Henri Vainio

IEEE 802.1X -standardin mukaisen posture-tarkistuksen suunnittelu ja testaus ICTLAB-ympäristössä

Opinnäytetyö
Tieto- ja viestintätekniikka

2019

Kaakkois-Suomen ammattikorkeakoulu

Tekijä/Tekijät	Tutkinto	Aika
Henri Vainio	Insinööri (AMK)	Marraskuu 2019
Opinnäytetyön nimi IEEE 802.1X -standardin mukaisen posture-tarkistuksen suunnittelu ja testaus ICTLAB-ympäristössä		59 sivua 7 liitesivua
Toimeksiantaja Kaakkois-Suomen ammattikorkeakoulu, Xamk ICTLAB		
Ohjaaja Vesa Kankare		

Tiivistelmä

Tämän opinnäytetyön tavoitteena on tutustua IEEE 802.1X -standardin mukaiseen posture-tarkistukseen. Tarkoitus on sekä teorian että käytännön tasolla selvittää Cisco Identity Services Engine -pääsynhallintajärjestelmän posture-ominaisuuden toiminta ja hyödyt sekä testata sen toimintaa käytännössä Xamkin ICTLAB:n verkkoympäristöä muistuttavassa virtuaalilaboratoriossa. Työn pohjalta laaditaan tiivistetty ohjeistus posturen mahdollista laajamittaisempaa tulevaisuuden käyttöönottoa varten oikeassa lähiverkossa. Posture määritetään vain langalliseen verkkoon.

Posture on Identity Services Enginen (ISE) tarjoama lisäturvaominaisuus 802.1X-porttitodennukselle, joka mahdollistaa porttitodennettujen työasemien pääsynhallinnan lähiverkossa erilaisten vaatimusten avulla. Esimerkkejä tällaisista vaatimuksista ovat työasemille asennetut ohjelmat, laitteistokokoonpano tai niiden käyttämät todennusmenetelmät. Tässä työssä posture määritetään siten, että kaikissa ICTLAB:n verkon 802.1X-todennetuissa työasemissa on oltava ajantasaiset kriittiset Windows-päivitykset ennen kuin niiden pääsy verkkoon sallitaan. Puuttuvat päivitykset työasemat ohjeistetaan asentamaan verkon sisäiseltä WSUS-palvelimelta. Tämä parantaa verkon tietoturvaa siten, että uusimpien päivitysten myötä verkon työasemilla on vähemmän haavoittuvuuksia, joita esimerkiksi hakkerit voisivat hyödyntää. Päivitykset myös takaavat järjestelmän paremman toimivuuden.

Opinnäytetyön alkuvaiheessa tutustuttiin ensin 802.1X-standardiin, joka määrittelee porttikohtaisen todennuksen lähiverkoissa, ja siihen liittyviin todennusprotokolliin, kuten EAP, EAPOL ja RADIUS. Samalla perehdyttiin myös ISE:een sekä posturen teoriaan, kuten sen toimintaperiaatteeseen ja määrityksen ohjeistukseen. Tämän jälkeen luotiin virtuaalitopologia Xamkin Virtual Lab -ympäristöön, jossa posture-tarkistuksen käyttöönottoa pystyttiin onnistuneesti testaamaan. ICTLAB:n verkon muutostöiden johdosta suunnitelmista testata posturea oikeassa lähiverkkoympäristössä jouduttiin lopulta luopumaan, mutta määritystä päästiin kuitenkin testaamaan BK0128-luokkahuoneen kahdella fyysisellä työasemalla yhdistämällä fyysinen runkokytkin ja kaksi asiakaskytkintä virtuaalitopologiaan ristiinkytkennän ja Multicast VPN:n avulla.

Työn lopputuloksena oli siis onnistunut testaus kahdella fyysisellä työasemalla ICTLAB:n verkon mukaisessa ympäristössä ja sen pohjalta laadittu ohjeistus.

Asiasanat

posture, ISE, WSUS, porttitodennus, pääsynhallintajärjestelmä, lähiverkot

Author (authors)	Degree	Time
Henri Vainio	Bachelor of Information Technology	November 2019

Thesis title

IEEE 802.1X Posture Check Design and Testing for ICTLAB Environment

59 pages
7 pages of appendices

Commissioned by

South-Eastern Finland University of Applied Sciences, Xamk ICTLAB

Supervisor

Vesa Kankare

Abstract

The goal of this thesis is to study and test IEEE 802.1X authentication-based posture check. The purpose is to study the operation and benefits of the posture feature provided by Cisco Identity Services Engine administration system both in theory and practice and test it in a virtual environment similar to Xamk ICTLAB local area network. As a result of testing a summarized set of instructions of the whole implementation will be written at the end of this document in case a wide scale deployment in the actual local area network is ever considered in the future. Posture check in this thesis is only configured on wired network.

Posture is an additional security feature on top of 802.1X port-based authentication provided by Identity Services Engine (ISE). It allows the checking of compliance (posture) of endpoints before allowing them to connect to your network. This makes it possible to create a certain set of requirements towards endpoints based on installed software, hardware configurations or authentication methods before they are deemed compliant and permitted access to the network. In this thesis a basic posture check with a requirement of up-to-date Windows Critical Updates on all client workstations is configured. In the implementation the missing updates on workstations can and must be remediated and installed via internally managed WSUS server before granting them access to join the network. This provides more safety to network due to endpoints always being critically patched without extra vulnerabilities that could be exploited. Updates also ensure better operation of the system.

At the start of the thesis 802.1X standard and the related protocols including EAP, EAPOL and RADIUS were studied. At the same time a deeper look was taken at ISE and the posture process itself. After this it was time to create a virtual topology in Xamk Virtual Lab environment on which a successful posture deployment could be tested. Due to ongoing network modifications in ICTLAB, plans of testing posture in real environment had to be given up. Despite this a test on two physical workstations in classroom BK0128 could successfully be carried out by connecting the virtual topology to physical devices (a core switch and two access switches) with the help of crossed connection and MultiCast VPN configuration.

The end result of the thesis was a successful posture check test on two physical workstations on a virtual network resembling the real ICTLAB environment and detailed step-by-step instructions based on that.

Keywords

posture, ISE, WSUS, port-based authentication, administration system, local area networks

SISÄLLYS

KÄSITTEET JA LYHENTEET

AD	Active Directory eli aktiivihakemisto on Windows-palvelimen rooli ja Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu. Se sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista, ja sen avulla niitä voidaan hallita keskitetysti.
IEEE 802.1X	Porttikohtainen todennus, jonka avulla käyttäjät todennetaan portin kautta, ja näin ollen estetään luvattomien käyttäjien tai laitteiden pääsy kohdeverkkoon. Todennuksessa käytetään jotain EAPOL-protokollaa. 802.1X on IEEE:n (Institute of Electrical and Electronic Engineers) määrittelemä standardi.
ISE	Identity Services Engine. Se on Ciscon kehittämä verkon- ja pääsynhallintaan tarkoitettu ohjelmisto, jolla voidaan valvoa ja hallita verkon käyttäjiä ja työasemia erilaisilla politiikoilla ja säännöillä.
Posture	Posture on Cisco ISE:n palvelu, joka on eräänlainen verkon työasemille tehtävä turvatarkastus. Se mahdollistaa erilaisten vaatimusten asettamisen päätelaitteille verkkoon pääsyn sallimiseksi. Posture-ominaisuuden avulla työasemille voidaan määrittää ns. noudattavuus-tila (compliance), jonka perusteella niiden verkkoon pääsyn tasoa voidaan säädellä erilaisilla valtuutuskäytännöillä.
WSUS	Windows Server Update Services on Windows-palvelimella toimiva ohjelmisto, jonka avulla voidaan hallita päivitysten jakamista Windows-työasemille. Eräänlainen yrityksen sisäinen Microsoft Update -palvelin.

1 JOHDANTO

Tänä päivänä tietoturva ja siihen liittyvät asiat ovat merkittävässä asemassa osana yrityksien ja organisaatioiden toimintaa. Heikko tietoturva voi aiheuttaa yrityksille tai organisaatioille merkittäviä taloudellisia menetyksiä ja pahimmassa tapauksessa vaarantaa koko niiden toiminnan, jos niiden kriittiset ja arkaluotoiset tiedot päätyvät vääriin käsiin. Sen vuoksi on tärkeää, että tiedot ja tietojärjestelmät pidetään vain niiden käyttöön oikeutettujen saatavilla. Oleellinen osa hyvää tietoturvaa on myös varmistaa verkkoon liittyvien päätelaitteiden turvallisuus, koska juuri ne ovat alttiita erilaisille haittaohjelmille ja kyberhyökkäyksille, jotka pahimmillaan voivat saastuttaa koko verkon. Tämän työn tavoitteena on suunnitella tietoturvaa parantavan IEEE 802.1X -standardin mukaisen posture-tarkistuksen käyttöönotto Kaakkois-Suomen ammattikorkeakoulun ICTLAB-ympäristön langalliseen verkkoon sekä testata sen toimintaa pienimuotoisesti käytännössä.

Posture, joka suomeksi käännettynä tarkoittaa sanaa ’ryhti’, on verkon päätelaitteille suoritettava erilaisiin määriteltäviin ehtoihin ja vaatimuksiin perustuva turvallisuustarkistus, jonka perusteella selvitetään, kuinka hyvin ne noudattavat verkolle asetettuja turvallisuusstandardeja. Posturen pohjalta työasemille määräytyy ns. compliance-tila (vaatimustenmukaisuus), jonka perusteella niiden yhteys lähiverkkoon joko sallitaan tai evätään. Tarkoituksena on estää suojaamattomia ja mahdollisesti verkon tietoturvaa vaarantavia päätelaitteita liittymästä verkkoon. Tämä on erityisen tärkeää aikakaudella, jolloin erilaisia tietoturvaa vaarantavia haavoittuvuuksia ja tietoturva-aukkoja ohjelmistoista ja laitteista löydetään päivittäin. Sen vuoksi esimerkiksi päivittämättömiin työasemiin liittyy merkittäviä tietoturvariskejä ja ne muodostavat uhkan lähiverkon turvallisuudelle. Posture pyrkii lievittämään tätä ongelmaa varmistamalla, että verkkoon liittyvät työasemat täyttävät verkon turvallisuuden takaamiseksi asetetut vaatimukset, kuten sen, että niille on asennettu ajantasaiset käyttöjärjestelmän tietoturvapäivitykset tai asianmukainen virustorjuntaohjelmisto. Kriteereitä voi olla myös monia muita, ja on verkonvalvojan itsensä päätettävissä, mitä nämä lopulta ovat.

Posture-tarkistukseen liittyy läheisesti myös työasemien korjaustoimenpiteet (remediation), jossa posture-tarkistuksessa puutteelliseksi havaitut työasemat

”korjataan” eli niihin asennetaan tarvittavat ajantasaiset päivitykset tai ohjelmistot korjauspalvelimen (remediation server) avulla. Tämän jälkeen niiden pääsy verkkoon voidaan sallia.

Opinnäytetyön toimeksiantaja on Kaakkois-Suomen ammattikorkeakoulu Xamk ja tarkemmin sanottuna sen tietotekniikkayksikkö ICTLAB. Työn toteutus tapahtuu kevään ja kesän 2019 aikana.

Samaan aihepiiriin, pääasiassa Windows-ympäristössä toteutettuun porttikohtaiseen todennukseen, liittyviä muita opinnäytetöitä ovat muun muassa Laura Gummeruksen ja Petteri Iivosen IEEE 802.1x todennus & käyttöönotto Fenniassa (2010), Anssi Kinnusen IEEE 802.1X ja porttikohtainen todennus Windows-ympäristössä (2014) sekä Jarno Mäkelän Porttikohtainen autentikointi (2015).

1.1 Opinnäytetyön tavoitteet

Tässä työssä posturen käyttöönotto ICTLAB:ssa on tarkoitus suunnitella ja testata siten, että verkon työasemien Windows-päivitysten ajantasaisuus tarkistetetaan posturen avulla ja tärkeiden päivitysten puuttuessa määrätään ne lataamaan kyseiset päivitykset sisäiseltä WSUS-palvelimelta verkkoyhteyden sallimiseksi. Posture helpottaa verkon ylläpitoa muun muassa siten, että se pakottaa verkon käyttäjät itse manuaalisesti lataamaan työasemilleen tarvittavat kriittiset päivitykset ja varmistaa samalla, ettei yhdessäkään verkkoon liittyvässä työasemassa ole tietoturvaa vaarantavia haavoittuvuuksia ainakaan puuttuvien tietoturvapäivitysten osalta. Toteutus hyödyttäisi laajamittaisessa käytössä ICTLAB:ia erityisesti siksi, että koululla on vastikään otettu käyttöön BYOD-luokka (Bring Your Own Device), jossa oppilaat voivat tuoda ja liittää verkkoon omia päätelaitteitaan, joiden ohjelmistojen ja käyttöjärjestelmien turvallisuutta ei luonnollisestikaan nykyisellään voida varmistaa.

Työn varsinaisena tutkimusongelmana on selvittää, miten posture-ominaisuus toimii ja mistä eri vaiheista sen käyttöönotto ICTLAB-ympäristössä koostuu. Samalla on tarkoitus tarkastella ja selvittää, miten se parantaa ICTLAB:n lähi-

verkon nykyistä tietoturvaa jo aikaisemmin testatun porttikohtaisen todennuksen lisänä. Tutkimusongelma voidaan erikseen ja laajemmin määritellä seuraavilla tutkimuskysymyksillä:

- Mikä on posture?
- Miten posture toimii?
- Miten sen avulla voidaan ICTLAB:n verkkoympäristöstä tehdä entistä turvallisempi?
- Mitkä ovat posturen määrittämisen eri vaiheet?

Työ on suoraa jatkumoa Ville Naumasen (2018) opinnäytetyölle, jossa ICT-LAB-ympäristöön suunniteltiin ja toteutettiin 802.1X-porttikohtainen todennus. Tarkoitus onkin hyödyntää jo olemassa olevaa toteutusta, ja määrittää posture-tarkistus sen päälle tietoturvaa entisestään parantavana lisäominaisuutena. Näin ollen koko 802.1X-porttitodennuksen käyttöönoton vaiheita ei tulla perustavanlaatuisesti käymään läpi, vaan keskitytään enemmän itse posture-ominaisuuteen ja sen määrittämiseen.

Työ koostuu kahdesta eri osiosta, joista toinen on teoriaosio ja toinen käytännön toteutus. Teoriaosuudessa käydään läpi IEEE 802.1X-standardin ja siihen liittyvien yhteys- ja autentikointiprotokollien taustaa ja teoriaa sekä perehdytään posture-tarkistuksen perustoiminnallisuuteen. Työn käytännön osuus on tarkoitus jakaa kahteen osaan. Ensimmäisessä vaiheessa luodaan virtuaalinen testiympäristö Jaakko Nurmen virtuaalilaboratorioon, jossa porttikohtaisen posture-palvelun käyttöönotto voidaan suunnitella ja toteuttaa, minkä jälkeen toisessa vaiheessa sitä voidaan pienimuotoisesti testata käytännössä ICT-LAB:n luokkatilan muutamalla työasemalla.

1.2 Tutkimusmenetelmän valinta

Opinnäytetyön tutkimusmenetelmäksi valikoitui kehittämistutkimus, joka menetelmänä vastaa parhaiten sen sisältöä ja tarkoitusperää. Se on monimenetelmäinen tutkimusmuoto, jossa yhdistyvät kvalitatiiviset ja kvantitatiiviset tutkimusmenetelmät, mutta se voi myös pelkästään olla kvalitatiivista tutkimusta (Kananen 2012, 19). Kehittämistutkimus koostuu kahdesta osasta: kehittämistyöstä sekä siihen liittyvästä tutkimuksesta. Salonen (2013, 25) kuvaa kehittä-

mishankkeen perimmäistä tarkoitusta seuraavasti: ”Kehittämishankkeen tuloksena syntyy tuotos, joka sisältää uuden tiedon lisäksi palvelun, tuotteen, oppaan, mallin, toimintatavan tai minkä tahansa innovaation, joka on aikaisempaa parempi tai kokonaan uusi.” Tämän työn tarkoitus on pyrkiä parantamaan ICTLAB-ympäristön tietoturvaa entisestään suunnittelemalla ja testaamalla jo aikaisemmin toteutetun 802.1X-porttitodennuksen käyttöönoton päälle verkon työasemien Windows-päivitysten ajantasaisuuden tarkistava posture-tarkistus sekä tarkastella kyseisen ominaisuuden toimintaa noin yleisellä tasolla. Suunnittelun ja testaamisen pohjalta välittyy myös ICTLAB:n henkilökunnalle lisätietoa niin posture-palvelusta kuin siihen vaadittavasta Cisco Identity Services Engine -ohjelmiston ominaisuuksista ja käytettävyydestä, mikä luo työhön tutkimuksellista otetta.

Työn varsinainen konkreettinen tuotos tulee olemaan sen pohjalta laadittu tiivistetty ohjeistus posture-tarkistuksen laajamittaiseen käyttöönottoon ICTLAB-ympäristössä, mikäli ISE-ohjelmiston hankinta tulee Xamkille lähitulevaisuudessa ajankohtaiseksi. Tällä hetkellä koululta puuttuvat ISE:n käyttölisenssit, minkä johdosta opinnäytetyö joudutaan toteuttamaan ohjelmistosta saatavilla olevan 90 päivän kokeilujakson avulla. Kokeilujakson aikana pyritään testaamaan sekä 802.1X-standardin mukainen posture-tarkistuksen käyttöönotto, että tarkastelemaan ICTLABin henkilökunnan suhtautumista uuteen ohjelmistoon. Näin selviää, onko koulun tulevaisuudessa kenties kannattavaa ostaa ohjelmiston varsinainen käyttölisenssi, jolloin posturea ja muita ISE:n ominaisuuksia voitaisiin hyödyntää laajemmin niin verkkoympäristön parantamisessa kuin opiskelukäytössä.

2 IEEE 802 STANDARDI

IEEE 802 on joukko IEEE-standardointijärjestön (Institute of Electrical and Electronics Engineers) kehittämiä ja ylläpitämiä lähiverkkostandardeja. IEEE-järjestön työryhmä 802:n vastuualueisiin kuuluu lähi- ja kaupunkiverkkojen (LAN ja MAN) standardoiminen ja sen tunnetuimpia standardeja ovat Ethernet ja WLAN. Standardien tarkoitus on luoda yhteinen perusta erilaisille lähiverkoille ja verkkolaitteille ja varmistaa niiden välinen yhteensopivuus. (IEEE 802 2018).

802-standardiperhe käsittää useita eri lähi- ja kaupunkiverkkostandardeja, joista jokaisen kehityksestä vastaa oma kehitysyksikkönsä. Merkittävimpiä 802-standardeja/työryhmiä ovat:

802.1: 802 LAN/MAN -arkkitehtuurin, -internetliikenteen ja -tietoturvan kehitys
802.3: Ethernet-lähiverkkotekniikka
802.11 Langattomat lähiverkot (WLAN) (Geier 2008, 22.)

Tässä työssä käsitellään IEEE 802.1X-standardiin pohjautuvaa posture-tarkistusta, joten teoriaosuudessa keskitytään ensin pohjustamaan kyseisen standardin perusteita. IEEE 802.1 -standardeihin kuuluva 802.1X määrittelee porttitodennuksen Ethernet- ja WLAN-verkoissa. Tämän vuoksi standardit 802.3 ja 802.11 ovat sen kannalta erityisen tärkeitä, sillä ne määrittelevät porttitodennusta hyödyntävän median, jota pitkin todennustiedot ja -liikenne kulkevat. (Geier 2008, 22.)

2.1 802.1X

802.1X on lähiverkossa käytettävä standardi porttikohtaiselle todennukselle. Se määrittelee asiakkaaseen ja palvelimeen perustuvan pääsynhallinnan ja autentikointiprotokollan, joiden avulla voidaan estää luvattomien laitteiden tai käyttäjien pääsy lähiverkkoon fyysisten porttien kautta. Standardi on AAA-mallin mukainen (Authentication, Authorization, Accounting) eli sen avulla voidaan sekä hallita että seurata verkon käyttöä. Autentikointipalvelin (authentication server) todentaa jokaisen kytkinporttiin tai langattomaan tukiasemaan yhdistetyn laitteen. 802.1X toimii OSI-mallin toisella eli siirtoyhteyskerroksella (Data Link layer) kaikissa IEEE 802-standardin mukaisissa verkoissa. (Cisco, 2016.)

802.1X-porttitodennuksen alussa verkkokytkimen tai langattoman tukiaseman portti, johon päätelaite on kytketty, sallii vain EAPOL-liikenteen (Extensible Authentication Protocol over LAN), jonka avulla itse todennus tapahtuu. Normaali liikenne kohdeverkkoon onnistuu vasta, kun todennus on suoritettu onnistuneesti ja portti on authorized-tilassa. (Cisco, 2016.)

Todennus tapahtuu kolmen eri komponentin välillä: Käyttäjää tai päätelaitetta, joka yrittää yhdistää kohdeverkkoon, kutsutaan asiakkaaksi (supplicant). Itse

todennuksen tekee puolestaan siihen varta vasten tarkoitettu autentikointipalvelin (authentication server), yleensä RADIUS-palvelin. Välikätenä todennuksessa toimii autentikaattori (authenticator), joka on päätelaitteille verkon liityntäpiste, yleensä kytkin tai langaton tukiasema. Sen tehtävänä on välittää käytettävän todennusmenetelmän tiedot asiakkaan ja autentikointipalvelimen välillä. Autentikaattori joko avaa tai sulkee liityntäportin asiakaslaitteelle riippuen todennuksen onnistumisesta ja autentikointipalvelimelta saadusta vastauksesta. (Cisco, 2016.)

2.2 Porttitodennuksen hyödyt

802.1X-porttitodennus varmistaa, etteivät luvattomat käyttäjät tai asiakaslaitteet pääse käsiksi verkon suojattuihin resursseihin, kuten palvelimiin, sovelluksiin tai tietokantoihin. Ilman todennusta kuka tahansa voi joko kytkeä päätelaitteensa verkkokaapelilla kytkinporttiin tai vaihtoehtoisesti yhdistää langattoman verkon tukiasemaan, mikä luo merkittävän tietoturvariskin yksityisissä verkoissa. (Geier 2008, 36.)

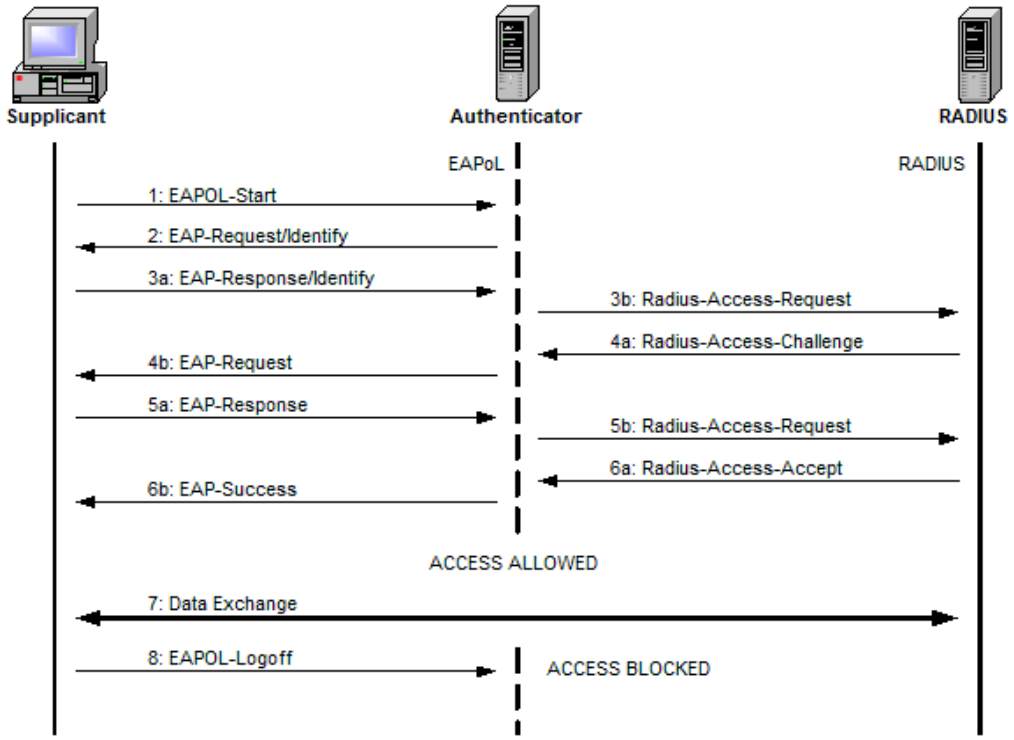
Riippuen käytetystä todennusmenetelmästä porttitodennus vaatii kirjautuneelta käyttäjältä aina joko pätevät, sisäisen palvelimen tietokannasta löytyvät käyttäjätunnukset, suojausvarmenteen tai molemmat. (Geier 2008, 44.)

2.3 Toimintaperiaate

802.1X-porttitodennuksen toiminta perustuu EAP-protokollaan (Extensible Authentication Protocol), jonka avulla todennuksessa tarvittavat tiedot, kuten käyttäjän tunnistetiedot (käyttäjätunnus/salasana) tai digitaaliset varmenteet (digital certificate), välitetään laitteelta toiselle.

Todennusprosessi (kuva 1) alkaa siten, että päätelaite eli asiakas kytkeytyy verkkokytkimen Ethernet-porttiin verkkokaapelilla tai vaihtoehtoisesti yhdistää langattoman verkon tukiasemaan yrittäessään saada pääsyä kohdeverkkoon. Kun kytkin tai tukiasema eli autentikaattori havaitsee portissa liikennettä, se lähettää asiakkaalle EAP-Request/Identity-paketin, jolla se pyytää päätelaitteelta tunnistetietoja. Tässä kohtaa todennusta mikään muu kuin EAP-liikenne ei pääse kytkimen läpi kohdeverkon suojattuun osaan. (Geier 2008, 47.)

Tämän jälkeen asiakas vastaa autentikaattorin pyyntöön lähettämällä sille tunnistetiedot sisältävän EAP-Response/Identity-paketin, minkä jälkeen kytkin alkaa toimia välittäjänä asiakkaan ja autentikointipalvelimen välillä. (Geier 2008, 47.)



Kuva 1. IEEE 802.1X -porttitodennuksen perusperiaate ja viestinvaihto (VOCAL Technologies.)

Kun kytkin vastaanottaa asiakkaan tunnistetiedot, se muuntaa kyseisen paketin RADIUS Access-Request -muotoon ja välittää sen palvelimelle (Geier 2008, 49.). Autentikaattorin ja palvelimen välisten salausavaimien on kuitenkin vastattava toisiaan, jotta palvelin ylipäänsä käsittelee kyseisen pyynnön. On hyvä huomata, että asiakaslaitteen ja autentikaattorin välinen kommunikaatio tapahtuu EAPOL-protokollalla (Extensible Authentication Protocol over LAN) avulla, jolloin EAP-viestit sisällytetään EAPOL-paketteihin. Autentikaattorin ja autentikointipalvelimen (RADIUS) välinen viestintä sen sijaan tapahtuu RADIUS-protokollan avulla, jolloin EAP-viestit sisällytetään RADIUS-paketteihin. (Geier 2008, 45 ja 49.)

RADIUS Access-Request -paketin vastaanotettuaan autentikointipalvelin vertaa asiakkaalta saamiaan tunnistetietoja sen omaan tai mahdollisesti ulkoi-

seen tietokantaan ja tekee sen perusteella päätöksen todennusprosessin jatkamisesta. Jos tunnistetiedot eivät ole päteviä, eli ne eivät vastaa palvelimen omia tietoja, todennus epäonnistuu ja palvelin lähettää kytkimelle Radius-Access Reject -viestin. Tämän autentikaattorikytkin muuntaa edelleen EAP-Failure-viestiksi ja lähettää asiakaslaitteelle epäonnistuneen todennuksen merkiksi. Tässä tapauksessa asiakkaan pääsy verkkoon voidaan kokonaan estää, jolloin kytkimen liityntäportti jää unauthorized-tilaan, tai vaihtoehtoisesti siirtää se rajoitettuun VLAN:iin. (Geier 2008, 46–47.)

Mikäli tunnistetiedot kuitenkin ovat päteviä, jatkuu todennusprosessi seuraavalla tavalla: palvelin lähettää autentikaattorille RADIUS Access-Challenge-paketin, jonka tämä edelleen muuntaa EAPOL-muotoon ja välittää asiakkaalle. Paketin sisältö ja lähetettyjen viestien määrä riippuu tässä kohtaa käytettävästä todennusmenetelmästä. Tiedot käytettävästä EAP-tunnistemenetelmästä sisältyvät RADIUS Access-Challenge -pakettiin. (Cisco, 2016.)

Tässä kohtaa todennus alkaa ikään kuin alusta, kun asiakas ja palvelin ovat sopineet keskenään yhteisen todennusmenetelmän. RADIUS Access-Challenge -viestiin asiakas vastaa todennusmenetelmän edellyttämillä tunnistetiedoilla, jotka voivat vaihdella nimi/salasana-yhdistelmästä erilaisiin suojausvarmenteisiin todennustavasta riippuen.

Mikäli asiakas vastaa haasteeseen asianmukaisilla tunnistetiedoilla, palvelin lähettää sille RADIUS Access-Accept -paketin, jonka autentikaattori muuntaa EAP-Success muotoon ja välittää asiakkaalle merkkinä onnistuneesta todennuksesta. Tämän jälkeen autentikaattori eli kytkin tai langaton tukiasema muuttaa portin, johon asiakas on yhdistänyt, authorized-tilaan eli sallii siinä normaalin liikenteen kohdeverkkoon. (Geier 2008, 50.)

3 PORTTITODENNUKSEN TÄRKEÄT PROTOKOLLAT

3.1 EAP

EAP (Extensible Authentication Protocol) on porttitodennuksessa käytettävä standardi tai viitekehys. Nimestään huolimatta se ei kuitenkaan ole varsinainen protokolla, vaan enemmänkin viitekehys erilaisille todennusmenetelmille. EAP toimii OSI-mallin toisella eli siirtoyhteyskerroksella (Data Link layer). Sitä

käytetään hyvin yleisesti Point-to-Point-yhteyksissä sekä IEEE 802-mukaisissa verkoissa, jotka eivät vaadi toimiakseen IP-protokollaa. (RFC 3748, 2004. 3.)

EAP:n hyötyjä ovat sen arkkitehtuurin joustavuus. Sen käyttötarkoitus on valita sopiva todennusmenetelmä sen jälkeen, kun autentikaattori pyytää palvelimelta siihen liittyviä lisätietoja. Sen sijaan, että EAP vaatisi autentikaattoriin tarvittavan päivityksen tukemaan tiettyä todennusmenetelmää, se sallii backend-autentikointipalvelimen käytön, jolloin itse palvelin hoitaa todennusmenetelmän toteutuksen ja autentikaattori toimii vain läpimenolaitteena (pass-through device). Tällöin todennusmenetelmien valikoima riippuu täysin palvelimesta ja sen tukemista protokollista. (RFC 3748, 2004, 3.)

Eri EAP:n tukemia todennusmenetelmiä ovat muun muassa LEAP, EAP-TLS, EAP-MD5, PEAP ja EAP-MSChapV2 (Extensible Authentication Protocols 2018).

3.2 EAPOL

EAPOL (Extensible Authentication Protocol over LAN) on IEEE 802.1X -verkoissa käytössä oleva paketointitekniikka, jonka avulla EAP-viestit paketoidaan ja kuljetetaan laitteelta toiselle. EAPOL-liikennettä tapahtuu pääsääntöisesti asiakaslaitteen ja autentikaattorin välillä porttikohtaisessa todennuksessa. (Geier 2008, 55.)

EAPOL-kehyksessä on neljä kenttää, jotka määrittävät sen version, tyypin, pituuden sekä sisältyvän datan. Tyyppikentän (Packet Type) mukaan määräytyy viestin tyyppi, joka voi olla EAP-packet, EAPOL-Start, EAPOL-Logoff, EAPOL-Key tai EAPOL-Encapsulated-ASF-Alert. (Geier 2008, 58.)

EAPOL-Start-kehys aloittaa nimensä mukaisesti porttitodennuksen, kun autentikaattori havaitsee liityntäportin linkin nousevan ylös, jolloin se lähettää asiakaslaitteelle kyseisen paketin. Jos linkki on jo ylhäällä ennen todennusta, on asiakkaan itsensä alustettava todennus lähettämällä sama paketti autentikaattorille. EAPOL-Logoff on puolestaan paketti, jonka asiakas lähettää autentikaattorina toimivalle kytkimelle tai tukiasemalle todennuksen loppuvaiheessa,

millä se haluaa viestittää haluavansa poistua verkosta ja lopettaa todennusprosessin. Paketin saatuaan kytkin tai tukiasema palauttaa portin unauthorized-tilaan. Muilla EAPOL-kehyksillä on itse todennusprosessiin liittyviä tarkoitusperiä. EAPKey-kehyksiä esimerkiksi käytetään salaus- ja allekirjoitusavaimien välittämiseen todennuksessa, jolloin pystytään paremmin todentamaan, onko verkkoon pääsyä tavoitteleva laite luvallinen vai ei. (Geier 2008, 59–60.)

3.3 PEAP-MSCHAPv2

PEAP (Protected Extensible Authentication Protocol) on EAP-todennuksen muoto, jossa asiakkaan ja palvelimen välille luodaan suojattu ja salattu TLS-tunneli tiedonsiirtoa varten. Tunneli luodaan käyttäen pätevää palvelimen lähettämää suojausvarmennetta (server certificate), jonka avulla todennuspalvelin todistaa asiakkaalle olevansa luotettava. PEAP vaatii suojausvarmenteen ainoastaan palvelimelta, joten erillistä asiakasvarmennetta ei tarvitse erikseen asentaa jokaiselle todennettavalle työasemalle. Sen sijaan asiakaslaitteella tulee olla asennettuna CA:n (certification authority) allekirjoittama juurivarmenne (root certificate), jonka avulla se pystyy varmistamaan palvelimen esittämän varmenteen todenperäisyyden. Palvelinvarmenteen ja asiakkaalle asennetun juurivarmenteen tulee myös olla saman CA:n allekirjoittamia. (Cisco 2011.)

PEAP ei itse tee varsinaista todennusta, vaan se luo ainoastaan turvallisen yhteyskäytävän muille EAP-protokollille. Yleisin PEAP:n kanssa käytettävä todennusprotokolla on MSCHAPv2, jonka viestinvaihto kulkee salattuna PEAP-tunnelin sisällä. MSCHAPv2-todennus perustuu käyttäjänimi/salasana-yhdistelmään ja se tukee molemminpuolista, sekä asiakkaan että palvelimen todentamista. Protokollan viestinvaihdossa käytetään laitteiden välisiä salausavaimia, jotka yksinään ovat kuitenkin haavoittuvaisia erilaisille sanakirjahyökkäyksille. Yhdessä PEAP:n kanssa se muodostaa kuitenkin turvallisen todennusmenetelmän, koska kaikki viestit lähetetään suojattuna TLS-tunnelissa. (Cisco 2011.)

3.4 RADIUS

RADIUS (Remote Authentication Dial-In User Service) on käyttäjien tunnistukseen ja tilastointiin kehitetty protokolla. RADIUS perustuu palvelimen ja asiakaslaitteen eli NAS:n (Network Access Server) väliseen kommunikaatioon, joka käydään UDP-protokollan avulla (User Datagram Protocol). (Cisco 2006.)

RADIUS on avoin standardi, toisin kuin TACACS+ -protokolla, joka on Ciscon kehittämä ja patentoima yksityisomisteinen vastaava ratkaisu. RADIUS suorittaa sekä todennuksen että valtuutuksen samanaikaisesti ja tilastoinnin erikseen. (Carroll 2004, 16.)

RADIUS tarvitsee toimiakseen sekä asiakaslaitteen että palvelimen. Asiakaslaite on yleisesti NAS-laite, jona voi toimia esimerkiksi verkkokytkin tai langattoman verkon tukiasema. RADIUS-protokollan toimintaperiaatteena on, että RADIUS-asiakas lähettää loppukäyttäjän tunnistetiedot, kuten käyttäjänimi/salasana-yhdistelmän RADIUS-palvelimelle tarkastettavaksi, minkä jälkeen palvelin lähettää sille vastauksena tunnistusprosessin tuloksen. Asiakaslaite tekee päätöksen käyttäjän pääsyn sallimisesta verkkoon palvelimen vastauksen perusteella. Mikäli käyttäjän tai päätelaitteen tunnistetiedot ovat pätevät, kytkin tai langaton tukiasema avaa portin, jolloin käyttäjällä on pääsy kohdeverkkoon. Toisaalta, jos tunnistetiedot eivät vastaa palvelimella olevia tietoja, käyttäjän pääsy verkkoon evätään. (Cisco 2006.)

4 POSTURE-TARKISTUS

Posture on verkkoon liittyville työasemille suoritettava turvatarkastus, jolla varmistetaan työasemien täyttävän verkon turvallisuuden takaamiseksi määritetyt kriteerit. Tarkistus vaatii toimiakseen 802.1X-porttitodennuksen, tai vaihtoehtoisesti jonkun muun todennusmenetelmän (esim. MAB tai VPN), jonka avulla varsinaiset käyttäjät tai työasemat todennetaan. Näin ollen posturen kohdalla ei voida puhua kokonaan erillisestä asiasta vaan enemmänkin 802.1X –todennuksen lisäominaisuudesta. (Posture Services on the Cisco ISE Configuration Guide 2019.)

Cisco-ympäristössä posture on Cisco Identity Services Engine -verkonhallintaohjelmiston (ISE) palvelu, joka mahdollistaa päätelaitteiden compliance-tilan

määrittämisen agenttiskannauksen avulla, minkä perusteella niiden pääsyn tasoa verkkoon voidaan säännöstellä (Cisco Identity Services Engine Administrator Guide, Release 2.2 2019).

Työasemalta vaadittavat asiat voi verkonvalvoja itse määrittää siihen tarkoitetulla ISE:n posture-käytännöillä (posture policies) ja yleisimpiä sellaisia ovat muun muassa ajantasaiset käyttöjärjestelmän tietoturvapäivitykset, asianmukaisen virustorjuntaohjelmiston asennus ja virustunnisteiden ajantasaisuus työasemalla, rekisteriavaimet jne. Näiden perusteella posture tutkii työaseman sen yrittäessä yhdistää joko langalliseen tai langattomaan verkkoon ja lopputuloksen perusteella joko sallii tai evää sen pääsyn sinne. Näin ollen pelkkä onnistunut porttitodennus ei enää riitä verkkoon pääsyyn, vaan myös itse työaseman on oltava ns. ”turvallinen”.

Itse posture-tarkistuksen suorittaa työasemalla oleva posture-agentti, kuten Cisco AnyConnect Secure Mobility Client- tai Network Admission Control Agent -ohjelma (NAC), joka myös toimeenpanee ISE-palvelimelta saamansa posture-käytännöt ja asiakkaiden valtuutuksen. Se siis toimii ISE:n ns. välittäjänä työasemilla eli se suorittaa varsinaisen valtuutuksen ja tekee päätöksen verkkoon pääsyn sallimisesta, mutta ohjeet siihen se saa tiukasti ISE:ltä. Agentti myös välittää tiedot asiakkaan posture-tilasta palvelimelle tilastointia varten.

Posture-tarkistuksen määritykset työssä tulevat koostumaan seuraavista osa-alueista:

- **Client provisioning** – Määrittää resurssienjakokäytännöt, joita tarvitaan posture-agentin sekä sen tarvitsemien moduulien ja määritysprofiilien jakamiseen työasemille. Voidaan myös puhua työasemien ”varustamisesta”.

- **Posture policy** – Posture-käytäntö, joka määrittää vaatimukset, joiden perusteella työaseman katsotaan noudattavan verkon tietoturvakäytäntöjä. Kun työasema täyttää posture-tarkistuksen edellyttämät vaatimukset, sen tilaksi katsotaan ”compliant” (vaatimusten mukainen) ja yhteys kohdeverkkoon voidaan sallia.

- **Authorization policy** – Valtuutuskäytäntö määrittää kohdeverkon resursseihin pääsyn tason ja mahdolliset työasemalle jaettavat palvelut riippuen sen posture-tilasta.

4.1 Client provisioning

Jotta posture-tarkistus voidaan suorittaa, tarvitsee asiakaslaitteelle jakaa posture-agentti, joka on työasemalle kiinteästi asennettava tai selaimessa toimiva ohjelma. Posture-agentti suorittaa itse työaseman tarkastuksen ja välittää tiedot siitä ISE-palvelimelle. Aikaisemmin posture-agenttina on Cisco-ympäristössä yleisesti käytetty NAC Agent -ohjelmaa (Network Admission Control), mutta sen tuen loppumisen myötä sen on korvannut Cisco AnyConnect Secure Mobility Client, jota myös tässä työssä käytetään. Luonnollisestikaan todennuksen alussa asiakkaalla ei vielä ole pääsyä kohdeverkkoon tai Internettiin, josta se voisi agentin ladata ja asentaa. Sen sijaan asiakaslaite on tarkoitus uudelleenohjata ISE:n omaan resurssienjakoportaaliin (Client Provisioning Portal), kun alustava 802.1X-todennus on suoritettu onnistuneesti. Portaalista työasema saa ladattua itselleen posture-agentin asennustiedostot, mikäli näin on ISE:n resurssienjakokäytännöissä määritetty ja asennustiedostot on etukäteen ladattu palvelimelle.

Kuten todettua, posture-agentti voi olla pysyvä kiinteästi työasemalle asennettava ohjelma tai web-pohjainen instuntokohtainen sovellus. Kiinteän ohjelman kohdalla asennus on kertaluontoinen ja seuraavalla yhdistämiskerralla se latautuu automaattisesti, kun taas web-pohjainen selaimessa toimiva agentti täytyy joka kerta ladata uudestaan ja se poistuu istunnon päätteeksi. Posture-agentin välityksellä voi myös suorittaa mahdolliset korjaustoimenpiteet, jolloin asiakas voi yhdellä painalluksella ladata korjauspalvelimelta kaikki tarvittavat päivitykset tai puuttuvat ohjelmistot. (Posture Services on the Cisco ISE Configuration Guide 2019.)

4.2 Posture policy

Posture-tarkistuksen keskeisimmät määritykset ovat posture-käytännöt, jotka määrittävät verkkoon yhdistämistä yrittävältä työasemalta vaadittavat kriteerit. Käytäntöjä voi luoda tiedoston olemassa olon, rekisteriavaimen, prosessin, sovelluksen, Windows-päivitysten tai esimerkiksi asennetun antivirus-ohjelmiston ja sen määrityspäivitysten ajantasaisuuden mukaan. Kriteerit koskevat ennalta määrätyt ehdot täyttäviä päätelaitteita tai käyttäjiä esimerkiksi käyttäjäryhmän tai käyttöjärjestelmän perusteella. Näin ollen Windows-, Mac- ja Linux-

koneille voi määrittää omat erilliset kriteerinsä. Posture-agentti tarkistaa työaseman ja antaa sille sen pohjalta posture-tilan. (Posture Services on the Cisco ISE Configuration Guide 2019.)

Eri posture-tiloja ovat:

- **Tuntematon (Unknown)** – Posture-tilaa ei voitu määrittää, koska tietoa ei kerätty. Yleensä todennuksen alkuvaiheessa, jolloin asiakaskoneella ei vielä ole asennettuna posture-agenttia.
- **Vaatimusten vastainen (Noncompliant)** – Posture-tarkistuksen yhteydessä työasema ei täyttänyt yhtä tai useampaa vaatimusta.
- **Vaatimusten mukainen (Compliant)** – Työasema noudattaa kaikkia pakollisia vaatimuksia.

Vaatimukset perustuvat konfiguroitaviin ehtoihin tai näiden yhdistelmiin (compound rules). Jokaiseen vaatimukseen tai kriteeriin voidaan myös liittää korjaustoimenpide, joka auttaa työasemaa täyttämään annetun vaatimuksen, esim. antivirus-ohjelmiston asennus tai päivitys tai käyttöjärjestelmän kriittinen tietoturvapäivitys. (Posture Services on the Cisco ISE Configuration Guide 2019.)

4.3 Authorization policy

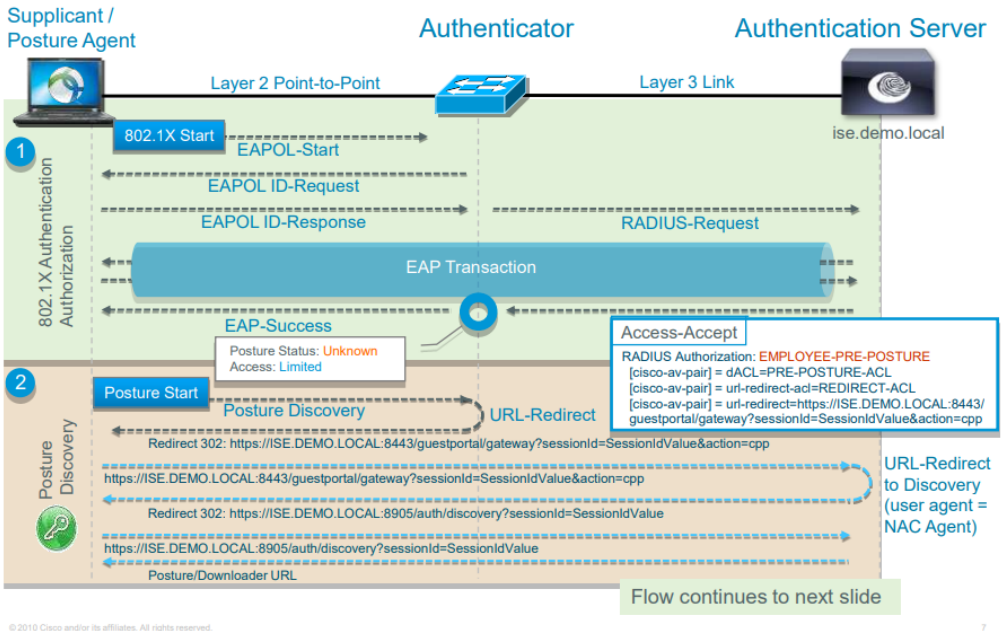
Posture-tilan perusteella authorization policy eli valtuutuskäytäntö määrittää kohdeverkkoon pääsyn tason, jonka perusteella myös määräytyvät työasemalle tarjottavat palvelut. Tarkistuksessa Compliant-statuksen saavat työasemat saavat suoraan pääsyn verkkoon, kun taas Noncompliant tai Unknown-statuksen saavat päätelaitteet voidaan hetkellisesti asettaa karanteeniin, jolloin niiden pääsy verkon resursseihin on rajattu. Yleensä niiden pääsy sallitaan ainoastaan posture- ja korjauspalveluihin. Asiakas saa näin ollen mahdollisuuden korjata puutteelliseksi havaitun työaseman, ja mikäli korjaustoimenpiteet suoritetaan onnistuneesti, tehdään posture-tarkastus uudelleen, jolloin asiakaslaite saa tilakseen Compliant ja sen myötä pääsyn verkkoon. (Posture Services on the Cisco ISE Configuration Guide 2019.)

4.4 Posturen toimintaperiaate

Posturen päätapahtumaketju 802.1X-todennuksessa koostuu viidestä eri vaiheesta (kuvat 2 ja 3):

1. Kun 802.1X-todennus on kytketty päälle, verkkoon liittyvä asiakaskone neuvottelee asiakaskytkimen eli autentikaattorin kanssa aloittaakseen 802.1X-todennusprosessin. Alkaa EAP-tiedonsiirto, jossa kytkin toimii välittäjänä asiakaskoneen ja RADIUS-palvelimen (esimerkissä Cisco Identity Services Engine) välillä. Mikäli todennus suoritetaan onnistuneesti, saa asiakaslaite palvelimelta posture-tilakseen Tuntematon (Unknown). Tämä johtuu siitä, että asiakaskoneella ei vielä tässä vaiheessa tunnistusta ole asennettuna agenttia, jonka avulla varsinainen posture-tila voitaisiin määrittää.

2. ISE ohjeistaa kytkintä uudelleenohjaamaan 802.1X-todennetun asiakkaan portaaliin, josta se voi ladata itselleen tarvittavan kiinteän agenttiohjelman tai vaihtoehtoisesti web-pohjaisen väliaikaisen agentin, joka poistuu istunnon päättymisen jälkeen. Saadun agentin muoto riippuu palvelimelle tehdyistä määrityksistä ja ryhmäkäytännöistä. Parametrit uudelleenohjaukseen autentikaattorikytkin saa 802.1X-todennuksen päättävässä RADIUS Access-Accept -paketissa.

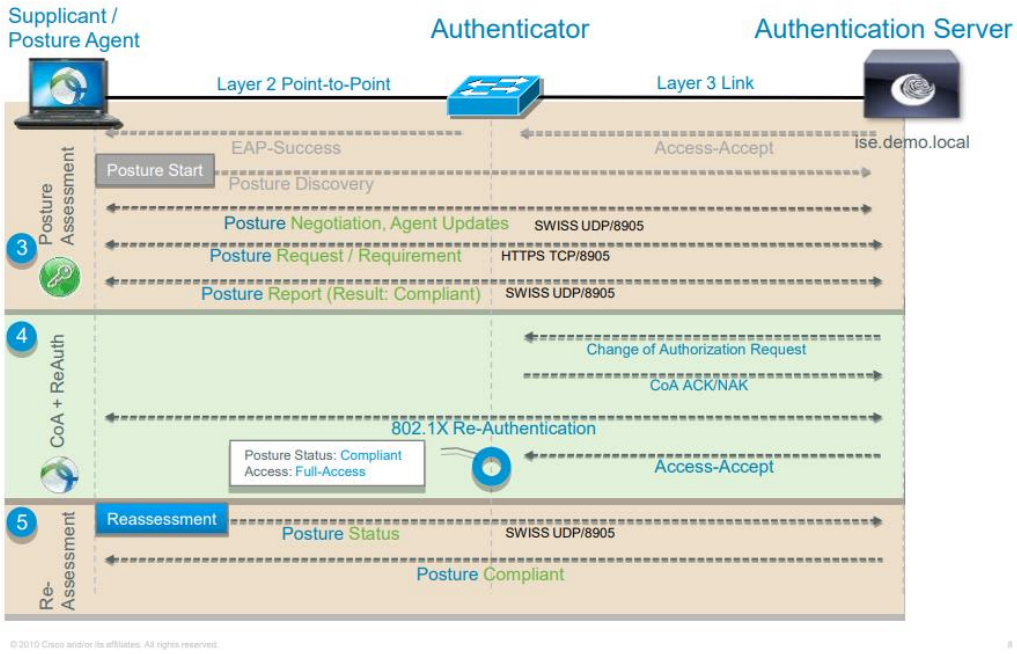


Kuva 2. IEEE 802.1X Posture –tapahtumaketju (vaihe 1) (Cisco.)

3. Kun asiakaskoneella on asennettuna agentti-ohjelma (NAC Agent tai Cisco AnyConnect), posture-tapahtumaketju alkaa heti työaseman yrittäessä liittyä verkkoon tai käyttäjän sisäänkirjautumisen yhteydessä, riippuen määrityksistä. Agentti-ohjelman ja ISE:n välinen kommunikaatio tapahtuu Swiss-protokollan avulla, ja sen lopussa määräytyy asiakkaalle posture-tila.

4. Kun posture-tarkistus on suoritettu, lähettää ISE autentikaattorikytkimelle Change of Authorization -pyynnön, joka käynnistää 802.1X-uudelleentodennuksen. ISE lähettää kytkimelle saatua posture-tilaa vastaavat valtuutusattribuutit valtuutuskäytännön mukaisesti, minkä perusteella määräytyvät asiakaslaitteen pääsyoikeudet verkkoon.

5. Jos määrityksissä on otettu käyttöön jaksottaiset tarkistukset, tarkistus suoritetaan säännöllisin väliajoin uudestaan mahdollisten muutosten varalta. Asiakkaan posture-tilan muuttuessa posture-tapahtumaketju alkaa alusta. (ISE Posture Style Comparison for Pre and Post 2.2 2018.)



Kuva 3. IEEE 802.1X Posture –tapahtumaketju (vaihe 2) (Cisco.)

5 CISCO IDENTITY SERVICES ENGINE (ISE)

Cisco Identity Services Engine eli ISE on verkonhallintaohjelmisto, joka mahdollistaa erilaisten turvallisuus- ja pääsynhallintakäytäntöjen luomisen ja täytäntöönpanon yrityksen sisäverkkoon liittyneillä työasemilla. Se on hyvin skaalautuva ja sopii erityisen hyvin identiteetinhallintaan suurissa, jopa miljoonia päätelaitteita käsittävissä verkoissa, joissa käyttäjillä on käytössään useita erilaisia laitteita ja sovelluksia. (Release Notes for Cisco Identity Services Engine, Release 2.6 2019.)

Lyhyesti kuvailtuna ISE:n avulla voi monipuolisesti hallita, mitkä käyttäjät pääsevät verkkoon ja mihin palveluihin heillä on pääsy. Sitä voi käyttää perinteisenä todennus- eli RADIUS-palvelimena ja sen avulla voi todentaa niin langallisen kuin langattomankin verkon sekä VPN-yhteydellä verkkoon yhdistävät käyttäjät. Todennus voi perustua pätevään suojausvarmenteeseen, laitteiden MAC-osoitteisiin tai muunlaiseen laiteprofilointiin. Niiden perusteella ja erilaisten valtuutuskäytäntöjen avulla voidaan työasemat sijoittaa tiettyihin VLAN-verkkoihin. Todennuksen tai valtuutuksen läpäisemättömät työasemat voidaan näin ollen sijoittaa esimerkiksi vieraille tarkoitettuun guest VLANiin, jossa niillä on vain rajoitettuja oikeuksia tai niiltä voidaan kokonaan estää verkkoon pääsy. (Release Notes for Cisco Identity Services Engine, Release 2.6 2019.)

Tässä työssä ISE toimii sekä RADIUS-palvelimena 802.1X-todennuksessa että suorittaa työasemilla posturen, jonka tuloksen perusteella verkkoyhteys joko sallitaan tai evätään.

6 TYÖN VAATIMUKSET

IEEE 802.1X -pohjainen posture-tarkistus toimii osana porttitodennusta, joten sen määrittämiseksi tarvitsee itse porttitodennuksen olla toiminnassa. Xamkin ICTLAB:ssa on jo alustavasti testattu ja otettu käyttöön 802.1X-porttitodennus, joten posture-tarkistuksen konfiguroimista tullaan jatkamaan sen pohjalta. Topologiaan voi tulla pieniä muutoksia, mutta suurin muutos tulee olemaan RADIUS-palvelinohjelmiston vaihtuminen testeissä Microsoftin Windows Serverin NPS-palvelusta (Network Policy Server) Ciscon ISE-ohjelmistoon (Identity Services Engine), joka tukee posture-toiminnallisuutta. Windows Server 2016

-palvelinohjelmistossa vastaavaa toiminnallisuutta ei enää ole NAP-ominaisuuden (Network Access Protection) tuen loppumisen Windows 10 -käyttöjärjestelmän myötä (Windows Dev Center 2018).

Kuten porttitodennuksessa yleensäkin, tarvitaan konfiguraatioon kolme keskeistä komponenttia: asiakas eli työasema, autentikaattori eli asiakkaille verkon liityntäpiste sekä autentikointipalvelin hoitamaan 802.1X-porttitodennus. Tämän päälle määritetään ISE:n avulla verkkoon posture-toiminto, joka tarkistaa verkkoon liittyvän työaseman käyttäjän sisäänkirjautumisen jälkeen.

Porttitodennus ja posture vaativat työasemilta ja verkkolaitteilta 802.1X-tuen ja yhteensopivuuden. Windows 10 -käyttöjärjestelmä, jota työssä tullaan käyttämään asiakaskoneissa, sisältää oman sisäänrakennetun 802.1X supplicant-ohjelmiston, joten sen kohdalla ei jouduta tekemään erityistoimenpiteitä. Myöhemmin posture-määrityksen käyttöönoton jälkeen 802.1X-todennuksen tekee työasemille asennettu AnyConnect-asiakasohjelma.

802.1X-yhteensopivien kytkimien ja päätelaitteiden lisäksi täytyy autentikointipalvelimen tukea RADIUS- ja EAP-protokollaa. ISE tukee molempia, joten tämä ei ole ongelma.

Haastavimman osuuden työlle luonee tarve yhdistää kaksi eri ympäristöä eli Windows Server 2016 -palvelimen ominaisuudet yhteen Cisco ISE:n kanssa. Valitettavasti vain ISE tukee posturen kaltaista palvelua, mikä tekee siitä toteutuksen kannalta välttämättömän. Mikäli Windowsin oman NAP-ominaisuuden tukea ei olisi lopetettu, olisi koko työ tehty Windows-palvelimen omilla työkaluilla. Tämä olisi helpottanut toteutusta merkittävästi, koska kaikki työssä käytetyt palvelinroolit aina Active Directory -käyttäjätietokannasta RADIUS-palvelimen ominaisuuksiin olisivat olleet yhdessä ja samassa paikassa. Toisaalta tänä päivänä eri valmistajien laitteiden ja ohjelmistojen yhteensopivuus on hyvä ja niiden yhdistäminen tehty mahdollisimman helpoksi, joten tämä ei todennäköisesti tule tuottamaan suurempia ongelmia. Samalla tämä luo mahdollisuuden testata ICTLAB:ssa täysin uutta ISE-ohjelmistoa, ja antaa henkilökunnalle palautetta sen ominaisuuksista ja käytettävyydestä.

7 KÄYTÄNNÖN TOTEUTUS

Tavoitteena on suorittaa työn käytännön toteutus kahdessa vaiheessa, joista ensimmäinen on posture-tarkistuksen suunnittelu ja käyttöönotto eristetyssä ja verkon toiminnan simulointiin ja testaamiseen tarkoitetussa virtuaalilaboratorioympäristössä. ICTLABin virtuaalilaboratorion on suunnitellut ja toteuttanut opinnäytetyönään Jaakko Nurmi (2016). Nurmi vastaa myös laboratorion ylläpitämisestä ja jatkokehittämisestä, joten hänen kanssaan tullaan tekemään jonkin verran yhteistyötä ja hän tulee osaltaan auttamaan virtuaalitestauksen saattamisessa onnistuneesti maaliin.

Mikäli virtuaalitestaus suoritetaan onnistuneesti, tavoitteena on toisessa vaiheessa laajentaa toteutusta ICTLABin varsinaiseen lähiverkkoon. Tämän toteutuminen on kuitenkin epävarmaa, koska ISE:n käyttöönottamiseen vaadittavat muutostoimenpiteet verkossa ovat merkittävät ja melko monimutkaiset, minkä lisäksi posturen käyttöönotto saattaa aiheuttaa merkittäviä häiriöitä verkon käyttäjille. Jos ISE:n ja posturen käyttöönotto oikeassa lähiverkkoympäristössä kuitenkin toteutetaan, se tullaan tekemään pienimuotoisesti ja siten, ettei siitä aiheudu verkon käyttäjille suurempaa haittaa. Näin ollen testaamiseen riittää muutama käyttäjä ja työasema sekä verkon runko- ja access-kytkin. Posture-tarkistuksen käyttöönotto laajamittaisemmin ei aikataulun tai resurssien puitteissa ole muutenkaan mahdollista tarvittavien Cisco Identity Services Enginen käyttölisenssien puuttuessa.

7.1 Ensimmäinen vaihe: virtuaalilaboratorio ja topologian luominen

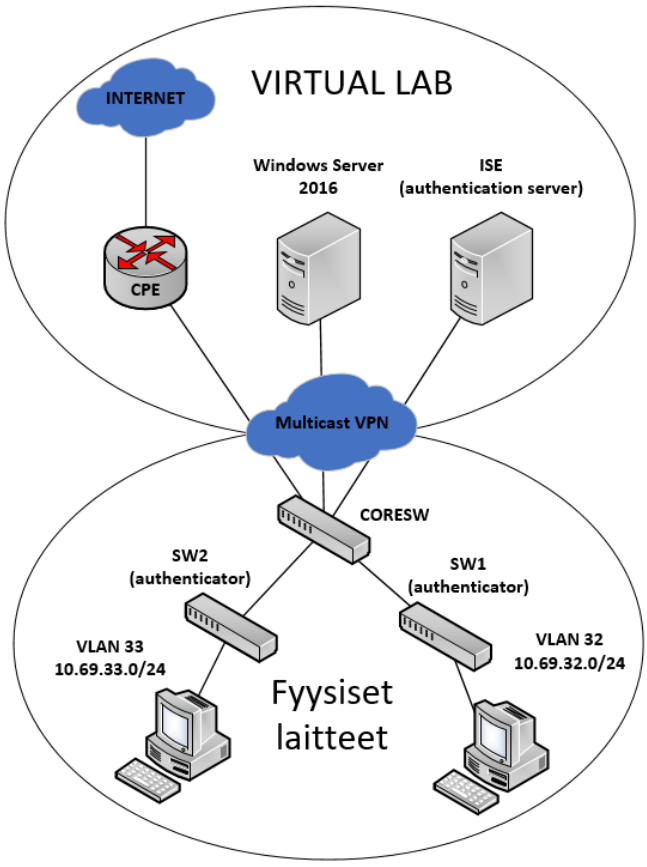
Työn käytännön toteutus aloitettiin luomalla virtuaalinen testiympäristö ja topologia Xamkin Virtual Lab -ympäristöön.

Työ perustuu vahvasti Ville Naumasen opinnäytetyönään (2018) ICTLAB:iin tehdylle 802.1X-todennukselle ja sen vuoksi itse porttitodennuksen käyttöönottamisen eri vaiheet ovat hyvin samankaltaisia. Sen vuoksi tässä työssä niitä ei käydä perustavanlaatuisesti läpi, vaan keskitytään enemmän itse posture-ominaisuuden käyttöönottoon.

Windows-palvelimen aktiivihakemiston määritykset ja käyttäjienluonti sekä PEAP-todennuksessa tarvittavien suojausvarmenteiden asennus työasemille ja ISE-palvelimelle on tehty etukäteen.

Alun perin testauksen alkuvaiheessa luotiin koko topologia verkkolaitteineen virtuaalilaboratorioon vastaamaan todellista ICTLAB-ympäristöä pienessä mittakaavassa. Työn edetessä havaittujen ongelmien seurauksena jouduttiin kuitenkin siirtymään niin sanottuun hybridiratkaisuun eli virtuaali- ja oikeiden fyysisten laitteiden yhdistelmään, johtuen virtuaalikytkinten IOS-testiversion puutteellisista ominaisuuksista. Virtuaalikytkimet eivät muun muassa tukeneet http-uudelleenohjaukseen liittyviä parametreja, mikä teki mahdottomaksi työasemien uudelleenohjaamisen resurssienjakoportaaliin posture-agentin lataamista varten. Virtuaalikytkimien sijaan jouduttiinkin ottamaan käyttöön fyysiset Cisco Catalyst 3560- ja 2960 -kytkimet, jotka laboratorioinsinööri Jaakko Nurmen toimesta yhdistettiin Multicast VPN:llä virtuaalisiin Windows Server 2016- ja Cisco ISE 2.6 -palvelimiin sekä internetin reunareitittimeen.

Lopullinen testitopologia (kuva 4):



Kuva 4. Testitopologia

7.2 Windows Server 2016 -palvelimen määritykset

Windows-palvelimen tärkein tehtävä topologiassa on toimia käyttäjätietokantana 802.1X-todennuksessa Active Directory Domain Services -palvelinroolin avulla. Myös Cisco ISE:ä voitaisiin käyttää identiteetinhallintaan ja käyttäjätodennukseen, mutta työn sujuvuuden takaamiseksi käytetään siihen tarkoitukseen aktiivihakemistoa, koska se soveltuu erityisen hyvin Windows-ympäristöihin ja sellainen on jo valmiina käytössä ICTLAB-ympäristössä. Tämä myös tulee helpottamaan posturen käyttöönottoa oikeassa ympäristössä, jossa suurin osa tarvittavista määrityksistä on jo valmiiksi tehtynä. Ainoa lisätoimenpide, joka tästä seuraa on ISE-palvelimen määrittäminen käyttämään ulkoista käyttäjätietokantaa.

Toinen merkittävä asia, johon Windows-palvelinta tullaan työssä käyttämään, on Windows-päivitysten jakaminen verkon työasemille WSUS-palvelinroolin (Windows Server Update Services) avulla. Tätä tullaan hyödyntämään myös postureen liittyvissä korjaustoimenpiteissä, joissa verkon asiakaslaitteille jaetaan puuttuvat kriittiset Windows-päivitykset porttitodennuksen yhteydessä. WSUS-palvelinroolin määrityksiin perehdytään tarkemmin luvussa 7.3.5.

Windows-palvelin toimii virtuaalitestauksessa myös DNS-palvelimena sekä vastaa suojausvarmenteiden luomisesta ja allekirjoittamisesta, joten muut sille asennettavat palvelut ovat DNS Server sekä Active Directory Certificate Services. Luodut PEAP-todennuksessa vaadittavat suojausvarmenteet on jaettu työasemille Windows-palvelimen ryhmäkäytännöillä (Group Policy Management).

7.3 Cisco ISE:n ja posturen määritykset

Määrityksissä lähdetään ensin liikkeelle lisäämällä käytössä olevat kytkimet RADIUS-asiakkaiksi ISE:ssä kohdasta *Administration* > *Network Resources* > *Network Devices*. Nimetään käytössä olevat kytkimet kuvaavasti ja annetaan niille IP-osoite ICTLABin osoiteavaruudesta. Valitaan kytkimet käyttämään todennukseen RADIUS-asetuksia, jolloin ISE hyväksyy sen ja kytkinten välisen

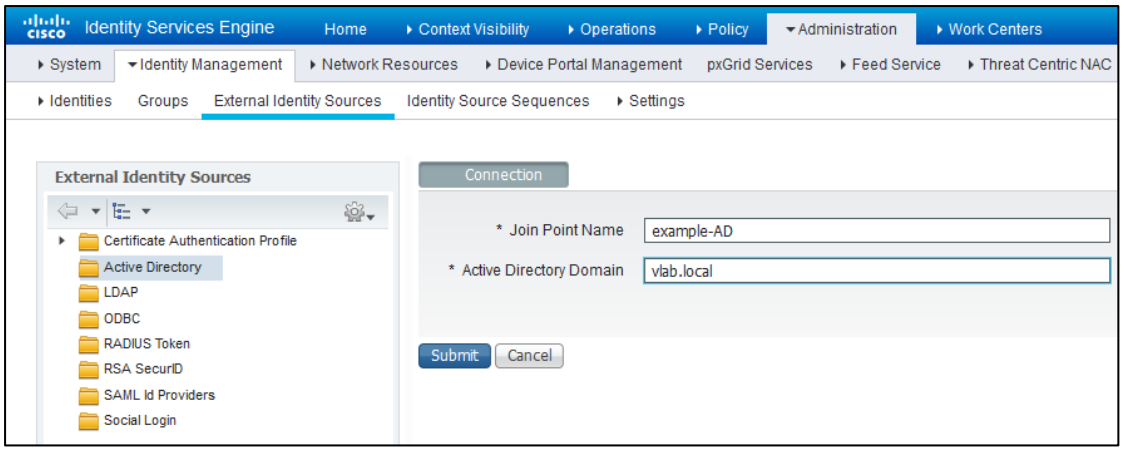
RADIUS-liikenteen. ISE toimii topologiassa todennuspalvelimena ja sen ja autentikaattorikytkinten välinen viestinvaihto 802.1X-todennuksessa tapahtuu RADIUS-protokollan avulla.

Kun kyseinen toimenpide on tehty, voidaan siirtyä ISE:n ja posturen muihin määrityksiin.

7.3.1 Active Directoryn yhdistäminen ISE:een

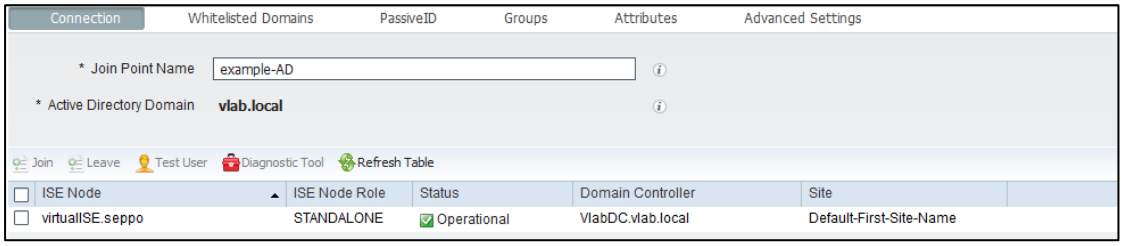
Ennen varsinaisen posturen määrittämistä täytyy ISE integroida eli yhdistää Active Directoryyn eli Windows-palvelimen aktiivihakemistoon käyttäjätunnistusta varten. Vastoin ennakko-oletuksia ISE:ssä tämä toimenpide on tehty hyvin helpoksi, eikä se vaadi kuin muutaman asetuksen määrittämisen ja hiiren klikkauksen.

Määritetään ISE sen graafisesta käyttöliittymästä käyttämään Windows-palvelimen aktiivihakemistoa ulkoisena käyttäjätietokantana. Tämä tapahtuu valitsemalla *Administration* > *Identity Management* > *External Identity Sources* > *Active Directory*. Lisätään haluttu aktiivihakemisto ja toimialue kohdasta *Add* ja annetaan sille kuvaava nimi (Kuva 5).



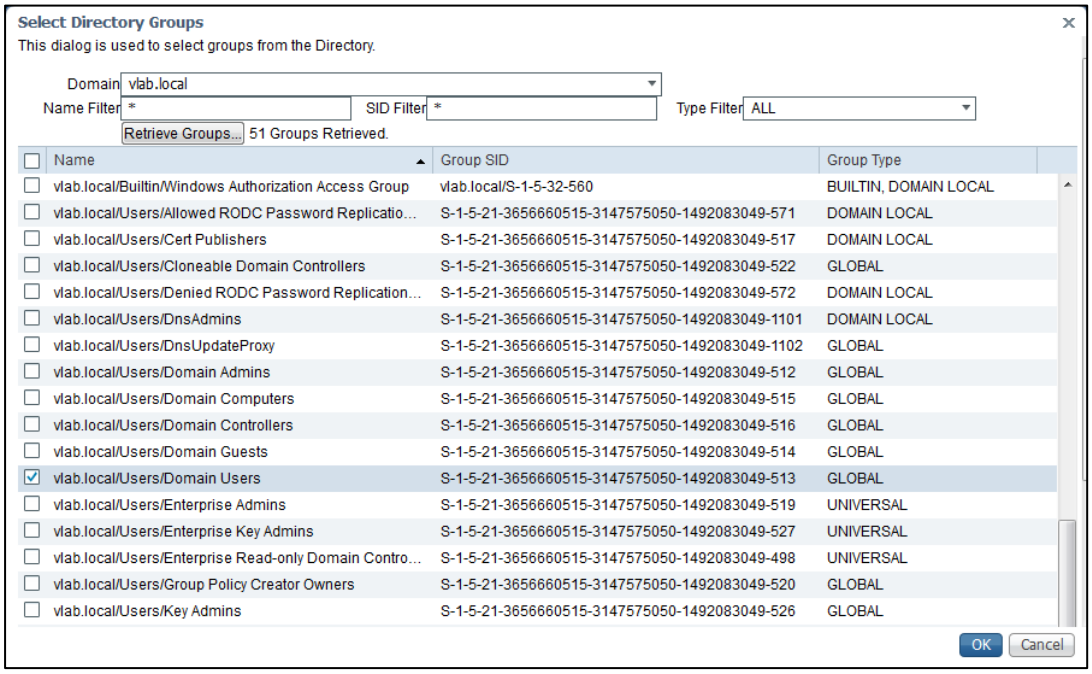
Kuva 5. Liitettävän aktiivihakemiston ja toimialueen (domain) lisääminen

Seuraavaksi ISE kysyy käyttäjätunnuksia AD-ympäristön Domain Admin -käyttäjältä toimenpiteen vahvistamiseksi. Syötetään kyseiset tunnukset ja painetaan *Ok*. Varsinainen aktiivihakemiston liittäminen osaksi ISE:ä on tehty (Kuva 6).



Kuva 6. Onnistunut toimialueen lisäys

Kun varsinainen aktiivihakemisto ja haluttu toimialue on liitetty osaksi ISE:ä, joudutaan vielä määrittämään toimialueen käyttäjäryhmä, jotta sitä voidaan käyttää parametrina valtuutuskäytäntöjen tekemisessä (Cisco 2015). Painetaan *Groups*-välilehti > *Add* > *Select Groups From Directory*, jonka jälkeen valitaan listalta haluttu toimialueen käyttäjäryhmä, tässä tapauksessa kaikki vlab.local-toimialueen käyttäjät (Kuva 7).



Kuva 7. Käyttäjäryhmän lisäys ISE:ssä

7.3.2 Resurssien jako päätelaitteille (Client Provisioning)

Client Provisioning -käytännöillä voidaan työasemille jakaa välttämättömiä ohjelmistoresursseja verkon sisäiseltä palvelimelta verkkoon kirjautumisen yhteydessä. Cisco ISE:een voi luoda erilaisia resurssienjakokäytäntöjä ja -sääntöjä, muun muassa käyttöjärjestelmien tai tiettyjen käyttäjäryhmien mukaan, joilla varmistetaan, että luvallinen käyttäjä saa sisään kirjautuessaan tarvitta-

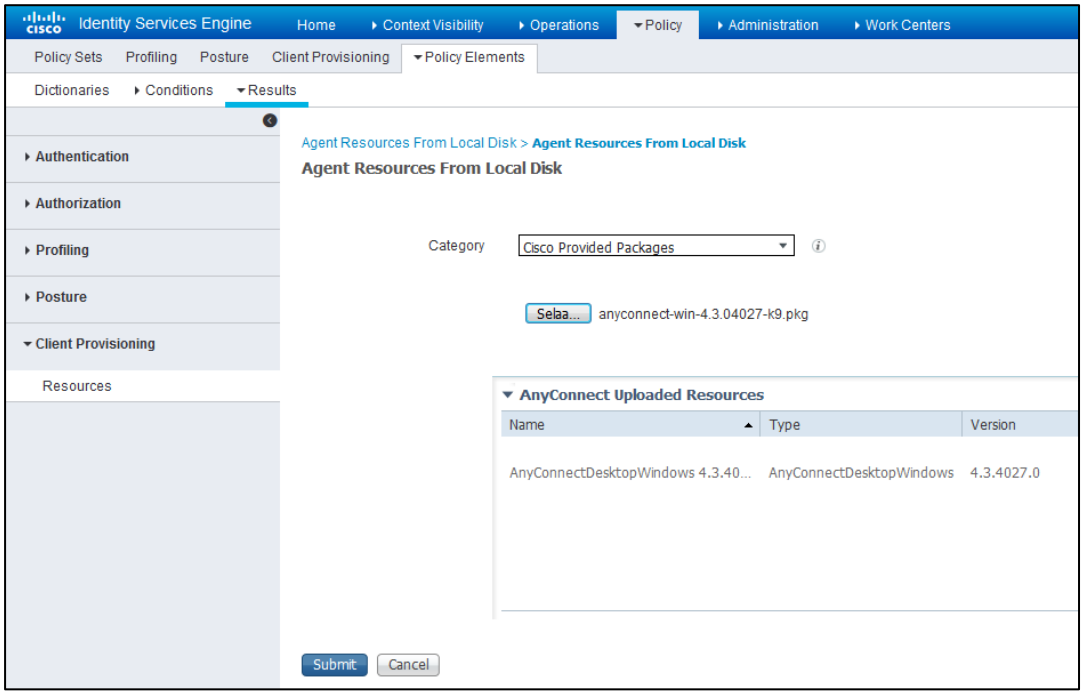
vien ohjelmien asennustiedostot posture-tarkistuksen suorittamiseksi. Posturen käyttöönotossa tällainen välttämätön resurssi on posture agent -ohjelma, jolla itse turvallisuustarkistus suoritetaan.

Cisco ISE -ympäristössä voidaan käytäntöjä hyödyntää myös puutteellisten työasemien ”korjaamisessa” esimerkiksi virustorjuntaohjelmiston tai muiden välttämättömien ohjelmistojen asennustiedostojen jakamisessa. Resurssienjako helpottaa huomattavasti porttitodennuksen ja posture-prosessin sujuvuutta, sillä sen avulla työasema voi muutamalla hiiren klikkauksella suorittaa kaikki tarvittavat asennustoimenpiteet, eikä esimerkiksi ulkoista internet-yhteyttä tarvita.

Ennen varsinaisten Client Provisioning -käytäntöjen määrittämistä, täytyy itse jaettavien ohjelmistoresurssien sijaita ISE-palvelimella. Sen vuoksi ensimmäinen tehtävä asia on ladata kyseiset ohjelmat palvelimelle. Asennettavat resurssit ovat työssä posture-agenttina toimivan AnyConnect Secure Mobility Clientin asennustiedosto, sen vaatima Compliance-moduuli, ISE:ssä luotu posture-profiili sekä erillisellä Network Access Manager -editorilla luotu verkkoprofiili.

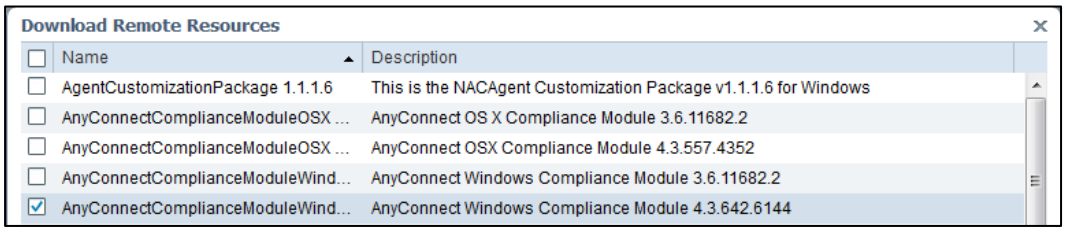
Compliance-moduuli on Ciscon toimittama oleellinen osa AnyConnectia, joka sisältää tiedot eri valmistajien tuotteista ja ohjelmistoista mukaan lukien niiden nimi- ja versiotiedot. Se on ikään kuin ohjelmakirjasto, joka mahdollistaa työaseman posture-tilan arvioimisen ja määrittämisen esimerkiksi sille asennettujen ohjelmien ja tiedostojen perusteella. On tärkeää, että toteutuksessa käytetään Compliance-moduulin uusinta versiota ja se päivitetään tarvittaessa, jotta tiedot valmistajista ja tuoteversioista pysyvät ajan tasalla. (Cisco Identity Services Engine Administrator Guide, Release 2.2 2019.)

ISE:n graafisesta käyttöliittymästä valitaan *Policy > Policy Elements > Results*, jonka jälkeen laajennetaan *Client Provisioning* -kohtaa ja valitaan *Results.* AnyConnectin asennustiedostot on etukäteen ladattu Ciscon omilta sivuilta ja ne löytyvät käytössä olevan työaseman paikalliselta levyltä. Painetaan siis *Add > Agent Resources from Local Disk* ja valitaan kategoriaksi *Cisco Provided Packages*. Levyltä valitaan AnyConnectin asennustiedosto (kuva 8).



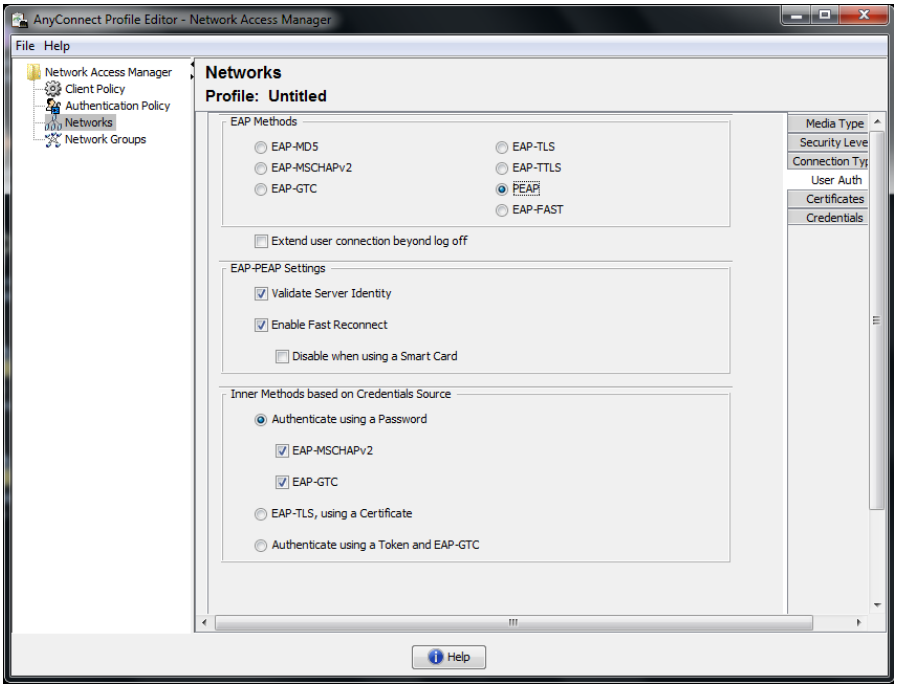
Kuva 8. AnyConnectin asennustiedoston lataaminen palvelimelle

Compliance-moduulin saa ladattua suoraan ISE:n kautta internetin välityksellä Ciscon omilta verkkosivuilta samalla periaatteella painamalla *Add* > *Agent Resources from Cisco site* ja valitsemalla avautuvasta valikosta kyseisen moduulin uusimman version (kuva 9):



Kuva 9. Compliance-moduulin lataaminen palvelimelle

Tämän jälkeen tarvitsee vielä luoda erilliset verkko- ja posture-profiilit, joilla määritetään verkkoon yhdistämisen tapa ja todennusmenetelmä sekä posturen asetukset. NAM- eli verkkoprofiili luodaan Ciscon omalla Network Access Manager -profiilieditorilla, jossa määritetään verkkoon yhdistämisen tavaksi langallinen verkko eli wired sekä todennustavaksi 802.1X ja PEAP-MSCHAPv2 (kuva 10):



Kuva 10. NAM-profiilin luominen editorilla (Network Access Manager Profile)

Profiilissa voidaan myös määrittää, kysyykö AnyConnect Windowsiin kirjautumisen jälkeen vielä erikseen käyttäjätunnuksia, vai käytetäänkö kertakirjautumista eli single sign-on -menetelmää, jolloin 802.1X-todennuksen suorittamiseen riittää pelkkä Windowsin sisäänkirjautuminen.

NAM-profiili täytyy luoda työasemalla, jolle on asennettuna Network Access Manager -editori ja se täytyy sen jälkeen tallentaa .xml-muodossa ja tuoda ISE:n resurssihakemistoon (Resources). Tämä tapahtuu valitsemalla Resources-valikossa *Add* > *Agent Resources from local disk*. Paketin kategoriaksi valitaan *Customer Created Packages* ja tyypiksi *AnyConnect Profile*, jonka jälkeen nimetään se kuvaavasti. Tämän jälkeen *Browse*-valintaa painamalla valitaan kyseinen profiilitiedosto ja tuodaan se ISE:een painamalla *Submit.*

Posture-profiili (kuva 11) sen sijaan voidaan luoda suoraan ISE:ssä *Resources*-valikossa valitsemalla *Add* > *AnyConnect Posture Profile.* Profiilissa määritetään muun muassa se, miten posture-agentti eli AnyConnect-ohjelma löytää ISE-palvelimen. Jättämällä kohdan *Discovery host* tyhjäksi agentti etsii palvelimen automaattisesti ja lisäämällä kohtaan * *Server name rules* kohtaan asteriskimerkin *, agenttiohjelma ottaa yhteyden kaikkiin havaitsemiinsa palvelimiin.

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Discovery host			The server that the agent should connect to
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com

Kuva 11. Posture-profiilin luominen ja muokkaus (Discovery host ja * Server name rules)

Profiilissa voidaan muokata myös työasemien korjausaikaa kohdassa *Remediation timer* (kuva 12). Korjausaika määrittää sen, missä ajassa työasemien tulee asentaa tarvittavat korjaukset ennen kuin istunto päättyy. Tässä kohtaa muutettiin aika kolmeksi tunniksi eli 180 minuutiksi, koska puolittain virtuaalilaboratoriossa toimiva lähiverkko on hidas, ja esimerkiksi Windows-päivitysten lataus verkon läpi kestää melko kauan. Mikäli työasema ei korjausajan päättymiseen mennessä ole saanut asennettua tarvittavia korjauksia, määrittelee ISE työaseman vaatimusten vastaiseksi (non-compliant), jolloin posturen jälkeen suoritettavassa 802.1X-uudelleentodennuksessa ISE välittää kytkimelle RADIUS-Access Reject -viestin ja liityntäportti jää unauthorized-tilaan.

ISE Posture Agent Profile Settings > **New Profile**

* Name: AC_Posture
Description:

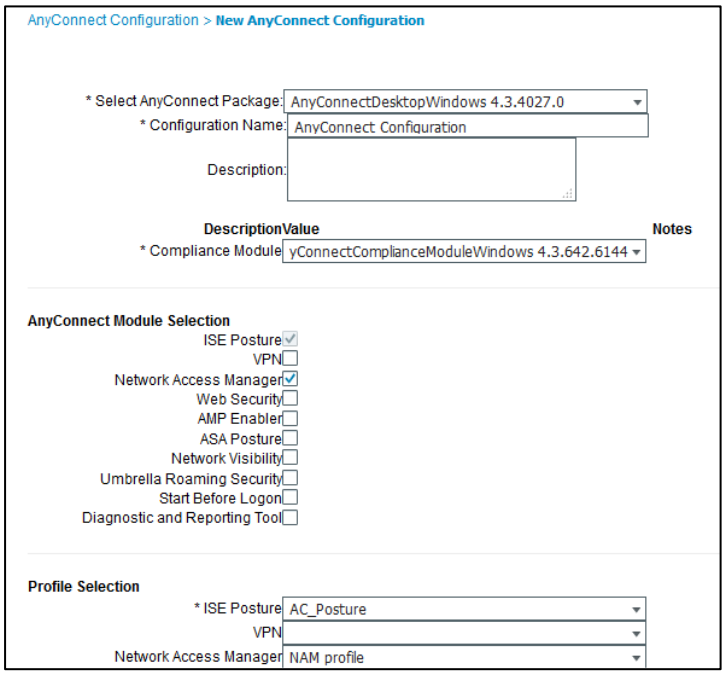
Agent Behavior

Parameter	Value	Notes	Description
Enable debug log	No		Enables the debug log on the agent
Operate on non-802.1X wireless	No		Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	OSX: N/A	Enables signature checking of executables before the agent will run them.
Log file size	5 MB		The maximum agent log file size
Remediation timer	180 mins	The default is empty which means use the global setting. The default of global setting is 4.	The time the user has for remediation before they will be tagged as non-compliant

Kuva 12. Posture-profiilin luominen ja muokkaus (Remediation timer)

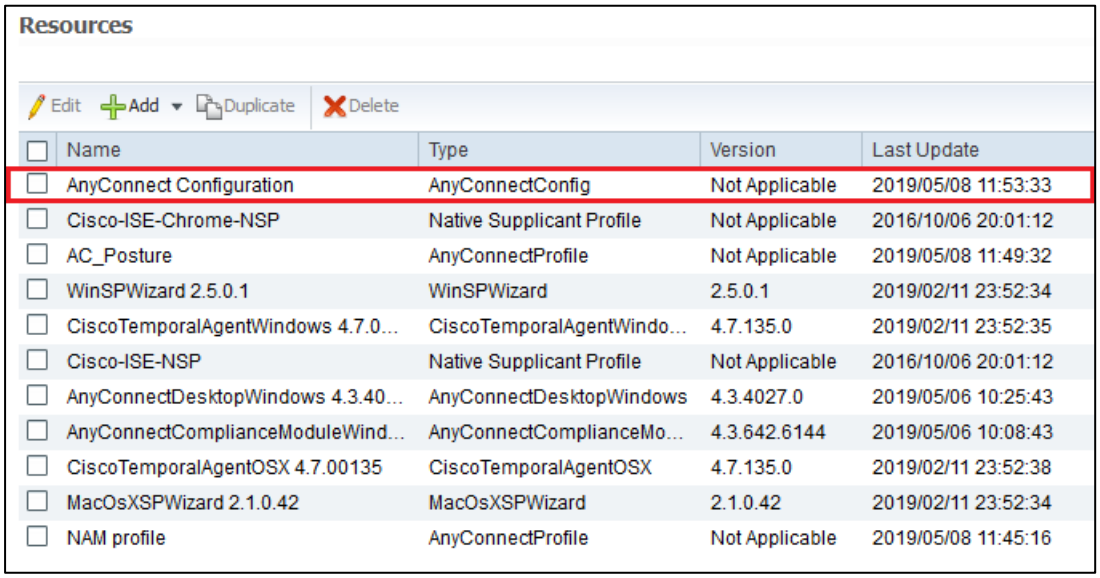
Kun tarvittavat kentät on muokattu, painetaan lopuksi *Submit,* jolloin profiili tallentuu ISE:n resursseihin.

Lopuksi yhdistetään kaikki ISE:n resursseista löytyvät AnyConnectin osat yksittäiseksi AnyConnect Configuration -paketiksi. Tämä tapahtuu painamalla *Add > AnyConnect Configuration,* jonka jälkeen valitaan AnyConnectin asennustiedosto, Compliance-moduuli sekä NAM- ja Posture-profiilit (kuva 13).



Kuva 13. AnyConnect Configuration -paketin luominen

Yksittäisen määrityspaketin avulla asiakaslaite saa sekä AnyConnect-ohjelman asennuksen, että siihen liitettävät moduulit ja määritykset yhdellä kertaa. AnyConnect Configuration -paketti löytyy nyt siis ISE:n omasta resurssihakemistosta, kuten kuvasta 14 ilmenee:

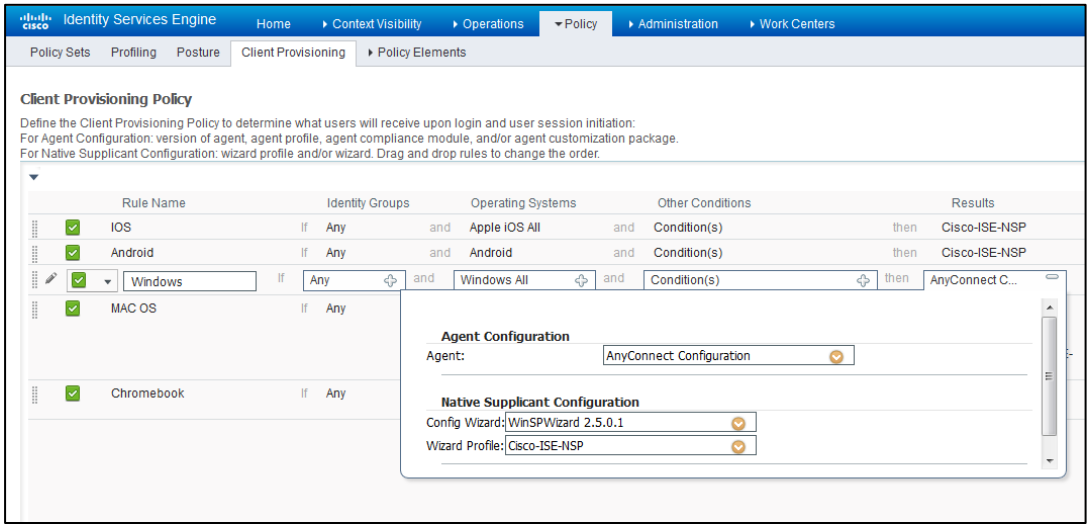


Kuva 14. Cisco ISE:n resurssihakemisto (Resources)

Nyt kun varsinaiset posture-agentin resurssit löytyvät palvelimelta, täytyy kyseiset resurssit vielä jakaa onnistuneen käyttäjätodennuksen tehneille työase-

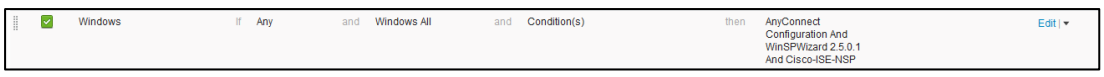
mille verkkoon liittymisen yhteydessä. Tämä tapahtuu resurssienjakokäytännöillä (Client Provisioning Policy), joiden luomiseen siirrytään seuraavaksi. Resurssienjakokäytäntöjen luominen tapahtuu Cisco ISE:ssä kohdasta *Policy* > *Client Provisioning*. ISE:een on jo valmiina luotu Windows-koneille tarkoitettu resurssienjakokäytäntö, jota voidaan muokata omiin tarkoituksiin sopivaksi.

Muokataan sääntöä niin, että Windows-koneet saavat verkkoon yhdistäessään ladattavakseen AnyConnect Configuration -paketin. Vaihdetaan siis säännön *Results*-kenttään kyseinen paketti, mutta pidetään muut kentät ennallaan (kuva 15). Vahvistetaan muokkaamiset painamalla ISE:n alareunasta *Save*.



Kuva 15. Resurssienjakokäytännön muokkaaminen

Sääntöön voisi myös halutessaan määritellä tietyn aktiivihakemiston käyttäjäryhmän, jolloin se koskisi vain kyseisiä käyttäjiä, mutta mahdollisten ongelmien välttämiseksi testivaiheessa määritetään sääntö yleispätevänä koskemaan kaikkia Windows-työasemia (kuva 16).



Kuva 16. Windows-työasemien resurssienjakokäytäntö

7.3.3 Valtuutuskäytäntöjen luominen (Authorization Policy)

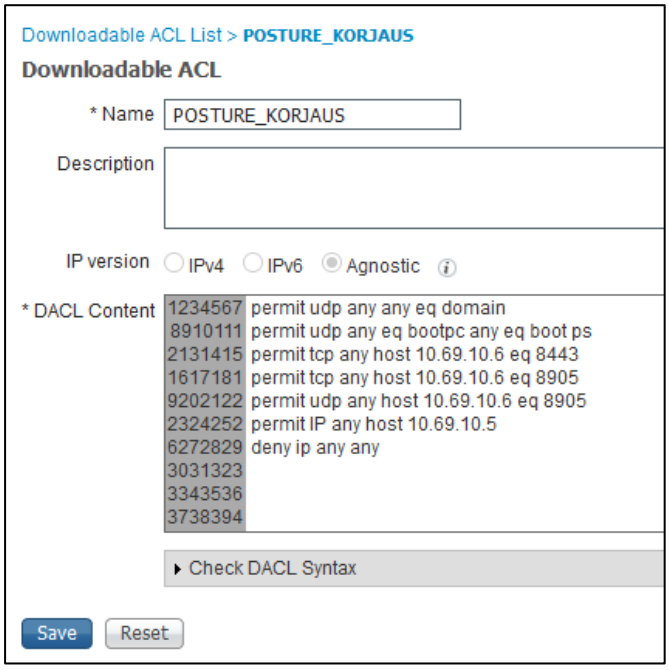
Resurssienjakokäytäntöjen luomisen jälkeen on aika siirtyä luomaan RADIUS-palvelimen, eli tässä tapauksessa ISE:n valtuutuskäytäntöjä, joilla määritetään

porttitodennuksen ja posturen jälkeen käyttäjän ja työaseman verkkoon pääsyn taso. Tiettyjen kriteerien, kuten käyttäjäryhmän tai posture-tilan perusteella voidaan ISE:n avulla verkon työasemien pääsyä verkon resursseihin säädellä tai rajoittaa. Tässä työssä määritetään valtuutuskäytännöt niin, että ne käyttäjät, joiden työasemat eivät täytä verkon vaatimuksia, asetetaan karanteeniin. Tähän kategoriaan kuuluvat siis kaikki posture-tarkistuksessa Non-compliant- ja Unknown-statuksen saavat laitteet. Käytännössä tämä tarkoittaa sitä, että niiden pääsy verkkoon on rajattu, ja ne saavat yhteyden ainoastaan resurssienjako- ja korjauspalveluihin. Sen sijaan Compliant-tilan saavat työasemat saavat normaalin pääsyn verkkoon ja internetiin.

Luodaan valtuutuskäytännöt sekä resurssienjaolle että posturelle. Jotta käyttäjät, joilla ei ole esiasennettuna AnyConnect Mobile Security Client -ohjelmaa, voisivat ladata ja asentaa sen työasemalleen, täytyy heidät verkkoselaimen avatessaan uudelleenohjata ISE:n omaan resurssienjakoportaaliin (Client Provisioning Portal). Kyseinen uudelleenohjaus tapahtuu sille tarkoitetulla valtuutuskäytännöllä sekä verkon aktiivilaitteeseen (Cisco Catalyst 2960G -kytkin) luodulla pääsylistalla (Access Control List).

Ensimmäisenä luodaan ISE:ssä authorization profile eli valtuutusprofiili, joka lopuksi liitetään itse valtuutuskäytäntöön. Valtuutusprofiilin tarkoituksena on rajata asiakaslaitteen pääsyä verkkoon sekä samalla mahdollistaa sen uudelleenohjaus resurssienjakoportaaliin. Liikenteen rajoittaminen vain resurssienjako- ja korjauspalveluihin tapahtuu ladattavalla pääsylistalla (dACL), jonka ISE välittää verkkokytkimelle 802.1X-istunnon ollessa käynnissä.

ISE:stä valitaan *Policy* > *Policy Elements* > *Results* ja kohdasta *Authorization* valitaan *Downloadable ACLs*, josta päästään luomaan ladattava pääsylista. Painetaan *Add*, annetaan kuvaava nimi dACL:lle ja syötetään siihen seuraavat arvot (kuva 17):

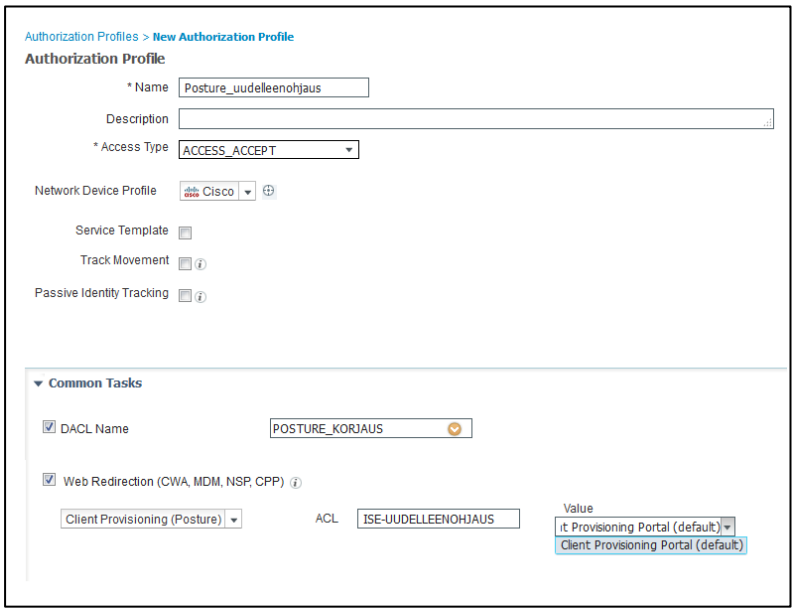


Kuva 17. dACL:n luominen

Kyseisen ladattavan pääsylistan tarkoitus on sallia verkon toiminnalle oleellinen liikenne, kuten DNS, DHCP sekä posture-agentin kommunikointi ISE:n kanssa verkkokytkimen läpi, ja estää kaikki muu liikenne. Erikseen sallitaan myös asiakkaan liikenne Windows-palvelimelle (IP-osoite 10.69.10.5), joka työssä toimii WSUS-palvelimena korjaamaan Windowsin kriittiset tietoturvapäivitykset. Kun ISE alustavassa 802.1X-todennuksessa välittää kytkimelle asiakkaan sen hetkistä posture-tilaa (Unknown) vastaavat valtuutusattribuutit, lisää kytkin dACL:n voimassa olevaan todennusistuntoon, jolloin kaiken muun liikenteen paitsi pääsylistassa erikseen sallitun läpimeno kytkimessä estetään. Pääsylista tulee olemaan käytössä niin kauan, kunnes asiakaslaite on tehnyt työasemalleen vaaditut korjaustoimenpiteet ja saanut tilakseen Compliant, jolloin ISE välittää kytkimen portille Change of Authorization -pyynnön ja tapahtuu 802.1X-uudelleentodennus.

Tämän jälkeen luodaan valtuutusprofiili (kuva 18), johon kyseinen dACL liitetään. Valtuutusprofiiliin määritetään myös https-uudelleenohjaukseen liittyvät parametrit. Valtuutusprofiili luodaan kohdasta *Policy* > *Policy Elements* > *Results* > *Authorization* > *Authorization Profiles*. Profiilin nimeämisen lisäksi liitetään siihen juuri luotu dACL sekä määritetään kohdasta *Web Redirection* uudelleenohjauksen lopputulemaksi resurssienjakoportaali eli *Client Provisioning*

Portal. Nimetään myös uudelleenohjaukseen tarkoitettu pääsylista *ISE-UUDELLEENOHJAUS*, jotta ISE tietää kertoa kytkimelle mitä pääsylistaa sen tulee käyttää liikenteen uudelleenohjauksessa resurssienjakoportaaliin. Huom. kyseisen samannimisen pääsylistan täytyy löytyä konfiguroituna verkkokytkimeltä.



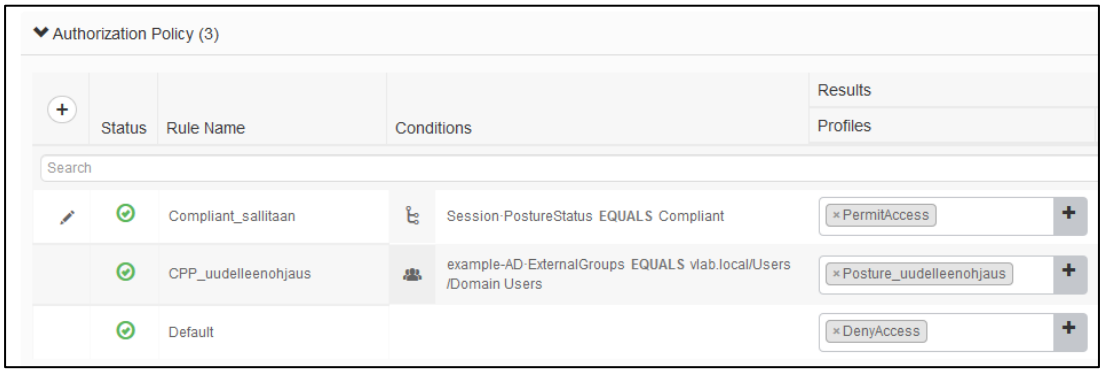
Kuva 18. Valtuutusprofiilin (Authorization Profile) luonti

ISE välittää määritetylle RADIUS-asiakkaalle eli kytkimelle cisco-av-pairs -attribuutit (kuva 19), joiden tehtävänä on ohjeistaa kytkintä käyttämään juuri nimettyä pääsylistaa uudelleenohjaukseen sekä mahdollistaa uudelleenohjauksen tapahtuminen kyseenomaiseen URL-osoitteeseen. Kyseinen URL-osoite on istuntokohtainen, ja voimassa vain kyseisen porttitodennuksen ajan.

Kuva 19. Cisco-av-pair -attribuutit ja uudelleenohjaus URL

Viimeisenä vaiheena luodaan varsinainen valtuutuskäytäntö kohdasta *Policy* > *Authorization*. Luodaan kaksi uutta sääntöä, joiden perusteella posture-tarkistuksen suorittaneiden ja Compliant-tilan saaneiden työasemien pääsy verkkoon sallitaan suoraan ja oletuksena kaikki aktiivihakemiston toimialueen käyt-

täjät uudelleenohjataan resurssienjakoportaaliin. Tämä saadaan aikaan liittämällä sääntöön aiemmin luotu valtuutusprofiili. Valitaan sääntö koskemaan toimialueen vlab.local kaikkia käyttäjiä, jotka lisättiin erikseen ehdoksi työn alussa. Valtuutuskäytäntöjen (kuva 20) prosessointijärjestys ISE:ssä on ylhäältä alaspäin, joten tärkeysjärjestyksessään merkittävimmän säännön tulee olla ensimmäisenä.



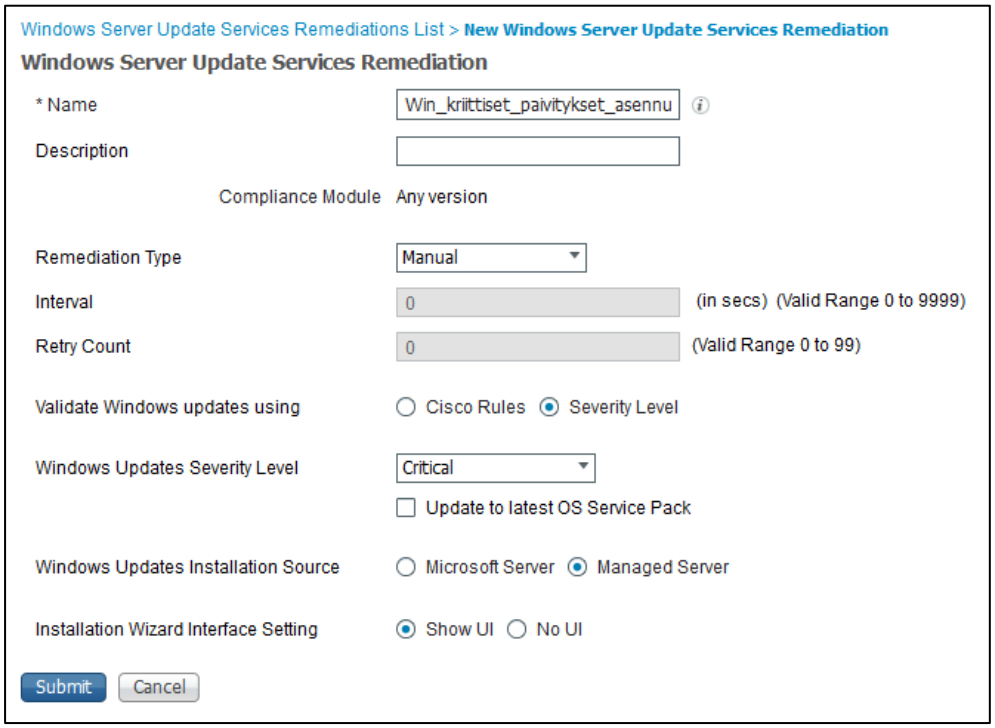
Kuva 20. Valtuutuskäytöntöjen luominen

7.3.4 Posture-käytäntöjen luominen (Posture Policy)

Kun sekä resurssienjako- että valtuutuskäytännöt on luotu, siirrytään posturen kannalta oleellisimpaan vaiheeseen eli posture-käytännön tekoon. Nämä käytännöt lopullisesti määrittävät työasemalta vaadittavat asiat ja niihin voidaan samalla sitoa erinäisiä korjaustoimenpiteitä. Jokaisella posture-vaatimuksella voi olla sille erillinen vaadittava korjaustoimenpide, jonka työasema voi suorittaa tarkistuksen yhteydessä.

Tässä työssä testataan vain posturen perustoiminnallisuutta ja posture-vaatimukseksi asetetaan vain Windows-koneiden kriittisten tietoturvapäivitysten asennus ja ajantasaisuus. Laajamittaisemmassa posturen käyttöönotossa vaatimuksia voisi määrittää useampia erilaisia ja niiden tasoja säädellä niin, että osa vaatimuksista olisi pakollisia ja osa suositeltavia. Ensimmäinen vaihe posture-käytännön luomisessa on määrittää siihen liitettävä korjaustoimenpide, jonka jälkeen luodaan posture-ehdot ja niihin liittyvät vaatimukset. Sääntöihin voidaan myös eritellä tietyn käyttöjärjestelmän työasemat sekä käyttäjäryhmät kuten valtuutuskäytäntöjen kohdalla.

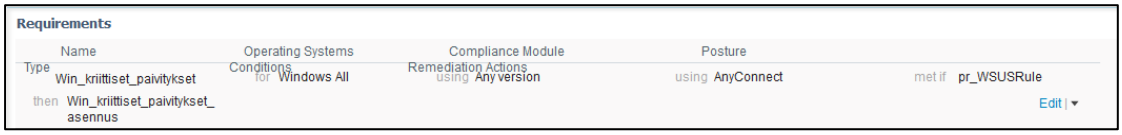
Määritetään korjaustoimenpide, joka tarkastaa Windows-koneen kriittiset päivitykset, ja niiden puuttuessa asentaa ne työasemalle. Tämä tehdään ISE:ssä kohdasta *Policy* > *Policy Elements* > *Results*, josta laajennetaan kohtaa *Posture.* Sen sisältä valitaan *Remediation Actions* > *Windows Server Update Remediation* ja lisätään uusi korjaustoimenpide painamalla *Add.* Määritetään korjaus seuraavilla arvoilla (kuva 21):



Kuva 21. WSUS-korjaustoimenpiteen luominen

Vaadittavien päivitysten tärkeys asetetaan kohdasta *Windows Updates Severity Level* ja valitaan *Critical*. Kyseisestä ikkunasta valitaan myös palvelin, josta työasema lataa päivitykset itselleen. Koska topologiassa on käytössä sisäinen Windows-palvelin, jolla on yhteys internetiin ja jota käytetään päivitysten jakamiseen, valitaan *Windows Updates Installation Source* valinnasta *Managed Server.* Huom. tämän tekemiseksi täytyy myös itse työasemat määrittää käyttämään WSUS-palvelinta päivitysten lataamiseen ryhmäkäytännön avulla, mihin palataan myöhemmin.

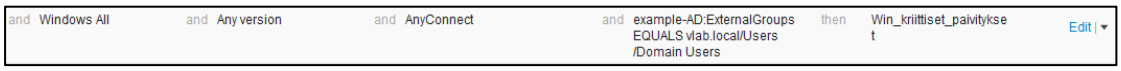
Tämän jälkeen määritetään varsinainen posture-vaatimus (kuva 22), johon liitetään sekä posture-ehto (posture condition) että juuri luotu korjaustoimenpide.



Kuva 22. Posture-vaatimuksen luonti

Määritettyjen ehtojen avulla posture-agentti tarkistaa kyseisen ehdon paikkansapitävyyden ja määrää sen perusteella jatkotoimenpiteet, kuten korjauksen. Ehtoja voi määrittää itse tai käyttää Ciscon omia ennalta määritettyjä ehtoja, kuten tässä esimerkissä. Vaatimuksessa käytetään *pr_WSUSRule*-ehtoa, joka löytyy kohdasta *Cisco Defined Condition > Regular Compound Condition. pr_WSUSRule* on ns. dummy-ehto, joka toimii vaatimuksen määrityksessä vain ”täytteenä”. Varsinainen Windows-päivitysten validointi tehdään niiden vaativuustason (severity level) eikä Cisco-sääntöjen perusteella, kuten korjaustoimenpiteen kohdalla aiemmin määritettiin. Kyseisen toimenpiteen tekee posture-agentti.

Lopuksi liitetään kaikki aiemmin luotu yhteen posture-käytännöksi Windows-työasemille (kuva 23) valitsemalla *Policy > Posture.* Määritetään käytäntö sovellettavaksi kaikkiin vlab.local-toimialueen käyttäjiin, joilla on työasemallaan asennettuna AnyConnect-ohjelma.



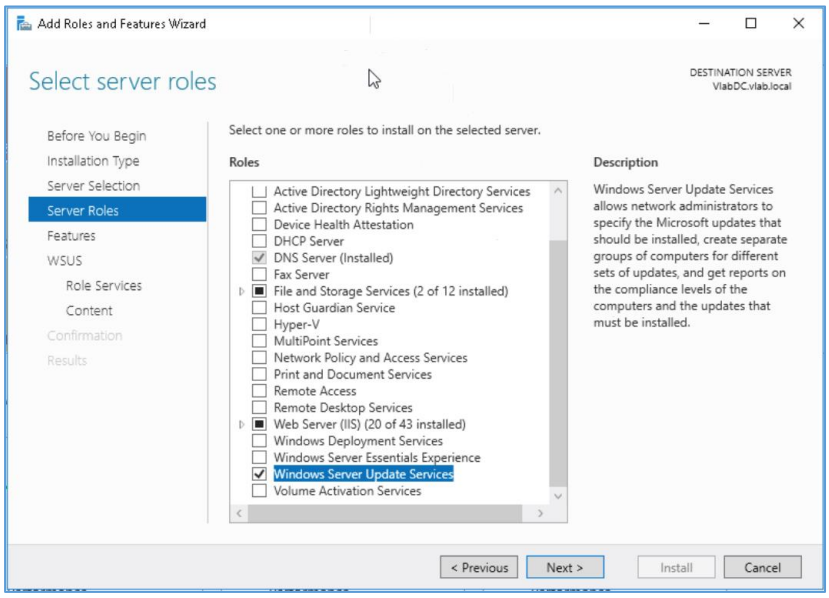
Kuva 23. Posture-käytäntö

7.3.5 WSUS-palvelinrooli ja Windowsin kriittiset päivitykset

Topologiassa käytetään sisäistä Windows-palvelinta kriittisten päivitysten jakamiseen. Kyseisen tehtävän hoitaa WSUS-palvelinrooli (Windows Server Update Services), jonka asennukseen ja määritykseen siirrytään seuraavaksi. WSUS-palvelimen tarkoituksena on, että se toimii sisäverkon Windows Update -tietokantana, eli päivitykset verkon koneille ladataan sen kautta eikä internetistä.

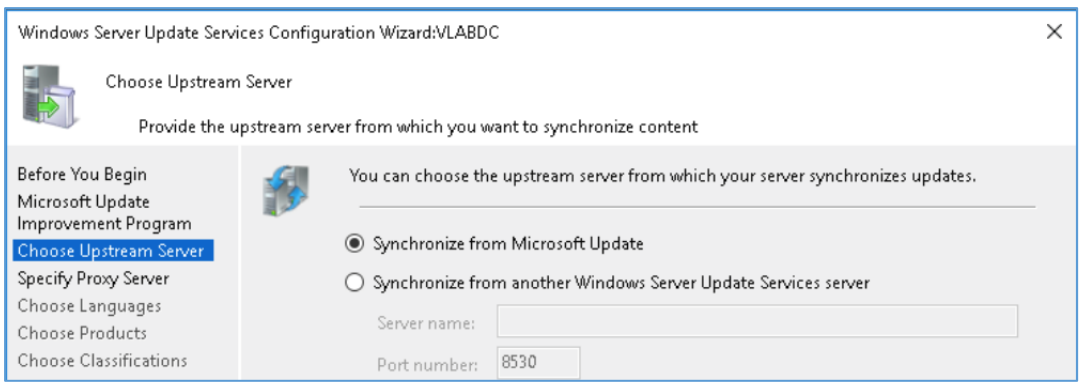
Ensin WSUS täytyy asentaa, kuten mikä tahansa muukin palvelinrooli (kuva 24). Tämä tapahtuu Windows Server 2016 -käyttöjärjestelmässä *Server Man-*

agerissa kohdasta *Add Roles and Features > Role-based or feature based installation*, valitaan kyseinen palvelin, painetaan *Next* ja valitaan *Windows Server Update Services.* Loput asetuksista voidaan jättää oletusarvoihinsa, joten viimeistellään asennus painamalla jäljellä olevissa valikoissa *Next* ja lopuksi painetaan *Install.*



Kuva 24. WSUS-palvelinroolin asennus

WSUS-palvelimeen joudutaan vielä määrittämään asetukset, ennen kuin se on käyttövalmis (kuva 25). Määritys on suhteellisen suoraviivainen ja se voidaan tehdä oletusasetuksilla. Määritysvaiheen päätarkoitus on synkronoida WSUS internetin kautta Microsoftin oman päivityspalvelun eli Microsoft Updaten kanssa. Määrityksessä voidaan myös asettaa palvelin synkronoitumaan uudelleen tietyin väliajoin, jolloin sen tarjoamat päivitykset pysyvät ajan tasalla. Tarvittaessa sille voi määrittää myös erillisen välityspalvelimen (proxy server), mutta sellaista ei tässä työssä ole käytössä.

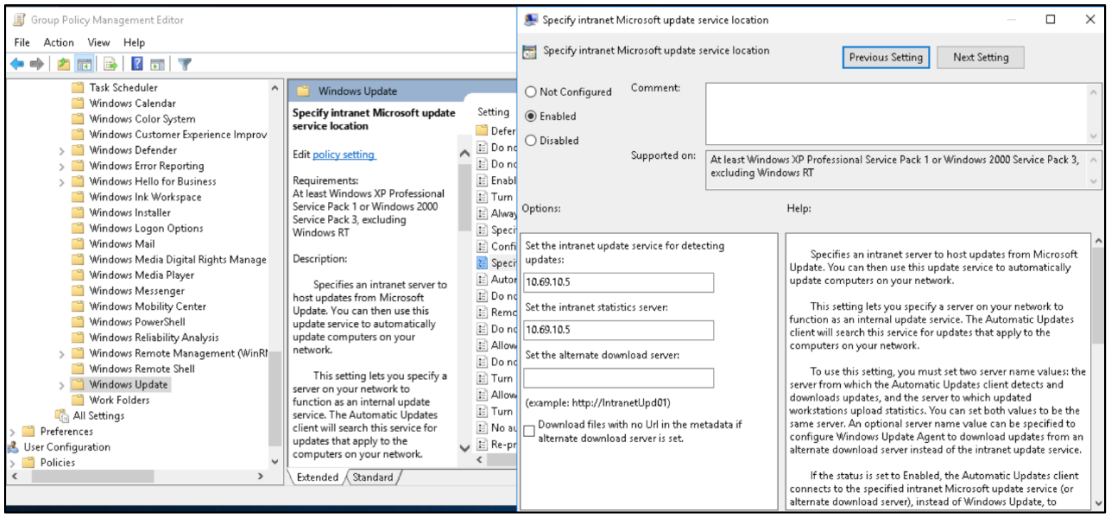


Kuva 25. WSUS-määritysikkuna

Jotta Windows-työasemat voivat ottaa yhteyttä WSUS-palvelimeen ja jotta niille saadaan jaettua sen kautta päivitykset, täytyy ne määrittää käyttämään *Automatic Updates* -palvelua, joka toimii WSUS-palvelimen asiakasohjelmana (client). Suuressa ympäristössä usealla työasemalla tämä on helpointa tehdä ryhmäkäytännön avulla. Palvelun voi työasemilla ottaa käyttöön myös paikallisesti yksitellen, mutta ryhmäkäytäntö helpottaa suuremmassa tuotantoympäristössä kyseistä prosessia merkittävästi.

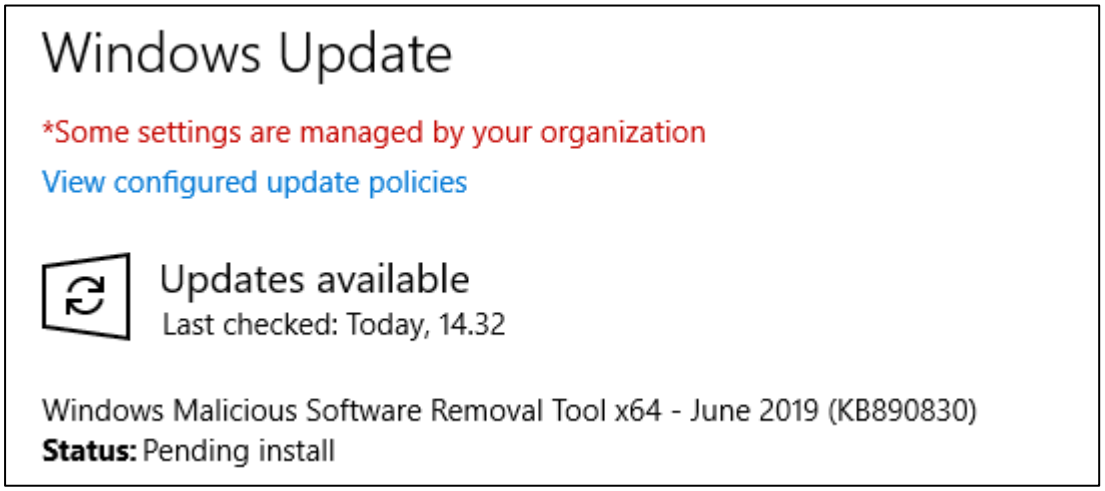
Avataan *Group Policy Management* ja navigoidaan Domains-valikon alta vlab.local-toimialueen kohdalle ja sinne jo valmiiksi luotuun Students-organisaatioyksikköön (organizational unit). Klikataan hiiren oikealla kyseistä OU:ta ja valitaan *Create a GPO in this domain, and Link it here.* Sääntö nimetään asianmukaisesti WSUS policy -nimellä ja siirrytään itse säännön muokkaamiseen. Klikataan hiiren oikealla kyseenomaista sääntöä ja painetaan *Edit*. Laajennetaan avautuvia alavalikkoja kohdasta *Computer Configuration > Policies > Administrative Templates > Windows Components*, josta valitaan kohta *Windows Update*. Avautuvasta oikeanpuoleisesta valikosta etsitään kohta *Configure Automatic Updates*, josta hiiren oikealla painetaan *Edit*. Määritetään palvelu käyttöönotettavaksi valitsemalla *Enabled ja* valitaan tässä tapauksessa ensimmäinen vaihtoehto eli *Notify for download and notify for install,* jolloin työasemille tulee ilmoitus, kun päivityksiä on valmiina ladattavaksi. Lopuksi vahvistetaan tehdyt muutokset painamalla *OK.*

Viimeisimpänä muokataan samaa ryhmäkäytäntöä siten, että se määrää Students-organisaatioyksikön työasemat käyttämään Windows Update -päivitysten lähteenään WSUS-palvelinta. Kohdassa Windows Update avautuvasta sivuvalikosta valitaan tällä kertaa kohta *Specify intranet Microsoft update service location,* josta hiiren oikealla valitaan *Edit*. Otetaan kyseinen ryhmäkäytäntöasetus käyttöön painamalla *Enabled* sekä syötetään vaadittuihin kenttiin WSUS-palvelimen IP-osoite (kuva 26):



Kuva 26. WSUS-ryhmäkäytännön luonti

Kirjaudutaan verkon domain-käyttäjällä työasemalle ja päivitetään sen ryhmäkäytäntöasetukset avaamalla Windowsin komentorivi ja syöttämällä siihen *gpupdate /force*, jolloin juuri luotu ryhmäkäytäntö tulee voimaan. Tarkistetaan vielä työasemalta, että se todella lataa Windows-päivitykset WSUS-palvelimelta avaamalla *Windows Update* ja varmistamalla, että siellä lukee *Some settings are managed by your organization* (kuva 27). Näin saadaan myös varmistus sille, että ryhmäkäytäntö on otettu käyttöön onnistuneesti ja vastaisuudessa Windows-päivitysten jakoa työasemalle hallitaan keskitetysti WSUS-palvelimelta.



Kuva 27. Windows Update –valikko Windows 10 -työasemalla

7.4 Kytkimien määritykset

Viimeinen vaihe työssä on tehdä tarvittavat määritykset verkkokytkimiin, jotka toimivat asiakaslaitteille verkon liityntäpisteinä ja autentikaattoreina 802.1X-todennuksessa. Kytkimet on aiemmin työssä määritetty RADIUS-asiakkaiksi ISE:n hallintapaneelista ja ainoat puuttuvat toimenpiteet ovat luoda niihin uudelleenohjauspääsylista, jolla portteihin tulevan liikenteen uudelleenohjausta resurssienjakoportaaliin säännöstellään, sekä kytkeä varsinainen porttitodennus päälle.

Ensimmäisenä määritetään uudelleenohjauspääsylista valittuihin kytkimiin. Tärkeää on myös muistaa antaa pääsylistalle sama nimi kuin aiemmin ISE:ssä valtuutusprofiilia luodessa luvussa 7.3.3, jolloin kytkin käyttää kyseistä pääsylistaa uudelleenohjaukseen ISE:ltä saatujen valtuutusattribuuttien mukaisesti. Tässä tapauksessa nimetään pääsylista *ISE-UUDELLEENOHJAUS* ja määritetään se kytkimen komentoriviltä seuraavasti:

```
#ip access-list extended ISE-UUDELLEENOHJAUS
    #deny udp any eq bootpc any eq bootps
    #deny udp any any eq domain
    #deny udp any host 10.69.10.6 eq 8905
    #deny tcp any host 10.69.10.6 eq 8905
    #deny tcp any host 10.69.10.6 eq 8443
    #deny ip any host 10.69.10.5
    #permit ip any any
```

Uudelleenohjauspääsylistan tehtävänä on suodattaa sellainen verkon toiminnan kannalta oleellinen liikenne, jota ei ole tarkoitettu uudelleenohjattavaksi, kuten DHCP- ja DNS-liikenne. Kyseisessä pääsylistassa *deny*-komento ei estä liikennettä kokonaan, vaan ainoastaan määrittelee kyseisen liikenteen ei-uudelleenohjattavaksi. Kaikki *permit*-komennolla sallittu liikenne sen sijaan uudelleenohjataan resurssienjakoportaaliin, kuten valtuutusprofiilissa aiemmin määritettiin. Tässä työssä pääsylista on konfiguroitu siten, että DHCP-, DNS-, sekä asiakaslaitteen ja ISE:n välinen liikenne (IP-osoite 10.69.10.6) päästetään normaalisti suoraan kytkimen läpi ilman uudelleenohjausta. Erikseen es-

tetään uudelleenohjaus myös asiakkaan ja Windows-palvelimen väliseltä liikenteeltä, joka esimerkissä on tehty *deny ip any host 10.69.10.5* -ehdolla. Asiakaslaitteen ja palvelimien välisen liikenteen on tapahduttava normaalisti, jotta muun muassa käyttäjä pystytään todentamaan ja päivitykset jakamaan WSUS-palvelimelta.

Deny udp any eq bootpc any eq bootps -komennolla estetään DHCP-liikenteen uudelleenohjaus.

Deny udp any any eq domain -komennolla puolestaan varmistetaan, ettei DNS-liikennettä uudelleenohjata.

Deny udp/tcp any host 10.69.10.6 eq 8905 -komento varmistaa, ettei asiakkaan ja ISE:n välisen udp- ja tcp-liikenne porttiin 8905 uudelleenohjaudu. ISE käyttää tätä porttia muun muassa posture-kommunikaatioon agenttiohjelman kanssa sekä resurssienjaossa.

Deny tcp any host 10.69.10.6 eq 8443 -komento kieltää ISE:een porttiin 8443 päin menevän tcp-liikenteen uudelleenohjaamisen. ISE:n resurssienjakoportaali käyttää porttia 8443, joten siihen suuntaan menevää liikennettä ei uudelleenohjata.

Deny ip any host 10.69.10.5 -komento estää Windows-palvelimelle menevän IP-liikenteen uudelleenohjauksen.

Permit ip any any -komennolla sallitaan kaikki muu IP-liikenne uudelleenohjattavaksi resurssienjakoportaaliin.

Jotta kytkin pystyy katkaisemaan asiakkaan http-pyynnöt ja uudelleenohjaamaan sen resurssienjakoportaaliin alustavan valtuutuskäytännön tullessa voimaan, täytyy kytkin olla määritetty toimimaan http-palvelimena. Tämän saa kytkimessä päälle Global configuration -tilassa komennolla *ip http server*.

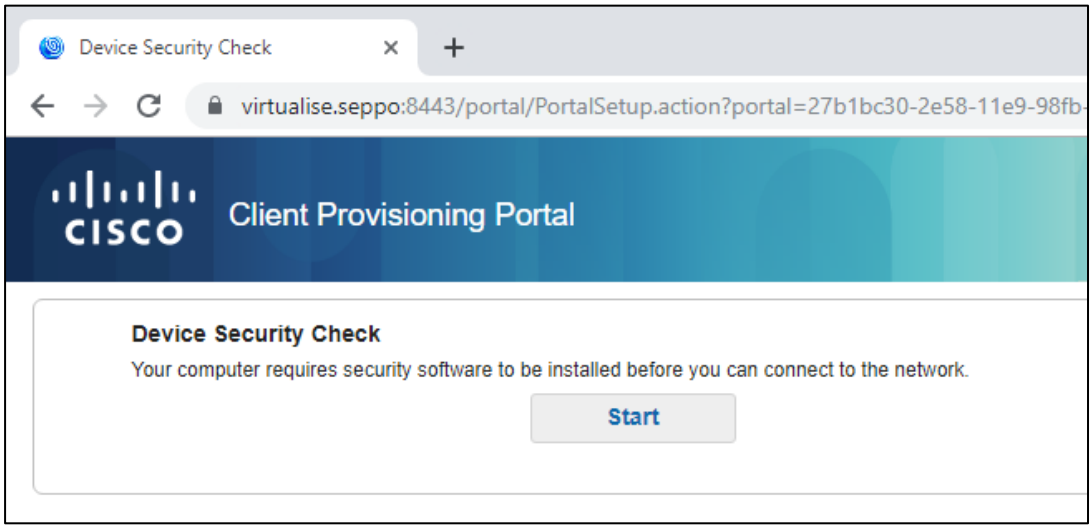
Posturen kannalta kaikki tärkeimmät määritykset on tehty. Viimeisenä vaiheena kytketään 802.1X-todennus päälle kytkimistä. 802.1X-protokollan käyt-

töönottamisen ohjeet Xamkin ICTLAB-ympäristössä on käyty läpi Ville Naumasen opinnäytetyössä *802.1X-porttikohtaisen todennuksen suunnittelu ICT-LAB-ympäristöön* (2018).

7.5 Posturen testaus työasemalla

Testataan posturen toiminta Windows 10 -työasemalla kirjautumalla sisään vlab.local-toimialueen käyttäjällä. Tässä vaiheessa alustavan porttitodennuksen tulisi tapahtua ja kytkimen verkkoporttiin kytketyn työaseman saada rajattu yhteys verkon resursseihin, kuten valtuutuskäytännöissä oli määritetty. Asiakaslaitteella ei ole esiasennettuna posture-agenttia, joten posturen suorittamiseksi sen tulee ladata ja asentaa itselleen sellainen ISE:n resurssihakemistosta.

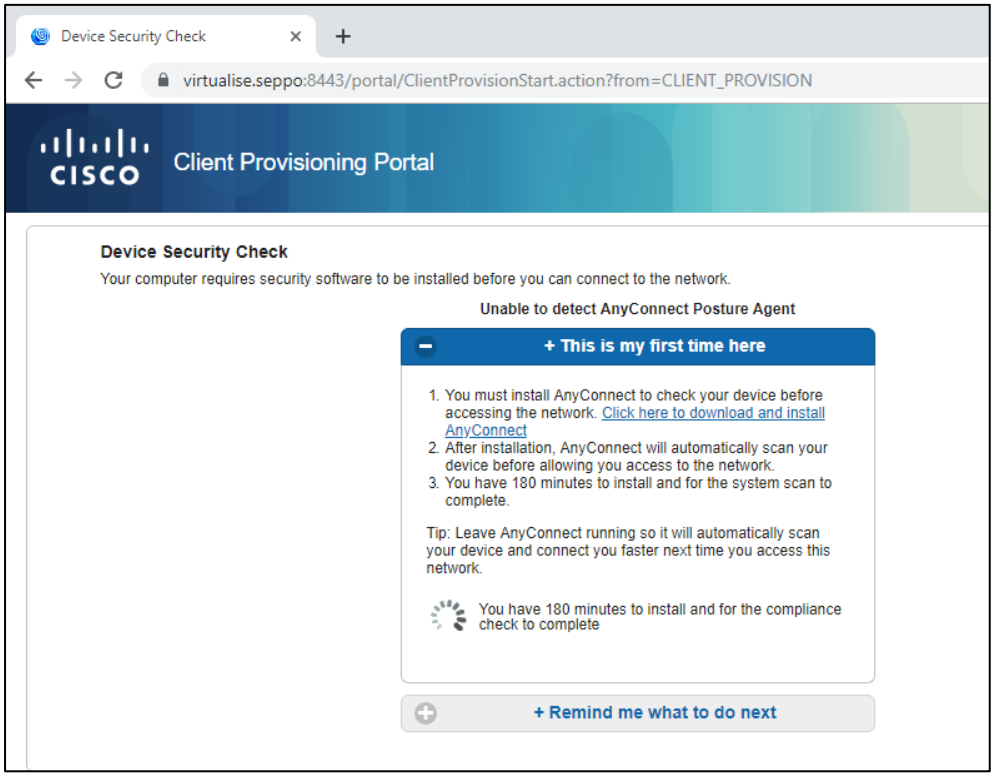
Verkkoselaimen avaamisen ja verkkosivulle navigoimisen yhteydessä tapahtuu uudelleenohjaus resurssienjakoportaaliin valtuutuskäytännön mukaisesti, koska kyseessä on vlab.local-toimialueen käyttäjä ja sen alustava posture-tila on *Unknown* (kuva 28):



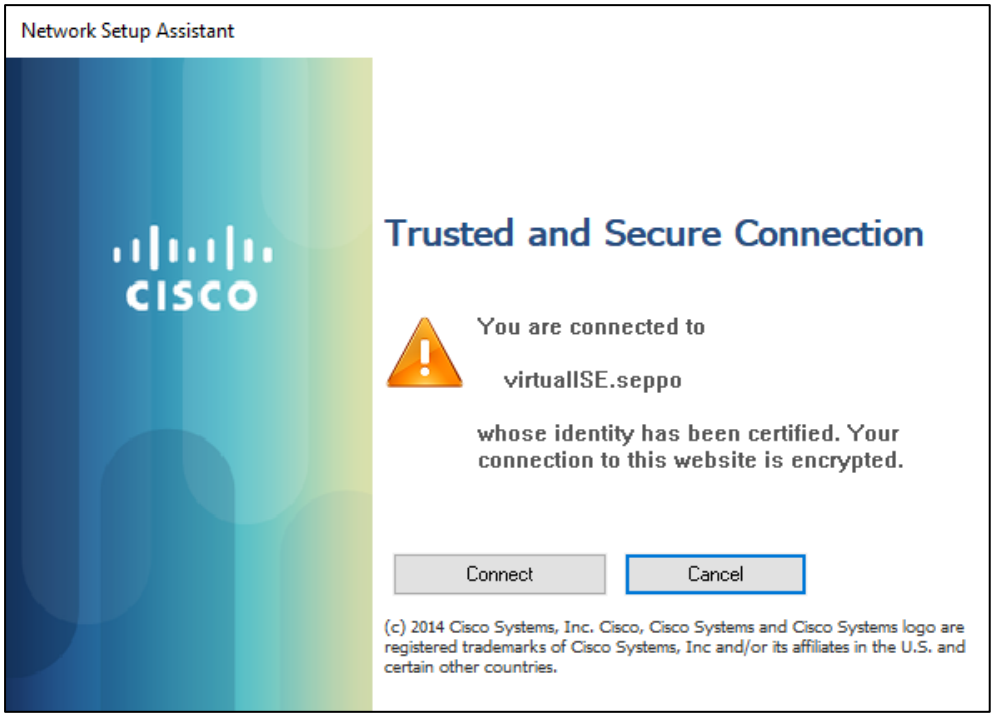
Kuva 28. Resurssienjakoportaali (Client Provisioning Portal)

Sivu vaatii turvallisuustarkistuksen suorittamista ennen verkkoyhteyden sallimista. Aloitetaan se painamalla *Start*, jolloin ISE tarkistaa työaseman agenttiohjelman varalta. Mikäli tarkistus ei havaitse koneella agenttiohjelmaa, tarjoaa portaali Cisco AnyConnect Secure Mobility Client -ohjelman lataamista

(kuva 29) varsinaisen turvallisuustarkistuksen suorittamista varten. Seurataan ohjeita ja asennetaan se työasemalle (kuva 30).



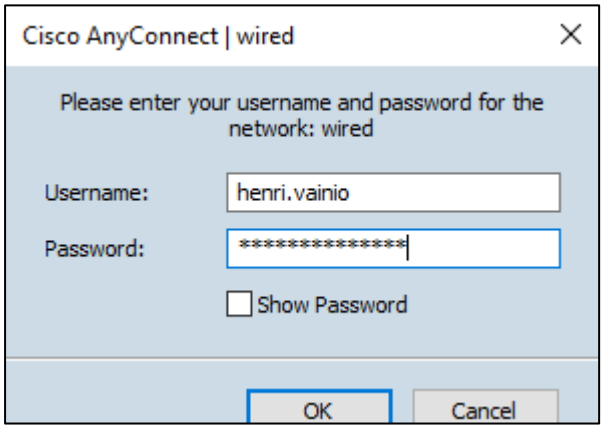
Kuva 29. Posture-agentin havaitseminen työasemalla



Kuva 30. AnyConnectin asennus

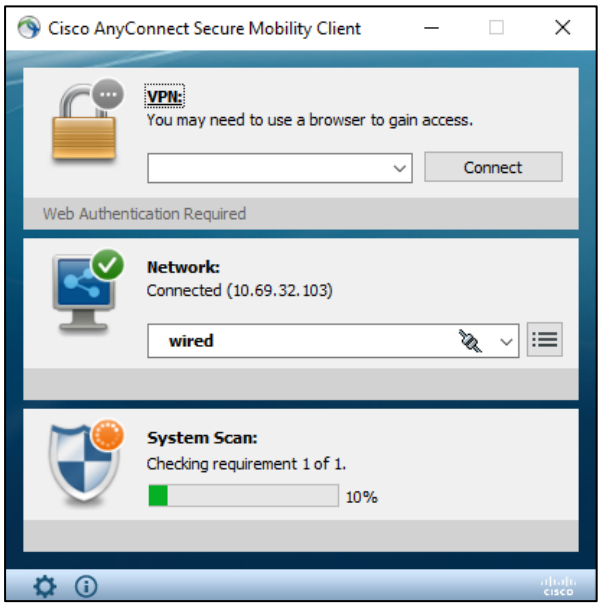
AnyConnect-asiakasohjelma ja kaikki sen tarvitsemat moduulit lataantuvat ja asentuvat työasemalle yhdellä kertaa. Vastaisuudessa AnyConnect hoitaa posturen lisäksi 802.1X-mukaisen asiakaspuolen PEAP-todennuksen, eikä siihen enää tarvita Windowsin omaa sisäänrakennettua supplicant-ohjelmaa.

AnyConnectin asennuksen jälkeen tarvitaan vielä käyttöjärjestelmän uudelleenkäynnistys, jonka jälkeen ponnahtaa työpöydälle AnyConnect-kirjautumisikkuna, jossa pyydetään käyttäjältä kirjautumistunnuksia porttitodennusta varten (kuva 31).



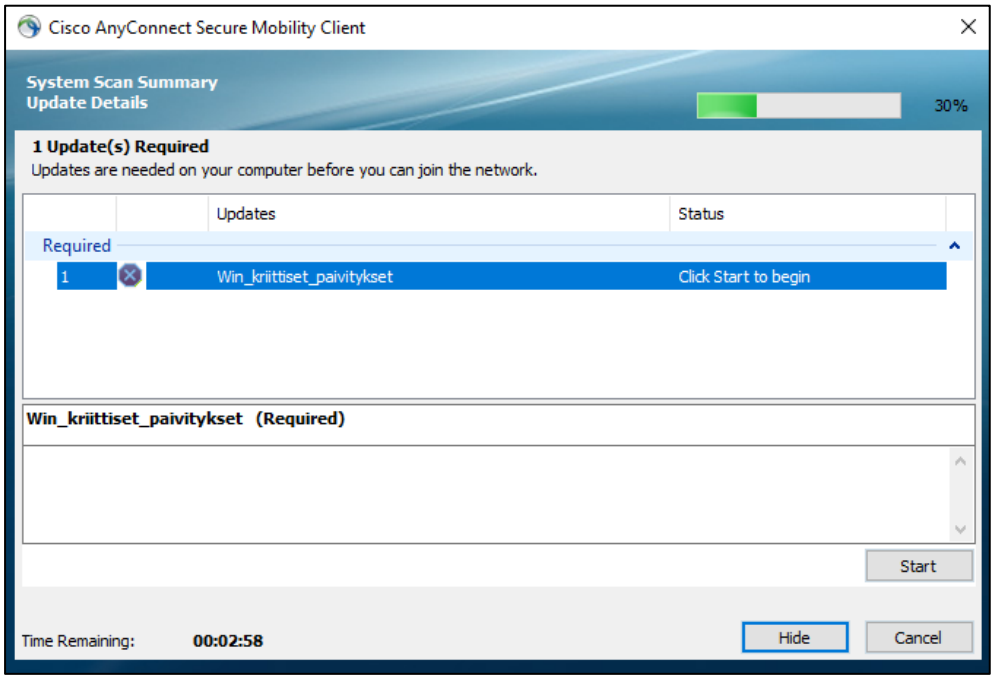
Kuva 31. AnyConnect-kirjautumisikkuna

Kun porttitodennus on suoritettu onnistuneesti ja käyttäjä todennettu, suorittaa AnyConnect posture-tarkistuksen heti perään puuttuvien tietoturvapäivitysten varalta (kuva 32):

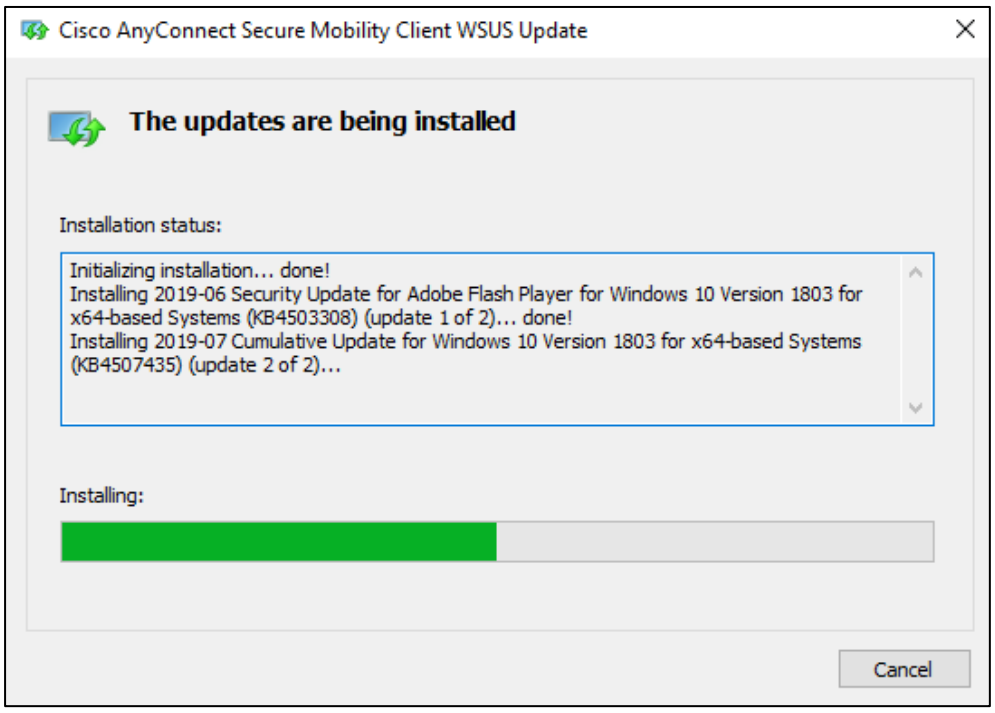


Kuva 32. Posture-tarkistus AnyConnectissa

Mikäli agenttiohjelma havaitsee työasemalla puuttuvia päivityksiä, huomauttaa se käyttäjälle siitä, että verkkoon ei voida liittyä ennen kuin pakolliset Windows-päivitykset on asennettu. Samalla se tarjoaa korjausmahdollisuutta WSUS-palvelimen välityksellä, jolloin käyttäjä voi *Start*-nappulaa painamalla käynnistää puuttuvien päivitysten lataamisen ja asennuksen (kuva 33 ja 34):

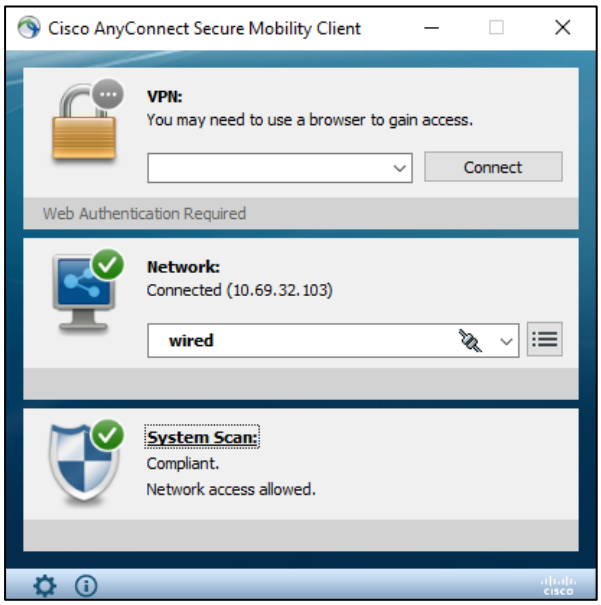


Kuva 33. Verkkoon liittymiseen vaadittavat korjaustoimenpiteet

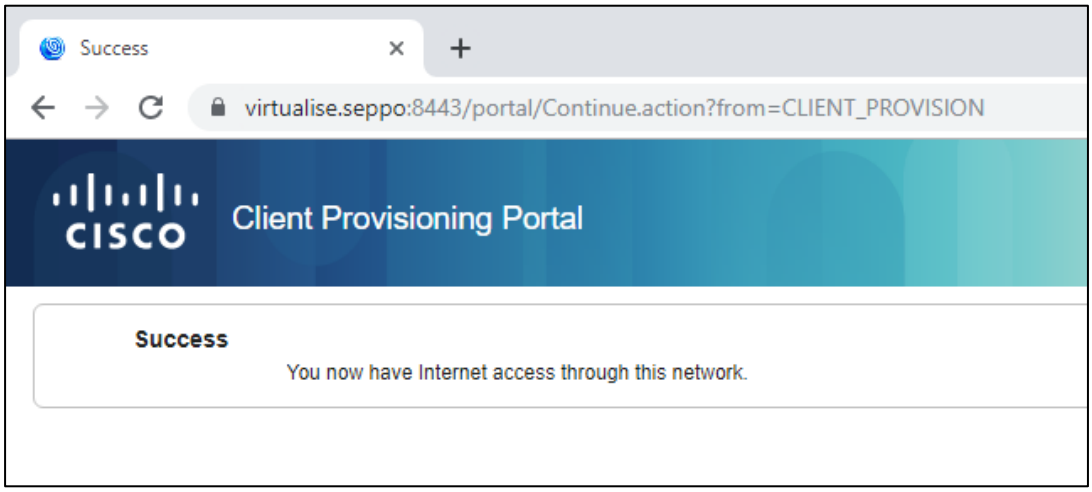


Kuva 34. Windows-päivitysten lataus ja asennus AnyConnect-asiakasohjelman kautta

Kun tarvittavat päivitykset on asennettu, alkaa posture-tapahtumaketju alusta ja asiakaskone saa tilakseen *Compliant* eli se määritellään vaatimusten mukaiseksi (kuva 35). Tämän jälkeen työaseman yhteys lähiverkkoon ja internetiin voidaan valtuutuskäytännön mukaan sallia (kuva 36).



Kuva 35. Compliant-tila onnistuneen posture-skannauksen jälkeen



Kuva 36. Yhteys Internetiin sallitaan, koska työasema sai tarkistuksessa posture-tilakseen Compliant

8 TESTAUS GAMELAB-LUOKAN TYÖASEMILLA

Virtuaalitestauksen jälkeen tarkoitus oli testata koko konfiguraatiota ICTLABin varsinaisessa verkossa ja tuotantokytkimillä. Lyhyen keskustelun jälkeen laboratorioinsinööri Jaakko Nurmen kanssa tultiin kuitenkin siihen tulokseen, että kyseinen operaatio osoittautuisi liian vaikeaksi ja monimutkaiseksi etenkin, kun ICTLABissa oli sillä hetkellä käynnissä merkittävät verkon muutostoimenpiteet. Jotta toteutusta kuitenkin päästäisiin testaamaan varsinaisilla luokkahuoneen työasemilla, päädyttiin kompromissiin, jossa muutama vähäisellä käytöllä ollut GameLabin BK0128-luokan työasema poistettiin ictlab-toimialueesta, ja liitettiin ristikytkennällä käytössä olleisiin Catalyst-kytkimiin ja näin ollen liitettiin osaksi puolittain virtuaalista lähiverkkoa ja vlab.local-toimialuetta. Aktiivihakemistoon lisättiin muutama testikäyttäjä sekä lisättiin testattavat työasemat siellä oikeaan OU-ryhmään, jolloin jo määritetyt ryhmäkäytännöt, kuten varmenteiden jako ja WSUS-määritykset, saatiin helposti käyttöön. Työasemien käyttöjärjestelmät olivat jo ajan tasalla, joten testin suorittamiseksi jouduttiin niiltä poistamaan muutama Windowsin kriittiseksi määrittelemä tietoturvapäivitys.

Lopputuloksena saatiin toimiva kokonaisuus ja konfiguraatio, jossa porttitodennetut käyttäjät joutuivat suorittamaan posture-tarkistuksen ennen kuin he saivat pääsyn lähiverkkoon tai Internetiin. Posture tarkisti työasemien Windowsin kriittisten päivitysten asennuksen ja ajantasaisuuden ja tarjosi samalla mahdollisuuden korjata eli asentaa puuttuvat päivitykset tarkistuksen päätteeksi suoraan WSUS-palvelimelta. Kun vaadittavat korjaustoimenpiteet oli tehty, valtuutti RADIUS-palvelin eli ISE kyseiset työasemat eli salli niiden pääsyn Internetiin, kuten sen valtuutussäännöissä oli määritelty.

9 YHTEENVETO

Työn tarkoitus oli tutustua ja testata Cisco ISE:n posture-palvelua 802.1X-porttitodennuksen päällä Xamkin ICTLAB-ympäristön langallisessa verkossa tietoturvaa parantavana ominaisuutena. Työtä jatkettiin Xamkin entisen opiskelijan Ville Naumasen opinnäytetyönään toteuttaman porttitodennuksen ohjeistuksen pohjalta.

Työ tehtiin kahdessa osassa, joista ensimmäisessä eli teoriaosiossa hankittiin tietoa ja perehdyttiin 802.1X-standardiin, sen toimintaperiaatteeseen ja siihen läheisesti liittyviin protokolliin. Samalla tutustuttiin myös itse posture-ominaisuuteen ja sen perustoiminnallisuuteen ja hyötyihin. Toinen osa eli käytännön osuus tehtiin virtuaalilaboratiossa, jossa posturen käyttöönottoa päästiin harjoittelemaan oikeaa ICTLABin verkkoympäristöä muistuttavassa suljetussa ympäristössä. Alun perin käytännön osuus oli tarkoitus jakaa kahteen vaiheeseen, joista toinen koostuisi virtuaalitestauksesta ja toinen pienimuotoisesta käyttöönotosta varsinaisessa tuotantoverkossa. Koska kaikkia määrityksiä ei kuitenkaan saatu toimimaan virtuaalilaboratorion testi-IOS-versioilla, jouduttiin puolet topologiasta vaihtamaan ristiinkytkennän ja multicast-VPN:nän avulla fyysisiksi laitteiksi. Tällä ns. ”hybridi”-topologialla tehtiin lopulta yhdellä kertaa niin VirtualLab-testaus kuin varsinainen käyttöönotto BK0128-luokkatilan työasemilla. Tuotantoverkon laitteilla testaamisesta päätettiin lopulta luopua, koska ICTLABissa oli työn tekemisen hetkellä käynnissä merkittävät verkon muutostoimenpiteet ja tarvittavien ohjelmistojen ja laitteiden asennus sekä määritysten muuttaminen olisi osoittautunut liian monimutkaiseksi operaatioksi.

Jo työn alussa oli lähtökohtaisesti selvää, ettei posturea voitaisi ainakaan lähitulevaisuudessa ottaa laajamittaiseen käyttöön ICTLABin verkossa, johtuen koululta puuttuvista Cisco ISE:n käyttölisensseistä. Työn tarkoitus oli myös siinä mielessä posturen määrittämisen lisäksi tutustua ja saada lisätietoa ISE:n käytettävyydestä ja ominaisuuksista mahdollista tulevaisuuden hankintaa varten. Työn aikana laboratorioinsinööri Jaakko Nurmi myös selvitti lisenssien hintoja ja Xamkille aiheituvia kustannuksia, mikäli kyseinen ohjelmisto päätettäisiin tulevaisuudessa ostaa koulun käyttöön. Pitkällisen pohdinnan jälkeen tultiin siihen johtopäätökseen, että ISE:n lisenssikustannukset ICTLABin mittakaavassa osoittautuisivat liian kalliiksi koululle ainakin lähitulevaisuudessa. Muutoin henkilökunta piti kyllä ohjelmistoa kiinnostavana ja monipuolisena, eikä sulkenut täysin pois sen myöhempää käyttöönottoa.

Opinnäytetyöhön asettamani tavoitteet tuli suurimmaksi osaksi täytettyä. Posture-tarkistus saatiin onnistuneesti konfiguroitua Windows-päivitysten osalta ja myös työasemien korjaus WSUS-palvelimen avulla onnistui. Alun perin suunnitelmissa oli lisätä myös muita posture-vaatimuksia, kuten pakollinen

virustorjuntaohjelmiston asennus, mutta työn edetessä ilmenneiden ja sitä hidastaneiden ongelmien seurauksena niistä päätettiin luopua. Virustorjuntaohjelmaan liittyvän korjaustoimenpiteen käyttöönotto olisi myös vaatinut erillisen korjauspalvelimen määrittämistä, mihin saatavilla oleva ohjeistus oli vähäistä.

Kokonaisuudessaan opinnäytetyö oli opettavainen kokemus, joka omalta osaltaan edisti ja syvensi koulutuksessa opittuja taitoja. IEEE 802.1X-standardi ja siihen liittyvät käsitteet tulivat paremmin tutuiksi ja lisää käytännön kokemusta kertyi erityisesti ISE:n ja Windows Server 2016 -palvelinkäyttöjärjestelmän ja sen eri roolien käytöstä.

Nyt kun posturen perustoiminnallisuus on testattu, tulevat opiskelijat voisivat jatkokehittää toteutusta edelleen lisäämällä siihen lisää erilaisia posture-vaatimuksia. Posturen voisi määrittää siten, että ISE tarkistaa työaseman minkä tahansa virustorjuntaohjelmiston varalta, ja mikäli se ei havaitse sellaista, antaa se komentokehotteen asentaa sellainen korjauspalvelimelta. Tämän voisi mahdollisesti toteuttaa Windows-palvelimella luomalla sinne hakemistojaon, jossa tarvittavan virustorjuntaohjelmiston asennustiedostot sijaitsisivat sekä määrittämällä tarvittavat korjaustoimenpidesäännöt ISE-palvelimella.

Toinen jatkokehityskohde olisi ottaa ISE:n posture käyttöön langattomassa verkossa WLC:n (Wireless LAN Controller) ja langattomien tukiasemien avulla. Tähän toteutukseen voisi ottaa käyttöön myös verkon VLAN-segmentoinnin, jota tässä työssä ei varsinaisesti tullut tehtyä. Verkon segmentoinnissa langattomaan verkkoon yhdistävät käyttäjät voitaisiin pistää erilliseen vieras VLANiin, jossa heille annettaisiin rajoitetummat pääsyoikeudet. Langattoman verkon posture-toteutuksessa voitaisiin myös hyödyntää selainpohjaista väliaikaista agenttiohjelmaa resurssienjaossa. Väliaikaisagentti olisi istuntokohtainen, jolloin vierasverkon käyttäjien ei tarvitsisi fyysisesti asentaa koneilleen mitään, vaan posture suoritettaisiin selaimessa ja kaikki siihen liittyvät tiedostot poistuisivat istunnon päätteeksi.

LÄHTEET

Carroll, B. 2004. Cisco Access Control Security – AAA Administration Services. Indianapolis.

Cisco. 2006. How Does RADIUS Work? WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html [viitattu 15.2.2019].

Cisco. 2011. Wired 802.1X Deployment Guide. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp387013 [viitattu 10.2.2019].

Cisco. 2012. Posture Assessment with ISE. PDF-dokumentti. Saatavissa: https://www.cisco.com/c/dam/global/cs_cz/assets/expo2012/pdf/T_SECA4_ISE_Posture_Gorgy_Acs.pdf [viitattu: 12.4.2019].

Cisco. 2015. Active Directory Integration with Cisco ISE 2.x. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/ise_active_directory_integration/b_ISE_AD_integration_2x.html [viitattu 15.5.2019].

Cisco. 2016. Catalyst 6500 Release 12.2SX Software Configuration Guide. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html [viitattu 7.2.2019].

Cisco Identity Services Engine Administrator Guide, Release 2.2. 2019. Cisco. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.html#concept_657B7414B2B942BFB8331B2357B9EFB1 [viitattu 7.8.2019].

Extensible Authentication Protocols. 2018. Cisco. PDF-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/access_registrar/6-1/user/guide/user_guide/eap.pdf [viitattu 4.2.2019].

Geier, J. 2008. Implementing 802.1X Security Solutions for Wired and Wireless Network. Indianapolis: Wiley Publishing, Inc.

IEEE 802. 2018. IEEE 802 LAN/MAN Standards Committee. WWW-dokumentti. Saatavissa: http://www.ieee802.org [viitattu 14.1.2019].

ISE Posture Style Comparison for Pre and Post 2.2. 2018. Cisco. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-22/210523-ISE-posture-style-comparison-for-pre-and.html [viitattu 19.3.2019].

Kananen, J. Kehittämistutkimus opinnäytetyönä: Kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Naumanen, V. 2018. 802.1X-porttikohtaisen todennuksen suunnittelu ICTLAB-ympäristöön. Opinnäytetyö. Kaakkois-Suomen ammattikorkeakoulu. Tieto- ja viestintätekniikan koulutusohjelma. PDF-dokumentti. Saatavissa: https://www.theseus.fi/handle/10024/150626 [viitattu 21.1.2019].

Posture Services on the Cisco ISE Configuration Guide. 2019. Cisco. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116143-config-cise-posture-00.html [viitattu 7.1.2019].

Release Notes for Cisco Identity Services Engine, Release 2.6. 2019. Cisco. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/release_notes/b_ise_26_RN.html [viitattu 20.5.2019].

RFC 3748. 2004. Extensible Authentication Protocol (EAP). WWW-dokumentti. Saatavissa: https://tools.ietf.org/html/rfc3748 [viitattu 11.2.2019].

Salonen, K. 2013. Näkökulmia tutkimukselliseen ja toiminnalliseen opinnäytetyöhön. WWW-dokumentti. Saatavissa: http://julkaisut.turkuamk.fi/isbn9789522163738.pdf [viitattu 9.1.2019].

Windows Dev Center. 2018. Network Access Protection. WWW-dokumentti. Saatavissa: https://docs.microsoft.com/en-us/windows/desktop/nap/network-access-protection-start-page [viitattu 29.1.2019].

KUVALUETTELO

Liite 1/1

802.1X POSTUREN MÄÄRITYKSEN OHJEET

Oheen on laadittu tiivistetty ohjeistus posturen määrittämiseen ICTLABin koneille. Tätä ohjeistusta voidaan hyödyntää, mikäli posturen laajamittaisempi käyttöönotto tulee tulevaisuudessa ajankohtaiseksi. Määritykset tehdään pääsääntöisesti ISE:ssä ja Windows-palvelimella.

ISE:n määritykset

Active Directoryn määrittäminen ulkoiseksi käyttäjätietokannaksi

ISE täytyy määrittää käyttämään Windows-palvelimen Active Directory Domain Services -palvelua ulkoisena käyttäjätietokantana. Siirrytään ISE:n käyttöliittymässä kohtaan *Administration > Identity Management > External Identity Sources > Active Directory*

1. Lisätään haluttu aktiivihakemisto painamalla *Add*, nimetään se kuvaavasti ja syötetään myös halutun toimialueen nimi (ICTLAB). Toimenpiteen vahvistamiseksi ISE kysyy domain adminin tunnuksia, jotka syötetään niitä vaativaan kenttään.
2. Lisätään halutun toimialueen käyttäjäryhmä sääntöparametriksi, jolloin sitä voi käyttää ehtona ISE:n eri sääntöjä luodessa. Navigoidaan *Groups > Add > Select Groups From Directory* ja valitaan käyttäjäryhmä *Domain Users* ICTLABin toimialueesta.

Resurssienjako

Tarkistetaan kohdasta *Administration > System > Settings > Client Provisioning*, että resurssienjako on kytketty päälle. Kohdassa *Enable Provisioning* tulee olla *Enable*.

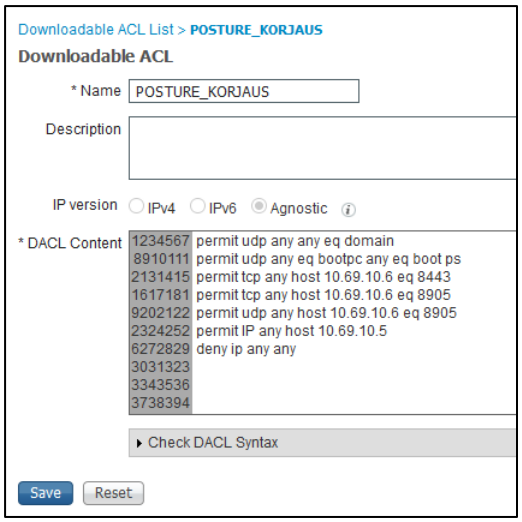
1. Lisätään ne ohjelmistoresurssit, jotka työasemille halutaan posturen yhteydessä jakaa ISE:n resurssihakemistoon kohdasta *Policy > Policy Elements > Results.*
2. Painetaan *Add* ja ladataan tarvittavat ohjelmistot ja moduulit ISE:een Ciscon sivuilta valitsemalla *Agent Resources from Cisco site.* Valitaan Compliance-moduulin uusin versio. AnyConnectin asennustiedostot täytyy erikseen ladata Ciscon sivuilta ja tuoda ne ISE:een paikalliselta levyasemalta. Tuodaan ISE:n hakemistoon myös tarvittavat verkko- ja posture-profiilit, jotka täytyy määrittää erillisellä Network Access Manager -editorilla. Posture-profiilin voi myös luoda paikallisesti ISE:ssä valitsemalla *Resour-*

ces-valikossa *Add* > *AnyConnect Posture Profile*. Profiileissa voidaan muokata parametrejä käyttöönoton tarpeiden mukaisesti. Yhdistetään kaikki osat yhdeksi AnyConnect Configuration -paketiksi valitsemalla *Add* > *AnyConnect Configuration*, johon valitaan kaikki aikaisemmin ladatut tiedostot.

3. Määritetään resurssienjakokäytäntö kohdasta *Policy* > *Client Provisioning*. Vaihdetaan Windows-käytännön *Results*-kenttään juuri luotu AnyConnect Configuration -paketti. Vahvistetaan muutokset painamalla *Save*.

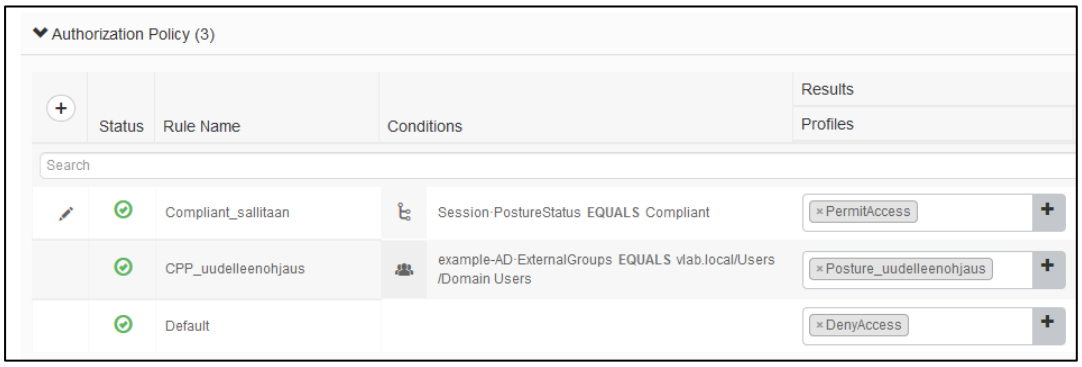
Valtuutus

Valtuutuskäytäntöjen avulla säädellään käyttäjien ja työasemien pääsyn tasoa verkkoon todennusmenetelmän, käyttäjäryhmän tai posture-tilan perusteella. Ensimmäisenä luodaan valtuutusprofiili kohdasta *Policy* > *Policy Elements* > *Results*. Mikäli asiakaslaitteen pääsyä verkkoon ennen posturen suorittamista halutaan rajata, luodaan ladattava pääsynhallintalista *Authorization*-valikon alapuolelta kohdasta *Downloadable ACLs*. Nimetään se ja syötetään siihen kuvassa olevat arvot:



1. Luodaan valtuutusprofiili (authorization profile) *Authorization*-valikon alta kohdasta *Authorization Profiles*. Profiili nimetään halutulla tavalla, jonka jälkeen valitaan *Common Tasks* -kohdan alapuolelta juuri luotu dACL sekä *Web Redirection (CWA, MDM, NSP, CPP)*. ACL-kenttään kirjoitetaan kytkimelle määritetyn uudelleenohjauspääsylistan nimi. (HUOM! Kytkimelle määritetyllä pääsylistalla tulee olla SAMA nimi.) Valitaan avautuvasta valikosta *Client Provisioning (Posture)* ja arvoksi (*value*) määritetään *Client Provisioning Portal (default)*.
2. Viimeisenä luodaan itse valtuutuskäytäntö. Siirrytään kohtaan *Policy* > *Authorization*, jonne luodaan kaksi uutta sääntöä. Ensin luodaan uudelleenohjaussääntö kaikille toimialueen käyttäjille, jonka perusteella ne uudelleenohjataan onnistuneen 802.1X-todennuksen jälkeen resurssienjako-

portaaliin. Ehdoksi valitaan siis ICTLAB:n toimialueen kaikki käyttäjät (*ictlab.local/Users/Domain Users*) ja *Results*-kenttään valitaan aikaisemmin luotu valtuutusprofiili. Toinen sääntö luodaan koskemaan kaikkia posture-tarkistuksessa compliant-tilan saaneita työasemia, joiden pääsy verkkoon sallitaan suoraan. Ehdoksi määritetään *Session PostureStatus EQUALS Compliant* ja *Results*-kenttään arvo *PermitAccess*. HUOM! Prosessointijärjestys ISE:ssä on ylhäältä alaspäin, joten tärkeimmän säännön tulee olla listauksessa ensimmäisenä.



Posture-käytännöt

Luodaan posture-käytäntö, jossa määritetään posturen työasemalta vaatimat asiat. Tässä esimerkissä vaatimukseksi asetetaan ajantasaiset Windows-käyttöjärjestelmän kriittiset päivitykset ja korjaustoimenpiteeksi puuttuvien päivitysten asennus WSUS-palvelimelta. Posture-käytännön luonti koostuu, ehdon, vaatimuksen sekä korjaustoimenpiteen määrittämisestä.

1. Luodaan korjaustoimenpide navigoimalla valikoista *Policy* > *Policy Elements* > *Results*. *Posture*-valikosta valitaan kohta *Remediation Actions* > *Windows Server Update Remediation*. Annetaan korjaukselle asianmukainen nimi ja valitaan siihen seuraavanlaiset asetukset:

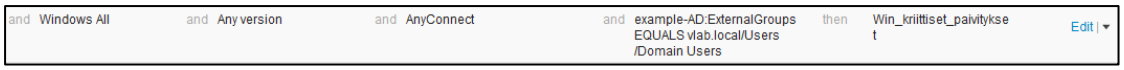
- *Remediation Type:* **Manual**
- *Validate Windows Updates using:* **Severity Level**
- *Windows Updates Severity Level:* **Critical**
- *Windows Updates Installation Source:* **Managed Server**
- *Installation Wizard Interface Setting:* **Show UI**

2. Määritetään posture-vaatimus menemällä *Policy* > *Policy Elements* > *Results* > *Posture*. Tämän alta valitaan kohta *Requirements*. Luodaan uusi vaatimus seuraavilla arvoilla:

- *Nimi:* **Win_kriittiset_paivitykset**
- *Operating Systems:* **Windows All**
- *Condition:* **pr_WSUSRule**
- *Action:* **Win_kriittiset_paivitykset_asennus**

pr_WSUSRule on ns. dummy-ehto, joka ei varsinaisesti itse tee mitään, mutta sitä käytetään ISE:ssä paikanpitäjäehtona (placeholder condition) WSUS-vaatimusten määrityksessä. Ehto on Ciscon valmiiksi määrittämä ja se löytyy kohdasta *Cisco Defined Condition* > *Regular Compound Condition*.

3. Viimeisenä vaiheena luodaan varsinainen posture-käytäntö kaiken edellä määritetyn pohjalta. Mennään *Policy* > *Posture* ja luodaan uusi sääntö Windows-työasemille. Käyttäjäryhmäksi valitaan ICTLAB:n toimialueen käyttäjät ja posture-agentiksi *AnyConnect*. Sääntöön liitetään juuri luotu posture-vaatimus eli *Win_kriittiset_paivitykset*.



WSUS-palvelimen määritys (Windows Server 2016)

Jos WSUS-palvelinrooli on jo asennettuna Windows-palvelimelle, voidaan siirtyä suoraan sen asetusten määrityksiin. Muussa tapauksessa palvelinrooli täytyy ensin asentaa *Server Managerissa* kohdasta *Add Roles and Features* > *Role-based or feature based installation*. Valitaan asennettavaksi *Windows Server Update Services*, jonka asennus voidaan suorittaa oletusarvoilla.

Asennuksen jälkeen palvelin kysyy WSUS-määrityksiä. Valitaan WSUS synkronoitumaan *Microsoft Update* -palvelun kanssa. Tarvittaessa voidaan myös määrittää välityspalvelin WSUS-palvelimelle.

Ryhmäkäytäntöjen luominen

Ryhmäkäytännöillä, eli Group Policy -säännöillä nopeutetaan WSUS-määritysten käyttöönottoa Windows-työasemilla AD-ympäristössä. Luodaan ryhmäkäytäntö, jonka avulla määrätään työasemat käyttämään *Automatic Updates* -palvelua, jonka avulla WSUS-päivitykset jaetaan niille. Samaan ryhmäkäytäntösääntöön tehdään myös määritys, jossa kerrotaan työasemille WSUS-palvelimen IP-osoite eli missä kyseinen palvelin sijaitsee.

1. Avataan *Group Policy Management* ja Domains-valikon alta valitaan ICTLABin toimialue. Valitaan haluttu OU (organizational unit), klikataan sitä hiiren oikealla ja valitaan *Create a GPO in this domain and Link it here.*
2. Nimetään sääntö kuvaavasti (esimerkissä WSUS policy).
3. Klikataan hiiren oikealla sääntöä ja painetaan *Edit*. Siirrytään avautuvista alavalikoista *Computer Configuration* > *Policies* > *Administrative Templates* > *Windows Components*. Valitaan *Windows Update* ja oikeanpuoleisesta sivuvalikosta *Configure Automatic Updates*. Klikataan valintaa hiiren oikealla ja painetaan *Edit*. Valitaan *Enabled* ja yksi kolmesta tavasta ladata ja asentaa päivitykset (esimerkissä *Notify for download and notify for install*). Vahvistetaan tehdyt muutokset painamalla *OK*.

4. Samassa ryhmäkäytäntösäännössä osoitetaan verkon työasemat myös käyttämään määritettyä WSUS-palvelinta Windows Update -tietokantanaan. Valitaan *Windows Update > Specify intranet Microsoft update service location.* Hiiren oikealla *Edit* ja valitaan asetusvalikossa *Enabled*. Syötetään vaadittuihin kenttiin WSUS-palvelimen IP-osoite (esimerkissä 10.69.10.5) ja tarvittaessa porttinumero (8530 http-liikenteelle). Vahvistetaan muutokset painamalla *OK*.
5. Otetaan määritykset käyttöön työasemilla päivittämällä niiden ryhmäkäytäntöasetukset syöttämällä komentoriville *gpupdate /force*. WSUS-käyttöönoton voi tarkistaa Windows-työasemalla avaamalla Windows Update -valikon ja varmistamalla, että siellä lukee *Some settings are managed by your organization*. On hyvä myös tarkistaa, että *Automatic Updates* -palvelu on kytketty päälle menemällä *Run > services.msc* ja varmistaa, että *Windows Update*-palvelua tuplaklikatessa päivitysten asennustapa on *Automatic*.

Kytkimien määritys

Kytkimet täytyy 802.1X-todennuksen käyttöönottoa varten RADIUS-asiakkaiksi ISE:ssä. Tämä tehdään ISE:n käyttöliittymässä kohdasta *Administration > Network Resources > Network Devices*. Nimetään kytkin, annetaan sille IP-osoite ICTLABin osoiteavaruudesta ja määritetään se käyttämään RADIUS-asetuksia. RADIUS-asetuksissa joudutaan määrittämään muun muassa salausavain (shared secret), joka täytyy myös määrittää asiakaskytkimille.

Luodaan uudelleenohjauspääsylista kaikkiin valittuihin autentikaattorikytkimiin.

1. Annetaan pääsylistalle sama nimi kuin aikaisemmin ISE:n valtuutusprofiilia luodessa esimerkissä (ISE-UUDELLEENOHJAUS). Konfiguroidaan se seuraavalla tavalla, jotta verkon kannalta tärkeää liikennettä, kuten DNS- ja DHCP-liikennettä ei uudelleenohjata, vaan ne kulkevat normaalisti kytkimen läpi:

#ip access-list extended ISE-UUDELLEENOHJAUS

#deny udp any eq bootpc any eq bootps

#deny udp any any eq domain

#deny udp any host 10.69.10.6 eq 8905

#deny tcp any host 10.69.10.6 eq 8905

#deny tcp any host 10.69.10.6 eq 8443

#deny ip any host 10.69.10.5

#permit ip any any

Posturen kannalta välttämättömät määritykset

#ip http server

- Määrittää kytkimen toimimaan http-palvelimena. Mikäli kytkintä ei ole määritetty http-palvelimeksi, portteihin tulevan liikenteen uudelleenohjausta resurssienjakoportaaliin ei tapahdu, koska kytkin ei osaa käsitellä siihen liittyviä pyyntöjä. Posture-agentti ei myöskään löydä ISE-palvelinta ilman http-protokollaa.

#radius-server vsa send accounting

- määrittää RADIUS-kytkimen tunnistamaan valmistajakohtaiset tilastointiominaisuudet

#radius-server vsa send authentication

- määrittää RADIUS-kytkimen tunnistamaan valmistajakohtaiset todennusominaisuudet

#aaa server radius dynamic-author

- Mahdollistaa kytkimen Change of Authorization –pyyntöjen vastaanottamisen RADIUS-palvelimelta eli liityntäportin valtuutustilan dynaamisen muuttamisen, mikäli valtuutuksessa tapahtuu muutoksia, kuten posturen suorittamisen jälkeen, jolloin tapahtuu 802.1X-uudelleentodennus.

Tämän jälkeen kytketään 802.1X-porttitodennus päälle asiakaskytkimistä. Pääpiirteissään ohjeet tähän löytyvät Ville Naumasen opinnäytetyöstä *802.1X-porttikohtaisen todennuksen suunnittelu ICTLAB-ympäristöön*, mutta käydään nyt kytkimien määritysten tärkeimmät vaiheet läpi.

802.1X:n käyttöönotto (global configuration mode)

#aaa new-model

- kytketään AAA-protokolla ja siihen liittyvät menetelmät, mukaan lukien RADIUS päälle.

#aaa authentication dot1x default group radius

- määrittää RADIUS-protokollan 802.1X-todennuksen todennus- ja yhteysprotokollaksi

#aaa authorization network default group radius

- määrittää käyttäjien valtuutuksen RADIUS-palvelimelle

#dot1x system-auth-control

- käynnistää kytkimessä 802.1X-protokollan.

#radius server ISE

- määrittää RADIUS-palvelimen nimen.

#address ipv4 10.69.x.x (esimerkissä 10.69.10.6)

- komennolla kerrotaan kytkimelle, mistä osoitteesta RADIUS-palvelin löytyy

#key xxxxx

- palvelimelle aiemmin määritetty salausavain turvallisen RADIUS-liikenteen takaamiseksi

Kytkinportin määritykset (interface)

#authentication port-control auto

- Ottaa 802.1X-todennuksen käyttöön kytkimen liityntäportissa

#dot1x pae authenticator

- Kytkinportin määritteleminen autentikaattoriksi oletusparametreillä