Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Victoria Vorobieva

Opinnäytetyö

Network Access Protection ja sen implementoiminen WPK-verkkoon

Työnohjaaja: Harri Hakonen
Tampere 10/10

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

Tekijän nimi	Victoria Vorobieva
Työn nimi	Network Access Protection ja sen implementoiminen WPK-verkkoon
Sivumäärä	69
Valmistumisaika	Joulukuu 2010
Työn ohjaaja	Harri Hakonen

Tiivistelmä

Opinnäytetyön tavoitteena on suunnitella ja toteuttaa Network Access Protection -palvelu verkkoon. NAP-suojauksella estetään saastuneiden työasemien pääsyä tuotantoverkkoon. NAP-tekniikkaa voidaan ottaa käyttöön sekä langallisissa että langattomissa verkoissa, toimintaperiaate on sama. Työssäni toteutin langallisesti toimivan NAP-suojauksen.

Tein työn toimeksiantona Tampereen ammattikorkeakoulun opiskelijoiden rakentamaan ja kehittämään WPK-nimiseen verkkoon.

Työn teoriaosuus käsittelee verkon pääsynvalvontaa, sen osa-alueita ja toteutustapoja, myös NAP-suojauksen perusteita ja toimintaperiaatetta. Käytännön osuudessa käyn läpi ympäristön rakentamisen vaihe vaiheelta.

Työn tuloksena sain konfiguroitua toimivan ympäristön. Tämä opinnäytetyö voi toimia ohjeistuksena samankaltaisen ympäristön rakentamiseen.

Avainsanat: verkon pääsynvalvonta, Windows Server 2008, porttikohtainen autentikointi

Tampere University of Applied Sciences
Information technologies

Author	Victoria Vorobieva
Name of thesis	Network Access Protection and its Implementation into WPK-Network
Number of pages	69
Date	December 2010
Thesis supervisor	Harri Hakonen

Abstract

The purpose of this thesis is to design and implement Network Access Protection services into network. Network Access Protection prevents infected computers from signing into backbone network. NAP technique can be used with or without wires, the principle is the same. In this work wired Network Access Protection services were implemented.

This thesis was carried out as an assignment to Tampere University of Applied Sciences. NAP was implemented into WPK-Network, which is developed and administered by students of the university.

The theory section of this thesis tells about network access, its areas and implementing types, also the basics of NAP and its working principles. In the practice section building an NAP environment step by step is described.

As a result of my thesis, I created a working environment. This thesis can be used as a manual for constructing similar environments.

Keywords: Network access, Windows Server 2008, port-based authentication

Sisällysluettelo

Johdanto

Aiheen opinnäytetyöhöni sain Tampereen ammattikorkeakoulun lehtori Harri Hakoselta. Aihe liittyy Windows Server 2008 mukana tulleen NAP-palvelun suunnitteluun ja käyttöönottoon.

Tutkimuksen lähtökohtana on WPK-verkossa syntynyt tarve NAP-suojauksen implementoimiselle. Tutkimusstrategiana käytän tapaustutkimusta laadullisin menetelmin toteutettuna, tutkimustietoa hankin dokumentteja ja artikkeleita tutkien.

Opinnäytetyön tarkoituksena on suunnitella ja toteuttaa Network Access Protection -palvelu, jolla toteutetaan WPK-verkkoon liitettävien työasemien todennus. NAP:n avulla varmistetaan, että kaikki verkkoon kytkettävät koneet ovat tietoturvaltaan ajan tasalla ja vastaavat asetettuja tietoturvavaatimuksia.

Henkilökohtaisena tavoitteenani on perehtyä palvelun ominaisuuksiin, asennukseen, käyttöön ja siihen liittyviin ongelmiin. Työni teoriaosuudessa kerron verkon pääsynvalvontakäsitteestä, -ominaisuuksista ja -toteutustavoista.

1 Nykytilanne ja verkon pääsynvalvonnan tarve

Tietoverkkojen kehitys on tuonut mukanaan uudenlaisia tietoturvariskejä. Nykyään verkkojen kytkentätavat ovat muuttuneet merkittävästi. Useat eri tahot eri puolilta maapalloa voivat olla kytkettyjä toisiinsa verkkojen avulla, minkä seurauksena verkon sisältämän tiedon luonne ja haavoittuvuus ovat laajentuneet.

Työntekijöiden pääsy yritysverkkoihin omilta työasemilta on yleistynyt. Käyttäjät voivat kytkeytyä verkkoon käyttäen kannettavia tietokoneita, puhelimia, pda-laitteita tai muita langattomia laitteita. Vaikka yritysverkon ulkorajat olisivat suojattu virustorjunnalla ja palomuureilla, sisäverkkoon tuotu saastunut työasema on suuri tietoturvauhka. Koneen verkkoon liittämisen ja sen keskitetysti hoidettavan päivittymisen välille syntyy haavoittuvuusikkuna, joka voi kestää useita tunteja tai päiviä. Näin ollen tietoverkkojen turvallisuudesta on muodostunut verkon ylläpitäjille keskeinen haaste. (Tietokone.fi, 2007.)

Verkon pääsynvalvonnalla yritys voi varmistaa, että sisäverkkoon pääsevät vain riittävän terveydentilan omaavat työasemat. Tietoturvapolitiikka määrittelee verkkoon kytkettävän koneen terveydentilan mm. seuraavilta osin: koneen virustorjuntaohjelmisto on ajan tasalla, kaikki kriittiset ohjelmapaikkaukset ovat asennettuna, kone on vapaa viruksista ja haittaohjelmista. (Tietokone.fi, 2007.)

2 Verkon pääsynvalvonta

Verkon pääsynvalvonnalla (Network Access Control, NAC) tarkoitetaan kaikkia toimintoja ja menettelyjä, joiden avulla suoritetaan päätelaitteiden tai järjestelmien tunnistaminen ja varmistetaan, että verkkoon käsiksi pääsevät vain oikeuden omaavat tahot. Toisin sanoen, NAC valvoo laitteiden pääsyä verkkoon ryhmäkäytäntöjen avulla. (Wikipedia.org 1, 2009.)

2.1 Ominaisuudet

Verkon pääsynvalvonnan tärkeimmät ominaisuudet ovat nollapäivähyökkäysten vähentäminen, ryhmäkäytäntöjen täytäntöönpano, identiteetin ja pääsyn hallinta.

Nollapäivähyökkäykset kuuluvat haasteellisimpiin tietoturvariskeihin. Nollapäivähyökkäyksissä käytetään hyväksi julkistamattomia tai uusia haavoittuvuuksia, joihin ei vielä ole saatavilla ohjelmapäivityksiä. Näiden paikkaamattomien aukkojen läpi rikolliset voivat päästää haittaohjelmia. Nykyajan verkon pääsynvalvonnan ohjelmistot ennaltaehkäisevät nollapäivähyökkäyksiä valvomalla työasemilta lähtevää verkkoliikennettä myös asemien verkkoon liittämisen jälkeen. Epäilyttävän verkkoliikenteen havaittuaan (esimerkiksi portti- ja osoiteskannaukset sekä DoS- ja DDoS-hyökkäykset) saastunut asema pakotetaan karanteeniin. (Guardsite.com.)

Verkon pääsynvalvonnan tehtävä on estää luvattomien käyttäjien tai saastuneiden laitteiden kirjautuminen verkkoon. Yrityksissä eri tietokoneita käytetään eri tarkoituksiin, tietoturvasyistä on tärkeää, ettei esimerkiksi sähköpostin katseluun tarkoitetulla työasemalla olisi pääsyä yrityksen tietokantoihin tai muuhun luottamukselliseen aineistoon. Myös verkossa olevien laitteiden päivitykset halutaan pitää ajan tasalla ja palomuurit aktiivisena. Ratkaisuna tähän on verkkoon pyrkivien laitteiden terveydentilan tarkistus tietoturvapolitiikkojen avulla. Tietoturvapolitiikkasäännöstö määrittelee keneltä tai miltä laitteelta, milloin, miten

ja millä oikeuksilla pääsy verkkoon tai tiedostoihin sallitaan, sekä mahdollistaa työasemapäivityksien ajastamisen. (Networkworld.com, 2007.)

Verkon pääsynvalvonnan ratkaisut toimivat kahdella periaatteella riippuen siitä, laitetaanko politiikat täytäntöön työasemien verkkoon liitämistä ennen (Pre-admission) vai sen jälkeen (Post-admission).

Pre-admission-tilassa työasemien terveydentilaa tarkistetaan ennen kuin työasemille annetaan pääsy verkkoon. Näin vältetään verkkoon pääsy asemilta, joiden virustorjuntaohjelmisto ei ole ajan tasalla tai muut tietoturva-asetukset eivät vastaa yrityksen tietoturvapolitiikkaa. Post-admission-tilassa valvotaan käyttäjien verkkoliikennettä ja käyttäytymistä verkossa niiden liityttyä verkkoon. (Networkcomputing.com.)

Verkon pääsynvalvonnan ratkaisut voivat toimia linjalla (inline) tai sivussa (out-of-band). Linjalla toimivat ovat sijoitettu verkkoon pyrkivän päätelaitteen ja itse verkon väliin. Tällaisen rakenteen etu on siinä, että saadaan tarkistettua kaikkea työasemalta verkkoon ja takaisin kulkevaa liikennettä. Sivussa toimivat eivät vaadi rakennemuutoksia verkkoon, vaan hallitsevat verkon pääsynvalvonnan laitteita keskitetystä hallintapisteestä. (Networkcomputing.com.)

2.2 Pääsynvalvonnan menetelmät

Pääsynvalvonnan menetelmillä rajoitetaan verkkoympäristön käyttöä. Perinteisiä pääsynvalvonnan menetelmiä ovat roolipohjainen, sääntöpohjainen, pakollinen ja harkinnanvarainen. Tietolähteenä tässä osiossa olen käyttänyt Barrettin, Weissin ja Hausmanin kirjaa ”Security+. Exam Cram”. Kirja on tarkoitettu valmentamaan tietoturva-ammattilaisia Security+-sertifikaattitutkinnon suorittamiseen. Kirjassa käsitellään pääsynvalvontaa, autentikointia, kryptografiaa ja muita tietoturvaan liittyviä aiheita.

2.2.1 Roolipohjainen

Roolipohjaisessa pääsynvalvonnassa (Role-based Access Control, RBAC) käyttöoikeudet verkon resursseihin perustuvat rooleihin. Tavallisesti roolit vastaavat organisaation toimenkuvia. Roolit voivat olla ”sihteeri”, ”myyntipäällikkö”, ”palkanlaskija”. Roolien oikeudet kohdistuvat yleensä ei itse tiedostoihin vaan siihen mitä toimintoja tiedostoille voidaan tehdä. Roolipohjainen pääsynvalvonta vähentää verkon ylläpitoa, sillä työntekijän toimenkuvan vaihtuessa on helppoa vaihtaa rooli toiseen sen sijaan, että kävisi läpi joka tiedoston käyttöoikeusmäärittelyn. (Informit.com, 2007.)

2.2.2 Sääntöpohjainen

Sääntöpohjaisessa pääsynvalvonnassa (Rule-based Access Control, RBAC) järjestelmän ylläpitäjä luo sääntöjä ja vaatimuksia, joita käyttäjän tulee täyttää päästäkseen käsiksi haluamaansa tietoon tai suorittaakseen haluamansa toimenpiteen. Sääntöpohjaisen pääsynvalvonnan avulla voidaan vaikuttaa laajasti siihen mitä käyttäjä on oikeutettu tehdä järjestelmässä. Esimerkiksi voidaan myöntää luku-, kirjoitus- tai muokkausoikeus tiettyyn tiedostoon riippuen käyttäjätilistä, siitä mihin ryhmään käyttäjä kuuluu tai mihin aikaan vuorokaudesta käyttäjä yrittää tiedostoa avata. (Barrett & Weiss & Hausman, 26, 2003.)

2.2.3 Pakollinen

Pakollista pääsynvalvontaa (Mandatory Access Control, MAC) käytetään korkean tietoturvallisuustason järjestelmissä, kuten hallinto- ja sotilastietojärjestelmät. Tämän tyyppisissä ratkaisuissa käyttöoikeusmäärittely tapahtuu järjestelmän tasolla, eikä käyttäjä edes tiedoston omistajana voi myöntää siihen oikeuksia. Tällä varmistetaan, etteivät käyttäjän huoli-

mattomuudestakaan korkean turvallisuusluokan tietoihin pääsisi sellaiset käyttäjät, jotka eivät niihin ole oikeutettuja. (Barrett & Weiss & Hausman, 26, 2003.)

Pakollisen pääsynvalvonnan järjestelmässä kaikki tieto ja käyttäjät lajitellaan eri turvallisuusluokkiin, jotta käyttöoikeudet tiedostoon voitaisiin myöntää, käyttäjän täytyy kuulua ylempään tai vähintään saman tason tietoturvallisuusluokkaan kuin itse tiedostokin. Turvallisuusluokat jakautuvat myös kategorioihin, jotka voivat vastata yrityksen johtoportaita, osastoja ja eri projekteja. Näin ollen vaikka käyttäjä kuuluisi oman osastonsa huippusalaiseen tietoturvallisuusluokkaan, pääsyä toisen osaston tiedostoihin hän ei saa. (Barrett & Weiss & Hausman, 26, 2003.)

2.2.4 Harkinnanvarainen

Harkinnanvaraisessa pääsynvalvonnassa (Discretionary Access Control, DAC) tiedostojen omistaja myöntää tiedostoon kohdistuvat käyttöoikeudet ja päättää mitä toimintoja tiedostolle käyttöoikeuden saavat käyttäjät voivat suorittaa. Harkinnanvarainen pääsynvalvonta on riskialtista varsinkin, kun kyseessä on luottamuksellinen ja salainen tieto. (Barrett & Weiss & Hausman, 26, 2003.)

2.3 Agentilla vai ilman

Valitessa verkon pääsynvalvontaohjelmistoa yritys voi päätyä kahteen ratkaisuun: agentittomaan tai agentilliseen ohjelmistoon riippuen lopullisen ratkaisun kustannus-, turvallisuus- ja toiminnallisuustasosta.

Agentillinen ohjelmisto vaatii agenttiohjelman asennuksen verkon jokaiselle päätelaitteelle. Agentti voi lukea työaseman laitteiston ja asennetun ohjelmiston versionumerot, konfigu-

raatiotiedostot ja muuta spesifistä tietoa. Kerätyn tiedon agentti toimittaa keskuspalvelimelle, joka varmistaa täyttääkö työasema yrityksen tietoturvapolitiikan asetetun turvallisuustason. (Tlcitgroup.com.au, 2006.)

Agenttipohjaisten ohjelmistojen edut ovat:

- Vähentävät käyttäjätuen kuormitusta, sillä agenttien avulla voi automatisoida monia tehtäviä, kuten käyttäjätiedotus, raportointi, käyttäjien ohjeistus, koneiden päivittäminen.
- Käyttöönotto- ja ylläpitokustannukset ovat pienempiä.
- Ei turhia sisäänkirjautumisia. Agenttipohjainen pääsynvalvonta ei vaadi tilin luomista päätelaitteelle eikä porttien jättämistä suojaamattomiksi.
- Vierastunnuksella kirjautuvien asemien perusteellinen tarkistus web-agentteja käyttäen.
- Päätelaitteiden syvempi terveydentilan tarkistus. Agenttiohjelmat reagoivat kaikkiin laitteella tapahtuviin konfiguraatiomuutoksiin, silloinkin kun työasema ei ole kirjautuneena verkkoon.
- Karanteenijärjestelmä saastuneita työasemia varten. (Tlcitgroup.com.au, 2006.)

Agentittomat verkon pääsynvalvonnan ratkaisut verkkoon pyrkivien asemien turvallisuustarkistusta varten voivat käyttää muita teknologioita kuten:

- Probe-pakettien lähettäminen. Probe-viesteillä etsitään verkkoon kirjautuneita päätelaitteita ja saadaan selville mitä palveluita laitteet tarjoavat, mikä käyttöjärjestelmä on asennettu koneisiin ja muita ominaisuuksia. Probe-viestit eivät tutki koneelle asennettuja ohjelmistoja, eivätkä koneella pyöriviä prosesseja, joten verkkoon kirjautumisen jälkeen saatuja virustartuntoja ei pystytä paljastamaan.
- Etäkäyttö (Remote login). Toimivat vain Windows-pohjaisten järjestelmien kanssa, joissa päätelaitteelle kirjautuminen tapahtuu WMI:n avulla (Windows Management Instrumentation). Tätä teknologiaa käyttävät ohjelmistot lukevat päätelaitteiden rekisteriä ja konfiguraatiotiedostoja.

- Verkon tietoliikenteen monitorointi reaaliajassa (Inline scanning). Sovellukset eivät ota kantaa pääteasemien ohjelmistoon, konfiguraatiotiedostoihin eivätkä prosesseihin. Ne huomaavat vain tunnetut verkon väärinkäyttäjät, jotka lisäävät verkkoliikennettä, mutta eivät haavoittuvuuksia. (Tlcitgroup.com.au, 2006.)

2.4 Korjaavia toimenpiteitä

Verkon pääsynvalvonta ei vain estä saastunutta työasemaa kirjautumasta verkkoon, vaan tarjoaa myös mekanismit työaseman päivittämiseksi määrätylle turvallisuustasolle. Tällaisia mekanismeja ovat karanteeniverkot ja captive-portaalit.

Karanteeniverkko on tuotantoverkosta eristetty verkko, johon sijoitetaan epäilyttäviksi tai saastuneiksi turvallisuustarkistuksessa osoittautuneet koneet. Työasemat voidaan ohjata karanteeniverkkoon OSI-mallin siirtoyhteyskerroksella eristämällä saastunut asema kokonaan pois verkosta tai verkkokerroksella antamalla asemalle IP-osoite karanteeniverkosta. (Tietokone.fi, 2007.)

Karanteenijärjestelmä muodostuu neljästä vaiheesta: tarkastus, eristys, korjaavat toimenpiteet ja kumoaminen.

Tarkastusvaiheessa työasemalle asennettu agenttiohjelma tutkii aseman turvallisuustasoa ja raportoi tiedot karanteenipolitiikasta vastaavalle palvelimelle. Kun agentin asentaminen päätelaitteelle ei ole hyödynnettävissä, käytetään muita ratkaisuja, jotka eivät vaadi agenttien asentamista. Tarkastuksen aikana selvitetään, ovatko kriittiset turvallisuuspaikkaukset asennettu, ovatko virustorjuntaohjelmiston tietokannat ajan tasalla, ovatko tietoturvapolitiikan vaadittavat sovellukset asennettu ja onko asemalle asennettu laitonta ohjelmistoa. (Nec.co.jp, 2007.)

Eristysvaiheessa työasemat, jotka eivät vastanneet määriteltyjä pääsyvaatimuksia, eristetään tuotantoverkosta ja laitetaan karanteeniverkkoon. Karanteeniverkon toteuttamiseen on useita tapoja. Se voi olla esimerkiksi oma virtuaaliverkko eli VLAN, johon voidaan sijoittaa myös päivityksiä hoitavia palvelimia. Vaihtoehtoisesti asema voidaan ohjata vierasverkkoon, josta on pääsy vain Internetiin. (Nec.co.jp, 2007.)

Korjaavien toimenpiteiden avulla päivitetään (automaattisesti tai manuaalisesti) eristetyt työasemat tietoturvapolitiikan vaatimalle tasolle. Tässä vaiheessa asemille ajetaan virustorjuntaohjelmiston päivitykset, asennetaan ohjelmapaikkauksia ja poistetaan laiton ohjelmisto.(Nec.co.jp, 2007.)

Kumoamisvaiheessa suoritetun päivittämisen jälkeen työasema käynnistetään uudelleen ja ohjataan tuotantoverkkoon.(Nec.co.jp, 2007.)

Karanteeniverkkoon toteuttamiseen on useita tapoja. Yasutome, Adachi ja Yoshida artikkelissaan (Nec.co.jp, 2007.) luokittelevat viiteen eri metodiin:

- Virtuaaliverkot. Virtuaaliverkkoja tukevan kytkimen avulla karanteeniverkosta ja tuotantoverkosta tehdään omat virtuaaliverkot. Verkkoon pääsyä anova työasema käy läpi IEEE 802.1x- tai DHCP-todennuksen. Todennuksen onnistuessa työasema saa IP-osoitteen tuotantoverkosta ja epäonnistuessa karanteeniverkosta.
- Yhdyskäytävä palomuurina. Karanteeniverkko eristetään tuotantoverkosta yhdyskäytävällä. Tämä metodi sopii verkkoon, jossa käytetään kiinteitä IP-osoitteita.
- Työaseman oma palomuuri. Verkko, johon työasema kytkeytyy, riippuu työasemalle asennetun palomuurin suodatuksen tuloksista. Metodi vaatii agenttiohjelman asennuksen koneelle.
- Palvelimen palomuuri. Sovelluspalvelimelle asennettu palomuuri suodattaa verkkoliikennettä. Pääsyn sovelluspalvelimelle saavat vain riittävän terveydentilan omaavat työasemat. Tätä tapaa käytetään palvelimien suojaamiseksi, sillä työasemilta estetään pääsy vain palvelimelle, pääsyä muualle verkkoon ei kielletä.

- Etäkäyttö. Tämä ratkaisu käyttää kytkintä, joka mahdollistaa pääsyn tuotantoverkkoon ulkoa. Etäyhteydellä verkkoon pyrkivien päätelaitteiden terveydentilan tarkistukseen on omat politiikat, minkä takia voidaan tarvita kahta eri karanteeniverkkoa: yksi etäkäyttäjiä varten ja toinen muita laitteita varten.

Toinen tapa tuotantoverkosta estettyjen työasemien päivittämiselle on Captive-portaalit. Captive- portaali on tekniikka, jonka avulla käyttäjät ohjataan tietylle web-sivulle, jossa niille tarjotaan ohjeistusta ja työkaluja koneensa päivittämiseen vaadittavalle turvallisuustasolle. Kaikki muu verkkoliikenne koneelta on kiellettyä, kunnes kone läpäisee tietoturvatarkastuksen. (Personaltelco.net.)

3 Todentava ympäristö

Pääsynvalvontaa toimeenpannaan todentamismenetelmien avulla. Jyväskylän yliopiston tietohallintokeskus (jyu.fi) määrittelee todentamisen (authentication) seuraavasti: ”käyttäjän tai palvelun identiteetin varmistaminen”.

Todentaminen voi perustua kolmeen periaatteeseen:

- Siihen mitä käyttäjä tietää. Käyttäjä tietää käyttäjänimensä ja salasanansa. Joissakin palveluissa todentamisessa voidaan kysyä muuta tietoa, esimerkiksi sosiaaliturvatunnuksen loppuosaa, käyttäjän äidin tyttönimeä, syntymäpäivää tai mitä tahansa muuta informaatiota, jonka käyttäjä tietää.
- Siihen mitä käyttäjällä on. Äly-, sirukortti tai tietokone (tietokoneen MAC-osoite).
- Siihen mikä käyttäjä on. Tähän ryhmään kuuluvat käyttäjän biometriset ominaisuudet, kuten sormenjäljet tai silmän verkkokalvo. (Stamp, 154, 2006.).

Autentikointiin liittyy tiivisti valtuutus (authorization). Valtuutuksella käyttäjille annetaan pääsy niihin resursseihin ja palveluihin, joihin he ovat oikeutettuja. (Techtarget.com.)

Suojatun verkkoon pääsyn mahdollistamiseksi tarvitaan todentava ympäristö. Windows-verkoissa todentavaan ympäristöön kuuluvat: aktiivihakemisto (Active Directory, AD), ryhmäpolitiikat (Group Policy), RADIUS-protokolla (Remote Authentication Dial In User Service) ja julkisen avaimen järjestelmä (Public Key Infrastructure, PKI). Ympäristön lopullinen rakenne muodostuu sen perusteella mitä tapoja verkkoon liittymiseen on käytössä.

Todentavan ympäristön toteutus jää tämän työn rajauksen ulkopuolelle. Network Access Protection käyttää toiminnassaan WPK-verkkoon jo valmiiksi asennettua todentavaa ympäristöä, jota muokataan tämän projektin tarpeiden mukaisesti.

3.1 Aktiivihakemistopalvelu

Aktiivihakemisto (Active Directory, AD) on käyttäjätietokanta ja hakemistopalvelu, joka sisältää tiedot käyttäjistä, tietokoneista ja muista verkon elementeistä. Aktiivihakemisto toimii objektien keskitettynä hallintapisteenä. (Msdn.microsoft.com, 2009.)

Aktiivihakemistopalvelu kuuluu osana Windows Server 2000 ja Windows Server 2003 käyttöjärjestelmiin. Windows Server 2008:an on sisällytetty jatkokehitetty versio Active Directorysta, joka on saanut nimeksi Active Directory Domain Services (AD DS). AD DS tukee verkon tietoturvallisuutta tunnistamalla verkkoon pyrkiviä käyttäjiä ja valvomalla käyttöoikeudet verkon resursseihin. (Davies & Northrup, 231, 2008.)

Käyttäjät tunnistautuvat aktiivihakemiston käyttäjiksi käyttäjätunnus ja salasana -parilla. Kun käyttäjä on tunnistettu, sen tietoja voidaan käyttää resurssien käyttöoikeuksien käsittelyssä. Joka aktiivihakemistoon luotu objekti saa oman SID-tunnuksen (Security ID), jota käytetään resursseihin pääsynvalvonnassa. Kun käyttäjä yrittää päästä verkon tiedostoihin, Windows vertaa käyttäjän SID-tunnusta resursseihin liitettyyn oikeusmäärittelyyn, mikäli tunnukset täsmäävät käyttäjä saa pääsyn tiedostoihin sille määrätyillä oikeuksilla. (Itpro.fi, 2007.)

Käyttöoikeuksien hallinta voi toteuttaa myös ryhmien tasolla. Ryhmä on joukko käyttäjä- ja tietokonetilejä, joita käsitellään yhtenä yksikkönä. Silloin ryhmän jäsenet saavat ryhmän SID-tunnuksen ja sitä kautta kaikki ne oikeudet, jotka on ryhmälle myönnetty. (Davies & Northrup, 234, 2008.)

3.2 Ryhmäkäytännöt

Ryhmäkäytännöt (Group policy) aktiivihakemiston kanssa toteutettuna ovat verkon ylläpitäjän keskeinen väline käyttäjien ja tietokoneiden hallitsemiseksi. Ryhmäkäytäntöprofiileja voidaan kohdistaa toimipaikkaan (site), toimialueeseen (domain) tai organisaatioyksikköön (Organizational Unit, OU) ja niitä liitetään ryhmäkäytäntöobjekteihin (Group Policy Object, GPO). Ryhmäkäytäntöteknologiaa tukevat Windows Vista-, Windows XP-, Windows Server 2003- ja Windows Server 2008 -käyttöjärjestelmät. (Davies & Northrup, 240, 2008.)

Ryhmäkäytäntöjen avulla pystytään hallitsemaan Windows-koneita monipuolisesti ja tarkasti. Yhtä objektia kohti on mahdollista määrittää yli 1 000 erilaista asetusta: IT-kouluttajana ja tietokirjailijana vuodesta 1985 toiminut Rousku mainitsee artikkelissaan (Micropc.net, 2005) Windows XP SP2 -työasemassa olevan kaikkiaan 1 378 ryhmäkäytäntöasetusta. Ryhmäkäytäntöjen avulla verkonvalvoja voi helpottaa verkon ylläpitoa automatisoimalla erilaisia hallintatehtäviä, kuten järjestelmän päivittäminen ja sovellusten asentaminen, ohjelmistojen toiminnallisuuden rajoittaminen tietyiltä käyttäjäryhmiltä, käyttäjien ja käyttäjäryhmien tietokoneympäristön yhtenäistäminen myös erilaisten tietoturva-asetusten määrittäminen. (Davies & Northrup, 240, 2008.)

Ryhmäkäytännöt jakautuvat käyttäjäasetuksiin ja tietokoneasetuksiin. Tietokoneasetukset koskevat laitteistoa ja sovelluksia ja ovat käyttäjäriippumattomia. Käyttäjäasetukset koskevat aktiivihakemistotasolla kirjautuvia käyttäjiä tai paikallisesti työasemalle kaikkia kirjautuvia käyttäjiä. Tietokoneasetukset astuvat voimaan tietokoneen käynnistymisen tai ryhmäkäytäntöjen päivittymisen aikana. Käyttäjäasetukset toimeenpannaan käyttäjän kirjautuessa tietokoneelle sekä myös käytäntöjen päivittymisen aikana. (Micropc.net, 2005.)

3.3 Julkisen avaimen järjestelmä

Julkisen avaimen järjestelmällä (PKI) tarkoitetaan teknologiaa, jonka avulla varmistetaan verkon yli lähetettävän viestin aitouden sekä viestin lähettäjän ja vastaanottajan henkilöllisyydet. Julkisen avaimen järjestelmä perustuu avainpareja hyödynnettävään epäsymmetriseen salausmenetelmään. (Wikipedia.org 2, 2009.)

Julkisen avaimen infrastruktuurin osatekijät ovat:

- Varmentaja (Certificate Authority, CA) on varmenteita myönnettävä taho. Varmentaja tarkistaa varmenteen hakijan henkilöllisyyden ja allekirjoittaa myönnetyn varmenteen omalla salaisella avaimella. Suomen virallisen PKI:n varmentaja on väestörekisterikeskus, varmenteen hakijan henkilöllisyyden todentamisen puolestaan hoitaa poliisi. Maailman laajuisesti tunnettuja varmentajia ovat Thawte, Entrust, VeriSign.
- Varmenne (certificate) on ihmisen tai yrityksen henkilötodistus Internetissä.
- Digitaalinen allekirjoitus on sähköinen allekirjoitus, jolla voidaan allekirjoittaa lähetettävän viestin sisältö. Niin kauan kuin viesti pysyy muuttamattomana, sen allekirjoitus yhdistetään varmenteeseen. (Wikipedia.org 2, 2009.)

Julkisen avaimen infrastruktuuri mahdollistaa luottamuksellisen kommunikoinnin kahden toisilleen ennestään tuntemattoman osapuolen kesken. Näiden osapuolten henkilöllisyys varmistaa kolmas osapuoli (varmentaja), johon kumpikin viestittäjä luottaa. Myönnetyssä varmenteessa varmentaja yhdistää julkisen avaimen sen haltijaan, tällä saadaan estettyä pääsyn tiedostoihin ulkopuolisilta. (Ficora.fi, 2007.)

Windows Server 2008:ään sisällytetty Active Directory Certificate Services mahdollistaa palvelimen toimimisen varmentajana. (Davies & Northrup, 239, 2008.)

3.4 RADIUS

RADIUS-palvelimet hoitavat keskitetysti verkkoon pyrkivien tahojen tunnistuksen, valtuutuksen ja tilastoinnin RADIUS-protokollan avulla. RADIUS-protokolla oli suunniteltu aikoinaan sisäänsoittopalveluissa tapahtuvaan tunnistukseen, nykyään protokollaa tukevat mm. langattomat tukiasemat, Ethernet-kytkimet, VPN- ja DSL-palvelimet. (Davies & Northrup, 243, 2008.)

RADIUS-todennuksen infrastruktuuriin kuuluvat:

- Asiakas. Verkkoon pääsyä anova käyttäjä tai laite.
- Verkonpääsypalvelin (Network Access Server, NAS). Verkkoon pääsyä käyttäjille myöntävä palvelin, joka on puolestaan myös RADIUS-palvelimen asiakas.
- RADIUS-palvelin. Palvelin, joka vastaanottaa ja käsittelee RADIUS-asiakkaiden tai välimuistipalvelimen lähettäviä yhteydenottoja ja tilastointiviestejä.
- Käyttäjätilitietokanta. Lista käyttäjistä oikeuksineen.
- RADIUS-välimuistipalvelin. Välimuistinpalvelin reitittää RADIUS-yhteydenottopyyntöjä ja tilastointiviestejä RADIUS-palvelimen ja asiakkaiden välillä. (Davies & Northrup, 243–245, 2008.)

Todennusprosessi käynnistyy käyttäjän yrittäessä päästää verkkoon NAS-laitteen (esimerkiksi kytkin) kautta. NAS-laite RADIUS-asiakkaana lähettää RADIUS-palvelimelle Access-Request viestin, joka sisältää tietoa käydystä todentamisprosessista, kuten porttinumero, johon verkkoon pyrkivä käyttäjä on kytkeytynyt, käyttäjänimi ja haastejono. RADIUS-palvelin tarkistaa käyttäjän oikeellisuuden. Tarkistuksen onnistuessa palvelin etsii tietokannastaan ehdot, joilla käyttäjä päästetään verkkoon ja lähettää listan näistä konfigurointiarvoista RADIUS-asiakkaalle Access-Accept-viestissä. Mikäli käyttäjä ei läpäise oikeellisuuden tarkistusta, palvelin lähettää Access-Reject-viestin, joka tarkoittaa, että tunnistamispyyntö ei kelvannut. (Microsoft.com 1, 2003.)

4 Miten verkkoa valvotaan

Verkon ylläpitäjän päätavoitteena on pitää verkko terveenä, havaita viat mahdollisimman nopeasti ja tunnistaa vikojen alkuperät. Verkonvalvonnalla varmistetaan, että verkon terveydentila vastaa yrityksen määrittämää tietoturvatasoa. Sääntöpohjaisen verkonvalvonnan keinot määräytyvät sen mukaan, mikä haittaohjelmien ennaltaehkäisyohjelmisto verkossa on käytössä (ovatko asennettu palvelimelle vai paikallisesti, miten päivittämiset hoidetaan), tietokoneiden konfiguraatioasetuksista ja muista asetetuista tietoturvallisuusvaatimuksista.

Esimerkiksi työaseman päästämiseksi verkkoon siltä voidaan vaatia seuraavien sääntöjen täyttymistä:

- Kaikki järjestelmän kriittiset päivitykset ovat asennettuna.
- Virustorjuntaohjelmisto on asennettuna ja valvoo poislähtevää sekä sisääntulevaa liikennettä, myös virukset tunnistava tietokanta on ajan tasalla.
- Vakoiluohjelmien torjuntaohjelmisto on asennettuna ja tarkkailee aktiivisena olevia palveluita ja vastaanotettavia tiedostoja, torjuntaohjelmiston viimeisimmät päivitykset ovat ladattu.
- Roskapostitorjunta on asennettu ja monitoroi kaikki vastaanotetut sähköpostiviestit.
- Paikallinen palomuuri on asennettu ja aktiivisena, myös palomuurin poikkeusluettelo (List of exceptions) on määriteltynä.
- Työaseman automaattinen IP-osoitteen haku on kytketty pois päältä tai vastaavasti voidaan vaatia sen olevan päällä.

Kun tiedetään kuinka turvallinen verkosta halutaan, sääntöjen asettaminen ei ole vaikeaa. Verkonvalvonnan haasteellisin vaihe on varmistaa, että kaikki tuotantoverkkoon päästetyt työasemat täyttävät tietoturvavaatimukset.

Ongelman ratkaisemiseksi Microsoft kehitti Network Access Protection (NAP) palvelun, jonka oli tarkoitus tulla Windows Server 2003 R2 -käyttöjärjestelmän mukana

vuonna 2005. Ensimmäinen versio NAP:sta oli monimutkainen ja vaikeasti konfiguroitava. Osittain siitä syystä ja osittain sen takia, että Microsoft halusi tehdä NAP:n yhteensopivaksi Ciscon NAC:n (Network Admission Control) kanssa, NAP oli vedetty pois lopullisesta Windows Server 2003 R2:n julkistuksesta. Microsoft teki työtä NAP:n kehittämiseksi ja nyt Network Access Protection on ensisijainen tietoturvallisuustyökalu Windows Server 2008 -käyttöjärjestelmässä. (Cyberguru.ru.)

5 NAP-suojauksen kuvaus ja toiminta

NAP (Network Access Protection) on ohjelmistovalmistaja Microsoftin kehittämä sääntöpohjainen käyttöoikeuksia valvova tekniikka, jolla suojataan verkko vaarallisilta ja saastuneilta tietokoneilta. NAP tulee vakiona Windows Server 2008 -käyttöjärjestelmässä, NAP-clientit ovat valmiiksi asennettuna Windows Vista-, Windows 7 -käyttöjärjestelmissä ja ovat saatavilla myös Windows XP SP3 -työasemiin erillisenä päivityksenä. Muiden valmistajien tuotteisiin tarvitaan jonkinlaisia päivityksiä, jotta ne toimivat NAP-teknologian kanssa. (Microsoft.com 2, 2008.)

NAP-suojauksen avulla Windows-verkoissa verkon ylläpitäjät pystyvät asettamaan tietoturvallisuusehdot NAP-yhteensopiville työasemille ja rajoittamaan saastuneiden asemien pääsyä lähiverkkoon. NAP-yhteensopivat koneet voivat päivittyä automaattisesti vaaditulle turvallisuustasolle. On tärkeää muistaa, että NAP ei tee mitään luvattoman verkkoon pääsyn estämiseksi. Jos rikollinen omistaa työaseman, joka täyttää vaaditut ehdot, NAP ei häntä pysäytä. NAP:n tehtävänä on estää pääsyn verkkoon sallituilta käyttäjiltä, jotka käyttävät epäturvallisia tietokoneita. (Cyberguru.ru.)

5.1 Ominaisuudet

NAP:n kolme tärkeää puolta ovat:

- Terveydentilan tarkistaminen. Kun työasema yrittää pääsyä verkkoon, sen terveydentilaa verrataan verkon ylläpitäjän asettamiin ehtoihin. Verkon ylläpitäjät määrittelevät myös sen mitä tehdään, jos asema ei vastaa turvallisuusvaatimuksia.
- Terveydentilan korjaaminen. Saastuneiden työasemien automaattinen päivittäminen erillisten ohjelmistohallintaohjelmien avulla (Microsoft System Management Server, Microsoft System Center Configuration Manager 2007.).

- Verkkoon pääsyn rajoittaminen. Verkon suojaaminen saastuneilta koneilta, rajoittamalla niiden pääsyä tuotantoverkkoon. Työaseman turvallisuustarkistuksen perusteella, NAP voi myöntää sille pääsyn verkkoon täysin oikeuksin, ohjata työaseman erilliseen verkkoon tai estää pääsemästä verkkoon kokonaan. Poikkeuksena voidaan sallia tai estää pääsyn verkkoon asemilta, jotka eivät tue NAP-teknologiaa. (Davies & Northrup, 572, 2008.)

NAP on laajennettava alusta. NAP-suojaus tarjoaa infrastruktuurikomponentteja ja API-rajapintoja (Application Programming Interface), joiden avulla voidaan lisätä erilaisia komponentteja koneiden terveydentilan tarkistukseen, verkkoliikenteen ja pääsynvalvontaan. (Davies & Northrup, 573, 2008.)

5.2 Komponentit

Jotta verkon toimintaa voitaisiin hahmottaa paremmin, täytyy ensin tutustua Microsoftin käyttämiin käsitteisiin. Näihin käsitteisiin kuuluvat asiakaskone (Enforcement Client, EC), NAP-suojauksen täytäntöönpanopalvelin (Enforcement Server, ES), System Health Agent (SHA), System Health Validator (SHV), NAP-suojauksen terveydenarviointipalvelin (NAP Policy Server, NPS) ja Remediation Server.

5.2.1 Asiakaskone ja NAP-täytäntöönpanopalvelin

Asiakaskone on mikä tahansa lähiverkkoon pyrkivä työasema, jonka käyttöjärjestelmä kykenee suorittamaan System Health Agent -komponentteja. Tällä hetkellä tällaisia käyttöjärjestelmiä ovat Windows XP SP3, Windows Vista, Windows 7 sekä Windows Server 2008. Kolmansilta osapuolilta on saattavana tukea myös Mac- ja Linux-koneille. NAP-täytäntöönpanopalvelin (käyttöjärjestelmänä Windows Server 2008) nimensä mukaisesti

panee täytäntöön NAP-suojauksen määrittämät politiikat eli suorittaa asiakaskoneiden politiikkojen mukaisen tarkastuksen. (Windowsnetworking.com, 2009.)

5.2.2 SHA ja SHV

SHA on asiakasohjelma, joka käynnistyy työasemalla ja tutkii sen terveydentilaa seuraamalla aseman Windows Security Centerin asetuksia. SHA luo arvion asiakaskoneen terveydentilasta (Statement of Health, SoH). Esimerkiksi virustorjuntaohjelmistoa monitoroivan SHA:n SoH voi sisältää tietoa siitä, onko virustorjunta asennettu koneelle, onko se aktiivisena vai otettu pois käytöstä, mikä on asennetun ohjelmiston versio ja ovatko viimeisimmät päivitykset ladattuna. Mikäli jotkin näistä kohdista päivittyvät, SHA luo uuden terveydentila-arvion. Pitääkseen ajan tasalla voimassaolevan tiedon koneen kokoonpanosta, NAP-clientit käyttävät System Statement of Health (SSoH) -tietokantaa, johon tallentuvat tiedot ja versionumerot NAP-asiakaskoneesta, koneelle asennetuista SHA -agenteista ja niiden luomista terveydentila-arvioista. (Windowsnetworking.com, 2009.)

Palvelimelle asennettu terveydentilan tarkastaja (System Health Validator, SHV) vastaanottaa SHA:n lähettämiä tietoja ja vertaa niitä palvelimelta löytyvään järjestelmävalvojan asetettuun tietoturvakäytäntösäännöstöön. Näin saadaan selville, onko kyseinen asiakasasema käytäntöjen mukainen ja mikäli se ei ole, mitä toimenpiteitä vaaditaan aseman päivittämiseksi vaadittavalle turvallisuustasolle. Joka SHV tuottaa arvion (Statement of Health Response, SoHR), joka sisältää terveydentilan korjaamiseen tarvittavat toimenpiteet. Virustorjuntaohjelmiston tapauksessa, sen SoHR voi sisältää viimeisimpien päivitysten versionumeron ja palvelimen IP-osoitteen, jolta asema voi käydä lataamassa päivitykset. SHA-agenttien tapaan, SHV-agentit myös käyttävät arvioista koostuvaa tietokantaa (System Statement of Health Response, SSoHR). (Davies & Northrup, 577, 2008.)

Kun NAP-asiakaskone yrittää pääsyä verkkoon, se lähettää SSoH-tietokantansa arvioitavaksi NAP-terveyspalvelimelle (NPS) NAP-täytäntöönpanopisteen kautta. NPS suorittaa

SHV-agenttien avulla päätelaitearvioinnin ja lähettää paluuviestinä SSoHR. NAP-asiakaskone ohjaa SoHR:t niitä vastaaville SHA-agenteille. Turvallisuussääntöjen vastaiset SHA:t automaattisesti suorittavat terveydentilan korjaavia toimenpiteitä, mikä taas saa aikaan uusien SoH-arvioiden luonnin ja koko terveydentilan validointiprosessi alkaa alusta. Kaikki politiikka- ja terveystilamuutokset heijastuvat verkkoon dynaamisesti. (Davies & Northrup, 573, 2008.)

5.2.3 NPS

Windows Server 2008 -ympäristössä NPS toimii RADIUS- ja välityspalvelimen roolissa. RADIUS-palvelimena NPS hoitaa tunnistuksen ja valtuutuksen tarjoamalla AAA-palveluita eri verkkoon kytkentätavoille. NPS käyttää tietokantanaan Microsoftin Active Directorya, josta hakee verkkoon pyrkivien käyttäjien ja tietokoneiden profiilitiedoista autentikointi- ja valtuutustiedot.

NPS toimii myös ns. terveydenarviointipalvelimena. Verkon ylläpitäjät tallentavat palvelimelle yrityksen tietoturvapolitiikkasäännöstön, jota NPS vertaa asiakaskoneen terveystilaan konetarkistusta suorittaessa. Sääntöjen vastaisille asemille NPS kertoo mitä toimenpiteitä asemien täytyy suorittaa ennen kun niitä voitaisiin päästää lähiverkkoon.

5.2.4 Päivityspalvelin

Päätelaitetarkistuksesta sääntöjen vastaisiksi osoittautuneet asemat ohjataan karanteeniverkkoon, jossa sijaitsevat päivityspalvelimet (Remediation Servers), joilta asemat voivat käydä hakemassa päivitykset ja korjaukset niihin vikoihin, joiden takia ne olivat tulleet estetyiksi pääsemästä tuotantoverkkoon. Päivityspalvelimena voivat toimia DNS-palvelin tai tiedostopalvelimet, jotka jakavat ohjelmistopäivitykset.

5.2.5 NAP-pakotustavat

Windows XP SP3, Windows Vista, Windows 7 ja Windows Server 2008 tukevat neljää pakotustapaa:

- Internet Protocol Security (IPSec) -yhteydet
- IEEE 802.1X-autentikoinilla toteutetut yhteydet
- VPN-etäyhteydet
- DHCP -osoitejaolla toteutetut yhteydet.

Näiden lisäksi Windows Server 2008 ja Windows Vista -käyttöjärjestelmissä on tuki Terminal Service (TS) -yhdyskäytäväyhteyksille.

Verkonvalvojat voivat ottaa NAP:n käyttöön yhden tai useamman edellä mainitun teknologian yhteydessä. Ennen kuin työasema saa IP-asetukset käytettäviksi, NAP vaatii aseman todistamaan terveytensä.

IPsec

IPsec on suojaustasoltaan vahvin NAP:n pakotustapa. IPsec on joukko TCP/IP-perheeseen kuuluvia protokollia, jotka hoitavat liikenteen salauksen, toisen osapuolen todentamisen ja eheyden varmistamisen. (Wikipedia.org 3, 2009) Turvallisuustarkistuksen läpäisseille koneille voidaan asettaa ehtoja verkossa turvalliseen kommunikointiin IP-osoite- tai TCP/UDP-porttikohtaisesti. Kun työasema liittyy verkkoon ja saa IP-asetukset, se voi kommunikoida vain muiden terveiden asemien kanssa. (Microsoft.com 2, 2008.)

IPsec hyödyntää myös varmenteita. IPsec-pakotustapa vaatii Health Registration Authoritoryn (HRA) -ominaisuuden asennuksen. Kun työasema todistaa olevansa terve, HRA hankkii sille X.509-sertifikaatin, jota käytetään yhdessä muiden turvallisuusehtojen kanssa aseman todentamiseen verkossa. (Microsoft.com 2, 2008.)

IEEE 802.1X

Porttikohtainen autentikointi. Verkkoon liittämistapana on langallinen (kytkin) tai langaton. Niitä koneita varten, jotka eivät ole selvinneet terveystarkistuksesta, kytkimellä tai langattomalla tukiasemalla on tarjolla ”rajoitetun pääsyn profiili”, jonka avulla voidaan työasemat esimerkiksi pakottaa karanteeniverkkoon.

VPN

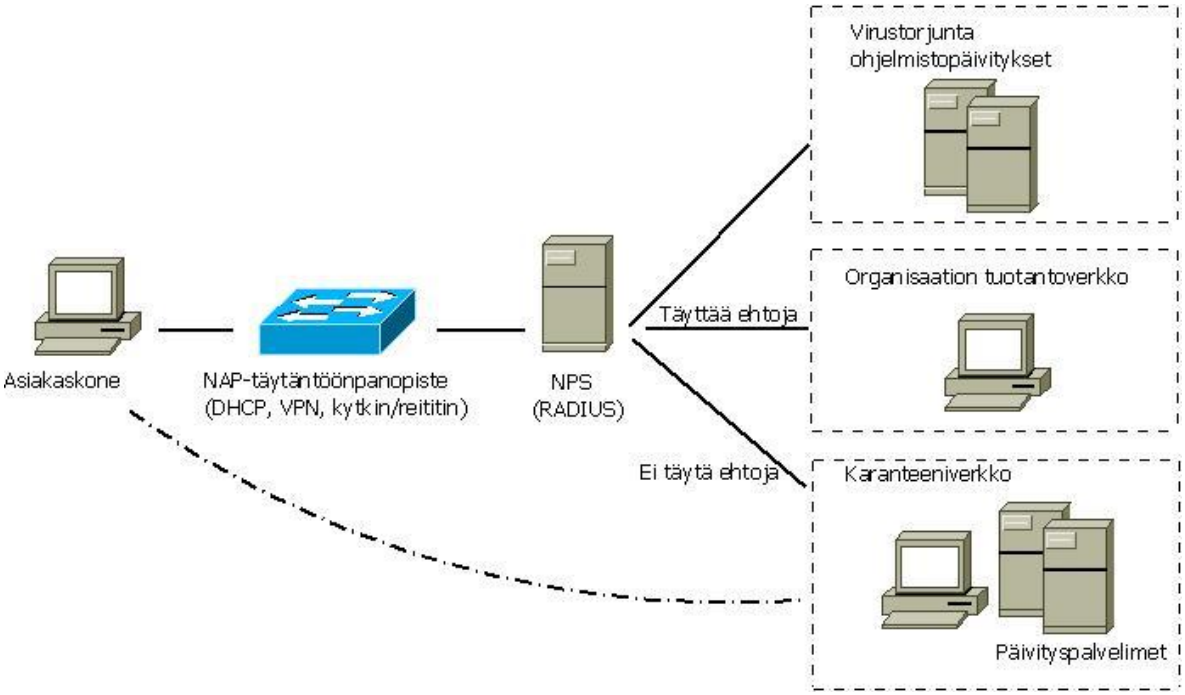
Pääsy toimialueeseen etäyhteyden kautta vain terveille työasemille, saastuneet asemat ohjataan eristettyyn verkkoon.

DHCP

DHCP-palvelimen käyttöjärjestelmänä on oltava Windows Server 2008. Vain terveet asemat saavat tuotantoverkon IPv4-asetukset, muut asemat ohjataan karanteeniverkkoon. Suojaustasoltaan tämä on heikoin tapa, sillä käyttäjä, jolla on työasemaansa järjestelmävalvojan oikeudet, pystyy muuttamaan koneen IP-asetuksia.

5.3 Toiminta

Vaikka NAP-suojausta konfiguroidaan verkon yksilöllisten tarpeiden mukaiseksi, verkon toimintaperiaate säilyy samana. Kuva 1 esittää NAP-tekniikkaan pohjautuvan verkon rakennetta ja toimintaa:

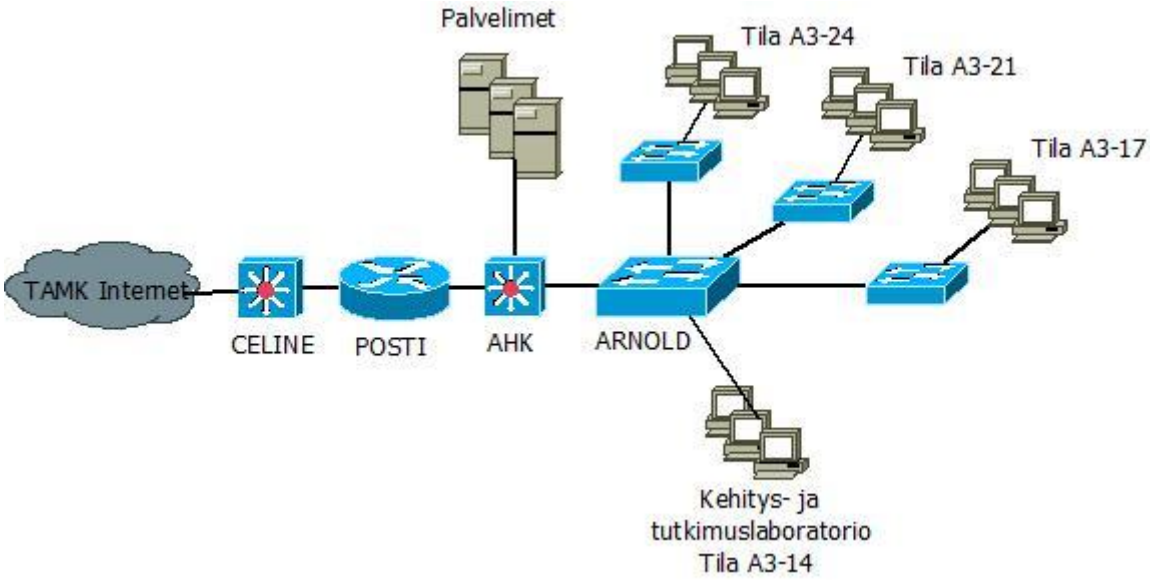


Kuva 1: NAP-verkko

Verkkoon pyrkivä työasema välittää tiedot kokoonpanostaan ja terveydentilastaan NAP-täytäntöönpanopisteelle. NAP-täytäntöönpanopisteenä voi toimia VPN-, DHCP-palvelin, kytkin tai reititin. NAP-täytäntöönpanopiste edelleen ohjaa asiakaskoneelta saadut tiedot Network Policy -palvelimelle (NPS). NPS vertaa aseman terveydentilaa määritettyihin ehtoihin. Jos asema vastaa ehtoja, se saa pääsyn organisaation lähiverkkoon. Mikäli kone ei täytä ehtoja, sen ohjataan eristettyyn VLAN-verkkoon. Karanteeniverkosta asemat pääsevät päivityspalvelimelle, jolta ne voivat hakea tarvittavat päivitykset. Tämän jälkeen päivitetyt asemat voivat anoa uudelleen pääsyä verkkoon.

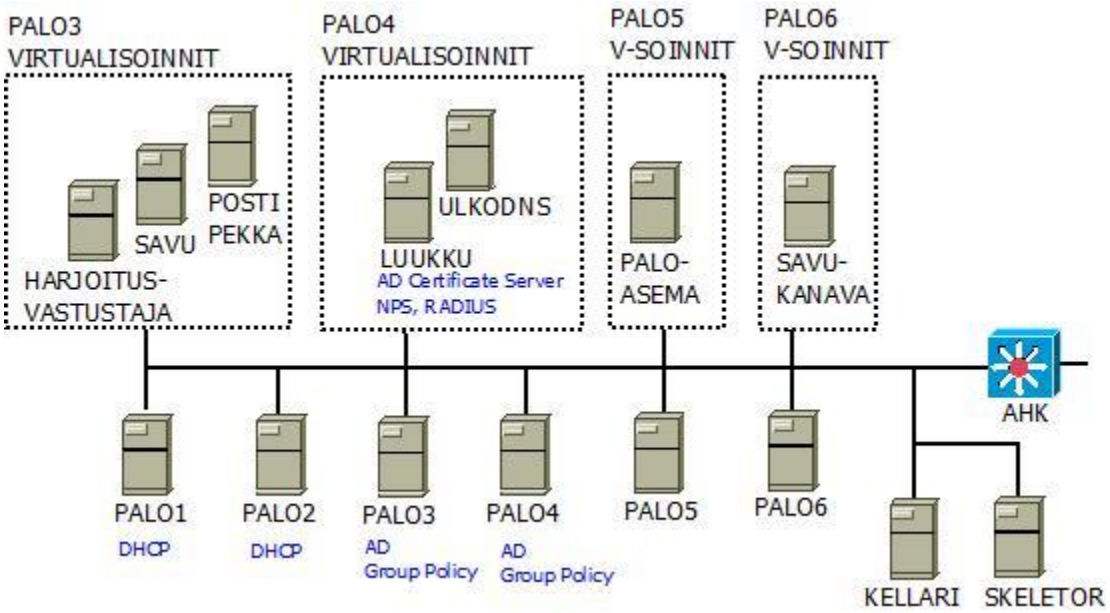
6 WPK-verkon kuvaus

”WPK-verkko on Tampereen ammattikorkeakoulun tieto- ja viestintäteknologian osaamiskeskuksen henkilöstön rakentama ja ylläpitämä opiskelu-, tutkimus- ja kehitysympäristö” (wpk.tpu.fi, 2009). WPK-verkko on erillinen Tampereen ammattikorkeakoulun verkosta ja palvelee erityisesti tietoverkkopalvelujen linjaa opiskeluun liittyvissä asioissa. WPK-verkko on loogiselta topologialtaan tähtimäinen, fyysisellä tasolla verkko koostuu RJ-45 kaapeloinnista ja osittain valokuidusta, 70-työasemista ja 17-verkon aktiivilaitteesta. Verkko kattaa kehitys- ja tutkimuslaboratorion ja neljä luokkaa, joissa järjestetään käyttöjärjestelmiin ja tietoverkkopalveluihin liittyviä opintojaksoja. Kaavio kuvassa 2 havainnollistaa WPK-verkon nykyistä rakennetta:



Kuva 2: WPK-verkon nykyinen rakenne

WPK-verkossa on 8 fyysistä palvelinta, joista osa on jaettu useaan erilliseen virtuaaliympäristöön, eli yhteensä fyysisiä ja virtualisoituja palvelimia on käytössä 15. Kuvassa 3 on esillä verkon palvelimet ja tämän työn kannalta tärkeämmät palvelimien tarjoamat palvelut:



Kuva 3: WPK-verkon palvelimet

7 NAP-suojauksen asennus ja käyttöönotto

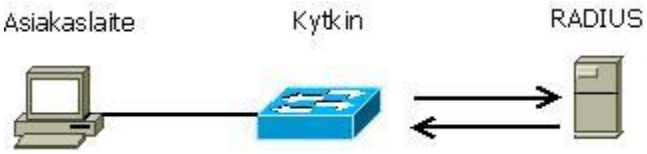
Tässä osiossa käyn läpi NAP-suojauksen käyttöönoton vaiheita. Aloitin työn valitsemalla NAP-pakotustavan.

7.1 802.1x-autentikointi

NAP-pakotustavaksi valitsin 802.1x:n sen verkkoon tuoman tietoturvallisuuden perusteella. Seuraavaksi käyn läpi 802.1x-autentikointiin liittyviä käsitteitä ja autentikoinnin toimintaa.

802.1x porttikohtainen todentaminen (Port Based Authentication) on IEEE:n standardi, jota käytetään Ethernet- ja WLAN-verkoissa. 802.1x-autentikoinnin tehtävänä on estää luvattoman asiakaslaitteen liikennöinti lähiverkon liityntäpisteen kautta sekä myöntää sallitulle asiakaslaitteelle ne verkkoresurssit, joihin käyttäjällä on pääsyoikeudet. (Cisco.com, 2009.)

Kuva 4 esittelee 802.1x-autentikoinnin toimintaa.



Kuva 4: 802.1x-autentikointi

Asiakaslaite kytkeytyy verkkoon liityntäpisteen kautta. Liityntäpisteenä voi toimia kytkimen portti tai tukiasema langattomassa verkossa. 802.1x-autentikoinnissa asiakaslaitteelle luodaan kaksi loogista porttia (auktorisoitu ja auktorisoimaton). Auktorisoimattoman portin kautta ei kulje muuta kuin linkkitason liikennettä, eli koko autentikointiprosessi tapahtuu linkkitasolla. (Cisco.com, 2009.)

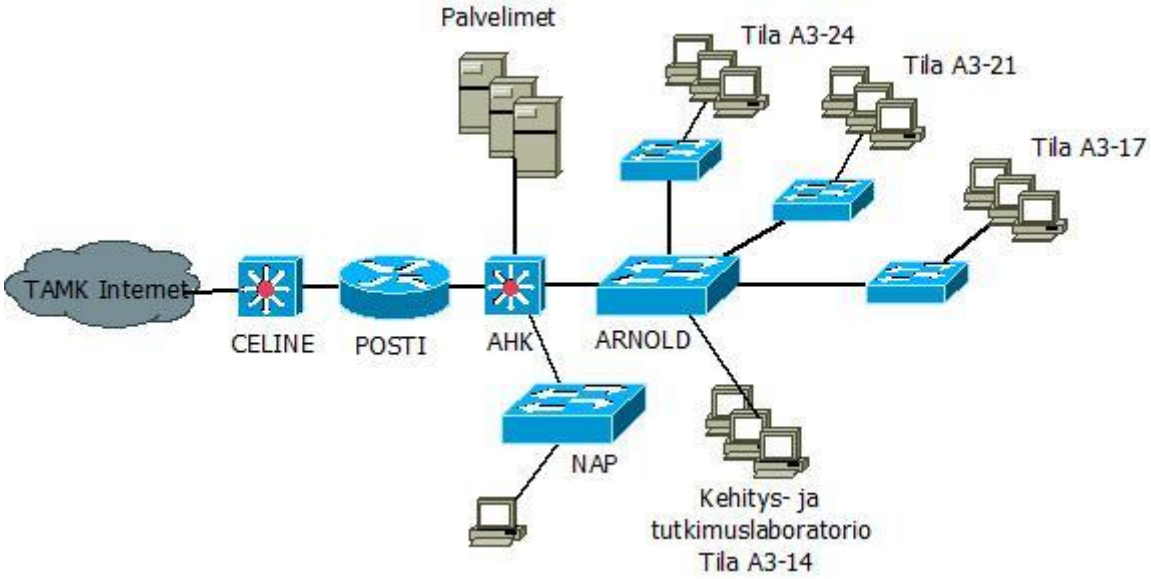
Kytkin (autentikaattori) vastaa asiakaslaitteen ja autentikointipalvelimen välisestä liikenteestä. Kytkin välittää autentikointipalvelimelle asiakkaalta saadut autentikointitiedot. Autentikointipalvelin (tässä tapauksessa RADIUS-palvelin) suorittaa autentikoinnin ja välittää autentikoinnin tuloksia autentikaattorille. Mikäli autentikointi on onnistunut, kytkin muuttaa portin, johon asiakas on kytkettynä auktorisoiduksi ja laittaa sen oikeaan aliverkkoon. (Cisco.com, 2009.)

802.1x-autentikointi tapahtuu verkon reunalla, joten tunnistamattomia käyttäjiä ei päästetä liikennöimään verkon liityntäpistettä pidemmälle, mikä myös vähentää verkon kuormaa. Kun käyttäjä on todettu, autentikoinnin tuloksen perusteella kytkimen portti siirtyy oikeaan virtuaaliverkkoon. Näin käyttäjät eivät ole sidottuja yhteen tiettyyn verkkoporttiin, vaan he pääsevät verkkoon mistä tahansa kytkimen portista.

7.2 Verkkolaitteiden asennus ja konfigurointi

Sain käyttööni siirtokerroksella toimivan Cisco Catalyst 2960 -kytkimen, jonka IOS-versio (Internetwork Operating System) ei tukenut 802.1x (EAP over IEEE 802.1x) -metodia, joten seuraava toimenpiteeni oli IOS:n päivittäminen. Päivitin kytkimen IOS:n 12.2(50)SE1-versioon. Kytkimen etuna on myös lisäporttien saaminen.

Kuva 5 havainnollistaa WPK-verkon rakennetta kytkimen verkkoon liittämisen jälkeen:



Kuva 5: WPK-verkon muutettu rakenne

AHK-kytkin

WPK-verkon AHK-niminen kytkin toimii VTP-protokollan palvelin-tilassa (server mode), eli se välittää VLAN-informaatiota verkon asiakas-tilassa (client mode) toimiville kytkimille. AHK-kytkimelle konfiguroin trunk-linkin NAP-kytkintä varten sekä loin kaksi virtuaaliverkkoa:

- VLAN 30 (Unhealthy). Virtuaaliverkko, johon sijoitetaan terveystarkastuksessa hylätyt ja autentikoimattomat käyttäjät, myös ne käyttäjät, joiden tietokone ei tue NAP-ominaisuutta.
- VLAN 31 (Healthy). Virtuaaliverkko, johon sijoitetaan autentikoidut ja terveystarkastuksen läpäisseet käyttäjät.

NAP-kytkin

NAP-kytkin toimii VTP-asiakas-tilassa (client mode), eli se vastaanottaa AHK-kytkimen lähetettämää VLAN-informaatiota ja sen mukaan päivittää omaa VLAN-tietokantaa. NAP-kytkin suorittaa verkkoon pyrkivien asiakaskoneiden autentikoinnin. Autentikointia varten

kytkimelle oli tehty seuraava konfiguraatio (Tässä kerron vain autentikoinnin kannalta olennaiset komennot, kytkimen konfiguraatio kokonaisuudessaan on tämän työn liitteenä.):

```
aaa new-model
aaa authentication dot1x default group radius local
aaa authorization network default group radius local
dot1x system-auth-control
interface FastEthernet0/1
 description NAP-client port
 switchport mode access
 authentication event no-response action authorize vlan 30
 authentication port-control auto
 dot1x pae authenticator
interface GigabitEthernet0/1
 switchport mode trunk
interface Vlan1
 ip address 172.16.1.27 255.255.0.0
radius-server host 172.16.1.54 auth-port 1645 acct-port 1646
key *****
```

Konfiguraation selitykset:

`aaa new-model` sallii aaa -palvelut globaalisesti.

`aaa authentication dot1x default group radius local` määrittää kytkimen käyttämään 802.1x-autentikointia, protokollana toimii RADIUS. Tapauksessa, kun RADIUS-palvelimelle ei saada yhteyttä, kytkin käyttää autentikointiin paikallista tietokantaa.

`aaa authorization network default group radius local` määrittelee kytkimen käyttämään RADIUS:ta myös valtuutuksessa. Tämä komento mahdollistaa dynaamisen VLAN:n.

`dot1x system-auth-control` kertoo kytkimelle, että autentikoinnissa käytetään 802.1x:ää.

`authentication event no-response action authorize vlan 30` määrittelee VLAN:n, johon sijoittuvat autentikoimattomat työasemat.

`authentication port-control auto` kytkee autentikoinnin päälle liitynnässä

`dot1x pae authenticator` kytkee autentikaatorin päälle.

`radius-server host 172.16.1.54 auth-port 1645 acct-port 1646 key *****` määrittelee RADIUS-palvelimen parametreja, kuten IP-osoitetta, autentikointiporttia, valtuutusporttia ja salasanaa.

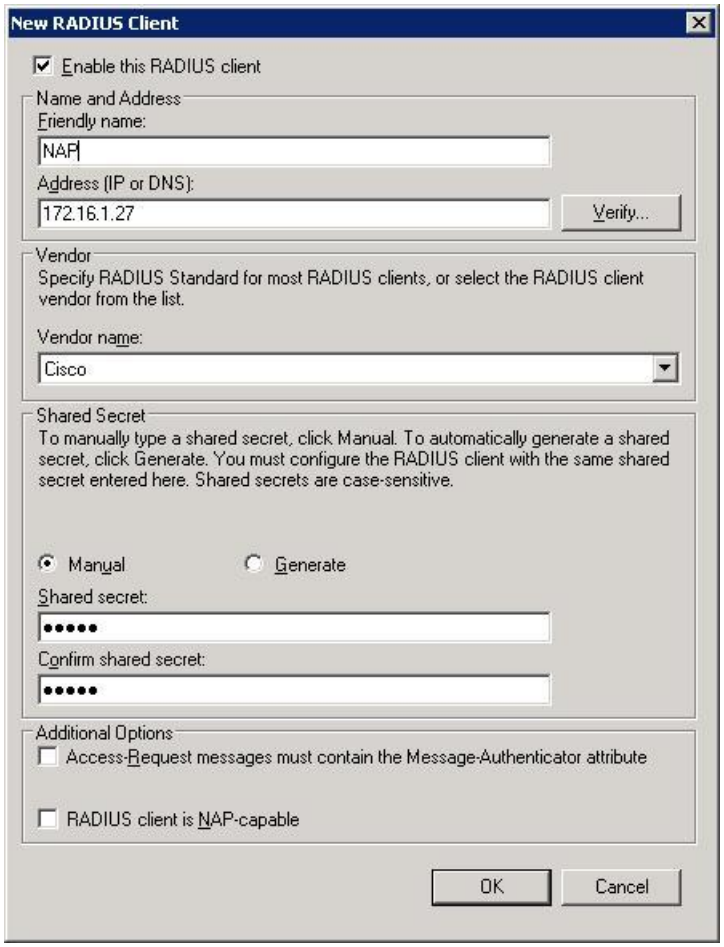
POSTI-reititin

POSTI-reititin on WPK-verkon reunareitin. Reunareitittimen avulla sisäverkko suojataan ulkoverkolta erilaisilla pääsynvalvontalistoilla ja porttisuodattimilla. POSTI-reitittimelle lisäsin pääsylistat, joissa 30- ja 31-virtuaaliverkkojen koneilta sallitaan pääsy ulkoverkkoon:

```
access-list 1 permit 172.16.0.0 0.0.255.255
```

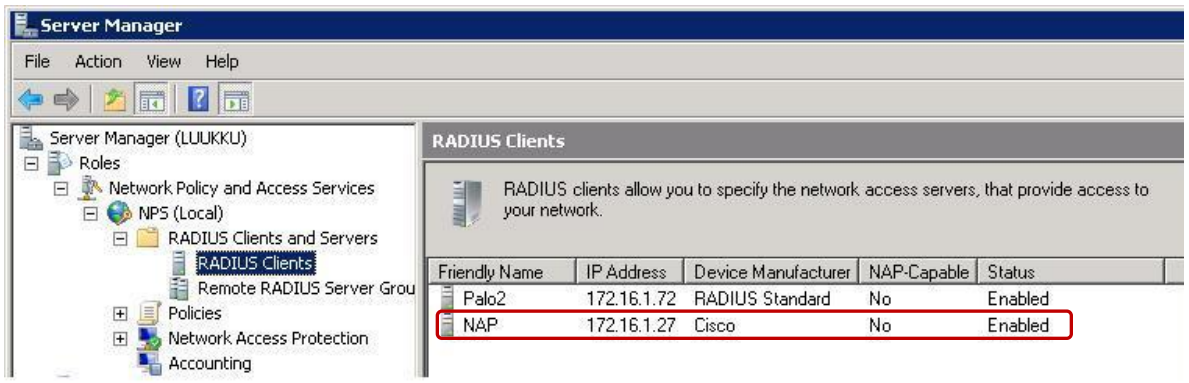
7.3 RADIUS

Mikäli NAP-laillisuustarkastuksen suorittava laite on eri kuin NPS-palvelin, täytyy kyseinen laite lisätä NPS-palvelimen RADIUS-asiakaslistalle. WPK-verkon NPS-palvelimena toimii LUUKKU (jatkossa käytän LUUKKU-palvelimesta myös nimitystä NPS-palvelin). Asiakkaan lisääminen RADIUS-palvelimelle tapahtuu Server Manager -konsolin kautta: Kun klikkaa hiiren oikeata painiketta Radius Client -kohdan päällä, avautuu New Radius Client -ikkuna, johon kirjataan uuden RADIUS-asiakkaan tietoja, kuten kuvasta 6 näkee:



Kuva 6: Uuden RADIUS-asiakkaan lisääminen

Kuvassa 7 nähdään, että lisätty RADIUS-asiakas ilmestyy RADIUS Clients -listalle:



Kuva 7: RADIUS-asiakkaat

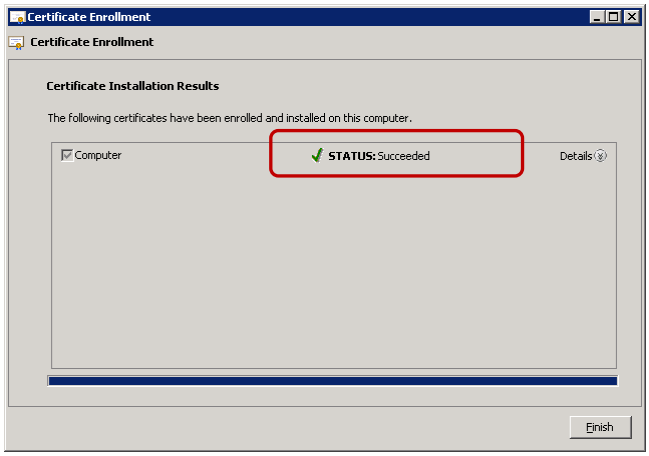
7.4 Juurisertifikaatti

Autentikoinnissa tullaan käyttämään PEAP-liikennöintiprotokollaa, joka vaatii TLS-sertifikaattia NPS-palvelimessa. Tätä varten asensin Enterprise root CA:n WPK-verkon juurisertifikaattipalvelimelle eli LUUKKU:lle. Enterprise root CA:n asennus onnistuu Windows Components Wizard:n avulla, joka löytyy ohjauspaneelin kautta.

Palvelinpuoleisen PEAP-autentikoinnin mahdollistamiseksi NPS-palvelin käyttää tietokonesertifikaattia omasta paikallisesta kannastaan. Sertifikaattia hankitaan palvelimelle juurisertifikaattipalvelimelta Certificae Managerin avulla. Certificate Managerissa navigoidaan kuvassa 8 esitetyn polun mukaisesti:

Kuva 8: Sertifikaatin vastaanottaminen

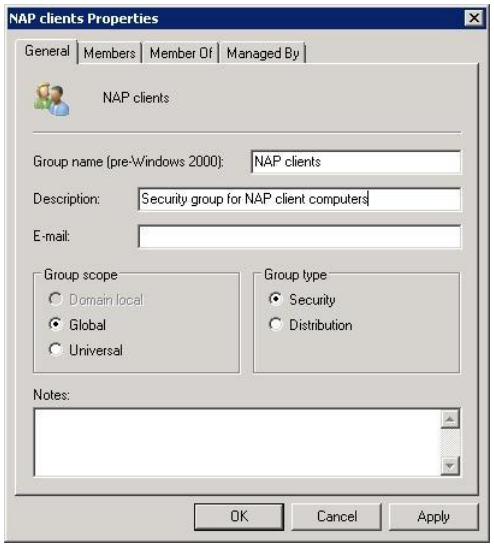
Tämän jälkeen hyväksytään sertifikaatin ja varmistetaan, että sertifikaattiasennus-status on Succeeded (kuva 9):



Kuva 9: Asennettu sertifikaatti

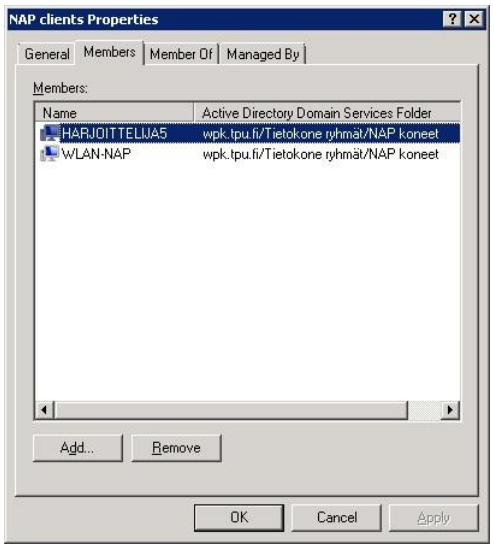
7.5 Aktiivihakemisto

WPK-verkon aktiivihakemisto on kahdennettu vikasietoisuuden saavuttamiseksi PALO3- ja PALO4-palvelimille. Aktiivihakemistoon olen luonut ”NAP clients” -käyttäjäryhmän, johon myöhemmin linkitän ryhmäpolitiikan (kuva 10):



Kuva 10: NAP clients -ryhmän asetukset

Tähän käyttäjäryhmään on tarkoitus lisätä vain ne tietokoneet, joita NAP-turvallisuustarkastus tulee koskemaan. Lisäsin ryhmään muutaman testikoneen (kuva 11):



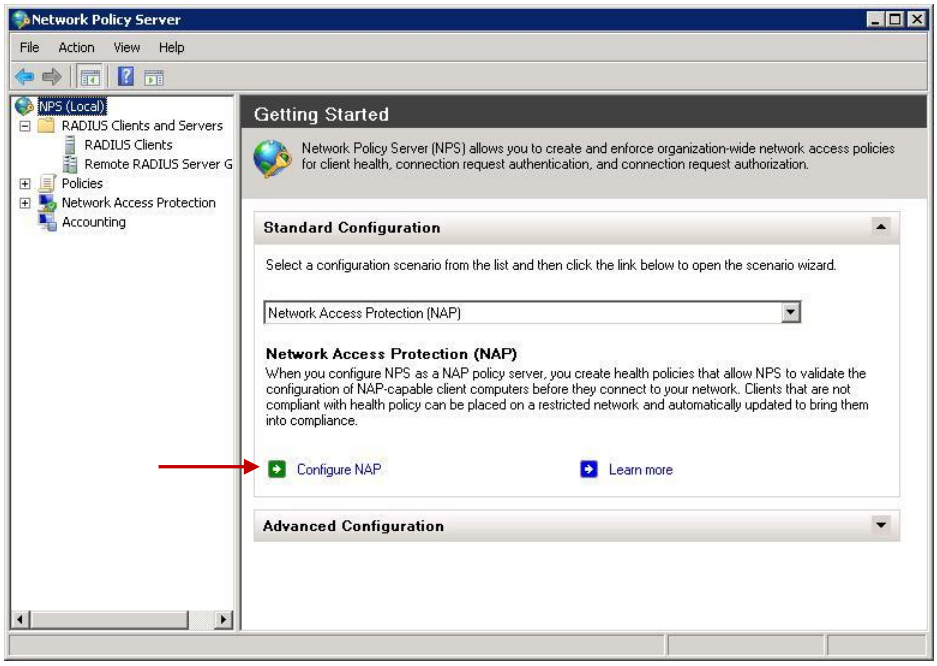
Kuva 11: NAP clients -ryhmän jäsenet

7.6 NPS

NPS-palvelin (LUUKKU) toimii työasemien terveystilatarkastajana. NPS-palvelimen konfiguroiminen tapahtuu Wizardin avulla. Konfiguroinnin aikana määritellään:

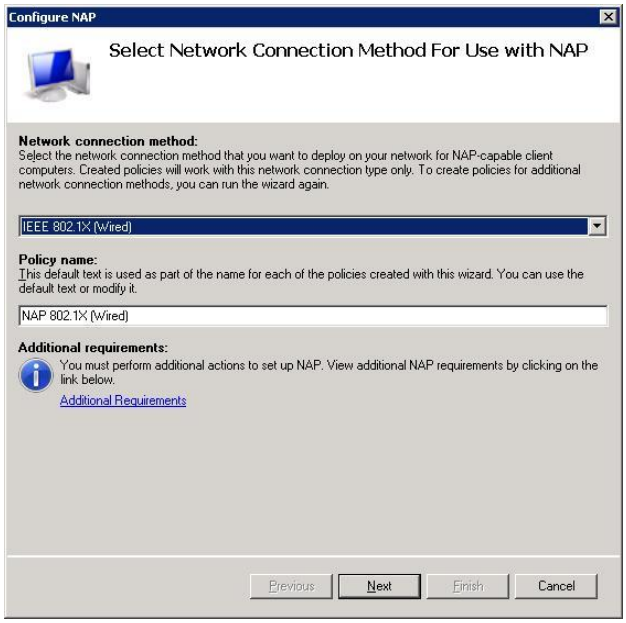
- SHV:t. Ehdot, joita työaseman tulee täyttää päästäkseen tuotantoverkkoon.
- Terveyspolitiikat. Työasemien terveystilan arviointi perustuen SHV:n ilmoittamiin arvoihin.
- Verkkopolitiikat. Oma profiili terveitä ja saastuneita työasemia varten, joissa määritellään mihin verkkoon mikäkin kone ohjataan, virtuaaliverkko määräytyy RADIUS-palvelimelta saadun attribuutin mukaan.
- Verkkoyhteyden anomispolitiikat. Politiikat määrittelevät millä tavalla työasemat anovat pääsyä verkkoon, tässä tapauksessa työasemilta vaaditaan PEAP-autentikoinnin suorittamista.
- Päivityspalvelinryhmät. Halutessa saastuneiksi todetuille työasemille voi määrittää päivityspalvelimet, joilta työasemat voivat käydä lataamassa puuttuvat päivitykset.

NAP Wizard käynnistetään NPS-konsolista (konsoli avautuu komentokehotteen komennolla nps.msc). Konsolissa valitaan NPS (Local) ja klikataan Configure NAP (kuva 12):



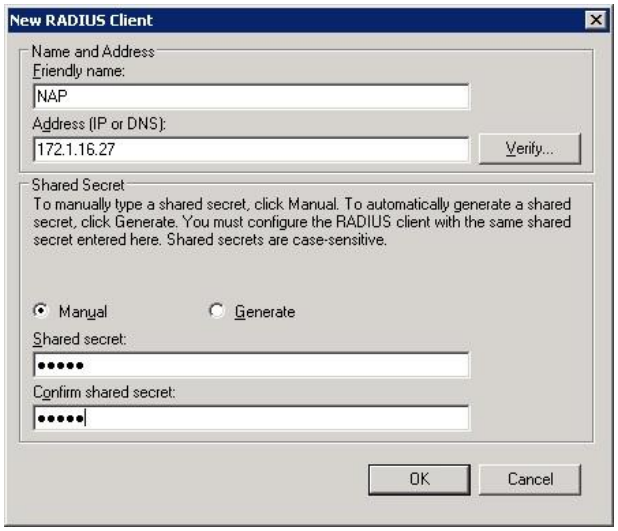
Kuva 12: NAP Wizardin käynnistäminen

Verkkoyhteysmetodiksi valitaan lankayhteyden (kuva 13):



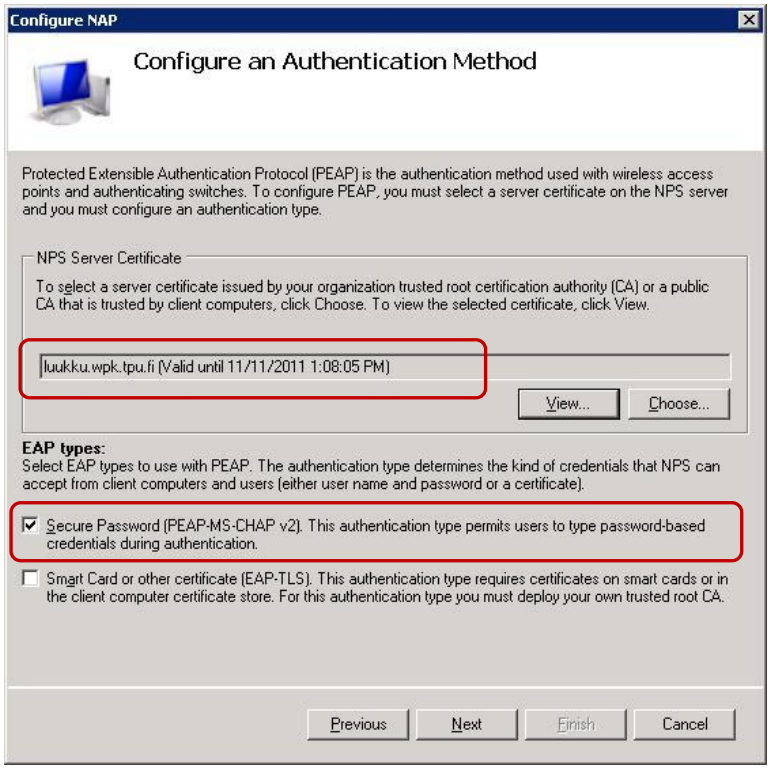
Kuva 13: Verkkoyhteysmetodin valinta

Seuraavaksi lisätään autentikaattorina toimivan kytkimen tiedot (kuva 14):



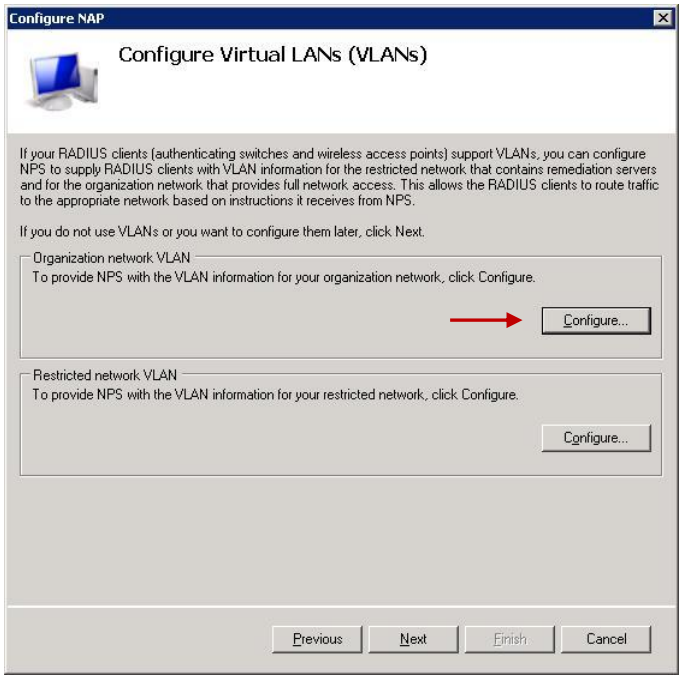
Kuva 14: Kytkimen tiedot

ja varmistetaan, että aikaisemmin asennettu sertifikaatti näkyy NPS Server Sertificate -kohdassa ja EAP-tyypiksi on valittu Secure Password (kuva 15):



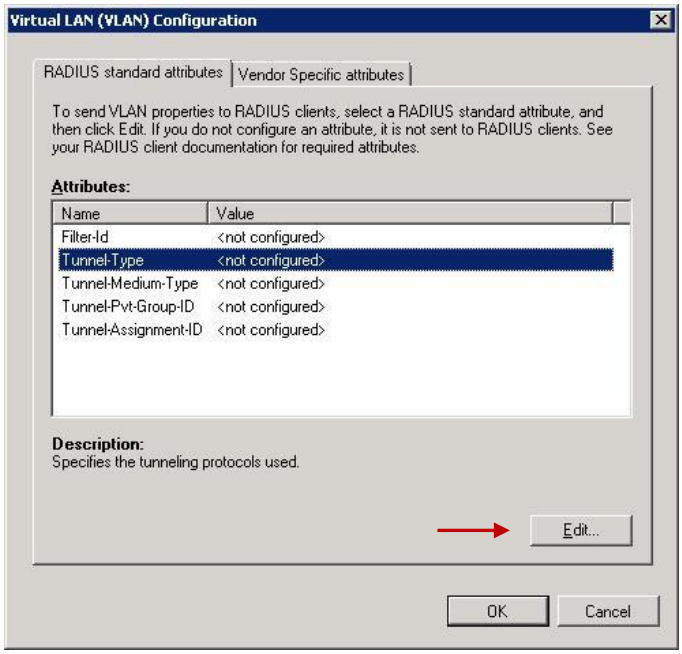
Kuva 15: Autentikointimetodin konfiguroiminen

Tämän jälkeen siirrytään virtuaaliverkkojen konfiguroimiseen (kuva 16):



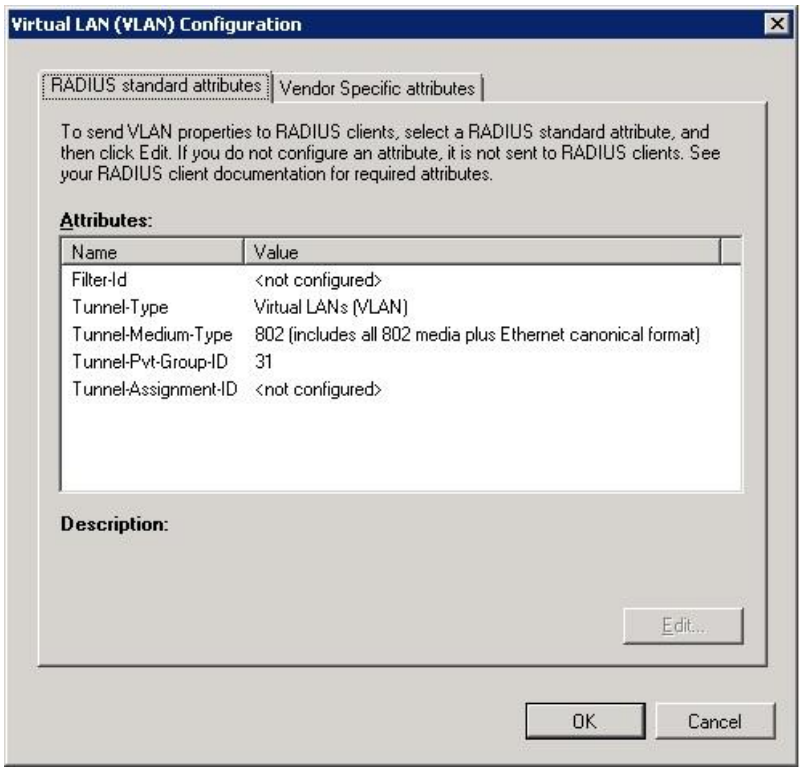
Kuva 16: Virtuaaliverkkojen konfigurointi

Ensin määritellään virtuaaliverkot terveille ja saastuneille työasemille. Profiilin attribuutit ovat seuraavat (kuva 17):



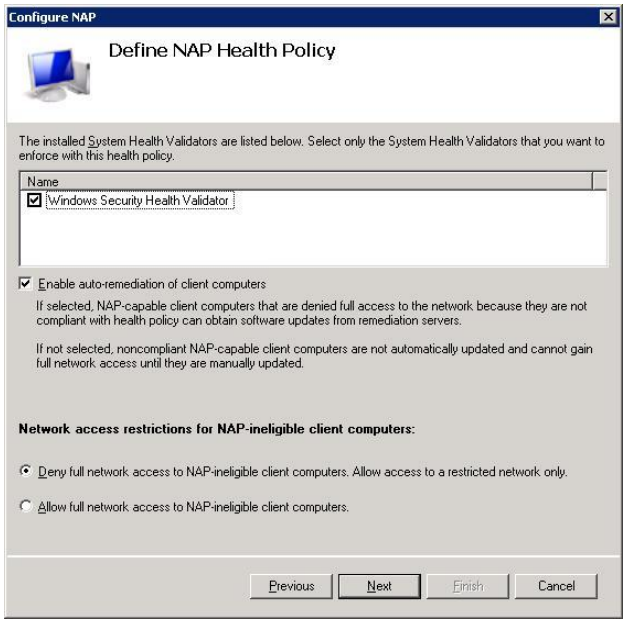
Kuva 17: VLAN:n profiilin konfigurointi

Autentikoinnin toiminnan kannalta tärkeämmät attribuutit ovat Tunnel-Type, Tunnel-Medium-Type ja Tunnel-Pvt-Group-ID. Tunnel-Typen ja Tunnel-Medium-Typen arvoiksi tulee Commonly used for 802.1x, Tunnel-Pvt-Group-ID:n arvo esittää kyseessä olevan VLAN-verkon ID-numeroa. Attribuuttien arvoa pääsee muuttamaan valitsemalla attribuutti ja painamalla Edit-painiketta. Konfiguroin VLAN-verkkojen profiilit kuvan 18 mukaisesti (Tunnel –Pvt-Group-ID Healthy verkolle on 31 ja karanteeniverkolle 30):



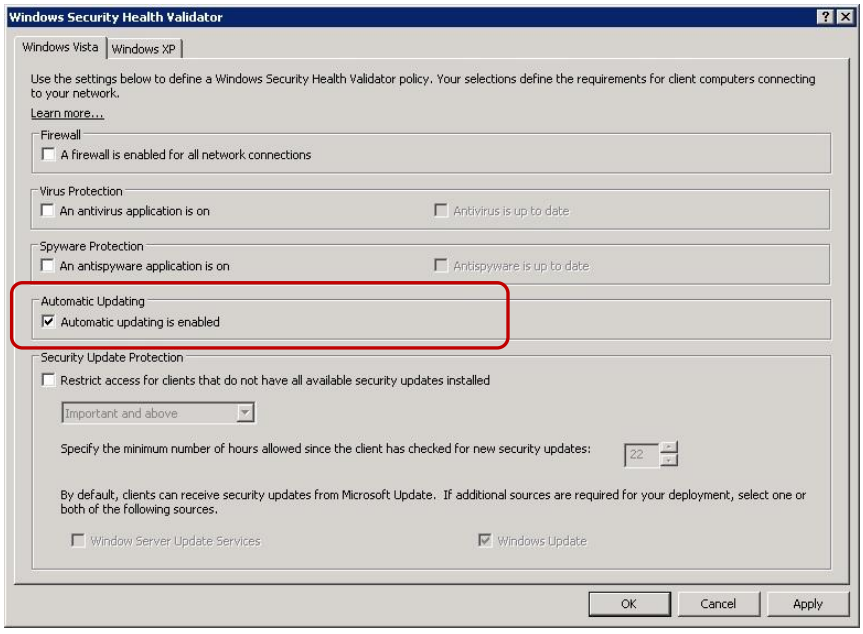
Kuva 18: Virtuaaliverkko terveille työasemille

Tämän jälkeen wizard siirtyy terveyspolitiikan määrittelyyn. Varmistetaan, että WSHV on valittuna (kuva 19):



Kuva 19: Terveyspolitiikan määrittely

Kun kaikki politiikat on luotu, siirrytään SHV:n konfiguroimiseen (NPS-konsoli – Network Access Protection – System Health Validators). Windows XP- ja Windows Vista -käyttöjärjestelmille on omat SHV:t, kumpaankin SHV:hen määrittelin automaattiset päivitykset pakollisiksi (kuva 20):



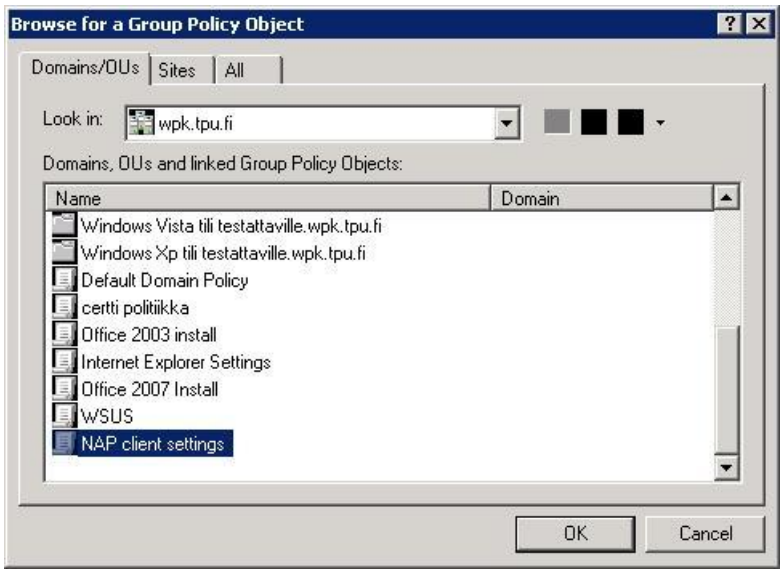
Kuva 20: SHV

NPS-palvelin on konfiguroitu NAP-terveyspalvelimena.

7.7 Ryhmäpolitiikat

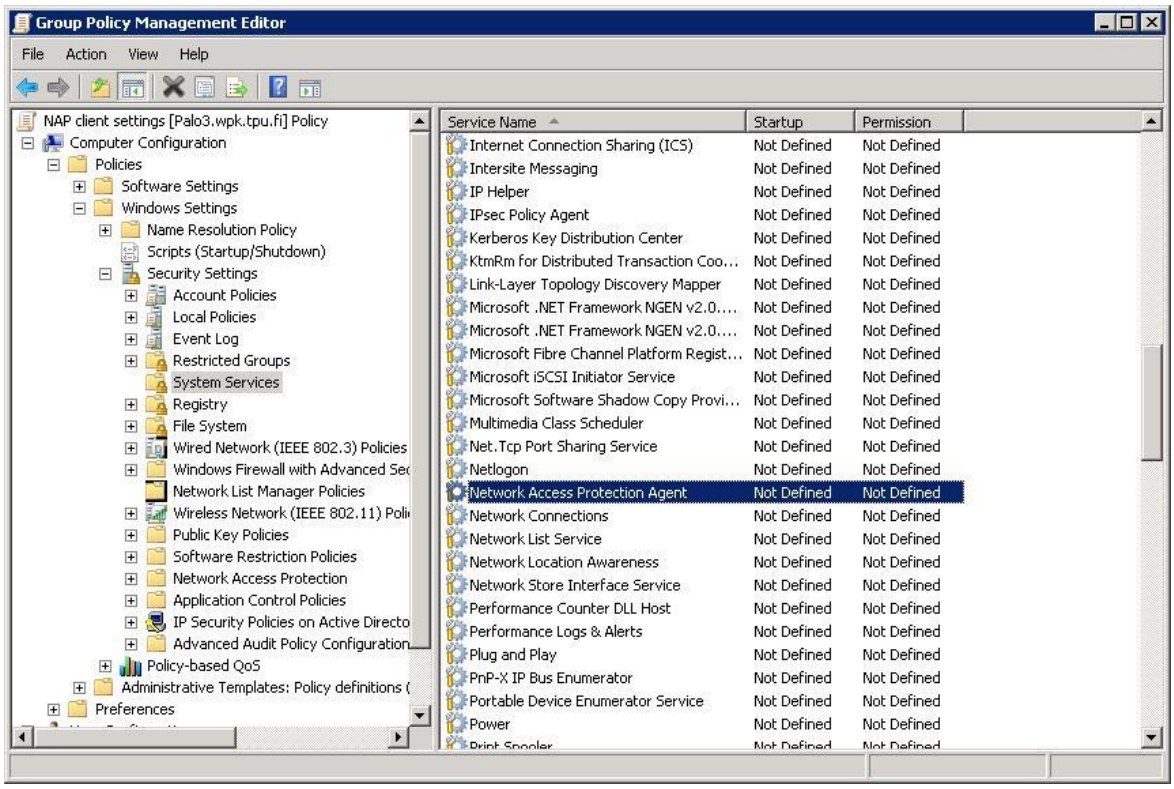
WPK-verkon ryhmäpolitiikat ovat aktiivihakemiston tapaan kahdennettu PALO3- ja PALO4-palvelimille. PALO3-palvelimelle ryhmäkäytäntöjen hallintokonsolin (Group Policy Management console) avulla luodaan uusi ryhmäkäytäntöobjekti nimeltään ”NAP client settings”. Käytäntöihin määritellään työasemat, joita nämä käytännöt tulevat koskemaan, NAP-suojauksen agentti palvelun ja Wired Autoconfig -palvelun asetuksia sekä Security Centerin käyttöliittymän.

Jotta pääsisi muokkaamaan GPO:n käytäntöjä, täytyy kyseisen GPO:n avata Group Policy Management -editoriin. Editori käynnistyy komentokehotteesta komennolla gpme.msc. Ensin valitaan ryhmäkäytäntö, jota halutaan käsitellä (kuva 21):



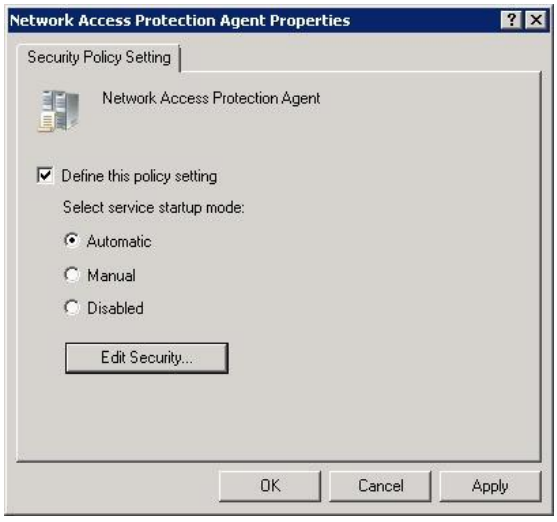
Kuva 21: wpk.tpu.fi –toimialueen ryhmäkäytäntöobjektit

Painamalla OK-painiketta avautuu editori. Ensin navigoidaan tietokoneasetuksiin Policies/Windows Settings/Security Settings/System Services -polun mukaisesti ja kaksoisklikataan Network Access Protection Agent (kuva 22):



Kuva 22: System Services

Network Access Protection Agentin asetuksista otetaan ryhmäkäytäntöasetus käyttöön ja sen käynnistystavaksi valitaan automatic (kuva 23):

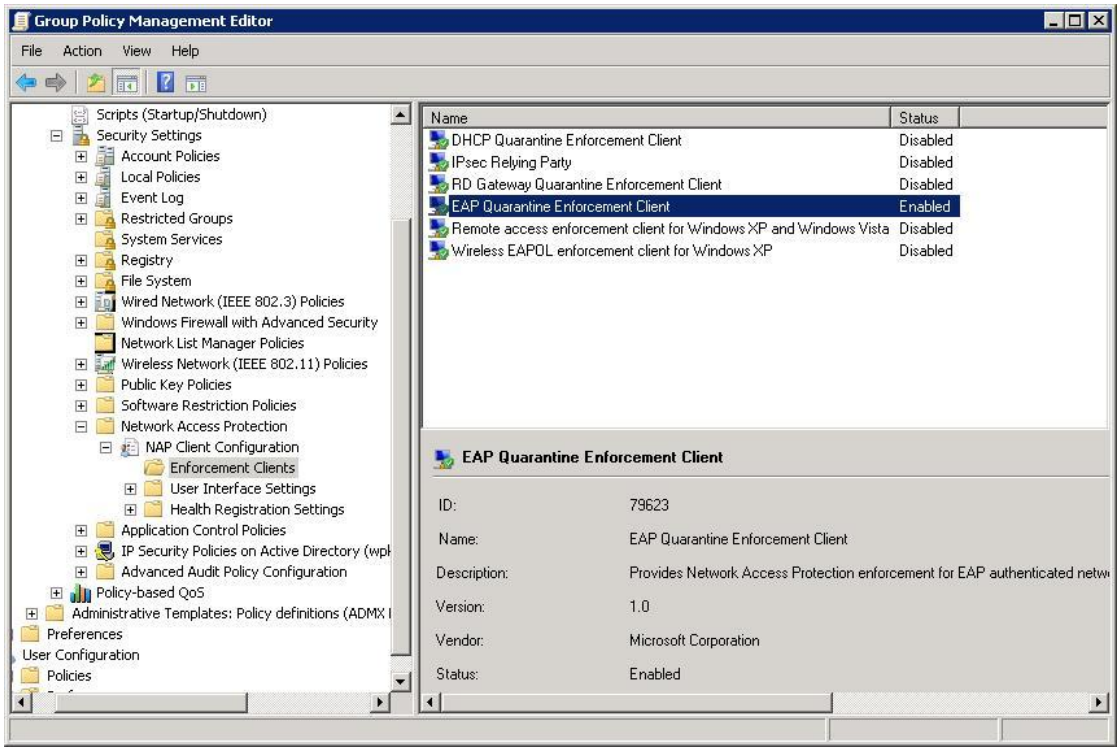


Kuva 23: Network Access Protection Agentin asetukset

Saman polun alta palvelut-listalta löytyy myös Wired AutoConfig, jolle tehdään täysin samat toimenpiteet kuten aikaisemmin Network Access Protection agentille (kuva 24):

Kuva 24: Wired AutoConfig

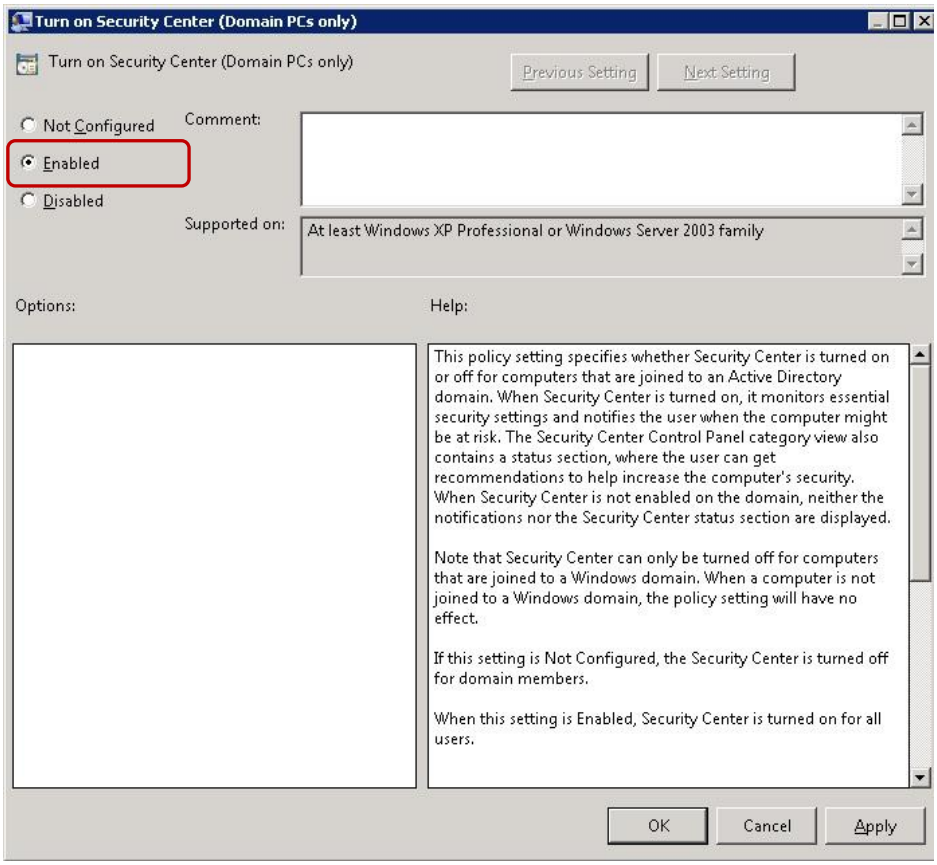
Seuraavaksi mennään Network Access Protection/NAP Client Configuration/Enforcement Clients -polun alle, klikataan sen alta löytyvää EAP Quarantine Enforcement Clientiä (karanteenin pakotusasiakastoiminto) ja vaihdetaan sen statukseksi Enabled (kuva 25):



Kuva 25: EAP Quarantine Enforcement Client

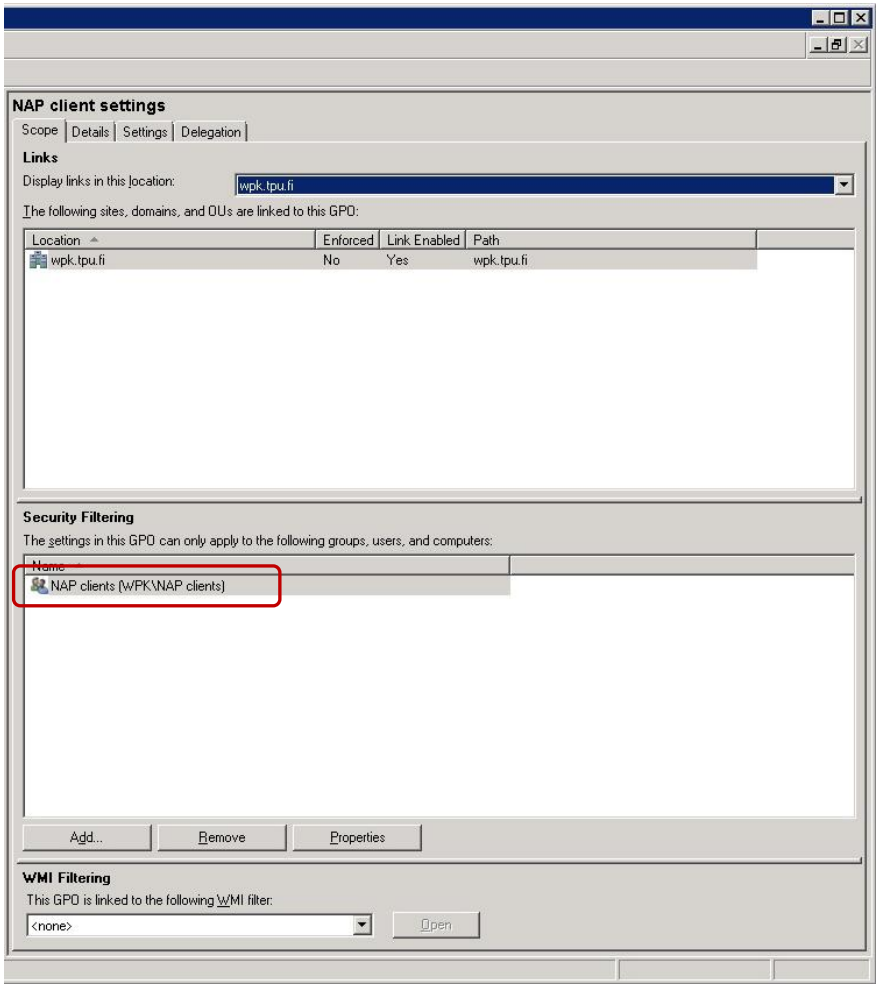
Konsoli-ikkunan vasemmasta laidasta klikataan NAP Client Configuration ja avatusta Asetukset-ikkunasta valitaan Enabled.

Navigoidaan Computer Configuration/Policies/Administrative Templates /Windows Components /Security Center -polun alle, kaksoisklikataan konsolin vasemmassa laidassa olevaa Turn on Security Center (Domain PCs only) ja valitaan Enabled (kuva 26):



Kuva 26: Turn on Security Center

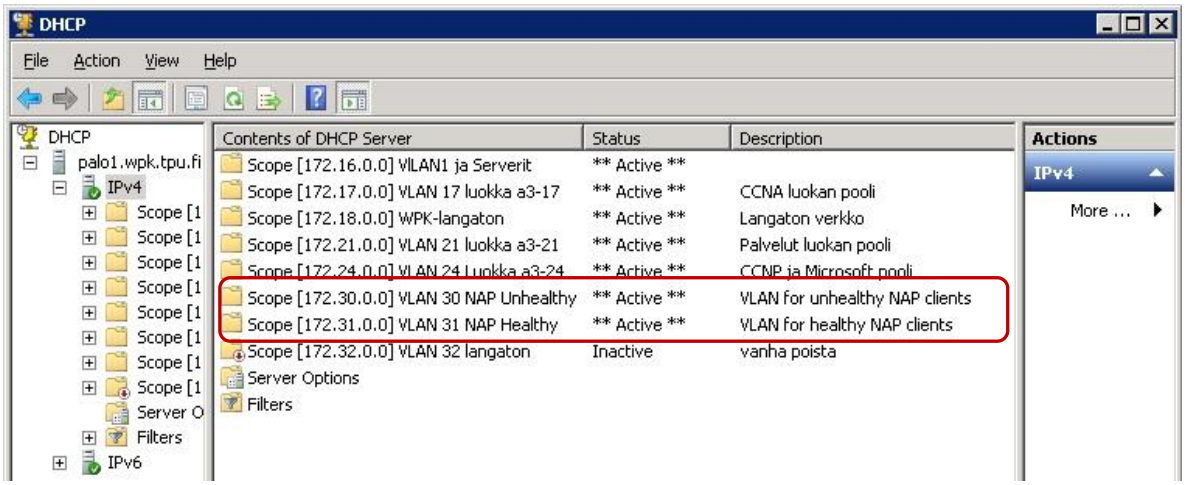
Seuraavaksi määritellään työasemia, joita äsken luotu GPO tulee koskemaan. Group Policy Managerissa navigoidaan NAP clients settings -ryhmäkäytäntöobjektiin, Security Filtering -kohdasta otetaan pois Authenticated Users ja lisätään sen tilalle NAP clients -käyttäjäryhmä (kuva 27):



Kuva 27: Security Filtring

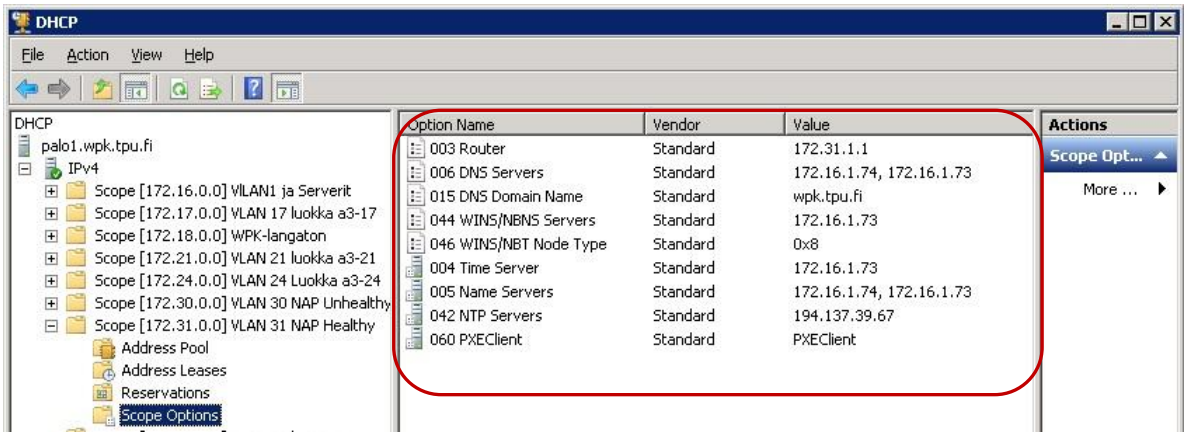
7.8 DHCP

PALO1 ja PALO2 toimivat WPK-verkon DHCP-palvelimina. PALO1-palvelimelle määritin IP-osoiteavaruudet jaettavaksi aiemmin luotuja virtuaaliverkkoja varten, eli yksi Healthy-virtuaaliverkkoa varten ja yksi Unhealthy-virtuaaliverkkoa varten (kuva 28):



Kuva 28: IP-osoiteavaruudet virtuaaliverkoille

IP-osoiteavaruudet luodaan wizardin avulla, esimerkiksi Healthy-virtuaaliverkkoa varten määritellään jaettavan osoiteavaruuden välille 172.31.0.1 – 172.31.255.254, verkkomaskiksi 255.255.0.0 ja muita asetuksia, kuten kuvasta 29 näkyy:



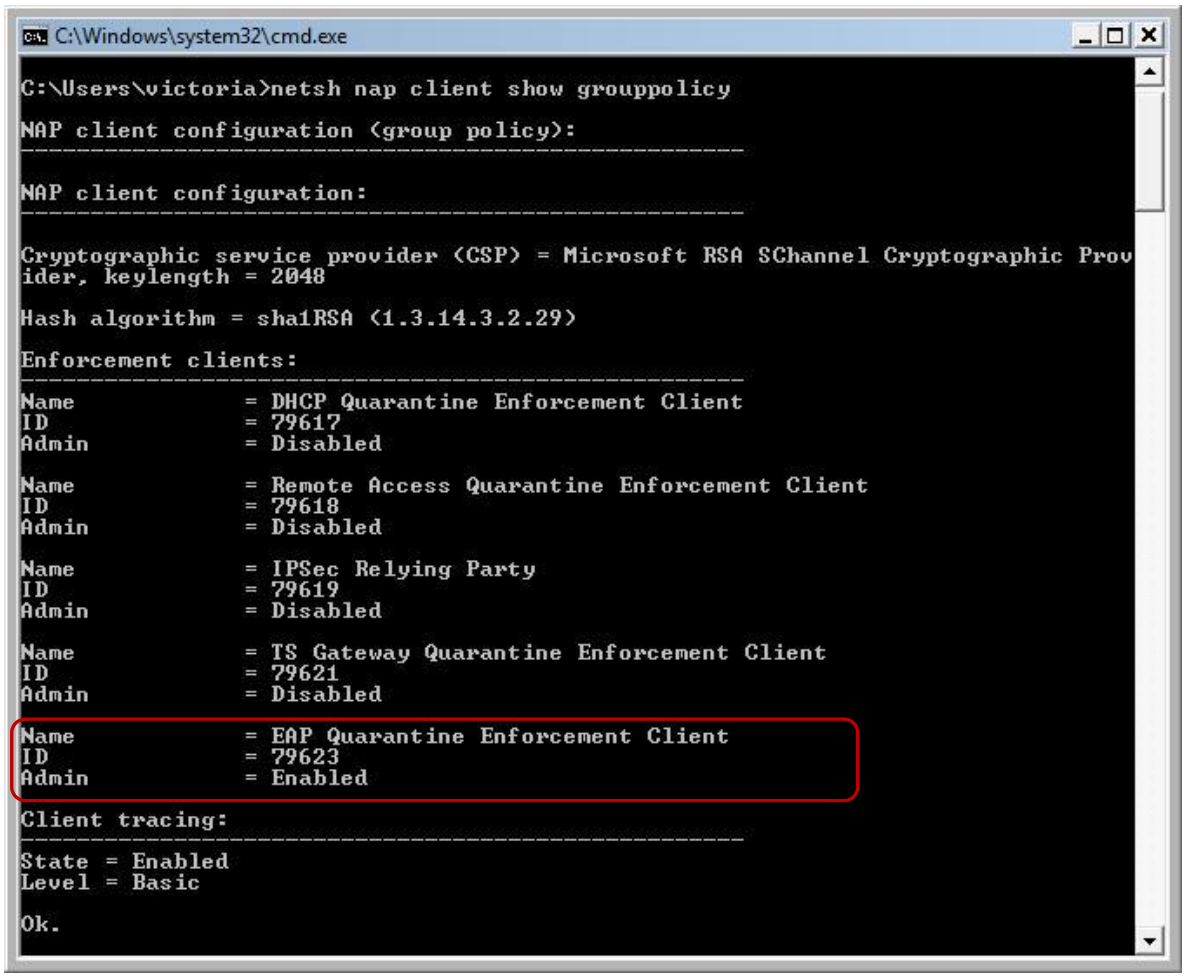
Kuva 29: IP-osoiteavaruuden asetukset

7.9 Työasemat

Testityöasemina käytetään Windows Vista ja Windows XP työasemia (tämän aliluvun kuvakaappaukset on otettu Vista-koneella). Koneiden toimialueen jäseniksi liittämisen jälkeen, lisätään ne NAP clients -ryhmään. Tässä vaiheessa työasemat täytyy käynnistää uudelleen, jotta ryhmäpolitiikan kautta tulleet muutokset astuisivat voimaan. Komentokehotteesta voidaan tarkistaa, saivatko työasemat kaikki ryhmäkäytäntöasetuksensa. Tätä varten käytin kahta eri komentoa:

netsh nap client show grouppolicy

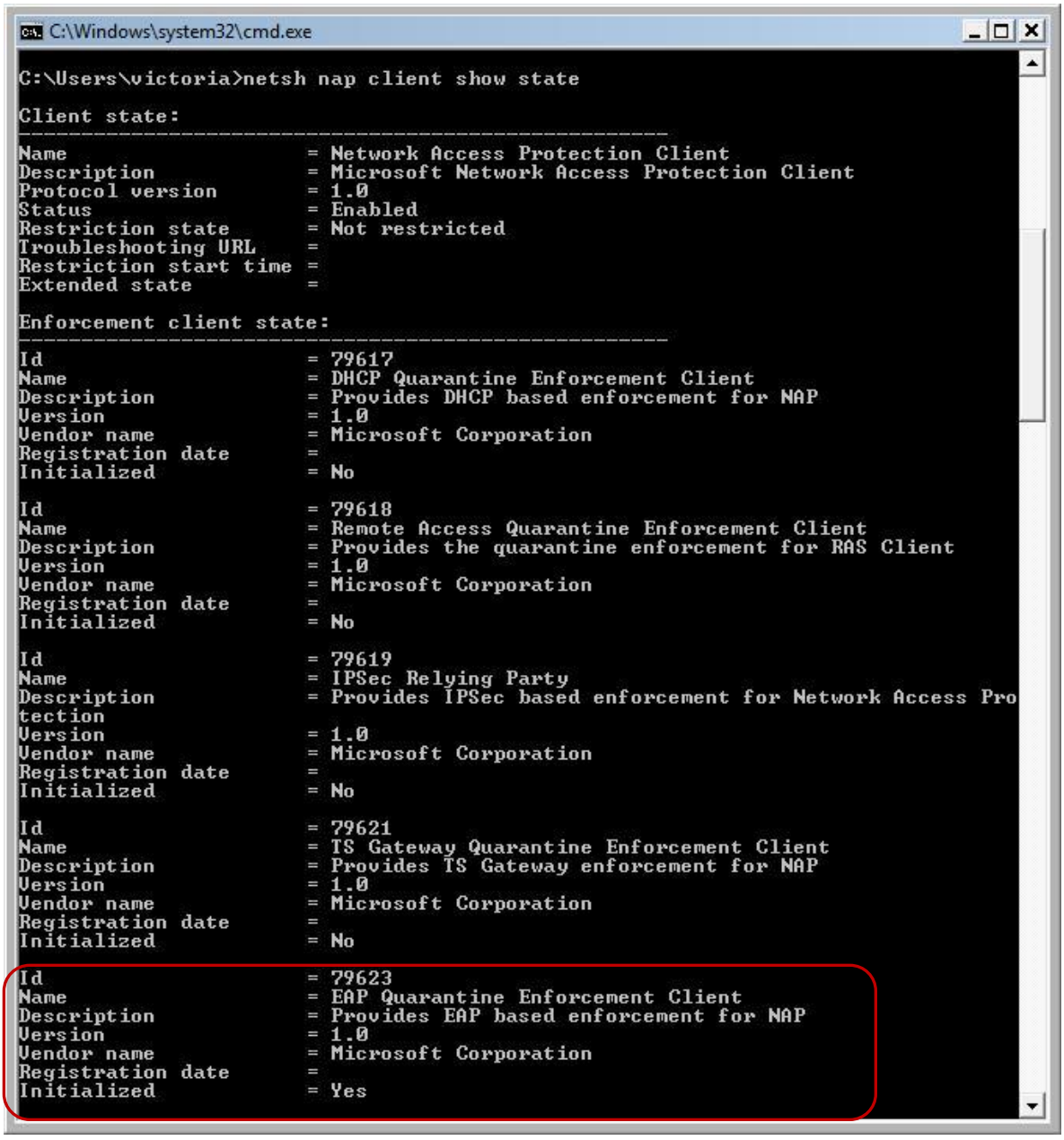
Kuvassa 30 näkyy komennon tuloste. EAP Quarantine Enforcement Clientin statuksena tulee olla Enabled:



Kuva 30: Ryhmäkäytäntöasetusten tarkastaminen komentokehotteesta

netsh nap client show state

Tämän komennon tulosteesta täytyy tarkistaa, että EAP Quarantine Enforcement Clientin Initialized-status on Yes (kuva 31):

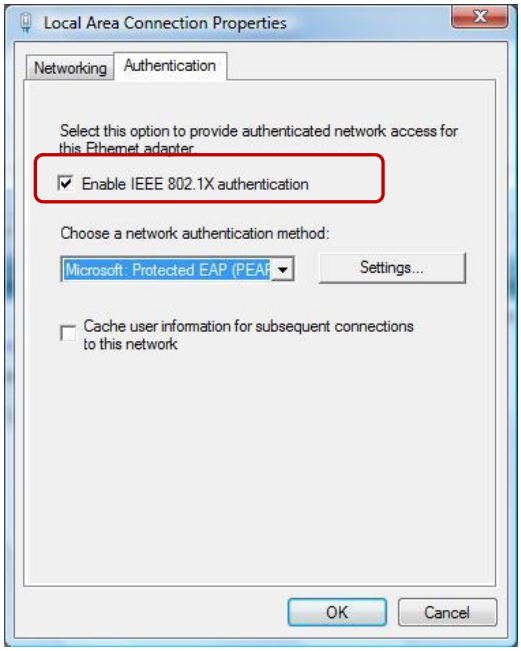


Kuva 31: Ryhmäkäytäntöasetusten tarkastaminen komentokehotteesta

Jos työasema ei saa ryhmäpolitiikan kautta oikeita asetuksia (niin kuin omalla kohdalla kävikin), täytyy silloin käydä Windowsin palveluissa (ohjauspaneeli – valvontatyökalut -

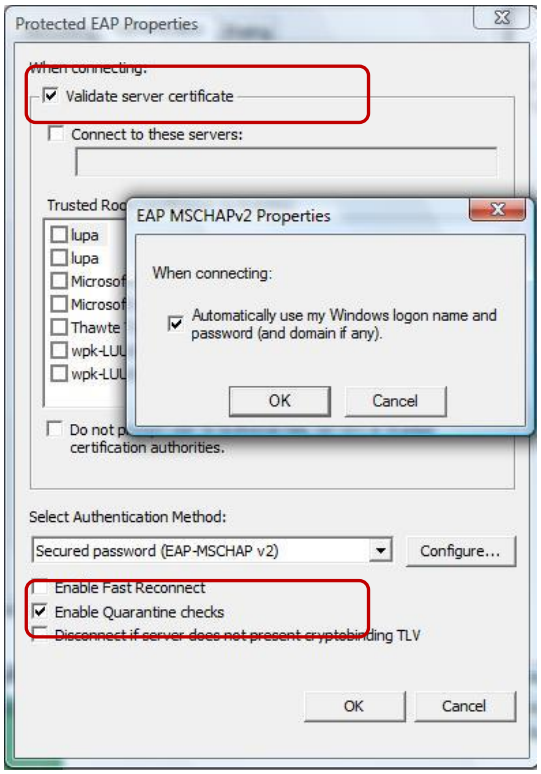
palvelut) laittamassa käsin Network Access Protection agentti – ja Wired Auto Config palvelut automaattisesti käynnistettäviksi ja käynnistää työasema uudelleen.

Seuraava toimenpide on autentikointitavan määrittäminen ja NAP-tarkastuksen päälle kytkentä lähiverkkoyhteyden asetuksista. Lähiverkkoyhteyden asetuksissa Authentication-välilehdellä täytyy varmistaa, että IEEE 802.1x -todennus on otettu käyttöön ja todennusmenetelmäksi on valittu PEAP (kuva 32):



Kuva 32: 802.1x -todennuksen käyttöönotto

Jos Authentication-välilehti puuttuu, todennäköisesti Wired Auto Config (automaattinen lankaverkon määrittäminen) -palvelu ei ole käynnistetty. Tämän jälkeen todennusmenetelmän asetuksista täytyy vahvistaa palvelinsertifikaatti ja ottaa karanteenitarkastukset käyttöön (kuva 33):



Kuva 33: Suojatut EAP-ominaisuudet

8 NAP-suojauksen toimivuuden testaaminen

Projektini viimeinen vaihe oli testata NAP-suojauksen toimivuutta WPK-verkon ympäristössä. Testausta suoritin vaihtamalla työasemien asetuksia verkon vaadittujen turvallisuusehtojen vastaisiksi. Tarkkailin työaseman siirtämistä tuotantoverkosta karanteeniin sekä työaseman että kytkimen päästä.

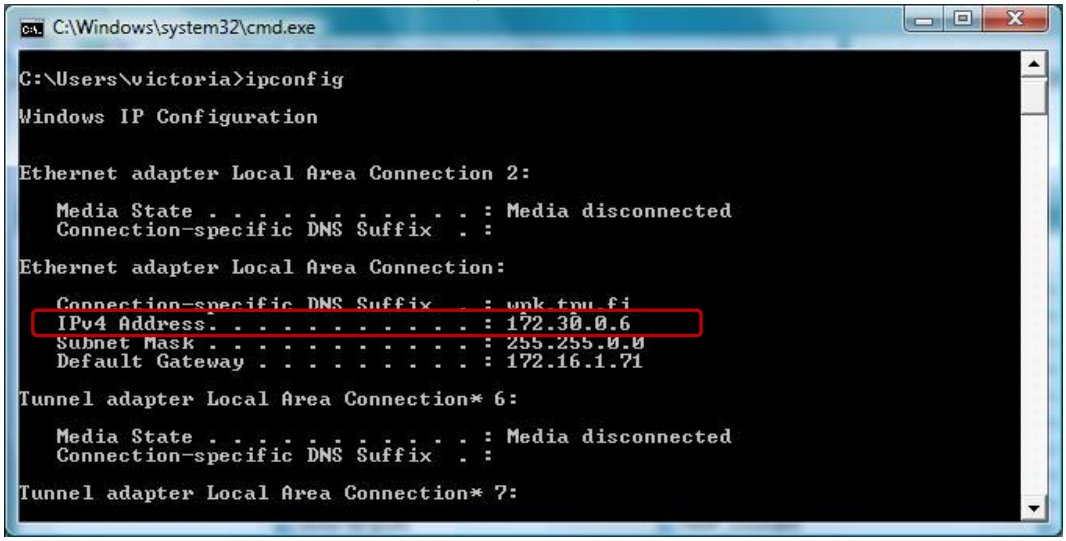
Konfiguroimani SHV:n mukaan työasemissa pitää automaattiset päivitykset olla päällä, joten lähdin testaamaan NAP-suojausta kytkemällä pois päältä automaattiset päivitykset. Hetken päästä ruudun alakulmaan ilmestyi tekstikupla, joka ilmoitti siitä, että työaseman asetukset eivät enää vastaa verkon vaatimuksia ja koneen verkkoyhteys on rajallinen (kuva 34):

Kuva 34: Työasema ei täytä vaadittuja turvallisuusehtoja

Kaksoisklikkaamalla tekstikuplaa, sain näkyville enemmän tietoa tapahtuneesta, mm. ohjeet kuinka työaseman saa taas ”terveeksi” (kuva 35):

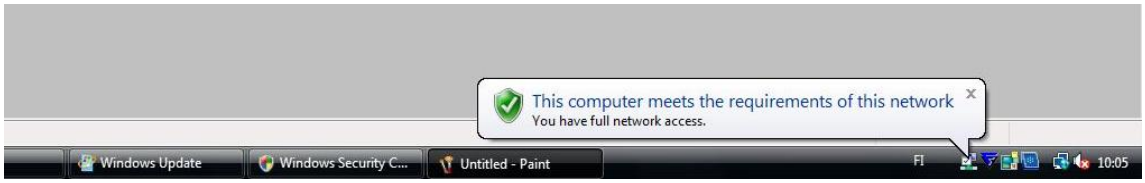
Kuva 35: Ilmoitus työaseman kelpaamattomuudesta verkkoon

Kuvassa 36 olevasta kuvakaappauksesta näkee, että työasema sai osoitteekseen karanteeniverkkoon kuuluvan IP-osoitteen, eli 172.30-alkuisen osoitteen:



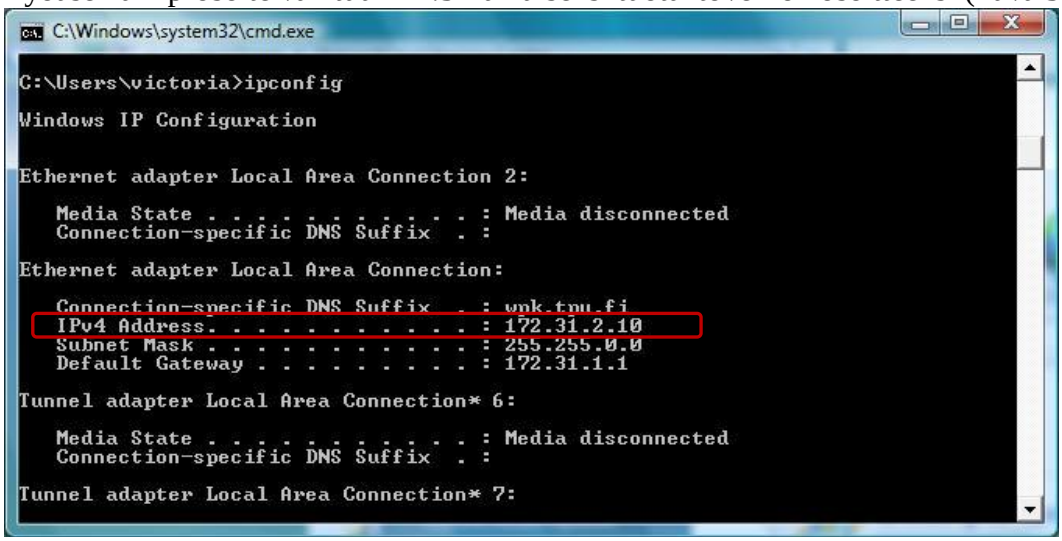
Kuva 36: Unhealthy-verkossa olevan työaseman IP-asetukset

Tämän jälkeen kytkin automaattiset päivitykset takaisin päälle. Windowsin SHA huomaa, että työaseman terveystila on muuttunut ja työasema taas täyttää tuotantoverkon vaatimukset, joten kone välittömästi siirtyy tuotantoverkkoon (kuva 37):



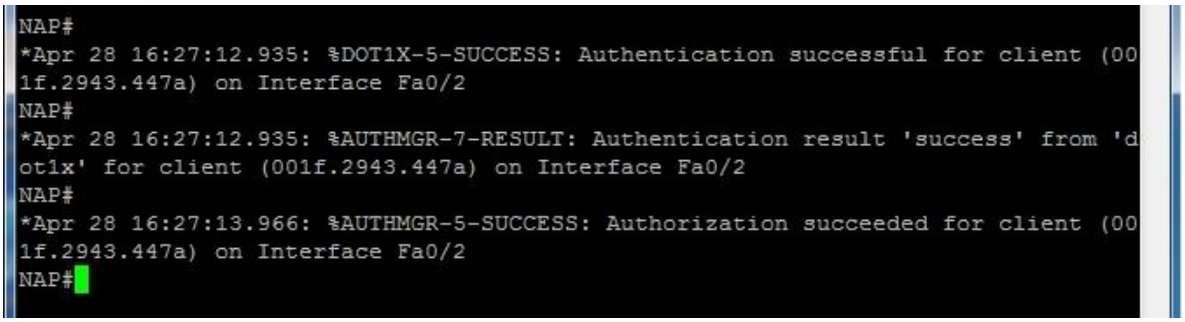
Kuva 37: Työasema täyttää vaaditut turvallisuusehdot

Työaseman ip-osoite vaihtuu 172.31-alkuiseksi tuotantoverkon osoitteeksi (kuva 38):



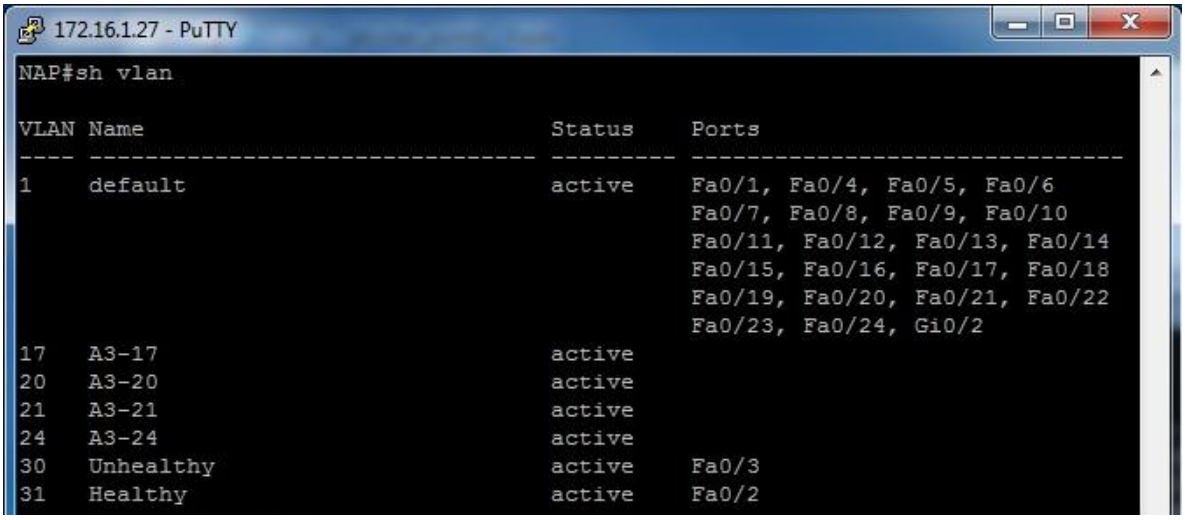
Kuva 38: Healthy-verkossa olevan työaseman IP-asetukset

Seuraava kaappauskuvasarja havainnollistaa, mitä tapahtuu kytkimen päässä, kun työaseman terveystila muuttuu. Työasema on liitetty kytkimen Fa0/2-porttiin, käynnistäessä työasema autentikoituu verkkoon (kuva 39):

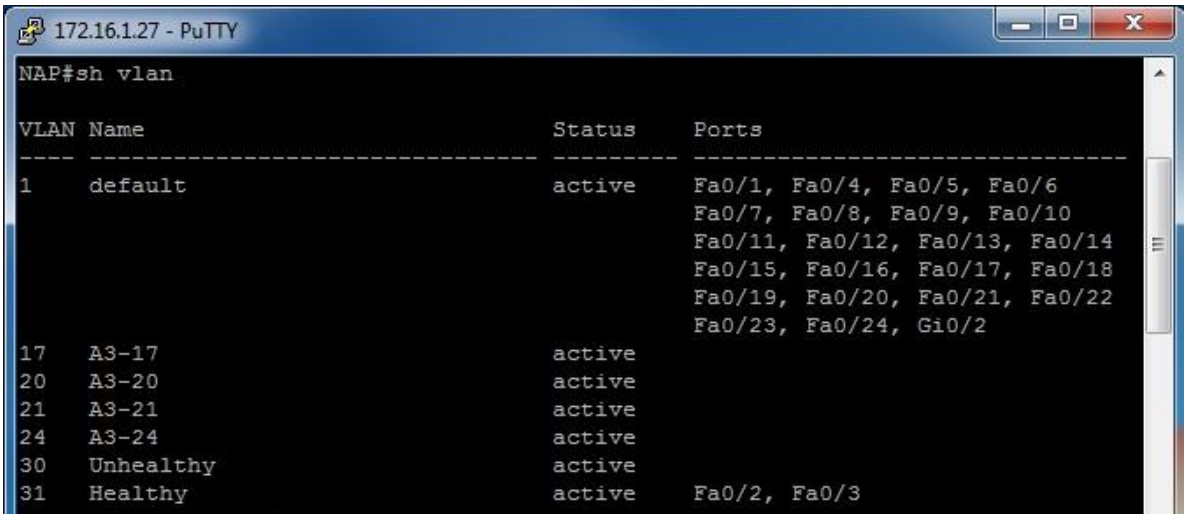


Kuva 39: Kytkin autentikoi työaseman

Autentikoinnin onnistuessa kytkin siirtää Fa0/2-portin tuotantoverkkoon, epäonnistuessa – karanteeniverkkoon. Komennolla **show vlan** pääsee katsomaan mihin VLAN:iin mikäkin portti on sijoitettu (kuva 40-41):

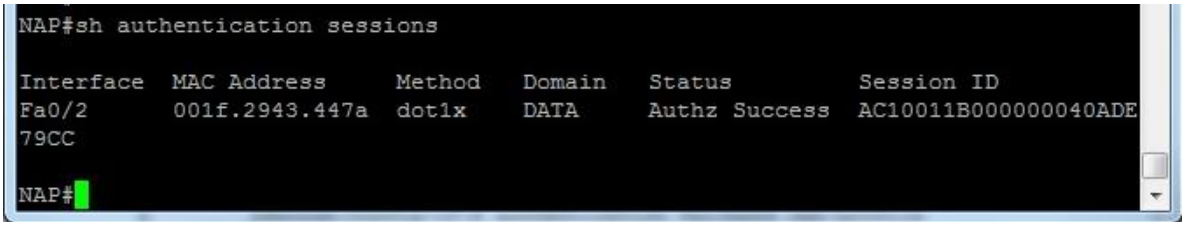


Kuva 40: Show vlan -komento, portti Fa0/2 tuotantoverkossa



Kuva 41: Show vlan -komento, portti Fa0/2 karanteeniverkossa

Komennolla show authentication sessions voidaan tarkistaa autentikointi-istuntoja (kuva 42):



Kuva 42: Show authentication sessions -komento

9 Yhteenveto

Tämän opinnäytetyön tarkoitus oli tutkia verkon pääsynvalvontaa, selvittää mitä todentavan ympäristön rakentaminen vaatii ja myös tutustua NAP-suojauksen toimintaan. Työn alkuosassa tutustuin pääsynvalvonnan perusteisiin ja toimintatapoihin sekä todentavan ympäristön osiin ja NAP-teknologian toimintaperiaatteeseen.

Tärkeämpinä tietolähteinä käytin it-suunnattuja internet-sivustoja, kuten tietokone.fi, ficora.fi, micropc.net ja itpro.fi. Suurin osa tiedoista on hankittu Daviesin ja Northrupin kirjasta ”Server 2008. Networking and Network Access Protection (NAP)”. Joseph Davies on palkittu tekninen kirjoittaja, joka on toiminut TCP/IP:n ja verkkoteknologian kouluttajana vuodesta 1993 lähtien. Kirjan apukirjoittaja Tony Northrup on Windowsin hallinnan, verkon ja turvallisuuden asiantuntija. Kirja kertoo yleisesti verkon pääsynvalvonnasta sekä NAP-suojauksen toimintaperiaatteesta ja konfiguroinnista.

Kun olin ottanut teoriasta selvää, siirryin teorian soveltumiseen käytännössä. Ensimmäiseksi päivitin kytkimen ohjelmiston ja konfiguroin sen suorittamaan siihen kytkettyjen työasemien 802.1x-todentamisen. Seuraavaksi konfiguroin NAP:n käyttämät palvelut tukemaan porttikohtaista autentikointia ja tein muutoksia DHCP-, NPS-, aktiivihakemisto-, sertifikaatti- ja ryhmäpolitiikkapalveluihin. Viimeisenä asensin testityöasemat ja säädin ne todentamaan itsensä verkkoon pyrkiessä.

NAP-suojauksella ei-toivotuilta työasemilta on estetty pääsy WPK-verkkoon ja hylätyt asemat ohjataan eristettyyn karanteeniverkkoon. Karanteeniverkkoon pääsevät myös kaikki autentikoimattomat koneet eli karanteeniverkko toimii ns. vierasverkkona, sillä verkosta on pääsy Internetiin. Myös porttikohtaisen autentikoinnin ja dynaamisen VLAN:n ansiosta kytkimen portit aktivoituvat vain tarpeen mukaan, eivätkä käyttäjät ole sidottuja yhteen tiettyyn porttiin, vaan he voivat vapaasti liikkua tilasta toiseen ja silti verkkoon kytkeytyessä saavat oikeat resurssit käyttöönsä. Kaikki tämä säästää verkon valvojan aikaa työ-

asemien terveyden ja kokoonpanon valvomisessa sekä vierastunnusten ylläpitämisessä ja tekee verkosta turvallisemman.

Työtä tehdessä eniten ongelmia aiheutti kytkimen konfigurointi. Konfiguraatiostani puuttui yksi komento minkä takia autentikointi ei toiminut. Vian ratkaisemiseksi luin kytkimen manuaalit sekä Ciscon konfigurointioppaita. Vaikka tämä työn osuus oli haastava, konfigurointiosaamiseni kehittyi merkittävästi.

Alkuperäisen suunnitelman mukaan tämän päättötyön piti olla valmis talvella v. 2009-2010. Tein opinnäytetyötä työharjoittelun ja ansiotyön ohella, mikä aiheutti aikataulun venymisen. Mikäli tulevaisuudessa kohdalleni osuu toisen opinnäytetyön tekeminen, varaan sille paremman ajankohdan niin että pystyisin keskittymään täysin työn tekemiseen. Työn lopputuloksena viivästyksistä huolimatta sain konfiguroitua toimivan ympäristön.

Tämä opinnäytetyö voi toimia ohjeistuksena samankaltaisen ympäristön rakentamiseen. Tulevaisuudessa ympäristön voi jatkokehittää konfiguroimalla langattoman NAP-suojauksen.

Lähteet

Davies, Joseph & Northrup, Tony 2008. Windows Server 2008. Networking and Network Access Protection (NAP). Redmond, Washington: Microsoft Press

Stamp, Mark 2006. Information security: principles and practice. Hoboken, New Jersey: John Wiley & Sons, Inc.

Barrett, Diane & Weiss, Martin & Kirk Hausman 2003. Security+ Exam Cram. Que Publishing

Verkkolähteet

Tietokone.fi: Työasemat tarkastukseen.
[WWW-sivu].[viitattu 7.5.2009]
Saatavissa:
http://www.tietokone.fi/lukusali/artikkelit/2008tk04/nacvertailu.htm

Wikipedia.org 1: Network Access Control.
[WWW-sivu].[viitattu 7.5.2009]
Saatavissa:
http://en.wikipedia.org/wiki/Network_Access_Control

Wikipedia.org 2: PKI
[WWW-sivu].[viitattu 7.8.2009]
Saatavissa:
http://fi.wikipedia.org/wiki/PKI

Wikipedia.org 3: IPsec

[WWW-sivu].[viitattu 1.8.2009]

Saatavissa:

http://en.wikipedia.org/wiki/Ipsec

Guardsite.com: WatchGuard Zero Day Protection.

[WWW-sivu].[viitattu 22.5.2009]

Saatavissa:

http://www.guardsite.com/ZeroDayProtection.asp

Networkworld.com: Doing your NAC policy homework.

[WWW-sivu].[viitattu 22.5.2009]

Saatavissa:

http://www.networkworld.com/news/tech/2007/011507-techupdate-nac.html

Networkcomputing.com: Tutorial: Network Access Control (NAC).

[WWW-sivu].[viitattu 22.5.2009]

Saatavissa:

http://www.networkcomputing.com/data-protection/tutorial-network-access-control-nac.php

Tlcitgroup.com.au: Agentless and agent-based network access control.

[WWW-sivu].[viitattu 24.5.2009]

Saatavissa:

www.tlcitgroup.com.au/event-Infoexpress/Agent-vs-Agentless.pdf

Nec.co.jp: Quarantine network in the age of internal governance.

[WWW-sivu].[viitattu 25.5.2009]

Saatavissa:

http://www.nec.co.jp/techrep/en/journal/g07/n01/t070104.pdf

Jyu.fi: Autentikointi (todennus).
[WWW-sivu].[viitattu 8.6.2009]
Saatavissa:
https://www.jyu.fi/thk/ohjeet/sanasto/autentikointi

Personaltelco.net: Captive Portal
[WWW-sivu].[viitattu 8.6.2009]
Saatavissa:
http://wiki.personaltelco.net/CaptivePortal

Techtarget.com: What is authorization?
[WWW-sivu].[viitattu 8.6.2009]
Saatavissa:
http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci211622,00.html

Msdn.microsoft.com: Active Directory Domain Services.
[WWW-sivu].[viitattu 9.6.2009]
Saatavissa:
http://msdn.microsoft.com/en-us/library/aa362244(VS.85).aspx

ITpro.fi: Active Directory.
[WWW-sivu].[viitattu12.06.2009]
Saatavissa:
http://www.itpro.fi/wiki/sivut/Identiteetti%20ja%20hakemistot/Active%20Directory.aspx

Informit.com: Role-Based Access Control in Computer Security.
[WWW-sivu].[viitattu 15.6.2009]
Saatavissa:
http://www.informit.com/articles/article.aspx?p=782116

Micropc.net: Työasemat ruotuun ryhmäkäytännöillä.
[WWW-sivu].[viitattu 16.6.2009]
Saatavissa:
http://mikropc.net/rml/arkisto/mikropc/pdf/0303200540.pdf

Ficora.fi: Julkisen avaimen infrastruktuuri.
[WWW-sivu].[viitattu 29.6.2009]
Saatavissa:
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/pki.html

Securiteam.com: An Analysis of the RADIUS Authentication Protocol.
[WWW-sivu].[viitattu 10.7.2009]
Saatavissa:
http://www.securiteam.com/securitynews/6L00B0U35S.html

Microsoft.com 1: How IAS Technology Works.
[WWW-sivu].[viitattu 12.7.2009]
Saatavissa:
http://technet.microsoft.com/en-us/library/cc773343(WS.10).aspx

Microsoft.com 2: Introduction to Network Access Protection
[WWW-sivu].[viitattu 1.8.2009]
Saatavissa:
http://download.microsoft.com/download/8/d/9/8d9b3e54-6db7-4955-9e36-58a3f0534933/NAPIntro.doc

Cyberguru.ru: Защита доступа к сети Network Access Protection (NAP) в Windows 2008 Server.

[WWW-sivu].[viitattu 1.8.2009]

Saatavissa:

http://www.cyberguru.ru/operating-systems/windows-server2008/server2008-nap.html

Windowsnetworking.com: Network Access Protection.

[WWW-sivu].[viitattu 15.8.2009]

Saatavissa:

http://www.windowsnetworking.com/articles_tutorials/Network-Access-Protection-Revisited-Part1.html

Cisco.com: Release Notes for NAC/NAP Interoperability Architecture 1.0

[WWW-sivu].[viitattu 25.11.2009]

Saatavissa:

http://www.cisco.com/en/US/docs/security/nac-nap/1.0/release/notes/NACNAPRN.html

Wpk.tpu.fi: Tervetuloa WPK-verkon kotisivuille.

[WWW-sivu].[viitattu 25.11.2009]

Saatavissa:

https://www.wpk.tpu.fi/default.html

Cisco.com: Configuring IEEE 802.1x Port-Based Authentication

[WWW-sivu].[viitattu 12.01.2010]

Saatavissa:

http://www.cisco.com.ru/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_see/configuration/guide/sw8021x.html#wp1025060

Liitteet

Liite 1: NAP-kytkimen konfiguraatiotiedosto

```
Current configuration : 3933 bytes

version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname NAP

boot-start-marker
boot-end-marker

enable password *****

username cisco password 0 *****
aaa new-model

aaa authentication dot1x default group radius local
aaa authorization network default group radius local

aaa session-id common
system mtu routing 1500
ip subnet-zero

no ip domain-lookup

dot1x system-auth-control

spanning-tree mode pvst
spanning-tree portfast default
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id

vlan internal allocation policy ascending
```

```
interface FastEthernet0/1
 description NAP-client port
 switchport mode access
 authentication event no-response action authorize vlan 30
 authentication port-control auto
 authentication periodic
 dot1x pae authenticator

interface FastEthernet0/2
 description NAP-client port
 switchport mode access
 authentication port-control auto
 authentication periodic
 dot1x pae authenticator

interface FastEthernet0/3
 description NAP-client port
 switchport mode access
 authentication port-control auto
 authentication periodic
 dot1x pae authenticator

interface GigabitEthernet0/1
 switchport mode trunk

interface GigabitEthernet0/2
 switchport mode trunk

interface Vlan1
 ip address 172.16.1.27 255.255.0.0
 no ip route-cache

ip http server
ip http secure-server
radius-server host 172.16.1.54 auth-port 1645 acct-port 1646 key ssalc

control-plane

line con 0
 password *****
 logging synchronous
line vty 0 4
 password *****
 logging synchronous
line vty 5
 password *****
```

```
 logging synchronous
line vty 6 15

end
```