LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Remote Access palvelinroolin kartoitus

– Case Laurea

Vaartela, Miikka

2015 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Remote Access palvelinroolin kartoitus – Case Laurea

Miikka Vaartela
Tietojenkäsittely
Opinnäytetyö
Lokakuu, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Miikka Vaartela

Remote Access palvelinroolin kartoitus – Case Laurea

Vuosi 2015 Sivumäärä 26

Tämä opinnäytetyö käsittelee Remote Access palvelinroolia, joka on looginen ryhmittely verkkoon pääsyyn liittyvistä teknologioista. Opinnäytetyön tavoitteena on laatia tietopaketti, joka tarjoaa kattavaa tietoa etäkäytöstä Microsoftin tarjoamia palveluita käyttäen. Opinnäytetyön tietoperustassa käsitellään Remote Accessiin sisältyviä kolmea roolipalvelua. Roolipalvelut ovat DirectAccess, Routing And Remote Access ja Web Application Proxy, jotka kaikki ovat etäkäyttöön tarkoitettuja palveluita.

Tutkimuksessa käydään läpi edellä mainittujen teknologioiden toimintamallit sekä tarkastellaan niiden tietoturvaa ja etuja verrattuna muihin samantyyppisiin teknologioihin. Näiden palveluiden sisältämät ominaisuudet käydään läpi loogisessa järjestyksessä. Työssä käsitellään lyhyesti myös työhön liittyvien roolipalveluiden historiaa.

Opinnäytetyö on toteutettu toimeksiantona Laurea-ammattikorkeakoulun tietohallinnolle. Tietohallinnolla oli tarve saada tietoa varsinkin uusimman tekniikan eli Web Application Proxyn toiminnasta ja miten sitä voitaisiin parhaiten käyttää hyväksi Laurean palveluissa. Kuitenkin tutkimuksessa analysoitiin kokonaisuutena kaikkia kolmea roolipalvelua, jotta saatiin hyvä yleiskäsitys etäkäytön toiminnasta Remote Access palvelinroolin avulla.

Tutkimus toteutettiin laadullisen tutkimuksen tapaan keräämällä tietoa parhaiksi todetuilta verkkosivuilta ja omaa ammattitaitoa hyödyntäen. Aineistona on käytetty Microsoftin teknologioita. Ajankohtaisimmat lähteet löytyvät Microsoftin verkkosivuilta.

Asiasanat: DirectAccess, Routing and Remote Access, Web Application Proxy

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Business Information Technology

Miikka Vaartela

A Survey on Remote Access Server Role – A Case Study of Laurea

Year 2015 Pages 26

This thesis is a detailed study of the Remote Access server role, which is a logical grouping of network access technologies. The purpose of this thesis is to compose an information package which provides comprehensive information about remote access using the services of Microsoft. The theoretical part of this thesis deals with the three role services of the Remote Access server role, which are DirectAccess, Routing and Remote Access and Web Application Proxy.

This survey investigates how the above-mentioned technologies work, and focuses on their information security and benefits compared to other similar technologies. The properties of these services are reviewed in a logical order. The study also deals with a brief history of the role services discussed in this study

This study was assigned by the IT administration of Laurea. The IT administration had a need for information, especially about the latest technology, Web Application Proxy's function and how it can be best used to the benefit of Laurea's services. However, the study looked at the overall role of all three services in order to provide a good overview of the operations which the Remote Access server role allows.

The survey was conducted in the way of qualitative research by collecting information from trusted websites and with the use of my own professional knowledge. The material used in this thesis is mainly found on the internet, because it is Microsoft's proprietary technology so the most current sources are best found on Microsoft's own website.

Keywords: DirectAccess, Routing and Remote Access, Web Application Proxy

Sisällys

1 Johdanto

Etäkäyttö viittaa kykyyn päästä käsiksi tietokoneeseen etäältä. Näin työntekijä voi työskennellä missä tahansa, säilyttäen pääsyn muualla sijaitsevaan verkkoon, kuten yrityksen sisäiseen verkkoon. Etäkäyttöön tarvittava yhteys voidaan muodostaa käyttämällä lähiverkkoa, laajaverkkoa tai virtuaalista erillisverkkoa.

Yleisesti etäyhteyden muodostamiseksi tarvitaan, sekä paikalliseen tietokoneeseen ja etätietokoneeseen asennettu etäyhteysohjelma. Etäyhteysohjelmia on monia ja ne voivat erota tarkoituksiltaan hyvin paljon. Vaihtoehtoisesti on myös palveluntarjoajia, jotka tarjoavat etäyhteyttä Internetin kautta.

Nykypäivänä idea etäkäyttäjästä on jo arkipäiväinen vaikka käyttäjien pitääkin vielä löytää tiettyjä teknologioita, joiden avulla voidaan muodostaa etäyhteys haluttuun järjestelmään. Käyttäjää, joka työskentelee eri paikassa missä hänen tietokoneensa sijaitsee, kutsutaan etäkäyttäjäksi. Etäkäyttäjä tarvitsee käyttöönsä etäyhteyden, joka muodostetaan joko internetin tai yksityisten verkkojen välille. Älypuhelimien ja muun kannettavan teknologian yleistymisen myötä on myös kysyntä etäyhteyksille kasvanut huomattavasti käyttäjien halutessa entistä tuottavammiksi myös toimiston ulkopuolella. (Techopedia 2015)

Tämän Opinnäytetyön tavoitteena on koota kattava tietopaketti Microsoft Remote Accessista ja sen sisältämästä kolmesta roolipalvelusta; DirectAccess, Routing and Remote Access ja Web Application Proxy. Tilaaja voi ottaa tarvittaessa toimivan tekniikan käyttöönsä monessa eri järjestelmässä. Hyvänä esimerkkinä tästä on TEM-matkalaskujärjestelmän käyttö etänä miltä tahansa henkilökohtaiselta laitteelta, kuten puhelimelta, tabletilta tai kannettavalta tietokoneelta.

Opinnäytetyö on toteutettu toimeksiantona Laurea-ammattikorkeakoulun tietohallinnolle. Laurea-ammattikorkeakoulu toimii osakeyhtiömuotoisena (Laurea-ammattikorkeakoulu Oy). Omistuspohja on 97-prosenttisesti kunnallinen. Laurea on Suomen kolmanneksi suurin ammattikorkeakoulu aloituspaikkojen määrän perusteella ja tällä hetkellä Laureassa opiskelee n. 8000 opiskelijaa ja työskentelee n. 500 työntekijää.

2 Toimeksiantaja ja menetelmät

Opinnäytetyö toteutettiin toimeksiantona Laurea-ammattikorkeakoulun tietohallinnolle. Opinnäytetyön tavoitteena oli koota kattava tietopaketti Microsoft Remote Accessista ja sen sisältämästä kolmesta roolipalvelusta; DirectAccess, Routing and Remote Access ja Web Application Proxy. Tietopakettia voidaan hyödyntää etäkäytön mahdollisuuksien kehittämisessä tulevaisuudessa.

Työn tilaajana on Laurea-ammattikorkeakoulun tietohallinto. Laurean tietohallinto on vastuussa Laurean tietotekniikasta. Laurea-ammattikorkeakoulu toimii osakeyhtiömuotoisena, Laurea-ammattikorkeakoulu Oy. Omistuspohja on 97-prosenttisesti kunnallinen. Sen omistajia ovat Espoon kaupunki, Vantaan kaupunki, Keski-Uudenmaan ammattikoulutusyhtymä, Hyvinkään kaupunki, Länsi-uudenmaan ammatti-koulutusyhtymä, Porvoon kaupunki, Kauniaisten kaupunki, Kirkkonummenkunta ja Invalidiliitto ry. Laurea on aloituspaikkojen määrän perusteella Suomen kolmanneksi suurin ammattikorkeakoulu ja tällä hetkellä Laureassa opiskelee n. 8000 opiskelijaa ja työskentelee n. 500 työntekijää.

Laurean paikallisyksiköt sijaitsevat pääkaupunkiseudun läheisyydessä: Hyvinkäällä, Keravalla, Leppävaarassa, Lohjalla, Otaniemessä, Porvoossa ja Tikkurilassa.
Laurea on Federation of Universities of Applied Sciences (FUAS) yhteistyöryhmän jäsen. Laurean lisäksi yhteistyöryhmään kuuluvat Hämeen sekä Lahden ammattikorkeakoulut.

Laurea-ammattikorkeakoulussa on tarjolla kymmenen eri koulutusohjelmaa, joista kuutta on mahdollista opiskella englanninkielisenä. Kaikissa koulutusohjelmissa sovelletaan työelämää lähellä olevaa Laurean kehittämää Learning by Developing -toimintamallia. Valmistuvien opiskelijoiden työllistymisprosentti on erittäin korkea: 96,4%.
(Laurea 2015.)

Tutkimus toteutettiin laadullisen tutkimuksen tapaan keräämällä tietoa parhaiksi todetuilta verkkosivuilta ja omaa ammattitaitoa hyödyntäen. Aineistona on käytettävänä lähinnä internetistä löytyvää tietoa, sillä kyseessä on uusiutuvaa tekniikkaa, joten tieto saattaa vanheta hyvinkin nopeasti.

3 Remote Access ja etäkäyttö

Yhä useampi käyttäjä on tutustunut etäkäyttöön ollakseen tuottavampi myös toimiston ulkopuolella. IDC:in (International Data Corporation) mukaan vuoden 2008 kolmannella neljänneksellä oli piste, jolloin tietokoneiden valmistajat toimittivat ensimmäistä kertaa enemmän kannettavia tietokoneita kun työasemia maailmanlaajuisesti. (Businesswire 2008)

Kuitenkaan käyttäjien tapa päästä käsiksi resursseihin verkossa ei ole muuttunut. Vaikka pääsy verkkoon onnistuu lähes mistä tahansa, on kuitenkin yrityksillä palomuurit jotka estävät pääsyn organisaatioiden sisäisiin verkkoihin. Yleisesti vain käyttäjät, jotka ovat fyysisesti yhdistetty sisäisiin verkkoihin voivat käyttää niiden tarjoamia resursseja. Tämä tuo ylläpidolle ongelmia sillä tietokoneita päivitetään yleisesti tietokoneen ollessa yhteydessä sisäverkkoon. Tämä rajoitus kierretään tarjoamalla VPN-palveluita. (Microsoft 2010)

Remote Access palvelinrooli on looginen ryhmittely seuraavista verkkoon pääsyyn liittyvistä teknologioista.

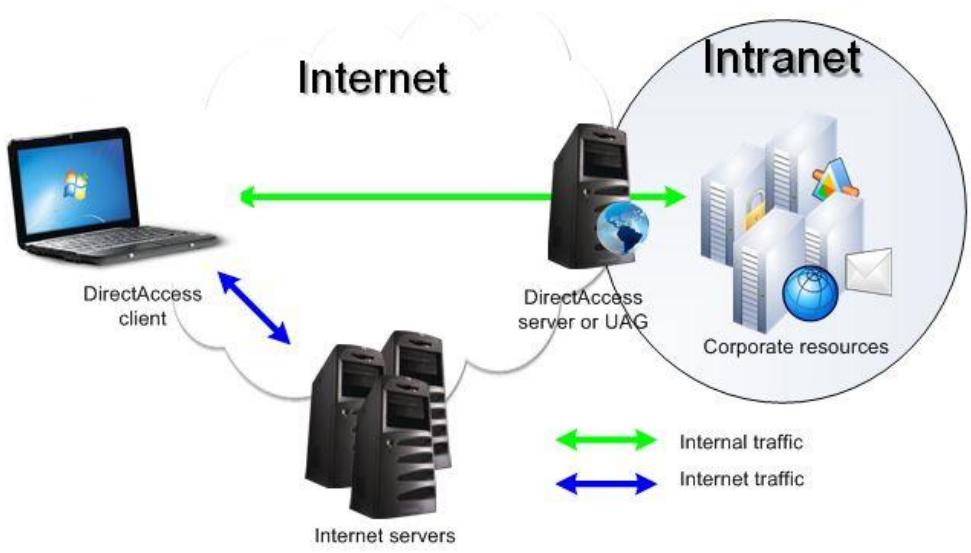
- DirectAccess
- Routing and Remote Access
- Web Application Proxy

Nämä teknologiat ovat roolipalveluita, jotka sisältyvät Remote Access palvelinrooliin. Remote Access sisältyy Windows Server 2008, 2012 ja 2012R2 käyttöjärjestelmiin. (TechNet Microsoft 2014)

4 DirectAccess

DirectAcces on roolipalvelu joka sisältyy Remote Acces palvelinrooliin. Se on pohjiltaan hyvin samantyyppinen kuin perinteinen VPN, mutta sillä on siihen nähden kuitenkin useita etuja. Suurin etu on, että DirectAccess-yhteydet ovat läpinäkyvämpiä kuin VPN-yhteydet. Kun käyttäjät normaalisti avaavat ja sulkevat VPN-yhteyden manuaalisesti, DirectAccess- yhteydet tekevät saman automaattisesti. Tämä läpinäkyvyys tarkoittaa, että heti kun käyttäjän laite on yhdistettynä internettiin, käyttäjä pääsee käsiksi yrityksen sisäiseen verkkoon ja yrityksen resursseihin muodostamatta yhteyttä manuaalisesti. DirectAccess-yhteys aloitetaan ennen kuin käyttäjä kirjautuu laitteeseen. Tämä automaattinen yhteys toimii molempiin suuntiin ja mahdollistaa järjestelmävalvojille etähallinnan laitteista.

DirectAccess otettiin käyttöön ensimmäistä kertaa Windows Server 2008 R2 ja Windows 7 käyttöjärjestelmien myötä. DirectAccess mahdollistaa etäkäyttäjälle turvallisen pääsyn yrityksen yhteisiin jaettuihin resursseihin, verkkosivuihin ja sovelluksiin yrityksen sisäverkossa ilman VPN-verkkoon yhdistämistä. DirectAccess luo kaksisuuntaisen yhteyden sisäisen verkon kanssa joka kerta kun DirectAccessiin liitetty tietokone on kytkettynä internettiin. Käyttäjien ei tarvitse miettiä sisäiseen verkkoon kytkeytymistä, ja ylläpitäjät voivat hallita etänä tietokoneita toimiston ulkopuolelta, vaikka tietokoneet eivät ole yhdistettynä VPN:in



Kuva 1 DirectAccess erottaa julkisen ja sisäisen liikenteen. (Blogs TechNet 2012)

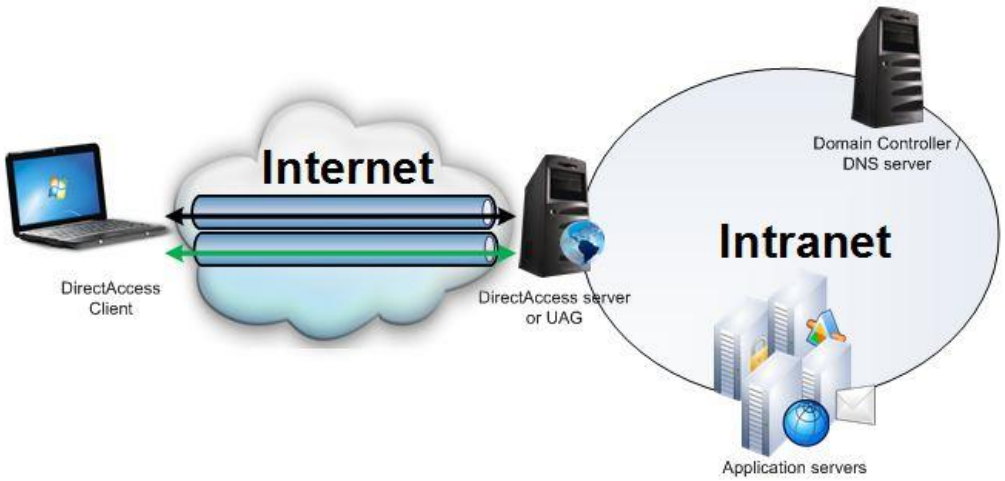
DirectAccess roolipalvelulla Windows Server 2008 R2 käyttöjärjestelmässä oli seuraavat tavoitteet organisaatioille

- DirectAccess parantaa liikkuvien työntekijöiden tuottavuutta liittämällä heidän tietokoneensa automaattisesti ja saumattomasti heidän yrityksensä sisäiseen verkkoon milloin tahansa kun internet-yhteys on käytettävissä
- DirectAccessin avulla ylläpitäjät voivat hallita tietokoneita päivittämällä ryhmäkäytäntöasetuksia ja jakamalla ohjelmistopäivityksiä milloin tahansa kun tietokone on kytkettynä verkkoon.
- DirectAccess erottaa sisäisen verkon julkisen verkon liikenteestä. Kun sovellus joka sijaitsee DirectAccess päättellä yrittää selvittää nimen, se vertaa nimeä NRPT (Name Resolution Policy Table):n sääntöihin. Jos vastaavuuksia ei löydy, DirectAccess pääte käyttää DNS-palvelimia nimen selvittämiseen. (Blogs TechNet 2012)

4.1 Tunnelit

DirectAccess on rakennettu vankan perustan omaavien standarditeknologioiden päälle, jotka ovat Internet Protocol Security (IPSec) ja Internet Protocol version 6 (IPv6). DirectAccess käyttää IPsec:iä käyttäjän ja tietokoneen autentikoimiseen, sallien sen hallita tietokonetta ennen käyttäjän sisäänkirjautumista. Vaihtoehtoisesti voidaan myös vaatia älykorttia käyttäjien tunnistautumiseen. DirectAccess myös hyödyntää IPsec:iä tarjoamaan salausta kommunikaatioon internetissä.

Asiakasohjelma luo IPSec-tunnelin IPv6 liikenteelle DirectAccess-palvelimelle, joka toimii porttina intranetiin.



Kuva 2 DirectAccess-yhteys muodostuu sisäiseen verkkoon käyttäen IPseciä ja IPv6:ta (Microsoft 2010)

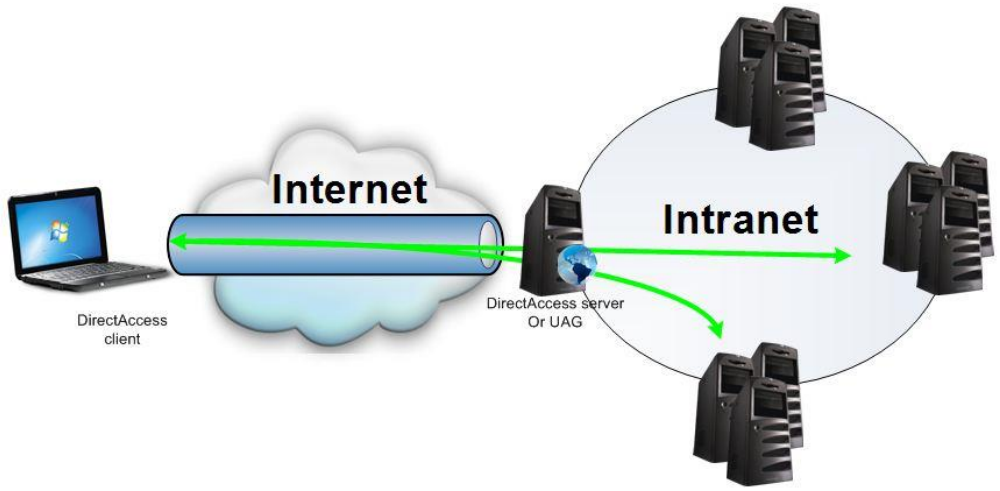
IPsec Encapsulating Security Payload (ESP) tunneli käyttää tietokonesertifikaattia, joka tarjoaa pääsyn organisaation sisäiseen verkon DNS-palvelimelle ja domain controllerille. Tämä sallii tietokoneen automaattisesti lataavan ryhmäkäytäntöasetukset ja hoitavan autentikoinnin käyttäjän puolesta.

IPsec ESP-tunneli, joka käyttää sekä tietokonesertifikaattia ja käyttäjätiedoilla tunnistautumista, todentaa käyttäjän ja tarjoaa pääsyn yrityksen sisäverkon resursseihin ja sovelluspalvelimiin. Esimerkiksi. tämän tunnelin olisi oltava pystytettynä ennen kuin Microsoft Outlook voisi ladata sähköpostia sisäverkon Microsoft Exchange-palvelimelta.

Tunneleiden DirectAccess-palvelimelle pystyttämisen jälkeen asiakastietokone voi aloittaa liikenteen lähettämisen sisäverkkoon näiden tunneleiden läpi. DirectAccess-palvelin voidaan määrittää hallitsemaan mitä sovelluksia etäkäyttäjät voivat ajaa ja mihin sisäverkon ominaisuuksiin heillä on pääsy. DirectAccess-päätteet voivat muodostaa yhteyden sisäverkkoon valitsemalla kahdesta eri IPsec suojauksesta: end-to-end- tai end-to-edge. (Microsoft 2010)

4.1.1 End-to-end suojaus

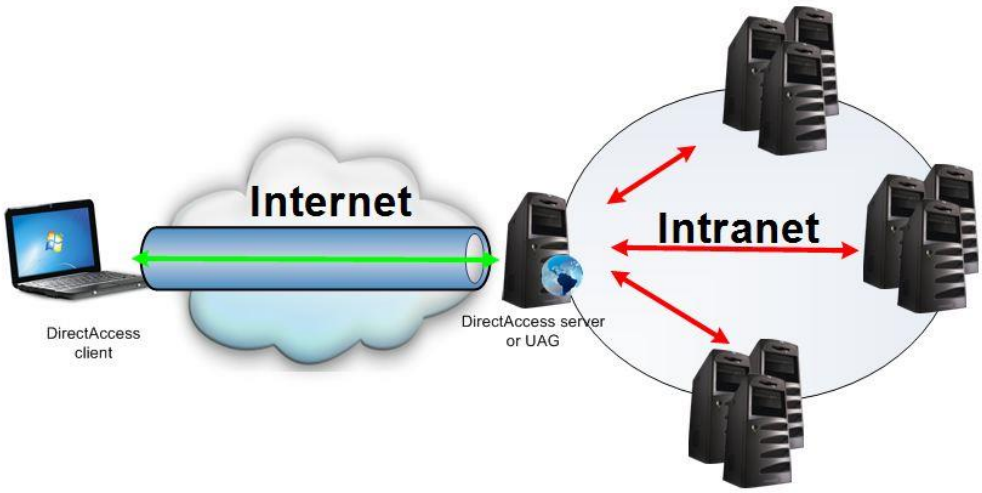
End-to-end suojauksella DirectAccess-päätteet muodostavat IPsec-session DirectAccess-palvelimen lävitse jokaiseen sovelluspalvelimeen johon ne ottavat yhteyden. Tämä tarjoaa parhaan mahdollisen turvallisuuden koska tässä tekniikassa on mahdollista määrittää pääsynvalvonta DirectAccess-palvelimella. Kuitenkin tämä arkkitehtuuri vaatii sovelluspalvelimien käyttävän Windows Server 2008 tai Windows Server 2008 R2 käyttöjärjestelmää ja käyttävän IPv6- ja IPsec protokollia.



Kuva 3 DirectAccess-päätteet muodostavat IPsec-session DirectAccess-palvelimen lävitse jokaiseen sovelluspalvelimeen johon ne ottavat yhteyden. (Microsoft 2010)

4.1.2 End-to-edge suojaus

Tässä suojauksessa DirectAccess-päätteet muodostavat IPsec-session IPsec-yhdyskäytäväpalvelimeen (joka on oletusarvoisesti samassa tietokoneessa kuin DirectAccess-palvelin). Ipsec-yhdyskäytäväpalvelin välittää tämän jälkeen suojaamattoman liikenteen sovelluspalvelimiin sisäverkkoon. Tämä arkkitehtuuri ei vaadi IPsec:iä yrityksen sisäverkkoon ja toimii minkä tahansa IPv6:ta tukevan sovelluspalvelimen kanssa. (TechNet Microsoft 2012)



Kuva 4 DirectAccess-päätteet muodostavat IPsec-session IPsec-yhdyskäytäväpalvelimeen (Microsoft 2010)

4.2 DirectAccess autentikointi

DirectAccess todentaa tietokoneen ennen kuin käyttäjä kirjautuu sisään. Tyypillisesti konetodennus antaa pääsyn vain domain controllereille ja DNS-palvelimille. Sisäänkirjautumisen jälkeen DirectAccess varmentaa käyttäjän ja käyttäjä voi päästä käsiksi mihin tahansa resursseihin mihin hänellä on lupa. DirectAccess tukee standardia käyttäjätodennusta käyttämällä käyttäjänimeä ja salasanaa. Parempaan turvallisuuteen on suositeltavaa käyttää lisäksi tunnistautumiseen tarkoitettuja älykortteja. Tämän tyyppinen kokoonpano sallii käyttäjälle pääsyn internettiin ilman älykorttia, mutta vaatii sitä kuitenkin yhdistettäessä yrityksen sisäverkkoon. Älykortti-todennus estää hyökkääjän, joka on päässyt käsiksi käyttäjän salasanaan ja käyttäjätunnukseen, (mutta ei älykorttiin) pääsyn sisäverkkoon. Tämä toimii samoin myös toiseen suuntaan, jolloin hyökkääjä pääsee käsiksi älykorttiin, mutta hänellä ei ole tietoa käyttäjän salasanasta, eikä käyttäjätunnuksesta. (Microsoft 2010)

4.3 DirectAccess ja Network Access Protection

Kannustaakseen noudattamaan yrityksen turvallisuuspolitiikkaa, sekä vähentääkseen haittaohjelmien leviämistä, vaatimustenvastaisia päätteitä voidaan rajoittaa käyttämästä sisäisen verkon resursseja ja rajoittaa liikennettä vaatimustenmukaisten koneiden kanssa. Käyttämällä Network Access Protectionia (NAP). DirectAccessin kanssa, järjestelmänvalvojat voivat vaatia DirectAccess-koneiden olevan puhtaita haittaohjelmista ja noudattavan yrityksen turvallisuuspolitiikkaa. Esimerkiksi tietokoneet voivat saada yhteyden DirectAccess-palvelimeen vain, jos niillä on viimeisimmät tietoturvapäivitykset, anti-malware määritelmät ja muut suojausasetukset. Käyttämällä NAP:ia yhdessä DirectAccessin kanssa, edellytyksenä on, että DirectAccess-koneet, joissa on NAP käytössä toimittavat terveys-sertifikaatin varmennukseksi luodessaan yhteyden DirectAccess-palvelimen kanssa. Terveys-sertifikaatti sisältää tietokoneen identiteetin, sekä todisteen järjestelmän terveestä tilasta. Terveys-sertifikaatti on hankittava ennen yhteyden muodostamista DirectAccess-palvelimelle. Käyttämällä NAP:ia DirectAccessin kanssa, vaatimustenvastainen tietokone, jossa on mahdollisesti haittaohjelma, ei voi muodostaa yhteyttä organisaation sisäverkkoon. Tämä rajoittaa haittaohjelman kykyä levitä. NAP:ia ei ole pakollista käyttää DirectAccessiin kanssa, mutta se on suositeltavaa. (Microsoft 2010)

5 Routing And Remote Access

Routing and Remote Access service (RRAS) tukee etäkäyttäjää tai site-to-site yhteyttä käyttämällä Virtual Private Networkia (VPN) tai dial-up yhteyttä. Routing and Remote Access Service on Microsoftin rajapinta ja palvelinohjelma, joka mahdollistaa sovelluksien luomisen käyttöjärjestelmän RRAS palveluiden hallinnoimiseen. Kehittäjät voivat myös käyttää RRAS:ia toteuttaakseen reititysprotokollia. (Msdn Microsoft 2015)

5.1 Reitittäminen

Reititin on laite, joka hallitsee tiedonkulun verkon osiin tai aliverkkoihin. Reititin ohjaa saapuvat ja lähtevät paketit, joten se tietää tietoverkkojen toisiinsa liittyvät suhteet. Heijastamalla verkkoliikennettä ja reitittämistarpeita, perustuen laitteiden ja applikaatioiden määrään ja tyyppiin mitkä ovat organisaatiossa käytössä, voidaan päättää käytetäänkö fyysistä reititinlaitteistoa, ohjelmisto-pohjaista reititintä vai molempien yhdistelmää. Yleisesti fyysiset reitittimet käsittelevät paremmin raskaampia reititysvaatimuksia, kun taas halvemmat ohjelmisto-pohjaiset reitittimet ovat riittäviä käsittelemään kevyempiä reitityskuormia.

Ohjelmisto-reititysratkaisu, kuten Routing and Remote Access service, voi olla ihanteellinen pienessä segmentoidussa verkossa, jossa on suhteellisen kevyt liikenne aliverkkojen välillä. Toisaalta yrityksen verkkoympäristöt, joilla on suuri määrä verkon osia ja laaja skaala suoritustuskykyvaatimuksia, voivat tarvita moniakin fyysisiä reitittimiä suorittamaan eri rooleja koko verkkoon. (Technet Microsoft 2014)

5.2 Etäkäyttö

Määrittämällä Routing and Remote Accessin toimimaan etäkäyttöpalvelimena, voidaan yhdistää etä -tai liikkuvia työntekijöitä organisaation verkkoihin. Etäkäyttäjät voivat työskennellä samalla tavalla, kuin heidän tietokoneensa olisi kytkettynä fyysisesti yrityksen verkkoon.

Kaikki palvelut, jotka ovat tyypillisesti saatavilla LAN-yhdistetylle käyttäjälle (mukaan lukien tiedostojen ja tulostimien jakaminen, Web server access ja viestintä) ovat käytössä Remote Access-yhteyden avulla. Esimerkiksi palvelimella, jossa on käytössä Routing and Remote Access, voidaan päätteellä käyttää selainta asemien yhdistämiseen ja tulostimien yhdistämiseen. Koska asemakirjaimet ja Universal Naming Convention (UNC) nimet ovat täysin tuettuja Remote Accessissa, useimmat kaupalliset ja räätälöidyt sovellukset toimivat ilman muutoksia. Palvelin, jossa on käynnissä Routing and Remote Access, tarjoaa kaksi erityyppistä etäkäyttö liitettävyyttä, jotka ovat VPN ja Dial-up networking (Technet Microsoft 2014)

5.2.1 Virtual private networking (VPN)

VPN on turvattujen point-to-point yhteyksien luomus, joka kulkee yksityisen- tai julkisen verkon, kuten internetin poikki. VPN-client käyttää erityisiä TCP/IP-pohjaisia protokollia (näitä kutsutaan tunnelointiprotokolliksi) tehdäkseen virtuaalisen kutsun virtuaaliseen porttiin VPN-palvelimella. Hyvä esimerkki VPN verkosta on VPN-asiakasohjelma, joka muodostaa VPN-yhteyden etäkäyttöpalvelimelle, joka on yhteydessä Internettiin. Etäkäyttöpalvelin vastaa virtuaaliseen kutsuun, varmentaa kutsujan ja siirtää dataa VPN-asiakasohjelman ja yrityksen verkon välillä.

Toisin kuin puhelinverkkoyhteydessä, VPN on aina looginen, epäsuora yhteys VPN-asiakasohjelman ja VPN-palvelimen välillä julkisen verkon, kuten Internetin yli. Varmistaakseen turvallisuuden, tieto, joka lähetetään yhteyksien välillä, on salattava. (Technet Microsoft 2014)

5.2.2 Dial-up networking

Puhelinverkkoyhteydessä, etäyhteys-asiakasohjelma muodostaa väliaikaisen puhelinverkkoyhteyden fyysiseen porttiin etäkäyttöpalvelimeen käyttäen palveluntarjoajan palveluita, kuten analogista puhelinta tai ISDN:ia. Hyvä esimerkki tästä on puhelinverkkoyhteyden muodostava asiakasohjelma, joka soittaa etäkäyttöpalvelimen yhden portin puhelinnumeroon. Puhelinverkkoyhteydet analogisen puhelinlinjan tai ISDN:in yli ovat suora fyysinen yhteys puhelinverkkoyhteyden asiakasohjelman ja palvelimen välillä. Tiedot voidaan salata tässäkin tapauksessa, mutta sitä pidetä vaadittavana. (Technet Microsoft 2014)

5.3 RRAS Multitenant Gateway

Jos käytössä on Hyper-V Network Virtualization tai jos käytössä on virtuaalisesti hallittuja verkkoja, jotka ovat käytössä VLAN:ien kanssa, voidaan RRAS ottaa käyttää virtuaalikone-pohjaisena ohjelmiston yhdyskäytävänä ja reitittimenä, joka sallii pilvipalvelutarjoajien ja yritysten välille verkkoliikenteen reitityksen fyysisten ja virtuaalisten verkkojen välille.

RRAS Multinentant Gatewayn kanssa voidaan antaa halutulle ryhmälle oikeus muodostaa VPN-yhteys virtuaalikone-verkon resursseihin mistä tahansa. On myös mahdollista luoda ryhmälle site-to-site VPN-yhteys ryhmän resurssien ja organisaation datakeskuksen välille. Lisäksi voidaan määrittää RRAS Multinentant Gateway Border Gateway-protokollan kanssa dynaamista reititystä varten ja voidaan myös ottaa käyttöön NAT, joka tarjoaa internet-yhteyden virtuaalikoneille. (Technet Microsoft 2014)

6 Web Application Proxy

Web Application Proxy on roolipalvelu, joka sisältyy Remote Access palvelinrooliin. Molemmat näistä sisältyvät Windows Server 2012 R2 käyttöjärjestelmään. Web Application Proxy tarjoaa käänteisen välityspalvelimen toiminnot Web-sovelluksiin yrityksen sisäisen verkon sisällä käyttäen mitä tahansa päätelaitetta yrityksen sisäverkon ulkopuolelta. Web Application Proxy ennalta todentaa pääsyn Web-sovelluksiin käyttämällä Active Directory Federation Services (AD FS) -palvelua. Web Application Proxy toimii myös AD FS:n välityspalvelimena. (Technet Microsoft 2014)

Pääasiassa Web Application Proxy toimii kahdella tavalla. Se tekee organisaation kykeneväksi antamaan loppukäyttäjälle organisaation ulkopuolella valkoidun pääsyn sovelluksiin, jotka sijaitsevat yrityksen sisällä sijaitsevilla palvelimilla. Samaan aikaan Web Application Proxy toimii myös barrikadina yrityksen sovellusten ja internetin välillä.

Web Application Proxy toimii yhdessä ominaisuuksien kuten Workplace Join:in kanssa. Tämän avulla käyttäjä voi rekisteröidä omia laitteitaan Active Directoryn kanssa. (Searchwindowdsserver Techtarget 2013)

6.1 Sovelluksiin pääsyn tarjoaminen

Web Application Proxy tarjoaa organisaatioille mahdollisuuden tarjota yrityksen ulkopuolella sijaitseville loppukäyttäjille valikoidun pääsyn yrityksen sisällä sijaitseville palvelimille. Prosessia, jossa sovellus annetaan saataville ulkoisesti, kutsutaan julkaisuksi (engl. Publish). Toisin kuin perinteisissä VPN-ratkaisuissa, julkaistaessa sovelluksia Web Application Proxyn avulla loppukäyttäjät pääsevät käsiksi ainoastaan sovelluksiin, jotka päätetään julkaista. Kuitenkin Web Application Proxya voidaan käyttää myös VPN:in kanssa. (Technet Microsoft 2014)

6.2 Sovellusten julkaisu

Web Application Proxyn julkaisu mahdollistaa loppukäyttäjälle pääsyn yrityksen sovelluksiin käyttäjän omilta laitteiltaan, jolloin käyttäjät eivät ole riippuvaisia yrityksen tarjoamista tietokoneista. Loppukäyttäjä voi käyttää kotikonetta, tablettia tai älypuhelinta pääsyyn julkaistuihin sovelluksiin. Lisäksi loppukäyttäjiltä ei vaadita ylimääräisten sovellusten asentamista omille laitteilleen päästäkseen käsiksi julkaistuihin sovelluksiin. Web Application Proxya voidaan käyttää standardeilla selaimilla. Web Application Proxy palvelee käänteisenä välityspalvelimena mille tahansa sovellukselle, joka on julkaistu sen kautta, jonka vuoksi loppukäyttäjä

kokee yhdistämisen samanlaiseksi kuin se yhdistettäisiin suoraan sovellukseen. (Technet Microsoft 2014)

6.3 Sovelluksiin pääsy

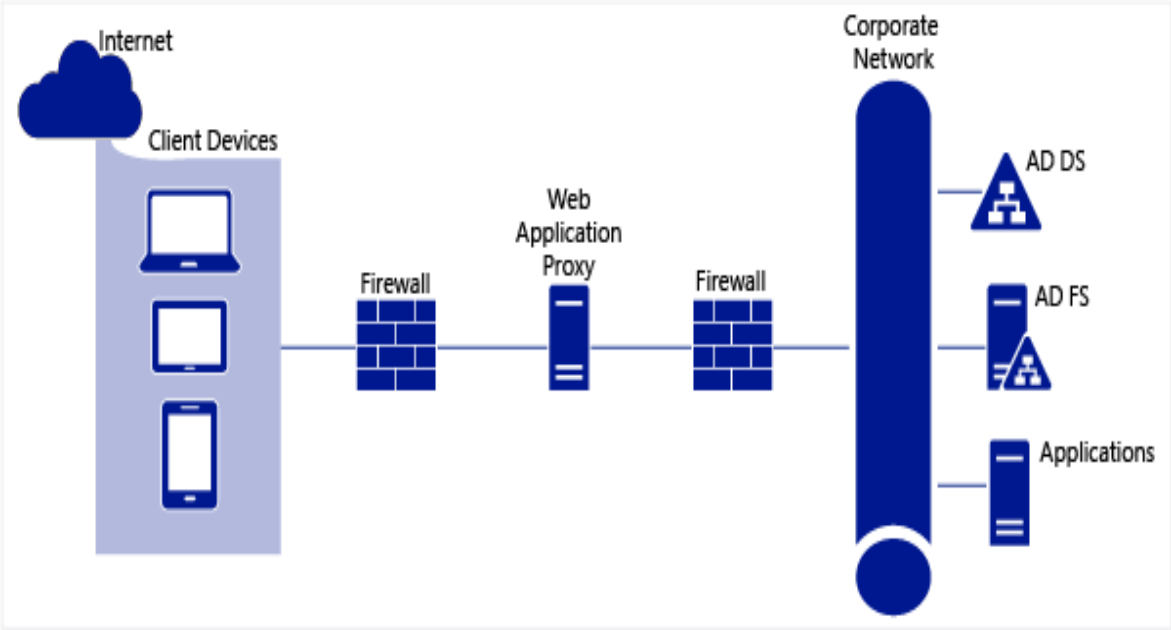
Web Application Proxy on aina otettava käyttöön AD FS:n kanssa. Näin voidaan hyödyntää AD FS:n ominaisuuksia, kuten SSO:ia. Tämän avulla käyttäjän tarvitsee suorittaa todennus vain yhden kerran. Suojellakseen pääsyä sovelluksiin yrityksen sisällä, on suositeltavaa antaa pääsy vain todennetuille ja valtuutetuille käyttäjille. Julkaistaessa sovelluksia Web Application Proxyn kautta, tämä saavutetaan AD FS:n kanssa, joka tarjoaa todennuksen ja valvoo pääsyä julkaistuihin sovelluksiin. (Technet Microsoft 2014)

6.4 Sovellusten suojaaminen ulkoisilta uhilta

Web Application Proxy toimii muurina internetin ja yrityksen sisäisten sovellusten välillä. Otettaessa Web Application Proxy käyttöön ja julkaistaessa ohjelmia sen kautta, tulevat ohjelmat käyttöön ulkopuolisille käyttäjille heidän omilla laitteillaan, kuten tableteilla, tietokoneilla ja puhelimilla. Nämä laitteet eivät ole liitettyjä yrityksen toimialueeseen (engl. Domain), josta syystä ne luokitellaan automaattisesti hallinnoimattomiksi laitteiksi, jotka ovat epäluotettavia yrityksen verkossa. Yrityksen käyttäessä Web Application Proxya on kuitenkin tarkoitus mahdollistaa pääsy tärkeään informaatioon juuri näillä laitteilla mistä vain ja milloin vain. Web Application Proxy tarjoaa lukuisia tietoturva vaihtoehtoja yrityksen verkon suojaksi ulkoisilta uhilta. Todennukseen käytetään AD FS:n, jotta voidaan varmistaa, että vain halutut käyttäjät pääsevät käsiksi yrityksen sovelluksiin. (Technet Microsoft 2014)

6.5 Tietoturvasuosituksia

Suositellussa käyttöönotossa Web Application Proxy on sijoitettu ns. Demilitarisoidulle alueelle eli aliverkkoon, joka yhdistää yrityksen omat järjestelmät esim. internettiin tai muuhun turvattomaan alueeseen. Palomuurien tuoman tietoturvan lisäksi Web Application Proxy tarjoaa kuitenkin ylimääräisen suojan sovelluksille ulkoisia uhkia vastaan.



Kuva 5 Web Application Proxyn toimintamalli (Technet Microsoft 2014)

Kun HTTPS-liikenne, joka on suunnattu Web Application Proxyn julkaisemaan osoitteeseen, saapuu, Web Application Proxy sulkee muun liikenteen ja käynnistää uudet pyynnöt julkaistuille sovelluksille. Kun käyttäjä ottaa yhteyden julkaistuun sovellukseen, ei yhteys ole suoraan kiinni sovelluksessa vaan sitä käytetään Web Application Proxyn kautta.

Kaikki muu liikenne, joka saapuu Web Application Proxyyn, tiputetaan, eikä sitä ohjata julkaistuille sovelluksille. Tämä sisältää mitkä tahansa laittomat HTTP tai HTTPS pyynnöt, joita voidaan käyttää osana erilaisia palvelunestohyökkäyksiä.

Mikä tahansa todentamispyyntö, joka saapuu Web Application Proxyyn ja sisältää todentamisvaltuuden AD FS:tä tarkastetaan. Näin voidaan varmistaa, että todennus on tarkoitettu päätteelle, josta pyyntö on tullut. Tämä tehdään tarkistamalla, että päätelaite vastaa todentamispyyntöön, joka tunnistaa laitteen, mikä on todennettu AD FS:ssä. (Technet Microsoft 2014)

6.6 Käyttäjien ja laitteiden todentaminen

Julkaistaessa sovelluksia Web Application Proxyn kautta, prosessia, jossa käyttäjät ja laitteet varmennetaan ennen pääsyä sovelluksiin, kutsutaan etukäteisautentikoinniksi (engl. pre-authentication). Web Application Proxy tukee kahden tyyppistä ominaisuutta, jotka ovat AD FS etukäteisautentikointi ja Pass-through etukäteisautentikointi.

Käytettäessä Active Directorya AD FS etukäteisautentikointiin, käyttäjältä vaaditaan autentikointi AD FS- palvelimelle ennen kun Web Application Proxy ohjaa käyttäjän julkaistulle sovellukselle. Näin varmistetaan, että kaikki sovelluksiin kohdistuva liikenne on varmennettua.

Pass-through etukäteisautentikoinnissa käyttäjän ei tarvitse syöttää käyttäjätietojaan ennen yhdistämistä julkaistuihin sovelluksiin. Sovellus, joka on asetettu käyttämään Pass-Through etukäteisautentikointia, ei vaadi käyttäjää syöttämään tietojaan päästäkseen käsiksi yrityksen verkkoon, mutta voi vaatia käyttäjää syöttämään käyttäjätietonsa tarkastellakseen sovellusten sisältöä.

Jotta käyttäjä pääsisi helposti käsiksi sovelluksiin käyttäen AD FS etukäteisautentikointia, loppukäyttäjän tulisi käyttää yhtä seuraavista asiakasohjelmista (engl. client).

- Mikä tahansa asiakasohjelma mikä tukee http-uudelleenohjausta; esimerkiksi selain, suorittaa Web Application Proxy asianmukaiset toimet saapuvan pyynnön osalta ja uudelleenohjaa käyttäjän autentikoituun osoitteeseen ja takaisin alkuperäiseen Web-osoitteeseen, tällä kertaa autentikoidun todisteen kanssa.

- Rikkaat asiakasohjelmat (engl. Rich client), jotka käyttävät http-basic autentikointia, esimerkiksi. Exchange tai ActiveSync.

- Mikä tahansa asiakasohjelma, joka käyttää MSOFBA-autentikointia; esimerkiksi, Word, Excel tai PowerPoint. Tässä tapauksessa käyttäjä joka yrittää päästä käsiksi dokumenttiin käyttäjän ”viimeisimmät dokumentit” listasta, joka on tallennettu palvelimelle, joka sijaitsee yrityksen sisäisessä verkossa.

- Windows Storen sovelluksilla ja RESTful sovelluksilla asiakasohjelmien kanssa, jotka käyttävät Web Authentication Brokeria autentikointiin. Sovelluksen avaaminen onnistuu omilta laitteiltaan. Laite hoitaa autentikoinnin AD FS:tä Web Authentication Brokerin välityksellä. Näin sisällytetään käyttäjälle varmennus myöhempiä pyyntöjä varten. (Technet Microsoft 2014)

6.7 Todentamiskyky

Käytettäessä AD FS:ä autentikointiin, hyödytään kaikista palveluista mitä AD FS tarjoaa. Workplace Join on uusi palvelu AD FS:ssä Windows Server 2012 R2 käyttöjärjestelmässä. Se mahdollistaa käyttäjien omien laitteiden, jotka eivät normaalisti olisi liitettynä yrityksen toimialueeseen, liittämisen Workplaceen. Näitä laitteita ovat esimerkiksi henkilökohtaiset kannettavat tietokoneet, tabletit ja älypuhelimet. Kun tämä palvelu on otettu käyttöön, AD FS:in ylläpitäjä voi asettaa kaikille sovelluksille tai yksittäisille sovelluksille vaatimuksen, jolla laitteille vaaditaan tunnistautuminen ennen pääsyä julkaistuille sovelluksille. Tunnistautumisessa voidaan käyttää hyväksi esimerkiksi SSO:ia tai MFA:ia.

7 Yhteenveto

Aiheeseen liittyvää suomenkielistä lähdemateriaalia oli vähän käytettävissä. Tämä toi osaltaan oman haasteensa, sillä asia oli teknistä ja monipuolista. Tutkimus oli mielenkiintoinen ja työn tavoite, kerätä tietoa etäkäyttöön liittyvistä roolipalveluista, kosketti suurta käyttäjämäärää. Tutkimusta tehdessä käsitys Remote Accessin hyödyistä vahvistui ja syntyi ymmärrys siitä kuinka Remote Access joustavoittaa sekä lisää mahdollisuuksia eri järjestelmien käytössä yritysympäristössä.

Tätä tietopakettia voidaan hyödyntää esimerkiksi TEM-matkalaskujärjestelmän kanssa Web Application Proxyn avulla. Tutkimusta tehdessä selvisi, että Web Application Proxy on Laureassa käytössä jo monien palveluiden pohjana ja Laurealla on tarkoitus käyttää sitä lisääntyvässä määrin. Työssä haluttiin perehtyä toimeksiantajan kanssa yhdessä sovitusti Remote Access-kokonaisuuteen laajemmin.

Jatkokehittämisen aiheena työtä voi laajentaa varsinkin tietoturvaan liittyen. Vuonna 2016 julkaistaan uusi Windows Server 2016, joka tuo joukon uusia ominaisuuksia Web Application Proxyyn. Tämä tuo mukanaan uusia haasteita, joita kannattaa tutkia ja keskittää työ ainoastaan Web Application Proxyyn sen ollessa jatkossa entistä tärkeämpi työkalu etäkäyttöön liittyen. Käyttöohje Remote Accessin käyttöönotosta on myös hyvä tehdä.

Lähteet

Blogs Technet. 2012. Windows Server 2012 Direct Access. Viitattu 10.9.2015.
http://blogs.technet.com/b/meamcs/archive/2012/05/03/windows-server-2012-direct-access-part-1-what-s-new.aspx

Businesswire.2008. PC Market Will Slow As Financial Turmoil Spreads, According to IDC. Viitattu 29.9.2015
http://www.businesswire.com/news/home/20081203005281/en/PC-Market-Slow-Financial-Turmoil-Spreads-IDC#.VgpMn0Y9k8k

Cisco. 2014. Network Address Translation (NAT) FAQ. Viitattu 23.9.2015.
http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

Cisco. 2014. VLAN Overview. Viitattu 22.9.2015.
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vlans.html#wp1032048

Instantssl. 2015. HTTP VS HTTPS. Viitattu 22.9.2015.
https://www.instantssl.com/ssl-certificate-products/https.html

Live Laurea. 2015. Viitattu 23.9.2015.
https://live.laurea.fi/fi/laurea_info/organisaatio/Sivut/default.aspx

Microsoft. 2010. Technical Overview of Direc-tAccess in Windows 7 and Windows Server 2008 R2. Viitattu 9.9.2015.
http://www.microsoft.com/en-us/download/details.aspx?id=17039

Msdn Microsoft. 2009. RESTful XHTML - RESTful Services With ASP.NET MVC. Viitattu 23.9.2015.
https://msdn.microsoft.com/en-us/magazine/dd943053.aspx

Msdn Microsoft. 2014. Rich Client Application Walkthroughs. Viitattu 22.9.2015.
https://msdn.microsoft.com/en-us/library/188ht7d8%28v=vs.90%29.aspx

Msdn Microsoft. 2015. Security Token Service. Viitattu 22.9.2015.
https://msdn.microsoft.com/en-us/library/ee748490.aspx

Msdn Microsoft. 2015. Routing and Remote Access Service. Viitattu 20.9.2015.
https://msdn.microsoft.com/en-us/library/Aa446768

Searchwindowsserver Techtarger. 2013. Web Application Proxy definition. Viitattu 10.9.2015.
http://searchwindowsserver.techtarget.com/definition/Web-Application-Proxy

TechNet Microsoft. 2014. About single sign-on. Viitattu 30.9.2015.
https://technet.microsoft.com/en-us/library/cc995112.aspx

TechNet Microsoft. 2014. Active Directory Federation Services Overview. Viitattu 18.9.2015.
https://technet.microsoft.com/en-us/library/hh831502.aspx

TechNet Microsoft. 2015. Configure Basic Authentication (IIS 7) Viitattu 23.9.2015.
https://technet.microsoft.com/fi-fi/library/cc772009%28v=ws.10%29.aspx

TechNet Microsoft. 2015. Domain Name System. Viitattu 23.9.2015.
https://technet.microsoft.com/fi-fi/network/bb629410.aspx

Technet Microsoft. 2010. Overview of Hyper-V. Viitattu 22.9.2015.
https://technet.microsoft.com/en-us/library/cc816638%28WS.10%29.aspx

TechNet Microsoft. 2013. Roles, Role Services, and Features. Viitattu 22.9.2015.
https://technet.microsoft.com/en-us/library/cc754923.aspx

TechNet Microsoft. 2001. Virtual Private Networking: An Overview. Viitattu 22.9.2015.
https://technet.microsoft.com/en-us/library/bb742566.aspx

TechNet Microsoft. 2014. Routing and Remote Access. Viitattu 17.9.2015.
https://technet.microsoft.com/en-us/library/dn636119.aspx#bkmk_rras

Technet Microsoft. 2012. Using DirectAccess. Viitattu 10.9.2015.
https://technet.microsoft.com/en-us/windows/dn168168.aspx

TechNet Microsoft. 2014. What Is Routing and Remote Access. Viitattu 23.9.2015.
https://technet.microsoft.com/en-us/library/cc771052%28v=ws.10%29.aspx

TechNet Microsoft. 2014. Working with Web Application Proxy. Viitattu 2.9.2015.
https://technet.microsoft.com/en-us/library/dn584113.aspx

Techopedia. 2015. Remote User. Viitattu 30.9.2015
https://www.techopedia.com/definition/5554/remote-user

Windows Microsoft. 2015. What is a proxy server? Viitattu 23.9.2015.
http://windows.microsoft.com/en-us/windows-vista/what-is-a-proxy-server

Kuvat

Liitteet

Liite 1

LAUREA AMMATTIKORKEAKOULU | Yhdessä enemmän |

Terminologiaa

AD FS - Active Directory Federation Services on Microsoftin kehittämä ohjelmisto-osa, joka voidaan asentaa Windows Server käyttöjärjestelmiin tarjoamaan käyttäjille single sign-on pääsy järjestelmiin ja sovelluksiin yli organisaation rajojen. (TechNet Microsoft 2014)

Basic access authentication - perusautentikointi on menetelmä, jolla pyytää autentikoimaan käyttäjänimen ja salasanan avulla. (Technet Microsoft 2015)

DNS - Domain Name System on tietokanta, joka muuntaa verkkotunnukset IP-osoitteiksi. Palvelu muuntaa nimet järkevästi luettaviksi, kuten esimerkiksi www.google.com. (TechNet Microsoft 2015)

HTTPS - Hypertext Transfer Protocol Secure on tiedon suojattuun siirtoon tarkoitettu HTTP-protokollan ja TLS/SSL-protokollan yhdistelmä. (Instantssl 2015)

Hyper-V - Hyper V on tekniikka, joka mahdollistaa virtuaalisen palvelinympäristön luomisen. (Technet Microsoft 2010)

MFA - Multifactor autentikointi voidaan konfiguroida vaatimaan käyttäjiä tunnistautumaan useammalla kuin yhdellä tapaa; esimerkiksi salasanalla tai älykortilla. (Technet Microsoft 2014)

NAT - Network address translation on osoitteenmuunnostekniikka, jonka avulla julkisen IP-osoitteen käyttö onnistuu useammalla verkkoa käyttävällä laitteella. (Cisco 2014)

Proxy - Proxy eli välityspalvelin suodattaa ja varastoi tiedostoja, joita siirretään verkossa. (Windows Microsoft 2015)

Roolipalvelu - Roolipalvelut ovat ohjelmia, jotka tarjoavat valikoituja palveluita. Asennettaessa rooli, voidaan valita mitä palveluita tarjotaan muille käyttäjille ja tietokoneille organisaation sisällä. (Technet Microsoft 2013)

REST - Representational State Transfer on WWW:n ohjelmistoarkkitehtoninen tyyli. REST antaa rajoituksia komponenteille, jotka voivat johtaa korkealaatuisempaan ja ylläpidettävämpään arkkitehtuuriin. (Msdn Microsoft 2009)

Liite 1

LAUREA AMMATTIKORKEAKOULU | Yhdessä enemmän |

Rich Client - Rikas asiakasohjelma on tyypillisesti itsenäinen ohjelma, joka sisältää graafisen käyttöliittymän. (Msdn Microsoft 2014)

SSO - Single sign-on (SSO) on palvelu, joka antaa käyttäjälle mahdollisuuden suorittaa todennus vain yhden kerran, jolloin pääsy julkaistuille palveluille onnistuu sen jälkeen ilman autentikointia. (TechNet Microsoft 2014)

Token - Token on autetinkointitapa, joka sallii käyttäjän syöttää käyttäjätunnuksen ja salasanan, jotta saadaan token, joka antaa käyttäjän hakea tiettyjä resursseja käyttämättä käyttäjätunnusta ja salasanaa. Kun token on saatu, käyttäjä voi tarjota sitä, jonka jälkeen saadaan pääsy tietyksi ajaksi tiettyihin resursseihin. (Msdn Microsoft 2015)

VLAN - Virtual LAN eli virtuaalilähiverkko on tekniikka, jolla voidaan jakaa loogisiin osiin fyysinen tietoliikenneverkko. Virtual LAN on ominaisuuksiltaan sama kuin normaali lähiverkko, mutta sen avulla pystytään jakamaan osastoja omiin verkkoihin. (Cisco 2014)

VPN - Virtual Private Network on yksityisen verkon laajennus joka kattaa tiedonsiirron jaettujen tai julkisten verkkojen, kuten internetin yli. (TechNet Microsoft 2012)