HAAGA-HELIA
ammattikorkeakoulu

Network Access Protection – teknologian käyttöönotto globaalissa yritysverkossa

Antti Ollila

Opinnäytetyö
Tietojenkäsitetlin koulutusohjelma
2013

HAAGA-HELIA ammattikorkeakoulu

Koulutusohjelma

Tiivistelmä

23.09.2013

Tekijä tai tekijät Antti Ollila	**Ryhmätunnus tai aloitusvuosi** 2008
Raportin nimi Network Access Protection –teknologian käyttöönotto globaalissa yritysverkossa	**Sivu- ja liitesivumäärä** 20 + 17
Opettajat tai ohjaajat Sauli Isonikkilä	

Yrityksen sisäverkon tietoturvan tärkeyttä ei voida korostaa tarpeeksi liiketoiminnan jatkuvuuden kannalta. Tekninen tietoturva on kustannustehokas ratkaisu parantaa yrityksen tietoturvaa ja ehkäisee ennalta verkkohyökkäyksiä.

Network Access Protection on Microsoftin vuonna 2008 julkaisema osa Windows Server käyttöjärjestelmää. Sen tehtävänä on tarkastaa jokaisen verkkoon pyrkivän tietokoneen terveydentila ja verrata sitä järjestelmän pääkäyttäjän asettamaan tavoitetasoon. Mikäli tavoitetaso ei täyty, tietokone ohjataan rajoitettuun verkkoon. Kun tarvittava tietoturvan taso on saavutettu, kone voi tarkastuttaa terveydentilan uudestaan ja saada rajoittamattoman pääsyn verkkoon.

Projektissa käytetään DHCP-pakotustapaa eristämään tietokoneet rajoitettuun verkkoon. Kyseinen pakotustapa on teknologian pakotustavoista heikoin, ja se ennaltaehkäisee tahatonta verkon saastuttamista. Suojauksesta ei ole hyötyä, jos joku haluaa tahallaan saastuttaa yrityksen tietoverkon ja omaa tarvittavan tietotaidon sen tekemiseen.

Tämän opinnäytetyöprojektin tarkoituksena on hankkia tarvittava tieto Network Access Protection –teknologian käyttöönottoa varten, rakentaa toimiva konsepti teknologiasta virtuaaliympäristössä ja ottaa teknologia käyttöön yrityksen verkossa.

Projekti toteutettiin toimeksiantona yritykselle pääosin keväällä 2013.

Projektin tuloksena sain otettua käyttöön Network Access Protection –teknologian kuudessa yrityksen seitsemästä toimistosta, joissa on paikallinen palvelin.

Asiasanat
Network Access Protection, Windows Server 2008 R2, tietoturva

HAAGA-HELIA
University of Applied Sciences

Abstract

23.09.2013

Degree programme

Authors Antti Ollila	**Group or year of entry** 2008
The title of thesis Implementing Network Access Protection –technology in a global corporate network	**Number of pages and appendices** 20 + 17
Supervisor(s) Sauli Isonikkilä	

The security of a company's internal network cannot be emphasized enough for the sake of business continuity. Different technical solutions for information security are usually cost-effective ways to improve corporate information security and prevent network attacks.

Network Access Protection has been part of Windows Server operating systems since 2008. Main function of the technology is to check the health state of computers that are trying to gain access to the corporate network and compare it to reference level set by network administrator.
If the reference level is not met, the computer in question can be directed to a restricted network until the required level of security has been met. When the level is met, the computer can request access again and gain unrestricted access to the corporate network.

The solution in this project will rely on DHCP-enforcement of Network Access Protection. The enforcement in question is the weakest of the four different enforcement method and it will only prevent accidental damage to the corporate network. DHCP-enforcement does not help if a person with enough knowledge wants to sabotage the network.

The purpose of this project is to gain enough knowledge and information to deploy Network Access Protection, build a working proof of concept in a virtualized environment and finally deploy the technology in the production environment of company X.

This project was implemented in spring 2013 as an assignment from the company.

As the result I managed to deploy Network Access Protection successfully six of the seven offices worldwide.

Key words
Network Access Protection, Windows Server 2008 R2, information security

Sisällys

1 Johdanto

Yrityksen sisäverkon tietoturvan tärkeyttä ei voida korostaa tarpeeksi liiketoiminnan jatkuvuuden kannalta. Asiakasyritys on viime vuosien aikana noussut suureksi globaaliksi toimijaksi alallaan ja ei ole järkevää pitää jokaisessa toimistossa palkkalistoilla IT ammattilaista. Ihmisresurssit ovat kalliita ja verkon tietoturvan ollessa kyseessä tekniset ratkaisut tulevat usein halvemmiksi ja tehokkaammiksi kuin ihmiset.

Yrityksen toimiessa maailmanlaajuisesti, on käytännössä mahdotonta valvoa luotettavasti verkkoon liitettyjä laitteita ja niiden tietoturvatasoa jokaisessa toimipisteessä. Riskiä lisää myös se, että suurin osa yrityksen tietokoneista on kannettavia tietokoneita joita työntekijät käyttävät myös yrityksen sisäverkon ulkopuolella.

Verkon tietoturvan parantamiseksi Microsoft on julkaissut Windows Server 2008 – palvelinkäyttöjärjestelmän mukana Network Access Protection – teknologian. Teknologia tarkastaa jokaisen sisäverkkoon pyrkivän tietokoneen ja varmistaa että verkon järjestelmänvalvojan ennalta määrittelemät ehdot täyttyvät, ennen kuin tietokoneelle myönnetään rajoittamaton pääsy verkkoon. Tämän kaltaisia ehtoja ovat esimerkiksi käyttöjärjestelmän päivitysten taso sekä ajan tasalla oleva virustorjuntaohjelmisto. (Microsoft 2008, 1.)

Mikäli ennalta määritellyt ehdot eivät täyty, tietokone suljetaan pois yrityksen sisäverkosta. Järjestelmänvalvoja voi halutessaan määrittää erikseen palvelimet, joihin rajoitetulla yhteydellä pääsee. Tälläisiä palvelimia voivat esimerkiksi olla päivityspalvelimet, joiden avulla rajoitettu tietokone voi päivittää itsensä saavuttaakseen tarvittavan tietoturvan tason päästäkseen sisäverkkoon. (Microsoft 2008, 1-2.)

Opinnäytetyöni tarkoituksena on ottaa yllämainittu teknologia käyttöön tilaajayrityksen verkossa. Tämä opinnäytetyö on raportti teknologian käyttöönoton suunnittelusta, testaamisesta ja itse käyttöönotosta.

Oppimistavoitteena minulla on soveltaa koulussa sekä työelämässä oppimiani Windows – palvelinympäristön ylläpitotaitoja sekä osoittaa osaamiseni hakea lisää tietoa aiheesta Microsoftin julkaisemaa painettua sekä verkkomateriaalia hyväksikäyttäen.

2 Network Access Protection

Network Access Protection, lyhennettynä NAP, on Microsoftin Windows Server 2008:n mukana julkistama sisäverkon suojausteknologia. Se auttaa vähentämään yrityksen sisäverkkoon kohdistuvia tietoturvariskejä työasemien tietoturvan osalta. Teknologia mahdollistaa yrityksen sisäverkkoon pyrkivien tietokoneiden päivitystason valvonnan sekä turvallisuusriskeiksi koettujen tietokoneiden verkkoon pääsyn rajoittamisen kunnes tarvittava tietoturvan taso on tavoitettu. (Microsoft 2008, 1.)

2.1 NAP:n tehtävä

Network Access Protection – teknologian tehtävä on tarkastaa sisäverkkoon pyrkivät tietokoneet tietoturvariskien varalta. Teknologia kykenee tarkastamaan Microsoftin sekä monien muiden ohjelmistovalmistajien sovellusten päivitystason. Mikäli taso ei vastaa järjestelmänvalvojan määrittämää tasoa, tietokoneen pääsyä verkkoresursseihin voidaan rajoittaa. (Microsoft 2008, 2-3.)
Rajoitetusta verkosta voi määrittää erikseen pääsyn tarvittaviin paikkoihin, kuten esimerkiksi välityspalvelimen kautta internetiin tai päivityspalvelimille. Päivityspalvelimille tai internetiin pääsy vaaditaan, että tietokone voi noutaa tarvittavat päivityksen ennalta määritellyn tietoturvatason saavuttamiseksi. (Microsoft 2008, 2-3.)

Halutessaan järjestelmänvalvoja voi myös ottaa teknologian käyttöön seurantamoodissa, missä palvelin ilmoittaa järjestelmänvalvojalle tietokoneet joiden konfiguraatioissa on puutteita, mutta ei estä verkkoon pääsyä(Microsoft 2007).

Network Access Protection valvoo pelkästään tietoturvan teknistä tasoa. Se ei poista muun muassa sitä riskiä, että käyttäjä, joka omaa tarvittavat käyttöoikeudet ja jonka tietokoneella on tietoturva vaaditulla tasolla, tahallaan tai tahattomasti ajaa verkossa haittaohjelmia. (Microsoft 2011b.)

2.2 NAP:n ominaisuudet

Kaikki Network Access Protection – teknologian ominaisuudet perustuvat verkkoon pyrkivien tietokoneiden terveystarkastukseen(eng. Health state validation). Nimensä mukaan kyseinen ominaisuus tarkastaa tietokoneen ”terveyden” eli päivitysten tason ja sen että palomuuri ja virustorjuntaohjelmistot ovat kytkettyinä päälle.
Toinen teknologian tärkeä ominaisuus on se, että se voi pakottaa verkkoon pyrkivän, toimialuueeseen kuuluvan koneen asentamaan tarvittavat päivitykset jos yrityksen sisäverkossa on sitä tukeva hallintapalvelin. NAPn tukemia hallintapalvelinohjelmistoja ovat esimerkiksi Microsoft System Management Server ja Windows Server Update Services. (Microsoft 2008, 4; Vorobieva 2010, 24-25.)

2.3 NAP:n komponentit

Vaikka teknologian toimintaperiaate itsessään on hyvin yksinkertainen, koostuu se useista eri komponenteista. Kyseiset komponentit voidaan karkeasti jakaa kahteen ryhmään, asiakaskoneella toimiviin ja palvelimella toimiviin komponentteihin.
Alla on listaus komponenteista sekä lyhyt kuvaus niiden ominaisuuksista. (Microsoft 2008, 4; Vorobieva 2010, 24-26.)

Statement of Health (SoH)	Statement of Health on koneen luoma terveysraportti, joka lähetetään NAP Agentille.
System Health Agent (SHA)	System Health Agentit tarkastavat, että palvelimelta määritellyt terveysvaatimukset täyttyvät ja lähettävät näistä Statement of Health -raportin NAP Agentille.
NAP Agent	NAP Agentti kerää yhteen kaikki terveysraportit ja lähettää ne eteenpäin NAP-hallintapalvelimelle.
Enforcement Client (EC)	Enforcement Client panee täytäntöön NAP-palvelimelta määritellyn eristyspolitiikan tarvittaessa.

Taulukko 1: Asiakaskoneella toimivat komponentit

Remediation Server	Remediation Server on palvelinkone, jolta löytyvät tarvittavat päivitykset ja määritykset tietokoneen saattamiseksi kelpoiseksi liittymään sisäverkkoon.
System Health Validators (SHVs)	System Health Validatorit toimivat palvelinpuolella System Health Agenttien vastineena. Validatorit tarkastavat NAP-agentin lähettämät raportit ja koostavat niistä vastineen asiakaskoneen terveysraportille.
Health Policies	Health Policies, eli terveyssäännöt, määrittävät asiakaskoneilta vaaditun tietoturvatason.
Statement of Health Response(SoHR)	SoHR on raportti joka, lähetetään takaisin asiakaskoneen Enforcement Clientille. Mikäli raportti ilmoittaa kaiken olevan kunnossa, asiakaskone päästetään sisäverkkoon. Ja jos kaikki ei ole kunnossa, asiakaskoneelle lähetään tieto, mitä pitää korjata.

Taulukko 2: Palvelinkoneilla toimivat komponentit

2.4 NAP:n eri toteutustavat

Network Access Protection teknologia tukee neljää eri toteutustapaa. Nämä eri tavat ovat listattuna alla, osa tavoista tarvitsee sitä tukevan laitteiston toimiakseen, kun taas osa toimii pelkästään ohjelmiston avulla(Microsoft 2008, 4.)

2.4.1 IPsec-toteutus

IPsec-toteutustapa on Network Access Protectionin pakotustavoista vahvin. Se myös antaa järjestelmänvalvojalle eniten mahdollisuuksia koneiden tarkistuksen ja pääsyn rajoittamisen suhteen. Nimensä mukaan IPsec-toteutus käyttää IPseciin kuuluvia protokollia tietokoneen turvatason tarkistamiseen. (Microsoft 2012.)
Tämän toteutuksen suurin vahvuus on se, että terveystarkastusta tai pääsynvalvontaa ei voi ohittaa toisin kuin joissain heikommissa toteutustusmalleissa. IPsec-liikenne voidaan myös salakirjoittaa eli kryptata ja se ei tarvitse mitään erityistä laitteistoa toimiakseen, kunhan kaikki palvelin- ja asiakaskoneet ovat konfiguroitu tukemaan sitä. (Microsoft 2012a.)

2.4.2 IEEE 802.1X-toteutus

IEEE 802.1x on standardoitu portteihin perustuva verkon pääsynvalvontateknologia. Se kuuluu osaksi IEEE 802.1 verkkoprotokollaryhmää. Tämä toteutustustapa tarvitsee sitä tukevan verkkolaitteiston toimiakseen. Toteutustavan vahvuutena on se, että rajoitettu verkko voidaan toteuttaa kytkimiin virtuaaliverkkoja hyväksikäyttäen. (Microsoft 2008, 5; Vorobieva 2010, 28.)

2.4.3 VPN-toteutus

VPN-toteutustapaa voidaan hyödyntää silloin, kun asiakastietokoneet pyrkivät verkkoon muualta kuin yrityksen sisältä. Toteutusta varten IT-ympäristössä pitää olla jo käytössä Microsoftin VPN yhteydet. (Microsoft 2012b; Microsoft 2008, 5).

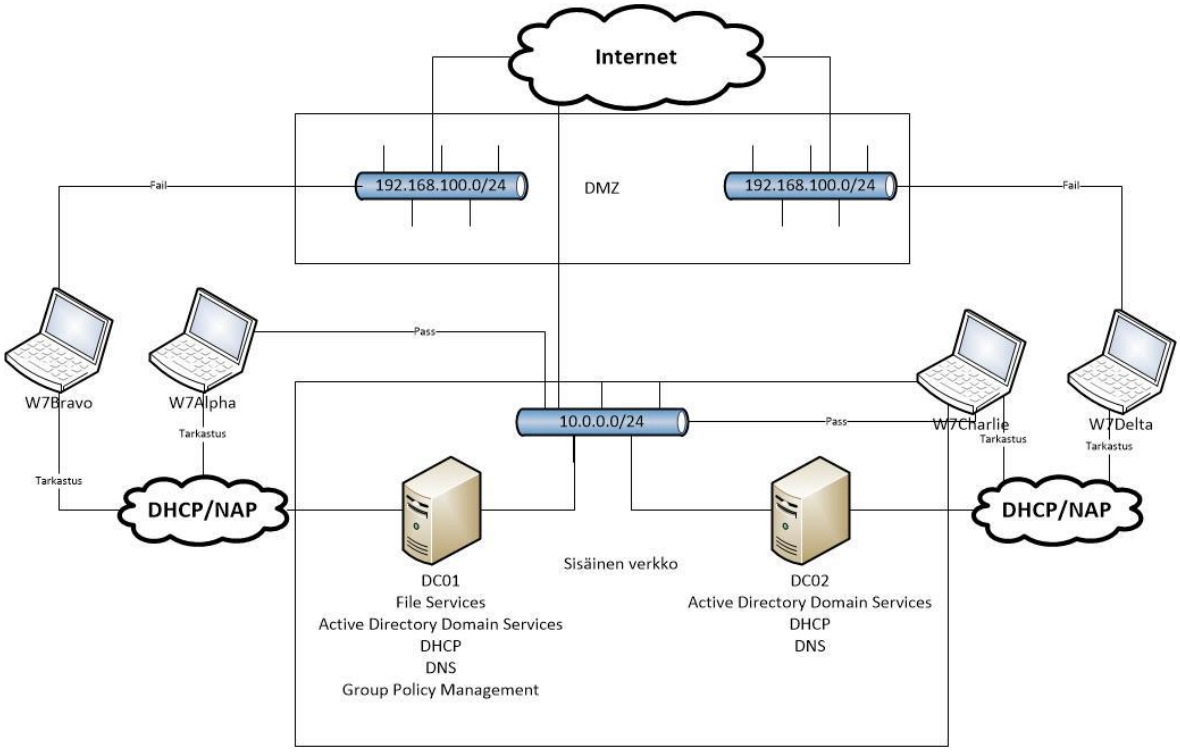
2.4.4 DHCP-toteutus

DHCP-toteutus on Network Access Protection teknologian heikoin toteutustapa. Sitä käytettäessä, kone tarkistetaan vain kun se hakee uutta verkko-osoitetta DHCP-palvelimelta. Tavan vahvuus on se, että se on helppo ottaa käyttöön, eikä se tarvitse mitään muita ohjelmisto- tai laitehankintoja. (Microsoft 2008, 6.)

3 Testaus virtuaaliympäristössä

Yrityksen verkon monimutkaisuuden takia testaus on erittäin suuressa osassa opinnäytetyöprojektia.
Testausta varten rakennetaan testiympäristö, joka jäljittelee yrityksen olemassa olevaa tuotantoinfrastruktuuria. Testausta varten tarvitaan kaksi virtuaalista palvelinta sekä kaksi virtuaalista työasemakonetta. Testiverkossa on kaksi sitea, joiden tarkoitus on toimia eri toimipisteiden verkkolokaatioina. Alaluvuissa on tarkemmat tiedot testiympäristöstä sekä testitapauksista.

Testiympäristö on toteutettu yksinkertaistettua Microsoftin laboratorioympäristöä jäljitellen. Testiympäristö on rakennettu VMWare Workstation virtualisointiohjelmiston päälle. Alustava testaussuunnitelma löytyy liitteestä 1.



Kuva 1: Testiympäristö

3.1 Testipalvelimet

Testiympäristössä molemmilla siteilla toimii yksi palvelin. Pääkonttorin palvelimen nimi on DC01 ja sivukonttorin DC02. Molemmissa palvelimessa käyttöjärjestelmänä toimii

Windows Server 2008 R2. Pääkonttorin palvelimen IP-osoite on 10.0.0.1 ja sivukonttorin 10.0.0.2.

Pääkonttorin palvelimella on käytössä seuraavat roolit ja ominaisuudet:

- Active Directory Domain Services
- DHCP Server
- DNS Server
- File Services
- Group Policy Management
- Network Policy and Access Services
    - Network Access Protection
        - Windows Security Health Validator
        - F-Secure Health Validator
- Active Directory Certificate Services
- Web Server(IIS)

Sivukonttorin palvelimessa on käytössä seuraavat roolit:

- Active Directory Domain Services
- DHCP Server
- DNS Server

3.2 Testityöasemat

Testiympäristössä toimii kaksi virtuaalista työasemakonetta. Molemmissa koneissa on käyttöjärjestelmäksi asennettuna Windows 7 Enterprise edition. Ensimmäinen testikone on Client1, siihen on asennettu kaikki saatavilla olevat Microsoftin päivitykset sekä F-Secure Client Security 9.32.

Toinen työasema on nimeltään Client2. Erona Client1 koneeseen on se, että Client2 tietokoneelle ei ole asennettu Microsoftin päivityksiä eikä ajan tasalla olevaa virusturvaa.

Testauksen aikana molempien koneiden kokoonpanoa tullaan muuttamaan testitapauksen niin vaatiessa.

3.3 Testiverkot

Testiympäristön toimialueena toimii Microsoftin ohjeistuksen mukaisesti corp.contoso.com ja vierailijaverkkona toimii restricted.contoso.com
Testiympäristössä eri toimipisteitä simuloidaan luomalla kaksi eri Active Directory siteä. Ensimmäinen site on pääkonttorin verkko ja toinen site simuloi toisessa paikassa sijaitsevaa konttoria.

3.4 Testitapaukset

Alla on lueteltuna eri testitapauksen jolla teknologian käyttöönottoa lähdetään testaamaan. Testitapausten määrä lisääntyy tarvittaessa, mikäli testauksessa tulee vastaan odottamattomia ongelmia.
Testausympäristön rakentaminen ja testaaminen aloitetaan asentamalla kaksi palvelinkonetta, DC01 sekä DC02. Kun palvelinkoneet on saatu asennettua, roolit konfiguroitua sekä ominaisuudet otettua käyttöön, asennetaan yksi asiakaskone ilman mitään ylimääräistä. Asiakaskoneen nimi on Client01.
Palvelinkoneen system health validatorin säännöstöä lähdetään tiukentamaan asteittain ja jokaiset tiukennuksen jälkeen asiakaskone yritetään saada sisään luotettuun verkkoon.

Testaamisen tarkoituksena on varmistua siitä, että teknologia toimii sekä määrittää haluttu Network Access Protectionin taso silmälläpitäen tietoturvaa, mutta rajoittamatta liikaa käyttäjiä.

3.4.1 Testi 1: Molemmat työasemat pääsevät sisäverkkoon ennen teknologian käyttöönottoa

Liitetään molemmat työasemat toimialueeseen ja testataan että kaikki sisäverkon levyjaot toimivat.

3.4.2 Testi 2: NAP:n käyttöönotto seurantatilassa

Teknologia otetaan käyttöön seurantatilassa, jossa kaikki koneet pääsevät rajoituksettomasti verkkoon, mutta palvelimen lokitiedostoon tulee merkintä koneista jotka eivät täytä pääsyvaatimuksia.
Tässä testivaiheessa ainoana turvallisuusvaatimuksena on se, että Windowsin oma palomuuri on kytketty päälle.
Pääsy testataan molemmilla tietokoneilla, toisessa ei ole palomuuri päällä.

3.4.3 Testi 3: NAP:n muiden vaatimusten käyttöönotto

Network access protectionin hallinnasta otetaan käyttöön Windowsin päivitysten tarkastus sekä F-Secure tarkastus. Tässä testivaiheessa testataan myös F-Securen omaa NAP liitännäistä Windows Serverille. Sen avulla voidaan tarkastella syvemmin tietoturvaohjelmiston määrityksiä.

3.4.4 Testi 4: NAP:n täysimääräinen käyttöönotto

Testiympäristössä siirrytään käyttämään täyttä pakotusta seurantatilan sijaan. Toisessa koneessa on palomuuri päällä, toisessa ei.

3.4.5 Testi 5: Koneen saattaminen turvalliseen tilaan

Testataan että tietokoneen tietoturvatason päivittäminen tarvittavalle tasolle onnistuu vierailijaverkon kautta.

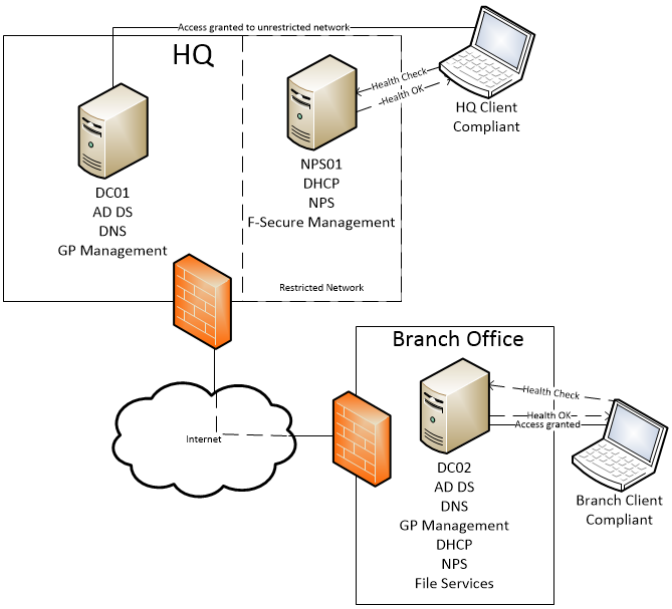
3.5 Suurimmat testiongelmat

Testivaiheen ensimmäinen suurempi ongelma oli System Health Validatorien ja Remediation Servereiden sijoittaminen pääkonttorin ulkopuolella.
Ongelmaksi tässä tapauksessa ilmeni se, että jokaisessa ulkokonttorissa on vain yksi palvelinkone, jossa pyörii kriittisiä palveluita kuten hajautetut levyjaot ja Active Directory Domain Services. Kyseisen palvelinkoneen IP-osoite tulisi lisätä restricted-verkon koneiden reititystauluihin, mikäli sillä pyörisi System Health Validator tai Remediation Server. Tämä muutos sallisi myös rajoitetun verkon koneille täyden pääsyn paikalliselle

palvelimelle, täten tekemällä hyödyttömäksi NAP-teknologian ominaisuuden rajoittaa verkkoon pääsyä.

Ongelma voitaisiin kiertää sillä, että ainut dedikoitu Network Policy Services-palvelun omaava palvelinkone, jossa on System Health Validator ja Remediation server, olisi pääkonttorilla Helsingissä.
Tämä vaihtoehto tosin ei toimisi jos VPN-tunneli ei olisi toimintakunnossa ulkopuolisen konttorin ja pääkonttorin välillä.
Samalla katoiaisivat kaikki yrityksen käytössä olevan hajautetun tiedostojärjestelmän hyödyt.

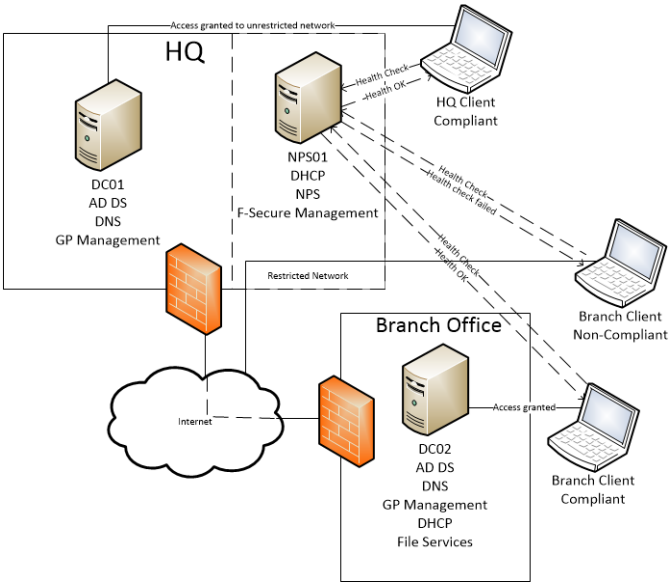
Kuvan 2 tapauksessa sivukonttorin tietokoneet pääsevät aina käsiksi paikalliseen palvelimeen, mutta ne eivät näe verkon muita koneita. Pääkonttorilla pääsy olisi rajoitettu vain yhteen palvelimeen, eli pääkonttorilla verkon suojaus toimisi niin kuin pitääkin.



Kuva 2: Jokaisella konttorilla on oma SHV

Kuvan 3 tapauksessa sivukonttorin koneet suorittavat terveystarkastuksen aina pääkonttorilla sijaitsevalle NPS -palvelimelle. Tässä tapauksessa tietokone, joka ei täytä terveysvaatimuksia, ei pääse käsiksi myöskään sivukonttorin tiedostojakoihin.

Haittapuolena tässä tapauksessa on se, että mikäli yhteys ei toimi pääkonttorin ja sivukonttorin välillä, sivukonttorin tietokoneet joutuvat olemaan rajoitetussa verkossa niin kauan kunnes yhteys konttoreiden välillä toimii taas.



Kuva 3: Pääkonttorilla on keskitetty SHV

Ongelman ratkaisemiseksi selvitetään mahdollisuutta hankkia toinen verkkokortti sivukonttorien palvelimiin, jotta saataisiin hajautettu levyjako toiseen aliverkkoon terveystarkastuksen kanssa.
Vaihtoehtoisesti palvelimelle voisi asentaa yhden vähätehoisen virtuaalikoneen joka toimisi NPS eli terveystarkastuspalvelimena.

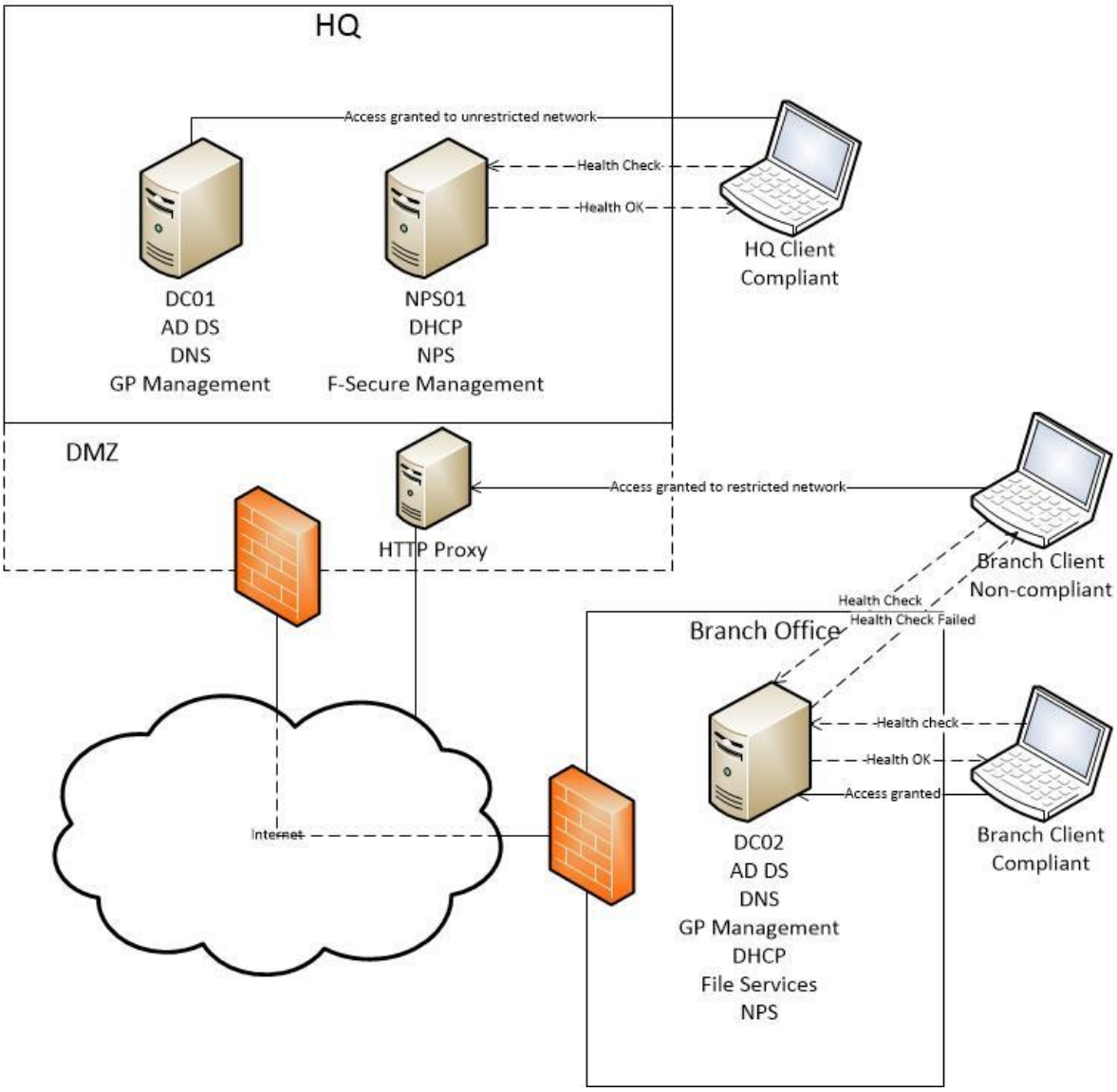
3.6 Testauksen tulokset

Heti testauksen alkumetreillä todettiin, että projekti on paljon haastavampi kuin aluksi luultiin. Eristystä ei pystytty toteuttamaan suunnitellussa laajuudessa DHCP-teknologiaa käyttäen, joten ei-yhteensopivien koneiden eristys jouduttiin toteuttamaan hieman yksinkertaisemmalla, alla kuvatulla tavalla.

Pitkän testausjakson ja Helsingin toimiston käyttöönoton jälkeen päädyttiin ottamaan käyttöön malli, joka mahdollistaa liikenteen internetiin koneille jotka eivät täytä vaatimuksia, mutta estää pääsyn muualle yrityksen verkkoon.
Tämä tapahtuu ohjaamalla http-liikenne välityspalvelimen kautta ulospäin.

NAP:n estämän koneen verkkomaski on tällöin 255.255.255.255, eli kone ei näe verkossa mitään muita koneita kuin ne, mitkä sille on network policy serverin asetuksissa määritelty.
Kyseessä olevan yrityksen tapauksessa nämä palvelimet ovat itse NAPia toteuttava palvelin sekä välityspalvelin.

Asiakaskoneet saavat välityspalvelimen kautta käyttöönsä sähköpostin, internetyhteyden ja pikaviestimet, joita saatetaan tarvita tukipyynnöissä ja muussa kommunikaatiossa. Tämän ratkaisun haittapuoli on se, että kaikkien toimistojen rajoitettujen verkkojen internetliikenne kulkee pääkonttorissa sijaitsevan välityspalvelimen kautta. Malli on havainnoillistettu kuvassa 4.



Kuva 4: Turvattomat koneet ohjataan verkkoon välityspalvelimen kautta

4 Käyttöönotto

Suunnitelmien mukaan Network Access Protection-teknologia otetaan käyttöön hyödyntäen DHCP-pakotustapaa. Tähän toteutustapaan päädyttiin yrityksen maailmanlaajuisen infrastruktuurin monimutkaisuuden takia. DHCP-pakotusta käytettäessä ei tarvitse investoida uuteen infrastruktuuriin tai ottaa NAP-teknologian ulkopuolisia ylimääräisiä palveluita käyttöön palvelimilla. Pakotusstapa on kuitenkin myöhemmin helppo päivittää vahvempaan myöhemmin tarpeen niin vaatiessa tai rinnalle voidaan ottaa käyttöön toinen pakotustapa täydentämään suojausta.

Käyttöönotto vaiheistetaan niin, että aluksi teknologia otetaan käyttöön vain yhdessä toimistossa. Tämä tehdään sen takia, että voidaan löytää ja korjata mahdolliset ongelmatilanteet ennen maailmanlaajuista käyttöönottoa.
Testauksen lopussa tehtiin myös päätös, että kaikki koneet jotka eivät saavuta tarvittavaa tietoturvan tasoa, kierrätetään verkkoon pääkonttorilla Helsingissä sijaitsevan välityspalvelimen kautta. Tällä tavalla tietokone saa internetyhteyden, mutta se ei näe verkon muita koneita, eikä pääse käsiksi sisäverkon muihin resursseihin.

4.1 Valmistelut

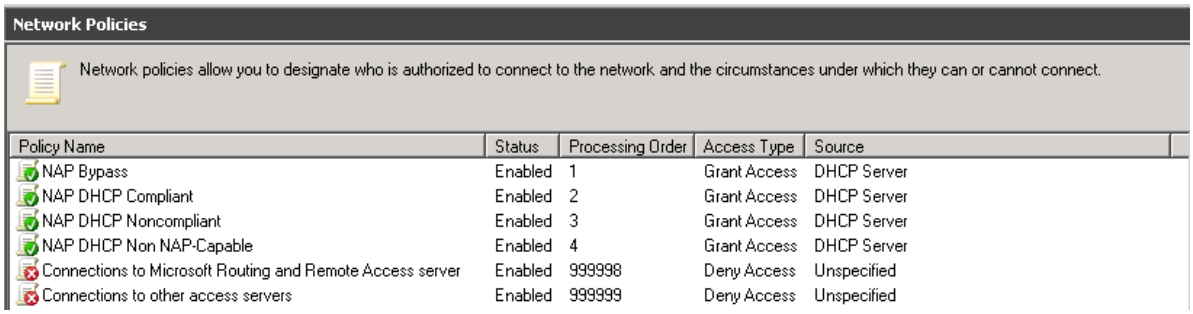
Teknologian käyttöönottoa varten jokaisella Network Access Protectionia toteuttavalla palvelimella tulee ottaa käyttöön seuraavat roolit:

- DHCP
- Network Policy and Access Services

DHCP-palvelu toteuttaa tietokoneiden eristämisen silloin kun Network Policy and Access Services (NPS) sitä vaatii.

DHCP:n asetuksiin lisätään erikseen tiedot eristysverkkoa varten, tarvittavat tiedot ovat oletusreititin, nimipalvelimet ja domainpääte eristetyille koneille. Tilaajayrityksen tapauksessa pääte sai etuliitteet restricted, kuten Microsoftin ohjeistuksissa on suositeltu. DHCP tarjoaa mahdollisuuden luokittaa erilaiset asetukset. Oletusluokka on default class. Nämä edellämainitut asetukset asetettiin käyttämään Default Network Access Protection classia, etteivät ne sekoitu normaaliasetusten kanssa. (Microsoft 2008b, 20.)

Suurin osa kaikesta konfiguraatiotyöstä tapahtuu NPS:n puolella. Nimensä mukaan siellä määritellään verkko- ja pääsypolitiikat.
Ensimmäiseksi määriteltiin verkkopoltitiikat seuraavalla tavalla:



Kuva 5: Verkkopolitiikat

Kuvassa 4 on määriteltyinä kolmen Network Access Protection oletuspolitiikan lisäksi NAP Bypass. Kaikki koneet joka kuuluvat Active Directoryssä NAP Bypass ryhmään, käyttävät tätä politiikkaa. Kyseinen ryhmä ja politiikka luotin siksi, että aika-ajoin on tarvetta päästää sisäverkkoon tietokoneita, jotka eivät yllä tarvittavalle tietoturvan tasolle.
Muut kolme pääsyryhmää tulevat oletuksena NAP:n mukana. Nimiensä mukaan compliant ryhmää käyttävät tietokoneet joilla on tarvittava tietoturvan taso saavutettu. Noncompliant –ryhmään kuuluu taas ne koneet, jotka eivät ole saavuttaneet tarvittavaa tietoturvan tasoa.
Non NAP-Capable ryhmän politiikkaa käyttävät ne tietokoneet ja laiteet, jotka eivät pysty hyödyntämään Network Access Protectionia. Tämänkaltaisia koneita ovat esimerkiksi Windows XP SP2 ja sitä vanhemmat Windows-tietokoneet sekä Linux ja OSX jakelut.

Tämän jälkeen Network Policy Servicesillä määritellään Security Health Validatorien asetukset. Esimerkiksi Windows Security Health Validatorille voidaan määritellä seuraavat ehdot:

- Palomuuri on päällä
- Virustorjunta/haittaohjelmien torjunta on päällä
- Virustorjunta/haittaohjelmien torjunta on ajantasalla
- Windowsin automaattiset päivitykset ovat päällä

- Viimeisimmät päivitykset ovat asennettuna

Järjestelmään saisi asennettua myös muita security health validatoreja esimerkiksi virustorjuntaohjelmiston valmistajalta. Nämä liitännäiset jäävät tämän projektin ulkopuolelle.

Koneet jotka eivät läpäise yllämainittuja vaatimuksia, suljetaan verkkomaskin avulla pois muusta verkosta niin, että ne eivät näe muita verkossa olevia tietokoneita. Tätä varten koneiden reititystauluun pitää esitellä palvelimet, jotka auttavat saavuttamaan tarvittavan suojauksen tilan. Näitä palvelimia kutsutaan nimellä remediation servers. Samaan ryhmään lisättiin myös yrityksen http-proxy palvelin, että rajoitetut koneet pääsevät internetiin.
Remediation servers ryhmään kuuluu kolme palvelinta: http-proxy palvelin, paikallinen dhcp-palvelin ja virustorjuntaohjelmiston hallintapalvelin. Viimeisin sitä varten, että virustorjuntaohjelmisto on myöhemmin helpompi liittää Network Access Protectionin piiriin.

Kesken käyttöönoton huomattiin, että Network Policy and Access Services ei tue minkäänlaista replikointia eri palvelimien välillä eli yllämainitut asetukset pitäisi tehdä joka konttorille erikseen.
Asiaa helpotti kuitenkin se, että asetukset voidaan viedä .xml tiedostoon seuraavalla komennolla:

```
netsh nps export filename=”config.xml” ExportPSK=YES
```

Tämä voidaan puolestaan tuoda uudelle palvelimelle komennolla

```
netsh nps import filename=”config.xml”
```

(Microsoft 2012c.)

4.2 NAP ilman rajoituksia

Ennen varsinaista käyttöönottoa teknologiaa testattiin ottamalla se päälle määrittämättä toimenpiteitä jos turvallisuusvaatimukset eivät täyty. Näin saatiin selville että teknologia itsessään toimii.
Jo tässä vaiheessa työasemien terveydentilaa seurattiin NAPia toteuttavien palvelimien lokitiedostojen kautta.

Seuranta osoittautui kuitenkin hankalaksi siitä syystä, että Microsoftilla ei ollut tarjota ilmaiseksi mitään kunnon työkalua lokien seurantaan.

4.3 Siirtymävaihe

Teknologia otettiin ensiksi käyttöön jokaisella toimistolla niin kutsutussa probation, eli siirtymätilassa. Siirtymätilassa asetetaan takaraja, mihin mennessä koneiden pitää olla NAP-yhteensopivia verkkoon pääsyn turvaamiseksi.
Hyvänä puolena tässä tilassa on se, että DHCP:n hallinnasta ja NPS-palvelimen lokitiedostoista erottaa ongelmalliset koneet helpommin kuin edellisessä vaiheessa ja niiden ongelmat on mahdollista paikantaa ja korjata ennen täyttä käyttöönottoa.

4.4 Täyden suojauksen käyttöönotto

Kun siirtymämoodia hyväksikäyttäen varmistuttiin siitä, että ongelmakoneita ei enää ole yrityksen verkossa, oli aika siirtyä täyteen suojaukseen. Pääkonttorilla Helsingissä tietokoneet olivat parhaassa kunnossa, joten teknologia päätettiin ottaa ensimmäisenä käyttöön siellä.
Tämän jälkeen NAPia käyttämään siirryttiin Amsterdamissa. Essenin toimistolla oli group policyn käyttöönoton kanssa teknisiä ongelmia, joiden selvityksen takia teknologia päätettiin ottaa käyttöön ensin Aasian toimistoilla.

Paikallisen palvelimen vikatilasta johtuen, Toronton konttorin käyttöönotto päätettiin jättää tämän projektin ulkopuolelle.

4.5 Loppupäätelmät

Network Access Protection saatiin otettua käyttöön onnistuneesti yhtä toimipistettä lukuunottamatta kaikissa suunnitelluissa kohteissa. Haasteita aiheutti eniten ensimmäisen vaiheen rajoituksettoman valvonnan tulosten seuraaminen, koska Windows Server 2008 R2 ei erittele lokilla eri tilakoodille ongelmallisia tietokoneita.
Ongelma ratkesi kuitenkin seurantatilan käyttöönoton jälkeen, jolloin turvattomat tietokoneet oli helpompaa tunnistaa palvelimen lokilta.

Täyden suojauksen käyttöönoton jälkeen huomattiin ongelmia siinä, että Windows 7 ei aina ilmaise rajoitetussa verkossa oloa käyttäjälle tarpeeksi selkeästi. Tämä ongelma johti siihen, että loppukäyttäjät eivät aina osanneet hakea apua verkko-ongelmiinsa.
Heti käyttöönoton jälkeen, teknologia mahdollisti ylläpitäjien kannalta paremmat mahdollisuudet verkon pääsyn hallintaan ja seurantaan.

5 Yhteenveto

Opinnäytetyöni tarkoitus oli tutustua Microsoftin Network Access Protection –teknologiaan ja ottaa se käyttöön tilaajayrityksen verkossa. Aloitin opinnäytetyöprojektin etsimällä sopivaa lähdemateriaalia teoriataustaa varten. Teoriataustaa työstäessäni sain myös itse tarvittavan perustiedon projektin toteutusta varten.

Teknologian testausta varten rakensin VMWare Workstation –virtualisointiohjelmistoa hyväksikäyttäen kahden palvelinkoneen ja kahden työaseman virtuaaliympäristön. Tietokoneen tehot meinasivat testausvaiheessa tulla vastaan useaan otteeseen hankaloittaen testaamista. Testauksen aikana myös todettiin, että projekti tulee olemaan haastavampi kuin ennalta oltiin ajateltu. Haasteina olivat erityisesti yrityksen toimistojen erilaiset tietoturvakäytännöt ja uusi, monimutkainen hajautettu tiedostojärjestelmä.

Käyttöönotto päätettiin toteuttaa asteittain aloittaen Helsingissä sijaitsevasta pääkonttorista. Tämä sen takia koska Helsingissä on aina IT-asiantuntija paikalla, jos jokin asia ei toimi käyttöönoton jälkeen.
Käyttöönottoa jatkettiin tämän jälkeen yrityksen Saksan ja Alankomaiden toimistoissa vähäisen aikaeron takia.

Kun tekniikka todettiin toimivaksi kolmessa eri toimipisteessä, Network Access Protection -teknologia päätettiin ottaa käyttöön myös Aasiassa. Ensiksi teknologian sai käyttöön Singaporen ja Hong Kongin toimistot, jonka jälkeen suojaus toteutettiin yrityksen suurimmassa toimistossa Shanghaissa.

Pohjois-Amerikassa teknologiaa ei otettu käyttöön tämän projektin puitteissa johtuen paikallisen palvelimen vikatilasta, joka esti uusien roolien käyttöönoton. Vikatila saadaan korjattua vasta syksyllä uuden palvelimen hankinnan myötä. Tätä varten kuitenkin saadaan helposti tuotua konfiguraatio toisen konttorin palvelinkoneelta.

Käyttöönotto sujui ilman suurempia ongelmia, vaikka aikaa meni suunniteltua enemmän joidenkin toimistojen tietokoneiden ja käyttäjien huonon tietoturvatason vuoksi.

Käyttöönoton jälkeen työstettiin vielä yritykselle kattava dokumentaatio koko järjestelmästä.

Jatkotoimenpiteenä voidaan esimerkiksi nostaa Network Access Protectionin pakotustasoa IEEE802.1X- tai IPSec-tasolle ja ottaa käyttöön kolmansien osapuolten tarjoamia NAP-liitännäisiä. Tämä työ myös antaa hyvän tiivistelmän NAP:n ominaisuuksista sekä tarjoaa mallin siitä, miten teknologia voidaan ottaa käyttöön DHCP-toteutustavalla.

5.1 Tulosten merkittävyys

Projektin tuloksena saatiin toteutettua tilaajayritykselle toimiva verkon suojausjärjestelmä joka hyödyntään Network Access Protection –teknologiaa.
Heti teknologian käyttöönoton jälkeen havaittiin useiden toimistojen sisäverkoissa laitteita, jotka eivät sinne kuulu. Teknologia mahdollistaa automatisoinnin edellisen kaltaisten laitteiden pääsynvalvontaan puuttumalla mahdollisiin tietoturvariskeihin ennaltaehkäisevästi.
Tietoturvan kannalta parannus on merkittävä, koska ennen käyttöönottoa sisäverkkoon kuulumattomat laitteet saatettiin havaita vasta sen jälkeen, kun ne olivat liittyneet verkkoon, jos silloinkaan.
Terveystarkastusten myötä saatiin myös toinen tapa tarkastaa asiakaskoneiden virustorjuntaohjelmiston, palomuurin ja käyttöjärjestelmäpäivitysten tarvittava taso.
Kustannuksien puolesta projekti oli myös edullinen, koska uusia laitehankintoja tai ohjelmistolisenssejä ei tarvittu. Ainoa välillinen kustannus oli projektin työstöön käytetyt työtunnit.

Lähteet

Davies, J. Northrup, T. 2008. Windows Server 2008 Networking and Network Access Protection(NAP). Microsoft Press.

F-Secure. 2012. Microsoft Network Access Protection (NAP) support. Luettavissa: http://www.f-secure.com/en/web/business_global/support/article/kba/15625/k/nap/p/1. Luettu: 11.11.2012

Microsoft Corporation. 2007. Network Access Protection (NAP) Deployment Planning. Luettavissa: http://blogs.technet.com/b/nap/archive/2007/07/28/network-access-protection-deployment-planning.aspx. Luettu: 29.4.2013

Microsoft Corporation. 2008a. Introduction to Network Access Protection. White Paper. Luettavissa: http://technet.microsoft.com/en-US/network/cc984252.aspx. Luettu: 30.10.2012

Microsoft Corporation. 2008b. Step By Step Guide: Demonstrate DHCP NAP Enforcement in a Test Lab. Luettavissa: http://www.microsoft.com/en-us/download/details.aspx?id=2409. Luettu: 9.5.2013

Microsoft Corporation. 2011. Network Access Protection. Luettavissa: http://technet.microsoft.com/en-us/network/bb545879.aspx. Luettu: 28.9.2012.

Microsoft Corporation. 2011. Network Access Protection Security Best Practises. Luettavissa: http://technet.microsoft.com/en-us/library/bb694218.aspx. Luettu: 12.4.2013

Microsoft Corporation. 2012a. Understanding NAP IPsec Enforcement. Luettavissa: http://technet.microsoft.com/en-us/library/cc726008.aspx. Luettu: 29.4.2013

Microsoft Corporation. 2012b. VPN Enforcement Configuration. Luettavissa: http://technet.microsoft.com/en-us/library/dd125382(v=ws.10).aspx. Luettu: 29.4.2013

Microsoft Corporation. 2012c. Export NPS Server Configuration for Import on Another Server. Luettavissa: http://technet.microsoft.com/en-us/library/cc732059%28v=ws.10%29.aspx. Luettu: 27.8.2013

Muttilainen, Lauri. 2009. Network access protection etätyökäytössä. HAAGA-HELIA, opinnäytetyöt.

Northrup, T. Mackin, J. 2008. Configuring Windows Server 2008 Network Infrastructure. Microsoft Press.

Tech Republic. 2007. SolutionBase: Configuring Network Access Protection for Windows Server 2008. Luettavissa: http://www.techrepublic.com/article/solutionbase-configuring-network-access-protection-for-windows-server-2008/178022. Luettu: 28.9.2012

Virkki, P. Somermeri, A. 1997. Projektityö – kehittämisen moottori. Edita Oy.

Vorobieva, Victoria. 2010. Network Access Protection ja sen implementoiminen WPK-verkkoon. Tampereen Ammattikorkeakoulu, opinnäytetyöt.

Liitteet

Liite 1. Testaussuunnitelma

Testausympäristö

Testausympäristöä varten tarvitaan vähintään kaksi Windows Server 2008 R2 palvelinkonetta sekä neljä virtuaalityöasemaa erilaisia testaustapahtumia varten. Työasemia on kaksi kappaletta verkkoa kohden, toinen asemista täyttää vaadittavat ehdot ja toinen ei. Testaustarkoituksessa koneiden kokoonpanoja tullaan muuttamaan mahdollisesti. Testaukseen tarvitaan myös kaksi erillistä verkkoa simuloimaan eri toimistoja.

Palvelimet

Palvelinkäyttöjärjestelmänä toimii Windows Server 2008 R2.
Ensimmäisessä palvelinkoneessa on seuraavat roolit ja ominaisuudet päällä:

- Active Directory Domain Services
- DHCP Server
- DNS Server
- File Services
- Group Policy Management

Toisessa palvelinkoneessa on seuraavat roolit päällä:

- Active Directory Domain Services
- DHCP Server
- DNS Server

Työasemat

Ensimmäinen ja toinen työasema:

- Nimet: W7alpha, W7charlie
- Käyttöjärjestelmä: Windows 7 Enterprise x64
- Päivitykset: Ajan tasalla
- Muut asennetut ohjelmistot:
    - F-Secure Client Security 9.31
    - Microsoft Office Professional Plus 2010

Kolmas ja neljäs työasema:

- Nimi: W7bravo, W7delta
- Käyttöjärjestelmä: Windows 7 Enterprise x64
- Päivitykset: Ei asennettu
- Muut asennetut ohjelmistot:
    - Microsoft Office Professional Plus 2010

Verkot

Testiympäristössä on kaksi eri avaruudessa toimivaa sisäverkkoa, nämä kuvastavat toimistoja, jotka toimivat eri maissa. Molemmilla toimistoilla on myös niin kutsuttu vierailijaverkko, johon koneet, joiden tietoturvataso ei ole kohdillaan ohjataan.

Pääkonttori - sisäverkko

IP-avaruus: 10.200.50.0/24

Palvelin: DC01, jossa pyörii ensimmäiselle palvelinkoneelle määritetyt palvelut

Samassa lokaatiossa toimivat koneet: W7Alpha, W7Bravo

DMZ ”vierailija” –verkko

IP-avaruus: 192.168.100.0/24

Tähän verkkoon ohjataan koneet, jotka eivät läpäise NAP-tarkastusta

Sivukonttori – sisäverkko

IP-avaruus: 10.200.60.0/24

Palvelin: SRV01, jossa pyörii toiselle palvelimelle määritetyt palvelut

Samassa lokaatiossa toimivat koneet: W7Charlie, W7Delta

DMZ ”vierailija” –verkko

IP-avaruus: 192.168.100.0/24

Tähän verkkoon ohjataan koneet, jotka eivät läpäise NAP-tarkastusta

Liite 2. NPSConfig.txt

Connection request policy configuration:

Name = Use Windows authentication for all users
State = Enabled
Processing order = 999999
Policy source = 0

Condition attributes:

Name	Id	Value
Condition0	0x1006	"0 00:00-24:00; 1 00:00-24:00; 2 00:00-24:00; 3 00:00-24:00; 4 00:00-24:00; 5 00:00-24:00; 6 00:00-24:00"

Profile attributes:

Name	Id	Value
Auth-Provider-Type	0x1025	"0x1"

Connection request policy configuration:

Name = NAP DHCP
State = Enabled
Processing order = 1
Policy source = 3

Condition attributes:

Name	Id	Value
Condition0	0x1006	"0 00:00-24:00; 1 00:00-24:00; 2 00:00-24:00; 3 00:00-24:00; 4 00:00-24:00; 5 00:00-24:00; 6 00:00-24:00"

Profile attributes:

Name	Id	Value
Auth-Provider-Type	0x1025	"0x1"
Override-RAP-Auth	0x1fb0	"FALSE"

Event log configuration:

Accepted authentication requests = Enabled
Rejected authentication requests = Enabled

File log configuration:

Accounting = Enabled
Authentication = Enabled
Periodic accounting status = Enabled
Periodic authentication status = Enabled
Directory = C:\Windows\system32\LogFiles
Format = ODBC formatting
Delete old logs = Enabled
Frequency = Monthly logs
Max size = 10 MB

Ports configuration:

Accounting ports = xxxx,zzzz
Authentication ports = xxxx,zzzz

Network policy configuration:

Name = Connections to other access servers
State = Enabled
Processing order = 999999
Policy source = 0

Condition attributes:

Name	Id	Value
Condition0	0x1006	"0 00:00-24:00; 1 00:00-24:00; 2 00:00-24:00; 3 00:00-24:00; 4 00:00-24:00; 5 00:00-24:00; 6 00:00-24:00"

Profile attributes:

Name	Id	Value
NP-Allow-Dial-in	0x100f	"FALSE"
NP-Authentication-Type	0x1009	"0x3" "0x4" "0x9" "0xa"
Quarantine-Update-Non-Compliant	0x1fc8	"TRUE"
Framed-Protocol	0x7	"0x1"
Service-Type	0x6	"0x2"

Network policy configuration:

Name = Connections to Microsoft Routing and Remote Access server
State = Enabled
Processing order = 999998
Policy source = 0

Condition attributes:

```
Name                            Id          Value
----------------------------------------------------
Condition0                       0x1033      "^311$"

Profile attributes:

Name                            Id          Value
----------------------------------------------------
NP-Allow-Dial-in                    0x100f      "FALSE"
NP-Allowed-EAP-Type                 0x100a
"1A000000000000000000000000000000" "0D000000000000000000000000000000"
NP-Authentication-Type              0x1009      "0x5" "0x4" "0xa" "0x3" "0x9"
Quarantine-Update-Non-Compliant         0x1fc8      "TRUE"
Framed-Protocol                     0x7         "0x1"
Service-Type                        0x6         "0x2"
MS-Filter                           0x102f

                ============================================
====================
                IPFILTER_IPV4INFILTER               Action: DENY
                ------------------------------------------------------------
                Address . . . . . : 0.0.0.0
                Mask. . . . . . . : 0.0.0.0
                Protocol. . . . . : 0
                Source Port . . . : 0
                Destination Port. : 0
                ------------------------------------------------------------

MS-MPPE-Encryption-Policy               0xfffffffa7  "0x2"
MS-MPPE-Encryption-Types                0xfffffffa6  "0xe"

Network policy configuration:
----------------------------------------------------
Name            = NAP DHCP Compliant
State           = Enabled
Processing order = 1
Policy source    = 3

Condition attributes:

Name                            Id          Value
----------------------------------------------------
Condition0                       0x1fbd      "NAP DHCP Compliant"

Profile attributes:

Name                            Id          Value
----------------------------------------------------
```

```
Ignore-User-Dialin-Properties           0x1005      "TRUE"
NP-Allow-Dial-in                        0x100f      "TRUE"
NP-Authentication-Type                  0x1009      "0x7"
MS-Quarantine-State                     0x1faf      "0x0"
Quarantine-Update-Non-Compliant         0x1fc8      "TRUE"
Framed-Protocol                         0x7         "0x1"
Service-Type                            0x6         "0x2"
Saved-Machine-HealthCheck-Only          0x1fdc      "0x1"

Network policy configuration:
----------------------------------------------------------
Name            = NAP DHCP Noncompliant
State           = Enabled
Processing order = 2
Policy source    = 3

Condition attributes:

Name                                Id          Value
----------------------------------------------------------
Condition0                          0x1fbd      "NAP DHCP Noncompliant"

Profile attributes:

Name                                Id          Value
----------------------------------------------------------
Ignore-User-Dialin-Properties           0x1005      "TRUE"
NP-Allow-Dial-in                        0x100f      "TRUE"
NP-Authentication-Type                  0x1009      "0x7"
MS-Quarantine-State                     0x1faf      "0x0"
Quarantine-Update-Non-Compliant         0x1fc8      "TRUE"
Framed-Protocol                         0x7         "0x1"
Service-Type                            0x6         "0x2"
Saved-Machine-HealthCheck-Only          0x1fdc      "0x1"

Network policy configuration:
----------------------------------------------------------
Name            = NAP DHCP Non NAP-Capable
State           = Enabled
Processing order = 3
Policy source    = 3

Condition attributes:

Name                                Id          Value
----------------------------------------------------------
Condition0                          0x1fbb      "^1$"

Profile attributes:
```

```
Name                                Id          Value
-------------------------------------------------------
MS-Extended-Quarantine-State        0x1fd9      "0x0"
Ignore-User-Dialin-Properties       0x1005      "TRUE"
NP-Allow-Dial-in                    0x100f      "TRUE"
NP-Authentication-Type              0x1009      "0x7"
MS-Quarantine-State                 0x1faf      "0x0"
Quarantine-Update-Non-Compliant     0x1fc8      "TRUE"
Framed-Protocol                     0x7         "0x1"
Service-Type                        0x6         "0x2"
Saved-Machine-HealthCheck-Only      0x1fdc      "0x1"

Server registration:
-------------------------------------------------------
Status = Un-registered

Remediation server configuration:
-------------------------------------------------------
Group   = Group Name
Address = xxxxx
Name    = xxxxx

Remediation server configuration:
-------------------------------------------------------
Group   = Group Name
Address = yyyyy
Name    = yyyyy

Remediation server configuration:
-------------------------------------------------------
Group   = Group Name
Address = zzzzz
Name    = zzzzz

SHV configuration:
-------------------------------------------------------
Id                  = 79744
Name                = Windows Security Health Validator
Vendor              = Microsoft Corporation

Description         = The Windows Security Health Validator defines the policy
that client computers must be compliant with.

Version             = 1.0


Policy server unreachable      = Noncompliant
Remediation server unreachable = Noncompliant
```

System Health Agent failure = Noncompliant
NAP server failure = Noncompliant
Other errors = Noncompliant

Health policy configuration:

Name = NAP DHCP Compliant
Configuration = All must pass
Id = 79744 subid = 0

Health policy configuration:

Name = NAP DHCP Noncompliant
Configuration = One or more must fail
Id = 79744 subid = 0

SQL log configuration:

Connection =
Description =
Accounting = Enabled
Authentication = Enabled
Periodic accounting status = Enabled
Periodic authentication status = Enabled
Max sessions = 20

Ok.

Liite 3. Yritykselle laadittu kuvaus järjestelmästä. Osa tiedoista poistettu bisneskriittisyyden vuoksi

Contents

Network Access Protection Overview

Network Access Protection (NAP) is a network security technology introduced by Microsoft along with Windows Server 2008. It is used to verify the health of networked computers before letting them into the company network. If the health conditions are not met, the computer will be directed to restricted network and denied access to company resources.

To function the servers running NAP has to run Windows Server 2008 or later and the client trying to access needs to run Windows Vista or later.

Servers and Services needed for NAP deployment

Network Access Protection technology needs the following services, servers, roles and features to function:

Headquarters Server

- Active Directory Domain Services
- DHCP Server
- DNS Server
- File Services
- Group Policy Management
- Network Policy and Access Services
    - Network Access Protection
        - Windows Security Health Validator
        - F-Secure Health Validator
- Active Directory Certificate Services
- HTTP Proxy Service

Branch Office Servers

- Active Directory Domain Services
- DHCP Server
- DNS Server
- Network Policy and Access Services
    - Network Access Protection
        - Windows Security Health Validator

NAP Client Computer Description

GIA Group computer are mainly Lenovo T4XXs series laptops with Windows 8 or Windows 7 installed so every regular computer should have built-in NAP agent with the operating system.

Standard Laptop Installation

Operating System	Windows 7 Enterprise 64-bit or Windows 8 Pro 64-bit edition
Office Suite	Microsoft Office 2010 Professional Plus or Office 2013
Anti-Virus/Firewall	Up to date client security solution

NAP Policy Overview

The following policies are set with Network Access Protection

Policy Name	Status	Processing Order	Access Type	Source
NAP DHCP Compliant	Enabled	3	Grant Access	DHCP Server
NAP DHCP Noncompliant	Enabled	4	Grant Access	DHCP Server
NAP DHCP Non NAP-Capable	Enabled	5	Grant Access	DHCP Server
NAP DHCP Other Devices	Enabled	6	Grant Access	DHCP Server
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

Below are the descriptions of each policy

NAP DHCP Compliant

Device using this policy has passed all the health checks and has full unrestricted access to the company network.

NAP DHCP Noncompliant

Device using this policy has failed one or more NAP health checks and is using restricted network. The computer may apply for unrestricted access again after it is compliant with the access policy.

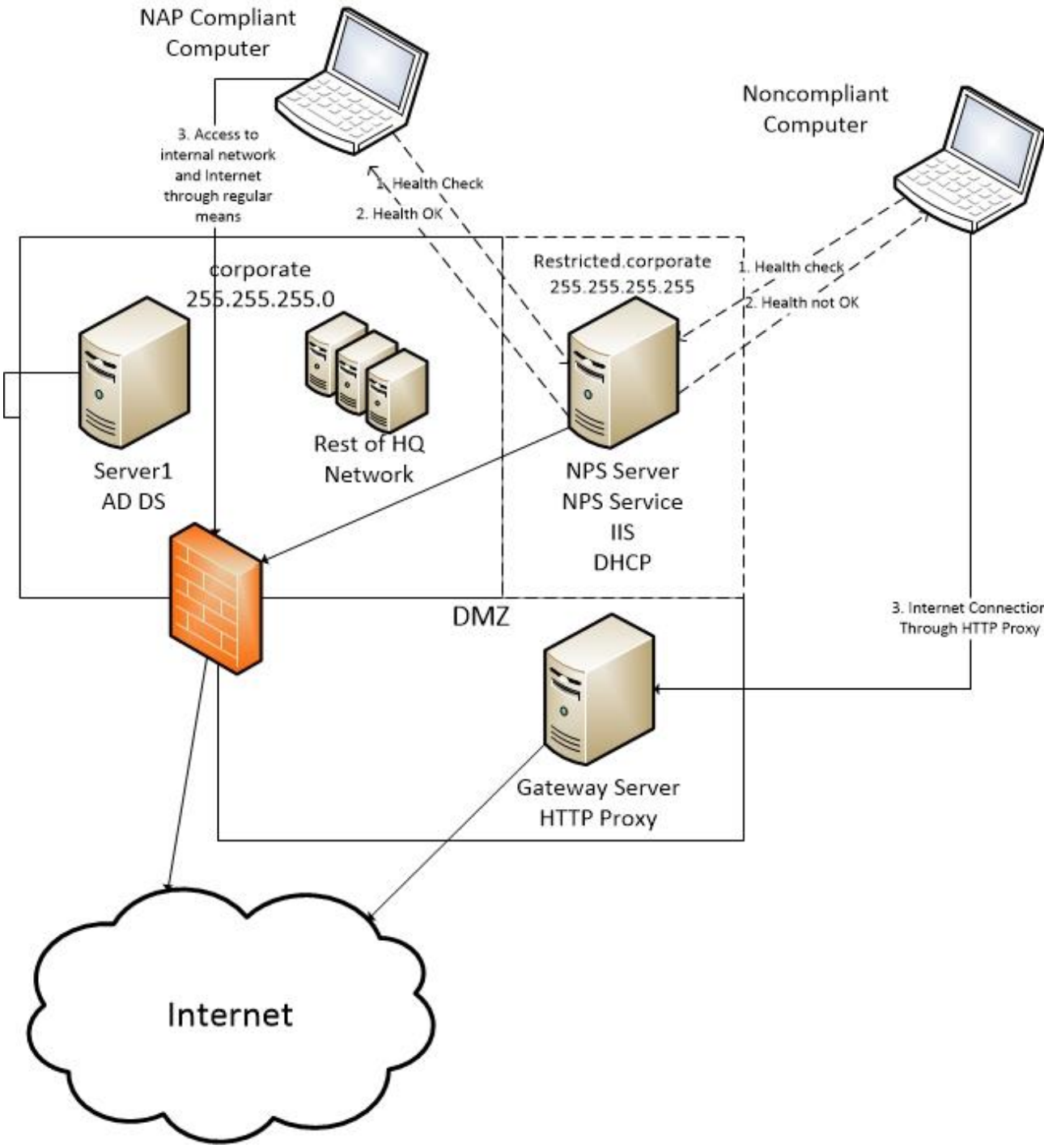
NAP DHCP Non NAP-Capable

Device using this policy is not capable of using network access protection agent but is a member of domain computers group. This group is enabled to provide connectivity for problematic computers.

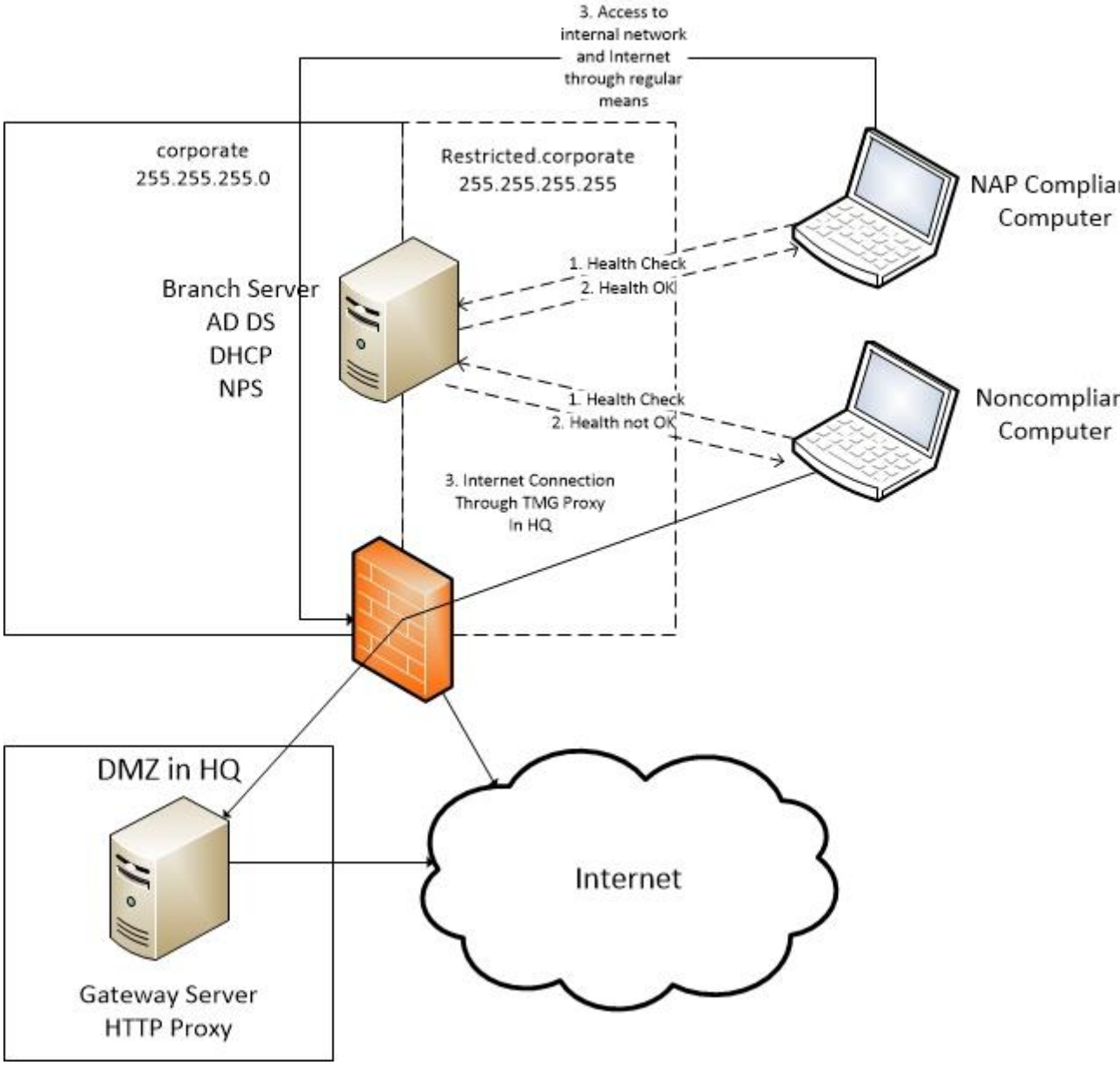
NAP DHCP Other Devices

This group contains all the other Non-NAP-Capable devices which are not members of the domain computers group. It might contain devices like mobile phones or non-company computers.

HQ Nap Visualization



Branch Office Nap Visualization



Satellite office NAP Visualization

The computers in satellite office are not subject to NAP health checks at the moment.

VPN access with NAP

Computers can access internal company resources from outside by logging into a VPN portal.

The portal uses two-way authentication with domain password and One-Time Password which is sent to user's mobile phone.

Computers using VPN are not subject to NAP health checks at the moment. Later on it is possible to implement NAP to VPN connections also.

Troubleshooting restricted computers

Computers applying for full network access needs to meet the following requirements:

1. The computer needs to have NAP client turned on
2. The computer needs to have Anti-Virus up to date and firewall turned on
3. The computer needs to be part of Domain Computers group in Active Directory
4. The computer needs to be connected to the wired office network

NAP Client is not on

The most probable cause to this is that computer isn't member of the NAP Client Computer group in Active Directory.

To fix this problem, add the computer the the abovementioned group, run gpupdate /force on the local computer and restart the machine.

If the computer is running Windows XP SP2 or earlier or Linux, it needs to be added to NAP Client Bypass –group.

The computer's Anti-Virus is not up to date or Firewall is not turned on

The Anti-Virus software might have too old virus definitions (14 days). Or it might not have F-Secure Client Security installed at all.

To fix this problem, update the virus definitions in the restricted network or install/reinstall F-Secure.

If the computer is running Linux, it needs to be added to NAP Client Bypass -group.

The computer is not part of Domain Computers group

All computers join the Domain Computer group in Active Directory when they are joined to the domain. The most likely case when this has not happened is that the computer is not installed correctly or the domain join is not complete.

To fix this problem, check that the computer is installed according to company standards.

The computer is not connected to wired office network

To access internal company resources, the computers need to be connected to the wired office network.

To fix this problem, check the network cabling and network adapter drivers on the client computer.

Liite 4. Turva-asetusten mukainen statement of health

Client state:

Name = Network Access Protection Client
Description = Microsoft Network Access Protection Client
Protocol version = 1.0
Status = Enabled
Restriction state = Not restricted
Troubleshooting URL =
Restriction start time =
Extended state =
GroupPolicy = Configured

Enforcement client state:

Id = 79617
Name = DHCP Quarantine Enforcement Client
Description = Provides DHCP based enforcement for NAP
Version = 1.0
Vendor name = Microsoft Corporation
Registration date =
Initialized = Yes

Id = 79619
Name = IPsec Relying Party
Description = Provides IPsec based enforcement for Network Access Protection
Version = 1.0
Vendor name = Microsoft Corporation
Registration date =
Initialized = No

Id = 79621
Name = RD Gateway Quarantine Enforcement Client
Description = Provides RD Gateway enforcement for NAP
Version = 1.0
Vendor name = Microsoft Corporation
Registration date =
Initialized = No

Id = 79623
Name = EAP Quarantine Enforcement Client
Description = Provides Network Access Protection enforcement for EAP authenticated network connections, such as those used with 802.1X and VPN technologies.
Version = 1.0

Vendor name = Microsoft Corporation
Registration date =
Initialized = No

System health agent (SHA) state:

Id = 79744
Name = Windows Security Health Agent

Description = The Windows Security Health Agent monitors security settings on your computer.

Version = 1.0

Vendor name = Microsoft Corporation

Registration date =
Initialized = Yes
Failure category = None
Remediation state = Success
Remediation percentage = 0
Fixup Message = (3237937214) - The Windows Security Health Agent has finished updating the security state of this computer.

Compliance results =
Remediation results =

Id = 79922
Name = F-Secure System Health Agent
Description = The F-Secure System Health Agent monitors the protection status of F-Secure products on your computer.
Version = 1.00
Vendor name = F-Secure Corporation
Registration date = 12/03/2013 11:47:45
Initialized = Yes
Failure category = None
Remediation state = Success
Remediation percentage = 100
Fixup Message = (9) - Client is compliant
Compliance results =
Remediation results = (0x00000000) - Client is compliant

Id = 88048
Name = Intel(R) AMT SHA
Description = Intel(R) AMT SHA Application
Version = VER_PRODUCTVERSION_STR
Vendor name = Intel(R)
Registration date = 16/07/2013 10:24:03

```
Initialized            = No
Failure category       = None
Remediation state      = Success
Remediation percentage = 0
Fixup Message          = (0) -

Ok.
```