TAMPEREEN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

Citrix Access Gateway SSL VPN –järjestelmän käyttöönotto

Karo Kaarakainen

Tietojenkäsittelyn koulutusohjelma
Maaliskuu 2007
Työn ohjaaja: Harri Hakonen

TAMPERE 2007

TAMPEREEN
AMMATTIKORKEAKOULU

Tekijä(t) Karo Kaarakainen

Koulutusohjelma(t) Tietojenkäsittely

Opinnäytetyön nimi Citrix Access Gateway SSL VPN -järjestelmän käyttöönotto

Työn valmistumis-kuukausi ja -vuosi Maaliskuu 2007

Työn ohjaaja Harri Hakonen

Sivumäärä: 116

TIIVISTELMÄ

Tämä opinnäytetyö käsittelee toimeksiantajani Visma Software Oyj:n tietoverkkoon implementoitavan Citrix Access Gateway SSL VPN -järjestelmän käyttöönottoa. Citrix Access Gateway -järjestelmä on laitepohjainen SSL VPN -yhdyskäytävä, jossa yhdistyvät perinteisen IPSec VPN:n ja SSL VPN:n parhaat ominaisuudet. Opinnäytetyön aihe sai alkunsa Visma Software Oyj:n tarpeesta hankkia uusi VPN-järjestelmä vanhan käytössä olleen Windows-käyttöjärjestelmään integroidun IPSec VPN -järjestelmän tilalle.

Opinnäytetyön tavoitteena on ottaa käyttöön ja konfiguroida Citrix Access Gateway -järjestelmä, jonka avulla käyttäjille mahdollistetaan helppokäyttöinen ja tietoturvallinen pääsy Visma Software Oyj:n sisäverkkoon. Järjestelmän asennukseen ja konfigurointiin on pääasiassa käytetty apuna Citrix System Inc.-yhtiön julkaisemia sähköisiä järjestelmänvalvojan oppaita.

Opinnäytetyön tuloksena on saatu aikaan Visma Software Oyj:n sisäverkon tietoturvan paraneminen uuden Citrix Access Gateway -järjestelmän käyttöönoton myötä sekä lisäksi etäkäyttäjille samalla helppokäyttöinen ja turvallinen SSL VPN -järjestelmä. Tähän järjestelmään integroitiin lisäksi SafeWord for Citrix -autentikointijärjestelmä, jolla varmistetaan etäkäyttäjien autentikointi heidän kirjautuessaan Citrix Access Gateway -järjestelmään.

Tulevaisuudessa Citrix Access Gateway -järjestelmän käyttöä laajennetaan täyden VPN-yhteyden lisäksi niin sanotun Kiosk Mode -tilan käyttöön, jolloin järjestelmään voidaan ottaa rajoitettu SSL VPN -yhteys esimerkiksi lentoasemien Internetkioskeista tietoturvallisesti.

Avainsanat Etäkäyttö Verkonhallinta Tietoliikenneverkot Tietoturva

TAMPERE
POLYTECHNIC

Author(s)	Karo Kaarakainen
Degree Programme(s)	Business Information Systems
Title	Citrix Access Gateway SSL VPN system implementation
Month and year	March 2007
Supervisor	Harri Hakonen

Pages: 116

ABSTRACT

This thesis focuses on the implementation of the Citrix Access Gateway SSL VPN system to the network infrastructure of Visma Software. Citrix Access Gateway is a hardware-based SSL VPN gateway that combines the best features of IPSec VPN and SSL VPN. The subject of this thesis started out from the need of a new VPN system to replace the old Windows-based IPSec VPN.

The goal of this thesis is to mobilize and configure the Citrix Access Gateway system that provides its users easy and safe access to the internal network of Visma Software. The system is installed and configured mainly with the help of electronic administrator's guides by Citrix Systems Inc.

The result of this thesis is better data security in the internal network of Visma Software due to the implementation of the Citrix Access Gateway system. At the same time, remote users can now use this SSL VPN system securely and handy. In addition, the SafeWord for Citrix authentication system was also integrated to the Citrix Access Gateway system, and now remote users can be authenticated before they get access to the system.

In the future, the utilization of the Citrix Access Gateway system will be widened so that it is possible to mobilize the so-called Kiosk Mode status where remote users can form a restricted SSL VPN connection securely from internet kiosks located at airports.

Keywords Remote access Network management Communications network Data security

Sisällysluettelo

Käsitteet

Active Directory	Käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista.
CHAP	CHAP (Challenge Handshake Authentication Protocol) on paranneltu versio PAP-protokollasta. Siinä salasana kulkee aiemmin linkkitasolla neuvotellulla algoritmilla salattuna, jossa usein käytetään MD5-algoritmia.
CIDR	CIDR (Classless Inter-Domain Routing) mahdollistaa IPv4-osoiteluokkien yhdistämisen tai jakamisen pienempiin osiin (aliverkkoihin) käyttämällä eripituista aliverkkopeitettä, joka kertoo, kuinka monta bittiä IP-osoitteen alusta kuuluu sen verkko-osaan. Loput bitit yksilöivät laitteen.
DMZ	DMZ (Demilitarized zone) on tietoverkon alue, joka sijaitsee yrityksen sisä- ja ulkoverkon välissä. DMZ-alueella sijaitsee yleensä yritysten WWW-, FTP-, SMTP sekä DNS-palvelimet.
DNS	DNS (Domain Name System) on nimenselvennysprotokolla TCP/IP-verkkoihin, joka muuntaa alfanumeeriset DNS-nimet ip-osoitteiksi. Siten verkon tietokoneet voi kommunikoida keskenään.
EAP	EAP-protokollaa (Extensible Authentication Protocol) käytetään päätelaitteen ja autentikointipalvelimen välisessä autentikointitiedon siirrossa.
ESP	ESP-protokollaa (Encapsulating Security Payload) käytetään pakettivirtojen salaamiseen IPSec VPN-protokollan sisällä.
Frame Relay	Frame Relay on alueverkkotekniikka, jolla yhdistetään yrityksen lähiverkkoja toisiinsa. Toisin sanoen sillä yhdistetään asiakasverkoissa olevat reitittimet toisiinsa.
IPSec	IPSec (IP Security Protocol) käsittää TCP/IP-protokollaperheeseen kuuluvia tietoliikenneprotokollia internet-yhteyksien suojaamiseen mm. salaukseen, osapuolten todennukseen sekä tiedon eheyden varmistamiseen. IPSecin tiedonsiirto toteutetaan OSI-mallin verkkokerroksella (3. kerros).

L2TP	L2TP (Layer 2 Tunneling Protocol) on Microsoftin ja Ciscon yhdessä kehittämä VPN-tunnelointiprotokolla, joka toimii OSI-mallin 2. kerroksella ja tukee IP-protokollan lisäksi muita protokollia.
MD5	MD5 (Message-Digest algorithm 5) on 128-bittinen tarkistussumma, jota käytetään tarkistamaan, onko tietyn tiedoston sisältö muuttunut (esim. tahallinen väärennös tai tiedonsiirtovirhe).
MS-CHAP	MS-CHAP-protokolla (Microsoft Challenge Handshake Authentication Protocol) poikkeaa CHAP-protokollasta muun muassa sen paremmin kontrolloidun uudelleen-autentikointi- ja salasanan vaihto mekanismin kannalta.
NetBIOS	NetBIOS-nimenselvennystä (Network Basic Input/Output System) käytetään liittämään laitteen NetBIOS-nimi ip-osoitteeseen. Käytetään tavallisesti ”tiedostojen ja tulostimien jakamiseen Microsoft- verkoissa”-prosessissa.
OSI-malli	OSI-malli (Open Systems Interconnection Reference Model) kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa. Kukin kerroksista käyttää yhtä alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäs.
PAP	PAP (Password Authentication Protocol) on vanhin autentikoinnissa käytetty protokolla, jossa käyttäjätunnus ja salasana kulkevat selkokielisenä verkossa.
PPP	PPP-protokolla (Point-to-Point Protocol) toimii yleensä OSI-mallin 2. kerroksen protokollana synkronisten ja asynkronisten verkkojen yli. PPP rakennettiin toimimaan usean verkko-kerroksen protokollan kanssa kuten IP, IPX, ja AppleTalk.
PPTP	PPTP (Point-to-Point Tunneling Protocol) on VPN-tunnelointiprotokolla, joka pohjautuu PPP-protokollaan. PPTP-protokolla on PPP-protokollan laajennus, joten se voi tunneloida muitakin protokollia kuin TCP/IP-protokollaa.
RPC	RPC (Remote Procedure Call) on teknologia, jossa ohjelmisto pyytää sen alirutiinin tai prosessin suorittavan toimenpiteen, jota ajetaan toisella päätelaitteella samassa tietoverkossa.

SSL VPN	SSL VPN (Secure Sockets Layer Virtual Private Network) on tekniikkaa, jossa VPN-yhteyden tiedonsiirto muodostetaan SSL-yhteyden yli OSI-mallin kuljetuskerroksella (4. kerros).
TCP/IP	TCP/IP (Transmission Control Protocol / Internet Protocol) koostuu useista tietoverkkoprotokollista, joita käytetään internet-liikennöinnissä. IP-protokolla vastaa pakettien reitittämisestä verkossa ja TCP-protokolla kahden päätelaitteen välisestä tiedonsiirtoyhteydestä, pakettien järjestämisestä sekä pakettien uudelleenlähettämisestä.
TLS	TLS (Transport Layer Security) on salattu tiedonsiirtoprotokolla, jota käytetään muun muassa verkkopankkien www-sivustojen liikenteen salaamiseen.
VPN	VPN (Virtual Private Network) on yksityinen näennäisverkko, johon voidaan ottaa salattu yhteys julkisen verkon yli.
WEP	WEP-salaus (Wired Equivalent Privacy) käytti alunperin 40-bittistä salaista avainta lähetettävien pakettien salaamiseen langattomassa verkossa. Nykyisin kuitenkin voidaan käyttää 64- tai 128-bittistäkin salausta.
X.25	X.25-protokollapino on suunniteltu käytettäväksi pakettikytkentäisella yhteydellä WAN-verkoissa (Wide Area Network) käyttäen puhelin- tai ISDN-laitteita (Integrated Services Digital Network).

1 Johdanto

Opinnäytetyöni aiheena on uuden monipuolisemman ja tietoturvallisen SSL VPN -järjestelmän (Secure Sockets Layer Virtual Private Network) käyttöönotto ja konfigurointi toimeksiantajani Visma Software Oyj:n tietoverkkoon käyttäen Citrix Systems Inc -yhtiön kehittämää Citrix Access Gateway -järjestelmää. Samalla tämä järjestelmä korvaa vanhan käytössä olleen Windows-käyttöjärjestelmään integroidun IPSec VPN -järjestelmän (IP Security Protocol VPN), joka muodostaa pelkän VPN-yhdyskäytävän eri verkkojen välillä eikä tarjoa mahdollisuutta yhtä monipuoliseen pääsy- ja yhteyspolitiikkojen konfigurointiin ja hallintaan kuin Citrix Access Gateway -järjestelmä. Citrix Access Gateway on laitepohjainen SSL VPN -yhdyskäytävä, jossa yhdistyvät perinteisen IPSec VPN:n ja SSL VPN:n parhaat ominaisuudet. Käyttöön tarvittava laitteisto koostuu yhdyskäytävälaitteesta sekä yhtäaikaisista käyttäjälisensseistä. Visma Software Oyj:n tarpeisiin hankittiin lisäksi myös optiona saatava Citrix Advanced Access Control -ohjelmisto, joka mahdollistaa yhteyden muodostavien päätelaitteiden tutkimisen esimerkiksi niiden tietoturvatason perusteella ennen järjestelmään kirjautumista. Siten voidaan jo alkuvaiheessa evätä pääsy järjestelmään pääsypolitiikkojen avulla. Lisäksi Citrix Advanced Access Control -ohjelmisto mahdollistaa selainpohjaisen Access Center -portaalin, jonka kautta käyttäjille voidaan julkaista Citrix MetaFrame Presentation Server -ympäristön sovelluksia, tarjota mahdollisuus sähköpostijärjestelmän selainpohjaiseen versioon sekä liittää jaetut verkkolevyt osaksi portaalisivustoa.

Suoritin opintoihini kuuluvan viiden kuukauden työharjoittelun Visma Software Oyj:ssä Espoon toimipisteessä tietohallintoosastolla samalla, kun vakinainen työsuhteeni siellä alkoi vuoden 2006 toukokuussa. Tarjolla oli heti alusta lähtien useita erilaisia ideoita opinnäytetyön aiheeksi, joista Citrix Access Gateway -järjestelmän käyttöönotto yrityksen tietojärjestelmässä vaikutti haasteellisimmalta.

Opinnäytetyöni alkupuolella käyn läpi Visma Software Oyj:n tietoverkon infrastruktuuria, johon Citrix Access Gateway -järjestelmä integroidaan käsittäen palvelimet, tietoturvan ja Citrix MetaFrame Presentation Server -järjestelmän sekä muut verkon palvelut ja resurssit. Järjestelmistä tarkemmin tulen käymään läpi Citrix MetaFrame Presentation Server -järjestelmän, joka voidaan liittää osaksi uutta Citrix Access Gateway -järjestelmää. Seuraavaksi käsittelen VPN-protokollien ja erityisesti SSL VPN -protokollan teoriaa, jotta lukijalle muodostuu käsitys uudessa integroitavassa Citrix Access Gateway -järjestelmässä käytettävästä SSL VPN -tekniikasta. Työn laajin osuus koostuu Citrix Access Gateway -järjestelmän käyttöönoton ja konfiguroinnin lisäksi myös siihen liitettävästä SafeWord for Citrix -autentikointijärjestelmän implementoinnista. Tämä järjestelmä tuo lisäturvaa Citrix Access Gateway -järjestelmään kirjauduttaessa, kun tavallisten verkkotunnusten lisäksi käytetään SafeWord-toukasta (kts. sivu 27) saatavaa yksilöllistä ja vaihtuvaa salasanaa. Työn loppupuolella on vielä yhteenvetokappale koko Citrix Access Gateway SSL VPN -järjestelmän käyttöönoton onnistumisesta sisältäen vastaan tulleet yllättävät ongelmat sen konfiguroinnissa sekä asennuksessa ja käytössä käyttäjillä.

1.1 Toimeksiantajan esittely

Visma Software Oyj on pohjoismainen ohjelmistoyritys, joka kehittää, markkinoi ja myy asiakkuuksienhallinnan ja toiminnanohjauksen tietojärjestelmiä eri toimialoille kuten urakointiin, energia-alalle, teollisuuteen, tukku- ja erikoistavarakaupalle, kiinteistöhallintaan ja tilitoimistoille. Päätuotteina tällä hetkellä ovat Nova-, Econet-, Liinos6 sekä VISMA CRM -ohjelmistot. Tuotekehityksestä 95 % tapahtuu Suomessa.

Visma Software Oyj on osa norjalaista Visma-konsernia, johon kuuluu sen lisäksi konsultointiyritys Visma Services, joka tarjoaa taloushallinnon ulkoistuspalveluita. Koko konsernissa työskentelee n. 2000 ja Suomessa yli 200 asiantuntijaa kahdeksalla eri paikkakunnalla, joista Espoon Leppävaarassa on Suomen pääkonttori. Visma Software Oyj:llä on Suomessa n. 14000 yritysasiakasta.

Suomessa työskentelevistä 200 henkilöstä n. 100 henkilöä on käyttänyt IPSec VPN -etäyhteyttä muodostaessaan yhteyden Visma Software Oyj:n sisäverkkoon, joista kaikki siirtyvät uuden Citrix Access Gateway SSL VPN -järjestelmän käyttöön.

Visma Software Oyj:n toimipisteiden välinen tietoverkko on rakennettu TDC Song -verkko-operaattorin IP (internet Protocol) VPN -verkon päälle. Kaikkien toimipisteiden lähiverkot on yhdistetty siten, että paikallisilta verkko-operaattoreilta on vuokrattu kaistaa TDC Songin runkoverkkoon saakka, jota käyttäen lähiverkot saadaan yhdistettyä. Toimipisteistä Vaasa, Espoo sekä Jyväskylä käyttävät 10 megabitin kaistaa ja Turku, Tampere sekä Kuusamo neljän megabitin kaistaa Songin runkoverkkoon yhteyksissään. Visma Software Oyj:n emoyhtiöön Norjaan on käytössä 10 megabitin kaista. Kaikkien toimipisteiden liikenne on reititetty Jyväskylän palvelinkeskuksen kautta internetiin käyttäen 10 megabitin kaistaa. Langallisen lähiverkon nopeus on 100 megabittiä sekunnissa kaikissa toimipisteissä.

1.2 Opinnäytetyön tavoite

Opinnäytetyön tavoitteena on ottaa käyttöön ja konfiguroida Citrix Access Gateway SSL VPN -järjestelmä, jonka avulla käyttäjille mahdollistetaan helppokäyttöinen ja tietoturvallinen pääsy Visma Software Oyj:n sisäverkkoon. Tavoitteen saavuttamiseksi käytän opinnäytetyössäni apuna pääasiassa Citrix System Inc. -yhtiön julkaisemia sähköisiä järjestelmänvalvojan oppaita, mutta hyödynnän lisäksi oppimaani sekä muuta aiheeseen liittyvää dokumentaatiota.

2 Verkon infrastruktuuri ja sen palvelut

Tässä luvussa käydään läpi Visma Software Oyj:n verkkoinfrastruktuuria, jossa uusi Citrix Access Gateway -järjestelmä otetaan käyttöön. Useat sisäverkon palvelut liittyvät joko osittain tai kokonaan uuden SSL VPN -järjestelmän avulla tietoturvallisesti käytettäviin resursseihin. Tarkemmin näistä resursseista keskityn Citrix MetaFrame Presentation Server -järjestelmään sekä tietoverkon palvelimiin.

2.1 Tuotantoympäristön ohjelmistot ja palvelut

Sisäverkon palveluihin kuuluvat muun muassa Citrix MetaFrame Presentation Server -ympäristö, jonka kautta sisäisessä käytössä on toiminnanohjausjärjestelmä (ERP) Nova Pro sekä asiakkuuksienhallintajärjestelmä (CRM) Visma CRM. Lisäksi osaamisenhallintaan kehitetty kolmannen osapuolen ohjelmisto Elbit Skills sekä prosessienhallintaohjelma QPR ovat osa verkkoinfrastruktuuria. Myös projektinhallintaan on oma järjestelmänsä, Microsoft Project Server -ympäristö. Visma Software Oyj:ssä on käytössä intranet-järjestelmä, joka kantaa nimeä Vintra. Vintraan on koottu tärkeimmät tiedot koko organisaatiosta ja sen yksiköistä, henkilöstöstä ja henkilöstöasioista sekä lisäksi sisäisiä ja ulkoisia tiedotteita. Siksi Vintraa voidaan käyttää hyvänä apuna esimerkiksi uutta työntekijää perehdyttäessä yrityksen tapoihin ja järjestelmiin. Lisäksi sekä vanhoja että uusia työntekijöitä varten on olemassa helpdesk-sivusto Kanada sekä laatuportaali QPR, johon on koottu yrityksen kaikki prosessikuvaukset.

Julkisista palveluista tärkeimmät ovat yrityksen www-sivut osoitteessa *www.vismasoftware.fi*, josta löytyy yritysasiakkaille helpdesk-sivustot, rekrytointiosio, tiedotteita koskien kurssitarjontaa, uutisia sekä Visma Software Oyj:n yritysesittely.

Sähköpostijärjestelmänä käytössä on Microsoft Exchange 2003, jota käytetään Microsoft Office 2003 -ohjelmiston mukana tulevalla Microsoft Outlook 2003 -ohjelmalla. Exchange Server -ohjelmisto on asennettu kahdelle palvelimelle, joista toinen sijaitsee DMZ-alueella (Demilitarized zone) ja toinen lähiverkossa.

2.2 Verkkolevyt ja muut palvelut

Kaikissa toimipisteissä on langallisen verkon lisäksi 11 megabitin nopeudella toimiva langaton verkko, jossa käytetään WEP-salausta (Wired Equivalent Privacy) ja autentikointiin sertifikaattia, joka asennetaan verkosta kaikille toimialueen päätelaitteille. Käytännössä tällä estetään langattoman verkon käyttö tehokkaasti ulkopuolisilta.

Videoneuvotteluja varten toimipisteiden välillä on käytössä Tandberg-videoneuvottelulaitteet. Jokaisesta toimipisteestä voidaan ottaa monipisteneuvottelu soittamalla virtuaaliseen konferenssiin, johon neuvottelun kaikki osapuolet soittavat. Kaikkiin videoneuvotteluihin on mahdollista osallistua myös matkapuhelimen tai muun PDA-laitteen (Personal Digital Assistant) välityksellä. Lisäksi käyttäjät voivat osallistua videoneuvotteluihin myös omalta kannettavalta tietokoneeltaan, kunhan käytössä on web-kamera.

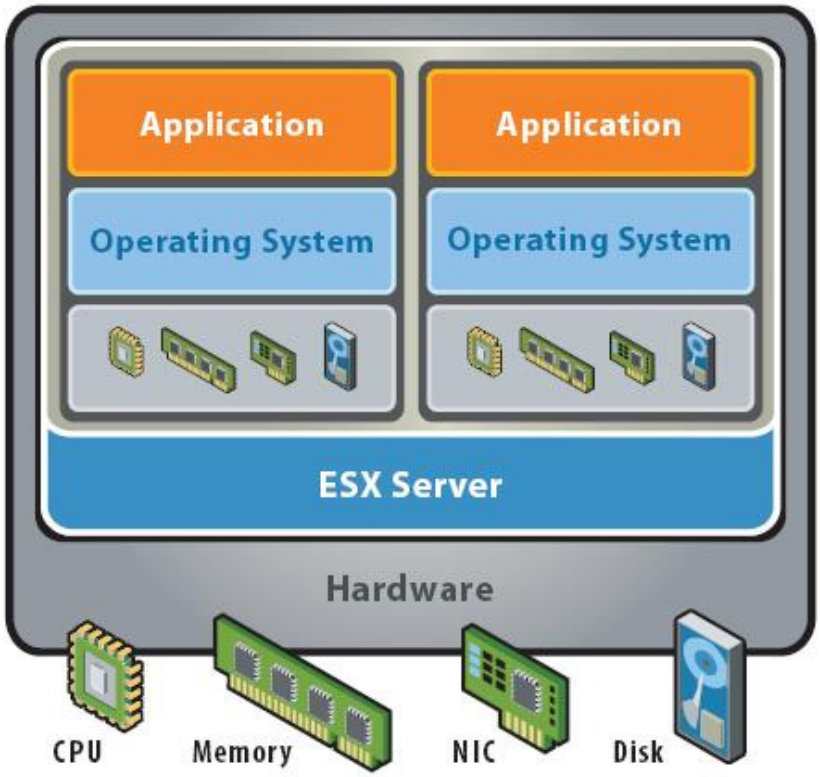
Sisäverkon palveluihin kuuluu myös kaikille käyttäjille mapattu Z-verkkolevy, jossa jokaisella osastolla on omat kansionsa. Lisäksi jokaiselle käyttäjälle on luotu oma kansio U-verkkolevylle, joka on toteutettu käyttäen Active Directory -hakemistopalvelua. Myös toimipistekohtaisesti muutamia verkkolevyjä on mapattu vain tietyn toimipisteen käyttöön.

2.3 Palvelimet

Verkon infrastruktuurissa jokaisessa toimipisteessä paitsi Oulussa on oma toimialueen ohjauskone, jotka replikoivat tietojaan keskenään verkossa tapahtuvista muutoksista. Nämä palvelimet sisältävät yhtäläisen tiedon Active Directory -hakemistopalvelusta ja kontrolloivat päätelaitteiden pääsyä verkon resursseihin. Ohjauskoneilla määritellään toimialuetta ja sen sisältämiä jäsenpalvelimia sekä muita tietokoneita koskevat käytännöt. Ohjauskoneiden lisäksi verkossa on jäsenpalvelimia, joiden roolina on toimia tiedosto-, sovellus-, tietokanta-, www- tai sertifikaattipalvelimina. Suurimmassa osassa palvelimista on käytössä Windows Server 2003 -käyttöjärjestelmä, mutta muutama vanhempi Windows 2000 sekä Windows NT 4.0 -käyttöjärjestelmää käyttävä palvelin on historiatiedon takia edelleen käytössä. Varmuuskopiot tärkeimmistä palvelimista sekä datasta otetaan nauhalle suurimmissa toimipisteissä. Lisäksi pienemmistä toimipisteistä tärkein data kopioidaan verkon yli Jyväsky-

län palvelinkeskuksen ohjauskoneille, jolloin data saadaan varmistettua myös käyttäen nauha-asemia,.

Visman verkkoinfrastruktuurissa on käytössä virtuaalipalvelimien käyttönottoon ja hallintaan tarkoitetut VMware ESX Server- sekä Microsoft Virtual Server 2005 R2 -järjestelmät. VMware ESX Server -järjestelmä asennetaan suoraan laitteistopohjaiseen palvelimeen ennen varsinaisen käyttöjärjestelmän asennusta. VMware ESX Server -järjestelmä muodostaa laitteiston komponenttien ja palvelinkäyttöjärjestelmän väliin ns. virtualisointitason, joilloin palvelimella voidaan ajaa yhtä tai useampaa samoja komponentteja käyttävää käyttöjärjestelmää yhtäaikaa (kuva 1). (VMware Inc. 2006: VMware ESX Server)



Kuva 1. Käyttöjärjestelmien virtualisointi samalla fyysisellä palvelimella. (VMware Inc. 2006: VMware ESX Server)

Järjestelmä tuo muun muassa huomattavia säästöjä laitehankintojen jäädessä pienemmiksi sekä virtuaalipalvelimien hallinnointi helpottuu. Luotuja virtuaalikoneita voidaan tarvittaessa siirtää helposti levyltä toiselle ilman että asennuksia tehtäisiin uudelleen; virtuaalikone pysäytetään ja kopioidaan haluttuun paikkaan ja käynnistetään uudestaan, jolloin se on jälleen valmis käyttöön. VMware ESX Server -järjestelmää hallitaan www-sivuston kautta. Uusien virtuaalikoneiden luonti sekä niiden ja

vanhojen virtuaalikoneiden hallinta hoidetaan tätä kautta. Uutta Citrix Access Gateway -järjestelmää varten luodaan Windows Server 2003 -käyttöjärjestelmällä varustettu virtuaalikone, johon päivitetään viimeisimmät tietoturvapäivitykset ennen Citrix Advanced Access Control -ohjelmiston asennusta. Luvusta 7 ”Citrix Advanced Access Control – asentaminen” alkaen kerrotaan järjestelmän asennuksesta lisää.

Microsoft Virtual Server 2005 R2 voidaan asentaa kaikkien yleisimpien x86 Windows-käyttöjärjestelmien päälle, jossa voidaan ajaa useita yhtäaikaisia virtuaalikoneita varustettuna Windows Server -käyttöjärjestelmillä mukaan lukien myös Windows XP Professional. Järjestelmä tukee myös 64-bittisiä käyttöjärjestelmiä perinteisten 32-bittisten lisäksi kuten VMware ESX Server -järjestelmä. Järjestelmässä käytettävät virtuaalikoneet muodostavat VHD-tiedoston (Virtual Hard Disk), jota ajetaan ja johon tallennetaan muutokset palvelimen kovalevyltä. Virtuaalipalvelimien konfiguraatiot tallentuvat puolestaan VMC-tiedostoon (Virtual Machine Configuration). Visma Software Oyj:n sisäverkossa kaikki tuotanto- ja testikäytössä olevat virtuaalikoneet sijaitsevat neljällä eri palvelimella. Virtual Server 2005 R2 -ohjelmiston asennuksen yhteydessä asennetaan virtuaalipalvelimien luontiin ja hallintaan suunniteltu komponentti, jota käytetään www-sivuston kautta.

Jokaisessa toimipisteessä Oulua lukuun ottamatta on käytössä laitteistopohjaisia palvelimia eli vähintään toimialueen ohjauskone sekä erillinen tiedostopalvelin. Laitteistona suurimmassa osassa palvelimia on perinteiset räkkimalliratkaisut sekä yksittäisiä pöytäkone-tyyppisiä ratkaisuja. Tärkein ja monipuolisin vikasietoisuuden sekä hallittavuuden kannalta oleva palvelinjärjestelmäratkaisu Jyväskylän palvelinkeskuksessa on kuitenkin HP Blade System, jossa käytetään SAN-tiedostojärjestelmää (Storage Area Network) erillisten kuitukorttiohjaimien avulla.

2.4 Tietoturva

Tietoturvaan Visma Software Oyj:n verkkoinfrastruktuurissa on panostettu paljon. Koko tietoverkko toimii TDC Songin IP VPN -verkon päällä, ulko- ja sisäverkon välissä on laitteistopohjainen palomuuri sekä kaikissa verkon päätelaitteissa etähallittava virustorjunta- ja palomuuriohjelmisto. Palomuuriratkaisu on toteutettu laitteistopohjaisesti ulkoverkon ja DMZ-alueen sekä DMZ-alueen ja sisäverkon välillä. Julkiset palvelimet kuten posti- ja www-palvelin on esimerkiksi sijoitettu DMZ-alueelle, johon yhteydet toimivat sekä ulko- että sisäverkosta, mutta yhteydet

DMZ-alueelta vain ulkoverkkoon. Tosiasiassa vaikka kräkkeri pääsisikin murtautumaan palomuurin läpi jollekin julkiselle palvelimelle, estäisi palomuuri DMZ-alueen ja sisäverkon välillä murtautumisyrityksen. Tätä opinnäytetyötä kirjoittaessani olemme ottamassa piakkoin käyttöön IPS-laitteen (Intrusion Prevention System), jolla voidaan estää ja tarkkailla verkon liikennettä sekä mahdollisesti luvattomasti verkkoon lisättyjen ohjelmistojen tai palvelimien lisäämistä.

2.5 Active Directory -hakemistopalvelu

Active Directory on hakemistopalvelu, johon tallennetaan tietoa verkkoresursseista koko toimialueella. Active Directory -hakemistopalvelussa käytetään LDAP-verkkoprotokollaa (Lightweight Directory Access Protocol), jolla voidaan hakea tietoa hakemistopalveluista sekä modifioida haettua tietoa. Active Directory -hakemistopalvelun avulla voidaan asettaa koko toimialueen kattavia käytäntöjä, jaella ja asentaa ohjelmia ja tärkeitä päivityksiä hallitusti ja keskitetysti. Active Directory koostuu puuhierarkiasta eri objekteineen, joita sijoitetaan organisaatioyksiköihin. Näihin lukeutuvat muun muassa resurssit, käyttäjät ja palvelut. Organisaatioyksiköihin taas voidaan vaikuttaa ryhmäkäytännöillä.

Fyysisesti Active Directory -hakemistopalvelun sisältämä tieto on toimialueen ohjauskoneilla, jotka replikoivat tietoa keskenään käyttäen RPC-protokollaa (Remote Procedure Call). Poiketen aiemmista Windows-versioista, joissa käytettiin NetBIOS:ia kommunikointiin, Windows 2000 ja 2003 Server -käyttöjärjestelmissä Active Directory on täysin integroitu DNS-nimipalvelun (Domain Name System) kanssa.

Ohjauskoneella on käytössä DFS-järjestelmä (Distributed File System) eli keskitetty tiedostojen jakelujärjestelmä, jolla voidaan jaella yhdestä keskitetystä paikasta muille toimipisteiden ohjauskoneille tai jäsenpalvelimille polku, josta tiedostot löytyvät. Visma Software Oyj:n tietojärjestelmässä kaikki tarvittavat tiedostojaot on koottu Z-verkkolevyn alle, joka näkyy jokaisessa toimipisteessä samankaltaisena.

Tärkeimmät ryhmäkäytäntömääritykset tulevat Default Domain Policy -ryhmäkäytäntöobjektista, jolla asetetaan muun muassa salasana- ja käyttäjätilikäytännöt, sertifikaatit sekä Windows-päivitysten haku ja asentaminen päätelaitteille. Käyttäjäasetuksiin vaikuttavat määritykset ovat esimerkiksi salasanasuojattu näytönsäästäjä sekä kielletyt tiedostojenvaihto-ohjelmat.

Päätelaitteisiin kohdistetaan myös muita ryhmäkäytäntöjä, joilla tuodaan käyttäjille oikeuksia tärkeimpien asennettujen ohjelmistojen asennuskansioihin sekä rekisteriin. Lisäksi Windows-palomuuriin on lisätty säännöt etätyöpöytäyhteydestä, ICMP-protokollasta (Internet Control Message Protocol) sekä sallituista porttien ja ohjelmien poikkeuksista. Ryhmäkäytännöllä tuodaan määritykset uusille asennettaville koneille tietyissä organisaatioyksiköissä. Näissä organisaatioyksikössä asennetaan lisäksi tarvittavat ohjelmat verkosta kuten Citrix MetaFrame Presentation Server -asiakasohjelmisto sekä Citrix Endpoint Analysis -asiakasohjelmisto, josta kerrotaan tarkemmin luvun 9 ”Advanced Access Control – konfigurointi ” yhteydessä. Organisaatioyksiköiden sisällä päätelaitteet jaetaan kolmeen kategoriaan, joihin jokaiseen vaikuttaa eri ryhmäkäytäntö. Users-haarassa käyttäjille pakotetaan päätelaitteelleensa vain peruskäyttäjän oikeudet, mutta Powerusers-haarassa määrittyy tehokäyttäjän oikeudet. Admin-ryhmään sijoitetaan koneet, joissa käyttäjillä on oltava järjestelmänvalvojan oikeudet päätelaitteellensa.

Koko toimialueen ohjauskoneita koskeviin ryhmäkäytäntöihin on määritelty oikeudet toimialueen järjestelmänvalvojille, palvelimien paikallisille järjestelmänvalvojille sekä palvelimien hallintaryhmän jäsenille. Toimialueen järjestelmänvalvojilla on oikeudet toimialueen kaikkiin päätelaitteisiin sekä palvelimiin.

2.6 Citrix MetaFrame Presentation Server 4.0 -järjestelmä

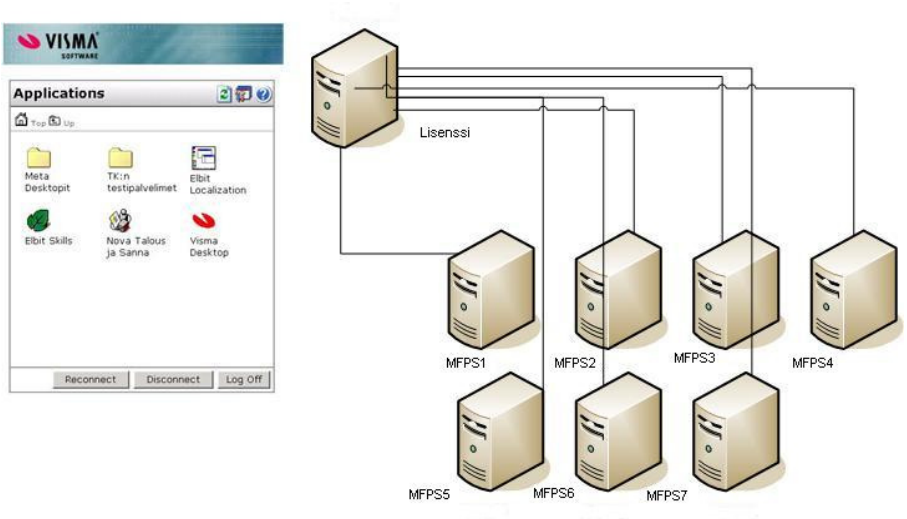
Citrix MetaFrame Presentation Server -ympäristö mahdollistaa ohjelmistojen tarjoamisen käyttäjille tietoturvallisesti ja keskeytyksettä lähes minkä tahansa verkkoyhteyden yli kuten julkisen internetin, lähiverkkoyhteyden tai puhelinverkkoyhteyden yli. Järjestelmä on käyttöjärjestelmistä riippumaton, joten käyttäjän päätelaitteessa voi olla Windows, Linux tai Unix-pohjainen käyttöjärjestelmä ja myös kannettavilla PDA-laitteilla järjestelmän käyttö on mahdollista. Citrix MetaFrame Presentation Server -järjestelmä on skaalautuva ja julkaistut sovellukset ovat aina käyttäjien saatavilla. Palvelimia voidaan yhdistää palvelinfarmiksi, joista kaikkia hallitaan kuin yhtä ainutta palvelinta. (Getting Started with MetaFrame Presentation Server 2005: 14)

Järjestelmä mahdollistaa usean käyttäjän yhtäaikaisen istunnon, joista jokainen on erillinen ja turvattu istunto yhdellä tai useammalla palvelimella. Järjestelmään voidaan asentaa lähes mikä tahansa ohjelmisto, kuten toimisto-ohjelmistot, jotka sitten julkaistaan käyttäjille ilman, että niitä olisi asennettava jokaiselle

käyttäjälle erikseen. Julkaistuihin ohjelmistoihin käyttäjät pääsevät käsiksi Web Inteface -sivuston kautta, jossa ohjelmistojen kuvakkeet ovat käytettävissä. Kuvaketta klikkaamalla aukeaa yhteys Citrix-etätyöpöydälle, jossa itse ohjelmisto käynnistyy ja ajetaan kokonaisuudessaan. (Getting Started with MetaFrame Presentation Server 2005:15)

Yhteyttä varten käyttäjät tarvitsevat Citrix MetaFrame Presentation Server -asiakasohjelmiston. Asiakasohjelmistossa käytetään ICA-protokollaa (Independent Computing Architecture) tietojen välittämiseen päätelaitteelta julkaistuihin resursseihin palvelimelle. ICA-protokolla hoitaa käyttäjän näppäimistön ja hiiren painallukset sekä ruudunpäivitykset palvelimen ja käyttäjän päätelaitteen välillä, joten sovellus näyttää käyttäjän näkökulmasta ajettavan paikallisesti, tosiasiassa siis kokonaan palvelimella. (Getting Started with MetaFrame Presentation Server 2005:16)

Citrix MetaFrame Presentation Server -järjestelmän palvelimina Jyväskylän palvelinkeskuksessa toimii kahdeksan palvelinta, joista yksi toimii farmin kantapalvelimena ja loput seitsemän toimivat Citrix MetaFrame Presentation Server -ympäristön farmipalvelimina (kuva 2). Lisenssipalvelu on asennettu lisenssipalvelimelle, johon on myös asennettu Web Interface -käyttöliittymä julkaistujen sovelluksien käynnistämistä varten. Verkkoyhteydet Web Interface -käyttöliittymästä palvelinfarmiin päin on toteutettu käyttäen https-protokollaa (Secured Hyper Text Transfer Protocol). Web Interface -käyttöliittymä on julkaistu myös Vintra-intranetin etusivulla sekä ryhmäkäytännöillä myös Internet Explorer -selaimen suosikeissa kaikille käyttäjille.



Kuva 2. Citrix MetaFrame Presentation Server -infrastruktuuri

Citrix MetaFrame Presentation Server -ympäristö päivitettiin jo ennen tämän opinnäytetyön kirjoittamista versiosta 3.0 uuteen 4.0-versioon käyttäen apuna Citrix MetaFrame Presentation Server Administrator´s Guide -opusta. Päivitys tehtiin silmällä pitäen uutta Citrix Access Gateway -järjestelmää sekä toi mukanaan lisäksi joukon bugikorjauksia sekä uusia ominaisuuksia. Tässä opinnäytetyössä ei käydä läpi versiopäivitykseen ja ympäristön ominaisuuksiin liittyviä asioita. Sen sijaan ympäristön käyttöön tarvittavien Citrix MetaFrame Presentation Server -asiakasohjelmistojen sekä niiden konfigurointia käyn läpi pintapuolisesti seuraavassa luvussa.

2.7 Citrix MetaFrame Presentation Server -asiakasohjelmiston konfigurointi

Citrix MetaFrame Presentation Server -ympäristössä julkaistujen ohjelmistojen käyttöön tarvittava Citrix MetaFrame Presentation Server -asiakasohjelmisto on jaeltu ja asennettu käyttäjien päätelaitteille käyttäen Active Directory -hakemistopalvelun ohjelmistonasennus-politiikkaa ryhmäkäytäntöjen avulla. Asiakasohjelmistosta tähän tarkoitukseen riittää ohjelmiston msi-paketti (Microsoft Windows Installer), joka asentuu käyttäjien päätelaitteelle seuraavan uudelleenkäynnistymisen yhteydessä. Visma Software Oyj:n sisäverkossa jaeltavaa Citrix MetaFrame Presentation Server -asiakasohjelmistoa on muokattu omia tarpeitamme vastaavaksi käyttäen Windows-käyttöjärjestelmissä sisäänrakennettua msiexec-ohjelmaa. Sillä voidaan periaatteessa muokata kaikkia eri ohjelmistojen msi-paketteja, jotka muokkauksen jälkeen sisältävät halutun asennusskenaarion. Citrix on juuri tätä muokkausmahdollisuutta varten julkaissut Citrix MetaFrame Presentation Server Client Package -ohjelmiston, joka sisältää Program Neighborhood -komponentin, Program Neighborhood Agent -agentin sekä Citrix MetaFrame Presentation Server -asiakasohjelman.

Normaalisti käyttäjät käyttävät Citrix MetaFrame Presentation Server -ympäristön julkaistuja sovelluksia Web Interface -käyttöliittymän avulla internetsivuston kautta päätelaitteen selaimella. Muokattujen Citrix MetaFrame Presentation Server Client Package -ohjelmistokokonaisuuden avulla käyttäjille voidaan tuoda julkaistut sovellukset suoraan päätelaitteen työpöydälle ja käynnistä-valikkoon. Siten julkaistujen sovelluksien käyttö helpottuu entisestään.

Asiakasohjelmistoa muokataan antamalla paikallisen järjestelmänvalvojan oikeuksilla komentokehotteessa komento msiexec /a ica32pkg.msi, jolloin asennusvelho käynnistyy. Asennusvelhon aikana valitaan Citrix MetaFrame Presentation Server -asiakasohjelmisto sekä Program Neighborhood ja Program Neighborhood Agent -ohjelmistot ja niiden määritykset. Kun asennusvelho on valmis, tehdään vielä tarvittavat muutokset appsrv.ini, pn.ini sekä wfclient.ini-tiedostoihin, jotta Citrix MetaFrame Presentation Server -ympäristön julkaistuja sovelluksia voidaan käyttää suoraan työpöydältä (Saunders 2005 & Harwood 2002). Appsrv.ini-tiedostossa määritellään käytettävät sovelluspalvelimet Citrix MetaFrame Presentation Server -ympäristössä sekä muut käyttäjäkohtaiset asetukset (Citrix System Inc 2005: Appsrv.ini Parameters Deciphered). Pn.ini-tiedosto sisältää Program Neigborhood -ohjelmiston asetukset, joissa määritellään käytettävät palvelinfarmit ja niissä sijaitsevat ohjelmistokokonaisuudet (Citrix Systems Inc. 2005: Pn.ini Parameters Deciphered). Wfclient.ini-tiedostossa määritellään Ica Client -ohjelmiston käynnistämistä koskevat asetukset. Tähän tiedostoon ei tehdä muutoksia.

Kun käyttäjä asentaa edellä muokatun asiakasohjelmiston päätelaitteelleen, niin käyttäjän tarvitsee aukaista vain kerran työpöydältä löytyvä Citrix Program Neighborhood -kuvake ja antaa Windows-verkon käyttäjätunnus ja salasana, jolloin ohjelmisto ottaa yhteyttä Citrix MetaFrame Presentation Server -palvelinfarmiin. Yhteyden muodostuttua käyttäjän päätelaitteen työpöydälle ja käynnistä-valikkoon ilmestyvät kaikki käyttäjälle määritellyt sovellukset, joita voidaan alkaa saman tien käyttämään.

3 VPN-verkkoprotokollat

VPN on lyhenne sanoista Virtual Private Network, jolla tarkoitetaan virtuaalista yksityisverkkoa. Määritelmänsä mukaisesti VPN:llä voidaan luoda joko laitteisto- tai ohjelmistototeutuksena tehtävä ratkaisu, jolla organisaation sisäverkko ulotetaan turvallisesti turvattoman julkisen verkon, esimerkiksi Internetin yli.

VPN-tekniikalla voidaan yhdistää joko kaksi tai useampia sisäverkkoja keskenään tai yksittäinen verkon aktiivilaite, esimerkiksi etätyöntekijän tai yhteistyökumppanin työasema organisaation verkkoon. VPN:ssä kaikki siirrettävä data suojataan salauksella, joka estää internetin yli välitettävän liikenteen sisällön näkymästä kolmansille osapuolille. Liikenteen salaamisen lisäksi VPN-ratkaisuissa liikennöivät osapuolet todennetaan ennen yhteyden muodostamista.

Käytännössä VPN-yhteys muodostetaan tunneloimalla kaikki liikenne jonkin liikenteen salaavan protokollan sisään. Yleisesti käytössä olevia VPN-protokollia ovat PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IPSec sekä suosiotaan viime vuosina reippaasti kasvattanut SSL VPN. VPN-tekniikoilla voidaan suojata kaikki turvattoman verkon yli VPN-tunnelissa lähetettävä liikenne, eikä suojaus tällöin ole riippuvainen sovellustason protokollista.

3.1 Point-to-Point Tunneling Protocol

PPTP-protokollan on kehittänyt Microsoft yhdessä useiden teknologia-yhtiöiden kanssa. Se on eniten tuettu VPN-yhteysprotokolla Windows-käyttäjien joukossa ja on samalla ainut VPN-yhteysprotokolla, joka on tuettu Windows 98 ja NT-käyttökärjestelmissä. PPTP-protokolla on itse asiassa PPP-protokollan (Point-to-Point Protocol) laajennus, joka toimii OSI (Open Systems Interconnection)-mallin siirtoyhteyskerroksella välittäen IP-paketteja (Internet Protocol) sarjalinkkien yli. PPTP-protokollassa käytetään muun muassa PAP- (Password Authentication Protocol), CHAP- (Challenge Handshake Authentication Protocol), MS-CHAP- (Microsoft Challenge Handshake Authentication Protocol) ja EAP-tunnistusprotokollia (Extensible Authentication Protocol) autentikointiin VPN-yhteyksissä. (Shinder 2005)

Koska PPTP-protokolla muodostaa tunnelin osapuolien välille ja ei sisällä sellaisenaan salausta, varminta on käyttää sitä yhdessä Microsoft Point-to-Point Encryption -protokollan (MPPE) kanssa, jotta tietoturvallinen VPN-tunneli saadaan muodostettua. PPTP-yhteyksiä varten tehdyt palvelimet voidaan ottaa helposti käyttöön, koska tarvittava asiakasohjelmisto on valmiiksi asennettuna useimpiin Windows-käyttöjärjestelmiin ja jota useat laite- ja ohjelmistopohjaiset palomuuriratkaisut myös tukevat. (Shinder 2005)

3.2 Layer 2 Tunneling Protocol (Shinder 2005)

L2TP-protokollan ovat kehittäneet Microsoft ja Cisco yhteistyössä yhdistämällä PPTP:n ja Ciscon oman L2F-protokollan (Layer 2 Forwarding). L2TP-protokollaa voidaan käyttää IP-verkkojen lisäksi Frame Relay-, ATM- ja X.25-verkoissa. L2TP-protokolla on PPTP:n tavoin tuettu useiden palomuuriratkaisujen valmistajien kanssa kuten ISA Server, Checkpoint ja Watch Guard.

L2TP-protokolla on valmiiksi sisäänrakennettu Windows 2000, XP ja 2003 Server -käyttöjärjestelmiin, mutta asiakasohjelmisto voidaan asentaa myös muihin vanhempiin Windows-käyttöjärjestelmiin.

Dataliikenteen salaukseen käytetään ESP:tä (Encapsulating Security Payload). L2TP:ssä käytetään digitaalisia sertifikaatteja käyttäjän ja päätelaitteen tunnistukseen. PPTP:ssä ainoastaan tunnelin yli liikkuva data voidaan salata, mutta sen aitoutta ei voida taata, toisin kuin L2TP:ssä, jossa datan täytyy pysyä muuttumattomana yhteyden yli. Lisäksi datan lähettäjä varmistetaan aina. Myös palvelimelle kaapattujen ja samalla uudelleen lähetettyjen käyttäjätunnuksien suoja estää hakkerilta niiden käytön.

3.3 Internet Protocol Security

IPSec VPN -yhteysprotokollaa voidaan käyttää erillään L2TP:stä yhdistämään kahden toimipisteen lähiverkot OSI-mallin verkkoyhteyskerroksella. Useiden suurten teknologiayritysten laitteistopohjaiset VPN-ratkaisut, kuten Ciscon PIX -palomuurit, tukevat IPSec VPN:ää. IPSec VPN toimii ainoastaan IP-verkoissa ja suojaa paketit, jotka siirretään kahden yh-

dyskäytävän välillä, joissa on oltava VPN-asiakasohjelmisto asennettuna.

Autentikointiin käytetään IKE-prokollaa (Internet Key Exchange), jossa on käytössä joko ennalta jaettu avain tai tietoturvallisempi digitaalinen sertifikaatti. IPSec VPN suojaa useimmilta yleisiltä hyökkäyksiltä kuten ”man-in-the-middle”- ja palvelunestohyökkäyksiltä. Monien laitevalmistajien IPSec VPN-asiakasohjelmistoihin voidaan konfiguroida politiikkoja, joilla varmistetaan, että VPN-yhteyttä muodostavassa päätelaitteessa on esimerkiksi palomuuri- tai virustorjuntaohjelmisto asennettuna ennen kuin yhteys sallitaan. IPSec VPN toimii Windows-pohjaisista käyttöjärjestelmistä Windows 2000, XP ja 2003 Server -käyttöjärjestelmissä, mutta ei vanhemmissa Windows 95, 98 tai ME -käyttöjärjestelmissä. (Shinder 2005)

3.4 Secure Sockets Layer

Perinteisen SSL VPN -protokollan etuna muihin VPN-yhteysprotokolliin on, että päätelaitteilla ei välttämättä tarvita erillistä VPN-yhteysohjelmistoa, koska VPN-yhteyden muodostamiseen käytetään internet-selainta kuten Internet Explorer. Toisaalta tämä tarkoittaa sitä, että verkkoprotokollien käyttö SSL VPN:ssä on muita VPN-protokollia rajoittuneempaa. Mutta toisaalta taas voidaan puhua turvallisuuden paranemisesta, sillä SSL VPN:llä voidaan rajoittaa pääsy vain tiettyihin ohjelmistoihin kun taas IPSec VPN:llä on pääsy koko organisaation verkkoon. Jos ohjelmistoja ei voida käyttää selaimen avulla suoraan, tarvitaan lisäksi erityisiä Java-appletteja tai ActiveX-komponentteja, joilla selain saadaan käyttämään ohjelmistoja. Tämä taas vaatii sen, että selaimessa on sallittu aktiivisten sisältöjen suorittaminen. Toisaalta tämä mahdollistaa haitallisten ohjelmakoodien suorittamisen päätelaitteella, varsinkin jos sallitaan allekirjoittamattomien sisältöjen ajaminen. Lisäksi on varmistettava, että selaimeen asennettavat lisäosat ovat digitaalisesti allekirjoitettuja. (Shinder 2005)

SSL VPN käyttää liikennöintiin porttia 443 ja sillä suojataan tavallinen http-liikenne (Hyper Text Transfer Protocol) portissa 80, joka suojattuna huomataan https-protokollasta (Secured Hyper Text Transfer Protocol) (Steinberg & Speed 2005:3). Salauksen lisäksi lähetettävästä datasta muodostetaan MD5-tiiviste (Message Digest), jolla varmistetaan, että sen sisältö ei muutu yhden päätelaitteen lähettäessä sen ja toisen vastaanottaessa sen (Steinberg & Speed 2005:6).

SSL VPN:n yhteyden muodostus toimii OSI-mallin istuntokerroksella, joten se mahdollistaa verkkoon pääsyn rajoittamisen huomattavasti joustavammin kuin esimerkiksi IPSec VPN. Data kapseloidaan OSI-mallin esitystapa- ja sovelluskerroksilla. Joissakin SSL VPN -ratkaisuissa on mahdollista myös tunneloida jopa verkkokerroksella liikkuvaa tietoa (Steinberg & Speed 2005:15). Myös SSL VPN:ssä käytetään digitaalisia sertifikaatteja palvelinautentikointiin. Kuten IPSec VPN:ssä, myös SSL VPN:ssä on mahdollista tarkistaa päätelaitteen virus- ja palomuuriohjelmistot ennen VPN-yhteyden muodostamista erityisten applettien avulla. (Shinder 2005)

VPN-yhteyden luottamuksellisuus sekä lähetettävän datan aitous varmistetaan salaamalla se monimutkaisella algoritmillä, jonka oletettavasti vain kumpikin VPN-yhteyden osapuolista ymmärtää. Salauksessa käytetään joko symmetristä tai asymmentristä salausta, joista symmetristä algoritmiä käytetään salaamaan koko yhteys SSL-istunnon sisällä kun taas asymmetristä algoritmia käytetään jakamaan symmetrinen yhteysavain turvallisesti käyttäjän ja SSL VPN:n välillä. Symmetrisessä algoritmissa samaa avainta käytetään sekä datan salaamiseen että sen purkamiseen, kun asymmetrisessä algoritmissa käytetään avainpareja: julkinen ja salainen avain. Lähetettävä data salataan vastaanottajan julkisella avaimella, jonka vastaanottaja voi avata vain omalla salaisella avaimellaan. (Steinberg & Speed 2005:7-8)

SSL-protokollaa käyttävillä internet-sivustoilla käytetään sertifikaatteja varmistamaan sivuston aitous käyttäjille. Sertifikaatti on aitoustodistus, joka kertoo, että yhteys on todella otettu esimerkiksi tiettyyn www-palvelimeen johon alun perin yritettiin ottaa yhteys. Sertifikaatit allekirjoittaa digitaalisesti jokin luotettava taho eli ns. kolmas osapuoli (Certificate Authority, CA), joka varmistaa, että sertifikaatin haltija todella on se, joka hän sanoo olevansa.

4 Citrix Access Gateway ja SafeWord-järjestelmät

Citrix Access Gateway on SSL VPN -verkkoprotokollaan perustuva laitteistopohjainen VPN-järjestelmä, jolla käyttäjille voidaan tarjota tietoturvallinen pääsy verkon resursseihin yhden pisteen kautta. Järjestelmässä yhdistyvät sekä IPSec- että SSL VPN -protokollien parhaat ominaisuudet ilman monimutkaista ja kallista implementointia ja hallintaa. Se tukee kaikkia ohjelmistoja ja protokollia minkä tahansa palomuurin läpi (Access Gateway Administrator´s guide 2005:15), kuten VoIP-protokollaa (Voice over IP). Järjestelmän laitteistossa on Linux-käyttöjärjestelmä, joka pyörii Intelin P4-prosessorin ja 1 gigabitin muistin avustuksella. Laitteisto tukee 2000 yhtäaikaista käyttäjää. Informaation ja datan suojaamiseen käytetään SSL- ja TLS-salausta (Transport Layer Security). Järjestelmä voidaan liittää saumattomasti olemassa olevaan Citrix MetaFrame Presentation Server -järjestelmään (Getting started with Access Gateway 2005:9).

Järjestelmän käyttöönotto sekä ylläpito on nopeaa, helppoa ja kustannustehokasta, mikä tulee tarkemmin esille tämän opinnäytetyön tulevissa kappaleissa. Käyttäjien kannalta Citrix Access Gateway -järjestelmän käyttö vaikuttaa työpöytämäiseltä ja ns. ”aina-päällä”-yhteydeltä. Järjestelmässä on sisäänrakennettu internet-matojen torjumiseen tarkoitettu asiakasohjelmisto sekä päätelaitteen skannauksen mahdollistava komponentti (Access Gateway Administrator´s guide 2005:15).

4.1 Citrix Advanced Access Control -ohjelmisto

Järjestelmä tarjoaa etäkäyttäjille saumattoman ja tietoturvallisen pääsyn yrityksen tietoverkon sovelluksiin ja muihin verkkoresursseihin kuten verkkolevyille, intranetiin sekä sähköpostijärjestelmään aivan samoin kuin jos käyttäjä työskentelisi sisäverkossa toimistolla. Tämän mahdollistaa Citrix Access Gateway -järjestelmään integroitava Citrix Advanced Access Control -ohjelmisto, josta kerron tarkemmin myöhemmin tässä luvussa. Lisäksi järjestelmää on mahdollista käyttää myös ns. Kiosk Mode -tilassa, jossa järjestelmään muodostetaan osittainen VPN-tunneli julkiselta tietokoneelta (Access Gateway Administrator´s guide 2005:15). Kiosk Mode -tilassa Citrix Access Gateway -järjestelmä lähettää ainoastaan kuvaa yhteyden yli eikä lainkaan dataa. Tällä estetään väliaikaisten tiedostojen sekä selaimen keksien jääminen julkisen tietokoneen levylle; yhteyden aikana niitä käytetään suoraan Citrix Access Gateway -

järjestelmän sisällä (Access Gateway Administrator´s guide 2005:28).

Citrix Advanced Access Control -ohjelmiston avulla järjestelmänvalvojat voi kontrolloida erilaisiin resursseihin pääsyä kuten sovellukset, tiedostot, www-sisältö, sähköpostin liitetiedostot sekä tulostaminen huomattavasti tarkemmin kuin jos käytettäisiin pelkkää Citrix Access Gateway -järjestelmää ilman sitä. Citrix Advanced Access Control -ohjelmisto antaa samalla mahdollisuuden kontrolloida pääsyä näihin resursseihin sekä mitä niille voidaan tehdä perustuen käyttäjän rooliin, paikkaan, päätelaitteen tyyppiin sekä yhteyteen.

Citrix Advanced Access Control -ohjelmisto koostuu kolmesta komponenttikokonaisuudesta, joita ovat SmartAccess, SmoothRoaming ja Secure by Design.

SmartAccess-komponentin avulla analysoidaan pääsyskenaario ja sen perusteella sallitaan tietyntasoinen pääsy resursseihin vaarantamatta tietoturvallisuutta. SmartAccess toimii käyttäen kahta vaihetta, joista ”tieto” (sense) analysoi käyttäjän pääsyskenaarion ja ”vastaus” (respond) sallii tietyntasoisen pääsyn resursseihin. Koska käyttäjän pääsyä resursseihin ja toimenpiteitä niissä voidaan hyvinkin tarkasti kontrolloida, ei käytetä pelkkiä ”sallittu” tai ”kielletty” -vastauksia käyttäjien yhteysyrityksiin. (Citrix Access Gateway with Advanced Access Control Administrator´s Guide 2005:11)

Tämä käy hyvin ilmi esimerkistä, jossa tietty käyttäjä kirjautuu Citrix Access Gateway -järjestelmään lentoaseman internetkioski-päätteestä, jolloin käyttäjän sallitaan vaikkapa vain katsoa ja lukea sähköpostin liitetiedostoja, mutta niiden lataaminen, editoiminen tai printtaaminen ei ole sallittua. Samalle käyttäjälle voidaan kuitenkin sallia täydet oikeudet resursseihin, kun hän kirjautuu järjestelmään kotoaan käsin yrityksen päätelaitteella. (Citrix Access Gateway with Advanced Access Control Administrator´s Guide 2005:11)

SmoothRoaming-komponetilla tarkoitetaan tietyntasoisen pääsyn automaattista käyttöönottoa, kun käyttäjät liikkuvat paikasta toiseen käyttäen erityyppisiä päätelaitteita erilaisissa verkoissa (Citrix Access Gateway with Advanced Access Control Administrator´s Guide 2005:11)
Secure by Design -komponentilla tarkoitetaan koko järjestelmään pääsyn-mallia, jossa sekä yrityksen data että verkon koskemattomuus säilyvät muuttumattomina. (Citrix Access Gate-

way with Advanced Access Control Administrator´s Guide 2005:12)

Nämä aiemmin luetellut komponentit muodostavat yhdessä kokonaisuuden, joka huolehtii käyttäjien päätelaitteiden jatkuvasta skannauksesta yhteyden muodostamisen ja itse yhteyden aikana, jotta se vastaa määriteltyä turvallisuustasoa. Komponentit vastaavat VPN-yhteydestä, jossa muodostetaan suora SSL VPN -tunneli verkkoresurssien avulla yrityksen lähiverkkoon ja sen palvelimille, palveluihin ja verkkoihin. Komponenttien avulla järjestelmänvalvojat voi määrittää politiikkoja, joissa voidaan sallia tai kieltää käyttäjältä jokin toimenpide koskien esimerkiksi tiettyjä tiedostoja. Vain selainpohjainen yhteys mahdollistaa järjestelmään pääsyn kannettavista PDA-laitteista, joissa ei voida käyttää asiakasohjelmistoa yhteyden muodostamiseen. Tietoturvallinen pääsy yrityksen sähköpostijärjestelmään on mahdollista selainpohjaisen käyttöliittymän avulla. Järjestelmän käyttöliittymä sekä hallinnointityökalut tukevat englannin kielen lisäksi mm. japania, saksaa, espanjaa sekä ranskaa. Uusista ominaisuuksista vanhempaan Citrix Access Gateway 4.0 -järjestelmään nähden on tullut autentikointijärjestelmiin liittyen tuki LDAP-protokollalle, jota käytetään muun muassa Microsoftin Active Directory -hakemistopalvelussa (Citrix Access Gateway with Advanced Access Control Administrator´s Guide 2005:12)

4.2 SafeWord for Citrix -autentikointijärjestelmä

SafeWord for Citrix on useisiin Citrix-ympäristöihin tarkoitettu autentikointiratkaisu, jolla käyttäjät voidaan tunnistaa heidän kirjautuessaan esimerkiksi Citrix Access Gateway -järjestelmään. Siten SafeWord for Citrix -järjestelmällä voidaan suojata yritysten Citrix- ja VPN-järjestelmät vahvemmalla autentikoinnilla tavanomaisen salasanalla kirjautumisen sijaan. (Secure Computing Inc. Business case solutions brief 2007:5)

Järjestelmässä käytetään SafeWord-toukkaa, josta käyttäjät saavat ennen jokaista kirjautumista Citrix Access Gateway -järjestelmään uuden vaihtuvan salasanan. Avaimenperän kokoista laitetta – jossa on näyttö ja yksi näppäin salasanan generoimista varten – nimitetään toukaksi sen englanninkielisen sanan ”token” takia, josta suomen kieleen on muotoutunut toukkasana. Salasana koostuu sekä numeroista että kirjaimista, joka muodostetaan käyttäen jokaiselle toukalle ainutlaatuista algoritmia. Autentikoinnista vastaavassa palvelimessa on tieto jokaisesta tietylle käyttäjille konfiguroidusta toukasta, jolloin autentikointipalvelin käyttää täysin samaa algoritmia laskiessaan

toukasta saatavaa salasanaa ja sen perusteella sallii tai kieltää käyttäjältä pääsyn resursseihin. Jokainen kerran käytetty salasana on sen käytön jälkeen tarpeeton, joten niiden varastaminen ja käyttö uudelleen on rikollisissa tarkoituksissa hyödytöntä, sillä autentikointipalvelin hävittää jokaisen käytetyn salasanan. (Secure Computing Inc. App note 2007:3)

Koska Citrix Access Gateway -järjestelmän avulla etäkäyttäjät voi muodostaa tietoturvallisen ja salatun SSL VPN -yhteyden yrityksen tietoverkkoon, on tähän tunneliin pääsy myös suojattava kunnolla. Tavallisten käyttäjätunnusten ja salasanojen avulla tunneli on heikosti suojattu, sillä tutkimusten mukaan kolmesta neljään prosenttia käyttäjistä valitsee erittäin heikon salasanan, joka on joko sama kuin oma käyttäjätunnus, sana ”salasana” tai käyttäjän etunimi. Lisäksi kaksi prosenttia käyttäjistä valitsee salasanakseen jonkun turhamaisen sanan kuten ”madonna” tai helposti arvattavan kuten ”kullannuppu” tai vastaavan. Jopa 35 % ihmisistä valitsee salasanan, joka jollain tavalla liittyy heidän työympäristöön. Näihin kuuluvat muun muassa oman lapsen tai avopuolison valokuvat, joita saattaa löytyä henkilön työpisteen pöydältä. Tällaisen henkilökohtaisen tiedon saattaa älykäs hyökkääjä onkia käyttäjältä vaikka rupatellessa hississä tämän kanssa. (Secure Computing Inc. Business case solutions brief 2007:3)

Niinpä monien yritysten sisällä IT-osaston toimesta on otettu käyttöön monimutkaisten salasanojen käytäntöjä, joissa salasanojen on oltava tietyn pituisia, salasana on vaihdettava vähintään kuukauden välein ja 15:ta viimeisintä salasanaa ei voida käyttää uudestaan. Lisäksi salasanan on sisällettävä sekä isoja että pieniä kirjaimia, numeroita sekä symboleja. Tämä johtaa väistämättä siihen, että ensinnäkin käyttäjät unohtavat salasanansa helposti, mikä aiheuttaa IT-osastolle turhaa työtä sekä toiseksi turvallisuusriski saattaa kasvaa, sillä käyttäjät kirjoittavat monimutkaisen salasanan paperilapulle ja sijoittavat sen jonnekin työpisteensä näytön alle helposti löydettäväksi. Vahva salasanapolitiikka ei siis suojele ketjun heikointa lenkkiä eli loppukäyttäjää vastaan. (Secure Computing Inc. Business case solutions brief 2007:3)

Brittiläisen tutkimuksen mukaan suuri osa toimiston työntekijöistä kertoisi salasanansa työkaverille, ja uskomatonta mutta totta, kaksi kolmesta myös tutkimuksen haastattelijalle. Englantilaisessa tutkimuksessa todettiin yli 90 % ihmisistä paljastavan salasanansa saadakseen ilmaisen kynän palkinnoksi. On siis enemmän kuin perusteltua suojata Citrix-järjestelmät yrityksen sisäverkossa lisäturvaa antavalla autentikointijärjestelmällä ku-

ten SafeWord for Citrix. (Secure Computing Inc. Business case solutions brief 2007:4.) Vaikka tutkimuksen henkilöt luovuttivat omat salasanansa näinkin helposti, toukkaa he tuskin kuitenkaan noin vain kenellekään luovuttaisivat. Todennäköisempää on sen häviäminen ja siinä tapauksessa toukka poistettaisiin heti järjestelmästä, jolloin sen laittomasta käytöstä tulee hyödytöntä. Lisäksi toukasta saatavien salasanojen kirjoittaminen ylös paperille vaikka seuraavien 10 koodin osalta on turhaa, sillä järjestelmä ei hyväksy aiempia salasanoja enää viimeisimmän järjestelmään syötetyn koodin jälkeen.

Vahvan autentikoinnin lisäksi SafeWord for Citrix -autentikointijärjestelmä on vaivaton asentaa jo olemassa olevaan ympäristöön eikä vaadi lisäsijoituksia laitteistoon. Se integroidaan yhteen Active Directory -hakemistopalvelun kanssa, jossa Active Directory Users and Groups -työkaluun asentuu ohjelmalaajennus. Näin ollen järjestelmä ei vaadi monimutkaista erillistä konfigurointia ja koulutusta sen käyttöön. Erillistä käyttäjätietokantaa ei siis tarvita, jolloin säästetään sekä hallinnoinnissa aikaa että rahaa. Jokaisen Active Directory -hakemistopalvelussa olevan käyttäjän kohdalla voidaan asettaa toukka käyttöön, lisätä siihen mahdollinen pin-koodi, tuoda uusien hankittujen ja käyttöönotettavien toukkien tietoja järjestelmään sekä luoda ongelmatilanteissa käyttäjille hätäsalasanoja Citrix-järjestelmiin pääsyksi. (Secure Computing Inc. Product overview 2007:1-2)

SafeWord for Citrix -autentikointipalvelu voidaan asentaa useisiin Windows 2000 ja 2003 Server -käyttöjärjestelmiin, jotta häiriötilanteissa autentikointipalvelu jatkuu katkeamattomana esimerkiksi palvelinrikon sattuessa. Järjestelmä mahdollistaa myös yksinkertaiset kuormantasausominaisuudet sekä toukkakirjastojen ja konfigurointiasetusten automaattisen varmuuskopioinnin. Tämä kaikki edellyttää järjestelmässä olevan synkronointitoiminnon käyttöönottoa. Kuormantasaus siirtää autentikointipyynnöt yhden palvelimen kuormituksen ollessa korkealla muille autentikointipalvelimille. Myös kaikki järjestelmään tehtävät konfiguraatiomuutokset yhdelle palvelimelle replikoituvat muille järjestelmän palvelimille automaattisesti. (Secure Computing Inc. App note 2007:3-4)

SafeWord for Citrix -autentikointijärjestelmän käyttöönotosta sekä konfiguroinnista Visma Software Oyj:n tietoverkossa kerrotaan tarkemmin luvussa 8 ”SafeWord for Citrix -autentikointijärjestelmän käyttöönotto”.

5 Citrix Access Gateway -aktiivilaitteen asennus

Citrix Access Gateway -laite voidaan asentaa erilaisiin verkkoratkaisuihin tekemättä muutoksia jo olemassa oleviin laitteistoihin tai ohjelmistoihin. Niinpä laitteisto on yhteensopiva muiden verkon aktiivilaitteiden, kuten palomuurien, reitittimien ja palvelimien ja kuormantasaajien kanssa.

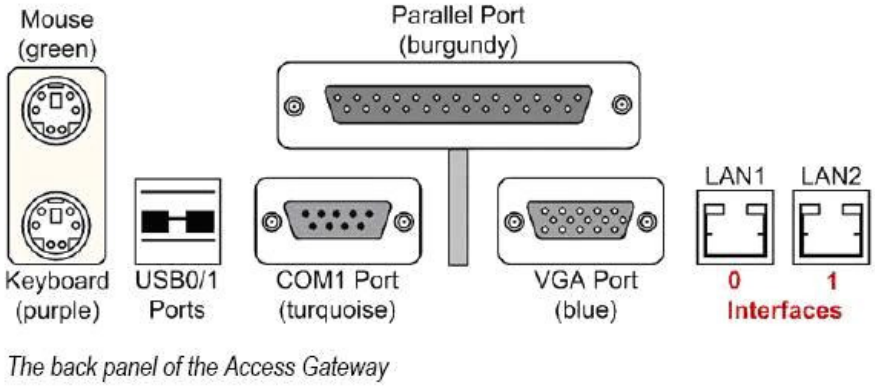
5.1 Asennuksen valmistelu

Asennuspaketin tarvikkeiden lisäksi asennukseen tarvitaan verkkokaapeli laitteen kytkemiseksi kytkimeen. Laitteessa on kaksi ethernet-liitäntää, jotka mahdollistavat todellisen asennuksen DMZ-alueelle eli yksi liitäntä ulkoista ja yksi sisäistä ip-osoitetta varten. Visma Software Oyj:n verkossa laite sijoitetaan DMZ-alueelle, johon tulee yksi ethernet-liitäntä palomuurista. Toinen ethernet-liitäntä kytketään Citrix Access Gateway -laitteesta sisäverkkoon erillisen kytkimen kautta. Räkkikiinnitystä varten laitteeseen kiinnitetään kiskot, joiden avulla laite voidaan kiinnittää turvallisesti laitetelineeseen muiden palvelimien rinnalle.

Laitteen konfigurointia varten DMZ-alueelle täytyy tiedossa olla sen julkinen ip-osoite ja verkkomaski, sisäverkon Citrix Advanced Access Control -palvelimeen viittaava ip-osoite ja verkkomaski, FQDN (Fully Qualified Domain Name), palomuurin ip-osoite sekä portti 443 verkkoliikennettä varten. (Getting Started with Access Gateway: 11)

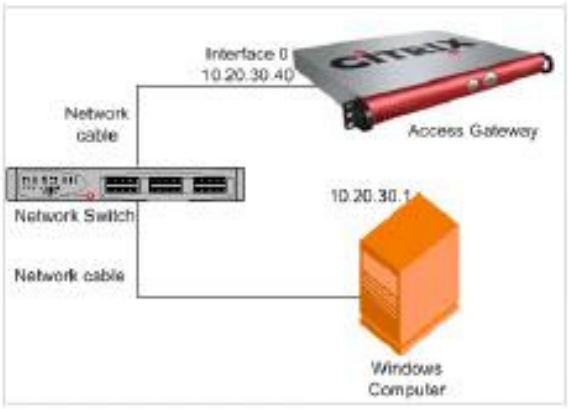
5.2 Asennus ja konfigurointi

Laitetta voidaan konfiguroida usean eri liitännän kautta, kuten USB- (Universal Serial Bus) ja sarjaportin kautta, mutta kätevintä sitä on hallinnoida etäkoneelta suoraan ethernet-liitännän kautta (kuva 3). Laitteen konfigurointiin käytetään Citrix Access Gateway Administration -työkalua, jonka käytöstä kerrotaan lisää hiukan myöhemmin tässä luvussa.



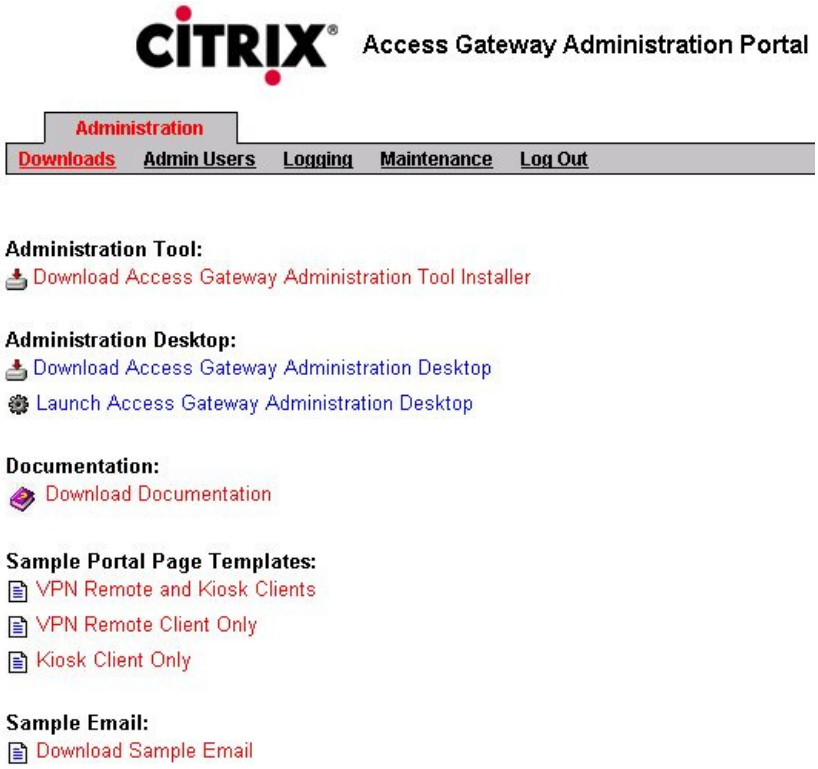
Kuva 3. Citrix Access Gateway -laitteen liitännät (Getting Started with Access Gateway 2005:14)

Laitteen varsinainen asennus alkaa sen kiinnittämisellä palvelinräkkiin, jonka jälkeen sen voi kytkeä verkkovirtaan. Laite kytketään verkkoon kuvan 4 mukaisesti, jolloin sen voi kytkeä päälle heti liitäntöjen kytkemisen jälkeen.



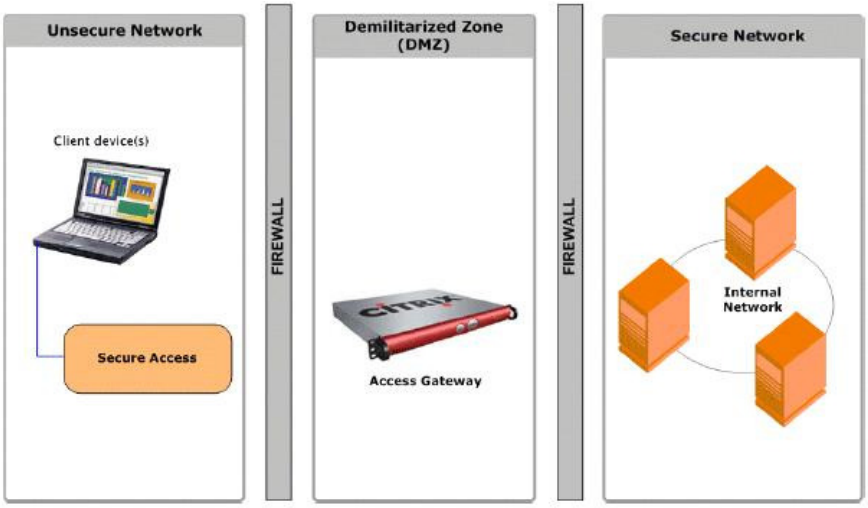
Kuva 4. Citrix Access Gateway -laitteen kytkeminen muihin aktiivilaitteisiin (Getting Started with Access Gateway 2005:14)

Citrix Access Gateway Administration -hallintatyökalu otetaan käyttöön lataamalla se Citrix Access Gateway Administration -portaalista avaamalla internet-selain osoitteeseen https://10.20.30.40:9001, joka on laitteen ethernet0-liitännän vakio ip-osoite. Portaalissa voidaan sen lisäksi muun muassa vaihtaa järjestelmänvalvojan salasanaa, ladata Citrix Access Gateway -järjestelmän käyttöopas sekä päivittää tai palauttaa järjestelmän ohjelmisto (kuva 5). (Getting Started with Access Gateway 2005: 13-14)



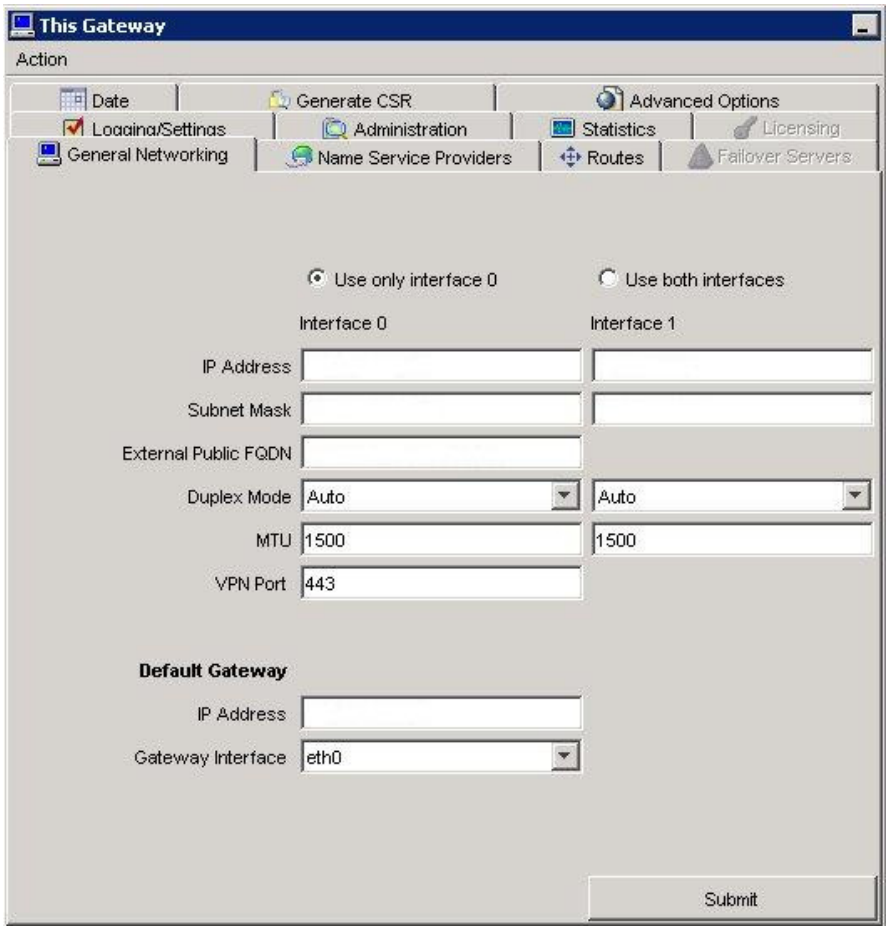
Kuva 5. Kuvaruutukaappaus Citrix Access Gateway Administration -portaalista

Citrix Access Gateway Administration -hallintatyökalu asennetaan järjestelmänvalvojan päätelaitteelle ja myöhemmin lisäksi Citrix Advanced Access Control -palvelimelle. Asennuksen jälkeen sillä tehdään vain kerran yksi konfigurointi, josta kaikki asetukset siirtyvät myös muille mahdollisesti verkossa oleville Citrix Access Gateway -laitteille. Visma Software Oyj:n verkossa on käytössä DMZ-skenaarion (kuva 6) mukainen käyttöönotto. (Getting Started with Access Gateway 2005: 14)



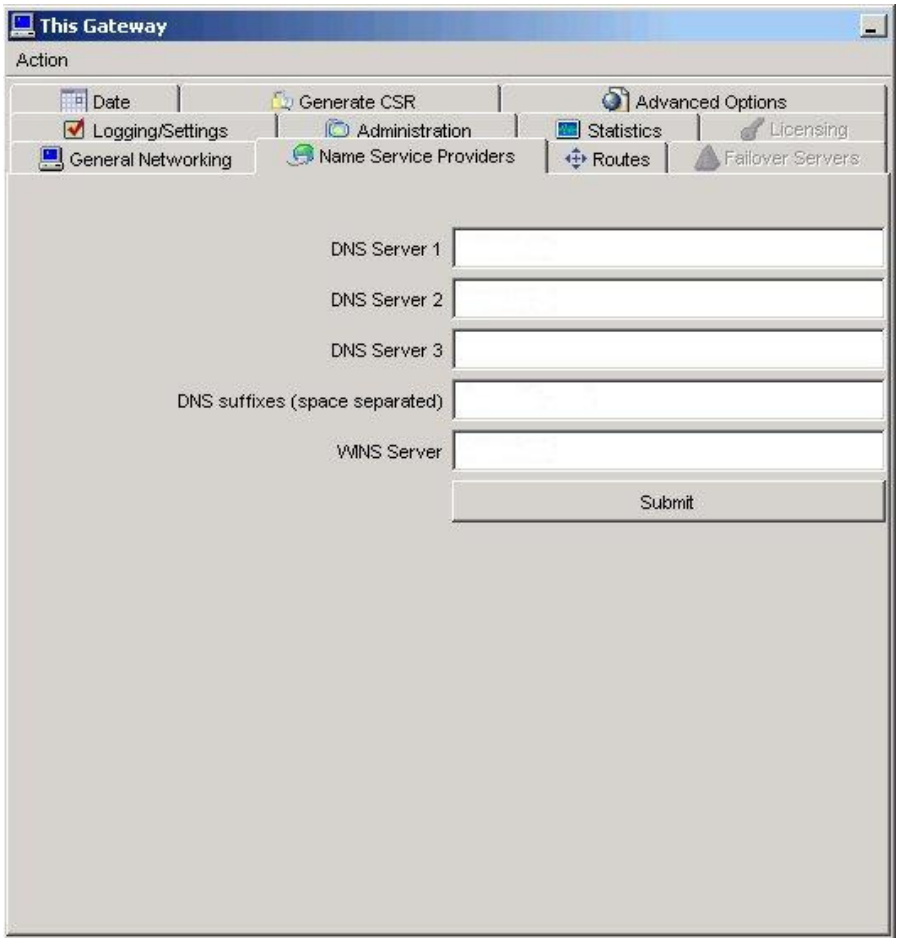
Kuva 6. Citrix Access Gateway -laitteen asennusskenaario DMZ-alueelle (Getting Started with Access Gateway 2005:18)

Laitteen konfigurointi (kuva 7) aloitetaan sen ulkoisen ip-osoitteen määrittelyllä valitsemalla Citrix Access Gateway Cluster -välilehdeltä General Networking -välilehti, jossa valitaan käytettäväksi vain interface 0-liitäntää ja antamalla siihen ip-osoite ja aliverkonpeite. Lisäksi määritellään ulkoinen julkinen domainnimi (FQDN). Duplex mode ja MTU-arvot sekä VPN-liikenteen portti 443 jätetään vakioarvoihinsa. Oletusyhdyskäytäväksi tulee palomuurin ip-osoite, jota DMZ-alueen muut palvelimet myös käyttävät. (Getting Started with Access Gateway 2005: 17)



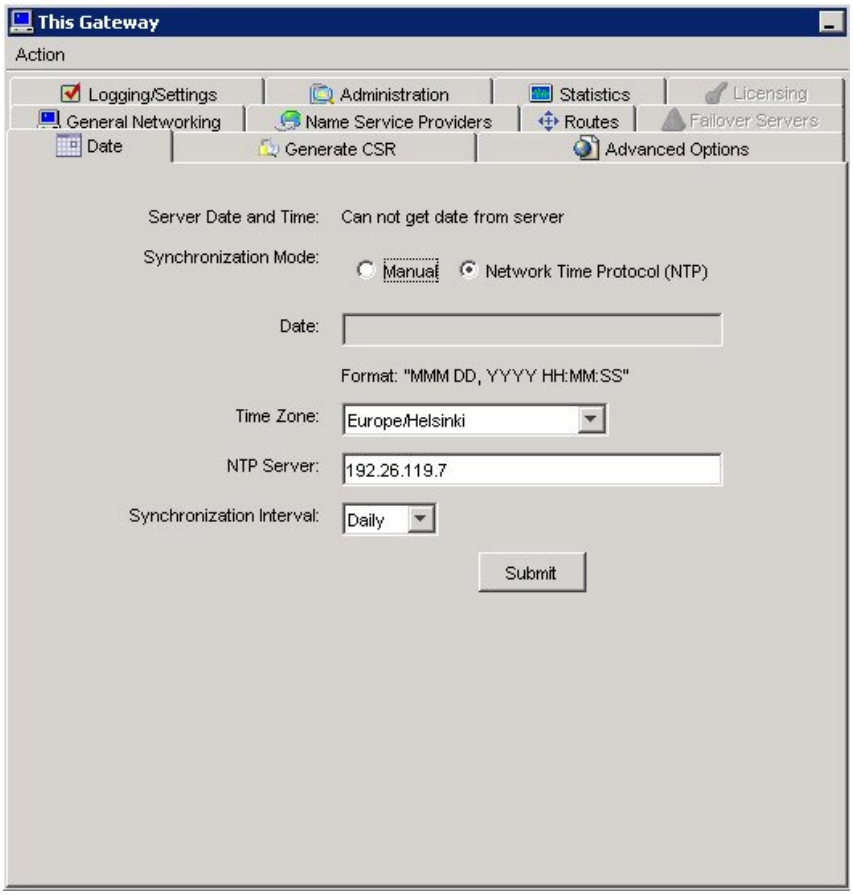
Kuva 7. Citrix Access Gateway -laitteen verkkoasetukset

Name Service Providers -välilehdellä määritellään käytettävien DNS-palvelimien ip-osoitteet, domain-päätteen etsintälista sekä WINS-palvelin (Windows Internet Naming System) (kuva 8). (Getting Started with Access Gateway: 17)



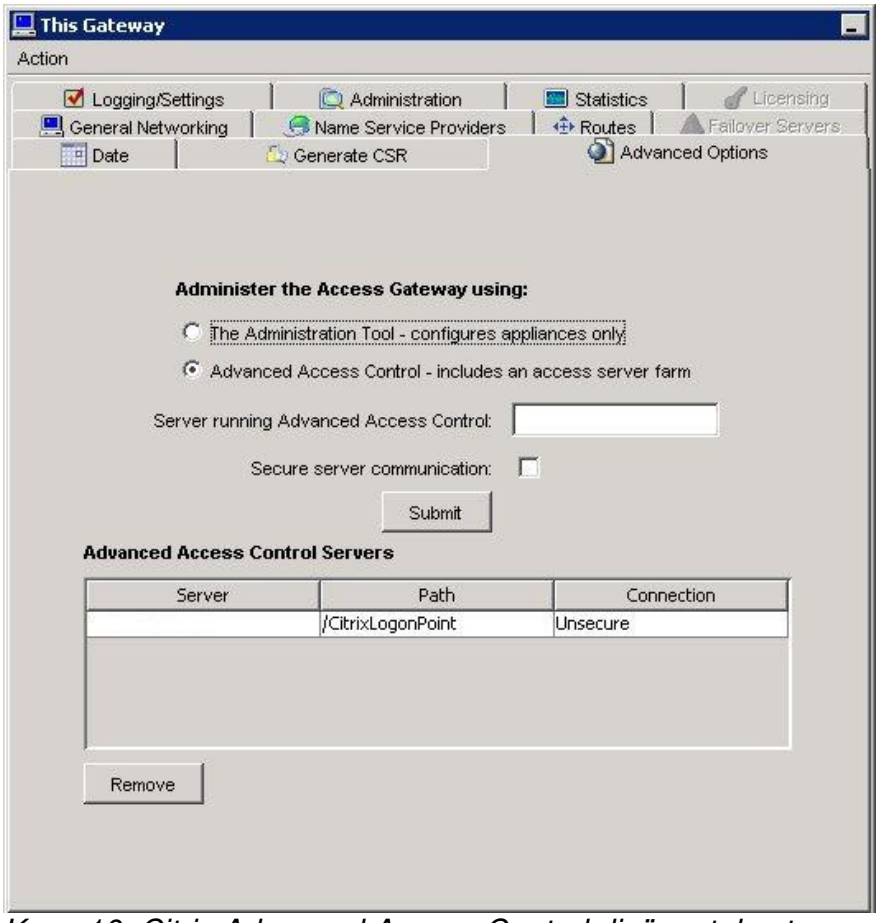
Kuva 8. Nimipalvelinasetukset

Staattinen reititys ei ole käytössä, joten tälle välilehdelle ei tehdä muutoksia. Sen sijaan Date-välilehdellä määritellään käytettävän julkisen NTP-palvelimen (Network Time Protocol) ip-osoite sekä aikavyöhyke ja synkronointi-intervalliksi päivittäinen (kuva 9).



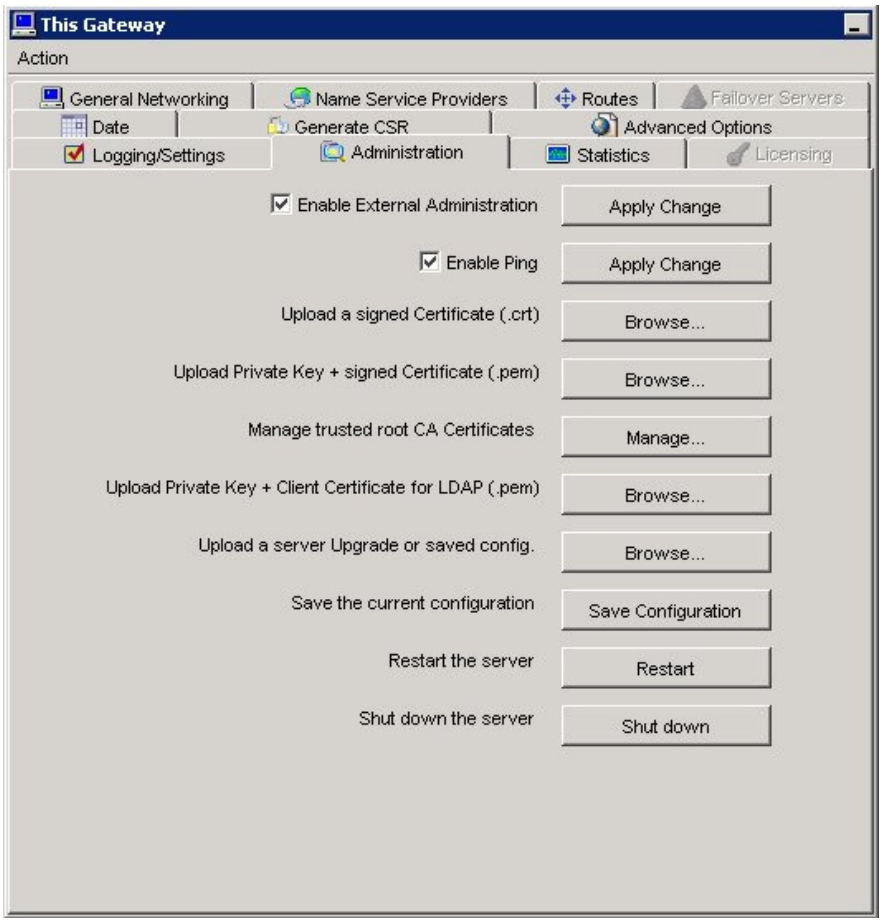
Kuva 9. Ajan synkronoinnin asetukset verkon kautta

Lisäasetukset-välilehdellä voidaan valita, miten Citrix Access Gateway -laitetta hallinnoidaan. Koska Citrix Access Gateway on hankittu Citrix Advanced Access Control -ohjelmiston kanssa, voidaan sitä jatkossa konfiguroida suoraan Citrix Advanced Access Control -palvelimelta. Ohjelmisto mahdollistaa monipuolisemmat konfigurointimahdollisuudet verrattuna pelkän Citrix Access Gateway –laitteen konfiguroimiseen. Ominaisuus saadaan käyttöön valitsemalla ”Advanced Access Control - includes an access server farm” -vaihtoehto ja lisäämällä käytetyn palvelimen ip-osoite sille varattuun ruutuun (kuva 10). (Getting Started with Access Gateway 2005: 20)



Kuva 10. Citrix Advanced Access Control -lisäasetukset

Administration-välilehdellä voidaan vaikuttaa ylläpidollisiin asioihin. Laitteen etähallinta otetaan käyttöön ja sisäverkon aktiivilaitteiden pingaaminen sallitaan ulkoverkosta. Laitteeseen on myös mahdollista ladata sertifikaatteja ja talletettuja konfiguraatioita sekä käynnistää ja sammuttaa laite tarvittaessa (kuva 11).



Kuva 11. Citrix Access Gateway -laitteen hallinnointiasetukset

Asennus vaatii vielä laitteen hankinnan mukana tulleen lisenssitiedoston lataamisen laitteeseen. Toimenpide tehdään Licensing-välilehdeltä. Kaikista lisenssitiedostoista on suositeltavaa ottaa varmuuskopio siltä varalta, jos ohjelmiston asennus täytyisi tehdä laiterikon vuoksi uudestaan. Samoin koko konfiguraatiosta on otettava varmuuskopio, joka palautettaessa sisältää myös ladatut lisenssitiedostot.

5.3 Palomuurisäännöt

Citrix Access Gateway -järjestelmän VPN-liikenteeseen käytettävä Secure Access -asiakasohjelmisto käyttää porttia 443 verkkoliikenteeseen käyttäjän päätelaitteen sekä Citrix Access Gateway -laitteen välillä. Tämän portin kautta kulkee SSL VPN -liikenne, jolloin lähetettävä data siirtyy päätelaitteen ja Citrix Access Gateway -laitteen välillä salattuna. Seuraavassa kerron tarkemmin tämän kaiken mahdollistavista palomuurisäännöistä.

Sisään tulevan liikenteen palomuurisääntöihin tehdään ensimmäinen sääntö, jossa sallitaan liikenne millä tahansa protokollalla ja mistä tahansa ip-osoitteesta Citrix Access Gateway -laitteen ip-osoitteeseen portista 443. Toisella säännöllä sallitaan kaikki liikenne sisäverkossa lähiverkosta toiseen. Kolmas sääntö koskee TCP/IP-liikennettä (Transmission Control Protocol/IP Protocol) DMZ-alueelta Citrix Access Gateway -laitteen ip-osoitteesta Citrix Advanced Access Control -palvelimen ip-osoitteeseen porteissa 80 ja 443. DNS-nimenselvennystä varten neljäntenä sääntönä sallitaan udp-liikenne DMZ-alueelta Citrix Access Gateway -laitteen ip-osoitteesta sisäverkon toimialueen ohjauskoneille käyttäen porttia 53. Viides sääntö koskee icmp-liikennettä DMZ-alueelta Citrix Access Gateway -laitteesta sisäverkkoon päin porteissa 8 ja 30. Citrix Access Gateway -laitteen hallintaa ja konfigurointia varten sallitaan TCP/IP-liikenne Jyväskylän lähiverkosta DMZ-alueelle Citrix Access Gateway -laitteeseen porteissa 9001, 9002 ja 9005. Siten laitetta on mahdollista hallinnoida myös www-sivuston kautta Citrix Access Gateway Administration -hallintatyökalun lisäksi.

Palomuurisääntöjen muokkauksen sekä Citrix Access Gateway -laitteen konfiguroinnin jälkeen laite on vielä käynnistettävä uudestaan, jonka jälkeen se on valmis tuotantokäyttöön. Jotta koko Citrix Access Gateway -järjestelmä voitaisiin ottaa käyttöön, Citrix Advanced Access Control -ohjelmisto on ensin asennettava ja konfiguroitava käyttöön käyttäen Citrix Access Suite -konsolia. Ohjelmiston asennus Citrix Advanced Access Control -palvelimelle käydään läpi luvussa 7 ”Citrix Advanced Access Control - asentaminen”.

6 Citrix Access Gateway – pääsynhallinnan strategia

Tässä luvussa käyn läpi Citrix Access Gateway:n pääsynhallintaan liittyvät suunnitelmat ennen varsinaisen Citrix Advanced Access Control -ohjelmiston asennusta hallintakonsoleineen. Ensimmäinen projektin osa – järjestelmän hankintapäätös ja sen soveltuvuus yrityksen infrastruktuuriin – oli jo tehty ennen työsuhteeni alkamista Visma Software Oyj:ssä sen tietohallinnon puolesta. Osallistumiseni itse projektiin alkoi riskianalyysin teolla, joka tehdään tällaisten hankinta- ja käyttöönottoprojektien yhteydessä tietoverkon infrastruktuurin arvioimisen jälkeen. Kolmantena osana suunnitelmaa oli varsinaisen pääsynhallinnan suunnittelu.

6.1 Tietoverkon infrastruktuurin arvioiminen

Järjestelmän hankintapäätökseen vaikutti osaltaan tietoverkon laajuus laitteistoineen ja etäkäyttäjien suuri määrä sekä tärkeimpänä tietoturva, jota haluttiin lisätä ja parantaa. Käyttäjien käytössä tulevat olemaan samat resurssit kuin vanhan Windows VPN -yhteyden kautta: jaetut verkkolevyt, intranet (Vintra), Citrix-etätyöpöytä (Citrix Metaframe Presentation Server -ympäristön julkaistut ohjelmistot) sekä muut palvelut. Tarkoituksena on taata käyttäjille ns. Full VPN -yhteys, jolloin heillä on pääsy kaikkiin verkon resursseihin.

6.2 Riskianalyysi

Riskianalyysin laatimisessa otetaan huomioon, minkälaisiin resursseihin käyttäjien olisi päästävä, miten arkaluontoista dataa ne sisältävät ja mistä ympäristöstä tähän dataan voi päästä käsiksi. Uhkana koetaan toimialueen ulkopuoliset ja mahdollisesti suojaamattomat, ilman virustorjuntaa olevat koneet, joissa käyttäjillä on lisäksi järjestelmänvalvojan oikeudet. Tällöin olisi periaatteessa virusten ja matojen pääsy tietoverkkoon VPN-putken läpi täysin mahdollista ja todennäköisempää kuin jos tietoverkkoon pääsisi vain toimialueeseen liitetyllä ja tietyllä virustorjuntaohjelmistolla varustetulla koneella. Juuri nämä riskit halutaan välttää koskien Full VPN -yhteyttä, toisaalta kotikoneiden pääsy vain tiettyyn tietoverkon osaan sallitaan myöhemmin

käyttöönotettavalla Kiosk Mode -yhteystyypillä, johon pääsynhallinnan strategia suunnitellaan tarkemmin tulevaisuudessa.

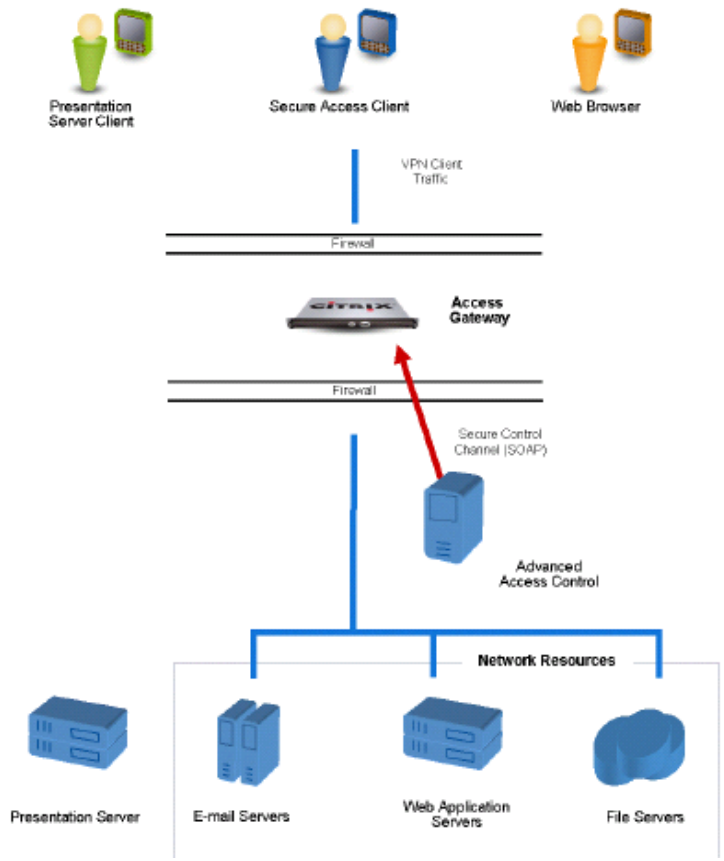
6.3 Pääsynhallinnan toteutus

Käyttäjille tarjotaan vain täyttä SSL VPN -yhteyttä järjestelmän käyttöönoton ensimmäisessä vaiheessa. Niinpä käytössä on kaikki tietoverkon resurssit, kuten jos käyttäjä työskentelisi toimistolla ollessaan kytkeytyneenä sisäverkkoon. Kaikille työntekijöille yhteyttä ei kytketä, vaan ainoastaan paljon matkustavat sekä muutoin työnsä puolesta etäyhteyttä tarvitsevat henkilöt voivat uutta yhteyttä jatkossa käyttää. Kiosk Moden ollessa tulevaisuudessa käytössä (2. vaihe), sillä sallitaan pääsy tiettyihin verkon resursseihin rajoitetuin oikeuksin esimerkiksi lentoasemilla olevilta internet-päätteiltä.

Riskianalyysissä esiin tullut uhka viruksien ja matojen pääsystä sisäverkkoon puoltaa pääsynhallinnan ja yhteyspolitiikkojen suhteen kallistumaan siihen, että vain toimialueeseen liitetyt ja virustorjunta-ohjelmistolla varustetut koneet päästetään sisäverkkoon. Ohjelmistoversion ja sen mallitiedoston (pattern file) on täytettävä vaaditut ehdot. Näitä ja muita mahdollisia päätelaitteiden skannauksia järjestelmässä suorittaa Endpoint Analysis -ohjelmisto, joka suoritetaan aina, kun käyttäjä ottaa päätelaitteellansa järjestelmään yhteyttä. Toinen mahdollinen tapa kontrolloida yhteyksiä järjestelmään on käyttää ns. jatkuvia skannauksia (Continuous scans), joilla voidaan varmistaa, että yhteyden aikana päätelaite täyttää jatkuvasti sille asetetut vaatimukset.

Yhteyspolitiikan sääntöihin konfiguroidaan Active Directory -käyttäjäryhmä, johon kaikkien etäkäyttäjien on kuuluttava. Secure Access -asiakasohjelmiston toiminta etäyhteyden muodostamisen aikana ja etäyhteyttä varten tarvittavien virtuaalisten ip-osoitteiden luovuttaminen päätelaitteille konfiguroidaan halutulla tavalla. Pääsynhallintapolitiikkaan määritellään myös sallitut verkkoresurssit ja niissä sallittavat käyttäjien toimenpiteet.

Citrix Access Gateway -laitteisto sijoitetaan DMZ-alueelle palomuurin sisäpuolelle (kuva 12) ja Citrix Advanced Access Control -palvelin sisäverkkoon VMWare-alustalle virtuaalikoneeksi. Näin ollen palomuuri suojaa palvelinta samoin kuin muitakin palvelimia sisäverkossa. Käyttäjän koneella olevalta asiakasohjelmistolta sallitaan liikenne DMZ-alueelle ulkoverkosta ja VPN-yhteyden vaatima liikenne avataan myös DMZ-alueelta sisäverkkoon käyttäen tiettyjä portteja ja protokollia.



Kuva 12. Citrix Access Gateway -laitteen sijoittaminen DMZ-alueelle (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 20)

Autentikointimuodoksi järjestelmään integroidaan Secure Computing -yhtiön SafeWord for Citrix -autentikointijärjestelmä, jossa tavallisen Windows-verkon käyttäjätunnuksen ja salasanan lisäksi käytetään toukasta saatavaa vaihtuvaa koodia lisäturvana kirjautumiseen. SafeWord for Citrix -autentikointijärjestelmän käyttöönotosta kerrotaan tarkemmin kappaleessa 8 ”SafeWord for Citrix -autentikointijärjestelmä”.

Mahdollisen laiterikon takia palvelimesta otetaan levykopio toiselle palvelimelle aina kun konfigurointeihin tai palvelimen ase-

tuksiin tehdään isompia muutoksia käyttäen apuna kopiointiin tarkoitettua skriptiä. Lisäksi näistä muutoksista siirtyy dataa SQL-tietokantaan toiselle palvelimelle, jossa se myös varmistetaan vielä nauhalle. Laitteistossa on myös mahdollisuus kahdennettuun ratkaisuun, jossa toisen koneen hajotessa toinen pitäisi järjestelmää yllä. Tätä ratkaisua ei vielä kuitenkaan tässä vaiheessa Visma Software Oyj:ssä oteta käyttöön.

Useita Citrix Advanced Access Control -palvelimia on mahdollista konfiguroida yhteen tai usempaan rooliin pääsynhallintafarmissa. Tietokantapalvelimet ja Citrix Advanced Access Control -palvelimet on mahdollista klusteroida, jotta yhden palvelimen kaatuessa toinen palvelin takaa tarvittavat palvelut käyttäjille yhteyksien katkeamatta. Visma Software Oyj:n tietoverkossa käytetään sekä yhtä pääsynhallinta- että yhtä jo olemassa olevaa tietokantapalvelinta.

Käyttäjille on mahdollista luoda muokattu Access Center- tai vakiomuotoinen navigointi-sivusto, joista sisäverkon palveluita käytetään. Access Center -sivustolle on mahdollista tuoda julkaistut sovellukset esimerkiksi Citrix MetaFrame Presentation Server -ympäristöstä tai liittää Microsoft Outlook -sähköpostijärjestelmä osaksi sitä. Vakiomuotoisella navigointi-sivustolla näkyy kaikki sallitut ja konfiguroidut integroinnit Presentation Server -ympäristöön, verkkoresursseihin tai tiedostojakoihin. Näistä kumpaakaan ei Vismassa oteta käyttöön, vaan täyden VPN-yhteyden muodostamisen jälkeen käyttäjillä on etätoimistolla käytössään samat palvelut kuten toimistolla ollessa.

7 Citrix Advanced Access Control – asentaminen

Tässä luvussa käyn läpi ohjelmiston asennukseen liittyvät seikat kuten ohjelmisto- ja laitteistovaatimukset sekä käyttäjätileihin, asiakasohjelmistoihin ja ominaisuuksiin liittyvät lisenssointivaatimukset. Ennen varsinaista asennusta on myös käytävä läpi tehtäviä, jotka on tehtävä ja tarkistettava, jotta ohjelmisto voidaan asentaa. Kappaleen loppupuolella käyn vielä läpi varsinaisen ohjelmistoasennuksen.

7.1 Ohjelmisto-, laite- ja ominaisuusvaatimukset

Citrix Advanced Access Control -ohjelmisto vaatii asentuakseen ja toimiakseen kunnolla Windows 2000/2003-palvelimelta vähintään 512 megatavua muistia sekä service pack 2 -paketti asennettuna. Ohjelmisto käyttää myös .NET Framework 1.1 -versiota service pack 1 -paketilla varustettuna sekä Microsoftin MDAC:n (Microsoft Data Access Components) versiota 2.7. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 32)

Citrix Advanced Access Control -ohjelmisto käyttää Microsoft SQL Server 2000:ta (tai uudempi) varten käyttäjätiliä, jolla on oikeudet luoda tietokanta SQL-palvelimelle ja myös kirjoittaa ja lukea tietoa tietokannasta. Käyttäjätili on db_datareader ja db_datawriter-ryhmien jäsen. Microsoft SQL 2000 tukee ns. Mixed Mode -autentikointia, joka hyväksyy Windows-käyttäjätilien lisäksi SQL-palvelintilit. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 34)

Farmin palvelimien ja niiden palveluiden välistä kommunikointia ja liikennöintiä varten on myös luotava palvelukäyttäjätili, jolla on oltava seuraavat ominaisuudet. Tili kuuluu järjestelmänvalvojat-ryhmään kaikilla farmin palvelimilla. Tili ei vanhene koskaan, kuten ei sen salasanakaan. Jos ryhmäkäytäntöjen avulla kohdistetaan palvelimen paikallisiin järjestelmänvalvojat-ryhmään rajoitettuja politiikkoja, on palvelutilin kuuluttava johonkin politiikalla lisättyyn hallintaryhmään. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 35)

Lisenssoinin hoitaa farmin lisenssi-palvelin, joka toimii lisenssipalvelimena myös Citrix Metaframe Presentation Server -järjestelmälle.

Citrix Advanced Access Control -ohjelmiston monipuolisten ominaisuuksien hyödyntämistä varten on sekä palvelimilla, että loppukäyttäjien päätelaitteilla oltava tietyt komponentit ja ohjelmistot asennettuina. Farmin WWW-palvelimella tarvitaan Microsoftin Word, Excel, Powerpoint ja Visio (2000 tai uudemmat), jotta HTML Preview -ominaisuutta voidaan käyttää siten, että dokumentit avautuvat suoraan selaimessa katselua varten. Turvallisuuden vuoksi kannattaa kaikista Office-ohjelmista laittaa makrosuojaus korkeimmalle mahdolliselle tasolle ja poistaa käytöstä luotto kaikkiin asennettuihin lisäosiin ja malleihin. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 38)

Live Edit -ominaisuutta varten päätelaitteissa on oltava asennettuna Live Edit Active X -komponentti, Internet Explorer 6.0 tai uudempi sekä Office 2000 -ohjelmisto tai uudempi. Live Edit tarjoaa käyttäjälle mahdollisuuden muokata dokumentteja suoraan selaimessa palvelimelle ilman, että niitä tallennettaisiin omalle päätelaitteelle ollenkaan. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 39)

Selainpohjainen sähköposti olisi myös mahdollista liittää osaksi Citrix Access Gateway -järjestelmän Access Center -portaalia joko siihen sisäänrakennetulla järjestelmällä tai käyttäen Microsoft Outlook Web Access -järjestelmää (OWA) integroituna siihen. Kuvassa 13 listataan vaaditut komponentit, joiden on oltava asennettuna suhteessa tuettuihin sähköpostijärjestelmiin. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 40) Visma Softwaressa OWA:a käytetään oman erillisen www-sivuston kautta, joten sitä ei liitetä Citrix Access Gateway -järjestelmään.

	Advanced Access Control Web Email	**Outlook Web Access**	**iNotes/Domino Web Access**
Required Mail Server	Microsoft Exchange Server, Versions 5.5, 2000, or 2003 with all service packs and critical updates installed	Microsoft Exchange Server, Versions 5.5, 2000, or 2003 with all service packs and critical updates installed	IBM Lotus Domino Server, Versions R5 or R6
Required Server Administration Tools	Microsoft Exchange System Management Tools Microsoft Exchange 5.5 Administrator	Microsoft Exchange System Management Tools Microsoft Exchange 5.5 Administrator	N/A
Supported Web Browsers	Internet Explorer 6.0 SP1 Safari 1.1 and 1.3 Netscape Navigator 7.1 and 7.2 Mozilla Firefox 1.0	Internet Explorer 6.0 SP1	Internet Explorer 6.0 SP1

Kuva 13. Järjestelmävaatimukset (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 40)

Olemassa olevan Citrix MetaFrame Presentation Server -järjestelmän integroiminen Citrix Advanced Access Control -järjestelmään vaatii päätelaitteilla asennettuna olevan Citrix MetaFrame Presentation Server -asiakasohjelmiston version 8.0 tai uudemman. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 43.) Vismassa on käytössä tätä kirjoittaessani versio 9.2.

Ennen Citrix Access Gateway -järjestelmän käyttöä, käyttäjien päätelaitteella tulee olla asennettuna seuraavat yleisimmät komponentit. Päätelaitteiden käyttöjärjestelmän on oltava vähintään Windows 2000 SP 4 -paketilla varustettuna tai Windows XP Home/Pro-versio SP 2 -paketilla varustettuna ja Internet Explorer 5.5 tai uudempi selain. Kuvasta 14 selviää muihin päätelaitteisiin tarvittavat komponentit. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 45)

Devices	Operating System	Web Browser
Desktop workstations	Microsoft Windows: Windows XP Home/Professional SP2 Windows 2000 Professional SP4	Internet Explorer 5.5 SP2 Internet Explorer 6.0 SP1 Netscape Navigator 8.0 Mozilla Firefox 1.0.4
	Apple Macintosh OS X (English only) 10.3.9 or greater	Safari 1.2 Netscape Navigator 8.0 Mozilla Firefox 1.0.4
	Red Hat Linux	Netscape Navigator 8.0 Mozilla Firefox 1.0.4
PDAs and Smartphones	PalmOS 5.2.1 (Palm Tungsten C)	PalmSource Web Browser 2.0
	Microsoft Pocket PC 2003 (HP iPaq Pocket PC h6300)	Internet Explorer
	Microsoft Windows Mobile 2003 (Smartphone)	Internet Explorer
	RIM BlackBerry (BlackBerry 7100t)	Default Web Browser

Kuva 14. Työasema ja PDA-laitteiston järjestelmävaatimukset (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 45)

Citrix Advanced Access Control -ohjelmisto lähettää kaiken sisällön päätelaitteiden selaimille käyttäen HTML- ja JavaScript–koodattuja Web-sivuja. Selaimilta vaaditaan lisäksi, että JavaScriptien suorittaminen sekä allekirjoitettujen ActiveX-komponenttien lataus onnistuu. Jos käyttäjien päätelaitteilla olevat asiakasohjelmistot pakotetaan käyttämään Javalla toteutettua asiakasohjelmistoa, on selaimessa sallittava myös Java Applettien lataaminen. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 46)

Päätelaitteissa on oltava asennettuna Endpoint Analysis -asiakasohjelmisto, joka kerää päätelaitteesta tietoa ja lähettää sen palvelimelle ennen kirjautumista järjestelmään. Kaikkien ActiveX-komponenttia asennukseen käyttävien asiakasohjelmistojen osalta on huomioitava, että ne vaativat asentuakseen

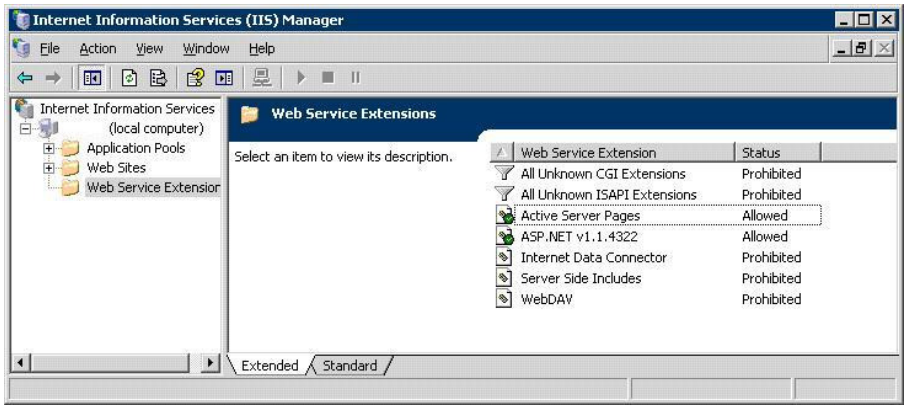
järjestelmänvalvoja oikeudet koneelle. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 46-47) Visma Software Oyj:n tietoverkon käyttäjillä on vain user-tasoiset oikeudet koneilleen, joten asiakasohjelmistot on asennettu käyttäen erillistä Asentaja-tunnusta. Tällä tunnuksella on rajoitetut järjestelmänvalvojan oikeudet päätelaitteille, mutta kaikkien ohjelmistojen asennukseen kuitenkin riittävät. Siten myös VPN-putken muodostamiseen päätelaitteen ja Citrix Access Gateway -laitteen välille tarvittavan Secure Access -asiakasohjelmiston asentamiseen käytetään tätä tunnusta.

7.2 Ennen asennusta

Muutamia seikkoja otetaan huomioon ennen varsinaisten ohjelmistojen asentamista. Ensimmäinen toimenpide on, että palvelimet päivitetään viimeisimmillä Microsoftin kriittisillä päivityksillä. Jotta asennettavien ohjelmistojen asennus sujuisi ilman ongelmia, varmistetaan vielä, että palvelinympäristö vastaa ohjelmistolle ja sen komponenteille ja niiden ominaisuuksille asetetut vaatimukset. Visma Software Oyj:n palvelinympäristössä on jo valmiina Citrix lisenssi -palvelin Citrix MetaFrame Presentation Server -ympäristöä varten, joten sitä käytetään myös uuden VPN-järjestelmän kanssa. Seuraavaksi asennetaan itse ohjelmistot, jonka jälkeen niihin ajetaan vielä viimeisimmät Citrixin julkaisemat hotfixit ja service packit.

Web Services -lisäosista tarvitaan ASP.NET (Active Server Pages), joka konfiguroidaan käyttämällä Internet Information Services (IIS) Manageria. Samalla täytyy WebDAV-laajennus poistaa käytöstä, koska Outlook Web Access -sähköpostiohjelmiston käyttäjien saapuneet-kansiot eivät muuten näy oikein. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 32-33.) Lisäyksenä edelliseen, että ongelma tulee vastaan Access Center -sivuston kautta julkaistussa ja integroidussa Outlook Web Access –ohjelmistossa, mutta ei kuitenkaan suoraan Outlook Web Access web-sivustoa käytettäessä.

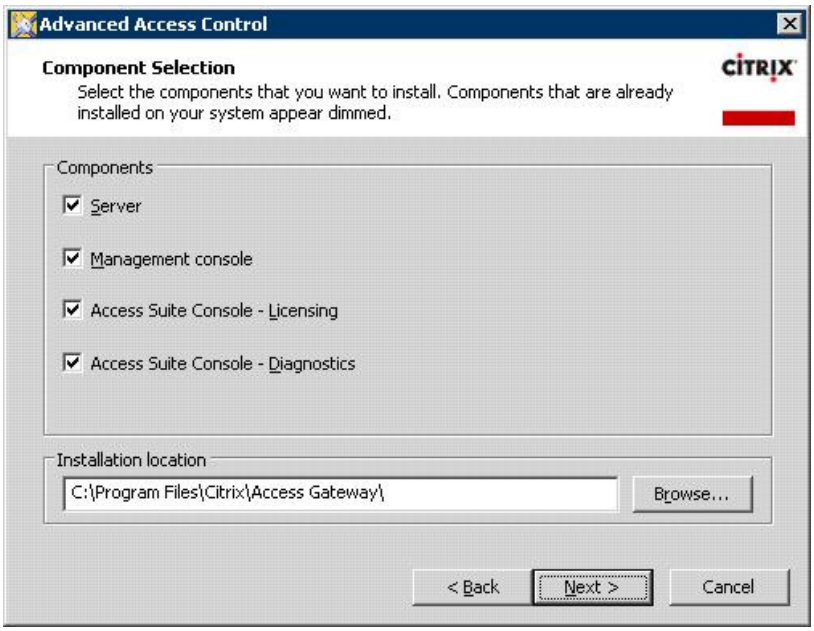
Jotta IIS:ssä saataisiin ASP.NET toimintaan, täytyy ohjauspaneelin hallintatyökaluissa olevalla IIS managerilla sallia sekä ASP.NET että Active Server Pages. Jotta Web Proxy-palvelu toimisi, on FrontPage Server web-laajennus otettava pois päältä. Kun ASP.NET on otettu käyttöön, on se vielä rekisteröitävä komennolla aspnet_regiis.exe-i komentokehotteessa (kuva 15). (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 32-33)



Kuva 15. IIS:n asetukset

7.3 Citrix Advanced Access Control -ohjelmiston asennus

Asennus aloitetaan Citrix Advanced Access Control CD-ROM-levyn laittamisella CD-asemaan, jolloin asennusvelho käynnistyy automaattisesti. Käynnistyneestä ikkunasta valitaan Product Installations -linkki, joka tuo esiin kaikki asennettavissa olevat ohjelmistot, joista valitaan Citrix Advanced Access Control. Lisenssisopimuksen hyväksymisen jälkeen avautuneessa ikkunassa valitaan palvelimelle asennettavat ohjelmiston komponentit (kuva 16).



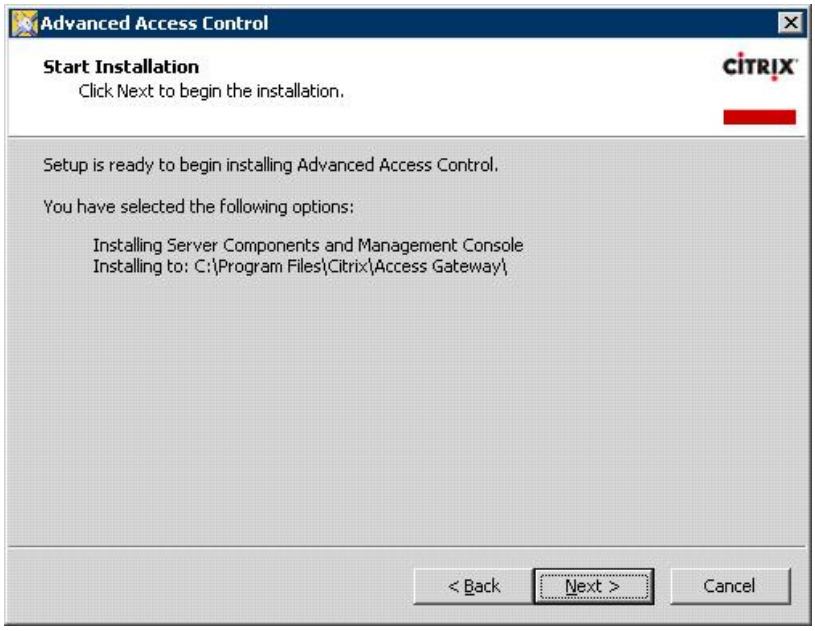
Kuva 16. Asennettavat ohjelmistokomponentit

Selainpohjaista sähköpostijärjestelmää varten palvelimelle olisi asennettava Microsoft Exchange System Management Tools sekä HTML Preview -ominaisuutta varten Office-paketti (kuva 17).

Kuva 17. Microsoft Office -paketista kertova infoikkuna

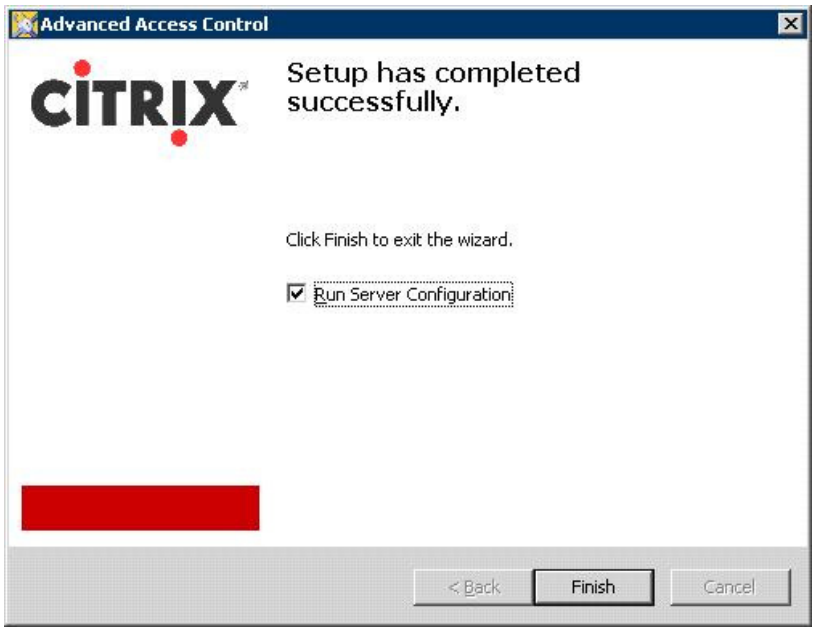
HTML Preview -ominaisuuksia ei oteta tällä erää käyttöön, sillä Visma Software Oyj:n tietojärjestelmässä on jo käytössä selainpohjainen Outlook Web Access etäkäyttöä varten ja HTML Preview -ominaisuutta tarvittaisiin vain, jos käytössä olisi Access Center -portaalia käyttävä Logon Point.

Seuraavaksi tarkistetaan vielä, mitä asennusvelholla ollaan asentamassa ja mihin polkuun (kuva 18).



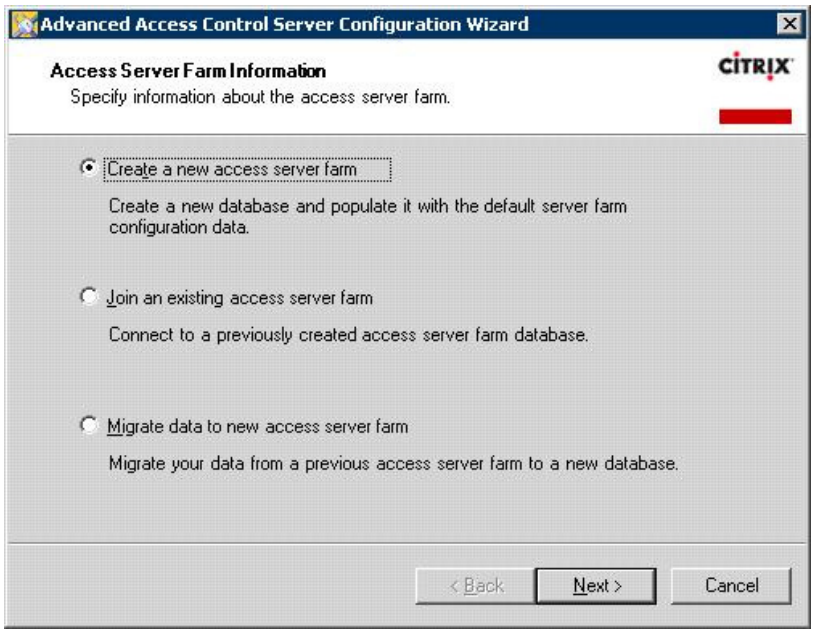
Kuva 18. Asennuspolku

Kun Citrix Advanced Access Control -ohjelmiston asennus on valmis, ajetaan vielä palvelimen konfigurointi-velho (kuva 19).



Kuva 19. Palvelimen konfigurointi

Ensimmäinen toimenpide on luoda uusi tietokanta jo olemassa olevalle SQL-palvelimelle, jonne Citrix Advanced Access Control -ohjelmiston konfigurointi sekä muu data tallentuu ja josta tarvittaessa voidaan palauttaa data laiterikon sattuessa (kuva 20).

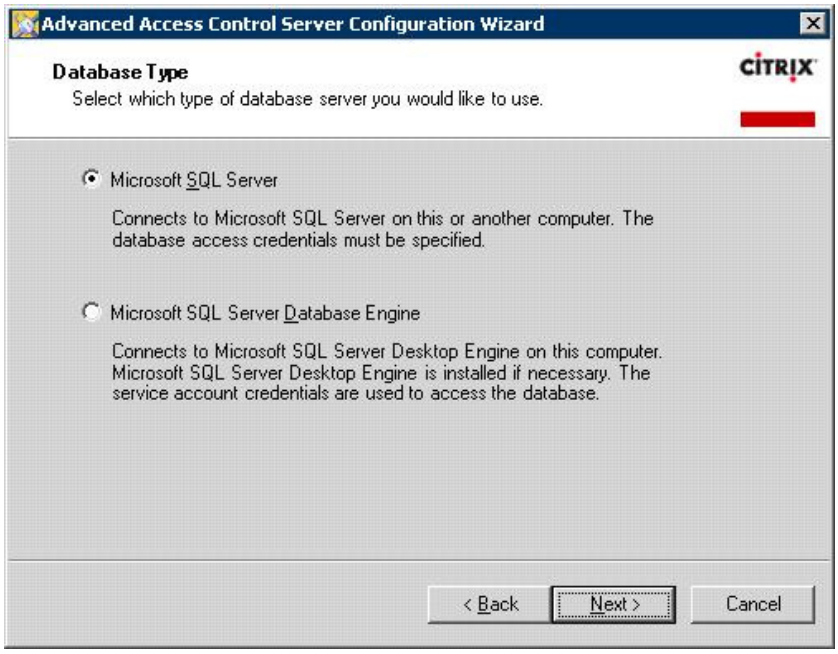


Kuva 20. Tietokannan luonti

Määritellään aiemmin luotu palvelutili, joka hoitaa datan tallentamisen SQL-palvelimelle (kuva 21).

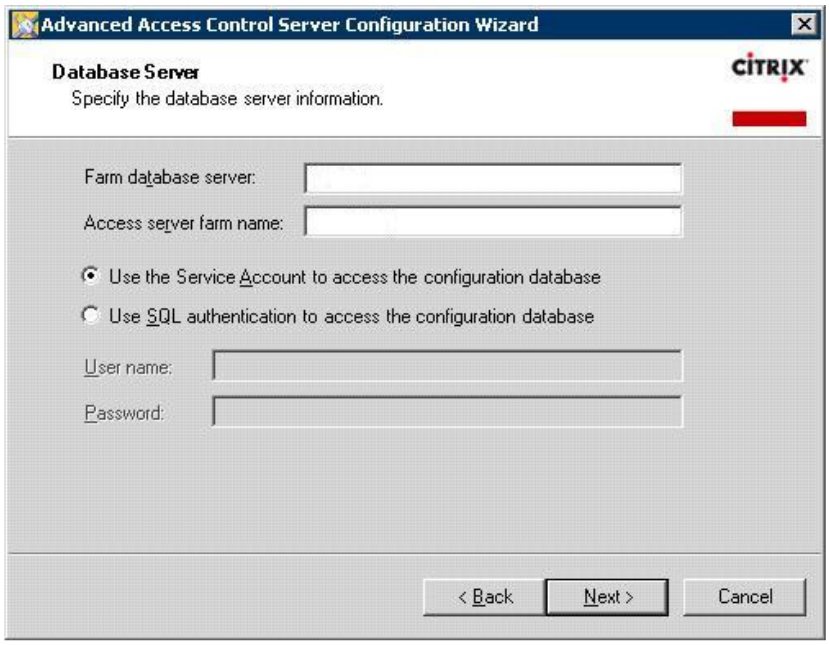
Kuva 21. Palvelutilin luonti

Seuraavaksi valitaan jo olemassa oleva SQL-palvelin, jota käytetään datan tallentamiseen sen tietokantaan (kuva 22).



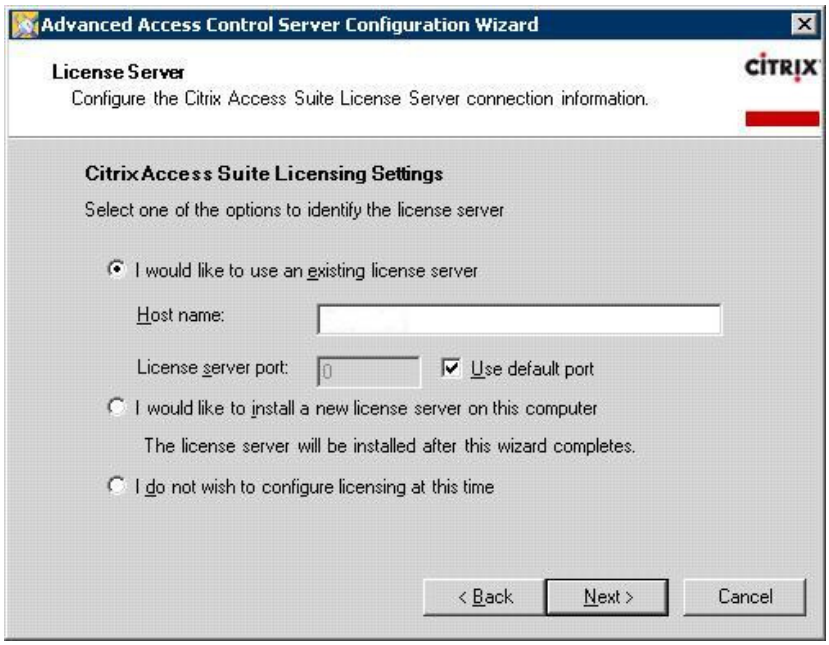
Kuva 22. SQL-palvelimen valinta

Asennusvelhon seuraavassa vaiheessa määritellään SQL-palvelimen tietokannalle nimi sekä aiemmin luotu palvelutili, jota käytetään konfigurointidatan siirtoon (kuva 23).



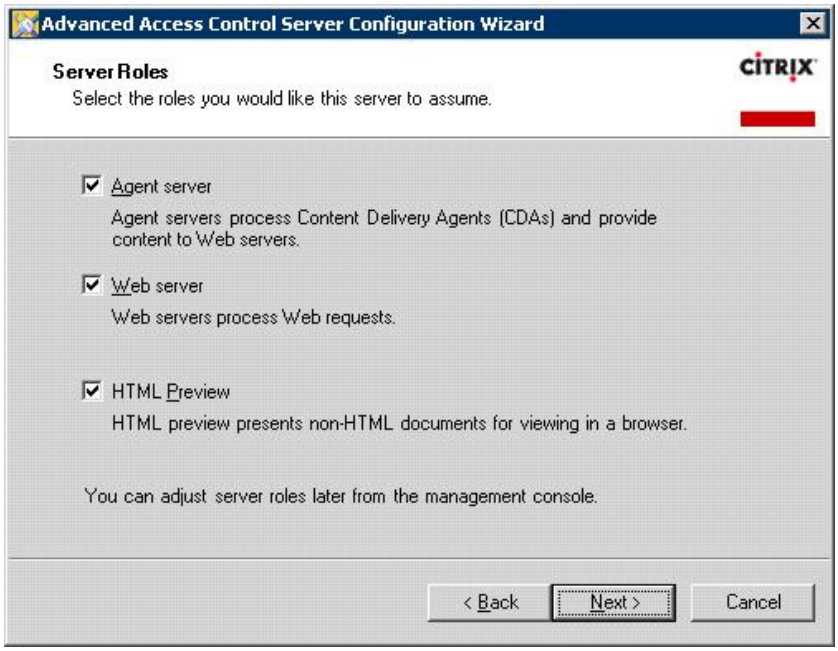
Kuva 23. SQL-palvelimen ja Citrix Access Gateway -farmin konfigurointi

Lisenssipalvelimena käytetään samaa palvelinta, jota hyödynnetään Citrix MetaFrame Presentation Server -ympäristön kanssa (kuva 24).



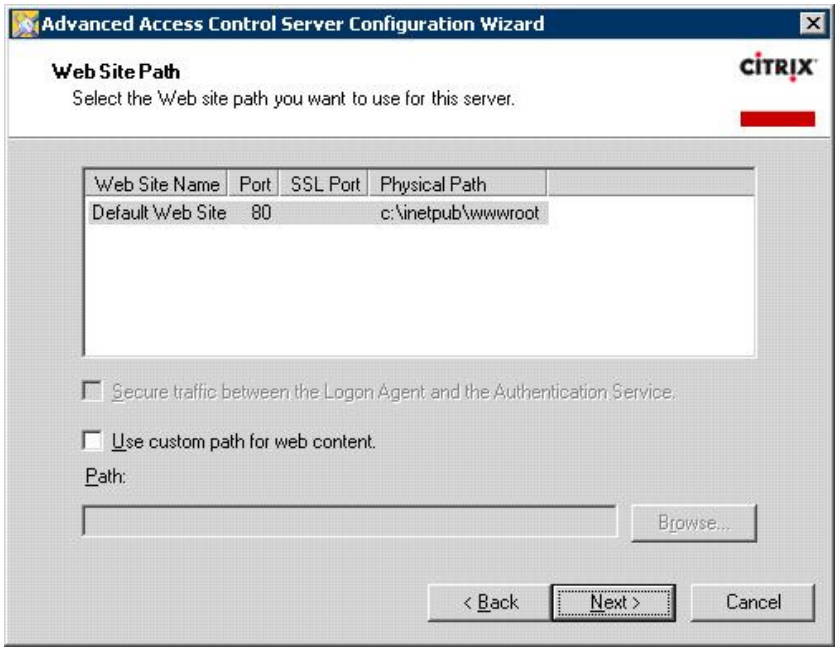
Kuva 24. Lisenssipalvelimen asetukset

Palvelimen rooliksi valitaan kaikki käytettävissä olevat, jotta kaikki ominaisuudet ovat tarvittaessa käytössä otettaessa niitä käyttöön (kuva 25).



Kuva 25. Palvelimen roolit

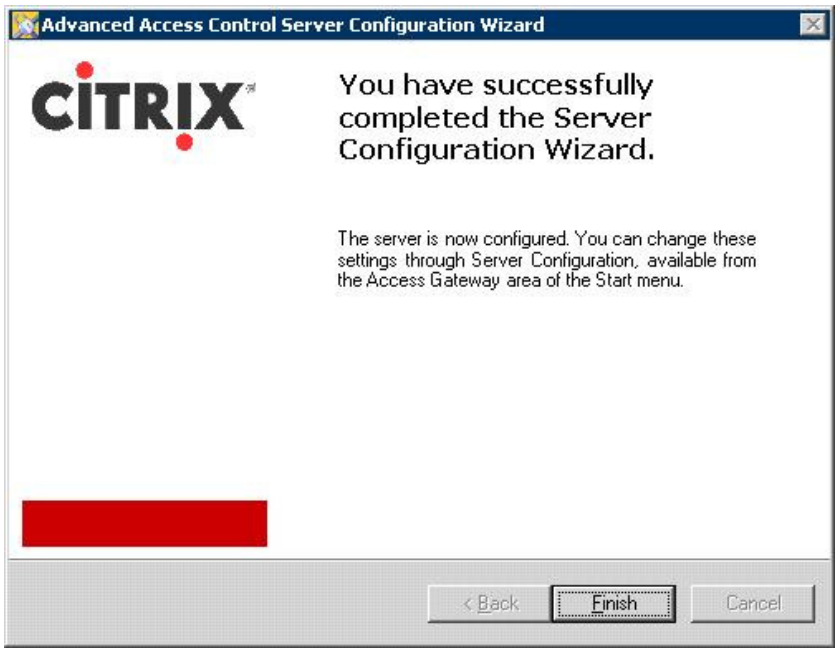
Web-palvelua varten valitaan vakiomuotoinen oletussivusto käyttäen porttia 80 http-liikenteelle (kuva 26).



Kuva 26. Oletussivuston asetukset

Tarkistetaan vielä asennusvelhon lopuksi, mitä asetuksia valittiin asennettavaksi (kuva 27). Asennus on mennyt onnistuneesti läpi (kuva 28).

Kuva 27. Palvelimen konfiguroinnin yhteenveto



Kuva 28. Asennus on valmis

7.4 Citrix Access Suite Console -hallintakonsolin asennus

Citrix Access Suite Console -hallintatyökalulla konfiguroidaan ja hallinnoidaan Citrix Advanced Access Control -ohjelmiston eri komponentteja. Se toimii Microsoft Management Console -ympäristössä, johon voidaan asentaa ns. snap-in eli ohjelmalisäke. Citrix Advanced Access Control -ohjelmiston mukana tuleva Citrix Access Suite Console on muokattu ohjelmalisäke. Lisäksi on mahdollista muokata juuri tarkoituksiin sopiva hallintakonsoli useista eri ohjelmalisäkkeistä kuten Microsoft SQL Enterprise Manager yhdessä Citrix Access Suite Consolen kanssa.

Hallintatyökalu voidaan asentaa joko Citrix Advanced Access Control -palvelimelle tai erilliselle palvelimelle, joissa on jo valmiiksi asennettuina Microsoft Windows 2000 Server Service Pcak 4 tai uudempi käyttöjärjestelmä sekä lisäksi. .NET Framework 1.1 SP1 ja Microsoft Data Access Components (MDAC) versio 2.7.

Asennusvelho käynnistetään Citrix Advanced Access Control Server CD:ltä, josta valitaan Product Installations- ja Citrix Advanced Access Control -kuvakkeet. Lisenssisopimuksen hyväksymisen jälkeen valitaan asennettavaksi komponentiksi vain Management Console ja asennusvelho suorittaa asennuksen automaattisesti loppuun.

7.5 Citrix Access Gateway Administration Tool - asennus

Jo aiemmin järjestelmänvalvojan päätelaitteelle asennettu Citrix Access Gateway Administration -hallintatyökalu voidaan asentaa myös Citrix Advanced Access Control -palvelimelle, jotta Citrix Access Gateway -järjestelmän kaikki hallintatyökalut sijaitsevat samalla palvelimella. Ohjeet tämän hallintatyökalun asentamiseen löytyvät kappaleesta 5 ”Citrix Access Gateway -aktiivilaitteen asennus”.

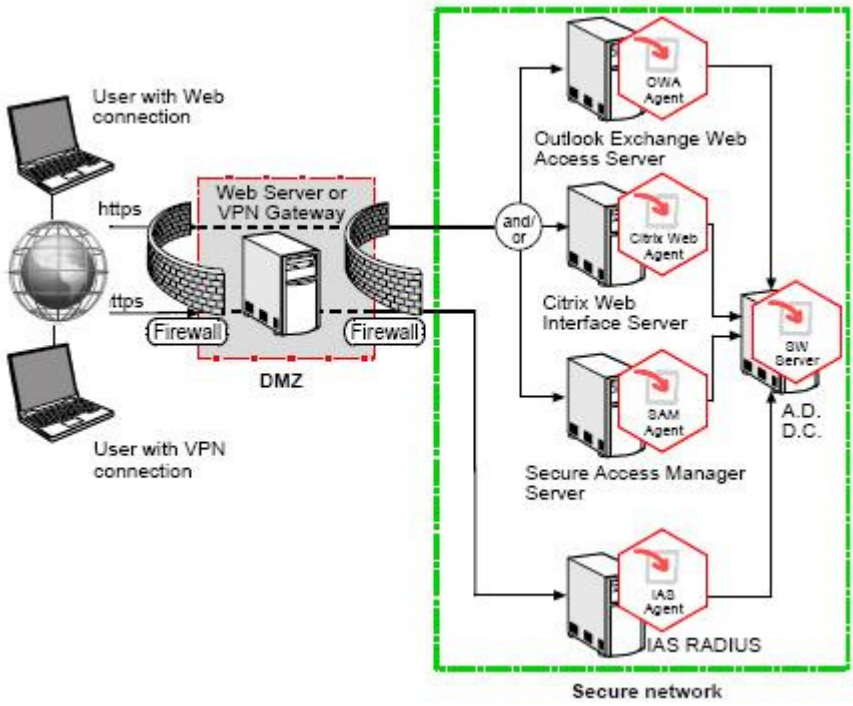
8 SafeWord For Citrix -autentikointijärjestelmä

SafeWord for Citrix (jäljempänä SafeWord) on yhdysvaltalaisen Secure Computing -yrityksen yksi useista tietoturvaan liittyvistä tuotteista. SafeWord-ohjelmisto tuo lisäturvaa Windows-pohjaisille alustoille tarjoamalla vahvan autentikoinnin käyttäjille heidän käyttäessään VPN-yhteyksiä, selainpohjaista Outlook Web Accessia, Radiukseen perustuvia tekniikoita ja Citrix-ohjelmistoja. Jokaisella käyttäjällä on oma SafeWord-toukka, josta saadaan jokaista järjestelmään kirjautumista varten uusi numero/kirjain-salakoodi. Tämä varmistetaan SafeWord-palvelimella, joka tuntee juuri tietyn käyttäjän salakoodin käyvän vain omaan palvelimelle rekisteröityyn toukkaan. Näin ollen toukan varastaminen, kopioiminen tai salasanojen uudelleenkäyttö tulee rikollisille hyödyttömäksi.

Safeword on helposti integroitavissa Citrix-tuotteiden ja Microsoft Active Directory -hakemistopalvelun kanssa, joten sen ylläpito on vaivatonta ja käyttäjien pääsy verkon resursseihin on helppoa.

8.1 Komponentit ja niiden toiminnot

SafeWord-ohjelmiston ydinkomponentit koostuvat kolmesta osasta eli SafeWord Server, SafeWord Management Console (jäljempänä SMC) ja Auto Updater. Näiden lisäksi on valittavissa käyttötarpeen ja -kohteen mukaisesti lisäkomponentteja (agentteja) kuten Internet Authentication Service (IAS) Agent, SafeWord Agent for Citrix Web Interface (käytetään Citrix MetaFrame Presentation Server -ympäristössä), Secure Access Manager (SAM) Agent sekä Outlook Web Access (OWA) Agent. Kuvassa 29 on demonstroitu yhtä mahdollista tietojärjestelmäskenaariota. (SafeWord product guide 2006: 3)



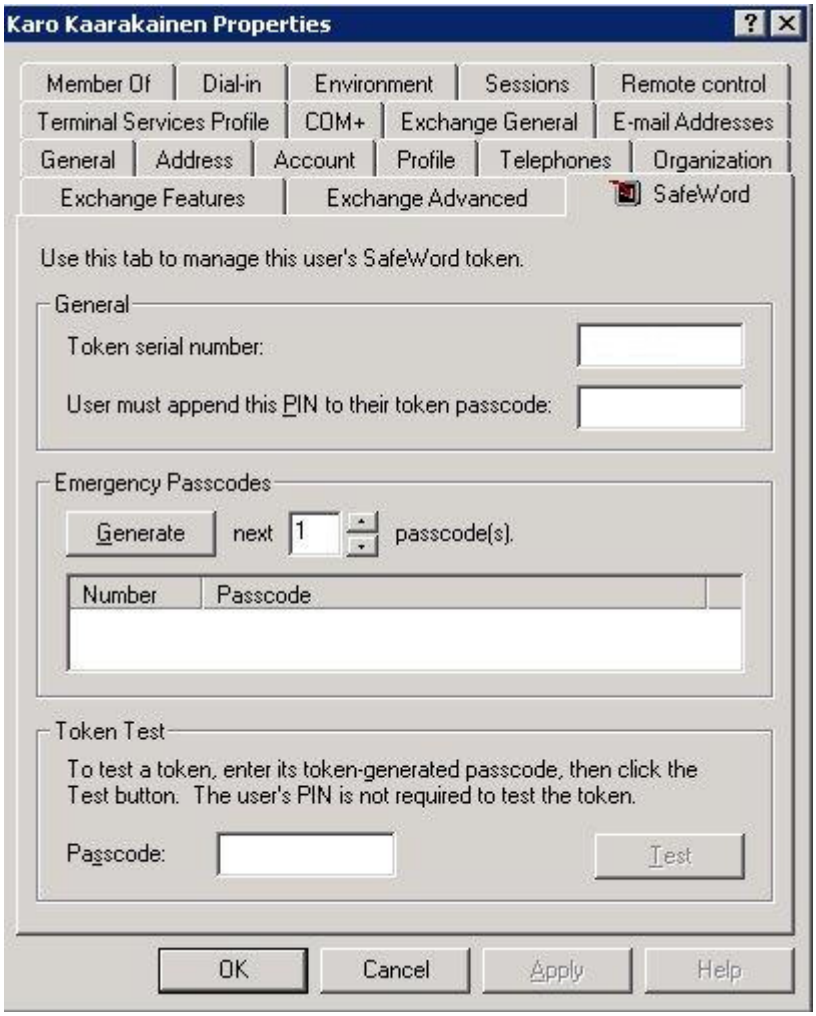
Kuva 29. SafeWord-autentikointipalvelun implementointi (SafeWord product guide 2006: 3)

Safeword Server koostuu neljästä eri osakomponentista. SafeWord database -kantaan talletetaan tiedot käyttäjille rekisteröidyistä toukista. Authentication Engine varmentaa vaihtuvan salasanan kirjautumisen yhteydessä, että kuuluuko se kirjautuvalle käyttäjälle. Administration Service on käytössä aina, kun järjestelmänvalvoja tai loppukäyttäjä tekee järjestelmään muutoksia käyttäen SMC:tä tai User Center -käyttöliittymää.

User Centerin (kuva 30) tarkoituksena on nimensä mukaisesti tarjota loppukäyttäjille helppokäyttöinen selainpohjainen käyttöliittymä, jossa he pystyvät itse aktivoimaan toukkansa ilman järjestelmänvalvojien apua. Loppukäyttäjän on myös mahdollista liittää toukkaansa pin-koodi, synkronoida uudelleen toukkansa sekä testata sen toimivuutta aktivoinnin jälkeen. (Safeword product guide 2006:4)

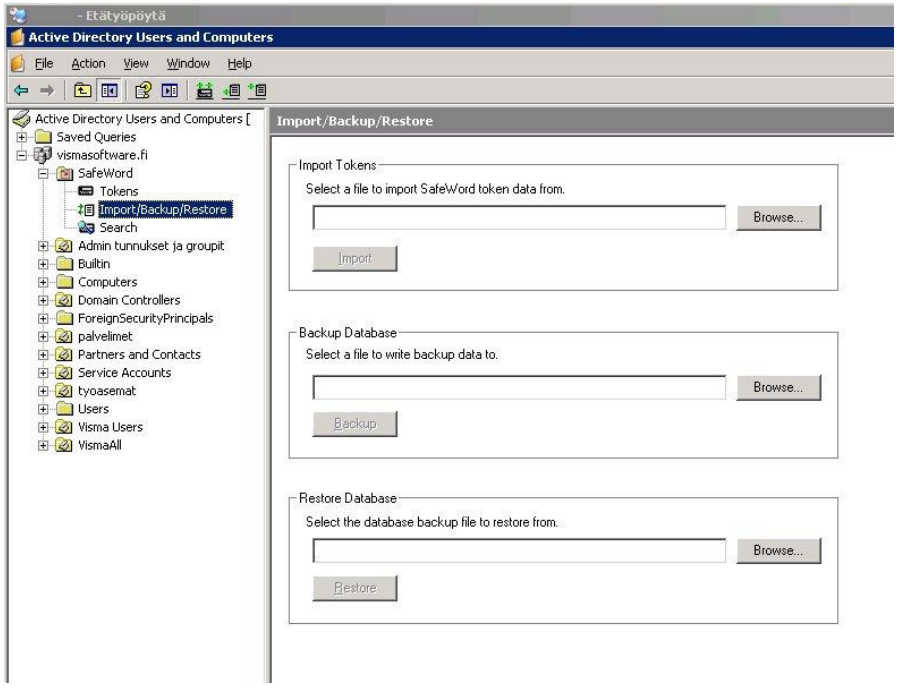
Kuva 30. User Center -portaali

SMC:lla hallitaan käyttäjiä Active Directory Users and Computers -hallintatyökalun (kuva 31) kautta kahdella eri osalla. Käyttäjähallintaikkunan SafeWord-välilehdellä järjestelmänvalvoja voi myös liittää käyttäjälle tietyn toukan, lisätä siihen pin-koodin, generoida varalta salasanoja ja myös testata liitetyn toukan toimivuutta.



Kuva 31. Hallintatyökalun SafeWord-lisäosa

Samassa hallintatyökalussa on myös vasemman ikkunan puuhierarkiassa SafeWord-komponentissa (kuva 32) kohta ”tokens”, josta voidaan listata toukat, etsiä tietyn käyttäjän ja toukan liitosta sekä tuoda uusia toukkaluetteloja järjestelmään. Lisäksi varmuuskopiointi ja palauttaminen onnistuvat samoin helposti.



Kuva 32. SafeWord-hallintakonsoli

Auto Updater -palvelun avulla SafeWord-ohjelmisto kaikkialla järjestelmässä päivittyy automaattisesti, kun uusia ominaisuuksia ja päivityksiä tulee saataville. Päivityksistä tulee ilmoitus, jos järjestelmän joku osa on vanhempaa versiota. Auto Updater käynnistyy aina, kun SMC käynnistetään. Muiden SafeWord-komponenttien osalta päivitys voidaan tehdä manuaalisesti, jolloin järjestelmänvalvoja voi itse valita, mitä päivityksiä asennetaan. (Safeword product guide 2006:6)

Safeword IAS Agent toimii Microsoftin IAS-palvelun (Internet Authentication Service) kanssa, jota käytetään erilaisten autentikointitapojen yhteydessä kuten RADIUS, IPSec VPN ja SSL VPN. Siten käyttäjien on mahdollista päästä verkon resursseihin käsiksi vain autentikoitumalla SafeWord-toukasta saatavalla salasanalla vakiotunnusten lisäksi. (Safeword product guide 2006:6)

Safeword Agent for Web interface -agenttia käytetään sillä Citrix-palvelimella, jossa itse Web interface on asennettuna ja jos-

ta on yhteys SafeWord palvelimelle. Agentti ”sieppaa” jokaisen pyynnön päästä verkkoon ja ohjaa ne edelleen Authentication Engine -komponentille käyttäjän ja salasanan varmennusta varten. Kun käyttäjä on autentikoitu hyväksytysti, pääsy sallitaan ja muussa tapauksessa kielletään. (Safeword product guide 2006:6)

Secure Access Manager (SAM) Agent käyttää hyväkseen SafeWordin hallintatyökaluja ja asentuu suoraan Citrix Secure Access Manager -komponentin päälle. SAM Agent lisää myös tähän komponenttiin vahvan autentikoinnin. SafeWord OWA Agent toimii yhdessä Microsoft Exchange Serverin kanssa, jotta käyttäjän kirjautuessa Outlook Web Accessiin tarvitaan normaalien Windows-tunnusten lisäksi vaihtuva salasana SafeWord toukasta. (Safeword product guide 2006:7)

8.2 Järjestelmävaatimukset

Ennen autentikointipalvelimen asennusta ohjauspalvelimelle käydään läpi ensimmäiseksi toiminnalliset perusedellytykset sekä järjestelmävaatimukset (Safeword product guide 2006:10-11):

Perusedellytykset:

- Windows 2000/2003 ohjauspalvelin
- Active Directory
- Citrix-järjestelmä: Citrix MetaFrame Presentation Server, Web Interface, Secure Access Manager tai Citrix Access Gateway -järjestelmä
- Internet-yhteys

Järjestelmävaatimukset:

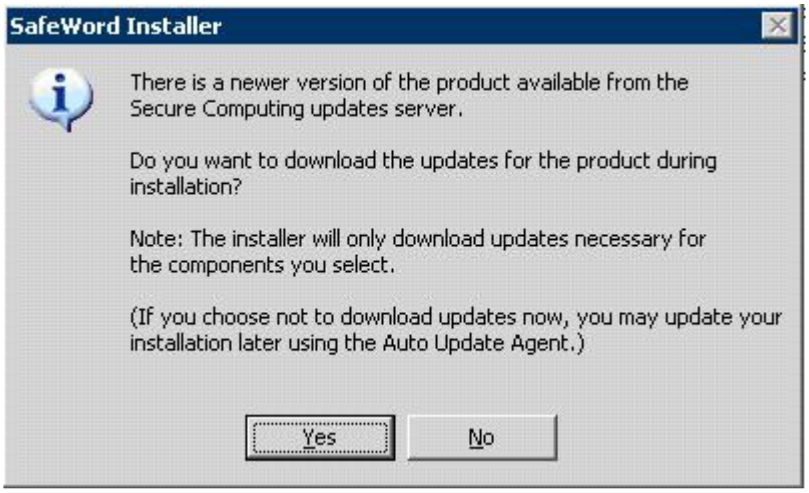
- Prosessori Intel Pentium 3 (550mhz tai parempi)
- Käyttöjärjestelmä Windows 2000/2003 Server viimeisimmällä korjauspaketillla
- Muistia 256 MB, 512 MB suositeltava
- Kovalevytilaa 300 MB, 2 GB suositeltava

Kaikki edellytykset asennukselle ovat siis olemassa, kun suositellut arvot ylittyvät. Seuraavaksi asennetaan autentikointipalvelu toimialueen ohjauspalvelimelle.

8.3 Autentikointipalvelun asennus ja konfigurointi ohjauspalvelimelle

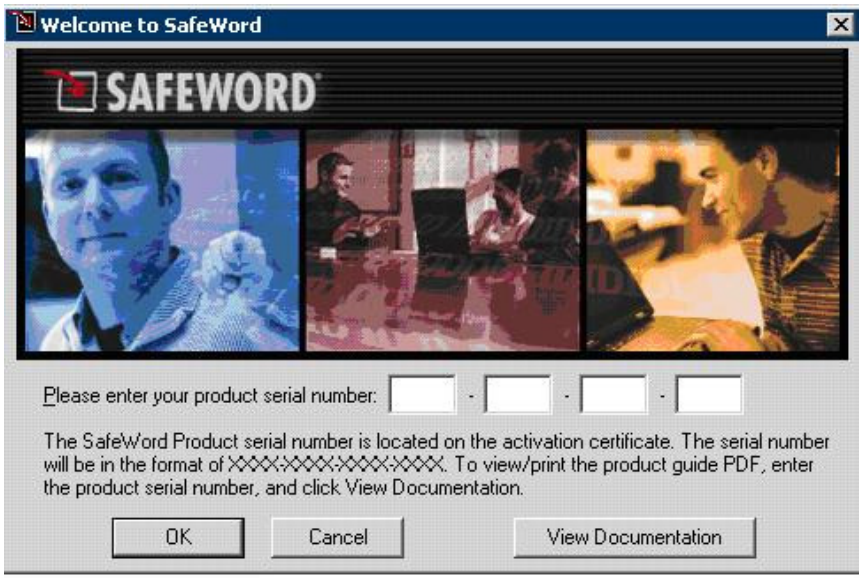
Autentikointipalvelu asennetaan ohjauspalvelimelle Jyväskylän palvelinkeskukseen. Kun edellisessä alaluvussa kerrotut vaatimukset varsinaiselle asennukselle ovat olemassa, voidaan asennus palvelimelle aloittaa ohjelmiston CD-ROM-levyltä.

Heti asennuksen käynnistyttyä työpöydälle ilmestyy CD-ROM-levyllä olevien asennustiedostojen päivityksestä ilmoittava ruutu (kuva 33) ennen kuin itse ohjelmisto asennetaan. Ladattavan päivitystiedoston koko riippuu asennettavan ohjelmiston versiosta.



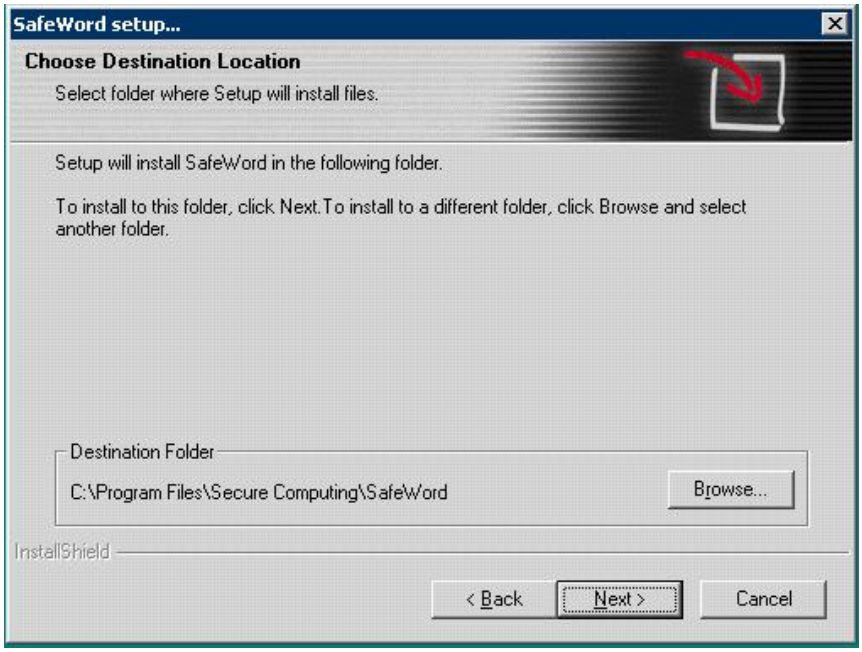
Kuva 33. Ohjelmiston päivittäminen

Kun päivityspaketti on ladattu, asennusvelho pyytää syöttämään ohjelmiston lisenssiavaimen (kuva 34). Lisenssiavain sijaitsee CD-ROM-levyn mukana tulleessa lehtisessä. (Safeword product guide 2006:13)



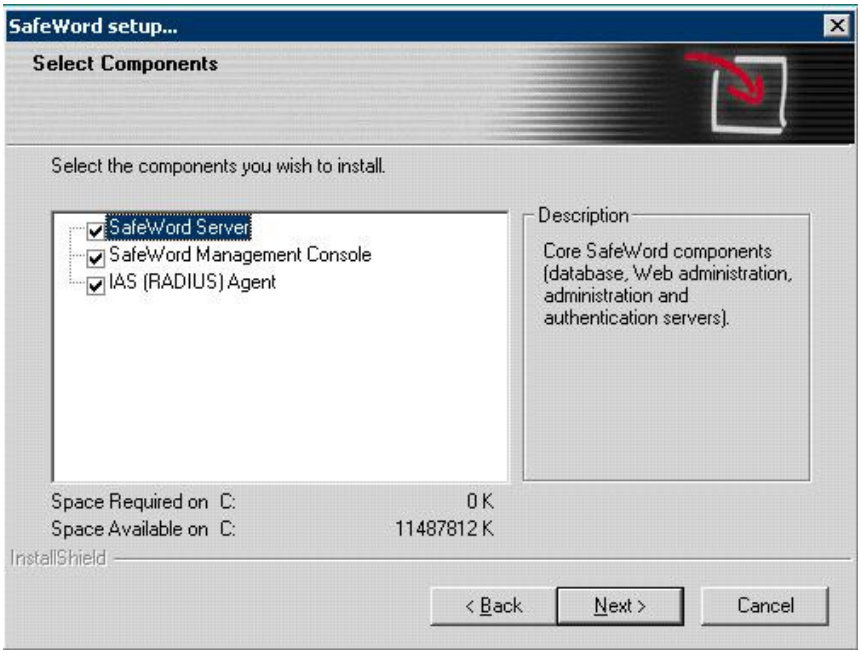
Kuva 34. Lisenssiavaimen syöttäminen

Kun oikea lisenssiavain on syötetty ja hyväksytty, käynnistyy varsinainen ohjelmiston komponentit asentava asennusvelho. Tervetuloa-ikkunasta sekä käyttöoikeussopimuksen hyväksymisestä mennään eteenpäin painamalla seuraava, jolloin seuraavassa ikkunassa valitaan asennuspolku (kuva 35). Asennusvelhon määrittelemä oletuspolku käy hyvin, joten painetaan seuraava. (Safeword product guide 2006:13)



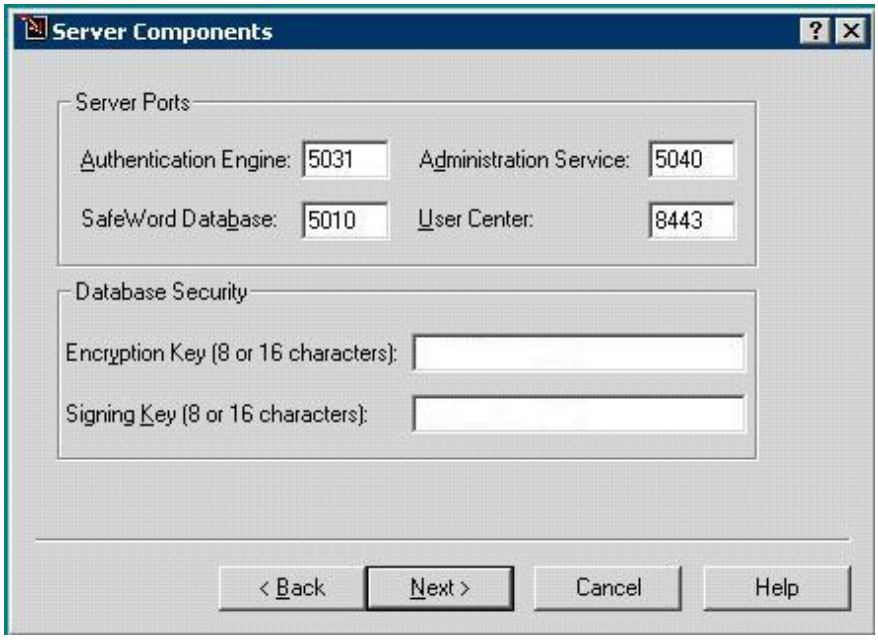
Kuva 35. Asennuspolku

Autentikointipalvelun asentamiseen tarvitaan SafeWord-palvelinosa, sen hallintatyökalu sekä autentikointia varten IAS-agentti (kuva 36). Painamalla seuraava päästään ohjelmistokansion valintaan, joka voidaan jättää vakioksi. Tämän jälkeen painetaan vielä kerran seuraava, jolloin asennusvelho asentaa ohjelmiston automaattisesti valittujen toimenpiteiden pohjalta. (Safeword product guide 2006:13)



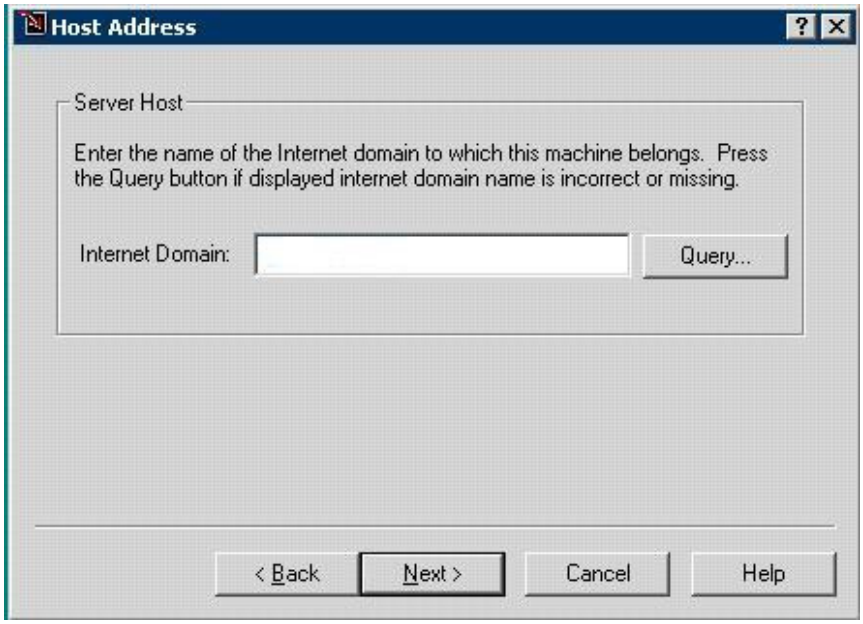
Kuva 36. Asennettavat ohjelmistokomponentit

Kun asennusvelho on valmis, käynnistyy SafeWord-palvelinosan konfigurointi hallinnointia varten. Ensimmäiseksi määritellään palvelimen käyttämät portit (kuvassa 37 vakioportit) autentikointimoottoriin, hallintapalveluun, SafeWord-tietokantaan sekä käyttäjille mahdollistettuun User Center-sivustoon. Lisäksi määritellään haluttu salausavain sekä allekirjoitusavain. (Safeword product guide 2006:16)



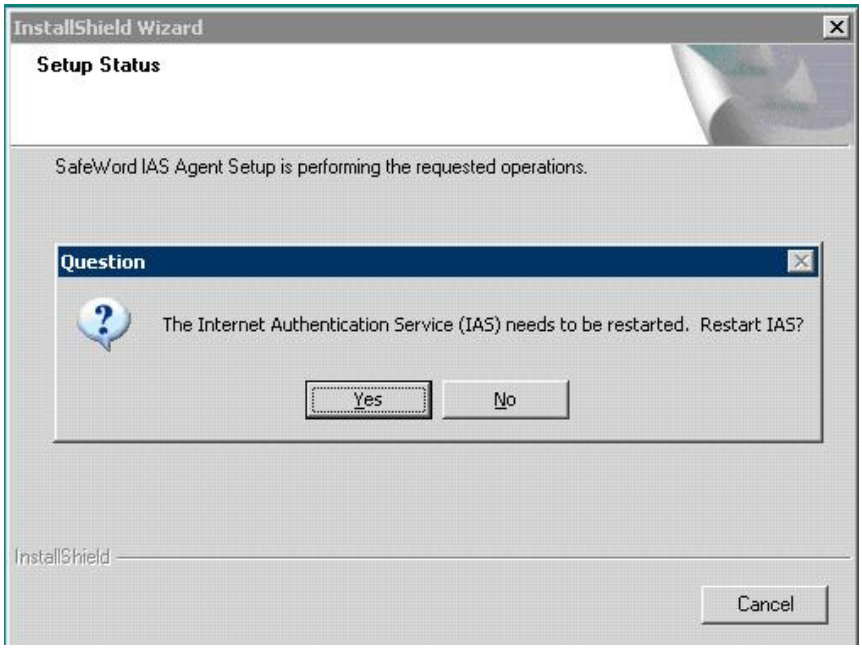
Kuva 37. Porttien määritykset

Painetaan seuraava, jolloin päästään määrittelemään toimialueen nimi isäntäkenttään, jossa vaaditaan FQDN-nimi (kuva 38). (Safeword product guide 2006:17)



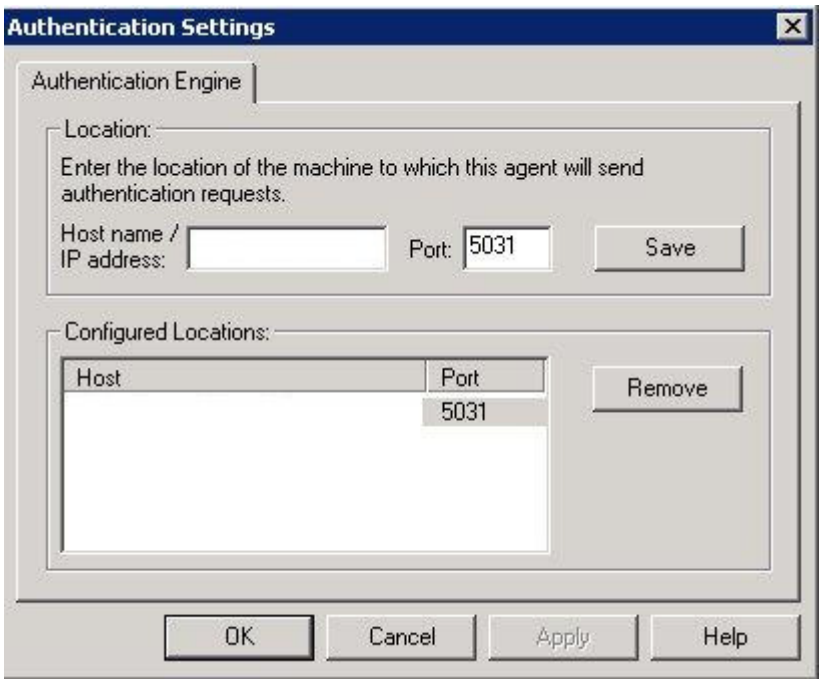
Kuva 38. Toimialue

Lopuksi vielä käynnistetään IAS-palvelu uudestaan, jolloin autentikointipalvelun asennus ohjauspalvelimelle on valmis (kuva 39). (Safeword product guide 2006:17)



Kuva 39. IAS:n uudelleenkäynnistäminen

Ennen SafeWord for Citrix -autentikointijärjestelmän aktivoimista sekä liittämistä käyttäjätileihin Active Directory -hakemistopalvelussa, on Citrix Advanced Access Control -palvelimelle asennettava vielä SafeWord Secure Access Manager -agentti, joka vastaa autentikointiliikenteestä varsinaiselle autentikointipalvelimelle. Välitetyn liikenteen datan perusteella tarkistetaan, että tietty toukka on rekisteröity juuri tietylle käyttäjälle. Asennus tehdään samalta CD-ROM-levyltä, josta autentikointipalvelukin asennettiin ohjauspalvelimelle. SafeWord Secure Access Manager -agentin konfiguroinnissa määritellään hallintapalvelimen FQDN-osoite sekä käytetty portti 5031, jotta yhteys autentikointimoottoriin saadaan toimimaan (kuva 40). (Safeword product guide 2006:43,49)

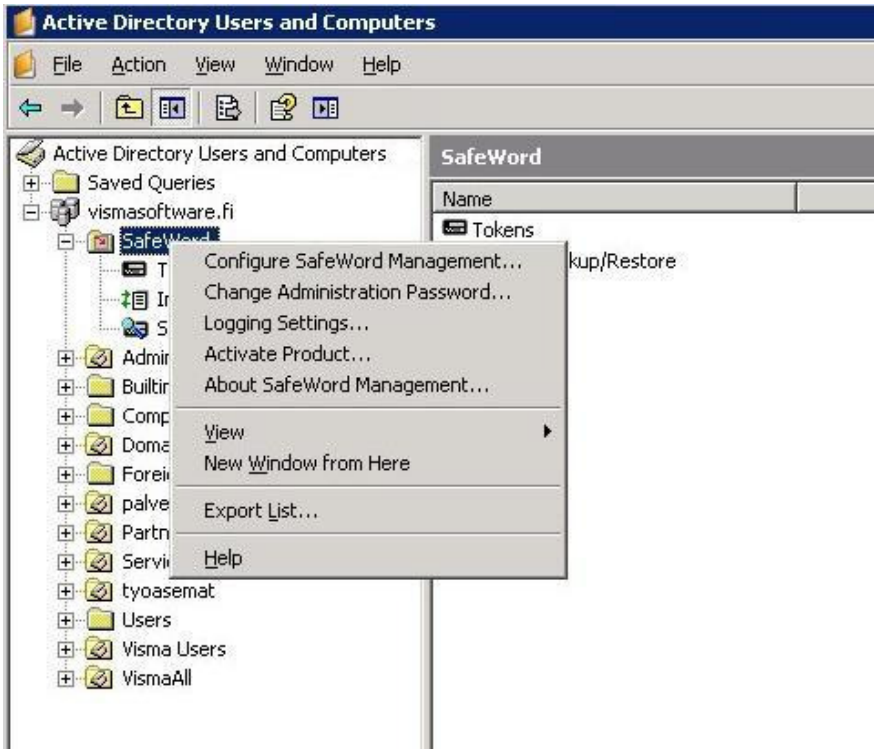


Kuva 40. Autentikointipalvelimen asetukset

SafeWord-autentikointijärjestelmä täytyy aktivoida ja rekisteröidä, jotta sen kaikki ominaisuudet saadaan käyttöön. Ohjelmiston sekä toukkien lisenssikoodit löytyvät ohjelmiston mukana tulleesta aktivointisertifikaatista, josta ohjelmiston lisenssikoodin tunnistaa 16-merkkisestä koodista alkaen kirjaimilla ”RAxx xxxx xxxx xxxx” ja toukkakirjaston vastaavan alkaen kirjaimilla ”TKxx xxxx xxxx xxxx”.

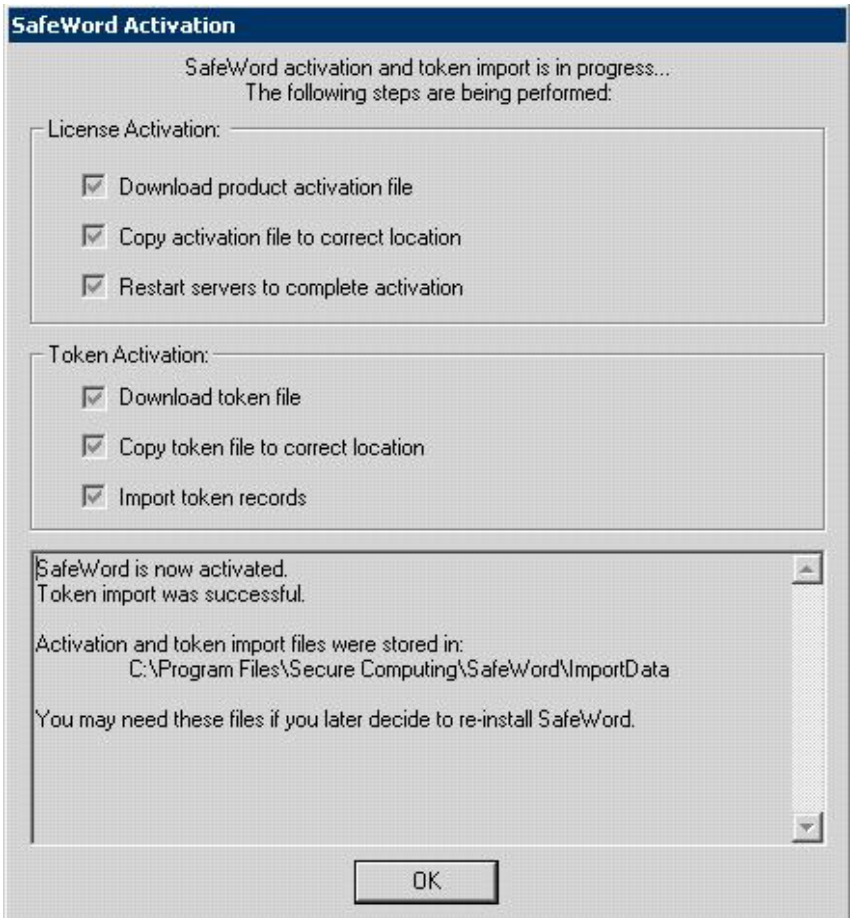
Aktivointi tehdään käyttäen SafeWord Management Console -hallintatyökalua. Hallintatyökalua varten käynnistetään ohjauspalvelimella Active Directory Users and Computers antamalla komentokehotteessa käsky dsa.msc. Tässä työkalussa näkyy nyt tavallisen puuhierarkian lisäksi myös SafeWord-kansio, joka

itse asiassa on SafeWord Management -hallintatyökalu. Ensimmäistä kertaa hallintatyökalua käynnistettäessä on vaihdettava järjestelmänvalvojan salasana. Sen jälkeen kansiota hiiren oikealla klikkaamalla saadaan esiin valikko, josta käynnistetään ohjelmiston aktivointi valitsemalla Activate Product (kuva 41). (Safeword product guide 2006:21)



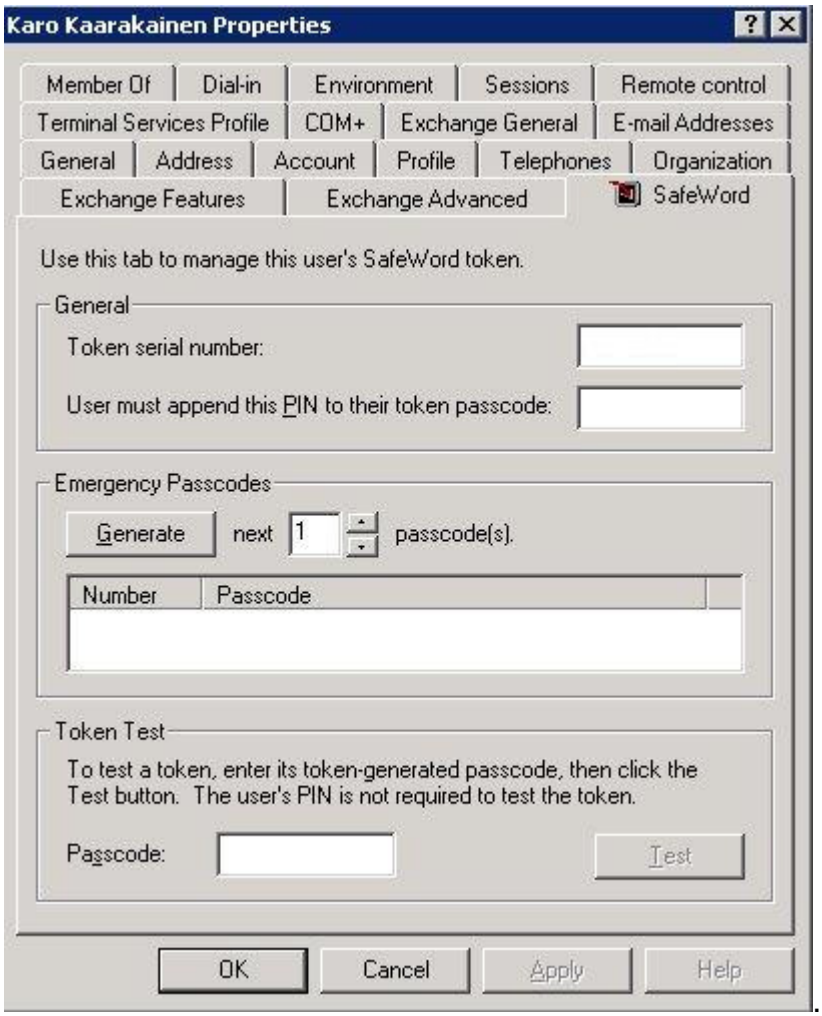
Kuva 41. Ohjelmiston aktivointi

Näin ollen saadaan auki www-lomake, johon täytetään tarvittavat tiedot lisenssikoodeista sekä muut yritystä koskevat tiedot. Kaiken ollessa kohdallaan ja varmasti oikein, painetaan lähetänappia, jolloin tiedot välittyvät Secure Computing -yrityksen aktivointipalvelimelle, jossa tiedot tarkastetaan. Kun tiedot on tarkastettu, latautuu samaiselta palvelimelta lisenssiavain sekä toukkien datatiedosto automaattisesti oikean asennuskansioon palvelimelle (kuva 42). Näistä tiedostoista otetaan samalla varmuuskopio, jotta palvelinrikon sattuessa voidaan sekä ohjelmisto että toukat aktivoida uudelleen paikallisesti. (Safeword product guide 2006:21)



Kuva 42. Aktivoinnin WWW-lomake

Ohjelmiston aktivointi on valmis, joten toukkien liittäminen käyttäjätunnuksiin voidaan aloittaa ja siten jaella toukat käyttäjille. Toukkien liittäminen käyttäjätunnukseen tehdään avaamalla Active Directory Users and Computers -työkalu, jossa haluttujen käyttäjien ominaisuuksissa valitaan SafeWord-välilehti. Tällä välilehdellä liitetään tietyssä toukassa oleva yksilöllinen sarjanumero sille varattuun kenttään ja painetaan ok (kuva 43) (Safeword product guide 2006:28-29)



Kuva 43. Toukkien sarjanumeron lisääminen

Kun toukkien liittämiset käyttäjätunnuksiin on tehty, toimii SafeWord-autentikointi uuteen Citrix Access Gateway -järjestelmään kirjauduttaessa.

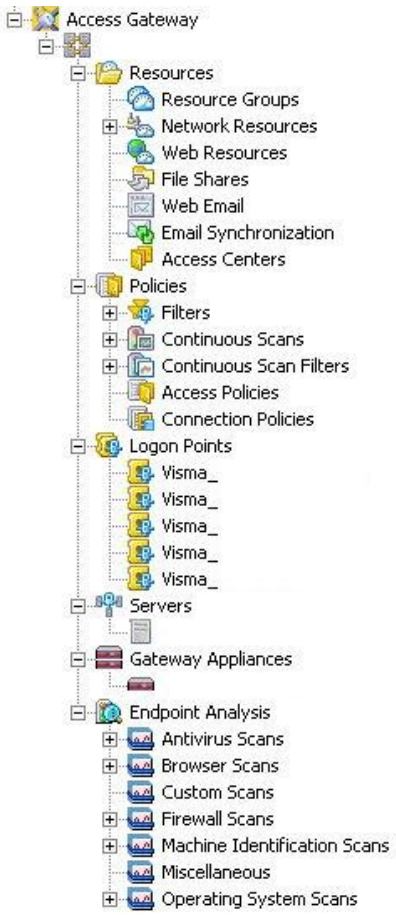
9 Citrix Advanced Access Control – konfigurointi

Citrix Access Gateway -järjestelmän käyttöönottoa varten tarvitaan vielä Citrix Advanced Access Control -ohjelmiston konfigurointi käyttäen Citrix Access Suite -hallintakonsolia. Aiemmin tässä opinnäytetyössä käytiin läpi Visma Software Oyj:n verkkoinfrastruktuuri, johon ensin asennettiin laitteisto eli Citrix Access Gateway -laite ja konfiguroitiin se käyttäen Citrix Access Gateway Administration -hallintatyökalua. Seuraavaksi asennettiin Citrix Advanced Access Control -ohjelmisto järjestelmän hallinnointiin ja konfigurointiin sekä SafeWord for Citrix -autentikointijärjestelmä parantamaan tietoturvaa järjestelmään kirjauduttaessa. Viimeinen vaihe uuden SSL VPN -järjestelmän asennuksessa ja käyttöönotossa on muun muassa pääsy- ja yhteyspolitiikkojen, kirjautumispisteiden (logon point), verkkoresurssien sekä Endpoint Analysis -skannauksien määrittelyt Citrix Advanced Access Control -ohjelmistoon käyttäen Citrix Access Suite -hallintakonsolia Citrix Advanced Access Control -palvelimella.

9.1 Verkon komponenttien etsintä

Citrix Access Suite -hallintakonsolia käynnistettäessä ensimmäistä kertaa käynnistyy automaattinen etsintä-toiminto, joka etsii kaikki Citrix Access Gateway -järjestelmään liittyvät komponentit sekä hallintapalvelimelta että Citrix Access Gateway -laitteistoista. Aina kun järjestelmään lisätään tai siitä poistetaan komponentteja tai hallintaoikeuksia muutetaan, on etsintä tehtävä manuaalisesti uudestaan, jotta järjestelmänvalvojan käytössä on ajantasainen näkymä verkon komponenteista. (Access Gateway with Advanced Access Control Administrator´s Guide 2005: 66)

Aiemmin luodun palvelinfarmin lisäksi hallintakonsolin puuhierarkiassa näkyy etsintä-toiminnon jälkeen useita eri komponentteja. Puuhierarkia koostuu seuraavista komponenteista: resurssit, politiikat, kirjautumispisteet, palvelimet, Access Gateway -laitteet sekä Endpoint Analysis -skannauskomponentit (kuva 44).



Kuva 44. Yleiskuva Citrix Advanced Access Control -ohjelmiston puuhierarkiasta ja komponenteista

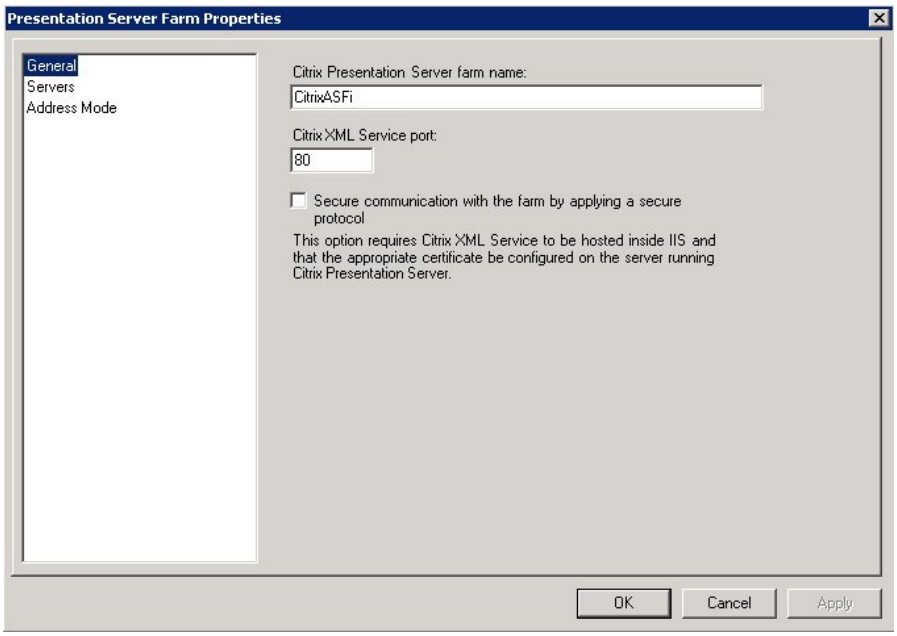
9.2 Citrix MetaFrame Presentation Server -integrointi

Citrix Access Gateway -järjestelmään voidaan liittää olemassa oleva Citrix MetaFrame Presentation Server -järjestelmä. Tällöin kaikki julkaistut resurssit voidaan tarjota käyttäjille Access Center -portaalien kautta joko käyttämällä Web Interface -käyttöliittymää tai tiedostotyyppiassosiointia (file type association). Jälkimmäistä käytettäessä dokumentit avataan tarvittavassa sovelluksessa palvelinpäässä, kunhan menetelmä on sallittu esimerkiksi politiikoilla. (Access Gateway with Advanced Access Control – Administrator´s Guide: 70.) Hyöty tulee esiin

käytettäessä Kiosk Mode –yhteystyyppiä esimerkiksi lentoasemien internetkioskeista, jonne VPN-yhteyden aikana ei tallenneta dataa.

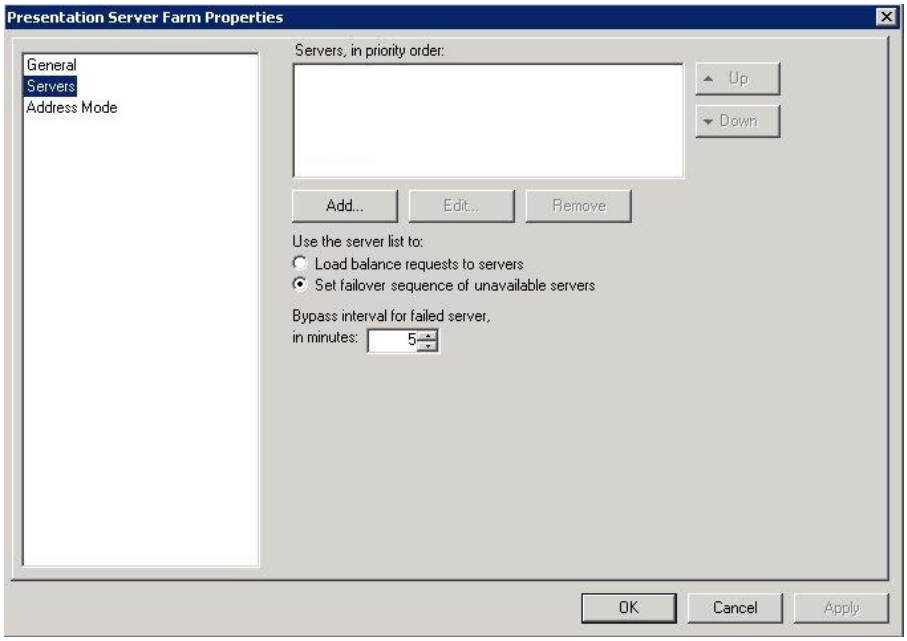
Ennen liittämistä ja konfigurointia varmistetaan, että samoille käyttäjäryhmille kiinnitetyt julkaistut resurssit on myös kiinnitetty resursseihin palvelinfarmissa. Kaikkiin Presentation Server -ympäristössä julkaistuihin resursseihin on myös oltava pääsy Citrix Access Gateway -järjestelmän kautta, joten resurssien ominaisuuksista on kyseinen ominaisuus otettava käyttöön. Lisäksi kaikkien Citrix MetaFrame Presentation Server -farmin palvelinten ominaisuuksissa on mahdollistettava luotettujen pyyntöjen lähettäminen Citrix XML -palveluun. (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 71)

Citrix MetaFrame Presentation Server -farmin liittäminen Citrix Access Gateway -järjestelmään aloitetaan muokkaamalla palvelinfarmin ominaisuuksia. Presentation Server Farms -välilehdeltä valitaan uusi ja annetaan liitettävän Presentation Server -farmin nimi. Samassa yhteydessä olisi myös mahdollista salata linkki järjestelmien välillä (kuva 45).



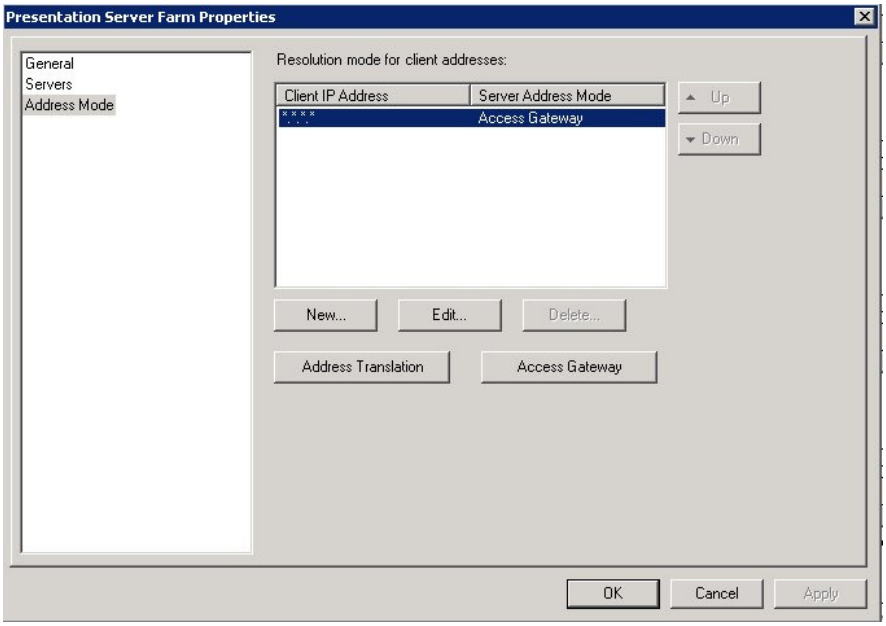
Kuva 45. Citrix MetaFrame Presentation Server -ympäristön asetukset

Seuraavaksi lisätään käytettävien Citrix MetaFrame Presentation Server -farmin palvelimien ip-osoitteet ja otetaan käyttöön ”Failover Sequence Support”, jotta yhteys verkon resursseihin säilyisi katkeamattomana huolimatta jonkun palvelimen kaatumisesta (kuva 46). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 71-72)



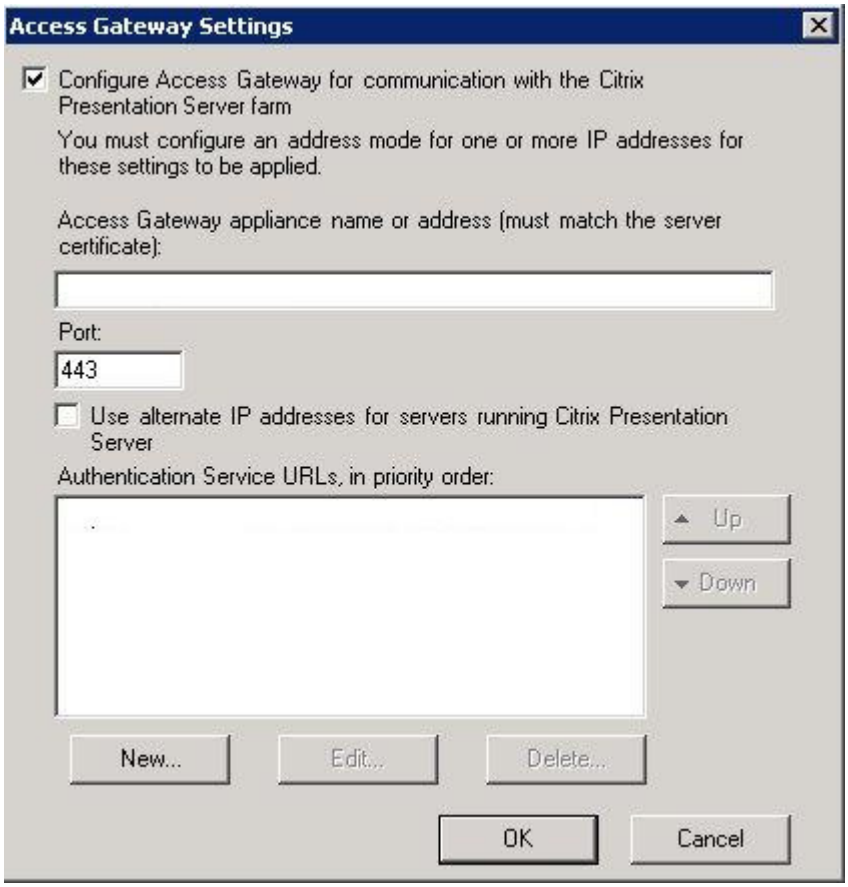
Kuva 46. Citrix MetaFrame Presentation -ympäristön palvelimet

Viimeisenä vaiheena konfiguroidaan vielä address mode -välilehdellä, kuinka järjestelmään yhteyden muodostavalle Secure Access -asiakasohjelmistolle määritetään ip-osoite. Samalla konfiguroidaan uusi osoitemoodi ja valitaan palvelimen osoitemoodiksi Access Gateway ja jätetään ip-osoite tyhjäksi (kuva 47).



Kuva 47. Palvelimen osoitetyyppi

Access Gateway -näppäimen alta määritellään Citrix Access Gateway -laitteiston FQDN-nimi ja portiksi 443. Autentikointipalvelun osoite on jo valmiina sille varatussa kentässä, sillä konfigurointi tehdään Citrix Advanced Access Control -palvelimella (kuva 48). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 73)



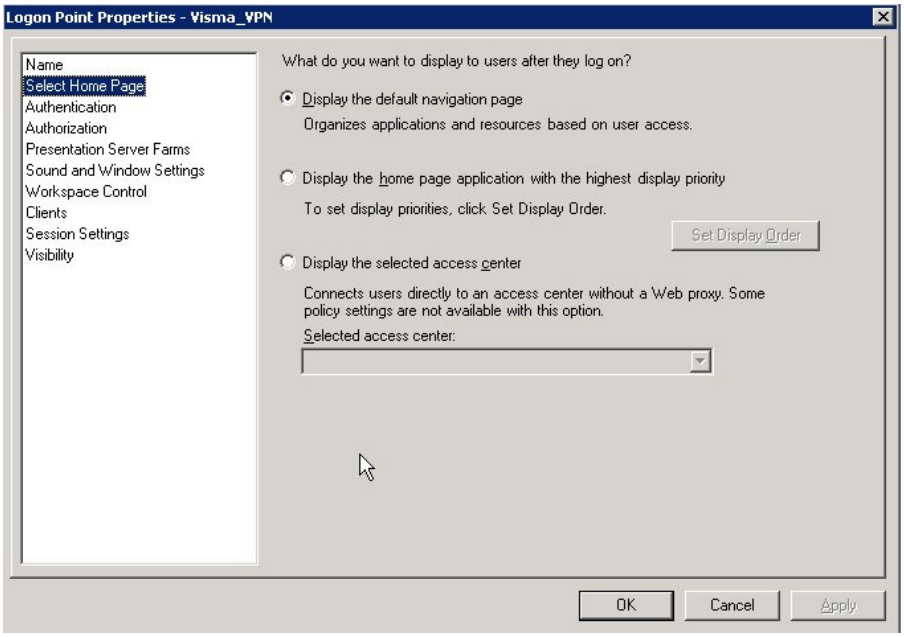
Kuva 48. Citrix Access Gateway -laitteen asetukset

9.3 Logon Point – konfigurointi

Logon Point on järjestelmään kirjautumisen mahdollistava sivusto, johon käyttäjät ensimmäiseksi ottavat yhteyden selaimellaan alkaessaan käyttää järjestelmää. Hallintakonsolin avulla Logon Point -komponenttiin määritellään käytettävä autentikointi, asiakasohjelmistojen käyttö, järjestelmän kotisivun osoite sekä pääsy sallittuihin palvelinfarmeihin. Logon Point -kirjautumispisteitä voidaan luoda eri laitteille ja käyttäjille sen mukaan, mitä resursseja halutaan niille sallia.

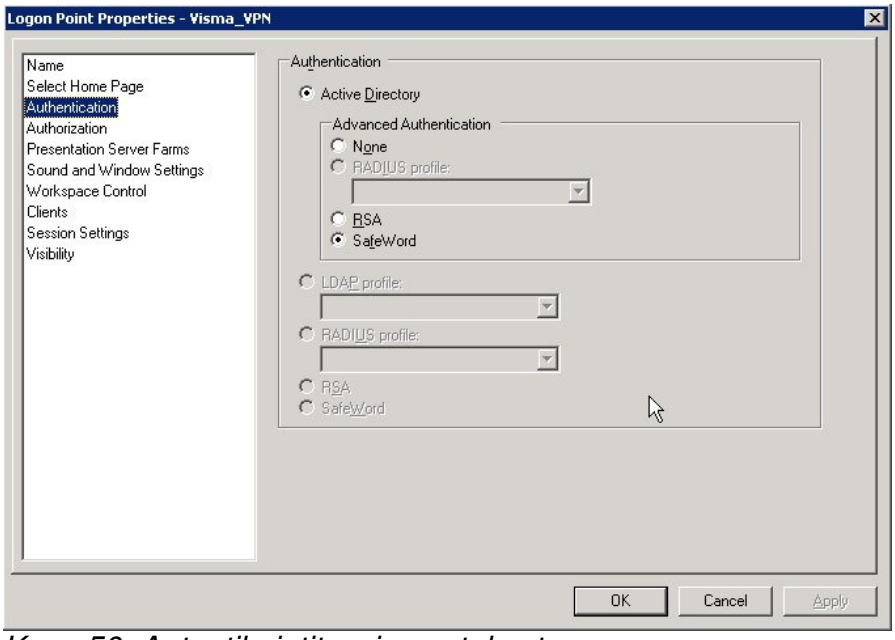
Uusi Logon Point luodaan valitsemalla Logon Points -komponentin kohdalla hallintakonsolissa ”Create logon point”, jolle

kannattaa antaa kuvaava nimi sekä tarkempi lisäselvennys vielä kuvaukseen. Kotisivuksi valitaan vakio navigointisivusto, vaikka itse sivusto konfiguroidaan sulkemaan itsensä automaattisesti kun VPN-yhteys on avattu (kuva 49). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 75-76)



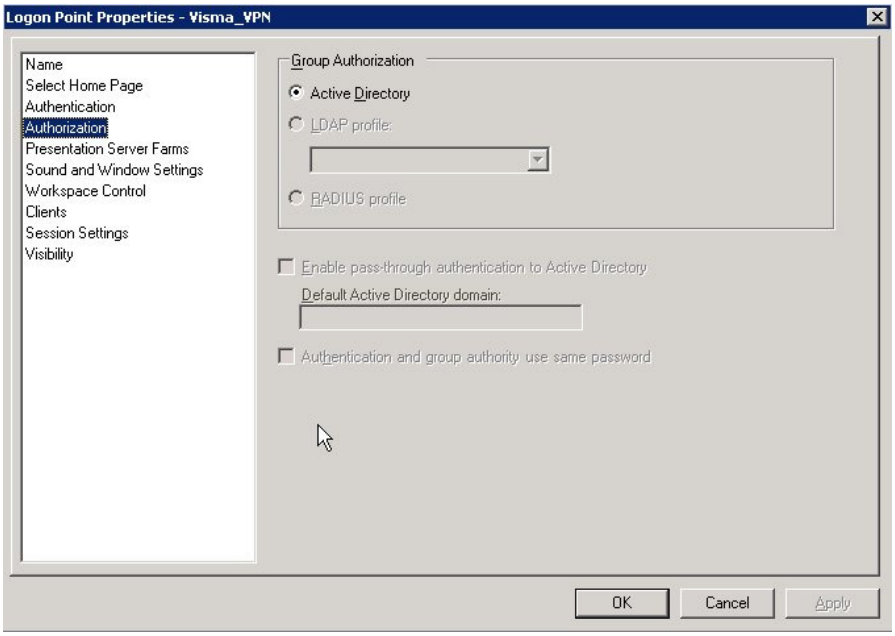
Kuva 49. Logon Point -sivuston kotisivun asetukset

Autentikointi-välilehdellä valitaan käytettäväksi LDAP-autentikointi, johon liitetään tietoturvaa parantava SafeWord for Citrix -autentikointijärjestelmä (kuva 50). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 75-76)



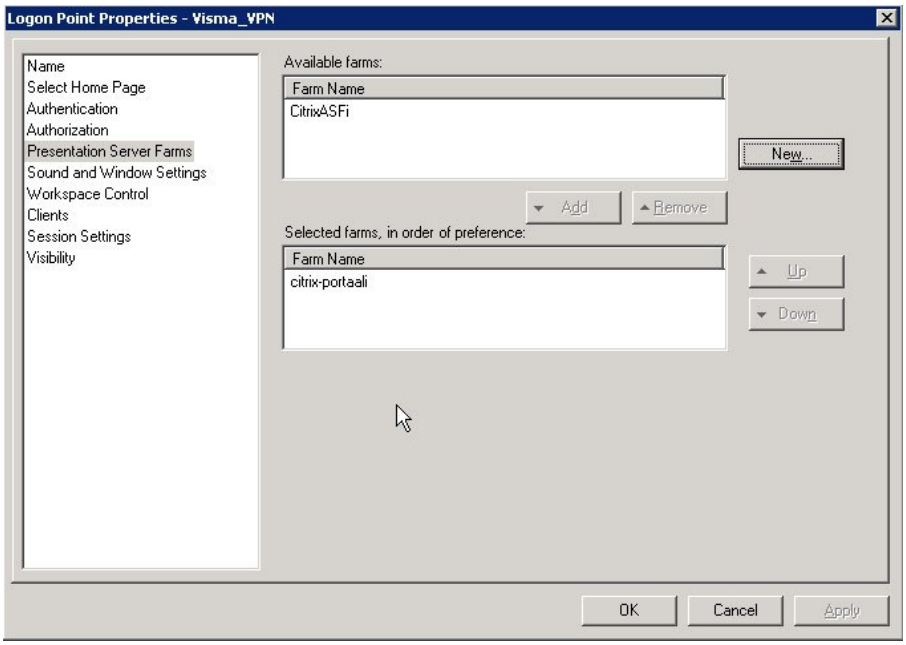
Kuva 50. Autentikointityypin asetukset

Autorisointina käytetään myös LDAP:ia (kuva 51).



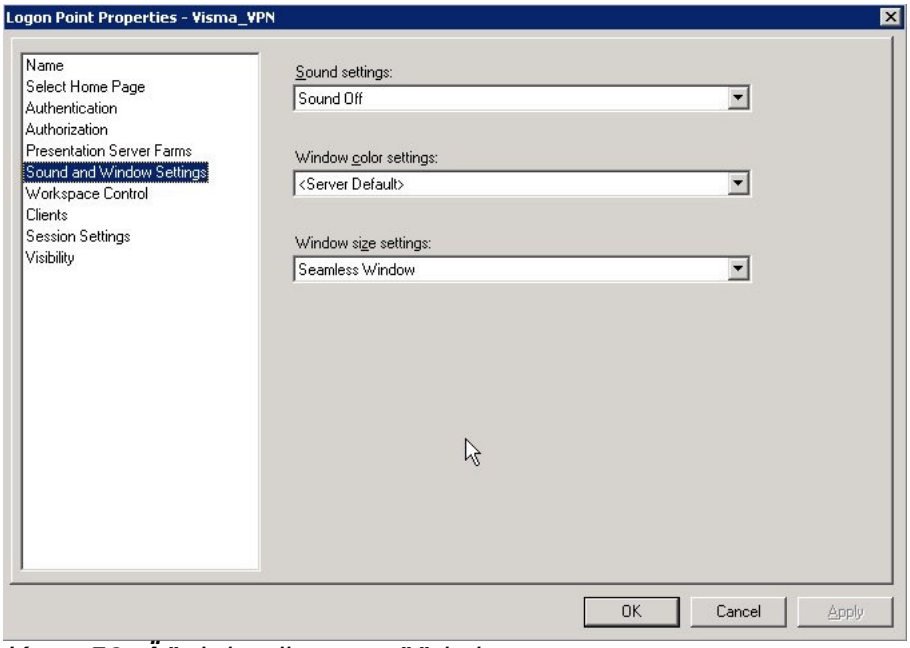
Kuva 51. LDAP-autorisointi

Käytettävä Citrix MetaFrame Presentation Server -farmi lisätään saatavilla olevista farmeista käytettäviin farmeihin (kuva 52). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 75-76)



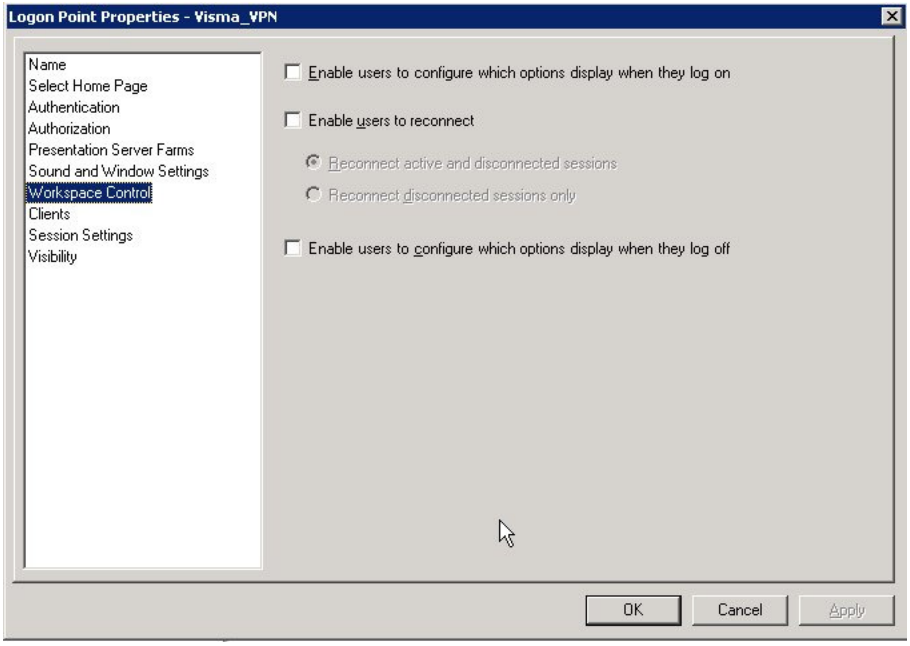
Kuva 52. Käytettävän Citrix MetaFrame Presentation Server -farmin asetukset

Äänen, ikkunan värien ja koon asetuksia voi muuttaa niiden välilehdellä (kuva 53). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 75-76)



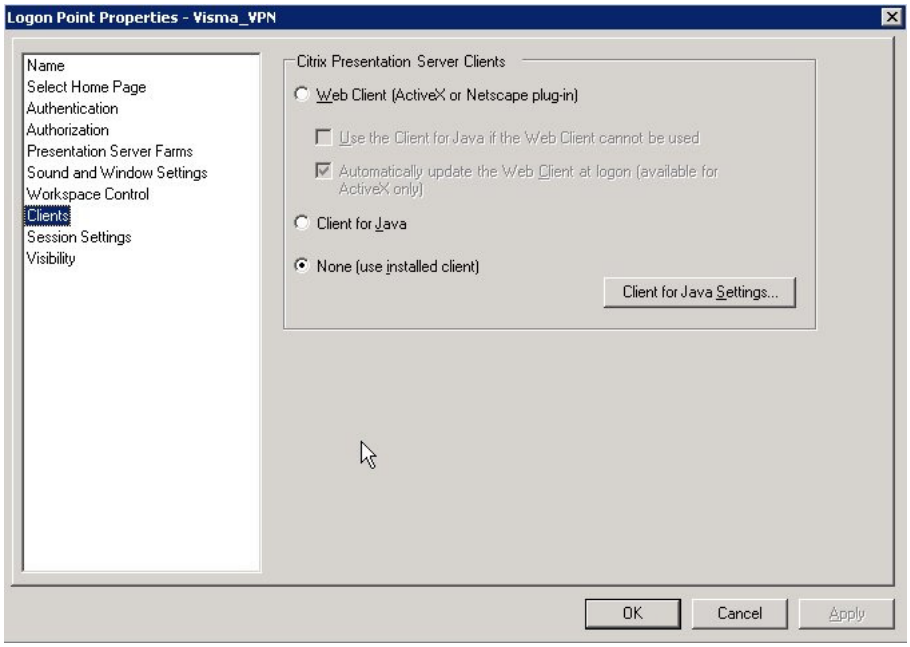
Kuva 53. Ääni- ja ulkoasumääritykset

Käyttäjien työtilan hallinnan asetuksia muokataan Workspace Control -välilehdellä, jossa on asetukset esimerkiksi uuden yhteyden ottamiseen, jos aiempi yhteys katkeaa äkillisesti (kuva 54). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 75-76)



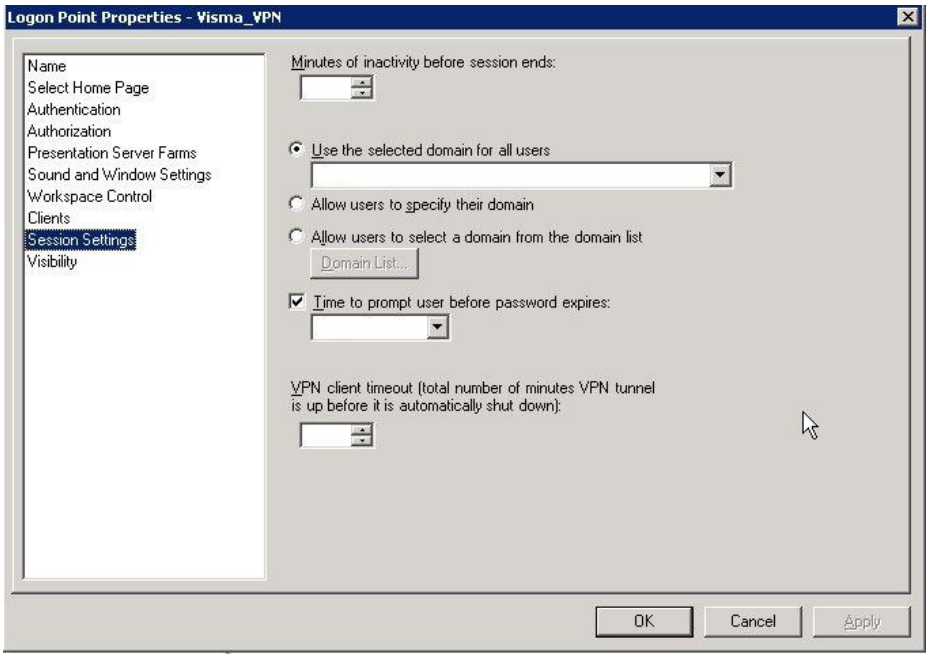
Kuva 54. Työtilan kontrolloinnin asetukset

Käytettävä Secure Access -asiakasohjelmisto asennetaan ensin suoraan sivuston kautta käyttäen ActiveX-komponenttia (kts. luku 9.9 ”Päätelaitteiden ohjelmistojen asennus ja konfigurointi”) ja asennuksen jälkeen konfigurointia muutetaan siten, että kirjautuessa käytetään jo asennettua asiakasohjelmistoa (kuva 55). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 77)



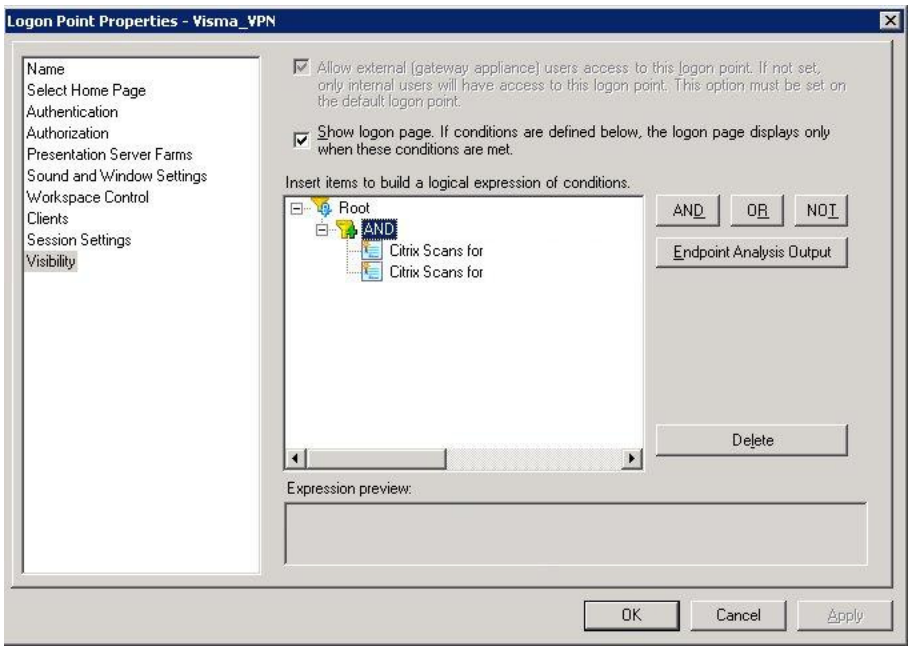
Kuva 55. Käytettävän asiakasohjelmiston asetukset

Yhteyden istunnon asetuksiin muokataan haluttu valmiustilan aika minuutteina, käytettävä toimialue, salasanan vaihdosta ilmoittaminen sekä VPN-yhteyden automaattikatkaisu minuutteina (kuva 56). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 77)



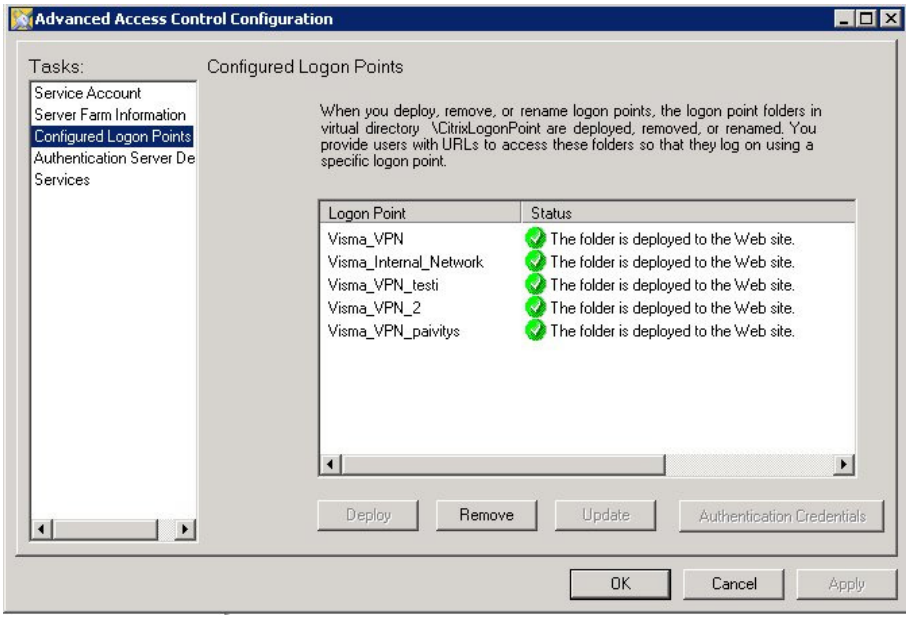
Kuva 56. Istuntokohtaiset määritykset

Logon Point -komponentin konfiguroinnin viimeisessä vaiheessa valitaan käytettävät Endpoint Analysis -skannaukset (kts. luku 6 ”Citrix Access Gateway – pääsynhallinnan strategia”), jotka vaikuttavat kirjautumissivun näkyvyyteen (kuva 57). Jo aiemmin mainitut toimialueeseen kuuluvuus- ja virustorjuntaohjelmistoskannaukset tarkistavat päätelaitteen tilan ja joko sallivat tai kieltävät pääsyn kirjautumissivulle. (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 77)



Kuva 57. Kirjautumissivun näkyvyyden politiikka-asetukset

Aiemmin luotu Logon Point -sivusto on vielä julkaistava itse sivustolle käyttämällä Server Configuration -työkalua, joka asennettiin aiemmin Citrix Advanced Access Control -palvelimelle Citrix Advanced Access Control -ohjelmiston asennuksen yhteydessä. Käynnistetään Server Configuration -työkalu ja valitaan Configured Logon Points -välilehti ja sieltä äsken luotu Logon point ja julkaistaan se web-sivustolla valitsemalla Deploy (kuva 58). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 77)



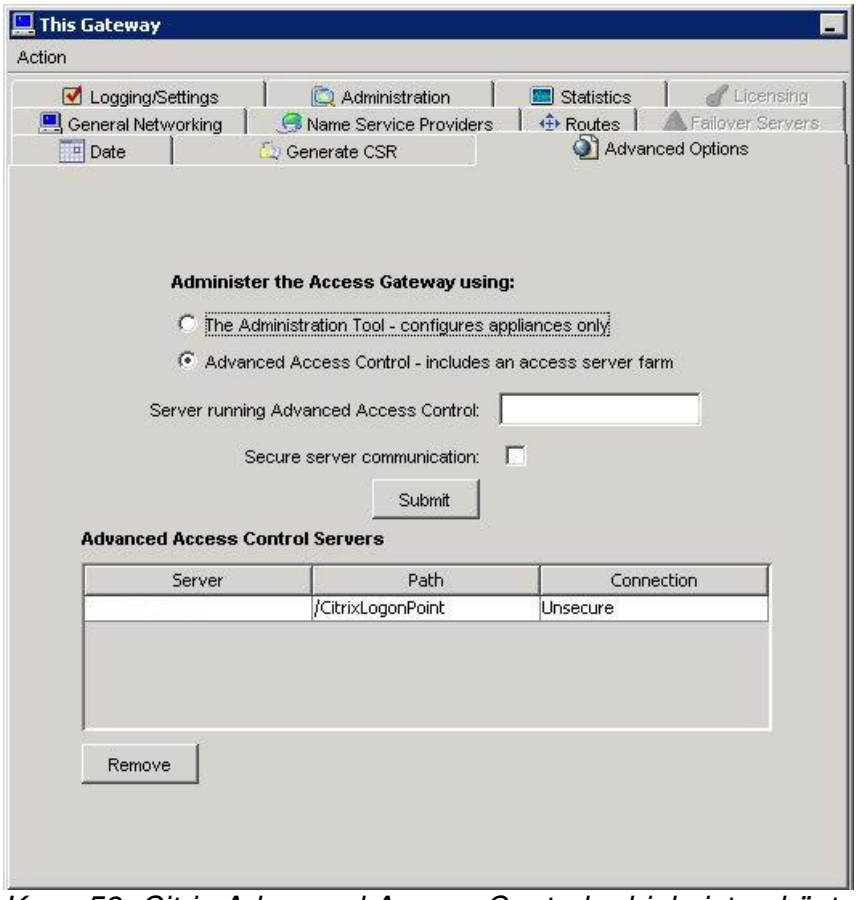
Kuva 58. Logon Point -sivuston julkaisu Citrix Access Gateway -laitteelle

Julkaistu Logon Point luo kansion CitrixLogonPoint-hakemistoon Citrix Advanced Access Control -palvelimella, johon käyttäjät ottavat yhteyden www-selaimella. Koska kaikki käyttäjät kirjautuvat juuri tähän Logon Pointiin, siitä tehdään oletussivusto.

Jos tulee tarvetta muokata julkaistuja Logon Point -sivustoja, niitä voidaan muokata valisemalla Edit logon point. Tämän muutoksen ja uusien Logon Point -sivustojen lisäämisen, web-sivuston muokkaamisen tai Logon Point -sivuston uudelleenjulkaisun jälkeen muutokset täytyy päivittää valitsemalla Refresh logon page information. Logon Point -sivustojen poistaminen onnistuu tarpeen vaatiessa, kun poistaa ensin niihin liittyvät politiikat. Tämän jälkeen poistetaan vielä hallintakonsolista kyseisen Logon Point, jonka jälkeen käydään Server Configuration -työkalulla poistamassa ao. Logon Point. (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 79-81)

9.4 Citrix Access Gateway -laitteen konfigurointi

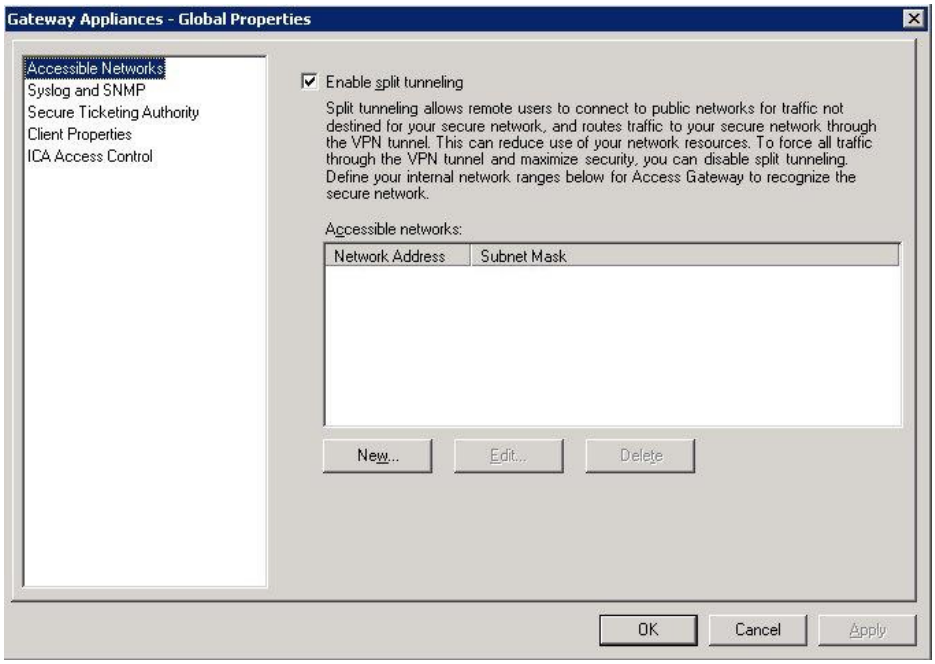
Jotta kaikki pääsynhallintaan liittyvät ominaisuudet saadaan käyttöön Citrix Advanced Access Control -ohjelmistossa ja sen Citrix Access Suite -hallintakonsolissa, on Citrix Access Gateway -laitteen asetuksissa tehtävä seuraava konfigurointi. Kuten jo aiemmin kappaleessa 5 ”Citrix Access Gateway -aktiivilaitteen asennus” totesin, Citrix Access Gateway Administration -hallintatyökalulla otetaan käyttöön Citrix Advanced Access Control -ohjelmisto lisäasetukset-välilehdellä, jotta koko järjestelmää voidaan hallinnoida sitä käyttäen (kuva 59). (Access Gateway Administrator´s Guide 2005: 36.) Näin ollen Citrix Advanced Access Control -ohjelmiston hallintakonsolilla voidaan muokata esimerkiksi sallittuja verkkoresursseja, joihin pääsy on sallittu vain Citrix Access Gateway -järjestelmän läpi (Split Tunneling), ottaa käyttöön SNMP-protokollan kirjaukset sekä luoda pääsylistoja asiakasohjelmistojen ulospäin suuntautuvalle liikenteelle.



Kuva 59. Citrix Advanced Access Control -ohjelmiston käyttöönotto

Split Tunneling -ominaisuus mahdollistaa liikenteen ohjaamisen yrityksen verkkoon tai yleiseen internetiin, kun yrityksen sisäverkon verkko-osoitteet on siihen määritelty. Siten Secure Access -asiakasohjelmisto osaa reitittää sisäverkkoon kohdistuvan liikenteen salattuna VPN-putken läpi ja muun liikenteen normaalisti sen ulkopuolelta. Split Tunneling -ominaisuuden käyttöönotto parantaa asiakasohjelmiston yhteyden tehokkuutta ja vähentää ”Access denied”-ilmoituksen mahdollisuutta, kun käyttäjät pyrkivät sisäverkkoon tai yleiseen internetiin. Toisaalta taas sen poistaminen käytöstä parantaa tietoturvaa, kun kaikki Secure Access -asiakasohjelmiston lähettämä data kulkee Citrix Access Gateway -laitteen kautta. Verkkoresurssien määrittelyssä pitää olla tarkkana, sillä käyttäjät pääsevät vain niihin verkkoihin, joita laitteeseen on määritelty. Siten yleinen internet on esimerkiksi sallittava ip-osoitteella 0.0.0.0 käyttäen aliverkonpeitettä 0.0.0.0. (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 82)

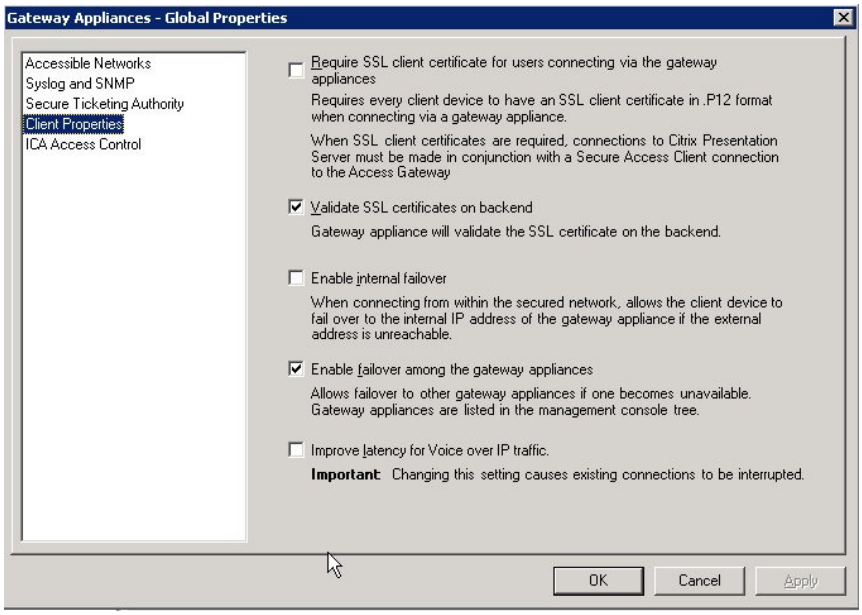
Sallitut verkkoresurssit voidaan konfiguroida Gateway Appliances -komponentissa valitsemalla Accessible Networks -välilehti ja määrittelemällä sisäverkon ip-osoitteet ja aliverkonpeite tai käyttäen CIDR:ia (Classless Inter-Domain Routing) (kuva 60). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 83)



Kuva 60. Sisäverkon ip-osoitteiden asetukset

Client Properties -välilehden asetuksilla määritetään Secure Access -asiakasohjelmiston ja Citrix Access Gateway -laitteen

välinen kommunikointi verkkoliikenteen osalta. Asetuksissa määritellään Citrix Access Gateway -laite tarkistamaan SSL-palvelinsertifikaatit. Se taas parantaa turvallisuutta sisäisille yhteyksille, jotka lähtevät Citrix Access Gateway -laitteesta. SSL-palvelinsertifikaattien tarkistus toimii tärkeänä verkkoturvallisuuden mittarina, sillä se auttaa torjumaan esimerkiksi ”man-in-the-middle”-hyökkäyksiä. Citrix Access Gateway -laite vaatii asentamaan kunnollisen juurisertifikaatin, jota käytetään palvelinsertifikaattien allekirjoitukseen. Lisäksi otetaan käyttöön Citrix Access Gateway Failover -ominaisuus, joka mahdollistaa tietyn Citrix Access Gateway -laitteen määrittelyn ensisijaiseksi yhdyskäytäväksi tietyille käyttäjille tai käyttäjäryhmille (kuva 61). (Access Gateway with Advanced Access Control – Administrator´s Guide 2005: 85)



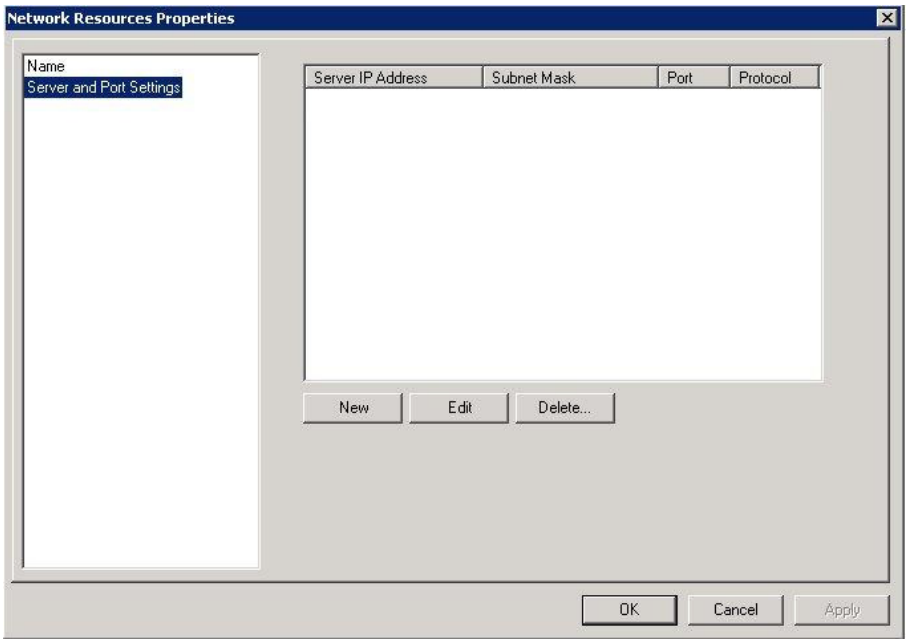
Kuva 61. Citrix Access Gateway -laitteen asetuksia

9.5 Resurssien lisääminen

Citrix Advanced Access Control -ohjelmistoon voi lisätä eri resursseja käyttäen Citrix Access Suite -hallintakonsolia, joihin käyttäjille halutaan sallia pääsy. Näihin kuuluvat verkko- ja internetresurssit, tiedostojaot, sähköposti sekä Access Center -portaalit. Visma Software Oyj:n Citrix Access Gateway -järjestelmään määritellään vain verkkoresurssit, sillä Citrix Access Gateway -järjestelmää käytetään toistaiseksi vain pelkän VPN-yhteyden muodostamiseen sisäverkkoon, jolloin kaikkiin resursseihin sallitaan pääsy. Näin ollen sisäverkossa käyttäjillä on

samat oikeudet Active Directory -hakemistopalvelun kautta, mitkä heillä olisi ollessaan fyysisesti toimistolla.

Verkkoresursseja lisätään Resources-komponentin alta valitsemalla Network Resources -välilehti hiiren oikealla ja sieltä kohta Add network resource. Verkkoresurssille määritellään nimi sekä palvelimen tai verkon ip-osoite sekä aliverkonpeite ja lisäksi mahdolliset rajoitukset portteihin ja protokolliin (kuva 62). Verkkoresursseissa on valmiina ”Entire network”-resurssi, joka sallii tai kieltää pääsyn kaikkiin palveluihin ja palvelimiin turvatussa verkossa. Kun Split Tunneling -ominaisuus on käytössä, edellä mainittu verkkoresurssi ei kuitenkaan ylitä Citrix Access Gateway -laitteeseen määritettyjä sallittuja verkkoja. Kun tarvittavat resurssit on luotu, niihin täytyy vielä liittää pääsypolitiikka, joka sallii tai kieltää käyttäjiltä pääsyn resurssiin. (Access Gateway with Advanced Access Control – Administrator´s Guide: 90-91.) Pääsy- ja yhteyspolitiikkojen konfiguroinnista kerrotaan tarkemmin tuonnempana.



Kuva 62. Verkkoresurssien määrityksiä

9.6 Pääsynhallinta politiikkojen avulla

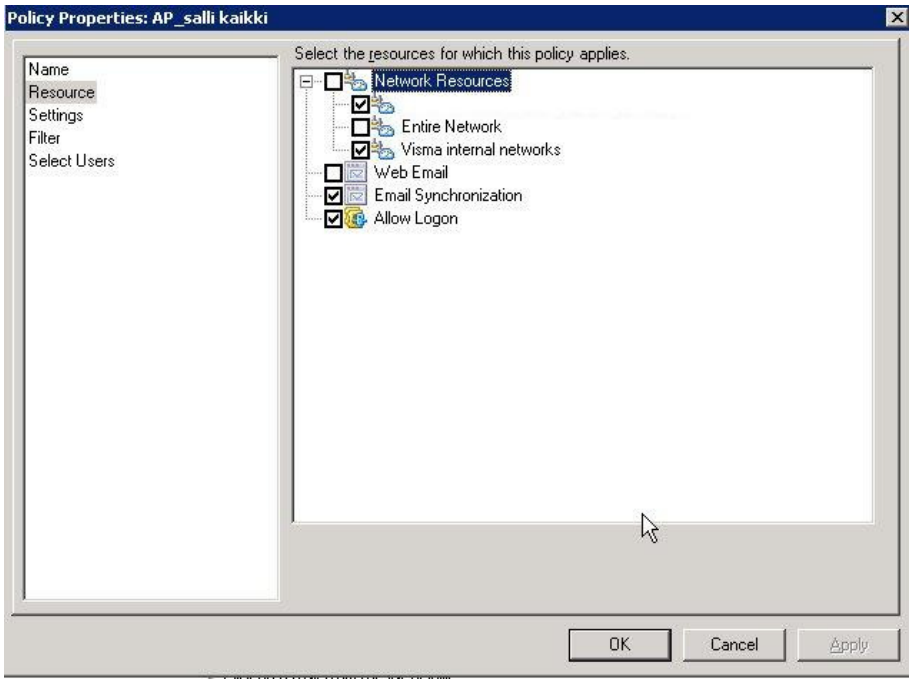
Citrix Access Gateway -järjestelmässä voidaan kontrolloida ja siten rajoittaa tai sallia käyttäjien pääsyä määriteltyihin eri resursseihin luomalla pääsy- ja yhteyspolitiikkoja. Käyttäjien päästyä kiinni tiettyihin resursseihin, voidaan myös rajoittaa tai sallia, mitä he voivat tehdä kyseisissä resursseissa.

Politiikkoihin voidaan lisätä erilaisia suodattimia, jotka perustuvat tiettyyn käyttäjään, käyttäjän autentikoinnin tasoon, käyttäjän käyttämään päätelaitteeseen tai mistä käyttäjä kirjautuu järjestelmään. Käyttäjien pääsyä resursseihin voidaan rajoittaa vaikkapa vaatimalla tietty virustorjunta- tai palomuuriohjelmisto. Käyttäjien mahdollisuutta tehdä tiettyjä toimenpiteitä sallituissa resursseissa perustuu tiettyyn käyttäjäskenaarioon.

Oletusasetuksena Citrix Access Gateway -järjestelmässä käyttäjiltä ei ole pääsyä yhteenkään resurssiin, ennen kuin järjestelmänvalvoja konfiguroi pääsypolitiikkojen avulla sallitun pääsyn järjestelmään. Pääsypolitiikkaan määritellään, kenellä on pääsy ja mihin resursseihin ja millaisten sääntöjen puitteissa pääsy sallitaan tai kielletään. Pääsypolitiikkojen konfiguroinnin määrää voidaan vähentää luomalla resursseille ryhmiä, joissa on erityyppisiä resursseja kuten verkkoresurssit ja tiedostojaot. (Access Gateway with Advanced Access Control – Administrator´s Guide: 103-104)

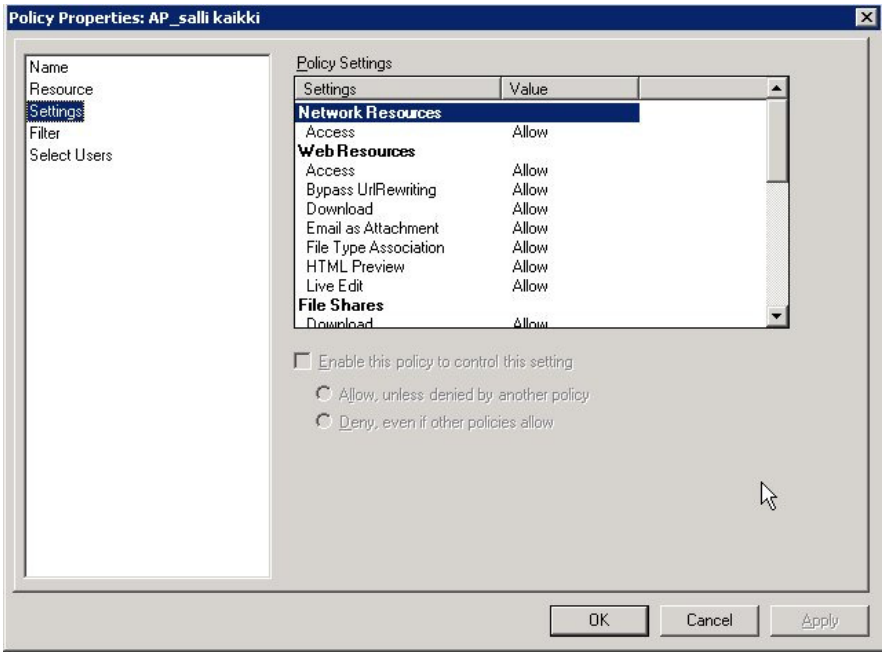
9.6.1 Pääsypolitiikan konfigurointi

Pääsypolitiikka luodaan valitsemalla Policies ja sieltä Access Policies, jossa napsauttamalla sitä hiiren oikealla valikosta valitaan Create access policy. Politiikalle kannattaa antaa sekä kuvaava nimi että tarkka kuvaus. Seuraavaksi valitaan ne resurssit, joihin käyttäjiltä sallitaan pääsy. Visma Software Oyj:n konfiguraatiossa pääsy sallitaan kaikkialle sisäverkon resursseihin (kuva 63). (Access Gateway with Advanced Access Control – Administrator´s Guide: 106-107)



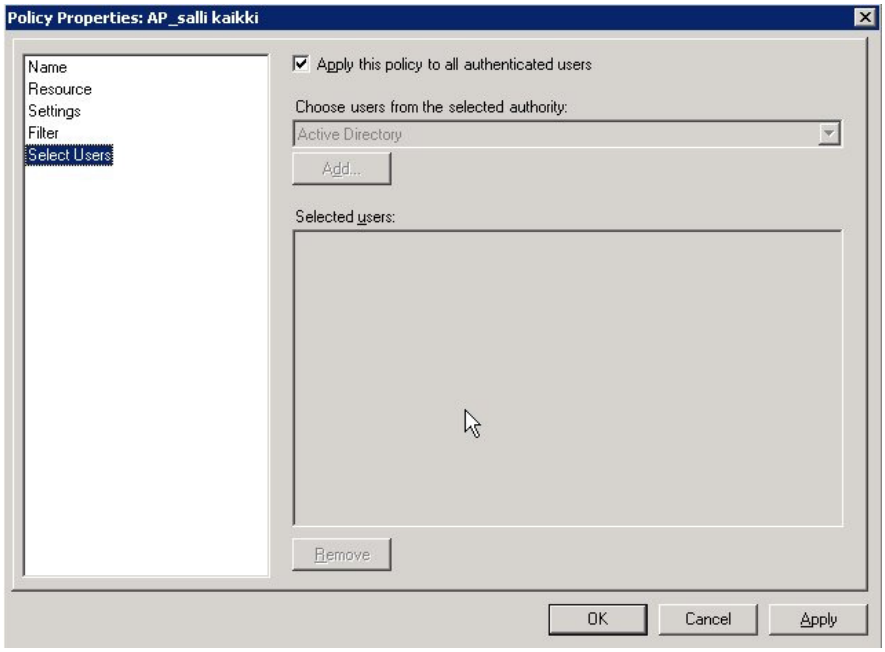
Kuva 63. Pääsynhallintapolitiikan resurssiasetukset

Asetuksissa voidaan erittäin tarkasti määrittää eri resurssien ja niiden komponenttien kieltäminen tai salliminen. Visma Software Oyj:n tietojärjestelmään konfiguroidaan sallituiksi kaikki eli rajoitukset resurssien käyttöön tulevat vasta käyttäjien päästyä sisäverkkoon (kuva 64).



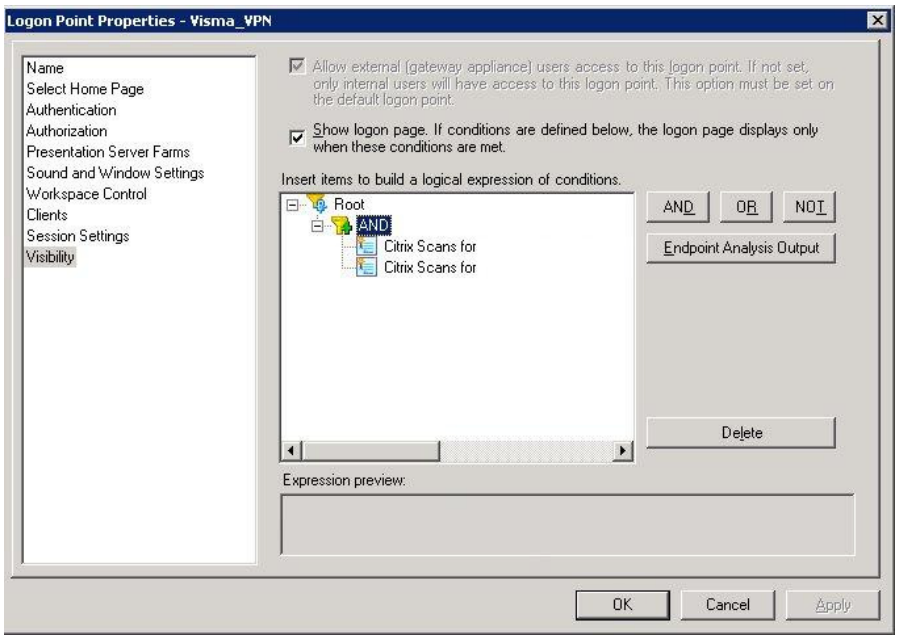
Kuva 64. Pääsynhallintapolitiikan resurssien toimenpideasetukset

Pääsypolitiikkaan on mahdollista myös vaikuttaa luodulla erilaisilla suodattimilla, joiden konfiguroinnista kerrotaan hiukan myöhemmin. Asennusvelhon lopuksi valitaan vielä ne käyttäjät, joita tämä politiikka koskee (kuva 65).



Kuva 65. Sallitut käyttäjäryhmät

Vaikka pääsypolitiikka onkin nyt luotu ja käyttäjillä pääsy verkon resursseihin, täytyy tietoturvaa parantaa vielä jo ennen varsinaista kirjautumissivua Endpoint Analysis -skannauksilla. Sallituissa resursseissa on sisällä myös ”Allow Logon”-resurssi, jolla voidaan edellä mainituilla skannauksilla varmistaa, että käyttäjän päätelaiteessa on virustorjuntaohjelmisto ja että se kuuluu toimialueeseen. Endpoint Analysis -skannaukset otetaan käyttöön Logon Pointin asetuksissa Visibility-välilehdellä, jossa voidaan käyttää loogisia operaattoreita (OR, AND, NOT) eri skannauksien liittämisessä toisiinsa ja siten saavuttaa tietty vaatimustaso koneille ennen sivustolle kirjautumista (kuva 66). (Access Gateway with Advanced Access Control – Administrator´s Guide: 112-113)



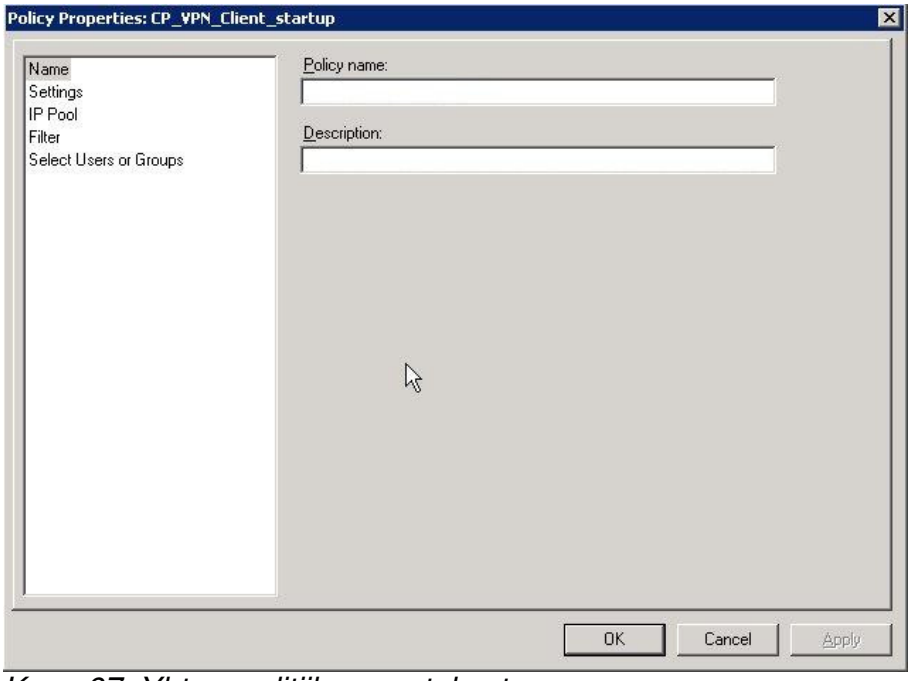
Kuva 66. Kirjautumissivun näkyvyyteen vaikuttavat politiikat

Käytännössä tämä tarkoittaa alkuvaiheessa sitä, että uuden Citrix Access Gateway SSL VPN -järjestelmän käyttöönoton myötä muilla kuin yrityksen tietokoneilla ei enää verkon resursseihin pääse kiinni. Kun Endpoint Analysis -skannaus on suorittanut sivustolla tarkistuksen koneelle, jossa tätä vaadittua tietoturvatasoa ei ole, tulee automaattisesti ilmoitus ”Access is denied”. Tulevaisuudessa järjestelmän käyttöä kuitenkin laajennetaan siten, että muun muassa internetkioskeista sallitaan rajoitettu yhteys sisäverkon tiettyihin palveluihin, joissa voidaan suorittaa rajoitettuja toimenpiteitä. Tämä taas edellyttää uusien pääsypolitiikkojen suunnittelua ja konfigurointia.

9.6.2 Yhteyspolitiikan konfigurointi

Yhteyspolitiikalla kontrolloidaan Secure Access -asiakasohjelmiston yhteyksiä käyttäjän päätelaitteelta Citrix Access Gateway -laitteelle saakka. Myös yhteyspolitiikkoihin voidaan vaikuttaa suodattimilla, joilla määritellään milloin tietty politiikka on voimassa. Yksi kätevimmistä suodattimista on jatkuva skannaus-suodatin (Continuous Scan Filter), joka koko yhteyden ajan jatkuvasti monitoroi sen toimintaa ja katkaisee automaattisesti yhteyden, jos käyttäjän päätelaite ei enää jostain syystä vastaisi suodattimessa määritettyjä vaatimuksia. Visma Software Oyj:n tietojärjestelmässä tätä suodatinta ei oteta käyttöön, sillä päätelaitteet ja niissä olevat ohjelmistot ovat niin paljon toisistaan poikkeavia, että on mahdotonta ottaa käyttöön prosessi- tai rekisteriskannausta. (Access Gateway with Advanced Access Control – Administrator´s Guide: 114)

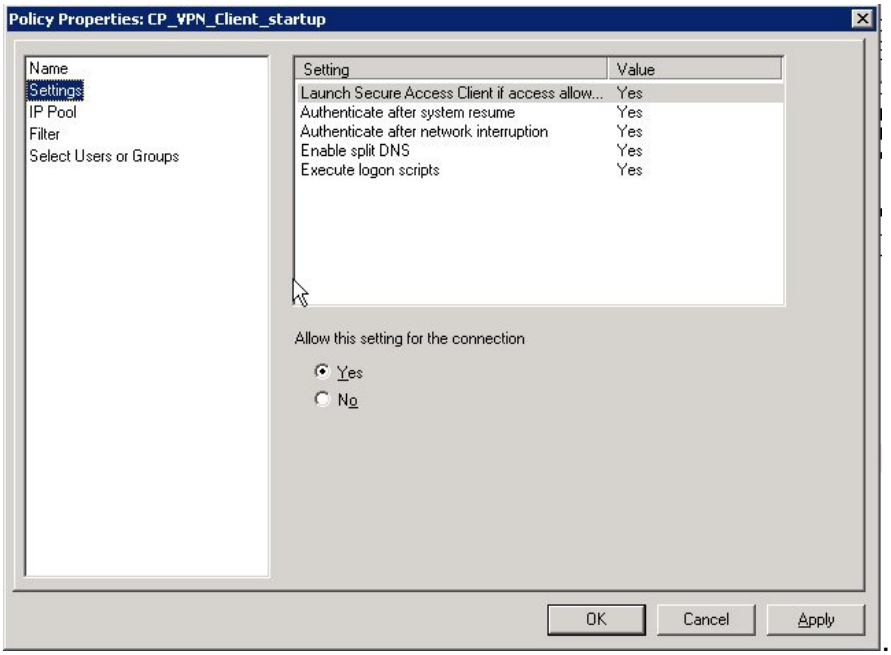
Uusi yhteyspolitiikka konfiguroidaan valitsemalla Policies-komponentin alta Connection Policies -komponentti ja edelleen Common Tasks -ikkunassa kohta ”Create connection policy”. Yhteyspolitiikalle kannattaa antaa kuvaava nimi sekä tarkempi selvitys vielä kuvaukseen (kuva 67). (Access Gateway with Advanced Access Control – Administrator´s Guide: 114)



Kuva 67. Yhteyspolitiikan asetukset

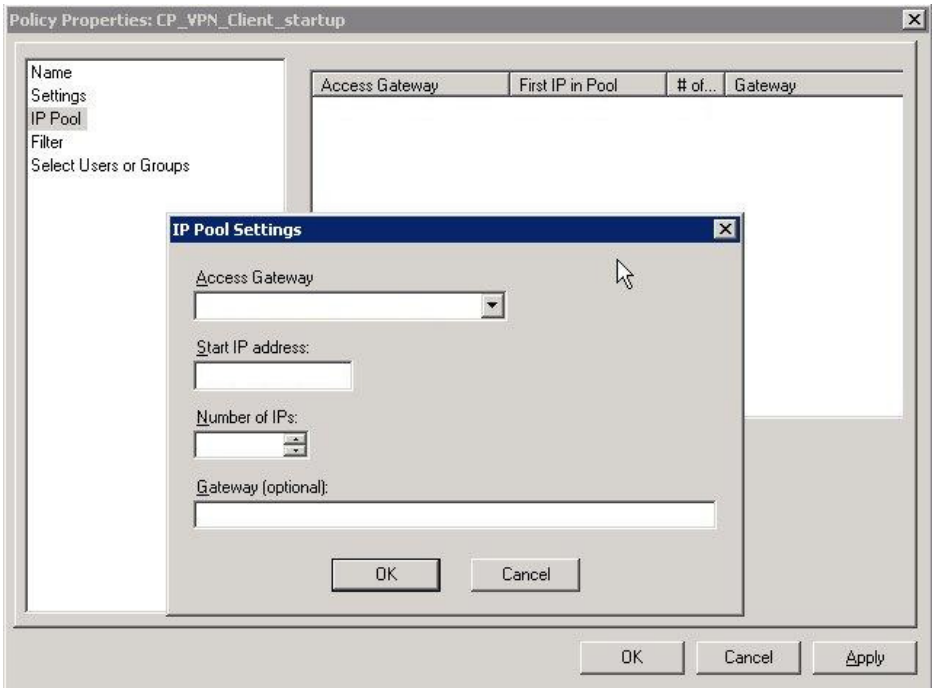
Yhteyden asetuksissa määritellään Secure Access -asiakasohjelmisto käynnistymään, jos pääsy järjestelmään on sallittu. Si-

ten myös muita yhteyden asetuksia päästään konfiguroimaan. Jos käyttäjän päätelaite menee standby- tai hibernate-tilaan, käyttäjä pakotetaan autentikoimaan uudelleen järjestelmään. Sama tilanne on, jos syystä tai toisesta verkkoyhteyteen tulee katkoksia tai katkeaa kokonaan. Enable Split DNS -ominaisuuden käyttöönotolla varmistetaan paikallisten DNS-nimipalvelinten käyttö, jos etä DNS-nimipalvelimia ei ole saatavilla. Logon-skriptit ajetaan myös yhteyden muodostumisen jälkeen (kuva 68) (Access Gateway with Advanced Access Control – Administrator´s Guide: 115)



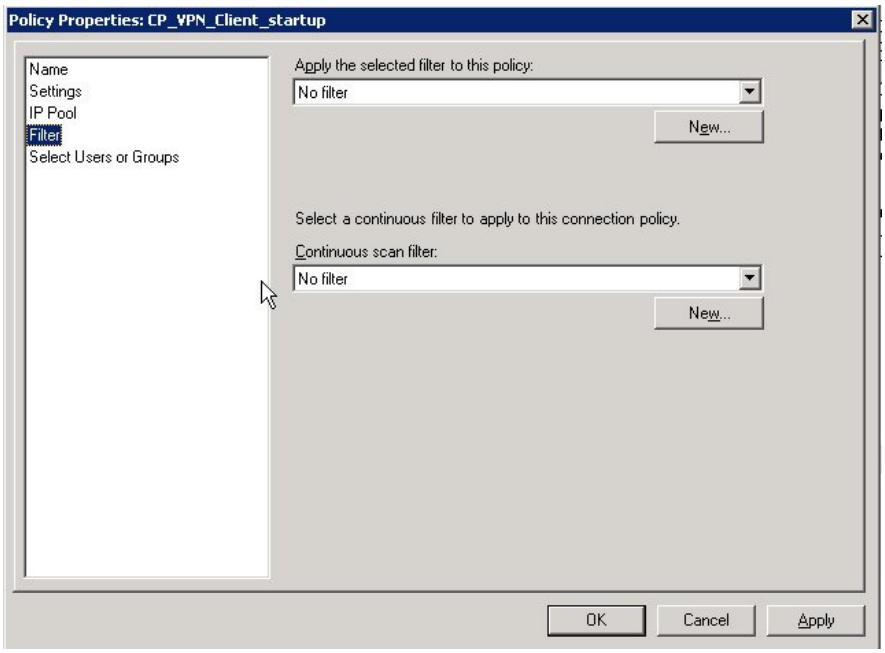
Kuva 68. Yhteyspolitiikan lisäasetuksia

IP-osoitevarastosta päätelaitteille määritellään jaettavaksi virtuaalisia ip-osoitteita. Lisäksi on konfiguroitava Citrix Access Gateway -laitteen ip-osoite. Vaihtoehtona on vielä lisätä oletusyhdyskäytävän ip-osoite, jos sellainen olisi käytössä (kuva 69). Jotta IP-osoitteita saataisiin jaeltua ja käyttöön, on jokainen Citrix Access Gateway -laite käynnistettävä konfiguroinnin jälkeen uudelleen. (Access Gateway with Advanced Access Control – Administrator´s Guide: 115)



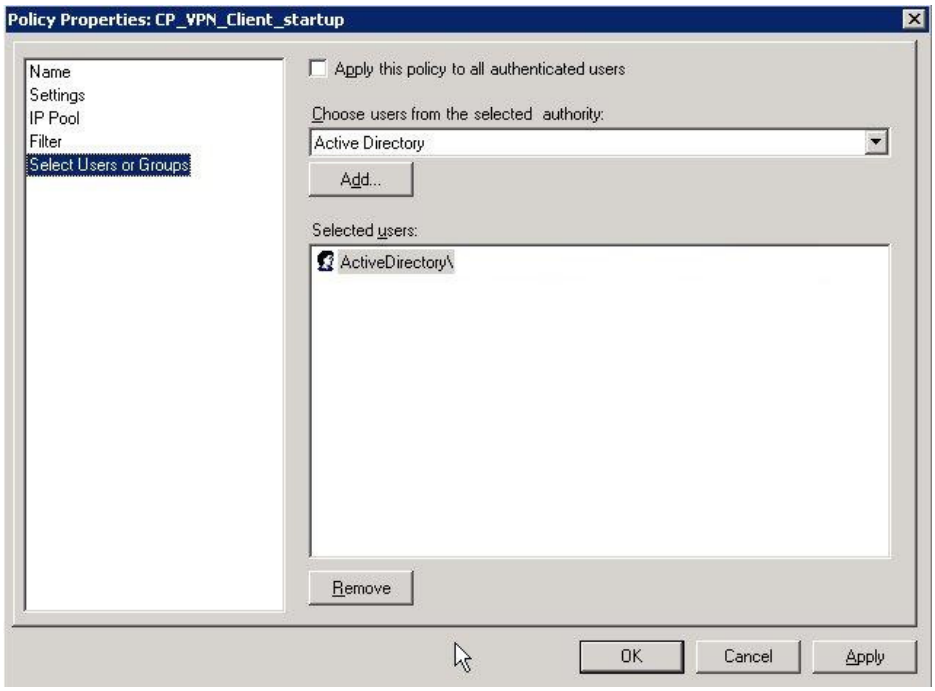
Kuva 69. Yhteyspolitiikan ip-osoitevaraston asetukset

Yhteyspolitiikkaan vaikuttavat suodattimet valitaan kohdasta Filter, jonne voidaan lisätä kahdenlaisia suodattimia. Suodatin voi määritellä vaatimukset autentikoinnille, Endpoint Analysis -skannauksille tai Logon Pointeille. Suodatin tarkistaa politiikan vaatimukset vain kerran kirjautumisen aikana. Jatkuvan skannauksen suodatin taas määrittelee vaatimukset prosesseille, tiedostoille tai rekisterimerkinnöille, joiden täytyy löytyä käyttäjän päätelaitteesta. Suodatin tekee jatkuvaa tarkistamista koko yhteyden aikana (kuva 70). Toistaiseksi Visma Software Oyj:n Citrix Access Gateway -järjestelmään ei oteta käyttöön verkkoyhteyteen vaikuttavia suodattimia. (Access Gateway with Advanced Access Control – Administrator´s Guide: 115)



Kuva 70. Yhteyspolitiikan suodatinasetukset

Yhteyspolitiikan asetuksiin täytyy vielä määrittää ne käyttäjät tai käyttäjäryhmät, joita kyseinen politiikka koskee (kuva 71). Active Directory -hakemistopalveluun on jo aiemmin määritelty käyttäjäryhmä, johon kuuluvat kaikki ne käyttäjät, joille täysi VPN-yhteys sallitaan.



Kuva 71. Yhteyspolitiikan etäkäyttäjäasetukset

Mikäli olisi tarvetta luoda useampi yhteyspolitiikka, niiden tärkeysjärjestystä voidaan muuttaa valitsemalla Connection Policies ja Common Tasks -ikkunassa valitaan Set Priority Order. Ylinnä olevalla politiikalla on tärkein prioriteetti muihin alla oleviin nähden. (Access Gateway with Advanced Access Control – Administrator´s Guide: 116)

9.6.3 Suodattimien konfigurointi politiikkoja varten

Suodattimet määrittelevät olosuhteet, jonka mukaan politiikat otetaan käyttöön. Suodattimiin voidaan konfiguroida neljä eri komponenttia, joihin suodatin vaikuttaa. Käyttäjän kirjautuessa tietylle Logon Point -sivustolle, suodatin pakottaa tietyn politiikan päälle. Käyttäjän autentikoinnissa suodatinta käytetään tietyllä tavalla riippuen siitä, kirjautuuko käyttäjä pelkällä salasanalla vai käytetäänkö monimutkaisempaa autentikointia. Myös päätelaitteiden Endpoint Analysis -skannauksien tuloksista riippuen suodatin käynnistää politiikan. Lisäksi päätelaitteella mahdollisesti olevien SSL-sertifikaattien perusteella voidaan

tietty politiikka pakottaa niin ikään päälle. (Access Gateway with Advanced Access Control – Administrator´s Guide: 116)

Politiikkasuodattimet konfiguroidaan valitsemalla Policies-komponentin alta Filters ja edelleen Common Tasks -ikkunassa Create Filter. Seuraavaksi suodattimelle annetaan nimi ja kuvaus. On mahdollista luoda joko tyypillinen tai kustomoitu suodatin, johon voidaan lisätä useita eri suodattimia yhteen ryhmään. Edellä mainitut komponentit konfiguroidaan valitsemalla uusi suodatin. Kuten Endpoint Analysis -skannauksien kanssa oli Logon Point -komponentin asetuksissa, voidaan myös suodattimissa käyttää loogisia operaattoreita yhdistettäessä eri suodattimien ominaisuuksia. (Access Gateway with Advanced Access Control – Administrator´s Guide: 117)

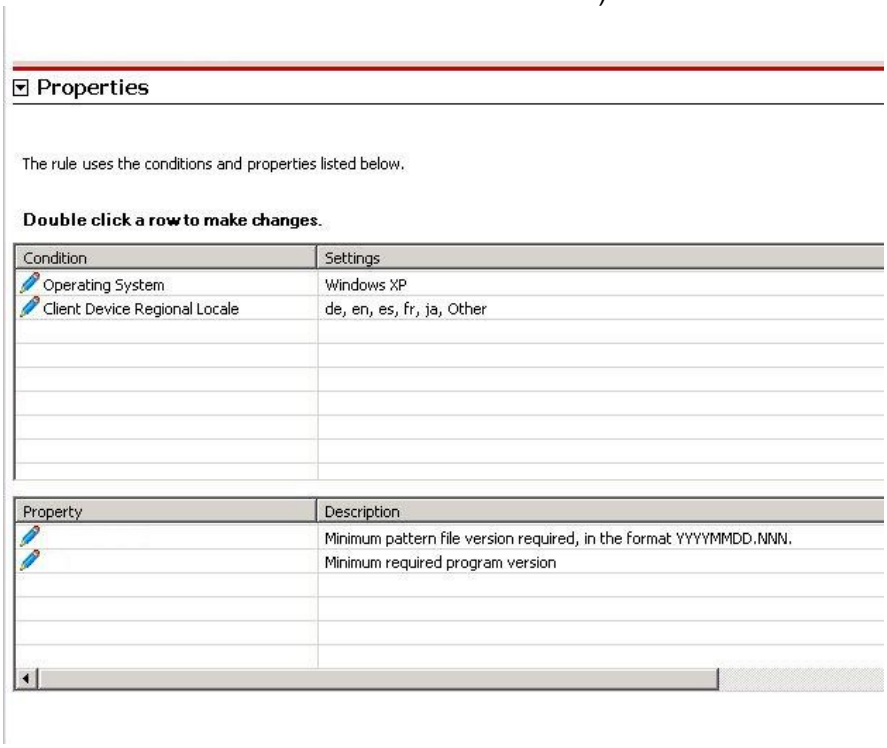
Jatkuvan skannauksen suodattimilla voidaan yhdistää useita eri jatkuvia skannauksia, joilla tarkistetaan päätelaitteen tietty käynnissä oleva prosessi tai rekisterimerkintä. Myös niissä on mahdollista käyttää loogisia operaattoreita. (Access Gateway with Advanced Access Control – Administrator´s Guide: 119)

Jatkuvan skannauksen suodattimet määritetään valitsemalla Policies-komponentin alta Continuous Scan Filters ja Common Tasks -ikkunassa luodaan uusi suodatin. Suodattimen nimen ja kuvauksen jälkeen vaatimukset-välilehdellä valitaan ne määritykset, jotka käyttäjien päätelaitteissa on oltava käyttäen mahdollisesti loogisia operaattoreita. (Access Gateway with Advanced Access Control – Administrator´s Guide: 119)

9.6.4 Endpoint Analysis ja Continuous Scan -skannaukset

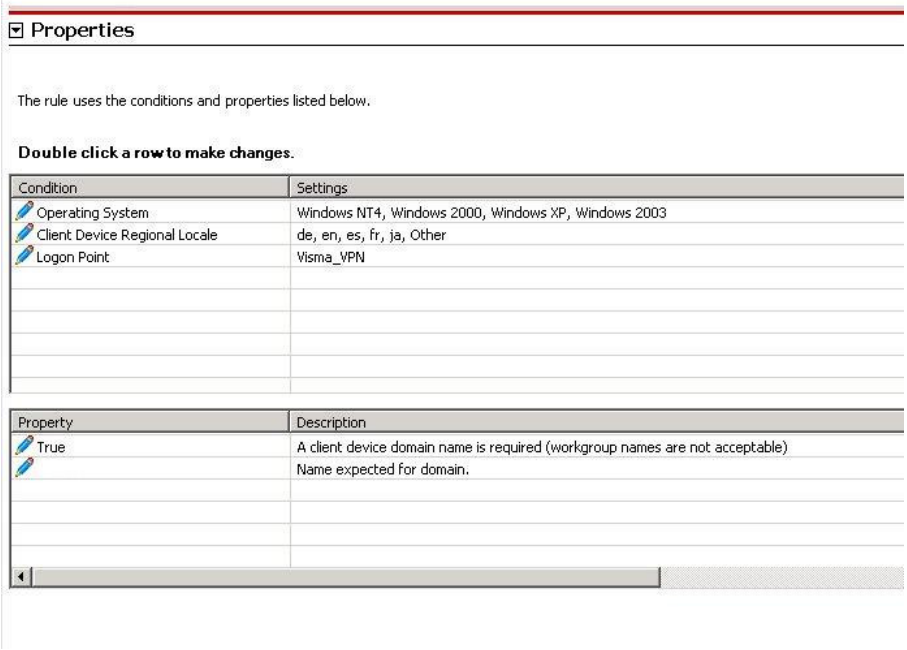
Endpoint Analysis on prosessi, joka käynnistyy käyttäjän navigoidessa selaimella Citrix Access Gateway -järjestelmän kirjautumissivustolle. Prosessi tarkistaa käyttäjän päätelaitteessa olevia tietoja esimerkiksi virustorjuntaohjelmasta, käyttöjärjestelmästä ja palomuurista ennen kuin laitteelle sallitaan pääsy kirjautumissivulle. Endpoint Analysis -prosessi ajetaan vain kerran kirjautumisen aikana. Jatkuvalla skannauksella taas pystytään tarkkailemaan päätelaitteen tiedostoja, rekisterin tietoja sekä käynnissä olevia prosesseja kirjautumisen jälkeen koko yhteyden aikana. Siten voidaan katkaista yhteys sisäverkkoon, jos äkillisesti esimerkiksi virustorjuntaohjelman ajettava exe-tiedosto sammuu vaikka viruksen tai troijalaisen toimesta. (Access Gateway with Advanced Access Control – Administrator´s Guide: 151)

Skannaukset konfiguroidaan valitsemalla Endpoint Analysis -komponentin alta tietty skannauspaketti ja sen alta tarkemmin itse ohjelmistoon liittyvä skannaus. Visma Software Oyj:n Citrix Access Gateway -järjestelmässä käytetään yhtä virustorjunta-ohjelmisto-skannausta (kuva 72). Luodaan uusi skannaus, jolle määritellään kuvaava nimi sekä olosuhteet, jolloin skannaus ajetaan. Sen jälkeen luodaan vielä sääntö, johon määritellään vaadittu vähimmäisversio itse ohjelmasta sekä minimi pattern-tiedostoversio (kuva 72). (Access Gateway with Advanced Access Control – Administrator´s Guide: 153)



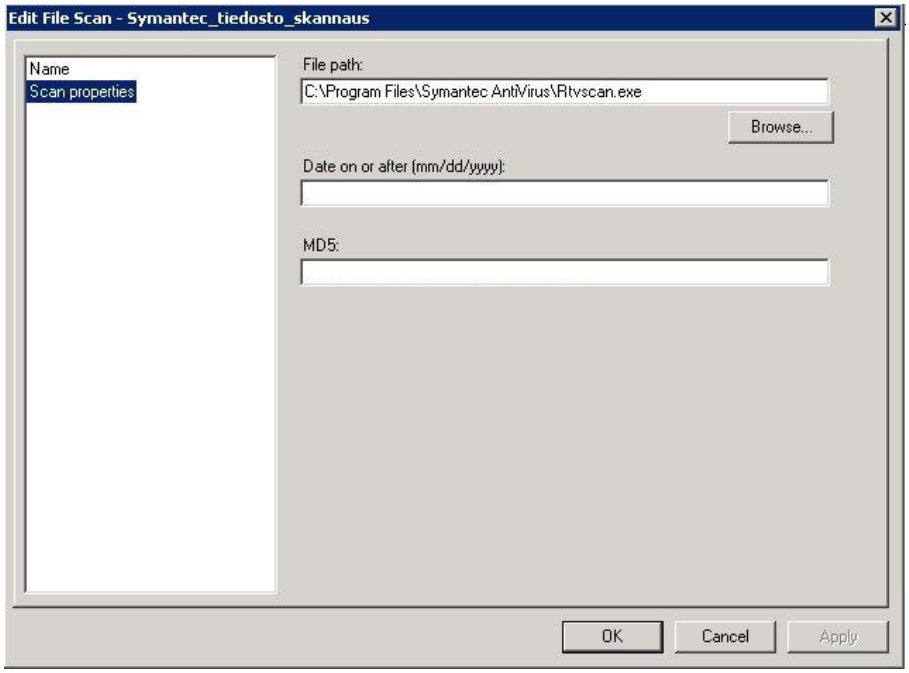
Kuva 72. Virusohjelmiston skannausasetukset

Toinen käyttöönotettava Endpoint Analysis -skannaus on päätelaitteen tunnistamisen skannaus, jossa tarkistetaan kuuluko päätelaite määriteltyihin toimialueisiin (kuva 73).



Kuva 73. Toimialueeseen kuuluvuuden skannausasetukset

Jatkuva skannaus luodaan käyttäen Policies-komponentin alta löytyvän Continuous Scan -haaran kolmesta eri skannausoptiosta. Siten on mahdollista luoda joko tiedostoon, prosessiin tai rekisterimerkintään kantaaottava jatkuva skannaus. Common Tasks -ikkunasta valitaan haluttu skannaus, johon määritellään tarvittavat tiedot esimerkiksi vaadittavasta tiedostosta, sen polusta ja digitaalisesta allekirjoituksesta (MD5) (kuva 74). (Access Gateway with Advanced Access Control – Administrator´s Guide: 165)

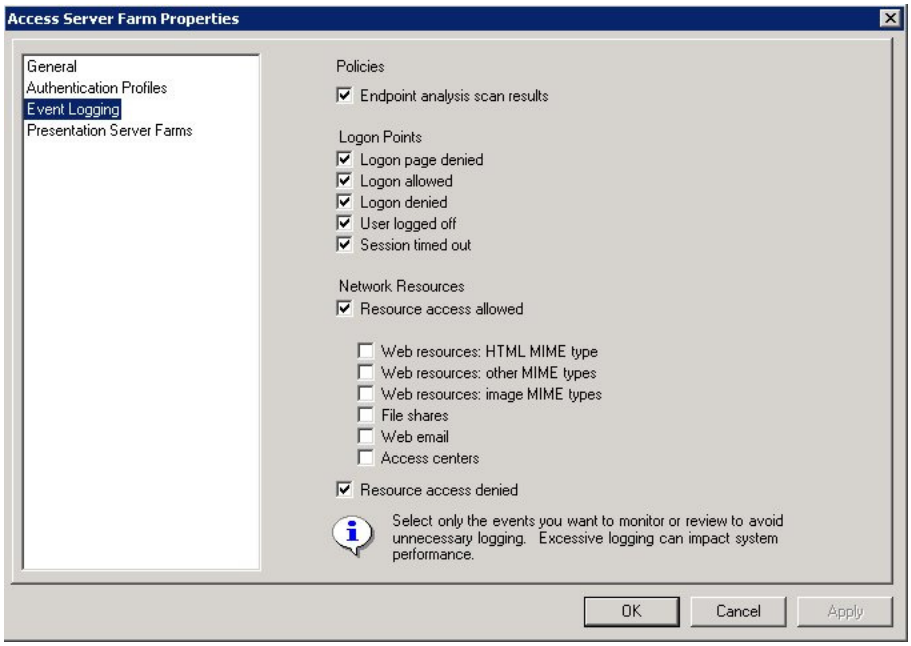


Kuva 74. Virustorjuntaohjelmiston skannausasetukset

Jatkuvia skannauksia ei niiden tehokkuudesta huolimatta oteta käyttöön Citrix Access Gateway -järjestelmässä johtuen useista eritasoisista ja toisistaan poikkeavista päätelaitteista ja niiden ohjelmistoista. Niinpä käyttöömme on riitettävä tietoturvallinen opinnäytetyössäni aiemmin kuvattu Endpoint Analysis -skannaus kirjautumisen yhteydessä.

9.7 Järjestelmän tapahtumien kirjaukset

Tärkeä osa järjestelmän toimivuuden ja käyttäjien eri toimenpiteiden seuraamisen kannalta on näiden tapahtumien kirjaukset tiedostoon mahdollisten ongelmatilanteiden ja järjestelmästä löytyvien heikkouksien varalta. Seurantaan voidaan esimerkiksi liittää onnistuneet ja epäonnistuneet kirjautumisyritykset järjestelmään sekä tiettyihin resursseihin. Lisäksi on otettava tarkoin huomioon, mitä kaikkea kannattaa seurata, jotta järjestelmä ei kuormittuisi ”turhasta” seurannasta. (Access Gateway with Advanced Access Control – Administrator´s Guide: 213) Kirjausasetuksista otetaan käyttöön aiemmin kuvatun konfiguraation puitteissa kirjautumisyrityksiin liittyvät toiminnot, Endpoint Analysis -skannaukset sekä resursseihin kohdistuneet epäonnistuneet pääsyt (kuva 77).



Kuva 77. Järjestelmätapahtumien kirjauksien asetukset

Kuvassa 77 näkyvät optiot on konfiguroitu Citrix Access Gateway -farmin ominaisuuksissa valitsemalla Edit Farm Properties Common Tasks -ikkunassa. Kirjaustiedostoa voidaan tarkastella lähemmin Windowsin tapahtumienvalvonta-työkalun kautta, jonne Citrix Advanced Access Control -ohjelmisto luo CitrixAGE Audit -nimisen objektin. Sen ominaisuuksia, kuten kokoa ja kirjausajanjaksoa, voidaan muokata tarpeisiin sopivaksi vakiodun 5 120 kilobitin ja seitsemän päivän sijaan. Samalla voidaan määrittää käytettäväksi toimintoa, joka ylikirjoittaa määritettyä ajanjaksoa vanhemmat kirjaustiedot. Kummatkin näistä asetuk-

sista jätetään vakioarvoihinsa. (Access Gateway with Advanced Access Control – Administrator´s Guide: 215-216)

Citrix Access Suite -hallintakonsolissa voidaan käyttää myös sisäänrakennettua Event Log Consolidator -komponenttia tapahtumien tarkastelemiseen. Sen saa käyttöön valitsemalla puuhierarkiassa Citrix Access Gateway -pääkomponentin ja Other Tasks -ikkunassa valitaan View Events. Itse ohjelman päävalikossa otetaan kirjaukset päälle valitsemalla Collect ja sitten valitaan haluttu raportti tarkasteltavaksi. Mahdollisia raportteja ovat esimerkiksi käyttäjien kirjautumiset järjestelmään ja Logon Pointeihin sekä epäonnistuneet tai evätyt pääsyt resursseihin. Ohjelma voidaan konfiguroida ottamaan tietyin väliajoin tapahtumia talteen, joka tässä tapauksessa jätettiin viiden sekunnin vakioarvoonsa. (Access Gateway with Advanced Access Control – Administrator´s Guide: 216)

9.8 Komponenttien yhdistäminen järjestelmäksi

Aiemmin kerroin kaikista Citrix Advanced Access Control -ohjelmiston eri komponenttien konfigurointiin liittyvistä toimenpiteistä. Seuraavaksi näistä kaikista konfiguroiduista komponenteista luodaan yhteen toimiva järjestelmä, jota käyttäjät voivat käyttää tietoturvallisesti työskennellessään etätoimistolla. Kun järjestelmä on käyttöönottoa vaille valmis, tarvitaan vielä tarvittavien asiakasohjelmistojen asennus käyttäjille sekä ohjeistus uuden järjestelmän käyttöön. Tästä kerron tarkemmin seuraavassa luvussa.

Loppujen lopuksi komponenttien yhdistäminen toimivaksi järjestelmäksi on sangen helppoa. Tärkeimmiksi komponenteiksi muodostuvat kirjautumispiste eli Logon Point, pääsy- ja yhteyspolitiikat, Endpoint Analysis -skannaukset sekä resurssit, joihin käyttäjille haluttiin sallia pääsy. Logon Point -komponenttiin konfiguroitiin tärkeimpänä vahvan autentikoinnin käyttöönotto. Jotta myös siihen kirjautuminen sallittaisiin vain tietyntyyppisiltä päätelaitteilta, otettiin käyttöön toimialueeseen ja virustorjuntaohjelmistoon liittyvät Endpoint Analysis -skannaukset Visibility-välilehdellä. Verkkoresursseihin määriteltiin sisäverkon ip-osoiteavaruus aliverkonpeitteellä sekä 0.0.0.0 ip-osoite 0.0.0.0 maskilla, käsittäen koko internetin kaikilla protokollilla kaikista porteista. Tämän jälkeen pääsypolitiikkaan määriteltiin luodut verkkoresurssit, joihin käyttäjät pääsevät kiinni sekä annettiin täydet oikeudet kyseisiin resursseihin. Ainut käyttöönotettava VPN-yhteysmuotohan on täysi VPN, jossa sisäverkot oikeudet määräytyivät Active Directory -hakemistopalvelun perusteella.

Yhteyspolitiikka konfiguroitiin jo aiemmin kerralla kuntoon, joten siihen ei tarvitse muita komponentteja enää liittää.

Citrix Access Gateway -järjestelmä on nyt konfiguroitu ja komponentit yhdistetty toimivaksi kokonaisuudeksi, joten sen käytön mahdollistavien asiakasohjelmistojen asennus päätelaitteille sekä SafeWord-toukkien käytön opastus käyttäjille tehdään seuraavaksi.

9.9 Päätelaitteiden ohjelmiston asennus ja konfigurointi

Viimeisenä toimenpiteenä Citrix Access Gateway -järjestelmää käyttöönotettaessa tarvitaan vielä sen käytön mahdollistavien ohjelmistojen – tarkemmin asiakasohjelmistojen – asennus käyttäjien päätelaitteille. Jotta järjestelmän käyttöönotto ja käyttö olisi mahdollisimman yksinkertaista käyttäjille, ohjelmistojen asennus tehdään automaattiseksi. Järjestelmän www-sivuston osoite tuodaan muun muassa automaattisesti käyttäjien päätelaitteiden työpöydille Active Directory -hakemistopalvelun ryhmäkäytännöillä

Asennusskenaarioissa käytetään hyväksi Active Directory -hakemistopalvelua, jonka avulla ohjelmistojen asennus tehdään verkon kautta pakottamalla kyseinen politiikka tiettyyn organisaatioyksikköön, jossa päätelaitteet Active Directory -hakemistopalvelun puuhierarkiassa sijaitsevat. Käytännössä tässä on kaksi mahdollisuutta. Toisessa asennusskenaariossa käytetään Access Client Package -ohjelmistoa, joka sisältää kaikki tarvittavat asiakasohjelmistot sekä uuden Citrix Access Gateway -järjestelmän että Citrix MetaFrame Presentation Server -ympäristön käyttöön ilman että konfiguroitaisiin ja tehtäisiin erillisiä jaettavia msi-paketteja jokaisesta järjestelmästä erikseen. Toinen asennusskenaario taas sisältää kaksi eri msi-pakettia; yksi Endpoint Analysis -asiakasohjelmistoa ja yksi Citrix MetaFrame Presentation Server -asiakasohjelmistoa varten. VPN-yhteyden muodostamiseen tarvittavaa asiakasohjelmistoa ei Active Directory -hakemistopalvelun kautta voida jaella, koska se on saatavilla vain exe-tiedostona eikä msi-pakettina. Siksi sen asennus tehdään kirjautumissivuston kautta Activex-komponenttina.

Kummassakin asennusskenaariossa on puolensa. Access Client Package -ohjelmiston uuden version ilmestyessä kaikki sen sisältämät asiakasohjelmistot voidaan päivittää hallitusti kerralla. Huono puoli on se, että päivityksiä ilmestyy verkkaiseen tahtiin. Usean msi-paketin jakelun puoltavia seikkoja tukee se, että yhden asiakasohjelmiston päivittyessä muokataan vain

yhtä asiakasohjelmistoa ja muut säilyvät koskemattomina. Toisaalta tästä aiheutuu IT-osastolle lisätyötä Access Client Package -ohjelmistoa enemmän.

Access Client Package -ohjelmisto sisältää kolme eri Citrix Access Suite -komponenttia eli Citrix MetaFrame Presentation Server -ympäristöön, Citrix Access Gateway -järjestelmään sekä Citrix Password Manager -ohjelmiston käyttöön tarvittavat asiakasohjelmistot. Tästä msi-paketista voidaan muokata halutunlainen käyttämällä hyväksi Windows-käyttöjärjestelmissä olevaa msiexec.exe-ohjelmaa, joka ajetaan hallinta-moodissa komentokehotteessa muodossa *msiexec.exe /a [polku msi-pakettiin].* Kun ohjelman suoritus on käynnistetty, pakettiin voidaan liittää halutut asiakasohjelmistot sekä muokata tuleva asennus päätelaitteille tietynlaiseksi. Lopullisen jakelupaketin kokoa on myös mahdollisuus pienentää käyttäen File Size Reduction -ominaisuutta poistamalla turhia käyttämättömiä tiedostoja asennuspaketista. Muokatussa asennuspaketissa otettiin mukaan kaikki asiakasohjelmistot ja asennuksen eteneminen tehtiin täysin automatisoiduksi. Tiedostokokoa ei myöskään pienennetty. (Readme for the Access Client Package, Version 4.1)

Usean asiakasohjelmiston jakelussa paketit jaellaan sellaisenaan Active Directory -hakemistopalvelusta päätelaitteille, mutta Secure Access -asiakasohjelmisto vaatii jo vähän enemmän askartelua. Ilman automaattista jakelua verkosta asiakasohjelmistojen asennus suoraan esimerkiksi exe- tai msi-tiedostosta vaatii järjestelmänvalvojan oikeudet, joita suurimmalla osalla käyttäjistämme ei ole omalle päätelaitteelleen. Niinpä Secure Access -asiakasohjelmisto on asennettava kirjautumissivulta siten, että selaimen ja samalla Citrix Access Gateway www-sivuston pikakuvake raahataan komentokehotteeseen, joka on käynnistetty Asentaja-tunnuksella. Tällöin kyseisessä selaimessa on järjestelmänvalvojan oikeudet ja ActiveX-komponentti asentuu normaalisti ja asentaa VPN-yhteyden käyttöön tarvittavan Secure Access -asiakasohjelmiston oikein. Selaimessa on tietysti oltava sallittuina ActiveX-komponenttien hyväksyminen sekä Active Scripting -toiminto päällä. Active Directory -hakemistopalvelun kautta Citrix Access Gateway -sivusto on pakotettu luotettuihin sivustoihin selaimissa. Aiemmin tässä opinnäytetyössä kuvailemani konfiguraatio Citrix Access Gateway -järjestelmän puitteissa ei vaadi muita asiakasohjelmistoja asennettavaksi, jotta täyden VPN-yhteyden kautta kaikki verkot palvelut olisivat käytettävissä kuten toimistolla sisäverkossa ollessa. Siksi näistä asennusskenaarioista käytetään jälkimmäistä ohjelmistojen jakoon Active Directory -hakemistopalvelusta.

10 Yhteenveto

Olen opinnäytetyössäni käynyt läpi Citrix Access Gateway SSL VPN -järjestelmän käyttöönoton ja konfiguroinnin Visma Software Oyj:n verkkoinfrastruktuuriin. Järjestelmän käyttämästä VPN-tekniikasta olen pyrkinyt teoriaosuudessa tuomaan esille tiivistetysti kaiken olennaisen sekä valottamaan Citrix Access Gateway -järjestelmässä ja SafeWord-autentikointijärjestelmässä käytettyjen komponettien ja ohjelmistojen perusteita. Opinnäytetyön lukijalle on pyritty antamaan eväitä mahdolliseen työn hyödyntämiseen vastaavan järjestelmän implementoinnissa jossain toisessa verkkoinfrastruktuurissa ilman useiden manuaalien ja oppaiden lukemista, kun käytössä olisi vain tämä opinnäytetyö.

Tälle järjestelmälle oli tarvetta Visma Software Oyj:ssä, kun haluttiin vaivaton ja helposti hallinnoitava SSL VPN -järjestelmä yrityksen etäkäyttäjien yhteyksiä varten internetin yli. Järjestelmässä käytettävän SafeWord-autentikoinnin avulla päästiin käytännössä eroon monimutkaisten salasanojen ja muun tietoturvakäytäntöjen käytöstä Microsoft Active Directory -ympäristössä etäkäyttäjien osalta. Citrix Access Gateway SSL VPN -järjestelmän myötä OSI-mallin ylempien kerrosten protokollia voidaan hyödyntää suoraan VPN-putken läpi SSL-salattuna.

Järjestelmän käyttöönottoprojekti alkoi jo vuoden 2006 keväällä ja tuotantokäytössä järjestelmä oli marraskuussa 2006. Siitä huolimatta tämä opinnäytetyö valmistui vasta vuoden 2007 keväällä, koska aikaa itse työn kirjoittamiseen ei jäänyt tarpeeksi samalla kun järjestelmää testattiin ja otettiin käyttöön mukaan lukien vakituisen työn hoitaminen sekä perhe-elämä. Järjestelmän ollessa käytössä jo muutaman kuukauden, oli tämän opinnäytetyön kirjoittamisellekin tarpeeksi aikaa. Samalla saatiin arvokasta kokemusta järjestelmän toimivuudesta käyttäjillä, josta kerron lisää seuraavassa.

Järjestelmän käyttöönoton jälkeen käyttäjien päätelaitteille asennettavien asiakasohjelmistojen käyttöönotossa ei ilmennyt suurempia ongelmia muutamia tapauksia lukuun ottamatta. Näissä tapauksissa SSL VPN -tunnelin muodostamiseen tarvittava Secure Access -asiakasohjelmisto ei asennuksen jälkeen joko käynnistynyt tai muodostanut tarvittavaa tunnelia päätelaitteen ja Citrix Access Gateway -laitteen välille. Syyksi paljastui erilaisilla oikeuksilla olevat päätelaitteet sekä niiden käyttäjät. Jos käyttäjällä oli järjestelmänvalvojan oikeudet päätelait-

teellensa, ohjelmisto asentui oikein, mutta sen käyttö saman käyttäjän tunnuksilla ei onnistunut ennen kuin käynnistystä kokeiltiin toisen peruskäyttäjän tunnuksilla. Tämän jälkeen myös järjestelmänvalvojan oikeuksilla oleva käyttäjä pystyi käynnistämään ohjelmiston. Toisessa asennusskenaariossa peruskäyttäjän oikeuksilla olevalle koneelle tehty asennus käyttäen Asentaja-tunnusta asensi edelleen ohjelmiston oikein, mutta sen käyttö perustason tunnuksilla oli mahdotonta. Tämä ongelma poistui, kun ohjelmisto käynnistettiin kerran paikallisen päätelaitteen järjestelmänvalvojan tai toimialueen järjestelmänvalvojan tunnuksilla, jonka jälkeen perustason tunnuksilla ohjelmisto käynnistyi oikein. Kolmas erikoinen ongelma ilmeni sellaisen käyttäjän päätelaitteella, jossa oli asennettuna jokin selaimeen integroitu tiedostojen etsintään tarkoitettu lisäosa kuten MSN Toolbar- tai Google Desktop Search -ohjelma. Tällöin selaimella kyllä pääsi kirjautumissivulle asti, mutta kirjautumisen jälkeen selain ilmoitti herjan ”sivua ei löydy”. Ongelma korjaantui aiemmin mainittujen ohjelmien poistolla päätelaitteesta ja uudelleenkäynnistymisen jälkeen.

Järjestelmän käytön suhteen ongelmia on ilmennyt ajoittain vain DNS-nimenselvennyksessä, joka ilmenee heti VPN-tunnelin auettua, kun Secure Access -asiakasohjelmisto ei osaa käyttää suoraan paikallisia DNS-määrityksiä, vaan yrittää hakea niitä etäpalvelimelta. Tähän ongelmaan auttoi DNS-pinon tyhjennys manuaalisesti heti VPN-tunnelin muodostuttua. Ongelmasta päästään mahdollisesti lopullisesti eroon, kun vuoden toisella neljänneksellä järjestelmä päivitetään nykyisestä 4.2.2-versiosta uuteen 4.5.1-versioon, johon on tehty useita VPN-yhteyteen ja Secure Access -asiakasohjelmiston toimivuuteen vaikuttavia korjauksia.

Järjestelmän päivittämisen myötä myös etäkäyttäjien päätelaitteiden eri ohjelmistokomponentit päivitetään verkon kautta uusimpiin versioihin, jotta järjestelmästä saadaan kaikki hyöty irti. Vuoden 2007 toisen neljänneksen aikana aloitetaan myös järjestelmän 2. vaiheen käyttöönoton suunnittelu eli ns. Kiosk Mode -yhteystyypin implementointi. Tällöin olisi myös yrityksen ulkopuolisista päätelaitteista, kuten internetkioskit lentoasemilla, päätelaitteet kotona sekä mobiilit laitteet, pääsy rajoitetusti sisäverkkoon.

Itse koin tämän opinnäytetyön tekemisen todella mielekkäänä ja samalla erittäin haasteellisena, sillä minulla ei ollut juuri minkäänlaista osaamista yhdestäkään Citrix-ympäristöön liittyvän järjestelmän toiminnallisuudesta. Työssä eteenpäin on auttanut tietysti kollegoiden tuki, mutta eniten kuitenkin oma halu ja in-

nostus tutustua uusiin järjestelmiin ja niiden käyttämiin tekniikoihin. Ennen tämän opinnäytetyön aloittamista tutustuin Citrix-järjestelmiin Visma Software Oyj:n tietojärjestelmässä vajaan puolen vuoden ajan, joten aivan pohjalta työtä ei tarvinnut kuitenkaan lähteä työstämään.

Opinnäytetyöni alussa määrittelemäni tavoite ja tarkoitus ovat toteutuneet varsin mallikkaasti, kun Citrix Access Gateway -järjestelmän käyttöönotto onnistui suunnitellusti sekä sillä saatiin aikaan tietoturvallinen sekä samalla helppokäyttöinen VPN-järjestelmä käyttäjille. Muutamista ohjelmistojen asennusongelmista huolimatta käyttäjien päätelaitteille sekä jo mainitsemaani DNS-ongelmaa lukuun ottamatta järjestelmän käyttöönotto kokonaisuutena on mennyt aika suunnitellusti läpi. Haasteita on kuitenkin vielä paljon edessä Kiosk Mode -yhteystyypin suunnittelun ja käyttöönoton myötä sekä sen esitestauksessa muutamalla käyttäjällä. Opinnäytetyön tekemisestä on ollut minulle erittäin paljon hyötyä ammatillisen osaamisen kehittämisessä. Lisäksi itse Citrix Access Gateway -järjestelmän suunnittelu-, konfigurointi- ja ylläpitovaiheet ovat antaneet paljon vinkkejä myös projektityöskentelystä. Oikeastaan ainut asia, joka näin jälkeenpäin harmittaa, on opinnäytetyön ja samalla oman valmistumisen pitkittyminen aikatauluongelmien ja ajan riittämättömyyden vuoksi.

Lähteet

Citrix Systems, Inc 2005. Access Gateway Administrator´s Guide. Citrix Access Gateway 4.2. [online] [viitattu 28.1.2007]. http://support.citrix.com/servlet/KbServlet/download/8497-102-14189/VPN_AdminGuide.pdf

Citrix Systems, Inc 2006. Appsrv.ini Parameters Deciphered. [online] [viitattu 18.1.2007]. http://support.citrix.com/article/CTX331178

Citrix Systems, Inc 2005. Citrix Access Gateway with Advanced Access Control Administrator's Guide. Citrix Access Gateway 4.2, Citrix Access Suite. [online] [viitattu 29.1.2007]. http://support.citrix.com/servlet/KbServlet/download/8511-102-14188/Advanced_Access_Control_Guide.pdf

Citrix Systems, Inc 2005. Getting Started with Citrix Access Gateway. Citrix Access Gateway 4.2. [online] [viitattu 28.1.2007]. http://support.citrix.com/servlet/KbServlet/download/8035-102-14001/AG_GettingStarted.pdf

Citrix Systems, Inc 2005. Getting Started with MetaFrame Presentation Server: Citrix MetaFrame Presentation Server 4.0 for Windows, Citrix MetaFrame Access Suite, Version 1.1 [online] [viitattu 16.1.2007]. http://support.citrix.com/servlet/KbServlet/download/6356-102-13850/Getting_Started.pdf

Citrix Systems, Inc 2005. MetaFrame Presentation Server Administrator's Guide. Citrix® MetaFrame® Presentation Server 4.0 for Windows, Citrix MetaFrame Access Suite. [online] [viitattu 16.01.2007]. http://support.citrix.com/servlet/KbServlet/download/6338-102-14087/Administrators_Guide.pdf

Citrix Systems, Inc 2005. Pn.ini Parameters Deciphered. [online] [viitattu 18.1.2007]. http://support.citrix.com/article/CTX145271

Citrix Systems, Inc 2006. Readme for the Access Client Package, Version 4.1. [online] [viitattu 16.2.2007]. http://support.citrix.com/article/CTX108321

Saunders, Jeremy 2005. Creating A Pre-configured ICA Client. [online] [viitattu 18.01.2007]. http://www.appdeploy.com/packages/detail.asp?id=539

Secure Computing Inc. 2007. SafeWord for Citrix: App note. [online] [viitattu 2.2.2007]. http://www.securecomputing.com/pdf/SW4C-ServerSync-appnote.pdf

Secure Computing Inc. 2007. SafeWord for Citrix: Business case solutions brief. [online] [viitattu 2.2.2007]. http://www.securecomputing.com/pdf/SW4C-access-sb.pdf

Secure Computing Inc. 2007. SafeWord for Citrix: Product overview. [online] [viitattu 4.2.2007]. http://www.securecomputing.com/pdf/sw4c_po.pdf

Secure Computing Inc. 2006. SafeWord product guide. [online] [viitattu 10.2.2007]. http://www.securecomputing.com/techpubs_download.cfm?id=1608

Shinder, Debra Littlejohn 2005. Comparing VPN Options. [online] [viitattu 23.1.2007]. http://www.windowsecurity.com/articles/VPN-Options.html

Steinberg, Joseph. Speed, Timothy 2005. SSL VPN: Understanding, evaluating, and planning secure, web-based remote access. [online] [viitattu 24.1.2007]. http://sslvpnbook.packtpub.com/SSL_VPN_SampleExcerpt3_How_SSLVPNs_Work.pdf

Ted Harwood 2002. Installing and Deploying Citrix ICA Clients. [online] [viitattu 18.01.2007]. http://www.awprofessional.com/articles/article.asp?p=29637&seqNum=1&rl=1

VMware Inc. 2006. VMware ESX Server: Platform for virtualizing servers, storage and networking. [online] [viitattu 12.1.2007]. http://www.vmware.com/pdf/esx_datasheet.pdf