# Microsoft Azure -pilvipalvelun käyttöönotto valtion yhteisessä tietoliikennepalvelussa

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Visamäki, syksy 2016

Arttu Salmi

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Visamäki
Tietojenkäsittely

TIIVISTELMÄ

**Tekijä** Arttu Salmi **Vuosi** 2017

**Työn nimi** Microsoft Azure -pilvipalvelun käyttöönotto valtion yhteisessä tietoliikennepalvelussa

TIIVISTELMÄ

Työn toimeksiantajana toimi Valtion tieto- ja viestintätekniikkakeskus (Valtori). Valtori tuottaa toimialariippumattomat ICT-palvelut asiakkailleen, jotka koostuvat valtionhallinnon organisaatioista.

Pilvipalvelut ja pilvestä saatava palvelinkapasiteetti ovat tällä hetkellä pinnalla IT-alalla. Myös valtionhallinto on kiinnostunut laajentamaan kapasiteettipalveluitaan ja kapasiteettiaan pilveen. Opinnäytetyössä keskityttiin Microsoft Azure -pilvipalveluun ja sen mahdollisuuksiin toimia pilvikapasiteettina Valtorin asiakkaille.

Työ oli toiminnallinen opinnäytetyö, jossa keskeinen idea oli kuvata ylätasolta tietoliikenteen nykytila, sekä ensimmäinen vaihe, jossa rakennetiin liityntä valtion yhteisistä tietoliikennepalveluista (VY-verkko) Azure-yksityiseen pilveen Microsoft ExpressRoute -liityntäyhteyttä hyödyntäen. Työssä käytetyt tietoliikenteen topologia- ja skenaariokuvaukset ovat suuntaa-antavia ja osin hypoteettisia, jotta työ voitiin pitää julkisena. Valtorin sisäiseen käyttöön luotiin tarkat tietoliikenteen topologiakuvaukset.

Työssä sovellettiin opinnäytetyön tekijän omaa tietämystä valtionhallinnon tietoliikenneverkkoihin liittyen, sekä teoriaosuudessa tutustuttiin pilvipalveluihin yleisesti. Teoria ja käytännön tietämys yhdistäen, voitiin johtaa ylätason skenaariokuvaukset, miltä mahdollisesti Valtorin pilvipalveluiden tietoliikennetopologia voisi näyttää tuotantomallissa.

**Avainsanat** Tietoliikenne, pilvipalvelu, Microsoft Azure, VY-verkko

**Sivut** 33 s.

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES



Visamäki
Degree Programme in Business Information Technology

**Author** Arttu Salmi **Year** 2017

**Subject of Bachelor's thesis** Commissioning Microsoft Azure cloud services in governmental telecommunication services

ABSTRACT

The thesis was commissioned by the Valtion tieto- ja viestintätekniikkakeskus (Valtori). Valtori produces business independent ICT-services to its customers, which consist of central government organizations.

At the moment cloud services and server capacity that comes from the cloud, are very popular in IT-sector. The central government is also interested to expand its capacity services in the cloud services. The focus of the thesis is in Microsoft Azure cloud services and its potential to be cloud capacity to Valtori´s customers.

The study was a functional thesis, were the main idea was to describe the current state of network topology, and describe the first phase where a link between the government shared telecommunication network (VY-verkko) and Microsoft Azure cloud services was built, using Microsoft ExpressRoute peering technology. Scenario and topology pictures that were used in this thesis, are directive and partly hypothetical, so the thesis can be public. For Valtori´s internal use, the author made accurate telecommunication topology pictures.

In this thesis the author applied his own practical knowledge about governmental telecommunication networks, and in the theory part the author familiarized himself with cloud services in general. The theory combined with the practical know-how, the author have the information needed, when planning Valtori´s cloud services telecommunication topology in production form.

**Keywords** Telecommunication, cloud services, Microsoft Azure, VY-verkko

**Pages** 33 p.

SISÄLLYS

KÄSITELUETTELO

| | |
|---|---|
| LAN | LAN (engl. Local Area Network) tarkoittaa paikallista, esimerkiksi yrityksen yhden toimipisterakennuksen verkkoa. |
| MPLS | MPLS (engl. Multiprotocol Label Switching) tarkoittaa liikenteenvälitystekniikkaa, jolla kuljetetaan esimerkiksi IP-paketteja ennalta määriteltyjen yhteyksien ylitse nopean runkoverkon solmujen kautta ilman, että solmujen tarvitsee tehdä reititystä. |
| MPLS-VPN | MPLS-tekniikkaa hyödyntäen tehty virtuaalinen erillisverkko (VPN). |
| NAT | NAT (engl. Network Address Translation) tarkoittaa IP-osoitteelle tehtävää osoitteenmuunnosta, jolla esimerkiksi privaatti lähde IP-osoite muunnetaan palomuurilla internettiin näkyväksi toiselle IP-osoitteelle. |
| Oletusreitti | Tarkoittaa reitittimen lähettämän IP-paketin seuraavaa hyppyä, eli seuraavaa reititintä mitä oletuksena käytetään kaikille IP-paketeille. |
| OSI-malli | (engl. Open Systems Interconnection Reference Model) kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemää kerrosta. |
| PEERAUS | Peeraus (engl. Peering) tarkoittaa kahden operaattorin verkkojen sisäistä yhdysliikennettä. |
| VPN | VPN (engl. Virtual Private Network) tarkoittaa virtuaalista erillisverkkoa, jolla kaksi tai useampia yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon. |
| WAN | WAN (engl. Wide Area Network) tarkoittaa usein operaattorien käyttämää maantieteellisesti laajaa yhtenäistä verkkoa, joka yhdistää esimerkiksi useita asiakkaan LAN-verkkoja yhdeksi verkoksi. |

AZURE KÄSITELUETTELO

| | |
|---|---|
| ExpressRoute | ExpressRoute-yhteys tarkoittaa Microsoftin tarjoamaa dedikoitua tietoliikenneyhteyttä Azuren ja asiakkaan välillä. |
| MSEE | (engl. Microsoft Enterprise edge router) tarkoittaa ExpressRoute yhteydessä käytettävää reititintä, joka yhdistää asiakkaan verkon ja Azuren. |
| NSG | NSG (engl. Network Security Group) tarkoittaa palomuurin kaltaista tai vastaavaa palvelua Azure-ympäristössä. |

| | |
|---|---|
| VM | VM (engl. Azure Virtual Machine) tarkoittaa Azure-ympäristössä virtuaalista palvelinta. |
| VNET | VNET (engl. Azure Virtual Network) tarkoittaa Azure-ympäristössä virtuaalista verkkoa. |

# 1 JOHDANTO

Opinnäytetyön toimeksiantajana on Valtion tieto- ja viestintätekniikkakeskus Valtori. Valtorin tehtävänä on tuottaa toimialariippumattomat ICT-palvelut asiakkailleen, jotka muodostuvat valtionhallinnon virastoista ja laitoksista.

Työ on hyvinkin ajankohtainen, koska Valtorin asiakkailla on jo käytössään jonkin verran Microsoft Azure -pilvipalvelua, mutta ongelmaksi muodostuu keskitetyn tietoliikenneratkaisumallin puuttuminen. Nykytilassa yhteyden pilvipalvelun ja asiakkaan välillä on usein rakennettu ilman Valtorin tietoliikenteen kokonaisratkaisua. Asiakkaiden tietoliikenneverkoista on erilaisia ratkaisumalleja, miten tietoliikenneyhteydet on tällä hetkellä toteutettu, mikä aiheuttaa ongelmia yhteyksien kokonaishallinnan osalta. Yhteydet asiakkaan ja pilvipalvelujen välillä pitäisi toteuttaa Valtorin toimesta keskitettyä tietoliikenneratkaisua käyttäen ja näin toimien päästäisiin yhtenäiseen ja keskitettyyn ratkaisumalliin myös tietoliikenneyhteyksien osalta pilvipalvelun ja asiakkaan välillä.

Opinnäytetyön idea syntyi Valtorin asiakastarpeista pilvipalveluita kohtaan. Valtorin tehtävä olisi tuottaa kokonaisratkaisu, kuinka pilvipalveluita käytetään ja tuotteistaa lopulta valtion pilvipalvelut yhdeksi kapasiteettipalvelun tuotteeksi. Työssä ei käsitellä Valtorin käynnissä olevaa pilvipalveluiden tuotteistusprojektia, vaan työ on esikartoitus valtionhallinnon tietoliikenteen nykytilasta pilvipalveluiden osalta.

Opinnäytetyössä keskitytään Microsoft Azure -pilvipalvelutuotteeseen ja sen mahdollisuuksiin toimia yhtenä käyttöpalveluiden pilvipalveluympäristönä Valtorin asiakkaille. Työssä kuvataan tietoliikennettä ylätason loogisin topologiakuvin, joiden on tarkoitus auttaa hahmottamaan rajapinnat sekä yhteydet valtion tietoliikennepalveluiden ja Azure-pilvipalvelun välillä.

Työssä pyritään vastamaan kysymyksiin: Kuinka ja millä tavalla tai tekniikoilla voidaan valtionhallintoon ja sen tietoliikenneverkkoihin implementoida yhtenä Valtorin kapasiteettipalveluympäristönä pilvipalvelut? Mistä teknisistä asioista koostuu Microsoft Azure -palvelun käyttöönotto valtion yhteisessä tietoliikennepalvelussa hyödyntäen Azuren ExpressRoute -yhteyttä? Kuinka tehdään Valtorin asiakkaan liittäminen ExpressRoute-yhteyteen?

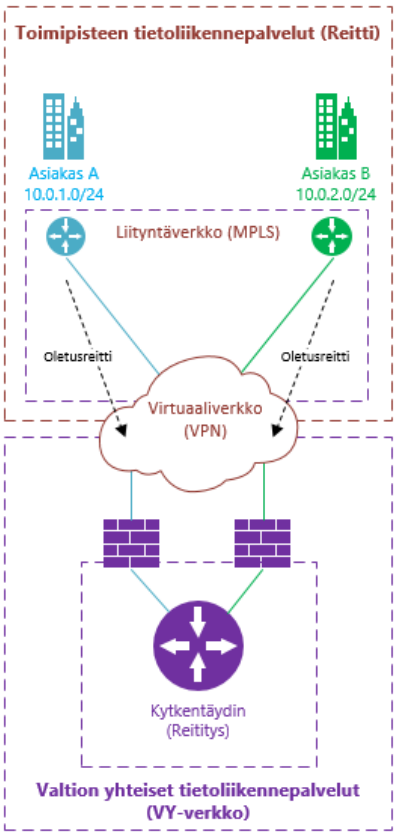
Toimin Valtorissa valtion yhteisissä tietoliikennepalveluissa (VY-verkossa) tietoliikennetehtävissä. Omat motiivit työn tekemiseen ja sen sisältöön liittyen ovat tietoliikenneasioissa.

# 2 VALTORIN TIETOLIIKENNEPALVELUT

Valtion tieto- ja viestintätekniikkakeskus Valtori on valtiovarainministeriön hallinnonalalla toimiva palvelukeskus ja valtion virasto. Valtorin tehtävänä on tuottaa valtionhallinnon organisaatioille toimialariippumattomat ict-palvelut. Toimialariippumattomilla ict-palveluilla tarkoitetaan palveluita, joiden tuottaminen tai järjestäminen ei vaadi merkittävää toimialakohtaista osaamista ja jotka perustuvat yleisesti käytettyihin laite- ja ohjelmistoratkaisuihin ja – teknologioihin. Palvelujen ja ratkaisujen asiakaskohtainen variointi ei tee niistä toimialakohtaisia (Valtori 2013).

Valtorin asiakkaisiin kuuluvat valtionhallinnon virastot ja laitokset, valtion liikelaitokset, muut julkisen hallinnon viranomaiset, julkisoikeudelliset laitokset, eduskunta, valtion talousarvion ulkopuoliset rahastot ja julkista hallinto- tai palvelutehtävää hoitavat yritykset tai yhteisöt.

Valtorin tietoliikennepalvelut pitää sisällään työn aiheeseen liittyen toimipisteen tietoliikennepalvelut (Reitti) sekä valtion yhteiset tietoliikennepalvelut (VY-verkko). Reitti ja VY-verkko yhdessä muodostavat valtion hallinnon organisaatioille yhteisen tietoliikenteen kokonaisratkaisun. Tietoliikenteen looginen kuvaus (Kuva 1) joka käsittää Valtorin tietoliikennepalvelut tarvittavin osin esitettynä.




Kuva 1. Valtorin tietoliikennepalvelut sisältäen toimipisteen tietoliikennepalvelut sekä valtion yhteiset tietoliikennepalvelut (Salmi 2017).

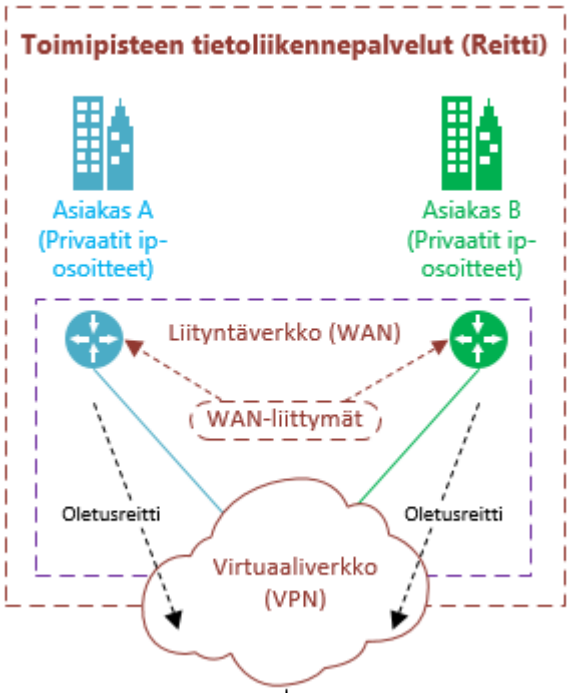
## 2.1 Toimipisteen tietoliikennepalvelut Reitti

Valtorin toimipisteen tietoliikennepalvelut Reitti sisältää kuvan 2 mukaisesti asiakkaiden lähiverkot LAN-verkot (Local Area Network) sekä lähiverkot yhdistävän operaattorin liityntäverkon WAN-verkon (Wide Area Network). Operaattorin WAN-verkosta on VPN-yhteydet (Virtual Private Network) valtion yhteisiin tietoliikennepalveluihin (VY-verkkoon).

Reitti-palvelu tarjoaa valtionhallinnon organisaatioille (Valtori 2016) seuraavat palvelut:

- asiakastarpeen mukaiset toimipisteen sisäiset langattomat ja/tai kiinteät tietoliikenneyhteydet
- toimipisteen liittymän Valtion yhteisiin tietoliikennepalveluihin, VY-verkkoon (Kuva 2: WAN-liittymät ja liityntäverkko sekä liityntäverkosta VPN-yhteys VY-verkkoon)
- lähi- ja liityntäverkkojen suunnittelun ja toteutuksen sekä ylläpidon ja hallinnan.

Toimipisteen tietoliikennepalvelut kuvataan kuvassa 2 olevalla tavalla. Siinä kuvataan vain oleelliset ja työlle relevantit kokonaisuudet tietoliikenneyhteyksineen.




Kuva 2. Toimipisteen tietoliikennepalvelut (Reitti) (Salmi 2017).

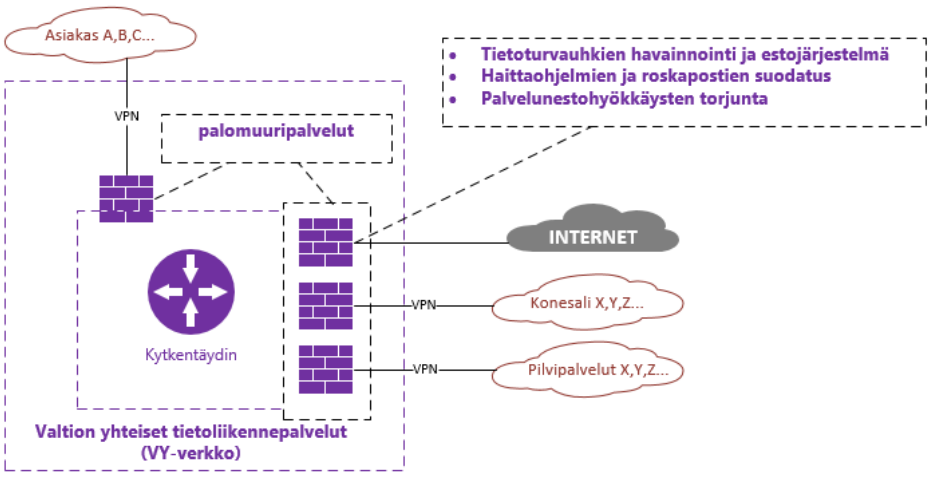
Kuvassa 2-, asiakas A ja asiakas B kuvaavat Valtorin asiakkaita. Asiakkailla on Reitti-palvelun mukaiset WAN-liittymät Valtorin liityntäverkkoon. WAN-liityntäverkossa asiakkaiden yhteydet luodaan omiin VPN-virtuaaliverkkoihinsa. Tietoliikennepakettien oletusreitti asiakkaan virtuaaliverkosta ulos ohjataan VY-verkossa sijaitsevaan kytkentäytimeen jatkoreititykseen.

## 2.2 Valtion yhteiset tietoliikennepalvelut (VY-verkko)

Valtion yhteiset tietoliikennepalvelut (VY-verkko) toimii valtionhallinnon organisaatioiden tietoliikenteen reitityspisteenä. VY-verkon idea on tarjota yhteinen keskitetty tietoliikenneratkaisu, jonka keskittävänä tietoliikenteen solmupisteenä toimii VY-verkon kytkentäydin. Kytkentäydin on maantieteellisesti hajautettu ja varmennettu ja tarjoaa nopean, luotettavan ja turvallisen tavan kytkeytyä valtion yhteisiin palveluihin, toisiin organisaatioihin sekä ulkoisiin palveluihin, kuten internetiin (Valtori 2016).

Valtion yhteisiin tietoliikennepalveluihin sisältyy myös olennaisena osana ja yhtenä kokonaisuutena tietoturvapalvelut, jotka sisältävät, palomuuripalvelut, tietoturvauhkien havainnointi ja estojärjestelmän, haittaohjelmien ja roskapostin suodatuksen sekä palvelunestohyökkäysten torjunnan (Valtori 2016).

Valtion yhteiset tietoliikennepalvelut kuvataan kuvan 3 mukaisesti, sisältäen esimerkiksi asiakaskohtaiset-, konesali- ja internetpalomuurit sekä työhön liittyen Azure-pilvipalveluympäristön palomuurin, mihin ExpressRoute-yhteys on päätetty.




Kuva 3. Valtion yhteiset tietoliikennepalvelut (VY-verkko) (Salmi 2017).

# 3 PILVIPALVELUT YLEISESTI

Antonio Regaladon kirjoittaman blogikirjoituksen mukaan sana pilvilaskenta (Cloud Computing) esiintyi kirjoitushetkellä vuonna 2011 internetissä 48 miljoonaa kertaa. Opinnäytetyön kirjoitushetkellä Google-hakukone tuottaa 83 miljoonaa osumaa. Pilvipalvelut sanana voi tarkoittaa useaa eri asiaa teknisesti, mutta tavallisesti pilvi mielletään vain internetin välityksellä tarjottavana kapasiteettina, josta esimerkiksi loppukäyttäjälle suunnattua sovellusta käytetään internetin yli tietämättä sen tarkemmin, missä itse sovellusta tuottavat palvelimet sijaitsevat. Usein pilvipalveluista tuotettuja sovelluksia käyttävälle asiakkaalle ei ole edes relevanttia tietoa se, mistä ja miten sovellusta tuotetaan, vaan suurin kiinnostuksen kohde onkin sovelluksen käytettävyys.

Käytännössä pilvipalvelu tarkoittaa kunkin pilvipalvelutoimittajan omistamaa suurta määrää fyysisiä konesaleja sijoitettuna maantieteellisesti eri paikkoihin, jotka on virtuaalisesti yhdistetty toisiinsa. Konesalit yhdistettynä toisiinsa luovat taas valtavan maailmanlaajuisen pilvipalvelukapasiteetin, johon voidaan kytkeytyä kaikkialta internetistä.

Esimerkiksi Microsoft Azure -pilvipalvelua käytettäessä- asiakkaalle voidaan antaa oma rajattu osuus pilvipalvelusta, josta asiakas maksaa käytön mukaan. Vaihtoehto on kustannusmielessä erittäin houkutteleva verrattuna asiakkaan omaan fyysiseen konesaliin, missä konesalitilasta, sisältäen käytännössä koko konesalitilan laitteistoineen, joista asiakas maksaa kuluja, riippumatta konesalin käyttöasteesta. Yleisesti pilvikapasiteetissa maksetaan vain käytön mukaan, asiakkaan ei tarvitse maksaa itse infrastruktuurista tai pilvialustasta jolla pilvikapasiteettia pyöritetään, koska sen osuuden hoitaa kokonaan pilvipalveluntoimittaja palveluna. Asiakas maksaa siis pelkästään vain palvelimista ja siitä kapasiteetista jota todellisuudessa käyttää (Kankare 2016).

Pilvipalvelun yksi tärkeimmistä valteista on sen käytettävyys ja itsepalvelu, jotka sisältävät palvelimien nopean käyttöönoton sekä resurssien tehokkaan hyödyntämisen. Pilvipalvelua käyttävä asiakas voi itsenäisesti hallita pilvialustan päällä toimivaa virtualisointikerrosta, missä esimerkiksi virtuaalipalvelimet ja niiden tietoliikenne toteutetaan. Asiakkaalla on käytettävissään juuri ne palvelut mitä hän tarvitsee ja haluaa (Kankare 2016).

Pilvipalvelussa kustannukset perustuvat siis aina käyttöön, toisin kuin perinteisessä konesalikapasiteetissa, jossa asiakas ostaa palvelinraudan konesaliin ja tästä hän maksaa täyden hinnan, oli se käytössä tai ei. Pilvipalvelussa maksetaan ainoastaan esimerkiksi palvelimesta, joka on käynnissä. Yhtä hyvin asiakas voi sammuttaa palvelimen ja näin olleen palvelimesta ei synny asiakkaalle kustannuksiakaan.

Hyvä esimerkki pilvipalvelun tehokkuudesta on sieltä julkaistava palvelu, jonka käyttö- tai ruuhkahuippu sijoittuu tiettyyn ajanjaksoon vuodesta. Tällaisen esimerkkipalvelun kapasiteetti pitäisi perinteisesti mitoittaa käyttöpiikin mukaan. Käyttöpiikki voi hyvinkin olla vain yksi kuukausi vuodesta, joten perinteisestä fyysisestä konesalista ja fyysisin palvelimin toteutetun

palvelun kapasiteetin pitää olla mitoitukseltaan tuon yhden käyttöpiikkikuukauden kokoinen. Asiakas maksaa siis yhden käyttöpiikkikuukauden mukaan mitoitetusta palvelusta kaksitoista kuukautta, joista yksitoista kuukautta palvelun kapasiteetti on ylimitoitettua.

Vastaava esimerkki toteutettuna pilvipalveluna, jossa esimerkkipalvelun kapasiteetin käyttöpiikkikuukautta varten pilvipalvelusta voidaan helposti allokoida lisää kapasiteettia auttamaan palvelun käyttöpiikinaikaista kuormaa. Muina kuukausina palvelua voidaan tuottaa kevyemmällä pilvikapasiteetilla ja maksetaan juuri siitä kapasiteetista mikä on käytössä, eikä turhasta. Esimerkkipalvelun kapasiteettia voidaan myös automatisoida niin, että kun ruuhkahuippu palveluun syntyy, pilvipalvelun automaation kautta nostetaan käyttöä vastaavaa lisäkapasiteettia hoitamaan lisääntynyt kuorma palvelussa (Kankare 2016).

## 3.1 Pilvipalvelun ja pilvilaskennan erot

Pilvipalvelun (Cloud Services) ja pilvilaskennan (Cloud Computing) välillä on vaikea tehdä selkeää rajanvetoa. Frank Gensin blogikirjoituksessa vuodelta 2008 eroa avataan näin:

*"Cloud Services = Consumer and Business products, services and solutions that are delivered and consumed in real-time over the Internet" (Gens 2008).*

*"Cloud Computing = an emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet (i.e., enabling cloud services)" (Gens 2008).*

Gensin mukaan pilvipalvelut tarkoittavat loppukäyttäjille tarjottavia valmiita palveluita, sovelluksia ja ratkaisuja, jotka ovat käytettävissä reaaliaikaisesti internetin yli. Pilvilaskenta hänen mukaan tarkoittaa yksinkertaistettuna ohjelmistokehittäjille, palvelun tarjoajille sekä yritysten it-osastoille tarkoitettua pilvipalvelualustaa, jossa on käytössä pilvilaskentapalveluntarjoajan loppuasiakkaalle tarkoitettu käyttöliittymä palvelussa tapahtuviin konfigurointeihin, esimerkiksi virtuaalipalvelimien käyttöönottoon pilvikapasiteetista.

Erosen blogissa pilvilaskentaa käsitellään samanarvoisena tai yhtäläisenä terminä-, kuin pilvipalvelua, jossa kapasiteetti- ja ohjelmistopalvelut, jotka palveluiden käyttäjät saavat käyttöönsä palveluna, ilman oman laitteiston tai ohjelmiston hankkimista. (Eronen 2016.)

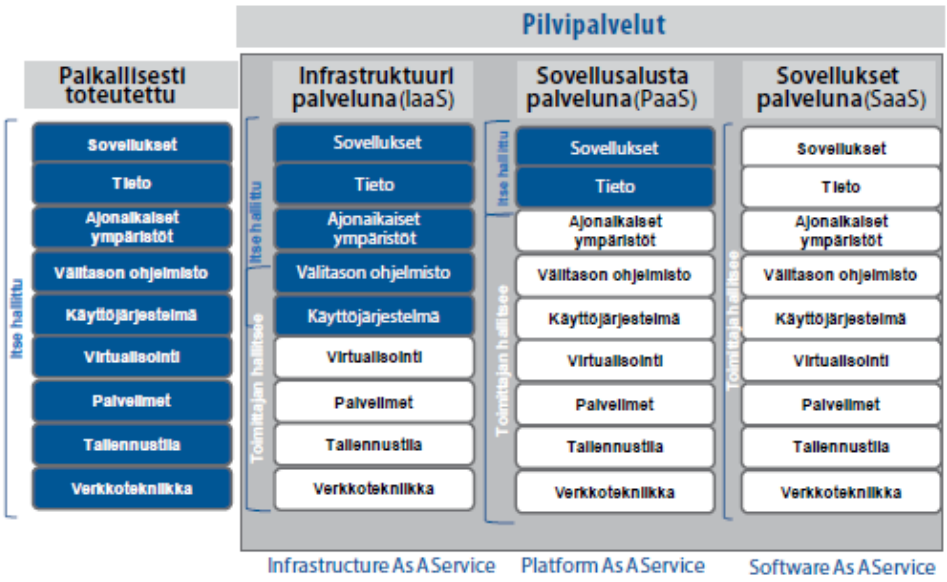
Yleisesti pilvilaskennan ja pilvipalvelun erot tutkimistani lähteistä löytyneiden artikkeleiden ja julkaisuiden mukaan näyttää olevan siinä, kuka niitä käyttää. Yhteenvetona pilvilaskentaa käyttävät ohjelmistokehittäjät, sovellusten tarjoajat ja yritysten IT-osastot. Pilvilaskennan avulla tehdään pilvipalveluita, joita käyttävät loppukäyttäjät, jotka käyttävät valmiita sovelluksia esimerkiksi Google Drive ja Microsoft One Drive.

Pilvipalvelun ja pilvilaskennan välillä on siis terminologisesti vaikea tehdä selkeää rajanvetoa. Pilvilaskenta terminä on ehkä vanhahtava, eikä sitä Suomen kielessä juurikaan käytetä, vaikka sitä kutsutaankin Englannin kielellä cloud computing, josta suora Suomennos olisi pilvilaskenta. Usein 2010 jälkeen tehdyissä Suomenkielissä julkaisuissa tai artikkeleissa puhutaankin vain pilvipalvelusta, eikä erikseen pilvipalvelusta ja pilvilaskennasta.

Tässä opinnäytetyössä pilvipalvelusta puhuttaessa, tarkoitetaan sillä IaaS-luokittelun (Infrastructure As A Service) mukaista omatoimista palvelumallia, missä palveluntarjoaja tarjoaa pilvipalveluun käytettävän alustainfrastruktuurin sisältäen itse pilvipalvelun virtualisointialustan, palvelimet ja niiden kiintolevyt sekä pilvipalvelualustan ytimen tietoliikenteen. Asiakkaalle tarjotaan selainpohjainen hallintaliittymä, minkä kautta asiakas pystyy itse hallinnoimaan virtuaalisoituja palvelimia, käyttöjärjestelmiä, kapasiteettia sekä palvelimien tietoliikenneyhteyksiä sisältäen itse palomuurauksen. (Konkka 2016.)

## 3.2 Pilvipalveluiden palvelumallit

Valtion konesali- ja kapasiteettipalvelustrategia ohjeessa (15/2014 Liite 1) puhutaan valtionhallinnon kapasiteettipalveluiden luokittelusta. Ohjeessa valtionhallinnon kapasiteettipalvelut jaetaan neljään yleiseen eri palvelumalliin (Kuva 4). Luokittelusta ensimmäinen vasemmalta alkaen on paikallisesti toteutettu kapasiteetti, missä paikallisesti toteutettu tarkoittaa omaa tai palveluntarjoajan fyysistä konesalia, jonka maantieteellinen sijainti on tiedossa. Seuraavat kolme IaaS-, PaaS-, ja SaaS -palvelumallia sopivat hyvin pilvipalveluiden tuottamisessa käytettäviin palvelumalleihin. Näitä palvelumalleja toki käytetään myös omissa fyysisissä konesaleissa, missä asiakas ostaa esimerkiksi palvelimet palveluntuottajalta käyttöjärjestelmätasoon asti asennettuna. Pilvipalvelumalleihin IaaS-, PaaS- ja SaaS -mallit sopivat erinomaisesti yleisinä malleina kapasiteettipalvelun tuottamiseen erinäisille asiakastarpeille.



Kuva 4. Kuva palvelumalleista valtion konesali- ja kapasiteettipalvelustrategia ohjeessa (Valtiovarainministeriö).

IaaS-, PaaS- ja SaaS-mallit sopivat siis peruslähtökohtina kapasiteettipalvelun tuottamiseen asiakkaan ja palveluntarjoajan välillä, mutta muutkin variaatiot IaaS-, PaaS- ja SaaS-mallien väliltä ovat mahdollisia.

SaaS-mallin mukaan pilvipalvelua kokonaispalveluna tarjoava toimittaja vastaa kaikesta muusta, paitsi itse käytöstä. Tässä kohtaa voisi puhua avaimet käteen -palvelusta, missä asiakkaalle tarjotaan pilvipalvelut täysin palveluna. SaaS-mallin palvelusta hyvä esimerkki on Microsoftin Office 365, joka tarjotaan asiakkaille SaaS-palveluna ja asiakas ei välttämättä tiedä sovelluksen tuottamiseen liittyvistä asioista, vaan ostaa sovelluksen käyttöoikeuden täysin palveluntarjoajan kokonaispalveluna tuotettuna.

PaaS-mallissa asiakkaan vastuulla on palvelumallin tieto- ja sovelluskerros. Mallissa asiakas ottaa enemmän vastuusta pilvipalvelussa toimimisesta, mutta silti palveluntarjoajalla jää vielä suurin osa palvelumallin kerroksista vastuulleen. Käytännön esimerkkinä-, asiakkaalla voisi olla pilvipalvelussa jokin sovellus, jota se itse hallinnoi ja pilvipalveluntarjoajan vastuulle jää sovellukselle tarvittavan alustan tuottaminen.

IaaS-malli on ehkä yleisin tapa ottaa pilvipalvelut käyttöön. Asiakas käytännössä hallitsee itse käyttöjärjestelmätasosta ylöspäin kaiken, aina sovellustasoon asti ja pilvipalveluntarjoaja hoitaa virtualisointikerroksesta alaspäin verkkotekniikkatasoon kaiken asiakkaalle palveluna. Käytännön esimerkkinä voisi olla-, palvelimien siirto paikallisesti toteutetusta konesalista pilvipalveluun, josta ne tarjotaan asiakkaalle jatkossa IaaS-mallin mukaisesti ja pilvipalveluntarjoaja ottaa vastuulleen virtualisointitasosta alaspäin kaiken aina verkkotekniikkatasoon asti.

## 3.3 Pilvipalveluiden jakelumallit

Pilvipalveluiden jakelumalleista käytetään yleisesti kolmea eri määritelmää, jotka ovat, yksityinen pilvi (Private Cloud), julkinen pilvi (Public Cloud), hybridipilvi (Hybrid Cloud).

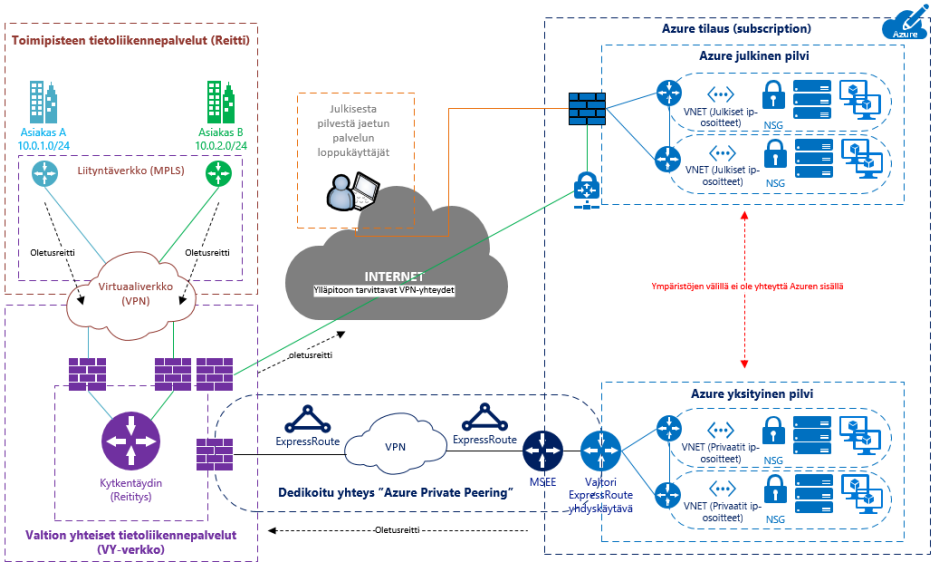
Tietoliikenteen näkökulmasta pilvipalvelut voidaan myös jakaa kolmeen eri määritelmään, kun tarkastellaan yhteyksiä eri pilvipalveluiden jakelumallien välillä.

Kuvissa 5, 6 ja 7 kuvataan pilvipalveluiden jakelumalleja ja niiden eroja Valtorin tietoliikenneyhteyksiä tarkastellen. Yhteyksistä kuvataan, asiakkaan verkko, joka on liitettynä kytkentäytimeen, internetin kautta tulevat loppukäyttäjät sekä jakelumallin mukaiset pilvipalvelun toteutusmallit ja niiden vaikutus esimerkiksi tietoliikennepakettien reititykseen

### 3.3.1 Julkinen pilvi

Julkinen pilvi (Public Cloud) tarkoittaa käytännössä internetin välityksellä tarjottavaa pilvipalvelua, jossa pilvipalvelun tarjoaja omistaa, hallinnoi ja

operoi kaikkia resursseja, jotka sijaitsevat palveluntarjoajan omissa konesaleissa. Yhteydet julkiseen pilveen on helppo rakentaa, koska yhteydet luodaan internetin yli, eikä tietoliikenneyhteyksien erityisjärjestelyille ole tarvetta. Julkinen pilvi ja sen kapasiteetti jaetaan virtuaalisesti kaikkien asiakkaiden kesken, ja näin ollen kaiken tiedon jota julkisessa pilvessä käsitellään olisi ainakin valtionhallinnon osalta syytä olla julkista.



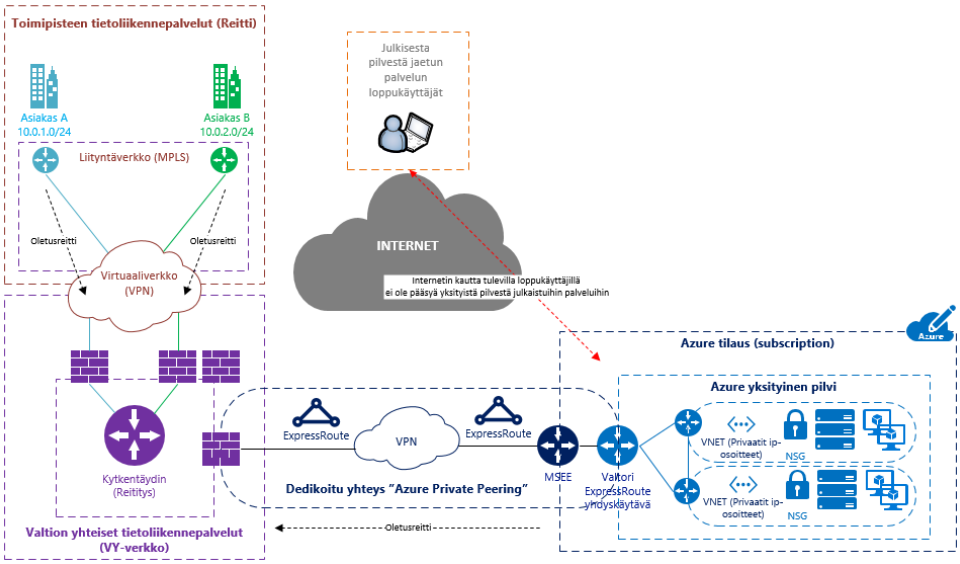

Kuva 5. Toteutus, missä asiakkaalla on Azuresta yksityinen sekä julkinen pilvi (Salmi 2017).

Julkisesta pilvestä julkaistaan palveluita internetin yli tuleville loppukäyttäjille. Ylläpitoyhteydet olisi hyvä luoda internetin yli esimerkiksi VPN-yhteyksiä käyttäen. Tässä kuvaamassani toteutusmallissa julkisen ja yksityisen pilven välillä ei sallita yhteyttä, vaan julkinen sekä yksityinen pilvi on puhtaasti jaettu kahdeksi eri kokonaisuudeksi.

### 3.3.2 Yksityinen pilvi

Yksityinen pilvi (Private Cloud) tarkoittaa asiakkaan omaa ympäristöä, joka ei ole jaettu muiden asiakkaiden kanssa. Yksityinen pilvi voi sijaita asiakkaan omassa konesalissa, missä asiakas toteuttaa itse virtualisointialustan-, tai ostaa sen palveluna pilvipalvelua konesaliin tarjoavalta palveluntuottajalta. Esimerkiksi Azuren tapauksessa-, yksityinen pilvi sijaitsee palveluntarjoajan konesalissa, josta asiakkaan käyttöön tarjotaan oma rajattu yksityinen ympäristö ja tietoliikenneyhteys. Tässä tapauksessa asiakas tietää maantieteellisesti maan jossa asiakkaan yksityinen pilvi sijaitsee, mutta asiakas ei tiedä konesalin fyysistä sijaintia. Asiakkaan omasta konesalista tarjottava virtualisoitu yksityinen pilvi on tietoturvallisesti huomattavasti parempi ratkaisu, koska yksityisen pilven maantieteellinen sijainti on tiedossa. Näin ollen yksityisessä pilvessä oleva tieto sijaitsee esimerkiksi Suomen rajojen sisäpuolella ja täyttää siten asiakkaan mahdollisen tietoturvavaateen tiedon maantieteellisestä sijainnista. Jos asiakkaalla ei ole esimerkiksi tietojen maantieteellisen sijainnin suhteen erityisvaatimuksia tietoturvan osalta, niin sitten myös palveluntuottajan omista konesaleista tuotettu yksityinen pilvi on vaihtoehto.

Tietoliikennemielessä kuva 6 mukaisesti yksityiseen pilveen on vain pääsy asiakkaan verkosta ja esimerkiksi rajapintaa suoraan internettiin ei ole olemassa. Jos taas yhteys internetiin suoraan yksityisestä pilvestä on olemassa, voidaan ympäristöä kutsua ennemminkin hybridipilveksi.



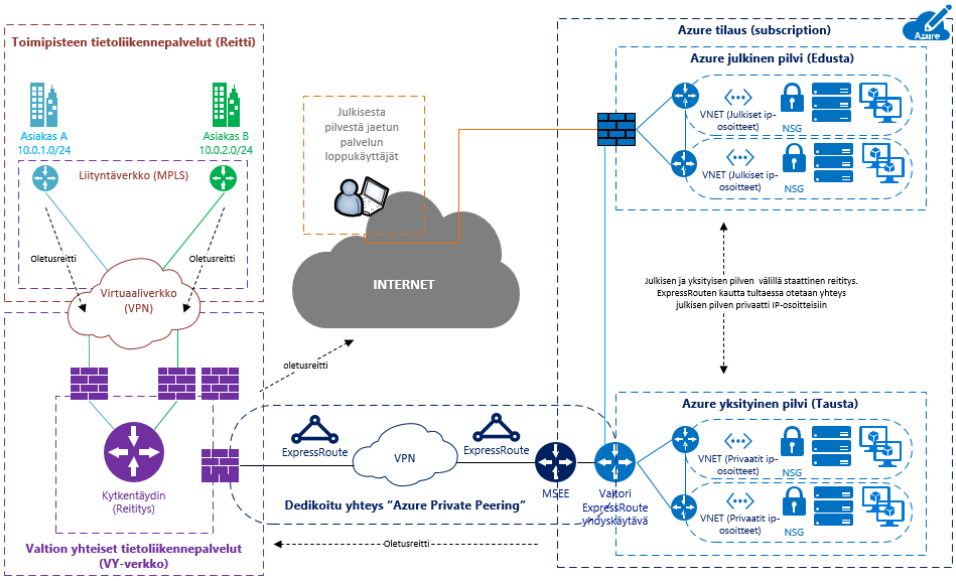

Kuva 6. Toteutus, missä asiakkaalla on käytössä vain Azuren yksityinen pilvi (Salmi 2017).

Kuvan 6 mukaan, asiakkaalla on käytössään Azuren yksityinen pilvi, jonka yhteys on rakennettu kytkentäytimen ja Valtorille dedikoidun Azure ExpressRoute -yhteyden välityksellä. Tässä ratkaisumallissa yksityisestä pilvestä ei voida tarjota palveluja internetin kautta tuleville loppukäyttäjille, vaan yksityinen pilvi on tarkoituksenmukaisesti saavutettavissa vain kytkentäytimen kautta privaateilla IP-osoitteilla, joilla kytkentäytimen asiakkaat voivat palveluita sieltä käyttää.

### 3.3.3 Hybridipilvi

Hybridipilvi (Hybrid Cloud) sisältää molempien, yksityisen ja julkisen pilven piirteitä. Kuvan 7 hybridimallissa-, julkisen pilven ympäristö tarjoaa palveluita internetin suuntaan loppuasiakkaille, esimerkiksi asiakkaan extranetin ja yksityisen pilven ympäristö tarjoaa asiakkaan verkon suuntaan tarkoitettuja palveluita, joita ei ole tarkoitettu internetin suuntaan jaettaviksi, esimerkiksi asiakkaan intranet.

Hybriditoteutuksissa erityisesti tietoturva tulee ottaa huomioon ja tarkempaan tarkasteluun, koska internetrajapinta on olemassa ja hybridipilven haavoittuvuus on syytä tiedostaa. Julkisen ja yksityisen pilven tietoliikenne olisi hyvä suojata palomuurein, jotta järjestelmien pääsynhallintaa ja valvontaa voidaan toteuttaa tietoliikennepakettien tasolla julkisen ja yksityisen pilven rajapinnassa.




Kuva 7. Toteutus, missä asiakkaalla on hybridimallin mukainen pilviympäristö (Salmi 2017).

Kuvassa 7 on kuvattu ratkaisumalli hybridiympäristöstä. Ero aikaisempiin toteutusmalleihin on julkisen ja yksityisen pilven välinen staattinen yhteys. Staattisella yhteydellä tarkoitetaan julkisen ja yksityisen pilven välillä olevaa tietoliikenneyhteyttä, jossa tietoliikennepakettien reititys määritellään erikseen yksityisen ja julkisen pilven reitittimen välillä. Näin saadaan palvelimien väliset tietoliikenneyhteydet toimimaan myös tietoliikenteen osalta. Ylläpitoyhteydet palvelimiin luodaan ExpressRoute-yhteyden kautta palvelimien privaatteja IP-osoitteita käyttäen. Internetin kautta tulevat loppukäyttäjät käyttävät palvelimien julkisia IP-osoitteita.

Pilvipalvelussa sijaitsevat virtuaaliverkot (VNET) voidaan segmentoida loogisiin kokonaisuuksiin, esimerkiksi edustaverkko (Front End) ja taustaverkko (Back End). Variaatioita verkkojen segmentointiin loogisiin kokonaisuuksiin löytyy monia erilaisia, mutta tässä ratkaisumallissa segmentit on jaettu edusta- ja taustaverkkoihin. Edustasegmentti voisi toimia verkkoalueena, johon luodaan sovelluksen tai palvelun edustapalvelimet, esimerkiksi web-palvelimet, kun taas taustasegmenttiin voitaisiin laittaa, esimerkiksi data- tai tietokantapalvelimet.

# 4 VALTORI MICROSOFT AZURE

Lähtötilanteessa Valtorilla oli jo oma Azure-tilaus, jota hyödyntäen pystyttiin määrittelemään Azuren yksityisen pilven ja Valtorin tietoliikenneverkon välille ExpressRoute-yhteys. Tässä luvussa kuvataan Azure-pilvipalvelua yleisesti ja tietoliikenneyhteyksien määrittelylle tarvittavin osin.

## 4.1 Azure-tilaukset

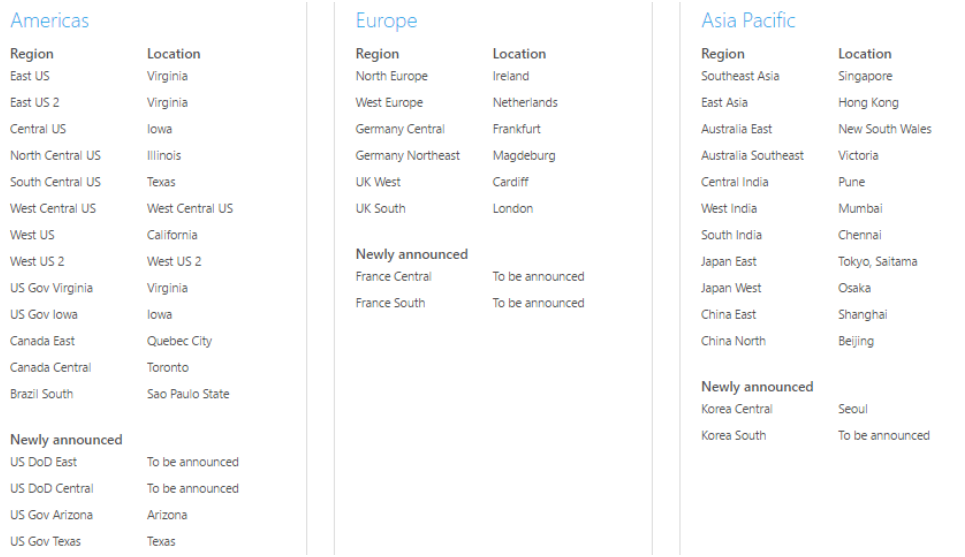
Azure-pilvipalvelussa tilauksilla (subscription) tarkoitetaan asiakasympäristöjä. Yksi tilaus on yksi asiakasympäristö joka sisältää Azure-pilvipalvelun käyttöliittymien kautta kaiken tarvittavan kontrollin pilvipalveluiden käyttämiseen IaaS-mallin mukaisesti. Valtorin tapauksessa-, Valtorilla on päätilaus, johon liitetään alitilauksia. Valtori hallinnoi Azuren päätilausta ja tarvittaessa luo asiakkailleen päätilauksen alle omia alitilauksia. Alitilauksella Valtorin asiakas saa käyttöönsä Azure-portaalin kaikkine palveluineen, mutta Valtorilla on silti hallussaan päätilaus Azure-palveluun. Näin toimien asiakas saa käyttöönsä IaaS-mallisesti pilvipalvelun ja voi siellä tehdä haluamiansa asioita.

Valtorilla on myös mahdollisuus tarjota asiakkailleen-, esimerkiksi PaaS-mallin mukaisesti palvelua, jossa asiakas ostaisi Valtorilta vain virtuaalipalvelimen ja Valtori hoitaisi kaiken muun virtuaalipalvelimen alustan osalta ja asiakkaan vastuulle jäisi virtuaalipalvelimen sovellustasosta huolehtiminen. Yhteenvetona, Valtorilla on hallussaan päätilaus Azure-palveluun ja asiakkaille luodaan alitilauksia päätilauksen alle, mikä helpottaa esimerkiksi laskutusta, kun voidaan alitilauksien perusteella laskutuskin osoittaa alitilauksesta koituneista kustannuksista asiakaskohtaisesti.

Tämäkin toiminta- ja hallintamalli tulee muovautumaan, kun Valtorin pilvipalveluiden tuotteistus etenee. Tilanne on siis tämä kirjoitushetkellä joulukuussa 2016.

## 4.2 Azuren alueet

Azure-palvelun arkkitehtuuri perustuu alueisiin (Region), joita on tällä hetkellä maailmanlaajuisesti yli 36 kappaletta. Alla olevassa kuvassa 8 on lista paikoista, mistä tuotetaan tällä hetkellä Azure-palvelua eri puolilta maailmaa.



Americas

| Region | Location |
|---|---|
| East US | Virginia |
| East US 2 | Virginia |
| Central US | Iowa |
| North Central US | Illinois |
| South Central US | Texas |
| West Central US | West Central US |
| West US | California |
| West US 2 | West US 2 |
| US Gov Virginia | Virginia |
| US Gov Iowa | Iowa |
| Canada East | Quebec City |
| Canada Central | Toronto |
| Brazil South | Sao Paulo State |
| **Newly announced** | |
| US DoD East | To be announced |
| US DoD Central | To be announced |
| US Gov Arizona | Arizona |
| US Gov Texas | Texas |

Europe

| Region | Location |
|---|---|
| North Europe | Ireland |
| West Europe | Netherlands |
| Germany Central | Frankfurt |
| Germany Northeast | Magdeburg |
| UK West | Cardiff |
| UK South | London |
| **Newly announced** | |
| France Central | To be announced |
| France South | To be announced |

Asia Pacific

| Region | Location |
|---|---|
| Southeast Asia | Singapore |
| East Asia | Hong Kong |
| Australia East | New South Wales |
| Australia Southeast | Victoria |
| Central India | Pune |
| West India | Mumbai |
| South India | Chennai |
| Japan East | Tokyo, Saitama |
| Japan West | Osaka |
| China East | Shanghai |
| China North | Beijing |
| **Newly announced** | |
| Korea Central | Seoul |
| Korea South | To be announced |

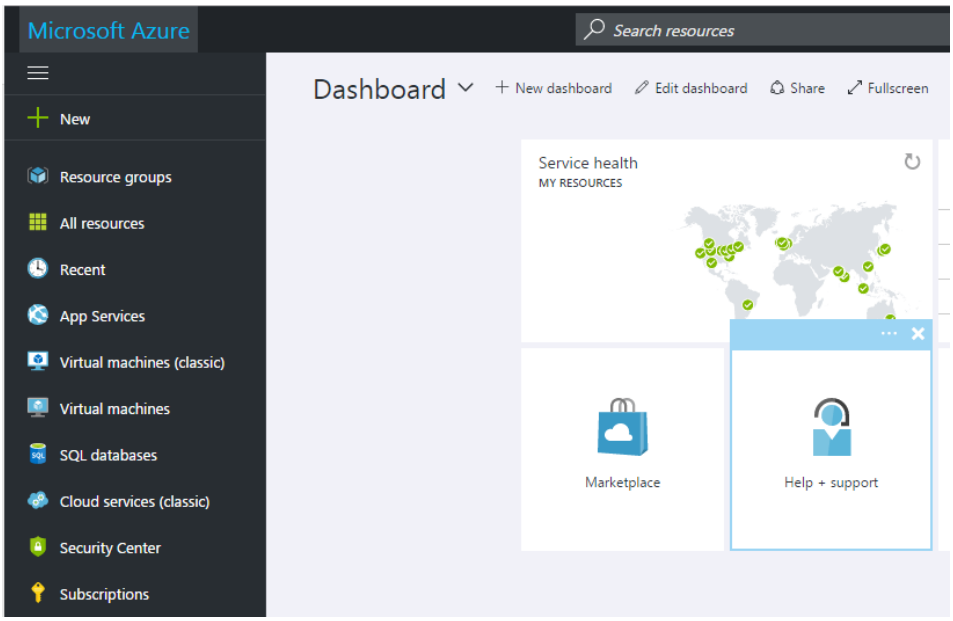
Kuva 8. Azure-alueet maantieteellisesti (Microsoft 2016).

Euroopassa olevat asiakkaat pääsääntöisesti hyödyntävät Pohjois-Euroopan (West Europe) konesaleja Hollannissa ja Länsi-Euroopan (West Europe) konesaleja Irlannista. Azure-pilvipalvelun tietoliikenneyhteyksien suorituskykyyn on erityisesti panostettu. Palvelinkeskusten sisäiset kuituverkkoyhteydet ovat jopa 30 000 gigabittiä sekunnissa ja todennäköisesti myös konesalien välissä yhteyksissä päästään lähes samoihin erittäin suorituskykyisiin nopeuksiin (Kankare 2016).

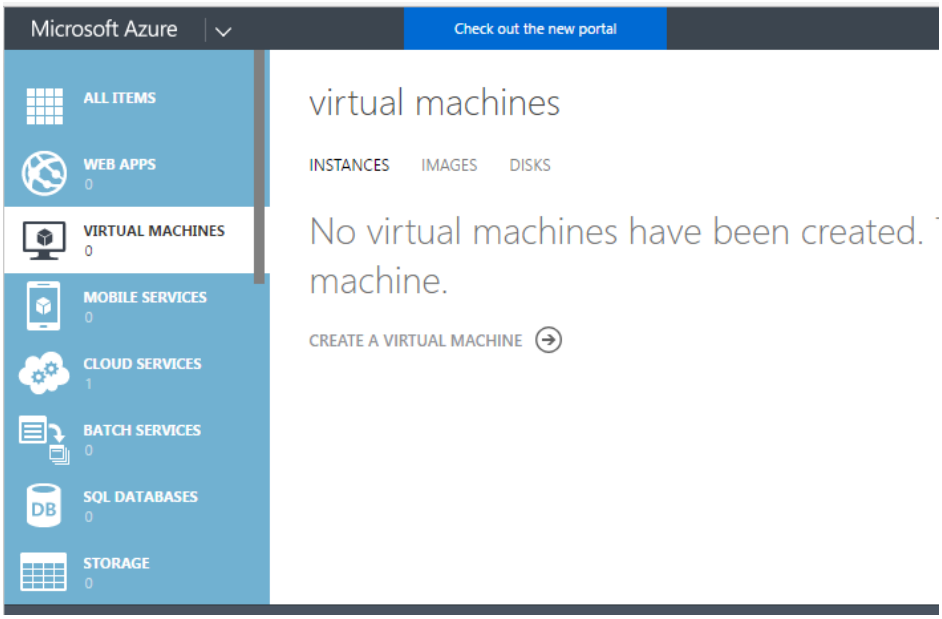
Palvelu voidaan pystyttää tiettyyn alueeseen, esimerkiksi Länsi-Euroopan alueeseen Hollantiin, mutta asiakas ei voi itse valita mihin konesaliin fyysisesti Länsi-Euroopan alueella palvelu sijoittuu. Asiakkaan palvelu perustetaan Microsoftin toimesta johonkin konesaliin, joka kuuluu Azure-palvelun Länsi-Euroopan alueen kapasiteettiin (Microsoft, 2016).

## 4.3 Azure-käyttöliittymät

Azure-pilvipalvelun hallinnointi ja konfiguraatiotyöt tehdään web-pohjaisilla käyttöliittymillä. PowerShell (PS) -komentokehotteen (Kuva 11) kautta konfiguraatiotöitä voidaan myös tehdä, mutta jos käyttäjä haluaa visuaalisen web-pohjaisen käyttöliittymän, niin vaihtoehtoja on kaksi, Azure Resource Manager (ARM) (Kuva 9) tai Azure Classic deployment (Classic) (Kuva 10). ARM-malli edustaa uusinta Azuren-käyttöliittymää, kun taas Classic-malli on ensimmäinen, mikä Azuren käyttöönotossa on lanseerattu. Käyttöliittymistä on tärkeä tiedostaa, että kirjoitushetkellä kaikkia Azure-palvelun konfiguraatiotöitä ei voi tehdä uudella ARM-käyttöliittymällä, vaan käyttäjä joutuu osittain turvautumaan vielä Classic-malliin. Hyvin pitkälle kuitenkin käyttäjä pystyy toimimaan uudella ARM-käyttöliittymällä ja lisäämällä siihen PowerShell-komennot, ja käytännössä kaikki Azuren-palvelut ovat käytössä ja konfiguroitavissa Azure-palvelussa (Microsoft 2017).




Kuva 9. Uusin Azure ARM-käyttöliittymä. (kuvakaappaus Valtorin Azure -palvelusta).



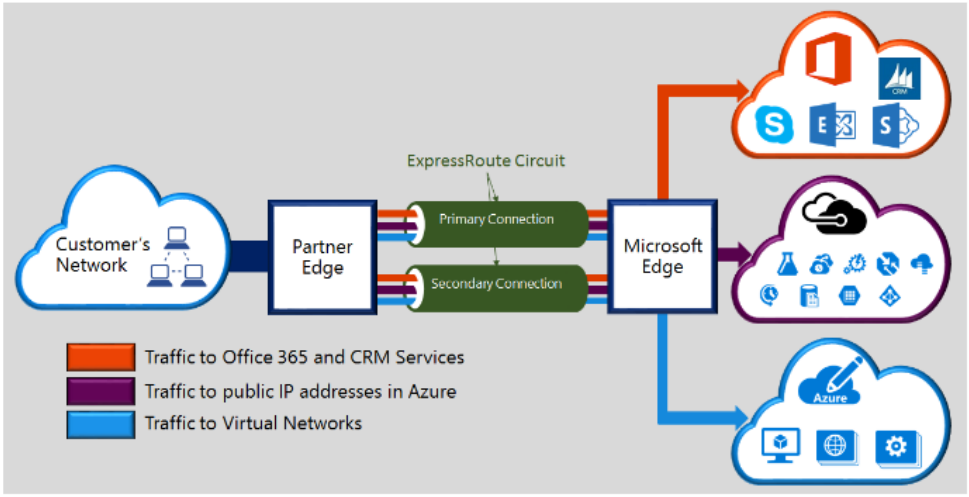

Kuva 10. Azure ARM-käyttöliittymää edeltänyt Azure Classic-käyttöliittymä (kuvakaappaus Valtorin Azure -palvelusta).


Kuva 11. Windows PowerShell ISE -komentotulkki on hyvä työkalu web-käyttöliittymien ohella (kuvakaappaus PowerShell-komentotulkista).

## 4.4 Microsoft Azure ExpressRoute

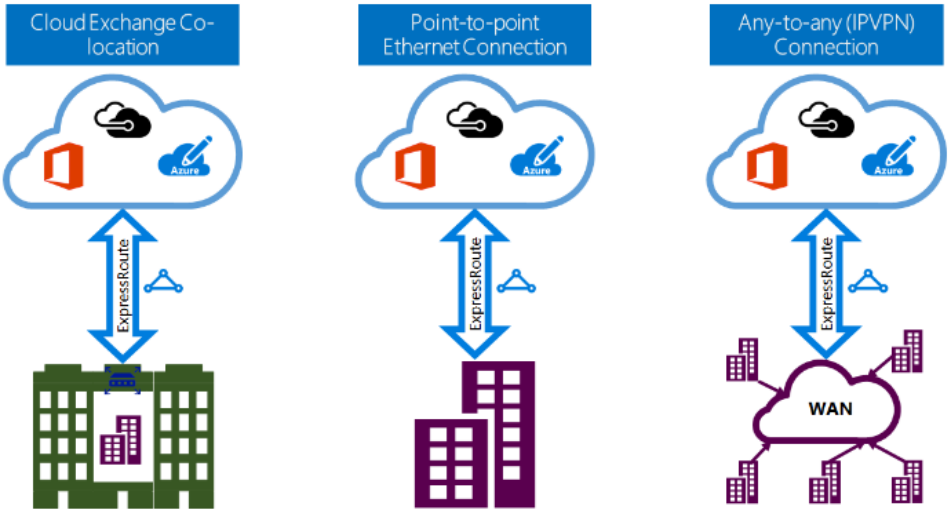
Microsoft Azure ExpressRoute tarjoaa yksityisen ja asiakkaalle dedikoidun tietoliikenneyhteyden Azure-palveluun. ExpressRoute luo mahdollisuuden laajentaa asiakkaan verkkoa (On-premises) Azureen asiakkaalle dedikoidulla OSI-mallin L3-verkkokerrostason tietoliikenneyhteydellä (Microsoft, 2017).

Kuvan 12 mukaisesti ExpressRoute-piiri (Circuit) konfiguroidaan Microsoftin kumppanioperaattorin verkon PE- (Partner Edge) ja MSEE (Microsoft Edge) -reitittimien välillä. Yhteys on aina kahdennettu ensisijaiseen ja toissijaiseen yhteyteen (Primary/Secondary Connection), jo pelkästään SLA-vaatimusten täyttymisen takia. Tärkeää myös huomioida, että ExpressRoute-yhteys ei kulje missään vaiheessa julkisen internetin yli ja näin ollen yhteys tarjoaa alhaisempaa latenssia, nopeampia yhteyksiä, luotettavuutta sekä enemmän tietoturvaa (Microsoft, 2017).




Kuva 12. Microsoft ExpressRoute tuotekuvaus (Microsoft 2016).

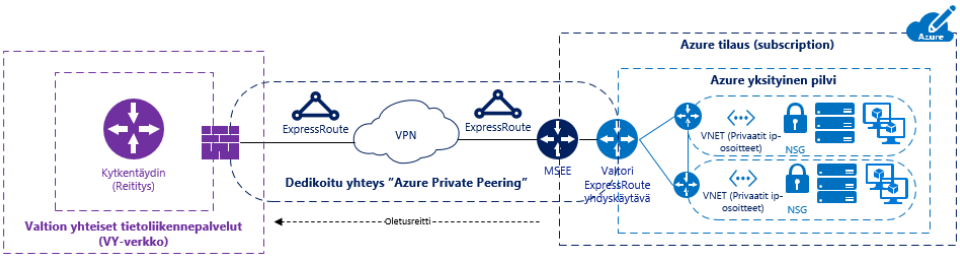
Kuvassa 13 ExpressRoute -yhteyksiä voidaan rakentaa asiakkaan verkon ja Azure -palvelun välille kolmella eri tavalla, joita ovat, Co-located at a cloud exchange, Point-to-point Ethernet connections-, ja Any-to-any (IPVPN) networks.




Kuva 13. ExpressRoute-tekniikan eri yhteysvaihtoehdot (Microsoft 2016).

Valtorin ExpressRoute -yhteyden määrittelyvaiheessa ja Valtorin verkkoarkkitehtuurin sekä kytkentäytimen Valtorille palveluna tarjoavan operaattorin arkkitehtuuriin sopi parhaiten Any-to-any (IPVPN) -yhteys, jota kutsutaan tyypillisesti MPLS-VPN-yhteydeksi.

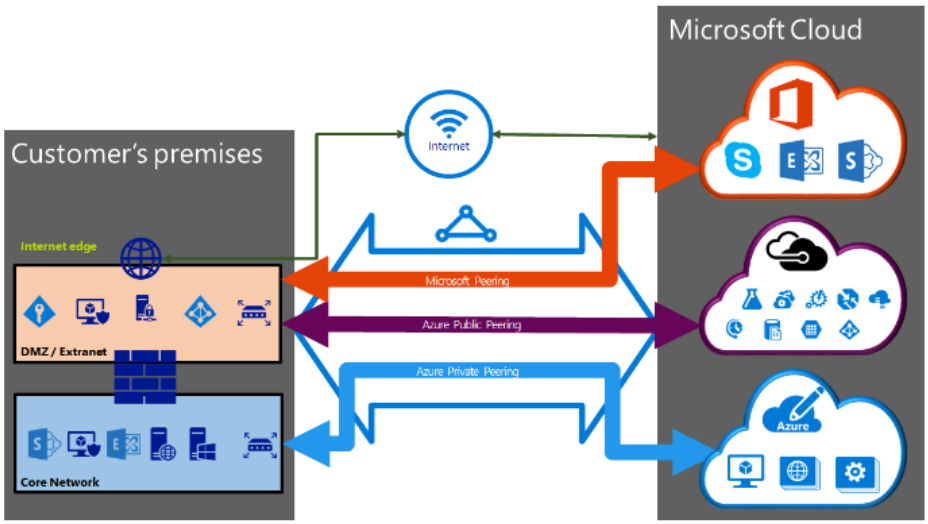
MPLS-VPN-yhteys Valtorin tapauksessa tarkoittaa kuvan 14 kaltaista toteutusta, missä kytkentäytimen operaattorilta tilattiin Valtorille dedikoitu MPLS-VPN. Yhteys vietiin Euroopan kumppanioperaattoripilven välityksellä tiettyyn maantieteelliseen Azure-alueeseen, jossa se päätetään Microsoft pilven reunalla olevaan MSEE-reunareitittimelle. Yhteyden konfiguroinnin jälkeen asiakas luo ensimmäisen virtuaaliverkkonsa sekä sille yhdyskäytävän. Luodun uuden virtuaaliverkon yhdyskäytävän seuraava hyppy (next hop) on MSEE-reititin, mikä reitittää taas liikenteen ExpressRoute-yhteydelle. Kuvasta 14 näkee hyvin, kuinka ExpressRoute -yhteys muodostaa asiakkaan sekä Azure -palvelun välille loogisen ja asiakkaalle dedikoidun yhteyden pilvipalveluun.




Kuva 14. Kytkentäytimen ja Azuren välinen ExpressRoute -yhteys (Salmi 2017).

### 4.4.1 ExpressRoute-peeraus

ExpressRoute-piirillä on eri käyttötarkoituksiin peerausdomaineja (Peering Domain), jotka ovat, Microsoft (Microsoft peering), Azure julkinen (Azure Public peering), Azure-yksityinen (Azure Private peering).



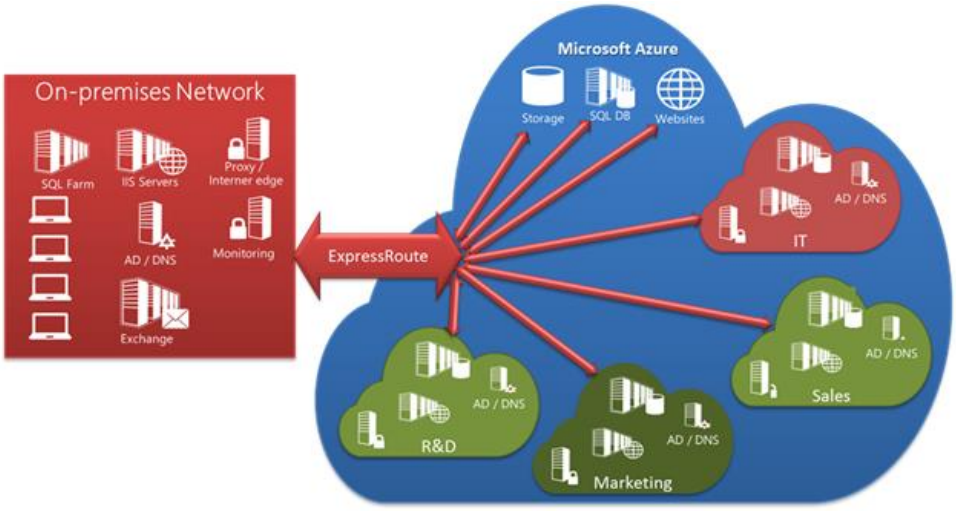

Kuva 15. ExpressRoute -yhteyden peeraus (Microsoft 2016).

Jokainen kuvan 15 peeraus konfiguroidaan Microsoftin toimesta omiksi tietoliikenneyhteyksiksi, joilla on omat reititinparit. Yksityinen peeraus (Azure Private Peering) luo yhteyden asiakasverkon sekä Azure-yksityisen pilven välille. Yksityisen peerauksen välityksellä asiakkaan on mahdollista laajentaa asiakasverkkoaan Azureen. Yhteyden yli voidaan käyttää ja reitittää asiakkaan valitsemia privaatteja IP-osoitteita, joten yhteydet yksityisessä pilvessä oleviin palvelimiin on helppoa toteuttaa, eikä esimerkiksi IP-osoitteiden takia tarvitse tehdä NAT-konfiguraatioita palomuureihin. Yksityinen pilvi toimii asiakasverkon loogisena jatkeena. (Microsoft, 2016.)

Julkinen peeraus (Azure Public Peering) on tarkoitettu julkisille palveluille, jotka toimivat julkisilla IP-osoitteilla julkisesta pilvestä. Julkisen peerauksen välityksellä on mahdollista tuoda Microsoftin julkisen pilven palvelut asiakasverkkoon. Julkisen pilven palveluita ovat esimerkiksi-, Azure-Storage ja SQL-tietokannat. Julkisen peerauksen yhteys voidaan päättää myös asiakasverkon DMZ-alueelle, jolloin Azuren julkisiin palveluihin voidaan reitittää tietoliikenne julkisen peerauksen sekä ExpressRoute-yhteyden kautta, kierrättämättä liikennettä internetin välityksellä. (Microsoft, 2016.)

### 4.4.2 ExpressRoute ja useat tilit

ExpressRoute-yhteys luodaan Azure-tilillä tehtävillä konfiguraatioilla. Tämä ei tarkoita sitä, että ExpressRoute-yhteys olisi vain yhteyttä luodessa käytetyn tilin käytettävissä, vaan ExpressRoute-yhteyteen voidaan liittää toisia Azure-tilejä.




Kuva 16. Useat eri tilit ja yksi ExpressRoute -yhteys (Microsoft 2014).

Kuvassa 16 on esitetty skenaario, jossa yksi ExpressRoute-yhteys on jaettu usean tilin kesken. Skenaariossa ExpressRoute-yhteyteen on liitetty organisaation eri osastot, joille on annettu omat tilaukset Azureen. Azure-tilaus edustaa aina yhtä Azure-pilviympäristöä, jonka esimerkiksi tietoliikenneyhteydet ovat omia kokonaisuuksiaan, tai tilikohtaisia. Tilien tietoliikenne voidaan yhdistää asiakasverkon (On-premises) suuntaan konfiguroimalla tilit yhden ExpressRoute-yhteyden piiriin. Useiden tilien käyttämistä puoltaa esimerkiksi laskutus, joka tässä skenaariossa tapahtuisi tilikohtaisesti osastojen omista pilviympäristöistä, mutta ExpressRoute-yhteyden kustannukset jaettaisiin kaikkien osastojen kesken.

# 5 KEHITTÄMISTYÖN TAVOITE JA TARKOITUS

Kehittämistyön keskeisenä tavoitteena oli tarkastella Microsoft Azure-pilvipalvelutuotteen eri ratkaisumalleja sekä tietoliikenneyhteyksiä erilaisissa skenaarioissa. Tietoliikenteen ylätason topologiakuvilla toimeksiantaja saa lisäymmärrystä pilvipalveluiden tietoliikenteen toiminnasta Valtorin pilvipalveluiden tuotteistusta varten. Pilvipalvelut ja asiakasverkot yhdistävät erilaiset tietoliikenteen skenaariokuvat auttavat toimeksiantajaa ymmärtämään paremmin, miten ja millä tekniikoilla pilvipalveluita voidaan käyttää ja kuinka pilvipalveluita voidaan liittää valtionhallinnon tietoliikenneverkkoihin.

Kysymykset joihin pyritään teoriaosuuden sekä käytännön osuuden avulla vastaamaan ovat seuraavat:

- Kuinka, millä tavalla ja tekniikoilla voidaan valtion yhteisiin tietoliikennepalveluihin yhdistää yhtenä Valtorin käyttöpalveluympäristönä pilvipalvelut Azure-pilvipalvelut?
- Mistä asioista koostuu Microsoft Azure-palvelun käyttöönotto valtion yhteisessä tietoliikennepalvelussa hyödyntäen Azuren ExpressRoute -yhteyttä?
- Kuinka onnistuu Valtorin asiakkaan (valtionhallinnon virasto) liittäminen ExpressRoute-yhteyteen?

Tietoperustassa käytiin läpi Azure-pilvipalvelun liittyviä tietoliikenneasioita, joita seuraavassa toteutusosiossa toteutetaan. Työn tuloksia voidaan hyödyntää Valtorilla sisäisesti tuomaan lisäkäsitystä Microsoft Azure -pilvipalveluun liittyvien tietoliikenneyhteyksien toteutustavoista sekä tulevan pilvipalvelukonseptin tuotteistustyössä. Tietoperustassa käytiin läpi pilvipalveluita yleisellä tasolla, perustuen tämän päivän tietämykseen. Tämän jälkeen luodaan yhteys tietoperustan sekä käytännön toteutuksen välille.

Yleistä vertailua eri pilvipalvelun toimittajien kesken ei tehty, vaan asiakastarpeiden ja halujen mukaan työn pilvipalvelun toimittajana toimii Microsoft Azure, koska Valtorin asiakaskunnassa on Azurea jo jonkin verran käytössä. Tietoliikenneyhteydet luodaan VY-verkon ja Azure-pilvipalvelun välille ExpressRoute-yhteyttä hyödyntäen. Toteutuksen suunnittelu lähtee nykytilanvälikartoituksesta, missä kuvataan, miten asiakkaiden yhteydet on nyt rakennettu ja miten tavoiteltava yhteystapa tuo keskitetyn ratkaisun VY-verkkoon. Tietoliikenneyhteydet Azure-pilvipalvelun ja VY-verkon välillä kuvataan ylätason tietoliikenteen topologiakuvauksilla, nykytila sekä tavoitetila huomioituna.

# 6 NYKYTILAN KARTOITUS JA ERI SKENAARIOT

Tässä luvussa on kuvattuna erilaisia tietoliikenteen yhteystapoja Azure-pilvipalvelun ja VY-verkon välillä sekä muutamalla sanalla niiden hyviä ja huonoja puolia. Tavoitteena on löytää ratkaisu, joka tukee parhaiten Valtorin palvelutuotantoa sekä asiakastarpeita. Asiakkaan tarpeissa pitää huomioida tietoliikennetopologian nykytila, se miten asiakas on tällä hetkellä liitetty valtion yhteisiin tietoliikennepalveluihin VY-verkkoon. Liitynnästä VY-verkkoon puhuttaessa-, tarkoitetaan tietoliikennetermein tietoliikennepakettien oletusreitin osoittamaa suuntaa, joka voi olla joko-, asiakkaalta oman internetliittymän kautta internetiin tai asiakkaalta Valtorin toimittaman liityntäverkon kautta VY-verkkoon ja siitä eteenpäin esimerkiksi internetiin.

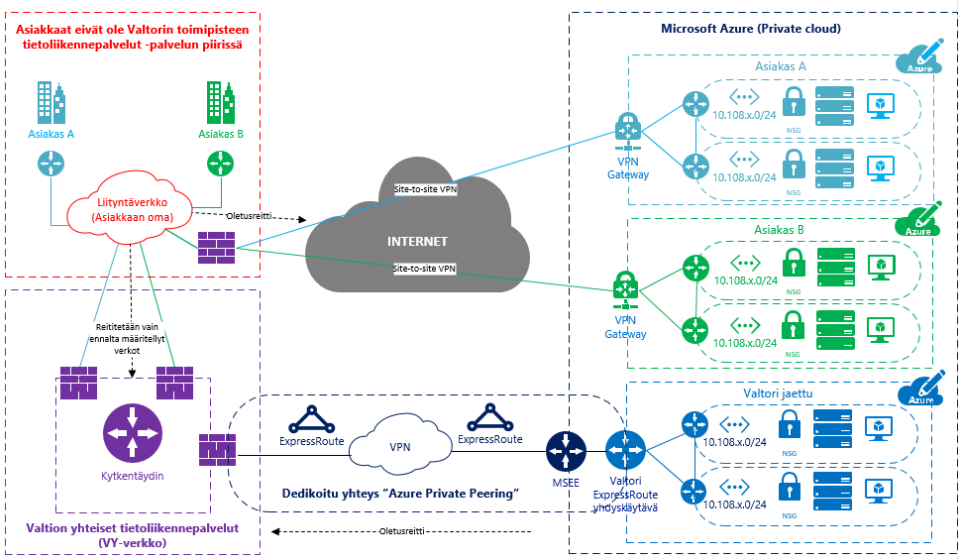
Valtorilla on käynnissä projekti, joka yhdenmukaistaa asiakkaiden tietoliikennetopologiaa. Projekti ja siirtymäkausi on pitkä ja saattaa kestää monia vuosia. Pilvipalvelut pitää kuitenkin saada käyttöön jo siirtymäkauden aikana, joten erilaiset tietoliikenteen nykytilan topologiakuvaukset tulevat tarpeeseen suunniteltaessa pilvipalveluiden tietoliikenteen tavoitearkkitehtuuria. Valtori on tuotteistanut toimipisteen tietoliikennepalvelut -palvelun, jonka suurin osa valtionhallinnon organisaatioista tulee ottamaan käyttöön lähivuosina. Valtion yhteiset tietoliikennepalvelut (VY-verkko) -palvelun piirissä ovat kaikki Valtorin asiakkaat tarvittavilta osilta, mutta toimipisteen tietoliikennepalvelut -palvelun mukanaan tuomaa oletusreittiä ei vielä kaikilla organisaatiolla ole lähi- tai liityntäverkkotopologioissaan.

Skenaariokuvissa 1-3 kuvataan ylätason tietoliikenteen topologiakuvauksilla yleisimmät asiakkaan tietoliikenneskenaariot. Kuvissa painotetaan myös tietoliikennepakettien oletusreitin suuntaa ja sen merkitystä.

## 6.1 Skenaario 1

Skenaariossa 1 (Kuva 17) asiakas ei ole Valtorin toimipisteen tietoliikennepalvelut -palvelun piirissä ja asiakkaalla on oma toimipisteet yhteen liittävä liityntäverkko, jossa asiakas ja liityntäverkon palveluntarjoaja hoitaa tietoliikennepakettien reitityksen. Oletusreitti osoittaa asiakkaan omasta internetliittymästä internetiin, joten ainoastaan asiakkaan liityntäverkosta erikseen reititetyt paketit kulkevat Valtorin kytkentäytimen kautta edelleen reititettäväksi haluttuun kohteeseen. Asiakkaan tietoliikennetopologian nykytilassa yhteydet Azure-palveluun on rakennettu asiakkaan oman internetliittymän kautta.

Tässä skenaariossa huonoa on se, että Valtori ei voi tuottaa keskitettyä tietoliikenneratkaisua asiakkaalle Azure-palveluun liittymiseen, vaan asiakkaan pitää itse konfiguroida esimerkiksi site-to-site VPN ja kytkeytyä oman internetmuurin kautta suoraan internetin yli Azureen.

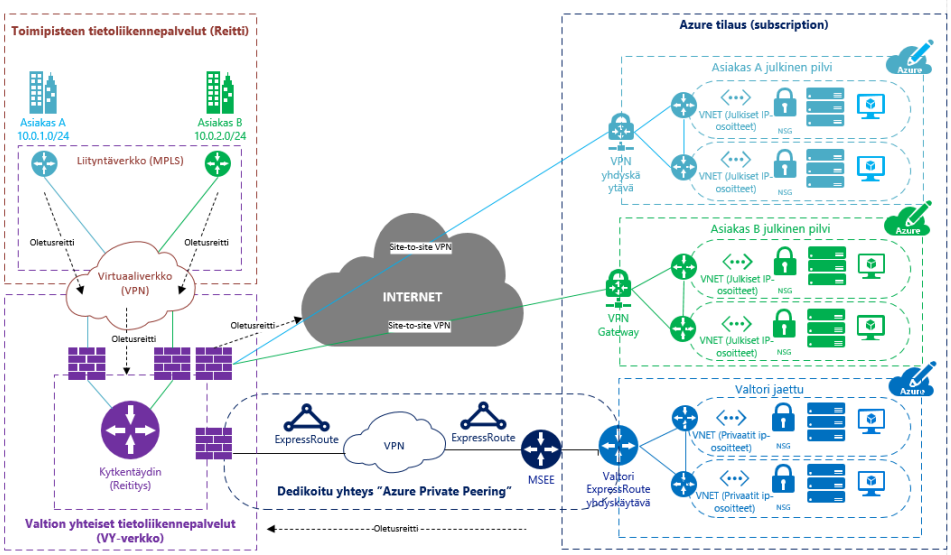



Kuva 17. Skenaario 1: yhteys asiakkaan oman internet liittymän kautta Azure-private ympäristöön (Salmi 2017).

Asiakkaan olisi mahdollista ottaa tässäkin skenaariossa Valtorin yksityinen pilvi käyttöön ohjaamalla staattisilla reitityksillä privaatti-IP-osoitteet kohti kytkentäydintä, joka edelleen reitittää paketit Valtorin yksityiseen pilveen ExpressRoute-yhteyden kautta. Asiakaskohtaiset räätälöinnit eivät kuitenkaan ole järkeviä, koska ne tuottavat ongelmia palvelutuotantoon esimerkiksi vianselvitystilanteissa.

## 6.2 Skenaario 2

Skenaariossa 2 (Kuva 18) asiakas on liitetty Valtorin toimipisteen tietoliikennepalvelut Reitti -palvelun piiriin ja yhteiseen keskitettyyn liityntäverkkoon. Oletusreitti osoittaa kytkentäytimeen ja kaikki tietoliikennepaketit ohjataan kytkentäytimeen edelleen reititettäväksi, mikä on myös tavoiteltu tietoliikenteen reititystopologia.

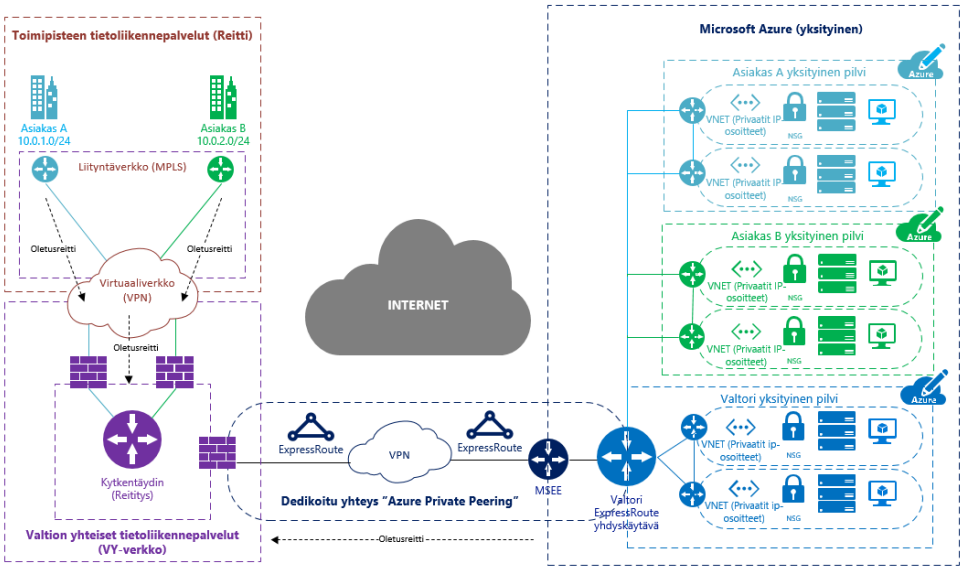


Kuva 18. Asiakkaan yhteys kytkentäytimen internet liittymän kautta Azure-yksityiseen ympäristöön (Salmi 2017).

Ongelma tässäkin skenaariossa, samoin kuin skenaariossa 1, on yhteystapa, miten tietoliikenne reititetään Azure-palveluun. Yhteydet luodaan kytkentäytimen internetliittymän kautta Azure-palveluun, eikä ExpressRouten-yhteyden kautta, mikä olisi tavoiteltava yhteystapa. Se miksi asiakkailla on yhteyksiä terminoitu VY-verkon internetmuurin kautta, johtuu yksinkertaisesti siitä, että ExpressRoute-yhteyttä ei ollut silloin, kun ensimmäiset asiakkaat ottivat Azure-palvelua omaan käyttöönsä.

## 6.3 Skenaario 3

Skenaario 3 (Kuva 19) on tavoitetopologia Azure-palveluun liittymiseen kytkentäytimestä. Asiakas on toimipisteen tietoliikennepalvelut -palvelun piirissä, joten oletusreitti osoittaa kytkentäytimeen. Kytkentäytimen ja Azure-palvelun välille on rakennettu ExpressRoute-yhteys, joten tietoliikennepaketit eivät missään reitin välissä kulje puhtaasti internetin yli, vaan Valtorille dedikoidun ExpressRoute-yhteyden välityksellä.




Kuva 19. Asiakkaan yhteys kytkentäytimen ExpressRoute-yhteyden kautta Azure-yksityiseen ympäristöön (tavoite) (Salmi 2017).

# 7 TIETOLIIKENNEYHTEYKSIEN RAKENTAMINEN

Luvussa 7 esitellään Valtorin ja VY-verkon välille rakennettavan ExpressRoute-liityntäyhteyden rakennusvaiheet-, sekä ylätason topologiakuvaukset testiskenaarioista. Luvussa käydään myös läpi yleisesti IP-osoitteiden merkitystä tietoliikenteen sekä pilvipalveluiden osalta.

## 7.1 IP-osoiteistus

Valtori hallinnoi ja allokoi Azure-palveluun käytettäviä privaatteja IP-osoitteita. Kun asiakas haluaa Azure-yksityisen ympäristön käyttöönsä, tulee Valtorin allokoida tarkoitukseen tarvittavat IP-osoitteet. Asiakas ei voi käyttää omia IP-osoitteitaan, kun liikennöidään Valtorille dedikoidun ExpressRoute-yhteyden välityksellä, koska yhteys ja sen tietoliikennereitit on konfiguroitu tietylle verkkosegmentille, josta IP-osoitteita jaetaan. Näin toimien tietoliikennepakettien reititykseen ei tarvitse tehdä muutoksia asiakkaiden käyttöönotoissa.

Työssä ei käsitellä IP-osoitteiden teoriaa syvällisemmin, mutta työn ymmärtämiseen kannalta IP-osoitteista on hyvä tietää privaatit IP-osoitteet ja niiden verkkoalueet. Taulukon 1 mukaisesti-, privaattien IP-osoitteiden verkkoalueet, joita ei reititetä esimerkiksi internetissä.

Taulukko 1. Esimerkki privaateista IP-osoitealueista (Salmi 2017).

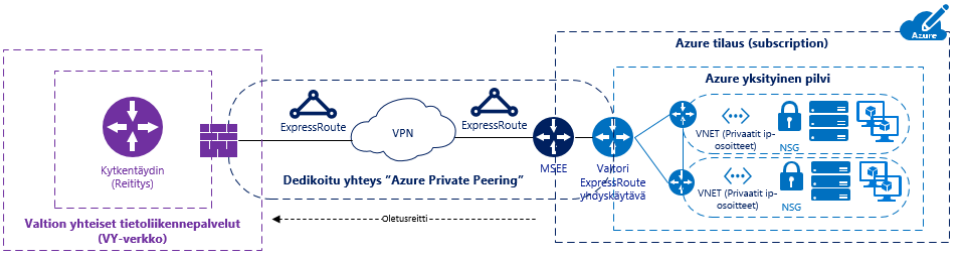
| IP-verkkoalue | IP-verkon maski | IP-verkon ensimmäinen IP-osoite | IP-verkon viimeinen IP-osoite | IP-osoitteiden kokonaismäärä |
|---|---|---|---|---|
| 10.0.0.0 | /8 | 10.0.0.1 | 10.255.255.254 | 16777214 |
| 172.16.0.0 | /12 | 172.16.0.1 | 172.31.255.254 | 1048574 |
| 192.168.0.0 | /16 | 192.168.0.1 | 192.168.255.254 | 65534 |

Kaikki taulukon 1 verkkoalueet ovat käytettävissä Azure-palvelussa privaatteina IPv4 IP -osoitteina. Pilvipalveluiden tietoliikennekonfiguraatioita suunniteltaessa-, esimerkiksi 10.0.0.0/8- tai 192.168.0.0/16 -verkkoalueiden IP-osoitteet käyvät hyvin määriteltäessä tietoliikenneyhteyksiä asiakasverkon ja Azure-palvelun välillä.

## 7.2 Microsoft Azure ExpressRoute ja Azure-yksityinen

Microsoft Azure ExpressRoute -yhteyden välityksellä on mahdollista kytkeytyä kaikkiin Azure-palvelun tarjoamiin jakelumalleihin ja niiden eri variaatioihin. Kuvan 20 mukaisesti ja tietoliikennettä ajatellen-, ensivaiheessa Azure-yksityisen ympäristön käyttöönotto valtion yhteisissä tietoliikennepalveluissa on loogisin vaihtoehto, koska virtuaaliverkoista oletusreitti osoittaa aina kytkentäytimen suuntaan. Toisin sanoen, kaikki tietoliikennepaketit ohjataan kytkentäytimeen tai toiseen virtuaaliverkkoon Azure-palvelun sisällä, mutta internetiin suoraan Azure-yksityisestä ympäristöstä ei ole pääsyä, eikä se edes reititysteknisesti olisi mahdollista, kun oletusreitti kytkentäytimeen on käytössä. Internettiin pääsee vain kytkentäytimen

kautta. Näin toimien Valtorilla on kokonaiskuva tietoliikenteestä, mitä kytkentäytimen ja Azure-palvelun välillä liikkuu tietoliikennepakettien tasolla.




Kuva 20. VY-verkon ja Azure-yksityisen pilven yhdistävä ExpressRoute-yhteys (Salmi 2017).

Liikennettä Azure-yksityisen ympäristön sekä VY-verkon kytkentäytimen välillä suodatetaan kytkentäytimessä sijaitsevalla palomuurilla, johon kyseinen ExpressRoute-yhteys on päätetty. Kytkentäytimen palomuurin säännöstö, kuvan 21 mukaisesti, oletusarvoisesti blokkaa (drop) kaiken liikenteen Azure-palvelusta kytkentäytimeen ja toisin päin.

| Source | Destination | VPN | Service | Action | Track |
|---|---|---|---|---|---|
| Any | Any | Any Traffic | Any | drop | Log |

Kuva 21. Kytkentäytimen palomuurin drop-sääntö (kuvakaappaus Valtorin Azure -palomuurin säännöstä).

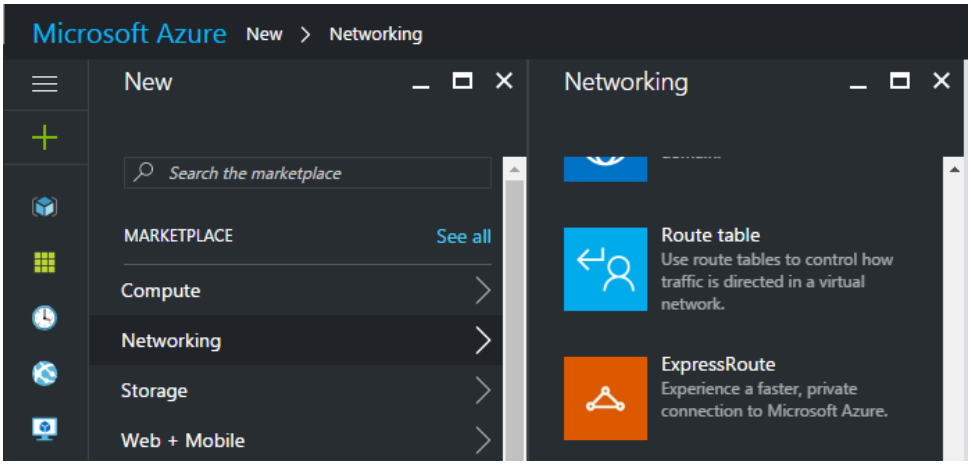
Vain ja ainoastaan erikseen sovittaessa ja asiakkaan Azure-yksityisen ympäristön käyttöönotossa määriteltävien palomuurisääntöjen asennus palomuurille on sallittua. Kaikilla sääntöriveillä on loki (log) päällä. Myös blokattu (drop) liikenne tulee näkyviin palomuuriin liikennelokiin, mistä voidaan tutkia, minkälaisia yhteydenottoyrityksiä kytkentäytimen suuntaan yritetään muodostaa tai toisin päin.

Seuraavissa luvuissa käydään läpi pääkohdilta yhteyksien luontiin tehdyt tarvittavat toimenpiteet. Tarkalle tasolle konfiguraatioiden esittelemisessä ei mennä tietoturvasyistä. Tarkat konfiguraatiotiedot annetaan Valtorin palvelutuotannon sisäiseen käyttöön.

## 7.3 ExpressRoute-yhteyden konfigurointi

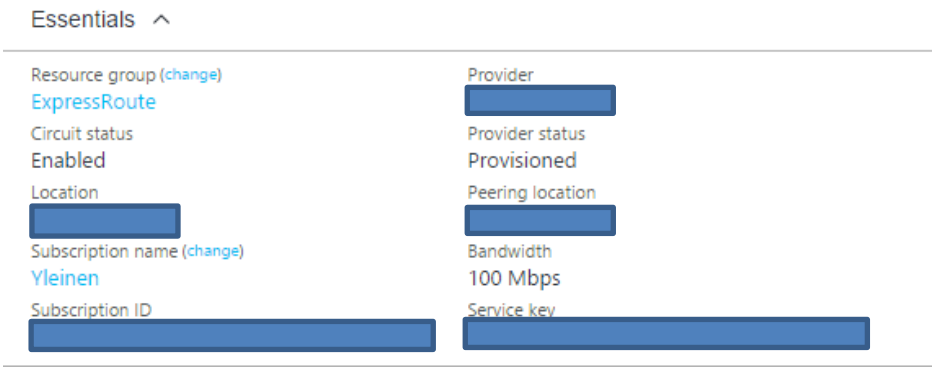
Valtorin tapauksessa ExpressRoute-yhteyden tilaaminen tapahtui kytkentäytimen Valtorille palveluna toimittavan operaattorin kautta. Operaattori teki tarvittavat konfiguraatiot yhteistyössä Euroopassa sijaitsevan kumppanioperaattorin kanssa. Valtorille dedikoitu ExpressRoute-yhteys konfiguroitiin päästä-päähän (peeraus) operaattorien verkkojen välityksellä. Yhteyden konfigurointivaiheessa valittiin ExpressRoute-yhteydelle tietoliikennepakettien reititykseen oletusreitti kytkentäytimen suuntaan, mikä tuki Azure-yksityisen ympäristön käyttötarvetta sekä tavoiteltua tietoliikenteen reititystopologiaa.

Kuvan 22 esimerkin mukaisesti ExpressRoute-yhteyden konfigurointityöt tehdään Azure-portaalissa. Konfigurointi aloitetaan navigoimalla Azure-portaalissa vasemmasta ylälaidasta New -> Networking ja valitaan Express-Route.




Kuva 22. Luodaan ExpressRoute -yhteys Azure -portaalissa (kuvakaappaus Valtorin Azure -palvelusta).

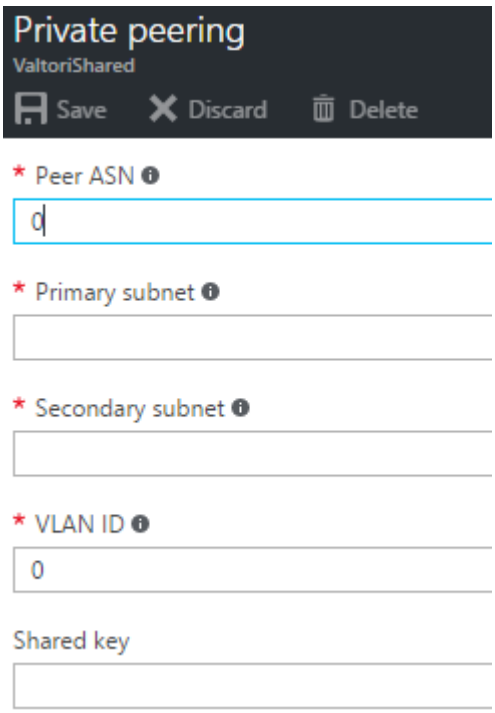
Täytetään avautuvaan lomakkeeseen suunnitellun konfiguraation mukaiset tiedot. Konfiguraation suunnittelulla tarkoitetaan operaattorien kanssa suunniteltuja ExpressRoute-yhteyteen liittyviä luottamuksellisia konfiguraatiotietoja. Yhteyden luonnin jälkeen ExpressRoute-yhteyden konfiguraatio pitäisi näyttää kuvan 23 mukaiselta. Tässä kohdassa on erittäin tärkeää huomioida yhteyden muodostamisen tila (provider status), että se on provisioned, mikä tarkoittaa, että yhteys on nyt konfiguroitu päästä-päähän onnistuneesti.




Kuva 23. Huomaa provider status -kenttä, että se on Provisioned (kuvakaappaus Valtorin Azure -palvelusta).

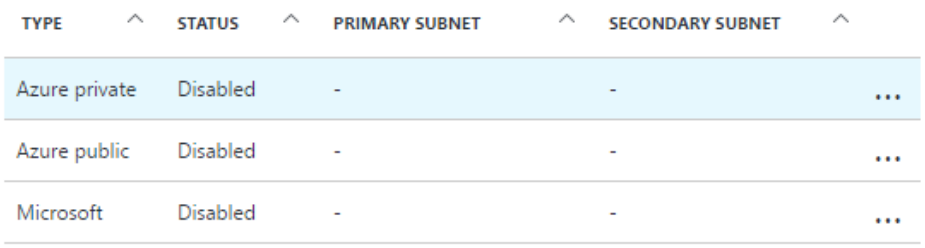
Microsoftin ExpressRoute-ohjeen mukaan, yhteyden peerauksia pitäisi myös konfiguroida, mutta huomasin, että tavoitellulla yhteystavalla niihin ei saanut koskea. Tein ensin peeraukset ohjeen mukaan, mutta en saanut ExpressRoute-yhteyttä kuitenkaan toimimaan. Yhteyden sain lopulta toimintakuntoon, kun poistin kaikki konfiguraatiotiedot peerauksista. Kuvan 24 lomakkeen mukaisia tietoja ei siis saa täyttää ja asiakkaan ei pidä konfi-

guroida yhteyden peerauksia, vaikka se mahdollista Azure-portaalissa onkin. Yhteyden asiakkaalle toimittaa palveluna ExpressRoute-yhteyttä toimittavat operaattorit.




Kuva 24. Yksityisen peerauksen konfiguraatiolomake (kuvakaappaus Valtorin Azure -palvelusta).

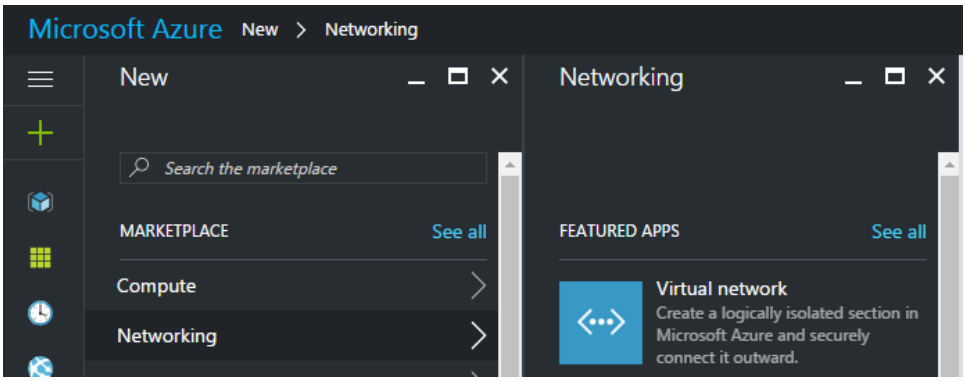
Tilanteen Valtorin tapauksessa pitää näyttää kuvan 25 mukaiselta, jossa tila (status) on disabled. Ainoastaan tällä peeraus-konfiguraatiolla yhteys toimii halutulla tavalla.




Kuva 25. Valtorin tapauksessa, kaikki peeraukset disabled-tilassa (kuvakaappaus Valtorin Azure -palvelusta).

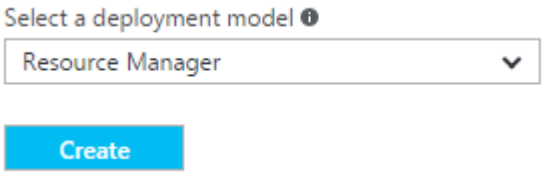
## 7.4 Virtuaaliverkon liittäminen ExpressRoute-yhteyteen

Luodaan ensimmäinen virtuaaliverkko (VNET), joka liitetään luotuun ExpressRoute-yhteyteen. Azure-portaalin vasemmasta yläkulmasta klikataan plusmerkkiä (New) ja valitaan Network, jonka alta Virtual Network (Kuva 26).




Kuva 26. Luodaan uusi virtuaaliverkko (VNET) (kuvakaappaus Valtorin Azure -palvelusta).

Virtuaaliverkko luodaan käyttäen Resource Manager -mallia, kun käytetään uusinta Azure-portaalin ARM-käyttöliittymää. Seuraavaksi klikataan Create (Kuva 27).

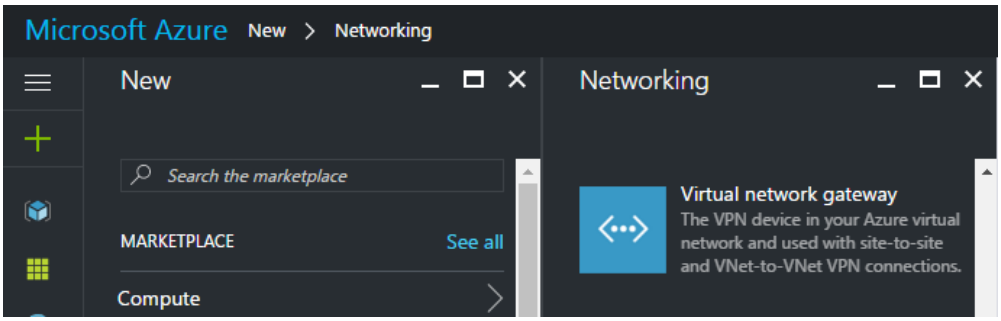



Kuva 27. Valitaan Resource Manager (ARM) (kuvakaappaus Valtorin Azure -palvelusta).

Konfiguraatio topologiakuvassa näyttää kuvan 28 mukaiselta. Siinä on luotu yksi virtuaaliverkko Valtorin tilauksen alle ja Valtorin yksityiseen ympäristöön Azure-palvelussa.

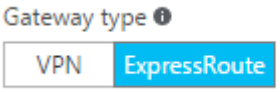

Kuva 28. Yksi virtuaaliverkko luotu Valtorin tilauksen alle (Salmi 2017).

Jotta virtuaaliverkosta pääsisi liikennöimään kytkentäytimen suuntaan, pitää uudelle virtuaaliverkolle luoda yhdyskäytävä (Gateway). Yhdyskäytävän luonti tapahtuu samalla tavalla kuin virtuaaliverkon luonti. Kuvan 29 mukaisesti-, Klikataan New -> Networking ja valitaan Virtual Network Gateway.




Kuva 29. Luodaan virtuaaliverkolle yhdyskäytävä (kuvakaappaus Valtorin Azure -palvelusta).

Kun konfiguroidaan Azure-palveluun virtuaaliverkkoa, joka tulee liitettäväksi ExpressRoute-yhteyteen, pitää konfiguraatiossa valita yhdyskäytävän tyypiksi kuvan 30 mukaisesti ExpressRoute.

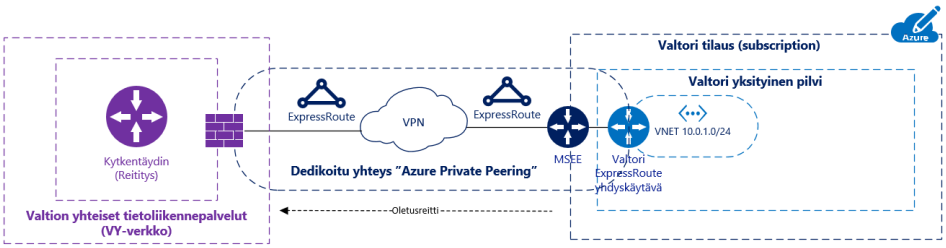



Kuva 30. Valitaan yhdyskäytävätyypiksi ExpressRoute (Salmi 2017).

Topologiakuvaan lisätään kuvan 31 mukaisesti virtuaaliverkolle yhdyskäytävä, jonka välityksellä virtuaaliverkosta voidaan liikennöidä toisiin virtuaaliverkkoihin tai oletusreittiä kytkentäytimen suuntaan.

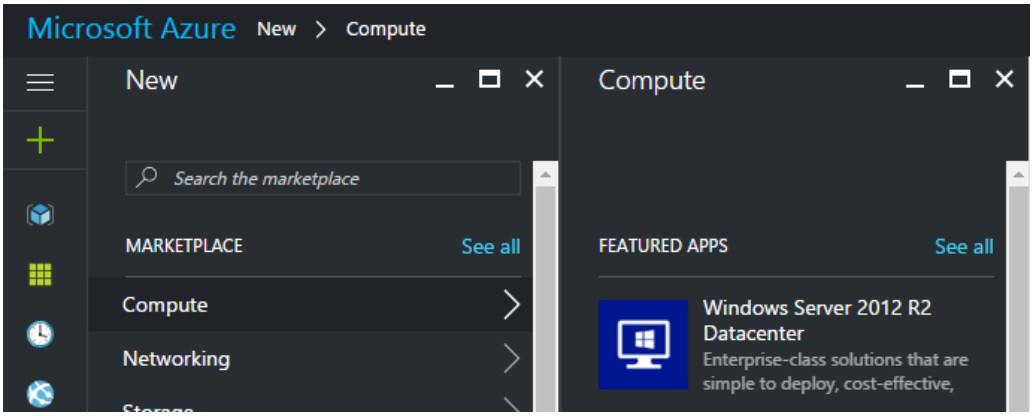

Kuva 31. Virtuaaliverkko liitettynä yhdyskäytävään (Salmi 2017).

Luodaan yhteys virtuaaliverkon yhdyskäytävän ja ExpressRoute-yhteyden välille, jonka jälkeen tilanne topologiakuvassa näyttää kuvan 32 mukaiselta:



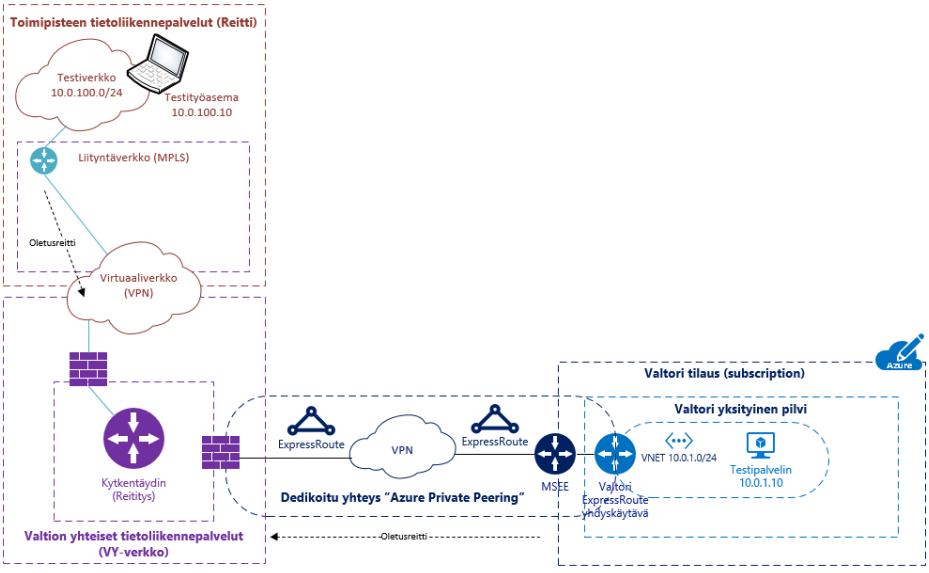

Kuva 32. Virtuaaliverkko liitettynä yhdyskäytävän välityksellä VY-verkon ja Azuren väliseen ExpressRoute-yhteyteen (Salmi 2017).

Virtuaaliverkon ja tarvittavan yhdyskäyvän luonnin jälkeen luodaan virtuaaliverkkoon palvelin, jota voidaan käyttää avuksi yhteystesteissä ExpressRoute-yhteyttä testattaessa kytkentäytimen ja Azuren välillä. Virtuaalipalvelimen luonti on suoraviivaista ja helppoa. Luodaan uusi virtuaalipalvelin virtuaaliverkkoon, joka on liitetty ExpressRoute-yhteyteen. Klikataan kuvan 33 mukaisesti New -> Compute ja valitaan virtuaalipalvelimeksi Windows server 2012 R2.




Kuva 33. Luodaan virtuaalipalvelin Azure -palveluun yhteystestejä varten (kuvakaappaus Valtorin Azure -palvelusta).

Annetaan virtuaalipalvelimelle tarvittavat tiedot, joista tärkeimpinä käyttäjätunnus ja salasana. Liitetään palvelin aiemmin luotuun virtuaaliverkkoon, joka tässä tapauksessa on verkko, joka on liitetty ExpressRoute-yhteyteen. Palvelimen luonnin jälkeen tilanne on topologiakuvassa kuvan 34 mukainen, jossa Valtorin testiverkossa on testityöasema ja Azure-palvelussa testipalvelin.




Kuva 34. Testiverkossa työasema sekä Azuressa testipalvelin yhteystestejä varten (Salmi 2017).

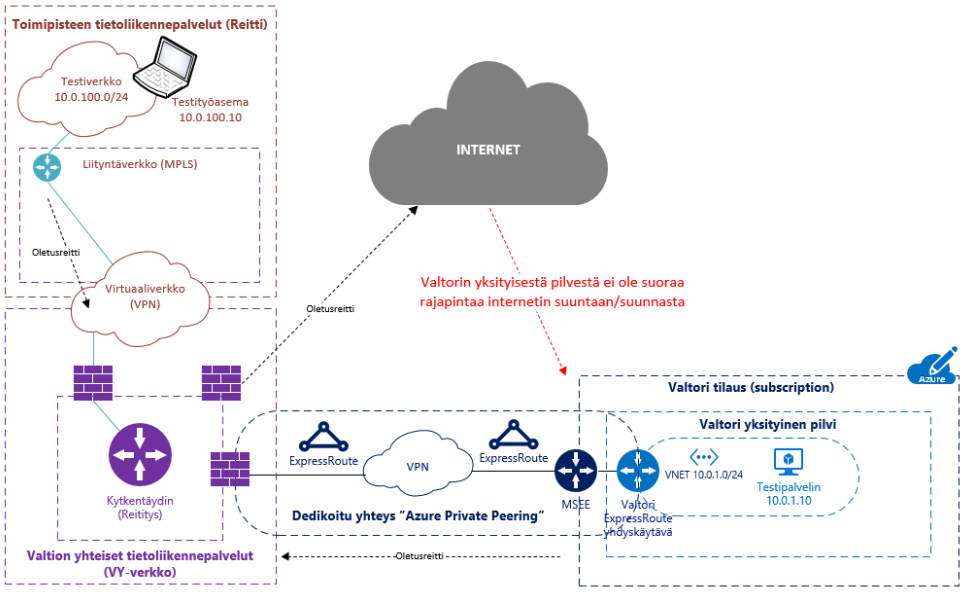
Ennen testejä pitää varmistaa, että testipalvelimien välissä olevien palomuurien säännöt ovat kunnossa, jotta voidaan testata esimerkiksi etätyöpöytäyhteyttä testipalvelimien välillä. Tässä tapauksessa palomuurisäännöt

ovat jo kunnossa, eli voidaan testata yhteyttä. Testasin vain etätyöpöytäyhteyden muodostamista Valtorin verkossa olevalta testityöasemalta Azure-palveluun luotoon testipalvelimeen ja yhteydet toimivat hienosti ja odotetulla tavalla. Yhteys Valtorin verkon ja Azure-yksityisen ympäristön välillä ExpressRoute-yhteyden välityksellä on muodostettu onnistuneesti, ja yksi työn tavoitteista on täytetty.

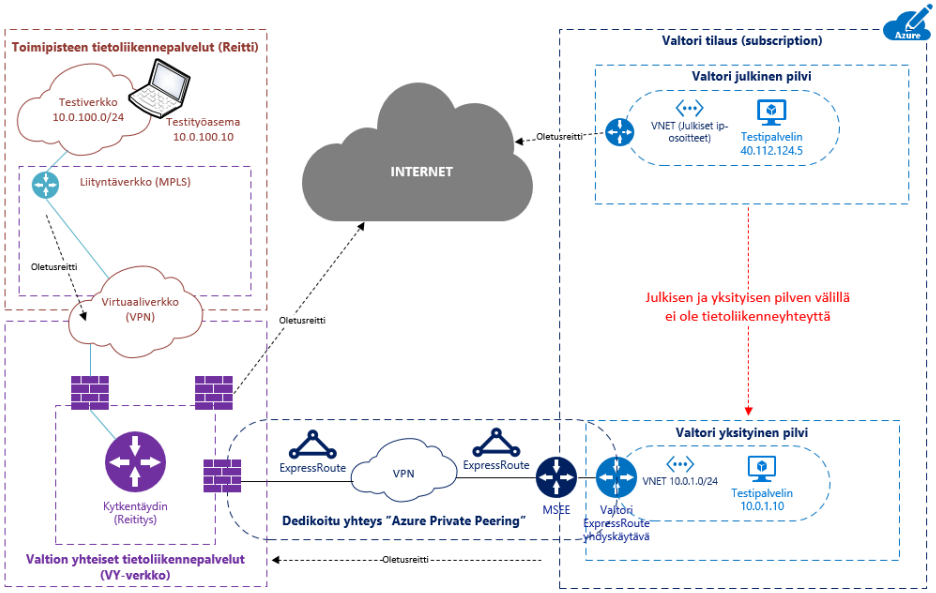
## 7.5 Valtorin ExpressRoute-yhteyden reititys

Valtorin ExpressRoute-yhteyteen liitetyt virtuaaliverkot saavat aina oletusreitin kytkentäytimen suuntaan ja kytkentäytimestä reititetään paketit aina ExpressRoute-yhteyden suuntaan, jos kohdeverkko on Azuressa Valtorin toimesta mainostettu. Tietoliikenteen oletusreitti on ainoastaan muutettavissa kytkentäytimen operaattorin toimesta oletusreitti poistamalla.

Oletusreitti kytkentäytimeen tarkoittaa käytännössä sitä, että Azure-yksityisen ympäristön virtuaaliverkosta, joka on liitetty ExpressRoute-yhteyteen, ei ole mitään mahdollisuutta liikennöidä muuhun suuntaan kuin kytkentäytimeen. Tämä on myös tietoturvasyistä pidettävä näin, koska missään vaiheessa tietoliikennepaketit eivät saa reitittyä internettiin hallitsemattomasti tai internetin suunnasta Valtorin Azure-yksityiseen ympäristöön. Jos ja kun halutaan Azure-yksityisestä ympäristöstä liikennöidä internetiin, tapahtuu se kytkentäytimen internetrajapinnan kautta (Kuva 35).




Kuva 35. Testiskenaarioon lisätty myös internetrajapinta (Salmi 2017).




Kuva 36. Testipalvelin julkisessa pilvessä (Salmi 2017).

Valtori voi halutessaan myös julkaista palveluita Azure-yksityisestä ympäristöstä internetiin ja skenaario näyttää silloin kuvan 36 mukaiselta. Internettiin tarjottavat palvelut luodaan palvelimille, joille annetaan julkinen IP-osoite, jolloin reititys on puhtaasti internetiin ja toisin päin. Tässä skenaariossa ja kuvan 36 mukaisesti-, julkinen ja yksityinen -ympäristö eivät keskustele keskenään Azure-palvelun sisällä, vaan siinä on selkeästi erotettu julkinen ja yksityinen ympäristö jo pelkästään reitityksillä omiin kokonaisuuksiinsa. Pitää huomioida, että palvelinten ylläpitoyhteydet myös reitietään internetin yli julkiseen ympäristöön.

Jos julkisesta ympäristöstä halutaan esimerkiksi yksityiseen ympäristöön, niin liikenne julkisen ympäristön palvelimelta lähtee oletusreittiä internettiin ja internetistä se pitää ottaa vastaan kytkentäytimen internetmuurilla. Yksityisessä ympäristössä on käytössä privaatit IP-osoitteet, joten yhteysesimerkin toteutukseen tarvitaan vielä NAT-osoitteen konfigurointia ja palomuuriavauksia. Ei siis ole kovin mielekästä rakentaa julkisen ja yksityisen ympäristön välillä integraatiota, niin kauan, kuin oletusreitti on käytössä yksityisestä ympäristöstä kytkentäytimen suuntaan. Tällä tietoliikennetopologialla kuitenkin päästään alkuun ja jatkokehitykseen jäävät sitten hybridiratkaisut, tai muut mahdolliset toteutus skenaariot.

# 8 JOHTOPÄÄTÖKSET JA POHDINTA

Työssä pohditut ja rakennetut valtionhallinnon tietoliikenneverkkoja koskevat yhteydet pilvipalveluihin ovat ensimmäisiä laatuaan toteutettuna ExpressRoute-tekniikalla. Oli ensiarvoisen tärkeää saada dokumentoitua ylätason tietoliikenteen topologiakuvilla, miten Valtorin asiakkaiden tietoliikenteen nyky- ja tavoitetila vaikuttaa Valtorissa tuotteistettavaan pilvipalvelukonseptiin.

Opinnäytetyö toimii esiselvityksenä tietoliikenteen nykytilasta, jossa samalla pohditaan myös tavoitetilaa ja sen mahdollisia ratkaisumalleja sekä ongelmatilanteita. Työ toimii myös Valtorille dokumenttina siitä, mitä tehtiin ja kuinka ExpressRoute-yhteys toteutettiin.

Haasteeksi muodostui työn julkisuus. Tietoliikennettä käsiteltäessä ja varsinkin valtionhallinnon tietoliikenneverkkoja-, paljon asioita kuuluu luottamuksellisen tai jopa salassa pidettävän tiedon piiriin, joten kuvaukset ja selvitykset ovat ylätasolta kuvattuna. Tarkemmat tekniset dokumentit, kuvaukset ja tiedot toimitetaan Valtorin palvelutuotannon sisäiseen käyttöön.

Valtionhallinnon pilvipalvelut ovat tätä lukua kirjoittaessa tuotteistusvaiheessa. Opinnäytetyöstä saadaan apua Valtorin pilvipalvelut-tuotteen tietoliikenneosuuden määrittelytehtäviin. Työ jää esiselvitykseksi Valtorin tietoliikenne vs. valtionhallinnon pilvipalvelut-tuotteen tuotteistusprojektiin, jossa siitä on hyötyä etsittäessä lopullista ratkaisumallia toimivien pilvipalveluiden tuottamiseen tietoliikennetasolla. Työ auttaa myös hahmottamaan kokonaiskuvaa tietoliikenteestä. Työssä on skenaariokuvauksien kautta esitetty, miten tietoliikenne käyttäytyy esimerkkitilanteissa, ja mitä ongelmia joistakin tietyistä tietoliikenteen kannalta ongelmallisista tilanteista voi syntyä.

Tärkeimpinä asioina pilvipalveluiden käyttöönotossa on riittävä tai tarpeeksi kattava suunnittelu, dokumentointi sekä resurssit. Työtä on paljon ja eri pilvipalvelutuotteiden kirjo on melko laaja. Jokaisella pilvipalvelutuotteella on omat erityispiirteensä, joiden hahmottamiseen sekä sisäistämiseen täytyy varata aikaa asiakkaan palvelutuotannon pilvipalveluiden tuottamiseen käytettäville resursseille. Resurssien on syytä myös olla riittävät, jotta tuotanto pyörii joustavasti sekä tehokkaasti. Näin toimien saadaan pilvipalveluiden ketteryys, joustavuus ja tehokkuus mahdollisimman hyvin siirrettyä suoraan asiakkaan käyttöön toimivana kokonaispalveluna, josta on oikeasti lisäarvoa asiakkaan omassa palvelutuotannossa.

# LÄHTEET


Eronen, H. (2016). IaaS, PaaS, SaaS? Mikä pilvipalvelu sopii yrityksellesi Blogijulkaisu 15.3.2016. Haettu 12.12.2016 osoitteesta http://blog.planeetta.net/iaas-paas-saas

Gens, F. (2008). Defining "Cloud Services" and "Cloud Computing" Blogijulkaisu 23.9.2008. Haettu 12.12.2016 osoitteesta http://blogs.idc.com/ie/?p=190

Kankare, V. (2016). Hallitusti pilveen: Osa 1 Tutustu - Elisa Webinaari. Youtube-Webinaari 5.12.2016. Haettu 12.12.2016 osoitteesta https://www.youtube.com/watch?v=KQKA4kJQG8k

Konkka, P. (2016). Pilvipalvelujen perusteet Blogijulkaisu 21.6.2016. Haettu 12.12.2016 osoitteesta http://www.sensoan.com/fi/2016/06/21/pilvipalvelujen_perusteet/

Microsoft (2015). Introducing Microsoft Azure.
Haettu 12.12.2016 osoitteesta https://docs.microsoft.com/en-us/azure/fundamentals-introduction-to-azure

Microsoft (2017). Azure Resource Manager vs. classic deployment: Understand deployment models and the state of your resources.
Haettu 20.1.2017 osoitteesta https://docs.microsoft.com/fi-fi/azure/azure-resource-manager/resource-manager-deployment-model

Microsoft (2017). ExpressRoute technical overview.
Haettu 20.1.2017 osoitteesta https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction

Microsoft (2016). ExpressRoute circuits and routing domains.
Haettu 20.1.2017 osoitteesta https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peering

Microsoft (2014). Enabling Multiple Subscriptions to Share an ExpressRoute Circuit. Haettu 20.1.2017 osoitteesta https://azure.microsoft.com/en-us/blog/enable-multiple-subscription-expressroute/

Regaldo, A. (2011). Who Coined 'Cloud Computing'? Blogijulkaisu 31.10.2011. Haettu 15.12.2016 osoitteesta
https://www.technologyreview.com/s/425970/who-coined-cloud-computing/

Valtori (2013). Tietoa Valtion tieto- ja viestintätekniikkakeskus Valtorista.
Haettu 14.12.2016 osoitteesta http://www.valtori.fi/fi-FI/Tietoa_Valtorista

Valtori (2016). Toimipisteen tietoliikennepalvelu Reitti.
Haettu 2.2.2017 osoitteesta: http://www.valtori.fi/fi-Fi/Palvelut/Tyoskentely-ymparistön_palvelut/Tietoliikennepalvelut/Toimipisteen_tietoliikennepalvelu_Reitti