Jeremia Kunnari

Omien laitteiden käyttöön soveltuvien WLAN-ratkaisujen vertailu

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

29.5.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Jeremia Kunnari Omien laitteiden käyttöön soveltuvien WLAN-ratkaisujen vertailu 45 sivua 29.5.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja(t)	yliopettaja Matti Puska asiakaspalvelun päällikkö, Pasi Ulkuniemi

Tämän insinöörityön päämääränä oli tarkastella kolmen eri valmistajan NAC:in, eli Network Access Control-palvelinta tai -laitetta Bring Your Own Device WLAN-ympäristön toteuttamisen ja ylläpidon kontekstissa. Tämän lisäksi luotiin vastaavanlainen testiympäristö Aruba ClearPass NAC:in ympärille. Testiympäristön tarkoitus oli toimia puhtaasti esimerkkinä.

Toimeksiantajana toimi Forte Netservices Oy ja tavoitteena oli selvittää miten eri BYOD WLAN-ratkaisut vertautuvat tällä hetkellä käytössä olevaan tuotteeseen. Tutkitut tuotteet olivat Aruba ClearPass, Cisco Identity Services Engine ja Packetfence.

Teoriaosuudessa tarkasteltiin langattoman lähiverkon, porttikohtaisen varmennuksen, sekä hakemistopalveluiden ja Microsoft Access Directoryn standardeja ja toimintaa.
Käytännön osuudessa jokaisen valmistajan NAC tutkittiin erikseen. Läpi käytiin niiden käyttämät teknologiat, luvatut ominaisuudet, yhteensopivuus sekä johtopäätökset.

Aruba ClearPass-esimerkkitoteutuksessa käytiin läpi verkon komponentit, testiympäristön rakenne, sekä BYOD-toiminnallisuuden testaus, joka koostui eri päätelaitteiden provisioimisesta verkkoon.

NAC:ien tarkastelussa saatiin tulokseksi selville kaikki tarvittavat tiedot, sekä arvio niiden suorituskyvystä ja toiminnalisuudesta BYOD WLAN-ympäristön toteuttamisessa ja ylläpidossa. Tuloksista voitiin päätellä, että vain Aruban ja Ciscon tuotteet olivat kaupallisesti päteviä. Esimerkkitoteutuksessa selvisivät todennäköisimmät ongelmat ympäristön kanssa, joita olivat integraatio muiden verkkolaitteiden kanssa, että päätelaitteiden ongelmat. Näistä huolimatta Aruba ClearPass todettiin toimivaksi ratkaisuksi. Tulokseksi saatuja tietoja voidaan käyttää myyntityössä, sekä perusteena harkitessa nykyisen ratkaisun käytön tulevaisuutta.

Avainsanat	omien laitteiden käyttö, langaton lähiverkko, Aruba, Cisco, Packetfence

Author(s) Title Number of Pages Date	Jeremia Kunnari Comparison of Bring Your Own Device WLAN solutions 45 pages 29 May 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Matti Puska, Principal Lecturer Pasi Ulkuniemi, Customer Service Manager

The purpose of this thesis was to study NACs, or Network Access Control servers or devices from three different manufacturers in the context of creating and maintaining a Bring Your Own Device Wireless LAN environment.

The client for the thesis was Forte Netservices Oy, and the goal was to analyze how the current product offering BYOD WLAN matched against other manufacturers' solutions. The solutions which were studied were Aruba ClearPass, Cisco Identity Services Engine and Packetfence. The thesis also includes a theoretical section reviewing the different technologies behind the functionality, as well as a closer look into an exemplary Aruba ClearPass based test environment.

Reviewing the NACs provided all the necessary information, resulting to an evaluation for efficiency and functionality of each product. It was concluded that each solution had their own perks, but only Aruba and Cisco devices were suitable for commercial production. The exemplary test demonstrated the problems that will likely be faced when building and maintaining a BYOD WLAN environment. This included issues with integration to network, as well as problems with end user devices. Even with these problems, Aruba ClearPass was confirmed as a functional product. The resulting information can be used by sales and while evaluating the future use of the current product.

Keywords	Bring Your Own Device, WLAN, Wi-Fi, NAC, Aruba, Cisco, Packetfence

Sisällys

Lyhenteet

AAA	*Authentication Authorization Accounting*. Protokolla todentamiseen, pääsyn sallimiseen ja kirjaamiseen .
AD	*Active Directory*. Microsoftin käyttäjätietokanta ja hakemistopalvelu.
AES-CCMP	*Advanced Encryption Standard//Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*. Langattoman tietoliikenteen salausmenetelmä.
API	*Application Programming Interface*. Ohjelmointirajapinta.
BYOD	*Bring Your Own Device.* Omien laitteiden tuominen organisaation verkkoon
CCK	*Complementary Code Keying*. Modulaatiotekniikka.
CN	*Common Name*. Hakemistopalveluissa käytetty objektin attribuutti.
CoA	*Change of Authorization*. NACin päätöksestä tehty pääsyoikeuksien muutos laitteelle.
CPPM	*ClearPass Policy Manager*. Aruban ClearPassin komponentti.
CSMA/CD	*Carrier Sense Multiple Access/Collision Detection*. Tietoliikenteessä käytetyn median varausjärjestelmä.
CSV	*Comma Separated Value*. Tiedosto sisältäen pilkulla eriteltyä tietoa.
DN	*Distinguished Name*. Hakemistopalveluissa objektin sijainti hakemiston hierarkiassa pilkulla eroteltujen RDN:ien summana.
DSSS	*Direct Sequence Spread Spectrum*. Suorasekventointiin perustuva modulaatiotekniikka.
EAP	*Extensible Authentication Protocol*. Todentamisprotokolla.

EAPOL *Extensible Authentication Protocol Over LAN*. Protokolla EAP:in käyttämiseen lähiverkossa.

FHSS *Frequency Hopping Spread Spectrum*. Taajuushyppelyyn perustuva modulaatiotekniikka.

GPL *GNU Public License*. Avoin ohjelmistolisenssi.

IDS *Intrusion Detection System*. Verkkotunkeutumisen tunnistava järjestelmä.

IEEE *Institute of Electrical and Electronics Engineers*. kansainvälinen tekniikan alan järjestö.

IETF *Internet Engineering Task Force*. Internet-protokollien standardoinnista vastaava organisaatio.

IPS *Intrusion Prevention System*. Verkkotunkeutumisen estävä järjestelmä.

ISE *Identity Services Engine*. Ciscon NAC.

LAN *Local Area Network*. Paikallisverkko.

LDAP *Lightweight Directory Access Protocol*. Laajasti tuettu hakemistopalveluprotokolla.

MAB *MAC Authentication Bypass*. Protokolla MAC-osoitteen avulla todentamiseen.

MAC *Media Access Control*. Siirtoyhteyskerroksen verkko-osoite.

MAN *Metropolitan Area Network*. Kaupunkiverkko.

MDM *Mobile Device Management*. Mobiililaitteiden hallinta.

MIC *Message Integrity Code*. Viestin eheyden tarkastusprotokolla.

MIMO *Multiple Input Multiple Output*. Useita antenneja lähettimessä ja vastaanottimessa käyttävä radiokommunikaatio.

NAC *Network Access Control*. Verkkoonpääsyä kontrolloiva laite.

NAP *Network Access Protection*. Microsoftin protokolla laitteen tilan tarkastukselle.

NAS *Network Access Server*. Verkkopääsyn mahdollistava laite.

NIDS *Network Intrusion Detection System*. Verkkotunkeutumisen tunnistusjärjestelmä.

NMAP *Network Mapper*. Verkkotiedostelussa käytetty ohjelma.

ODBC *Open Database Connectivity*. Avoin rajapinta tietokannoille.

OFDM *Orthogonal Frequency-Division Multiplexing*. Useita toisiaan häiritsemättömiä taajuuskanavia yhtäaikaisesti käyttävä modulointitekniikka.

OU *Organizational Unit*. Hakemistopalveluissa objekti, jonka sisälle voi sijoittaa muita objekteja.

OUI *Organizational Unit Identifier*. MAC-osoitteen osio valmistajatunnisteelle.

PAE *Port Authentication Entity*. Porttitodentamisen osapuoli.

PSK *Preshared Key*. Jaettu salasana.

RADIUS *Remote Authentication Dial in User Service*. AAA:ta toteuttava protokolla.

RC4 *Rivest Cipher 4*. Jonosalaustekniikka.

RDN *Relative Distinguished Name*. Hakemistopalveluissa objektin sisältämä attribuutin ja arvon muodostama pari.

SCEP *Simple Certificate Enrollment Protocol*. Protokolla varmenteiden jakamiselle lähiverkossa.

SISO *Single Input, Single Output*. Yksittäistä antennia lähettimessä ja vastaanottimessa käyttävä radiokommunikaatio.

SNMP *Simple Network Management Protocol*. Verkonhallintaan käytetty protokolla.

TACACS *Terminal Access Controller Access Control System*. AAA:ta toteuttava protokolla.

TKIP *Temporal Key Integrity Protocol*. Langattoman tietoliikenteen salausmenetelmä.

U-NII *Unlicensed National Information Infrastructure*. Yhdysvaltain FCC:n määrittelemä radiotaajuus.

VLAN *Virtual LAN*. Virtuaalinen paikallisverkko.

VPN *Virtual Private Network*. Virtuaalinen erillisverkko.

WEP *Wired Equivalent Privacy*. Langattoman tietoliikenteen salausmenetelmä.

Wi-Fi *Wireless Fidelity*. Langattoman lähiverkon vaihtoehtoinen nimitys.

WLAN *Wireless Local Area Network*. Langaton lähiverkko.

WPA *Wi-Fi Protected Access*. Langattoman tietoliikenteen salausmenetelmä.

1 Johdanto

Bring your own device, eli henkilökohtaisten päätelaitteiden käyttäminen jonkin organisaation, yleisimmin työpaikan verkossa on viime vuosina huomattavaksi kasvanut ilmiö. Omia laitteitaan verkkoon tuovat vieraat ja organisaation omat jäsenet, jotka haluavat käyttää omia laitteitaan työnteossa.

Älypuhelimien ja tablettien suosio on tehnyt ilmiöstä väistämättömän erityisesti langattoman verkon puolella, jolloin verkkojen ylläpitäjien on täytynyt reagoida tilanteeseen. Työpaikoilla on tässä mahdollisuus säästää huomattava määrä rahaa työntekijöiden päätelaitteiden hankinnassa, mutta vastapainona huoleksi jäävät tietoturva sekä ongelmat verkonhallinnassa ja -valvonnassa.

Bring your own device (tästä eteenpäin BYOD) on erittäin laaja ja monimuotoinen konsepti, mikä johtuu muun muuassa päätelaitteiden ja näiden käyttöjärjestelmien sekä ohjelmistojen jatkuvasta muutoksesta. Tämä tarjoaa huomattavia haasteita sekä BYOD-ratkaisujen tarjoajille, että niiden käyttäjille.

Täydellistä yhteensopivuutta on mahdotonta taata, jolloin eri pääsytasot verkkoon ovat lähes pakollisia. Tämä monimutkaistaa kuviota entisestään. Myös eri pääsytasojen toteutuksissa on huomattavia eroja laitevalmistajien kesken.

Insinöörityön toimeksiantajana toimii vuonna 2000 perustettu Forte Netservices Oy joka tarjoaa tietoliikenne- ja tietoturvapalveluja yrityksille sekä yhteisöille. Työssä selvitetään, miten yrityksen tällä hetkellä käyttämä BYOD-ratkaisu selviää vertailussa muihin.

Tarkemmin määriteltynä työn tarkoitus on selvittää kolmen eri valmistajan WLAN eli Wireless LAN BYOD -ratkaisujen ominaisuudet sekä käytetyt teknologiat. Näitä tarkastellen selviävät heikkoudet, vahvuudet sekä käyttöympäristöt joihin ratkaisut parhaiten soveltuvat.

Koska suurin osa BYOD-ominaisuuksista löytyy lähes poikkeuksetta NAC- eli Network Access Control -laitteista, keskittyy työ vain näiden laitteiden tarkasteluun BYOD WLAN -näkökulmasta.

Työ jakautuu kolmeen loogiseen osioon. Aluksi tarkastellaan pääpiirteittäin käytettyjä teknologioita, jonka jälkeen siirrytään itse BYOD-ratkaisujen tarkempaan tutkintaan. Tutkittavia laite- ja ohjelmistovalmistajien ratkaisuja on kolme: kaupalliset Aruba ja Cisco sekä GPL-lisensoitu Open Source -projekti Packetfence. Ratkaisujen ominaisuuksia, käytettyjä teknologioita, sekä heikkouksia ja vahvuuksia vertaillaan. Näin saadaan selville ympäristöt ja tilanteet, joissa ratkaisut parhaiten toimivat. Viimeiseksi luodaan käytännön toteutus Aruban laitteilla esimerkin vuoksi. Läpi käydään esimerkkiratkaisun komponentit, verkon rakennus, testaus sekä johtopäätökset.

2 Langaton lähiverkko IEEE 802.11

2.1 802.11-standardit

IEEE:n eli eli Institute of Electrical and Electronics Engineers -järjestön tarkoitus on kehittää teknologista innovaatiota ja esimerkillisyyttä ihmiskunnan hyväksi. Sen jäsenet tuottavat julkaisuja, konferensseja, teknologisia standardeja sekä ammatillisia ja opetuksellisia tilaisuuksia. [1.]

IEEE:n standardi 802 on tarkoitettu LAN- eli Local Area Network ja MAN- eli Metropolitan Area Network-ympäristöihin, 11 on taas tämän standardin alainen tutkimusryhmä, tarkoitettu erityisesti WLAN:ien eli langattomien lähiverkkojen tutkimiseen.[2;3.]

Tärkeimpiä 802.11-standardeja ovat alkuperäinen 1997-standardi, b a g ja n. Ne määrittelevät sekä fyysisen että Media Access Control –tason. Tärkeimmät erot ovat käytetyissä modulaatiotekniikoissa, taajuusalueessa sekä SISO/MIMO:n (Single Input, Single Output/Multiple Input, Multiple Output, eli käytettyjen antennien määrä sekä lähetys- että vastaanottopäässä) käytössä. Suurin osa muista kirjaimilla määritellyistä

alistandardeista ovat joko muutoksia tai lisäyksiä näihin. Kaikki standardit on myöhemmin yhdistetty yhdeksi dokumentissa IEEE-802.11-2007 ja myöhemmin IEEE-802.11-2012. [4;5;6;7, s. ix;8;9, s. ix;18..]

Alkuperäinen *802.11*-standardi käyttää 2,4 GHz:n radioaaltokaistaa joko DSSS-(Direct Sequence Spread Spectrum, suorasekventointi) tai FHSS-modulointia (Frequency Hopping Spread Spectrum, taajuushyppely). Vaihtoehtoisesti standardia voitiin käyttää myös infrapunalla. Datanopeus oli joko 1 tai 2Mbps. [18, s. 227, 258.]

Median käyttömetodiksi on määritelty Carrier Sense Multiple Access, sekä Collision Avoidance (CSMA/CD). Tämä käytti huomattavan osion käytettävästä kanavan kapasiteetista. Tätä standardia ei koskaan otettu laajasti käyttöön.[11.]

Alkuperäiseen standardiin tehdyssä lisäyksessä *802.11a* käytetty radioaaltokaista on taajuudeltaan 5 GHz, joka kulkee Yhdysvalloissa nimellä Unlicensed National Information Infrastructure (U-NII).

Käytetty modulointitekniikka on OFDM (Orthogonal Frequency-Division Multiplexing), jonka avulla pystytään saavuttamaan huomattavasti korkeampi datanopeus. Tuetut datanopeudet ovat 6–54 Mbps.[4, s.3.]

Standardi käyttää korkeampaa taajuutta, joka johtaa signaalin lyhyempään kantoalueeseen, häiriön sietoon, sekä signaalin läpäisykykyyn. Käytännössä 2,4 GHz:n alueella on kuitenkin huomattavasti enemmän häiriölähteitä.

802.11b oli toinen lisäys alkuperäiseen standardiin. Tässä 2.4 GHz:n kaista on edelleen käytössä, mutta uudella DSSS:ää laajentavalla CCK-modulaatiotekniikalla (complementary code keying) päästiin 5,5 ja 11 Mbps datanopeuksiin.[5, s.11.]

802.11b oli ensimmäinen laajasti käyttöön otettu langattoman lähiverkon standardi, jota markkinoitiin nimellä ’Wi-Fi’.[12;13.]

Kolmantena lisäyksenä *802.11g* käyttää OFDM-modulaatiota 2,4 GHz:n kaistalla antaen sen käyttäjille 54 Mbps:n maksimidatanopeuden. Standardi on edelleen laajassa käytössä.[6, s.15.]

Neljäs lisäys eli *802.11.n* pystyy käyttämään sekä 2,4, että 5 GHz:n kaistaa. Kanavien mahdollista kaistanleveyttä on nostettu 40 MHz:iin aikaisemman 20 MHz:n sijaan. Käytetty modulaatiotekniikka on edelleen OFDM, mutta maksimissaan neljää antennia sekä lähettimessä, että vastaanottimessa käyttävä MIMO (Multiple Input Multiple Output) mahdollistaa usean eri datavirran välityksen samaan aikaan. Nämä uudet lisäykset nostavat mahdollisen datanopeuden 600Mbps:ään. [8, s.10, 247.]

802.11ac on kehitteillä oleva standardi, joka käyttää 256 QAM-modulaatiota 5 GHz:n taajuusalueella. Uuden standardin tavoitteena on 1 Gbps nopeus.[14, s. 4-5..]

802.11ad on usean gigabitin datanopeuteen tähtäävä standardi, jonka taajuusalue on noin 60 GHz. Uutta standardia ajaa WiGig-järjestö, jonka hallitukseen kuuluu useita suuria teknologiayrityksiä.[15, s.2;16.]

2.2 802.11-turvastandardit

Langaton lähiverkko on huomattavasti turvattomampi kuin langallinen. Lähetetty tieto on kaikkien nähtävissä olettaen, että tarkastelija on signaalin kattamalla alueella.Tästä syystä ensimmäinen turvaprotokolla sisällytettiin jo alkuperäisen standardiin. Se kulki nimellä WEP eli Wired Equivalent Privacy. Tämä ensimmäinen ratkaisu havaittiin kuitenkin turvattomaksi, ja lisäys 802.11i mahdollisti kahden uuden protokollan käytön, WPA:n (802.11i luonnosversio, 2003) sekä WPA2:n (2004).

WEP on 802.11-standardin alkuperäinen turvaprotokolla. Se käyttää RC4-jonosalausta viestin salaukseen sekä CRC-32:ta datan eheyden tarkastukseen. Käytetyn avaimen koko on joko 64- tai 128-bittinen, josta alustusvektorin koko on 24 bittiä. Itse avain tässä on siis pituudeltaan 40- tai 104-bittinen.[18, s.60–70.]

Todennus tapahtui joko verkkoavaimen kanssa, tai avoimesti, jolloin kuka tahansa pystyi liittymään verkkoon.[18, s.60.]

WEP-salaus on mahdollista murtaa nykyisillä työkaluilla minuuteissa, joten sen käyttö ei ole suositeltavaa. [17.]

Siirtymäprotokollaksi *WEP*:in ja *WPA2*:n välille suunniteltu *WPA* käytti viestin salaukseen RC4 TKIP -salausta, ja datan eheyteen CRC-32:n lisäksi Michael-nimistä MIC-protokollaa (Message Integrity Check). TKIP salaa jokaisen paketin eri avaimella, mikä lisäsi tietoturvaa huomattavasti WEP:iin verrattuna. Viestin salaukseen on mahdollista myös käyttää *WPA2*:n AES-CCMP-protokollaa.

Autentikaatiosta, eli todennuksesta on kaksi versiota: WPA Personal sekä WPA Enterprise. Näistä WPA Personal käyttää verkkoon liityttäessä vain yhtä 256-bittistä Pre-shared Key -avainta. WPA Enterprise -todennuksessa taas käytetään hyväksi 802.1X-todennuspalvelua sekä porttikohtaista todentamista. [9, s.1193 - 1195.]

WPA2 ei käytä enää oletuksena RC4-jonosalausta, vaan siirtyy käyttämään AES-CCMP-salausprotokollaa. WPA2 käyttää uusia 4-Way-Handshake- ja Group-Key-Handshake -protokollia tarpeellisten salausavaimien luontiin käyttäjän liityttyä verkkoon. Tämä, sekä alkuperäinen todennus tukiasemalle tapahtuvat EAPOL-avainkehyksien avulla. Kuten WPA, WPA2 käyttää joko WPA-Personalia tai WPA-Enterpriseä todennuksessa. [9, s. 1205, 1254, 1264, 1377.]

3 Porttikohtainen käyttöoikeuksien hallinta IEEE 802.1X

Port Based Network Access Control, eli porttikohtainen käyttöoikeuksien hallinta luotiin rajoittamaan tuntemattoman laitteen tai käyttäjän pääsyä yksityisiin LAN- tai WLAN-verkkoihin.

EAP, eli Extensible Authentication Protocol on todennusmekanismin kehys jonka ympärille on rakennettu useita eri todennusmetodeja. Protokolla määritellään IETF:n dokumentissa RFC 2284.

EAP on käytössä sekä IEEE:n 802.11- ja 802.1X-standardeissa. Ensimmäiseksi sitä käytettiin PPP:n, eli Point-to-Point-protokollan todennussmetodina. Ensimmäisen kerran protokolta määriteltiin IETF:n, eli Internet Engineering Task Forcen RFC-dokumentissa 2284. [9, s. 12-54.]

EAPOL eli EAP Over Lan on keino paketoida EAP-protokolla omaksi OSI-mallin verkkotason protokollakseen, ja tällä on myös oma Ethertype-arvo datalinkki-tasolla. [19, s.87.]

3.1.1 Todennus

802.1x todennus tapahtuu kahden PAE:n (Port Access Entity) eli porttiin liittyvän taho, sekä tunnistuspalvelimen välillä EAP-protokollan avulla.

- Supplicant (PAE) on päätelaite, joka haluaa pääsyn verkkoon, kommunikoi Authenticator PAE:n roolissa olevan verkkolaitteen kanssa.

- Authenticator (PAE) on verkkolaite, joka todentaa Supplicant PAE:n tunnistuspalvelimen avulla, sekä välittää dataa Supplicant PAE:n ja tunnistuspalvelimen kanssa muuntaen pakettien muotoa tarvittaessa.

- Tunnistuspalvelin, sisältää tarvittavat käyttäjätiedot ja -oikeudet. Palvelin viestii Authenticator PAE:n kanssa ilmoittaen tälle joko hyväksyvän tai kieltävän vastauksen todennusyritykseen. [19, s.51.]

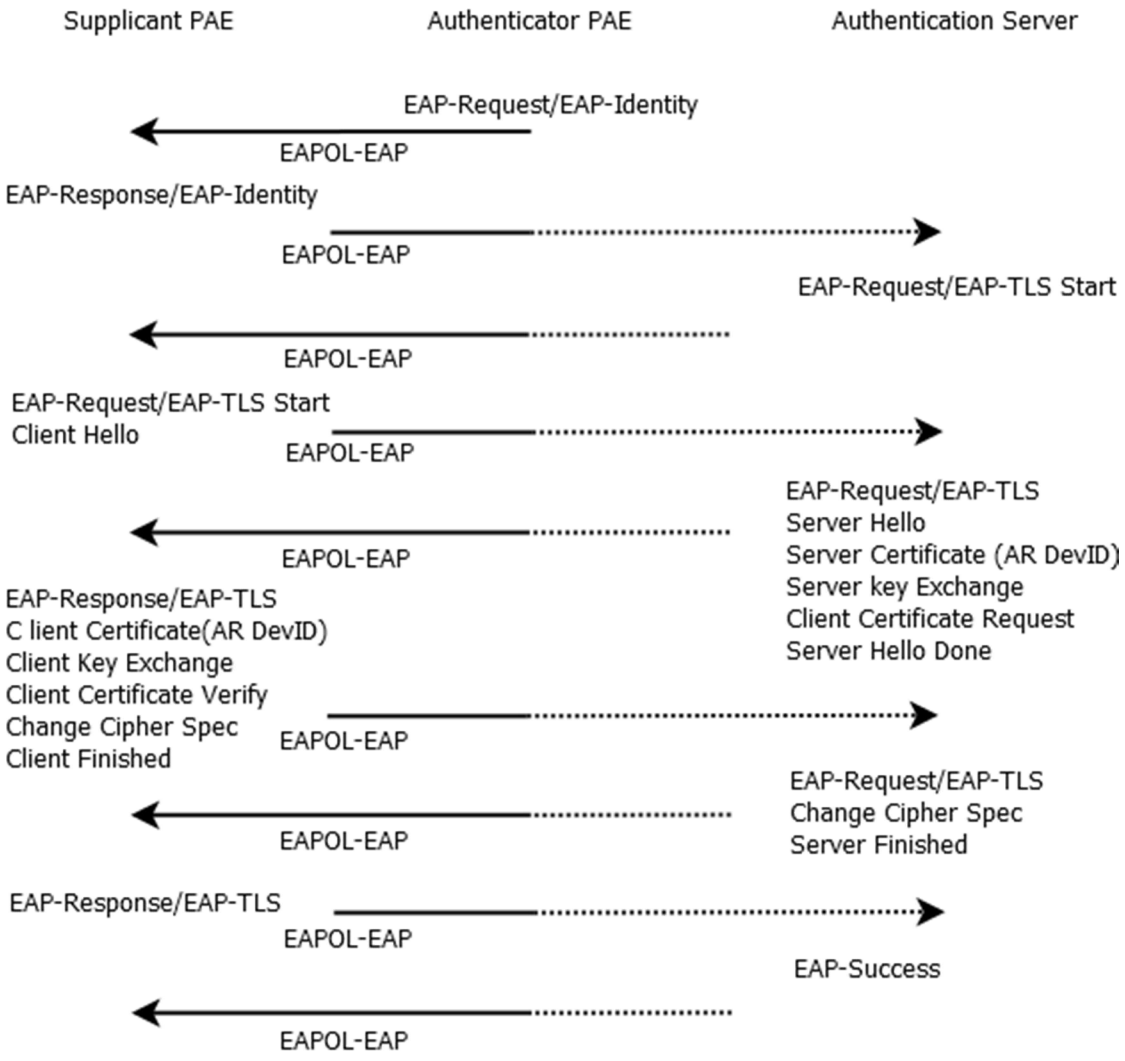
Todennus voidaan tiivistää kolmeen vaiheeseen [19, s.49-51.]:

1. Tunnistaessaan uuden laitteen portissaan todentava laite, esimerkiksi kytkin asettaa portin tilan ei-todennetuksi. Vain EAPOL-liikenne hyväksytään.

2. Authenticator PAE lähettää porttiin EAP-Request-paketteja (Supplicant PAE voi myös pyytää EAP-Request-paketteja Authenticator PAE:lta EAP-Start-paketin lähettämällä), joihin Supplicant PAE vastaa EAP-Response/Identity-paketilla. Tämä sisältää tarvittavan tunnisteen, esimerkiksi käyttäjätunnuksen. Tämän jälkeen Authenticator PAE muuntaa EAPOL-paketin tunnistuspalvelimen ymmärtämään muotoon ja lähettää sen eteenpäin. Authenticator PAE muuntaa pakettien muotoa aina välittäessään tietoa Supplicant PAE:n ja tunnistuspalvelimen välillä.

3. Tunnistuspalvelin vastaanottaa paketin, ja lähettää EAP-neuvotteluun ja todennukseen tarvittavat parametrit (esim. varmenne tai kertakäyttöinen haaste) Authenticator PAE:n kautta Supplicant PAE:lle. Tämä vastaa haasteeseen omilla tiedoillaan. Tunnistuspalvelin sekä Supplicant PAE neuvottelevat Authenticator PAE:n välityksellä vähintään kahdeksan EAP-paketin verran, jonka jälkeen tunnistuspalvelin joko hyväksyy todennuksen EAP-Success-paketilla tai hylkää sen käyttämällä EAP-Failurea.

Todennusprosessin esimerkki löyty kuvasta 1.



Kuva 1. Onnistunut 802.1X todennusprosessi [19, s.51.]

Mikäli verkkolaitteella ei ole mahdollista suorittaa yllämainitun kaltaista 802.1X todennusta, voidaan turvallisuutta ylläpitää MAB:illa, eli Mac Authentication Bypassilla. Jos laite ei vastaa autentikoijan 802.1X-kyselyihin, kyseisen laitteen MAC-osoite (Media Access Control) lähetetään tarkastettavaksi tunnistuspalvelimelle sekä käyttäjänimenä, että salasanana Authenticator PAE:n toimesta. Osoitetta verrataan palvelimen käyttäjätietokantaan, ja todennus hyväksytään tai hylätään tämän perusteella. MAB ei ole osa 802.1X standardia, vaan laitevalmistajien luoma laajennus siihen. [20.]

4 RADIUS ja AAA

IETF on avoin, internet-standardeja kehittävä organisaatio, jolla ei ole muodollista jäsenyyttä. IETF julkaisee dokumentteja nimellä ”RFC” eli Request For Comments. Tämä ilmaisee samalla dokumenttien avoimuutta ja jatkuvaa kehitystoimintaa. Huomioitavaa on, että kaikki IETF:n julkaisemat dokumentit eivät ole yleisessä käytössä olevia standardeja.[21.]

RADIUS, eli Remote Authentication Dial in User Service on AAA-protokolla (Authentication, Authorization and Accounting). Molemmat näistä termeistä ovat määritelty IETF:n RFC-dokumenteissa. RADIUS, sekä osa AAA-dokumenteista ovat käytössä olevia standardeja. [22;23;24.]

AAA eli Authentication, Authorization and Accounting on tietoturvarakenne, jonka avulla hallinnoidaan käyttäjien tunnistusta (Authentication), mihin resursseihin käyttäjillä on pääsy (Authorization), ja samalla pidetään kirjaa käyttäjien toimista (Accounting).

Todennuksessa (Authentication) käyttäjän henkilöllisyys todennetaan käyttämällä jotakin useista eri todennustavoista, esim. digitaalinen varmenne, Active Directory -tunnusta tai OTP:ta eli One-Time Passia. Ilman todennusta käyttäjä ei pääse hallittuihin resursseihin käsiksi. [24, kohta 1.2.]

Pääsyn sallimisessa (Authorization) tunnistetulle käyttäjälle määritellään resurssit, joihin hänellä on oikeudet verkossa. Määrittely voidaan tehdä monien asioiden perusteella, esimerkiksi käyttäjätunnuksen, käyttäjän IP-osoitteen tai kellonajan.

Määritellyt ominaisuudet voivat olla esimerkiksi sallittu pääsy erinäisiin resursseihin, käytettävissä oleva kaista, käyttäjälle jaettu IP-osoite tai monia muita asioita. Tämänhetkiset AAA-palvelimet pystyvät määrittelemään sekä kriteerit että käyttäjien roolit hyvin tarkasti. [22, kohta 5.]

Kirjaamisessa (Accounting) AAA-palvelin pitää kirjaa kaikista sen tapahtumista ajankohtineen. Tämä on tarpeellista järjestelmän toiminnan analysointiin, sekä mahdollisesti laskutukseen. [24, kohta 1.2.]

RADIUS on äärimmäisen tuettu, laajassa käytössä oleva AAA:ta tarjoava asiakas-palvelin-protokolla, ja ajaa todennuksen osaa myös IEEE 802.1X-toteutuksissa. RADIUS määriteltiin ensi kerran IETF:n RFC:n dokumenteissa 2865–2866. [22;23.]

Protokolla käyttää OSI-mallin kuljetuskerrosta, sekä UDP-portteja 1812 todennukseen ja pääsyn sallimiseen ja 1813 kirjanpintoon. Todennusviestit lähetetään epäturvallisina MD5-tiivistetiedostoina, mistä syystä RADIUS-liikenne kierrätetään usein VPN-tunnelin läpi. [22, Introduction, osa 2..]

RADIUS:in käyttäjät voidaan myös määritellä eri tunnistusalueisiin esimerkiksi Active Directory Domain Controllerin mukaan, mikä helpottaa käyttäjien erottelua organisaation tai hierarkian mukaan.

Ensimmäisissä toteutuksissa RADIUS-palvelin pystyi hallinnoimaan käyttäjien verkkoon pääsyä vain NASin, eli Network Access Serverin luodessa pyynnön, mutta kesäkuun 2003 RFC 3576 -laajennuksen myötä CoA eli Change of Authorization tuli osaksi protokollaa. CoA:n avulla RADIUS pystyy suorittamaan pääsyoikeuksia muokkaavia toimintoja ilman erillisiä pyyntöjä NAS:ilta. [25.]

5 Lightweight Directory Access Protocol

Lightweight Directory Access Protocol eli LDAP on TCP/IP:n päällä toimiva protokolla hakemistopalveluiden käyttöön. Sitä voidaan käyttää useiden eri hakemistojen, esimerkiksi Microsoftin Active Directoryn käyttämiseen. Käyttötarkoituksia voivat olla muun muuassa hakemiston lukeminen, muokkaaminen, etsiminen tai vertaustoimintojen (käyttäjän käyttöoikeuksien tarkastus) suorittaminen.

LDAP luotiin, jotta vanhempia X.500-hakemistopalveluprotokollien vuoksi ei tarvitsisi käyttää OSI-mallin protokollapinoa. Ensimmäinen versio protokollasta löytyy RFC-dokumentista, joka on päivätty kesäkuulle 1993.[26;27.]

LDAP:ta käytettäessä jokainen yksittäinen merkintä hakemistossa koostuu attribuuteista, joilla jokaisella on kuvaus tai nimi sekä yksi tai useampi arvo. Jokaisella merkinnällä on myös dn eli distinguished name, jossa määritellään sen sijainti hakemistorakenteessa. rdn on taas relative distinguished name, jolla merkintä löydetään sen nykyisestä paikasta merkintähierarkiassa. Merkinnän dn voi muuttua, mikäli sen sijaintia hakemiston sisällä muutetaan. Merkinnän absoluuttiseen todentamiseen suositellaankin UUID:n, eli Universally Unique Identifierin käyttöä. [28.]

Koska LDAP on TCP/IP:tä käyttävä protokolla, määritellään hakemiston juuri DNS-nimillä. LDAP:ssa käytetty termi on dc eli domain component. Jokaisella merkinnällä pitää olla myös ainakin yksi objectClass, joka määrittelee merkinnän tyypin. Muita yleisesti käytettyjä attribuutteja ovat cn eli common name, joka on merkinnän yleisesti käytetty nimitys hakemistossa, sekä ou eli organizational unit, johon useampi merkintä voi kuulua.[27, osio 4.]

Tässä esimerkkinä toimivassa LDAP-merkinnässä *Erkki Esimerkki* sijaitsee DNS-nimen *yritys.com* alla, sekä tämän sisältä löytyvän hakemistorakenteen hakemistosta *tyontekijat*. *Erkki Esimerkki* kuuluu objectClassiin *projektipaallikko*:

```
dn: cn=Erkki Esimerkki, ou=tyontekijat, dc=yritys, dc=com
cn: Erkki Esimerkki
mail: erkki.esimerkki@yritys.com
objectClass:projektipaallikko
```

LDAP käyttää oletuksena TCP-porttia 389 ja SSL eli Safe Secure Layer-tunneloituna taas porttia 636. SSL-tunneloituna protokollaa kutsutaan LDAPS:iksi, mutta tähän ei ole referenssejä RFC-dokumenteissa. Tähän on kuitenkin huomattavasti referenssejä muun muuassa Microsoftin Active Directoryn dokumentaatioissa.[27, osio 5.] [29.]

6 Active Directory

Active Directory eli aktiivihakemisto tai lyhyesti AD on Microsoft Windows domainissa eli toimialueessa käytetty hakemistopalvelu/käyttäjätietokanta. AD:ta osaavat kuitenkin hyödyntää myös monet Microsoftin ulkopuoliset tahot, laitteet sekä verkon palvelut. Active Directory on Windows Server -tuoteperheen komponentti, joka löytyy nimellä Active Directory Domain Services. Ensimmäinen versio Active Directorysta julkaistiin Windows 2000 Serverin yhteydessä.[30;31.]

6.1 Rakenne

Pienin yksikkö Active Directoryssa on *objekti*. Objekti voi olla monia asioita, esimerkiksi tulostin, palvelin, käyttäjä- tai päätelaitetili, ryhmä, kansio, ohjelma, palvelu tai tietoturvatason vaatimus laitteelle. Uusia objekteja luodessa voidaan päättää sen tyyppi, jolloin AD täyttää käyttäjän puolesta osan objektin attribuuteista, kuten GUID:n eli Globally Unique Identifierin. Muut attribuutit täyttää AD:n käyttäjä, riippuen objektityypin rajoitteista.

Objekti voi olla *container*, eli objekti joka voi sisältää muita objekteja, tai vaihtoehtoisesti *leaf*, josta tätä ominaisuutta ei löydy.

Skeema tarkoittaa Active Directory -tietokannasta löytyviä objektiluokkia ja objektien atribuuttiluokkia. Jokaiselle objektiluokalle määritellään pakolliset ja vaihtoehtoiset attribuuttiluokat, sekä mahdollinen toisesta objektiluokasta periytyminen. Jokainen AD:sta löytyvä objekti on jonkin objektiluokan jäsen. Sama pätee myös attribuutteihin ja attribuuttiluokkiin. Myös skeeman määrittelevät objektit löytyvät tietokannasta Class-Schema tai Attribute-Schema objekteina.

Jokaisella objektiluokalla Active Directoryssa on attribuutteja, jotka takaavat:

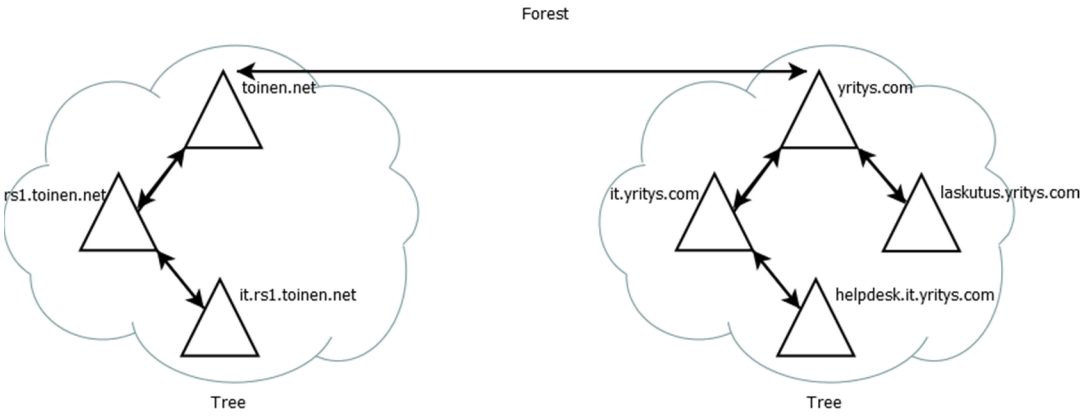
- yksilöllisen tunnistuksen
- yhteensopivuuden Windows NT 4.0 ja aikaisempien versioiden kanssa
- yhteensopivuuden LDAPin hakemistojen nimeämisstandardin kanssa.

Attribuutti voidaan merkitä indeksoitavaksi, jolloin Active Directoryn haut kyseisen attribuutin omistavaan objektiin nopeutuvat. Lisäksi attribuutti voidaan lisätä myös Global Catalogiin, joka sisältää useamman eri toimialueen AD-palvelimen (Tämän AD-rakenteen nimi on forest). Tämä kopioi kyseisen attribuutin jokaiselle AD-palvelimelle forest- eli metsärakenteen sisällä. [32.]

Paikallista domainia eli Windows-toimialuetta hallinnoi yksi tai useampi Domain Controller eli paikallinen Active Directory -palvelin. Toimialue määritellään DNS-nimellä, esim. yritys.com. Toimialueeseen kuuluvat Active Directory -palvelimen tietokannasta löytyvät objektit . Mikäli yhdellä toimialueella on useampi AD-palvelin, tiedot kopioidaan näiden välillä.

Tree eli puu on kokoelma toimialueita, jonka korkeammat tasot ovat alimman tason DNS-toimialueita. Toimialueiden välillä on transitiivinen luottamusuhde, joka jakautuu myös mahdolliseen forest-rakenteen alimman tason toimialueen kautta.

Forest eli metsä on kokoelma toisiinsa DNS-nimen kautta liittymättömiä toimialueita, joiden välillä on kaksisuuntainen ja transitiivinen luottamussuhde. Tämä on hyödyllinen, mikäli kaksi organisaatiota haluavat jakaa hakemistojen sisältämät tiedot. Kaikki AD-rakenteet ja näiden suhteet näkyvät kuvassa 2.



Kuva 2. Active Directoryn Tree- ja Forest-toimialuerakenteet.

7 BYOD WLAN -ratkaisujen vertailua

Aruba, Cisco ja Packetfence ovat tässä osiossa tarkasteltavat BYOD WLAN -ratkaisujen tarjoajat. Näistä Aruba ja Cisco ovat kaupallisia laite- ja ohjelmistovalmistajia. Packetfence on taas ilmainen GPL:n eli GNU Public Licensen alainen avoimen lähdekoodin projekti kaupallisella tuella. Aruba ja Cisco valittiin tarkasteltaviksi, koska molemmat ovat jo valmiiksi tunnettuja brändejä korkeatasoisista WLAN-ratkaisuistaan. Ominaisuuksien määrä on siis oletettavasti suuri, ja laajojen erojen löytäminen ratkaisujen välillä olisi potentiaalisesti mielenkiintoista. Sama pätee varmasti myös ilmaisen Packetfencen ja kaupallisten ratkaisujen välillä, mikä perustelee tämän kolmannen ratkaisuntarjoajan valinnan.

7.1 Aruba

Aruba on vuonna 2002 Yhdysvaltojen Kaliforniassa perustettu teknologiayritys, joka tunnetaan erityisesti WLAN-laitteistaan ja ratkaisuistaan. Yrityksen tuotteita ovat muun muuassa WLAN/LAN-kontrollerit, WLAN-tukiasemat, kytkimet sekä verkonhallintaohjelmat.[33.]

7.1.1 Aruba ClearPass

Aruban ClearPass on BYOD ja WLAN-ominaisuuksia tarjoava NAC eli Network Access Control ja se on saatavilla joko fyysisenä laitteena tai virtuaalipalvelimena. Se tarjoaa useita laajasti muokattavissa olevia ominaisuuksia, jotka pystytään integroimaan olemassaolevaan langattomaan verkkoinfrastruktuuriin RADIUS- ja Captive Portal-palvelimina. ClearPassin toiminnallisuus on jaettu eri komponenttien kesken, jotka on suurimmalta osalta integroitu keskenään. [34, s. 5.]

Tarjotut ominaisuudet ovat

- todennus
- pääsyoikeuksien hallinnointi
- kirjaaminen
- varmenneauktoriteetti
- laitteiden tyypin tunnistaminen
- laitteiden tilan tarkistaminen
- vierasportaali
- ulkopuolisten laitteiden turvattu verkkoon rekisteröinti ja liittäminen
- reaaliaikainen verkonvalvonta
- lokitiedostot
- korkea käytettävyys usean ClearPass-palvelimen kesken.

Suurin ClearPassin komponentti on ClearPass Policy Manager, josta löytyy valtaosa toiminnallisuudesta mukaan lukien ClearPass OnGuard, joka vastaa laitteiden tilan tarkastuksesta. ClearPass Onboard vastaa ulkopuolisen laitteden verkkoon liittämisestä, ja ClearPass Guest taas vierasportaalista. Sekä ClearPass Onboardia ja Guestia hallinnoidaan erillisestä Web GUI:sta kuin Policy Manageria, mikä

monimutkaistaa hieman asioita. MDM, eli Mobile Device Management on toistaiseksi mahdollista vain API:n, eli Application Programming Interfacen kautta.[34, s. 10; 35, s. 1.]

Palvelu

Service eli palvelu on ClearPassin suurin elementti, jonka tarkoituksena on luokitella pääsyoikeudet verkon todennustavan (esim. langaton 802.1X, vierasportaali, Onboard-toiminnallisuus) sekä laitteen ja tähän liittyvän käyttäjätilin ominaisuuksien mukaan.

Verkkoon liittyvän päätelaitteen palvelu tunnistetaan osumista Service Rule-listaan. Laite liitetään palveluun, mikäli sen todentamispyynnön tuntomerkit täyttävät Service Rulen vaatimukset.

Palvelun alle kuuluvat seuraavat toiminnot:

- todentaminen
- tietojen kerääminen käyttäjätietokannasta
- laitteen tilan tarkastus
- roolien sijoitus
- laitteen oikeuksien määrittely
- laitteen oikeudet määräävän profiilin sijoittaminen laitteelle.

Tavanomaisimmat palvelut löytyvät valmiina oletusprofiileina ClearPassin asennuksen jälkeen. Kaikki palveluun sisältyvät toiminnot ovat myös muokattavissa ja vaihdettavissa palvelun sisältä. [36, s.81-95.]

Todentaminen ja pääsyn salliminen

Todentaminen koostuu kahdesta osiosta, todennustavasta sekä käyttäjätietokannasta. Todennuksessa voidaan käyttää tavallisimpia 802.1X todennusprotokollia (EAP, PEAP-MSCHAP jne.), MAC-osoitteella todennusta tai ClearPassin web-portaalia.

Lähetettyjä todennustietoja verrataan sitten palvelussa määriteltyyn käyttäjätietokantaan tai -kantoihin. Täältä kerättyjä lisätietoja käyttäjästä, esimerkiksi AD:n eli Active Directoryn ryhmäjäsenyyttä voidaan käyttää myös perusteena pääsyn sallimiseen haluttuihin verkon resursseihin. [36, s.104.]

Tuetut käyttäjätietokannat ovat:

- Active Directory
- lightweight Directory Access Protocol-tietokanta
- Kerberos
- open Database Connectivity-yhteensopiva SQL-tietokanta
- token-palvelin, esim. RSA SecurID
- sisäinen tietokanta
- HTTP, eli Hypertext Transfer Protocol

Mikäli todennus ei onnistu yhteenkään palvelussa määriteltyyn käyttäjätietokantaan, kielletään käyttäjän pääsy verkkoon. [36, s. 101,117-118.]

Roolisijoitukset

Laitteelle sijoitetaan Role eli rooli sen täyttämien kriteerien mukaan. Nämä kriteerit kerätään käyttäjätietokannoista tai muista verkosta kerätyistä lähteistä. Rooli on siis eräänlainen kooste täytetyistä kriteereistä. Mikäli mitään kriteereitä ei täytetä, laitteelle määritetään oletusrooli. Yhdelle laitteelle on myös mahdollista sijoittaa useampi rooli, mikä se täyttää useamman roolin kriteerit.Roolit ovat yksi peruste, jolla sijoitetaan lopullinen verkkopääsyn profiili, eli Enforcement Profile. [36, s.139.]

Oikeuksien määrittely

Enforcement Policyn eli laitteen oikeuksien määrittelyn mukaan tehdään viimeinen päätös laitteen pääsyoikeuksista. Muuttujat, joiden mukaan päätös tehdään, ovat

laitteen tila (Posture), sille sijoitetut roolit sekä ClearPassiin konfiguroitu kellonaika ja päivämäärä. Enforcement Policyja voi olla vain yksi joka palvelussa. Lyhyesti ilmaistuna kyse on listasta ehtoja, joiden täyttyessä laitteelle sijoitetaan Enforcement Profile. [36, s.189.]

Enforcement Profile

Enforcement Profile eli laitteen oikeuksien profiili on lista attribuutteja, jotka ClearPass lähettää NAS:ille, jonka jälkeen laitteella on käytettävissään palvelussa määritellyt oikeudet. Nämä voivat olla muotoa RADIUS, TACACS (Terminal Access Controller Access-Control System), SNMP (Simple Network Management Protocol) ohjelmakohtainen (esim. Aruban Guest Access), RADIUS CoA eli Change of Authorization. Enforcement Profilelle määritellään myös laitetyypit, joiden kanssa se on käytettävissä. [36, s.190.]

Clearpass Profile

ClearPass Profile on tärkeä BYOD-elementti, jolla pystytään tunnistamaan päätelaitteen tyyppi. Tämän informaation perusteella verkkoon liittyvälle päätelaitteelle pystytään antamaan oikeanlainen ohjeistus ja ohjelmisto sekä pääsy organisaation verkkoon. Tämä helpottaa myös verkonvalvontaa. Profilointitasoja on kolme ja ne esitellään taulukossa 1.

Taulukko 1. ClearPass Profilen profilointitasot.

Profilointitaso	**Tarkkuus**	**Esimerkki**
DeviceCategory	pieni	Tietokone, printteri, älypuhelin
DeviceFamily	keskiverto	Windows, Linux, Android, Apple
DeviceName	suuri	Windows 7, Mac OS X 10.5

Sovellus kerää myös muita tietoja, kuten IP-osoitteen, MAC-osoitteen OUI:n eli Organizational Unit Identifierin (laitevalmistajan tiedot), laitteen isäntänimen sekä ajat, milloin laite ensimmäisen kerran tunnistettiin, ja milloin se on viimeksi havaittu

verkossa. ClearPass Profile hyödyntää useita eri verkkoelementtejä profiloinnissa, näitä ovat

- DHCP
- ClearPass Quickconnect-ohjelma päätelaitteilla
- HTTP-käyttäjäagentti ClearPass Guest- tai Onboard-komponentin kautta
- MAC-osoitteen OUI. MAC-osoite hankitaan joko 802.1X tai MAC-todennuksen kautta.
- Activesync-plugin, Exchange-palvelimelle asennettava liitännäinen
- ClearPass Onguard-agentti päätelaitteella
- SNMP
- Subnet Scanner, joka skannaa halutun aliverkon ja jatkaa löydettyjen IP-osoitteiden profilointia SNMP:n avulla.

Komponentti käyttää sisäänrakennettuja sääntöjä ja Aruban päivittyvää julkista tunnistetietokantaa profiloidakseen laitteet. ClearPass Profilen toiminta on hallinnoijalle lähes näkymätöntä, eikä vaadi juuri toimenpiteitä ylläpitoon. [36, s.55-58.]

Clearpass Onboard

Clearpass Onboard liittää organisaation ulkopuoliset laitteet turvallisesti verkkoon käyttäen 802.1X- tai PSK-todennusta. Tämän lisäksi Onboard pystyy muokkaamaan Onboarding-prosessin yhteydessä Windowsin verkkoasetuksia, Android- tai iOs laitteen välityspalvelinasetuksia, tai iOS-laitteen Passcode Policy, Exchange ActiveSync ja VPN-asetuksia.

Pääsy verkkoon määritellään laitekohtaisesti, mikä tarkoittaa että yksittäiset laitteet voidaan poistaa verkosta ilman ongelmia käyttäjätilien kanssa. Koska tämä perustuu laitekohtaisiin, yksilöllisiin varmenteihin, tämä ei ole mahdollista PSK-todennusta

käytettäessä. Myös provisioitujen laitteiden määrää per käyttäjä voidaan rajoittaa. [37, s.5.]

Tuetut käyttöjärjestelmät ovat Windows, Mac OS X, iOS ja Android. Tuetut järjestelmät voidaan jakaa kahteen kategoriaan, Onboard-Provisioningiin ja Over-The-Air-Provisioningiin. Näistä jälkimmäinen vaatii vain minimaaliset toimet loppukäyttäjältä. Jos laite ei ole Over-The-Air-Provisioning-yhteensopiva, tarvitsee siihen ladata erillinen Aruba Quickconnect-sovellus Onboarding-prosessin aikana. Todennuksen aikana laite saa käyttöönsä laitevarmenteen ja tarvittavat parametri verkkoon liittymiseen. Mikäli laite poistetaan verkosta, voidaan varmenne merkitä vanhentuneeksi tai poistaa kokonaan. Taulukossa 2. esitellään eri käyttöjärjestelmien provisiointitavat.

Taulukko 2. Clearpass Onboardin tukemat käyttöjärjestelmät langattoman verkon käytössä

Käyttöjärjestelmä	**Tuetut versiot**	**Provisiointitapa**
Microsoft Windows	XP, Vista ja 7	Onboarding
Apple iOS	4.x ja eteenpäin	Over the air
Apple Mac OS X	10.5 – 10.6	Onboarding
	10.7 ja eteenpäin	Over the air
Android	2.2 ja eteenpäin	Onboarding

Integrointi Clearpass Profilen kanssa johtaa siihen, että käyttöjärjestelmä ja laitetyyppi voidaan myös tunnistaa provisionnin aikana automaattisesti. Tämän perusteella voidaan varmistaa, että verkkoon liittyvä laite provisioidaan oikeilla parametreillä ja sille määritellyillä oikeuksilla. [37, s.8.]

ClearPass Onboard toimii CA:na, eli Certificate Authorityna joko Intermediate- tai Root-roolissa. Tuetut protokollat varmenteiden tarkastamiseen ovat sekä CRL (Certificate Revocation List) että OCSP (Online Certificate Status Protocol). Myös kaikki muut CA:lle tavanomaiset varmennetoiminnot ovat saatavilla.[37, s.9.]

ClearPass Onboardin vaatimukset olemassaolevalle WLAN-infrastruktuurille ovat

- Captive Portal-tuki

- luotettu SSL-varmenne ClearPass Onboard-palvelimella
- EAP-TLS- ja MSCHAPv2 -todennusmetodit ovat tuettuja verkossa
- CRL tai OCSP-protokolla tuettuna verkossa.

[37, s.11.]

Clearpass Guest

ClearPass Guest on komponentti väliaikaisten verkkotunnusten luomiseen vieraille, konsulteille tai muille toimintoa tarvitseville henkilöille ja laitteille. Muokattavissa olevat operaattoriprofiilit antavat vähemmän teknisille henkilöille, esimerkiksi aulatyöntekijöille tarvittavat työkalut vierastunnusten luomiseen ja hallinnointiin halutulla tasolla.

Vieraat eivät verkkoon liittyessään pääse kuin Captive Portaliin eli käyttäjän eristämiseen tarkoitettuun web-portaaliin. Tästä käyttäjä pääsee eteenpäin vain syöttämällä sivulle aikaisemmin saadut vierastunnuksensa. Vieraille voidaan tunnusten luomisen aikana asettaa eri rooleja, jotka antavat eri oikeudet verkossa.

Muita huomattavia ominaisuuksia ovat vieraille näkyvän web-portaalin vapaa muokkaus, vieraiden todennus MAC-osoitteella tai MAC-osoitteen ja vierastunnusten yhdistelmällä, vierastunnusten luomisen salliminen vieraille hallinnoijan luvalla tai ilman, Aruba Airgroup-integraatio, sekä vierastilien ClearPassiin tuominen ja sieltä vieminen HTML-, teksti-, CSV-, TSV- tai XML-tiedostoina.[38.]

Laitteiden tarkastus

ClearPass Policy Manager tukee kolmea eri tapaa laitteiden tilan tarkastamiseen ja parantamiseen:

- Laitteen tilan tarkastussäännöt Windows-, Linux ja Mac OS X OnGuard-agenttien avulla. Tarkastustulosten perusteella arvioidaan voidaanko laite liittää verkkoon. Toiminnalisuus esitellään taulukossa 3.

- Laitteen tilan tarkastukseen käytetyt palvelimet, ClearPass tukee Microsoft NPS-, eli Network Policy Server-palvelimen integraatiota, joka suorittaa Statement of Health-toimintoa Windowsin sisäisten NAP, eli Network Access Protection-agenttien kanssa.

- Auditointipalvelimet, joista tuettuina sekä NMAP, eli Network Mapper, että Nessus. Auditointituloksia voidaan käyttää perusteena pääsyroolien antamiseen laitteille. Nessuksen kautta saadaan selville myös laitteen haavoittuvuudet. Käytetään yleensä, jos laitteelta ei löydy liitännäisohjelmistoja posturoinnin tarkastamiseen.

Taulukko 3. ClearPassin suorittamat laitteen tilatarkastukset ja korjaukset (Posture).

Tarkistus	**Onguard Windows**	**Onguard Mac OS X**	**OnGuard Linux**	**Windows NAP-agent**
Laitteen tilan tarkastukset, X = tarkistus, Y = korjaustoimenpide				
Käyttöjärjestelmän versio ja päivitykset	X/Y			X/Y
Ohjelman versio ja päivitykset	X/Y			
Prosessi / Palvelu	X/Y		X/Y	
Rekisteri	X/Y			
Tiedosto	X/Y			
Applikaatio	X/Y			
Peer to Peer	X/Y			
USB-muisti	X/Y			
Virtuaalikoneet	X/Y			
Antivirus + versio + päivitykset	X/Y	X/Y		ei versio /Y
Antispyware + versio + päivitykset	X/Y	X/Y		ei versio /Y
Palomuuri + versio	X/Y	X/Y		vain prosessi /Y
Windows Update käytössä + asetukset				X/Y

Jokainen näistä tarkastuksista voi antaa yhden seuraavista tiloista:

- Healthy – laite läpäisi tarkastuksen.
- Checkup – laite läpäisi tarkastuksen, mutta tarvitsee päivityksen. Voidaan käyttää proaktiiviseen tilan parannukseen.
- Transient – tarkastus on kesken.
- Quarantine – laite ei läpäissyt testiä, jolloin pääsy rajataan palvelimiin jotka parantavat laitteen tilaa.
- Infected – laitteella on haittaohjelma. Pääsy verkkoon tulee estää, tai ainakin rajata tarkasti.
- Unknown – laite on tuntematon.

[36, s.151-152.]

Laitteen tarkastus tapahtuu NAP-agentilla. Mikäli käyttöjärjestelmästä ei oletuksena löydy NAP-agenttia, CPPM käyttää erikseen asennettavaa ClearPass OnGuardia. Tämän ominaisuudet ovat huomattavasti laajemmat kuin käyttöjärjestelmien oletusagentit, joten OnGuardin käyttö on suositeltavaa.

Sisäänrakennettu agentti löytyy suurimmasta osasta Microsoftin Windows-käyttöjärjestelmistä sekä muutamista Linux-distribuutioista, kuten CentOS, Fedora, Red Hat sekä SUSE. Mac OS X:n kanssa näin ei tosin ole, joten agentti pitää erikseen asentaa verkkoon liittymisen yhteydessä. OnGuard voidaan asentaa verkkoon liittyessä joko pysyvänä tai väliaikaisena agenttina. Jälkimmäistä voi käyttää esim. vierasportaalin kanssa.

Mikäli laitetarkistussääntöjen tarkastus tuottaa ei-halutun tuloksen, voidaan laitteelle suorittaa parannustoimenpide. Vaihtoehtona on myös käyttäjälle lähetettävä ohje tai linkki laitteen tilan korjaamiseksi [36, s.153-155.]

Mikäli Microsoft NPS-integraatio otetaan käyttöön, kaikki säännöt sekä niiden tarkastukset delegoidaan kyseiselle palvelimelle. Tarkastuksen jälkeen Microsoft NPS lähettää ClearPassille tarkastuksen tulokset käsiteltäviksi. [36, s.176.]

Auditointipalvelimet ovat vaihtoehto, mikäli laitetarkastusta tehdään laitteelle, joka ei tue NAP-agentteja, esimerkiksi vanhempi Windows-versio, tai jos laite tukee vain MAC-todennusta. ClearPassissa on sisäänrakennettuna NMAP- sekä Nessus-palvelin (Versio 2.X), mutta myös erilliset palvelimet ovat käytettävissä, Nessuksen tuetut versiot ovat 2.X ja 3.X.

Auditointipalvelimien tulee tietää laitteen IP-osoite ennen auditointia. Tämä voidaan tosin selvittää ClearPassin DHCP snooping -palvelulla.

NMAP-auditoinnin tulokset palauttavat aina tuloksen ’Healthy’, mutta kerättyjä tietoja voidaan käyttää auditoinnin jälkeisissä roolisijoitussäännöissä. Nessus taas palauttaa aina ’Healthy’ tai ’Quarantine’ tuloksen. [36, s.179-180.]

7.1.2 Vahvuudet ja heikkoudet

Aruban ratkaisu on hyvin kokonaisvaltainen, muokattavissa ympäristön tarpeisiin sekä skaalautuva. ClearPassin toteutuksesta kuitenkin näkee, että se on rakennettu useasta eri komponentista. ClearPassin sovellukset ClearPass Guest ja Onboard ovat oma kokonaisuutensa, joka on erikseen integroitu muiden ominaisuuksien kanssa. Mikäli kaikki ClearPassin osa-alueet olisi alun perin rakennettu toimimaan toistensa kanssa, olisi kokonaisuus huomattavasti selkeämpi ja toiminnaltaan luultavasti vielä nykyistä tasoakin parempi.

Ongelmaksi jää myös Onguard-clientin puute mobiililaitteista, jolloin näiden liittäminen verkkoon laitteen tilaan liittyviä kriteereitä käyttäen ei onnistu. Tämä lienee mahdollista toteuttaa MDM-integraatiota käyttäen, joka tosin on vasta tulevassa ClearPassin versiossa suoraan toteutettavissa. [39.]

Integraatio olemassa olevan infrastruktuurin kanssa näyttää erinomaiselta, eikä ominaisuuksia näytä juuri puuttuvan, oli käytössä sitten Aruban tai muun valmistajan WLAN-kontrolleri tai tukiasema. Tietenkin Aruba osaa parhaiten hyödyntää omaa

teknologiaansa, mutta yleisnäkymältä tilanne on hyvä. Lisätoiminnallisuutta tarjoavat vielä tietoturva-auditointiin tarkoitettujen palvelinohjelmistojen sekä Microsoftin NPS-palvelimen integrointi. Korkea käytettävyys useiden ClearPass-palvelimien kesken helpottaa sen suosittelemista suurempiinkiin verkkoympäristöihin.

7.2 Cisco

Cisco on vuonna 1984 perustettu monikansallinen yhtiö, joka tuottaa tietoverkkolaitteita sekä -palveluita. Ciscon valmistamat laitteet käsittävät reitittimiä, kytkimiä, IP-puhelimia, palomuureja ja paljon muuta. Yhtiöllä on myös oma arvostettu sertifiointiohjelmansa.[47, s.1-9.]

7.2.1 Cisco Identity Services Engine

Kuten Aruban ClearPass, Cisco Identity Services Engine (tästä eteenpäin ISE) on keskeisin osa Ciscon BYOD WLAN-ratkaisua, jossa suurin osa toiminnallisuudesta tapahtuu. ISE integroidaan verkkoon konfiguroimalla se RADIUS- ja Captive Portal-palvelimiksi paikallisille WLAN-kontrollereille, jonka jälkeen se suorittaa kaikki tarvittavat päätökset verkkoon pääsystä ja oikeuksista. ISE on saatavilla sekä fyysisenä laitteena, että VMware-virtuaalipalvelimena. [48.]

ISE:n ominaisuuksiin kuuluvat

- todennus
- pääsyoikeuksien hallinnointi
- laitteiden tyypin tunnistaminen
- ulkopuolisten laitteiden turvattu verkkoon liittäminen
- laitteen tilan tarkastus
- vierasportaali

- reaaliaikainen verkonvalvonta
- lokitiedostot
- korkea käytettävyys kahden ISE-palvelimen kesken.

Todennus

Cisco ISE:n Authentication Policyt, eli todennussäännöt koostuvat kahdesta osasta: Network Access Service eli säännöstö todennuksessa käytettävistä metodeista sekä Identity Source eli käyttäjätietokanta. Todennuksessa voidaan käyttää tavallisimpia 802.1X-protokollia (EAP, PEAP-MSCHAPv2 jne.), MAC-osoitteella todennusta tai ISE:n web-portaalia. Käyttäjätietokantoina voivat toimia yksi tai useampi seuraavista:

- Cisco ISE:n sisäinen kanta käyttäjille sekä laitteille
- Active Directory
- Lightweight Directory Access Protocol-tietokanta
- RADIUS token-palvelin (esim. RSA)
- Konevarmenteet

Käyttäjältä voidaan myös käyttäjätilin lisäksi vaatia joitakin yleisiä tai käyttäjätietokannasta löytyviä attribuutteja, esim. tiettyyn AD-ryhmään kuulumista. Todennussääntöjä voidaan ketjuttaa peräkkäin jos useampia lähteitä tai metodeja halutaan käyttää. Mikäli käyttäjää ei onnistuta todentamaan yhdessäkään näistä, todennus epäonnistuu. [49.]

Pääsyn salliminen

Laitteiden pääsyoikeuksien salliminen Cisco ISE:ssä tehdään Authorization Policyissa. Näissä tarkistetaan tunnistetun laitteen Identity Groupit, eli laitetyypit, attribuutit sekä muut ehdot vapaasti rakennettavalla sääntölistalla, ja näiden mukaan laitteelle sijoitetaan Authorization Profile, joka sisältää verkon pääsyoikeudet RADIUS ACL- ja VLAN-muodoissa.

Authorization Policyn attribuuteissa tuetaan seuraavia laitevalmistajakohtaisia laajennettuja RADIUS-syntakseja:

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

Käyttäjälle voidaan sijoittaa yksi tai useampi Authorization Profile, tai vaihtoehtoisesti Exception Authorization Profile, joka sijoitetaan laitteelle välittömästi ilman tarkastuksia. Ohjeissa ei kuitenkaan mainita, mitä tapahtuu, jos kahdessa samalle laitteelle sijoitetussa Authorization Profilessa jokin tietty arvo, esimerkiksi sijoitettava VLAN eroaa. [50.]

Laitetyypin tunnistus

Cisco ISE tukee laitteiden tyypin tunnistusta useiden eri attribuuttien perusteella. Oletuksena näihin kuuluvat:

- DHCP
- MAC
- SNMP
- IP
- RADIUS
- SNMP
- Netflow v5-9
- CDP, Cisco Discovery Protocol
- LLDP, Link Layer Discovery Protocol

ISE:stä löytyy lähes kaikille näistä protokollista oma erillinen probe eli komponentti, joka tarkkailee ja selvittää laitteiden attribuutteja.

Profilointipalveluun sisältyy myös oletuksena profilointiehtoja tavanomaisimmille päätelaitteille. Nämä eivät kuitenkaan aina ole ajan tasalla, sillä ne päivittyvät samaa tahtia kuin ISE:n versio.

Profiloinnin keskeisin komponentti on Profiling Policy, joka pisteyttää laitteen Profiling Conditionien eli tunnistusehtojen perusteella. Mikäli laite kerää tarpeeksi pisteitä näitä ehtoja täyttämällä, voidaan se sijoittaa Identity Groupiin eli tiettyyn laiteryhmään, jolla on omat pääsyoikeutensa Authorization Policyn kautta. Tarvittavaa pistemäärää voidaan muokata halutun kokoiseksi.

Profiling Conditioniin sisältyy laitteelta kerätyn attribuutin tyyppi (esim. SNMP), nimi (esim. hostname), operaattori (esim. ”sisältää”) sekä arvo. Kokonaisuutena tämä siis testaa laitteen jonkin attribuutin arvoa halutulla operaattorilla.

Profiling Policy rakentaa tunnistusehdoista, operaattoreista ja näiden perusteella luoduista säännöistä sääntölistan, joiden mukaisesti se toimii. Yksittäisen säännön mukaan voidaan joko lisätä laitteen profilointipisteitä, suorittaa NMAP-skannaus tai siirtyä Profiling Policyssa määriteltyyn Exception Policyyn eli poikkeussääntöön.

Poikkeussäännöissä voidaan suorittaa laitteelle CoA eli Change of Authorization jolla voidaan esimerkiksi suoraan sijoittaa laite staattisesti johonkin laiteprofiiliin ilman pisteytystä. Laitteiden profilointi onnistuu myös NMAP-skannauksen perusteella. [51.]

Laitteen tilan tarkastus

Mikäli laitteen verkkopääsyyn halutaan asettaa tarkempia kriteereitä, voidaan siltä varmistaa posture- tai 802.1x-agentin, sekä sen tiettyjen komponenttien olemassaolo. Ominaisuuden voi asettaa globaalisti toimintaan tai pois toiminnasta.

Mikäli ominaisuus on käytössä, tarvitaan Provisioning Resource Policy, jossa määritellään käytetyt posture-agentit, sekä niitten suorittamat toiminnot. Agenttien toiminnallisuus, käytetty versio sekä ulkonäkö ovat melko laajasti muokattavissa. Provisioning Resource Policyn säännöissä voidaan määritellä, mitkä Identity Groupit saavat mitkäkin agentit käyttöönsä.

Cisco ISE käyttää laitteen tilan tarkastukseen Windowsilla ja Mac OS X:lla toimivaa Cisco NAC agent -ohjelmaa. Myös väliaikaista NAC Web-agenttia voidaan käyttää. Tämä tukee yleisimpiä selaimia Windowsilla, Mac OS X:lla sekä myös Red Hat- ja Ubuntu-Linux distribuutioissa. Epäviralliset WPA_Supplicant ja Open1X Supplicant Linuxille ovat myös käytettävissä Cisco ISE:n kanssa.

Laitteen tilatarkastukset ja korjaustoiminnot voidaan määritellä Client Posture Assesment Policysta. Tämä tehdään laitteen Identity Groupin ja käyttöjärjestelmän mukaan. Tarkastuksiin voivat koostua ISE:n keräämien laitteeseen liittyvistä muuttujista kootuista ehdoista sekä NAC-agentit suorittamista tarkastuksista asiakaslaitteella. Myös NAC-agenttiin sisäänrakennettuja korjaustoimenpiteitä on saatavilla, mikäli laite ei täytä kaikkia vaatimuksia. Taulukossa 4. esitellään agenttien tukemat ominaisuudet eri käyttöjärjestelmille.

Taulukko 4. Cisco NAC-agenttien ominaisuudet

Protokolla	**Windows NAC-agentti**	**MAC OS X NAC-agentti**	**Web NAC-agentti**
Laitteen tilan tarkastukset			
Käyttöjärjestelmän versio ja päivitykset	X		X
Prosessi	X		X
Rekisteri	X		X
Tiedosto	X		X
Applikaatio	X		X
Antivirus + versio + päivitykset	X	X	X
Antispyware + versio + päivitykset	X	X	X
Windows Update käytössä + asetukset	X	X	X
WSUS-asetukset	X		X
Korjaustoimenpiteet			
Viesti käyttäjälle	X	X	X

Linkki sivustolle	X	X	X
Tiedostonjako	X		
Ohjelman käynnistys	X		
Antiviruksen päivitys	X		
Antispywaren päivitys	X		
Windows Update	X		
WSUS	X		

Laitteen tilatarkastuksen jälkeen käyttäjälle voidaan näyttää Posture Acceptable Use Policy, eli ehdot verkkoon liittymiseen. Cisco ISE tarkastaa halutuin aikavälein asiakaslaitteen tilan. Mikäli tämä ei ole hyväksytty, voidaan laitteelle suorittaa korjaustoimenpide posture-agentin toimesta, katkaista yhteys tai jatkaa yhteyttä ilman jatkotoimenpiteitä [52.]

On-Boarding ja My Devices Portal

Organisaation ulkopuolisten laitteiden yhdistäminen verkkoon voidaan tehdä joko suoraan laitteelta (On-Boarding), tai sitten laitteen tiedot tulee etukäteen lisätä organisaation käyttäjän henkilökohtaiseen My Devices Portaliin.

On-Boarding onnistuu Provisioning Resource Policyn alaluokasta Native Supplicant Profile. Täällä määritellään tuetut käyttöjärjestelmät sekä todennusmetodit. Mikäli laitteen käyttöjärjestelmälle tehdään profiili, voi käyttäjä rekisteröidä laitteensa omilla tunnuksillaan, ja joko käydä läpi 802.1x-agentin,asetusten ja varmenteen ohjeistetun asennuksen tai tehdä sen manuaalisesti riippuen ISE:n asetuksista.

Laitteen rekisteröinti verkkoon liittämisen jälkeen tapahtuu Self-provisioning portaalissa, missä käyttäjä lisää laitteen MAC-osoitteen sekä lyhyen kuvauksen laitteesta (esim. ”Android”).

Toinen vaihtoehto on My Devices Portal, erillinen portaali johon käyttäjät kirjautuvat organisaation omistamalta laitteelta. Kirjautumisen jälkeen käyttäjät pystyvät rekisteröimään henkilökohtaisen laitteensa kuten Self-provisioning portaalissa. Kun laite on lisätty, siirtyy se ”Pending...”-tilaan, kunnes uusi laite on onnistuneesti liitetty

verkkoon. Laitteet voi myös lisätä Blacklistiin eli kiellettyjen laitteiden listaan, jolloin ne eivät voi liittyä verkkoon ennen kiellon poistoa. Tämä on hyödyllistä, jos laite on vaikkapa kadonnut. [53.]

Guest Service

Cisco ISE sisältää web-portaalin vieraskäyttäjien todennukseen. Todennus tapahtuu väliaikaisilla vierastunnuksilla, joita voidaan luoda ja hallinnoida ISE:n hallinnasta erillisestä vierasportaalien hallinnoijien web-portaalista. Vierasportaalin hallinnoijia voi olla useita oikeuksiltaan eritasoisia ryhmiä ja käyttäjiä. Vierastilien oikeusia, tunnusten alkamisaikaa, käyttöaikaa ja muita ominaisuuksia voidaan hallinnoida reaaliaikaisesti näillä tileillä.

Vieraat voidaan laittaa hyväksymään Acceptable Use Policy, eli käyttöehdot. Vieraille annetaan myös mahdollisuus rekisteröidä omat laitteensa Device Registration Web-Auth Portalin kautta, muuttaa salasanansa, sekä myös luoda omat käyttäjätunnuksensa. Jälkimmäisen osalta ei näy juurikaan olevan tarkempia ominaisuuksia, esim. sponsorin hyväksynnän vaatiminen. Portaalien käyttämät html- ja kuvatiedostot ovat muokattavissa. [54.]

7.2.2 Vahvuudet ja heikkoudet

Cisco on sisällyttänyt ISE:een suuren määrän ominaisuuksia, jotka kaikki ovat hallinnoitavissa samasta sijainnista. Cisco ISEn konfiguraation rakenne ei ole aluksi erityisen selkeä, mutta eri asetusten määrä kertoo toiminnallisuuden muokattavuudesta. ISE vaikuttaa kokonaisvaltaiselta, mutta haastavalta ja huolenpitoa vaativalta ratkaisulta.

Laitteiden tunnistuksessa on olemassa valmiita profiileja, mutta ongelmana on näiden päivittäminen: Oletusprofiilit päivittyvät ISEn mukana, ja vaihtoehtoisesti laitteiden tunnistuksessa käytettävät säännöt ovat manuaalisesti luotavissa hallinnoijan toimesta. Kumpikin näistä vaihtoehdoista vaatii kuitenkin palvelun hallinnoijalta toimia. Uudet laitteet sekä vanhojen ohjelmistopäivitykset saattavat aiheuttaa tunnistussääntöjen tai ISE:n toistuvaa päivittämistä.

Laitteiden tilatarkastukset eivät ole erityisen kattavia, eikä näitä tueta mobiililaitteissa. Myös ISE:lle on luvattu MDM-integraatiota tulevaisuudessa, mutta toistaiseksi tämä toiminnallisuus ei ole saatavilla. ISE:n uskoisin toimivan parhaiten keskikokoisessa ei-standardissa ympäristössä, joka vaatii tarkemmat määrittelyt verkon toiminnoille.

7.3 Packetfence

Packetfence on GPL:n alainen Open Source NAC -ratkaisu 802.11 WLAN-integraatiolla sekä BYOD-ominaisuuksilla. Ratkaisu yhdistää monia olemassa olevia Open Source- sekä ilmaisohjelmistoja, kuin myös olemassa olevaa verkkoinfrastruktuuria. Packetfencen toteutukseen löytyy tarvittaessa myös kaupallinen tuki sen kehittäjiltä.

7.3.1 Packetfencen ominaisuudet

Packetfence tukee seuraavia Linux-käyttöjärjestelmiä 32- tai 64-bittisinä versioina:

- Red Hat Enterprise Linux 5.x/6.x Server
- Community ENTerprise Operations System (CentOS) 5.x/6.x

Toiminta on mahdollista muissakin Linux-distribuutioissa kuten Debianissa, Fedorassa ja Gentoossa.

Ilmoitetut ominaisuudet ovat

- langattoman verkon integraatio
- organisaation ulkopuolisten laitteiden verkkoon liittäminen.
- epäilyttävän toiminnan tunnistus Snort NIDS, eli Network Intrusion Detection-ohjelman avulla
- ongelmalaitteiden eristäminen
- laitteen skannaus haavoittuvuuksien varalta Nessuksella tai OpenVASilla
- laitteen tarkistus Microsoftin Statement of Health-protokollaa käyttäen
- captive Portalin kautta suoritettavat korjaustoimenpiteet asiakaslaitteelle

- VLAN- ja rooliperusteinen verkkopääsy
- vierasportaali
- laitetyypin verkkopääsyn automaattinen testaaminen, salliminen tai estäminen
- kaistankäytön valvonta
- laitteiden ryhmitys varapalvelin-toiminnallisuuteen
- vapaan lähdekoodin sovelluksina helposti muokattavissa
- korkea käytettävyys Linux-HA-ohjelmiston avulla.

[40;41.]

Packetfencen käyttämiä ilmais- ja Open Source -ohjelmistoja ovat:

- Apache
- Snort
- Suricata
- Netflow/IPFIX
- Net-SNMP
- FreeRADIUS
- Nessus
- OpenVAS

[42, s.7.]

Muista ratkaisuista eroten Packetfence käyttää vain asiakaslaitteiden käyttöjärjestelmistä jo valmiiksi löytyviä komponentteja, eikä sisällä lainkaan asiakasohjelmia päätelaitteiden tilan tarkastamiseen. Suuri vastuu toiminnasta sijoitetaan NAS:eille, sillä Packetfence oletusominaisuuksillaan käyttää RADIUS:ta tai SNMP:tä sijoittaakseen NAS:ilta jo löytyvän VLANin tai roolin käyttäjälle. [43.]

Merkittävin ominaisuus verrattuna muihin BYOD WLAN-ratkaisuihin on Snortin tai Suricatan integrointi NIDS, eli Network Intrusion Detection System-komponentiksi . Molemmat tarjoavat IDS/IPS:ää, eli Intrusion Detection/Prevention System-ominaisuutta sisäverkkoon, joka havaitsee ja estää kiellettyt toiminnot sekä haittaohjelmaliikenteen. Näistä Snortin päivitys onnistuu automaattisesti. Ohjelmien

aiheuttavan kuormituksen vuoksi on suositeltavaa ajaa näitä palveluita omilla alustoillaan. [42, s.42-46.]

Langattomien laitteiden yhteensopivuus

Koska Packetfence on Open Source -ratkaisu ilman suoraa tukea kolmannen osapuolen laitevalmistajilta, voi yhteensopivuus tulla päällimmäiseksi mieleen BYOD WLAN -ratkaisua harkitessa. Ilmoitettu lista tuetuista WLAN-kontrollereista on kuitenkin huomattavan laaja. Packetfence integroidaan näihin RADIUS- ja Captive Portal -palvelimena.

Huomioitavaa on, että kaikki tuetun WLAN-kontrollerin tukemat ja käyttämät langattomat tukiasemat ovat tätä kautta myös Packetfencen käytettävissä. Tuettujen laitteiden määrä on myös jatkuvassa kasvussa. [44.]

Todennus ja pääsyn salliminen

FreeRADIUS-moduli suorittaa Packetfencen 802.1X-toiminnot. Se tukee tavanomaisimpien tunnistusmetodien lisäksi huomattavaa määrää EAP-tyyppejä todennuksessa, oman wiki-sivustonsa mukaan eniten sekä kaupallisessa että Open Source -maailmassa. [45;46.]

WPA-Enterpriseä käytettäessä käyttäjä todennetaan RADIUS-palvelimelle jollakin vaadituista EAP-metodeilla, jonka jälkeen RADIUS tarkastaa vastaanotetut tiedot (esim. AD-tunnus, varmenne) ja vertaa näitä konfiguroituihin identiteettilähteisiinsä. [42, s.95-96.]

WPA-Enterprisen lisäksi todentaminen onnistuu tietenkin myös WPA-PSK- sekä Captive Portalin kautta. Jälkimmäisen ominaisuudet käydään läpi myöhemmissä kappaleissa.

Todentamisen jälkeen RADIUS oikeuttaa käyttäjän VLANiin tai NASin konfiguraatioista löytyvään käyttäjärooliin haluttujen muuttujien perusteella. Packetfence ei oletuksena käytä hyväkseen FreeRADIUS-modulin mahdollisuutta lähettää asiakaslaitteiden

käyttöön ACL- tai QoS-parametreja, joten vastuu käyttäjän pääsyoikeuksista jää NASin hoidettavaksi. [43.]

OAuth2-todentaminen

OAuth2, eli Open Authentication 2 integraatio mahdollistaa käyttäjän todentamisen käyttäjän Facebook-, Github- tai Google-tilin kautta. Oauth2-todentaminen on web-portaalin asetus. [42, s.61.]

Kirjaaminen ja laskutus

Käyttäjän kuluttamaa kaistaa ja verkossa käytettyä aikaa voidaan valvoa FreeRADIUS-komponentin avulla. Näille voidaan myös asettaa rajat, joiden ylittyessä käyttäjälle suoritetaan jokin toimi, vaikkapa eristys-VLANiin sijoitus. Kaistan määrä voidaan mitatata suunnan mukaan (sisään- tai ulospäin), tai sitten näiden summana.

Packetfence tukee myös verkkoon pääsyn laskutusta http://www.authorize.net-sivuston kautta. Integraatio tukee useamman muokattavan pääsytyypin valintaa oston yhteydessä. Authorize.net-integraatio on web-portaalin asetus. [42, s.48, 59.]

Ulkopuolisten laitteiden verkkoon rekisteröinti ja liittäminen

Mikäli käyttäjää tai laitetta ei tunnisteta, asetataan asiakaslaite rekisteröimättömien laitteiden VLANiin/rooliin, jossa käyttäjät voivat rekisteröidä laitteita tunnuksillaan Captive Portalin kautta. Laitteen rekisteröinnin yhteydessä sen tyyppi ja haavoittuvuudet voidaan arvoida Nessus- tai OpenVAS-integraatiota käyttäen ja sijoittaa se haluttuun VLANiin tai rooliin tämän perusteella. Kun laite on kertaalleen rekisteröity, lisätään se sisäiseen tietokantaan, jonka jälkeen sitä ei tarvitse rekisteröidä toista kertaa verkkoon uudelleen liityttäessä.

Erillinen portaalin ominaisuus löytyy myös pelikonsolien rekisteröinnille. Laitteet voi rekisteröidä tietylle käyttäjälle MAC-osoitteen perusteella. Packetfence tunnistaa automaattisesti konsolin tyypin MAC OUIn perusteella. [42 s.3, s.62.]

Vierasportaali

Vierasportaali on oletusasetuksilla saatavilla samassa VLANissa tai roolissa kuin laitteiden rekisteröinti. Täältä käyttäjien on mahdollista luoda omat tunnuksensa, anoa tunnuksia ja kirjautua sisään riippuen Packetfencen asetuksista. Vierasportaali on myös mahdollista avata internetiin päin, jolloin vieraat voivat anoa tunnuksia ennen paikalle saapumista. Anotut tunnukset hyväksytään erikseen vierasportaalin hallinnoijan toimesta, tai sallitaan automaattisesti. Vierastunnukset voidaan lähettää joko tekstiviestillä tai sähköpostitse.Vieraille voidaan tietenkin asettaa halutut VLANit tai roolit, aikarajoitukset ja aloitusajat.

Kuten muissakin BYOD WLAN -ratkaisuissa, vierasportaalille voidaan luoda omat hallinnoijansa, joilla ei ole pääsyä Packetfencen muihin ominaisuuksiin. Portaalin hallinnoijien oikeuksia voi myös muokata tarkemmin, esimerkiksi vieraskäyttäjien tunnusten käyttöajan voi rajata vain tiettyihin vaihtoehtoihin.

Mahdollisuus on luoda yksittäisiä tai useampia käyttäjiä kerralla. Myös vierastililistan luominen CSV-tiedostosta on mahdollista. [42, s.52-56.]

Laitteiden eristäminen

Käyttäjät voidaan myös tarvittaessa siirtää eristys-VLANiin, josta on pääsy vain tiettyihin resursseihin, esimerkiksi Remediation Portaliin, missä käyttäjälle annetaan keino tai ohjeita korjata käytetyn laitteen verkon standardien mukaiseksi sekä ainoastaan tähän tarpeelliset oikeudet. Optimaalista olisi konfiguroida VLAN yksityiseksi, jolloin saman VLANin jäsenet eivät pysty kommunikoimaan toistensa kanssa. Näin esimerkiksi haittaohjelmat eivät pääse leviämään. [42, s.34.]

Syitä eristykseen voivat olla esimerkiksi Windows Statement of Health -tarkastuksen epäonnistuminen, Nessus- tai OpenVAS-skannauksen tunnistama haavoittuvuus tai ei-haluttu laitetyyppi, Snortin verkkoliikenteestä havaitsema haittaohjelmatartunta tai kielletty toiminto, esimerkiksi P2P-liikenne.

Nessus- ja OpenVAS -integraatio

Nessusta tai OpenVAS:ia käytetään laitteiden tyypin ja haavoittuvuuksien havaitsemiseen. Skannaus laitteille voidaan suorittaa rekisteröinnin yhteydessä,

halutuin aikavälein tai Snort-tapahtuman perusteella. Skannausten tulosten perusteella voidaan laite sijoittaa eristys-VLAN:iin tai -rooliin.

Laitteiden tunnistukseen käytetään seuraavia keinoja:

- DHCP-sormenjälki
- selaimen User Agent, joka sisältää selain- ja käyttöjärjestelmätyypin
- MAC-osoite.

Nessus tai OpenVAS voidaan asentaa samalle fyysiselle tai virtuaaliselle alustalle kuin Packetfence, mutta suositeltavaa on käyttää näitä erillisinä palvelimina näiden aiheuttaman kuormituksen perusteella. [42, s.46-48.]

Statement of Health

Packetfencen Statement of Health -moduuli hyödyntää Microsoftin Windows-käyttöjärjestelmistä, XP SP2:sta eteenpäin löytyvää Network Access Protection -palvelua. Tämä pystyy välittämään tiedon laitteen Windows Update-, antivirus- ja palomuuri -ohjelmiston tilanteen SoH-protokollaa tukevalle palvelimelle.

Näiden tietojen perusteella asiakaslaitteita pystytään sijoittamaan haluttuin VLAN:eihin/rooleihin Packetfencessä ja ilmoittaa korjaustietoja Remedation Portalin kautta. [42, s.56-57.]

7.3.2 Vahvuudet ja heikkoudet

Packetfence eroaa ominaisuuksiltaan muista BYOD:ia toteuttavista NAC:eista siinä, että huomattava määrä vastuuta asetetaan NAS-laitteiden VLAN-, SNMP- ja rooliasetuksiin ja -ominaisuuksiin. Packetfencen integraatio verkkoon vaatii siis huomattavan määrän konfiguraatiota NAS-laitteille sen omien asetusten muokkaamisen lisäksi.

Päätelaitteiden tilan tarkistus on siirretty täysin Microsoftin Statement of Health -protokollalle sekä erillisille auditointi- ja NIDS-palvelimille, täysin päinvastoin kuin Aruban ja Ciscon ratkaisuissa joissa päätelaitteille ohjelman asentaminen on suuri osa

toiminnallisuutta. Snortin integraatio Packetfenceen nostaa Packetfencen tietoturvaominaisuudet omalle tasolleen, sillä NIDS-integraatio tarkastaa ja varmistaa päätelaitteiden lisäksi koko verkon tietoturvaa.

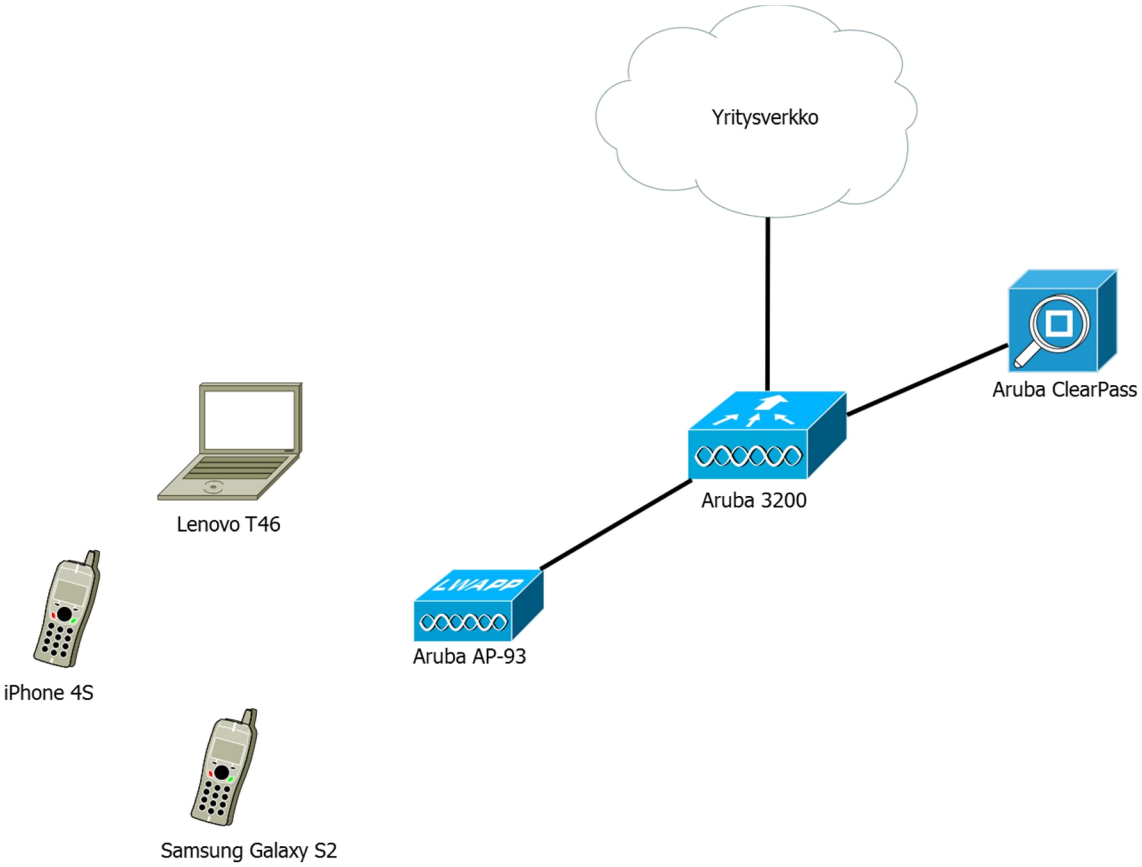
Koska Packetfence käyttää useita eri vapaan lähdekoodin ohjelmia, voi sen päivittäminen koitua ongelmalliseksi. On mahdollista, että jostakin näistä ohjelmista löytyy tietoturvaongelma, mutta sen päivittäminen taas rikkoo yhteensopivuuden muiden komponenttien kanssa. Lisäksi Packetfence-projektin mahdollisesti loputtua ei sen toimintaa jatkuvasti muuttuvassa verkkomaailmassa voi taata. Sama pätee tietenkin myös kaupallisten ratkaisujen vanhentuneisiin tuotteisiin, mutta vapaan ohjelmiston kehittäjillä ei ole mitään käytännön vastuuta tuotteen käyttäjille. Packetfenceä suosittelisin käytettäväksi testiympäristöissä sekä pienemmissä verkoissa.

8 Esimerkkitoteutus

Esimerkkiympäristö toteutettiin Aruban ClearPassia käyttäen. Muita verkon keskeisiä komponentteja olivat Aruba 3200 -WLAN-kontrolleri, sekä Aruban AP-93 langaton tukiasema. Koska Aruban WLAN-kontrollerilla konfiguroidaan huomattava määrä omia asetuksia, osa toiminnallisuudesta jätettiin kyseisen laitteen vastuulle. Aruba ClearPass toimi väliaikaislisenssillä versiossa 6.0.2.46902. Aruba 3200 -WLAN-kontrollerin ohjelmistoversio taas oli 6.1.2.6.

Toteutuksessa yritettiin saada toimintaan oma SSID vierasverkolle ja Onboarding-laiteprovisioinnille, sekä tietenkin tavanomainen langaton yritysverkko. Näistä vierasverkko jäi valitettavasti kesken, sillä ajan puute sekä integraatio Aruban WLAN-kontrollerin kanssa koitui ongelmalliseksi dokumentaatiosta huolimatta. Onboarding, eli laiteprovisiointi olisi ollut mahdollista toteuttaa yritysverkon kanssa saman SSID:n sisään, mutta kahden erillisen SSID:n ratkaisu vähensi mahdollisten ongelmatilanteiden määrää. Testiympäristössä päätettiin käyttää jälkimmäistä.

Onboarding-toiminnallisuutta testattiin Samsung Galaxy S2 -puhelimella (Android), kahdella iPhone 4S:llä (iOS) sekä Lenovo T46 -kannettavalla tietokoneella (Windows 7). Verkkokuva ympäristöstä on nähtävissä kuvassa 3.



Kuva 3. Esimerkkitoteutuksen verkkokuva

Samsung Galaxy S2 on Android-versio 4.1.2:ta käyttävä puhelin, ja se oli mutkattomin verkkoon rekisteröitävä vaaditusta Aruba Quickconnect -sovelluksesta huolimatta. Verkkoon liittymisen jälkeen käyttäjä avasi selaimen, joka ohjautui automaattisesti ClearPassin laiteprovisiointiportaaliin. Laite tunnistettiin automaattisesti Android-puhelimeksi ja käyttäjälle annettiin suora linkki Google Play Storesta ladattavaan Aruba Quickconnect -sovellukseen.

Latauksen ja asennuksen jälkeen käyttäjä palasi rekisteröintiportaaliin ja painoi ’Next’-painiketta. Sovellus asensi nyt varmenteen, sekä yritysverkon 802.1X-profiilin puhelimeen. Käyttäjältä pyydettiin yritysverkon tunnukset, joiden syötön jälkeen käyttäjä poistui automaattisesti provisiointiverkosta liittyen yritysverkkoon sen täysivaltaisena jäsenenä.

iOSia käyttävä *iPhone 4S* oli paperilla helpoin provisioitava laite, mutta se koitui käytännössä hieman ongelmalliseksi. Laite osasi provisiointiverkkoon liittyessään

ladata sekä varmenteen, että profiilin ilman erillisiä sovelluksia, mutta jälkimmäisen asennus päätyi virheilmoitukseen profiilin asennusvaiheessa oikeiden yritysverkkotunnuksien syöttämisestä huolimatta. Syytä ongelmaan ei löydetty.

Toista iPhone 4S -kappaletta käyttäessä profiilin ja varmenteen asennus onnistui, mutta liittyminen yritysverkon SSID:hen piti tehdä manuaalisesti huolimatta ClearPassin asetuksesta jonka mukaan tämän tulisi tapahtua automaattisesti.

Lenovo T46:lle asennettu Windows 7 vaati myös erillisen Quickconnect-ohjelman asennuksen, joka oli ladattavissa suoraan laiterekisteröintiportaalista. Mikäli käyttäjällä ei ole järjestelmänvalvojan tunnuksia, koituu ohjelman asennus ongelmalliseksi. Testissä kaikki sujui kuitenkin ongelmitta. Ohjelman asennuksen jälkeen se käynnistyi automaattisesti, asensi laitteelle varmenteen sekä 802.1X-profiilin ja liittyi yritysverkkoon käyttäjätunnusten vahvistuksen jälkeen.

Jokaisesta testatusta laitetyypistä saatiin laite liitettyä verkkoon, joten ClearPassin Onboarding-ominaisuus voidaan todeta toimivaksi ratkaisuksi. Testattavat laitteet tunnistettiin oikein ja niille tarjottiin oikeat keinot yritysverkon SSID:hen liittymiselle. Laitteiden verkkoon liittäminen oli mutkatonta toimiessaan oikein, mutta myös ongelmia esiintyi. Nämä rajoittuivat iOS-alustalle ja olisivat henkilökohtaisen arvioni mukaan työllistäneet yrityksen IT-tukea.

ClearPass Guestin toiminta jäi kokeilematta ajan puutteen sekä integraatio-ongelmien vuoksi. Muokattavat asetukset näyttivät kuitenkin tarjoavan kaikki tarpeelliset ominaisuudet, mikäli toiminnallisuus olisi saavutettu.

9 Yhteenveto

Insinöörityössä tutkittiin kolmen eri valmistajan BYOD WLAN -ratkaisuja Network Access Control-palvelimien osalta sekä Aruba ClearPass-ratkaisun toiminnan testaamiseen.

Teoriaosuudessa käytiin läpi tärkeimmät aiheeseen liittyvät teknologiat, protokollat sekä myös hieman niiden historiaa. Näihin kuuluivat IEEE:n 802.11- ja 802.1x-

standardit, IETF:n RFC-dokumentit AAA:n, RADIUS- ja LDAP-protokollien määrittelyille sekä Microsoftin Active Directoryn rakenteet.

Käytännön osuudessa tarkasteltiin valittujen valmistajien ominaisuuksia, yhteensopivuutta ja konfiguraatiomahdollisuuksia, sekä näistä johtopäätöksinä niiden vahvuuksia ja heikkouksia ja mahdollisesti muita huomioita.

Viimeisenä luotiin Aruban laitteista pienimuotoinen BYOD WLAN -testiympäristö, jossa testattiin laiden rekisteröimistä ja liittämistä verkkoon ClearPass NAC:ia käyttäen. Muita käytettyjä komponentteja olivat Aruba 3200 -WLAN-kontrolleri, Aruban AP-93-langaton tukiasema sekä tietenkin päätelaitteet. Tarkoituksena oli myös testata vierasportaalin toimintaa, mutta tämä epäonnistui johtuen ongelmista ClearPassin sekä WLAN-kontrollerin keskenäisen integraation asetuksien kanssa. Ongelmia esiintyi myös molempien iPhone S4 -laitteiden rekisteröimisessä ja liittämisessä verkkoon.

Laitteiden tarkastelussa selvisivät nykyisten kaupallisten ja ilmaisten NAC:ien ominaisuudet BYOD WLAN -käytössä. Testauksessa taas selvisi, että suurimmat ongelmat toimivan BYOD WLAN -ympäristön käyttöönoton kanssa ovat sekä laitteiden keskeisessä integraatiossa että päätelaitteissa. Aruba ClearPass todettiin ongelmista huolimatta toimivaksi ratkaisuksi.

Lähteet

1 About IEEE. 2013. Verkkodokumentti. IEEE. <http://www.ieee.org/about/index.html> Luettu 26.4.2013.

2 IEEE 802 Working Group & Executive Committee Study Group s. 2012. Verkkodokumentti. <http://grouper.ieee.org/groups/802/dots.shtml> Luettu 26.4.2013.

3 About IEEE P802.11 and How to Participate. 2011. Verkkodokumentti. IEEE. <http://www.ieee802.org/11/abt80211.html> Luettu 26.4.2013.

4 IEEE Std 802.11a-1999. 1999. Pdf-dokumentti. IEEE. <http://standards.ieee.org/getieee802/download/802.11a-1999.pdf> Luettu 3.5.2013.

5 IEEE Std 802.11b-1999. 1999. Pdf-dokumentti. IEEE. <http://standards.ieee.org/getieee802/download/802.11b-1999.pdf> Luettu 3.5.2013.

6 IEEE Std 802.11g-2003. 2003. Pdf-dokumentti. IEEE. <http://standards.ieee.org/getieee802/download/802.11g-2003.pdf> Luettu 3.5.2013.

7 IEEE Std 802.11-2007. 2007. Pdf-dokumentti. IEEE. <http://standards.ieee.org/getieee802/download/802.11-2007.pdf> Luettu 3.5.2013.

8 IEEE Std 802.11n-2009. 2009. Pdf-dokumentti. IEEE. <http://standards.ieee.org/getieee802/download/802.11n-2009.pdf> Luettu 5.5.2013.

9 IEEE Std 802.11-2012. 2012. Pdf-dokumentti. IEEE. <http://standards.ieee.org/getieee802/download/802.11-2012.pdf> Luettu 5.5.2013.

10 802.11.Verkkodokumentti. 2013. Wikipedia. <http://en.wikipedia.org/wiki/802.11> Luettu 5.5.2013.

11 IEEE 802.11 (legacy mode). 2012. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/IEEE_802.11_%28legacy_mode%29> Luettu 5.5.2013.

12 Organization. Verkkodokumentti. 2013. Wi-Fi Alliance. <http://www.wi-fi.org/about/organization> Luettu 5.5.2013.

13 Wireless Fidelity ‘Debunked’. 2007. Verkkodokumentti. Wi-Fi Planet. <http://www.wi-fiplanet.com/columns/article.php/3674591> Luettu 9.5.2013.

14 Understanding the IEEE 802.11ac Wi-Fi Standard. 2012. Pdf-dokumentti. Meru Networks. <http://www.merunetworks.com/collateral/white-papers/2012-wp-ieee-802-11ac-understanding-enterprise-wlan-challenges.pdf> Luettu 9.5.2013.

15 WiGig White Paper. 2010. Pdf-dokumentti. Wireless Gigabit Alliance. <http://wirelessgigabitalliance.org/?getfile=1510> Luettu 10.5.2013.

16 Membership. 2013. Verkkodokumentti. Wireless Gigabit Alliance <http://wirelessgigabitalliance.org/membership/> Luettu 10.5.2013.

17 An Inductive Chosen Plaintext Attack against WEP/WEP2. 2001. Verkkodokumentti. University of Maryland. <http://www.cs.umd.edu/~waa/attack/v3dcmnt.htm> Luettu 3.5.2013.

18 IEEE Std 802.11a-1997. 1997. Pdf-dokumentti. IEEE. Luettu 3.5.2013.

19 IEEE Std 802.1X-2010. 2010. Pdf-dokumentti. IEEE. <http://standards.ieee.org/getieee802/download/802.1X-2010.pdf> Luettu 6.5.2013.

20 MAC Authentication Bypass Deployment. 2011. Verkkodokumentti. Cisco <http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/config_guide_c17-663759.html#wp9000124> Luettu 6.5.2013.

21 Getting Started in the IETF. 2013. Verkkodokumentti. IETF. <http://www.ietf.org/newcomers.html> Luettu 26.4.2013. Luettu 3.5.2013.

22 RFC 2865. 2000. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc2865> Luettu 6.5.2013.

23 RFC 2866. 2000. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc2866> Luettu 6.5.2013.

24 RFC 3539. 2003. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc3539> Luettu 6.5.2013.

25 RFC 3576. 2003. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc3576> Luettu 6.5.2013.

26 RFC 1487. 1993. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc1487> Luettu 6.5.2013.

27 RFC 4511. 2006. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc4511> Luettu 6.5.2013.

28 RFC 4530. 2006. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc4530> Luettu 6.5.2013.

29 How to Enable LDAP over SSL with third party certification authority. 2011. Verkkodokumentti. Microsoft. <http://support.microsoft.com/kb/321051> Luettu 10.5.2013.

30 A Brief History of Active Directory Bridging. 2011. Verkkodokumentti. Centrify. <http://www.centrify.com/blogs/tomkemp/a_brief_history_of_active_directory_bridging.asp> Luettu 10.5.2013.

31 Understanding Active Directory. 2013. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/cc781408%28v=ws.10%29.aspx> Luettu 10.5.2013.

32 Understanding Schema. 2013. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/cc739086%28v=ws.10%29.aspx> Luettu 10.5.2013.

33 Corporate Summary. 2013. Pdf-dokumentti. Aruba. <http://www.arubanetworks.com/pdf/company/CorpOvw_Summary.pdf> Luettu 9.5.2013.

34 BYOD Whitepaper. 2012. Pdf-dokumentti. Aruba. <http://www.arubanetworks.com/pdf/technology/whitepapers/WP_BYOD.pdf > Luettu 9.5.2013.

35 ClearPass Policy Manager Data Sheet. 2013. Pdf-dokumentti. Aruba. <http://www.arubanetworks.com/pdf/products/DS_ClearPass_PolicyManager.pdf > Luettu 9.5.2013.

36 ClearPass Policy Manager 6.0 Deployment Guide. 2013. Pdf-dokumentti. Aruba. <http://support.arubanetworks.com/DOCUMENTATION/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=10426> Luettu 9.5.2013.

37 ClearPass Onboard 3.9.6 Deployment Guide. 2013. Pdf-dokumentti. Aruba. <http://support.arubanetworks.com/DOCUMENTATION/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=10647> Luettu 9.5.2013.

38 ClearPass Guest 6.0 Deployment Guide. 2013. Pdf-dokumentti. Aruba. <http://support.arubanetworks.com/DOCUMENTATION/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=10647> Luettu 9.5.2013.

39 Aruba WorkSpace gets futuristic with BYOD enterprise security. 2013. Verkkodokumentti. Slashgear. <http://www.slashgear.com/aruba-workspace-gets-futuristic-with-bring-your-own-device-enterprise-security-10277360/> Luettu 9.5.2013.

40 Packetfence Overview. 2013.Verkkodokumentti. Packetfence. <http://www.packetfence.org/about/overview.html> Luettu 6.5.2013.

41 Packetfence Advanced Features. 2013. Verkkodokumentti. Packetfence. <http://www.packetfence.org/about/advanced_features.html> Luettu 6.5.2013.

42 Packetfence Administration Guide. 2013. Pdf-dokumentti. Packetfence. <http://www.packetfence.org/downloads/PacketFence/doc/PacketFence_Administration_Guide-3.6.1.pdf> Luettu 6.5.2013.

43 Packetfence Technical Introduction. 2013. Verkkodokumentti. Packetfence. <http://www.packetfence.org/about/technical_introduction.html> Luettu 6.5.2013.

44 Packetfence Supported Switches and APs. 2013. Verkkodokumentti. Packetfence. <http://www.packetfence.org/about/supported_switches_and_aps.html#c1652> Luettu 6.5.2013.

45 EAP Methods. 2012. Verkkodokumentti. FreeRADIUS. <http://freeradius.org/features/eap.html> Luettu 6.5.2013.

46 Authentication. 2012. Verkkodokumentti. FreeRADIUS. <http://freeradius.org/features/authentication.html> Luettu 6.5.2013.

47 Form 10-K. Pdf-dokumentti. 2012. SECDatabase. <http://pdf.secdatabase.com/419/0001193125-12-388590.pdf> Luettu 5.5.2013.

48 Cisco ISE Data Sheet. 2013. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/data_sheet_c78-656174.html> Luettu 5.5.2013.

49 Cisco ISE, Managing Authentication Policies. 2013. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_auth_pol.html> Luettu 5.5.2013.

50 Cisco ISE, Managing Authorization Policies and Profiles. 2013. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_authz_polprfls.html> Luettu 5.5.2013.

51 Cisco ISE, Configuring Endpoint Profiling Policies. 2013. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_prof_pol.html> Luettu 5.5.2013.

52 Cisco ISE, Configuring Client Provisioning Policies. 2013. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_client_prov.html> Luettu 5.5.2013.

53 Cisco ISE, Device Access Management. 2013. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_mydevices.html> Luettu 5.5.2013.

54 Cisco ISE, User Access Management. 2013. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_guest_pol.html> Luettu 5.5.2013.