OULUN AMMATTIKORKEAKOULU

Juuso Mattila

NETWORK ACCESS CONTROL -JÄRJESTELMÄN VALINTA JA KÄYTTÖÖNOTTO

NETWORK ACCESS CONTROL -JÄRJESTELMÄN VALINTA JA KÄYTTÖÖNOTTO

Juuso Mattila
Opinnäytetyö
Kevätlukukausi 2019
Tietotekniikan tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma, laite- ja tuotesuunnittelu

Tekijä: Juuso Mattila
Opinnäytetyön nimi suomeksi: Network Access Control -järjestelmän valinta ja käyttöönotto
Opinnäytetyön nimi englanniksi: Choosing and deploying a Network Access Control system
Työn ohjaaja: Teemu Korpela OAMK
Työn valmistumislukukausi ja -vuosi: Kevätlukukausi 2019
Sivumäärä: 28

Tämän opinnäytetyön tilaama yritys haluaa pysyä nimeämättömänä, joten tilaajaa ei mainita. Aiheena oli valita yrityksen sisäiseen verkkoon sopivin Network Access Control -järjestelmä ja suunnitella sen käyttöönotto. Tarkoituksena oli parantaa lähiverkon turvallisuutta rajoittamalla tuntemattomien laitteiden pääsyä verkkoon. Tarve tälle huomattiin yrityksen sisäisessä turvallisuusauditoinnissa.

Aluksi vertailtiin kolmea vaihtoehtoa, jonka jälkeen alettiin testaamaan valittuja järjestelmiä.

Järjestelmien testauksissa keskityttiin saavuttamaan ennalta laadittuja vaatimuksia. Myös järjestelmien yleinen luotettavuus, toimivuus ja käytettävyys olivat kriteerejä.

PacketFence- ja Netreg-järjestelmät valittiin testaukseen. Molemmat järjestelmät todettiin toimiviksi ja ne saavuttivat monia vaatimuksia. Opinnäytetyö antoi hyvän pohjan järjestelmien käyttöönotolle. Yksi järjestelmä on jo otettu testikäyttöön.

Asiasanat: tietoliikenneverkko, autentikointi, turvallisuus

ABSTRACT

Oulu University of Applied Sciences
Information Technology, Option of Equipment and Product Design

Author: Juuso Mattila
Title of thesis: Choosing and deploying a Network Access Control system
Supervisor: Teemu Korpela OAMK
Term and year when the thesis was submitted: Spring 2019
Pages: 28

This thesis was made for a company that wants to stay unknown, so the name of the company is not mentioned. The topic was choosing a Network Access Control system and planning its deployment in the company internal network. The goal was to secure the local area network by limiting network access of unknown devices. The need for this was discovered in a company internal security audit.

First three NAC choices were compared. Afterwards the chosen systems were taken into testing.

In the tests the focus was to achieve certain predetermined goals. The general reliability, functionality and usage were also taken into notice.

PacketFence and Netreg systems were chosen for the tests. They both were declared functioning and they achieved many of the goals. This thesis gave a good basis for deploying the systems. One of the systems is already on test usage.

Keywords: Network, authentication, security

SISÄLLYS

1 JOHDANTO

Tämä opinnäytetyö tehtiin yrityksessä, jota ei nimetä. Aiheena oli valita yrityksen sisäiseen verkkoon sopivin Network Access Control -järjestelmä ja suunnitella sen käyttöön-otto. Tarkoituksena oli parantaa lähiverkon turvallisuutta rajoittamalla tuntemat-tomien laitteiden pääsyä verkkoon. Tarve tälle huomattiin yrityksen sisäisessä turvallisuusauditoinnissa.

Network Access Control (NAC) on tapa, jolla verkon hallintaa ja turvallisuutta vahvistetaan. Siinä hyödynnetään turvallisuuskäytänteitä ja sääntöjä. Näin ainoastaan sääntöjä noudattavat ja luotettavat päätelaitteet pääsevät kiinni verkkoon. NAC:lla tarkoitetaan myös verkon aktiivisuuden monitorointia ja hallintaa. (1.)

NAC toteutetaan pääasiassa ohjelmistoilla tai integroidulla ratkaisulla. NAC:n tärkeimmät tavoitteet ovat hallita verkkoon pääsyä, selvittää päätelaitteiden identiteetti autentikoinnilla, huolehtia turvallisuuskäytänteiden noudattamista sekä poistaa, estää ja vähentää turvallisuusriskejä verkosta. NAC koostuu käytänteistä, protokollista, työkaluista ja sovelluksista, jotka määrittelevät, mitä yksittäinen komponentti saa tehdä verkossa. Kokonaisvaltainen NAC-ratkaisu pätee kaikkiin päätelaitteisiin, kuten tietokoneisiin, palvelimiin, palomuureihin ja reitittimiin, sekä niiden tapaan yhdistyä verkkoon. (1.)

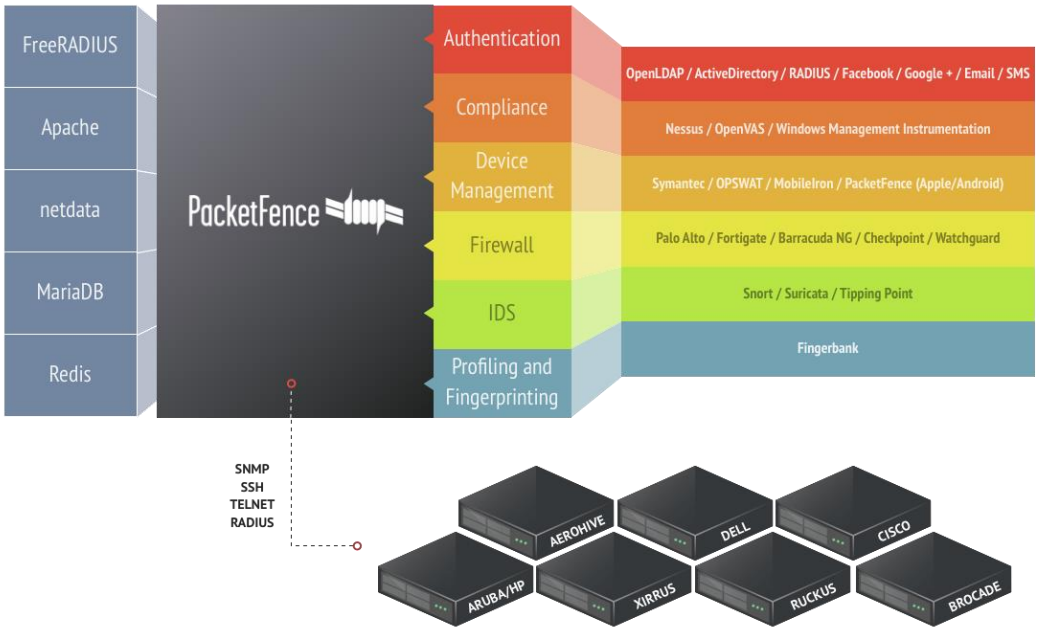
Yleisimmin laitteet autentikoituvat verkkoon joko IEEE 802.1X -standardin mukaisella tai MAC-osoitepohjaisella tavalla. 802.1X-metodi mahdollistaa laitteen identiteetin selvittämisen ennen verkkoon pääsyä. Remote Authentication Dial In User Service (RADIUS) hoitaa keskitetysti autentikoinnin ja käyttäjien hallinnan. Vain onnistuneen 802.1X-autentikoinnin jälkeen laite pääsee verkkoon. MAC-osoitemetodi autentikoi laitteen vertaamalla sen fyysistä MAC-osoitetta johonkin ennalta luotuun tietokantaan. Jos tuo MAC löytyy tietokannasta, laite pääsee verkkoon. Laitteen MAC:n lisääminen tietokantaan voidaan toteuttaa web-portal-rekisteröitymisellä. (2.)

2 NAC-JÄRJESTELMÄT

Tässä luvussa käyn läpi eri NAC-vaihtoehdot. Valitsin vertailuun käytetyimmät Open Source- eli avoimen lähdekoodin järjestelmät.

2.1 PacketFence

PacketFence on luotettu NAC-järjestelmä, jolla on täysi tuki asiakkaalle. Sen ominaisuuksia ovat mm. web-portaali rekisteröitymiselle ja ongelmien korjaukselle, langaton ja langallinen hallinta, BYOD (Bring your own device) -hallinta, 802.1X-tuki ja ongelmallisien laitteiden layer-2 -eristys. Se toimii niin pienissä kuin isoissakin verkoissa. (3.) Kuvassa 1 näkyy PacketFencen sisältämät komponentit ja niiden arkkitehtuuri.



KUVA 1. PacketFencen komponentti arkkitehtuuri (3).

Useimmat kytkimet, joissa on tuki MAC autentikoinnille ja/tai 802.1X:lle, toimivat PacketFencen kanssa (4).

PacketFence toimii täysin ”out-of-band”, eli se ei vaikuta verkon kaistankäyttöön. Yksi PacketFence-palvelin voi suojata jopa satoja kytkimiä ja tuhansia päätelaitteita. Myös kaistankäyttöön vaikuttava moodi on tarvittaessa käytettävissä. (3.)

PacketFencessä on FreeRADIUS-moduulilla tuettu langaton ja langallinen 802.1X-tuki. FreeRADIUS mahdollistaa useiden verkkojen turvaamisen keskitetysti, käyttäen samaa käyttäjä tietokantaa ja web-portaalia. Tämä saa aikaan yhtenäisen käyttäjäkokemuksen. (3.)

PacketFencessä on mahdollisuus käyttää ennakoivaa haavoittuvuuksien torjumista. Nessus- tai OpenVAS-skannauksia voidaan tehdä laitteisiin niiden rekisteröityessä tai muulloin. Epänormaaleja verkon aktiiviteettejä voidaan havaita ja näille voidaan tehdä toimia tarvittaessa. (3.)

PacketFencessä on integroitu security agent -ohjelma, joka voidaan asentaa verkkoon haluavaan laitteeseen ennen pääsyn antamista. Windows Management Insrumentation (WMI) mahdollistaa Windows-tietokoneiden tarkkailun ja komentojen antamisen etänä. (3.)

802.1X-autentikoinnin aikana PacketFence voi tarkistaa laitteen. Esimerkiksi voidaan tarkistaa, onko laitteessa oleva virustentorjuntajärjestelmä tai käyttöjärjestelmä ajan tasalla. Jos ei, laite voidaan eristää muista laitteista. Laitteiden eristämiseen on muutama vaihtoehto, esimerkiksi laitteen sijoittaminen eristettyyn VLANiin. (3.)

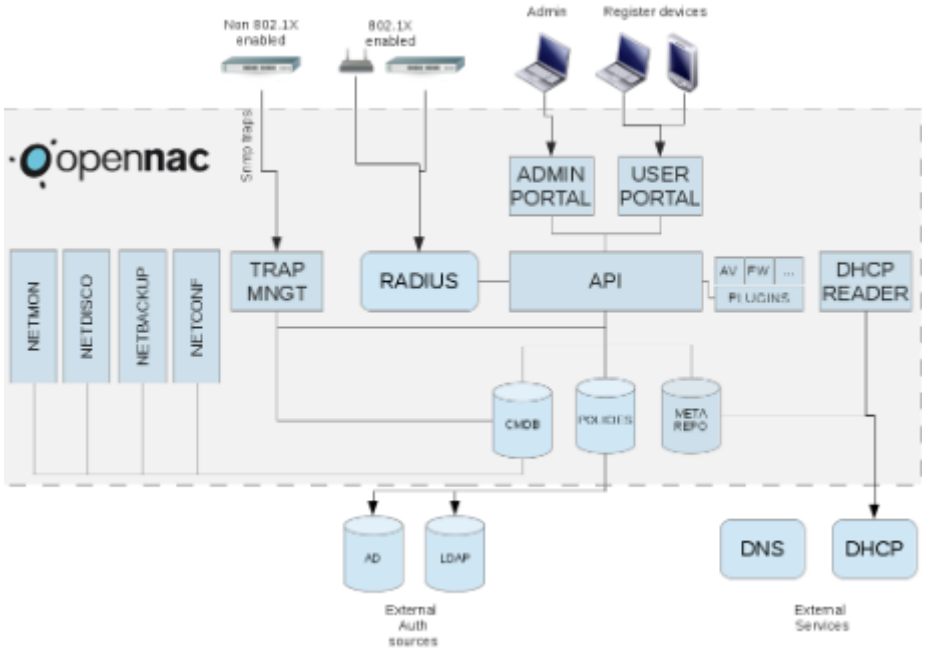
PacketFencessä on sekä web-pohjainen että komentolinjapohjainen hallintakäyttöliittymä (3).

2.2 OpenNAC

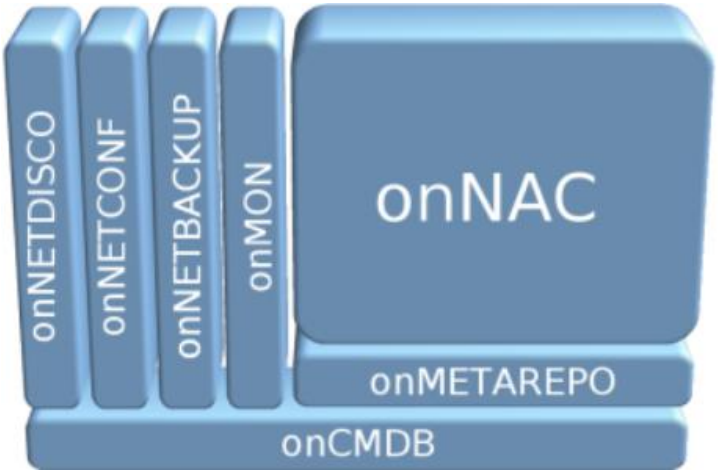
OpenNAC on NAC-järjestelmä, joka tarjoaa turvatun pääsyn lähi- ja laajaverkkoon. Se mahdollistaa autentikoinnin, auktorisoinnin ja auditoinnin verkkoon käytäntöpohjaisilla säännöillä. Tuki löytyy mm. Ciscon ja Alcatelin verkkolaitteille ja monille päätelaitteille kuten Windowsille, Linuxille, Macille, sekä älypuhelimille ja tableteille. (5.)

OpenNAC:iin kuuluu teollisuuden standardien mukaisesti mm. Radius-palvelin, 802.1x-, Active Directory- ja LDAP-tuki. Uusia ominaisuuksia voi lisätä helposti, sillä OpenNAC:n arkkitehtuuri on liitännäispohjainen. Myös olemassa oleviin jär-

jestelmiin integrointi onnistuu kätevästi. OpenNAC tarjoaa lisäominaisuuksia, kuten konfiguraation hallinnan ja verkon skannauksen, monitoroinnin ja varmuuskopioinnin. (5.) Kuvassa 2 näkyy OpenNAC:n yksityiskohtainen arkkitehtuuri ja kuvassa 3 OpenNAC:n pääkomponentit.



KUVA 2. OpenNAC:n yksityiskohtainen arkkitehtuuri (5).



KUVA 3. OpenNAC:n pääkomponentit (6).

OnNAC on NAC -järjestelmän ydin. Siinä valvotaan verkon autentikointia ja auktorisaatiota käytäntöjen mukaan. Management Consolen kautta ylläpitäjät voivat

etsiä ja hallita käyttäjiä käyttäjänimen, IP-osoitteen, MAC-osoitteen, verkkokytkimen tai fyysisen sijainnin perusteella. Auditointi ja raportointi ovat saatavissa verkon aktiivisuuden tarkkailemiseksi. (6.)

OnNETCONF on verkon konfiguraatiomoduuli, joka mahdollistaa konfiguroinnin web-käyttöliittymän kautta (6).

OnNETBACKUP on automaattinen verkon konfiguraation varmuuskopiointi- ja arkistointimoduuli (6).

OnNETDISCO on verkon skannausmoduuli. Sen avulla OpenNAC pysyy selvillä laitteista ja niiden aktiivisuudesta (6).

OnCMDB on käytännössä tietokanta, jossa tieto laitteista säilytetään. Sillä tietoa voidaan jakaa muille alustoille helposti (6).

OnMON on verkon monitorointimoduuli. Sillä monitoroidaan verkon kuntoa ja se hälyttää ylläpitäjiä jonkin ollessa pielessä. (6.)

2.3 NetReg

Netreg on autentikoitumisjärjestelmä, joka vaatii verkkoon yhdistyvän laitteen rekisteröinnin ennen verkkoon pääsyä. Siinä on erittäin yksinkertainen web-liittymä rekisteröintiä varten. Netreg tallentaa tiedot laitteesta ja käyttäjästä, jolloin sama laite pääsee jatkossa suoraan verkkoon. (7.)

Netreg eroaa PacketFencestä ja Opennacista huomattavasti. Netreg käyttää autentikoitumiseen pelkästään laitteen MAC-osoitetta. Siinä ei ole tukea 802.1X-autentikoinnille. Lisäominaisuutena Netregiin voi asentaa Nessus-haavoittuvuusskannerin, jolla laitteita voidaan skannata haavoittuvuuksien varalta. Netregissä ei ole varsinaista tietokantaa, vaan tiedot laitteista tallennetaan tekstitiedostoon.

Netregin toiminta perustuu DHCP (Dynamic Host Control Protocol) -palvelimeen, joka jakaa osoitteita laitteen rekisteröinnin perusteella. Rekisteröimättömät laitteet saavat IP-osoitteen, jolla pääsee vain Netregin rekisteröintisivulle. Kun laite on rekisteröitynyt, DHCP jakaa sille osoitteen, jolla pääsee verkkoon.

Netregissä on web-pohjainen ylläpitosivu. Sieltä voidaan tarkastella laitteita ja käyttäjiä. Sieltä voidaan myös rekisteröidä laitteita, jotka eivät voi käydä rekisteröimässä itseään rekisteröintisivulla.

KUVA 4. NetRegin ylläpitoweb-sivu.

3 TESTAUKSET

Gartnerin mukaan NAC -järjestelmää valittaessa kannattaa arvioida seuraavia ominaisuuksia: laitteen tunnistus ja luokittelu, verkon hallinta, yleisen tietoturvan tarkistus, vierailevien laitteiden hallinta ja integrointi muihin järjestelmiin (10).

Taulukossa 1 luotellaan yrityksen NAC -järjestelmän päävaatimukset ja prioriteetit.

TAULUKKO 1. NAC-vaatimukset (prioriteetit 1–5, 5 korkein)

MAC-osoitepohjainen autentikointi ja verkkoon pääsyn rajoittaminen. Tuntematon laite ei saa päästä kytkimen portista suoraan verkkoon.	5
Tuki 802.1X-protokollaa käyttäville laitteille.	5
Jokaisella rekisteröidyllä laitteella täytyy olla tunnettu omistaja.	4
Web-portaalipohjainen autentikaatio online-laitteille.	3
Web-portaalipohjainen autentikaatio offline-laitteille.	5
Listaus aktiivisista käyttäjistä, laitteista, MAC-osoitteista ja rekisteröitymispäivästä luettavaan muotoon.	4
Automaattinen synkronointi IPAM (IP Address Management) -työkaluun.	2
Rekisteröitymisen vanhentumisen ajan hallinta.	3

Testauksia varten saatiin HP Proliant DL Gen9 -palvelin. Siihen asennettiin Vmware ESXi 6.7 -virtualisointiohjelmisto. Siihen pystyttiin tekemään kaksi virtuaalikonetta, sekä PacketFencelle että OpenNAC:lle. Testauksia varten tarvittiin myös verkkokytkin. Kytkin on lähiverkon laite, johon muut verkon laitteet on kytketty ja joka välittää yhdestä laitteesta tulevan tietoliikenteen vain siihen verkon laitteista, johon se on tarkoitettu (13).

Testaus aloitettiin PacketFencellä, perustuen vaihtoehtojen dokumentaation laatuun ja määrään. PacketFencen dokumentointi oli huomattavasti selkeämpää. Myös PacketFencen käyttäjien keskustelupalstat olivat paljon aktiivisemmat.

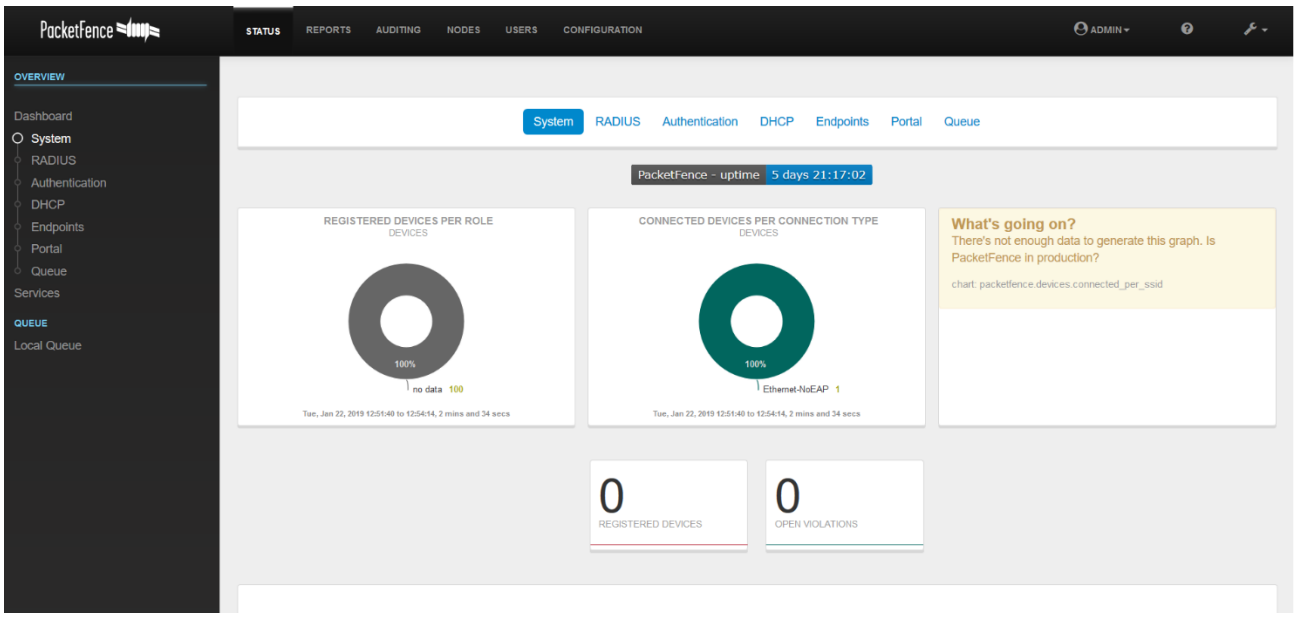
3.1 PacketFence

Asennuksen apuna käytin PacketFencen asennusdokumenttia (8).

PacketFenceä varten tein virtuaalikoneen, johon asensin Centos 7 -käyttöjärjestelmän. Virtuaalikoneelle annoin 6 prosessoria, 10 GB RAM-muistia, 300 GB:n kovalevyn ja kaksi verkkokorttia, suositusten mukaan. Kytkimeksi valitsin Cisco 2960:n, sillä siihen löytyi PacketFenceltä ohjeet ja se tukee 802.1X-protokollaa, MAC-osoitepohjaista autentikaatiota ja web-portaalikirjautumista.

PacketFencen asensin ohjeen kohdan 4.2 mukaan Centos 7 -virtuaalikoneeseen. Virtuaalikoneen käyttöönotossa oli pieniä ongelmia, kuten virtuaalisten verkkokorttien toiminta.

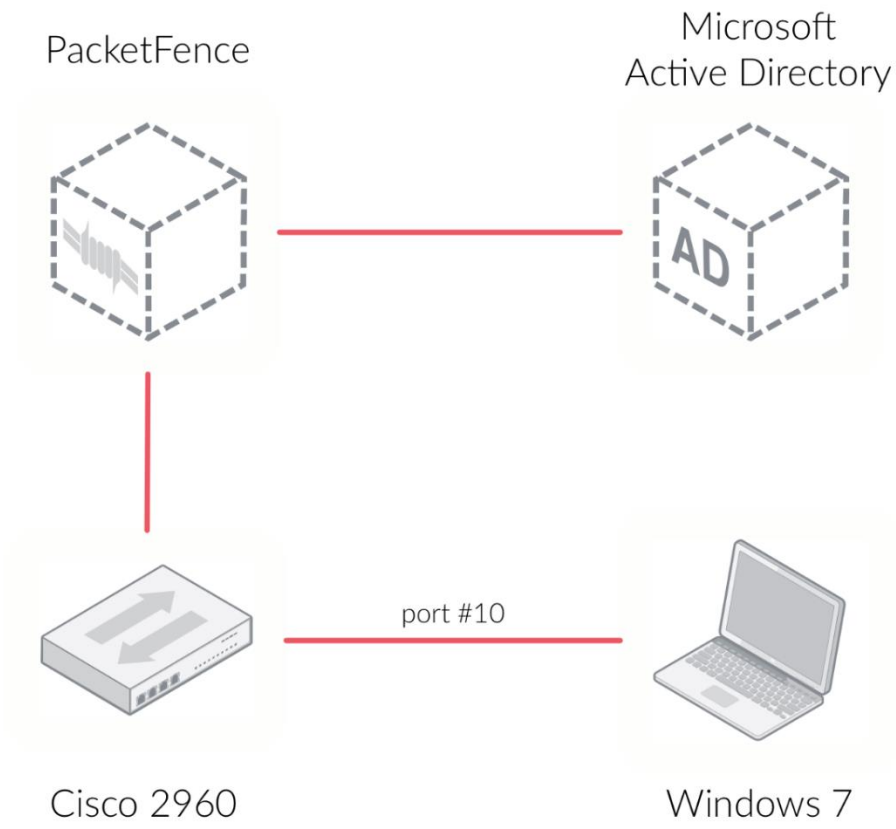
Asennuksen jälkeen pääsin selainpohjaiseen alustavaan konfigurointiin, jossa määriteltiin mm. verkkoasetukset, tietokannan asetukset ja ylläpitotunnukset. Tämän jälkeen PacketFence oli käyttövalmis. Kuvassa 5 näkyy PacketFencen käyttöliittymä puhtaan asennuksen jälkeen.



KUVA 5. PacketFencen ylläpitokäyttöliittymä puhtaan asennuksen jälkeen.

3.1.1 Tuki 802.1X laitteille

Testaus aloitettiin seuraamalla PacketFencen asennusdokumenttia kohdasta 5 (8). Ensimmäisenä aloin testaamaan 802.1X-autentikointia Microsoft Active Directoryn kautta. Active Directory on Windows-laitteille tarkoitettu tietokanta, jossa on tietoa käyttäjistä ja tietokoneista. Kuva 6 havainnollistaa testin rakennetta.

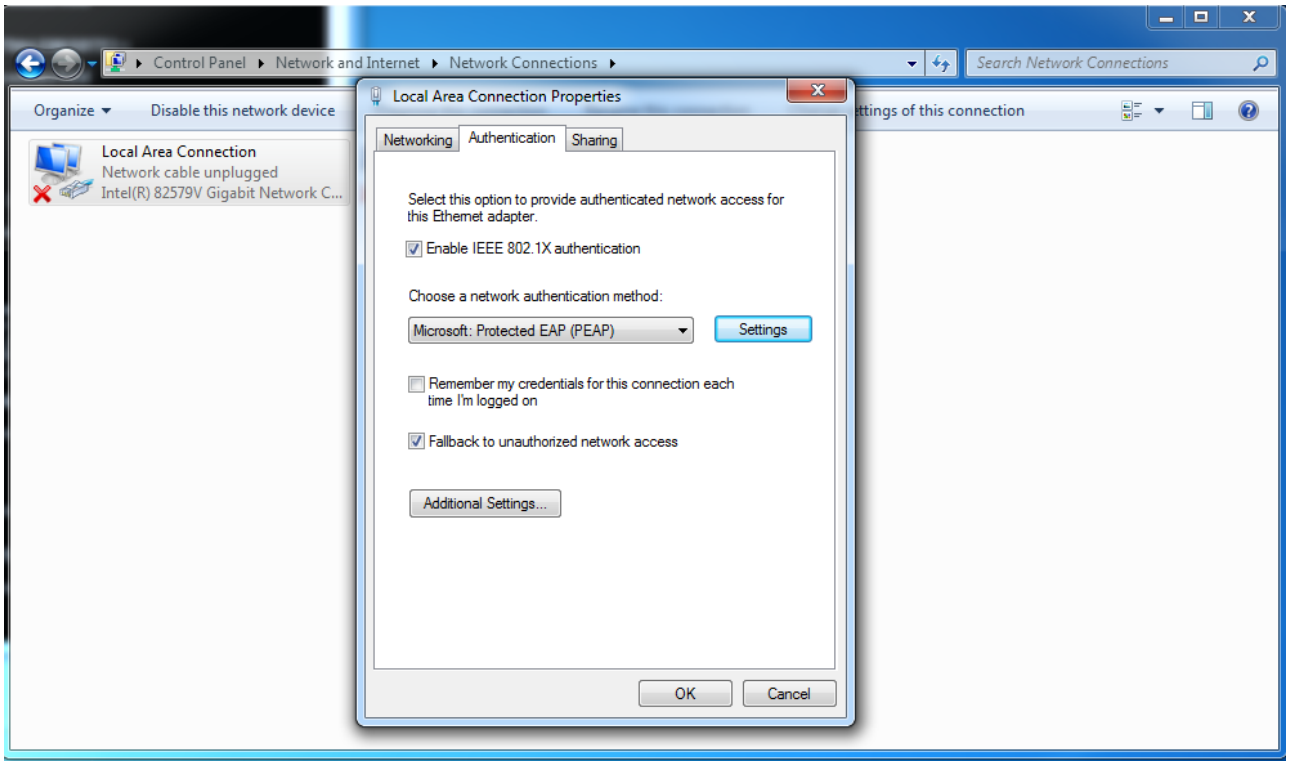


KUVA 6. 802.1X autentikointi AD:n avulla (8).

Tällä tavalla ratkaistaan vaatimus 802.1X-protokollaa käyttäville laitteille, joka on yksi korkeimmista prioriteeteistä. Käytännössä käyttäjän, joka kytkee tietokoneensa kytkimeen, täytyy syöttää käyttäjätunnus ja salasana, jotka PacketFence tarkistaa AD:sta. Jos tunnukset kelpaavat ja tietokone on lisättynä AD:hen, pääsee käyttäjä verkkoon.

PacketFence käyttää eri autentikaatiolähteitä ja yhdistymisprofiileja, joiden mukaan määräytyy esimerkiksi, käytetäänkö 802.1X-autentikoitumista vai ohjataanko kytketty laite web-portaaliin kirjautumaan.

Tässä testissä yhdistettiin PacketFence yrityksen omaan AD:hen, jonka jälkeen tuo AD määriteltiin autentikaatiolähteeksi. Sitten tehtiin yhdistymisprofiili, johon määriteltiin, mitä tapahtuu kun tietynlainen yhteys muodostetaan. Tässä tapauksessa määriteltiin, että Ethernet-EAP:n eli suojatun yhteyden muodostuessa ohjataan tämä laite AD-autentikaatiolähteeseen. Windows 7 -tietokone, joka tässä tapauksessa oli testilaitteena, ei normaalisti käytä 802.1X-autentikoitumista, joten se piti ottaa käyttöön. Ciscon kytkimeen konfiguroitiin 802.1X päälle ja lisättiin PacketFence Radius-palvelimeksi. Portti 10 konfiguroitiin tähän testiin käyttämään 802.1X-protokollaa. Kuvassa 7 näkyy kuinka 802.1X otetaan käyttöön Windows 7 -laitteessa.

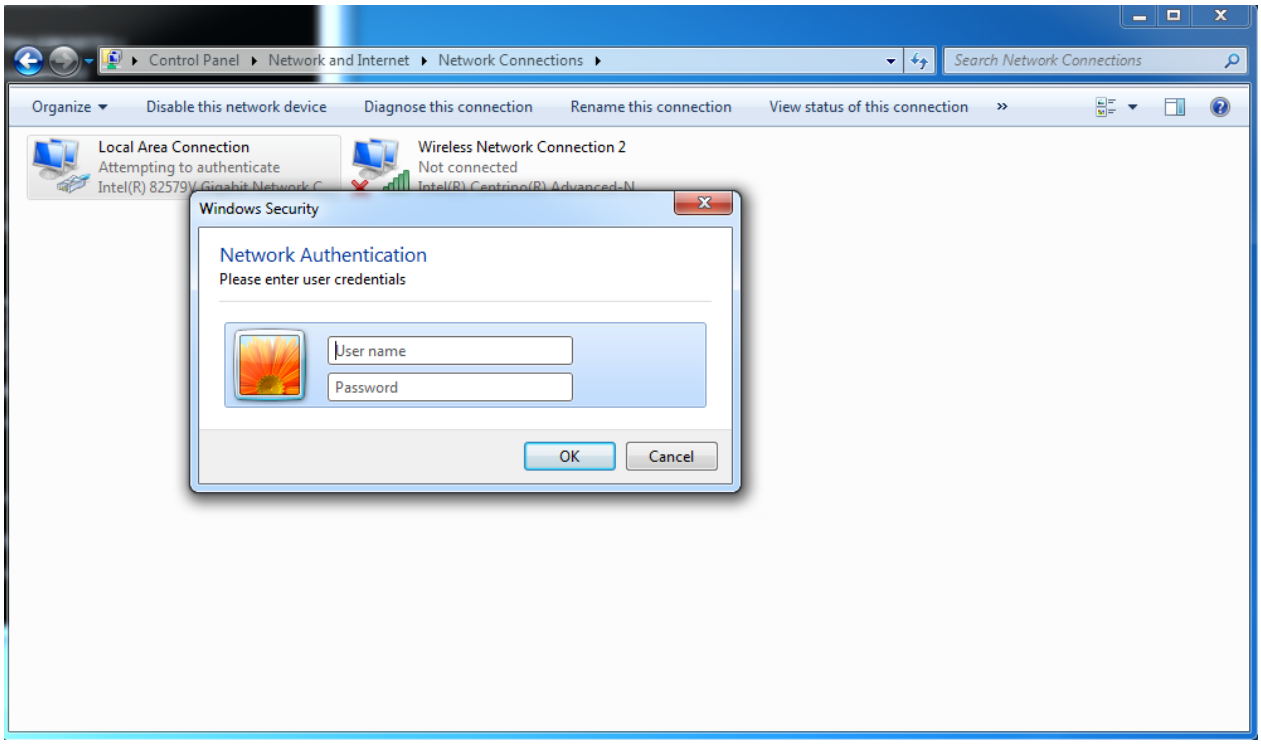


KUVA 7. 802.1X-protokollan aktivoiminen Windows 7 -laitteessa.

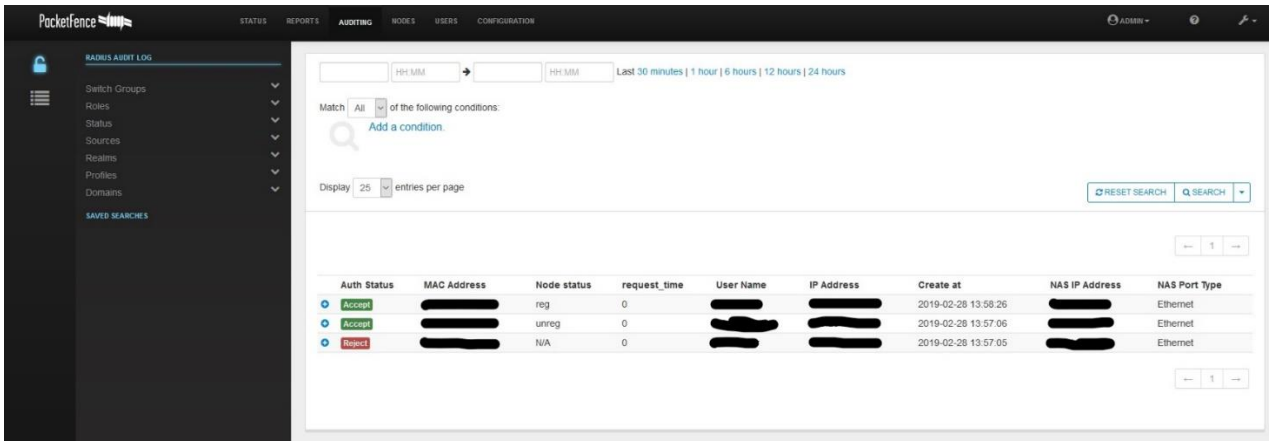
PacketFencen tulee myös olla tietoinen sen hallittavista varusteista, joten kytkin täytyi lisätä PacketFencen kytkinten konfiguraatioon. Tässä konfiguraatiossa määriteltiin kytkimen rooliksi VLAN ID:n mukaan määräytyvä rooli. Roolit ovat

luokkia, joihin yhdistettävät laitteet lajitellaan. Näille rooleille määriteltiin VLAN ID:t, joita ne käyttävät. Nämä olivat yrityksen omia sisäisiä VLANeja.

Testissä rooleja tarvittiin kaksi: rekisteröinti ja default. Rekisteröintiroolin VLA-Nista tuli olla yhteys AD -palvelimelle, jotta autentikointi toimi. Rekisteröimätön laite määräytyy aluksi rekisteröintirooliin, jolloin PacketFence ohjeistaa kytkimen antamaan laitteelle pääsyn rekisteröintiroolin VLANiin. Rekisteröinti tapahtuu Windows 7 -laitteella antamalla oikea käyttäjänimi ja salasana niitä kysyttäessä (kuva 8). Kuvassa 9 on PacketFencen ylläpitosivun näkymä autentikointitapahtumista.



KUVA 8. 802.1X-autentikoituminen Windows 7 -laitteella.



KUVA 9. PacketFencen näkymä autentikointitapahtumista. Reject on tullut, kun on annettu väärä salasana.

Onnistuneen autentikoinnin jälkeen laite saa default-roolin ja sen mukaisen VLA-Nin. Näin laite pääsee käsiksi verkkoon ja sen palveluihin. PacketFencessä näkyy rekisteröityneestä laitteesta mm. omistaja, aktiivisuus, kytkin ja kytkimen portti, IP-osoite, yhteyden tyyppi ja muita tietoja, joita voidaan lisätä myös manuaalisesti.

802.1X-autentikaatio sitä tukeville laitteille onnistui.

3.1.2 Web-portaalipohjainen autentikaatio

Tämä testi aloitettiin seuraamalla asennusdokumentin kohtaa 6 (8).

Tarkoituksena oli saada aikaan web-portaali, johon rekisteröimätön laite ohjataan rekisteröitymään. Testissä käytettiin lähes samaa rakennetta kuin aikaisemmassa testissä. Vain AD jätettiin pois.

Testiin tehtiin uusi autentikointilähde, joka pyytää käyttäjää hyväksymään käyttöehdot, jonka jälkeen autentikaatio menee läpi. Sitten tehtiin yhdistymisprofiili, joka ohjaa laitteen Ethernet-NoEAP:n eli suojaamattoman yhteyden syntyessä aikaisemmin tehtyyn autentikaatiolähteeseen.

Tässä testissä käytettiin samoja rooleja kuin aikaisemmassa 802.1X-autentikoinnissa, eli rekisteröinti ja default. Ensin yhdistyvä laite saa rekisteröintiroolin. Web-portaali -autentikoitumisen jälkeen laite saa default-roolin ja sen mukaisesti pääsyn verkkoon.

PacketFencen web-portaalia ei kuitenkaan saatu toimimaan. Ongelmana oli kytkimen konfigurointi PacketFencen päässä. PacketFenceen piti vaihtaa kytkimen asetuksia, jotta web-portaali -autentikointi saataisiin toimimaan. Näiden muutosten jälkeen laite ei saa kuitenkaan IP-osoitetta ollenkaan, jolloin yhteyttä web-portaaliin ei voida muodostaa.

Ratkaisua ongelmaan ei löytynyt tarpeeksi nopeasti, joten päätin siirtyä muihin testeihin. Web-portaalipohjainen autentikaatio jäi siis vielä tekemättä.

3.1.3 MAC-osoitepohjainen autentikointi

Rekisteröidyn laitteen MAC-osoite jää PacketFenceen muistiin, kuten huomattiin 802.1X-testissä. Sama laite pystyy siis yhdistymään verkkoon uudestaan ilman uutta rekisteröintiä.

Ongelmana on sellaisen laitteen rekisteröinti, joka ei tue 802.1X-protokollaa. Web-portaali olisi ollut hyvä vaihtoehto, mutta sitä ei saatu toimimaan. Jokainen verkkoon yhdistyvä laite tulee PacketFenceen näkyviin, jolloin laite pystytään rekisteröimään manuaalisesti PacketFencen ylläpitosivulta. Tämä kuitenkin vaatii liikaa manuaalista työtä isossa verkossa.

PacketFenceltä löytyi ohjeet kytkimen portin MAC-osoitepohjaisen autentikaation konfigurointiin. Kun portti on konfiguroitu näin, laite pääsee verkkoon vain, jos se on rekisteröity.

Tavoitteena oli saada MAC-osoitepohjainen autentikointi toimimaan, joka onnistui rekisteröinti tapaa lukuun ottamatta.

3.1.4 PacketFence yhteenveto

Taulukossa 2 on aikaisemmin esitetty vaatimuslista. Saavutetut vaatimukset ovat vihreällä, saavuttamattomat mutta mahdolliset keltaisella ja saavuttamattomaksi todetut punaisella.

TAULUKKO 2. PacketFencen testien tulokset

MAC-osoitepohjainen autentikointi ja verkkoon pääsyn rajoittaminen. Tuntematon laite ei saa päästä kytkimen portista suoraan verkkoon.	5
Tuki 802.1X-protokollaa käyttäville laitteille.	5
Jokaisella rekisteröidyllä laitteella täytyy olla tunnettu omistaja.	4
Web-portaalipohjainen autentikaatio online-laitteille.	3
Web-portaalipohjainen autentikaatio offline-laitteille.	5
Listaus aktiivisista käyttäjistä, laitteista, MAC-osoitteista ja rekisteröitymispäivästä luettavaan muotoon.	4
Automaattinen synkronointi IPAM (IP Address Management) -työkaluun.	2
Rekisteröitymisen vanhentumisen ajan hallinta.	3

Listaus aktiivisista käyttäjistä yms. on PacketFencen käyttöliittymässä jo hyvin luettavassa muodossa, mutta tavoitteena oli tietojen muuntaminen esim. CSV-tiedostoon, mikä ei ole mahdollista ilman vaativampia toimenpiteitä.

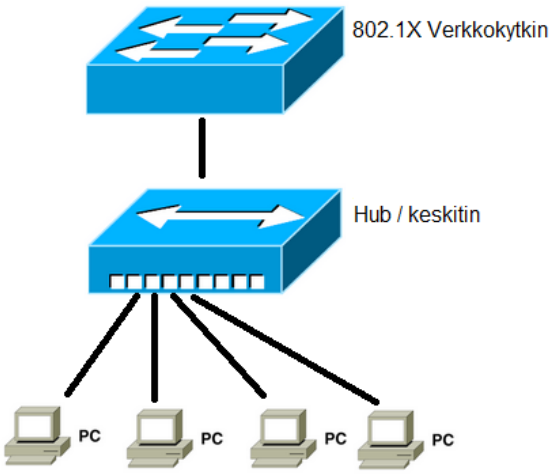
Automaatista synkronointia IPAM-työkaluun ei voi tehdä. CSV-tiedostosta olisi pystynyt lisäämään tietoa IPAM:iin mutta sekin vaatii toistuvaa manuaalista työtä.

Kun web-portaalipohjainen autentikaatio saadaan toimimaan, voidaan rekisteröidä myös ne laitteet, jotka eivät tue 802.1X-autentikoitumista. Laitteet, joissa ei ole web-selainta (offline-laitteet), täytyy rekisteröidä ylläpitosivulta manuaalisesti.

3.2 NetReg

Netregiä on yrityksessä testattu jo aikaisemmin ja huomattiin, että vaatimukset, joita PacketFence ei tässä vaiheessa täyttänyt, voidaan ratkaista Netregillä. Ongelmana PacketFencessä ovat myös keskittimet eli hubit.

Hub on verkkokytkintä yksinkertaisempi verkon komponentti. Se ottaa sisään tulevan liikenteen ja toistaa sen eteenpäin, tekemättä siihen mitään muutoksia. Hubiin kytketyt laitteet keskustelevat jatkuvasti keskenään (11). Yrityksen sisällä näitä käytetään yhdistämään monta laitetta samaan verkkoon. Esimerkiksi yhden huoneen kaikki tietokoneet ovat kytkettynä yhden hubin kautta samaan verkkoon. Näin saadaan yhden kytkimen portin konfiguroinnilla monelle tietokoneelle verkkoyhteys. Tätä tilannetta havainnollistetaan kuvassa 10.



KUVA 10. Tilanne, jossa useampi PC kytkeytyy hubin kautta yhteen kytkimen porttiin.

Tästä syntyy PacketFencen 802.1X-autentikoinnille ongelma. Ennen autentikointia kytkimen portti on rekisteröinti VLANissa. Näin yksikään hubin takana olevista laitteista ei pääse verkkoon. Kun yksi laite autentikoituu onnistuneesti, kytkin

vaihtaa portin normaaliin verkon VLANiin. Näin kaikki laitteet hubin takana pääsevät verkkoon. Netregin MAC-osoitepohjaisella autentikaatiolla tätä ongelmaa ei ole.

Seuraavaksi testattiin siis Netregiä. Netregin laitteiston vaatimukset olivat vähäiset, joten Netreg asennettiin kannettavalle PC:lle. Näin käyttöönotto helpottui verrattuna virtuaalikoneen konfigurointeihin. Asennuksessa apuna oli Netregin asennusohjeet (9).

Testausta varten tehtiin uusi verkko, josta Netregin DHCP-palvelu jakaa osoitteita. DHCP:lle tehtiin kaksi osoitteidenjakoavaruutta. Toisesta jaetaan rekisteröintiosoitteet ja toisesta verkon normaaliin käyttöön tarkoitetut osoitteet. Rekisteröinti avaruuden osoitteiden laina-aika on lyhyt, jolloin laite rekisteröidyttyään saa nopeasti uuden osoitteen.

Testi oli hyvin yksinkertainen rakenteeltaan. Komponentteina olivat kytkin, testilaite ja Netreg-palvelin. Ensin rekisteröimätön laite kytkettiin kytkimeen. Kytkimen portti oli konfiguroitu Netregille tehtyyn verkkoon. Testilaitteessa täytyy olla dynaaminen IP-osoitteen haku päällä, mikä yleensä Windows laitteissa on oletuksena päällä. Laitteen pyytäessä DHCP:ltä osoitetta Netreg tarkistaa laitteen rekisteröinnin. Tässä tapauksessa laite on rekisteröimätön, joten se saa rekisteröintiin tarkoitetun osoitteen. Kun laitteella yritetään mennä jollekin web sivulle, Netreg ohjaa laitteen rekisteröintisivulle. Tämä tehtiin konfiguroimalla Netregin nimipalvelujärjestelmä (DNS) siten, että kaikki Internet nimet selvitetään takaisin Netregin rekisteröintisivulle. Tämä toiminto on vain rekisteröimättömille laitteille, joten rekisteröidyt laitteet toimivat kuitenkin oikein.

Rekisteröinti sivulle tulee syöttää käyttäjänimi ja salasana, jotka tarkistetaan LDAP-palvelimelta. Rekisteröinnin onnistuttua laite saa noin yhden minuutin aikana uuden osoitteen ja laitteen tiedot tallennetaan Netreggiin.

Netreg lukee minuutin välein tiedostoa, johon rekisteröidyt laitteet tallennetaan. Havaitessaan uuden rekisteröinnin DHCP-palvelu täytyy käynnistää uudelleen, sillä DHCP-palvelu lukee rekisteröintitiedoston vain käynnistyessään. DHCP-palvelun käynnistyessä uusi rekisteröity laite saa uuden osoitteen. Tästä johtuu

tämä noin yhden minuutin kesto osoitteen vaihtumisessa. Kuvassa 11 näkyy Netregin ylläpitosivu.

KUVA 11. Netreg ylläpitosivun näkymä rekisteröidyistä laitteista.

Ylläpitosivulta nähdään laitteen käyttäjä, MAC-osoite, käyttöjärjestelmä ja rekisteröinnin päivämäärä. Sivulta voidaan myös tarkastella osoitteiden laina-aikoja, mitä osoitteita käytetään aktiivisesti ja tarkastella yhden käyttäjän kaikkia laitteita. Yhden käyttäjän laitteiden määrä on rajoitettavissa. Myös hakutoiminnolla voidaan hakea laitteita esimerkiksi käyttöjärjestelmän mukaan.

Rekisteröinnit voidaan poistaa joko ylläpitosivulta tai poistamalla rivejä suoraan rekisteröintitiedostosta. Tämä voidaan tehdä automaattisesti lyhyellä ohjelmalla, joka tarkastelee tiedostoa ja poistaa tarpeeksi vanhat rekisteröinnit.

Rekisteröity laite pääsee jatkossa suoraan verkkoon ja se pitää IP-osoitteensa samana tietyn ajan verran. Tämä aika on säädettävissä. Tämä helpottaa laitteiden etäkäyttöä.

Taulukossa 3 on aikaisemmin laadittu NAC vaatimuslista. Netreg testin saavutetut vaatimukset ovat vihreällä ja saavuttamattomat punaisella.

TAULUKKO 3. Netregin testien tulokset

MAC-osoitepohjainen autentikointi ja verkkoon pääsyn rajoittaminen. Tuntematon laite ei saa päästä kytkimen portista suoraan verkkoon.	5
Tuki 802.1X-protokollaa käyttäville laitteille.	5
Jokaisella rekisteröidyllä laitteella täytyy olla tunnettu omistaja.	4
Web-portaalipohjainen autentikaatio online laitteille.	3
Web-portaalipohjainen autentikaatio offline laitteille.	5
Listaus aktiivisista käyttäjistä, laitteista, MAC-osoitteista ja rekisteröitymispäivästä luettavaan muotoon.	4
Automaattinen synkronointi IPAM (IP Address Management) -työkaluun.	2
Rekisteröitymisen vanhentumisen ajan hallinta.	3

Tuloksista nähdään, että NetReg täyttää hyvin ne vaatimukset jotka PacketFenceltä jäivät täyttämättä.

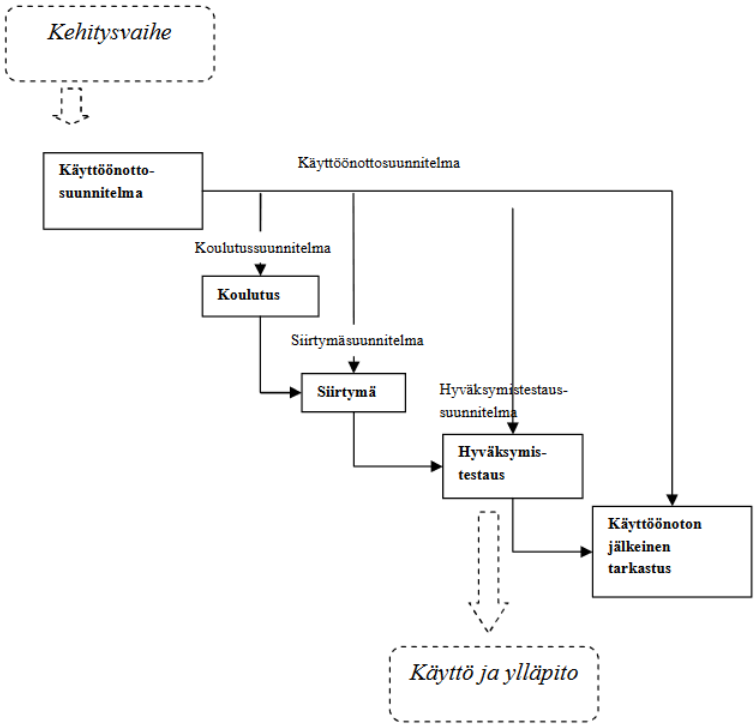
3.3 OpenNAC

Testausten edetessä huomattiin, että kaikki ominaisuudet, mitä OpenNAC:ssa on, löytyvät myös PacketFencestä. Uuden järjestelmän käytön opettelu on aina vaativaa ja aikaa vievää työtä. Tästä syystä OpenNAC jätettiin tästä työstä ulos. Se on kuitenkin varteenotettava vaihtoehto, jos PacketFenceä ei saada käyttöön yrityksen verkossa.

4 KÄYTTÖÖNOTTO

Tietojärjestelmän käyttöönotto on Arosen mukaan Hyötyläistä & Kalliokoskea (2001) siteeraten prosessi, jonka lopputuloksena uusi järjestelmä otetaan käyttöön. Teknisestä näkökulmasta tarkasteltuna järjestelmän käyttöönotolla tarkoitetaan valitun järjestelmän implementointia, parametrisointia ja mahdollisia tietokonversioita vanhasta järjestelmästä uuteen. (12, s. 6.)

Aronen on jakanut käyttöönottoprosessin viiteen vaiheeseen siteeraten Alteria (2002). Ensimmäinen vaihe on käyttöönottosuunnitelman laatiminen. Tämä suunnitelma sisältää kolmen seuraavan vaiheen suunnitelmat: koulutussuunnitelma kertoo, miten ja keitä koulutetaan, siirtymäsuunnitelma sisältää toimenpiteet uuteen järjestelmään siirtymiseksi ja hyväksymissuunnitelma kuvaa prosessit ja kriteerit, joilla järjestelmän toimivuus vahvistetaan hyväksytysti. Hyväksymissuunnitelman onnistuneen testauksen jälkeen voidaan uusi järjestelmä ottaa käyttöön. Käyttöönoton jälkeen suoritetaan tarkastuksia, jotta varmistetaan järjestelmän toimivuus ja eheys. (12, s. 8–9.) Kuvassa 12 on esitetty tämä vaiheitten jaottelu.



KUVA 12. Käyttöönottoprosessin vaiheet. (12, s. 8)

5 YHTEENVETO

Opinnäytetyön tavoitteena oli vertailla Network Access Control -järjestelmiä ja suunnitella valitun järjestelmän käyttöönotto. Työssä tutustuttiin kolmeen eri NAC:iin ja niiden ominaisuuksiin. Moni suunnitellun NAC vaatimuslistan vaatimuksista täyttyi järjestelmien testeissä. Testeissä olivat PacketFence ja Netreg. Näistä Netreg on otettu testikäyttöön, mutta PacketFencen testaukset jatkuvat.

PacketFencen käyttöönotto tulee olemaan vaativa. Yrityksessä on monia eri kytkimiä, jotka kaikki pitää konfiguroida eri tavalla. Jotkut kytkimet eivät edes tue 802.1X-autentikoitumista.

Kytkinten konfigurointi on suurin haaste. Verkossa on monia laitteita, jotka suorittavat kriittisiä toimintoja. Niiden yhteyksiä ei saa katkaista. PacketFencen käytössä on myös kerrottava verkon käyttäjille, miten verkkoon pääsee käsiksi. Muutoksen on oltava käyttäjille mahdollisimman huomaamaton. 802.1X autentikoinnissa käyttäjien tulee ottaa laitteestaan 802.1X käyttöön ja sitten kirjautua oikeilla käyttäjätunnuksilla verkkoon. On tutkittava, voiko autentikoinnin suorittaa SSO- eli Single Sign-On metodilla AD:n avulla. Esimerkiksi kirjautumalla Windows PC:lle käyttäjätilillä, joka on AD:ssa, PacketFence osaisi automaattisesti autentikoida laitteen. Näin saadaan käyttäjän manuaalinen kirjautuminen verkkoon eliminoitua.

Ennen käyttöönottoa on tehtävä lisää testauksia toiminnallisuuden varmistamiseksi. Tärkeää on, että käyttöönotto tehdään vähän kerrallaan. Näin ongelmien sattuessa vaikutusalue on mahdollisimman pieni.

Koska PacketFencen toimintaan kohdeympäristössä tuli ongelmia, otetaan Netreg käyttöön. Tällä hetkellä Netreg toimii kannettavassa PC:ssä. Se on syytä asentaa paremmalle alustalle kuten palvelimelle ja varmistaa toimivuus. Syytä olisi myös kahdentaa Netreg ja PacketFence. Netreg kahdennetaan asentamalla toinen Netreg-palvelin eri alustalle ja konfiguroimalla näiden Netreg-palvelimien DHCP-palveluista toinen pää- ja toinen toissijaiseksi palveluksi.

Käyttöönotto aloitetaan vähän kerrallaan. Ensimmäisenä aloitetaan kokeilu yhdessä työhuoneessa, jossa on hieman yli kymmenen henkilöä. Kun toimivuus todetaan, voidaan kokeilua laajentaa.

Netregin käyttöönotossakin on huomioitava käyttäjien opastus. Kytkinten konfiguraatioon ei tule suuria muutoksia, kuten PacketFencessä. Konfiguraation muutoksessa tulee kuitenkin yhteyskatkos, joka on huomioitava.

Netreg ei yksin ole riittävän vahva suojaus verkolle. Sen autentikointi perustuu pelkästään MAC-osoitteisiin, jotka osaava ilkeämielinen henkilö pystyy väärentämään saadakseen pääsyn verkkoon. Joka tapauksessa sisäiseen verkkoon tulee muutoksia. Näiden tarkka huomioiminen on aina tärkeää.

LÄHTEET

1. Network Access Control. Techopedia. Saatavissa: https://www.techopedia.com/definition/25865/network-access-control-nac. Hakupäivä 3.12.2018.

2. Understanding Authentication Methods. Aruba Networks. Saatavissa: https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/Authentication/AuthenticationMethods.htm. Hakupäivä 14.1.2019.

3. Overview. PacketFence. Saatavissa: https://packetfence.org/about.html#/overview. Hakupäivä 14.1.2019.

4. Supported network devices. PacketFence. Saatavissa: https://packetfence.org/about.html#/material. Hakupäivä 14.1.2019.

5. What is openNAC? Opennac. Saatavissa: http://www.opennac.org/opennac/en/about/what-is-opennac.html. Hakupäivä 14.1.2019.

6. Solution. Opennac. Saatavissa: http://www.opennac.org/opennac/en/solution.html. Hakupäivä 14.1.2019.

7. Valian, Peter – Watson, Todd K 2007. NetReg. Saatavissa: http://netreg.sourceforge.net/. Hakupäivä 4.2.2018.

8. Installation Guide 2018. PacketFence. Saatavissa: https://packetfence.org/doc/PacketFence_Installation_Guide.html. Hakupäivä 3.12.2018.

9. Jaques, Patrick M. 2005. Installing NetReg v1.5 HOWTO. NetReg. Saatavissa: http://netreg.sourceforge.net/contrib/NetReg-1.5.1-HowTo.pdf. Hakupäivä 4.2.2018.

10. What is Network Access Control (NAC)? Gartner. Saatavissa: https://www.gartner.com/reviews/market/network-access-control. Hakupäivä 2.4.2019..

11. Mitchell, Bradley 2018. What Are Ethernet and Network Hubs? Lifewire. Saatavissa: https://www.lifewire.com/ethernet-and-network-hubs-816358. Hakupäivä 2.4.2019.

12. Aronen, Outi 2010. Tietojärjestelmän käyttöönotto ja sen arviointi. Tampere: Tampereen teknillinen yliopisto. Saatavissa: https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/6600/aronen.pdf. Hakupäivä 3.4.2019.

13. TEPA-termipankki 2001. Hakusana kytkin. Sanastokeskus TSK. Saatavissa: http://www.tsk.fi/tepa/fi/haku/kytkin. Hakupäivä 3.4.2019.