KARELIA-AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

Aki Tanskanen

# Microsoft Forefront UAG -PORTAALIPALVELIMEN VAIHTO

Opinnäytetyö
Marraskuu 2014

Karelia AMMATTIKORKEAKOULU

**OPINNÄYTETYÖ**
**Marraskuu 2014**
**Tietotekniikan koulutusohjelma**

Karjalankatu 3
80200 JOENSUU
+358 50 260 6800

Tekijä
Aki Tanskanen

Nimeke
Microsoft Forefront UAG -portaalipalvelimen vaihto

Toimeksiantaja
Abloy Oy Joensuu

Tiivistelmä

Tässä opinnäytetyössä käsitellään Microsoft Forefront Unified Access Gateway-portaalipalvelimen vaihtoa yrityksessä. Se esittelee asennuksen ja keinot palvelimen käyttöönottoon ja käy läpi, millaiselle palvelimelle UAG asennettiin.

Opinnäytetyö toteutettiin Abloy Oy:n Network Solutions -yksikön ohjelmistokehitysosastolle. Ohjelmistokehitysosasto ylläpitää Abloy Oy:n palvelimien ohjelmistoja. Osasto sai tehtäväkseen vaihtaa fyysisen UAG-portaalipalvelimen uuteen virtuaaliseen palvelimeen, mikä siirtyi osittain opinnäytetyön tekijän tehtäväksi. Palvelin täytyi vaihtaa suorituskykyisemmäksi ja ohjelmisto päivittää uudempaan.

Opinnäytetyö oli toimintapainotteinen, eikä tutkimustyötä juurikaan tehty. Alkuperäisen aikataulun mukaan projektin oli tarkoitus valmistua maaliskuun 2014 loppuun mennessä, mutta aikataulu venyi kiireisen työtilanteen vuoksi. Itse palvelin tilattiin maaliskuun alussa, mutta asennukset päästiin aloittamaan vasta loppukeväästä. Asennusprojektissa ilmeni paljon ongelmia, jotka saatiin lopulta ratkaistua. Projekti oli täysin valmis vasta loppukesästä.

Kieli
suomi

Sivuja 24

Asiasanat
Forefront Unified Access Gateway 2010, ylläpito, palvelin

Karelia
UNIVERSITY OF APPLIED SCIENCES

**THESIS**
**November 2014**
**Degree Programme in**
**Information Technology**
Karjalankatu 3
FI 80200 JOENSUU
FINLAND
+358 50 260 6800

Author

Aki Tanskanen

Title
Microsoft Forefront UAG Portal Server exchange

Commissioned by
Abloy Oy

Abstract

This thesis deals with the basic initialization of Forefront Unified Access Gateway in a company. It presents the installation and deployment of a server and goes through what kind of a server UAG was installed to.

The thesis was carried out for the software development department of Abloy Oy Network Solutions business unit. The software development department maintains the server software of Abloy Oy. The department was given the task to change the physical UAG portal server to a new virtual server, which became partially a task for the author of the thesis. The server had to be changed to a more efficient one and the software needed to be upgraded.

The study was action-oriented, and very little research needed to be done. The project should have been ready by the end of March 2014, but the schedule was delayed because of the hectic work situation. The server itself was ordered in early March, but the installation began in the late spring. The installation was problematic, but all the issues were eventually resolved. The project was fully completed by the end of the summer.

Language
Finnish

Pages 24

Keywords

Forefront Unified Access Gateway 2010 , hosting, server

**Sisältö**

# 1 Johdanto

Forefront Unified Access Gateway on Microsoftin vuonna 2009 julkaisema, organisaatioiden käyttöön suunnattu ohjelmistoratkaisu, joka tarjoaa turvallisen etäyhteyden yrityksien verkkoihin etätyöntekijöille ja liikekumppaneille [2].

UAG-portaalipalvelin on palvelin, joka sijaitsee sisäverkon DMZ alueella, eli käytännössä se on ovi internetistä yrityksen sisäverkkoon. Abloy Oy:n portaali mahdollistaa suojatun etäyhteyden jälleenmyyjille Abloy Oy:n tuotteiden tilausohjelmiin internetin välityksellä. Portaalisivustoa käytetään Microsoftin Internet Explorer -selaimella ja ensimmäisellä käyttökerralla sivusto asentaa selaimeen UAG-lisäosakomponentin. Jokaiselle jälleenmyyjälle on luotu oma portaalitili, jossa on määritelty, mitä sovelluksia kyseinen jälleenmyyjä voi käyttää. Tiliin kirjaudutaan Ableyn portaalin nettisivulta käyttäjätunnuksella ja salasanalla. Kirjautumiseen on saatu lisäturvallisuutta Entrust-palveluntarjoajan tarjoamilla vaihtuvilla tunnusluvuilla. Abloy Oy on ottanut UAG-ohjelmiston käyttöön noin neljä vuotta sitten. Syynä tämän ohjelmiston valintaan on ollut se, että UAG on ainoana ohjelmistona mahdollistanut jälleenmyyjille paikallisesti asennetun Abloy- tuotteiden tilausohjelman VPN-yhteyden Abloy Oy:n sovelluspalvelimelle.

Opinnäytetyön tarkoituksena oli vaihtaa toimeksiantajalle UAG-portaalipalvelimet, koska nykyiset olivat vanhentumassa. Aikaisemmat käytössä olleet UAG-palvelimet olivat fyysisiä palvelimia, jotka oli tarkoitus vaihtaa virtuaalisiksi palvelimiksi ja asentaa UAG uudelleen.

Opinnäytetyön toimeksiannon sain Abloy Network Solutions -osastolta. Koulun sähköpostiini oli tullut viesti, että Abloy hakee työharjoittelijaa ANS-osastolleen. Päätin hakea paikkaa, vaikka työharjoitteluopintopisteet oli suoritettu, mutta ehtona oli, että Ableyltä löytyisi minulle opinnäytetyön aihe. Kävin työhaastattelussa ja siellä kävi ilmi, että minulle löytyisi opinnäytetyön aihe, eli UAG-palvelimien vaihto. Sain harjoittelupaikan Abloy Oy:lta ja ohjelmistotuen kokopäivätyön ohella tein opinnäytetyötä ohjelmistokehitysosaston valvovien silmien alla aina kun aikaa siihen oli.

# 2 Toimeksiantaja

Abloy Oy on ASSA ABLOY-konserniin kuuluva yhtiö, joka toimittaa lukitusratkaisuja maailmanlaajuisesti. Abloy Oy:n myyntituotteina ovat rakennus- ja laitelukot, mekaaniset ja sähkömekaaniset lukkorungot, ovensulkimet sekä rakennushelat. Abloyn tunnetuin tuote on levyhaittasylinteriin perustuva lukko, jonka Emil Henriksson keksi vuonna 1907.

ASSA ABLOY -konsernin liikevaihto oli vuonna 2013 5,6 miljardia euroa ja konsernissa on noin 43 000 työntekijää sekä se on listattu Tukholman pörssiin. ASSA ABLOY -konserniin Suomessa kuuluvat Abloy Oy:n Joensuun ja Björkbodan tehtaat. Abloy Oy:n henkilöstöä on 800 Suomessa ja 100 myyntiyksiköissä ulkomailla [1].

Abloy Oy Joensuun tehtaan tuotantotoiminta on jaettu liiketoimintayksiköihin. Nämä ovat lukot, sähkömekaaniset lukkorungot, Door Control, rakennushelat sekä Abloy Network Solutions.

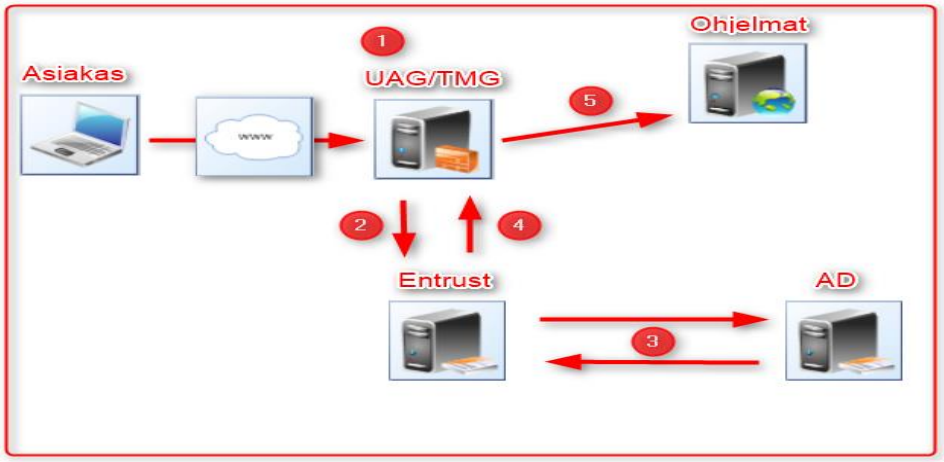
# 3 Opinnäytetyön lähtökohdat

Opinnäytetyö tehtiin toimintapohjaisesti ja tutkimustyötä ei juurikaan tehty. Projekti toteutettiin toimeksiantajan työympäristössä ja Abloyn ohjelmistokehitysosaston asiantuntijoiden valvonnassa.

Abloy Oy:n palvelimien palveluntarjoaja halusi, että nykyiset fyysiset palvelimet vaihdettaisiin uusiin, koska palvelimien käyttöikä oli loppumassa. Aikaisempia palvelimia oli kaksi, UAG-tuotantopalvelin ja UAG-testipalvelin. Vanhat palvelimet eivät olleet identtiset rautatasolla ja jo tästäkin syystä palvelimien uusiminen oli tärkeää. Nämä fyysiset palvelimet päätettiin korvata virtuaalisilla Windows 2008 R2-servereillä. Windows 2008 R2 palvelimet oli palveluntarjoajan

käyttösuositus. Vanha UAG-tuotantopalvelin oli tarkoitus korvata kahdella virtuaalisella palvelimella, koska se mahdollistaa kuormantasauksen käyttöönoton.

UAG-palvelin on sijoitettu verkon reunalle, jota kutsutaan DMZ-alueeksi. Seuraavassa verkon kuvassa on havainnollistettu, minne UAG-palvelin sijoittuu ja kuinka se toimii toimeksiantajan käyttötarkoituksessa (kuva 1).




Kuva 1. Verkon kuvaus.

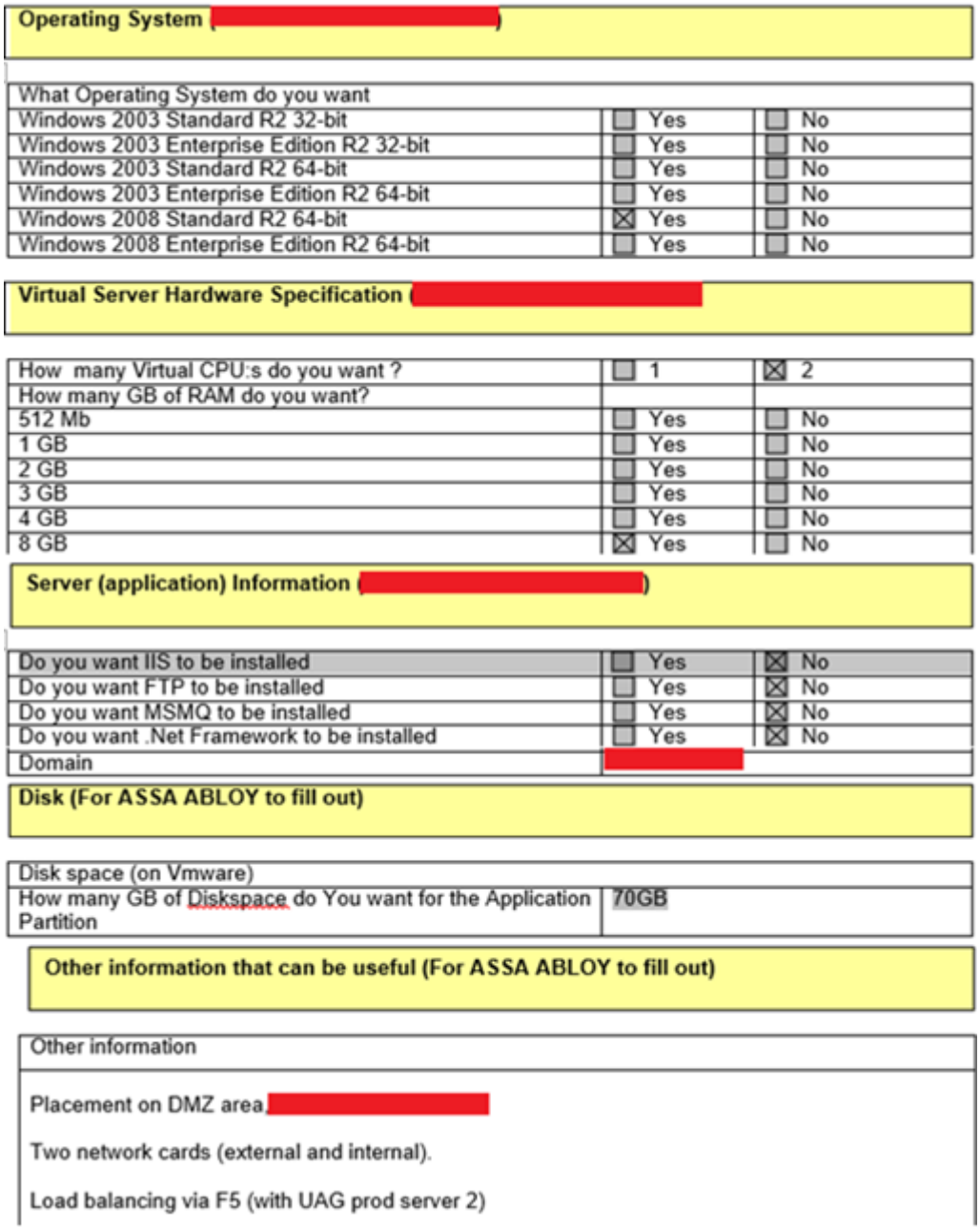
UAG:n toiminta kirjautumisen yhteydessä:

1. Käyttäjä kirjautuu UAG-portaalisivustoon käyttäjätunnuksella ja salasanalla.
2. UAG välittää Entrust-palvelimelle käyttäjän syöttämän käyttäjätunnuksen ja salasanan.
3. Entrust tarkastaa Active Directory -palvelimelta, löytyykö kyseiselle kirjautujalle käyttäjätiliä. Tilin löytyessä AD välittää tiedon takaisin Entrust-palvelimelle.
4. Enrtust-palvelin kysyy kirjautujalta haasteen, eli vaihtuvan tunnusluvun.
5. Jos käyttäjän antama Entrust-tunnusluku on oikein, niin salattu yhteys on avattu käyttäjälle UAG-palvelimen kautta palvelimelle, jossa käytettävät ohjelmat sijaitsevat.

Active Directory -palvelimella toimeksiantaja ylläpitää jälleenmyyjien käyttäjätunnuksia ja salasanoja. Entrust-palvelin on kolmannen osapuolen ylläpitämä tietoturvapalvelu, joka tarjoaa kaksivaiheisen kirjautumisen UAG-portaalin ja Active Direcoryn kautta Abloy Oy:n tuotteiden tilausohjelmiin.

# 4 Virtuaalipalvelimien tilaus

Uudet palvelimet tilattiin toimeksiantajan palvelimien palveluntarjoajalta. Uusia palvelimia tilattiin kolme, eli kaksi tuotantopalvelinta ja yksi testipalvelin. Abloy ylläpitää itse UAG-palvelimien ohjelmistoa, mutta palvelimia ylläpitää niiden palveluntarjoaja. Uudet palvelimet tilattiin tilauslomakkeella palveluntarjoajalta. Lomakkeella määriteltiin haluttujen palvelimien ominaisuudet (kuva 2).



**Operating System** [redacted]

| What Operating System do you want | | |
|---|---|---|
| Windows 2003 Standard R2 32-bit | ☐ Yes | ☐ No |
| Windows 2003 Enterprise Edition R2 32-bit | ☐ Yes | ☐ No |
| Windows 2003 Standard R2 64-bit | ☐ Yes | ☐ No |
| Windows 2003 Enterprise Edition R2 64-bit | ☐ Yes | ☐ No |
| Windows 2008 Standard R2 64-bit | ☒ Yes | ☐ No |
| Windows 2008 Enterprise Edition R2 64-bit | ☐ Yes | ☐ No |

**Virtual Server Hardware Specification** [redacted]

| How many Virtual CPU:s do you want ? | ☐ 1 | ☒ 2 |
|---|---|---|
| How many GB of RAM do you want? | | |
| 512 Mb | ☐ Yes | ☐ No |
| 1 GB | ☐ Yes | ☐ No |
| 2 GB | ☐ Yes | ☐ No |
| 3 GB | ☐ Yes | ☐ No |
| 4 GB | ☐ Yes | ☐ No |
| 8 GB | ☒ Yes | ☐ No |

**Server (application) Information** [redacted]

| Do you want IIS to be installed | ☐ Yes | ☒ No |
|---|---|---|
| Do you want FTP to be installed | ☐ Yes | ☒ No |
| Do you want MSMQ to be installed | ☐ Yes | ☒ No |
| Do you want .Net Framework to be installed | ☐ Yes | ☒ No |
| Domain | [redacted] | |

**Disk (For ASSA ABLOY to fill out)**

| Disk space (on Vmware) | |
|---|---|
| How many GB of Diskspace do You want for the Application Partition | 70GB |

**Other information that can be useful (For ASSA ABLOY to fill out)**

| Other information |
|---|
| Placement on DMZ area [redacted]<br>Two network cards (external and internal).<br>Load balancing via F5 (with UAG prod server 2) |

Kuva 2. Palvelimien ominaisuudet.

# 5 Forefront Unified Access Gateway

Forefront-perheen Unified Access Gateway tarjoaa kattavan ja turvallisen yhteyden etäkäyttäjälle yritysten tietoverkkoihin, järjestelmiin ja sovelluksiin. Se sisältää useita etäkäyttöteknologioita, kuten käänteisen välityspalvelimen, Virtual Private Network:n (VPN) sekä Microsoftin kehittelemät Direct Access ja Remote Desktop -palvelut. DirectAccessin sisällyttämisellä UAG-ohjelmistoon on ollut suuri merkitys UAG:n menestymisessä, koska DirectAccess mahdollistaa monien yritysten arvostaman saumattoman VPN-integraation. Etäkäyttäjät voivat ottaa yhteyden yrityksen sisäverkkoon useilla eri päätelaitteilla portaalisivuston kautta, jota isännöi IIS-palvelu, joka on sidottu UAG-ohjelmistoon [2].

Ohjelmistossa on sisäänrakennettu tuki Microsoftin Exchange Serverille (2003, 2007 ja 2010), SharePoint Portal -serverille(2003, 2007 ja 2010) ja Citrix Presentation -serverille. Se sisältää myös SSL-VPN-teknologian, joka mahdollistaa ulkopuolisten sovellusten sisällönvalvonnan. UAG on hyvin muokattavissa, ja sen kautta voidaan käyttää lähes mitä tahansa ohjelmistoja [2].

UAG toimii useiden eri todentamisjärjestelmien kanssa. Näihin kuuluvat muun muassa Active Directory, RADIUS, LDAP, NTLM, Lotus Domino, PKI ja TACACS+. Ohjelmistossa on käyttötuki myös Linuxille, Macintoshille ja iPhonelle [2].

Laitevaatimukset yksittäiselle palvelimelle on 4 GB keskusmuistia, 2.5 GB kiintolevytilaa, 32- tai 64-bittinen 2.66 GHz tuplaytiminen prosessori ja Windows Server 2008 R2 -käyttöjärjestelmä [2].

Unified Access Gateway ohjelmiston loi alun perin israelilainen yritys Whale Communications 1990-luvulla. Sen tarkoituksena oli kehittää VPN-mekanismiin perustuva etäkäyttöratkaisu ilman suoraa verkkoyhteyttä etäkäyttäjän ja yrityksen verkon välillä. Se kehiteltiin Israelin armeijan ja hallinnon tarpeisiin. Kehitettyä teknologiaa kutsuttiin nimellä ”Air Gap”. Ulkoisen ja sisäisen verkon kom-

munikaation mahdollisti kaksi erillistä 1U rack -mount -serveriä, jotka yhdistettiin toisiinsa SCSI-käyttöliittymällä varustetun muistipankin kautta [2].

Vuonna 2006 Microsoft osti Whale Communication -yrityksen. Kaupan jälkeen ”Air Gap” nimettiin Intelligent Application Gateway -serveriksi (IAG). Microsoft tarjosi tuotetta sekä esiasennettuna sovelluksena että virtuaalisovelluksena [2].

Vuonna 2008 Microsoft ilmoitti muuttavansa IAG:n nimen Forefront Unified Access Gatewayksi. Tuote julkaistiin 24. joulukuuta 2009 [2].

### 5.1 Asennus palvelimelle

Ennen asennusta tuli huomioida muutamia seikkoja järjestelmävaatimuksien lisäksi:

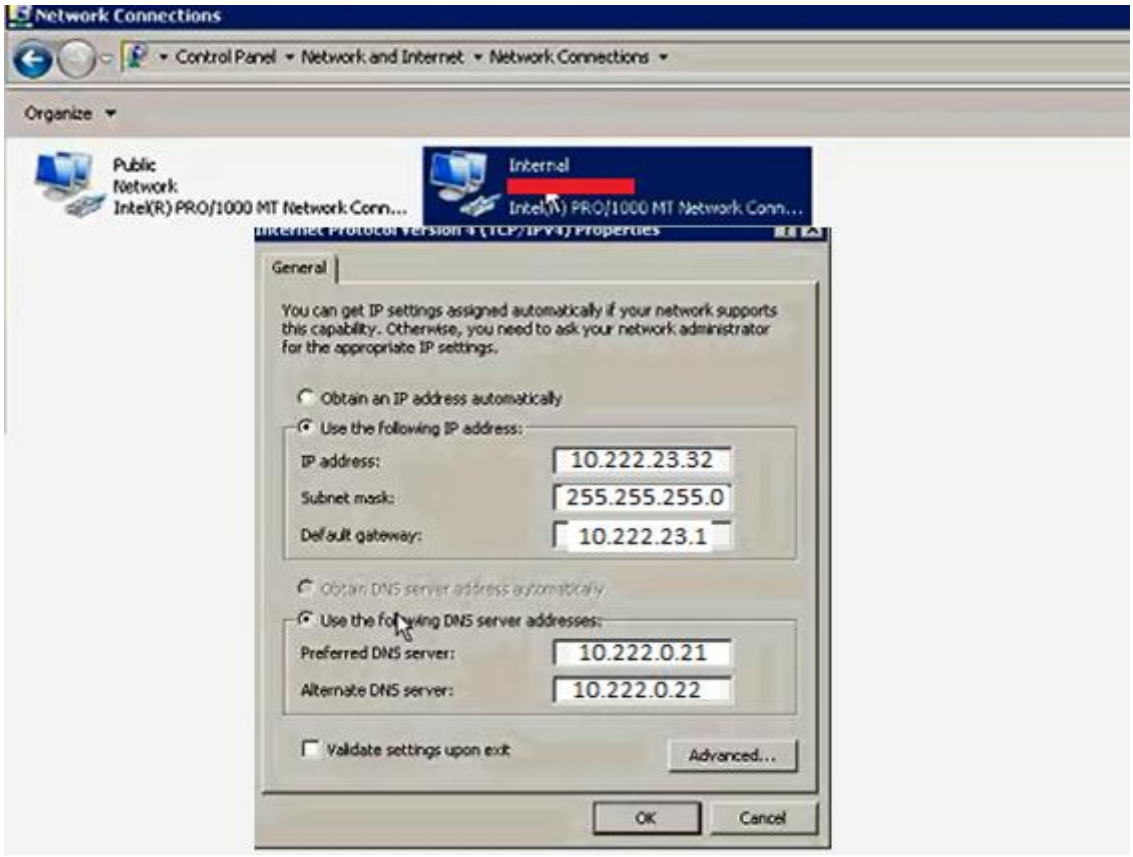
- Palvelin on oikeassa toimialueessa.
- Windows-päivitykset ovat ajan tasalla.
- Palvelimella ei ole aikaisemmin asennettua UAG:tä.
- Palvelimen käyttäjä on järjestelmänvalvoja.
- Internetyhteys on aktiivinen.
- Windowsin palomuuri on päällä.
- Palvelimen käyttäjän automaattinen uloskirjaus on pois päältä etätyöpöytäyhteyden aikana.

Forefront Unified Access Gateway 2010 SP1-asennuspaketti asentaa palvelimelle SQL Server 2008 tietokantaohjelmiston ja IIS-web-palvelun, joka mahdollistaa portaalinettisivun toimivuuden. Asennus sisältää myös Forefront Threat Management Gateway -ohjelmiston, joka toimii UAG:n palomuurina.

### 5.1.1 Asennuksen esivalmistelut

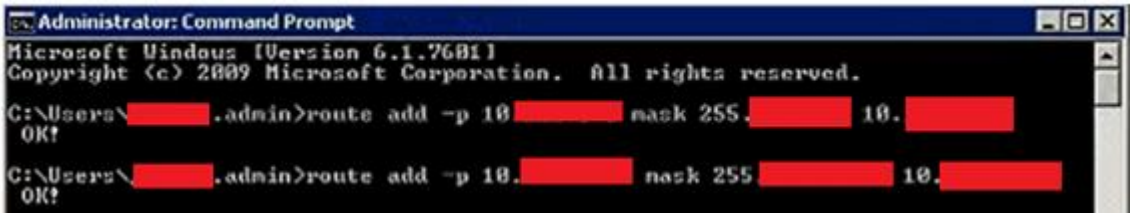
Asennusprosessi aloitettiin ottamalla etätyöpöytäyhteys tilattuun virtuaalipalvelimeen. Tärkeää oli huomioida, että etätyöpöytäyhteys oli ainut yhteys palvelimeen, koska palvelimien virtual manageriin, joka on virtuaalipalvelimien hallintatyökalu, ei ollut oikeutta. Käytännössä tämä tarkoitti sitä, että jos palvelin menisi sekaisin UAG:n asennuksessa eikä palvelimeen saataisi enää yhteyttä, palvelimien ylläpitäjälle täytyisi tehdä tukipyyntö.

Palvelimelle kirjautumisen jälkeen ladattiin Forefront Unified Access Gateway SP1 Microsoftin sivustolta. Palvelin tarkastettiin, jotta se olisi mahdollisimman puhtaassa tilassa. Ennen asennusta palvelin liitettiin Abloyn toimialueeseen, verkkokortit nimettiin sisäiseksi ja julkiseksi verkoksi. Public-verkko johti internettiin ja internal luonnollisesti sisäverkkoon (kuva 3).



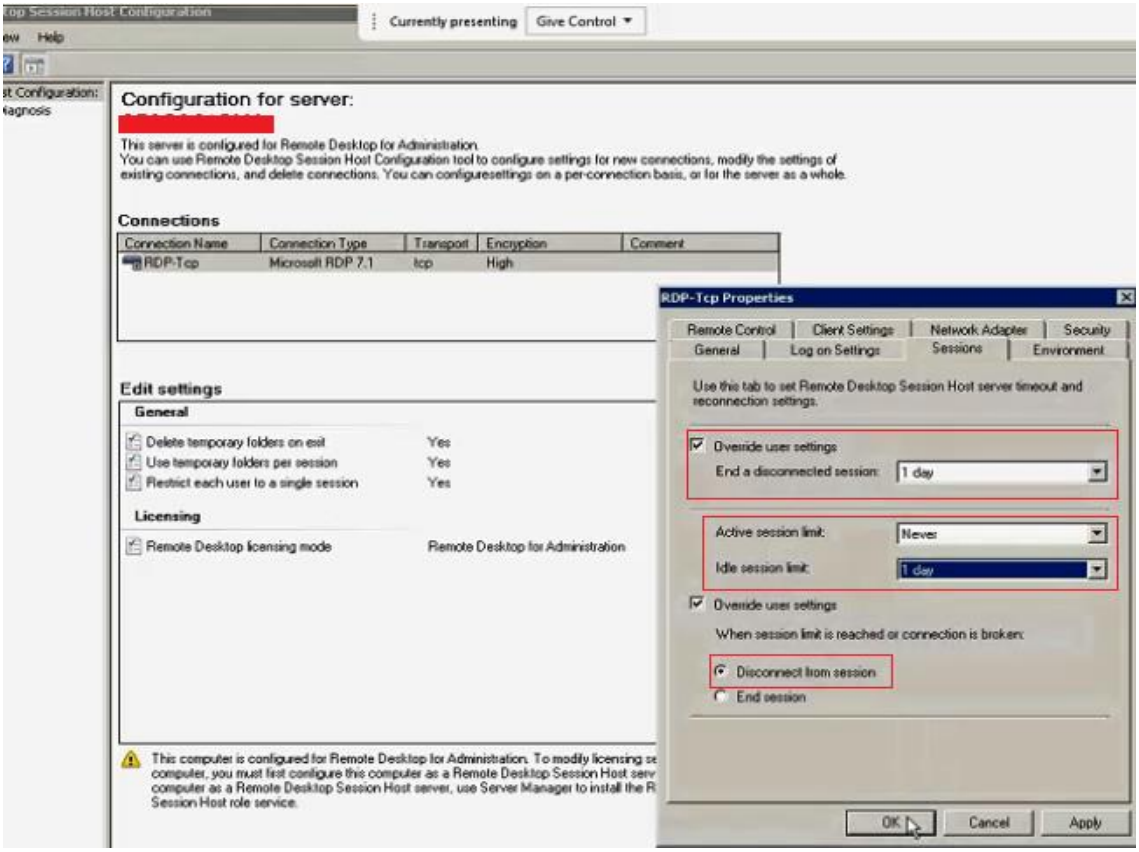

Kuva 3. Sisäverkon keksityt IP-osoitteet.

Tämän jälkeen lisättiin sallitut reitit komentokehotteessa Route add -komennolla Abloyn työasemilta default gatewayn kautta UAG:n aliverkkoon. Tämä täytyi tehdä siksi, koska UAG:n SP1 asennus sisältää myös TMG-palomuurin. Palomuuri asentuu UAG:n asennuksen yhteydessä ja estää kaikki vieraat yhteydet palvelimelle (kuva 4).




Kuva 4. Reitin lisääminen.

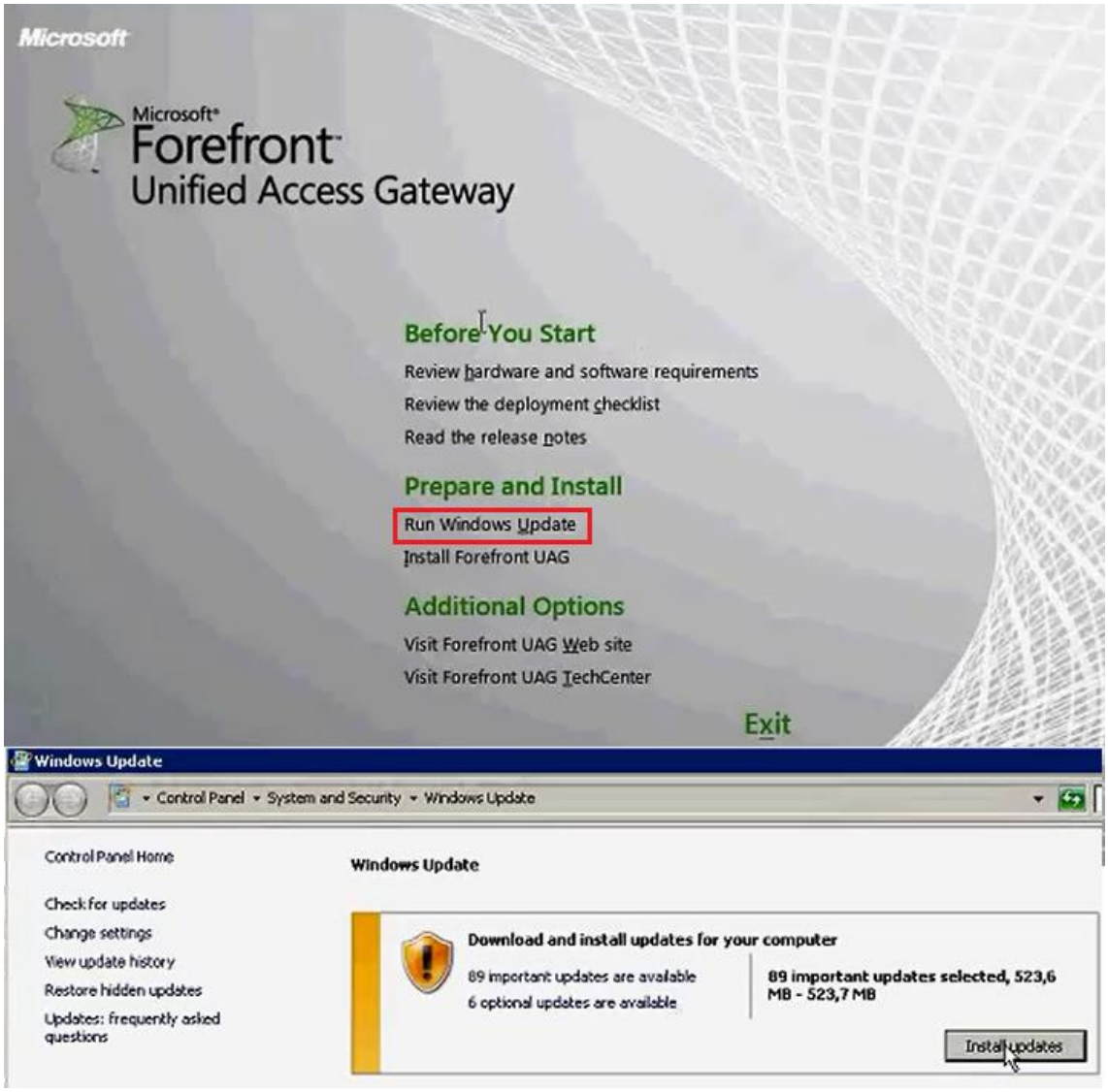
Palvelimen Remote Desktop Services-asetuksista täytyi käydä muuttamassa etätyöpöytäyhteyden TCP-asetuksia. Valinnaksi täytyi muuttaa ”disconnect from session”, koska vakiona se oli kohdassa ”End session” (kuva 5).




Kuva 5. Etätyöpöytäyhteyden TCP-asetukset.

Tämä muutos oli tärkeä, koska UAG:n asennuksen aikana asentuu myös TMG-palomuuri, joka katkaisee etätyöpöytäyhteyden. Vakiona ollut End session-asetus saisi aikaan kirjautuneen käyttäjän uloskirjautumisen, jos etätyöpöytä-yhteys menetetään pitkäksi aikaa. Tällöin asennuskin katkeaa.

UAG-asennustiedoston avattaessa suositeltiin tekemään Windows-päivitysten lataus, joten ne suoritettiin (kuva 6).




Kuva 6. UAG- asennusikkuna ja Windows-päivitysten asentaminen.

### 5.1.2 Unified Access Gatewayn asennus

Suoritettujen ensiasennusten jälkeen voitiin aloittaa itse Unified Access Gateway 2010:n asennus. Aikaisemmin ladatusta asennuspaketista suoritettiin ”Setup.exe”. Tämän jälkeen käynnistyi UAG-asennusikkuna (kuva 6), mistä valittiin ”Install Forefront UAG”. Ensimmäisen asennuspaketin asennus oli hyvin yksinkertainen, kunhan oli tehnyt huolella kaikki esivalmistelut. Asennuksen alussa hyväksyttiin käyttöehdot, ja sitten odoteltiin asennuksen valmistumista. Kun UAG SP1 ensiasennus oli valmis, palvelin täytyi käynnistää uudelleen. Palvelimen uudelleen käynnistyksen jälkeen TMG-palomuuriohjelmisto tuli käynnistää ja varmistaa, että se käynnistyi ongelmitta. TMG-palomuurin policyyn täytyi lisätä terminal serverin sisäverkon osoiteavaruus. Tällä varmistettiin, että palvelimeen saadaan yhteys vielä UAG:n ja TMG:n päivitysten jälkeen. Muutosten tallentamisen yhteydessä TMG pyysi kommentoimaan, mitä muutos koski, ja tieto tallentui palomuurin lokiin tulevaisuutta varten.

### 5.1.3 Threat Management Gatewayn päivittäminen

Unified Access Gateway SP1 -asennuspaketin mukana asentunut Threat Management Gateway -palomuuriohjelmisto täytyi päivittää omilla päivityspaketeilla, vaikka ensiasennuksessa kumpikin asentuivat samalta asennuspaketilta. Päivityksessä tuli ottaa huomioon, että päivitystä ei voinut tehdä suoraan uusimpaan versioon, vaan päivitykset täytyi tehdä asteittain oikeassa järjestyksessä.

UAG-ensiasennuspaketin mukana asentui TMG 7.0.9027.400 SP1 update 1 versio. Ensiasennuksen jälkeen päivitysjärjestys TMG:lle oli seuraava [6]:

- TMG, 7.0.9193.500, SP2
- TMG, 7.0.9193.644. SP2 Rollup 5

Näiden päivitysten jälkeen oli vasta mahdollista päivittää Unified Access Gateway.

### 5.1.4 Unified Access Gatewayn päivittäminen

Unified Access Gateway SP1 -asennuspaketti asensi 4.0.1752.10000 version UAG:sta. Tämän version asennuttua, ja kun TMG oli oikeassa järjestyksessä päivitettynä, oli aika päivittää UAG. Päivitysjärjestys oli seuraava [6]:

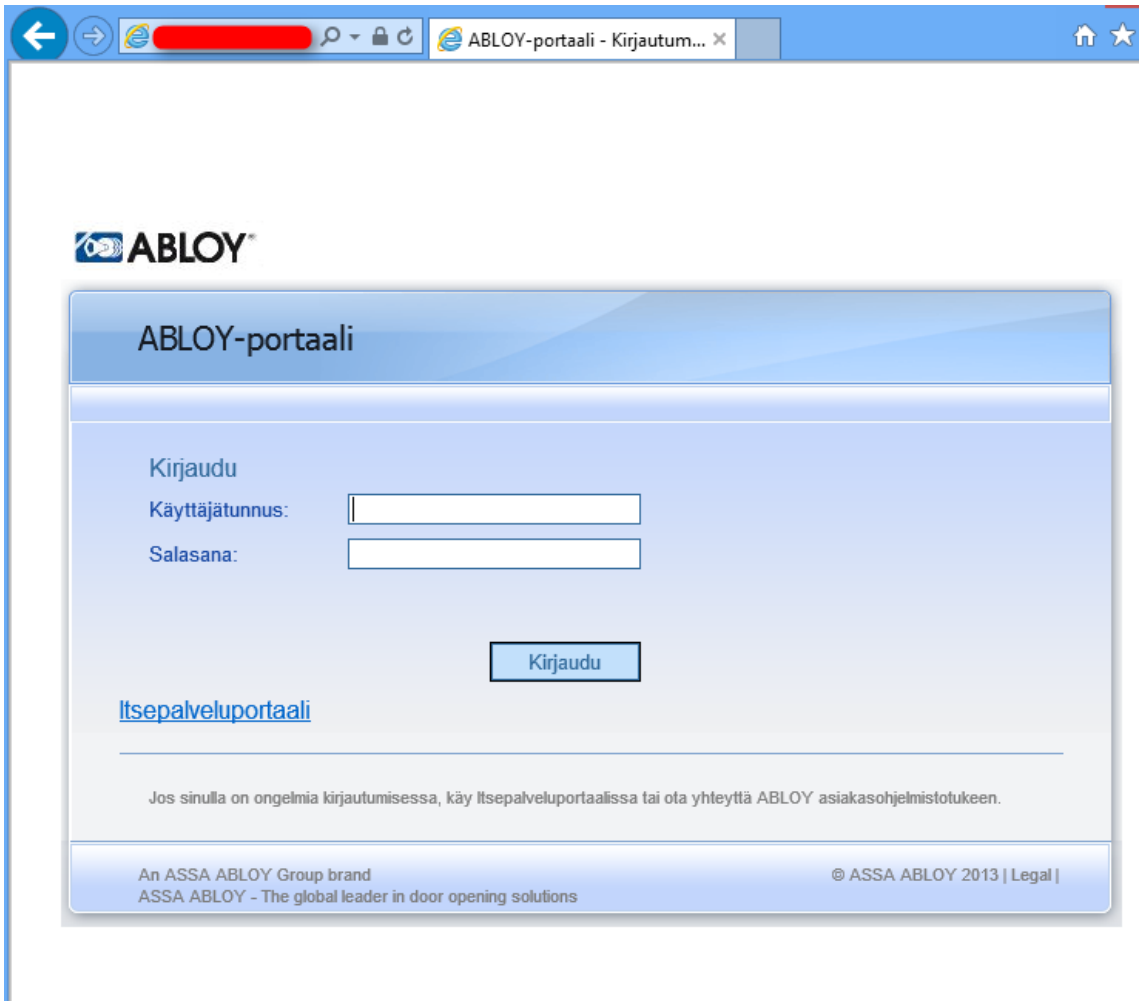
- UAG, 4.0.2095.10000, SP2, KB2710791 päivityksen keskeisin hyöty on mahdollistaa kirjautuminen UAG-portaaliin seuraavilla puhelimien käyttöjärjestelmillä: Windows Phone 7.5, iOS 5.x ja Android 4.x [3].

- UAG, 4.0.3123.10000, SP3, KB2744025 päivityksen keskeisin hyöty on mahdollistaa UAG-portaalin käyttö Internet Explorer 10 -selaimella [4].

- UAG, 4.0.3206.10100, SP3, KB2827350 päivityksen keskeisin hyöty on korjata portaalisivustoon kirjautumisessa esiintyneitä virheitä [5].

## 5.2 Käyttöönotto

UAG-ohjelmiston asennuksen jälkeen ei konfiguraatioita tehty uudelleen, koska vanhan palvelimen UAG-portaalin konfiguraatiot oli varmuuskopioitu ja ne palautettiin import-toiminnolla uuteen asennukseen. Tämä helpotti UAG:n käyttöönottoa merkittävästi, koska UAG-portaalisivuun oli aikojen saatossa tehty paljon muutoksia Abloy Oy:n tarpeisiin. Palvelimien palveluntarjoajalle tehtiin muutospyyntö palvelimien vaihdosta, eli uusi palvelin sai vanhan palvelimen IP-osoitteet ja portaali sivusto rupesi toimimaan (kuva 7).




Kuva 7. UAG-portaalisivu.

Tämän opinnäytetyön asennusosiossa käytiin läpi UAG:n kuudes asennusyritys, joka onnistui ongelmitta. Asennuksen aikana kohdattuihin ongelmatilanteisiin otetaan kantaa Ongelmatilanteet-luvussa 6.

# 6 Ongelmatilanteet

Opinnäytetyön suurimmaksi ongelmaksi osoittautui se, että UAG-portaalin asennuksesta virtuaalipalvelimelle ei löytynyt tietoa, koska ohjelma edusti rautapalvelimien aikakautta. Ongelmana oli myös vanhan UAG:n palvelimen suppea dokumentaatio. Asennuksessa jouduttiin etenemään onnistumisen ja erehdyksen periaatteella. Tiedon löytymistä ei auttanut Microsoftin uutisoima UAG-

tuen lopettaminen vuoden 2014 loppuun mennessä. Tämä johtui nähtävästi siitä, että UAG ei ollut kovin suosittu portaaliohjelmisto ja se on tunnettu hyvin kankeana ja vaikeasti ylläpidettävänä ohjelmistona.

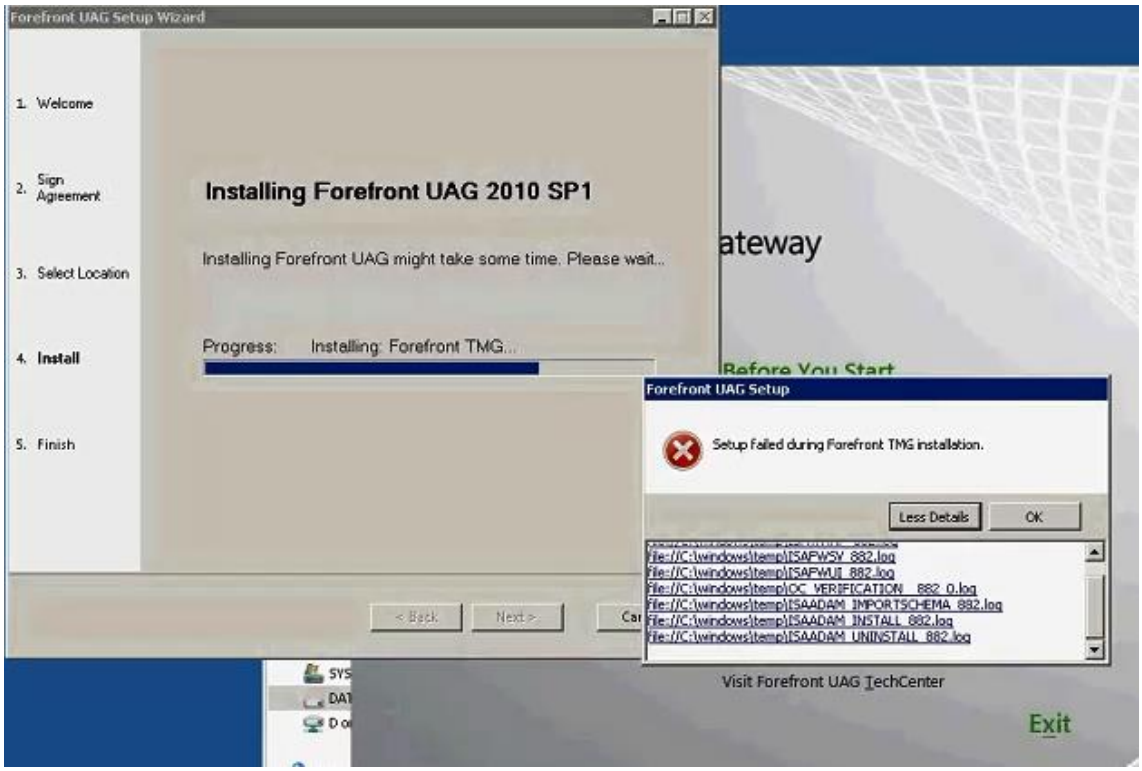
Ennen ensimmäisen asennuksen aloittamista ei tiedostettu, että sallitut reitit tulisi lisätä Abloyn työasemilta default gatewayn kautta UAG-palvelimen aliverkkoon. Reitin lisääminen olisi ollut tärkeää, koska UAG:n asennuksen aikana etätyöpöytäyhteys katkesi (kuva 8).


Kuva 8. TMG katkoi etätyöpöytäyhteyttä.

Katkoksen jälkeen UAG-palvelimeen ei saatu enää etätyöpöytäyhteyttä ja palvelimien ylläpitäjälle jouduttiin tekemään tukipyyntö palvelimen palauttamiseksi alkutilaan. Palvelimeen ei saatu etätyöpöytäyhteyttä, koska TMG-palomuuri oli asentunut ja esti kaikki vieraat yhteydet palvelimeen.

Toisella asennuskerralla lisättiin reitit palvelimelle ja aloitettiin UAG:n asennus alusta. Asennus katkaisi taas etätyöpöytäyhteyden, mutta palvelimelle päästiin

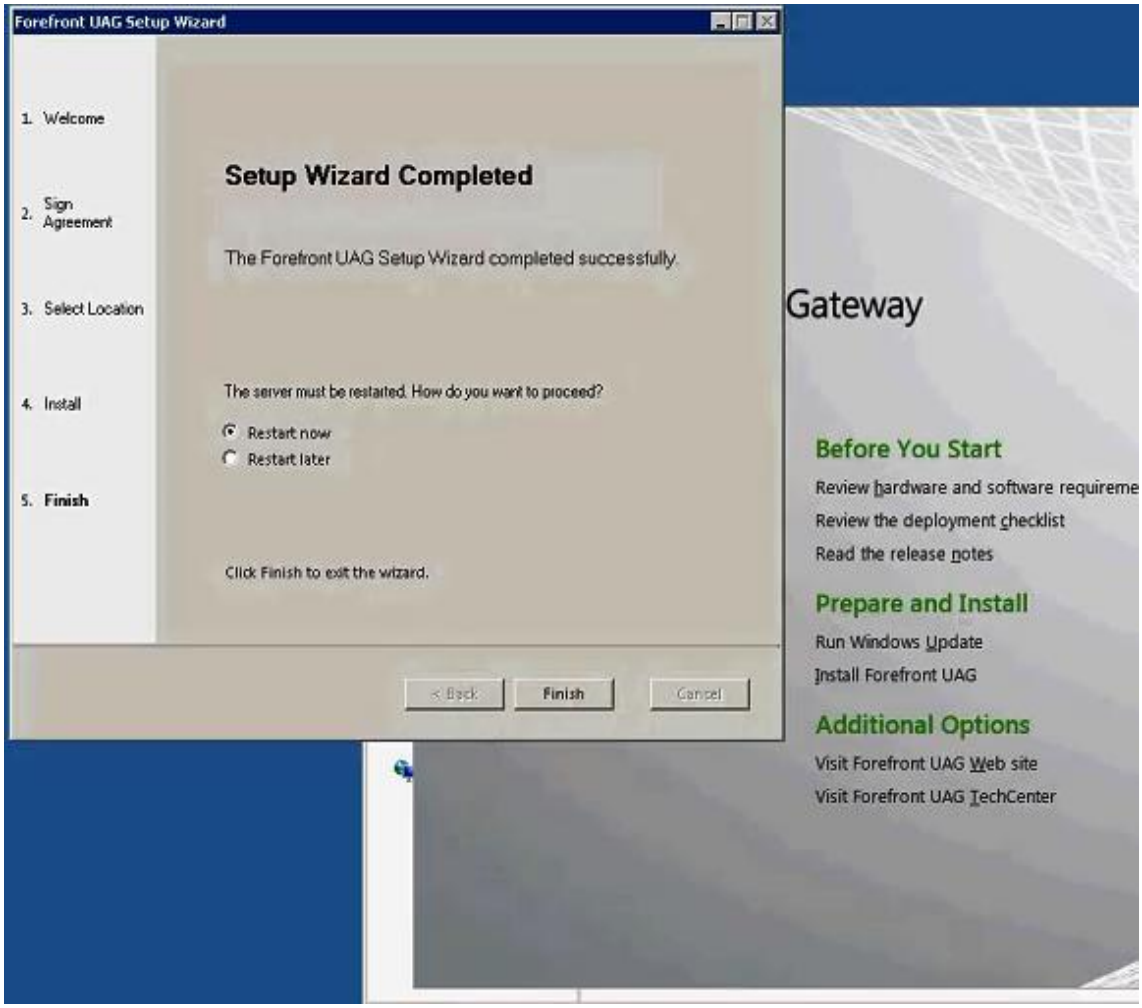
kirjautumaan takaisin, koska reitit oli lisätty. Palvelimelle kirjautuessa huomattiin, että UAG SP1 -asennus oli jäänyt kesken, eli palvelin ei pelkästään katkaissut etätyöpöytäyhteyttä vaan kirjasi myös käyttäjän ulos. Tällä kertaa poistettiin kaikki UAG SP1 -asennuksen asentamat komponentit ja asennus aloitettiin alusta. Asennuksen valmistuessa etäyhteys ei kerennytkään katketa vaan asennus antoi TMG:n asennusvirheen (kuva 9).




Kuva 9. TMG:n asennusvirhe.

Tässä vaiheessa ei vielä tiedetty mistä kyseinen virhe johtui. UAG SP1 -paketin asentamat komponentit poistettiin jälleen, ja Program Files -kansiosta poistettiin TMG-kansio, jota uninstall ei ollut poistanut. Asennus aloitettiin taas puhtaalta pöydältä. Nyt asennus eteni ilman edellä mainittua TMG:n virhettä, mutta etäyhteys katkesi taas. Tästä pystyi päättelemään, että TMG:n virheen aiheutti nähtävästi Program Files -kansioon jäänyt TMG:n kansio ja sen sisältö. Taas oli päädytty samaan tilanteeseen kuin aikaisemmin. Tällä kertaa päätettiin jatkaa asennusta poistamatta asentuneita lisäosia. Asennuksen aikana etäyhteys katkesi viidesti ja palvelimelle jouduttiin kirjautumaan joka kerta uudelleen. Palvelimelle takaisin kirjautuessa UAG SP1 -asennuspaketti piti käynnistää uudel-

leen, mutta asennus osasi jatkaa samasta kohdasta mihin se oli jäänyt. Lopulta asennus valmistui. (kuva 10).



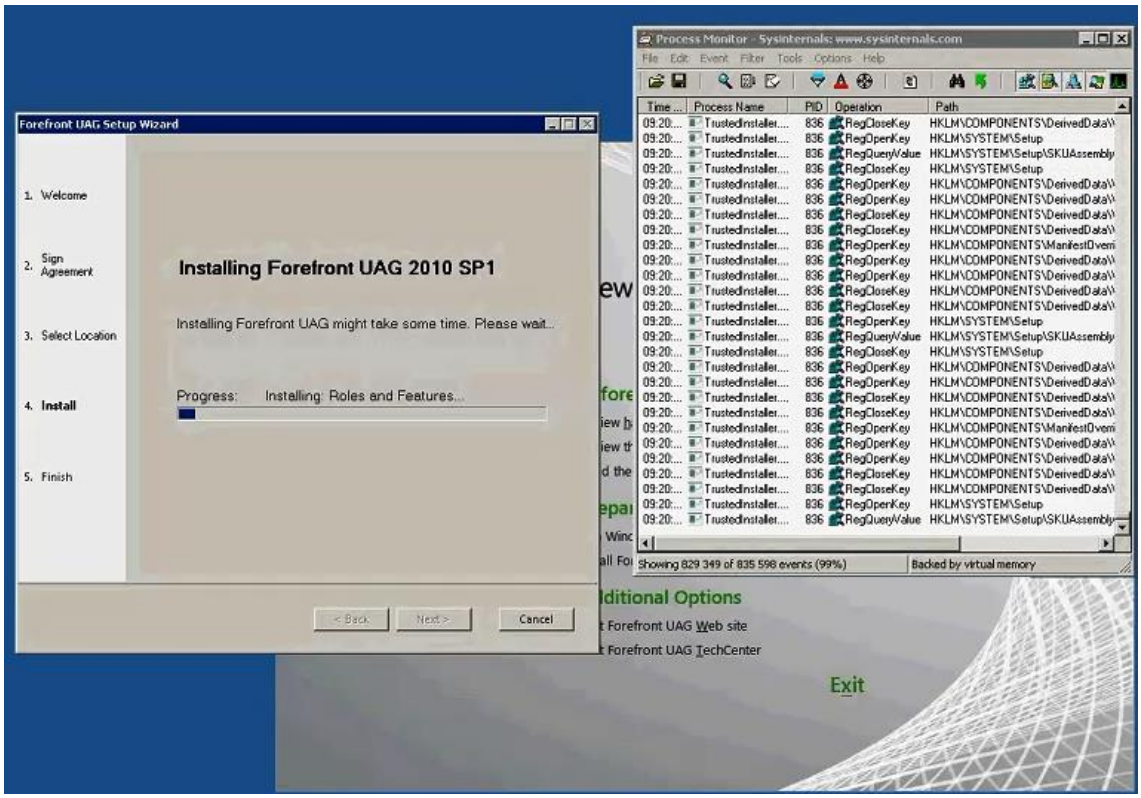

Kuva 10. Valmis asennus.

Palvelin käynnistettiin uudelleen ja TMG:n ensimmäisen päivityspaketin asennus aloitettiin. TMG:n päivityksen jälkeen palvelin käynnistettiin uudelleen, mutta palvelimeen ei saatu enää yhteyttä, vaikka sallitut reitit oli lisätty työkoneen ja palvelimen välille route add -komennolla (kuva 4). Ennen uudelleen käynnistystä TMG-palomuurin policyyn olisi täytynyt lisätä terminal serverin sisäverkon osoiteavaruus, jotta palvelimelle olisi päässyt takaisin. Palvelimien ylläpitäjälle jouduttiin tekemään taas tukipyyntö palvelimen palauttamiseksi alkutilaan.

Kolmannella asennuskerralla UAG SP1 saatiin asennettua ongelmitta, koska tiedettiin kuinka asennuksessa kuului edetä, lukuun ottamatta etätyöpöytäyh-

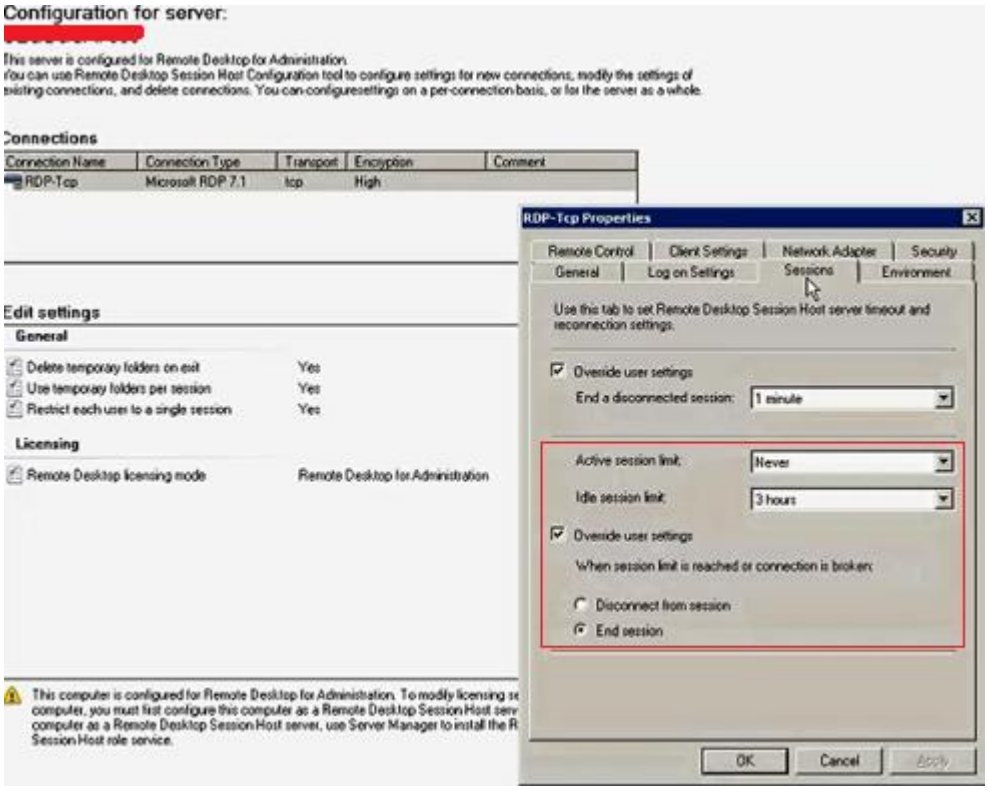
teyden katkeilua ja asennuksen uudelleenkäynnistelyä. Tämä herätti epäilyn, oliko UAG SP1 asentunut oikein, vaikka UAG ja TMG-palvelut käynnistyivätkin.

Etätyöpöytäyhteyden katkomista selvitettiin konsulttiyrityksen UAG-asiantuntijan kanssa. Ongelmaa yritettiin ratkaista palvelimen Process Monitorilla, joka laitettiin päälle asennuksen ajaksi (kuva 11).




Kuva 11. Process Monitorin käyttö asennuksessa.

Prosess Monitorista ei kuitenkaan ollut apua, koska asennus sai aikaan satojatuhansia tapahtumia ja niiden joukosta ongelman aiheuttaja olisi ollut mahdoton löytää. Konsulttiyrityksen UAG-asiantuntija oli mukana toisen UAG-palvelimen asennuksessa ja ongelma oli hänellekin haastava, mutta se saatiin ratkaistua. Ongelma etäyhteyden- ja asennuksen katkomiseen oli lopulta liiankin yksinkertainen. UAG-palvelimen etätyöpöytäyhteyden asetuksissa oli valinta end session päällä (kuva 12), ja tämän asetuksen takia etäkäyttäjä kirjattiin ulos palvelimelta, jos etätyöpöytäyhteys katkesi.




Kuva 12. UAG-palvelimen etätyöpöytäasetukset.

Opinnäytetyöprojektin alussa Microsoft ilmoitti lopettavansa UAG:n tuen 2014 vuoden loppuun. Tämän uutisen ansiosta projekti päätettiin kohdistaa vain yhden UAG-tuotantopalvelimen asennukseen, koska oli turhaa tuhlata resursseja toiseen identtiseen UAG-palvelimeen, jolla olisi mahdollistettu F5-kuormantasaus. Heräsi myös kysymyksiä, olisiko uutta UAG-palvelinta edes hyödyllistä ottaa vanhan palvelimen tilalle, koska uuden palvelimen käyttöhyöty olisi ollut vain vuoden loppuun. Tämän takia projekti päätettiin viedä loppuun vain yhdellä tuotantopalvelimella ja yhdellä UAG-testipalvelimella, joka asennettiin täysin identtisesti tuotantopalvelimen tapaan. Uudet UAG-tuotanto- ja testipalvelimet päätettiin jättää varapalvelimiksi, koska vanhan palvelimen oletettiin kestävän vuoden loppuun asti.

Vanhan UAG-palvelimen kanssa kuitenkin ilmeni pian ongelmia laitevian takia. Palveluntarjoaja joutui tästä syystä vaihtamaan komponentteja, koska palvelin oli rikkoutunut. Komponenttien vaihdosta johtuen TMG-palomuuri esti palvelimelle etäkirjautumisen, koska ohjelmisto koki laitepäivityksen tietoturvahyökkäyksenä. Vanhaa palvelinta ei saatu enää toimimaan, joten uudelle UAG-

palvelimelle tuli käyttöä. Uuteen tuotantopalvelimeen palautettiin vanhan palvelimen konfiguraatiot UAG-ohjelman import toiminnolla. Palvelin otettiin tuotantoon tekemällä tukipyyntö palvelimien palveluntarjoajalle. Palveluntarjoaja vaihtoi uuden palvelimen IP-osoitteet vastaamaan vanhan palvelimen IP-osoitteita ja näin uusi palvelin oli otettu käyttöön.

# 7 Pohdinta

Opinnäytetyö oli hyvin vaativa, koska UAG-ohjelmistosta ei ollut aikaisempaa kokemusta ja sen asennuksesta virtuaalipalvelimelle löytyi niukasti tietoa. Projekti viivästyi usealla kuukaudella, koska oli haastavaa saattaa aikataulut yhteen ohjelmistokehitys puolen henkilöiden kanssa tehdessäni UAG-projektia normaalin päivätyöni ohella. Olisi ollut helpompi valita opinnäytetyö, jota olisi voinut tehdä silloin, kun itselle sopii. Tämän opinnäytetyön kanssa se ei olisi onnistunut, koska asennuksessa ilmeni hyvin mystisiä ongelmia, ja harva iso organisaatio uskaltaisi antaa näin suuren vastuun pelkästään opinnäytetyön tekijälle ilman valvontaa. Opinnäytetyön kirjallista osuutta kirjoitin omalla ajalla projektin valmistuttua. Asennusongelmien ja Microsoftin uutisoiman UAG:n tuen lopettamisen takia mielessä saattoi käydä projektin kesken jättäminen, koska palvelinta ei ehkä oltu ottamassa käyttöön. Keskenjättäminen ei kuitenkaan ollut vaihtoehto ja oli tärkeää, että projekti vietiin loppuun kaikesta huolimatta, koska vanha palvelin hajosi ja lopetti toimintansa. Ilman valmiiksi tilattua ja asennettua UAG-palvelinta, ei sähköistä tilausjärjestelmää olisi saatu heti jälleenmyyjien käyttöön takaisin ja jälleenmyyjät olisivat joutuneet lähettämään tilauksensa manuaalisesti faxilla. Tämä olisi ollut todella huono asia toimeksiantajan kannalta, koska faxeja olisi tullut päivittäin useita satoja ja nämä tilaukset olisi toimeksiantaja joutunut syöttämään järjestelmään manuaalisesti.

Uuden UAG-palvelimen käyttöönottoon oli hyvä päättää projekti. Opinnäytetyöprojekti auttoi kehittämään stressinsietokykyä ja opetti ajankäytön suunnittelua sekä sen hallintaa. Kyseinen projekti ei olisi enää vaikea toteuttaa uudelleen,

koska nyt tiedän kuinka UAG:n virtuaalipalvelimelle asennus eroaa normaalista palvelinasennuksesta.

Tulevaisuudessa itse palvelimen päivitys on helpompaa, koska käytössä on virtuaalinen palvelin, eli suorituskyvyn lisääminen onnistuu ohjelmallisesti. Jos oletettaisiin, että UAG-portaalin käyttö jatkuisi tulevaisuudessa pidemmälle ja ohjelmisto täytyisi asentaa joskus uudelleen, niin se olisi helppo toteuttaa, koska nykyinen asennus on dokumentoitu videoiden. Kuitenkin UAG-ohjelmiston tuen päättymisen johdosta korvaavan portaalituotteen kehityshanke on jo aloitettu.

## Lähteet


1. ABLOY Oy. Vahva loppuvuosi ASSA ABLOYlle. 2014. http://www.abloy.fi/fi/abloy/abloyfi/Uutiset-Lehdisto/Uutiset2/2014/News-Category-2014/Vahva-loppuvuosi-ASSA-ABLOYlle. [Viitattu 8.9.2014]

2. Microsoft Corporation. Microsoft Forefront Unified Access Gateway. 2014. http://en.wikipedia.org/wiki/Microsoft_Forefront_Unified_Access_Gateway. [Viitattu 29.10.2014]

3. Microsoft Corporation. Description of Service Pack 2 for Forefront UAG. 2012. http://support2.microsoft.com/kb/2744025. [Viitattu 5.10.2014].

4. Microsoft Corporation. Description of Forefront UAG 2010 Service Pack 3. 2013. http://support2.microsoft.com/kb/2744025. [Viitattu 5.10.2014]

5. Microsoft Corporation. Description of Rollup 1 for Forefront UAG 2010 Service Pack 3. 2013. http://support2.microsoft.com/kb/2827350. [5.10.2014]

6. Winfrasoft. How to determine which build version of TMG 2010 and UAG 2010 is installed. 2014. How to determine which build version of TMG 2010 and UAG 2010 is installed. [5.10.2014]