LAUREA

IEEE 802.1X:n todennus & käyttöönotto Fenniassa

Gummerus, Laura
Iivonen, Petteri

2010 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

IEEE 802.1X:n todennus & käyttöönotto Fenniassa

Laura Gummerus & Petteri Iivonen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Maaliskuu, 2010

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Laura Gummerus & Petteri Iivonen

IEEE 802.1X todennus & käyttöönotto Fenniassa

Vuosi 2010 Sivumäärä 66

Tämän opinnäytetyön tarkoituksena on tutustua IEEE 802.1X:n porttipohjaiseen todentamiseen ja sen toimintaan. Tarkoituksena on myös todennuksen käyttöönotto Fenniassa. Keskitymme työssä porttikohtaisen autentikoinnin käyttöönottoon fyysisten laitteiden osalta. IEEE 802.1X:n tarkoituksena on estää ulkopuolisten pääsy yrityksen verkkoon.

Käytännön osuudessa tutkimme Windows Server 2003-palvelinympäristöön toteutettavaa 802.1X:n todennusta ja käymme läpi kaikki sen asennusvaiheet. Työssä kerromme, millaisia asetuksia tulisi määritellä palvelimille, tukiasemille sekä työasemille, jotta verkko toimisi tietoturvallisesti sekä haluamallamme tavalla. Tärkeintä olisi pystyä suojaamaan Fennian verkossa liikkuva tieto ja evätä verkkoon pääsy sinne kuulumattomilta laitteilta.

Työ tehdään vakuutusyhtiö Fennialle. Toteutamme työtä Pasilan pääkonttorissa. Fennia haluaa panostaa tietoturvallisuuteen ja 802.1X:ää pidetään erittäin tärkeänä tietoturvallisuutta parantavana suojauksena. Onnistuimme luomaan 802.1X:n suojauksen yrityksessä niin, että käyttäjä ei edes huomaa sen olemassaoloa vaan sallitut koneet menivät verkkoon täysin normaalisti. 802.1X:n avulla pystyimme myös parantamaan verkon valvontaa ja pitämään silmällä laitteita, jotka sinne pyytävät pääsyä.

Työn tutkimusmenetelmäksi valitsimme konstruktiivisen tapaustutkimuksen. Tutkimusmenetelmän avulla pyrimme löytämään olemassa olevaan tilanteeseen uuden ratkaisun.

Työssä käytimme teoreettisina viitekehyksinä Internetistä löytyneitä artikkeleita sekä muita luotettavia Internet sivustoja. Kirja lähteiksi löysimme Jim Geirin vuonna 2008 kirjoittaman kirjan IEEE 802.1X suojauksesta.

Asiasanat IEEE 802.1X, Radius-server, EAP, 802.1X autentikointi

Laurea University of Applied Sciences **Abstract**

Laurea Leppävaara

Information Technology Program

Laura Gummerus & Petteri Iivonen

IEEE 802.1X authentication & implementation in Fennia

Year 2010 Pages 66

The purpose of this thesis is to become acquainted with 802.1X authentication and also to find out how it works. In addition, implementation will be carried out in practice in the company. The thesis concentrates on port based authentication implementation with physical devices.

The practical section examines the Windows Server 2003 environment and 802.1X authentication. All necessary steps of 802.1X installation are studied. The thesis will describe what types of settings should be defined for servers, switches and to workstations so that the network will operate more safely in the future and also the way it is meant to work. The most important aspect is to secure the data belonging to Fennia and to dismiss any irrelevant device trying to access Fennia's network.

The thesis has been assigned by insurance company called Fennia and the project is carried out in the company head office in Pasila. Fennia is keen to invest in data security and 802.1X is considered a very important part of that. It was possible to create 802.1X protection in the company so that the user does not even notice its appearance. All the allowed workstations can access the network without problems. With the help of 802.1X it was also possible to improve Fennia's network surveillance and monitor all the devices trying to access it.

The constructive research method was chosen for the thesis. Based on the research method a new solution for the existing situation was found.

Reliable Internet sources such as articles and other pages were used in the thesis. A good book source about IEEE 802.1X authentication written by Jim Geir 2008 was also found.

Key words IEEE 802.1X, Radius-server, EAP, 802.1X authentication

Sisällys

1 Johdanto

Tietoturvallisuusasiat ovat nykypäivänä yrityksissä tärkeässä asemassa. Yritykset haluavat panostaa tietoturvallisuuteen ja suojata olemassa olevat tiedot. Vakuutusyhtiöillä on paljon sellaista tietoa, joka ei saa joutua ulkopuolisille tahoille. Samanaikaisesti verkosta on tullut kuitenkin yhä tärkeämpi ja haavoittuvampi työskentelyväline erityisesti yrityksille. Tämän vuoksi suojaustasoa halutaan parantaa. 802.1X porttikohtainen todentaminen on merkittävä osa suojauksen parantamiseksi. Suojauksen avustuksella yritys pystyy määrittelemään ne työasemat, jotka saavat käyttää yrityksen verkkoa.

Tämän opinnäytetyön tavoitteena on ottaa käyttöön porttipohjainen todentaminen 802.1X Fennian konttoreissa. Tarkoituksena on tutkia sen mahdollisuuksia sekä sitä, kuinka se sopii Fenniassa jo olemassa oleviin järjestelmiin. Työn tekemisen aikana oli tarkoitus myös kartoittaa, tarvittiinko Fenniassa uusia laitteistoja jo olemassa olevien rinnalle vai saammeko 802.1X:n toimimaan jo olemassa olevissa laitteistoissa.

Työn alussa esittelemme kohdeyrityksen ja kerromme, kuinka valitsimme aiheemme. Esittelemme myös Fenniassa käytössä olevat laitteet. Tämän jälkeen kerromme tarkemmin työn tavoitteista ja avaamme työssä käyttämämme keskeisimmät käsitteet. Työn lopussa kerromme, kuinka toteutimme testaukset Fenniassa ja otettiinko kohdeyrityksessä 802.1X käyttöön. Viimeisellä sivulla on yhteenveto, jossa pohdimme erityisesti sitä, oliko 802.1X Fennialle oikea ratkaisu ja paransiko se yrityksen tietoturvallisuutta.

Keskitymme aiheessamme ainoastaan fyysisiin portteihin ja niiden turvallisuuden parantamiseen, koska koemme niiden olevan yrityksen verkkoon pääsylle tärkeimpiä kohteita. Niitä on myös erittäin helppo käyttää hyväksi, koska todella harvat huomaavat niiden väärinkäyttöä. 802.1X:n avulla estetään luvattoman asiakaslaitteen kommunikointi lähiverkon liityntäpisteen kautta. Laite voi olla mikä tahansa laite, jossa on Ethernet-verkkokortti esimerkiksi tulostin.

2 Kohdeyritys

Kohdeyrityksemme on vakuutusyhtiö Fennia. Esittelemme tarkemmin kohdeyrityksemme alaotsikoiden avulla, jotta lukijalle välittyisi kokonainen kuva organisaatiosta, jossa toteutamme työtämme.

Kohdeyrityksemme on suuri, ja sillä on useita konttoreita ympäri Suomea. Eri konttoreilla on omaosaajia, jotka hallitsevat IT:n perustaidot. Asioita hoidetaan pääsääntöisesti Pasilan pääkonttorilta käsin. Työasemia yrityksellä on noin 1400, kytkimiä on noin 140 ja reitittimiä noin 60.

Kohdeyritys ehdotti meille työmme aihetta, koska sen mielestä tietoturvallisuutta pitäisi parantaa, ja 802.1X luo sille erinomaiset mahdollisuudet. Yrityksellä on myös toimipisteitä, joissa verkon käyttöä ei pystytä kunnolla valvomaan. Toteuttamamme suojauksen avulla saadaan ylimääräiset koneet pois yrityksen verkosta. Joillakin konttoreilla käy ulkopuolisia ihmisiä eikä konttoreiden kytkinkaappeja ole pystytty laittamaan lukolliseen tilaan. Tämä on selvä riskitekijä, ja 802.1X on siksi erittäin tervetullut vaihtoehto suojauksen parantamiseen.

Työtä varten saimme Fenniasta esimieheltämme listan kysymyksiä, joihin hän toivoi meidän vastaavan työmme puitteissa. Muuten kohdeyritys antoi vapaat kädet työn toteuttamiseen ja esimiehemme suostui myös siihen, että voimme toteuttaa työtämme tarvittaessa myös varsinaisella työajalla. Lähteenä Fennian esittelyssä käytetään Fennian omia kotisivuja.

2.1 Fennia-ryhmä

Fennia on perustettu vuonna 1882. Yhtiön nimi oli aluksi Palovakuutusyhtiö Fennia. Fennian historiassa on myös muita tärkeitä vuosilukuja, jolloin yhtiössä on tapahtunut erilaisia muutoksia. Vuonna 1928 perustettiin Suomen Liikkeenharjoittajien Keskinäinen Vakuutusyhdistys. Nimi muuttui vuonna 1934 Liikkeenharjoittajien Keskinäiseksi Vakuutusyhtiöksi. Vuonna 1947 seurasi uusi nimenvaihdos Yrittäjien Keskinäiseksi Vakuutusyhtiöksi kun Eläke-Varma perustettiin. Sen jälkeen yhtiön nimi on vaihtunut kolme kertaa. Vuonna 1963 Yrittäjien Vakuutus

ja vuonna 1984 Yrittäjien Fennia. Yhtiön historiaan kuuluu myös henkivakuutusyhtiö Novan perustaminen vuonna 1986. Vuonna 1998 syntyi Fennia-ryhmä ja vuonna 2001 Yrittäjien Fennia nimi muutettiin nykyiseen muotoonsa Fenniaksi. Tarkemmin Fennia-ryhmän rakenteeseen palataan opinnäytetyön kohdassa 2.1.2 (Fennia-ryhmä).

2.1.1 Fennian arvot

Arvot ovat lähtökohtana toimintatavoille. Fennia on valinnut viisi perusarvoa, jotka ovat laadukas palvelu, kannustava ilmapiiri, jatkuva kehittyminen, tuloksellinen toiminta ja yrittäjyys. Arvot edistävät asiakkaiden ja henkilöstön tyytyväisyyttä sekä tavoitteiden asettamista. Fennian arvoja voidaan luonnehtia tarkemmin seuraavilla tavoilla.

Laadukkaan palvelun lähtökohtana ovat asiakkaiden tarpeet ja odotukset. Palvelussa pyritään kehittämään toimintatapoja asiakkaiden riskinhallintaan ja toiminnan jatkuvuuden turvaamiseen

Kannustavan ilmapiirin luominen perustuu haasteeseen innostavasta ja yksilöä kunnioittavasta ilmapiiristä. Kannustavassa ilmapiirissä on mahdollisuus saavuttaa laadukkaita tuloksia. Työtovereihin suhtautuminen on kannustavaa ja rakentavaa sekä toiminta on avointa ja luotettavaa.

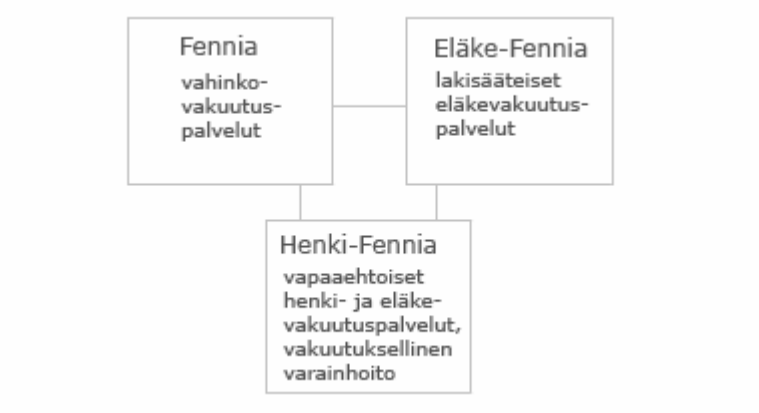
Jatkuvan kehittymisen takaa uudistumiskyky ja uudistumishalu. Jatkuva oppiminen ja hyvistä saavutuksista palkitseminen tukevat jatkuvaa kehittymistä.

Tulokselliseen toimintaan pyritään luomalla pysyviä asiakassuhteita ja kilpailutilanteissa etsitään uusia ja taloudellisesti kannattavia ratkaisuja. Yrittäjyydessä Fennia panostaa määrätietoisuuteen ja luoviin ideoihin. (Fennian arvot).

2.1.2 Fennia-ryhmän rakenne

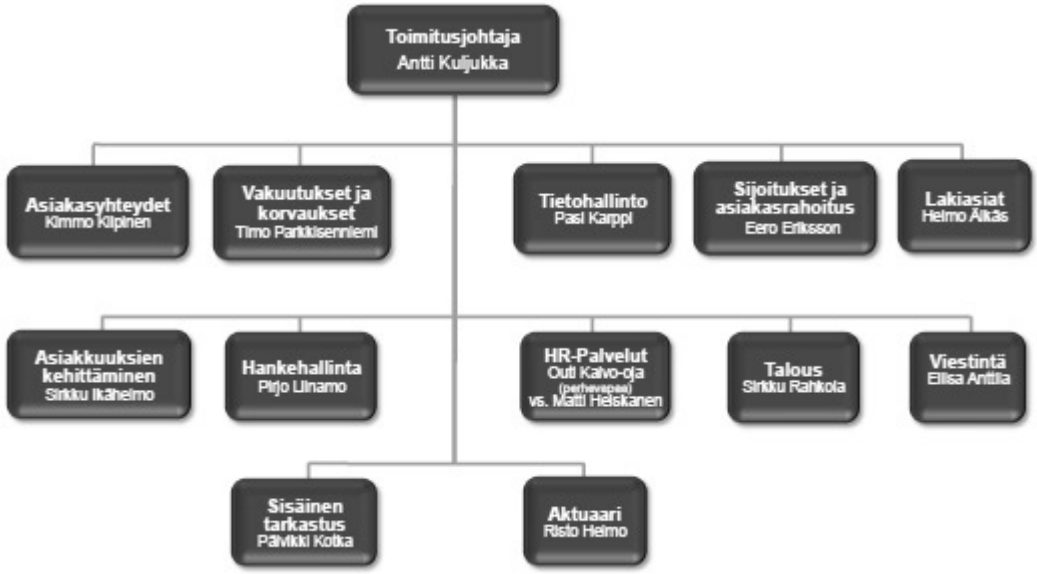
Fennia-ryhmä koostuu kolmesta yhtiöstä, jotka ovat vahinkovakuutusyhtiö Fennia, työeläkeyhtiö Eläke-Fennia ja henkivakuutusyhtiö- Fennia. Työssä keskitymme kuitenkin pelkästään vahinkovakuutusyhtiö Fennian tietoturvallisuuden parantamiseen. Fennian tehtävänä on tarjota yrityksille, yrittäjille ja kotitalouksille

kattavia vakuutuspalveluja. Kuviossa 1 esitellään Fennia-ryhmän rakenne. Organisaatiokaavio on esiteltynä Kuviossa 2.



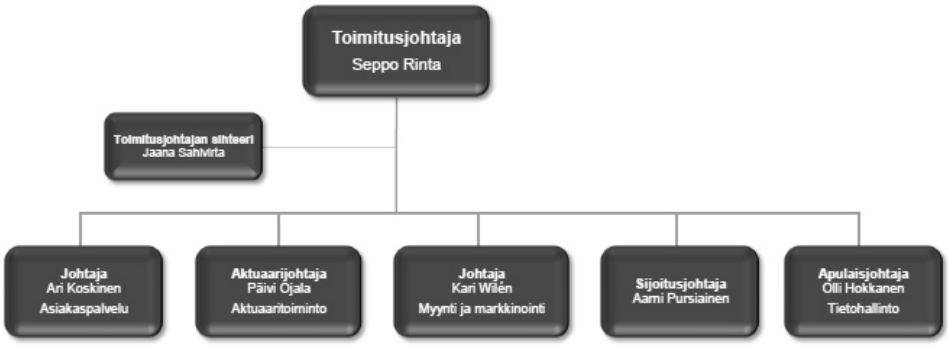
Kuvio 1 Fennia-ryhmän rakenne

Fennia on vahinkovakuutusyhtiö, jolla on Suomessa 60 konttoria. Fennian yhteistyökumppaneina toimivat erilaiset yrittäjäjärjestöt.



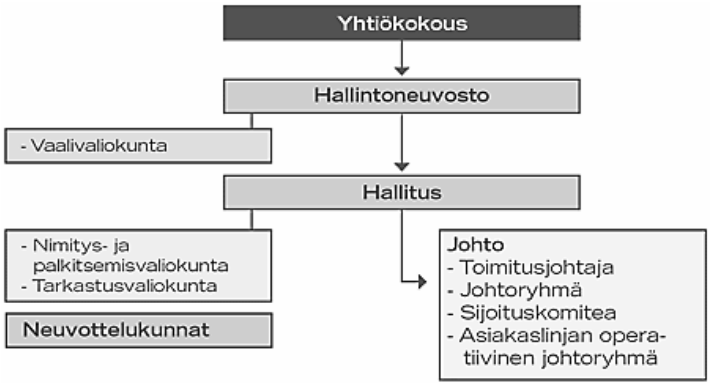
Kuvio 2 Fennia-vahinkovakuutuksen organisaatiokaavio

Henki-Fennia on erikoistunut vapaaehtoisiin henki-, eläke- ja säästövakuutuksiin. Henki-Fennia on kasvava yhtiö ja sillä on useita yhteistyökumppaneita. Henki-Fennian organisaatiokaavio on kuviossa 3.



Kuvio 3 Henki-Fennian organisaatiokaavio

Eläke-Fennia on työeläkeyhtiö, joka huolehtii työntekijöiden ja yrittäjien lakisääteisestä eläketurvasta. TyEL-vakuutuksella työnantaja turvaa työntekijänsä ja YEL-vakuutuksella yrittäjä turvaa oman eläke-etunsa. Eläke- Fennialla on laaja yhteistyökumppaneiden verkko. Kuviossa 4 on esiteltynä Henki-Fennian hallintoelimet.



Kuvio 4 Eläke-Fennia hallintoelimet

Fennia-ryhmän henkilöstön määrä on noin 1200 työntekijää. Uudet toimitilat pääkonttorille valmistuivat vuonna 2009 Helsingin Pasilaan Televisiokadulle. Uusissa

toimitiloissa sijaitsevat tällä hetkellä vakuutusyhtiö Fennian ja Henki-Fennian pääkonttorit. Eläke-Fennian pääkonttori sijaitsee Kansakoulunkujalla. Fennia-ryhmä on myös huomattava kiinteistöjen omistaja. Fennia-ryhmä omistaa noin 2000 asuntoa ja huomattavan määrän toimisto-, liike- ja varastotiloja. Fennia–ryhmä harjoittaa myös vuokraustoimintaa.

2.1.3 Fennian tietohallinto

Tietohallinto ylläpitää ja kehittää Fennian ja Henki- Fennian infraympäristöä. Fennian IT-palveluihin kuuluu käyttäjätukipalvelut, joita ovat puhelinpalvelu ja lähituki sekä järjestelmätuki. Tehtäviin kuuluu myös työasemien, sovelluksien, palvelimien, tietoliikenteen, konttorilaitteiden ja puhelinratkaisujen ylläpito ja kehittäminen. Fennian tietohallinto on vastuussa myös tietohallinnon sopimusten ja lisenssien hallinnasta. Tietohallinnossa työskentelee tällä hetkellä 21 Fennian omaa työntekijää. Lisäksi apuna toimii myös ulkopuolisia asiantuntijoita.

Osastolla työskentelee järjestelmäasiantuntijoita ja Service Deskin-asiantuntijoita. Asiantuntijatehtäviin kuuluu työasemien, sovellusten, palvelimien, tietoliikenteen, konttorilaitteiden ja puhelinratkaisujen ylläpito ja kehitys. Service Desk-asiantuntijat vastaavat käyttäjätukipalveluista.

2.2 Aiheen valinta

Työmme aiheeksi valitsimme 802.1X:n, joka on IEEE:n mukainen standardi. Aiheen valintaan vaikutti suuresti keskustelu esimiehemme kanssa. Pidimme palaverin, jossa pohdimme erilaisia työn aiheita ja tulimme siihen johtopäätökseen, että yrityksen kannalta tietoturvallisuuden parantaminen on kaikkein tärkeintä. Lisäksi aihe on erittäin mielenkiintoinen ja Fennian tietohallinnon kannalta oleellinen.

Aiheen valinta oli meille kohtalaisen helppoa, koska olemme molemmat kiinnostuneet tietoliikenteestä ja sen tietoturvallisuuden parantamiseen. Tämä on erityisesti vakuutusyhtiön kannalta tärkeää, jotta saavutetaan mahdollisimman hyvä tietoturvallisuuden taso. Olemme kumpikin työskennelleet Fennian tietohallinnossa harjoittelijana ja toinen meistä on nyt vakinaisessa työssä yrityksen tietohallinnossa.

2.3 Konttorien IT-infra

Nykyinen laitteisto ja ympäristö ovat täysin yhteensopiva 802.1X:n kanssa. Kytkimet sekä palvelin tulevat kuitenkin muuttumaan, koska tekniikka kehittyy koko ajan ja laitteistoja joudutaan kehittämään ajanmukaisiksi. Alla on tiedot millainen ympäristö Fennialla on tällä hetkellä käytössä.

Ciscon kytkimet: Cisco Systems 2950-2960 Series
Työasemat: Vista-käyttöjärjestelmä
Palvelin: Windows 2003 Server, tulevaisuudessa 2008
Tulostimet: HP-tulostimet ja monitoimilaitteet

3 Tutkimusmenetelmä

Työssä käytettävä tutkimusmenetelmä on konstruktiivinen tapaustutkimus, jossa käytännön ongelmaan yritetään löytää uusi ratkaisu. Konstruktiivinen tutkimus on yksi tapaustutkimuksen alametodi. (Lauronen,2003)

Tapaustutkimus tutkii jotain ilmiötä käytännön asiayhteydessä kokeellisin menetelmin. Tapaustutkimus kuuluu kvalitatiivisiin tutkimusmenetelmiin. Se sopii monille eri tieteenaloille. Tutkittavat tapaukset ovat ainutkertaisia. Niitä tutkitaan aina niiden omassa ympäristössä ja ajassa. Yleisimpiä tämän tutkimuksen soveltuvuusalueita ovat liiketaloustiede, hallintotiede ja kliininen psykologia. (Case tutkimus)

Tapaustutkimuksiin pätee sääntö, että ne pyrkivät tuottamaan intensiivistä ja yksityiskohtaista tietoa tutkittavasta tapauksesta. Tutkimus pyrkii antamaan tilaa ilmiöiden monimuotoisuudelle ja kompleksisuudelle eikä yritä yksinkertaistaa niitä. Tutkittava tapaus voi olla hyvin monenlainen. Se voi olla esimerkiksi yksilö tai ihmisryhmä, tapahtuma tai prosessi. Se voi olla myös maantieteellinen alue. Case pitää kuitenkin ymmärtää aina tiettynä kokonaisuutena. Tapaus ei ole koskaan otos jostain suuremmasta joukosta. Sillä ei myöskään pyritä tilastolliseen yleistämiseen. Tapauksen valintakriteerinä on yleensä teoreettinen kiinnostavuus kyseisen tutkimusongelman kannalta.

Case eli tapaus voi olla tieteenalallaan tyypillinen ja edustava tai toisaalta se voi olla ainutkertainen ja poikkeava ilmiö. Tapaustutkimuksessa tutkittavia tapauksia on vähän, yleensä vain yksi. Tutkimuksessa halutaan perehtyä ilmiön toimintalogiikkaan tai sen muotoutumisprosessiin. Case-tutkimus voidaan toteuttaa myös kahden tai useamman tapauksen vertailuna. Yleensä tässä tutkimuksessa lähdetään liikkeelle analysoitavasta tapauksesta eikä ulkopuolisista yleistävistä teorioista. Tapaustutkimus auttaa tutkittavan ilmiön syvällisessä ymmärtämisessä ja se toimii apuvälineenä muissa vastaavanlaisissa tapauksissa. Tutkimuksilla on siirrettävyysarvoa, vaikka ne eivät ole suoraan yleistettävissä (Tapaustutkimus.)

Määritelmän mukaan konstruktiivinen tutkimusmenetelmän on sellainen, jossa jo olemassa olevan tiedon pohjalta rakennetaan uusia innovaatioita ja tutkitaan kuinka ne tulisi rakentaa. (Järvinen & Järvinen 2004, 104). Innovaatio on tutkimuksen tekijän tai toimeksiantajan tavoittelema uudistus. Uudistuksen tarkoituksena on tuottaa hyötyä.

Konstruktiivisen tutkimuksen tavoitteena on luoda uusi konstruktio, jonka avulla ratkaistaan jokin käytännön ongelma. Konstruktio sitoutuu aina aikaisempaan teoriaan. Konstruktiivinen tutkimus on käsitteellistä konstruointia eli mallintamista, mallien toteutusta, testaamista sekä suunnittelua ja todellisuuden muuttamista havaittujen ongelmien ratkaisemiseksi (Tutkimus seminaari.)

Konstruktiivisen tutkimuksen etuna on se, että se pienentää kuilua tutkimuksen ja käytännön kehitystyön välillä. Tutkimus johtaa myös usein muutoksiin kohdeorganisaatiossa ja mahdollisesti myös laajempaan toiminnan kehittämiseen. Ratkaisun toteutettavuus ja sen käytännön toimivuus testataan aina huolellisesti (Tutkimus seminaari.)

Konstruktiivinen tutkimus kostuu kolmesta osasta, jotka ovat lähtötila, toteuttaminen ja tavoitetila (Järvinen & Järvinen 2004, 107). Tutkimuksen alussa selvitetään lähtötila. Omassa tutkimuksessamme kartoitamme ongelmakohdat sekä selvitämme, miten 802.1X:n suojaus pystytään toteuttamaan Fenniassa. Tällöin on myös tärkeää asettaa projektille tavoitteet, joiden saavuttamiseen pyritään. Lähtötila-kartoituksen jälkeen siirrytään toteuttamisvaiheeseen, joka merkitsee käytännön töiden tekemistä. Tutkimuksen lopuksi tarkastellaan sitä saavutettiinko haluttu lopputulos.

Tarkoituksenamme on tuottaa Fennialle yrityksen toivomuksen mukaan tietoturvallisuuden parannus. Työmme tavoitteena on tutkia sitä, kannattaako Fennian ottaa käyttöönsä 802.1X todennus ja samalla kartoittaa ne edut, joita uudistus tuo mukanaan. Tarkoituksenamme on myös ottaa kantaa siihen, millaiseen käyttöön todennus on tarkoitettu ja millaisia vaatimuksia se asettaa yritykselle esimerkiksi verkon tai laitteiston osalta. Opinnäytetyössämme innovaatio eli uudistus on Fennian tietoturvallisuuden parantaminen 802.1X:n käyttöönoton avulla.

Työn alussa teimme projektillemme aikataulun sekä projektisuunnitelman. Suunnitelmassa oli kirjattuna ne asiat, jotka meidän piti selvittää ennen työn aloittamista. Kartoitimme myös työnantajan vaatimukset ja tarpeet sekä rahalliset puitteet työn tekemiselle. Tärkein vaihe oli se kun kartoitimme asiakkaiden käyttämät laitteet sekä niiden yhteensopivuuden suojauksen toteuttamisen kannalta. Uutta suojausta toteuttaessa on tärkeä huomioida, että se pystytään ottamaan käyttöön myös yrityksen vanhoissa laitteissa. Ennen toteutuksen aloittamista haimme tietoa aiheesta internetistä sekä IT-alan kirjallisuudesta. Työpaikalla ohjaajanamme toimi järjestelmäasiantuntija Marko Tiainen. Häneltä saimme apua aina tarvittaessa.

Tarkoituksemme oli että olemme mukana myös todennuksen käyttöönotossa. Halusimme tämän työn myötä kehittää omaa tietoliikennetietämystämme ja laajentaa tietojamme tietoliikenne- ja tietoturvallisuusasioissa. Koemme, että työ antaa meille tärkeitä tietoja ja taitoja tulevaisuutta ajatellen.

Aihe on vaativa, mutta kiinnostusta herättävä. Erityisenä haasteena on luotettavan tiedon ja kirjallisuuden löytäminen. Myös konfigurointi kohdeyrityksemme ympäristöön asettaa omia vaatimuksia työllemme. Pyrimme työssämme vastaamaan kaikkiin tutkimusprojektin aikana eteen tuleviin haasteisiin.

4 Keskeisimmät käsitteet

Selitämme työssämme käyttämät keskeisimmät käsitteet sekä lyhenteet, jotta 802.1X suojaus olisi helpompi ymmärtää. Protokolliin palaamme vielä työmme kappaleessa 5, jolloin tulee tarkempi kuvaus protokollan toiminnasta.

Asiakas
Laite, jolla yhteys verkkoon halutaan muodostaa. Työssämme tämä tarkoittaa käyttäjän käyttämää työasemaa, joka on vastustettu verkkokortilla.

Asiakasohjelmisto
Asiakasohjelmistolla tarkoitetaan sovellusta. Asiakasohjelmiston toisena nimenä voidaan käyttää myös pääohjelma nimitystä.

Autentikaattori
Laite, joka toimii verkossa. Sisältää liityntäpisteen tai liityntäpisteitä. Välittää todennustietoja autentikointipalvelimelle ja toimii palvelimen antamien ohjeiden mukaisesti. Käytännössä joko muuttaa asiakkaan liityntäpisteen asiakkaalle sallituksi tai ei- sallituksi.

Autentikointipalvelin - AAA
Autentikointipalvelimella on lista käyttäjistä, joilla on lupa käyttää verkkoa. Näiden perusteella palvelin kertoo pyydetyt tiedot autentikaattorille. Käyttäjätietokanta voi sijaita myös ulkoisessa tietokannassa.

EAP
On autentikointi protokolla. Määrittelee mitenkä autentikointiviestit vaihtuvat asiakkaan, autentikaattorin ja AAA-palvelimen välillä. EAP:lla on monia eri versioita, joista jokaisella on erilaisia ominaisuuksia.

EAPOL
on paketointitekniikka, joka kuljettaa EAP viestejä.

IEEE 802 standardi

IEEE (Institute of Electrical and Electronics Engineers) standardointijärjestön työryhmä 802 standardoi lähi- ja kaupunkiverkkoja. Tarkemmin IEEE 802 standardista kerrotaan opinnäytetyön 4 kappaleessa.

LAN
LAN on lähiverkoista käytettävä lyhenne. Englanninkielisenä terminä käytetään Local Area Network. Lähiverkoilla tarkoitetaan tietoliikenneverkkoa, joka toimii rajoitetulla maantieteellisellä alueella.

Liityntäpiste
Kohta verkossa, jonka kautta verkkoon liitytään. Esimerkiksi kytkimen portti toimii verkon liityntäpisteenä.

PEAP
PEAP (Protected Extensible Authentication Protocol) on laillisuustarkistusprotokolla. Se hyödyntää EAP-TLS:ää ja tukee erilaisia laillisuustarkistusmenetelmiä.

Radius
Radius (Remote Authentication Dial In User Service) protokolla auttaa tunnistamaan käyttäjän. Tarkempi radiuksen kuvaus löytyy opinnäytetyöstä kohdasta 5.3.

Sertifikaatti
Sertifikaatilla tarkoitetaan varmennetta, jolla varmistetaan verkkoon pääsy laitteilla joilla on sinne oikeus.

Todennus
Todennuksella tarkoitetaan käyttäjän oikeellisuuden varmistamista.

5 IEEE 802-standardi

IEEE (Institute of Electrical and Electronics Engineers) on amerikkalainen tietoliikenteen alalla toimivat standardointijärjestö. IEEE-standardijärjestön työryhmä 802 standardoi lähi- ja kaupunkiverkkoja. Standardejen tarkoitus on määritellä asiat, jotka vaikuttavat laitteiden yhteistoimintaan. (IEEE802 standard.)

Lähiverkkostandardeista tärkeimmäksi on muodostunut IEEE:n (Institute of Electriacal and Electronic Engineers) 802-standardiperhe. (IEEE802 standard.)

Alunperin tarkoituksena oli tehdä yksi kattava ratkaisu. Tämä kuitenkin huomattiin mahdottomaksi useista erilaisista sovelluskohteista johtuen. Tämän vuoksi pyrkimys muutettiin yhteensopivaksi standardiperheeksi, jossa standardit 802.1 ja 802.2 ovat kaikille yhteisiä ja standardit 802.3-802.16 ovat lähiverkkostandardeja (IEEE802 standard.)

802-standardi koostuu seuraavista osastandardeista:

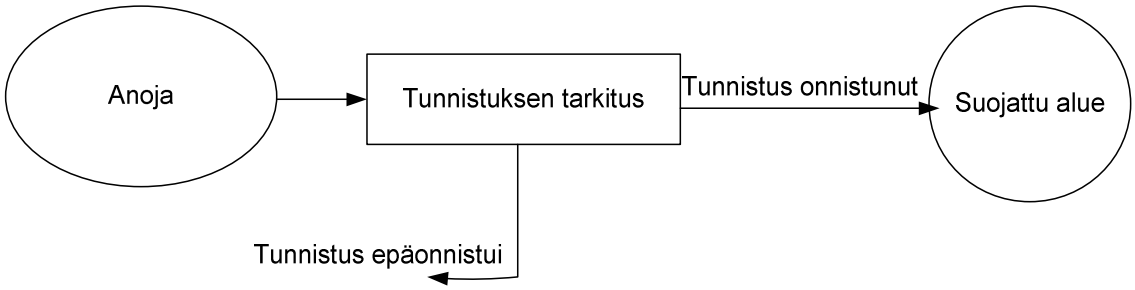
802.1: Määrittää osoitteiston, yhdysliikenteen ja arkkitehtuurin
802.2: Siirtoyhteyden ohjaus LLC (Logical Link Control), kaikille standardiverkoille yhteinen siirtoyhteysprotokolla. Määrittä kahden aseman välisen liikennöinnin kulun.
802.3: Kuulostelu- ja törmäyksen tunnistusväylä (CSMA/CD, Carrier Sense Multiple Access with Collision Detection), sisältää Ethernetin ja Starlanin. Kaapelointivaihtoehtoina ovat mm. paksu koaksiaalikaapeli (10BASE5, paksu Ethernet), ohut koaksiaalikaapeli (10BASE2, ohut Ethernet), parikaapeli (10BASET) ja valokuitu.
802.4: määrittelee valtuudenvälitykseen perustuvan vuoroväylän. Vuoroväylä on käytössä teollisuusautomaatiossa MAO-protokollakokonaisuudessa (Manufacturing Automation Protocol)
802.5: Määrittelee Vuororenkaan(Token ring)
802.6: määrittelee alueverkkoja. (MAN, Metropolitan Area Network) Valokuitutekniikalla toteutettu suunnilleen kaupungin käsittävä verkko. Määrittelee runkoverkon ja rakennuksissa olevien lähiverkkojen liittämisen kaupunkiverkkoon.
802.7: Laajakaistaverkko, laajakaistatekniikan soveltaminen lähiverkkoihin.
802.8: Määrittelee valokuidun käytön lähiverkoissa
802.9: Määrittelee puheen ja kuvan integroinnin lähiverkossa
802.10: Lähiverkkojen tietoturva

802.11: Langattomat lähiverkot

Standardin nimeksi tuli 802 sen johdosta, että se oli seuraavana vuorossa IEEE:n standardointi projektissa. Standardit ovat luettavissa järjestön nettisivuilla.

5.1 Yleistä 802.1X:stä

802.1X on standardi, jota voi käyttää lähiverkossa. Se toimii OSI-mallin toisella kerroksella eli linkkitasolla ja mahdollistaa pääsynvalvonnan IEEE802 verkossa. Tarkoituksena on todentaa portin kautta käyttäjä ja sitä kautta estää luvattomien laitteiden pääsy verkkoon. Tunnistus toteutetaan käyttäen jotakin EAPOL-protokollaa. Kuvassa 5 kuvataan yksinkertaisesti käyttäjän todennus. (Jim Geiner,2008 s. 23)



Kuva 5 Käyttäjän todentamisesta esimerkki

Suojauksen ollessa käytössä työasemien pitää todentaa olevansa oikeutettuja verkkopalvelun käyttäjiä. Tällaisia verkkopalveluja ovat esimerkiksi sähköposti ja Internet. Jos todennus onnistuu, pääsee työasemalta normaalisti käyttämään verkkopalveluita. Epäonnistunut todennus puolestaan sulkee työaseman pääsyn verkkopalveluista. (IPV6)

Kyseessä on hyvin yksinkertainen todennusmenetelmä. Asian voi esittää pienellä esimerkillä. Esimerkissä Seija saapuu lentoasemalle ja hän yrittää varmistaa koneensa lähdön Dallasissa. Lentoyhtiön edustaja haluaa varmistaa Seijan

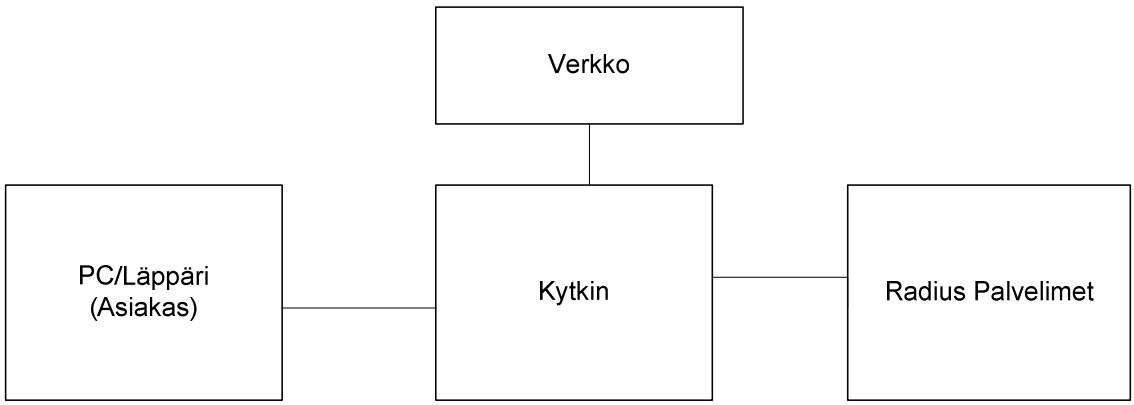
ajokortista, että kyseessä on oikea henkilö. Ajokortin kuvan ja muiden tietojen perusteella lentoyhtiön edustaja voi olla varma, että kyseessä on oikea Seija. Tämä on täysin samanlainen autentikointitapahtuma. Jos kyseinen henkilö ei olisi oikea Seija, ei hän saisi haluamaansa tietoa.

Tietotekniikassa todentaminen vaatii kuitenkin hieman enemmän tietämystä asioista. Verkkolaitteille on itse kerrottava mitä tehdään ja millaisilla ehdoilla käyttäjät saavat käyttää verkkoa. Ohjeistus ei jätä varaa virheille. Järjestelmien on myös oltava yhteensopivia, koska yksi epäsopiva laite saattaa estää todennuksen toiminnan ja se tuo taas suojaukselle täyden arvottomuuden. (Jim Geiner2008 s.54)

802.1X on tarkoitettu käytettäväksi kaikissa IEEE802 verkoissa. Se mahdollistaa laajemmat suojaukset kuin verkossa yleisesti käytettävät käyttäjähallintamenetelmät mahdollistavat. Muut menetelmät ovat yleensä rajoittaneet ainoastaan käyttäjän pääsyä palvelimelle sekä työasemiin. (Hakala-Vainio-Vuorinen 2006, s. 298)

Työmme tarkoituksena on estää luvattomien käyttäjien pääsy kytkinporttien kautta yrityksen verkkoon ja siihen 802.1X luo erittäin hyvät mahdollisuudet, jos sen toteuttaa yrityksessä oikealla tavalla.

Kuvassa 6 on esiteltynä tarkemmin 802.1X:n toimintaympäristö. Toimintaympäristö on samanlainen kuin se johon toteutamme suojausta. Ensimmäiseksi on asiakas eli käyttäjän käyttämä työasema. Käyttäjän halutessa verkkoon hän käynnistää tietokoneelta ohjelman. Työasema katsoo asetustiedoistaan mitä autentikointitapaa sen tulisi käyttää. Sen jälkeen työasema lähettää reitittimelle pyynnön määriteltyä autentikointitapaa käyttäen. Tukiasema välittää tiedon eteenpäin Radius-palvelimelle. Jos autentikointi onnistuu Radius ilmoittaa onnistumisesta reitittimelle ja päästää asiakkaan verkkoon. Jos todennus epäonnistuu, evätään asiakkaan pääsy verkkoon.



Kuva 6 802.1X toimintaympäristö

5.2 Synty

Paremman tietoturvallisuuden tarve ja käyttäjien kontrollointi loi tarpeen 802.1X:lle. Kytkimen portti on käyttäjien luonnollisin kontrollointipaikka, koska se toimii käyttäjälle lähiverkon pääsykohtana. (Jim Geiner 2008, s. 45)

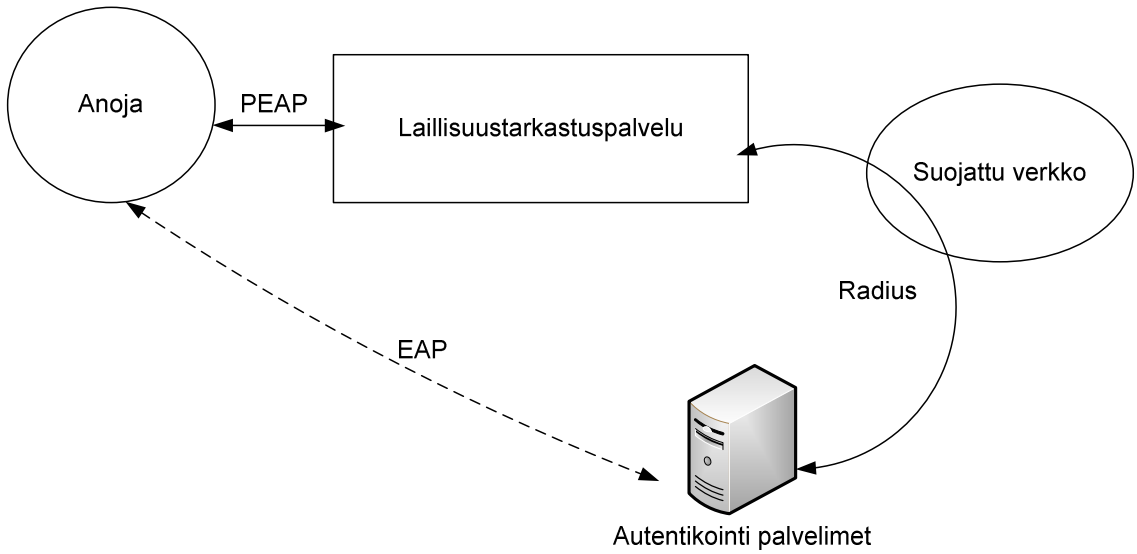
5.3 Toiminta

802.1X toimii porttikohtaisena todentamisena, jonka johdosta sen toimintaa voidaan kuvata laillisuustarkastuspalveluna. Se kommunikoi anojan kanssa ja välittää siltä saamansa tiedot autentikointipalvelimelle.(ipv6) Todennuksen suorittaa EAP-protokolla, johon palaamme luvussa 6. Kuvassa 7 on selitettynä enemmän porttikohtaisen todentamisen toiminta.

802.1X:n toiminnassa on kolme keskeistä osaa 1) anoja (supplicant) 2) autentikointipalvelin (autentication server), joka on yleensä radius-palvelin sekä 3) laillisuustarkastus palvelu (Autenticator). Anojalla tarkoitetaan asiakkaan laitetta, joka haluaa käyttää suojattua verkkoa. Tämän johdosta kone on ensiksi todennettava ennen verkkoon pääsyä. Anoja keskustelee autentikointipalvelimen kanssa käyttäen EAP-protokollaa. Kerromme tarkemmin EAP-protokollasta luvussa 6.

Laillisuustarkastuspalvelulla tarkoitetaan puolestaan verkkolaitetta, joka toimii OSI-mallin toisella tasolla, esimerkiksi kytkin on tällainen. Verkkolaite ei ota anojaa vastaan ennen kuin sen todentaminen on suoritettu. Kun todennus on onnistuneesti

suoritettu laillisuustarkastuspalvelu avaa portin, jotta käyttäjä pääsee käyttämään suojattua verkkoa.



Kuva 7 Porttikohtaisen todentamisen toiminta

802.1X suojaus saadaan käyttöön monenlaisissa käyttöjärjestelmissä. Windowsissa (XP, Vista, Windows 7) on sisäänrakennettu tuki 802.1X-protokollalle. Mac OSX on tukenut 802.1X:n toimintaa 10.3.2009 lähtien. Ainoastaan Linux-käyttöjärjestelmä vaatii erillisen ohjelman käyttämisen, jotta 802.1X voitaisiin ottaa käyttöön käyttöjärjestelmässä. Tässä työssä keskitymme kuitenkin Windows Vistassa toteutettuun suojaukseen, koska kohdeyrityksessämme on Vista-käyttöjärjestelmä käytössä työasemissa.

Vaatimuksena suojauksen käyttöönotolle on, että työasemien ja kytkimien on tuettava 802.1X protokollaa sekä Radius-palvelimen on tuettava EAP-protokollaa.

5.4 802.1X:n toimintaedellytykset

Olemme listanneet 802.1X:n toiminnanedellytykset. Ilman alla lueteltuja asioita 802.1X suojausta ei pystyttäisi ottamaan käyttöön.

- koneisiin Ethernet-verkkokortit
- Vistan Wired AutoConfig-palvelu
- vähintään kaksi IAS-palvelinta (yksi ensijainen, toinen vara)
- (Windows 2008 serverissä NPS)
- Windows 2003 tai 2008-serveri
- tietokoneiden sertifikaatit on asennettu IAS-palvelimelle
- tietokoneeseen sertifikaatteja IAS-palvelimelta
- koneissa on SP2
- kone saa IP-osoitteen.

5.5 Hyödyt ja haitat

802.1X:n käyttäjän tietoturvallisuus on paremmalla tasolla, koska se rajaa portilla käyttäjät. Se rajaa käyttäjät kahteen ryhmään, sallittuihin ja sallimattomiin. Jos käyttäjää ei tunnisteta, suojaus ohjaa käyttäjän pois. Jos käyttäjä taas tunnistetaan, päästetään hänet normaalisti sisään. Käyttäjä itse ei edes huomaa suojauksen olemassa oloa. Käyttäjä pystyy käyttämään konetta mistä tahansa alueen verkkoportista ja suojaus tehostaa liikkuvuutta sekä käytön helppoutta. Sillä on myös tuottavuutta nostava vaikutus.

Suojauksen käyttöönotolla estetään verkkoon pääsy koneilta, joille ei ole annettu lupaa käyttää Fennian verkkoa. Ainoastaan yrityksen omille koneille halutaan antaa pääsy Fennian verkkoon. 802.1X:n avulla pystymme rajaamaan käytön yrityksen haluamalla tavalla. Näin vähennämme riskejä ja rajaamme ne laitteet, jolla on pääsy verkkoon.

Suojauksen käyttöönotto korostaa ylläpidon merkitystä. Verkosta tulee yritykselle vielä tärkeämpi. Ongelmaksi voi muodostua se, että väärillä asetuksilla saatetaan estää sellaiselta koneelta pääsy Fennian verkkoon, jolle pääsyoikeus kuuluisi.

6 Aiheeseen liittyvät protokollat

6.1 EAP-protokollat

EAP eli Extensible Authentication Protocol on väline, joka suorittaa todentamisen. Todentamisen pystyy suorittamaan millä tahansa käytössä olevalla menetelmällä.

EAP vaatii toimiakseen asiakaskoneen, tukiaseman ja tunnistuspalvelimen. Protokolla tarjoaa todella hyvän turvallisuuden.

Normaali EAP-tunnistusprosessi alkaa siitä, kun palvelin lähettää käyttäjän järjestelmälle tunnistuspyynnön. Pyyntö sisältää tiedon siitä millaista tunnistusta palvelin haluaa. Käyttäjän kone lähettää vastauksen pyyntöön. Vastaus sisältää halutut tiedot. Tämä keskustelu jatkuu, kunnes käyttäjä on oikein tunnistautunut järjestelmään tai käyttäjän tunnus on todettu epäonnistuneeksi.

6.2 EAPOL

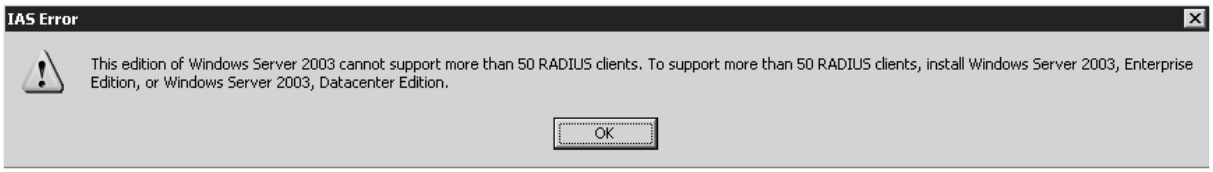
EAPOL (Extensible Authentication Protocol Over LAN) on paketointi tekniikka, jolla IEEE 802.1X protokollan EAP paketit kuljettaa. EAPOL keyn avulla pystytään tarkkailemaan epäonnistuneita autentikointi yrityksiä. (Implementing 802.1X s.55)

EAPOL ei kuitenkaan anna kirjautumismenetelmää, vaan sitä varten tulee käyttää EAP tyyppiä eli joko EAP-TLS:ää tai EAP-TTLS:ää. Nämä määrittelevät miten tunnistautuminen tapahtuu. EAP-TTLS on muuten sama kuin EAP-TLS, mutta on tunneloitu mikä puolestaan parantaa tietoturvallisuuden tasoa. EAP-TLS:n merkittävin etu on se, että se on riippumaton verkosta ja ohjelmista.

6.3 RADIUS

Alunperin Raudius (Remote Access Dial In User Service) - protokolla on kehitetty käyttäjien tunnistukseen käyttäjätunnuksen ja salasanan perusteella heidän kirjautuessaan esimerkiksi modeemilla palveluntarjoajan soittosarjaan. Nykyisin protokolla on otettu käyttöön myös monissa muissa tunnistusta vaativissa verkkopalveluissa. Radius-palvelimen tehtävä on tunnistaa käyttäjä ja välittää muut tarvittavat tiedot tunnistusta pyytävälle palvelulle. Protokolla on rakennettu UDP-protokollan päälle. (Implementing s. 71)

Radius-laitteet (clientit) lisätään IAS palvelimelle. Laitteita lisätessä yli 50 kappaletta vaaditaan Server 2003 Enterprise-versio. Tämän johdosta työmme toteutetaan Enterprise-versiolla. Kuvassa 8 on esiteltynä virheilmoitus, joka tulee kun laitteita lisätään yli 50 kappaletta.



Kuva 8 Virheilmoitus

7 Käyttöönoton teoria

Työssämme esiintyy myös maininta 802.1X:n käyttöönotosta Fenniassa. Tätä varten meidän on tutustuttava yleisesti uusien järjestelmien käyttöönottotapoihin yrityksissä. Fennialla ei ole yhteisesti sovittua tapaa tässä asiassa, joten joudumme itse miettimään, sitä minkälainen tapa olisi yritykselle paras. Pohdimme myös sitä minkälainen tapa sopisi parhaiten 802.1X:n käyttöönoton kanssa.

Yrityksen kannalta on erityisen tärkeätä se, että uuden asian käyttöönotto sujuu hyvin eikä se aiheuta ongelmia asiakkaille. Tämän johdosta testasimme 802.1X:n toimintaa erittäin tarkasti omassa testauslaboratoriossamme. Käyttämämme laboratorio vastaa täysin Fennian konttoreilla olevaa IT-infraa. Työmme pilotoitiin tarkasti tuotantoympäristössä ennen laajempaa käyttöönottoa. Tuotantoympäristömme ovat käyttöönoton kannalta samanlaisia, joten erilaisia määrityksiä ei tarvita. Suojausta toteuttaessamme teimme koko ajan tarkkoja muistiinpanoja, jotta suojauksen pystyisi tarvittaessa tekemään myös henkilö, jolla ei ole taustallaan sitä tietoa mitä meillä oli työtä tehdessämme.

Uuden asian, esimerkiksi suojauksen käyttöönotossa pitää ensimmäiseksi miettiä tarkkaan se ympäristö missä muutos toteutetaan. Lisäksi pitää miettiä sitä ketkä ovat käyttäjiä. Toiminnan kuvaaminen projektin aikana on myös tärkeää. Seuraavana vaiheena on muutoksen testaus ja viimeinen vaihe on uuden asian käyttöönotto. Testaus on tärkein vaihe ennen käyttöönottoa. Testaus tehdään, jotta uudesta asiasta pystytään kartoittamaan ongelmakohdat mahdollisimman tarkasti. Lisäksi etsitään asioita, joita voisi mahdollisesti tehdä toisella tavalla ennen käyttöönottoa.

Käyttöönotto on onnistunut silloin kun käyttäjät eivät ole huomanneet muutoksen aiheuttaneen ongelmia ja heidän oma työnsä on voinut jatkua lähes keskeytyksettä.

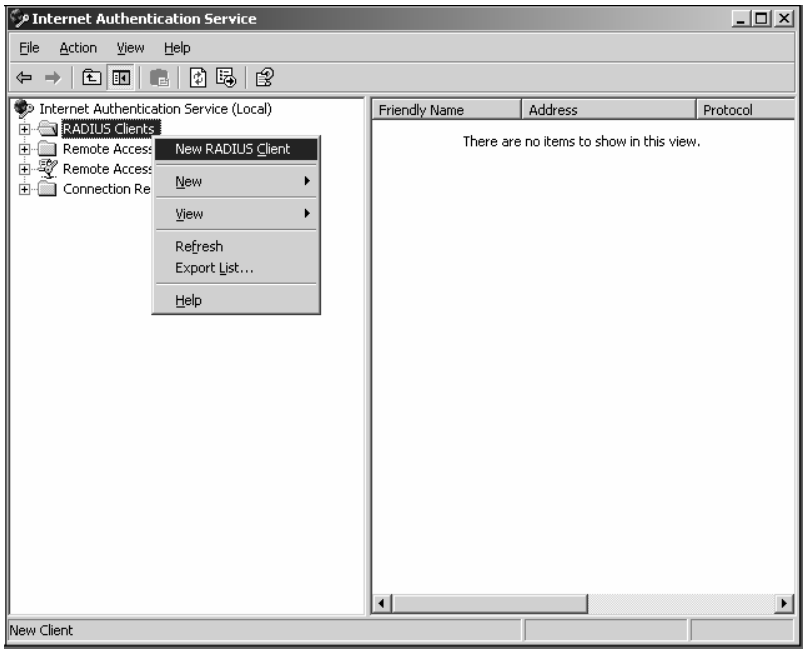
8 Käytännön toteutus Fenniassa

Käyttöönottotapana projektissa oli ns. suora käyttöönotto. Se toteutetaan niin, että suojaus integroidaan suoraan yrityksen olemassa olevaan järjestelmään. Tämä ei vaadi erillistä käyttäjäkoulutusta, koska käyttäjien ei pitäisi edes tietää suojauksen olemassa olosta. Heidän pitäisi pystyä käyttämään omia työpisteitään normaalisti, ilman erillisiä katkoksia. Tällöin käytännön toteutus olisi hyvin onnistunut.

8.1 Radius-palvelimen asetukset

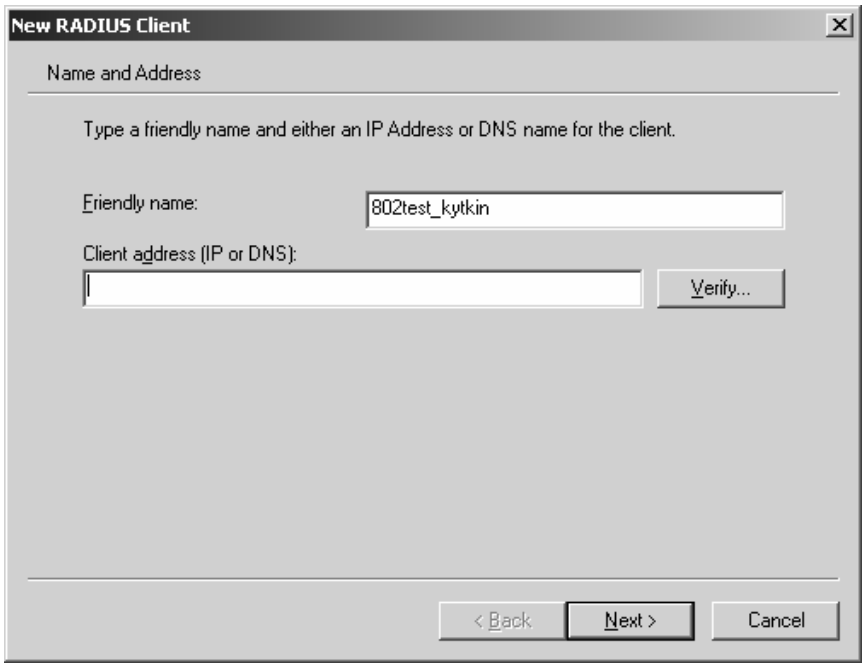
Tässä kohdassa esittelemme kuinka asetimme Radius-palvelimen asetukset sopivaksi 802.1X varten. Aivan aluksi teimme palvelimelle perusmäärittelyt ja asensimme palvelimelle IIS (Internet Information Services) ja IAS (Internet Authentication Services) palvelut. Tämän jälkeen pääsimme lisäämään valitut laitteet testiympäristöön.

Lisäsimme valitsemat laitteet Radius Clients hakemiston alle. Testiympäristössä meillä oli käytettävissä palvelimen lisäksi yksi Ciscon testikytkin 802.1X konfiguraatiota varten ja useita kannettavia.



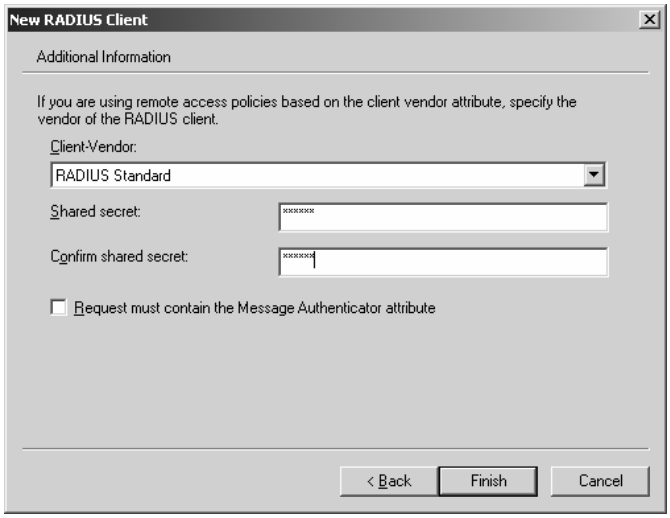
Kuva 9 Lisätään uusi laite Radius Client kohdan alle

Lisäsimme kytkimen 802test_kytkin nimellä, millä se on löydettävissä helposti muiden laitteiden joukosta. Määrittelimme laitteelle myös IP-osoitteen, mitä ei voitu tuoda näkyviin tietoturvallisuus syistä.



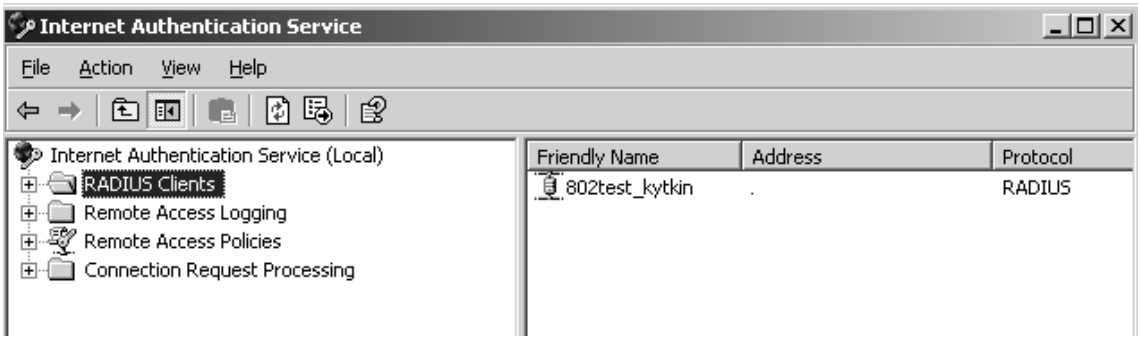
Kuva 10 Nimetään lisättävä laite ja annetaan sille IP-osoite

Annoimme laitteelle jo kytkimen konfiguraatiossa määritellyn avaimen, jonka avulla se pystyy olemaan yhteydessä Radius-palvelimeen.



Kuva 11 Avaimen lisääminen

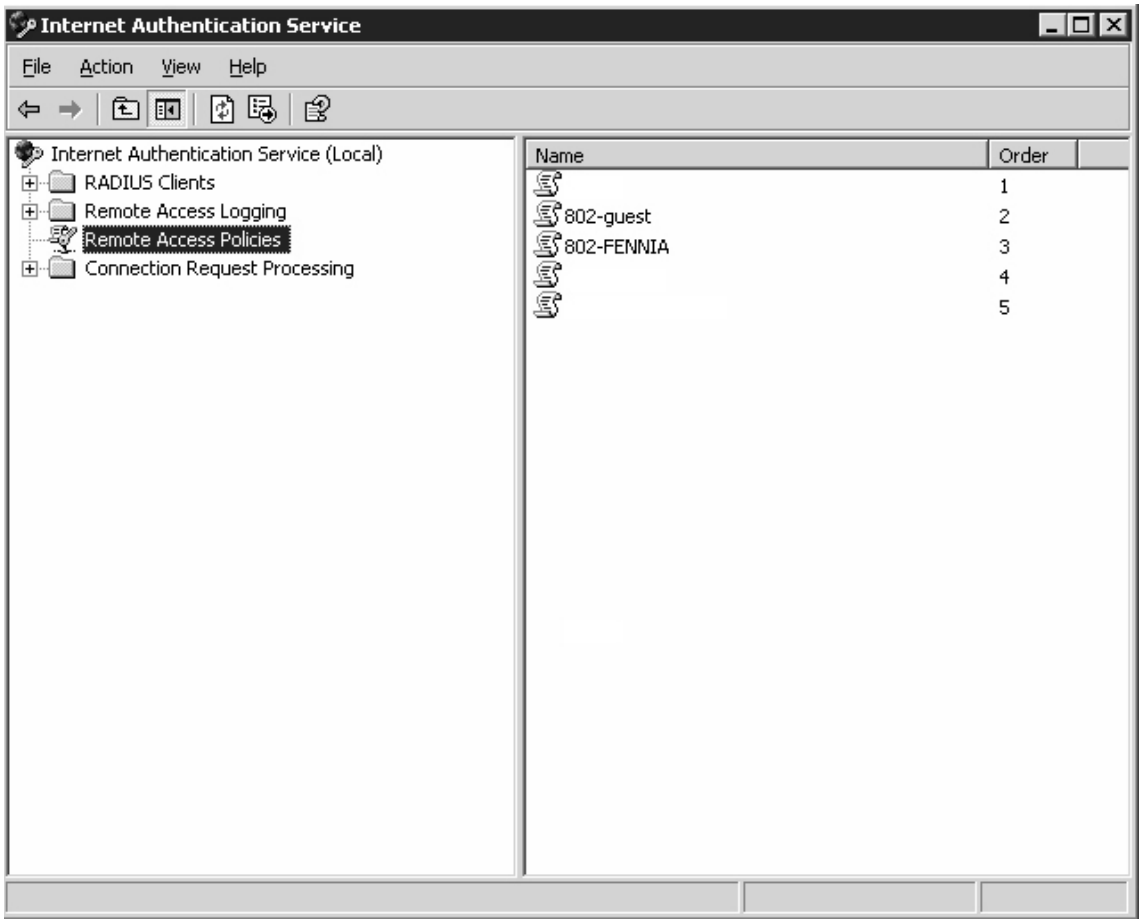
Laite lisättiin onnistuneesti Radius laitteiden alle. IP-osoite on peitettynä tietoturvallisuus syistä.



Kuva 12 IAS serverille luotu Radius laite

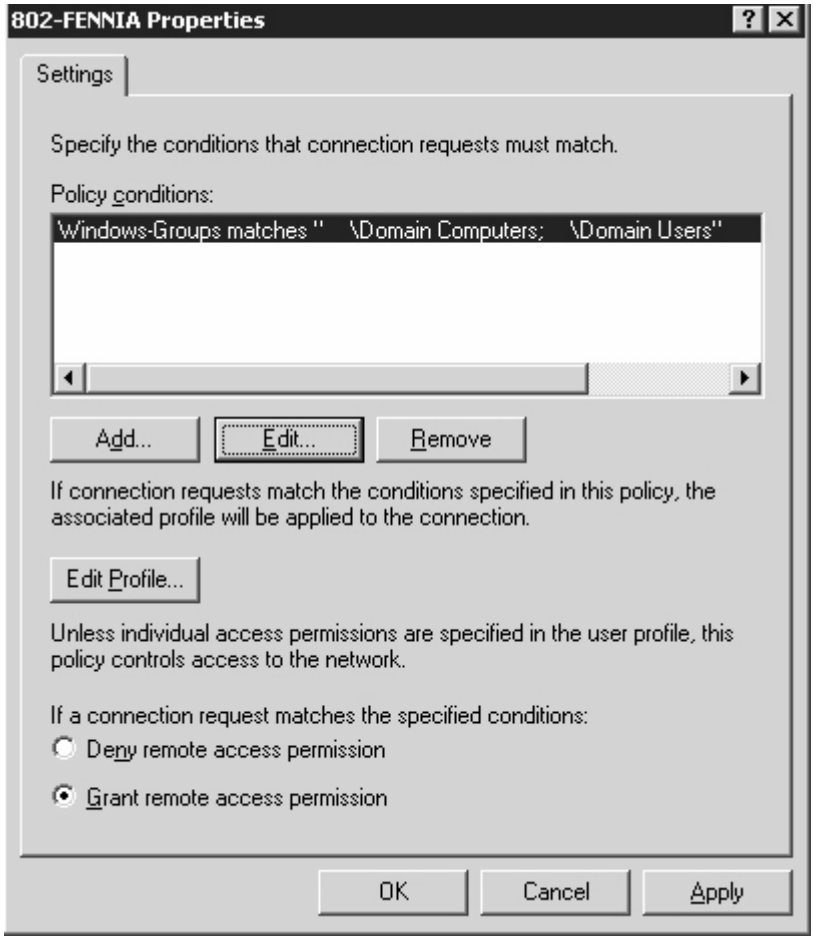
8.2 Sääntöjen luominen Radius-palvelimelle

Loimme Radius-palvelimelle säännöt, joiden avulla kone saadaan ohjautumaan oikeaan verkkoon. Oikeanlaisen autentikoitumisen jälkeen kone siirtyy ensin vierailijaverkkoon 802-guest säännön mukaisesti, minkä jälkeen se ohjataan tuotantoverkkoon. Säännöillä kerrotaan missä järjestyksessä kone ohjataan verkkoon. Koneen tulee olla Fennian domainissa, sekä nimettynä oikein.



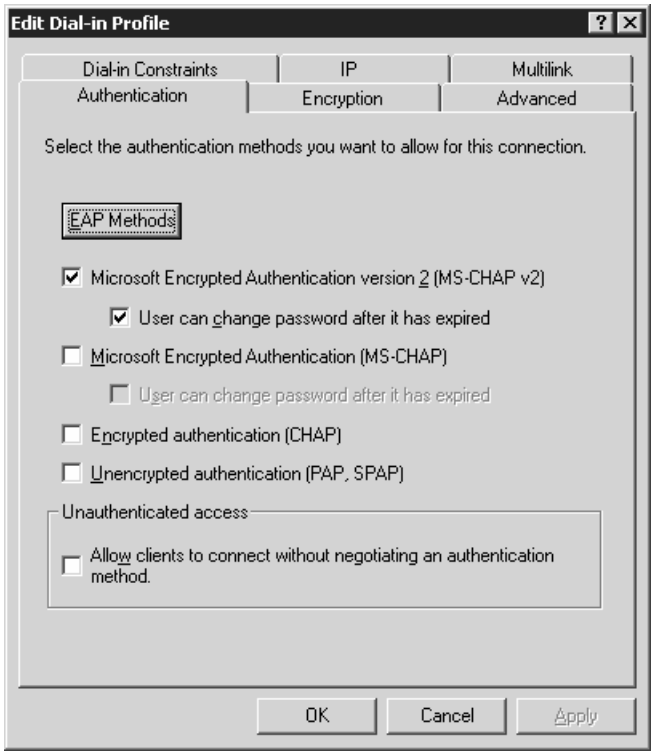
Kuva 13 Määritellyt säännöt

Palvelimen AD-järjestelmästä täytyy löytyä koneiden tiedot, jotta autentikoituminen olisi mahdollista. Koneen on kuuluttava kuvan 22 mukaisiin xx\Domain Computers ja xx\Domain Users AD:n ryhmiin, jotta ehdot täyttyisivät ja autentikoituminen sallittaisiin.



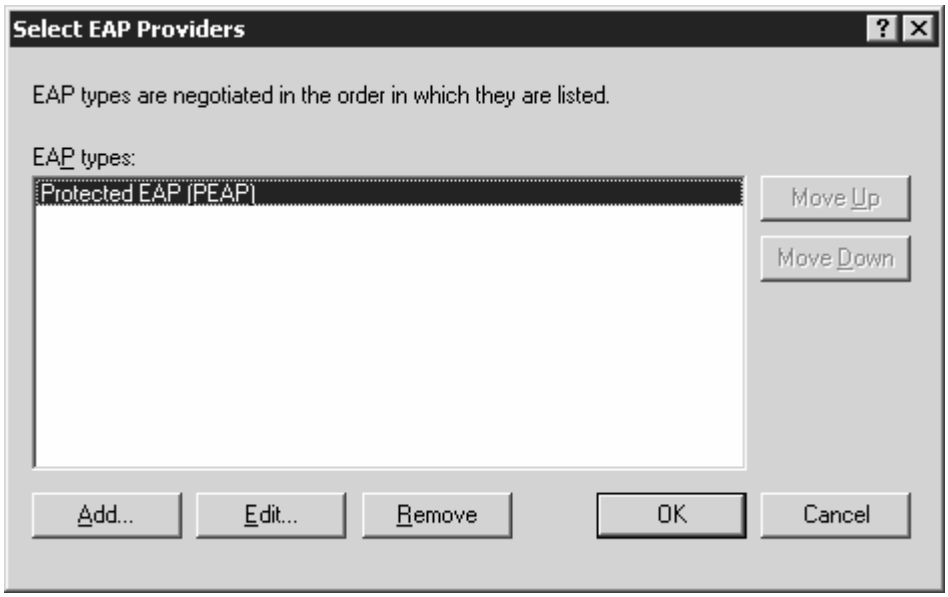
Kuva 14 Säännön ehdot

Valitsimme MS-CHAP v2 käyttöön oletusasetuksien mukaisesti, mikä myös mahdollistaa käyttäjälle salasanan vaihtamisen sen vanhentuessa. Ominaisuus on käytettävissä PEAP:n yhteydessä.



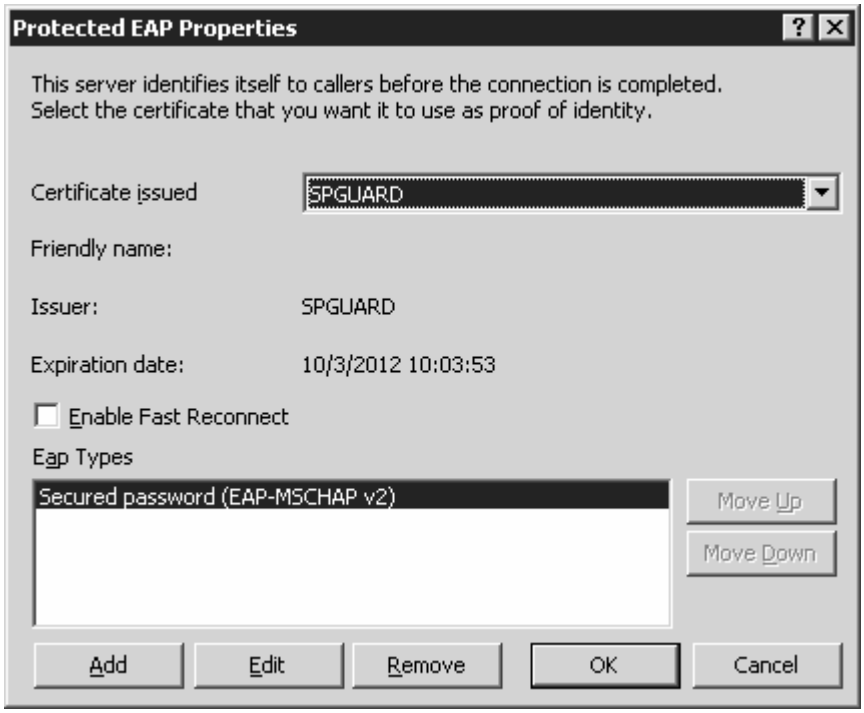
Kuva 15 Otettiin MS-CHAP v2 käyttöön oletusasetuksien mukaisesti

Valitsimme suojatun Protected EAP (PEAP) protokollaan käyttöön. Se oli ainut mahdollisuus käyttöjärjestelmän takia ja se on myös tietoturvan puolesta kannattavin vaihtoehto.



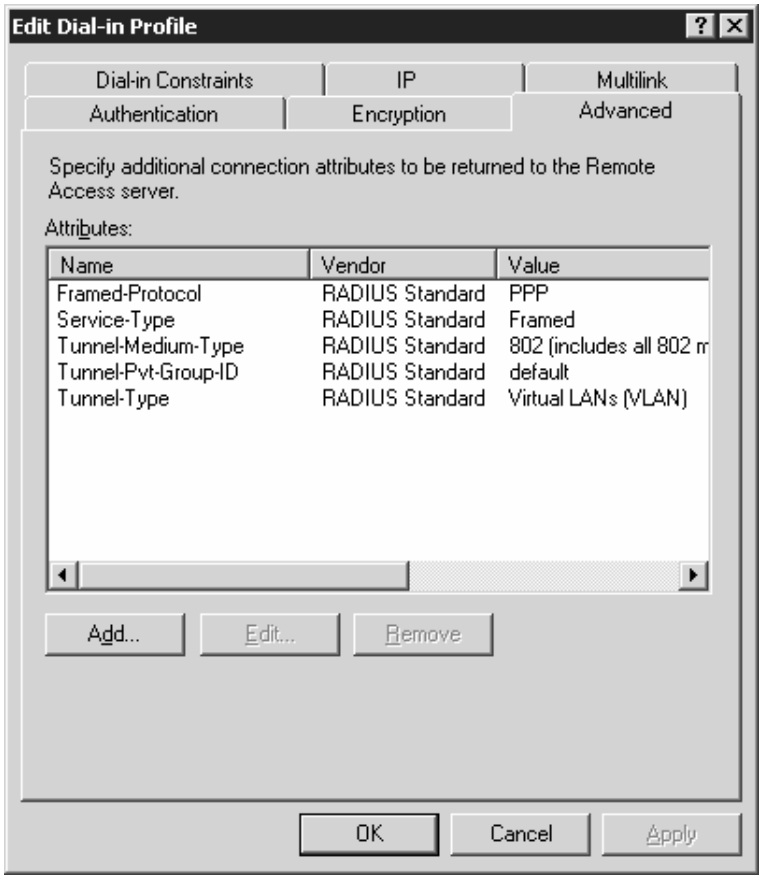
Kuva 16 Valittiin suojattu PEAP-protokolla käyttöön

Protokollan asetuksista määrittelimme luomamme sertifikaatin käyttöön. Sama sertifikaatti tarvitaan myös Fennian työasemiin. Tämä on edellytyksenä todennuksen onnistumiselle.



Kuva 17 Ilmoitetaan mitä sertifikaattia käytetään

Määrittelimme 802.1X:n käyttöönottoa varten oikeat attribuutit. Tärkeimmät näistä ovat ovat Tunnel-Medium-Type[65], Tunnel-Pvt-Group-ID[81] ja Tunnel-Type[64]. Tunnel-type ja Tunnel-Medium-Typen arvot täytyy määritellä kuvan mukaisesti. Ilman näitä VLAN-ohjauksia tekevä kytkin ei osaa ohjata liikennettä oikealla tavalla ja koko autentikoituminen epäonnistuu. Tunnel-Pvt-Group-ID:ta varten on AD:ssa luotuna oma ryhmä, minne lisäsimme testikäyttäjän. Attribuutin arvoksi annettiin AD:n VLAN-ryhmän nimi ja sama nimi täytyi myös löytyä kytkimen VLAN-konfiguraatiosta. Kytkin tarkistaa, että ryhmän nimi tai arvo pitävät paikkansa ja näillä ehdoin joko hyväksyy ja estää autentikoitumisen.



Kuva 18 Käytetyt attributit

8.3 Kytkimen konfigurointi

Työn liitteenä on tarkempi kuvaus kytkimen konfiguroinneista. Seuraavassa on selvitettynä ne asiat, jotka muutimme. Muutokset löytyvät liitteenä olevasta listasta mustalla kirjoitettuna.

Kaikki aaa komennot asensimme Cisco- manuaalin mukaisesti.

aaa new-model
aaa authentication login default group radius enable
aaa authentication dot1x default group radius
aaa authorization network default group radius

Määrittelimme kytkimeen 802.1X käyttöön.

dot1x system-auth-control

VLAN-ryhmä luotu käyttäjille joiden ei ole tarkoitus päästä yrityksen verkkoon.

vlan 89
 name guest

Tähän ryhmään koneet aluksi joutuvat, kunnes sertifikaatti on varmennettu.

vlan 100
 name guarantine

Tähän ryhmään työasema aluksi menee. Tässä vaiheessa verkkoyhteys ei ole vielä käytettävissä.

interface FastEthernet0/3
 description Tyoaseman Malli
 switchport access vlan 100

Määritellään portti automaattiseksi.

dot1x port-control auto

Säädetään aikaväli, kuinka usein uudelleen autentikoituminen tapahtuu.

dot1x timeout quiet-period 30

Määritellään ohjaus minne työasema joutuu, kun sertifikaattia ei ole.

dot1x guest-vlan 89 (vlan johon työasema menee jos ei ole sertifikaattia)

Sallitaan uudelleen autentikoituminen portille.

dot1x reauthentication

Määriteltiin Radius-palvelimen osoite ja portit (oletuksilla).

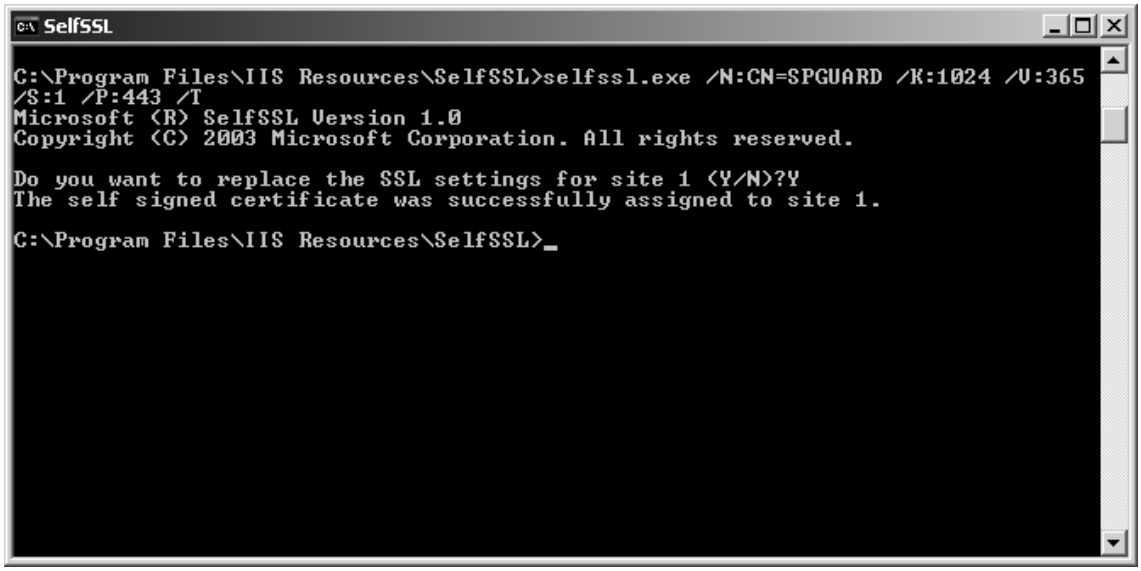
radius-server host X.X.X.X auth-port 1812 acct-port 1813 key XXXXXXXXXXXXX

8.4 Varmenteiden luominen ja hakeminen

802.1X:n suojauksessa on olennaista, että palvelimeen on luotu varmenne. Varmenne varmistaa sen, että laitteella on oikeus päästä yrityksen verkkoon. Testasimme suojauksen toimintaa itse luodulla varmenteella. Myöhemmin käyttöönoton yhteydessä on kuitenkin tarkoitus käyttää Soneralta ostettuja varmenteita.

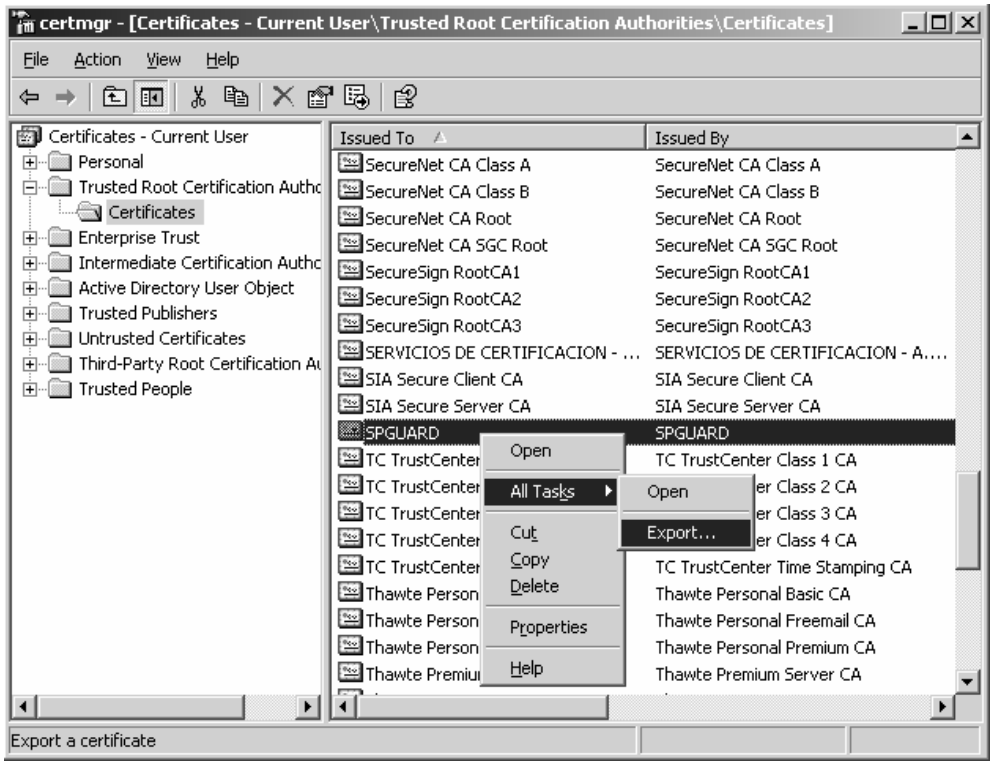
Ohjelma jolla teimme varmenteita on IIS palvelun lisäpalvelu. Esittelemme miten ohjelman asennus tapahtuu ja mitä asetuksia tulee valita, jotta ohjelma asentuisi oikealla tavalla. Tämän jälkeen varmenteet tulee vielä hakea laitteille, joilla halutaan mennä yrityksen verkkoon. Tärkeintä on saada varmenteet laitteille, joilla halutaan mennä yrityksen verkkoon. Varmenne tulee asennuksen jälkeen näkyviin laitteen verkkokortille sekä selaimen varmenteisiin.

Käytimme varmenteen luomiseen IIS Resources-paketin mukana tulevaa SelfSSL-ohjelmistoa. Komennon avulla määrittelimme varmenteelle nimen, avaimen koon ja voimassaoloajan. Varmenne tallentuu palvelimelle luotettujen varmenteiden päämyöntäjien alle.



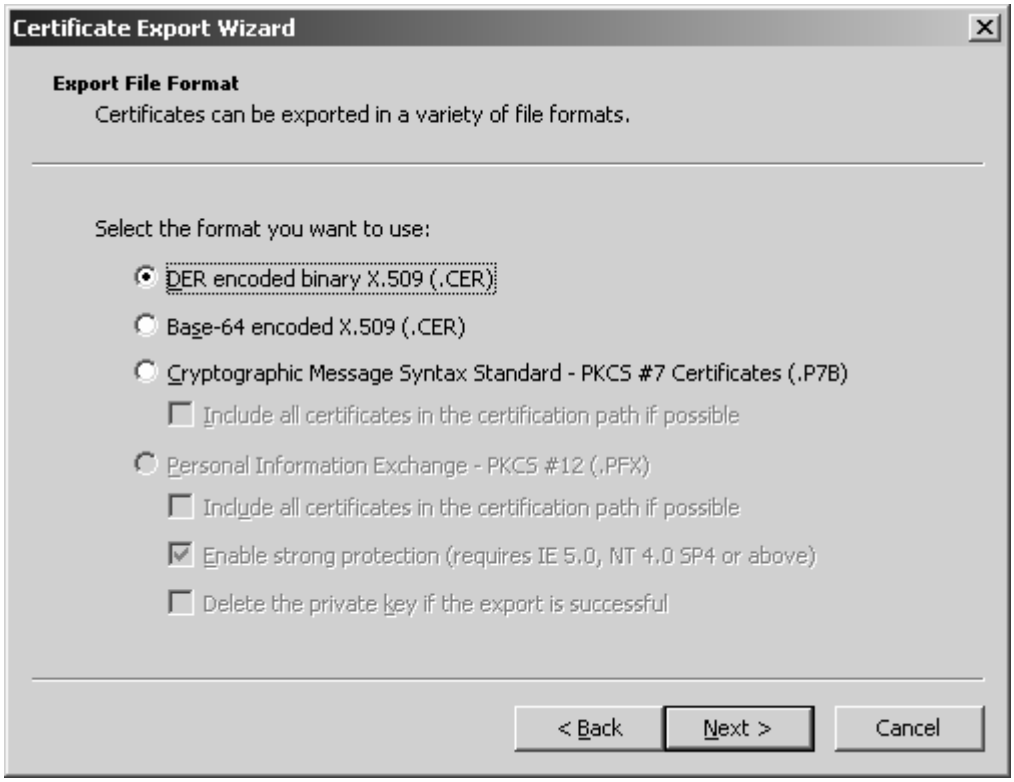
Kuva 19 Varmenteen luominen

Varmenne löytyi pienen etsimisen jälkeen varmenteiden hallinnasta. Sieltä se oli helppo ottaa talteen.



Kuva 20 Varmenteen talteenotto

Valitsimme varmenteen muodoksi DER X.509. Tätä muotoa käytetään useimpien varmenteiden luomiseen.

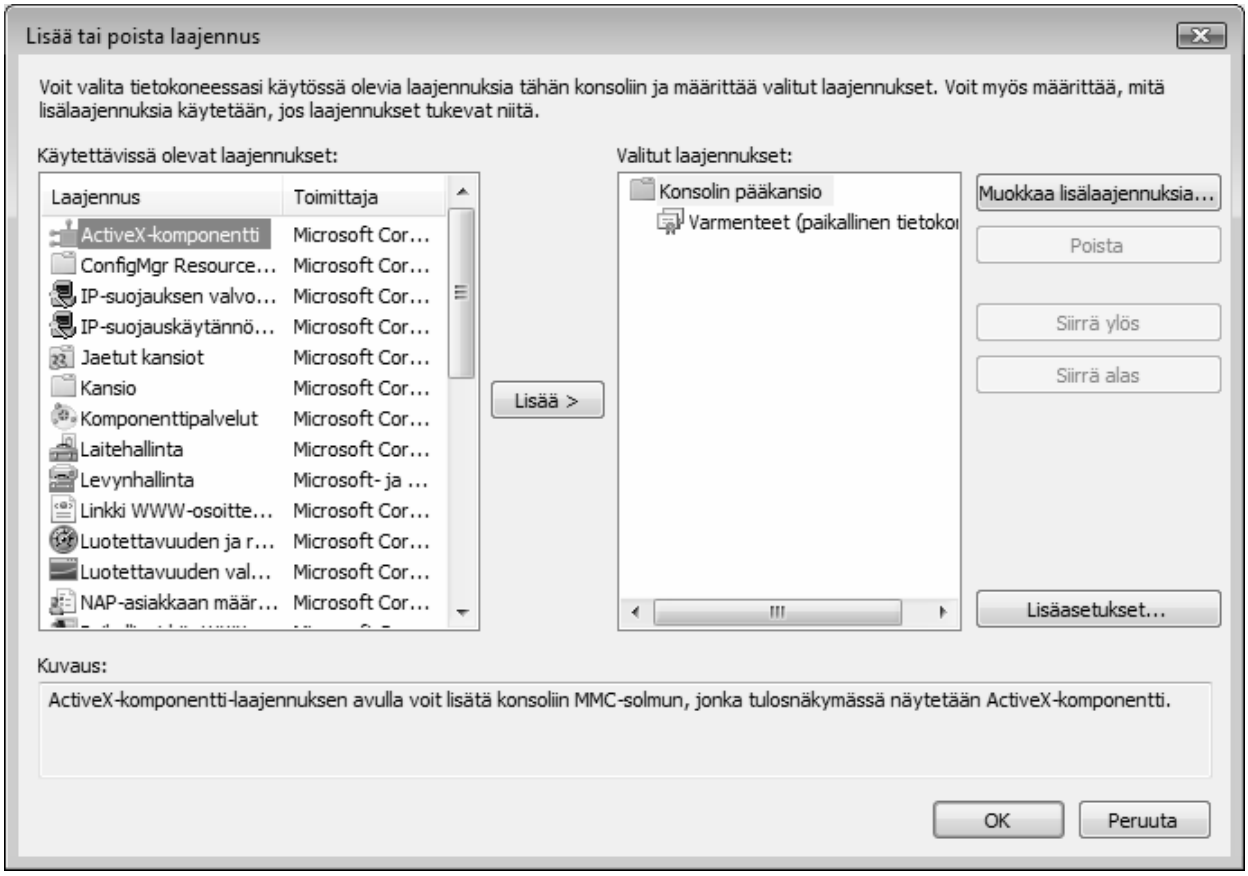


Kuva 21 Tallennettiin varmenne DER X.509 muotoon

8.5 Varmenteen tuominen työasemaan

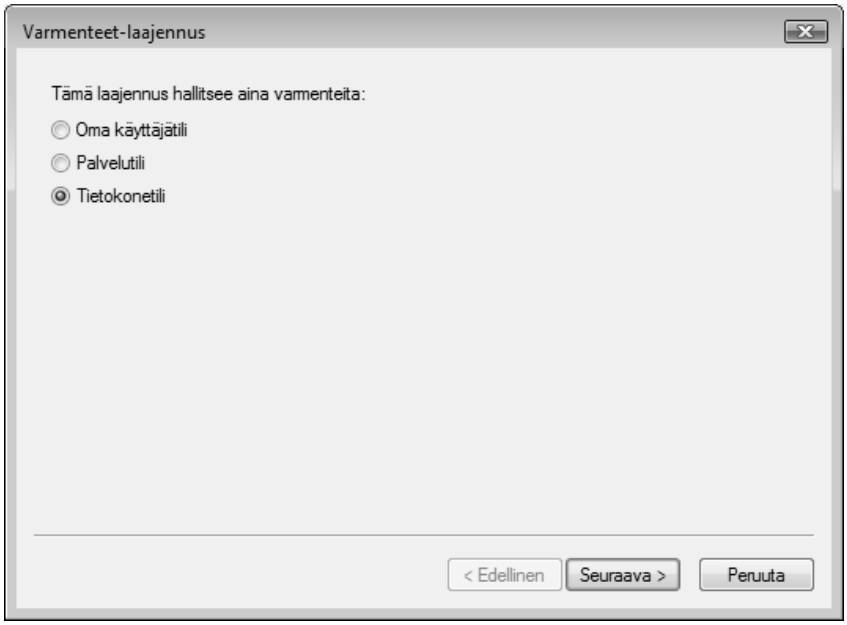
Vista-ympäristössä varmenteen tuominen oli pakollinen toimenpide PEAP-protokollan takia. Varmenteen tuominen osoittautui työssämme suunniteltua haastavammaksi. Varmenne saatiin kuitenkin lopulta tuotua tietokoneen konsolin kautta ja näkymään verkkosovittimen alla haluamalla tavalla.

Lisäsimme konsoliin laajennuksen, jotta saisimme varmenteen näkymään oikeassa paikassa.



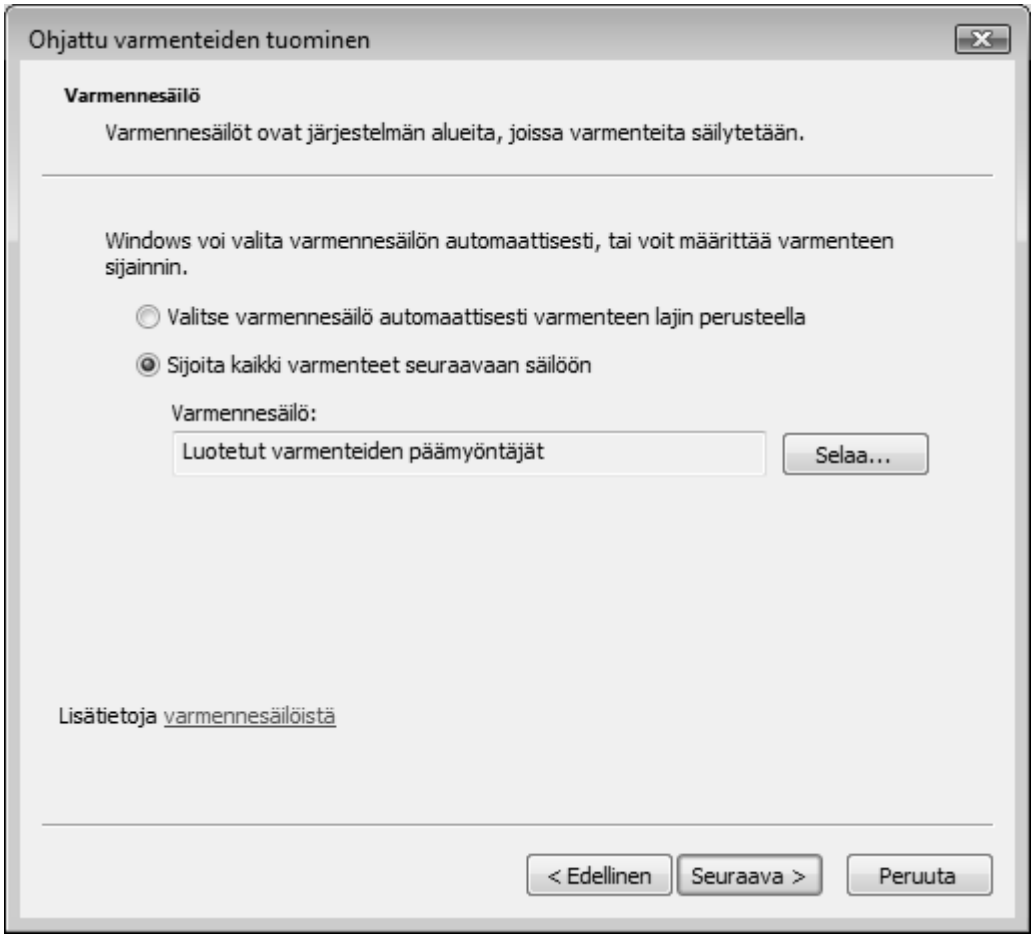
Kuva 22 Varmenteen tuominen työasemaan

Laajennuksen lisäämisessä on valittava Tietokonetili. Muuten muut käyttäjät eivät näe varmennetta, eivätkä pääse verkkoon, jos valitaan jokin toinen vaihtoehto.



Kuva 23 Tietokonetilin valinta

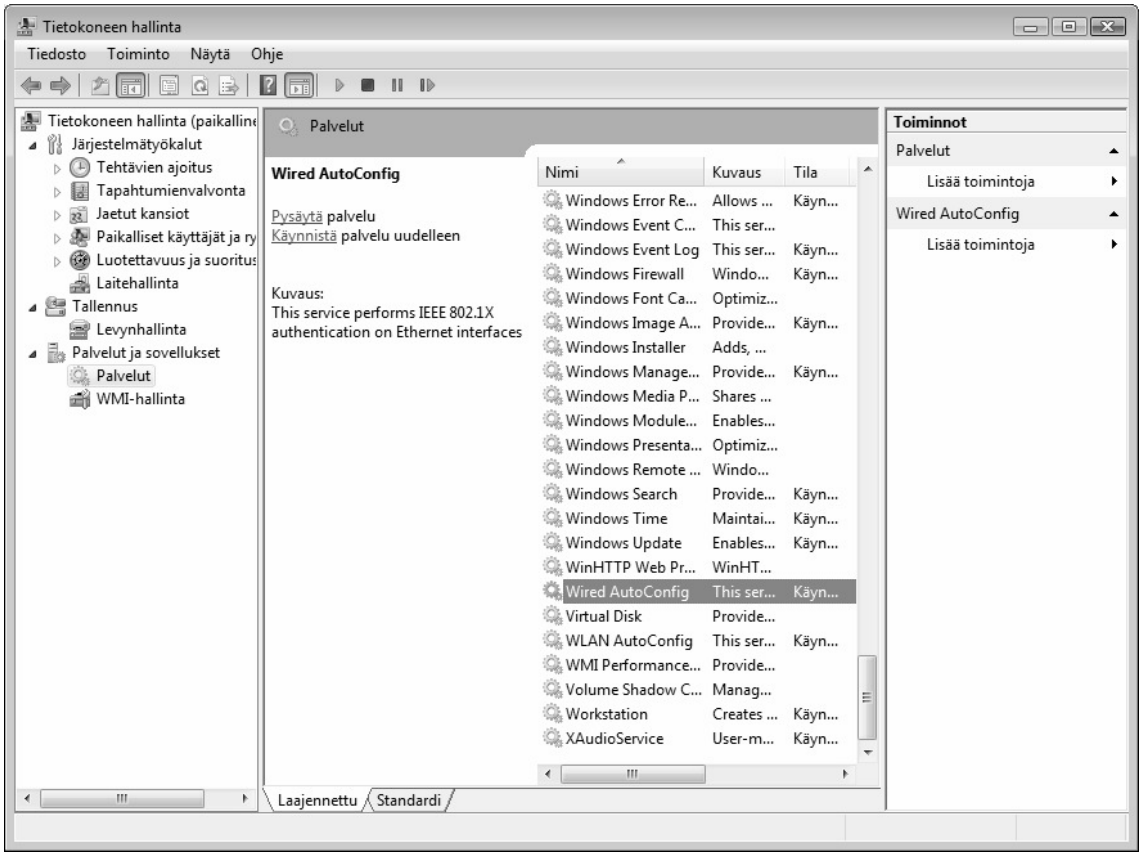
Varmenteen tuomisessa valitsimme luomamme varmenteen ja asensimme sen luotettujen varmenteiden päämyöntäjiin. Tällä tavoin saamme varmenteen näkymään verkkosovittimen todennus-välilehdellä.



Kuva 24 Varmenteen sijoittaminen

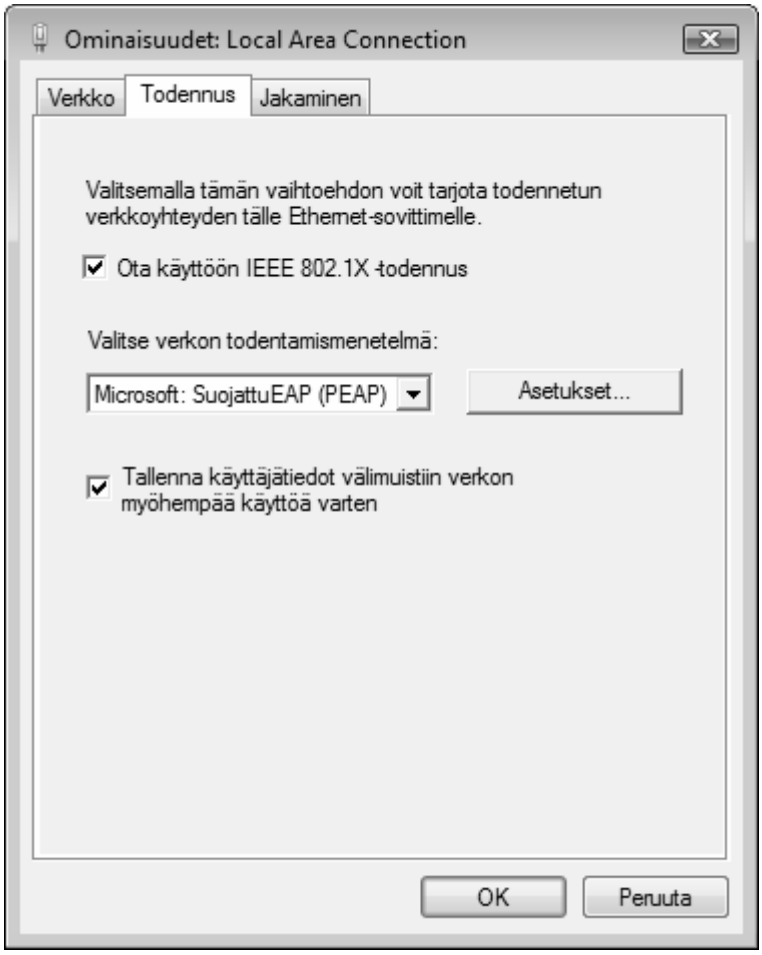
8.6 Työaseman asetukset

Vista ympäristössä 802.1X:n käyttöönotto vaatii tietokoneen hallinnasta Wired AutoConfig-palvelun käynnistämisen. Suomenkielisessä Vistassa palvelun nimenä käytetään automaattista lankaverkon määrittämistä, mikä aiheutti aluksi vaikeuksia. Palvelun käynnistäminen vaikuttaa verkkosovittimen asetuksiin ja tuo sinne todennus välilehden, josta palvelu kytketään päälle.



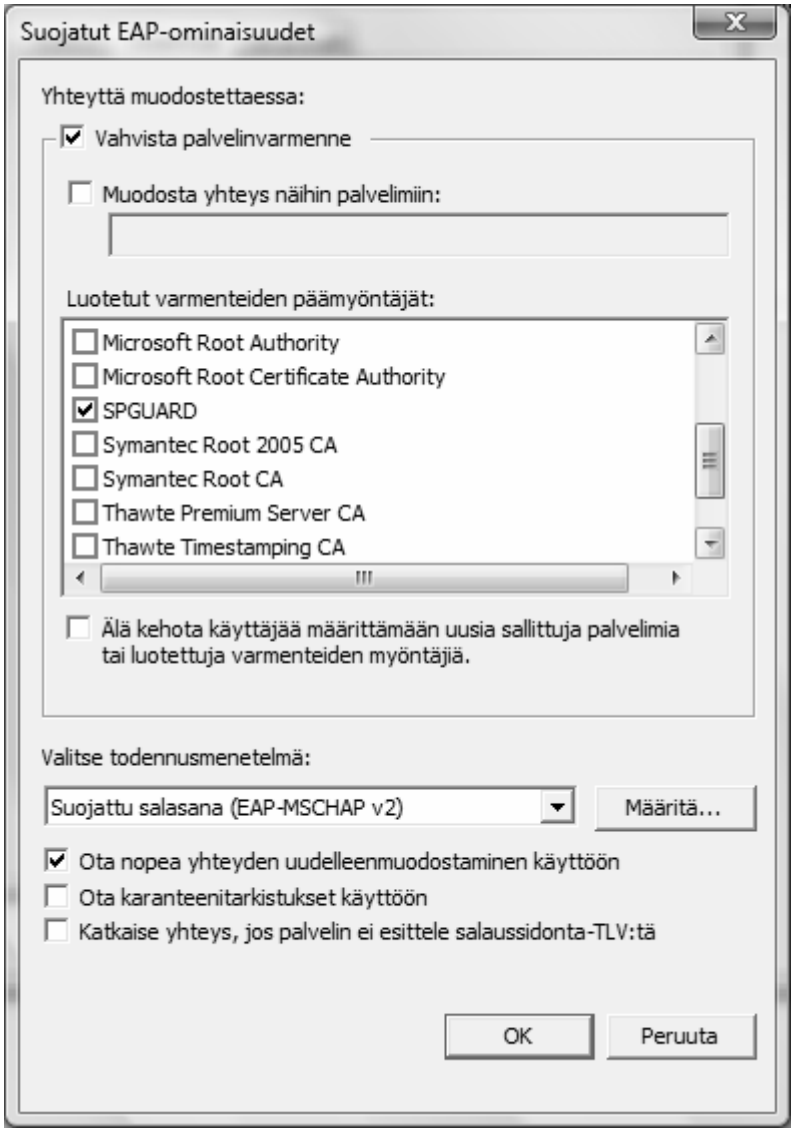
Kuva 25 Tietokoneen hallintasivulta Wired AutoConfig-palvelun käyttöönotto

Kun palvelu on käynnistetty, kytketään 802.1X:ää käyttävän tietokoneen verkkosovittimen asetuksista ominaisuus päälle. Vista ympäristössä valittavina on vain SuojattuEAP (PEAP), mikä on tietoturvallisuutta ajatellen oikea vaihtoehto Fennian käyttöön. PEAP-todenuksessa työasemaan vaaditaan myös oikeanlainen varmenne.



Kuva 26 Todennuksen käyttöönotto verkkoadapterista

Valitsimme protokollalle varmenteen, minkä se vaatii toimiakseen. Varmenteena käytimme aiemmin luotua varmennetta. Todennusmenetelmäksi valitsimme EAP-MS-CHAP v2 käyttäjän näkökulmaa ajatellen.



Kuva 27. Sertifikaatin valinta

9 Lopputulokset

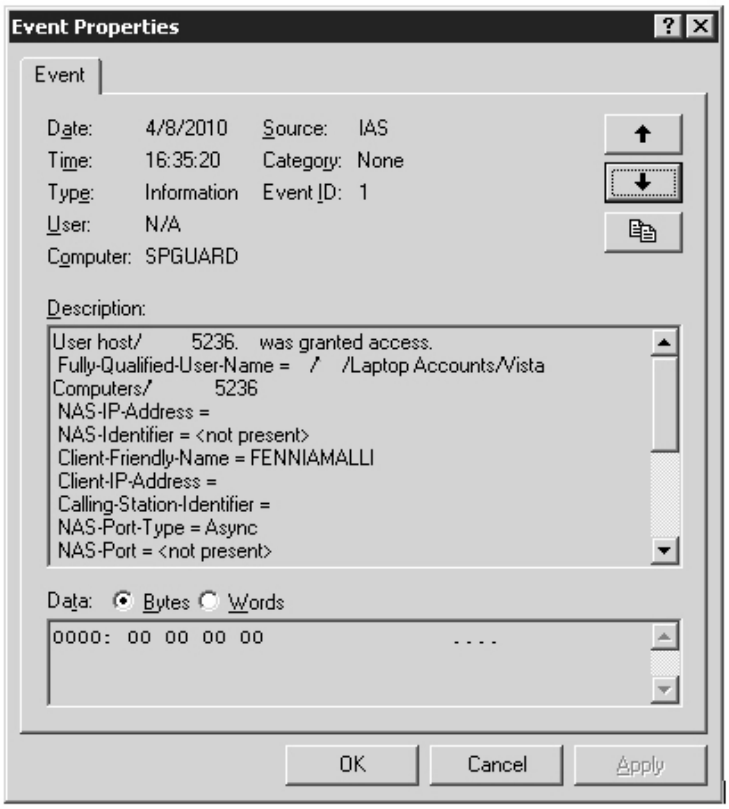
Suoritimme päättötyötä Pasilan pääkonttorin testauslaboratoriossa. Rakensimme laboratorion vastaamaan konttoriympäristöä. Halusimme testata mahdollisimman laajasti 802.1X:n toiminnan, joten otimme testaukseen kolme erilaista työasemaa. Yksi oli Fennian domainin alla oleva työasema, toinen oli messukone, jossa ei ole Fennian domainia ja kolmas kone oli kokonaan ulkopuolisen käyttäjän työasema. Pystyimme seuraamaan koneiden autentikointitapahtumia Radius-palvelimelta.

Ensin testauksen kanssa oli teknisiä ongelmia, koska emme saaneet asennettua sertifikaattia testauskoneille. Viime hetkinä löysimme ratkaisun, jolla saimme sertifikaatin tuotua testikoneille. Tämän jälkeen testaus onnistui ja saimme haluamamme lopputuloksen.

Lopputulos oli erittäin onnistunut. Autentikointi toimi määrittelemällämme tavalla ja pystyimme lokitiedostojen perusteella seuraamaan koneita, jotka ovat yrittäneet päästä yrityksen verkkoon sekä käyttäjiä, jotka pääsivät käyttämään yrityksen verkkoa. Lokitiedot tallentuivat Windowsin omaan lokiin sekä IAS-palvelimelle. Lokitiedoista otettiin myös joka yö varmuuskopiot, jonka johdosta tiedot olisi palautettavissa vaikka palvelin hajoaisi.

9.1 Työasema täyttää kaikki ehdot

Ensimmäisen testauksen suoritimme Fennian omalla työasemalla. Asensimme työasemaan luomamme varteen ja määrittelimme asetukset oikeiksi. Testaus onnistui heti ensimmäisellä kerralla ja saimme haluamamme tuloksen. Lokitapahtumasta voimme todeta, että koneelle xxxx5236.xx sallittiin pääsy ja palvelimme luotuun 802-FENNIA sääntöön. Autentikoinnissa on käytetty PEAP-protokollaan ja EAP-tyyppinä Secured password (EAP-MSCHAP v2).



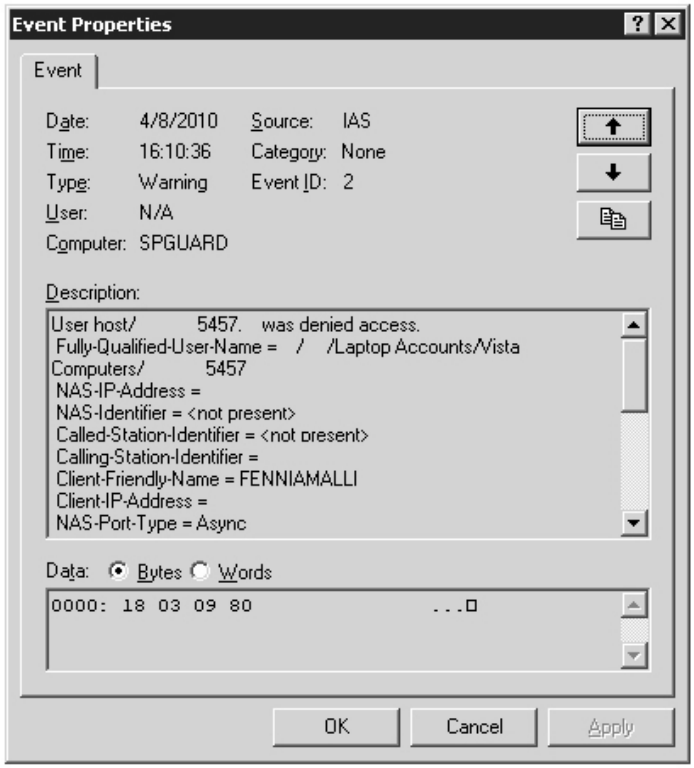
Kuva 28 Autentikoituminen onnistuu

Event Type: Information
Event Source: IAS
Event Category: None
Event ID: 1
Date: 4/8/2010
Time: 16:35:20
User: N/A
Computer: XXXXX
Description:
User host/xxxx5236.xx was granted access.
Fully-Qualified-User-Name = xx/XX/Laptop Accounts/Vista Computers/xxxx5236
NAS-IP-Address = X.X.X.X
NAS-Identifier = <not present>
Client-Friendly-Name = FENNIAMALLI
Client-IP-Address = X.X.X.X

Calling-Station-Identifier = XX-XX-XX-XX-XX-XX
NAS-Port-Type = Async
NAS-Port = <not present>
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = 802-FENNIA
Authentication-Type = PEAP
EAP-Type = Secured password (EAP-MSCHAP v2)

9.2 Työasemasta puuttuu sertifikaatti

Seuraava testaus suoritettiin työasemalla, jossa ei ollut varmennetta asennettuna. Autentikoinnin oli tarkoitus epäonnistua, koska emme halua päästää laitetta verkkoon, jos sillä ei ole varmennetta asennettuna. Saimme haluamamme tuloksen ja laitteen pääsy evättiin. Lokitapahtumasta näemme, että laitteelle xxxx5457.xx ei myönnetty pääsyä. Policy-Name kohdassa kone osuu sääntöön, mutta viimeisenä kerrotaan, että allekirjoitusta ei voitu varmistaa, mikä viittaa varmenteen puuttumisesta.

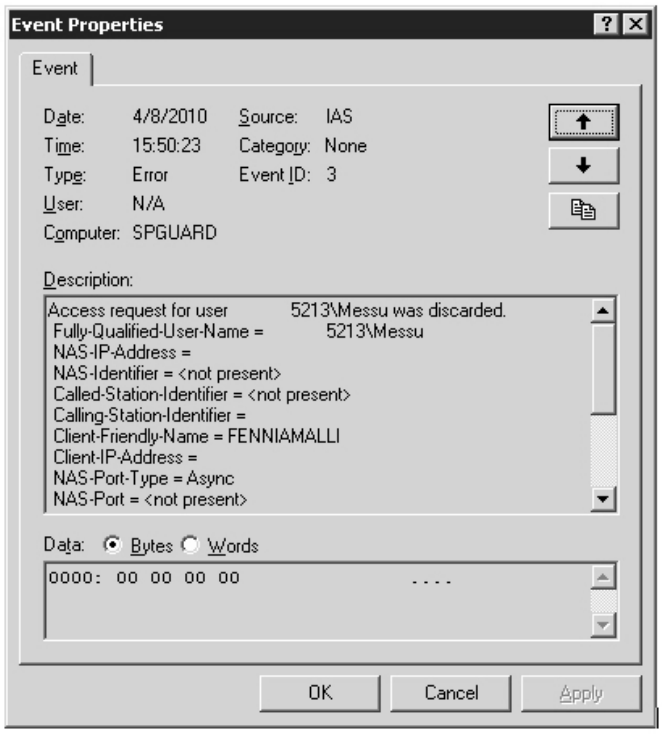


Kuva 29 Kirjautumisesta syntyvä virheilmoitus (sertifikaatti puuttuu)

Event Type: Warning
Event Source: IAS
Event Category: None
Event ID: 2
Date: 4/8/2010
Time: 16:10:36
User: N/A
Computer: XXXXX
Description:
User host/xxxx5457.xx was denied access.
Fully-Qualified-User-Name = xx/XX/Laptop Accounts/Vista Computers/xxxx5457
NAS-IP-Address = X.X.X.X
NAS-Identifier = <not present>
Called-Station-Identifier = <not present>
Calling-Station-Identifier = XX-XX-XX-XX-XX-XX
Client-Friendly-Name = FENNIAMALLI
Client-IP-Address = X.X.X.X
NAS-Port-Type = Async
NAS-Port = <not present>
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = 802-FENNIA
Authentication-Type = PEAP
EAP-Type = <undetermined>
Reason-Code = 262
Reason = The supplied message is incomplete. The signature was not verified.

9.3 Todennus epäonnistuu

Viimeinen testaus suoritettiin työasemalla, missä asetuksina oli määritelty koneen kuuluvan kokonaan eri työryhmään. Lokitapahtumasta nähdään, että kone pääse edes varmenteen tarkistamiseen asti, koska se ei osu palvelimelle luomaamme sääntöön. Lokista voimme tulkita vain, että kone xxxx5213\Messu ei päässyt liittymään verkkoon, koska työryhmää ei todennettu oikeaksi.



Kuva 30 Epäonnistunut todennus

Event Type: Error
Event Source: IAS
Event Category: None
Event ID: 3
Date: 4/8/2010
Time: 15:50:23
User: N/A
Computer: XXXXX
Description:

Access request for user xxxx5213\Messu was discarded.
Fully-Qualified-User-Name = xxxx5213\Messu
NAS-IP-Address = X.X.X.X
NAS-Identifier = <not present>
Called-Station-Identifier = <not present>
Calling-Station-Identifier = XX-XX-XX-XX-XX-XX
Client-Friendly-Name = FENNIAMALLI
Client-IP-Address = X.X.X.X
NAS-Port-Type = Async
NAS-Port = <not present>
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Reason-Code = 5
Reason = The user account domain cannot be accessed.

10 Työnantajan sanat tutkimuksesta

Saimme esimieheltämme lausunnon työstämme. Hän kommentoi työstämme seuraavaa:

Luin opinnäytetyön läpi ja se on erinomainen työ. Asia etenee selkeästi ja johdonmukaisesti ja lukija saa hyvän käsityksen siitä, mitä on tehty sekä mitkä on olleet työn tavoitteet ja miten ne on saavutettu. Myös kielellisesti työ on erittäin hyvätasoinen ja se on ymmärrettävä myös sellaiselle lukijalle, joka ei ole syvällinen IT-asiantuntija.

Työnantajan näkökulmasta aihevalinta oli hyödyllinen, koska Fenniassa on jo useita vuosia suunniteltu 802.1X:n käyttöönottoa, mutta eri syistä olemme aina aiemmin joutuneet luopumaan ratkaisusta. Tietoturvallisuus on kuitenkin vakuutusalalla erittäin korkealla prioriteetilla ja erityisesti pienten konttoreiden turvallisuuteen on haluttu löytää aiempaa tehokkaampia ratkaisuja. Tässä opinnäytetyössä suunniteltu ja toteutettu 802.1X-ratkaisu tuo erittäin hyvän lisän konttoreiden, ja koko Fennian, tietoliikenneturvallisuuteen ja siten osaltaan nostaa yrityksen tietoturvatasoa. Erityisen hyvää työssä oli myös se, että siinä löydettiin ratkaisu, joka ei vaatinut

investointeja tai muuten nostanut kustannuksia, vaan se pystyttiin toteuttamaan konfiguraatioita muuttamalla.

Tämä työ on Fennialla todelliseen tarpeeseen vastaava erittäin ja siten yhtiölle erittäin hyödyllinen.

11 Yhteenveto

Työssämme oli tarkoitus vastata kysymykseen, kuinka 802.1x-suojaus toteutetaan yrityksessä ja kannattaako Fennian ottaa kyseinen suojaus käyttöön. Työssä mietimme myös Fenniassa jo olemassa olevia laitteita ja pyrimme saamaan suojauksen niissä käyttöön, jotta yrityksen ei tarvitsisi ostaa uusia laitteita suojausta varten. Työn aikana mietimme myös, kuinka turvaamme järjestelmän jatkuvuuden. Tämä onnistuu palvelimen varmuuskopioinnin avulla ja kytkimen asetukset otetaan myös päivisin talteen ajastetulla varmuuskopioinnilla. Kaikki asetukset ovat vikatilanteen sattuessa helposti palautettavissa.

802.1X:n käyttöönotto on Fennialle erittäin tärkeää erityisesti niissä konttoreissa, joissa ei kovin helposti pääse seuraamaan verkon käyttöä. Tämän avulla yritys saa verkostaan pois ylimääräiset laitteet, joilla ei ole oikeutta käyttää suojattua verkkoa. Tämän johdosta Fennian kannattaa ottaa käyttöön 802.1X-salausmenetelmä. Suojaus on toteutettu ja testattu konttoriympäristöä ajatellen, ja se on helppo ottaa käyttöön missä tahansa Fennian konttorissa, jossa on oma konttoripalvelin.

Saavutimme kaikki työlle asetetut tavoitteet ja opimme todella paljon uusia asioita työtä tehdessämme. Kohtasimme erilaisia ongelmia ja jouduimme ratkomaan niitä, jotta saimme työmme valmiiksi. Haastavin vaihe työn tekemisessä oli sertifikaattien asentaminen yrityksen työasemille. Aluksi meillä oli ongelmia varmenteen tuomisessa Vista-ympäristössä pelkästään yhdelle työasemalle. Ongelma melkein esti onnistuneen testauksen suorituksen, koska ilman varmennetta koneet eivät mene määritelmämme mukaan verkkoon. Viime hetkellä ratkaisimme kuitenkin varmenneongelman ja saimme varmenteen tuotua yksittäisille työasemille testausta varten. Tämän jälkeen saimme myös tiedot onnistuneesta testauksesta, koska työasema meni verkkoon määritelmiemme mukaisesti. Järjestelmäämme jäi myös aina lokitiedot kirjautumisista. Epäonnistuneiden autentikointien lokitiedoista näimme, minkä niminen kone oli yrittänyt päästä verkkoomme ja selityksen, minkä

vuoksi kone ei päässyt käyttämään verkkoa. Onnistuneesta autentikoinnista tuli myös lokitieto, jossa ilmoitettiin käyttäjätunnus, jolla on oikeus käyttää verkkoa.

Lähteet

Kirjallisuus

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: WS Bookwell.

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

Järvinen, A. & Järvinen, P. 2004. Tutkimustyön metodeista. Tampere: Opinpajan kirja.

Kaj Granlund, 2003. Tietoliikenne. Jyväskylä: Docendo

Elektroniset lähteet

Case tutkimus. Viitattu 20.3.2010.
http://www.metodix.com/fi/sisallys/04_virtuaalikirjasto/dokumentit/aineistot/case tutkimus

Fennian arvot. Viitattu 1.2.2010.
http://www.fennia.fi/FenniaRyhma/FennianArvot.htm

Fennia-ryhmä. Viitattu 1.2.2010.
http://www.fennia.fi/FenniaRyhma/

IEEE 802 standards Viitattu 10.2.2010
http://standards.ieee.org/getieee802/

IPV6. Viitattu 10.1.2010.
http://ipv6.com/articles/wireless/8021x-Wireless.htm

Lauronen. Viitattu 13.2.2010.
http://www.tml.tkk.fi/Publications/Thesis/lauronen.pdf

Tag. Viitattu 10.1.2010.
http://www.tag.com/tech%20support/System%20Resources/Drivers%20&%20Utilities/Drivers/Current/7.2/MIL-BOOK%20201/WLAN/WLAN/Docs/FIN/security.htm#8021x

Tapaustutkimus. Viitattu 4.1.2010.
http://www.uta.fi/laitokset/sospol/sosnet/ammlis/tapaustut.htm

Tutkimus seminaari. Viitattu 28.12.2009.
http://www.tukkk.fi/tjt/TUTKIMUS/seminaari/abstr-konstr.html

802.1X protokolla. Viitatut 13.2.2010.
http://www.javvin.com/protocol8021X.html

Kuvalähteet

Eläke-Fennia hallintoelimet. Viitattu 1.2.2010.
http://www.elake-fennia.fi/widepage.aspx?SectionId=3076

Fennia ryhmän kaavakuva. Viitattu 1.2.2010.
http://www.fennia.fi/FenniaRyhma/

Fennia vahinkovakuutuksen organisaatiokaavio. Viitattu 1.2.2010.
http://lomakkeet.fennia.fi/lomakepalvelu/servlet/fi.efennia.lomakepalvelu.LomakeHandler?open=1046&contentType=application/pdf&url=906EC981090DF4D49A2D0B1633A33F16&name=Fennian%20organisaatio

Henki- Fennian organisaatiokaavio. Viitattu 1.2.2010.
http://lomakkeet.fennia.fi/lomakepalvelu/servlet/fi.efennia.lomakepalvelu.LomakeHandler?open=358&contentType=application/pdf&url=78952E7F7457C478F1A602E10C9CB45E&sessTransfer=uagwi5eq5nlbei2xcpk34fea

Kuvat ja kuviot

Liitteet

Liite 1 kytkimen koko konfigurointi

User Access Verification

Username:
Username: xxxxx
Password:

FENNIAMALLI >ena
Password:
FENNIAMALLI #sh run
Building configuration...

Current configuration : 7706 bytes
!
! Last configuration change at 13:30:48 EET Wed Feb 10 2010 by XX
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service pt-vty-logging
!
hostname XXXX
!
aaa new-model
aaa authentication login default group radius enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
enable secret 5 XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
!

```
clock timezone EET 2
clock summer-time EET recurring last Sun Mar 3:00 last Sun Oct 4:00
no errdisable detect cause pagp-flap
no errdisable detect cause dtp-flap
no errdisable detect cause link-flap
no errdisable detect cause gbic-invalid
no errdisable detect cause loopback
ip subnet-zero
!
no ip domain-lookup
ip domain-name XXXXXXXX
vtp domain xxxxxx
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
dot1x system-auth-control
!
mac access-list extended testi
!
!
vlan 89
 name guest
!
vlan 100
 name guarantine
!
interface FastEthernet0/1
 switchport trunk allowed vlan XX
 switchport mode trunk
 no ip address
 duplex full
 speed 100
 no snmp trap link-status
 spanning-tree portfast
```

```
!
interface FastEthernet0/2
 switchport access vlan 100
 switchport mode access
 no ip address
 speed 100
 no snmp trap link-status
 dot1x port-control auto
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/3
 description Tyoaseman Malli
 switchport access vlan 100
 switchport mode access
 no ip address
 speed 100
 no snmp trap link-status
 dot1x port-control auto
 dot1x timeout quiet-period 30
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/4
 description Kirjoittimen Malli
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security mac-address XXXX.XXX.XXX.XXX
 no ip address
 speed 100
 no snmp trap link-status
 dot1x guest-vlan 89
 spanning-tree portfast
```

```
!
interface FastEthernet0/5
 switchport access vlan 100
 switchport mode access
 no ip address
 speed 100
 no snmp trap link-status
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/8
 switchport access vlan 100
 switchport mode access
```

```
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/10
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
```

```
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/12
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/13
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
```

```
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/17
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/18
```

```
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/19
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/20
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/21
 switchport access vlan 100
 switchport mode access
 no ip address
```

```
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/22
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/23
 switchport access vlan 100
 switchport mode access
 no ip address
 no snmp trap link-status
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/24
 switchport access vlan 100
 switchport mode access
 no ip address
 speed 100
 no snmp trap link-status
 dot1x port-control auto
```

```
 dot1x host-mode multi-host
 dot1x guest-vlan 89
 dot1x reauthentication
!
interface GigabitEthernet0/1
 no ip address
!
interface GigabitEthernet0/2
 no ip address
!
interface Vlan1
 ip address X.X.X.X 255.255.255.0
 no ip route-cache
!
ip default-gateway X.X.X.X
no ip http server
!
access-list XX permit X.X.X.X.X.X.X.X
access-list XX permit X.X.X.X.X.X.X.X
snmp-server group XXXXX v3 auth read  notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF
snmp-server community XXXXX XX 99
snmp-server host X.X.X.X version 3 auth XXXXXX
radius-server host X.X.X.X auth-port 1812 acct-port 1813 key XXXXXXXXXXXXXX

radius-server retransmit 3
!
line con 0
 password 7 XXXXXXXXXXXXXXXX
 stopbits 1
line vty 0 4
 access-class 10 in
 password 7 XXXXXXXXXXXXXXXX
 transport input telnet
 transport output telnet
line vty 5 15
!
```

```
ntp clock-period 17179896
ntp server X.X.X.X
end
```