarve käyttää, jos RADIUS probe on käytössä, sillä RADIUS-protokollan Accounting Start -viesti suorittaa saman tehtävän, eli aktivoi SNMP Query proben. SNMP Trap probea suositellaan käytettäväksi esimerkiksi ennen RADIUS-protokollan käyttöönottoa tai tilanteessa, jossa halutaan saada vain näkyvyys verkkoon, eikä haluta suorittaa valtuutuksia tai tilastointia tunnistetuille laitteille. (Cisco Community 2021.)

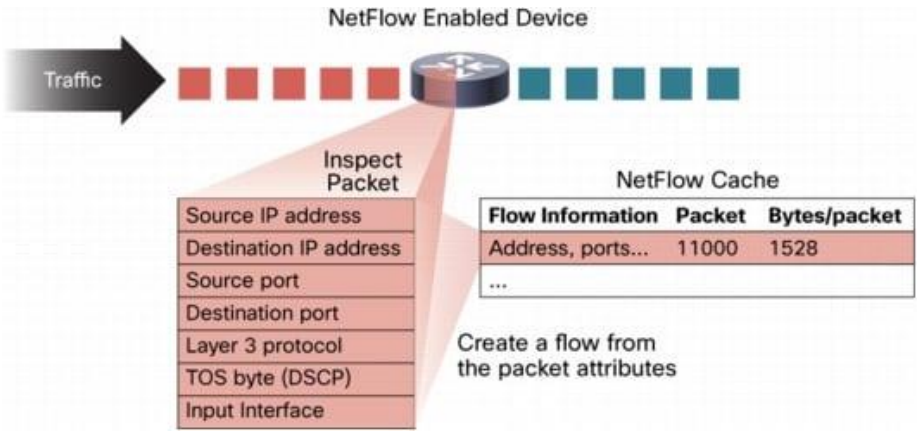
SNMP Query probea käytetään pyyntöjen lähettämisessä verkkokytkimille ja langattoman verkon kontrollereille, jotta ne jakaisivat päätelaitteista keräämäänsä tietoa ISE:lle. Näiden verkkolaitteiden keräämä tieto sijaitsee SNMP MIB:ssä (Management Information Base). ISE:n politiikkapalvelunoodi voi suorittaa SNMP Queryn joko System Querynä, joka on yleensä ajastettu tapahtumaan tietyn väliajoin ja silloin tietoa haetaan useammassa kytkinportissa olevasta päätelaitteesta tai vaihtoehtoisesti Interface Querynä, jolloin haetaan vain tietystä kytkinportista tietoa. (Cisco Community 2021.)

DHCP probet keräävät erilaisia attribuutteja DHCP paketeista. Kyseisiä attribuutteja voidaan kerätä käyttämällä DHCP probea tai DHCP SPAN (Switch Port Analyzer) probea. DHCP probea käytetään silloin, kun asiakkaan lähettämä DHCP-pyyntö välittyy suoraan ISE:n politiikkapalvelunoodille. Tämä toiminnallisuus on mahdollista toteuttaa konfiguroimalla verkkolaitteen DHCP Relay –toimintoon Cisco ISE:n IP-osoite. DHCP SPAN probea käytetään usein silloin, kun DHCP Relay –toiminto ei ole käytettävissä ja tässä tapauksessa kytkinportin tietoliikenne peilataan Cisco ISE:n politiikkapalvelunoodia kohti. (Cisco Community 2021.)

HTTP probe kerää päätelaitteesta tietoa sen yhdistäessä verkkopalvelimeen. Päätelaitteella käytettävä verkkoselain välittää tietoja verkkopalvelimelle käyttäen HTTP-pyynnön otsikkokenttää, joka tunnetaan nimellä User-Agent. Näitä tietoja ovat esimerkiksi päätelaitteen käyttöjärjestelmä sekä käytettävän verkkoselaimen valmistaja ja versionumero. Tämä otsikkokenttä on tärkein attribuutti, jonka HTTP probe kerää. ISE kerää tiedot tästä otsikkokentästä esimerkiksi URL-uudelleenohjauksen tai RADIUS proben laitesensorin avulla. (Cisco Community 2021.)

DNS proben tarkoituksena on selvittää FQDN (Fully Qualified Domain Name) –arvo käyttäen nimipalvelujärjestelmän Reverse Lookup -toimintoa. Selvittääksen päätelaitteen FQDN-arvon DNS proben on tiedettävä laitteen IP-osoite ja siihen liitetty MAC-osoite. DNS probea ei ole välttämätön käyttää, sillä FQDN-arvo voidaan usein selvittää käyttämällä muita ISE:n probeja. (Cisco Community 2021.)

NetFlow on Ciscon yksityisomisteinen protokolla tietoverkon liikenteen analysointiin. NetFlow pitää erikseen aktivoida verkon aktiivilaitteissa, kuten verkkokytkimissä, reitittimissä ja langattoman verkon kontrollereissa. Nämä aktiivilaitteet keräävät tietoa niiden läpi kulkevasta tietoliikenteestä ja välittävät ne NetFlow collector-palvelimelle, jonka tehtävänä on koostaa näistä tiedoista erilaisia raportteja. Vakiona NetFlowin keräämät tiedot lähetetään palvelimelle UDP-protokollan porttia 9996 käyttäen. NetFlow kerää oleellista tietoa verkkoliikenteestä, kuten kuvasta 8 selviää. (Cisco Community 2021.)

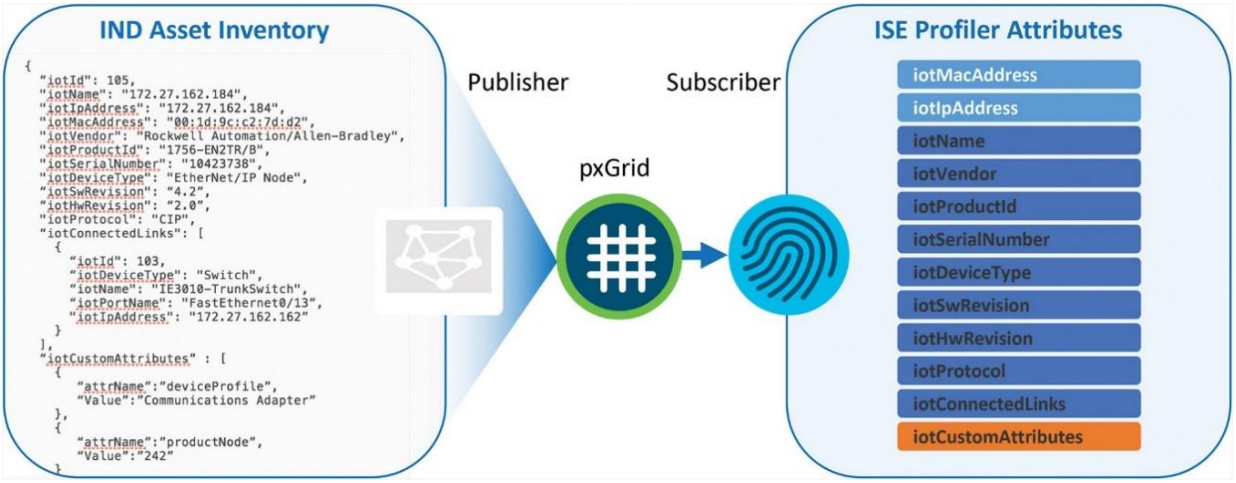


Kuva 8. NetFlow-protokollan toiminta (Cisco, 2012).

Network Scan proben toiminta pohjautuu avoimeen lähdekoodiin perustuvaan Network Mapper -ohjelmistoon. NMAP on työkalu tietoverkkojen skannaukseen ja sen avulla saadaan kattavaa tietoa verkkoon yhdistäneistä päätelaitteista. NMAP voi suorittaa esimerkiksi käyttöjärjestelmän skannauksia, josta selviää päätelaitteen käyttöjärjestelmä tai vaihtoehtoisesti SNMP porttien skannauksen, ja näiden porttien ollessa avoinna tämä probe voi kysyä lisätietoa päätelaitteesta. SNMP porttien skannaus on koettu hyödylliseksi varsinkin SNMP-protokollaa tukevien verkkotulostimien tai kameroiden osalta. Tämä on ainoa ISE:n probeista, jonka toimintaa kuvaillaan aktiiviseksi, sillä muut probet eivät ole suorassa yhteydessä päätelaitteisiin. (Cisco Community 2021.)

Active Directory (AD) proben avulla verkkoon yhdistettyjen ja yrityksen toimialueeseen liitettyjen päätelaitteiden käyttöjärjestelmistä saadaan vielä tarkempaa tietoa, kuten käyttöjärjestelmän versio ja Service Pack-tiedot. Tämän proben avulla on myös helppo erotella yrityksen toimialueeseen liitetyt päätelaitteet muista päätelaitteista. AD probe käyttää päätelaitteen isäntänimeä (hostname) hakiessaan vastaavuutta yrityksen toimialuepalvelimelta. (Cisco Community 2021.)

pxGrid-probe hyödyntää ISE:n pxGrid-noodia päätelaitteista kerättyjen tietojen välityksessä muiden verkonhallintaohjelmistojen välillä. Tiedonvälityksessä mukana olevat osapuolet joko jakavat tietoa (publish) tai vastaanottavat jaettua tietoa (subscribe). Tämän proben keräämät tiedot sisältävät muun muassa IP- ja MAC-osoitteen, laitevalmistajan, tuotekoodin, sarjanumeron ja laitteen tyypin. Laitevalmistajien on lisäksi mahdollista jakaa ISE:lle haluamiaan tietoja päätelaitteista käyttäen kustomoituja attribuutteja (Custom Attributes), joka mahdollistaa periaatteessa minkä tahansa päätelaitteen arvon seuraamisen ISE:ssä. pxGrid probea käytettiin aluksi Cisco IND:n (Industrial Network Director) -verkonhallintaohjelmiston kanssa, jonka tehtävänä on kerätä kattavaa tietoa teollisuusverkkoon (Industrial Ethernet) yhdistetyistä laitteista. Nykyään Cisco IND -verkonhallintaohjelmistossa on käyttöliittymä, joka mahdollistaa tämän tiedon jakamisen Cisco ISE:lle ja tiedon hyväksikäyttämisen profiloinnissa. Kuvassa 9 on esimerkki teollisuusverkon IoT-laitteesta kerätyistä tiedoista.



Kuva 9. ISE:n vastaanottamat tiedot IND:ltä. (Ciscopress 2019.)

TOTEUTUS

Opinnäytetyön toteutus alkoi yrityksen päätoimipisteen tietoverkkoon yhdistettyjen laitteiden kartoituksella. Kartoitus suoritettiin arkipäivänä toimistoajan ulkopuolella ja verkkoon yhdistettyjä laitteita oli kyseisenä ajankohtana tuhansia. Laitteet yksilöitiin MAC -osoitteen perusteella.

Kyseisessä toimipisteessä on paljon erilaista toimintaa tietoverkon näkökulmasta, kuten taloautomaatio-, valvontakamera-, teollisuusautomaatio-, valaistuksen ohjaus- ja sähköisiä lukitusjärjestelmiä sekä ihan perinteisiä toimistoympäristöjä, joissa sijaitsee työasemia ja verkkotulostimia. Toimipisteen sisältäessä näin laajan kirjon eri funktioista vastaavia ympäristöjä, on selvää, että erilaisia laiteryhmiä on paljon. Eri laiteryhmien suuri määrä tarkoittaa sitä, että Cisco ISE:ssä on luotava useita erilaisia profilointisääntöjä, jotta kaikille laiteryhmille saadaan määritettyä sopivat oikeudet yrityksen tietoverkon resursseihin.

Laitekartoituksen jälkeen alkoi suunniteluvaihe, jossa määriteltiin kuinka eri laiteryhmät todennetaan niiden yhdistäessä verkkoon.Laitteiden todennukseen on useita eri tapoja. Tässä opinnäytetyössä on tarkoituksena käyttää 802.1X-protokollaan perustuvaa todennusmenetelmää kaikilla yrityksen toimialueeseen liitetyillä työasemilla ja muilla tätä protokollaa tukevilla laiteryhmillä. 802.1X-todennuksen lisäksi käytetään MAB-todennusta, jolloin laitteet voidaan tunnistaa niiden MAC OUI -arvon perusteella. Autentikointiprosessiin kuuluu, että päätelaite yrittää ensin autentikointia MAB-todennusta käyttäen ja tämän epäonnistuessa suorittaa autentikoinnin loppuun 802.1X-standardin mukaista todennusta käyttäen.

Tämän opinnäytetyön keskiössä on muutaman eri laiteryhmän profiloinnin testaaminen ennen varsinaista profiloinnin käyttöönottoa tuotantokäytössä olevassa tietoverkossa. Testattaviin päätelaitteisiin kuuluu yrityksen toimialueeseen liitetty työasema, työaikapääte sekä kaksi erilaista valvontakameraa. Työasemat profiloidaan 802.1X-standardin mukaisesti ja muut laitteet määrittämällä niille MAB-profilointi Cisco ISE:ssä.

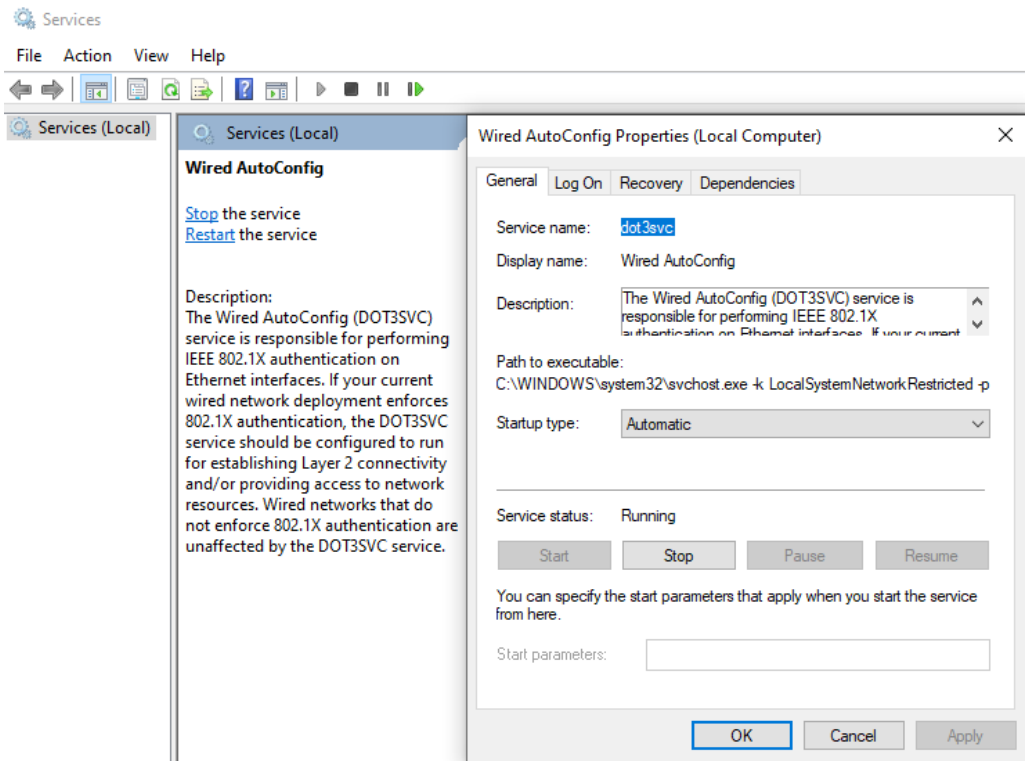
4.1 Työasemien pääsynhallintakonfiguraatiot

Yrityksen toimialueeseen liitetyt työasemat on määritettävä käyttämään 802.1X-todennusta, jota Windows 10 -käyttöjärjestelmä tukee natiivisti. Tämän lisäksi on olemassa myös kolmannen osapuolen ohjelmistoja, joiden avulla voidaan määritellä 802.1X-todennus käyttöön. Tämän opinnäytetyön kohdeyrityksessä käytetään Windows 10 -käyttöjärjestelmän natiivia 802.1X-asiakasohjelmaa.

Aluksi 802.1X-todennuksen konfiguraatiomuutokset suoritettiin omalla työasemallani muuttamalla paikallisia asetuksia ja testattiin, että todentaminen onnistuu suunnitellusti. Testausvaiheen jälkeen kyseiset konfiguraatiomuutokset laitettiin yleisesti jakoon yrityksen työasemille ryhmäkäytännön avulla. Konfiguraatiomuutokset tehtiin yrityksen toimialueen ohjauspalvelimen (engl. Domain Controller) ryhmäkäytäntöjen hallintakonsolissa (engl. Group Policy Management Console).

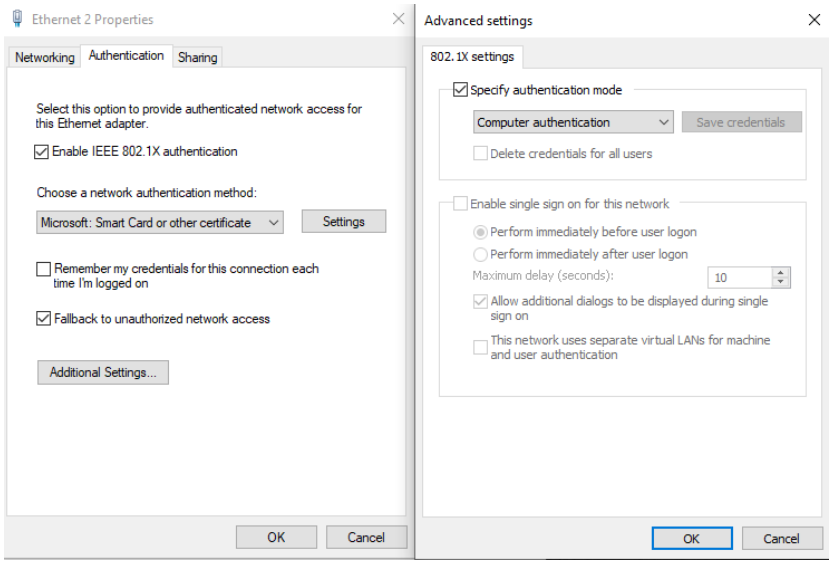
Windows 10 -käyttöjärjestelmäpohjaiset työasemat vaativat seuraavat muutokset, jotta 802.1X-todennusta voidaan käyttää:

Wired Autoconfig -palvelu on aktivoitava ja määritettävä käynnistymään automaattisesti. Tämä määritys suoritetaan Windowsin Services-valikosta, kuten kuvassa 10 esitetään.



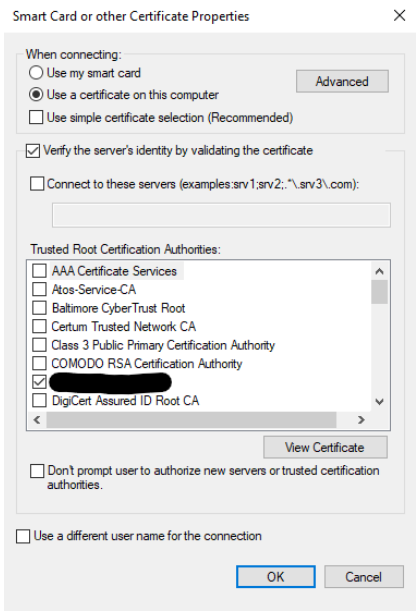
Kuva 10. Wired Autoconfig -palvelun käynnistäminen

Kuvassa 11 esitetään, kuinka työaseman verkkokortin asetuksista aktivoidaan 802.1X-todennus ja määritetään, että todennukseen käytetään yrityksen työasemille jaettua laitevarmennetta.



Kuva 11. 802.1X-todennuksen aktivointi työaseman verkkokortin asetuksissa

Kuvassa 12 esitetään, kuinka työaseman verkkokortin asetuksissa määritellään 802.1X-todennuksessa käytettävän juurivarmenteen myöntäjä. Kaikille yrityksen toimialueeseen liitetyille työasemille on jaettu laitevarmenne, jonka myöntäjä on valittuna kuvassa 12, joten oli loogista käyttää kyseistä laitevarmennetta 802.1X-standardin mukaisessa todennuksessa.



Kuva 12. Todennukseen käytettävän laitevarmenteen myöntäjän valinta

4.2 Verkkolaitteiden pääsynhallintakonfiguraatiot

Yrityksen lähiverkkolaitteisto koostuu pääosin Ciscon verkkokytkimistä ja langattomista tukiasemista. Testikäytössä oli Cisco Catalyst 2960x ja Cisco Catalyst 9300 -sarjan verkkokytkimet, joille määritimme 802.1X ja MAB-todennukselle vaadittavat konfiguraatiot. Päätelaitteina testausvaiheessa oli työaikapääte, kaksi valvontakameraa, työasema jota ei ole liitetty yrityksen toimialueeseen ja työsema, joka on liitetty yrityksen toimialueeseen. Näistä laitteista työaikapääte ja työasemat asetettiin virtuaalilähiverkkoon, jossa oli käytössä dynaaminen IP-osoitteiden jako DHCP:llä. Valvontakamerat asetettiin verkkoon, jossa laitteille määritetään käsin staattinen IP-osoite ja muut vaadittavat parametrit. Taulukossa 1 esitellään profilointitestauksen kannalta oleelliset virtuaalilähiverkot.

Taulukko 1. Profilointitestauksen virtuaalilähiverkot

VLAN nimi	VLAN ID	Käyttötarkoitus
Office	100	Toimistoverkko
CCTV	110	Valvontakameraverkko
Timetracking	120	Työajanseurantaverkko

Todennusvaiheessa autentikaattori välittää attribuutteja todennusta vaativasta päätelaitteesta RADIUS-palvelimelle, joka on vastuussa siitä, minkä tasoinen pääsy verkon resursseihin kyseiselle päätelaitteelle sallitaan. Tässä toteutuksessa autentikaattorina toimii verkkokytkin ja RADIUS-palvelimena Cisco ISE. Verkkokytkimet on konfiguroitava siten, että ne pystyvät välittämään tiedon niihin kytketyistä päätelaitteista Cisco ISE:lle. Verkkokytkimille on konfiguroitu seuraavat asetukset globaalisti:

Kuvassa 13 esitellään AAA-protokollan käyttöönottoon ja RADIUS-palvelimien määrittelyyn liittyvät komennot. AAA new-model -komento aktivoi AAA-protokollan kytkimessä. Radius server-komennolla määritellään RADIUS-palvelimen ja seuraavalla rivillä ilmoitetaan kyseisen palvelimen IP-osoite ja portit, joita käytetään RADIUS-viestien välittämiseen. Key-komento määrittää salausavaimen, jonka on oltava sama kuin Cisco ISE:lle asetettu salausavain. AAA group server radius -komento määrittää metodilistan, jossa spesifioidaan käytettävät RADIUS-palvelimet, tässä tapauksessa molemmat Cisco ISE:n noodit. Kytkimille on määritetty hallintaportti (management interface) ja ip radius source-interface -komento määrittää, että kytkimen ja Cisco ISE:n välillä kulkeva AAA-protokollaan liittyvä tieto välitetetään tämän hallintaportin kautta.

```
AAA new-model

radius server ISE01
address ipv4 10.0.0.1 auth-port 1812 acct-port 1813
key XXXXXXXXXXXX

radius server ISE02
address ipv4 10.0.0.2 auth-port 1812 acct-port 1813
key XXXXXXXXXXXX

AAA group server radius ISE
 server name ISE01_10.0.0.1
 server name ISE02_10.0.0.2
 ip radius source-interface Vlan111
```

Kuva 13. AAA-protokollan käyttöönotto ja RADIUS-palvelimien määrittely

Kuvassa 14 esitetyissä komennoissa viitataan aiemmin luotuun metodilistaan ja määritetään ISE vastaamaan autentikoinnista, autorisoinnista ja tilastoinnista.

```
AAA authentication dot1x default group ISE
AAA authorization network default group ISE
AAA authorization auth-proxy default group ISE
AAA accounting update newinfo
AAA accounting identity default start-stop group ISE
AAA accounting system default start-stop group radius
```

Kuva 14. AAA-toimintojen vastuunsiirto ISE:lle

Kuvan 15 komennoilla määritetään ISE:n noodit toimimaan CoA (Change of Authorization)-palvelimina.

```
AAA server radius dynamic-author
 client 10.0.0.1 server-key XXXXXXXXX
 client 10.0.0.2 server-key XXXXXXXXX
 auth-type any
```

Kuva 15. CoA-palvelimien määrittely

Olennainen osa onnistunutta laiteprofilointia ja autorisointia on päätelaitteen IP-osoitteen kartoittaminen, joka onnistuu Ciscon Device Tracking -ominaisuutta hyödyntäen. Kuvassa 16 esitetään verkkokytkimille määritettävät device-tracking policy -komennot. Molemmissa säännöissä aktivoidaan device tracking -ominaisuus ja määritetään ettei kyseinen ominaisuus kerää tietoa UDP-protokollasta. Alemman säännön limit address-count -komento määrittää kuinka montaa osoitetta enimmillään seurataan kytkinporttia kohden.

```
device-tracking policy IPDT_POLICY
 no protocol udp
 tracking enable

device-tracking policy MAX_CLIENT_2
 limit address-count 2
 no protocol udp
 tracking enable
```

Kuva 16. Device-tracking -sääntöjen luonti verkkokytkimellä

Device Sensor -ominaisuus on apuna ISE:n suorittamassa laiteprofiloinnissa. Verkkokytkin kerää tietoa päätelaitteista eri protokollien avulla, kuten CDP, LLDP ja DHCP avulla ja toimittaa nämä tiedot ISE:lle RADIUS-tilastointipakettien välityksellä. Kuvassa 17 esitellään verkkokytkimille määritettyjä device-sensor -komentoja.

RADIUS_CDP-lista kerää päätelaitteelta CDP-protokollan avulla tiedon laitteen isäntänimestä, ominaisuuksista, ohjelmistoversiosta ja laitteistosta.

RADIUS_DHCP-lista kerää päätelaitteelta DHCP-protokollan avulla tiedon laitteen isäntänimestä, DHCP-parametreista sekä laitteen tyypistä.

RADIUS_LLDP-lista kerää päätelaitteet LLDP-protokollan avulla tiedon laitteen isäntänimestä, ominaisuuksista ja tyypistä.

Listojen luonnin jälkeen ne otetaan käyttöön ja määritetään, että kytkin välittää tiedon ISE:lle kaikista päätelaitteen attribuuttien muutoksista.

```
device-sensor filter-list cdp list RADIUS_CDP
 tlv name device-name
 tlv name capabilities-type
 tlv name version-type
 tlv name platform-type

device-sensor filter-list dhcp list RADIUS_DHCP
 option name host-name
 option name parameter-request-list
 option name class-identifier

device-sensor filter-list lldp list RADIUS_LLDP
 tlv name system-name
 tlv name system-description
 tlv name system-capabilities

device-sensor filter-spec dhcp include list RADIUS_DHCP
device-sensor filter-spec lldp include list RADIUS_LLDP
device-sensor filter-spec cdp include list RADIUS_CDP
device-sensor notify all-changes

access-session attributes filter-list list RADIUS_PROFILING
 cdp
 lldp
 dhcp
access-session accounting attributes filter-spec include list RADIUS_PROFILING
```

Kuva 17. Device-sensor -ominaisuuden konfiguraatio

Seuraavaksi selitetään kuvassa 18 esiintyviä komentoja. Dot1x system-auth-control -komento aktivoi 802.1X-todennuksen globaalisti verkkokytkimellä. Radius-server attribute -komennoilla määritetään, mitä attribuutteja päätelaitteesta lähetetään ISE:lle todennuksen yhteydessä. Tässä toteutuksessa on muun muassa määritetty Service-Type -attribuutin sekä päätelaitteen IP-osoitteen lähetys ISE:lle.

```
dot1x system-auth-control
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 6 voice 1
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
```

Kuva 18. 802.1X-todennuksen aktivointi ja RADIUS-palvelimen attribuuttien määrittely

Policy-map -säännöstö määrittää verkkokytkimelle, kuinka sen on toimittava autentikointi- ja autorisointitapahtuman edetessä. Seuraavaksi on selitetty kuvassa 19 esitetty policy-map -säännöstö. Verkkokytkin käynnistää MAB-todennuksen havaitessaan uuden MAC-osoitteen kytkinportissa. MAB-todennuksen epäonnistuessa tai päätelaitteen lähettäessä EaPoL-kehyksen kytkin siirtyy 802.1X-todennukseen. Jos toinen edellä mainituista todennustavoista onnistuu, kytkin siirtyy autorisointivaiheeseen. Lisäksi säännöstössä on määritelty toimintoja poikkeustiloille, kuten verkkoyhteyden katkeamisen ISE:n ja verkkokytkimen välillä. Säännöstön lopussa on määritys, joka pakottaa autentikointitapahtuman uudelleenaloituksen 60 sekunnin kuluttua, jos päätelaite ei läpäise autorisointivaihetta.

```
policy-map type control subscriber MAB_1X_CLOSED_AUTH
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab retries 2 retry-time 0 priority 10
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
  60 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
```

Kuva 19. Verkkokytkimille määritetty policy-map -säännöstö

Verkkokytkimille määritettiin konfiguraatiomalli globaalisti, joka liitettiin kaikkiin kytkinportteihin. Konfiguraatiomallin käyttö selkeyttää kytkinportin konfiguraatiota ja helpottaa vianselvitystä, kun konfiguraatio on määritelty keskitetysti. Kuvassa 20 on esitetty verkkokytkimille määritetty konfiguraatiomalli.

```
template MAB_1X_CLOSED_AUTH
 dot1x pae authenticator
 switchport mode access
 mab
 access-session control-direction in
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber MAB_1X_CLOSED_AUTH
```

Kuva 20. Verkkokytkimille määritetty konfiguraatiomalli

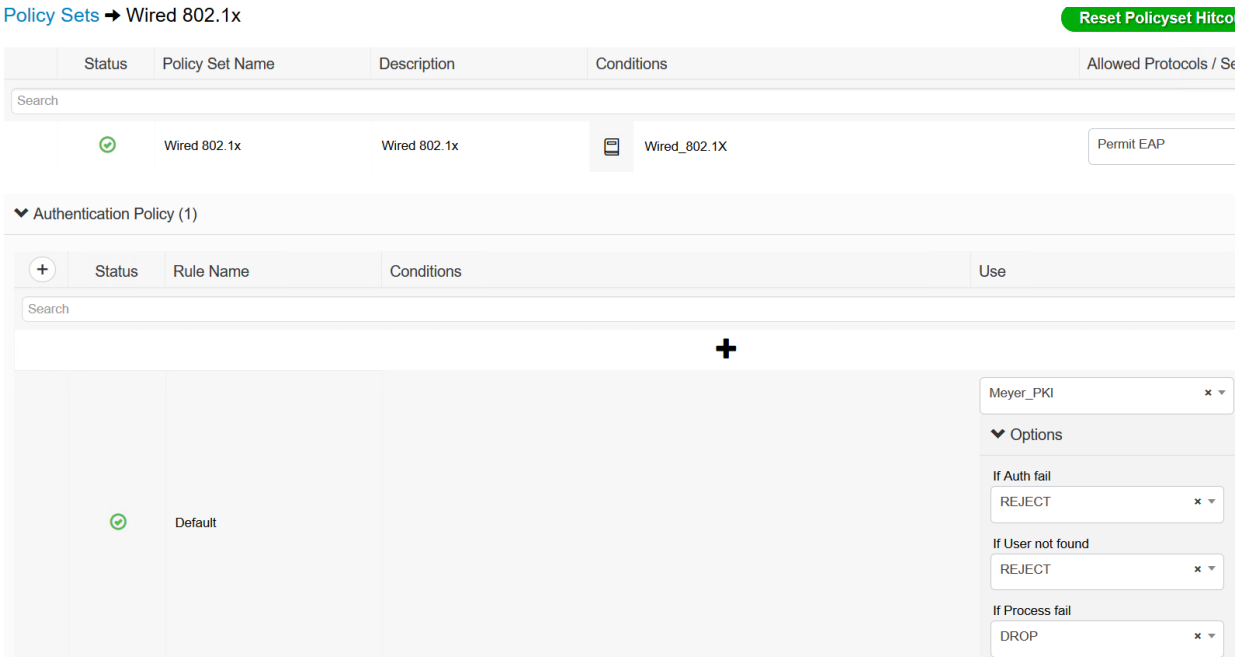
4.3 Cisco ISE:n pääsynhallintakonfiguraatiot

Cisco ISE:ssä luotiin erilaisia säännöstöjä eri laiteryhmille. Esimerkiksi 802.1X-todennusta tukeville laitteille, eli tässä tapauksessa yrityksen toimialueeseen liitetyille työasemille, luotiin omat 802.1X-säännöstöt. ISE:lle on määritettävä identiteettilähde, josta se tarkastaa määritetyt attribuutit todennusta yrittävästä päätelaitteesta. 802.1X-standardin mukaista todennusta tukevien laitteiden identiteettilähteenä käytettiin kohdeyrityksen aktiivihakemistoa. MAB-todennuksella todennettavista laitteista ISE kerää attribuutteja todennustapahtuman yhteydessä ja lisää nämä tiedot sisäiseen tietokantaan.

Kaikki laitteet yritetään ensin todentaa MABia käyttäen ja tämän epäonnistuessa siirrytään käyttämään 802.1X-standardin mukaista todennusta.

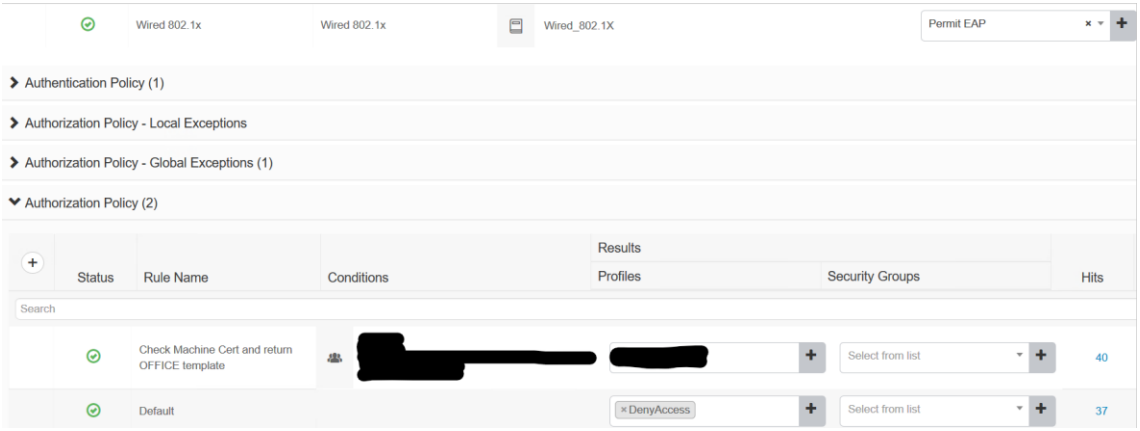
4.3.1 802.1X-todennuksen säännöstö

Yrityksen toimialueeseen liitettyjen työasemien todennus ja valtuutus tapahtuu 802.1X-todennustapaa käyttäen. Kuvassa 21 esitetään, kuinka Cisco ISE varmistaa, että päätelaitteelta löytyy todennuksessa käytettävä laitevarmenne. Autentikointi keskeytetään jos kyseistä laitevarmennetta ei löydy.



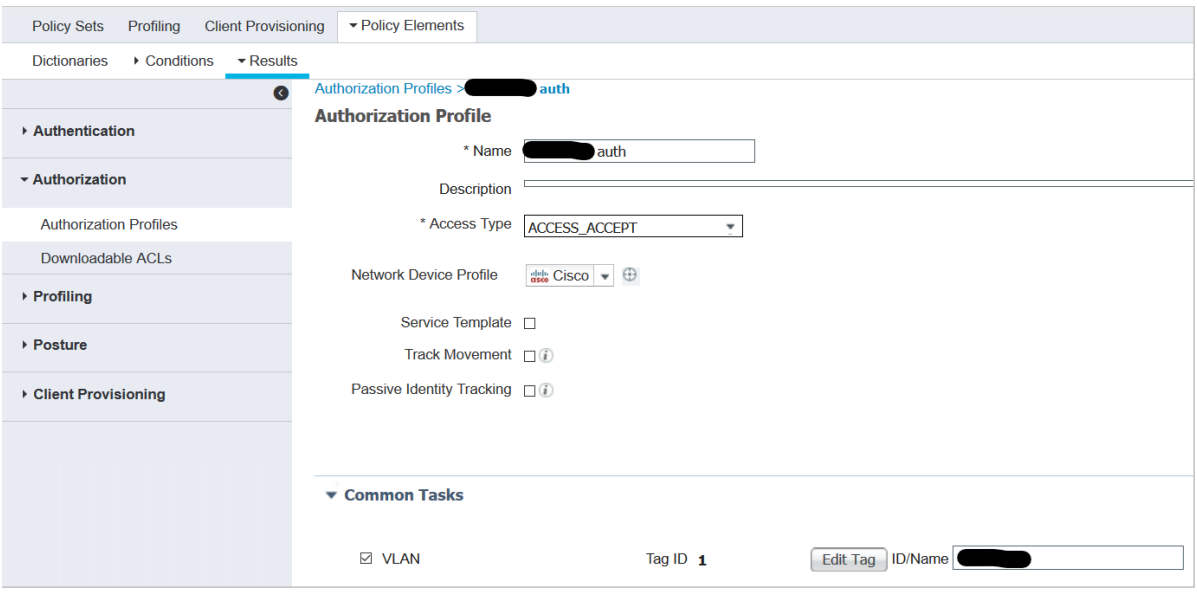
Kuva 21. 802.1X-todennusta tukevan päätelaitteen autentikointisäännöstö

Jos päätelaite todennetaan varmenteen avulla, se pääsee autorisointivaiheeseen, jossa tarkistetaan, onko kyseinen laite aktiivisena yrityksen aktiivihakemistossa. Edellä mainittu toimenpide on havainnoitu kuvassa 22. Jos päätelaite läpäisee molemmat edellä mainitut vaiheet, ISE palauttaa sille autorisointiprofiilin, joka myöntää pääsyn toimistoverkkoon. Muussa tapauksessa pääsyä ei myönnetä.



Kuva 22. 802.1X-todennusta tukevan päätelaitteen autorisointisäännöstö

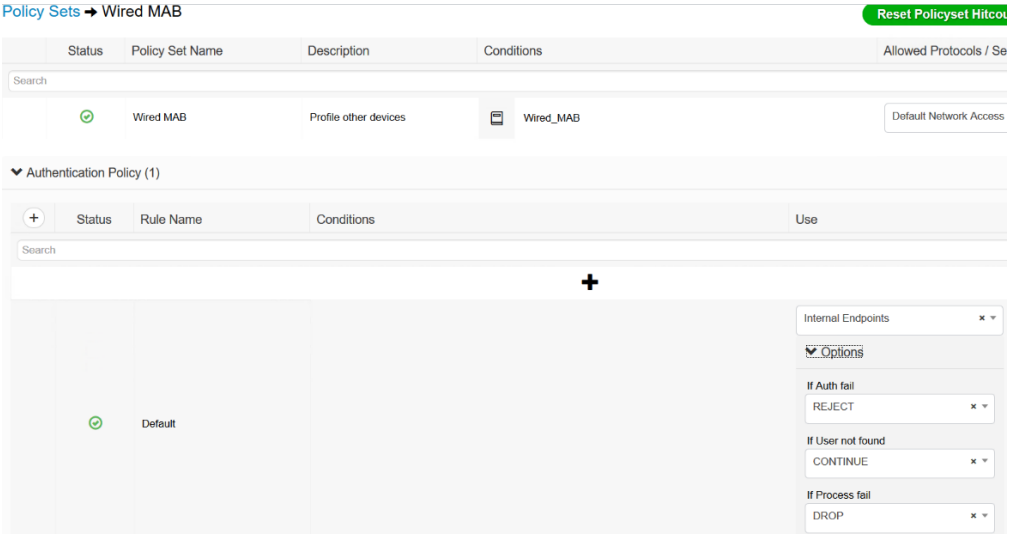
Kuvassa 23 on esitelty autorisointiprofiilin määrityksiä Cisco ISE:llä. Tämä autorisointiprofiili myöntää todennuksen läpäisseelle työasemalle pääsyn toimistoverkkoon.



Kuva 23. Onnistuneen 802.1X-todennuksen autorisointiprofiili

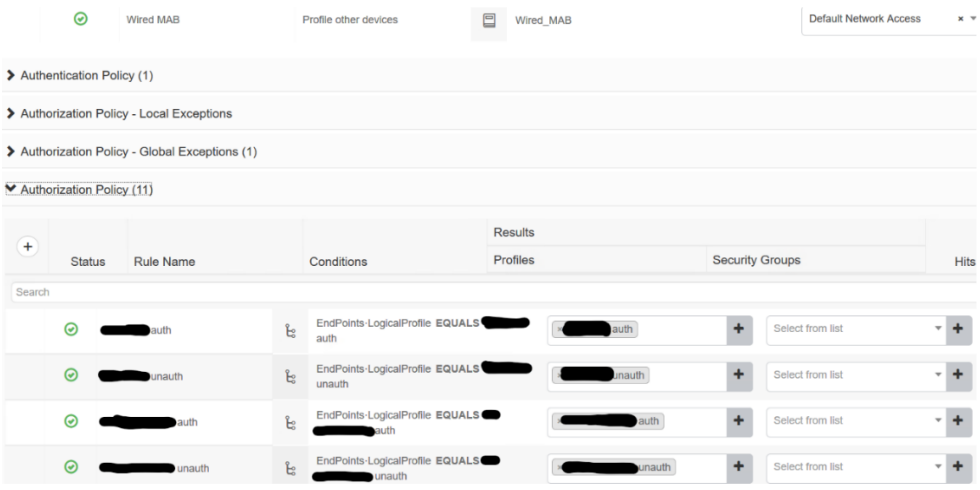
4.3.2 MAB-todennuksen säännöstö

ISE tallentaa päätelaitteiden MAC-osoitteet omaan tietokantaansa todennuksen yhteydessä. Yrityksellä ei ole käytössä päätelaitteiden MAC-osoitteet sisältävää erillistä tietokantaa, joten ISE:lle on määritetty sääntö, joka sallii myös muiden kuin ISE:n sisäisestä laitetietokannasta löytyvien laitteiden todennuksen, jotta ensimmäistä kertaa todennettavien laitteiden todennus on mahdollista. Tämä sääntö on esitetty kuvassa 24.



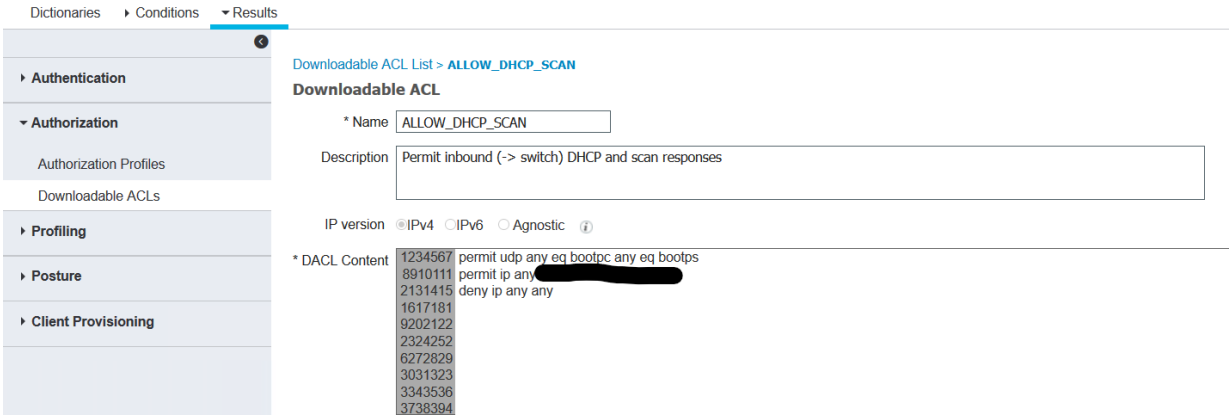
Kuva 24. MAB-todennuksen autentikointisäännöstö

Kuvassa 25 on esitelty MAB-todennuksella todennettujen laitteiden autorisointisääntöjä. Autorisointivaiheessa päätelaitteelle palautetaan joko unauth- tai auth-autorisointiprofiilin.



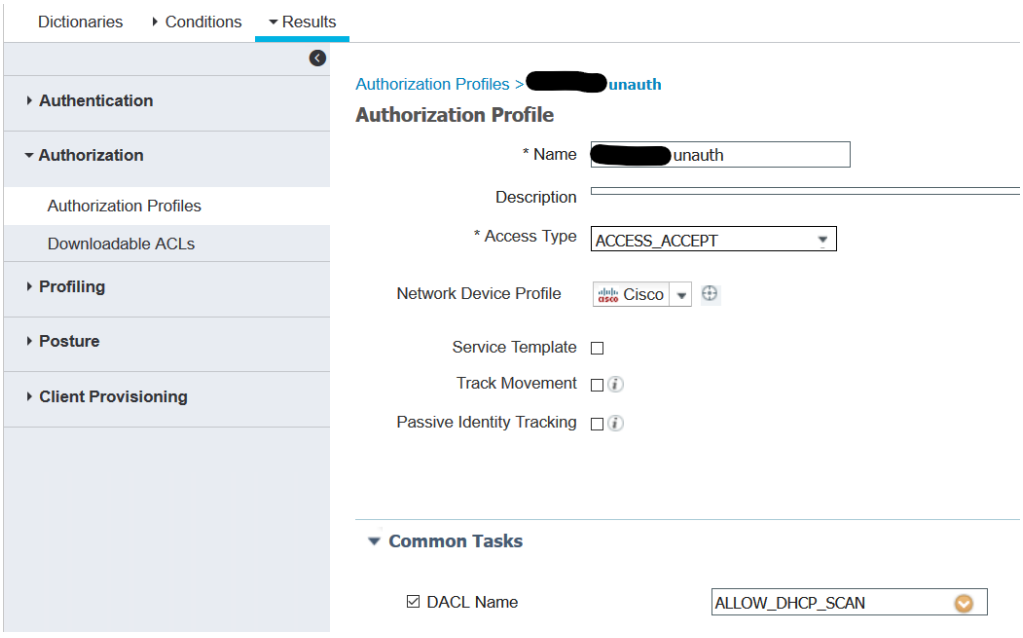
Kuva 25. MAB-todennuksen autorisointisäännöstö

Unauth-tuloksen saaneen päätelaitteen liikennöinti on rajoitettu DACL:ssä (Downloadable Access Control List) määritetyillä säännöillä. Tässä vaiheessa päätelaitteelta sallitaan liikennöinti ainoastaan BOOTP ja DHCP-protokollan käyttämien porttien kautta ISE:lle, jolloin päätelaitteesta saadaan lisätietoa. Kuvassa 26 on esitelty kyseinen DACL.



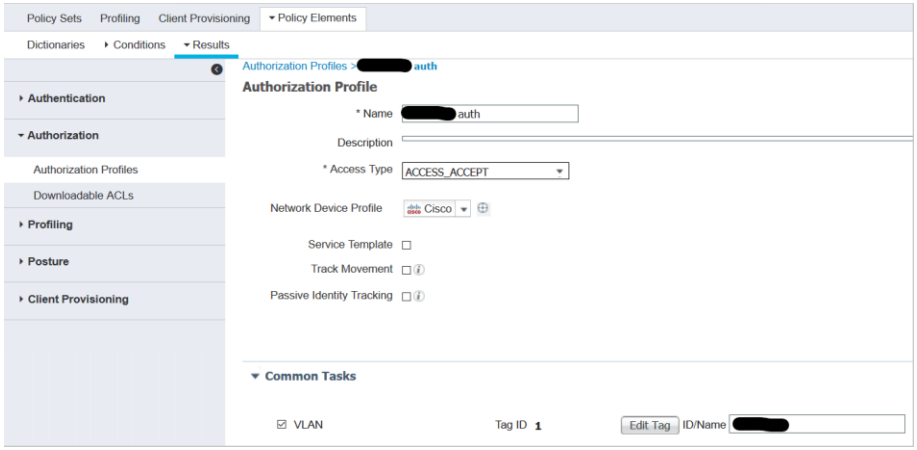
Kuva 26. Unauth-autorisointiprofiilin DACL

Aiemmin esitelty DACL-sääntö on liitetty päätelaitteelle palautettavaan unauth-autorisointiprofiiliin. Kuvassa 27 on esitelty kyseisen autorisointiprofiilin määritykset Cisco ISE:llä.



Kuva 27. Unauth-autorisointiprofiilin määritykset Cisco ISE:llä

Päätelaitteesta kerättyjen tietojen perusteella pääsy verkonresursseihin voidaan sallia tai kieltää. Jos päätelaite kuuluu laiteryhmään, jonka pääsy sallitaan, niin päätelaitteelle palautetaan kuvassa 28 esitelty autorisointiprofiili. Tämä profiili sallii kyseisessä verkossa normaalin liikennöinnin.



Kuva 28. Auth-autorisointiprofiilin määritykset Cisco ISE:llä

4.4 Päätelaitteiden todentamisen tarkistus verkkokytkimeltä

Päätelaitteiden todentamisen statuksen voi tarkistaa Cisco ISE:stä tai autentikaattorina toimivalta verkkokytkimeltä. Verkkokytkimeltä tarkistus onnistuu show authentication sessions -komennolla, joka listaa kaikki sillä hetkellä todennetut ja todentamista yrittävät laitteet. Kuvassa 29 on esimerkki verkkokytkimen show authentication sessions -komennon tulosteesta. Tämä komento kertoo muun muassa verkkokytkimen liityntäportin, päätelaitteen MAC-osoitteen, todennustavan ja todennuksen statuksen.

```
Testikytkin2#show authentication sessions
Interface               MAC Address    Method  Domain  Status Fg  Session ID
-----------------------------------------------------------------------------------------
Gi1/0/1                 XXXX.XXXX.XXXX mab     DATA    Auth       FB88200A00002B755F9D20BD
Gi1/0/4                 XXXX.XXXX.XXXX dot1x   DATA    Auth       FB88200A000025A05A1B0E09
Gi1/0/2                 XXXX.XXXX.XXXX N/A     UNKNOWN Unauth     FB88200A000025A35A1CFBA6

Session count = 3

Key to Session Events Blocked Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker
```

Kuva 29. Verkkokytkimen näkymä todennetuista laitteista

Todennetuista päätelaitteista saa yksityiskohtaisempaa tietoa show authentication sessions session-id XXXXXX details -komennolla, josta on esimerkki kuvassa 30. Tämä komento kertoo verkkokytkimen liityntäportin, todennustapahtuman yksilöivän IIF-ID:n, päätelaitteen IP- ja MAC-osoitteen, isäntänimen, todentamisen statuksen ja siinä käytetyn säännöstön sekä VLANin johon kyseinen laite on siirretty todentamisen perusteella. Kuvassa 30 esitellään tuloksia 802.1X-todennusta tukevasta päätelaitteesta.

```
Testikytkin2#show authentication sessions session-id FB88200A000025A05A1B0E09 details
Session id=FB88200A000025A05A1B0E09
           Interface:  GigabitEthernet1/0/4
              IIF-ID:  0x1FEB97D0
         MAC Address:  XXXX.XXXX.XXXX
        IPv6 Address:  Unknown
        IPv4 Address:  10.0.100.10
           User-Name:  XXXXXXXXXXXX
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  FB88200A000025A05A1B0E09
      Acct Session ID:  0x000000a2
              Handle:  0x6a000576
       Current Policy:  MAB_1X_CLOSED_AUTH


Server Policies:
          Vlan Group:  Vlan: 100


Method status list:
       Method           State
        dot1x           Authc Success
        mab             Stopped
```

Kuva 30. Yksityiskohtainen näkymä 802.1X:llä todennetusta päätelaitteesta

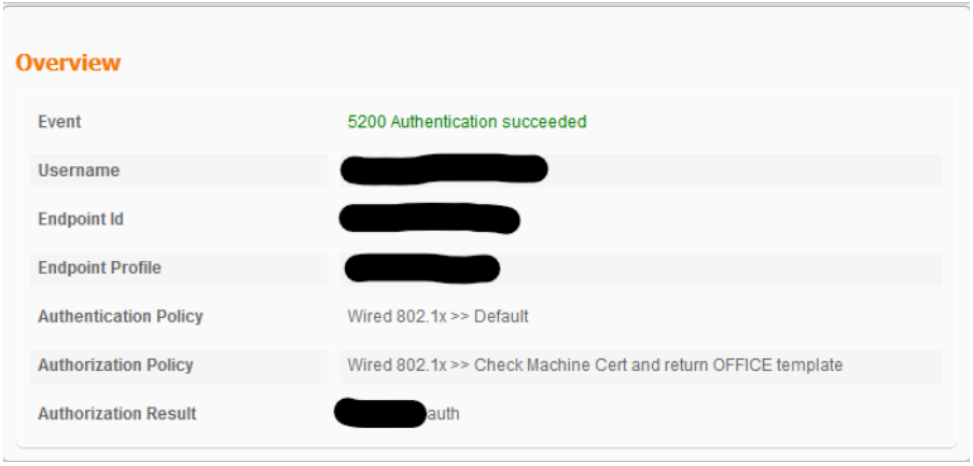
MAB-todennusta käytettäessä saadaan vastaavat yksityiskohtaiset tiedot todennustapahtumasta, kuten kuvassa 31 esitetään. Huomiona, että MAB-todennuksessa todennustapahtumassa näkyvä käyttäjänimi on kyseisen päätelaitteen MAC-osoite, kun taas 802.1X-todennuksessa käyttäjänimi on työaseman FQDN (Fully Qualified Domain Name).

```
Testikytkin2#show authentication sessions session-id FB88200A00002B755F9D20BD details
Session id=FB88200A00002B755F9D20BD
            Interface:  GigabitEthernet1/0/1
               IIF-ID:  0x1900991A
          MAC Address:  XXXX.XXXX.XXXX
         IPv6 Address:  Unknown
         IPv4 Address:  10.0.110.10
            User-Name:  XXXX.XXXX.XXXX
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  FB88200A00002B755F9D20BD
      Acct Session ID:  0x000000b9
               Handle:  0x61000b4e
       Current Policy:  MAB_1X_CLOSED_AUTH


Server Policies:
          Vlan Group:  Vlan: 110


Method status list:
       Method           State
          mab           Authc Success
```

Kuva 31. Yksityiskohtainen näkymä MABilla todennetusta päätelaitteesta

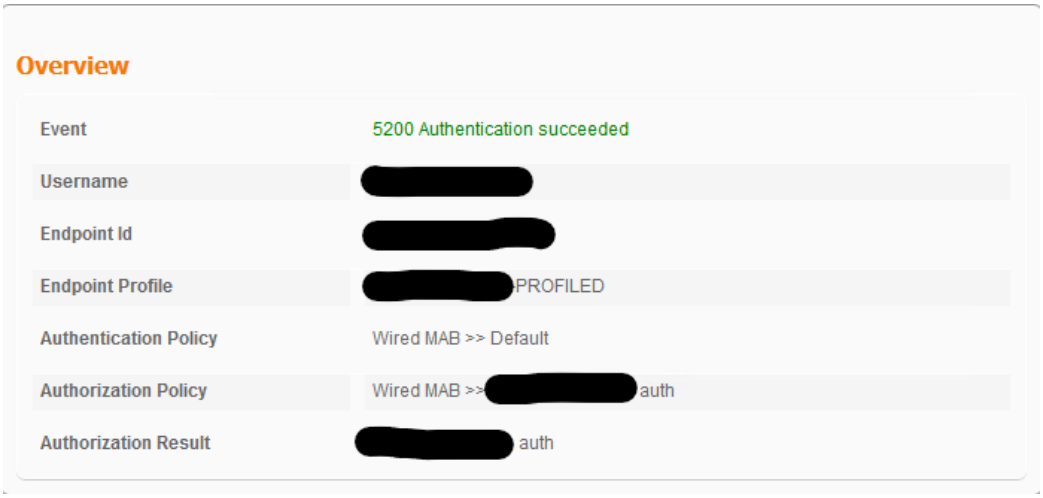
4.5 Päätelaitteiden todentamisen tarkistus Cisco ISE:ltä

Cisco ISE tuottaa listauksen kaikista verkkokytkimiin yhdistetyistä päätelaitteista. Cisco ISE:n RADIUS Live Logs -osiosta löytyy autentikointi- ja autorisointitapahtumien lisätiedot listattuna. Jokaisen tapahtuman kohdalta on mahdollista avata yksityiskohtainen raportti. Raportista selviää autentikoinnissa ja autorisoinnissa tapahtuneet vaiheet sekä lopputulos. Kuvassa 32 on esitelty 802.1X-todennuksen läpäisseen työaseman raportin yleiskatsaus. Käyttäjänimi on työaseman FQDN ja Endpoint Id on MAC-osoite.



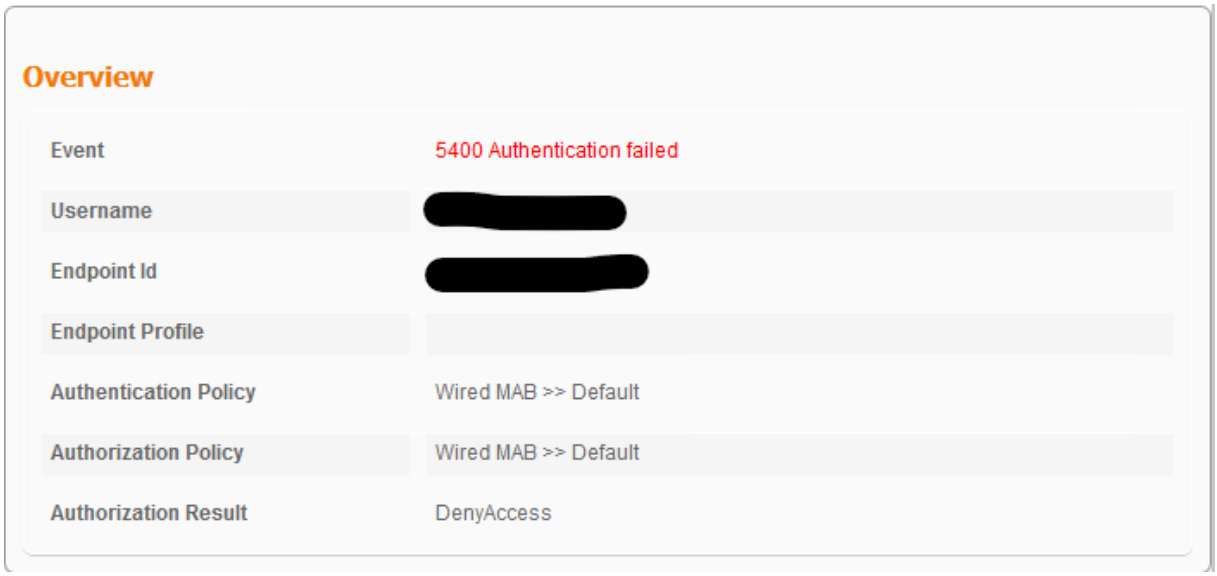
Kuva 32. 802.1X-todennuksen tarkistus ISE:ltä

Cisco ISE muodostaa kattavan raportin myös MAB-todennuksen läpikäyneistä päätelaitteista. Kuvassa 33 on esitelty MAB-todennuksen läpäisseen päätelaitteen raportin yleiskatsaus. Käyttäjänimi ja Endpoint Id on päätelaitteen MAC-osoite.



Kuva 33. MAB-todennuksen tarkistus ISE:ltä

Cisco ISE tuottaa yksityiskohtaisen raportin myös epäonnistuneista autentikoinneista. Kuvassa 34 on esitelty epäonnistuneen MAB-todennuksen raportin yleiskatsaus.



Kuva 34. Epäonnistuneen MAB-todennuksen tarkistus ISE:ltä

4.6 Havaitut ongelmat

Cisco ISE:n profilointipolitiikat on syytä testata huolellisesti ennen laajempaa käyttöönottoa. Tämän toteutuksen alkuperäisen suunnitelman mukaan oli tarkoitus yrittää 802.1X-todennusta kaikilla päätelaitteilla ennen MAB-todennukseen siirtymistä. Yhden testilaitteena olevan valvontakameran kanssa tämä ei kuitenkaan onnistunut. Kyseinen valvontakamera oli tarkoitus todentaa MAB-todennuksella, mutta laite käynnistyi uudelleen sen aikana, kun verkkokytkin tarjosi sille 802.1X-todennusta. Muutimme järjestyksen päinvastaiseksi, eli verkkokytkin tarjoaa MAB-todennustapaa ensin. Tämä ratkaisi ongelman kyseisen valvontakameran kanssa, eikä hidasta 802.1X-todennusta tukevien päätelaitteiden verkkoon pääsyä, sillä verkkokytkin siirtyy automaattisesti 802.1X-todennukseen, jos päätelaite lähettää EaPoL-kehyksen.

4.7 Seuraavat työvaiheet

Tämän opinnäytetyön jälkeen projekti jatkuu kohdeyrityksessä ja testausvaiheen jälkeen on vuorossa Cisco ISE:n käyttöönotto kaikilla yrityksen toimipisteillä. Käyttöönotto tapahtuu pienissä osissa tietoliikenteen katkosten minimoimiseksi. Toimistoympäristöt, jotka koostuvat pääosin 802.1X-todennusta tukevista työasemista sekä MAB:lla todennettavista verkkotulostimista, hoidetaan ensimmäisenä kuntoon, sillä testaustulosten mukaan näissä kohteissa tulee vähiten ongelmia vastaan. Haastavimpia kohteita ovat tuotantoympäristöt, joissa yhteen verkkokytkimeen on yhdistettynä monta erilaista laiteryhmää, jotka eivät usein tue 802.1X-todennusta, joten ne todennetaan käyttäen MAB-todennusta. Toimistöympäristöissä on mahdollista suorittaa käyttöönotto koko toimipisteelle samanaikaisesti, mutta haastavissa kohteissa käyttöönotto on tehtävä yksi verkkokytkin kerrallaan, jotta ongelmat voidaan ratkaista nopeasti ja tarvittaessa palauttaa verkkokytkimelle alkuperäinen konfiguraatio.

POHDINTA

Opinnäytetyön tavoitteena oli perehtyä identiteettipohjaisen pääsynhallinnan ja Cisco ISE:n profilointiominaisuuksien teoriaan ja suorittaa profilointipolitiikkojen testaus ennen varsinaista käyttöönottoa. Tämä tavoite saavutettiin ja oma tietotaito identiteettipohjaisesta pääsynhallinnasta kasvoi runsaasti tämän projektin myötä. Identiteettipohjaisen pääsynhallinnan käyttöönotto näin isossa yrityksessä vaatii tarkkaa suunnittelua ja testausta ennen käyttöönottoa. Kohderityksen tietoverkko sisältää runsaasti erilaisia laite- ja käyttäjäryhmiä, joten profilointipolitiikat kullekin ryhmälle on mietittävä tarkkaan ja käyttöönotto on suoritettava huolellisesti, jotta tietoliikenteen katkokset pystytään minimoimaan ja aiheuttamaan loppukäyttäjille mahdollisimman vähän haittaa.

Kohdeyrityksessä oli ennestään käytössä PKI (Public Key Infrastructure), joka helpotti huomattavasti Cisco ISE:n 802.1X-todennuksen käyttöönottoa. Valmis PKI-ympäristö mahdollisti jo olemassa olevien laitevarmenteiden käytön yrityksen toimialueeseen liitettyjen työasemien todennuksessa.

Projektin myötä tuli huomattua, kuinka identiteettipohjainen pääsynhallinta on sidoksissa loppukäyttäjän identiteetin tarjoavaan palveluun, tässä tapauksessa yrityksen toimialueeseen. Käytännössä tämä tarkoittaa sitä, että tietoverkon pääsynhallinta on riippuvainen identiteettilähteen luotettavuudesta ja toimivuudesta.

Tässä opinnäytetyössä toteutettua identiteettipohjaista pääsynhallintaa on mahdollista kehittää jatkossa ja hioa profilointipolitiikkoja vielä tarkemmiksi parantaen yrityksen tietoturvaa, kun on selvitetty kuinka eri laiteryhmät profiloituvat. Käyttöönottovaiheessa MAB-todennuksella todennettavat laitteet profiloitiin pelkästään MAC OUI -arvon ja IP-osoitteen perusteella. Tarkoituksena on ottaa käyttöön muitakin profilointiarvoja myöhemmässä vaiheessa, kun kaikki tietoverkon laiteryhmät ovat ISE:n hallinnassa.

Opinnäytetyön jälkeisiä jatkotoimenpiteitä ovat yrityksen sisäisen dokumentaation päivittäminen Cisco ISE:n osalta sekä ISE:n integrointi muihin Ciscon tuotteisiin, kuten DNA-Centeriin ja Stealthwatchiin, joiden avulla saadaan vielä enemmän näkyvyyttä tietoverkon liikenteeseen ja helpotetaan verkon hallintaa.

Identiteettipohjaisen pääsynhallinnan käyttöönotto on suositeltavaa, jos yrityksen tavoitteena on parantaa tietoverkkonsa turvallisuutta sekä saada näkyvyyttä tietoverkon käyttäjien toimintoihin.

LÄHTEET

Cisco. 2006. How Does RADIUS Work?. WWW-dokumentti. [Viitattu 25.04.2021]. Saatavissa: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

Cisco. 2011. MAC Authentication Bypass Deployment Guide, Cisco 2011. WWW-dokumentti. Viitattu [09.04.2021]. Saatavissa:https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html#wp9000125

Cisco. 2011. Wired 802.1X Deployment Guide – Cisco. WWW-dokumentti. [Viitattu 07.04.2021]. Saatavissa: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp386748%0A

Cisco. 2014. Cisco Identity Based Networking Services 2.0 At-a-Glance. WWW-dokumentti. [Viitattu 02.05.2021]. Saatavissa: https://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/aag_c45-731544.pdf

Cisco. 2018. Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW, Chapter: Understanding and Configuring VLANs. WWW-dokumentti. [Viitattu 09.04.2021]. Saatavissa: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html

Cisco. 2018. ISE Profiling Design Guide. WWW-dokumentti. [Viitattu 15.04.2021]. Saatavissa: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456#toc-hId-1893475311

Cisco. Cisco Identity Services Engine Administrator Guide, Release 2.7. WWW-dokumentti. [Viitattu 13.04.2021]. Saatavissa:https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/b_ise_27_admin_guide.html

D'Ambrosia, J. IEEE Working Groups and Study Groups. WWW-dokumentti. [Viitattu 19.03.2021]. Saatavissa: https://www.ieee802.org/

Geier, J, & Geier, JT 2008, Implementing 802. 1X Security Solutions for Wired and Wireless Networks, John Wiley & Sons, Incorporated, Hoboken. [Viitattu 07.04.2021]. ISBN 9780470370285. Saatavissa: ProQuest Ebook Central.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä:Docendo. [Viitattu 24.03.2021]. ISBN 9518461643. Saatavissa: Ellibs Library.

Holla, H. 2021. ISE Secure Wired Access Prescriptive Deployment Guide - Cisco Community. WWW-dokumentti. [Viitattu 12.05.2021]. Saatavissa: https://community.cisco.com/t5/security-documents/ise-secure-wired-access-prescriptive-deployment-guide/ta-p/3641515#toc-hId--499857652

IEEE. WHAT IS IEEE 802?. WWW-dokumentti. [Viitattu 19.03.2021]. Saatavissa: https://standards.ieee.org/featured/802/index.html

Integrating IT. 2018. WWW-dokumentti. [Viitattu 21.04.2021]. Saatavissa: https://integratingit.wordpress.com/2018/05/07/configuring-cisco-ise-dynamic-vlan-assignment/

Kaario, K. 2002. TCP/IP-verkot. Jyväskylä: Docendo. [Viitattu 24.03.2021]. ISBN 9518461074. Saatavissa: Ellibs Library.

Mamalgaha, L. 2019. What is A MAC Address and Why You Should Know About It?. WWW-dokumentti. [Viitattu 09.04.2021]. Saatavissa: https://medium.com/@lakshanmamalgaha/what-is-a-mac-address-and-why-you-should-know-about-it-9f970b3ba3fd

Meyer Turku Oy. 2020. About the shipyard. WWW-dokumentti. [Viitattu 12.04.2021]. Saatavissa: https://www.meyerturku.fi/fi/meyerturku_com/shipyard/company/about_the_shipyard_1/about_the_shipyard.jsp

Mitchell, C. & Sanbower, J. & Santuka, V. & Woland, A. 2019.Sharing the Context. WWW-dokumentti. [Viitattu 21.04.2021]. Saatavissa: https://www.ciscopress.com/articles/article.asp?p=2963461&seqNum=2

Priyanka Kumari. 2019. MAC Authentication Bypass. WWW-dokumentti. Viitattu [09.04.2021]. Saatavissa:https://www.linkedin.com/pulse/mac-authentication-bypass-priyanka-kumari/

RFC 1035. 1987. Domain Names – Implementation and Specification. WWW-dokumentti. [Viitattu 20.04.2021]. Saatavissa: https://tools.ietf.org/html/rfc1035

RFC 2131. 1997. Dynamic Host Configuration Protocol. WWW-dokumentti. [Viitattu 20.04.2021]. Saatavissa: https://tools.ietf.org/html/rfc2131

RFC 2132. 1997. DHCP Options and BOOTP Vendor Extensions. WWW-dokumentti. [Viitattu 20.04.2021]. Saatavissa: https://tools.ietf.org/html/rfc2132

Richter, A, & Wood, J 2015, Practical Deployment of Cisco Identity Services Engine (ISE) : Real-World Examples of AAA Deployments, Elsevier Science & Technology Books, Rockland, MA. [Viitattu 15.04.2021]. ISBN 9780128045046. Saatavissa: ProQuest Ebook Central.

Techopedia. What is Authentication Authorization and Accounting (AAA)? – Definition from Techopedia. WWW-dokumentti. [Viitattu 19.03.2021].Saatavissa: https://www.techopedia.com/definition/24130/authentication-authorization-and-accounting-aaa

Zeni, D. 2018. Cisco ISE: Wired and Wireless 802.1X Network Authentication. WWW-dokumentti. [Viitattu 07.04.2021]. Saatavissa: https://www.lookingpoint.com/blog/ise-series-802.1x