TURVALLINEN AUTENTIKOINTI LANGATTOMISSA LÄHIVERKOISSA

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2008
Ismo Turve

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

TURVE ISMO: TURVALLINEN AUTENTIKOINTI
LANGATTOMISSA LÄHIVERKOISSA

Tietoliikennetekniikan opinnäytetyö, 94 sivua

Kevät 2008

TIIVISTELMÄ

Langattomat lähiverkot (Wireless Local Area Networks, WLAN) ovat tänä päivänä yhä useammin yritysten varteenotettavien verkkoratkaisujen joukossa. Langattomien laitteiden tiedonsiirtonopeus on kasvanut viime vuosien aikana nopeasti samalla kun laitteiden hinta on laskenut. Lisäksi langaton verkko on helppo pystyttää ilman hankalia kaapelointeja ja mahdollistaa työasemien liikkuvuus säilyttäen lähiverkkoyhteydet. Langattomien verkkojen pahimpana uhkana nähdään kuitenkin niiden puutteellinen tietoturva.

IEEE 802.11 -standardin mukaisen langattoman lähiverkon rakenteen ja toiminnan perusperiaatteiden tuntemus kuuluu tänä päivänä jokaisen yrityksen lähiverkkojen hallinnasta vastaavalle henkilölle. Langattomien verkkojen tietoturvaa lisäävien suojaus- ja salausmenetelmien sekä käyttäjien luotettavan autentikoinnin mahdollistavien menetelmien hallitseminen on niin ikään tärkeää verkon turvallisuuden varmistamiseksi.

Turvallisuusratkaisuiden ohessa on tärkeää tutustua myös langattomia verkkoja vastaan kohdistuviin mahdollisiin hyökkäyksiin. Tietoisuus mahdollisista hyökkäystavoista mahdollistaa langattomiin verkkoihin kohdistuvien riskien arvioinnin, riskeihin varautumisen ja sitä kautta tietoturvallisen toiminnan.

Työssä tutustutaan langattomien lähiverkkojen tietoturvaan ja Microsoft Windows Server 2008 -palvelinkäyttöjärjestelmän tietoturvaominaisuuksiin WLAN-verkkojen kannalta ja toteutetaan Windows Server 2008 -palvelimen avulla testiverkko, jossa käytetään WEP- ja 802.1X-pohjaista todentamismenetelmää käyttäjien tunnistamiseen. Tässä opinnäytetyössä keskitytään Windows Server 2008 -palvelimen NPS (Network Policy Server) -rooliin ja NAP (Network Access Protection) toimintoon langattomien lähiverkkojen suojausmenetelminä.

Työssä onnistuttiin hyvin. Testausympäristö saatiin rakennettua suhteellisen helposti, vaikka valmistajan sivuilta ei vielä löytynyt dokumentaatiota 802.1X-tunnistusta käyttävälle langattomalle verkolle. Järjestelmän testaamisessa puolestaan keskityttiin järjestelmän toimintaan yleisesti eli järjestelmän ilmoitukseen rajoitetusta verkon käytöstä. Työn tuloksena on toimiva koulutus- ja testausalusta, jonka avulla voi tutustua eri salaustekniikoiden ja autentikointimenetelmien käyttöön sekä Windows Server 2008 -palvelinkäyttöjärjestelmän tietoturvaa lisääviin elementteihin.

Avainsanat: 802.1X, RADIUS, EAP, PEAP, MS-CHAPv2, Microsoft Windows Server 2008

LAHTI UNIVERSITY OF APPLIED SCIENCES

Faculty of Technology

TURVE ISMO: SECURITY IN WIRELESS AREA NETWORKS USING AUTHENTICATION

Bachelor´s Thesis in Telecommunications Technology, 94 pages

Spring 2008

ABSTRACT

Wireless Local Area Networks, WLANs, are used more often as the network solutions of enterprises. The speed of wireless data transmission has increased while the prices of wireless equipment are decreasing. In addition, building wireless networks is easy without complicated cables. Using wireless networks enables mobility while the workstations are connected to the network. The biggest thread against wireless networks is their lacking security.

Knowing the basis of IEEE 802.11 standard wireless local area networks is the duty of every PC advisor who takes care the netoworks of enterprises. Knowledge about security increasing encryption and protection methods combined to reliable user authentication is also very important for securing the wireless networks.

In addition to the iportance of knowing the security solutions, it is also important to acquaint oneself with the possible security attacks against wireless networks. Knowledge about the ways of attacking against wireless networks makes the evaluation of risks, preparing for risks and the security possible.

The aim of this thesis was to study the security of wireless local area networks and the Microsoft Windows Server 2008 server operating system security with wireless networks and to configure secure wireless access using WEP and 802.1X -based authentication. This thesis focused on the NPS role (Network Policy Server) and NAP (Network Access Protection) as methods ofsecuring wireless access.

Configuring the test network succeeded well, although there was no documentation about setting up wireless access using 802.1X authentication at the producer's website. Testing the configured system focused on how the configured system worked generally. The result of this thesis is a working training and test environment which helps in becoming acquainted with securing techniques, authentication and Microsoft Windows Server 2008 security components.

Key words: 802.1X, RADIUS, EAP, PEAP, MS-CHAPv2, Microsoft Windows Server 2008

Alkusanat

Haluan kiittää työn valvojaa, lehtori Jari Utriaista, rakentavasta ja nopeasta palautteesta työn aikana.

Lopuksi haluan vielä kiittää perhettäni ja ystäviäni henkisestä tuesta koko opintotaipaleeni aikana sekä erityisesti Heliä hänen antamastaan loputtomasta kannustuksesta ja jaksamisesta odotellessa työn valmistumista.

Heinolassa 30.5.2008

Ismo Turve

SISÄLLYS

SANASTO

AAA	Authentication, Authorization. Accounting. AAA-palvelut, jotka käsittävät kaikki ne menetelmät ja tiedot, joita tarvitaan yksittäisen asiakkaan tunnistamiseen, valtuuttamiseen ja laskuttamiseen.
AES	Advanced Encryption Standard. Toistaiseksi murtamaton 128-256 -bittinen salausalgoritmi.
BSS	Basic Service Set, peruspalveluryhmä. Yhden WLAN (Wireless Local Ara Network) -tukiaseman kattama alue.
CA	Certification Authority. Sertifikaatteja myöntävä palvelu, joka allekirjoittaa sertifikaatit yksityisellä avaimellaan.
CHAP	Challenge-Handshake Authentication Protocol. Haaste-vastaus autentikaatioprotokolla.
DHCP	Dynamic Host Configuration Protocol. Protokolla, joka jakaa IP (Internet Protocol)- osoitteita lähiverkkoon kytkeytyville laitteille.
EAP	Extensible Authentication Protocol. Todennusprotokollan runko, jolla neuvotellaan käytettävä todennusmekanismi.
ESS	Extended Service Set. Laajennettu palveluryhmä. ESS sisältää useamman WLAN-tukiaseman eli peruspalveluryhmän (Kts. BSS).
HTTP	Hypertext Transfer Protocol. Selainten ja WWW-palvelimien käyttämä tiedonsiirtoprotokolla.
IAS	Internet Authentication Service. Microsoftin kehittämä ohjelma, joka takaa käyttäjälle keskitetysti AAA-palvelut.
IEEE	Institute of Electrical and Electronics Engineers. Järjestö, jonka työryhmät kehittävät ja julkaisevat tietoliikenneverkkoihin liittyviä standardeja.
IETF	Internet Engineering Task Force. Internet-protokollien standardoinnista vastaava järjestö.

LAN	Local Area Network. Pienen alueen, kuten yrityksen toimipisteen, tietoverkko.
MAC	Media Access Control. Verkkokortin fyysinen osoite, joka koostuu verkon valmistajan omasta osoitteesta sekä juoksevasta sarjanumerosta.
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol. Microsoftin versio haaste-vastaus autentikaatioprotokollasta.
OFDM	Orthogonal Frequency-Division Multiplexing. Monikantoaaltomodulaatio, tiedon siirtoa lukuisilla toisiaan häiritsemättömillä taajuuskanavilla yhtä aikaa.
RADIUS	Remote Authentication Dial In User Service. RADIUS-protokolla on RADIUS-autentikointipalvelimissa käytettävä etäautentikointimenetelmä, joka on alun perin suunniteltu sisäänsoittopalveluissa tapahtuvaan tunnistukseen.
RSN	Robust Security Network. IEEE 802.11i -standardin mukainen WLAN
SSID	Service Set Identifier. Langattoman lähiverkon nimi.
TLS	Transport Level Security. Salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.
VLAN	Virtual Local Area Network. Ttekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin verkkoihin. Koneet voidaan jakaa omiin loogisiin verkkoihinsa riippumatta fyysisestä kaapeloinnista.
VPN	Virtual Private Network. Etätyöskentelyssä käytettävä yhteys, jolla saadaan aikaan suojattu yhteys verkon yli tietokoneiden välille.
WEP	Wired Equivalent Privacy. IEEE 802.11 suosituksen ensimmäinen työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä.
WLAN	Wireless Local Area Network. Langaton lähiverkko, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita

1 JOHDANTO

1.1 Opinnäytetyön tausta

Langaton lähiverkko eli WLAN (Wireless Local Area Network) on tietoliikenneratkaisu, jossa tietokoneet kommunikoivat toistensa kanssa radioaaltoja hyväksikäyttäen, joko itsenäisesti ad-hoc verkossa (IBSS, Independent Basic Service Set) tai tukiasemien (Access point) kautta ns. infrastruktuuriverkossa (BSS, Basic Service Set). Infrastruktuuriverkossa tukiasemat ovat kytkettyinä osaksi kiinteää lähiverkkoa. Tärkein langattoman tietoliikenteen etu verrattuna kaapeloinnilla toteutettuun tietoliikenteeseen on mahdollisuus työasemien liikuteltavuuteen lähiverkon alueella. Langaton tekniikka säästää myös kustannuksia kun kaapeloinnista voidaan ainakin osittain luopua. Langattomat verkot mahdollistavat myös tietoliikenneyhteyden sellaisiin paikkoihin, joihin yhteys muuten on mahdotonta toteuttaa maantieteellisten tai esteettisten syiden takia. (Ruotsalainen 2007, 9.)

Vuosituhannen vaihteessa suurimmat ongelmat langattomien verkkojen yleistymisessä olivat tiedonsiirtokapasiteetin rajallisuus sekä langattomien komponenttien saatavuusongelmat ja korkea hinta verrattuna langallisiin verkkotuotteisiin. Langattoman verkkotekniikan nopean kehityksen myötä vielä 2000-luvun alussa ollut tiedonsiirtokapasiteetin rajallisuusongelma on ratkennut nopeampien standardien kehityksen myötä. Myös langattomien verkkojen komponenttien hinta on viime vuosina laskenut nopeasti. Tällä hetkellä nopeita langattomia standardeja tukevat langattomat verkkosovittimet kuuluvat kannettavien tietokoneiden vakiokokoonpanoon. Myös langattomien tukiasemien hinta on laskenut selvästi vuosituhannen vaihteen jälkeen. Varsinkin PK-yrityksiin ja kotikäyttöön on saatavilla suhteellisen edullisia, monipuolisia, tietoturvallisia ja toimivia laitteita langattoman verkon toteuttamiseen. Tällä hetkellä langattomien verkkojen suurimmat ongelmat ja uhat liittyvät tietoturvallisuuteen sekä langattomien verkkokorttien aiheuttamaan tehonkulutukseen päätelaitteissa. (Helin, Karttunen & Pitkänen, 2002, 5-7; Puska 2005, 18-23.)

Maaliskuussa 2008 julkaistu Microsoft Windows Server 2008 sisältää monia tietoturvaan liittyviä uudistuksia verrattuna Windows Server 2003 -palvelinkäyttöjärjestelmään. Microsoft Windows Server 2008 802.1X NAP-järjestelmässä NPS-palvelu (Network Protection Server) kommunikoi 802.1X-yhteensopivan langat-

toman tukiaseman kanssa käyttäen RADIUS-protokollaa. Näillä palveluilla NPS-teknologia korvaa Windows Server 2003 -järjestelmässä toimivan Internet Authentication Service -palvelun (IAS).

1.2 Opinnäytetyön tavoitteet

Työn tavoitteena on selvittää Microsoft Windows Server 2008 Network Protection Server -roolin konfigurointia 802.1X-käyttäjätunnistuksen toteuttamiseksi sekä edistää tämän opinnäytetyön lukijan ymmärrystä IEEE 802.11-standardin lähiverkkojen tietoturvaa koskeviin asioihin. Kyseisen palvelinkäyttöjärjestelmän dokumentaatio turvallisen langattoman verkon asentamiseksi on vielä puutteellista, koska käyttöjärjestelmä on vasta julkaistu.

Opinnäytetyön lopputuloksena on toimiva ohjeistus IEEE 802.1X autentikointia käyttävän langattoman verkon asentamisesta käyttäen Microsoft Windows Server 2008 -palvelinkäyttöjärjestelmää.

2 LANGATON LÄHIVERKKO (WLAN)

2.1 WLAN-standardit

Langattoman lähiverkon ensimmäinen standardi, IEEE 802.11, julkaistiin vuonna 1997. IEEE 802.11 käyttää taajuusalueena 2,4 GHz taajuutta ja sillä päästään 1-2 Mb/s siirtonopeuksiin. 802.11-standardin tarkoituksena oli yhtenäistää langattomien lähiverkkojen toteutustapa. IEEE 802.11 määrittelee kolme fyysistä siirtotapaa, jotka ovat suorasekvenssihajaspektri (Direct Sequence Spread Spectrum, DSSS), taajuushyppely (Frequency Hopping Spread Spectrum, FHSS) ja infrapuna. Verkkotopologia voi olla ad hoc (tilapäisverkko) tai infrastruktuuriverkko. (Vesanen 2003.)

Jatkuvasti kehittyvien verkkosovellusten ja langattomien verkkojen laajentuneen käytön takia 802.11-standardin määrittämät nopeudet kävivät liian hitaiksi ja tarvittiin uusi standardi, joka vastaisi paremmin käyttäjien ja sovellusten vaatimuksia. IEEE julkaisi uuden 802.11b-standardin vuonna 1999. Standardi, joka käyttää myös nimeä 802.11hr (high rate), määrittelee verkkoyhteyden nopeudeksi 5,5 Mbps ja 11 Mbps, mikä tekee 802.11b:stä huomattavasti edeltäjäänsä nopeamman. Yhteys toimii edelleen samalla 2,4 GHz:n taajuudella. IEEE802.11b-laitteet ovat myös yhteensopivia uudempien IEEE802.11g-laitteiden kanssa, mutta silloinkin ne toimivat vain 11 Mbps nopeudella. (Hjelm 2005, 16-17.)

Samana vuonna 802.11b-standardin valmistumisen kanssa julkaistiin 802.11a-standardi 5 GHz taajuusalueella toimiville WLAN-laitteille. Taajuuden nostolla saatiin lisää kaistaa verkkoyhteyksien nopeuksien kasvattamiseksi. Myös siirtotekniikka koki muutoksen, sillä uusi standardi määritteli tiedonsiirtoa varten OFDM-tekniikan (orthogonal frequency division multiplexing), joka perustuu signaalin jakamiseen pienempiin alasignaaleihin. Muutoksien myötä saatiin verkkoyhteyksien nopeus kasvatettua 54 Mbit/s. (Hjelm 2005, 17.)

Vuonna 2003 IEEE ratifioi tutkimustyön tuloksena 802.11g-standardin, joka on risteytys 802.11a- ja 802.11b-standardeista. 802.11g käyttää tiedonsiirtoon CCK-OFDM-tekniikkaa ja tarjoaa vaihtoehtoiseksi siirtotavaksi PBCC-tekniikan. Standardi määrittää radiotaajuustekniikoista DSSS, HR-DSSS ja OFDM-tekniikat. 802.11g kykenee liikennöimään maksimissaan 54 Mbit/s nopeudella käyttäen 2,4 GHz:n taajuutta. 802.11g on täysin yhteensopiva vanhemman 802.11b-standardin

kanssa, jolloin liikennöintinopeus on maksimissaan 11 Mbit/s johtuen 802.11b modulaatiosta. (Laakso 2005, 22.)

OFDM-tekniikassa käytetään monia eri signaaleja, joilla digitaalinen data jaetaan koko käytössä olevalle spektrin alueelle. Signaalit lähetetään samaan aikaan rinnakkain eri kantoaalloilla. Jokaisella kantoaallolla lähetettävä bitti on taajuudeltaan kapea, mikä tarkoittaa sitä että se on ajallisesti pidempi. OFDM mahdollistaa suuret nopeudet, joita käytetään mm. 802.11a- ja 802.11g-standardeissa, hyödyntämällä koko taajuuskaistan spektrin tehokkaasti. OFDM sietää hyvin impulssimuotoisia häiriötekijöitä, sekä monitie-etenemisestä aiheutuvia häiriöitä. OFDM on kuitenkin herkkä taajuusvaihtelulle ja vaatii tarkan synkronoinnin. Yleisimpiä 802.11-standardeja vertaillaan taulukossa 1. (Puska 2005, 40.)

TAULUKKO 1. Yleisimpien käytössä olevien 802.11-standardien vertailua

STANDARDIEN VERTAILUA				
Standardi	Max. nopeus	Tod. nopeus	Taajuus	Liityntä
IEEE 802.11	2 Mbps	2 Mbps	2,4 GHz	FHSS
IEEE 802.11a	54 Mbps	31 Mbps	5 GHz	OFDM
IEEE 802.11b	11 Mbps	6 Mbps	2,4 GHz	DSSS
IEEE 802.11g	54 Mbps	20 Mbps	2,4 GHz	OFDM/DSSS
FHSS = Frequency Hopping Spread Spectrum				
DSSS = Direct Sequency Spread Spectrum				
OFDM = Orthogonal Frequency Division Multiplexing				

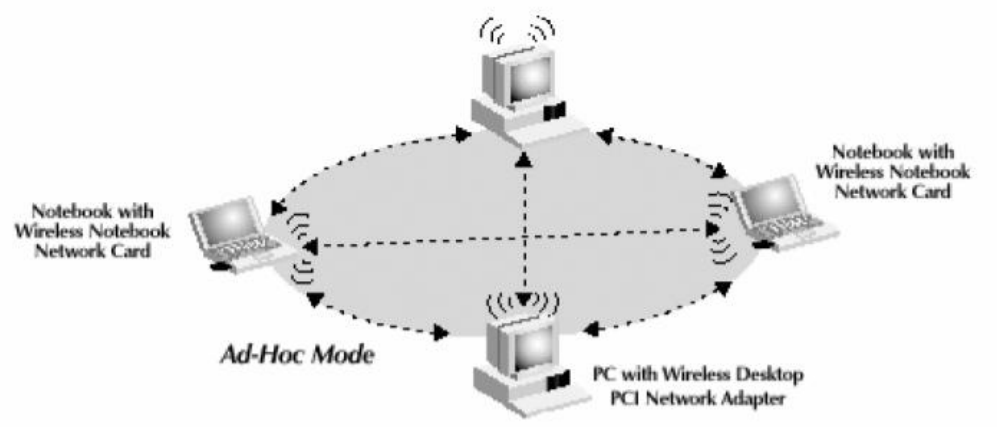
Muita 802.11-standardeja ovat 802.11e, -f, -h, -j, –i ja -n. 802.11i sisältää tietoturvaan liittyviä parannuksia. Se julkaistiin vuonna 2004 ja se sisältää 802.1X/EAP-ratkaisujen lisäksi myös AES salauksen. AES käyttää RC4:ää vahvempaa Rijndael-algoritmia ja 128-, 196- sekä 256-bitin salausavaimia. AES vaatii laitteisiin erillisen salauspiirin tai laitteiden suorituskyky putoaa huomattavasti. 802.11i soveltuu sekä staattisille, että dynaamisille salausavaimille ja yleensä sitä käytetään 802.1X-järjestelmässä. (Laakso 2005, 23.)

Parannellun 802.11n-standardin tiedonsiirrolle määrittämä nopeus on teoriassa 600 Mbit/s, mutta todellisuudessa sille luvataan noin 100-200 Mbit/s:n nopeus, joka on samaa luokkaa kuin perinteisellä 100 Mbit/s ethernet-kaapelilla. Samalla standardi tukee MIMO-tekniikkaa, jossa käytetään useampaa antennia ja useampaa kanavaa yhtä aikaa. Tätä tekniikkaa on jo käytetty 802.11g-standardissa epävirallisesti. Uusi MIMO-tekniikka mahdollistaa huomattavasti pidemmän kanta-

man kuin perinteinen yhden kanavan varassa toimiva tekniikka (kuten esim. 802.11b tai 802.11g). Virallisen IEEE 802.11-työryhmän projektiaikataulun mukaan IEEE arvioi hyväksyvänsä standardin joulukuussa 2009. (IEEE 802.11TM - The Working Group for WLAN Standards, 2008.)

2.2 WLAN-arkkitehtuuri

WLAN-ympäristössä tietokoneet voivat toimia joko itsenäisesti toistensa kanssa tai osana laajempaa verkkoa. Langattomille lähiverkoille on olemassa kaksi erilaista topologiaa eli verkkoarkkitehtuuria; ad-hoc ja infrastruktuuriverkko. Ad-hoc-verkon (KUVIO 1) yksinkertaisimmassa muodossa langattomat tietokoneet kommunikoivat suoraan toistensa kanssa tarvitsematta yhteyden muodostavaa tukiasemaa. Jos koneiden välinen etäisyys kasvaa liian suureksi, yhteys katkeaa. Kun ne taas palaavat tarpeeksi lähelle toisiaan, yhteys muodostuu automaattisesti uudestaan. Liikenne on rajoitettu vain verkkoon liittyneiden laitteiden välille eikä yhteyttä ulkopuolisiin verkkoihin ja niiden palveluihin ole. Ad-hoc verkko on helppo, nopea ja vaivaton toteuttaa mutta sen käyttö on rajoittunutta. Ad-hoc verkkoja käytetään usein tilapäisesti, esim. kokouksen ajan, jolloin kaikilla kokoukseen osallistujilla on käytössä samat materiaalit. (Ruotsalainen 2007, 10.)

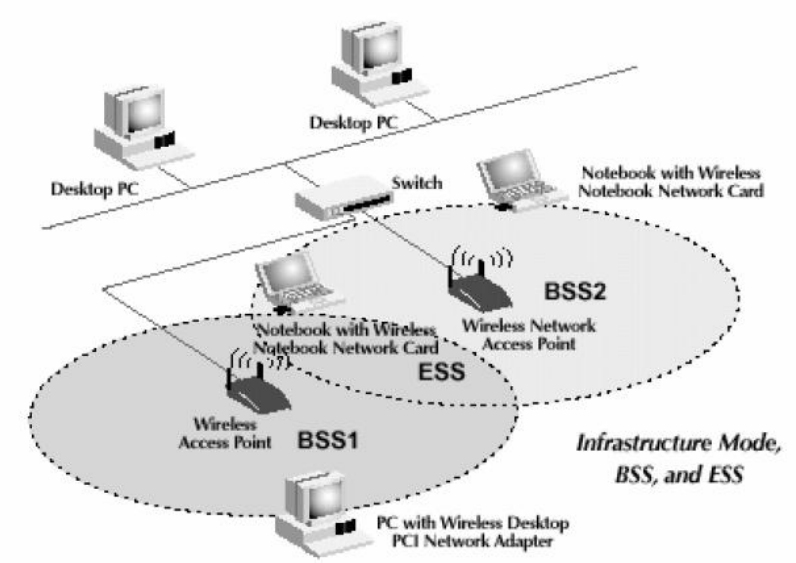


KUVIO 1. Ad-hoc verkko (Aittoniemi & Nenonen 2007)

Infrastruktuuritopologiassa (KUVIO 2) on yksi tai useampia tukiasemia (Access Point), johon työasemat ovat yhteydessä. Verkko ei kuitenkaan yleensä ole täysin langaton, vaan tukiasemat ovat kiinni perinteisessä lankaverkossa ja niiden välinen liikenne kulkee kaapelia pitkin, jolloin työasemat voivat käyttää myös lankaverkon palveluja. Tukiaseman tehtäviä ovat datan reititys määränpäähän, ruuhkan

kontrollointi, datayksiköiden koon vaihtelun kompensointi sekä työasemien tunnistus. Infrastruktuuriverkon luotettavuus perustuu tukiasemaan, jonka rikkoutuessa verkkoon liitetyt työasemat voivat perustaa oman Ad-hoc verkon, mutta samalla menettävät runkoverkon mahdollistamat palvelut. (Helin ym. 2002, 7; Ruotsalainen 2007, 11.)

ESS (KUVIO 2) muodostuu vähintään kahden BSS-infrastruktuuriverkon muodostaessa keskenään aliverkon. Usein ESS on yhteydessä kiinteään runkoverkkoon (DS, Distribution System), joka mahdollistaa runkoverkon palvelut. ESS-verkko muodostuu tukiasemien muodostamista soluista, joiden kantoalueella verkkoon liittyneellä työasemalla on mahdollisuus liikkua vapaasti. (Ruotsalainen 2007, 12.)



KUVIO 2. Infrastruktuuriverkot BSS ja ESS (Aittoniemi & Nenonen 2007)

Kun työasema liikkuu ja signaali tukiasemaan heikkenee työasema voi vaihtaa automaattisesti toiseen vahvemman signaalin tarjoamaan tukiasemaan. Yhteyden muodostaminen uuteen tukiasemaan on mahdollista tukiasemien vaihtaessa tietoja keskenään tukiasemaa vaihtavasta työasemasta. Vahvemman signaalin tarjoamalle tukiasemalle lähetetään pyyntö solun vaihtamisesta ja jos solun vaihto hyväksytään, yhteys heikomman signaalin tarjoamaan tukiasemaan puretaan. Verkon eri solujen sisällä tapahtuvaa vapaata liikkumista kutsutaan roamingiksi. (Ruotsalainen 2007, 12.)

Runkoverkko mahdollistaa tukiasemien välisen tietoliikenteen ja sen kautta voidaan myös kytkeytyä kiinteän verkon puolella olevaan lähiverkkoon. Suositukset määrittelevät runkoverkolle yhdeksän palvelua:

- Autentikointipalvelut (Authentication) valvovat verkkoon oikeutettujen päätelaitteiden liittymistä verkkoon.
- Autentikoinnin lopetuspalvelu (Deauthentication) jonka avulla päätelaite päättää istunnon. Päästäkseen takaisin verkkoon laitteen tarvitsee autentikoida itsensä uudelleen.
- Siirtotien suojaus (Privacy) palvelulla varmistetaan liikenteen suojaus niiltä laitteilta jotka on autentikoitu verkkoon. Palvelu antaa langattomalle verkolle langallista verkkoa vastaavaa tietosuojaa.
- Tiedonsiirtopalvelu (Data delivery) jolla mahdollistetaan luotettava keskustelu kahden verkkoon liittyneen laitteen välillä ja varmistetaan kuittauksien tiedonsiirto myös OSI-mallin 2. kerroksella, siirtokerroksella.
- Sidonta (Association), autentikoinnin jälkeen suoritettava palvelu jolla muodostetaan looginen yhteys työaseman ja tukiaseman välille. Sidonta palvelua tarvitaan resurssien varaamiseen päätelaitteelle ja yhteyden ohjaamiseen päätelaitteelle.
- Uudelleensidonta (Reassociation), tarvitaan, kun työasema siirtyy tukiaseman palvelualueelta toisen tukiaseman alueelle eli solujen väliseen siirtoon.
- Sidonnan purku (Deassociation), tarvitaan kun halutaan tukiaseman pakottavan päätelaitteen sidontaan tai kun päätelaite ei halua kiinteän verkon palveluja.
- Reitityspalvelu (Distribution), jonka avulla selvitetään vastaanottajan sijainti
- Integrointipalvelu huolehtii rajapinnasta IEEE 802.11 -verkon ja muiden verkkojen välillä. (Vesanen 2003; Ruotsalainen 2007. 13.)

2.3 WLAN-protokollat

2.3.1 Protokollapino

WLAN-standardeissa on määritelty ISO:n (International Organization for Standardization) OSI-mallin (Open System Interconnection) kaksi alinta kerrosta: fyysinen kerros ja siirtoyhteyskerros, josta standardit määrittelevät vain siirtoyhteyskerroksen alemman osakerroksen eli MAC-kerroksen. Sekä IEEE:llä että ETSI:llä (European Telecommunications Standard Institute) on standardi langattomille lähiverkoille. IEEE:n standardista käytetään nimeä IEEE 802.11 ja ETSI:n standardista HIPERLAN (High Performance Radio Local Area Network). (Aittoniemi & Nenonen 2007, 6)

802.11-protokolla määrittelee Media Access Control -kerroksen (MAC), joka keskustelee kolmen erilaisen fyysisen kerroksen kanssa. MAC-kerros huolehtii radiotien saatavuudesta fyysisestä kerroksesta riippumattomasti. OSI-mallin fyysinen kerros tuo rajapinnan varsinaiseen mediaan ja hoitaa varsinaisen signaloinnin verkon ylitse. MAC-alikerros on erillään fyysisestä kerroksesta, jotta mahdolliset uudet taajuuskaistat ja modulointimenetelmät voitaisiin helpommin päivittää järjestelmiin. (Lehtonen 2007, 24.)

2.3.2 Fyysinen kerros

Fyysisen kerroksen tehtävänä on IEEE 802.11-suosituksessa yhdistää MAC-kerros radiotielle. Se sijaitsee OSI-mallissa alimpana ja sen muihin tehtäviin kuuluvat sanomien välitys MAC-kerroksen ja fyysisen kerroksen välillä, datan modulointi siirtoteknologian mukaisesti sekä kuulostelua (engl. carrier sense) koskevien tietojen välitys MAC-kerrokselle. (Aittoniemi & Nenonen 2007, 5.)

Fyysinen kerros jakaantuu kahteen alikerrokseen; PMD-kerroksen toiminnot ovat siirtotekniikasta riippuvaisia ja PLCP-kerroksen toiminnot ovat yhtenäiset kaikille toteutustavoille. Radiotiellä tiedonsiirtokaistana käytetään alueita 2,4 - 2,485 GHz ja 5,725 - 5,825 GHz. Joitakin maakohtaisia rajoituksia ja laajennuksia taajuusalueluiden käytölle on olemassa. USA:ssa ja suurimmassa osassa Eurooppaa mainitut alueet ovat käytössä - Japanissa, Ranskassa ja Espanjassa käytetään hieman eri taajuuksia. Kyseiset taajuusalueet valittiin, koska niillä voidaan operoida

ilman lisenssiä missä tahansa maailmassa ja datasiirrossa voidaan käyttää LAN-verkkoihin sopivaa siirtonopeutta. (Vesanen 2003.)

2.3.3 Linkkikerros (Media Access Control)

Linkkikerros on jaettu kahtia, kuten perinteisissäkin lähiverkoissa, LLC- (Logical Link Control) ja MAC- (Media Access Control) kerroksiin. MAC-kerros määrittelee pääsyn fyysiseen kerrokseen ja huolehtii fyysisen siirtomedian saatavuudesta. LLC (Logical Link Control Layer) määrittelee standardin rajapinnan verkkokerrokseen, kuten LAN-verkossa yleensäkin. (Vesanen 2003; Lehtonen 2007, 24.)

IEEE802.11-standardin erona Ethernet-standardiin on, että Ethernet käyttää CSMA/CD (Carrier Sense Multiple Access with Collision Detection) -algoritmia ja WLAN CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) -algoritmia. Ensin mainittu algoritmi peruu operaation havaittuaan törmäyksen ja jälkimmäinen pyrkii perumaan operaation jo ennen kuin törmäys tapahtuu. Koska ilmassa tapahtuva liikennöinti kuluttaa enemmän resursseja kuin kaapelissa, kannattaa WLANissa käyttää törmäykset ehkäisevää algoritmia. Näin vältytään törmäyksiltä hieman pitempien viiveiden kustannuksella. Törmäyksiä saattaa silti tapahtua sillä WLAN-protokollassa virheellisen sanoman vastaanottaminen ja sanoman kuittauksen (acknowledgement, ACK) puuttuminen tulkitaan törmäykseksi. Törmäyksestä toipumiseen käytetään eksponentiaalista toipumista, ts. törmäyksen satuttua valitaan satunnainen viive, joka aina uuden törmäyksen sattuessa kaksinkertaistetaan. Toipumista käytetään myös onnistuneen lähetyksen jälkeen. CSMA/CA-algoritmin toimintaa voidaan kuvata seuraavasti:

- Halutessaan lähettää laite tutkii onko siirtotie vapaana. Mikäli siirtotiellä on muuta liikennettä, siirrytään eksponentiaaliseen toipumismenettelyyn.
- Vapaalle siirtotielle lähetetään RTS (Request To Send) -sanoma. Tähän odotetaan CTS (Clear To Send) -kuittausta. Mikäli kuittausta ei saada, siirrytään eksponentiaaliseen toipumismenettelyyn.
- Laite lähettää datasanoman ja odottaa kuittausta (ACK). Jos kuittausta ei saada, oletetaan törmäyksen tapahtuneen ja siirrytään eksponentiaaliseen toipumismenettelyyn. (Vesanen 2003.)

WLAN eroaa tavallisesta ethernetistä siirtoyhteyskerrostasolla vielä kolmessa kohdassa:

- WLAN käyttää pakettien eheyden takaamiseksi 32-bittistä CRC tarkistussummaa. Tämä tehdään normaalisti Ethernetissä ylemmissä kerroksissa, esimerkiksi TCP/IP-tasolla.
- Isot paketit voidaan pilkkoa ennen lähetystä pienentämään datan korruptoitumisen riskiä ruuhkaisessa tai häiriöpitoisessa ympäristössä. MAC-kerros on myös vastuussa pilkottujen pakettien uudelleen kokoamisesta.
- Kahdenvälisessä liikenteessä datapaketin vastaanottaja lähettää paketin lähettäjälle välittömästi ilmoituksen (ACK) mikäli paketti on asianmukaisesti vastaanotettu. (Vesanen 2003.)

2.4 Suojausmenetelmät

2.4.1 SSID (Service Set Identifier)

Langattomissa lähiverkoissa SSID tarkoittaa langattoman verkon verkkotunnusta. SSID:n avulla erotetaan samalla kuuluvuusalueella olevat langattomat verkot toisistaan ja sen avulla tietokoneet osaavat kytkeytyä haluttuun verkkoon. Tukiaseman asetuksissa määriteltävä SSID on enintään 32 merkin mittainen merkkijono (esim. "Kotiverkko"). Tukiasemissa on oletuksena laitteen valmistajien oletus SSID ja salasana. Valmistajien oletus SSID:t ja salasanat on helppo tarkistaa esim. valmistajien verkkosivuilta ja näin verkkoon voi päästä helposti käsiksi. Verkko tulisi nimetä heti verkon perustamisen jälkeen sellaiseksi, joka on hankala arvata. Tukiasemissa on myös oletuksena asetus, joka lähettää SSID-tiedon beacon-viestin mukana, eli verkko mainostaa itseään. Tämä broadcast SSID-asetus on syytä laittaa pois päältä, jolloin verkon nimen lähetys estetään. (MVNet 2007; Ruotsalainen 2007, 27.)

SSID:n piilottaminen ei kuitenkaan varsinaisesti piilota sitä kokonaan. Piilottaminen estää vain sen, että tukiasema ei enää lähetä SSID-tietoa beacon-viestin mukana. SSID kuitenkin lähetetään salaamattomana verkon yli useassa muussa tilanteessa. Esimerkiksi tietokoneen kirjautuessa langattomaan verkkoon SSID kulkee salaamattomana asiakaskoneen ja tukiaseman välillä, joten tarpeeksi kauan verkkoa kuuntelemalla on mahdollista saada piilotettu SSID selville (MVNet 2007.)

2.4.2 MAC-osoitepääsylistat

MAC-osoite on IEEE 802.11-standardin mukainen 48-bittinen heksadesimaaliluku, joka on yksilöllinen kaikissa verkkokorteissa. Osoitepääsylistojen yhteydessä pyritään tunnistamaan verkkoon pyrkivä laite. Suurin osa WLAN-laitteista tukee MAC-tunnistusta eli MAC-autentikointia, minkä avulla pystytään rajaamaan laitteet, joilla on pääsy verkkoon. Tukiasemaan määritellään hyväksytyt MAC-osoitteet ja pääsylistaan kuulumattomien laitteiden kommunikointi langattomassa lähiverkossa estetään. (Niemi 2007, 22.)

Suojauksen heikkoutena on se, että MAC-osoitteet kulkevat salaamattomina jokaisessa langattoman verkon paketissa, vaikka niissä itse data olisikin salattu. Liikennettä kuuntelemalla siihen tarkoitetuilla ohjelmilla saa MAC-osoitteet selville muutamissa sekunneissa. Useimmissa tietokoneissa verkkokortin MAC-osoitteen saa vaihdettua helposti. Näin yhteys verkkoon aukeaa helposti hyökkääjälle. Lisäksi MAC-osoitelistan ylläpitäminen on työlästä varsinkin, jos verkkoon lisätään uusia koneita usein tai verkkoa tarjotaan vierailijoille. (Niemi 2007, 22.)

2.5 Salausmenetelmät

2.5.1 WEP (Wired Equivalent Privacy)

WEP on IEEE 802.11-suosituksen ensimmäinen työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä. WEP-salauksessa (Wired Equivalent Privacy) tukiasemalle määritellään salausavain joka voi olla 64-, 128- tai 256-bittinen. Salausavaimen pituudesta riippuu se, kuinka kauan salauksen murtamisessa kestää eli mitä pidempi salausavain on, sen vaikeampi se on purkaa. (Niemi 2007, 23.)

WEP-salauksessa kaikki verkon datapaketit salataan käyttäen jaettua salausavainta (PSK, Pre Shared Key) sekä ns. alustusvektoria (IV, Initializion Vector), joka vaihtelee aina eri pakettien välillä. WEP-salauksessa jaettu salausavain on 40-, 104- tai 232-bittinen 5 - 29 merkkiä pitkä salasana, joka on vain tukiaseman ja siihen liittyneiden tietokoneiden tiedossa. Alustusvektori on taas 24-bittinen 3 merkkiä pitkä vaihtuva merkkijono. Alustusvektori lähetetään aina paketin otsaketiedoissa salaamattomana, jotta vastapuoli voisi purkaa paketin sisällön (Thomas 2005, 307.)

WEP-salauksessa tukiasemiin ja päätelaitteisiin määritetään staattinen salausavain, joka on sama kaikissa laitteissa ja kaikki data salataan samalla avaimella. Samana pysyvän avaimen voi selvittää kuuntelemalla liikennettä. Datapaketin lyhyen ja salaamattoman alustusvektorin voi arvata melko suurella varmuudella, tarkalleen $2^{24}=16,7*10^6$ paketin jälkeen samaa alustusvektoria joudutaan käyttämään uudelleen. (Vähä-Touru 2007, 21.)

2.5.2 WPA (Wi-Fi Protected Access)

WPA kehitettiin korjaamaan WEP:n puutteita ja mukaan on saatu myös tuki käyttäjien autentikoinnille. WPA käyttää salaukseen TKIP (Temporal Key Integrity Protocol) protokollaa ja 10 000 paketin välein vaihtuvia pidempiä salausavaimia. WPA-salausmenetelmässä käyttäjien autentikointi voidaan toteuttaa IEEE 802.1X -protokollan avulla. 802.1X autentikoi käyttäjän erillisen tunnistuspalvelimen käyttäjätietokantaa käyttäen. WPA tarjoaa TKIP-tekniikan ja 802.1X-tuen johdosta dynaamisen avaimensalauksen ja kaksisuuntaisen todennuksen. WPA:n huonona puolena on sen toiminta palvelunestohyökkäyksissä. Jos hakkeri tai tietämätön, luvallinen käyttäjä lähettää vähintään kaksi datapakettia sekunnissa väärää WPA-kryptausavainta käyttäen, sulkee tukiasema pääsyn kaikilta verkon käyttäjiltä yhden minuutin ajaksi. Tällä tavalla WPA-järjestelmä estää luvattomia käyttäjiä pääsemästä verkkoon. (Vähä-Touru 2007, 21.)

WPA-tekniikasta on olemassa kaksi eri versiota, yrityskäyttöön ja kuluttajakäyttöön. Ominaisuudet kummassakin ovat identtisiä, mutta yrityksille tarkoitetussa Enterprise-versiossa käytetään autentikointipalvelua. Enterprise-versiossa on käytettävä autentikointipalvelua, joka voi olla ulkoinen palvelin tai tukiasema, mikäli se tukee paikallista autentikointipalvelua. Autentikointipalvelun lisäksi Enterprise-versiossa on käytettävä porttikohtaista EAP-autentikointia. Standard-versio eli WPA-PSK (Pre-Shared Key) on kuluttajakäyttöön tarkoitettu versio, joka ei vaadi EAP-autentikointia, eikä autentikointipalvelua. Standard-versiossa kirjautuminen tapahtuu TKIP-salatulla salasanalla. (Hämäläinen 2007, 48.)

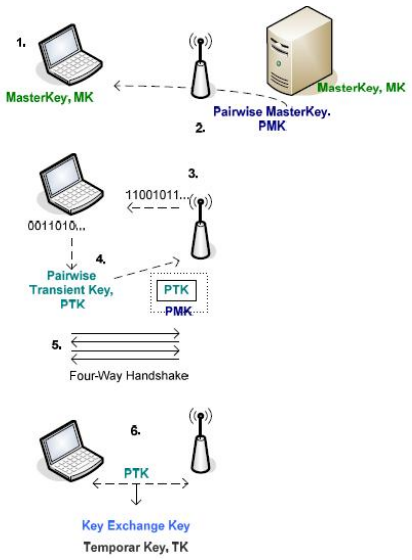
2.5.3 WPA2 (IEEE 802.11i / Robust Security Network)

WPA2 perustuu IEEE 802.11i-standardiin. Salaukseen voidaan käyttää TKIP:n sijaan AES-salausta, jota pidetään erittäin tehokkaana algoritmina. AES tosin vaatii enemmän suoritustehoa laitteilta ja vanhaa laitekantaa on vaikeampi päivittää tukemaan WPA2:ta. IEEE 802.11i -standardia käyttäviä WLAN-verkkoja kutsutaan myös nimellä RSN-verkko (Robust Security Network). Kyseistä standardia käytetään pääasiassa yhdessä 802.1X-järjestelmän kanssa. Parempien salausmenetelmien lisäksi 802.11i sisältää avainpareihin perustuvan avainhallinnan, jossa pääte ja tukiasema salaavat liikenteen pareittaisella lähetysavaimella, joka vaihtuu määräajoin. 802.11i sisältää myös esitunnistuksen (Pre-Authentication), jonka ansiosta langatonta päätettä voidaan siirtää eri yhteyspisteiden välillä ilman uudelleen tunnistautumisen aiheuttamia katkoksia. Esitunnistuksessa tunnistuspalvelin lähettää hyväksytyn käyttäjän tiedot kaikille verkon yhteyspisteille (Vähä-Touru 2007, 21.)

Kuten WPA-tekniikkaa, myös WPA2-tekniikkaa on mahdollista käyttää kahdessa eri tilassa, WPA2-Personal ja WPA2-Enterprise -tilassa. Enterprise-versio käyttää avaintenhallintaa, joka perustuu avainpareihin. Avaintenhallinta vaatii porttikohtaisen autentikoinnin (EAP) ja autentikointi-palvelun käytön mikäli tukiasema ei tue paikallista autentikointipalvelua. Työasemaan ja autentikointipalvelimeen (tukiasema) määritetään uniikki yleisavain, jonka avulla muut tarvittavat avaimet saadaan muodostettua. Työaseman ja tukiaseman välinen liikenne salataan määräajoin vaihtuvalla parittaisella lähetysavaimella. Standard-versio on suunniteltu kuluttajille ja se käyttää myös AES-algoritmia salaukseen, mutta ei vaadi autentikointipalvelua. Tukiasemiin kirjautuminen tapahtuu käyttämällä pelkästään salasanaa. (Hämäläinen 2007, 50.)

Seuraavassa käydään läpi IEEE 802.1i avaintenhallinnan toimintaa (kuvio 3):

- Työasemiin ja tunnistuspalvelimeen on määritelty valmiiksi yleisavain (Master Key, MK), jonka avulla prosessin muut avaimet luodaan.
- Työasema ja tunnistuspalvelin generoivat yleisavaimestaan (MK) parittaisen yleisavaimen (Pairwise Master Key, PMK), jonka tunnistuspalvelin toimittaa yhteyspisteelle.
- Työaseman ja tunnistuspalvelimen välinen yhteyspiste lähettää työasemalle bittijonon, josta työasema generoi oman bittijononsa kanssa parittaisen tilapäisavaimen (Pairwise Transient Key, PTK).
- Työasema lähettää yhteyspisteelle generoimansa parittaisen tilapäisavaimen (PTK), joka on salattu parittaisella yleisavaimella (PMK).
- Viestinvaihto kuitataan nelinkertaisella kättelyllä (Four-Way Handshake) työaseman ja yhteyspisteen välillä.
- Parittaisesta tilapäisavaimesta (PTK) lasketaan vielä avaintenvaihdon vahvistusavain ja salausavain (Key Exchange Key) sekä tilapäisavain (Temporary Key, TK), jota käytetään itse datan salaukseen työaseman ja yhteyspisteen välillä. (Vähä-Touru 2007, 23.)



KUVIO 3. 802.11i avaintenhallinta (Vähä-Touru 2007, 22.)

2.5.4 VPN (Virtual Private Network)

VPN (Virtual Private Network) on yleisnimitys toteutuksille joissa IP-liikenne salataan turvattoman verkon yli. VPN-ratkaisu tarjoaa mahdollisuuden liittää lähiverkot yhteen käyttäen internetiä siirtotienä (LAN-to-LAN). Langattoman lähiverkon VPN-ratkaisussa WLAN on turvaton verkko, jonka yli työasemat liikennöivät yrityksen lähiverkkoon. (Puska 2005, 85.)

Langattomassa lähiverkossa salattu yhteys muodostuu työaseman ja VPN-yhdyskäytävän välille, joiden välille syntyy kaksi tunnelia. Avaintenvaihtoa varten perustetaan tunneli (IKE), joka käyttää UDP-porttia 500. Tunnistuksen ja avainten vaihdon jälkeen muodostetaan datatunneli IPsec-IP-protokollanumeroa 50 käyttäen. Tunnelit päättävä laite voi olla VPN-palomuuri, -reititin tai VPN-keskitin. Työasemassa tarvitaan lisäksi erillinen VPN-ohjelmisto. VPN-yhdyskäytävä tarkistaa käyttäjänimen ja salasanan tunnistuspalvelimelta esimerkiksi RADIUS-protokollaa käyttäen. Mitään erillistä WLAN-verkon salausta tai autentikointia ei VPN-ratkaisussa tarvitse käyttää, koska VPN-ratkaisu itsessään huolehtii tarvittavista tietoturvatoimenpiteistä. (Puska 2005, 87.)

IPsec (Internet Protocol Security) on tällä hetkellä suosituin protokolla VPN-järjestelmien pohjaksi. IPsec-protokollan kanssa käytetään yleensä IKE-protokollaa (Internet Key Exchange) avaintenhallintaan ja DES-, 3DES- tai AES-algoritmia salaukseen. (Puska 2005, 87.)

2.6 Remote Authentication Dial In User Service (RADIUS)

2.6.1 RADIUS-protokolla ja sertifikaatit

RADIUS-protokolla on alun perin suunniteltu sisäänsoittopalveluissa tapahtuvaan tunnistukseen. Nykyään sitä käytetään RADIUS-autentikointipalvelimissa, joka on palvelinpohjainen tunnistamiseen, pääsynvalvontaan, asetustietojen välittämiseen ja käyttötilastointiin kehitetty yhteyskäytäntö. RADIUS-palvelin helpottaa merkittävästi verkon ylläpitoa, koska sen avulla käyttäjien todentaminen voidaan hoitaa keskitetysti. Käyttäjien todentamiseen voidaan käyttää erilaisia menetelmiä, kuten käyttäjätunnus-salasanaparia, sertifikaattia tai älykorttia. RADIUS-palvelimella voidaan helposti estää luvattomien tukiasemien liittäminen verkkoon,

koska se huomioi vain rekisteröityjen tukiasemien todentamispyynnöt. (Ruotsalainen 2006, 34.)

Sertifikaatti on sähköinen todistus, jonka myöntäjä allekirjoittaa sertifikaatin tiedot omalla salaisella avaimellaan. Sertifikaatin aitous voidaan tarkistaa myöntäjän julkisella avaimella. Varmenteella voidaan varmistua käyttäjän henkilöllisyydestä verkkopalvelussa tai verkkopalvelun aitoudesta. Sertifikaattia pidetään luotettavana, kun se täyttää sille asetetut edellytykset; sertifikaatin myöntäjä on luotettava, sertifikaatin myöntäjän yksityinen avain pysyy salassa, sertifikaatin myöntäjän julkinen avain on saatu turvallista kanavaa pitkin ja sertifikaatin käytössä oleva salaustekniikka on riittävän vahva. (Järvinen 2002, 379; Korhonen 2006, 18.)

2.6.2 RADIUS-protokollan toiminta

RADIUS-protokolla käyttää UDP-protokollan porttia 1812 viestien välittämiseen asiakkaalta palvelimelle. Käyttäjän kirjautuessa RADIUS-tunnistusta vaativaan järjestelmään liityntäpiste eli RADIUS-Client, (langattomissa verkoissa tukiasema, langallisissa verkoissa kytkin), lähettää Access-Request -viestin RADIUS-palvelimelle. Viestin parametreina lähetetään käyttäjätunnus, MD5-salattu salasana, asiakaslaitteen tunnus ja portti, johon käyttäjä on pyrkimässä. RADIUS-palvelin varmistaa, että viestin lähettäneen liityntäpisteen IP-osoite ja salasana on määritelty palvelimelle, ja jos määrittelyt ovat oikein, pyyntö käsitellään. (Ruotsalainen 2006, 35.)

Pyynnön käsittelyn aluksi RADIUS-palvelin tarkistaa käyttäjätunnuksen tiedot tietokantapalvelimelta (usein AD). Tietokannassa olevat tiedot sisältävät vaatimuksia, jotka käyttäjän on täytettävä. Vaatimuksia voivat olla salasana, porttinumerot tai liityntäpisteet, joihin käyttäjällä on oikeus. Tietokannassa voidaan esim. määritellä onko tietyllä käyttäjällä oikeus kirjautua verkkoon langatonta tukiasemaa käyttäen. Jos edellä mainitut ehdot täyttyvät, asiakkaalle lähetetään joko Access Accept-viesti (yhteys hyväksytään) tai Access-Challenge-viesti tai Access-Reject-viesti (yhteys hylätään). Access-Challenge-viestissä lähetetään käyttäjälle haaste/vastaus-tunnistusmenetelmällä satunnaisluku, jolla käyttäjän tarvitsee salata salasanansa ja lähettää salattu salasana viestin vastauksena. Kyseistä tunnistusta käytetään järjestelmissä, joissa käyttäjän kirjautuessa käyttäjä syöttää käyttäjätunnuksensa ja salasanansa, jolloin ensimmäisessä Access-Request-viestissä lähete-

tään vain käyttäjätunnus ja Access-Challenge-vastauksessa salattu salasana. (Ruotsalainen 2006, 36.)

Viestien vaihto RADIUS-Clientien ja RADIUS-palvelimen välillä on autentikoitu ns. Shared Key:n avulla. Tämä avain on molempien tiedossa, joten sitä ei koskaan lähetetä verkon yli ja ilman sitä autentikointi ei onnistu. Tietoturvan lisäämiseksi yhteydenottopyynnöt RADIUS-palvelimelle sallitaan vain erikseen määritellyiltä RADIUS-Clienteilta. Lisäksi käyttäjien salasanat lähetetään verkon yli aina salattuina. (Seppälä 2006, 8; Ruotsalainen 2006, 36.)

2.6.3 IEEE 802.1X -käyttäjäntunnistus

Vuonna 2001 julkistettu IEEE 802.1X tarjoaa huomattavia parannuksia langattomien lähiverkkojen turvallisuuteen. IEEE 802.1X on alun perin suunniteltu langallisten lähiverkkojen porttiautentikoinnin toteuttamiseksi, joka määrittelee miten EAP:tä käytetään IEEE 802:sta käyttävien välineiden (IEEE 802.11b, 802.11g ja ethernet-kytkimet) kanssa, mutta se soveltuu käytettäväksi myös langattomissa lähiverkoissa. WLAN-verkoissa tukiasema muodostaa jokaista käyttäjää kohden virtuaaliportin, jonka kautta liikennöinti voidaan sallia tai estää. IEEE 802.1X etuna on myös helppo laajennettavuus. IEEE 802.1X-standardissa on mahdollista ainoastaan EAP-autentikointimenetelmien käyttö. (Tuominen 2005, 21.)

Langattoman verkon IEEE 802.1X laillisuustarkistus käsittää kolme pääkomponenttia; varmistaja (tukiasema), anoja (asiakasohjelmisto) ja autentikointipalvelin (todennuspalvelu). Tukiasema ja autentikointipalvelin käyttävät kommunikoinnissa jotakin todennusprotokollaa. 802.1X ei määrittele käytettäväksi mitään tiettyä protokollaa, mutta useimmiten käytetään RADIUS-protokollaa jota käyttäen 802.1X-laillisuustarkistus käynnistää laillisuustarkistuspyynnön langattomasta asiakkaasta tukiasemaan, joka tarkistaa asiakkaan laillisuuden EAP (Extensible Authentication Protocol) -yhteensopivalta RADIUS-palvelimelta. RADIUS-palvelin voi tarkistaa joko käyttäjän tai järjestelmän laillisuuden. Käyttäjän laillisuus tarkistetaan salasanojen tai sertifikaattien avulla ja järjestelmän laillisuus tarkistetaan MAC-osoitteen tai sertifikaattien kautta. Teoriassa langattoman asiakkaan ei sallita liittyä verkkoon, ennen kuin tämä tapahtuma on valmis. (Dell 2007.)

802.1X:ssä voidaan käyttää useita laillisuustarkistusyhteyskäytäntöjä. EAP MD5 (EAP Message Digest 5), EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled TLS) ja PEAP (Protected EAP) ovat kaikki menetelmiä, joilla RADIUS-palvelin voi tunnistaa langattoman asiakkaan. RADIUS-laillisuustarkistuksessa käyttäjien henkilöllisyydet tarkistetaan esim. toimialuepalvelimen (AD; Active Directory) tietokannoista. (Dell 2007.)

802.1X-liikenne käynnistyy, kun todentamaton langaton laite, esimerkiksi kannettava tietokone, yrittää muodostaa yhteyden langattomaan tukiasemaan. Tukiasema vastaa avaamalla portin, joka sallii ainoastaan EAP-paketit asiakkaalta todennuspalvelimelle. Todennuspalvelin, esimerkiksi Radius-palvelin, sijaitsee käytännössä tukiaseman ”langallisella” puolella. Kunnes laite on todennettu, tukiasema estää muun liikenteen, esimerkiksi HTTP (Hypertext Transfer Protocol) -, DHCP (Dynamic Host Configuration Protocol) - ja POP3 (Post Office Protocol version 3) -liikenteen, kulkemisen kauttansa. Mikäli todennus onnistuu, portti avataan muullekin liikenteelle todennuspalvelimen sallimien oikeuksien mukaisesti. (Vähä-Touru 2007, 25.)

Vaikka 802.1X-standardi käyttää WEP-salausta, niin molemminpuolinen tunnistus ja dynaaminen avainten hallinta lisää huomattavasti WLAN-verkon turvallisuutta alkuperäiseen WEP-suojaukseen nähden. Dynaaminen avainten hallinta vähentää avainhyökkäyksille altistumista ja molemminpuolinen tunnistus auttaa varmistamaan sen, että työasemat kommunikoivat tunnettujen verkkojen kanssa. (Tuominen 2005, 21.)

2.6.4 EAP-TLS ja EAP-TTLS

EAP-TLS (Transport Layer Security) käyttää PKI:ta (Public Key Infrastructure) eli epäsymmetristen ja julkisten avainten sertifikaattien jakelujärjestelmää. Sertifikaatti on tarkoitettu tiettyyn käyttöön ja se on voimassa vain rajoitetun ajan. CA (Certification Authority) varmistaa luotettuna tahona allekirjoituksellaan sertifikaatin aidoksi ja sen tiedot oikeiksi. (Ruotsalainen 2006, 39.)

EAP-TLS-protokollalla mahdollistetaan kaksisuuntainen toteaminen, eli sekä asiakas että verkko autentikoivat toisensa siten, että palvelin esittää ensin sertifikaattinsa asiakkaalle, joka tarkistaa sertifikaatin kelpoisuuden. Sertifikaatin kelpoisuuden tarkistuksen jälkeen asiakas esittää oman sertifikaattinsa autentikointi-

palvelimelle, joka puolestaan tarkistaa asiakkaan sertifikaatin kelpoisuuden ja päättää asiakkaan pääsystä verkkoon. EAP-TLS:n heikkouksia ovat salaamattomana palvelimelle lähetettävät asiakkaan tiedot sekä se, että asiakaspäätteellä pitää olla asiakassertifikaatti joka kasvattaa järjestelmän ylläpitotöitä. (Ruotsalainen 2006, 39.)

EAP-TTLS (Tunneled Transport Layer Security) on TLS-salauksen seuraaja, joka helpottaa sertifikaattikäytäntöä ja ottaa käyttöön suojatun yhteyden (secure connection tunnel) käyttäjän autentikoinnin ajaksi. Kaksivaiheinen autentikointi alkaa salatun yhteyden muodostamisella asiakkaan ja todentamispalvelimen välille, jonka jälkeen todentamispalvelin autentikoituu omalla sertifikaatillaan asiakaskoneelle. Toisessa vaiheessa tunnelin sisällä todentamismekanismina voidaan käyttää mitä tahansa palvelimen tukemaa todentamismenetelmää. EAP-TTLS:ssä myös asiakas voi autentikoitua palvelimelle omalla sertifikaatillaan, mutta se ei ole välttämätöntä. EAP-TTLS:n toisessa vaiheessa voidaan tunnelin sisällä tapahtuva autentikointi suorittaa muutakin kuin EAP-protokollaa käyttäen, esim. CHAP-, PAP-, MS-CHAP- tai MS-CHAPv2-autentikointimenetelmillä. (Ruotsalainen 2006, 39; Hämäläinen 2007, 52.)

2.6.5 EAP-PEAP ja MS-CHAPv2

Cisco Systemsin, Microsoftin ja RSA Securityn yhdessä kehittämä PEAP (Protected EAP) muistuttaa EAP-TTLS-salausta. PEAP muodostaa suojatun yhteyden työaseman ja autentikointipalvelimen välille, mutta se ei salaa lainkaan liikennettä niin kuin muut EAP-tekniikat. PEAP:n tarkoituksena on tarjota kaksivaiheinen autentikontimenettely. Ensin luodaan turvallinen TLS-kanava autentikoivalta työasemalta palvelimelle, palvelin autentikoituu työasemalle omalla palvelinvarmenteellaan ja työasema pystyy autentikoitumaan palvelimelle omalla asiakasvarmenteellaan. Autentikoinnin toisessa vaiheessa, turvallisen kanavan muodostuttua suoritetaan varsinainen autentikoituminen, jossa käytetään jotain EAP-menetelmää. (Seppälä 2006, 11; Hämäläinen 2007, 52.)

Point-to-Point Protocol-autentikaatioprotokolliin (PPP) kuuluva MS-CHAP on Microsoftin versio Challenge-Handshake Authentication protokollasta (CHAP). MS-CHAP v2 on salasanaan perustuva haaste-vastaus-protokolla joka käyttää salausalgoritmina MD5:sta ja DES:iä. Palvelin, johon halutaan autentikoitua lä-

hettää haasteen yhteyttä yrittävälle laitteelle. Haaste tehdään molempiin suuntiin, eli myös autentikoiva laite lähettää oman haasteensa palvelimelle. Jos jompikumpi haasteista on väärä, evätään yhteys. CHAP-protokolla käyttää neljää viestityyppiä, Challenge, Response, Success ja Failure. Tunnistamista vaativa osapuoli lähettää Challenge-viestin, jossa se pyytää käyttäjältä käyttäjätunnusta sekä antaa haasteen. Käyttäjä vastaa Response-viestillä, joka sisältää käyttäjätunnus salasanaparista lasketun tarkistussumman. Jos tarkistussumma täsmää, tunnistautumista pyytävä laite lähettää Success-viestin ja mikäli tarkistussumma on väärä, lähetetään Failure-viesti. (Seppälä 2006, 10.)

Langattomien verkkojen kehityksen suunta on vahvasti yhteysnopeuksien kasvattamisessa ja tietoturvan lisäämisessä. OFDM-tekniikan käyttöönotto mahdollisti jo 54 Mbit/s nopeudet ja lähitulevaisuudessa odotetaan jopa 100-200 Mbit/s todelliseen nopeuteen yltävää 802.11n-standardia. 802.11n-standardin vahvistamista on odotettu jo kauan huolimatta siitä, että sen julkistamista on toistuvasti viivästetty.

Yhteysnopeuksien kasvun lisäksi huomiota on kohdistettu tärkeään suuntaan, langattomien verkkojen tietoturvaan. On otettu käyttöön vahvempia ja tehokkaampia salausalgoritmeja sekä pidempiä salausavaimia. Myös käyttäjien autentikointiin on kiinnitetty suunnittelussa huomiota. Kuitenkin langattomat verkot radiotien signaalin leviämisestä johtuen tulevat aina olemaan jossain määrin turvattomia eikä niihin voi täysin luottaa.

3 WLAN-TIETOTURVA

3.1 Tietoturvan tavoitteet

Tietoturva on perusta, jolle tärkeiden ja luottamuksellisten tietojen käsittely rakentuu. Yritysten näkökulmasta tärkeitä tietoja ovat mm. henkilöstöön, palkkoihin, tuotteisiin ja myyntilukuihin liittyvät tiedot. Niiden suojaaminen on yritystoiminnan jatkumisen edellytys. Tietoturva tarkoittaa käytännössä tietojen väärinkäytön estämistä. Se voidaan määritellä tiedon luotettavuudelle asetetuiksi kriteereiksi sekä järjestelyiksi, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvan ollessa riittävä tietoa voivat käyttää ja muokata vain ne henkilöt, joilla on lupa tiedon käyttöön. (Järvinen 2002, 21; Taito Oulu 400 2007.)

Tietoturvan perustavoitteet ovat:

- luottamuksellisuus: Kukaan ei pääse oikeudettomasti käyttämään tietoa, joka ei ole hänelle tarkoitettu.
- eheys: mikään ulkopuolinen taho ei pääse luvatta muuttamaan tiedon sisältöä. Myös tahattomasti aiheutuneet levyjen rikkoutumiset tai tiedonsiirrossa tapahtuneet virheet saatavat vaikuttaa tiedon eheyteen.
- saatavuus: Tietojen ja palvelujen saatavuus liittyy tietojärjestelmien toiminnan turvaamiseen. Tietojärjestelmien pitää toimia silloin kun tietoa halutaan käyttää.
- todentaminen: Luottamuksellisuus edellyttää todentamista, jolla varmistutaan kohteen todenmukaisuudesta, oikeellisuudesta tai alkuperästä, esimerkiksi tiedon käsittelijän henkilöllisyydestä varmistuminen
- pääsynvalvonta: huolehtii siitä, että vain todennetut henkilöt pääsevät käsiksi järjestelmän tietoihin. Pääsynvalvontaan liittyy myös käytön seuranta.
- kiistämättömyys: Eri menetelmin saatava varmuus siitä, ettei jälkikäteen voida kiistää jotain tehdyksi tai vastaanotetuksi. (Järvinen 2002, 22-27; Hakala & Vainio 2005, 342.)

Tietoturvasuunnittelun eräänä tavoitteena on luoda organisaatiolle toimiva tietoturvapolitiikka. Se muodostuu organisaation ylimmän johdon hyväksymistä käytännöistä, joiden avulla saavutetaan haluttu tietoturvallisuuden taso. Se laaditaan

yleisellä tasolla kuvaamaan, mikä on organisaation eri liiketoimintaprosessien edellyttämä tietojen turvaamisaste, millä menetelmillä haluttuun turvatasoon voidaan pyrkiä ja miten tietoturvallisuutta hallinnoidaan ja kehitetään. Tietoturvapolitiikka pitäisi kirjoittaa aina sellaiseen muotoon, että myös muut kuin tietojenkäsittelyn ammattilaiset voivat ymmärtää sen sisällön. Se ei myöskään saa sisältää sellaisia tietoja, jotka mahdollistaisivat hyökkäysten tai tietomurtojen suunnittelun (Hakala, Vainio & Vuorinen 2006, 14.)

3.2 Tietoverkkojen tietoturva

Tiedotusvälineissä ja julkisessa keskustelussa tietoverkkojen turvallisuus liittyy nimenomaan Internetiin, kuten sen kautta tuleviin hyökkäyksiin ja roskapostiin. Tietohallinnon näkökulmasta suurimmat ongelmat ovat yleensä oman sisäisen verkon eheydessä, käytettävyydessä ja luottamuksellisuudessa. Suurin osa tietoturvarikkomuksista tapahtuu edelleen organisaation sisällä (Hakala ym. 2006, 181.)

Tietoverkkojen tietoturvan erityispiirteitä ovat:

- Turvavaatimukset ovat usein yksinkertaisia esittää (luottamuksellisuus, autenttisuus, kiistämättömyys, eheys), mutta vaikeita toteuttaa
- Turvamekanismeja kehitettäessä tulee (luvattoman osapuolen) potentiaaliset vastatoimet ottaa huomioon. Näiden vastatoimien huomioiminen perustuu siihen, että turvaongelmaa katsotaan kokonaan toisesta näkökulmasta, jolloin tekniikoiden heikkoudet usein voidaan havaita
- Turvatoimet saattavat (edellisen nojalla) vaikuttaa ylimitoitetuilta eikä niiden tarpeellisuutta ole intuitiivisesti helppo nähdä
- Turvamekanismien suunnittelun jälkeen on vielä päätettävä missä niitä käytetään. Tämä koskee sekä fyysistä sijoittamista että sitä mille tasolle verkon loogisessa rakenteessa mekanismi asetetaan
- Turvamekanismien käyttö vaatii usein lisäresursseja ja saattaa vaikeuttaa normaaleja toimintoja. Niiden käyttöön tarvitaan salaista tietoa, jonka luonnista, jakelusta ja suojaamisesta tulee huolehtia. On mahdollista, että käytössä olevilla tiedonsiirtotekniikoilla ei turvatavoitteita saavuteta. (Kortelainen 2001, 6.)

Palomuuri (firewall) muodostaa tärkeimmän yksittäisen suojautumiskeinon verkosta tulevia tunkeilijoita vastaan. Palomuuri on portinvartijana organisaation oman lähiverkon ja julkisen tietoverkon välissä. Palomuuri tarkastaa yritykseen sisään tulevan liikenteen jokaisen paketin, mutta myös yrityksestä ulospäin suuntautuvan liikenteen. Palomuurina voidaan käsitteenä tarkoittaa hyvin erityyppisiä laitteita tai ohjelmistoja, joiden tehtävänä on estää asiattomien henkilöiden pääsy verkkoon tai tiettyyn verkon tarjoamaan palveluun. Palomuurit voidaan toimintansa puolesta jakaa kolmeen perustyyppiin: pakettisuodattimiin, välityspalvelimiin ja sovellustason yhdyskäytäviin. (Järvinen 2002, 315–316; Hakala ym. 2006, 187)

Pakettisuodattimet ovat laitteita, jotka hylkäävät liikennettä lähde- ja kohdeosoitteiden sekä sovellusten käyttämien porttinumeroiden perusteella. Välityspalvelimet (proxy) ovat laitteita, jotka avaavat käyttäjän puolesta yhteyden johonkin palveluun niihin etukäteen määriteltyjen asetusten perusteella. Välityspalvelut mahdollistavat usein myös laitteen käyttäjän luotettavan tunnistuksen eli autentikoinnin ennen yhteyden avaamista. (Hakala ym. 2006, 187-188.)

Tietoturvamielessä tehokkain palomuuri on sovellustason yhdyskäytävä, joka välittää liikenteen asiakas- ja palvelinohjelmiston välillä sekä tutkii jokaisen paketin sisällön. Sovellustason yhdyskäytävä toimii virustentorjuntaohjelmiston tavoin havaitessaan normaalista poikkeavia paketteja, niitä ei välitetä eteenpäin ja ne voidaan tarvittaessa tallentaa tarkempia analyysejä varten. Epäilyttävät paketit aiheuttavat hälytyksen, joka välitetään palomuurin käyttöhenkilöstölle. Sovellustason yhdyskäytävät tutkivat jokaisen paketin ennen niiden välittämistä eteenpäin, joka vaatii laitteelta huomattavaa prosessointitehoa. (Hakala ym. 2006, 187-188.)

Erillisten palomuuriohjelmistojen ja -laitteiden lisäksi verkoissa voidaan käyttää hyödyksi reitittimien sisältämiä IOS-pohjaisia pakettisuodatusominaisuuksia. Reitittimen ja siihen liitettyjen verkkojen sekä niiden laitteiden käyttöoikeudet määritellään ns. pääsylistojen (Access List) avulla. Niitä käytetään sekä varsinaisiin palomuuritoimintoihin että erilaisten päivitystietojen rajoittamiseen. (Hakala ym. 2006, 188.)

3.3 Langattoman verkon tietoturva

Langattoman tiedonvälityksen tärkein ominaisuus on signaalin leviäminen kaikkialle, jonka takia salakuuntelua on mahdoton täysin estää. Pienen lähiverkon liikenteen yksityisyys voidaan kenties taata rajoittamalla liikenne fyysisesti pieneen tilaan lähetystehoa rajoittamalla, mutta useimmiten langatonta liikennettä käytetään juuri sen paikkaan sitoutumattoman luonteen takia. Näin ollen yksityisyys pitää taata muilla ratkaisuilla, joka voi olla erittäin vaikeasti toteutettavissa. Erityisesti Internetiin liittyvät langattomat verkot vaativat erityisratkaisuja. (Vesanen 2003.)

Kun organisaation tietoliikenne siirtyy langattomiin välineisiin, on otettava huomioon ongelmat yksityisyyden suojaamisessa. On valittava politiikka, jolla yksityisyyden suoja toteutetaan. Voidaan rajoittaa langattomien laitteiden käyttöä, voidaan kehittää automaattisia ja henkilöiden käyttämiä turvaprotokollia tai sallitaan langattomien laitteiden vapaa käyttö yksityisyyden rajoittumisen kustannuksella. (Vesanen 2003.)

Langattomia verkkoja koskevat kaikki langallisten verkkojen tietoturvavaatimukset. Näiden lisäksi langattomuus ja radioaalloilla tapahtuva tiedonsiirto asettaa langattomille verkoille omia erityisiä tietoturvavaatimuksia. Langattomia verkkoja koskevat uhat voidaan jakaa kahteen pääkategoriaan; passiiviset ja aktiiviset uhat. (Vesanen 2003.)

Passiivisiin uhkiin kuuluvat liikenteen salakuuntelu ja liikenteen analysointi. Salakuuntelussa ulkopuolinen taho kuuntelee verkon liikennettä. Yleensä tarkoituksena on saada selville tietoa, jonka avulla voidaan tunkeutua verkkoon. Salakuuntelu on erittäin vaikea estettävä ja mahdoton havaita, joten siihen tulee varautua. Salakuuntelua voidaan estää tiedon salaamisella. Liikenteen analysoinnissa seurataan ainoastaan verkon liikennettä, ei viestien sisältöä. Myös analysointi voi tietyissä tapauksissa paljastaa luottamuksellista tietoa. (Vesanen 2003.)

Aktiivisia uhkia ovat siirtomedian häirintä tai katkaisu eli palvelunestohyökkäys, datan muokkaaminen ja tietojärjestelmään tunkeutuminen sekä väärennetyn tukiaseman perustaminen eli ns. välistävetohyökkäys. Tietojärjestelmään tunkeutumisesta puhutaan, kun ulkopuolinen taho onnistuu murtautumaan järjestelmään. WLANin ollessa usein kytkettynä langalliseen lähiverkkoon, murtautuja saattaa

päästä murtautumaan organisaation koko verkkoon. Ulkopuolinen taho voi periaatteessa myös tunkeutumatta verkkoon - muokata verkossa liikkuvaa dataa. Tämä voi tapahtua myös tahattomasti siirtovirheiden muodossa ja siihen on varauduttu tarkistussummien avulla jolloin tarkoituksellisen datan muokkauksen pitää aina muokata myös tarkistussummaa. (Vesanen 2003; Vähä-Touru 2007, 20.)

3.4 WLAN-tietoturvahyökkäykset

3.4.1 Hyökkäykset langattomiin lähiverkkoihin

Hyökkäykset langattomiin verkkoihin ovat samantyyppisiä kuin hyökkäykset langallisiin verkkoihin. Langattomuus aiheuttaa vain pieniä muutoksia hyökkäysmenetelmiin ja antaa hyökkääjälle uusia mahdollisuuksia. Vaikka langattomien verkkojen asennus onkin helppoa, verkon turvallisuuteen tulee panostaa enemmän kuin lankaverkoissa. Langattomat verkot ovat etenkin yrityksissä usein liitetty lankaverkkoon, tällöin mahdollisen hyökkäyksen tavoitteena saattaa olla tunkeutuminen lankaverkkoon ja sen jaettuihin resursseihin. Palvelimet ovat usein vahvasti suojattuja, mutta työasemien tietoturvapäivitykset, tietoturva-asetukset ja turvajärjestelyt saattavat olla huonosti hoidettuja. Yritys murtautua palvelimeen havaitaan yleensä helposti, mutta työasemaan tunkeutumista ei välttämättä huomata niin helposti. (Puska 2005, 69.)

Hyökkäykset tapahtuvat kolmea verkon perusominaisuutta, luottamuksellisuutta, eheyttä ja käytettävyyttä vastaan. Luottamuksellisuutta vastaan hyökättäessä pyritään kaappaamaan siirrettävää tietoa, selvittämään tunnistetietoja tai purkamaan salausavaimia, tavoitteena luottamuksellisen tiedon haltuun saaminen. Eheyttä vastaan hyökätään muuttamalla siirrettävää tietoa tai tietoja verkossa olevissa laitteissa. Käytettävyyttä vastaan hyökätään palvelunestohyökkäyksillä. (Ahvenainen 2003, 33.)

3.4.2 Langattoman verkon löytäminen

Langattoman verkon etsintä ei varsinaisesti ole hyökkäys langatonta verkkoa vastaan, mutta usein langattomaan verkkoon tunkeutuminen alkaa verkon paikallistamisella. Verkkojen etsintää kutsutaan yleisesti nimellä War Driving, nimitys tulee hakkeroinnin historiasta jatkeena War Dialingille. War Dialing oli modee-

miaikainen tapa etsiä satunnaisilla soitoilla modeemeja verkkoihin tunkeutumista varten. (Tuominen 2005, 27 - 28.)

Langattomia verkkoja voidaan paikallistaa erittäin helposti, tarvitaan vain langattomalla verkkokortilla varustettu kannettava tietokone. Esim. käyttöjärjestelmät Microsoft Windows XP ja Microsoft Windows Vista sisältävät langattomien verkkojen löytämiseen tarvittavia ohjelmistoja, joiden perusteella nähdään laitteen lähistöllä olevat langattomat verkot, joiden SSID:tä ei ole piilotettu. Internetistä löytyy lisäksi ilmaisia ohjelmia (esim. NetStumbler) joilla nähdään myös piilotetut SSID:t, sekä voidaan kerätä ja analysoida langattomien verkkojen lähettämiä tietoja. NetStumbler kertoo käyttäjälle tarvittavat tiedot verkon langattomista asetuksista. Ohjelma tukee myös GPS-laitteen käyttöä, joka helpottaa tulosten analysointia jälkikäteen. (Ahvenainen 2003, 33.)

3.4.3 Salakuuntelu

Salakuuntelulla tarkoitetaan verkossa kulkevan tiedon kaappaamista. Kerätystä tiedosta voidaan etsiä tunnistetietoja, verkkoinformaatiota sekä muuta hyökkääjää kiinnostavaa informaatiota. Salakuuntelu on myös osana monia muita hyökkäyksiä, jotka tarvitsevat kaapattua tietoa toteutukseensa. Salakuuntelun toteuttamiseen tarvitaan tietokoneen ja langattoman verkkokortin lisäksi kaappausohjelma eli haistelija (sniffer). Verkkokortille on vaatimuksena mahdollisuus asettaa se joko promiscuous- tai monitor-tilaan, jotta se kaappaisi myös muille laitteille tarkoitettua liikennettä. Normaalissa tilassa langaton verkkokortti hylkää muille kuuluvan liikenteen eikä käyttäjä pääse siihen käsiksi. Promiscuous-tilassa kortti assosioituu tukiaseman kanssa ja kaappaa sen jälkeen verkon liikennettä. Monitor-tilassa toimitaan täysin passiivisesti ilman assosioitumista. Haistelijat voivat kaapata kerrallaan kaiken yhdellä kanavalla siirtyvän liikenteen tai hyppiä kanavalta toiselle ja kaapata liikennettä kaikilta kanavilta, joilla sitä on. (Ahvenainen 2003, 36.)

Langattomia haistelijaohjelmia on saatavana ilmaiseksi Internetistä ja myös kaupallisia ratkaisuita on tarjolla (taulukko 2). Ilmaisia ohjelmia ovat esimerkiksi Kismet ja Ethereal. Näistä Kismet suorittaa vain tiedon kaappausta. Ethereal suorittaa tiedon kaappauksen ohella myös sen analysointia. WEP-salauksella voidaan vaikeuttaa salakuuntelua mutta sitä ei pystytä kokonaan estämään. Salatut paketit voidaan kaapata samoin kuin salaamattomatkin. Salattujen pakettien avaamiseen

tarvitaan salaukseen käytetty salausavain, joka saadaan murrettua esim. ilmaisella Aircrack-ng -ohjelmalla. Promiscuous-tilassa olevan haistelijan pystyy havaitsemaan seuraamalla tukiasemiin liittyneitä päätelaitteita. Passiivisen monitor-tilassa olevan haistelijan voi havaita tutkimalla laitteista lähtevää radiosäteilyä riittävän herkillä vastaanottimilla, sillä vastaanottotilassakin laitteista vuotaa säteilyä niin sanottuna lokaalivuotona ja suunta-antennin käyttö voi vahvistaa vuotavan säteilyn voimakkuutta merkittävästi. (Ahvenainen 2003, 36; MVnet 2007)

TAULUKKO 2. Langattoman verkon murtautumisohjelmia (Hämäläinen 2007, 38)

Ohjelma	Vaikeustaso	Aika*	Toimenpide
Kismet, Network Stumbler	Helppo!	Erittäin lyhyt	Piillotetun SSID:n määrittäminen
Kismet	Helppo!	Lyhyt	Verkon IP-alueen määrittäminen
Kismet, Network Stumbler	Helppo!	Erittäin lyhyt	Valmistajan ja mallin tunnistus
Kismet, Ethereal	Helppo!	Lyhyt	TCP dumbing (pakettien purkaminen/analysointi)
Kismet, Airsnort, Airodump, Aircrack, airreplay, Airodump-ng	Helppo!	Lyhyt	WEP-salauksen purkaminen
Airodump-ng, Aircrack, Kismet	Keskivaikea!	Keskipitkä	WPA \ TKIP -salauksen purkaminen
Airodump-ng	Vaikea!	Pitkä	WPA2-salauksen purkaminen
coWPAtty+Kismet	Vaikea!	Pitkä	WPA-PSK-salauksen purkaminen
???	Erittäin vaikea!	???	WPA-RADIUS-salauksen purkaminen
???	Erittäin vaikea!	???	AES

*Murtamiseen tarvittava aika riippuu yleensä käyttäjä- ja liikennemäärästä

3.4.4 Luvaton päätelaite

Löytynyttä langatonta verkkoa voidaan hyödyntää kytkemällä luvaton päätelaite (Roque Adapter) verkkoon. Usein verkkoon kytkeytymisen tavoitteena on ilmaisen internet-yhteyden hyödyntäminen tai tiedon etsiminen verkon sisältä. Mikäli verkkoa ei ole suojattu millään salausmenetelmällä ja verkon tukiasema mainostaa verkon SSID:tä, verkkoon päästään kytkeytymään yksinkertaisesti valitsemalla mainostetun verkon nimi tunkeutumiseen käytettävän työaseman langattomien verkkojen luettelosta. (Hämäläinen 2007, 46.)

Mikäli verkossa käytetään suojausmenetelmiä, tarvitaan verkkoon liittymistä varten verkon SSID, verkon IP-osoite ja mikäli verkossa on käytössä jokin salausmenetelmä, esim. WEP tai WPA, tarvitaan lisäksi salausavain. Edellä mainitut SSID

ja IP-osoite selviävät helposti esim. NetStumbler ohjelmalla, jolla voidaan myös selvittää verkossa olevia luvallisia MAC-osoitteita, mikäli MAC-suodatus on kytketty tukiasemassa päälle. WEP-salauksen ollessa päällä tarvitaan käytetyn salausavaimen murtamiseen esim. internetistä löytyvää Kismet ohjelmaa. Verkkoon liittymistä voidaan vaikeuttaa kytkemällä majakkatoiminto ja DHCP-palvelin pois päältä sekä ottamalla MAC-suodatus ja vähintään WEP-salaus käyttöön. Nämä keinot eivät kuitenkaan ole riittäviä takaamaan verkon turvallisuutta kehittyneiden murtamisohjelmien takia. (Ahvenainen 2003, 34; Thomas 2005, 313.)

3.4.5 MAC-osoitteen väärentäminen

MAC-osoitteen väärentäminen (MAC address spoofing) tarkoittaa verkkokortille valmistajan asettaman MAC-osoitteen muuttamista. Osoitteen muuttamista voidaan käyttää hyväksi monissa eri hyökkäystavoissa, kuten verkkoon kytkeytymisessä ja Man-in-the-Middle-hyökkäyksissä. Osoitteen väärentäminen onnistuu helposti useilla WLAN-tuotteilla. (Hämäläinen 2007, 42.)

MAC-osoitteen vaihtamisella voidaan pyrkiä verkon valvonnasta vastaavien hyökkäystentunnistusohjelmien harhauttamiseen tai tukiasemalle asetettujen pääsynhallintalistojen ohittamiseen. Hyökkäyksentunnistusohjelmat (NIDS, Network Intrusion Detection System) valvovat usein verkkoa MAC-osoitteiden perusteella ja tutkimalla yksittäisistä osoitteista tapahtuvaa liikennöintiä. Vaihtamalla MAC-osoitetta säännöllisesti hyökkääjä voi toteuttaa hyökkäyksiä valvonnan sitä huomaamatta. Verkkoon pääsyä voidaan rajoittaa MAC-osoitteiden perusteella sallimalla pääsy vain tietyille osoitteille. Hyökkääjä voi helposti verkon liikennettä seuraamalla selvittää sallittuja osoitteita ja sen jälkeen päästä verkkoon väärentämällä oman osoitteensa. (Ahvenainen 2003, 35.)

3.4.6 Kielletty tukiasema ja Man-in-the-Middle-hyökkäykset

Kielletyllä tukiasemalla (Roque Access Point) voidaan tarkoittaa kahta asiaa. Kyseessä voi olla luvallisen käyttäjän luvaton tukiasema, joka voi huonosti asennettuna muodostaa aukon koko verkon turvallisuuteen. Tämä tapahtuu yleensä työntekijän toimesta, joka haluaa langattoman verkon käyttöönsä, eikä ole saanut sitä syystä tai toisesta yritykseltä. Toinen ja yleisempi kielletyn tukiaseman käyttö keskittyy julkisiin WLAN-verkkoihin krakkereiden toimesta. Valetukiaseman teh-

tävänä on kerätä tietoa, kuten salasanoja, käyttäjänimiä, luottokortin numeroita ja mitä tahansa mistä voi olla hyötyä. Julkisten WLAN-verkkojen yleistyessä valetukiasemien käytöstä on muodostumassa vakava tietoturvallisuusuhka. (Hämäläinen 2007, 40.)

Valetukiaseman tarkoituksena voi olla myös palvelunestohyökkäyksen tai Man-in-the-Middle-hyökkäyksen (MitM) tekeminen. Päätelaitteet assosioituvat vain vahvimman tukiaseman kanssa. Käyttäjä voi yleensä määritellä vain verkon nimen, jonka jälkeen verkkokortti valitsee vahvimman signaalin omaavan yhteyden. Asettamalla suurella lähtöteholla ja suunta-antenneilla varustetun valetukiaseman oikeaan paikkaan voi hyökkääjä saada ainakin osan verkon päätelaitteista kadottamaan toimivan verkkoyhteytensä. Hyökkäykseen tarvittavan verkkoinformaation voi helposti selvittää haistelijan avulla. Man-in-the-Middle-hyökkäyksessä valetukiasemaa voidaan käyttää lähetettävän tiedon kaappaamiseen ja muuttamiseen. Hyökkääjä saa käyttäjät assosioitumaan omaan laitteeseensa ja kaappaa kaiken lähtevän liikenteen. Halutessaan hyökkääjä voi muokata kaappaamaansa tietoa ja lähettää sen edelleen alkuperäiseen kohdeosoitteeseen. Man-in-the-Middle-hyökkäystä voidaan vaikeuttaa käyttämällä vahvempia todentamismenetelmiä langattoman lähiverkon perusratkaisuna tarjottavien yhdensuuntaisten todennusmenetelmien sijaan. Vihamielisten tukiasemien havaitsemista varten on myös olemassa ohjelmia, kuten AirMagnet. Edellä esitettyjä hyökkääjien käyttämiä verkonhavaitsemisohjelmia voidaan käyttää myös vihamielisiä laitteita etsittäessä. (Ahvenainen 2003, 40.)

MitM-hyökkäyksissä voidaan käyttää menetelminä ARP- myrkyttämistä (Address Resolution Protocol Poisoning) tai huonosti suojatuissa verkoissa yksisuuntaisen todentamisen luomaa tietoturva-aukkoa. ARP-protokollaa käytetään selvittämään verkkolaitteiden fyysistä eli MAC-osoitetta. Ohjelmat käyttävät IP-osoitetta kohteen selvittämiseksi, mutta verkkokorttien on käytettävä ARP-protokollaa löytääkseen sitä vastaavan MAC-osoitteen. Tämä tapahtuu yleislähettämällä ARP-pyyntöpaketti, joka sisältää kohdeverkkokortin IP-osoitteen. Kaikki samassa verkossa olevat laitteet saavat pyynnön ja IP-osoitetta vastaava laite lähettää vastauksena ARP-paketin, joka sisältää sen MAC- ja IP-osoitteen. Lähettävä laite lisää nyt vastauksen mukana saadun MAC-osoitteen lähetettävien kehyksien kohdeosoitteeksi. Lisäksi laite tallentaa MAC- ja IP-osoitteen ARP-taulukkoon määräajaksi. Hyökkääjän verkkoon kytkemä laite voi lähettää kysyjälle valheellisen

ARP-vastauksen, jonka avulla laite saadaan lähettämään data hyökkääjän koneelle. Kyseinen tietoturva-aukko voidaan korjata käyttämällä SARP (Secure Address Resolution Protocol) -protokollaa, joka tarjoaa suojatun tunnelin jokaisen työaseman ja tukiaseman välille. ARP-myrkytyshyökkäyksen toteuttaminen langattomasta verkosta käsin on mahdollista suorittaa siis myös lankaverkossa oleville laitteille, jos tukiasema toimii siltana. (Ahvenainen 2003, 41, Hämäläinen 2007, 42.)

ARP-myrkyttämiseen ja MitM-hyökkäyksien toteuttamiseen löytyy valmiita ohjelmia. Dsniff, Ettercap ja AirJack ovat työkaluja, jotka osaavat hyökätä muun muassa SSH-yhteyksiä ja WEB-yhteyksiä vastaan. MitM-hyökkäys on mahdollista toteuttaa myös VPN-yhteyksiä vastaan. ARP-myrkyttämistä voidaan torjua sijoittamalla palomuuri langattoman verkon ja lankaverkon väliin. Tämä rajoittaa hyökkäykset langattomien laitteiden välille. Langattoman yhteyden suojaamiseksi voidaan käyttää myös vahvoja salausalgoritmeja suojaamaan siirrettävää tietoa. (Ahvenainen 2003, 42.)

3.4.7 Palvelunestohyökkäykset (DoS)

Langattomissa verkoissa toteutettu DoS-hyökkäys (Denial of Service) voi olla radioaaltojen häirintää, joka voi pahimmassa tapauksessa lamauttaa koko yrityksen langattoman verkon. Häirintä voidaan toteuttaa tehokkailla, fyysisesti lähelle häirittävää verkkoa sijoitettavilla radiolähettimillä, joilla luodaan niin paljon häiriötä langattoman verkon taajuusalueelle, että datan liikkuminen hidastuu merkittävästi tai lakkaa kokonaan datatörmäysten seurauksena. DoS-hyökkäykset tapahtuvat fyysisellä, siirtoyhteys- ja verkkotasoilla. Sovellus- ja kuljetustason hyökkäykset ovat samankaltaisia kuin lankaverkoissakin, palvelin saadaan lamautettua generoimalla liikaa pyyntöjä, niin ettei palvelin ehdi niitä käsitellä. TCP-protokollan ominaisuuksiin kohdistuvalla SYN-hyökkäyksellä aiheutetaan palvelimelle tai päätelaitteelle TCP-yhteyspyyntöjä, jotka johtavat sen puskureissa ylivuotoon ja kaikkien yhteyksien katkeamiseen. Kaistan ruuhkauttaminen puolestaan estää käyttäjiltä normaalin verkon käytön. Ruuhkauttaminen voidaan toteuttaa esim. IP-osoitteen väärentämiseen ja ICMP-pyyntöjen (Internet Control Message Protocol) lähettämiseen perustuvalla hajautetulla smurf-hyökkäyksellä. Langattomissa verkoissa käytettävää kaistaa on suhteellisen vähän, joten tämänkaltai-

set hyökkäykset ovat helppoja toteuttaa. (Ahvenainen 2003, 42 - 43; Hämäläinen 2007, 39 - 40.)

Jos hyökkäys tapahtuu monesta eri kohteesta samanaikaisesti, niin sitä kutsutaan DDoS-hyökkäykseksi (Distributed Denial of Service, hajautettu palvelunesto-hyökkäys). DDoS on erityisesti lankaverkoissa yleisempi hyökkäysmuoto kuin DoS. Radiotaajuuksia voidaan häiritä myös tahattomasti, sillä monet laitteet käyttävät samaa taajuutta kuin WLAN-tukiasemat. Laitteita, jotka operoivat 2,4 GHz:n taajuudella, ovat esimerkiksi mikroaaltouunit ja bluetooth-laitteet. Häirinnän estämisen toimenpiteitä voivat olla radiokanavien vaihtaminen tai häiriön lähteen löytäminen. Häiriön paikallistamiseen voidaan käyttää verkkoanalysaattoria. (Tuominen 2005, 26 - 27; Hämäläinen 2007, 39.)

DoS-hyökkäysten toteuttamiseen voidaan käyttää samoja ohjelmia kuin ARP-myrkyttämiseen ja MitM-hyökkäyksien toteutamiseenkiin. Todentamiseen ja assosiointiin liittyvien hyökkäyksien toteuttamiseen on olemassa Void11-ohjelma. DoS-hyökkäyksiä vastaan suojautuminen on hankalaa, koska suurin osa niistä perustuu protokollien normaaliin toimintaan. Osa hyökkäyksistä voidaan torjua ottamalla käyttöön kehittyneempiä todennusmenetelmiä ja staattisia verkkoasetuksia. (Ahvenainen 2003, 45.)

3.4.8 Hyökkäykset WEP-ratkaisuja vastaan

WEP-salauksen murtaminen kotikonstein on nykykoneilla hyvin helppoa. Parhaimmillaan WEP-salaus murtuu muutamissa minuuteissa käyttäen pakettien kaappaukseen ja salauksen murtamiseen suunniteltuja ohjelmistoja kuten Aircrack-ng-ohjelmistoa. Salausavaimen pituus vaikuttaa oleellisesti salauksen murtamisaikaan, mitä pidempää salausavainta käytetään, sitä hitaampaa on salauksen murtaminen. (MVnet 2007.)

Salaisen avaimen purkamiseen on olemassa kolmenlaisia hyökkäyksiä: sanakirjahyökkäys, voimahyökkäys ja tilastollinen hyökkäys. Sanakirjahyökkäys käyttää hyväkseen valmiita sanalistoja, joilla yritetään arvata oikeaa salasanaa. Useiden valmistajien langattomien lähiverkojen laitteet mahdollistavat salasanojen muodostamisen käyttäjän antaman fraasin perusteella sen sijaan että salasanat pitäisi kirjoittaa manuaalisesti. Tämä helpottaa sanakirjahyökkäyksen käyttämistä, jos käyttäjien määrittelemät fraasit eivät ole tehokkaasti valittuja. Tilastollisen hyök-

käyksen mahdollistavat alustusvektorien lähettäminen salaamattomana sekä niiden luonnista löytyneet heikkoudet. Voimahyökkäys ja sanakirjahyökkäys perustuvat oikean salasanan arvaamiseen ja oikean arvauksen verifiointiin kaapattujen pakettien avulla. Tilastollinen hyökkäys sen sijaan ratkaisee salasanan tavu kerrallaan. (Ahvenainen 2003, 37 - 38.)

3.4.9 Hyökkäykset WPA- ja 802.1X-ratkaisuja vastaan

WPA:n huonona puolena pidetään sen tapaa suojautua DDoS-hyökkäyksiltä. Kun palvelunestohyökkäys havaitaan, WPA sulkee koko verkon minuutiksi. Tällöin kaikki, myös verkon lailliset käyttäjät jäävät ilman verkkoa. WPA:sta on löydetty myös tietoturva-aukko, jota hyökkäystyökalu WPA Cracker käyttää hyväkseen. Tämä tietoturva-aukko muodostuu, kun langattomat tukiasemat lähettävät salausavaimeen liittyviä tietoja. Tietoturva-aukko ei uhkaa yritysratkaisuja, joissa on käytössä 802.1X-standardin mukainen autentikointi. WPA-salausmenetelmässä pitäisi pyrkiä käyttämään yli 20-merkkisiä salasanoja. (Tuominen 2005, 26.)

Heikoimpia EAP-toteutuksia vastaan voidaan suorittaa yhteyden kaappaus ja Man-in-the-Middle-hyökkäyksiä. Hyökkäykset mahdollistaa viestien aitouden tarkastamisen ja tilakoneiden synkronoimisen puute IEEE 802.1X ja IEEE 802.11–standardeissa. EAP-MD5 ja EAP-TLS-versioita vastaan voidaan suorittaa MitM-hyökkäys tekeytymällä tukiasemaksi ja lähettämällä EAP-success paketti päätelaitteelle. Tällöin päätelaite siirtyy todennettuun tilaan alkuperäisestä tilastaan riippumatta ja lähettää kaiken liikenteensä suoraan hyökkääjälle. Yhteyden kaappaus voidaan toteuttaa käyttäjän todennettua itsensä normaalisti, jonka jälkeen hyökkääjä lähettää hänelle MAC-disassociate-viestin. Käyttäjä menettää näin yhteytensä todennusjärjestelmän säilyessä edelleen todennetussa tilassa. Näin hyökkääjä voi käyttää yhteyttä ottamalla itselleen käyttäjän MAC-osoitteen. Tällainen hyökkäys vaatii salausavaimen tuntemista tai salauksen puuttumista verkosta. Salauksen ja dynaamisten avainten käyttäminen sekä kehittyneempien EAP-versioiden käyttäminen ehkäisee tällaisia hyökkäyksiä, mutta palvelunestomielessä hyökkäyksiä on edelleen mahdollista toteuttaa. (Ahvenainen 2003, 45.)

Langattomien tietoverkkojen tietoturvavaatimukset verrattuna langallisten verkkojen vaatimuksiin ovat haastavia. Radioaallot tiedonsiirrossa antavat omat vaatimuksensa tietoturvalle. Langattomia verkkoja uhkaavat passiiviset ja aktiiviset

uhat. Passiiviset uhat, salakuuntelu ja liikenteen analysointi ovat usein lähtökohtia aktiivisten uhkien toteuttamiselle. Passiivisia uhkia on erittäin vaikea, jos ei täysin mahdoton havaita. Aktiiviset uhat ovat yrityksen kannalta vaarallisempia ja mahdollisesti kohtalokkaampia. Aktiivisiin uhkiin lasketaan kaikki tiedonsiirron häirinnästä aina järjestelmään tunkeutumiseen.

Passiivisiin ja aktiivisiin uhkiin voidaan varautua monin, usein helpostikin toteutettavin tavoin. Tukiaseman SSID mainosten lähetysten estäminen, tehokkaiden salausmenetelmien käyttö, laiteohjelmistojen päivittäminen ja työasemakohtaisten palomuurien käyttö, langattomien laitteiden sijoittaminen palomuurien ulkopuolelle ja VPN:n käyttö, fyysisesti suojatut tukiasemat joiden radiotehoa on rajoitettu sekä tukiasemien ja muiden lokien aktiivinen tarkkailu ovat kaikki varteenotettavia menetelmiä langattomien verkkojen tietoturvan parantamiseksi, puhumattakaan verkon käyttäjien valistamisesta tietoturvalliseen toimintaan.

4 WINDOWS SERVER 2008 TIETOTURVAOMINAISUUDET

4.1 Network Policy Server ja Network Access Protection

Maaliskuussa 2008 julkaistu Microsoft Windows Server 2008 sisältää monia tietoturvaan liittyviä uudistuksia verrattuna Windows Server 2003 -palvelinkäyttöjärjestelmään. Tässä opinnäytetyössä keskitytään Windows Server 2008 palvelimen NPS-rooliin (Network Policy Server) ja NAP-toimintoon (Network Access Protection). Microsoft Windows Server 2008 802.1X NAP-järjestelmässä NPS kommunikoi 802.1X-yhteensopivan langattoman tukiaseman kanssa käyttäen RADIUS-protokollaa. Näillä palveluilla NPS-teknologia korvaa Windows Server 2003 -järjestelmässä toimivan Internet Authentication Servicen (IAS). (Microsoft Technet 2008.)

Network Policy -palvelin (Network Policy Server, NPS) toimii järjestelmän keskitettynä autentikoinnin, authorisoinnin ja tilastoinnin mahdollistavana RADIUS-palvelimena. RADIUS-viestit mahdollistavat autentikoinnin, authorisoinnin ja verkon tilastoinnin seuraavalla tavalla:

1. Asiakaslaite lähettää EAP-aloitusviestin langattomalle tukiasemalle (RADIUS-asiakkaalle).
2. Tukiasema vastaa EAP-viestillä, joka sisältää pyynnön asiakkaan identiteetistä.
3. Asiakaslaite vastaa EAP-paketilla, joka sisältää identiteetin. Tukiasema välittää viestin todennuspalvelimena toimivalle NPS-palvelimelle.
4. NPS-palvelin käsittelee Access-Request-viestin.
5. Tarvittaessa NPS-palvelin lähettää Access-Challenge-viestin tukiasemalle. Tukiasema käsittelee viestin ja lähettää käsitellyn Access-Request-viestin takaisin NPS-palvelimelle.
6. Yhteyspyynnön lähettäneen käyttäjän käyttäjätiedot ja oikeudet kirjautua langattomasti järjestelmään tarkistetaan AD-palvelimelta.
7. Yhteyspyyntö authorisoidaan sekä käyttäjätietojen, kirjautumisoikeuksien ja verkkokäytäntöjen mukaan.
8. Jos yhteyspyyntö on sekä autentikoitu ja authorisoitu, NPS-palvelin lähettää Access-Accept-viestin tukisemalle. Muussa tapauksessa NPS-palvelin lähettää tukiasemalle Access-Reject-viestin.

9. Tukiasema päättää yhteydenmuodostusprosessin asiakaslaitteen kanssa ja lähettää NPS-palvelimelle Accounting-Request-viestin yhteyden tilastointia varten.
10. NPS palvelin lähettää Accounting-Response-viestin tukiasemalle.

Tukiasema lähettää NPS-palvelimelle Accounting Request-viestin aina kun yhteys muodostetaan tai lopetetaan. (Microsoft Technet 2008.)

Network Access Protection (NAP) on tietokoneen kuntokäytännön (Health Policy) käyttöönottotekniikka, jonka avulla määritellään keskitetysti, mitkä työasemat ovat riittävän turvallisia pääsemään yrityksen verkkoon. Verkkokäytännöt määrittelevät asiakkaat joko sopiviksi (Compliant) tai epäsopiviksi (Noncompliant) verkon käyttäjiksi. Työasemat, jotka eivät autentikoinnin yhteydessä täytä kuntovaatimuksia, voidaan eristää (Quarantine) verkosta, kunnes kuntovaatimukset ovat täyttyneet. NAP:lla voidaan muun muassa selvittää, onko tuoreimmat ohjelmisto- ja tietoturvapäivitykset asennettu tai ovatko palomuuri ja virustorjunta päällä. Jos koneen asetukset eivät vastaa tietoturvavaatimuksia, pääsy verkkoon estetään tilapäisesti. Tilanne voidaan määritellä korjattavaksi automaattisesti tai käyttäjä voi korjata puuttuvat tietoturvaominaisuudet manuaalisesti, jonka jälkeen käyttäjä päästetään verkkoon. (Microsoft Technet 2008.)

4.2 802.1X-pakottaminen (Enforcement)

NAP-pakottaminen mahdollistaa kontrollin kaikille verkkoon 802.1X-yhteensopivien laitteiden kautta liittyville päätelaitteille, joissa on otettu käyttöön Network Access Protection Agent -palvelu ja EAP-karanteenin pakotusasiakas toiminto (EAP Quarantine Enforcement Client). 802.1X-laitteina voivat toimia kytkimet tai langattomat tukiasemat. (Microsoft Technet 2008.)

Verkkoon sopiviksi määritellyt päätelaitteet saavat täydet oikeudet verkon käyttöön. Verkkoon epäsopivien päätelaitteiden verkkoon pääsyä rajoitetaan IP-suodattimilla tai tunnelimäärityksillä, jotka lähetetään RADIUS-asiakkaalle (tukiasema tai ethernet-kytkin). IP-suodattimilla tehtävä verkon rajoittaminen tarkoittaa esimerkiksi pääsyn rajoittamista vain verkon oletusyhdyskäytävälle, jonka kautta kuntovaatimusten vastainen laite voi hakea tarvitsemansa tietoturvaohjelmiston päivityksen internetistä. Tunnelimäärityksillä voidaan eristää järjestelmän määritysten mukaan epäsopivat työasemat ohjaamalla ne eri VLAN:hin, jolloin ne

eivät voi kommunikoida verkon muiden työasemien kanssa. (Microsoft Technet 2008.)

802.1X-pakottaminen vertaa työaseman asetuksia verkon vaatimuksiin aina kun työasema yrittää autentikoitua järjestelmään. Lisäksi 802.1X-pakottaminen aktiivisesti monitoroi asiakaslaitteiden kuntotilaa ja rajoittaa automaattisesti verkon käyttöä niiltä työasemilta, jotka eivät ole järjestelmän vaatimusten mukaisia. (Microsoft Technet 2008.)

802.1X-autentikointiprosessin kuvauksessa kuvataan kuinka pakottaminen toimii:

1. Asiakaslaite ja langaton tukiasema aloittavat 802.1X-autentikointiprosessin.
2. Työasema lähettää käyttäjätietonsa ja salasanansa autentikointipalvelimena toimivalle NAP-kuntokäytäntö -palvelimelle (Health policy).
3. Jos käyttäjätiedot eivät täsmää toimialueen ohjauspalvelimen käyttäjätietojen kanssa yhteysyritys katkaistaan.
4. Jos käyttäjätiedot ovat oikeat, NAP-kuntokäytäntö -palvelin pyytää selvitystä työaseman kuntotilasta.
5. Työasema lähettää selvityksen kuntotilastaan NAP-kuntokäytäntö -palvelimelle.
6. NAP-kuntokäytäntö -palvelin käsittelee kuntotilaselvityksen ja päättää onko työasema sopiva ja lähettää päätöksestä tiedon työasemalle ja tukiasemalle. Jos työasema on epäsopiva, lähettää palvelin ohjeistuksen tukiasemalle työaseman verkon rajoittamisesta sekä ohjeen työasemalle toimenpiteistä työaseman kuntotilan korjaamiseksi.
7. Jos työasema on sopiva, tukiasema päättää 802.1X-autentikoinnin ja työasemalle myönnetään rajoittamaton verkon käyttö.
8. Jos työasema on epäsopiva, tukiasema päättää autentikointiprosessin ja rajoittaa verkon käyttöä.
9. Työasema lähettää päivityspyynnöt remediation-palvelimille.
10. Remediation-palvelimet mahdollistavat vaadittavien päivitysten saatavuuden ja työasema lataa päivitykset, jonka jälkeen työasema päivittää kuntotilaselvityksensä.
11. Työasema aloittaa 802.1X-autentikointiprosessin uudelleen ja lähettää päivitetyn selvityksen kuntotilastaan NAP-kuntokäytäntö -palvelimelle.

12. Mikäli vaadittavat muutokset työaseman kuntotilaan on saavutettu, NAP-kuntokäytäntö -palvelin päättää työaseman sopivaksi ja ohjaa tukiasemaa myöntämään työasemalle rajoittamattoman verkon käytön ja lähettää tiedon päätöksestä myös työasemalle.
13. Tukiasema päättää autentikoinnin ja työasemalle myönnetään rajoittamaton verkon käyttö. (Microsoft Technet 2008.)

4.3 RADIUS-asiakkaat (RADIUS Clients)

RADIUS-asiakkaiden päätehtävänä on yhteyspyyntöjen, autentikointiviestien ja tilastointiviestien välittäminen RADIUS-palvelimelle. RADIUS-asiakkaat voivat olla langattomia tukiasemia, 802.1X-yhteensopivia kytkimiä, VPN-palvelimia tai Dial-Up -palvelimia. Tässä opinnäytetyössä keskitytään RADIUS-asiakkaina toimiviin langattoman verkon tukiasemiin. (Microsoft Technet 2008.)

NPS:n asetuksissa määriteltävät RADIUS-asiakkaat käyttävät RADIUS-protokollaa kommunikoidessaan RADIUS-palvelimien kanssa. NPS-palvelimen konfiguroinnin yhteydessä määritellään tukiaseman nimi, IP-osoite tai DNS-nimi sekä Shared Secret, salasana, joka pitää olla yhtenäinen tukiasemaan konfiguroidun RADIUS Shared secret -salasanan kanssa. (Microsoft Technet 2008.)

4.4 Yhteyspyyntökäytännöt (Connection Request Policy, CRP)

Yhteyspyyntökäytännöillä määritellään RADIUS-asiakkaana tukiasema, jonka kautta autentikointipyynnöt välitetään NPS-palvelimelle ja tunnistuksessa käytettävä autentikointitapa. Valittu autentikointitapa voidaan määrittää ohittamaan myöhemmissä verkkokäytännöissä määriteltävät autentikoinitavat. RADIUS-asiakkaan tarkka määritys NPS-palvelimella lisää tietoturvaa, koska näin NPS-palvelin ei hyväksy määrittelemättömien tukiasemien yhteyspyyntöviestejä. (Microsoft Technet 2008.)

802.1X-suojattu yhteys käyttää salauksessaan WEP-salausta dynaamisesti vaihtuvilla avaimilla. Verkon todennusmenetelmänä käytetään EAP MS-CHAPv2:ta. Point-to-Point Protocol-autentikaatioprotokolliin (PPP) kuuluva MS-CHAP on Microsoftin versio Challenge-Handshake Authentication protokollasta (CHAP). MS-CHAP v2 on salasanaan perustuva haaste - vastaus -protokolla joka käyttää salausalgoritmina MD5:sta ja DES:iä. Palvelin, johon halutaan autentikoitua lä-

hettää haasteen yhteyttä yrittävälle laitteelle. Haaste tehdään molempiin suuntiin, eli myös autentikoiva laite lähettää oman haasteensa palvelimelle. Jos jompikumpi haasteista on väärä, yhteys evätään. CHAP-protokollassa käytetään neljää viestityyppiä, Challenge, Response, Success ja Failure . Käyttäjältä pyydetään käyttäjätunnusta ja käyttäjälle annetaan haaste Challenge-viestillä. Käyttäjä vastaa haasteeseen käyttäjätunnus-salasanaparista lasketun tarkistussumman sisältävällä Response-viestillä. Tarkistussumman täsmätessä tunnistusta pyytävä laite lähettää Success-viestin. Mikäli tarkistussumma ei täsmää, lähetetään käyttäjälle Failure-viesti. (Seppälä 2006.)

EAP MS-CHAPv2 vaatii palvelinsertifikaatin NPS-palvelimelta. Sertifikaatin avulla verkkoon kirjautuva työasema tunnistaa verkon johon se on kirjautumassa. Käytettävä autentikointimenetelmä ei kuitenkaan vaadi erillistä sertifikaattitunnistusta verkkoon kirjautuvalta työasemalta. NPS-palvelin käyttää varmenteen myöntäjänä (Certification authority) toimivan toimialuepalvelimen myöntämää tietokonesertifikaattia joka tallennetaan NPS -palvelimen sertifikaattisäilöön. Tietokonesertifikaatin manuaalisessa asennuksessa käytetään NPS-palvelimen Certificate Manageria. (Microsoft Technet 2008.)

Vaihtoehtoisena todennusmenetelmänä EAP MS-CHAPv2:n sijaan voidaan käyttää EAP-TLS:ää. Verrattuna EAP MS-CHAPv2 -todennusta käyttävään järjestelmään EAP-TLS:n käyttö vaatii tietokone- ja käyttäjäsertifikaattien käyttöä langattomassa työasemassa, muutoksia toimialueen oletuskäytännössä (Default Domain Policy), NPS-palvelimen yhteyspyyntökäytäntömäärityksissä ja työaseman verkkomäärityksissä. Toimialueen ohjauspalvelimelle (AD) luodaan ja otetaan käyttöön käyttäjäsertifikaatin mallipohja (Certificate Template) ja sertifikaattien myöntämisen automatisointi (Autoenrollment), jolloin ohjauspalvelin automaattisesti myöntää sertifikaatin kaikille sitä anoville toimialueen käyttäjille (Domain Users). Lisäksi otetaan käyttöön Group Policy Object Editoria käyttäen tietokonesertifikaattien luomisen automatisointi sekä käyttäjä- ja tietokonesertifikaattien myöntämisen automatisointi. NPS-palvelimen Connection Request Policyn määrityksessä käytettäväksi EAP-tyypiksi valitaan Smart Card or other Certificate. Asetus vaatii myös työasemalta saman EAP-tyypin käyttöönottoa langattoman verkon asetuksissa. (Microsoft Technet 2008.)

4.5 Kuntovaatimukset (System Health Validators, SHV) ja kuntokäytännöt (Health Policies)

NPS käyttää kuntovaatimuksia analysoimaan työaseman turvallisuustilaa. SHV:t liitetään kuntokäytäntöihin joiden perusteella järjestelmä tekee päätöksiä mahdollisista verkon rajoituksista. Työaseman kuntotila (Health Status) määritellään työaseman Network Access Protection Agent -palvelun System Health Agents (SHA) -komponentteja käyttämällä. SHA valvoo Windowsin tietoturvakeskuksen tilaa ja raportoi NAP Agent -palvelulle tietoturvakeskuksen ilmoitukset puutteellisesta turvallisuuden tilasta työasemassa. Windows Security Health Agent ja Windows Security Health Validator kuuluvat Windows Server 2008 ja Windows Vista -käyttöjärjestelmiin sekä Windows XP Service Pack 3 -järjestelmiin. (Microsoft Technet 2008.)

System Health Validator -kuntovaatimukset määritellään NPS-palvelimen NPS Microsoft Management Console (MMC) -konsolin Network Access Protection kohdassa. Kuntovaatimuksilla voidaan vaatia, että:

- Työasemissa on asennettu ja sallittu palomuurin käyttö
- Virustorjuntaohjelma on asennettu ja käytössä
- Virustorjuntaohjelmisto on päivitetty
- Haittaohjelmien poisto -ohjelma on asennettu ja käytössä
- Haittaohjelmien poisto -ohjelma on päivitetty
- Microsoft automaattiset päivityspalvelut (Update Services) on käytössä

Lisäksi, mikäli työaseman Windows Update Agent on rekisteröity palvelimen Windows Server Update Services (WSUS) -palveluun, NAP voi lisäksi tarkistaa, että saatavissa olevat päivitykset on asennettu työasemiin. (Microsoft Technet 2008.)

Määritellyt kuntovaatimukset liitetään NPS Microsoft Management Console (MMC) -konsolissa tehtäviin kuntokäytäntöihin, joissa määritellään yksinkertaisilla määrityksillä käytettävä kuntovaatimus ja tehtävät kuntovaatimustarkistukset (Client SHV checks). Yleisimmin käytettävinä vaihtoehtoina kuntovaatimustarkistuksille ovat Client passes all SHV checks (asiakas läpäisee kaikki kuntovaatimustarkistukset) jolloin asiakaslaite määritellään verkon vaatimusten kannalta sopivaksi ja Client fails one or more SHV checks (asiakas ei läpäise yhtä tai use-

ampaa kuntovaatimustarkistusta) jolloin asiakaslaite määritellään verkon vaatimusten kannalta epäsopivaksi ja sen verkon käyttöä rajoitetaan. Kuntokäytännöt puolestaan liitetään verkkokäytäntöihin seuraavassa luvussa esiteltävän esimerkin mukaan. (Microsoft Technet 2008.)

4.6 Verkkokäytännöt (Network Policies)

4.6.1 Verkkokäytännöt yleisesti

Verkkokäytännöt ovat määritelty sääntöjen kokoelma, joilla määritellään kuinka yhteysyrityksille joko määritellään valtuuksia (Authorisointi, Authorization) tai niitä rajataan (Constraints). Jokaiselle säännölle määritellään lupa yhteyden muodostamiseen tai kieltämiseen (Access Permission), täytettävät ehdot (Conditions), rajoitukset ja käytännön asetukset (Network Policy Settings). Jos yhteys on authorisoitu verkkokäytännön rajoitukset ja -asetukset voivat määrätä yhteydelle rajoituksia. Käytettäessa NAP:ia kuntokäytännöt lisätään verkkokäytäntöihin, jolloin työasemien kuntotila tarkistetaan authorisointiprosessin yhteydessä. (Microsoft Technet 2008.)

Tehdäkseen päätöksiä työasemien pääsystä verkkoon ja mahdollisista verkon rajoituksista NPS-palvelin käyttää verkkokäytäntöjä, jotka on konfiguroitu NPS Microsoft Management Console (MMC) -konsolissa. NPS tarkistaa authorisoinnin yhteydessä myös verkkoon kirjautumista yrittävän laitteen oikeudet kirjautua verkkoon langattoman tukiaseman kautta. Oikeudet tarkistetaan toimialueen ohjauspalvelimen käyttäjätietokannasta käyttäjän ja laitteen Dial-in ominaisuuksista, joissa määritellään onko kirjautujalla tarvittavat oikeudet. (Microsoft Technet 2008.)

Verkkokäytäntöjä voidaan ajatella erilaisina sääntöinä. Jokainen sääntö sisältää ehtoja ja asetuksia. NPS vertaa asetettuja ehtoja yhteyspyynnössä esitettäviin ominaisuuksiin. Jos ehdot ja ominaisuudet ovat yhtenevät verkkokäytäntöjen asetukset määrittelevät muodostettavan yhteyden. Jos NPS-palvelimelle on määritelty useampia verkkokäytäntöjä, katsotaan käytännöt järjestellyksi sääntöjen listaksi. NPS vertaa yhteyspyynnön ominaisuuksia ensin ensimmäiseksi määriteltyyn verkkokäytäntöön, sitten toiseen, kolmanteen jne. kunnes yhteneväisyys löytyy.

Yhteneväisyyden löytyessä kyseiseen verkkokäytäntöön konfiguroidut määritykset otetaan käyttöön. (Microsoft Technet 2008.)

Jokaisella verkkokäytännöllä on neljä ominaisuutta, yleisasetukset (Overview), ehdot (Conditions), rajaukset (Constraints) ja asetukset (Settings). Yleisasetuksissa määritellään onko verkkokäytäntö käytössä vai ei (Enabled/Disabled) ja myöntääkö vai kieltääkö käytäntö verkkoon pääsyn. Myös RADIUS-asiakkaan tyyppi ja verkkoyhteyden tyyppi voidaan määritellä yleisasetuksissa. (Microsoft Technet 2008.)

Verkkokäytännön ehdoissa määritellään ne ehdot, jotka yhteyspyynnön on täytettävä, jotta käytännön asetukset määrittelevät yhteyden tilan. Ehdoissa voidaan esimerkiksi määritellä verkkokäytäntö koskemaan vain jotain tiettyä toimialueen käyttäjäryhmää. Lisäämällä AD-palvelimella käyttäjiä määriteltyyn Domain-local -ryhmään voidaan helposti hallita käyttäjien oikeuksia ja rajoitteita verkon käyttöön. Käytettäessä NAP-ominaisuutta määritellään verkkokäytännön ehtona käytettäväksi erikseen määriteltäviä kuntokäytäntöjä. Jos halutaan esimerkiksi tehdä verkkokäytäntö verkon vaatimusten kannalta sopivaa asiakaslaitetta (laitetta, joka täyttää kaikki SHV tarkistukset) varten, määritellään kuntokäytäntö johon valitaan Client passes all SHV checks valinta ja otetaan se käyttöön verkkokäytännön ehdoissa. (Microsoft Technet 2008.)

Verkkokäytännöissä määriteltävät rajoitukset ovat vaihtoehtoisia lisämäärityksiä, jotka eivät ole pakollisia. Rajoituksilla voidaan evätä ne yhteyspyynnöt, jotka eivät täytä rajoituksissa määriteltyjä määrityksiä. Mikäli yhteyspyyntö ei täytä rajoituksen määrityksiä, yhteyspyyntö evätään. Rajoituksilla voidaan esimerkiksi rajata, että langaton kirjautuminen verkkoon sallitaan vain tiettynä kellonaikana (Day and time restrictions) tai määritellä tarkka yhteyden kestoaika (Session Timeout). Rajoitusten avulla voidaan hallita esimerkiksi kertakäyttöistä kirjautumista kertakäyttöisten käyttäjätunnus-salasanaparien avulla niin, että käyttäjän pääsy rajoitetaan internetiin puolen tunnin ajaksi. (Microsoft Technet 2008.)

Verkkokäytännön asetuksissa määritellään ne asetukset jotka NPS sallii niille yhteyspyynnöille jotka täyttävät kaikki verkkokäytännön ehdoissa määritellyt asetukset. Asetuksissa voidaan määritellä tukiasemalle lähetettäviä tunnelointimäärityksiä tai IP-suodattimia toimenpiteinä niitä asiakaslaitteita kohtaan jotka eivät täytä vaadittuja ehtoja. (Microsoft Technet 2008.)

4.6.2 NAP Access Permission- ja NAP-verkkokäytäntö -asetukset

Verkkokäytäntöjen konfiguroinnissa on tärkeää huomioida Access Permission asetusten Access granted/Access denied -valinta. Huolimatta siitä käytetäänkö NAP-kuntokäytäntöjä verkkokäytäntöjen ehdoissa, valitaan Access Permissions määrityksissä kohta Access granted, jolla hyväksytään asiakaslaitteen pääsy verkkoon. Näin mahdollistetaan myös kuntokäytäntöjen vastaisten asiakaslaitteiden pääsy verkkoon, mutta näiden laitteiden yhteyttä rajoitetaan NAP-verkkokäytäntö asetuksissa tehtävien määritelmien mukaisesti. Access denied -valinnalla voidaan tehdä ehdottomia ehtoja yhteyden kieltämisestä verkkokäytännön ehtojen mukaisesti esimerkiksi määrittelemällä ehdoissa ehdoton kielto jonkun käyttäjäryhmän kirjautumisesta langattoman tukiaseman kautta yrityksen verkkoon. (Microsoft Technet 2008.)

Verkkokäytäntöjen NAP-asetukset mahdollistavat lähiverkon palveluiden rajoittamisen verkkoon soveltumattomilta työasemilta kolmella eri tavalla:

- Allow full network access, mikäli yhteyspyyntö autentikoidaan ja authorisoidaan. Turvallisuus status merkitään logiin
- Allow limited access, niiden työasemien verkkoon pääsyä rajoitetaan, jotka eivät läpäise kuntovaatimuksia
- Allow full access for a limited time, työasemille annetaan täysi pääsy verkkoon tilapäiseksi ajaksi. (Microsoft Technet 2008.)

Automaattisen Remediation-toiminnon avulla rajoitettuun verkkoon siirretyt järjestelmän vaatimusten vastaiset työasemat voidaan määrätä päivittämään järjestelmänsä. Jos NAP-verkkokäytäntöasetukset on määritelty käyttämään automaattista Remediation-toimintoa SHA yrittää automaattisesti korjata työaseman tilan, esim. ottamaan käyttöön käytöstä poistetun Windowsin palomuurin. (Microsoft Technet 2008.)

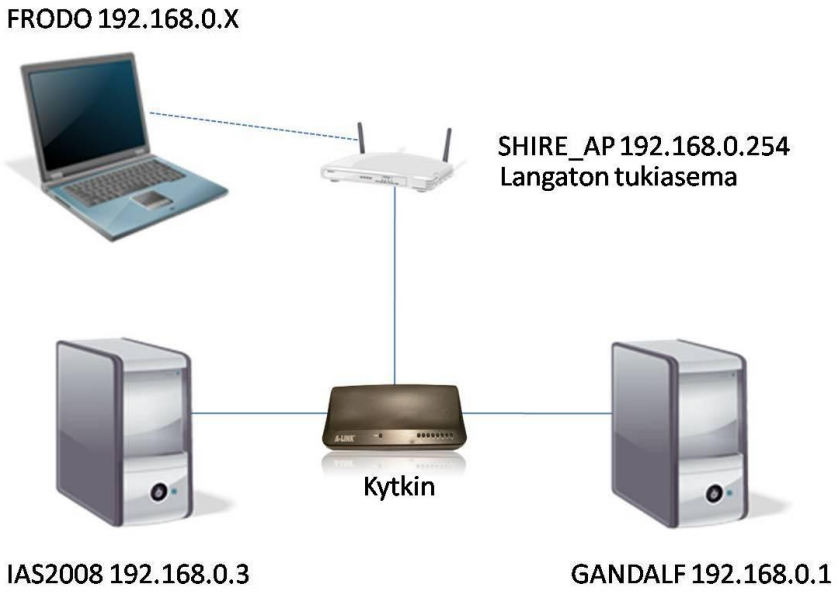
Asiakaslaitteille, joiden verkkoon pääsyä on rajoitettu, voidaan määritellä välityspalvelinryhmä (Remediation Server Group) tai URL-osoite ongelmanratkaisua varten (Troubleshooting URL). Välityspalvelinryhmä on listaus palvelimista, joille epäsopivilla asiakaslaitteilla on pääsy verkon rajoitusten mukaan. Välityspalvelimet voivat olla palvelimia, joita käytetään keskitetysti esimerkiksi järjestelmän päivitykseen tai vaihtoehtoisesti verkon oletusyhdyskäytävän IP-osoite, jolloin tarvittavat, puuttuvat päivitykset voidaan hakea internetistä. URL-osoite ongel-

manratkaisua varten aktivoituu kun käyttäjä klikkaa Troubleshoot-linkkiä epäsopiville asiakaslaitteille näytettävässä Network Access Protection -ikkunassa. WWW-sivulle tehdään ohjeistus miten käyttäjän tulee toimia saadakseen verkon täydet resurssit jälleen käyttöönsä. (Microsoft Technet 2008.)

5 KÄYTÄNNÖN TOTEUTUS

5.1 Toteutetun testiympäristön kuvaus

Työn käytännön toteutuksessa luodaan laboratorio-olosuhteissa testiympäristö, jossa voidaan tutkia Windows Server 2008 -verkon turvallisuuteen liittyviä uusia komponentteja. Testiympäristöön konfiguroidaan IEEE802.1X-autentikointia käyttävä kuvion 4 mukainen langaton verkkoympäristö. Testiympäristön IEEE802.1X-autentikointi käyttää PEAP-tyyppinä Microsoftin Challenge-Handshake Authentication protokollan versiota 2 (PEAP-MS-CHAP v2). Ympäristöön asennetaan kolme tietokonetta ja yksi langaton tukiasema. Yksi tietokoneista, anoja (Supplicant), on varustettu langattomalla verkkokortilla ja toimii testikoneena (FRODO). Yksi tietokone (GANDALF) toimii toimialuepalvelimena (Active Directory, AD) ja yksi Network Access Serverinä, autentikointipalvelimena (Authenticator) sekä RADIUS-palvelimena (IAS2008). Langaton tukiasema (Pass Through Authenticator) tukee RADIUS-tunnistusta ja 802.1X-autentikointia.



KUVIO 4. Testiympäristö

Kun testiympäristö on saatu konfiguroitua toimivaksi kokonaisuudeksi, järjestelmässä otetaan käyttöön ja testataan Microsoft Windows Server 2008 Network

Access Protection (NAP) ominaisuutta, 802.1X-autentikointia sekä tietoturvan lisäämistä vaatimalla asiakastyöasemilta tietoturvaan liittyvinä vaatimuksina palomuurin sekä automaattisten päivitysten käynnissä oloa.

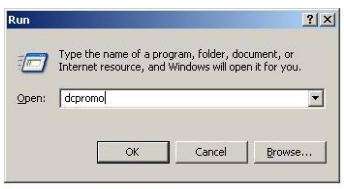
Tässä opinnäytetyössä NAP-pakottaminen toteutetaan NPS-palvelimella, 802.1X-yhteensopivalla langattomalla Cisco 1200-sarjan tukiasemalla ja Windows Server 2003 -toimialuepalvelimella. NAP-yhteensopivalla työasemalla (Windows Vista Ultimate) testataan erilaisia vaatimuksia joita määritellään NPS-palvelimen verkkokäytäntöihin ja turvallisuuskäytäntöihin käyttäen System Health Validatoreihin (SHV) määriteltyjä vaatimuksia. Vaihtoehtoina valitulle toteutukselle voidaan mainita Microsoft Windows Server 2003 Internet Authentication Service (IAS) ja Linux-ympäristössä toimiva FreeRADIUS-ohjelmisto.

5.2 Active Directoryn asennus

Työn aluksi toimialuepalvelimeksi asennettavaan tietokoneeseen asennetaan Windows Server 2003 Enterprise Edition -palvelinkäyttöjärjestelmä perusasetuksilla. Palvelimen IP-osoitteeksi määritellään valitusta 192.168.0.0/24verkosta osoite 192.168.0.1/24 ja palvelimen nimeksi annetaan GANDALF. IP-asetusten muuttamisen jälkeen palvelimen rooleiksi valitaan toimialuepalvelin (Active Directory, AD), DNS-palvelin, DHCP-palvelin ja Enterprise Root CA -palvelin shire.local-toimialueelle.

Roolien käyttöönoton jälkeen AD:lle lisätään testikäyttäjä (Bilbo) ja testissä käytettävä työasema (FRODO) sekä lisätään käyttäjäryhmä (WirelessUsers), johon testikäyttäjä ja työasema lisätään. Käyttäjäryhmän avulla hallitaan käyttäjiä joille on myönnetty oikeus kirjautua verkkoon langattomilla työasemilla.

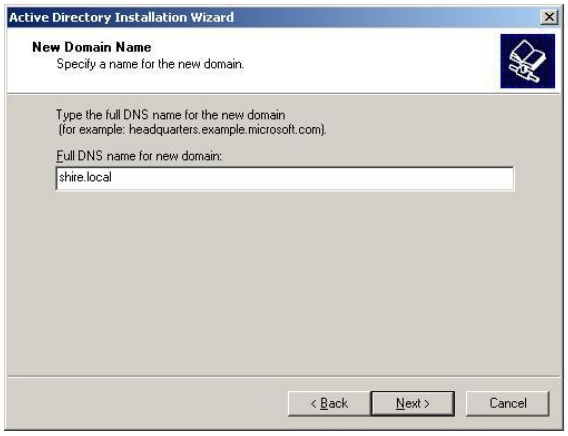
Toimialuepalvelimen asennus aloitetaan klikkaamalla Start, Run ja kirjoittamalla avautuvaan kenttään dcpromo (kuvio 5)



KUVIO 5. Toimialuepalvelimen asennuksen käynnistys

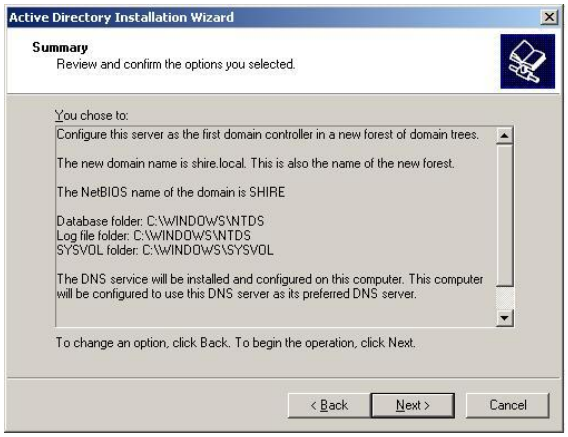
Asennuksen käynnistettyä valitaan avautuneesta ikkunasta valinta Domain Controller for new domain, jolloin määritellään asennettavaksi toimialueen ohjauskone uudelle toimialueelle sekä Domain in the new forest, jolla määritellään asennettavaksi toimialue uuteen metsään. Näiden määritysten jälkeen määritellään DNS-palvelun asennus ja konfigurointi asennettavaan palvelimeen.

Seuraavaksi määritellään uuden toimialueen nimeksi shire.local (kuvio 6) ja toimialueen NetBios-nimeksi SHIRE.



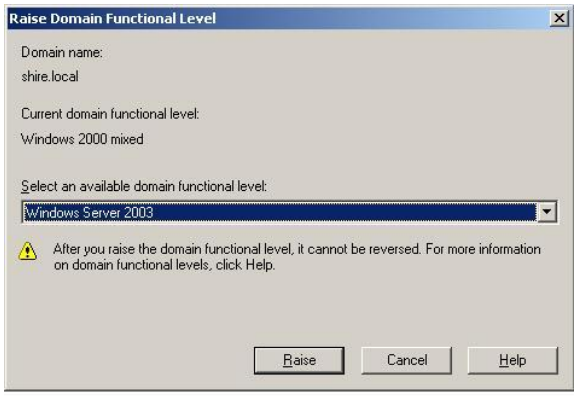
KUVIO 6. Domain name, toimialueen nimi

Asennuksen lopussa käytetään järjestelmän oletusasetuksia mm. toimialueen käyttäjätietokannan ja lokitiedostojen osalta (kuvio 7).



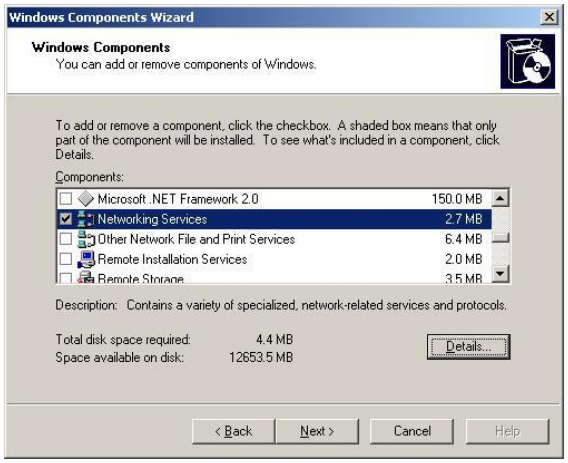
KUVIO 7. Yhteenveto toimialuepalvelimen asennuksesta

Toimialuepalvelimen asennuksen päätteeksi järjestelmä käynnistetään uudelleen, jonka jälkeen nostetaan toimialueen toiminnallinen tila asetukseen Windows Server 2003, avaamalla Active Directory Domains and Trusts -ohjelma Administrative Tools -valikosta ja klikkaamalla hiiren oikealla toimialueen ohjauspalvelinta gandalf.shire.local. Klikataan Raise Domain Functional Level ja valitaan Raise Domain Level -ikkunassa Windows Server 2003 (kuvio 8). Toiminnallisen tilan muutos mahdollistaa käyttäjien hallinnan ryhmien avulla.



KUVIO 8. Toimialueen toiminnallinen tila

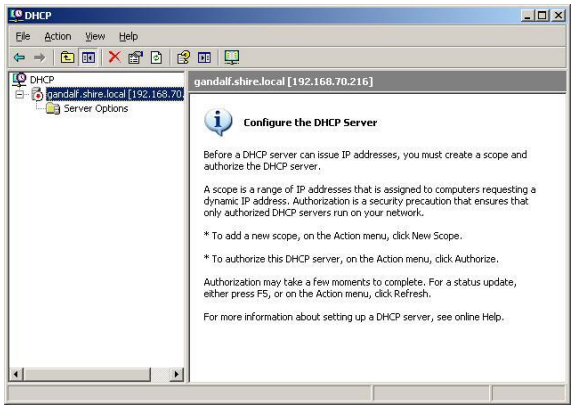
DHCP (Dynamic Host Configuration Protocol) asennetaan Networking Services -ryhmän kautta ohjauspaneelin lisää tai poista sovellus -toiminnolla (Add or Remove Programs) (kuvio 9).



KUVIO 9. DHCP:n asennus Networking Services ryhmän alta

DHCP-palvelun asennuksen jälkeen avataan DHCP-ikkuna (kuvio 10) Administrative Tools -valikosta ja authorisoidaan palvelu (Action -> Authorize). DHCP-palvelun konfigurointi aloitetaan klikkaamalla DHCP-palvelinta gan-

dalf.shire.local hiiren oikealla ja valitsemalla uuden alueen konfigurointi (New Scope).

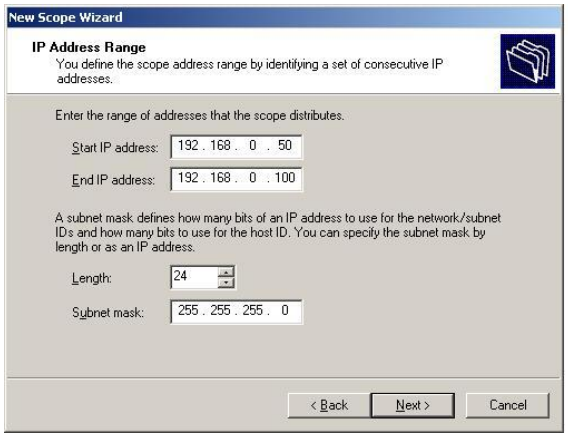


KUVIO 10. DHCP-asetukset

DHCP-alueen valinta aloitetaan määrittelemällä perustettavalle alueelle nimi ShireNet (kuvio 11).

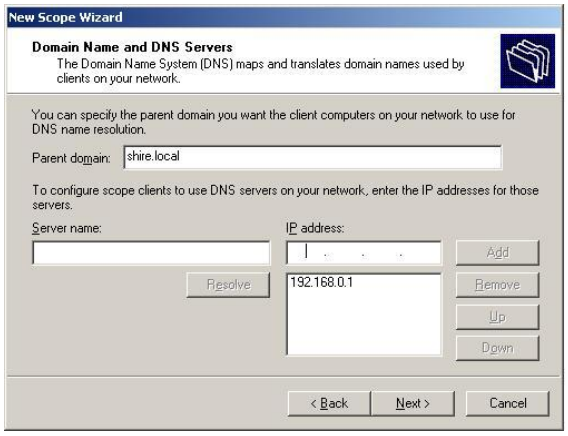
KUVIO 11. DHCP-alueen nimen valinta

Palvelun IP-osoitealueeksi valitaan alue 192.168.0.50-192.168.0.100 (kuvio 12).



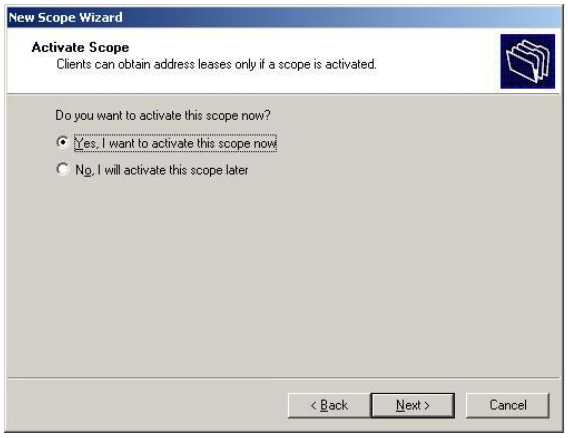
KUVIO 12. IP-osoitealueen määrittely

DHCP-asetuksiin määritellään lisäksi DNS-palvelun osoitteeksi palvelimen oma osoite 192.168.0.1, jolla välitetään tieto asiakaskoneille DNS-palvelimista (kuvio 13).



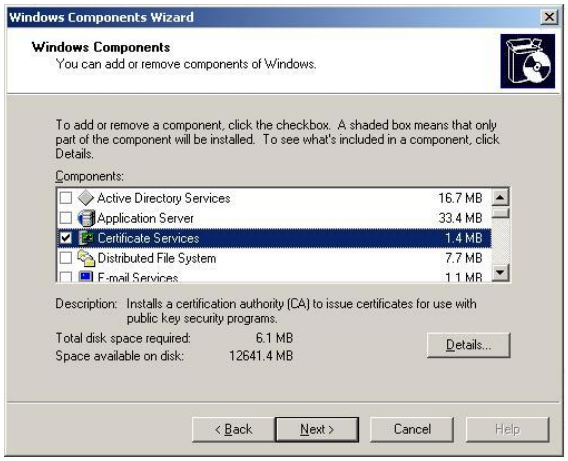
KUVIO 13. DNS-asetusten määrittely

DHCP:n asennuksen lopuksi luotu DHCP-alue aktivoidaan (kuvio 14).



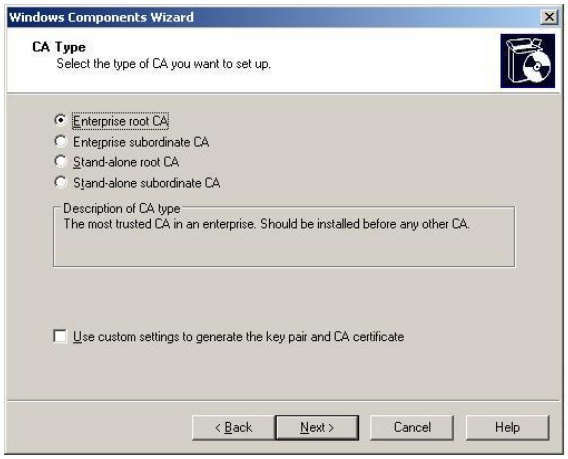
KUVIO 14. DHCP-palvelun aktivointi

Sertifikaattipalvelut asennetaan käynnistämällä ohjauspaneelin Lisää tai poista sovelluksista Lisää tai Poista Windowsin osia (Add/Remove Windows Components) valitsemalla Certificate Services ja klikkaamalla Next (kuvio 15).



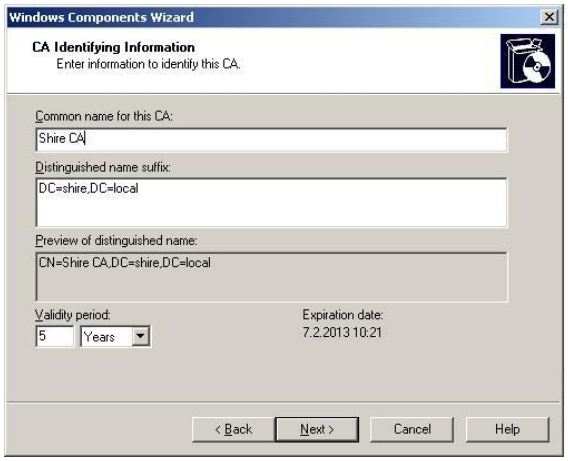
KUVIO 15. Sertifikaattipalvelujen asennuksen aloitus

CA Type-ikkunassa valitaan kuvion 16 mukaisesti Enterprise root CA



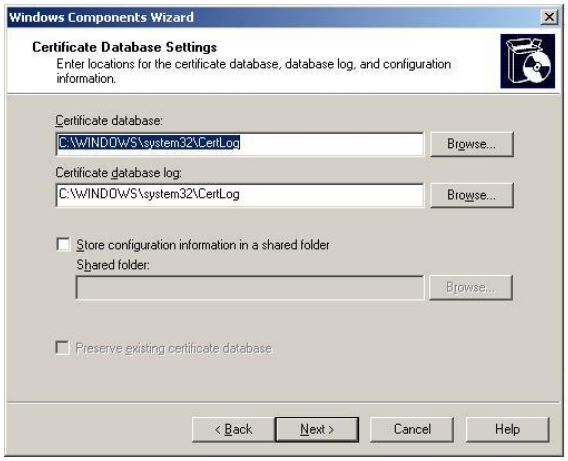
KUVIO 16. CA-palvelimen valinta

Sertifikaattipalvelimen nimeksi annetaan CA Identifying Information -ikkunassa SHIRE CA (kuvio 17).



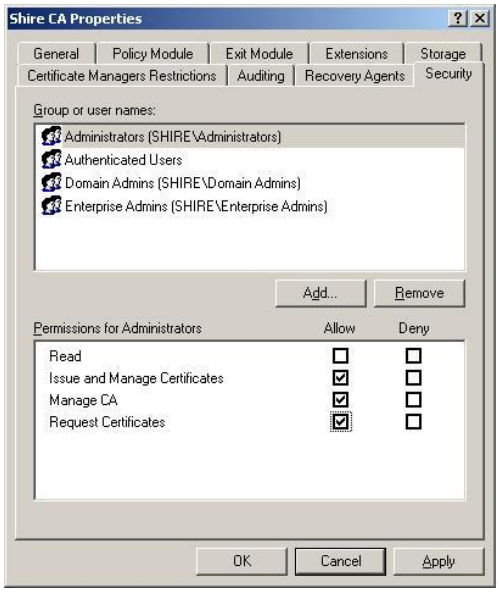
KUVIO 17. CA Identifying Information -nimen valinta

Certificate Database Settings -asetukset hyväksytään oletusarvoilla (kuvio 18).



KUVIO 18. Sertifikaattisäilön määrittely

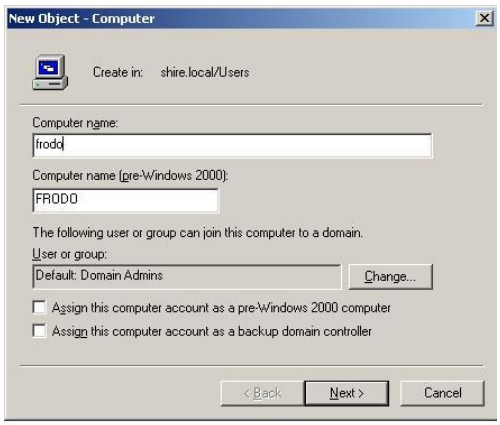
Järjestelmän antama varoitus Internet Information Services (IIS) -palvelun puuttumisesta hyväksytään klikkaamalla OK. Ilman IIS:ä sertifikaattien automaattinen jakelu lähiverkossa ei onnistu. Tarkistetaan vielä, että järjestelmänvalvojalle on annettu tarvittavat oikeudet juurisertifikaatin luomisen yhteydessä klikkaamalla Administrative tools, Certification Authority ja tarkistamalla SHIRE CA:n ominaisuuksista Security -välilehdeltä, että Administrator-ryhmällä on kuvion 19 mukaiset oikeudet.



KUVIO 19. Administrator-ryhmän oikeudet

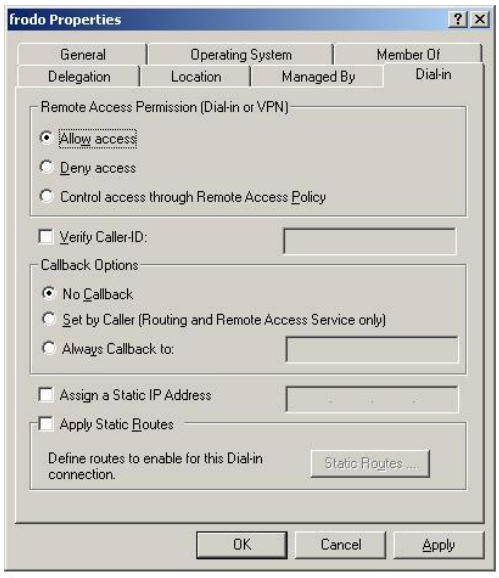
Lisätään seuraavaksi työasema toimialueelle. Avataan Active Directory Users and Computers -ikkuna ja laajennetaan shire.local -toimialue. New Object – Computer

-ikkuna saadaan auki klikkaamalla Users hiiren oikealla näppäimellä ja valitsemalla New, Computer. Avautuvaan ikkunaan annetaan kuvan mukaiset tiedot (kuvio 20).



KUVIO 20. Työaseman lisääminen toimialueelle

Toimialueelle lisätylle tietokoneelle annetaan vielä oikeus liittyä toimialueelle langatonta verkkoa käyttäen valitsemalla frodo-tietokoneen ominaisuuksista Dial-In -välilehti ja valitsemalla Remote Access Permissions (Dial-in or VPN) kohdassa Allow access (kuvio 21).



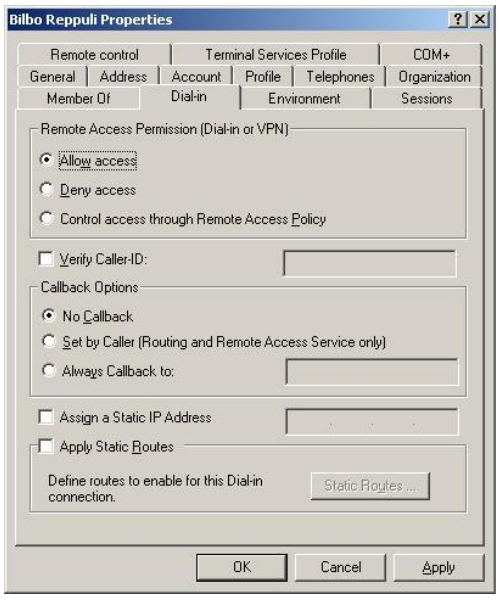
KUVIO 21. FRODO-työaseman ominaisuudet, Dial-In välilehti

Seuraavaksi luodaan Bilbo-niminen testikäyttäjä toimialueelle. Avataan Active Directory Users and Computers ikkuna ja laajennetaan shire.local toimialue. New Object – User ikkuna saadaan auki klikkaamalla Users hiiren oikealla näppäimellä

ja valitsemalla New, User Avautuvaan ikkunaan annetaan kuvion 22 mukaiset tiedot.

KUVIO 22. Mallina käytetty Bilbo-käyttäjä

Myös lisätylle käyttäjälle annetaan oikeus kirjautua toimialueelle langatonta verkkoa käyttäen valitsemalla Bilbo-käyttäjän ominaisuuksista Dial-In-välilehti ja valitsemalla kohdassa Remote Access Permissions (Dial-in or VPN) Allow access (kuvio 23).

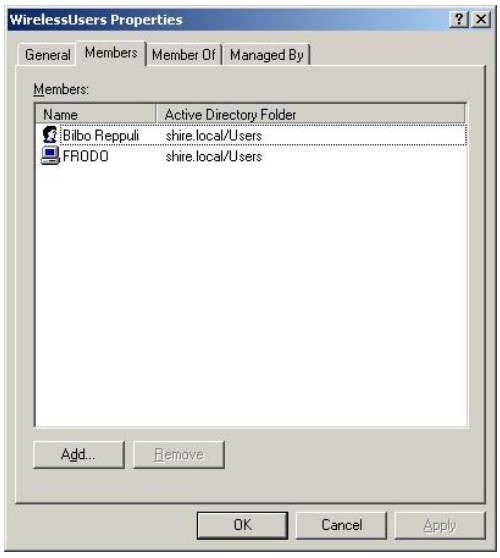


KUVIO 23. Langattoman kirjautumisen luvan myöntäminen

Langatonta kirjautumista varten muodostetaan vielä WirelessUsers-niminen ryhmä, jonka avulla on helpompi hallita käyttäjiä, joille mahdollistetaan järjestelmään kirjautuminen langattomilla työasemilla. Ryhmä lisätään klikkaamalla hiiren oikealla näppäimellä Users, valitsemalla New ja valitsemalla Group. New Object Group -ikkunassa annetaan kuvion 24 mukaiset tiedot.

KUVIO 24. Uuden käyttäjäryhmän luominen

Ryhmän luomisen jälkeen lisätään ryhmään jäseniksi luodut FRODO-tietokone ja Bilbo-käyttäjä (kuvio 25).



KUVIO 25. Käyttäjä ja työasema lisätty WirelessUsers-ryhmään

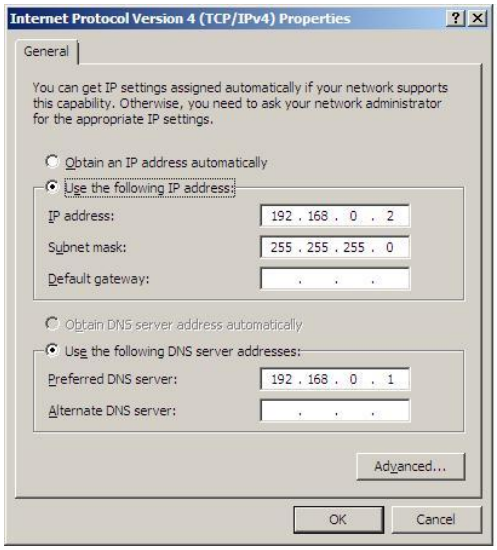
Näin on saatu asennettua Active Directory -toimialuepalvelin, DNS-palvelin, DHCP-palvelin ja Enterprise Root CA -palvelin shire.local-toimialueelle. Lisäksi toimialueelle on lisättynä testikäyttäjä (Bilbo) ja työasema (FRODO) sekä käyttäjäryhmä (WirelessUsers).

5.3 Network Protection Server -palvelimen asennus

NPS-palvelimeksi asennetaan Microsoft Windows Server 2008 perusasetuksilla. Palvelimen nimeksi annetaan IAS2008 ja IP-osoitteeksi 192.168.0.2. Tarkistetaan, että verkkoyhteys GANDALF-palvelimeen toimii, jonka jälkeen NPS-palvelin liitetään SHIRE.LOCAL-toimialueeseen. Tämän jälkeen palvelimella otetaan käyttöön NPS-palvelin rooli ja luodaan autentikoinnissa vaadittava tietokonesertifikaatti.

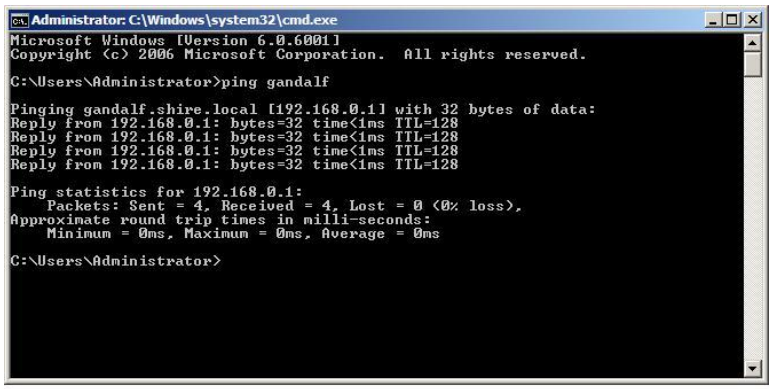
IAS2008-palvelimen konfigurointi NAP-kuntokäytäntö (Health Policy) palvelimeksi aloitetaan määrittämällä käytettävä langaton tukiasema RADIUS-asiakkaaksi määrittelemällä langattomien työasemien autentikointitavat yhteyspyyntökäytännöllä, ja luomalla verkkokäytäntö jolla sallitaan toimialuepalvelimen WirelessUsers-ryhmään kuuluville oikeus kirjautua verkkoon langatonta yhteyttä käyttäen.

Windows Server 2008 -palvelimen verkkoasetukset konfiguroidaan klikkaamalla Start, Server Manager. Avautuneessa Server Summary -ikkunassa klikataan View Network Connections, klikataan hiiren oikealla näppäimellä Local Area Connection ja valitaan Properties. IP-osoitteeksi määritellään 192.168.0.2, aliverkon peitteeksi 255.255.255.0 ja DNS-palvelimeksi 192.168.0.1 (kuvio 26).



KUVIO 26. NPS-palvelimen IP-asetukset

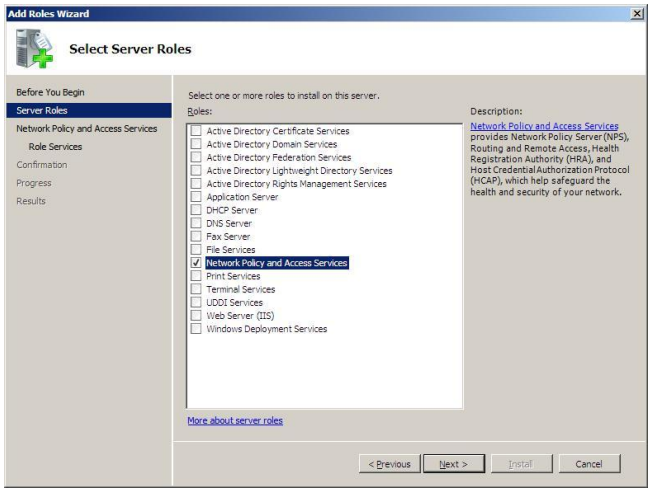
Tietoliikenneyhteyksien ja DNS-palvelimen toimivuus testataan komentokehotteessa antamalla komento ping gandalf (kuvio 27).



KUVIO 27. Tietoliikenneyhteyksien testaus IP-asetusten määrittelemisen jälkeen

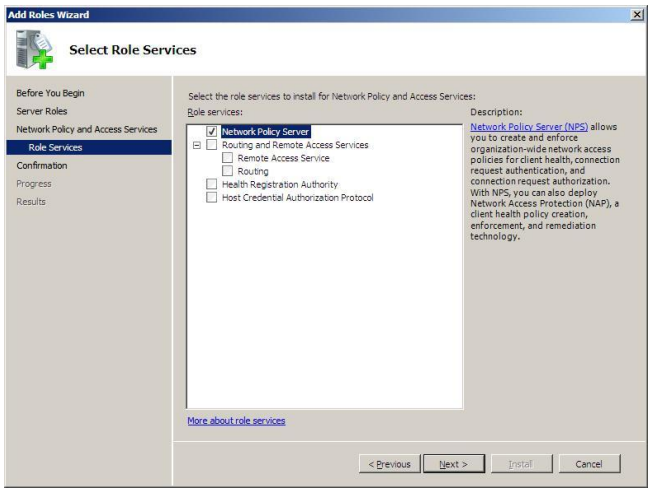
Asetusten testaamisen jälkeen NPS liitetään SHIRE.LOCAL -toimialueelle nimellä IAS2008. Järjestelmän ominaisuudet (System Properties) Windows Server 2008 -palvelinkäyttöjärjestelmässä vastaa vanhempien järjestelmien (Windows Server 2003) toimintoja.

Toimialueelle liitetyn palvelimen roolina toimii Network Policy Server, jonka asennus aloitetaan käynnistämällä Server Manager ja valitsemalla Add roles -kohdasta Roles Summary. Avautuvasta ikkunasta valitaan valinta Network Policy and Access Services (kuvio 28) ja klikataan Next kaksi kertaa.



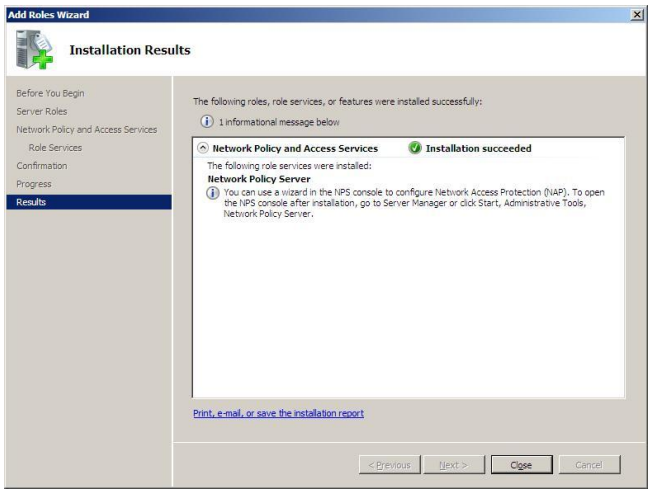
KUVIO 28. Network Policy and Access Services -roolin valinta

Select Role Services -ikkunassa valitaan valinta Network Policy Server (kuvio 29)



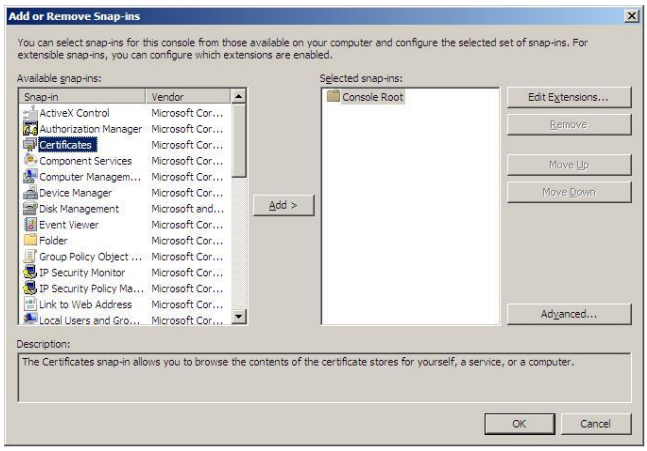
KUVIO 29. Palvelujen valinta Select Role Services -ikkunassa

Asennuksen jälkeen asennuksen onnistumisesta kerrotaan ikkunassa Installation Results (kuvio 30)



KUVIO 30. Onnistunut Network Policy Server -asennusilmoitus

Käytettävä EAP-MSCHAPv2-todennusmenetelmä vaatii NPS palvelimelta tietokonesertifikaattia. Luotu sertifikaatti tallennetaan palvelimen local computer -sertifikaattisäilöön. Sertifikaatti luodaan klikkaamalla Start, Run ja kirjoittamalla mmc avautuvaan ikkunaan. Avautuvassa konsoli-ikkunassa valitaan File-menusta Add/Remove Snapp-in. Add or Remove Snap-ins -ikkunassa valitaan Certificates ja Add (kuvio 31).



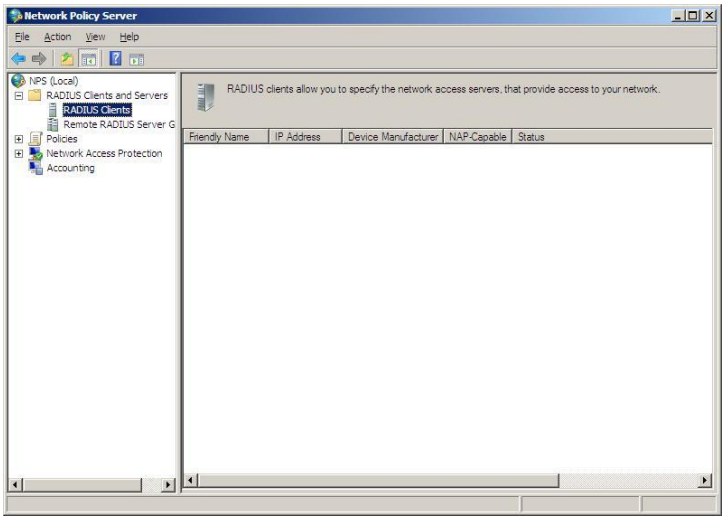
KUVIO 31. Add or Remove Snap-ins

Avautuvasta ikkunasta valitaan oletusasetukset Computer account, Local Computer ja klikataan Finish sekä suljetaan Add or Remove Snap-ins -ikkuna OK:ta painamalla. Auki jääneen konsoli-ikkunan vasemmassa paneelissa avataan Certificates, klikataan hiiren oikealla painikkeella Personal, valitaan All Tasks ja klikataan avautuvasta valikosta Request New Certificate, joka avaa Certificate Enrollment-ikkunan. Valitaan Computer, klikataan Enroll ja tarkistetaan, että sertifikaatin tuonti onnistui (kuvio 32).

KUVIO 32. Sertifikaatin tuonti onnistunut

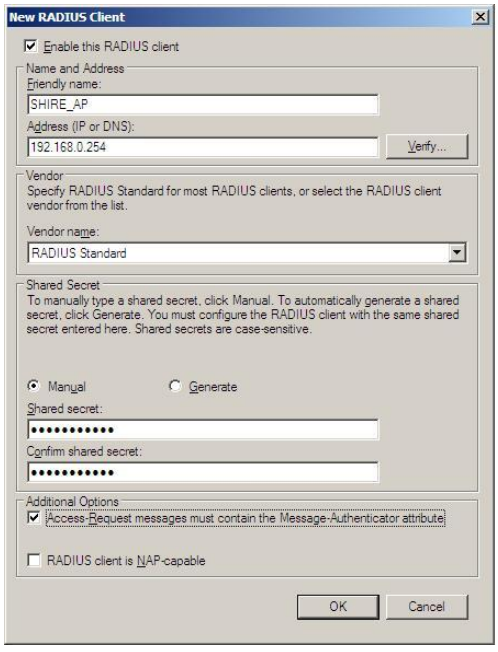
Yhteyspyyntöjen, autentikointiviestien ja tilastointiviestien välittämisen mahdollistavan RADIUS-asiakkaan konfigurointi aloitetaan avaamalla Network Policy Server Management -konsoli klikkaamalla Start, Run ja kirjoittamalla nps.msc.

Konsolissa tehdään jatkossa kaikki tarvittavat määritykset palvelimen toiminnallisuutta ajatellen (kuvio 33).



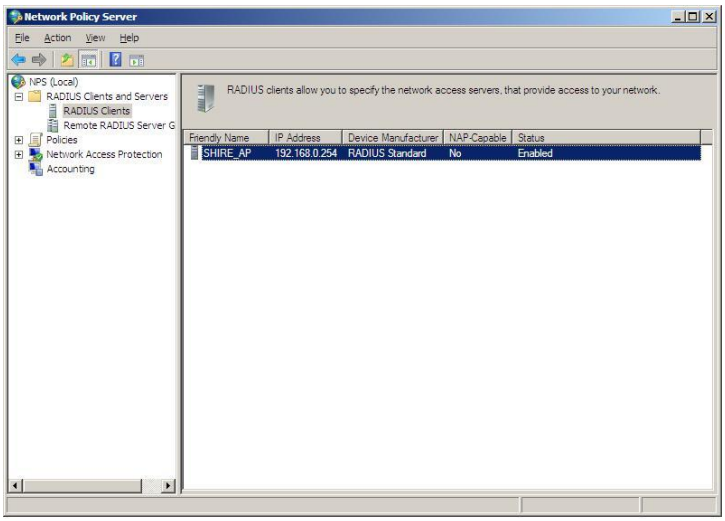
KUVIO 33. Network Policy Server management -konsoli

NPS-konsolin RADIUS Clients and Servers -valikko laajennetaan kaksoisklikkauksella ja valitsemalla hiiren oikealla näppäimellä RADIUS Clients -valikosta New RADIUS CLIENT. Avautuvassa ikkunassa Friendly name -kohtaan kirjoitetaan tukiaseman nimi (SHIRE_AP), tukiasemalle määritelty IP-osoite ja Shared Secret kohtaan sama salasana, jota käytetään myöhemmin tukiaseman konfiguroinnin yhteydessä (kuvio 34).



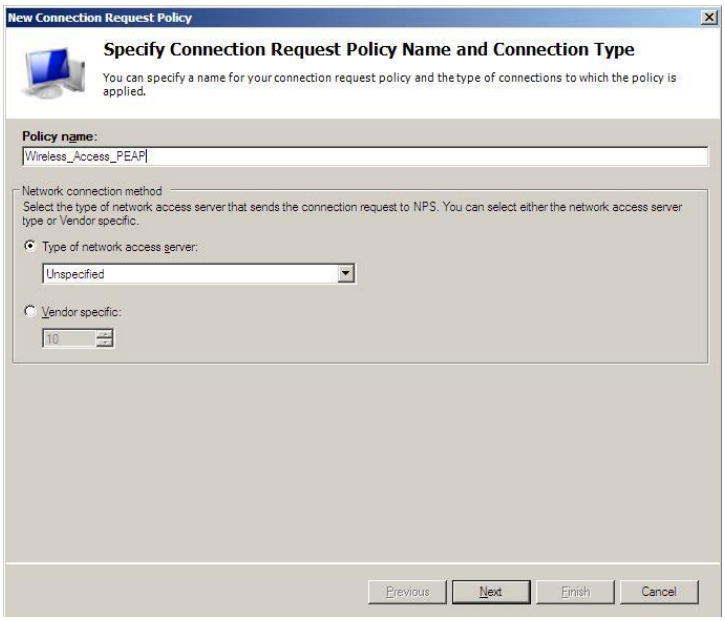
KUVIO 34. Shire_AP RADIUS-asiakkaan luonti

Konfiguroinnin tuloksena RADIUS Client näkyy NPS-konsolissa ja Clientin statuksena on Enabled (kuvio 35)



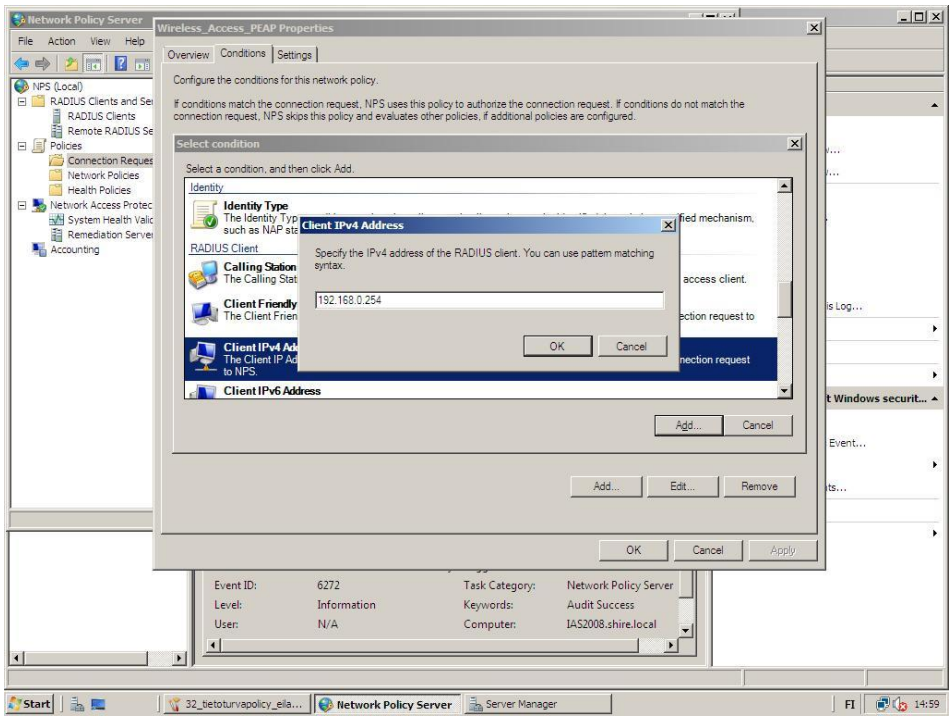
KUVIO 35. RADIUS-Client Enabled

Asiakkaan autentikointitavat ja käytettävä RADIUS-asiakas määritellään yhteyspyyntökäytännöllä (Connection Request Policy, CRP). RADIUS-asiakkaan määrittely lisää verkon tietoturvaa, koska vain määritellyista asiakkaista tulleet yhteyspyynnöt käsitellään. NPS-konsolissa laajennetaan kohta Policies ja otetaan pois käytöstä oletus CRP valitsemalla Use Windows authentication for all users hiiren oikealla painikkeella ja valitsemalla Disable. Uusi yhteyspyyntökäytäntö muodostetaan klikkaamalla hiiren oikealla painikkeella Connection Request Policies ja valitsemalla avautuvasta valikosta kohta New. Avautuvassa Specify Connection Request Policy Name and Connection Type -ikkunassa annetaan käytänteelle nimi (Wireless_Access_PEAP) (kuvio 36) ja jatketaan valitsemalla Next.



KUVIO 36. Connection Request Policy

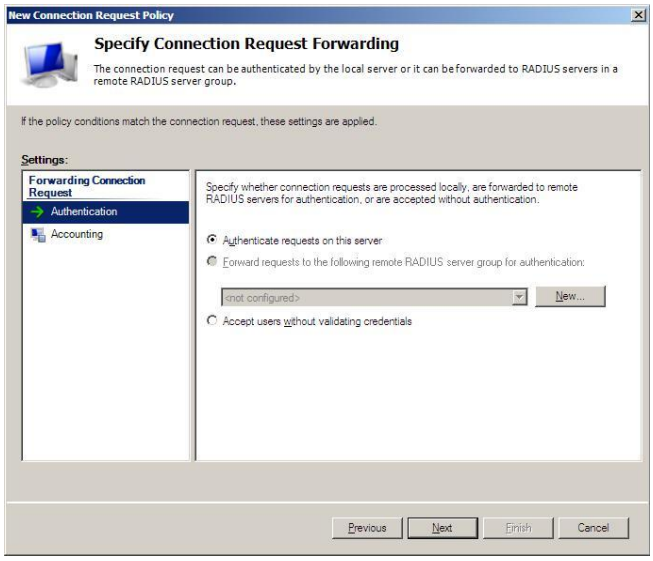
Valitaan Add, kaksoisklikataan RADIUS Client -kohdasta Client IPv4 Address ja kirjoitetaan tukiaseman IP-osoite 192.168.0.254 (kuvio 37)



KUVIO 37. RADIUS-Client määrittely

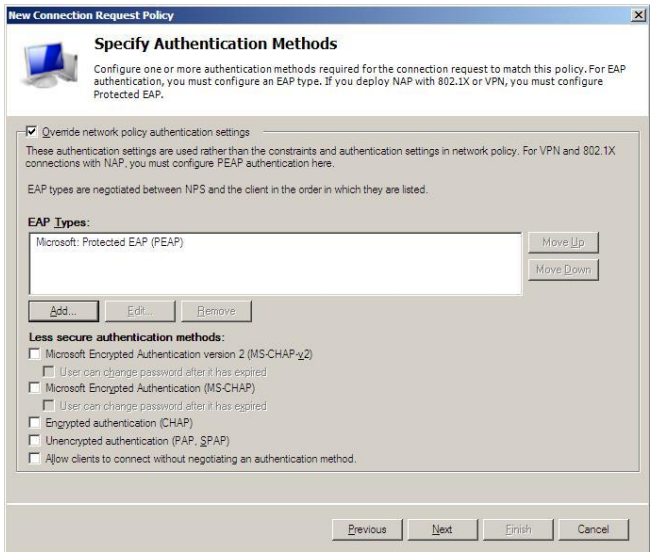
Valitaan Next ja tarkistetaan, että valinta Authenticate requests on this server -kohdassa Specify Connection Request Forwarding on valittuna (kuvio 38) ja klikataan Next. Authenticate requests on this server määrittelee käytettävän palveli-

men autentikointipalvelimeksi, eli autentikointipyyntöjä ei lähetetä edelleen jollekin toiselle palvelimelle.



KUVIO 38. Authenticate requests on this server

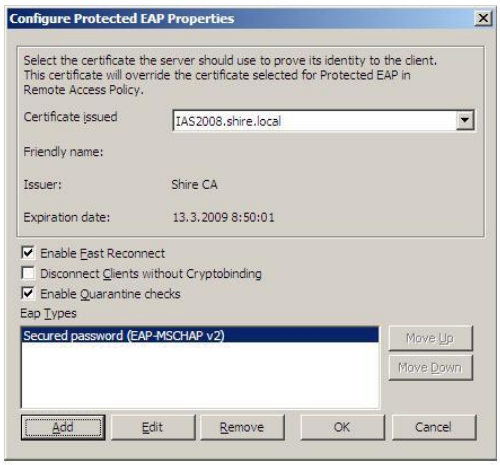
Specify Authentication Methods -ikkunassa valitaan Override network policy authentication settings, joka ohittaa myöhemmissä käytänteissä mahdollisesti käytettävät heikommat autentikointimenetelmät, valitaan käytettäväksi EAP-tyypiksi Microsoft Protected EAP (PEAP) ja jatketaan klikkaamalla OK (kuvio 39).



KUVIO 39. Autentikointimentelmän valinta

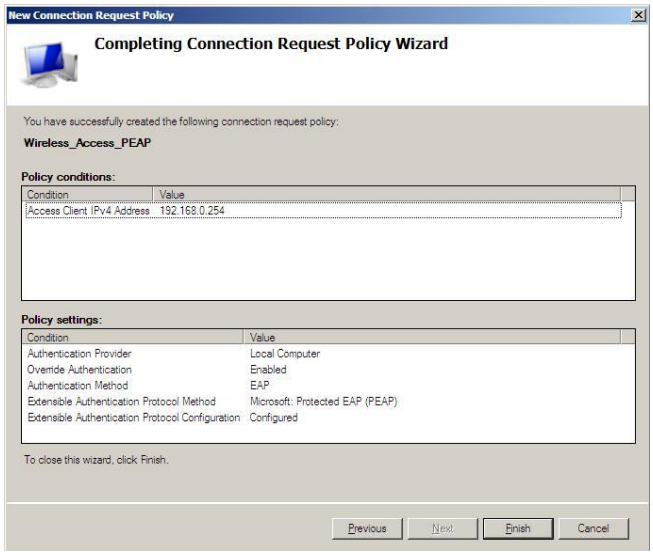
Valitaan edelleen Specify Authentication Methods -ikkunassa lisätty EAP-tyyppi, klikataan Edit ja varmistetaan avautuvasta Configure Protected EAP Properties -ikkunasta, että Enable Quarantine checks on valittuna sekä Certificate issued -

kohdassa on Certification Authority -palvelimena toimivan toimialuepalvelimen IAS2008 palvelimelle myöntämä sertifikaatti (kuvio 40).



KUVIO 40. Palvelinsertifikaatti

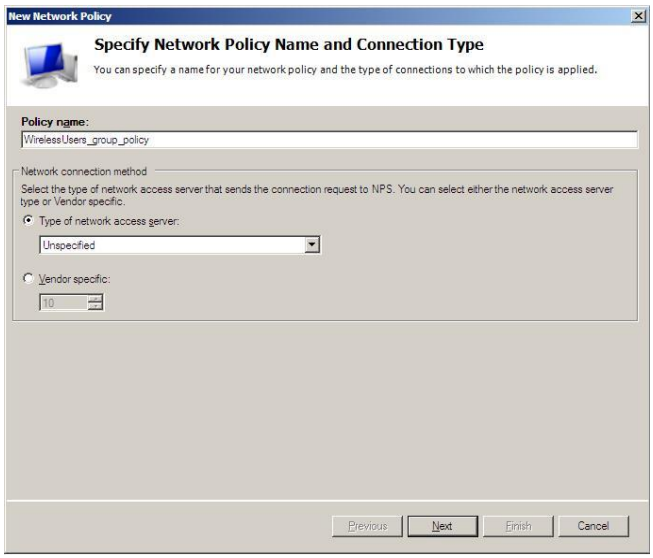
Klikkaamalla Next kaksi kertaa avautuu Completing Connection Request Policy Wizard -ikkuna, josta nähdään yhteenveto edellä luodusta käytänteestä (kuvio 41).



KUVIO 41. Connection Request Policy -määritykset

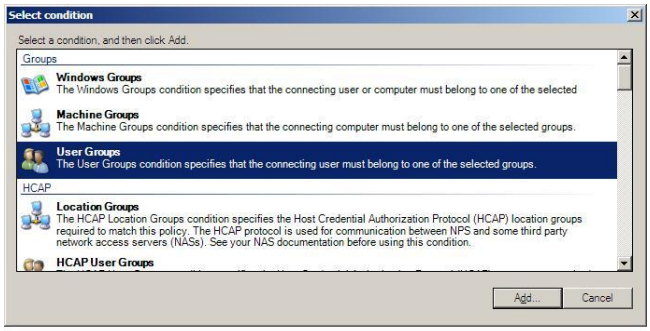
Seuraavaksi määritellään käytäntö, jolla kielletään verkkoon pääsy muilta kuin toimialueen WirelessUsers-ryhmään kuuluvilta käyttäjiltä ja tietokoneilta. Käytänteellä varmistutaan osaltaan siitä, että ne työasemat, joille ei erikseen ole annettu lupaa langattomaan kirjautumiseen, eivät pääse kirjautumaan verkkoon langattomia laitteita käyttäen.

Klikataan NPS -ikkunassa hiiren oikealla näppäimellä Network Policies ja valitaan New. Käytänteen nimeksi annetaan WirelessUsers_group_policy ja klikataan Next (kuvio 42).



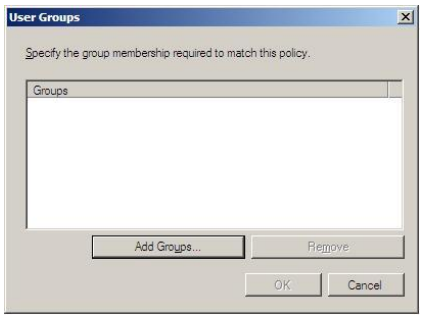
KUVIO 42. WirelessUsers_group_policy

Specify Condition -ikkunassa klikataan Add, valitaan avautuvasta Select Condition ikkunasta User Groups ja klikataan Add (kuvio 43).

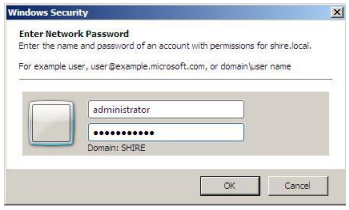


KUVIO 43. Käyttäjäryhmän määrittely

User Groups-ikkunassa klikataan Add Groups (kuvio 44) ja avautuvasta Select Groups-ikkunasta Advanced. Järjestelmä kysyy toimialuepalvelimen Domain Admin -oikeuksilla varustettua käyttäjätunnusta ja salasanaa (kuvio 45).

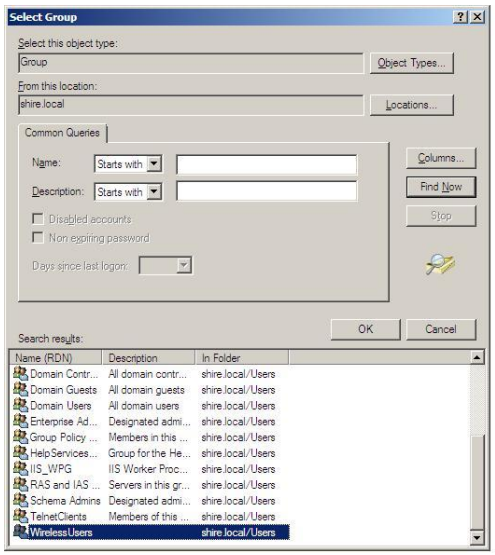


KUVIO 44. Käyttäjäryhmien valinta



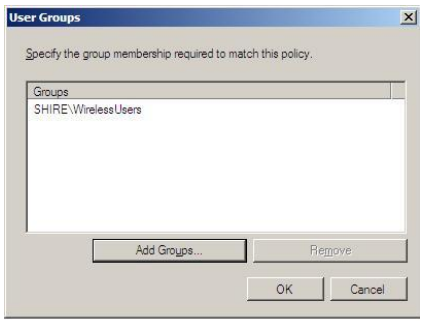
KUVIO 45. Pääsy AD-palvelimelle vaatii salasanan

Käyttäjätunnuksen ja salasanan antamisen jälkeen avautuu Select Groups-ikkunaan toimialueen ryhmät, joista valitaan WirelessUsers-ryhmä (kuvio 46).



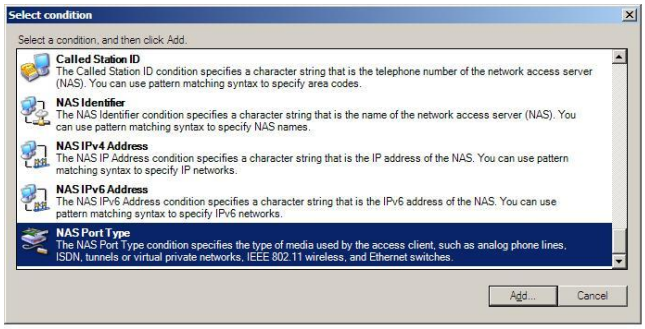
KUVIO 46. WirelessUsers-ryhmän valinta

Tarkistetaan vielä, että valittu ryhmä on oikea ja hyväksytään painamalla OK (kuvio 47).



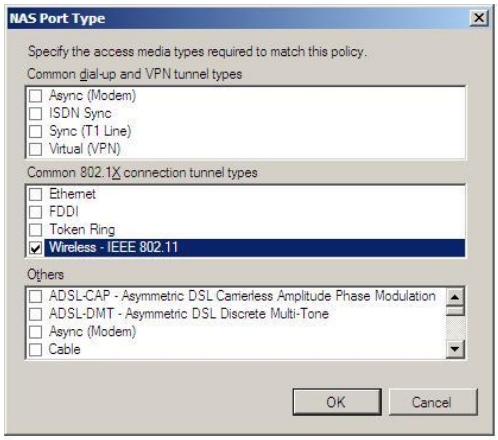
KUVIO 47. SHIRE\WirelessUsers-ryhmä valittuna

Määritellään vielä langattoman tukiaseman porttityypiksi Wireless - IEEE802.11 valitsemalla Specify Conditions -ikkunassa Add ja valitsemalla Select Condition -ikkunassa NAS Port Type ja klikkaamalla Add (kuvio 48).



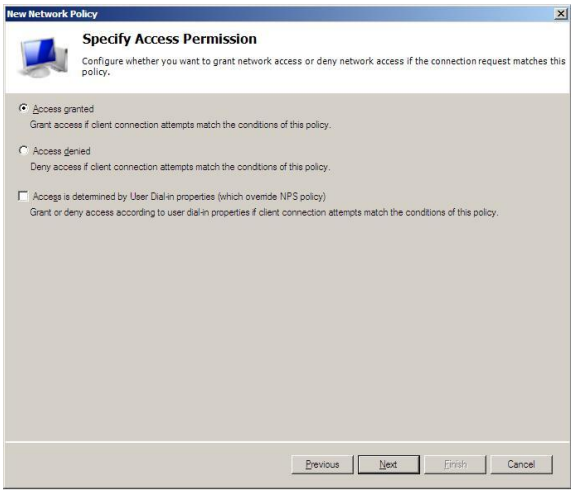
KUVIO 48. NAS Port Type

NAS Port Type-ikkunassa valitaan valinnaksi Wireless - IEEE802.11 ja klikataan OK (kuvio 49).



KUVIO 49. Wireless IEEE802.11 -valinta

Specify Access Permission -ikkunassa valitaan oletusarvo Access Granted (kuvio 50).



KUVIO 50. Specify Access Permissions -ikkuna

Muihin kohtiin ei tässä vaiheessa tarvitse valita mitään koska Connection Request Policyssä määriteltiin jo käytettävä autentikointitapa, joten voidaan klikata Next, kunnes käytäntö lopulta voidaan hyväksyä klikkaamalla Finish.

Nyt on saatu valmiiksi NPS-palvelimen verkkoasetukset ja liitetty palvelin SHIRE.LOCAL -toimialueelle, otettu käyttöön Network Policy Server -rooli, luotu CA-palvelimen myöntämä palvelinsertifikaatti, määritelty autentikointitapa ja käytettävä RADIUS-asiakas yhteyspyyntökäytännöllä, luotu verkkokäytäntö, jonka avulla rajataan ne käyttäjät, joilla on oikeus kirjautua verkkoon langattomia laitteita käyttäen.

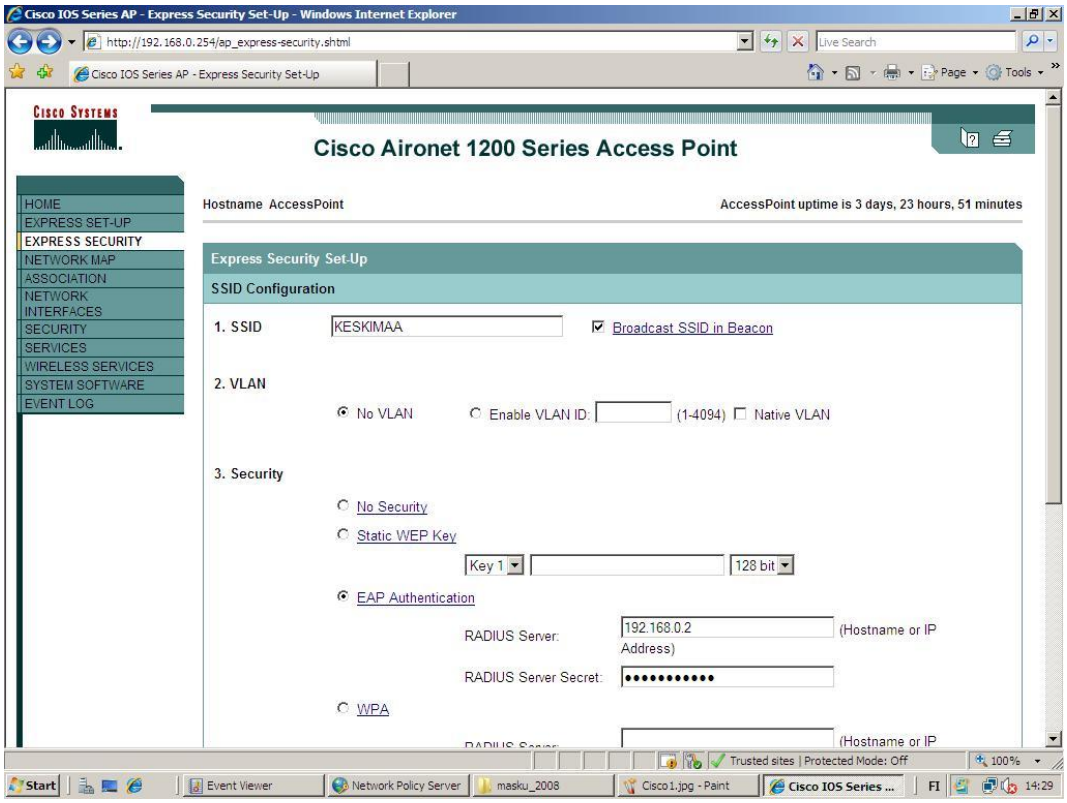
5.4 Cisco Aironet 1200 tukiaseman asennus

RADIUS-asiakkaana käytettävään Cisco Aironet 1200 -tukiasemaan määritellään tukiaseman IP-osoite 192.168.0.254, verkon SSID (KESKIMAA) ja otetaan käyttöön RADIUS-autentikointi.

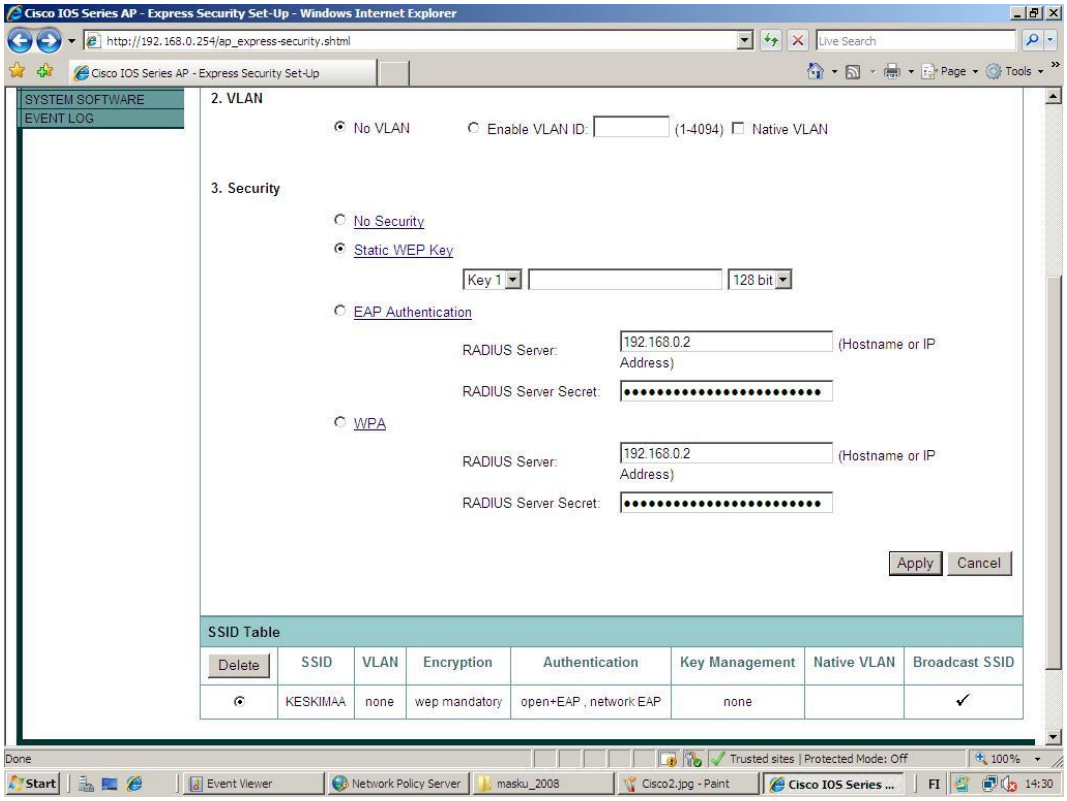
Määritellään Express Set-Up -sivulla tukiaseman Host Name (AccessPoint) IP-osoitteeksi 192.168.0.254/24 (kuvio 51).

KUVIO 51. Langattoman verkon nimi ja tukiaseman IP-asetukset

Express Security -välilehdellä määritellään verkon SSID (KESKIMAA) ja käytettävä autentikointimenetelmä, EAP Authentication. RADIUS palvelimena määritellään käytettäväksi IAS2008-palvelimen IP-osoitetta 192.168.0.2 ja RADIUS Shared Secret -kohtaan kirjoitetaan sama salasana, joka määriteltiin RADIUS-palvelimen konfiguraatiossa (kuvio 52, kuvio 53). Tukiaseman SSID:n mainostus (Broadcast SSID) jätetään päälle visuaalisuuden vuoksi, vaikka todellisessa konfiguroinnissa SSID:n mainostus tulee tietoturvasyistä kieltää.



KUVIO 52. SSID ja EAP Authentication -määritykset



KUVIO 53. SSID Tablesta selviää määritellyt asetukset

Muita määrityksiä tukiasemalle ei tässä vaiheessa tarvitse tehdä. Tukiasemaan on siis määritelty vain tukiaseman IP-osoite, verkon SSID ja otettu käyttöön EAP-autentikointi määrittelemällä käytettävä RADIUS-palvelin ja Shared Secret. Mikäli haluttaisiin ohjata kuntokäytäntöjen (Health Policy) määritysten mukaiset epäsopivat (Uncompliant) työasemat eri VLAN:hin kuin sopivat (Compliant) työasemat, konfiguroitaisiin käytettävät VLAN:it tukiaseman käyttöliittymän Services, VLAN -linkkien kautta. Tietoturvasyistä on kuitenkin muistettava, että tukiaseman oletuksena toimiva käyttäjätunnus-salasanapari on myös syytä vaihtaa.

5.5 Työaseman asennus

Testauksessa käytettävään FRODO-työasemaan asennetaan Microsoft Windows Vista Ultimate -käyttöjärjestelmä perusasetuksilla ja liitetään työasema SHIRE.LOCAL-toimialueelle. Työasemassa otetaan käyttöön Network Access Protection Agent ja EAP-karanteenin pakotusasiakas-toiminnot sekä aktivoidaan tietoturvakeskus. Työaseman asennus viimeistellään määrittelemällä käytettävä langaton verkko ja käytettävä autentikointitapa.

802.1X-pakottaminen lisää koko verkon tietoturvaa vertaamalla työaseman tietoturvakeskuksen raportoimia työaseman asetuksia verkon vaatimuksiin aina kun työasema yrittää autentikoitua järjestelmään. Lisäksi 802.1X-pakottaminen aktiivisesti monitoroi asiakaslaitteiden kuntotilaa ja rajoittaa automaattisesti verkon käyttöä niiltä työasemilta, jotka eivät ole järjestelmän vaatimusten mukaisia.

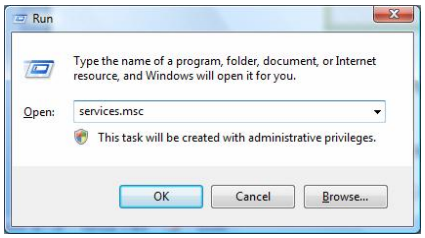
Koska toimialuepalvelin toimii DHCP -palvelimena, työaseman verkkokortille ei tarvitse tehdä muutoksia, vaan työasema saa automaattisesti verkkojohdon liittämisen jälkeen yhden verkon IP-osoitteista.

Työasema liitetään SHIRE.LOCAL -toimialueeseen klikkaamalla työpöydän Computer-painiketta hiiren oikealla ja valitsemalla Properties, Change Settings. System Properties -ikkunan Computer Name -välilehdellä klikataan Change ja avautuvaan Computer Name/Domain Changes -ikkunaan kirjoitetaan Computer name -kohtaan työaseman nimeksi FRODO. Valinnan Member of Domain -kohtaan kirjoitetaan toimialueen nimi SHIRE.LOCAL (kuvio 54).

KUVIO 54. Työaseman liittäminen toimialueelle

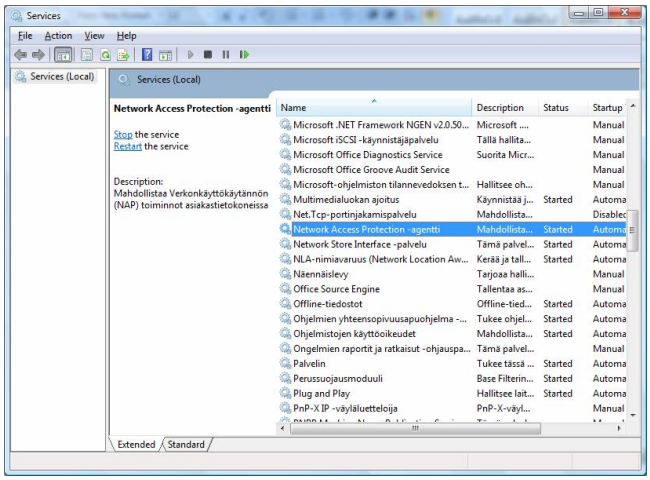
Avautuneeseen ikkunaan kirjoitetaan jonkin Domain Admin -ryhmään kuuluvan käyttäjän käyttäjätunnus ja salasana, jonka jälkeen avautuu ikkuna onnistuneesta asennuksesta.

Network Access Protection Agent -asennus aloitetaan avaamalla Palvelut-ohjelma (Services) klikkaamalla Käynnistä (Start), Kaikki ohjelmat (All Programs), Apu-ohjelmat (Accessories) ja Suorita (Run) ja kirjoitetaan avautuvaan ikkunaan services.msc (kuvio 55).



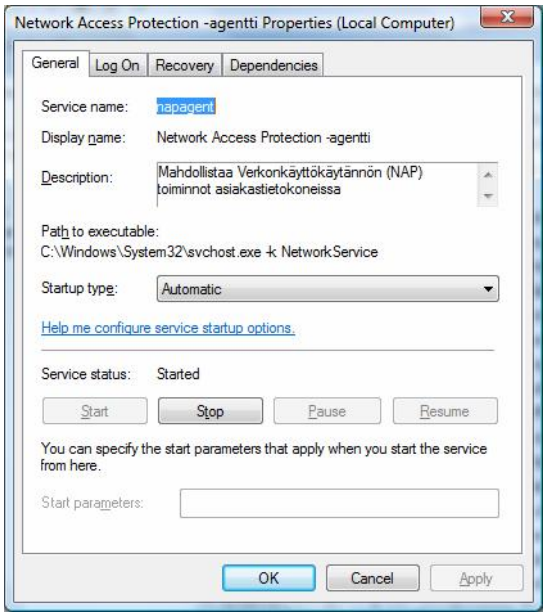
KUVIO 55. NAP -asennuksen alku

Avautuneessa palvelut-ohjelmassa valitaan Network Access Protection -agentti (Network Access Protection -agent) hiiren oikealla ja valitsemalla avautuvasta valikosta ominaisuudet (Properties) (kuvio 56).



KUVIO 56. Services ikkuna

Avautuvassa ominaisuudet-ikkunassa kohdassa Palvelun tila (Service Status) klikataan Käynnistä (Start), jolloin palvelu käynnistyy (kuvio 57).



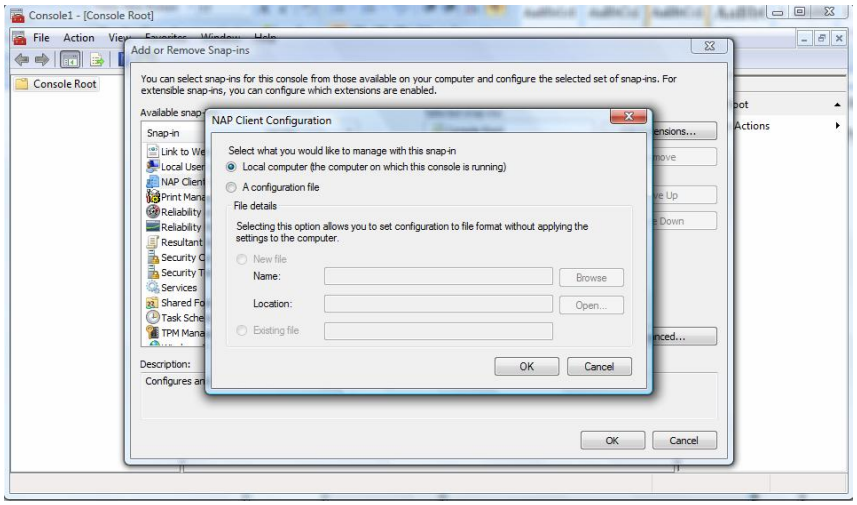
KUVIO 57. Network Access Protection Agent käynnissä

EAP-pakottaminen mahdollistaa työaseman asetusten, esim. Windows-palomuurin käyttöönottamisen automaattisesti Windows Security Health Validatorin ja Health Policyjen mukaan.

Tietoturvakeskuksen käyttöönotto on myös tärkeää, koska sitä kautta käyttäjä saa informaatiota tietoturvakeskuksen antamista työaseman tietoturvaan liittyvistä varoituksista ja asetuksista.

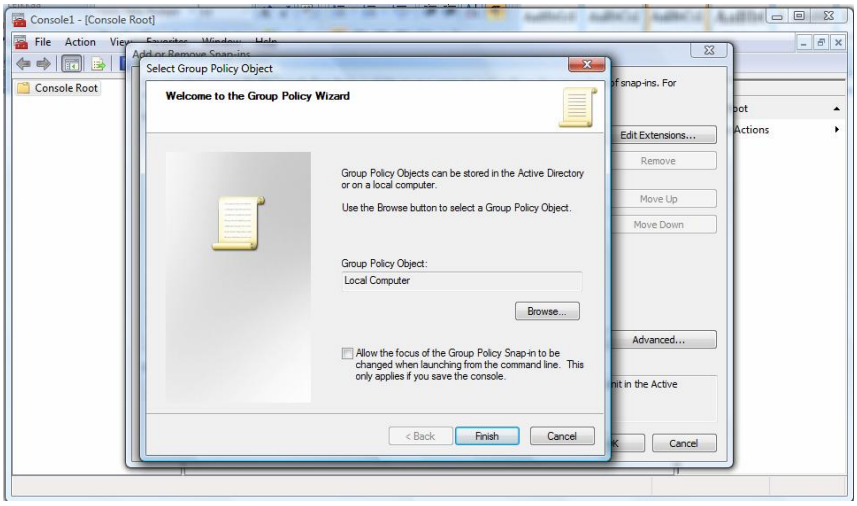
EAP-pakottaminen ja tietoturvakeskus otetaan käyttöön MMC (Microsoft Management Console) -konsolissa. Konsoli käynnistetään klikkaamalla Käynnistä (Start), Kaikki ohjelmat (All Programs), Apuohjelmat (Accessories) ja Suorita (Run) ja kirjoitetaan avautuvaan ikkunaan mmc.

Avautuneen konsoli-ikkunan Tiedosto (File) -valikosta valitaan Lisää tai poista laajennus (Add/Remove Snap-in). Avautuneesta ikkunasta valitaan NAP-asiakkaan määritys (NAP Client Configuration) ja klikataan Lisää (Add). NAP-asiakkaan määritys (NAP Client Configuration) -ikkunassa hyväksytään OK painiketta painamalla oletusasetus Paikallinen tietokone (Local Computer) -valinta (kuvio 58).



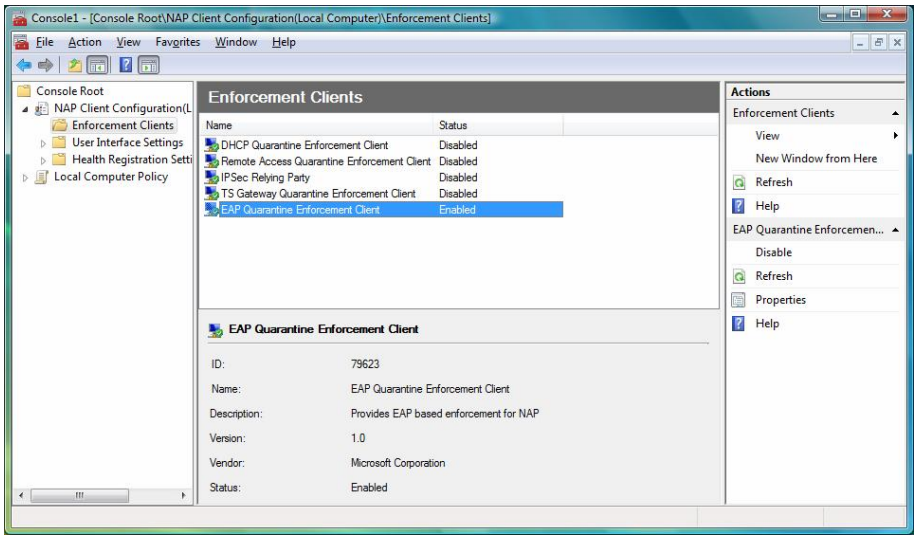
KUVIO 58. NAP-asiakkaan määritys

NAP-asiakkaan määritys (NAP Client Configuration) -ikkunassa valitaan vielä Ryhmäkäytäntöobjektien editori (Group Policy Object Editor) ja klikataan Lisää (Add). Avautuvasta ikkunasta hyväksytään oletusarvo Group Policy Object, Local Computer (kuvio 59).



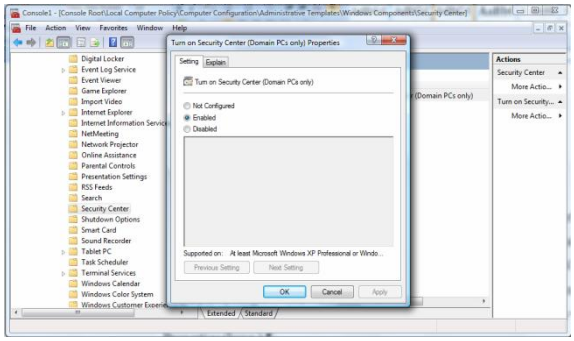
KUVIO 59. Ryhmäkäytäntöobjektin lisääminen

EAP-karanteenin pakotusasiakas -toiminto otetaan lopulta käyttöön kaksoisklikkaamalla NAP-asiakkaan määritys, Paikallinen tietokone (NAP Client Configuration, Local Computer) ja klikkaamalla Pakotusasiakkaat (Enforcement Clients). Pakotusasiakkaiden listalta klikataan EAP karanteenin pakotusasiakas (EAP Quarantine Enforcement Client) hiiren oikealla näppäimellä ja valitaan Ota käyttöön (kuvio 60).



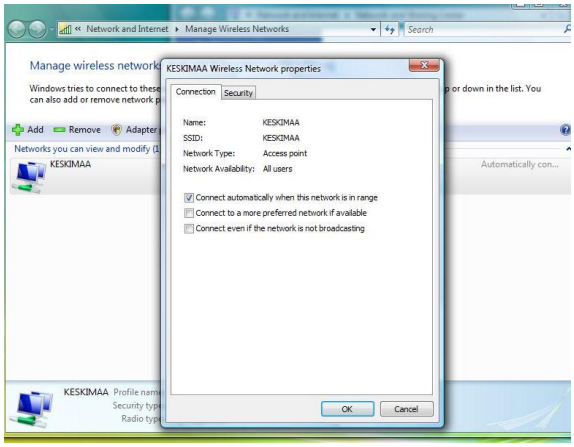
KUVIO 60. EAP karanteenin pakotusasiakas käynnissä

Tietoturvakeskus aktivoidaan kaksoisklikkaamalla konsolin vasemmasta paneelista Paikallinen tietokone -käytäntö (Local Computer Policy), Tietokoneasetukset (Computer Settings), Administrative Templates, Windows Components, Security Center. Konsolin keskipaneelista kaksoisklikataan Turn On Security Center, valitaan avautuvasta ikkunasta Enabled ja hyväksytään asetus klikkaamalla OK (kuvio 61). Tämän jälkeen konsoli-ikkuna voidaan sulkea tallentamatta.



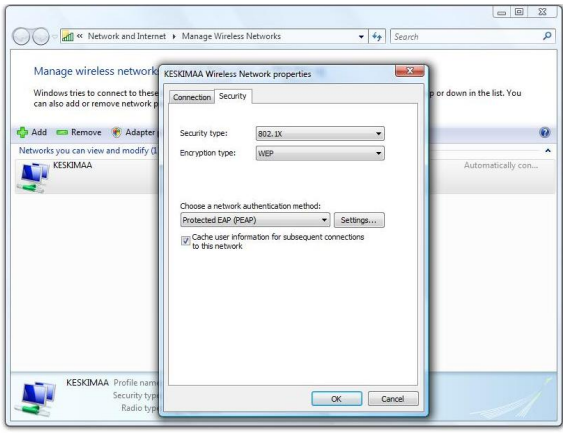
KUVIO 61. Tietoturvakeskuksen käyttöönotto

Työasemassa IEEE 802.1X-autentikointi otetaan käyttöön langattoman verkkokortin asetuksissa. Käynnistysvalikossa klikataan Network hiiren oikealla näppäimellä ja valitaan Properties, Manage Wireless Connections. Manage Wireless Connections -ikkunassa valitaan oikea langaton verkko (KESKIMAA) langattomien verkkojen luettelosta hiiren oikealla näppäimellä ja valitaan avautuvasta valikosta Properties (KUVIO 62).



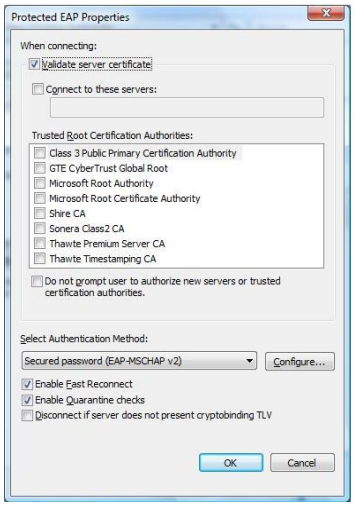
KUVIO 62. KESKIMAA-verkon ominaisuudet

Security välilehdeltä valitaan Security Typeksi 802.1X ja salausmenetelmäksi (Encryption Type) WEP. Autentikointimenetelmäksi (Authentication method) valitaan Protected EAP (PEAP) (kuvio 63) ja klikataan Settings.



KUVIO 63. Langattoman yhteyden Security -asetukset

Avautuneessa Protected EAP Properties -ikkunassa varmistaudutaan, että valinnat Enable Fast Reconnect, Enable Quarantine checks ja Validate Server certificate ovat valittuina. Mikäli autentikointipalvelimen määrityksissä olisi määritelty käytettäväksi EAP-TLS-autentikointia, tulisi tässä ikkunassa valita Select Authentication Method -kohdasta Use Smart Card or Other Certificate -valinta. (kuvio 64).



KUVIO 64. Protected EAP Properties -asetukset

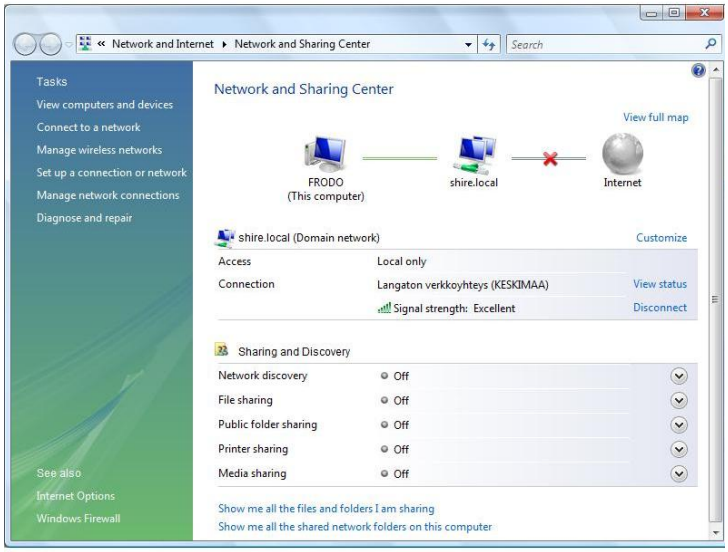
Varmistetaan vielä klikkaamalla Configure, että järjestelmä käyttää automaattisesti työasemalle kirjautuneen käyttäjätunnusta ja salasanaa käyttäjätietojen tarkistuksessa (kuvio 65).

KUVIO 65. EAP MSCHAPv2 -asetukset

Yllä esiteltyjen konfiguraatioiden ja autentikoinnin testaus suoritettiin yhdistämällä työasema KESKIMAA-verkkoon käyttäen toimialueen Administrator-käyttäjätiliä. Administrator-tili lisättiin WirelessUsers ryhmään ja lisäksi tilille annettiin Remote Access Permissions -oikeudet.

Testin tuloksena työasema autentikoitui verkkoon käyttäen IEEE802.1X autentikointia. Autentikoinnin onnistumisen voi tarkistaa NAP-palvelimen Event Vieweristä (kuvio 66 ja kuvio 67).

KUVIO 66. RADIUS-palvelimen Event Properties, autentikointi onnistunut

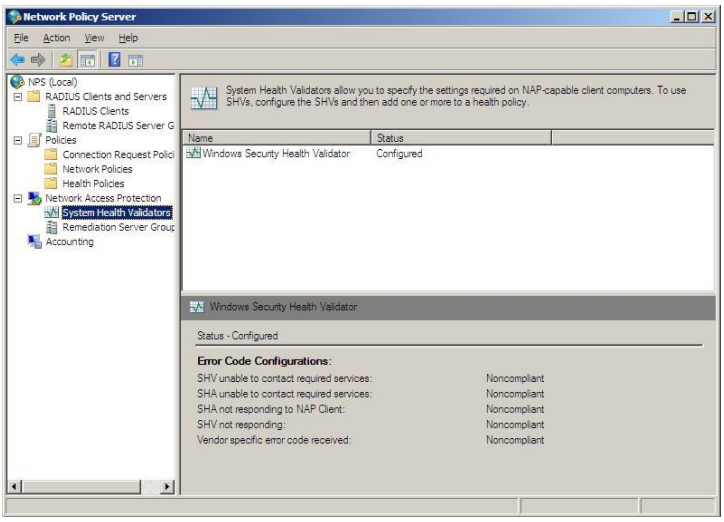


KUVIO 67. Työaseman Network and Sharing Center, työasema kirjautunut verkkoon.

Työasema on nyt liitetty SHIRE.LOCAL -toimialueelle, on otettu käyttöön Network Access Protection Agent ja EAP-karanteenin pakotusasiakas-toiminnot sekä aktivoitu tietoturvakeskus. Edellä mainitut toiminnot yhdessä välittävät NPS-palvelimelle tiedon työaseman kuntotilasta (Health State), jonka perusteella NPS-palvelin päättää onko työasema tarpeeksi turvallinen saadakseen täydet oikeudet verkon käyttöön vai rajoitetaanko työaseman oikeuksia siihen saakka kunnes se on jälleen järjestelmän vaatimusten mukainen. Työaseman asennuksen päätteeksi viimeisteltiin käytettävä langaton verkko ja autentikointitapa.

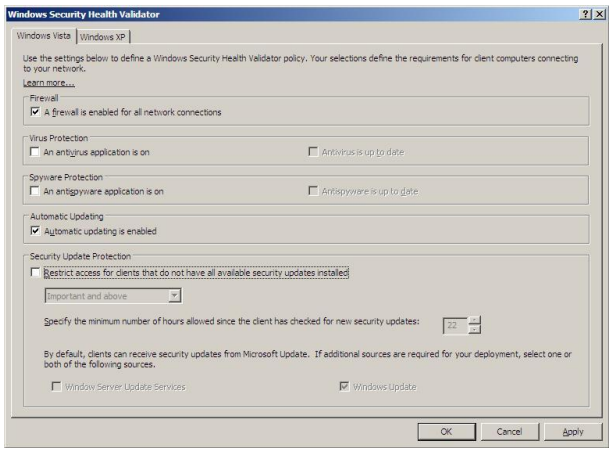
5.6 System Health Validator -konfigurointi ja käyttöönotto

NPS-palvelimessa määritellään SHV laajentamalla Network Policy Server -ikkunassa kohta Network Access Protection ja valitsemalla System Health Validators. Avataan System Health Validator Properties -ikkuna kaksoisklikkaamalla Windows Security Health Validator -kohtaa ikkunan oikeanpuoleisesta paneelista (kuvio 68).



KUVIO 68. Network Policy Server, System Health Validator

Valitaan avautuvassa Windows Security Health Validator-ikkunassa kuvion 69 mukaiset kohdat. Asetuksilla vaaditaan työasemalta palomuurin käytössä oloa kaikilla verkkosovittimilla sekä käyttöjärjestelmän automaattisten päivitysten käytössä oloa.



KUVIO 69. Järjestelmän Security Health Validator -vaatimukset

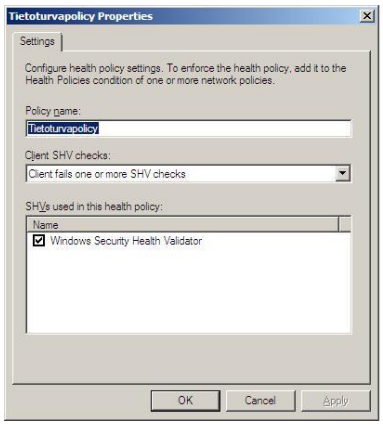
Windows Security Health Validator-ikkunassa tehtävillä voidaan vaatia, että:

- Työasemissa on asennettu ja sallittu palomuurin käyttö
- Virustorjuntaohjelma on asennettu ja käytössä
- Virustorjuntaohjelmisto on päivitetty
- Haittaohjelmien poisto-ohjelma on asennettu ja käytössä
- Haittaohjelmien poisto-ohjelma on päivitetty
- Microsoft automaattiset päivityspalvelut (Update Services) ovat käytössä

Lisäksi, mikäli työaseman Windows Update Agent on rekisteröity palvelimen Windows Server Update Services (WSUS) -palveluun, NAP voi lisäksi tarkistaa, että saatavilla olevat päivitykset on asennettu työasemiin.

5.7 Kuntokäytännön ja verkkokäytäntöjen konfigurointi

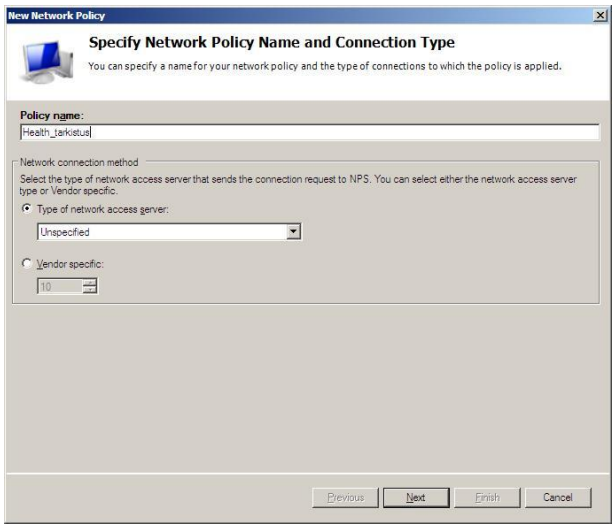
NPS-palvelimeen määritellään kuntokäytäntö (Health Policy) kaksoisklikkaamalla Network Policy Server -ikkunassa Health Policies ja valitsemalla New, Create. Määritellään Health Policy -ikkunassa (kuvio 70) luotavan käytännön nimi, käytettävä SHV (SHVs used in this health policy) ja ehdot SHV -tarkistuksille (Client SHV checks).



KUVIO 70. Tietoturvapolicy-niminen kuntokäytäntö

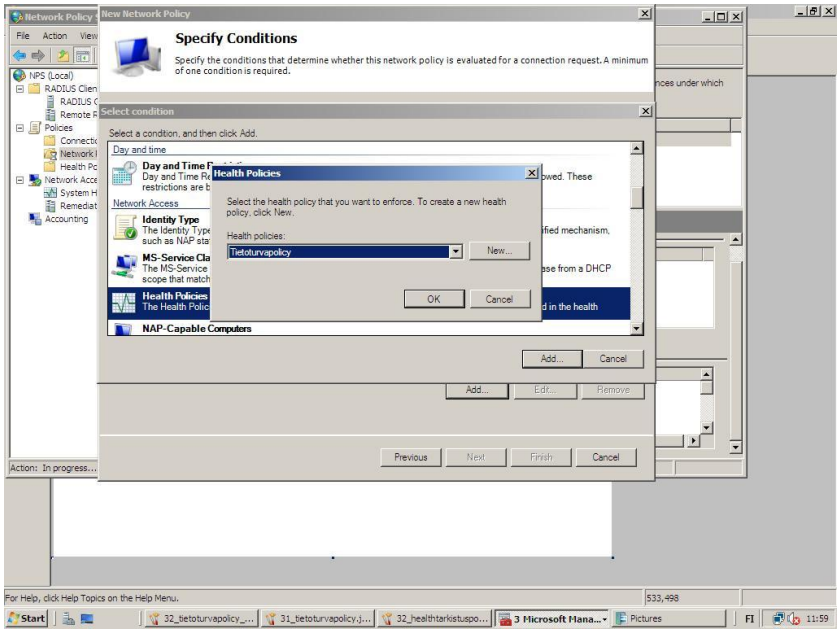
Yleisimmin käytettävinä vaihtoehtoina kuntovaatimustarkistuksille ovat Client passes all SHV checks (asiakas läpäisee kaikki kuntovaatimustarkistukset) jolloin asiakaslaite määritellään verkon vaatimusten kannalta sopivaksi ja Client fails one or more SHV checks (asiakas ei läpäise yhtä tai useampaa kuntovaatimustarkistusta) jolloin asiakaslaite määritellään verkon vaatimusten kannalta epäsopivaksi ja sen verkon käyttöä rajoitetaan.

Määritellään verkkokäytäntö klikkaamalla hiiren oikealla Network Policy Server ikkunassa Network Policies ja valitsemalla New (kuvio 71).



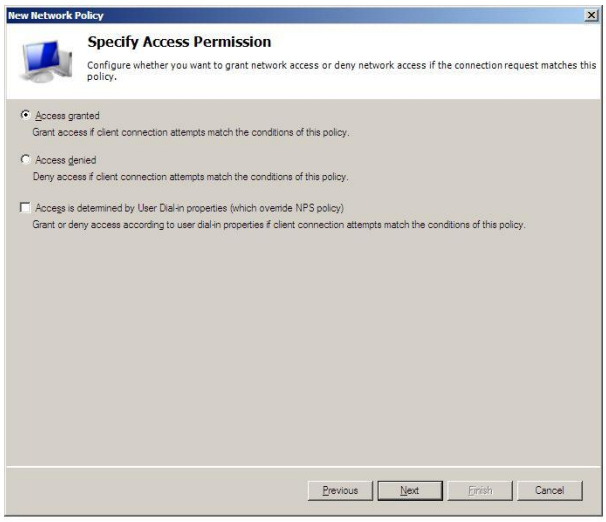
KUVIO 71. New Network Policy -ikkuna, käytännön nimeäminen

Määritellään Specify Network Policy Name and Connection Type -ikkunassa käytännölle nimi Health_tarkistus ja klikataan Next. Lisätään Specify Conditions -ikkunassa uusi määritelmä klikkaamalla Add. Kaksoisklikataan Select Condition -ikkunassa Network Access -kohdasta Health Policies. Valitaan avautuvassa Health Policies ikkunan pudotusvalikosta edellä konfiguroitu Tietoturvapolicy ja hyväksytään valinta klikkaamalla OK (kuvio 72).



KUVIO 72. Verkkokäytännön ehtojen määrittely

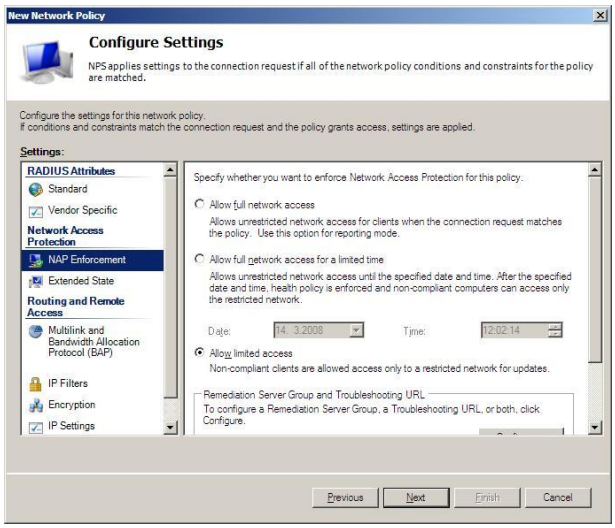
Siirrytään Specify Conditions -ikkunasta Specify Access Permissions -ikkunaan klikkaamaalla Next. Valitaan Specify Acccess Permissions -ikkunasta valinta Access granted (kuvio 73).



KUVIO 73. Access granted

Jatketaan Specify Access Permissions -valinnan jälkeen konfiguraatiota klikkaamalla Next kolme kertaa, koska autentikointiin liittyvät määritykset on tehty aiemmin yhteyspyyntökäytännön konfiguroimisen yhteydessä.

Valitaan Configure Settings -ikkunan vasemmasta paneelista NAP Enforcement ja valitaan avautuvasta oikeasta paneelista Allow limited Access (kuvio 74).



KUVIO 74. NAP Enforcements -asetus

Jätetään NAP Enforcements -kohdasta rasti Enable auto-remediation of client computers -ruudusta tässä vaiheessa pois, jotta jatkossa suoritettavassa testissä nähdään toimenpiteet epäsopivaa työasemaa kohtaan ilman pakotettua työaseman asetusten konfigurointia. Klikataan Next, kunnes käytäntö lopulta voidaan hyväksyä klikkaamalla Finish.

Testiympäristö on nyt saatu kokonaisuudessaan valmiiksi, eli kaikki kolme testiympäristön tietokonetta ja langaton tukiasema on konfiguroitu. Active Directory -toimialuepalvelin, DNS-palvelin, DHCP-palvelin ja Enterprise Root CA -palvelin ovat toiminnassa SHIRE.LOCAL -toimialueella ja testikäyttäjä sekä työasema on lisätty toimialueelle. Myös sekä NPS-palvelin, että testauksessa käytettävä kannettava työasema on liitetty SHIRE.LOCAL -toimialueelle. NPS-palvelimen yhteyspyyntökäytännön avulla RADIUS-asiakas välittää NAP-yhteensopivaksi konfiguroidun työaseman autentikointipyynnöt RADIUS-palvelimena toimivalle NPS-palvelimelle joten käyttäjä pystyy kirjautumaan toimialueelle.

NPS-palvelimessa on määritelty System Health Validator -vaatimukset jotka on liitetty Tietoturvapolicy-nimiseen kuntokäytäntöön. Tietoturvapolicy-kuntokäytäntö on otettu käyttöön Health_tarkistus-nimisen verkkokäytännön ehtona. Ehdon perusteella NAP-toiminto rajoittaa ehdot täyttävät eli epäsopivat asiakastyöasemat rajoitettuun verkkoon.

5.8 Suoritetut testit

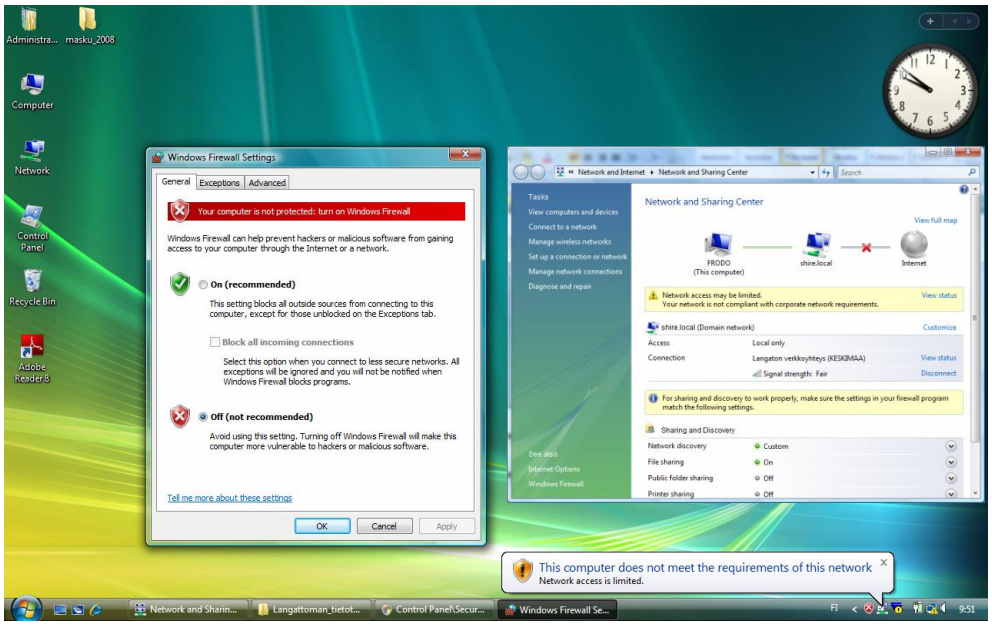
5.8.1 NAP-käyttöönotto ja testaus

Ensimmäinen suoritettava testi testasi NAP-järjestelmän toimintaa yleensä, eli pystyttiinkö määrittelemään rajoituksia verkkoon liittymiselle käyttäen Microsoft Windows Server 2008:n uusia ominaisuuksia. Testissä käytettiin edellä luotua Health_tarkistus -nimistä verkkokäytäntöä. Mikäli asiakastyöasema läpäisi SHV:ssä määritellyt vaatimukset (palomuuri ja automaattiset päivitykset käytössä) myönnettiin työasemalle täysi pääsy verkkoon (Full access). Mikäli jompikumpi ehdoista (tai molemmat ehdot) eivät täyttyneet, rajoitti NAP-toiminto työaseman pääsyä verkkoon. Testissä ei määritelty mitään erillistä verkon rajoitusta, vaan tyydyttiin siihen, että autentikointipalvelin ilmoitti rajoitetusta verkosta asiakkaan kohdalla sekä työasema ilmoitti käyttäjälle verkon rajoituksesta ja siihen liittyvästä syystä.

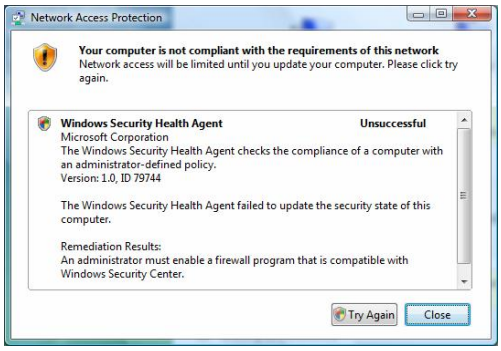
Testauksen toisessa testissä otettiin käyttöön automaattinen Remediation-toiminto ja testattiin toimiko järjestelmän automaattinen konfigurointi kun työaseman palomuuri tai automaattiset päivitykset poistettiin käytöstä.

Yllä esiteltyjen konfiguraatioiden ja autentikoinnin testaus suoritettiin yhdistämällä työasema KESKIMAA-verkkoon käyttäen toimialueen Administrator-käyttäjätiliä. Administrator-tili lisättiin WirelessUsers-ryhmään ja lisäksi tilille annettiin Remote Access Permissions oikeudet. Administrator-tiliä käytettiin, koska testeissä vaadittiin tietoturvakeskuksen konfigurointia johon testejä varten luodulla Bilbo-käyttäjällä ei ollut oikeuksia. Bilbo-käyttäjää käytettiin jatkossa järjestelmän käytettävyyden testaukseen toistuvien järjestelmään kirjautumisten yhteydessä tutkittaessa järjestelmän toimintaa.

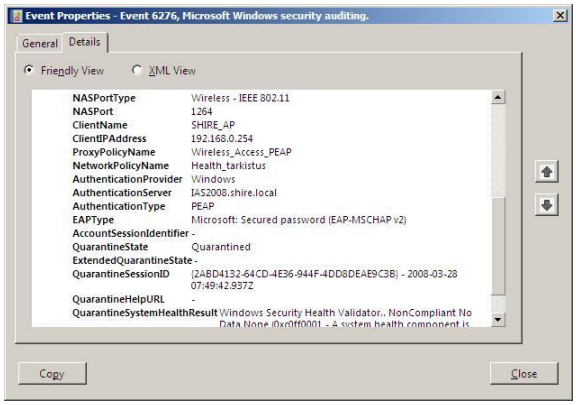
Testauksen aluksi tarkistettiin ping-komennolla, että työasema on yhdistetty verkkoon ja varmistettiin, että työasemalle asetetut palomuuriohjelmistot on poistettu käytöstä. Varmistuksen jälkeen järjestelmän palomuuri poistettiin käytöstä klikkaamalla Start, Control Panel, Security, Windows Firewall, Change Settings ja valittiin Off (not recommended) ja klikattiin Apply. Järjestelmän Windows Security Health Agent huomasi välittömästi kuntovaatimusten vastaisen palomuuriasetuksen (kuvio 75), ja antoi työaseman ilmaisinalueelle ilmoituksen lähiverkon järjestelmän vastaisista asetuksista (kuvio 76) ja siirsi työaseman karanteeniin rajoittaen verkon käyttöä (kuvio 77



KUVIO 75. Työaseman työpöytä kun Windows palomuuri on otettu pois käytöstä

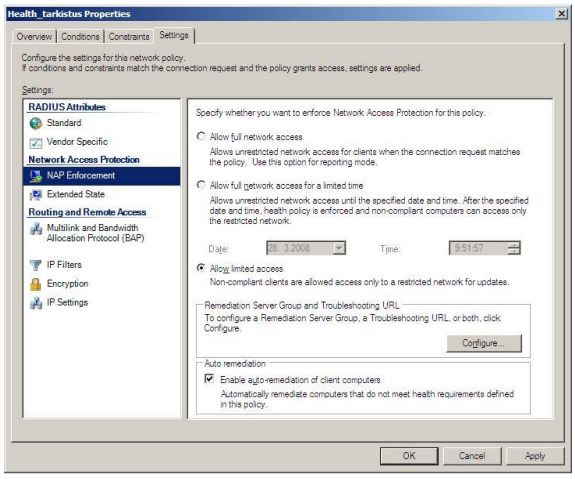


KUVIO 76. Windows Security Health Agentin ilmoitus



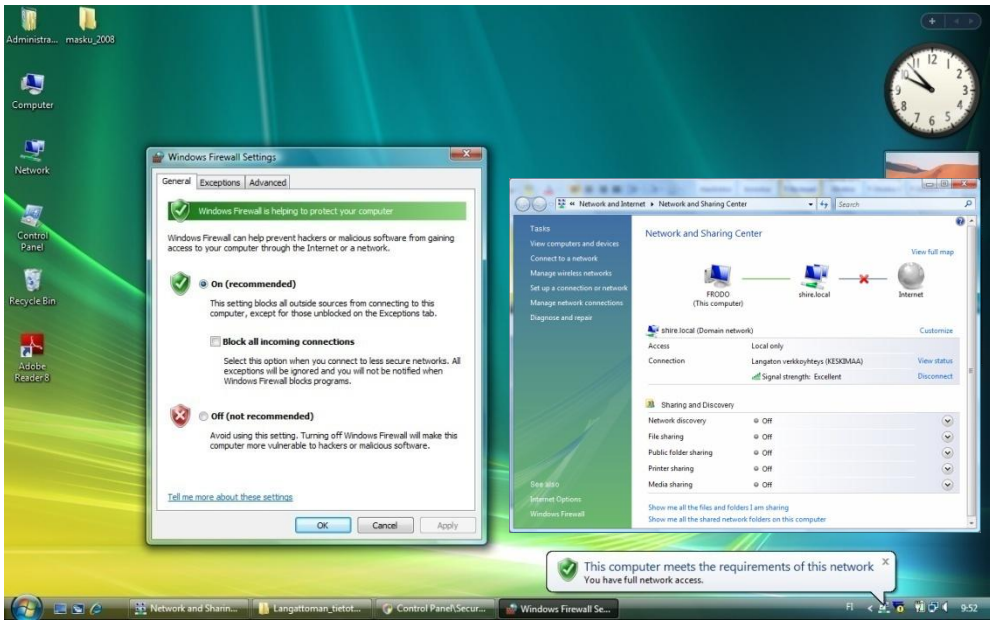
KUVIO 77. NPS-palvelimen Event Viewer, Event Properties

Tämän jälkeen otettiin käyttöön Auto remediation -toiminto NPS-palvelimen Health_tarkistus-verkkokäytännön Settings välilehdeltä valitsemalla Auto remediation -valinta (kuvio 78).

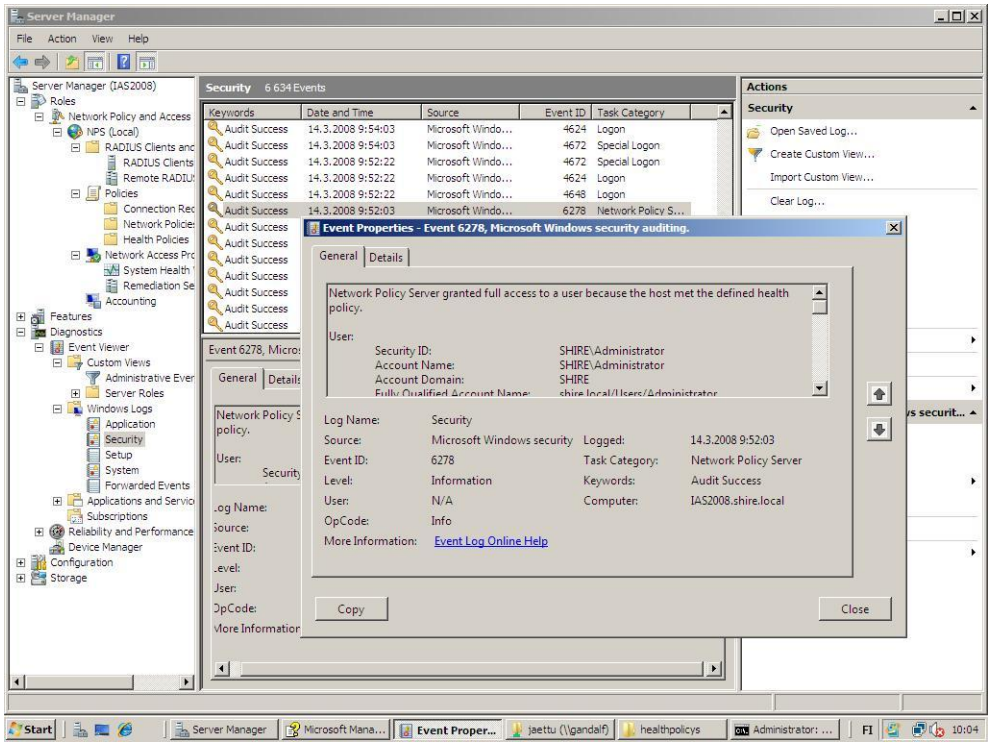


KUVIO 78. Auto remediation käyttöön.

Auto remediation käynnistää järjestelmän palomuurin ja poistaa verkon rajoitukset (kuvio 79 ja kuvio 80).



KUVIO 79. Työaseman työpöytä kun Auto remediation on otettu käyttöön



KUVIO 80. NPS-palvelimen Event Viewer, Event Properties

5.8.2 Testien tulokset

Testit onnistuivat odotusten mukaan ja kaikki toimi niin kuin pitikin. Konfiguroitu NPS-palvelin oli käynnissä lähes kahden kuukauden ajan ja palvelimen lokitiedostoissa ei ollut virheilmoituksia sen jälkeen kun konfiguraatio oli saatu toimivaksi. Kuluneiden kahden kuukauden aikana järjestelmään kirjauduttiin Bilbo-

käyttäjätunnuksella toistuvasti työaseman eri asetuksilla ilman ongelmia. Bilbo-käyttäjätunnuksella testattiin AD:n perustoimintoja, kuten salasanan vaihtoa, salasanan resetointia ja jaettujen resurssien jakamista käyttäjille lisäten Bilbo-käyttäjä eri domain local -ryhmiin, joille annettiin eri resursseille erilaisia oikeuksia. Mitään oleellista eroa verrattuna langattomaan kirjautumiseen ei peruskäytössä ilmennyt.

Järjestelmä testattiin myös palomuurien käytöstä poistamisen ja verkon rajoittamisen jälkeen ottamalla käyttöön F-Secure Internet Security 2008 -tuotteen palomuuri. Työaseman tietoturvakeskus havaitsi palomuurin käynnistymisen ja välitti tiedon NPS-palvelimelle, joka poisti verkon rajoitukset odotusten mukaisesti. Myös automaattinen työaseman asetusten korjaus Auto-remediation -toiminnon käytössä ollessa toimi täysin moitteettomasti ja viiveettä käynnistäen suljetun Windows-palomuurin tai käytöstä poistetun automaattinen päivitys -toiminnon.

Työaseman ilmoitukset käyttäjälle sekä verkon rajoituksista epäsopivien asetusten johdosta, että rajoitusten poistamisesta vaikuttavat selkeiltä ja johdonmukaisilta. Myös NPS-palvelimen Event Viewerin lokitiedot olivat selkeitä lukea ja ymmärtää.

Aivan ongelmitta työn käytännön osuus ei kuitenkaan onnistunut. Aluksi järjestelmää testattiin TELEWELL-EA510v3 -tukiasemalla, jonka RADIUS-tunnistusta ei saatu toimimaan odotetulla tavalla edes ohjelmistopäivityksen jälkeen. Ongelmien jatkuessa tukiasema vaihdettiin Cisco 1200 -sarjan tukiasemaan. Vaihdon jälkeen ongelmat tukiaseman kanssa eivät enää toistuneet. Toistuvia ongelmia aiheutti NPS-palvelimen komentokehotteessa tarvittavan gpedit /force -käskyn toistuva unohtaminen konfigurointien ja testauksen aikana. Kyseisellä käskyllä pakotetaan NPS-palvelimen käytäntöihin tehdyt muutokset välittömästi voimaan. Käskyn käyttämisen unohtaminen johti välillä ylimääräisiin konfiguraatiotoimiin.

6 YHTEENVETO

Tässä opinnäytetyössä tutustuttiin langattoman verkon autentikointimenetelmiin, langattomia verkkoja koskeviin tietoturvauhkiin ja -hyökkäyksiin. Työn teoriaosassa esiteltiin IEEE 802.11-standardin mukaisen langattoman lähiverkon rakennetta ja toiminnan periaatteita, käsiteltiin eri turvallisuusratkaisuja ja käyttäjien luotettavaa autentikointia mahdollistavia menetelmiä. Turvallisuusratkaisuiden esittelyn jälkeen tutustuttiin niitä vastaan olemassa oleviin hyökkäyksiin.

Työn käytännön osuudessa toteutettiin Microsoft Windows Server 2008 -palvelinkäyttöjärjestelmän avulla turvallinen testiverkko, jossa käytettiin WEP-salausta dynaamisilla avaimilla ja 802.1X-pohjaista todentamismenetelmää asiakkaan tunnistamiseen palvelimen NPS (Network Policy Server) -roolia ja NAP (Network Access Protection) -toimintoa käyttäen.

Testausympäristö saatiin rakennettua suhteellisen helposti, vaikka valmistajan sivuilta ei vielä löytynyt dokumentaatiota 802.1X-tunnistusta käyttävälle langattomalle verkolle. Järjestelmän testaamisessa puolestaan keskityttiin järjestelmän toimintaan yleisesti eli järjestelmän ilmoitukseen rajoitetusta verkon käytöstä.

Työtä tehdessä eniten ajatuksia herättivät langattomien lähiverkkojen monet turvallisuusuhat ja eri suojaus- ja salausmenetelmien murtamisen helppous. Kuitenkin, on muistettava, että jo vähäisinkin langattoman verkon suojaus ja salaus on parempi kuin verkkoa ei suojaisi ollenkaan. Jo pelkkä WEP-salaus kaikista heikkouksistaan huolimatta toimii langattoman verkon lukkona, jonka murtaminen tai edes murtamisen yrittäminen katsotaan rikoslain 38 luvun 8 §:ssa edessä tietomurroksi. On lisäksi muistettava, että mitä tärkeämpää tietoa verkon työasemissa ja palvelimissa säilytetään, sitä vahvempi verkon suojauksen tulee olla. Työn käytännön osassa käytettyä IEEE802.1X-autentikointi pidetään jo suhteellisen turvallisena.

Opinnäytetyön lopputuloksena on toimiva ohjeistus turvallisen IEEE802.1X-autentikointia käyttävän langattoman verkon asentamisesta käyttäen Microsoft Windows Server 2008- ja Microsoft Windows Server 2003 -palvelinkäyttöjärjestelmiä. Ohjeistuksen avulla voidaan konfiguroida turvallinen langattomaan verkkoon kirjautuminen niille yrityksille, joilla on käytössä, tai jotka suunnittelevat Microsoft Windows Server 2003 tai 2008 toimialuepalvelimen käyttöönottoa. Mi-

käli toimialuepalvelinta tai tarvetta toimialuepalvelimen käyttöön ei yrityksellä ole, on tarjolla muitakin ratkaisuja kuten WPA- tai WPA2-tekniikan käyttö. Lisävaihtoehtona voidaan mainita avoimeen lähdekoodiin perustuva ilmainen FreeRADIUS-ohjelmisto. Kyseisen ohjelmiston konfigurointi toimivaksi autentikointijärjestelmäksi voi kuitenkin Linux-pohjaisena olla liian haastava tehtävä Windows-käyttöjärjestelmiin tottuneille henkilöille.

Käytetyn järjestelmän keskitetty käyttäjätietojen hallinta sekä vapaus tietohallintoa työllistävistä sertifikaattien asennuksista puoltaa järjestelmän käyttöä yritysmaailman autentikointipalvelinjärjestelmänä. Dynaaminen avainten hallinta vähentää avainhyökkäyksille altistumista helpottaen myös tietohallinnon työtä kun jokaiseen työasemaan ei tarvitse konfiguroida hankalia avaimia. Molemminpuolinen tunnistus auttaa varmistamaan sen, että työasemat kommunikoivat tunnettujen verkkojen kanssa. 802.1X:n tilalla voitaisiin yhtä hyvin käyttää salausmenetelmänä joko WPA- tai WPA2 -Enterprise -tekniikoita. Loppujen lopuksi mainittujen tekniikoiden käyttöönotossa, hallinnassa tai tietoturvan tasoissa ei ole mainittavampia eroavaisuuksia. Yrityksille, joilla ei ole varaa tai halua autentikointipalvelimien hankintaan ja ylläpitoon, voidaan suositella WPA- tai WPA2-Personal salausmenetelmien käyttöä.

Työssä toteutettua järjestelmä tullaan käyttämään koulutus- ja testausalustana, jonka avulla voi tutustua eri salaustekniikoiden ja autentikointimenetelmien käyttöön sekä Windows Server 2008 -palvelinkäyttöjärjestelmän tietoturvaa lisääviin elementteihin. Järjestelmää tullaan tulevaisuudessa kehittämään luomalla toimialueelle lisää käyttäjiä, tietokoneita, Domain local- ja global -ryhmiä sekä jaettuja resursseja. Edellä mainittujen avulle demonstroidaan yrityksen verkkoa, johon mahdollistetaan langaton kirjautuminen. Lisäksi tarkoituksena on lisätä käyttöön vierailijaverkko, joka mahdollistaa yrityksen mahdollisten vierailijoiden internetyhteydet omilla langattomilla päätelaitteillaan tarvittaessa niin, etteivät vierailijat pääse yrityksen verkkoon.

LÄHTEET

Aittoniemi, P & Nenonen V. 2003. Langattomat lähiverkot [Verkkojulkaisu]. Lappeenrannan teknillinen yliopisto. [viitattu 7.12.2007]. Saatavissa: http://www.it.lut.fi/kurssit/06-07/Ti5316800/tyot/langattomat_lahiverkot_pasi_aittoniemi_ja_ville_nenonen.pdf

Ahvenainen, M. 2003. Langattomien lähiverkkojen turvallisuus [Verkkojulkaisu]. Teknillinen korkeakoulu. [viitattu 14.12.2007]. Saatavissa: http://keskus.hut.fi/julkaisut/tyot/diplomityot/977/Ahvenainen.pdf

Dell. 2007. Yleistietoja suojauksesta [Online]. [viitattu 11.12.2007]. Saatavissa: http://support.dell.com/support/edocs/network/P94583/fin/security.htm

Hakala, M., Vainio, M. 2005. Tietoverkon raketaminen. Jyväskylä: Docendo.

Hakala, M., Vainio, M., Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Helin, A., Karttunen, J & Pitkänen, J. 2002. WLAN ja tietoturva [Verkkojulkaisu]. Turun kauppakorkeakoulu. [viitattu 7.12.2007]. Saatavissa: http://www.tukkk.fi/tjt/OPETUS/TJTS11/Arkisto/wlan.pdf

Hjelm, T. 2005. Lähiverkkosuunnitelma Tampereen vanhuspalveluyhdistys Ry:lle [Verkkojulkaisu]. Tampereen ammattikorkeakoulu. [viitattu 9.12.2007]. Saatavissa: https://oa.doria.fi/bitstream/handle/10024/5076/TMP.objres.55.pdf?sequence=1

Hämäläinen, M. 2007. WLAN ja logistiikka-ala [Verkkojulkaisu]. Helsingin ammattikorkeakoulu. [viitattu 14.3.2008]. Saatavissa: https://oa.doria.fi/bitstream/handle/10024/28169/stadia-1191323663-0.pdf?sequence=1

IEEE, 2008. IEEE 802.11TM - The Working Group for WLAN Standards [Verkkodokumentti]. [Viitattu 15.3.2008]. Saatavissa: http://www.ieee802.org/11/

Järvinen, P. (2002) Tietoturva ja yksityisyys. Jyväskylä: Docendo Finland Oy.

Korhonen, J., 2006. Tietoturvallisen langattoman lähiverkon toteutus hakemistopalveluun integroituna. [Verkkojulkaisu]. Lahden ammattikorkeakoulu. [viitattu 19.12.2007]. Saatavissa: http://oppari.phkk.fi/julkaisu/2007-04-27-02.pdf

Kortelainen, J. 2001. Tietoverkkojen tietoturva [Verkkojulkaisu]. Oulun yliopisto. [viitattu 11.12.2007]. Saatavissa: http://www.tol.oulu.fi/kurssit/TieVerTur/TvTtLuennot.pdf

Laakso, J. 2005. WLAN-verkkojen tutkiminen freeware ohjelmilla [Verkkojulkaisu].Savonia ammattikorkeakoulu. [viitattu 11.12.2007]. Saatavissa: http://wirelessplatform.savonia-amk.fi/index2.php?option=com_docman&task=doc_view&gid=12&Itemid=87

Lehtonen, S. 2004. Turvallisuuden hallinta yrityksen langattomissa lähiverkoissa [Verkkojulkaisu]. Teknillinen korkeakoulu. [viitattu 9.1.2008]. Saatavissa: http://www.tml.tkk.fi/Publications/Thesis/lehtonen.pdf

Lehtonen, S. 2007. Wireless LAN [Verkkojulkaisu]. Teknillinen korkeakoulu. [viitattu 12.12.2007]. Saatavissa: http://www.netlab.hut.fi/opetus/s38118/s00/tyot/27/wlan_tekniikka.shtml

Microsoft, 2008. Step-by-Step Guide: Demonstrate NAP 802.1X Enforcement in a Test Lab [Verkkojulkaisu]. Microsoft. [viitattu 15.3.2008]. Saatavissa: http://www.microsoft.com/downloads/details.aspx?familyid=8a0925ee-ee06-4dfb-bba2-07605eff0608&displaylang=en

Microsoft. 2008. Step-by-Step Guide for Setting Up Secure Wireless Access in a Test Lab [Verkkojulkaisu]. Microsoft. [viitattu 15.3.2008]. Saatavissa: http://www.microsoft.com/downloads/details.aspx?familyid=0f7fa9a2-e113-415b-b2a9-b6a3d64c48f5&displaylang=en

Microsoft Technet. 2008. Windows Server 2008 [Verkkojulkaisu]. Microsoft. [viitattu 15.3.2008]. Saatavissa: http://technet.microsoft.com/fi-fi/windowsserver/2008/default(en-us).aspx

MVnet. 2007. Langattoman verkon murtaminen [Verkkojulkaisu]. MVnet. [viitattu 9.12.2007]. Saatavissa: http://www.mvnet.fi/index.php?osio=Tietokoneet&sivu=Langattoman_verkon_murtaminen

Niemi, T. 2007. Langattomat ethernet-teknologiat ja niiden tietoturva [Verkkojulkaisu]. Helsingin ammattikorkeakoulu. [viitattu 6.2.2008]. Saatavissa: https://oa.doria.fi/bitstream/handle/10024/5699/stadia-1176898778-3.pdf?sequence=1

Puska, M. 2005. Langattomat lähiverkot. Jyväskylä: Talentum Media Oy.

Ruotsalainen, P. 2006. Radius-palvelin WLAN-verkossa [Verkkojulkaisu]. Savonia ammattikorkeakoulu, Kuopio. [viitattu 6.12.2007]. Saatavissa: http://wirelessplatform.savonia-amk.fi/index2.php?option=com_docman&task=doc_view&gid=15&Itemid=87

Seppälä, K. 2006. Turvallinen kirjautuminen yrityksen WLAN-verkkoon RADIUS-tunnistuksen avulla [Verkkojulkaisu]. Lahden ammattikorkeakoulu. [viitattu 9.1.2008]. Saatavissa: http://oppari.phkk.fi/julkaisu/2007-04-27-12.pdf

Seppänen, L. 2001. Langaton lähiverkko [Verkkojulkaisu].Hämeen ammattikorkeakoulu. [viitattu 12.12.2007]. Saatavissa: http://trade.hamk.fi/~lseppane/courses/wlan/doc/Materiaali.pdf

Taito Oulu 400. 2007. Tietoturva [Verkkojulkaisu]. Oulun kaupunki. [viitattu 7.12.2007]. Saatavissa: http://www.ouka.fi/taito/tietopaketit/teema1/dokut/tietoturva.htm

Thomas, T. 2005. Verkkojen tietoturva. Helsinki: Edita Prima Oy.

Tuominen, T. 2005. WLAN tietoturva [Verkkojulkaisu]. Tampereen amattikorkeakoulu. [viitattu 14.12.2007]. Saatavissa: https://oa.doria.fi/bitstream/handle/10024/5143/TMP.objres.226.pdf?sequence=1

Vesanen, A. 2003. Langattomien lähiverkkojen tietoturva [Verkkojulkaisu]. Oulun yliopisto. [viitattu 11.12.2007]. Saatavissa: http://www.tol.oulu.fi/~avesanen/Langaton_TT/

Vähä-Touru, T. 2007. Langattoman lähiverkon toteutus [Verkkojulkaisu]. Tampereen ammattikorkeakoulu. [viitattu 9.12.2007]. Saatavissa: https://oa.doria.fi/bitstream/handle/10024/5048/TMP.objres.1013.pdf?sequence=1

Wilkman, T. 2006. Tietoturvallinen WLAN – CASE: Oy Information Chain Management Finland Ltd [Verkkojulkaisu]. Tampereen ammattikorkeakoulu. [viitattu 6.2.2008]. Saatavissa: https://oa.doria.fi/bitstream/handle/10024/5022/TMP.objres.854.pdf?sequence=