Aki Helkiö

DirectAccess-testiympäristön rakentaminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

10.10.2012

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Aki Helkiö DirectAccess-testiympäristön rakentaminen 42 sivua 10.10.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Kari Järvi

Tässä insinöörityössä tarkastellaan DirectAccess-tekniikkaa ja sen käyttämiä transitioteknologioita turvallisen ja automatisoidun yhteyden muodostamisessa. Työssä vertaillaan lyhyesti DirectAccessin etuja tavanomaiseen VPN-tekniikkaan. Tämän ohella käydään läpi tärkeimpiä käyttöönotossa tarvittavia komponentteja ja työvaiheita.

IPv6-protokollan tuomia etuja myös tarkastellaan lähemmin verkkotietoturvan ohella. Turvallisten etäyhteyksien toteutuksissa IPv6-protokollan käyttöönotto on edennyt vaiheittain. IPv4-protokollan käyttöä tullaan ylläpitämään vielä vuosia. Tämä johtuu siitä, että monet yritykset eivät vielä ole siirtyneet kokonaan uusimman protokollan käyttöön esimerkiksi kustannussyistä. Ennen kuin täysi muutos IPv6-verkkoihin toteutetaan, on tarpeellista käyttää transitioteknologioita verkon vaiheittaiseen muutokseen. Tähän tarpeeseen suunniteltuja transitioteknologioita tarkastellaan DirectAccess-tekniikan yhteydessä.

Työn alkuosassa käydään läpi IP-teknologian ja sen tietoturvan muodostamisessa käytetyt tärkeimmät osat. Lisäksi tarkastellaan tunneloinnin periaatetta ja varmenteiden oleellisuutta verkkotietoturvan osana. DirectAccess-palvelimen ja asiakaskoneen yhdistämisprosessi käydään läpi. Tämän ohella DirectAccessin käyttämät yleisimmät toteutus- ja yhteysmuodot pyritään kattamaan. Tämän lisäksi tarkastellaan Windows Server 2012 -version tuomia parannuksia DirectAccess-tekniikan käyttöönotossa. Työssä toteutettiin virtuaalisesti DirectAccess-teknologian käyttöönottoa varten simuloitu verkko, jonka avulla tarkasteltiin toteutuksen vaatimia vaiheita. Toteutus tehtiin Windows Server 2008 R2 -käyttöjärjestelmällä varustettujen koneiden avulla ja apuna käytettiin Microsoftin lähdekirjallisuutta sekä TechNet-verkkosivuja.

Avainsanat	Windows Server 2008, AD DS, VPN, DirectAccess

Author(s) Title Number of Pages Date	Aki Helkiö DirectAccess Test Environment 42 pages 10 September 2012
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Kari Järvi, Principal Lecturer

This thesis surveys the technologies needed in building a test environment for an automatized secure remote access environment using Microsoft DirectAccess technology. The advantages of DirectAccess are briefly compared with common VPN technologies. In addition, the required components needed to the deployment of DirectAccess are examined in more detail.

The advantages of IPv6 protocol are studied more closely together with network security. The introduction of IPv6 protocol has proceeded in phases. However the use of IPv4 will still continue for years due to high costs of newer network components that offer IPv6 capabilities. In order to make a complete change to IPv6, transition technologies are needed. These transition technologies are examined together with DirectAccess.

IP-technologies and the most important parts needed to form network security are examined in the first part of the thesis along with the use of certificate based authentication and tunneling techniques. The connection process between the DirectAccess server and the client together with the usual access models are also surveyed. Furthermore, the improvements of DirectAccess in Windows Server 2012 are examined. A simulated network for the deployment of DirectAccess technolgy was built in a virtualized environment. The components needed for the deployment were surveyed in this way. Two servers were installed with Windows Server 2008 R2 operating systems and were used to implement the use of DirectAccess technology along with one client computer equipped with Windows 7 Enterprise version. Microsoft source material and its TechNet web pages were used as reference in the study and to assist the installing process of the virtualized environment.

Keywords	Windows Server 2008, AD DS, VPN, DirectAccess

Sisällys

Lyhenteet

AH	Authentication Header. IPsec-todennusotsake.
AD	Active Directory, Aktiivihakemisto. Microsoftin Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu.
Autenttinen	Aito, väärentämätön, luotettava.
CA	Certification Authority, varmenteen myöntäjä.
CIDR	Classless Inter-Domain Routing. Internet-osoitteiden luokaton reititysmenettely, jossa käytetään vaihtelevanmittaista verkkopeitettä; myös verkkopeitteen esitysmuoto.
CRL	Certificate Revocation List, kumottujen varmenteiden luettelo.
DC	Domain Controller. Toimialueen ohjauskone.
DHCP	Dynamic Host Configuration Protocol. Menettely IPv4-osoitteiden ja parametrien automaattiseen jakeluun.
DHCPv6	Dynamic Host Configuration Protocol version 6. Menettely IPv6-osoitteiden ja parametrien automaattiseen jakeluun.
DMZ	Verkon osa, demilitarisoitu alue, joka yhdistää yrityksen yksityisen verkon turvattomampaan liityntään kuten internetiin.
DNS	Domain Name System. Internetin nimipalvelujärjestelmä, jonka avulla kuvataan symboliset verkkotunnukset internet-osoitteiksi ja päinvastoin. Voi sisältää myös muita kuvaustietueita, mm. sähkö-postin ja Aktiivihakemiston komponenttien määrittelyt.
ESP	Encapsulating Security Payload. IPsecin koteloitu salattu tietokenttä.

HEADER	Otsake. Tiedonsiirrossa käytettäviin siirtoyksikköihin (kehykset, pa-ketit, segmentit) liitetty hallinta- ja ohjaustietoa sisältävä rakenne.
HTTP	HyperText Transfer Protocol. Protokolla, jota www-palvelimet ja selaimet käyttävät tiedonsiirtoon.
HTTPS	HyperText Transfer Protocol Secure. Suojattu protokolla, jota www-palvelimet ja selaimet käyttävät tiedonsiirtoon.
ICMP	Internet Control Message Protocol. IPv4-ohjausprotokolla, jota käytetään ohjaus-, tila- ja virhesanomien välittämiseen.
ICMPv6	Internet Control Message Protocol version 6. IPv6-ohjausprotokolla, jota käytetään ohjaus-, tila- ja virhesanomien välittämiseen.
IKE	Sovellustason avaintenvaihtoprotokolla. IKE-osapuolet neuvottelevat yhteiset turvaparametrit.
IP	Internet-protokolla. Teknologia, joka mahdollistaa tiedon siirtämisen verkon yli.
IP-HTTPS	IP over HTTPS. Protokolla IPv6-pakettien siirtoon HTTPS-yhteyden yli.
IPv4	Internet Protocol version 4. Internet-protokolla versio 4.
IPv6	Internet Protocol version 6. Internet-protokolla versio 6.
IP Packet	IP-paketti, IP-datagrammi. Internet-liikennöinnin perussiirtoyksikkö.
IPSec	Internet Protocol Security. Joukko protokollia, jotka auttavat verkon tietoliikenteen suojaamisessa.
NAT	Network Address Translation. Menettely paikallisen osoitteen kuvaamiseen julkiseksi esimerkiksi verkkovierailun ajaksi.
OSI-malli	Open Systems Interconnection Reference Model. Tietoliikenteen viitemalli.

PKI	Public Key Infrastructure. Julkisten avainten hallintajärjestelmä.
GP	Group Policy, ryhmäkäytäntö, Aktiivihakemistossa sijaitseva keskitettyjen hallintatyökalujen joukko.
SSL	Secure Sockets Layer. Tietoverkkosalausprotokolla.
TCP	Transmission Control Protocol. Luotettava kuljetuskerroksen tiedonsiirtoprotokolla.
TCP/IP-malli	Transmission Control Protocol/Internet Protocol -malli. Tietoliikenteen viitemalli.
TSL	Transport Layer Security, aiemmin tunnettu nimellä Secure Sockets Layer (SSL), on salausprotokolla, jolla voidaan suojata internet-sovellusten tietoliikenne IP-verkkojen yli.
UDP	User Datagram Protocol. Epäluotettava kuljetuskerroksen tiedonsiirtoprotokolla.
Varmenne	Certificate. Varmentajan (Cerificate Authority) allekirkoittama sähköinen dokumentti, jolla identiteetti varmistetaan.
VPN-yhteys	VPN-yhteys on yhteyden osuus, jossa tieto salataan.
XML	Extended Markup Language. Tiedon mallinnuksessa käytettävä avoin merkkauskieli.

1 Johdanto

Palveluiden etäkäyttö on kasvanut merkittävästi viimeisten vuosien aikana. Suuret yritykset tarjoavat monipuolisia pilvipalveluita sekä yrityksen omiin tarpeisiin että tavallisille käyttäjillekin. Kaikki tieto ei kuitenkaan ole avointa, ja yrityksien projekteja, ohjelmistoja ja palveluita pyritään suojaamaan ulkopuolista käyttöä vastaan.

VPN-yhteydet, eli virtuaaliset yksityiset verkot, ovat yleisin tapa yhdistää kaksi erillistä verkkoa toisiinsa internetin välityksellä. VPN-sovelluksia käytetään erilaisissa ympäristöissä, mutta monissa tapauksissa yhteyden luominen ja yhteyksien katkeileminen ja uudelleen kytkeytyminen koetaan käyttäjien kannalta hankalaksi.

Microsoft on kehittänyt etäyhteyksille oman ratkaisunsa, joka eroaa toiminnallisuudeltaan jonkin verran tavanomaisista VPN-ratkaisuista. Palvelu on nimeltään DirectAccess, ja se toimii Windowsin Aktiivihakemistoympäristössä, jossa asiakkaiden ja palvelimen on oltava toimialueen jäseniä. DirectAccess-palvelun avulla käyttäjät voivat liikennöidä tietoturvallisesti ilman erikseen kytkettävää VPN-yhteyttä. Käyttäjällä on automaattisesti yhteys DirectAccess-palvelimeen aina, kun hän on liittyneenä internetiin.

DirectAccess-palvelun tärkeimmät edut perinteiseen VPN-yhteyteen nähden ovat automaattinen liittyminen palvelimeen, näkymätön uudelleenliittyminen yhteyskatkoksen jälkeen ja palomuurien konfiguroinnin helpottuminen. DirectAccess käyttää tiedon salaamiseen IPSec-protokollaa ja vaatii toimiakseen IPv6-ympäristön ja sekaverkoissa 6to4-, Teredo- ja IP-HTTPS protokollat.

Työssä selvitettiin DirectAccess-testijärjestelmän rakentamista Metropolian tietoverkkolaboratorion virtuaaliklusteriin VMware-ympäristöön. Aluksi käsitellään lyhyesti IP-protokollien rakenteesta painopisteen ollessa IPv6-protokollassa. Seuraavaksi tarkastellaan tietoliikenteen tietoturvaa ja tietoturvamenettelyjä. DirectAccess-protokolla esitellään yksityiskohtaisesti ja lopuksi kuvataan testijärjestelmän rakentamisessa huomioitavat seikat.

2 Internet-protokollat

Tietoliikenneprotokollia voidaan tarkastella OSI-viitemallin avulla (Open Systems Interconnection Reference Model). OSI-mallissa tietoliikenne ja sovellukset jaetaan seitsemälle kerrokselle niin, että alimpana on fyysinen kerros, joka määrittelee kaapeloinnin, liittimet ja signaalit. Ylimpänä on sovelluskerros, joka huolehtii ohjelmien viestien paketoimisesta. Hierarkia kasvaa alhaalta ylöspäin. Kuviossa 1 vasemmalla on esitetty kuva OSI-mallista. Siirtoyhteyskerros sisältää mm. lähiverkon palvelut. Internetprotokollat sijaitsevat verkkokerroksella. Kuljetuskerroksella ovat TCP- ja UDP-protokollat.

Toinen internetprotokollien kuvauksessa käytetty malli on TCP/IP-viitemalli, joka on nimetty kahden pääprotokollan, TCP:n ja IP:n mukaan. Se muodostaa itse asiassa internetin de facto -protokollastandardin, ja siihen liittyy runsaasti RFC-julkaisuja. TCP/IP-malli on esitetty kuviossa 1 oikealla. [4.]

Kuvio 1. OSI- ja TCP/IP-malli [4,5]

2.1 IP-protokollat

Vanhemman IP-protokollaversion IPv4:n osoitteen pituus on 32 bittiä. Se esitetään tavallisesti jaettuna neljään kahdeksan bitin mittaiseen osaan, oktettiin, jotka on koodattu desimaaliseksi ja erotettu toisistaan pisteellä.

Osoitteesta käytetään joskus myös nimitystä pisteosoite (engl. dotted address). IPv4-osoite on hierarkkinen. Sen alkuosa määrittelee verkon ja loppuosa työaseman osoitteen verkossa.

Osoiteavaruus on jaettu viiteen luokkaan, joista kolme ensimmäistä (luokat A, B ja C) on tarkoitettu täsmälähetysosoitteiksi (unicast), neljäs, luokka D, ryhmälähetykseen (multicast) ja viides on varattu tulevaisuuden tarpeisiin. Näitä osoitteita kutsutaan luokallisiksi osoitteiksi, ja osoitteen luokka näkyy suoraan ensimmäisen oktetin ylimpien bittien perusteella. Osoiteluokat esitetään taulukossa 1. [5.]

Taulukko 1. IPv4-osoiteluokat

Luokka	Alkubitit	Osoitteet	Verkko-bitit	Verkkojen lkm	Osoitteita verkossa
A	0	1.0.0.0-126.255.255.255*)	8	126	16777216
B	10	128.0.0.0-191.255.255.255	16	16384	65536
C	110	192.0.0.0-223.255.255.255	24	2097152	256
D	1110	224.0.0.0-239.255.255.255	-	-	-
E	1111	-	-	-	-

IPv4-osoitteisiin liittyy oleellisesti aliverkon peite (verkkopeite, net mask). Sen avulla kerrotaan, mikä osa osoitteesta kuuluu verkkoon ja mikä työasemaan. Verkkopeite on 32-bittinen luku. Sen eniten merkitsevästä osasta alkava peräkkäisten 1-bittien joukko määrittää verkon osuuden, ja lopun 0-bitit kertovat työaseman osuuden. Verkon tunnus saadaan IPv4-osoitteesta suorittamalla bittikohtainen ja-operaatio osoitteen ja verkkopeitteen välillä.

Osa IPv4-osoiteavaruudesta on varattu erikoistarkoituksiin. Verkot 10.0.0.0, 172.16.0.0-172.31.0.0 ja 192.168.0.0-192.168.255.0 ovat ns. yksityisiä verkkoja (private network). Niitä voidaan käyttää organisaatioiden sisäverkoissa vapaasti, mutta niitä ei reititetä ulkoiseen verkkoon.

Yksityisten verkkojen avulla IP-osoiteavaruutta voidaan käyttää tehokkaammin osoitteenmuunnostekniikan (NAT, Network Address Translation) avulla, jolla yksityiset osoitteet kuvataan julkisiksi osoitteiksi, kun paketti ohjataan julkiseen verkkoon. Yhtä julkista osoitetta voidaan käyttää useisiin samanaikaisiin yhteyksiin hyödyntämällä porttinumeroita (Port Address Translation, NAPT, PAT).

Verkkoa 169.254.0.0 käytetään automaattisessa osoitteiden luonnissa (Automatic Private IP Addressing, APIPA). Jos kone on konfiguroitu käyttämään dynaamista osoitteiden hakua eikä verkossa ole DHCP-palvelinta tai DHCP-palvelinta ei tavoiteta, APIPA-osoite otetaan käyttöön automaattisesti. Verkko 127.0.0.0 on varattu testikäyttöön.

IPv4-osoitteet voidaan jaotella myös käyttötapansa perusteella. Täsmälähetyksessä (unicast) paketti lähetetään yhdeltä lähettäjältä yhdelle kohteelle, joilla kummallakin on oma yksikäsitteinen osoitteensa. Yleislähetysosoite (broadcast) on tarkoitettu kaikille asemille ja käsitellään kaikissa samassa yleislähetysalueessa olevissa koneissa. Ryhmälähetys (monilähetys, multicast) esitetään omana osoiteluokkanaan, luokka D. Sen osoitteet ovat välillä 224.0.0.0-239.255.255.255. Ryhmälähetyksessä sama osoite konfiguroidaan kaikille saman ryhmän asemille.

1990-luvun alussa otettiin käyttöön luokattomat osoitteet (CIDR, Classless Interdomain Routing). Tässä menettelyssä osoiteluokilla ei ole merkitystä, vaan IP-osoite määritellään osoitteen ja verkkopeitteen avulla. Verkkopeitteen 1-bitit kertovat verkon ja loppuosa osoitteesta työaseman tunnuksen verkossa. Verkkopeite esitetään CIDR-osoittessa muodossa /n, jossa n on verkkopeitteen 1-bittien lukumäärä. Tämä esitystapa on otettu käyttöön myös luokallisten osoitteiden esittelyssä ja myöhemmin IPv6-osoitteissa.

Uudempi, jo monissa paikoin käytetty IP-protokolla on IPv6. Siinä osoitteen pituus on 128 bittiä. Teoreettisesti käytettävissä on 2^{128} eli $3{,}4 \times 10^{38}$ osoitetta. Osoitteissa 64 bittiä on varattu oletuksena verkolle ja 64 bittiä työasemalle. Osoitteet koodataan heksadesimaalisena neljän numeron (16 bittiä, sana) ryhmiin kaksoispisteillä erotettuina. Seuraavana on esimerkki IPv6-osoitteesta.

2001:DB8:0000:0000:0202:B3FF:FE1E:8329

Etunollat ryhmien sisällä voidaan jättää pois.

2001:DB8:0000:0000:202:B3FF:FE1E:8329

Jos osoite sisältää peräkkäisiä nollia ryhmän sisällä, ne voidaan lyhentää yhdeksi.

2001:DB8:0:0:202:B3FF:FE1E:8329

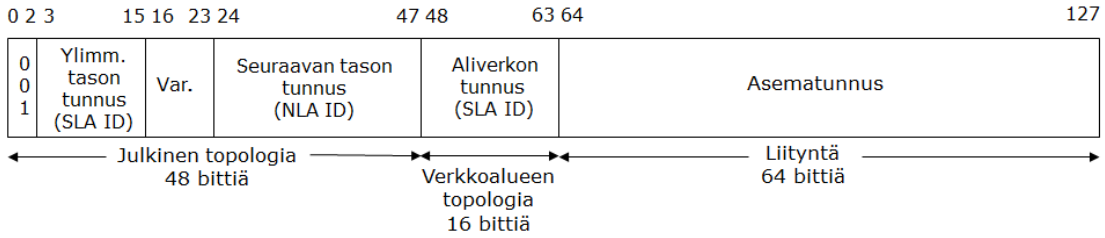
Jos osoite sisältää peräkkäisiä nollajoukkoja, ne voidaan yhdistää, ja merkitä kahdella peräkkäisellä kaksoispisteellä. Nollajoukkoja ei voida yhdistää, mikäli osoitteessa on useampia nollajoukkoja, jotka eivät ole peräkkäisiä.

2001:DB8::202:B3FF:FE1E:8329

Osoitteissa verkon osuus ilmaistaan osoitteiden perässä prefiksinä, kauttaviivalla eroteltuna samaan tapaan kuin CIDR-osoitteissa. Esimerkiksi osoitteesta fec0:0:0:1::1234/64 on poistettu etunollat ja yhdistetty yksi peräkkäinen nollajoukko, jolloin sen arvo on todellisuudessa fec0:0000:0000:0001:0000:0000:0000:1234/64. Ensimmäiset 64 bittiä ovat verkon tunnus (fec0:0000:0000:0001), prefiksi /64, ja loput 64 bittiä ovat asematunnus (0000:0000:0000:1234).

IPv6-osoitteet jaetaan IPv4-osoitteiden tapaan käyttötapansa mukaan eri osoitetyyppeihin. Näitä ovat täsmälähetysosoitteet (unicast), ryhmälähetysosoitteet (monilähetys, multicast) ja jokulähetysosoitteet (anycast). Yhteislähetystä (broadcast) ei ole määritelty standardissa.

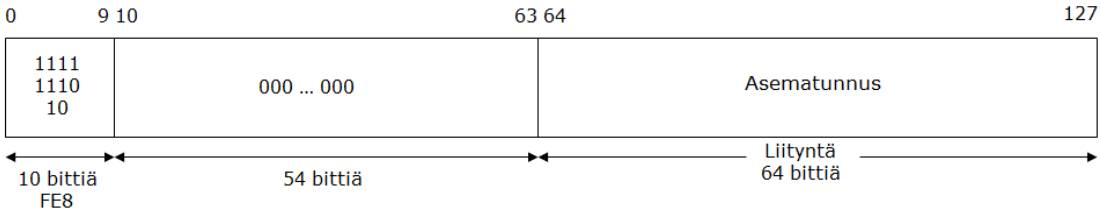
Julkiset täsmäosoitteet vastaavat julkisia IPv4-osoitteita. Ne ovat reitittyviä ja toimivat internetissä. Julkisen täsmäosoitteen prefiksi on alueella, joka alkaa biteillä 001. Kuviosta 2 nähdään osoitteen rakenne.



Kuvio 2. Julkinen IPv6-osoite

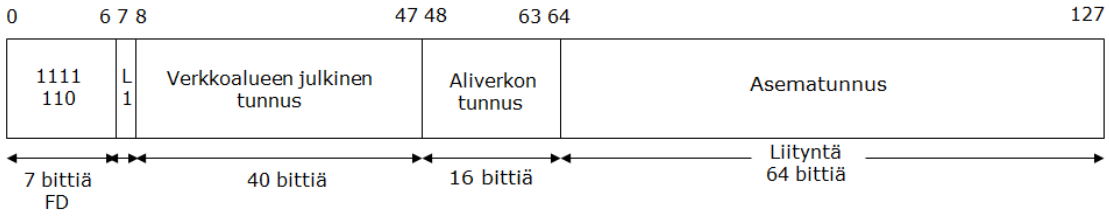
Linkkiosoitteita (Link local) käytetään kommunikoinnissa samassa linkissä sijaitsevien koneiden välillä. Ne vastaavat IPv4:n 169.254.0.0/16-osoitteita (APIPA). Ne konfiguroituvat aina automaattisesti verkkoliityntään, eli liitynnällä on aina ainakin linkkiosoite. Linkkiosoite alkaa arvolla fe80 (prefiksiFE80::/64). IPv6-reititin ei reititä näiden osoitteiden liikennettä toisiin segmentteihin.

Kun asema kytketään verkkoon, se luo itselleen automaattisesti linkkikohtaisen osoitteen, joka muodostuu prefiksistä ja yksikäsitteisestä asematunnuksesta. Kuviossa 3 on esitetty linkkiosoitteen rakenne.



Kuvio 3. Paikallisen IPv6-linkkiosoitteen rakenne

Yksikäsitteiset paikallisosoitteet (paikallisosoitteet, unique local unicast-osoitteet) ovat täsmäosoitteita, joiden avulla yritys voi rakentaa oman paikallisen osoiteavaruuden. Osoitteen rakenne on esitetty kuviossa 4.



Kuvio 4. Yksikäsitteisen IPv6-paikallisosoitteen rakenne

IPv6-osoitteen asematunnus muodostetaan yleensä liitynnän MAC-osoitteesta (Modifioitu EUI-64-osoite). Lähiverkon adapterin fyysisenä osoitteena, MAC-osoitteena, on IEEE:n määrittelemä 48-bittinen EUI-48-osoite, joka muodostuu 24 bitin valmistajatunnuksesta ja 24 bitin valmistajakohtaisesta sarjanumerosta. Se muunnetaan uudemmaksi 64-bittiseksi EUI-64-osoitteeksi lisäämällä valmistajakentän jälkeen arvo 0xFFFE. Modifioitu EUI-64-osoite saadaan tästä kääntämällä valmistajakentän universal/local-bitti (seitsemäs bitti eniten merkitsevästä päästä lukien).

Jos liitynnän osoite on esimerkiksi 00-AA-00-3F-2A-1C, se muunnetaan EUI-64-osoitteeksi lisäämällä valmistajakentän 00-AA-00 jälkeen FF-FE, jolloin tuloksena on 64-bittinen osoite 00-AA-00-FF-FE-3F-2A-1C. Seuraavaksi käännetään u/l-bitti ja tuloksena saadaan modifioitu EUI-64-osoite 02-AA-00-FF-FE-3F-2A-1C.

Kun IPv4- ja IPv6-protokollia käytetään yhtä aikaa, on turvauduttava yhteiskäyttötekniikoihin. Niitä ovat muunnostekniikat, joissa IPv6-paketeista muodostetaan IPv4-paketteja, tunnelointitekniikat, joissa IPv6-paketit viedään IPv4-verkon yli IPv4-paketeissa sekä yhteiskäyttö, jolloin protokollapinossa ovat käytössä samalla kertaa sekä IPv6- että IPv4 -protokollat.

2.2 Tunnelointi

Tunneloinnilla tarkoitetaan prosessia, jossa päätelaite kapseloi IP-paketin toiseen IP-otsakkeeseen. IPv6-IPv4-tunneloinnissa IPv6-paketti laitetaan IPv4-paketin sisään, jolloin IPv6-liikenne voidaan välittää IPv4-verkon ylitse. Automaattisesti konfiguroituvat tunnelit ovat IPv4-yhteensopiva IPv6-tunneli, joka on poistumassa käytöstä, 6to4-tunneli ja ISATAP-tunneli.

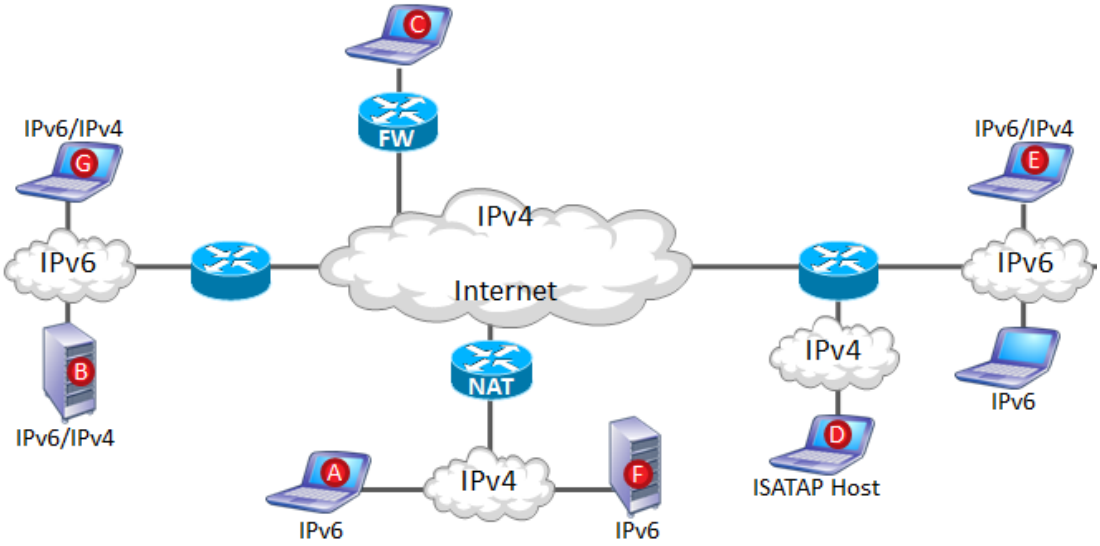
6to4-tunnelit rakentuvat automaattisesti reunareitittimiin. Ne hyödyntävät IPv6-6to4-osoitteessa olevaa IPv4-osoitetta seuraavasti. Kun reitittimeen tulee paketti, jonka kohdeosoitteen prefiksi on 2002::/16, reititin tietää, että se on ohjattava 6to4-tunneliin. Reititin erottaa 6to4-osoitteessa olevan IPv4-osoitteen, joka on kohdepään reitittimen osoite. Esimerkiksi IPv4-osoite on 157.54.1.26 eli heksadesimaalisena 9d36:017a on 6to4-muodossa 2002:9d36:17a::/48.

Toinen yleisesti käytetty tunnelointiprotokolla on ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), jota käytetään yhdistämään IPv4/IPv6-solmuja IPv4-verkon yli. Sen toiminta on samankaltainen 6to4-protokollan kanssa. Alun perin ISATAP tarkoitettiin tunnelointiin verkkoalueen sisällä. ISATAP-osoite muodostuu 64-bittisestä prefiksistä (julkinen täsmäosoite, linkkiosoite tai verkkoalueosoite) ja 64-bittisestä asematunnuksesta, joka muodostetaan ISATAP-tunnuksesta 0:5efe ja IPv4-osoitteesta. Esimerkiksi IPv4-osoite 10.1.1.100 on muotoa 2002:5414:8e4e:1::5efe:10.1.1.100, kun IPv6-prefiksi on 2002:5414:8e4e:1::/64.

Teredo on tekniikka, jossa IPv6-liikenne tunneloidaan IPv4-verkon yli, kun yhteiskäyttösolmut ovat IPv4-NAT:in takana. IPv6-paketit kapseloidaan tunneloinnissa IPv4:n UDP-paketteihin.

Sisäverkon yhteysvaihtoehdot ovat natiivi IPv6-reititys, jossa kaikki työasemat on varustettu IPv6-osoitteilla tai ISATAP-tunnelointi, jos joukossa on koneita IPv4-osoitteilla ja jotka eivät ole konfiguroitu IPv6 osoitteilla.

Ulkoverkossa, jossa liikenne kulkee IPv4-verkon ja NATin läpi, on käytettävä Teredo-tunnelointia. Jos työasemalla on julkinen IPv4-osoite, käytetään 6to4-tunnelointia. Jos mikään tunnelointiratkaisu ei ole mahdollinen, voidaan käyttää IP-HTTPS:ää.



Kuvio 5. Tunnelointivaihtoehtoja

Kuvio 5 selventää eri tunnelointivaihtoehtoja. Julkisen verkon kautta liitettyjen koneiden A ja B välillä on käytettävä Teredo-tunnelointia ja koneiden A ja C välillä vastaavasti IP-HTTPS:ää. IPv6-sisäverkossa koneiden D ja E välillä käytetään ISATAP-tunnelointia ja IPv4-sisäverkossa koneiden A ja F välillä 6to4-tunnelointia. Koneiden E ja G välille voidaan luoda internetin yli manuaalinen 6to4-tunneli, joka sijaitsee reunareitittimen välissä.

3 Internet-tietoturvaratkaisut

Tietoturva jaetaan viiteen osa-alueeseen, jotka ovat luottamuksellisuus, autenttisuus, kiistämättömyys, eheys ja käytettävyys. Luottamuksellisuus tarkoittaa, että tietoja voivat käyttää vain henkilöt, joilla on niihin käyttöoikeus. Autentikoinnin avulla tunnistetaan käyttäjät. Kiistämättömyys on tapahtumien kirjaamista myöhempää tarkastelua varten. Eheydellä tarkoitetaan tietojärjestelmässä tietojen muuttumattomuutta esimerkiksi tiedonsiirron aikana. Käytettävyys puolestaan on sitä, että tiedot ja järjestelmät ovat aina tavoitettavissa.

Tietojärjestelmien tietoturvaa voidaan tarkastella osa-alueittain. Tässä työssä tarkasteltiin tietoliikenteen turvallisuutta ja menetelmiä, joilla varmistetaan, etteivät ulkopuoliset pääse käsiksi siirrettäviin tietoihin.

3.1 IP-HTTPS

VPN-yhteydet käyttävät tavallisesti PPTP- tai L2TP/IPsec-tunnelointia tiedon turvalliseen siirtämiseen. Palomuurit ja proxyt eivät aina päästä tunneloitua liikennettä lävitseen, mistä syystä on kehitetty HTTPS-protokollaa käyttäviä ratkaisuja.

HTTPS on HTTP-protokollan ja SSL/TLS-protokollan yhdistelmä, jota käytetään tiedon suojattuun siirtoon internetissä. Tiedot salataan ennen lähettämistä SSL-protokollan tai TLS-protokollan avulla. HTTPS-liikenne läpäisee useimmat palomuurit ja proxyt.

Microsoft on kehittänyt IP over HTTPS (IP-HTTPS) -protokollan, jota käytetään IPv6-pakettien siirtoon HTTPS-yhteyden yli. Protokollassa määritellään roolit asiakas (client) ja palvelin (server). Kumpikin voi käyttää tiedonsiirtoon joko HTTPS- tai HTTP-protokollaa.

DirectAccessissa viimeisenä vaihtoehtona, mikäli natiivia IPv6 verkkoa ei ole saatavilla eikä yhteys muuten onnistu palvelimille, otetaan käyttöön IP-HTTPS.

3.2 IPsec

IPsec (Internet Protocol Security) on joukko TCP/IP-perheeseen kuuluvia protokollia, joiden avulla IP-liikenne suojataan. IPsec sijaitsee OSI-mallissa verkkokerroksessa, mikä antaa lisää joustavuutta verrattuna ylemmillä kerroksilla toimiviin salausratkaisuihin. Toisaalta verkkoliikenteen vakaus ja sanomien pirstoutuminen voivat aiheuttaa ongelmia. Niiden käsittely on tyypillisesti tapahtunut kuljetuskerroksessa.

IPsec on kooste avoimia standardeja, eikä se määrittele käytettäviä salausalgoritmeja, joten se on luonteeltaan hyvin yleinen ja joustava kokonaisuus. Tärkein IPsecin tehtävä on salata tai autentikoida liikenne IP-tasolla. IP-pakettien salaaminen on käytännöllisempää kuin esimerkiksi itsenäisten sovelluksien salaaminen, sillä sovelluksen tekijä on yleensä tällöin vastuussa tietoturvan kehittämisestä ja ylläpidosta. Täten keskitetty salaus protokollaan on tehokkaampaa ja vaivattomampaa. Koska IPsec sijaitsee OSI-verkkokerroksessa, se voi suojata sovelluksien lähettämät paketit, kuten etäyhteyden, sähköpostin, FTP- ja web-yhteydet. [1, s. 67.]

IPsec sisältää siis mekanismit lähetetyn tiedon salassapitoon, takuun ettei, tietoja ole käsitelty matkan varrella, tiedon alkuperän tarkastuksen ja eston toistohyökkäyksiä vastaan. Riippuen käyttötavasta IPSec-suojaus voidaan luoda kolmella tavalla: Host-to-Host-, Gateway-to-Gateway- ja Host-to-Gateway -periaatteilla. [1, s. 68.]

IPsec tukee DirectAccess-yhteyksissä kahta tunnelointimuotoa, joita ovat End-to-End ja End-to-Edge. End-to-End, eli päästä päähän, turvaa koko yhteyden alusta loppuun työasemilta intraverkon palvelimille. End-to-Edge turvaa vain DirectAccess-palvelimelle tulevan yhteyden antaen intrassa liikkuvan liikenteen mennä salaamattomana.

Paras turvallisuus DirectAccessin avulla saadaan käyttämällä End-to-End-yhteysmuotoa ja pitämällä intranetin palvelimet ajan tasalla. End-to-Edgen toimintaperiaate muistuttaa hyvin paljon VPN-teknologiaa ja se on paljon nopeampi ottaa käyttöön. End-to-Edge-yhteyttä käytetään, kun ei haluta IPv6:tta ja IPseciä samaan aikaa käyttöön kaikkiin verkon elementteihin. [8.]

3.2.1 IPsec-rakenne

IPsec käyttää kahta protokollaa liikenteen suojaamiseen. Ne ovat Authentication Header (AH) ja Encapsulated Security Payload (ESP). Nämä protokollat lisäävät uuden otsakkeen IP-pakettiin helpottaen muiden reitin välissä olevien laitteiden reitittämistä.

Liikenteen suojaamisen lisäksi IPsec käyttää suojaussidoksia, Security association (SA), joiden avulla sovitaan yhteyden muodostuksessa käytettävistä palveluista. Avainten hallintaan ja vaihtoon käytettävä infrastruktuuri eli Internet Key Exchange (IKE) on kolmas osa IPsec-kokonaisuutta. [1, s. 68.]

3.2.2 IPsec-yhteysmuodot

IPsec tukee kahta yhteysmuotoa: Transport modea ja Tunnel modea. Transport- ja Tunnel-muotojen suurin ero on niiden tapa salata IP-paketit. Transport mode salaa vain IP-paketin data payload -osan (hyötykuorma), kun taas Tunnel mode salaa koko alkuperäisen IP-paketin ja sijoittaa sen toisen IP-paketin sisälle, jotta mitään muutoksia ei paketin matkan varrella voida tehdä. [1, s. 75.]

3.3 Julkisen avaimen infrastruktuuri

1970-luvun puoliväliin asti symmetrinen kryptografia oli ainoa käytännöllinen tapa turvalliseen kommunikointiin. Tämä tarkoitti sitä, että kaikkien kommunikoivien tahojen oli tiedettävä sama salasana turvallisen yhteyden muodostamiseen.

Asymmetrinen salaus oli mahdollista, mutta siitä puuttui selkeä ja turvallinen tapa siirtää yksityisiä avaimia julkisen verkon ylitse. Whitfield Diffie ja Martin Hellman kehittivät vuonna 1976 selkeän julkisen avaintenvaihtomenetelmän, joka tuki asiakkaiden oikellisuuden todentamista. Tämän innoittamana nykypäivänä löytyy useita julkisien avaimien kryptografiajärjestelmiä, kuten RSA. [1, s. 410.]

Public key infrastructure (PKI), eli julkisen avaimen infrastruktuuri on asymmetriseen salaukseen, avainten luomiseen ja niiden käyttöön perustuva järjestelmä. Sen tarkoitus on todentaa ulkopuolisia tahoja digitaalisten allekirjoituksien ja sertifikaattien (varmenne) avulla. Tämän lisäksi se pyrkii mahdollistamaan turvallisen avainten vaihdon erilaisten tekniikoiden avulla riippuen valitusta tekniikasta. Julkisen avaimen kryptografia perustuu avainparien luomiseen, jossa avaimet on matemaattisesti linkitetty toisiinsa. Oma yksityinen avain salataan julkista avainta käyttäen, jolloin yksityisen avaimen selville saaminen viestistä on muodostettu hyvin haasteelliseksi ja työlääksi ilman vastaavaa avainparia.

Digitaalinen allekirjoitus on tunniste, jolla tiedetään keneltä informaatio tulee. Käytännössä allekirjoitus on asiakkaan yksityisellä avaimella allekirjoitettu salasana johonkin haluttuun viestiin. Viestin eheys ja alkuperä voidaan tämän avulla varmistaa tarkastamalla, kuka viestin on allekirjoittanut. Vastaanottaja voi näin allekirjoituksen ja julkisen avaimen avulla varmistaa, että viesti on pysynyt eheänä siirron aikana. Prosessi ei kuitenkaan ole näinkään yksinkertainen, vaan ennen viestin lähetystä on käytettävä jonkinlaista kryptografista tiivistefunktiota. Yksi tunnetuista tekniikoista on Secure Hash Algorithm (SHA). Tiiviste, eli hash value, toteutetaan käsittelemällä viesti matemaattisella algoritmilla ja muodostamalla siitä määrätyn pituinen jono bittejä.

Digitaaliset varmenteet ovat toinen tärkeä funktio allekirjoituksien ohella ja ne toimivat myös tiedon eheyden ja tietojen oikeellisuuden tarkistajina. Ne ovat käytännössä julkisien avaimien linkittäjiä, joiden avulla oikeaa yksityistä avainta vastaava pari voidaan todentaa oikealle omistajalle.

PKI koostuu monen komponentin yhteistoiminnasta. Tärkein niistä on varmenteen myöntäjä, Certification Authority (CA), joka luo, jakaa ja kumoaa digitaalisia varmenteita. CA jakaa varmenteet vain todennetuille asiakkaille, jotka on hyväksytty listalle. Asiakkaita voivat olla normaali tietokoneen käyttäjä, reititin, palvelin tai jokin muu verkkoon kytketty luotettu kohde. PKI-järjestelmiin on määriteltävä ennaltaan sallitut käyttäjät ja kohteet, joilla on oikeus rekisteröityä (enroll) PKI:n hallintaan.

Toinen tärkeä osa PKI-järjestelmää on rekisteröinnin hallinta, Registration Authority (RA), joka tehtävä on helpottaa CA:n toimintaa varmistamalla rekisteröityvien asiakkaiden oikeellisuus. Nykyisin tämä on useimmiten hyvin automatisoitu prosessi, mutta yhä voi löytyä tahoja, jotka pyytävät esimerkiksi lomakkeen täyttämistä ja sen tietojen varmentamista sähköpostiin lähetettyjen tietojen perusteella.

Julkisten avainten varmenteita ja CRL-listoja (Certificate Revocation List, kumottujen varmenteiden luettelo) varten PKI tarvitsee jonkinlaisen säiliön (repository), josta varmenteet ovat saatavilla asiakkaille. Tämä voi olla X.500-tyylinen hakemisto, johon on määritetty käyttäjäoikeudet LDAP-protokollan avulla käytettäväksi. Se voi myös olla etäpalvelimella sijaitseva tiedosto, johon on yhteys FTP- tai HTTP-protokollan avulla. [1, s. 412.]

Varmenteita on tarpeellista kuitenkin aika-ajoin poistaa käytöstä. Niille on usein annettu voimassaoloaika, jonka umpeutumisen yhteydessä CA kumoaa varmenteen listaamalla sen sarjanumeron CRL-listaan. Tämä voidaan toteuttaa myös ilman ajan umpeutumista esimerkiksi käyttäjän nimen vaihdon yhteydessä tai kun asiakkaan avainpari on vaarantunut. CA käsittelee useimmiten CRL-listoja, mutta on mahdollista valtuuttaa (delegate) listojen hallinta johonkin muuhun kohteeseen, joka on määritelty X.509-standardissa. [1, s. 413.]

Kun PKI on asennettu käyttöön ja sen yhteyteen on liitetty sallittuja asiakkaita, ensimmäinen toimintavaihe on asiakkaan rekisteröinti, jossa käyttäjätiedot tarkistetaan. Kun tiedot ovat kunnossa, asiakkaalle lähetetään avainpari. Avainpari koostuu julkisesta ja yksityisestä avaimesta. Näiden uusien avainparien generointi voidaan toteuttaa lähes missä tahansa luotetussa kohteessa, mutta useimmiten se tapahtuu CA:n toimesta.

Kun asiakas on rekisteröity ja vastaanottanut avaimet, se tarvitsee varmenteen, joka generoidaan annetuilla avaimilla. Avainparit on siirrettävä usein julkisen verkon yli jollain salaustekniikalla, jotta tiedon eheys ja muttumattomuus säilyy. DirectAccess käyttää Diffie-Hellman-avaintenvaihtotekniikkaa, joka on IKEv2-infrastruktuurin ominaisuus. IKEv2-määrittely löytyy RFC4306-dokumentista. Kun avaimet on todennettu, CA lähettää sertifikaatin saatavilla olevaan säiliöön. [1, s. 413.]

4 DirectAccess

4.1 Tuotekuvaus

DirectAccess mahdollistaa Windows 7- ja Windows 8 -käyttöjärjestelmällä varustettujen koneiden nopean liittämisen eri verkosta Windows Server 2008 R2 -toimialueeseen. Toisin kuin VPN-yhteydet, DirectAccess pyrkii muodostamaan koneiden välille suojatun yhteyden automaattisesti ilman, että käyttäjä avaisi erikseen yhteyden. Kaikki yrityksen tarjoamat resurssit, kuten ohjelmat, omat tiedostot ja henkilökohtaiset asetukset tuodaan koneelle käytettäväksi käynnistyksen yhteydessä, mikäli internetyhteys on saatavilla ja käyttäjä on kirjautunut sisään.

Oletusarvoisesti DirectAccess käyttää IPv6-over-IPsec-teknologiaa julkisten verkkojen läpi kulkevan tiedon salaamiseen. Parempaa salausta ja yhteyden muodostusta varten on käytössä varmenteisiin perustuva julkisen avaimen infrastruktuuri (PKI) ja autentikointia varten voidaan käyttää henkilökohtaisen salasanan ja tunnuksen kera henkilökohtaisia älykortteja.

Lisäksi DirectAccess on suunniteltu mahdollistamaan monenlaisia yhteyksien kombinaatioita, kuten internet- ja intraverkon liikenteen erottelu toisistaan, jotta yhteys muuhun maailmaan pysyisi mahdollisimman nopeana [2].

Järjestelmän ylläpitäjän työtä helpotetaan myös, sillä palvelimelle asennettu DirectAccess-manageri mahdollistaa etäkoneiden monitoroinnin sekä järjestelmän että ohjelmien päivittämisen. Kaikki hallinnointi ja päivitysten teko on mahdollista toteuttaa milloin vain, kunhan tietokone on kytketty internetiin [2].

4.2 Toimintaperiaate

DirectAccess-yhteystyyppejä on neljä eri kappaletta. Ensimmäinen ja toimivuudeltaan paras on julkisen IPv6-yhteyden avulla muodostaminen. Mikäli IPv6 ei ole mahdollinen, käytetään 6to4-tunnelointia, jolla IPv6 liikenne kapseloidaan IPv4 paketeiksi.

Taulukko 2. Yhteystyypit. [7, s. 444.]

Client-verkkoyhteystyyppi	DirectAccess-yhteystapa
Julkinen IPv6 osoite	Julkinen IPv6 osoite
Julkinen IPv4 osoite	6to4
Yksityinen (NAT) IPv4 osoite	Teredo
Yhteys internetiin, mutta palomuuri estää liikenteen.	IP-HTTPS

DirectAccess-asiakaskoneen (client) yhdistäminen sisältää monta automatisoitua vaihetta riippuen yhteyden kunnosta ja koneen turvallisuustiedoista. Taulukko 2 havainnollistaa yhteyden muodostamista.

Kun DirectAccess-asiakas kytketään verkkoon, se tarkistaa, onko yhteys intraan jo valmiina. Mikäli yhteyttä ei ole, se pyritään muodostamaan. Yhteys DirectAccess-palvelimeen muodostetaan oletusarvoisesti IPv6- ja IPsec-tekniikoilla. On kuitenkin vielä tavallista, että natiivia IPv6-verkkoa ei ole saatavilla, jolloin asiakas pyrkii käyttämään 6to4- tai Teredo-tekniikkaa paketoidakseen IPv6-liikenteen IPv4-paketteihin. Jos palomuuri tai proxypalvelin estää asiakasta käyttämästä 6to4- tai Teredo-tekniikoita, asiakas siirtyy automaattiesti käyttämään IP-HTTPS-protokollaa.

IPsec-tunneloinnin muodostamisen yhteydessä asiakas ja palvelin autentikoivat toisensa varmenteilla ja tietokoneen käyttäjätilitiedoilla.

Jos verkonkäyttökäytäntö (Network Access Protection, NAP) on käytössä ja konfiguroitu koneen kunnon tarkastamiseen, asiakas pyrkii saamaan varmenteen intranetistä kunnonhallintapalvelimelta (Health Registration Authority, HRA). HRA

välittää asiakkaan turvallisuustiedot kuntokäytäntöpalvelimelle (NAP Health Policy Server).

Verkkokäytäntopalvelimen (Network Policy Server, NPS) asettamien käytäntöjen perusteella NAP päättelee, onko asiakaskoneen järjestelmä kunnossa. Mikäli näin on, HRA antaa asiakkaalle kuntoisuusvarmenteen (health certificate).

Kun käyttäjä kirjautuu sisään, asiakas muodostaa intranet-tunnelin resursseihin. Asiakas ja palvelin todentavat toisensa varmenteilla ja käyttäjän kirjautumisessa käytetyillä tiedoilla. Mikäli NAP on käytössä palvelimella, asiakas lähettää kuntoisuusvarmenteen autentikointia varten. Kun yhteys on valmis, palvelin sallii asiakkaalle pääsyn niihin intran resursseihin, jotka ovat asiakkaalle sallittuja.

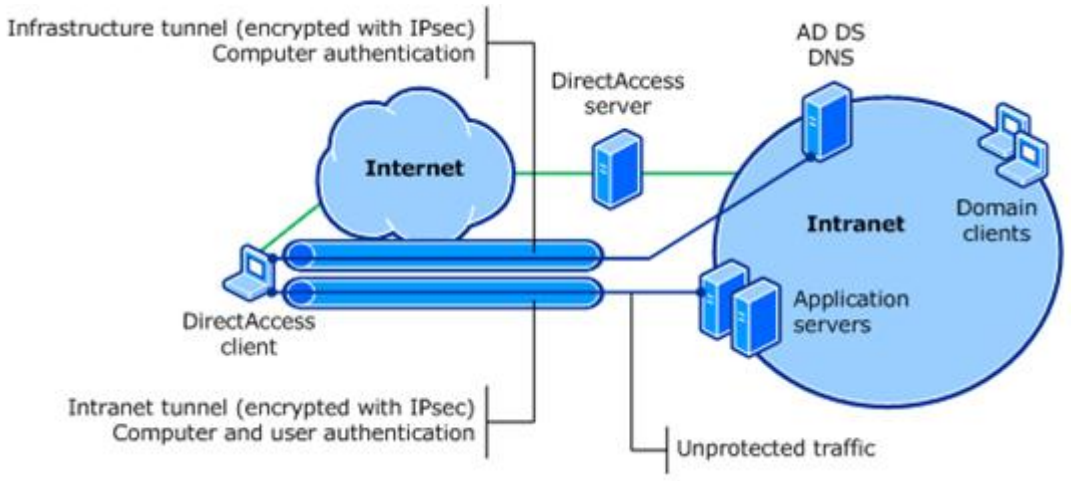
4.3 DirectAccess-yhteysmuodon valitseminen

DirectAccess-yhteysmuotoja on kolme, Full Intranet Access, Selected Server Access ja End-to-End Access. Nämä toteutukset ovat myös sidonnaisia fyysisen kokonaisuuden kanssa, riippuen toteutettavan intraverkon laajuudesta ja mahdollisesta aliverkotuksesta. Nämä toteutukset eivät myöskään ota huomioon usean DirectAccess palvelimen yhteiskäyttöä.

4.3.1 Full Intranet Access

Full Intranet Access -yhteys mahdollistaa asiakaskoneiden yhdistämisen kaikkiin intranetissä määritettyihin IPv6-resursseihin. Suurin etu Full Intranet Access -yhteydellä on sen nopea käyttöönotto ja samankaltaisuus VPN-toteutuksen kanssa. Se ei vaadi erillisiä sovelluspalvelimia DirectAccessin määriteltäväksi, eikä IPsec-suojattua liikennettä tarvitse määritellä sisäverkon alueeseen. [9, s. 34.]

Toteutusmalli vaatii kuitenkin kahden IPsec-tunnelin muodostamisen asiakkaan ja DirectAccess palvelimen välille. Tunnelit on nimetty infrastruktuuri- ja intranet-tunneleiksi. Kuvio 6 havainnollistaa Full Internet Access -mallin toimintaa, jossa liikenne on jaettu kahteen osaan [9].



Kuvio 6. Full Intranet Access -malli [9]

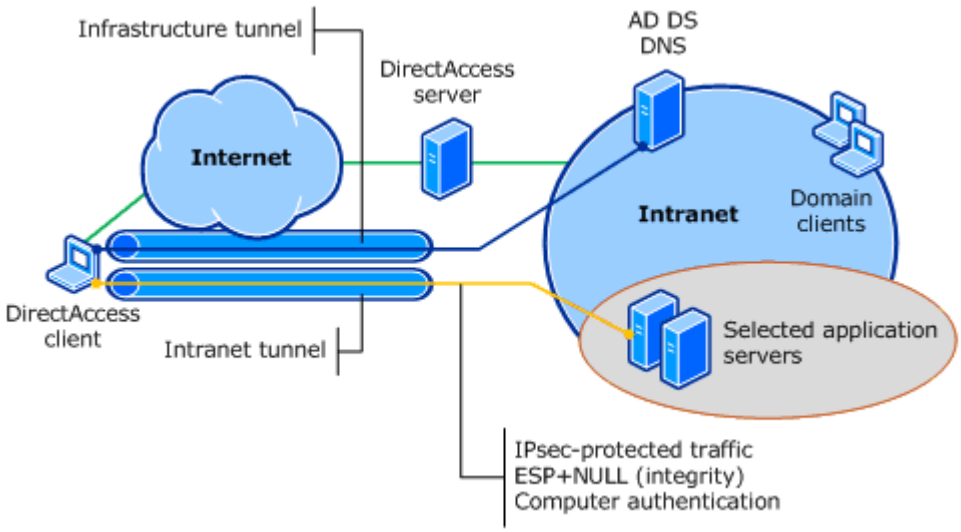
Infrastruktuuritunneli mahdollistaa asiakkaan yhteydet DNS- ja ADDS-palveluun. Se myös yhdistää muihin mahdollisiin hallinnointiin tarkoitettuihin palvelimiin intraverkon sisällä. Intranettunnelin kautta siirretään asiakkaan liikenne kaikkiin intraverkon resursseihin, kuten sovelluspalvelimelle.

Infrastruktuuritunneli käyttää vain tietokoneen autentikointi-informaatiota ja intranettunneli suorittaa sekä tietokoneen että käyttäjän autentikoinnin. Mikäli käytössä on älykorttien avulla toteutettu autentikointi, siirrettävä informaatio kulkee intranettunnelin kautta.

Käyttöönotossa on huomioitava Full Intranet Access -toteutuksen heikkoudet. Autentikointia ei toteuteta intraverkon sisäisiin resursseihin, mikä voi suuremmissa toteutuksissa muodostua tietoturvariskiksi. Toinen ongelma on suuri prosessointikuorma, jonka DirectAccess-palvelin joutuu käsittelemään IPsec-tunneleiden hallinnoinnin vuoksi. Kuormitusta voidaan vähentää siirtämällä IPsec-yhdyskäytävä erilliselle palvelimelle [9].

4.3.2 Selected Server Access

Toinen toteutusmalli on Selected Server Access, joka mahdollistaa rajoituksien tekemisen intraverkon resurssien käytölle. Se on monipuolisin ja joustavin kokonaisuus DirectAccessin yhteysmuodoista. sen avulla voidaan määritellä DirectAccess-asiakkaille tietyt palvelimet, jotka ovat heille sallittuja. Kuvio 7 havainnollistaa toteutusta.



Kuvio 7. Selected Server Access -malli [9]

Selected Server -mallissa yhteys intranettunnelissa on suojattu koko matkalta IPsec-tunnelilla ja se mahdollistaa ESP Null -kapseloinnin. Null-kapselointi on hyödyllinen ominaisuus, mikäli yhteys sisäverkon sisällä sisältää reitittimiä, jotka eivät kykene siirtämään IPsec-suojattuja paketteja. Tällöin IPsec toteuttaa normaalin informaation vaihdon luoden ensimmäisellä paketilla eheyden kohteeseen. Loput paketit kulkevat selkotekstinä sisäverkossa.

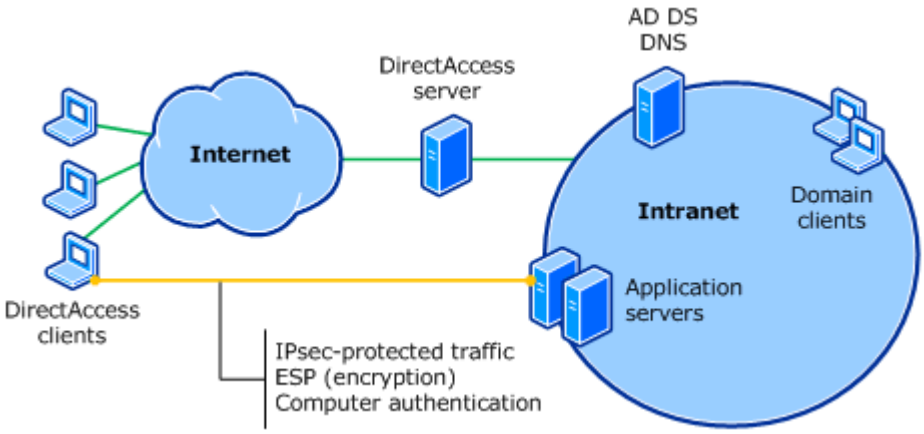
Monipuolisuus ja soveltuvuus ovat Selected Server -yhteyden tärkein etu. Toisin sanoen DirectAccess-asiakkaalle voidaan määrittää suojattu yhteys IPsec-tunnelilla tarvittaviin resursseihin ja samalla sallia suojaamaton yhteys muihin sisäverkon resursseihin.

Intranettunneli kuitenkin salaa kaiken liikenteen internetin välillä riippumatta valitusta yhteydestä intraverkossa. Infrastruktuuritunnelin toiminta ei muutu, se pysyy samanlaisena kuin Full Intranet -yhteydessä.

Etuna Selected Server Access -mallissa on sen mahdollisuus toteuttaa räätälöity ratkaisu omiin tarpeisiin. Tämä mahdollistaa End-to-End-yhteyden autentikoinnin ja tiedon turvaamisen monipuolisemmin verrattuna tavanomaiseen VPN-yhteyteen. Toteututus voidaan suoraan räätälöidä ohjatun DirectAccess-avustajan kanssa.

4.3.3 End-to-end Access

Kun End-to-End-yhteysmuoto valitaan käyttöön, DirectAccess-palvelimen tunnelien käyttö muuttuu. Infrastruktuuri- ja intranettunneleita ei oteta käyttöön, vaan kaikki informaation siirto toteutetaan suoraan IPsec-suojatulla tunnelilla. Kuvio 8 havainnollistaa End-to-End-yhteysmuodon toimintaa.



Kuvio 8. End-to-End Access -malli [9]

DirectAccess-palvelin toimii vain välikätenä siirtäen paketit päästä päähän kaikkiin sisäverkon resursseihin. Tämä vaatii tietysti sisäverkon reitittimiltä tukea yhteyden mahdollistamiseen.

4.4 DirectAccess-konfigurointi

DirectAccess on suunniteltu konfiguroitavaksi sen omalla graafisella Management Console -sovelluksella. Kaikki asetukset voidaan tallennetaa XML-muodossa tietokantaan, ja asetuksia voidaan jälkeenpäin muuttaa PowerShell-skripteillä.

Mikäli toteutettava DirectAccess-yhteys halutaan mukauttaa hyvin monimutkaiseen ympäristöön, on mahdollista ettei graafisen käyttöliittymän avulla voida tehdä kaikkia tarvittavia asetuksia. Asetukset voidaan kuitenkin toteuttaa myös Netsh (Network Shell) -sovelluksella ryhmäkäytäntöjen (Group Policy) avulla. Tässä työssä tarkastellaan vain graafisen DirectAccess Management Console -ominaisuuden käyttöä.

4.5 Windows Server 2012 -muutokset

Uuden Windows Server 2012:n yhteydessä DirectAccessin käyttöönottoa on huomattavasti helpotettu ja parannettu. Usean toimialueen käyttöönotto on suoraviivaisempaa ja suurin uutuus on tuki Server Core -tyyliselle asennukselle. Aikaisemmin DirectAccess on voinut toimia vain Windows Server 2008 R2 Enterprise -versiossa Windows 7 Enterprise- ja Ultimate-versioiden asiakaskoneiden yhteydessä.

Server Core on yksinkertaistettu ja karsittu Windowsin palvelinversio, jossa on hyvin karsittu garaafinen käyttöliittymä. Palvelimen hallinta ja komennot suoritetaan komentorivin kautta. Se sopii mainiosti DirectAcccesin käyttöönottoon vähäisemmän resurssienkäytön ansiosta. Komentorivillä toteutetaan kaikki asetukset ja DirectAccessin asentamista on helpotettu päivitetyillä PowerShell-ominaisuuksilla. Aikaisemmin hallintaa pystyi suorittamaan vain erillisillä komennoilla netsh:n ja GPO:n yhteistoiminnalla. Asentaminen ja konfigurointi on muodostettu helpommaksi ja yhtenäistetyksi PowerShellin päivitetyllä versiolla.

Käyttäjien monitorointi parannetaan monipuolisemmaksi koontinäytön (dashboard) avulla. Käyttäjien läsnäolon lisäksi saadaan tietoa käytetyistä ohjelmista ja asiakkaan statuksesta. Koontinäyttö näyttää statusinformaation käyttäjien toiminnasta ja niistä saa luoduksi myös raportit.

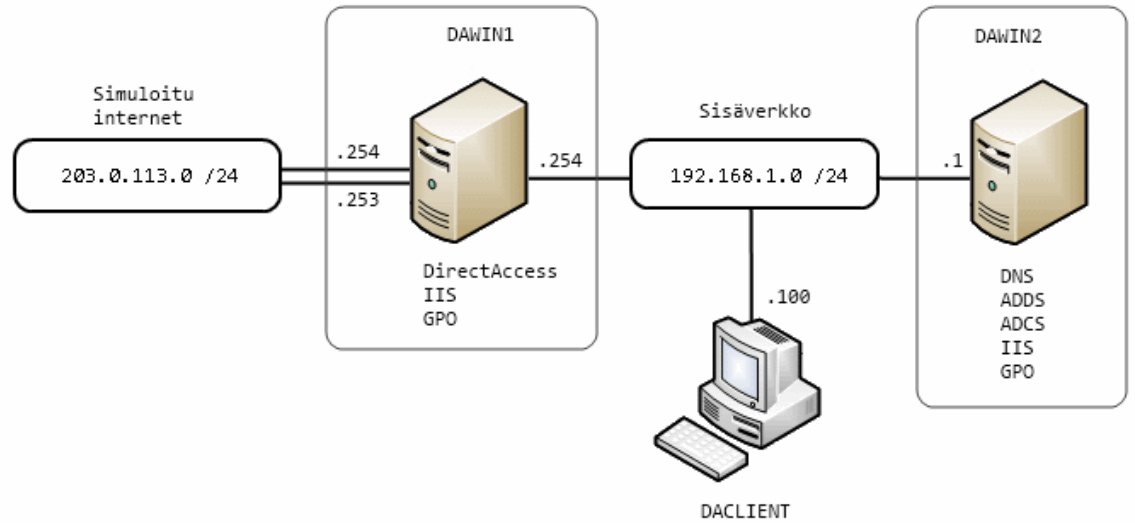
5 Simuloitu toteutus

5.1 Alkutoimenpiteet

Tässä työssä käytettiin kolmea tietoverkkolaboratorion VMware-klusterissa olevaa virtuaalikonetta, jotka oli liitety staattisilla IP-osoitteilla samaan aliverkkoon. Kaksi virtuaalikoneista määritettiin palvelimiksi ja yhdestä tehtiin asiakaskone. Toteutuksen tavoitteena oli tarkastella ja simuloida DirectAccessin käyttöönottoon vaadittavia komponentteja ja niiden yhteisvaikutusta DirectAccessin toimintaan.

Molemmille palvelimille asennettiin Windows Server 2008 R2 Enterprise ja asiakaskoneelle Windows 7 Enterprise. Konfigurointi suoritettiin suurimmalta osalta etänä RDP-tunneloinnin avulla.

DirectAccess vaatii toimiakseen kaksi julkista IPv4-osoitetta ja kaksi verkkosovitinta, joista yksi verkkosovitin on suunnattu internetiin ja toinen sisäverkkoon. DirectAccess on suunniteltu toimimaan verkon reuna-alueella reitittimen tyylisesti. Paras sijainti DirectAccessille olisi DMZ-vyöhyke.



Kuvio 9. Simuloitavan verkon rakenne

Jotta DirectAccess-ominaisuudesta saisi täyden hyödyn irti sisäverkossa, olisi suotavaa hajauttaa tarvittavat palvelut omille palvelinkoneilleen. Tässä toteutuksessa käytettiin vain yhtä sisäverkon palvelinta. Kuviossa 9 näkyy simuloitavan verkon kokonaisuus.

5.2 Palveluiden asennus ja konfigurointi

Ennen kuin DirectAccess-palvelin voidaan asentaa, on sisäverkkoon rakennettava useita palveluita. Vähintään yksi ohjauskone (DC, Domain Controller) on luotava hallinnoimaan verkkoa ja samalla Aktiivihakemiston avulla mahdolliset DirectAccess-asiakkaat jaoteltuna ryhmiin. PKI-järjestelmä muodostetaan Aktiivihakemiston ADCS-roolilla luomalla sertifikaattien hallinnoija (CA, Certification Authority) jakamaan sertifikaatteja. Jakelupisteet ja CRL-listat on luotava samassa yhteydessä. Tähän käytetään apuna IIS-roolin ominaisuuksia luomalla esimerkiksi virtuaalihakemisto, johon on mahdollista yhdistää internetistä käsin.

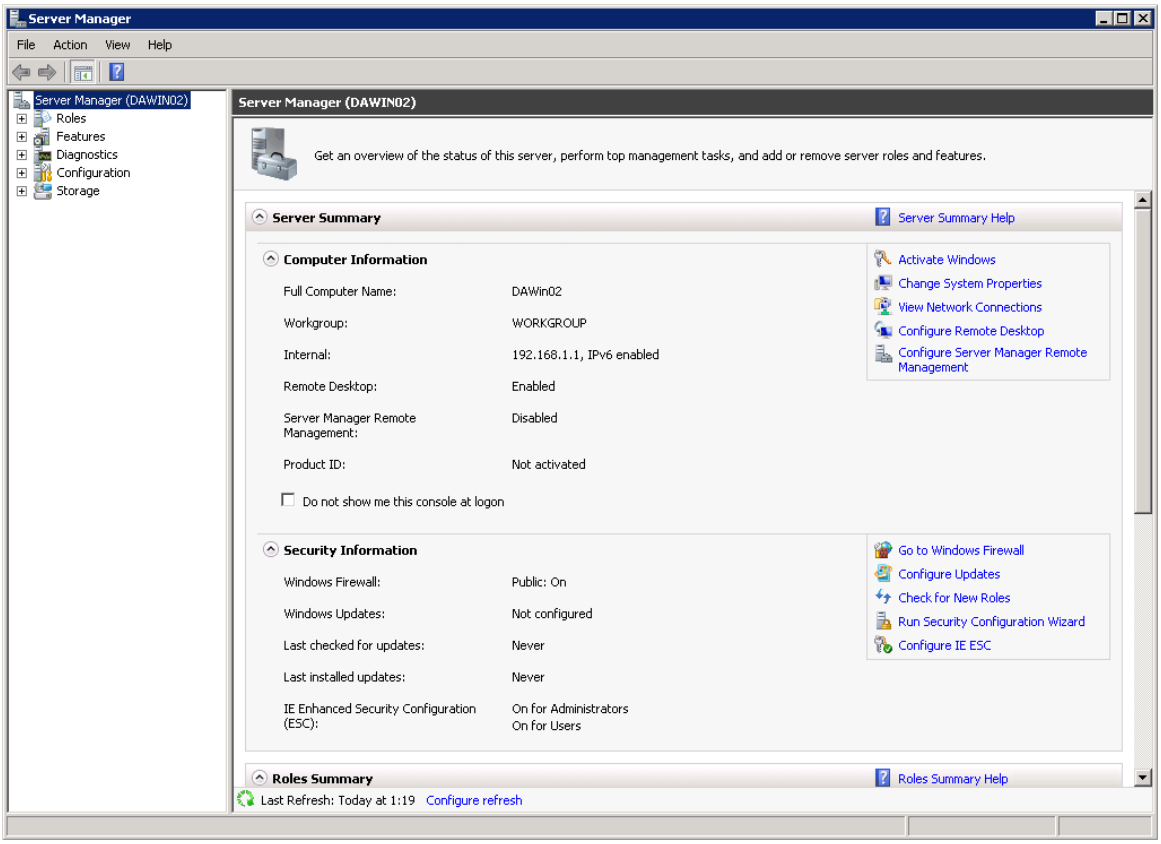
Toimialueen jäseneksi on liitettävä Windows 7 -käyttöjärjestelmällä varustettuja asiakaskoneita. Määrätyille asiakaskoneille on lisäksi luotava turvallisuusryhmä, johon on määritelty oikeus listautua DirectAccessin käyttöön. Asiakaskoneet on liitettävä tällaisen ryhmän jäseneksi.

Palomuuriasetuksia on muunneltava sallimaan DirectAccessin verkkoliikenne. ICMPv6-viestit esimerkiksi on sallittava kulkemaan verkossa mahdollistamaan Teredo-liikenne. Lisäksi ISATAP on sallittava poistamalla esto toimialueen DNS-palvelimelta.

Mikäli DirectAccess palvelin ei ole määrätty toimimaan verkkosijaintipalvelimena, eli NLS-kohteena, on määriteltävä ja luotava HTTPS-pohjainen URL-sijainti IIS-palvelimelle sisäverkkoon. Tämän sijainin perusteella DirectAccess-asiakaskoneet päättelevät, ovatko ne sisäverkossa vai internetissä. DirectAccess-palvelimelle voidaan myös asentaa IIS ja sen avulla tehdä siitä NLS-kohde.

5.2.1 Aktiivihakemiston komponentit

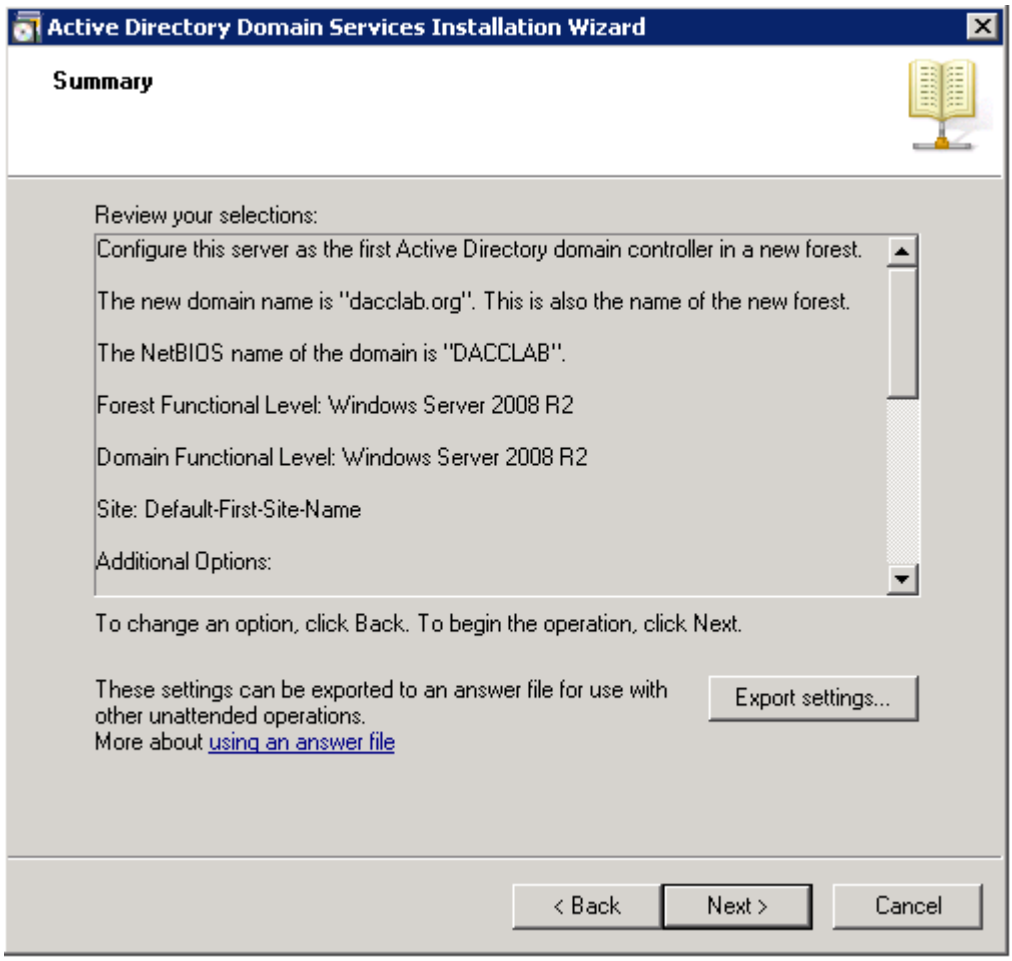
Server Manager -sovelluksen avulla voidaan palvelimelle asentaa yhtenäistetysti ja käytännöllisesti uusia rooleja ja ominaisuuksia. Kuvio 10 havainnollistaa Server Manager -sovelluksen ulkonäköä. Vasemmalla olevasta hakemistopuusta hallinnoidaan asennettuja rooleja, ominaisuuksia, diagnostiikkaa ja mahdollisia lisäkonfiguraatioita.



Kuvio 10. Server 2008 Server Manager.

Ensimmäisenä asennetaan ADDS-palvelu DAWIN02-palvelimelle. ADDS vaatii asennuksen yhteydessä .NET Framework 3.5.1:n asentamisen. Kun ADDS on asennettu, se pitää konfiguroida dcpromo-sovelluksella.

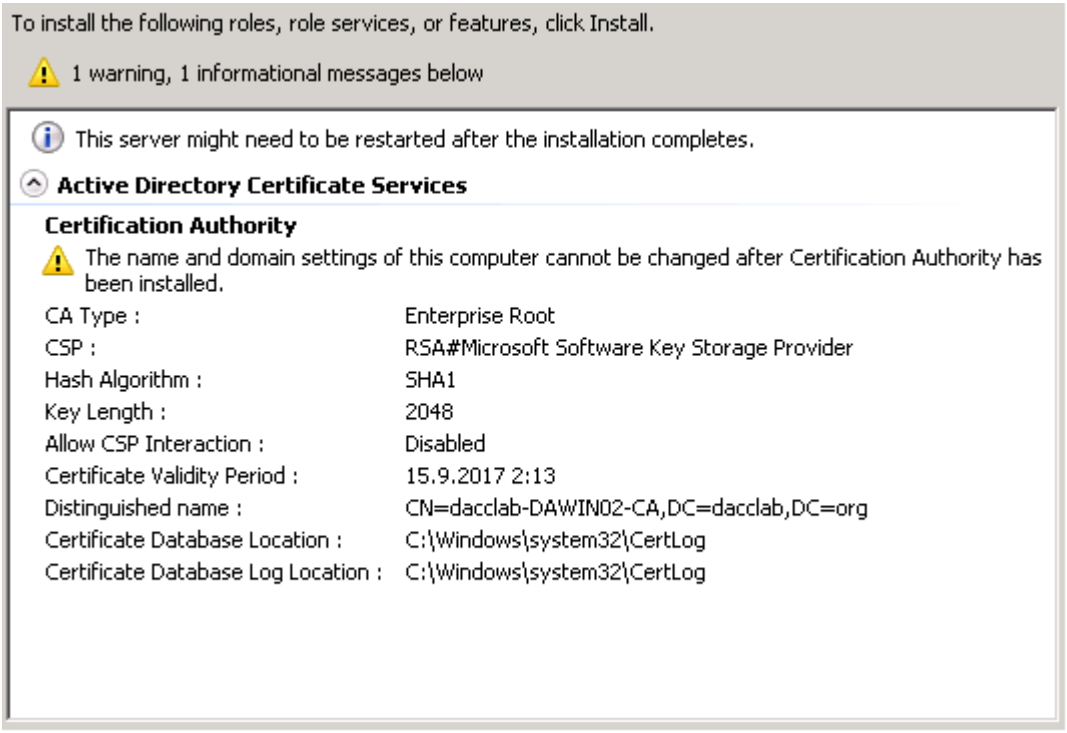
Dcpromon avulla luodaan uusi toimialue valinnalla New domain in a new forest. Uuden toimialueen nimeksi asetetaan dacclab.org ja se asetetaan toimimaan Windows Server 2008 R2 -tasolla. Asennuksen ohella asennetaan myös DNS-palvelu. Kuviossa 11 havainnollistetaan AD DS yhteenvetosivua.



Kuvio 11. Active Directory Domain Services Summary.

Kun ADDS on asennettu ja konfiguroitu, voidaan lisätä ADCS-rooli. ADCS-asennuksessa otetaan palveluksi käyttöön varmenteen myöntäjä (CA, Certification Authority). Määritellään käyttöön yrityksen varmenteen myöntäjä (Enterprise CA) ja tehdään siitä päämyöntäjä (Root CA). Tämä määrittely on simuloitavassa verkossa käytännöllisin vaihtoehto, koska yhteyksiä muihin varmentajiin ei voida luoda eikä määritellä.

Seuraava asennuksen vaihe on luoda uusi yksityinen avain. Tässä oletusarvot kelpaavat mainiosti. Kun kryptografiset asetukset ovat kunnossa, CA:lle annetaan nimeksi dacclab-DAWIN02-CA ja oletusarvoinen kelpoisuusaika. Nimen yhteydessä saadaan varoitus, joka ilmoittaa, ettei toimialueen nimeä tai asetuksia voida tämän jälkeen enää muuttaa. Kuvio 12 sisältää yhteenvedon asennetusta ADCS-palvelusta.



Kuvio 12. Active Directory Certificate Services Confirmation.

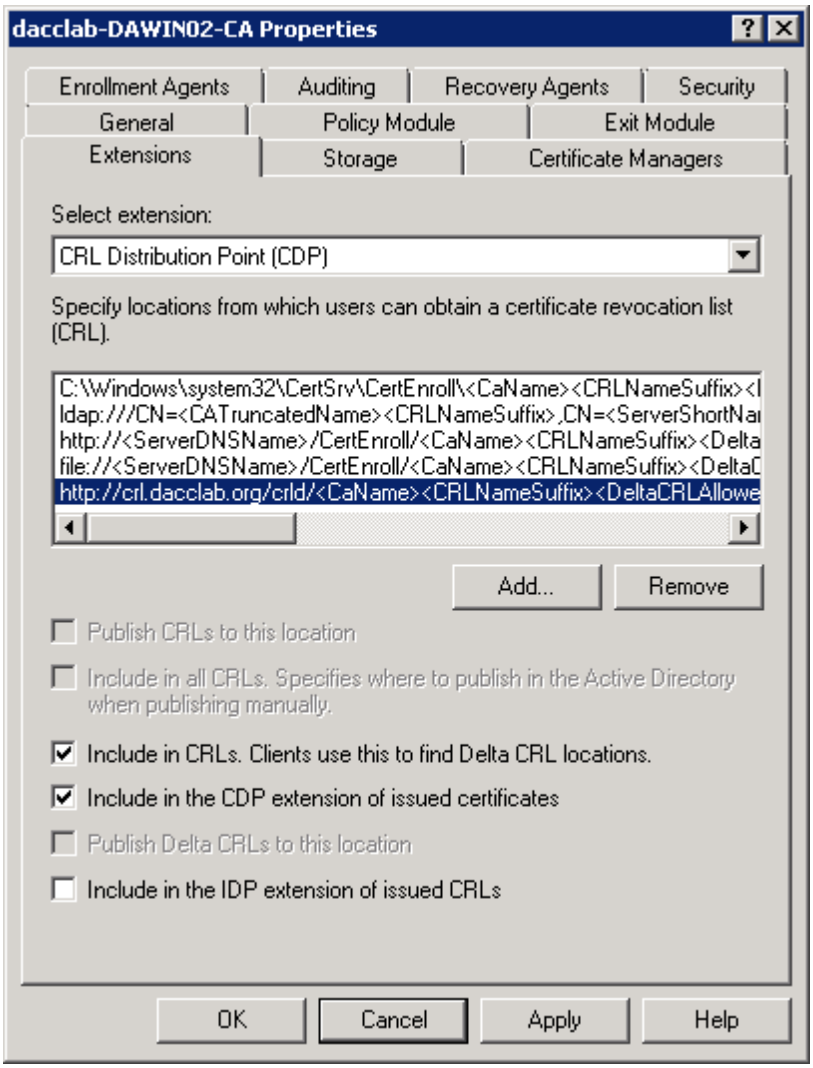
5.2.2 DNS-viittauksen ja CRL-listan luominen

DirectAccess-palvelin tullaan asettamaan varmenteita vastaanottavaksi kohteeksi. Täten se asetetaan myös network location -palvelimeksi, jonka määrittelyyn sisältyy DNS-viittauksen tekeminen.

Sisäverkon DAWIN02-palvelimelle asennettuun DNS-rooliin luodaan siis viittaus varmenteisiin, jotka tulevat olemaan saatavilla määriteltävästä pisteestä. Avataan Server Managerin hakemistopuusta suorien hakujen vyöhyke (Forward Lookup Zone) ja määritellään dacclab.org-alueeseen uusi osoitetietue (A-tietue). Tietueen nimeksi annetaan CRL ja IPv4-osoitteeksi asetetaan 192.168.1.254.

Seuraavaksi voidaan aloittaa CRL-jakelun asetukset. Hallinnointityökaluista avataan Server Manager tai Certificate Authority. ADCS-palvelun alta löytyy aikaisemmin luotu CA-elementti nimellä dacclab-DAWIN02-CA.

Avataan uuden CA:n asetukset ja lisätään Extensions-välilehteen sijaintimääritykset kolmelle muuttujalle. Kuvio 13 havainnollistaa muuttujien lisäystä.



Kuvio 13. CRL-jakelupisteen luominen.

Osoitteeksi on annettu:

http://crl.dacclab.org/crld/

Siihen liitetään CAName-, CRLNameSuffix- ja DeltaCRLAllowed -kentät. Lopullinen osoite viimeistellään lisäämällä pääte .crl sijaintimäärittelyyn seuraavasti:

http://crl.dacclab.org/crld/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

Uuden sijainnin lisäyksen jälkeen siihen on vielä liitettävä kuvion 13 mukaisesti ruksit liitosyhteyksiin Include in CRLs ja Include in the CDP extension of issued certificates.

Lopuksi hyväksytään asetukset ja käynnistetään ADCS-palvelu uudelleen. Tämä ottaa käyttöön uuden sijaintimäärittelyn jakelupisteelle.

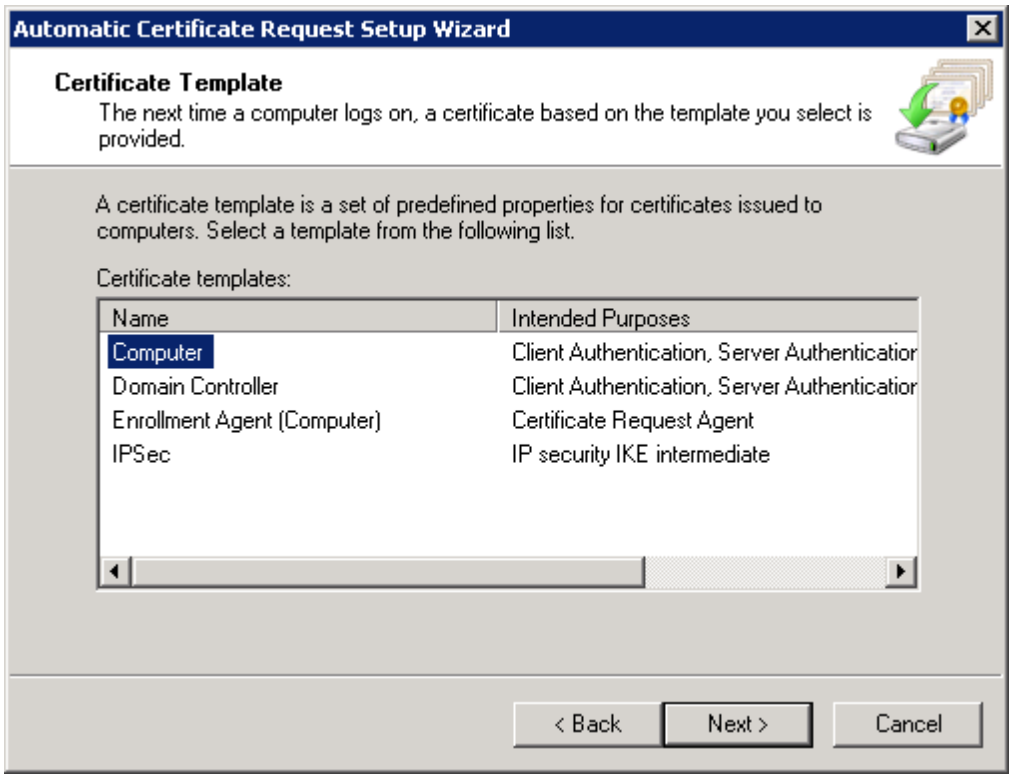
5.2.3 Varmenteiden automaattinen jakelu

Automaattinen asiakaskoneiden liittäminen toimialueeseen tehdään ryhmäkäytännön (GPO) avulla. Määritellään automaattisesti lähetettävä varmenne asiakaskoneille.

Avataan Server Manager jälleen ja Group Policy Management -hakemistopuusta valitaan dacclab.org, jonka ryhmäkäytäntöä (default domain GPO) muokataan. Group Policy Management Editorin hakemistopuussa lisätään sijaintiin:

Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Automatic Certificate Request Settings.

Luodaan kohteeseen uusi tietokone objekti kuvion 14 mukaisesti.



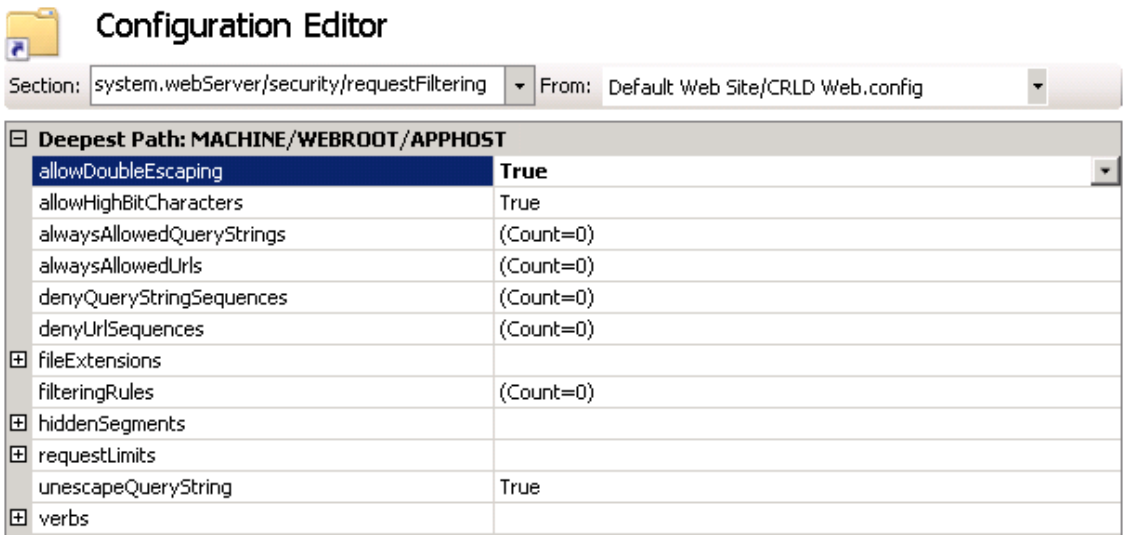
Kuvio 14. Automaattisen varmenteen haun asetukset.

5.2.4 IIS-asetukset

Molemmille sisäverkon palvelimille asennetaan Web Server (IIS) -rooli. Oletusarvot roolin asentamisessa kelpaavat mainiosti DAWIN02-palvelimelle. Mikäli Network Location -palvelimeksi asetetaan DAWIN01, on IIS-asennuksessa muistettava asentaa mukaan sinne IP and Domain Restrictions -palvelu.

Kun asennus on suoritettu, voidaan DAWIN02-palvelimelle luoda toinen CRL-jakelupiste, joka linkitetään web-pohjaiseen toteutukseen. Server Managerin kautta määritellään IIS-rooliin uusi virtuaalihakemisto Default Web Site -sivuston alle. Nimeksi asetetaan CRLD ja se linkitetään fyysiseen C:\CRLDkohde\ -kansioon.

Seuraavaksi mahdollistetaan kansioiden selaus. IIS-päänäkymästä valitaan Directory Browsing ja oikealla olevasta toiminnot-palstasta asetetaan hakemistojen selaus päälle. CRLD-hakemistosta avataan päänäkymä ja valitaan Configuration Editor. Section-kohdasta selataan paikkaan system.webServer\security\requestFiltering kuvion 15 mukaisesti.

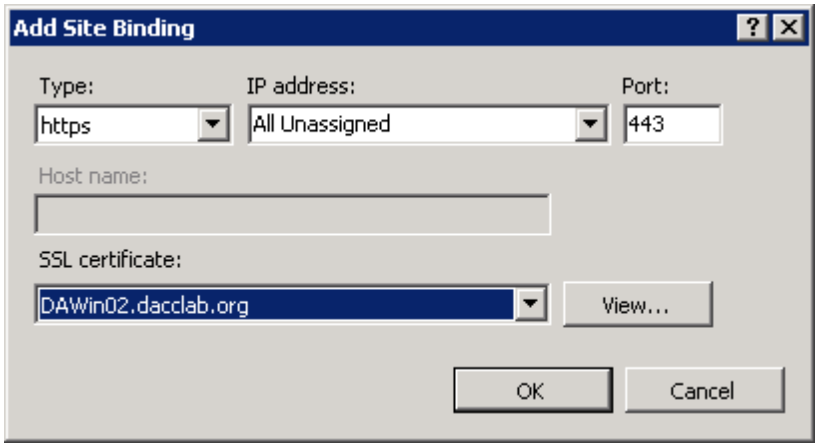


Kuvio 15. Configuration Editor.

Vaihdetaan allowDoubleEscaping-muuttujan boolean arvoksi true. Tämä toimenpide mahdollistaa URL-osoitteiden käytössä vapaamman määrittelyn.

5.2.5 HTTPS-asetukset

DirectAccessin käyttöönotossa on määriteltävä myös HTTPS-sertifikaatti. Tämä toteutetaan IIS-hakemistopuusta valitsemalla Default Web Site -sivusto. Toiminnot-palstasta valitaan bindings-toiminto. Kuvion 16 mukaisesti asetetaan tyypiksi https ja varmenteeksi valitaan aikaisemmin määritetty DAWin02.dacclab.org.

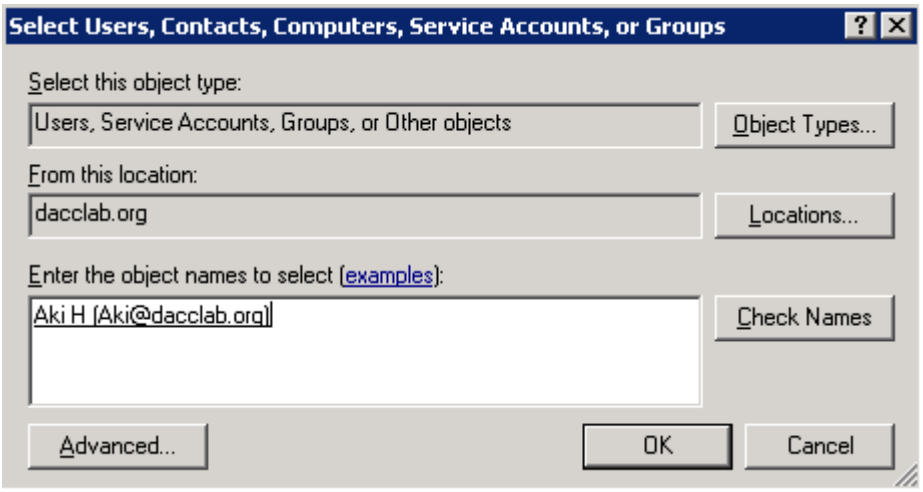


Kuvio 16. SSL-varmenteen linkitys.

5.2.6 Toimialueen pääkäyttäjän luominen

Ennen kuin muita koneita aiotaan liittää toimialueeseen, on hallintaa varten suositeltavaa luoda uusi pääkäyttäjä. Käyttäjien lisääminen tehdään Aktiivihakemiston Users and Computers -osiosta.

Avataan dacclab.org ja lisätään sinne uusi käyttäjäobjekti. Määritellään käyttäjätunnus ja samalla vielä salasana.



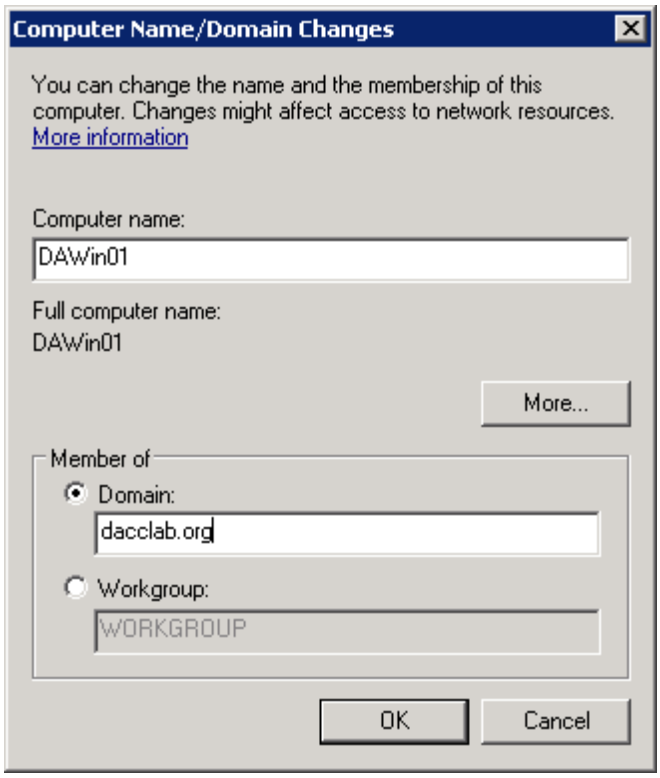
Kuvio 17. Käyttäjän lisääminen.

Kun toimialueen hallinnoija on luotu, tilille annetaan vielä pääkäyttäjän oikeudet valitsemalla Domain Admins -ryhmä Users-hakemistosta ja lisäämällä members-välilehden alle uuden käyttäjätilin nimi. Kuvio 17 havainnollistaa objektin nimen hakua.

5.2.7 Koneiden liittäminen toimialueeseen.

Sekä asiakaskone DAWIN7 että palvelin DAWIN01 on liitettävä dacclab.org-toimialueeseen. Ryhmäkäytäntöasetuksia tai DirectAccess-käyttöönottoa ei voida toteuttaa ilman toimialueyhteyttä.

Molemmilla koneilla liittäminen tehdään järjestelmän hallinnan System Properties -välilehdeltä. Tietokoneen nimi -välilehdeltä valitaan toimialueeseen liittäminen. Annetaan dacclab.org-nimi domain-kohtaan ja hyväksytään asetukset. Toimialueeseen liittyminen vaatii pääkäyttäjän oikeudet. Syötetään aikaisemmin määritetyn hallinnointitunnuksen tiedot. Hetken päästä ilmoitus jäsenyydestä ilmestyy näytölle uudelleen käynnistystä vaativan kehotuksen kera. Toimenpide suoritetaan molemmille koneille. Kuviossa 18 näkyy toimialueeseen liittämisen määrittely.

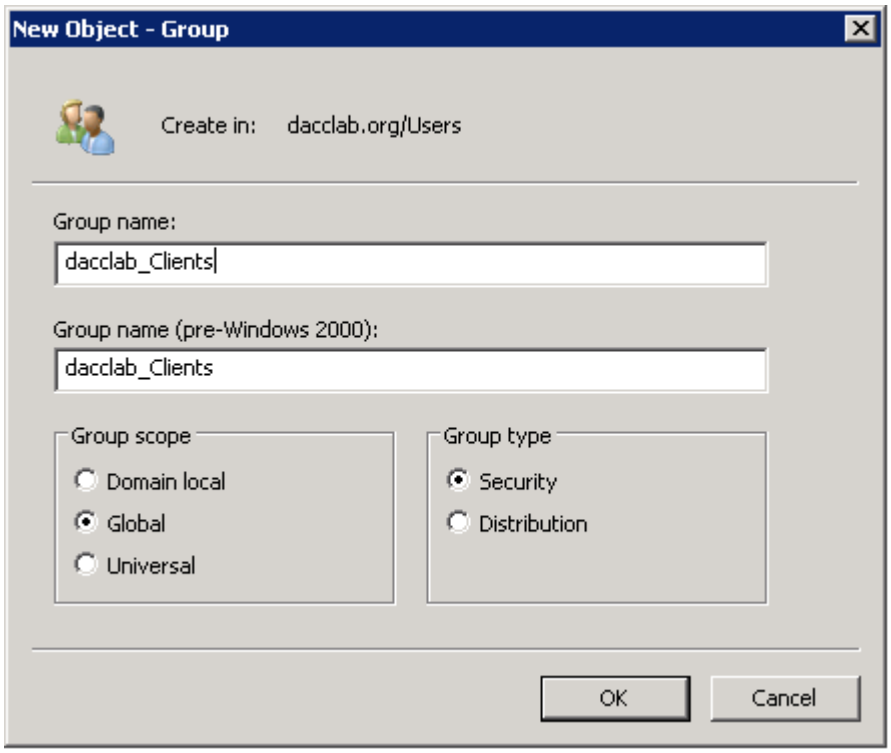


Kuvio 18. Toimialueeseen liittäminen.

5.2.8 DirectAccess-käyttäjäryhmän luominen

Luodaan uusi turvaryhmäobjekti DirectAccessin käyttöä varten. Tämä toteutetaan jälleen Server Managerin avulla aktiivihakemiston Users and Computers -hakemistopuussa.

Ryhmälle annetaan nimeksi dacclab_Clients kuvion 19 mukaisesti ja kohdealueeksi (scope) on muistettava määrittää global. Tyypiksi asetetaan turvaryhmä Security-valinnalla.



Kuvio 19. Uuden ryhmän luominen

Kun ryhmä on luotu, voidaan sen ominaisuuksia määritellä tarkemmin. Valitaan uuden ryhmän members-välilehti ja liitetään Windows 7 -asiakatietokone ryhmän jäseneksi. Tällä toimenpiteellä on mahdollista lisätä muitakin koneita hallittavaksi, mutta suurien käyttäjämäärien asettaminen on mahdollista myös PowerShell-skripteillä.

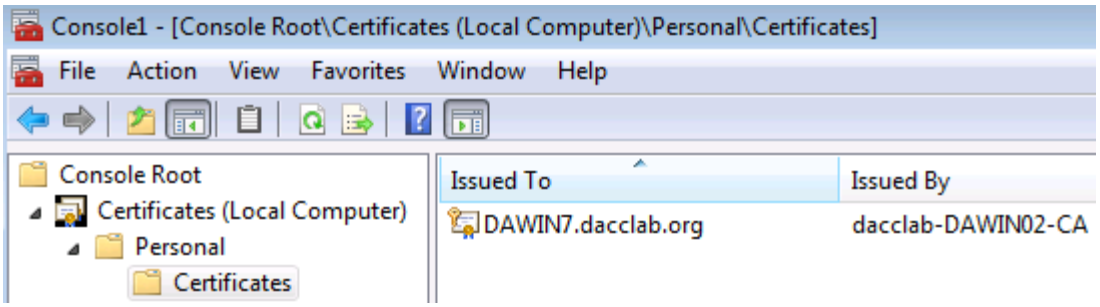
5.2.9 Varmenneasetukset

Kun pohjakonfiguraatiot on tehty ja tarvittavat käyttäjät on lisätty toimialueeseen, voidaan suorittaa loput tarpeelliset toimenpiteet. Certtempl.msc-sovelluksen asetuksista määritellään kirjautuneille käyttäjille eli Authenticated Users -ryhmän jäsenille lisäoikeuksia. Näille todennettuille käyttäjille valitaan aktiiviseksi enroll-kohta, eli mahdollisuus listautua varmenteiden pyytäjiksi. Isompaan ympäristöön toteutettaessa tällaista todentamista varten olisi syytä luoda DirectAccessille oma ryhmä, etteivät eri yhteyksien todennetut asiakkaat sotkeudu keskenään.

Jotta asiakaskone voisi yhdistyä turvallisesti verkon resursseihin, se tarvitsee varmenteen. Asiakaskoneella käynnistetään hallintakonsoli (MMC, Microsoft Management Console). Tyhjään konsoliin lisätään Add/Remove Snap-in -toiminnolla uusi varmennetili paikalliselle tietokoneelle. Tämän jälkeen MMC-ikkunaan ilmestyy varmenneobjekti, jonka kansionhallinnasta avataan hakemisto:

Console Root\Certificates\Personal\Certificates

Kuviossa 20 näkyy kuinka asiakastietokone on saanut varmenteen, jonka nimenä on DAWIN7.dacclab.org. Lisäksi sen käyttötarkoituksiin on määritetty todentaminen palvelin- ja käyttäjätasolla.



Kuvio 20. Asiakaskoneen varmenne

DAWIN01-palvelimelle on myös haettava varmenne IP-HTTPS-protokollaa varten. MMC-hallinnasta lisätään paikallinen varmenne samasta sijainnista kuin asiakaskoneella.

Valitaan uuden varmenteen rekisteröinti. Certificate Enrollment -asennusikkunan avulla määritetään uusi Web Server -linkitys ja lisämäärityksistä asetetaan uusi arvo palvelimelle:

CN=DAWIN02.dacclab.org

Varmennehakemistoon ilmestyy uusi elementti, jonka asennus ilmoitetaan onnistuneen. Mikäli DirectAccess-palvelimelle asennetaan NLS-palvelu, tulee lisävarmenne hakea vielä siihenkin tarkoitukseen MMC-hallinnan kautta.

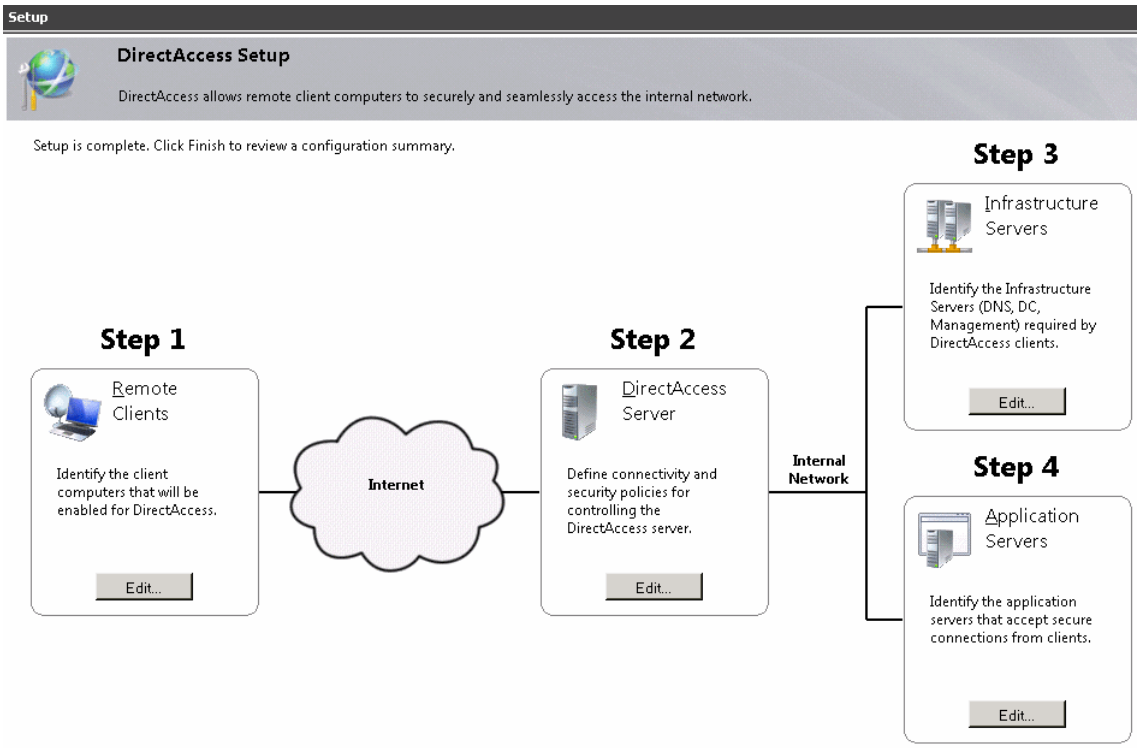
Tämän ohella IIS-roolin verkkosivujen hakemistopuusta on lisättävä bindings-toiminnolla NLS-kohteelle haettu SSL-varmenne. On suositeltavaa luoda NLS-sijainnille oma sivusto, johon linkitys tehdään.

5.3 DirectAccessin asentaminen

5.3.1 DirectAccess Setup ja ISATAP

DirectAccessin asetuksien määrittelyä varten suunniteltu asennusohjelma on käyttäjäystävällinen ja suoraviivainen asennustyökalu. Neljän vaiheen avulla tärkeimmät ja yleisimmät konfiguraatiot voidaan muodostaa tämän työkalun avulla.

Kuvio 21 havainnollistaa graafista käyttöliittymää DirectAccess Setup -sovellukselle. Ensimmäisessä vaiheessa asetetaan ja määritellään asiakaskoneet, toisessa Direct-Access-palvelimen reitittävät ominaisuudet, kolmannessa infrastruktuuripalvelimet ja neljäntenä mahdolliset sovelluspalvelimet.

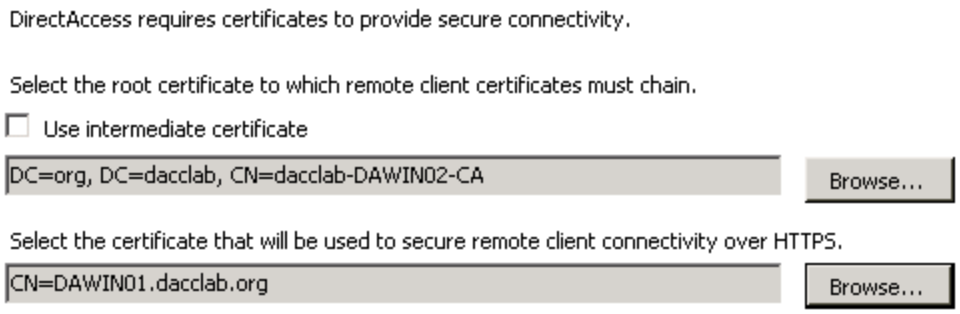


Kuvio 21. DirectAccess Setup

Ensimmäisen vaiheen valinnoissa ei tarvitse muuta kuin lisätä aikaisemmin määritelty dacclab_Clients-ryhmä listaan ja hyväksyä valinta. Mikäli eri ryhmiä olisi luotu esimerkiksi sovelluspalvelimien käyttäjiksi, nekin määriteltäisiin nyt.

Toisessa vaiheessa DirectAccess-palvelimen asetuksissa määritellään molemmille verkkokorteille osoiteavaruudet. Internetin suuntaan kytketty verkkosovitin, nimellä julkinen, määrätään käyttöön osoitteella 203.0.113.254 ja sisäverkkoon yhdistetty verkkosovitin, nimellä internal, otetaan käyttöön osoitteella 192.168.1.254. Tässä valikossa on myös määriteltävä käyttöön valinta mahdollisista älykorttien käytöistä.

Seuraava määrittelykohta DirectAccess-palvelimella on varmenneasetukset. Kun varmenteet on lisätty MMC-konsolilla aikaisemmin, ne näkyvät nyt selkeästi selaus-painikkeen avauksen yhteydessä. Kuvio 22 visualisoi päävarmenteen ja HTTPS-varmenteiden listausta.



Kuvio 22. DirectAccess-varmenteet.

Varmenteiden määrittelyn jälkeen päästään määrittämään kolmannen vaiheen asetukset eli infrastruktuuripalvelimien asetukset. Infrastruktuuripalvelimen ensimmäinen määrittely liittyy NLS-kohteeseen. DirectAccess voidaan asettaa NLS-palvelimeksi tai erillinen palvelin voidaan määrittää URL-osoitteella. Tässä toteutuksessa valittiin DirectAccess NLS-kohteeksi varmenteella.

DNS- ja DC-asetukset on määritettävä seuraavaksi. DNS suffix -määrittelyt muodostuvat automaattisesti listaan. Lisämäärittelyjä voidaan luoda listaan sisäverkon DNS-kyselyjä varten. NLS-palvelin on myös määriteltynä asetuksissa. Lisäksi local name resolution -valinta on tehtävä. Tämän avulla selvitetään, kuinka vapaasti voidaan

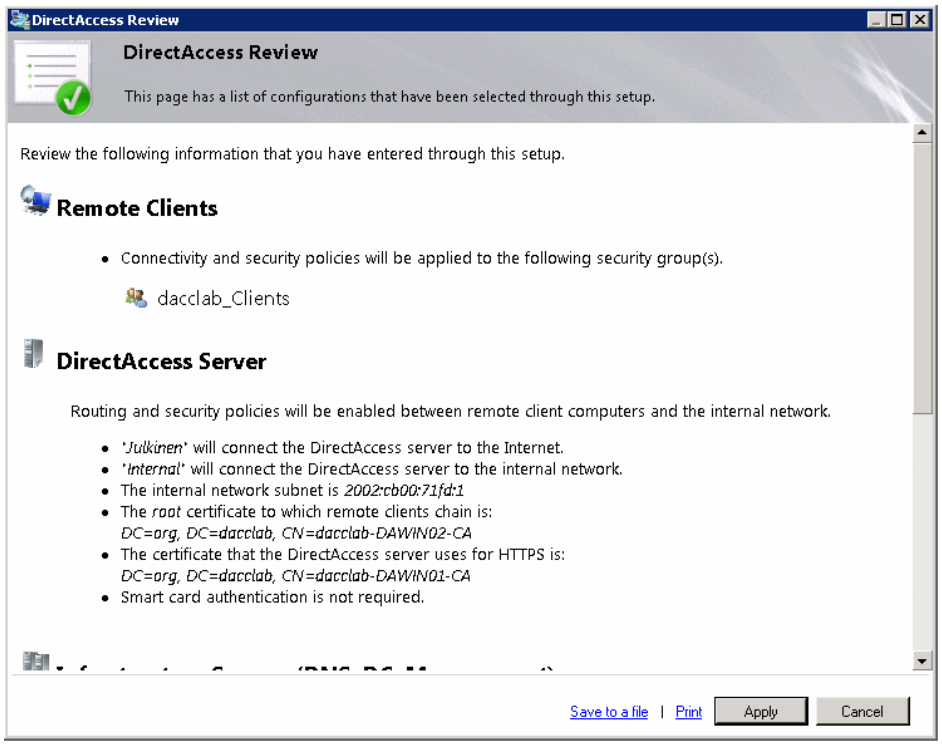
nimien DNS-hakua suorittaa esimerkiksi virhetilanteissa. Toteutuksessa käytettiin suositeltuja asetuksia. Hallinnointiin ja tarkkailuun on myös mahdollista määrittää asetuksia, mutta niitä ominaisuuksia ei otettu käyttöön.

Neljännessä vaiheessa voidaan vaikuttaa sovelluspalvelimen salausasetuksiin. Tämä vaikuttaa myös sisäverkon yleiseen salaukseen ja yhteyksiin eri palvelimille. Toteutuksen simuloinnissa ei käytetty sovelluspalvelinta, joten erillisen end-to-end -todentamisen tarvetta ei ollut. Erilaisten toteutusmallien, kuten Selected Server Access -mallin käyttöönotto määriteltäisiin tässä valitsemalla Require end-to-end authentication and traffic protection for the specified servers.

Jotta käyttöönotto onnistuisi, täytyisi valitut palvelimet määrittää turvallisuusryhmään ADDS-hallinnan kautta. IPsec-asetuksia voidaan tässä myös määrittää, mikäli halutaan yhteensopivuutta vanhempien laitteiden kanssa.

Lopulta, kun kaikki vaiheet on käyty läpi, on mahdollisuus tallentaa ja viimeistellä asetukset. Tarkasteltavaksi aukeaa review-osio, jossa näkyvät kaikki määrittelyt. Hyväksymme asetukset ja täten konfigurointi on suoritettu.

Konfiguraatio on mahdollista tallentaa xml-muotoon tässä vaiheessa. Tämä on hyödyllinen toiminto varmuuskopioinnin ja mahdollisesti uuden ympäristön rakentamisessa helpottava ominaisuus. Kuvio 23 havainnollistaa yhteenveto-sivua.



Kuvio 23. DirectAccess Review -ikkuna.

Kun DirectAccess on asennettu, on syytä asettaa ISATAP käyttöön tekemällä IPv6-asetuksien, ryhmäkäytäntöjen ja reititystaulujen päivitys. Ryhmäkäytäntöasetukset päivitetään suoraviivaisesti asiakaskoneella komennolla:

gpupdate

DAWIN02-koneella ja asiakaskoneella käynnistetään uudestaan iphelper-palvelu komennoilla net, käyttäen attribuutteja stop ja start:

net stop iphlpsvc

net start iphlpsvc

Tämän jälkeen tehdään DNS-asetuksien päivitys molemmilla koneilla komennolla:

ipconfig /flushdns

Kun ipconfig-komento on suoritettu, voidaan ping-komennolla varmistaa ISATAPin toimivuus sisäverkon palvelimelle ja DirectAccess-palvelimelle:

ping 2002:cb00:71fd:1:0:5efe:192.168.1.254

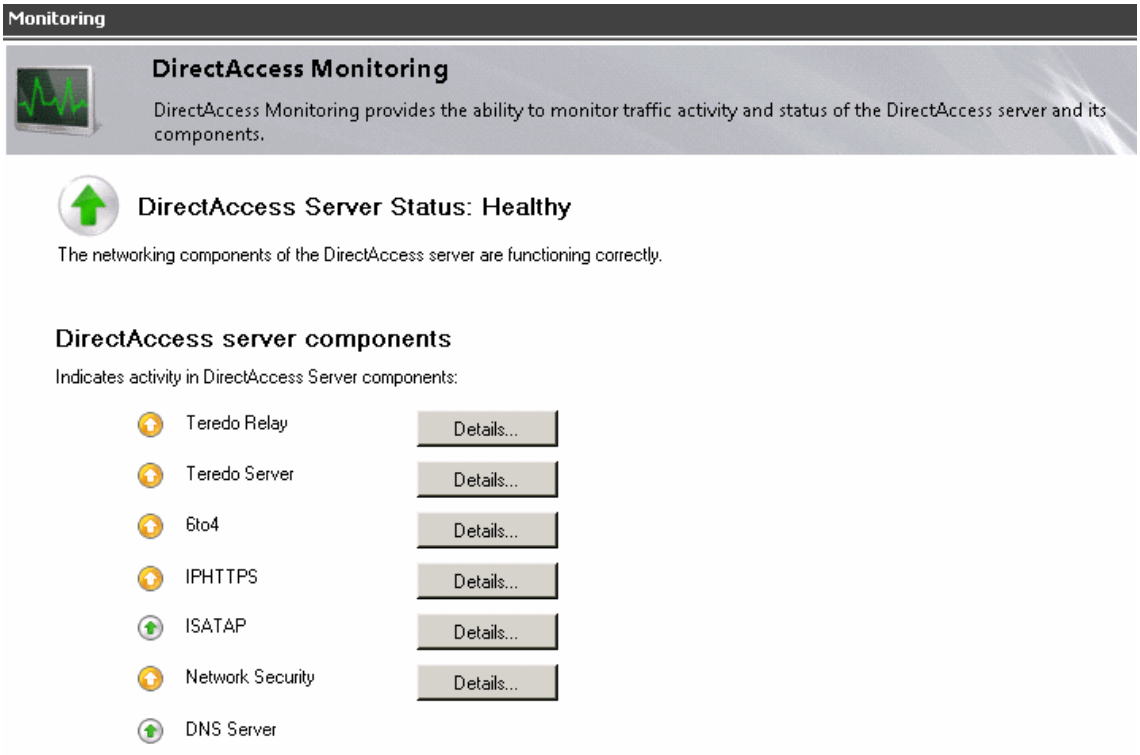
ping 2002:cb00:71fd:1:0:5efe:192.168.1.1

Lisäksi tarkastetaan DNS-palvelun toimivuus seuraavilla komennoilla:

ping dawin01.dacclab.org

ping dawin02.dacclab.org

Reply-viestit näkyvät ISATAP-osoitemuodossa, täten DNS toimii oikein.



Kuvio 24. DirectAccess Monitoring

Setupin ja testauksien jälkeen DirectAccess Monitoring -kohdasta nähdään, että asiakaskone, on kommunikoinut ISATAP-yhteydellä. Kuviossa 24 on näkymä verkon tarkkailuominaisuudesta.

5.3.2 Verkkosijaintipalvelin

DirectAccess palvelimesta voidaan tehdä verkkosijaintipalvelin (NLS, Network Location Server), joka kertoo asiakaskoneille ovatko ne sisäverkossa vai eivät. DirectAccess-palvelimelle on asennettava IIS-rooli ja siihen on linkitettävä varmenne määritettyyn verkkosivun sijaintiin.

Asiakaskoneen tekemä tarkistus sijainnista on hyvin suoraviivainen. DirectAccess-asiakaskoneen rekisterieditorilla voidaan havainnollistaa osoitetta, jonka avulla NLS-kohde määräytyy. Rekisterieditorilla avataan sijainti:

HKLM\software\policies\microsoft\windows\NetworkConnectivityStatusIndicator\CorporateConnectivity\

Elementillä DomainLocationDeterminationUrl on määriteltynä data-sarakkeessa URL-osoite NLS-palvelimeen. Tämä informaatio välitetään ryhmäkäytännön avulla.

DirectAccess-asiakaskone olettaa aina olevansa ulkoverkossa. Asiakaskone tarkastelee jatkuvasti internetyhteyden muutoksia, kuten verkkokaapelin irroittamista tai muutoksia IP-konfiguraatioissa. Mikäli asiakaskone toteaa olevansa sisäverkossa, se vaihtaa käyttöön toimialueprofiilin ja ISATAP-osoitteet. Tämä määräytyy Network Location Awareness -komponentin avulla. Mikäli NLS-palvelimeen ei saada yhteyttä, DirectAccess-komponentit otetaan käyttöön suojatun etäyhteyden muodostamista varten.

6 Yhteenveto

DirectAccess tarvitsee toimiakseen suuren määrän infrastruktuuria alleen. Tässä työssä käsiteltiin tarvittavien sisäverkon komponenttien asentamista, konfigurointia ja transitioteknologioiden käyttöä DirectAccessin yhteydessä.

DirectAccessin asentaminen on hyvin suoraviivainen prosessi, kun tarvittavat pohjakonfiguraatiot on toteutettu. DirectAccessin tarjoaman graafisen setup-sovelluksen avulla konfigurointi voidaan suorittaa vaivattomammin kuin netsh- ja gpo-komponenttien avulla manuaalisesti. Erilaisten yhteysmuotojen käyttöönotto on suunniteltu myös varsin selkeäksi, kun halutaan valita jokin Full Intranet-, Selected Server- ja End-to-End -yhteyksistä.

Kokonaisuudessaan DirectAccess on hyödyllinen työskentelyn mukavoittaja loppukäyttäjille. Tällaisia etäyhteyden toteutusmalleja tullaan näkemään varmasti yhä useammin ja todennäköisesti ne tulevat korvaamaan VPN-yhteyksien käytön ainakin suurempien yrityksien kokonaisuuksissa. Toisaalta DirectAccess tekniikkana pyrkii rikkomaan palvelimen ja reitittimen rajoja toiminnallisuudeltaan, joka voi siirtää ja mahdollisesti kilpailuttaa teknologian kehitystä reitittimien osalta. Etuna DirectAccess-tekniikalla on kuitenkin yhtenäinen Windows-ympäristö ja asiakaskoneiden toimialuealueen jäsenyys. Tämä mahdollistaa helpomman hallinnan ja samalla suurin osa komponenteista on varmasti yhteensopivia toteutuksen tekemiseen ja toimintaan.

Sisäverkon Windows Server 2008 R2 -palvelimelle asennusvaiheet ovat kuitenkin hyvin pitkät. Valmiiseen ympäristöön toteuttaminen vaatii tarkkaa suunnittelua ja vielä enemmän panostusta uuden ympäristön luomiseen. Mikäli verkkokokonaisuus on huomattavan suuri, voidaan Microsoftin Forefront Unified Access Gateway -tekniikkaa käyttää apuna toteutuksen teossa.

Suurin rajoite Windows Server 2008 R2 -version DirectAccess-toteutusmallissa on peräkkäisten julkisien IPv4-osoitteiden tarve. Lähes kaikki IPv4-osoitteet ovat jo käytössä, jolloin uuden verkon luominen on kohtuullisen haastavaa tällä ensimmäisellä DirectAccess-versiolla.

Mahdolliset yritykset, joilla saattaisi olla tarvetta DirectAccess- toteutukselle, eivät välttämättä lähde vieläkään suuressa mittakaavassa harkitsemaan tätä vanhempaa palvelintoteutusta etäyhteystoteutuksiinsa. Pikemminkin vasta sitten, kun Windows Server 2012 -versio otetaan käyttöön yrityksien verkkoihin, saadaan DirectAccessin suosiota kasvatetuksi.

Yhteistoimivuusvaatimukset IPv4- ja IPv6-protokollien välillä ovat toinen rajoite, joka vaikuttaa suuresti vielä monta vuotta, sillä transitioteknologioiden valinta, suunnittelu ja konfigurointi tuovat ylläpitoon lisähaasteita. Tällä hetkellä uuden Windows Server 2012 -version ohella julkaistu paranneltu tuki DirectAccessille tuo esiin paljon käytännöllisemmän asennus- ja ylläpitomahdollisuuden verkon hallinnoijille.

Lähteet

1 Christos, Douligeris. 2007. Network Security - Current status and future directions. USA: Wiley.

2 Enhance mobility and manageability with DirectAccess. 2008. Verkkodokumentti. <http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/windows-7/features.aspx#directaccess>. Luettu 20.4.2012.

3 Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. 1998.

4 Day J D, Zimmermann H. The OSI reference model. Proceedings of the IEEE 1983;71(12):1334-1340.

5 Stevens WR. TCP/IP illustrated. Volume 1, The protocols. Reading (MA): Addison-Wesley; 1994.

6 An examination of IPv4 and IPv6 networks : Constraints and various transition mechanisms. Southeastcon, 2008. IEEE; 2008.

7 Orin, Thomas; Ian McLean. 2011. MCITP Self-paced Training Kit: Windows Server 2008 Server Administrator (2nd Edition). USA: Microsoft Press.

8 DirectAccess Connections. 2010. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/dd637767%28v=ws.10%29.aspx>. Luettu 11.9.2012.

9 Joe, Davies. 2010. Design, Deployment, and Troubleshooting Guide. USA. Microsoft Corporation.