Aki Peltonen

Hybridipilvipalvelun verkkotekniikka

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

31.3.2016

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Aki Peltonen Hybridipilvipalvelun verkkotekniikka 29 sivua 31.3.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Janne Salonen

Tässä opinnäytetyössä on tarkoitus perehtyä pilvipalvelualustojen tietoverkko-ominaisuuksiin. Työ rajattiin hybridinä, eli osin yrityksen omana ja osin ulkoistettuna toteutettuun palveluun. Työssä keskitytään tietoverkkotekniikoihin, kuten virtuaaliverkkoihin ja erillisverkkoihin, joilla palvelut liitetään toisiinsa.

Opinnäytetyön kohteeksi valittiin hybridinä toteutetut palvelut, koska ulkoisten pilvipalveluiden käyttö on yritystoiminnassa jo vakiintunut käytäntö, ja usein yrityksen omat, sisäiset tietotekniikkapalvelut liitetään tavalla tai toisella pilvipalveluihin. Tämän opinnäytetyön kohteiksi on valittu kaksi tällä hetkellä suurinta pilvipalveluntarjoajaa, Amazon ja Microsoft.

Lisäksi tässä opinnäytetyössä käsitellään lyhyesti pilvipalveluntarjoajien tuotteita ja markkinaosuuksia, mutta pääosin keskitytään kahden suurimman palveluntarjoajan tietoverkkotekniikoihin.

Työhön käytettiin julkisesti saatavilla olevaa elektronista materiaalia, kuten palveluntarjoajien verkkosivuja ja muuta julkista materiaalia.

Opinnäytetyössä selvisi, että pilvipalveluiden markkinajohtaja on edelleen Amazon Web Services, mutta sen kilpailijat kuten Microsoft Azure tarjoavat kattavan ja varteenotettavan vaihtoehdon, varsinkin jos asiakkaalla on oma IT-infrastruktuuri ja voidaan esimerkiksi hyödyntää tuttuja hallintatekniikoita.

Tärkein periaatteellinen ero tarkasteltujen palveluntarjoajien palveluissa on se, että Amazon tarjoaa ainoastaan pilvipalveluja, kun taas Microsoftin tuotteet ja palvelut ovat asennettavissa myös yrityksen omiin konesaleihin. Lisäksi on huomattava, että molempien palveluntarjoajien käsitellyt verkkotekniset ratkaisut ovat huomattavasti toistensa kaltaisia, ja tukeutuvat pitkälti samoihin teknisiin ratkaisuihin.

Avainsanat	Hybridi, pilvipalvelut, Amazon, Microsoft

Author(s) Title Number of Pages Date	Aki Peltonen Networking techniques with hybrid cloud service 29 pages 31 March 2010
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Data Networks
Instructor(s)	Janne Salonen, Principal Lecturer

The aim of this thesis was to study the networking techniques used with cloud services. The work was limited to a hybrid cloud service, which is defined as a service hosted partly as an internal service and partly as an external service. The work concentrates on the networking techniques used to connect the services together, including virtual private networks and dedicated networks.

The hybrid service model was selected as the subject matter because using external cloud services is already an established practice within business operations and it is common to link internal services into external ones. Two largest cloud service providers, Amazon and Microsoft were selected as the study targets.

In addition, this thesis briefly discusses about different products offered by the service providers and their estimated market shares, yet focusing on networking technologies.

The work is based into the publications and electronic material available in public websites.

The thesis revealed that the Amazon Web Services dominates the cloud services market, but competitors such Microsoft Azure offer a potential alternative, especially if the customer has on-premises IT infrastructure and can take advantage of the familiar management techniques.

The most important difference of the examined service providers is that Amazon offers only cloud services, while Microsoft products and services can be installed in the data centers owned by the customer. It should also be noted that both network service providers technical solutions are substantially similar to each other, and rely largely on the same techniques.

Keywords	Hybrid, cloud service, Amazon, Microsoft

Sisällys

Lyhenteet

ACL	Access Control List, pääsylista tai käyttöoikeusluettelo.
API	Application Programming Interface, ohjelmointirajapinta.
APN	AWS Partner Network, Amazon-pilvipalveluntarjoajan partneriverkosto.
ARM	Azure Resource Model, Azuressa käytetty resurssimalli.
ASN	Autonomous System Number, autonomisen järjestelmän numerotunnus.
AWS	Amazon Web Services, tuotenimi Amazonin pilvipalvelualustalle.
BGP	Border Gateway Protocol, internetliikenteessä käytetty reititysprotokolla.
CLI	Command Line Interface, komentotulkki.
DaaS	Database as a Service, tietokanta pilvipalveluna.
DMZ	Demilitarized Zone, tietotekniikassa IP-aliverkko, josta on pääsy internetiin.
EC	Elastic Cloud, Amazonin tuotenimi pilvipalveluresurssille.
EC2	Elastic Cloud 2 tai Amazon Elastic Compute Cloud 2, kts. ed.
Gbps	Gigabit per second, tiedonsiirtonopeus gigabittiä sekunnissa.
HTTP	Hypertext Transfer Protocol, www-palvelujen käyttämä tiedonsiirtomuoto.
IaaS	Infrastructure as a Service, palveluna tarjottava infrastruktuuri.
ICMP	Internet Control Message Protocol, tiedonsiirto- tai kontrolliprotokolla.
IEEE	Institute of Electrical and Electronics Engineers, standardoiva järjestö.
IKE	Internet Key Exchange, salauksessa käytetty avaintenvaihtoprotokolla.
IP	Internet Protokol, Internetliikenteessä käytetty yhteyskäytäntöosoite.
IPSec	IP Security Architecture, salaukseen käytetty tietoliikenneprotokolla.
IPv4	Internet Protocol version 4, TCP/IP-mallin Internetkerroksen protokolla.
MPLS	Multiprotocol Label Switching, tietoliikennepakettien välitysmenetelmä.
NAT	Network Address Translation, IP-osoitteiden osoitteenmuunnos.
NIC	Network Interface Controller, verkkosovitin tai verkkokortti.
NIST	National Institute of Standards and Technology, standardoiva virasto.
NSG	Network Security Group, pääsylistoja sisältävä tietoturvamäärittely.
OSI	Open Systems Interconnection Reference Model, käsitemalli, tietoliikenne.
PaaS	Platform as a Service, palvelualusta ulkoistettuna palveluna.
PPPoE	Point-to-Point Protocol over Ethernet, tietoliikenneprotokolla.
SaaS	Software as a Service, sovelluspalvelu pilvipalvelusta.
SKU	Stock Keeping Unit, myytävä tuote tai myyntiyksikkö.
SLA	Service Level Agreement, asiakkaan ja palveluntarjoajan välinen sopimus.
SQL	Structured Query Language, relaatiotietokantojen standardoitu kyselykieli.
SSTP	Secure Sockets Tunneling Protocol, eräs VPN-tunnelointiprotokolla.
TCP	Transfer Control Protocol, tietoliikennepakettien välitysprotokolla.
UDR	User Defined Routes, termi käyttäjän tekemille reititysmäärityksille.

VLAN	Virtual Local Area Network, virtuaalilähiverkko.
VM	Virtual Machine, virtuaalikone.
VNet	(Microsoft) Virtual Network, Microsoftin termi virtualiverkolle.
VPC	Virtual Private Cloud, yksityinen virtuaaliverkko pilvipalvelussa.
VPN	Virtual Private Network, virtuaalinen erillisverkko.

1 Johdanto

Tässä opinnäytetyössä termillä hybridipalvelu tai hybridi pilvipalvelu tarkoitetaan palvelua, joka on Gartnerin sekä National Institute of Standards and Technologyn (NIST) määrittelyyn perustuen rakennettu niin, että osa tarjottavasta palvelusta on toteutettu yrityksen omana, sisäisenä palveluna, ja osa sijaitsee ulkoistettuna julkisessa pilvipalvelussa (Public Cloud). Sisäisen ja ulkoisen palvelun hallinta tehdään yhteisellä hallintajärjestelmällä ja palvelut liitetään toisiinsa määritellyillä tietoverkkoyhteyksillä. [1; 2; 3.]

Hybridinä toteutettu palvelu voi olla vain sisäisten asiakkaiden käyttöön tarkoitettu. Palvelua voidaan tarjota julkisen verkon kautta tai se voi olla näiden kombinaatio.

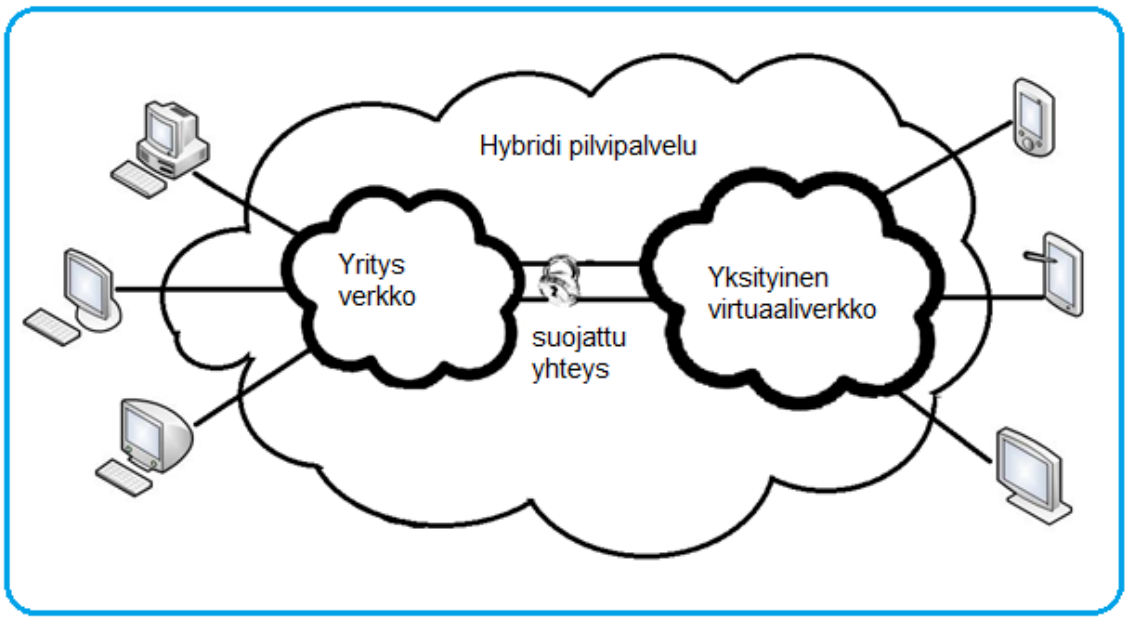
Tässä opinnäytetyössä ei ole tarkoitus testata tai käydä yksityiskohtaisesti läpi pilvipalvelun rakentamista kummankaan pilvipalveluntarjoajan tuotteilla, vaan löytää tuotteista erityisesti hybridinä toteutetulle pilvipalvelulle hyödyllisiä, verkkotekniikkaan ja verkonhallintaan liittyviä ominaisuuksia ja niiden mahdollisia eroja. Kummaltakin työn kohteeksi valitulta palveluntarjoajalta löytyy kattava julkinen dokumentaatio sähköisessä muodossa.

2 Hybridinä toteutettu palvelu

Nykyaikainen tietotekniikkapalvelu voidaan rakentaa hybridinä lukuisista syistä. Yrityksen omia sisäisiä resursseja voidaan nykyaikaisilla pilvipalvelunhallintamekanismeillä helposti laajentaa käyttämään ulkoisia resursseja, esimerkiksi palvelun ruuhkautuessa tai kun palvelulle tarvitaan tehokkaampi saatavuus globaalisti. Tällöin osa palveluista saatetaan nopeasti sijoittaa lähemmäs asiakasta, esimerkiksi kokonaan toiseen valtioon tai maanosaan.

Palvelulle voidaan tarvita monista syistä lisäkapasiteettia. Esimerkiksi testausympäristöjä voidaan tarvita kausiluontoisesti, tai palvelun käyttäjämäärät voivat vaihdella voimakkaasti eri vuodenaikoina. Hybridinä toteutettu palvelu voi tällöin olla myös kustannusten hallintaan sopiva väline, koska ulkoiset pilvipalvelut tyypillisesti aiheuttavat kuluja vain, kun niitä käytetään.

Lisäksi ulkoisen palvelun käyttö saattaa olla perusteltua esimerkiksi jatkuvuussuunnittelun tuloksena. Nykyiset pilvipalvelut esimerkiksi mahdollistavat varmistusdatan säilytyksen turvallisesti tai ulkoinen palvelu voi korvata vikaantuneen sisäisen palvelun automaattisesti. Palvelulle annetut tietoturvavaatimukset saattavat synnyttää tarpeen hybridinä toteutettuun palveluun, koska suurta tietoturvaa vaativa tieto voidaan tällöin säilyttää yrityksen sisäisissä järjestelmissä, ja sijoittaa vähemmän arkaluontoinen ulkoisiin palveluihin. [4; 5; 8.]



Kuvio 1. Periaatekuva, hybridi pilvipalvelu

3 Pilvipalveluntarjoajat

Markkinatutkimusten ja uutisoinnin perusteella voidaan todeta, että tällä hetkellä pilvipalveluiden tarjontaa dominoi vain muutama palveluntarjoaja. Suurin pilvipalveluiden tarjoaja on edelleen Amazon palvelualustallaan Amazon Web Services (AWS), mutta esimerkiksi Microsoft on Azure-palvelualustallaan lisännyt markkinaosuuttaan. Yksi uusimmista pilvipalvelumarkkinoille lähteneistä yrityksistä on hakukoneyhtiö Google, Google Compute Engine -palvelualustallaan.

Markkinatutkimusyhtiö Gartnerin toukokuussa 2015 julkaistun tutkimuksen mukaan esimerkiksi IaaS-pilvipalvelutyypin markkinajohtajat ovat Amazon ja Microsoft. Gartnerin mukaan Amazonilla oli vuonna 2015 kymmenen kertaa suurempi pilvipalvelukapasiteetti kuin sen neljällätoista suurimmalla kilpailijalla. Tässä opinnäytetyössä käsitellään tarkemmin ainoastaan Amazonin ja Microsoftin pilvipalvelualustojen ominaisuuksia. [6; 7; 9.]

4 Amazon.com, Inc ja AWS

Amazon (Amazon.com, Inc) on amerikkalainen sähköiseen kaupankäyntiin ja pilvipalveluihin erikoistunut yritys. Yritys on kooltaan Yhdysvaltain suurimpia, ja sen tuotevalikoima on laaja. Amazon on tunnettu verkkokauppapaikasta Amazon.com, mutta yritys esimerkiksi valmistaa kuluttajatuotteita, kuten sähköistä lukulaitetta Kindle. Amazonin pilvipalvelualusta Amazon Web Services (AWS) on perustettu vuonna 2002 ja Amazonin ensimmäinen verkkotallennuspalvelu avattiin vuonna 2006.

Amazon Web Services -pilvipalvelualusta tarjoaa lukuisia tuotteita eri pilvipalvelutyypeille, mutta kaikkia ei tarkastella tässä yhteydessä. Tässä opinnäytetyössä käsitellään tarkemmin vain Amazonin palvelualustan tietoverkko-ominaisuuksia kuten pilvipalvelujen liitettävyyttä asiakasyrityksen omiin tietoverkkoihin.

4.1 Amazon Web Services -pilvipalvelutuotteet

Amazonin pilvipalvelualusta Amazon Web Services (AWS) tarjoaa asiakkailleen laajan tuotevalikoiman. Tuotteita ei ole Amazonin markkinointimateriaalissa ryhmitelty esimer-

kiksi teknisten pilvipalvelutyyppien mukaan, vaan tuotteet on jaettu kolmeen pääluokkaan: infrastruktuuriin liittyviin palveluihin, sovelluksiin ja käyttöjärjestelmiin liittyviin palveluihin sekä sovelluskehitykseen ja tuotteiden hallintaan liittyviin palveluihin. Kunkin pääluokan alle on jaettu useita tuoteryhmiä. [10.]

Amazonin infrastruktuuripalvelut tarjoavat pilvipalvelutyypeille kuten IaaS, SaaS ja DaaS perinteisiä konesaliratkaisuja korvaavat palvelut pilvipalveluina. Luokasta löytyvät virtuaalikoneet, pilvisovellukset, relaatiotietokannat, tietovarastot sekä erilaiset verkko- ja levypalvelut. Hybridin palvelun rakentamiseen liittyvät tuotteet löytyvät Amazonin markkinointitermillä ”ydinpilvipalveluiksi” (Core Cloud Infrastructure Services) nimetystä tuoteryhmästä. Ryhmän palvelut on mahdollista rakentaa skaalattuina tai varustaa kuormantasauksella ja erilaisilla liitäntätuotteilla kuten yhdyskäytävillä tai erilaisilla integrointituotteilla.

Amazonin sovelluspalvelut ja alustapalvelut tarjoavat tuotteita pilvipalvelutyypeille kuten SaaS ja PaaS. Amazonin julkisessa materiaalissa alustapalvelut (Accelerate your Cloud Success with Rich Platform Services) on otsikoitu omaksi luokakseen, ja se sisältää esimerkiksi analysointituotteita (Business Intelligence, Data Warehouse), yrityssovelluksia (Desktop Virtualization, Email), mobiilialustoille suunnattuja tuotteita tai erilaisia liitäntä- ja välitystuotteita (Pipelines, Streaming, Internet of Things).

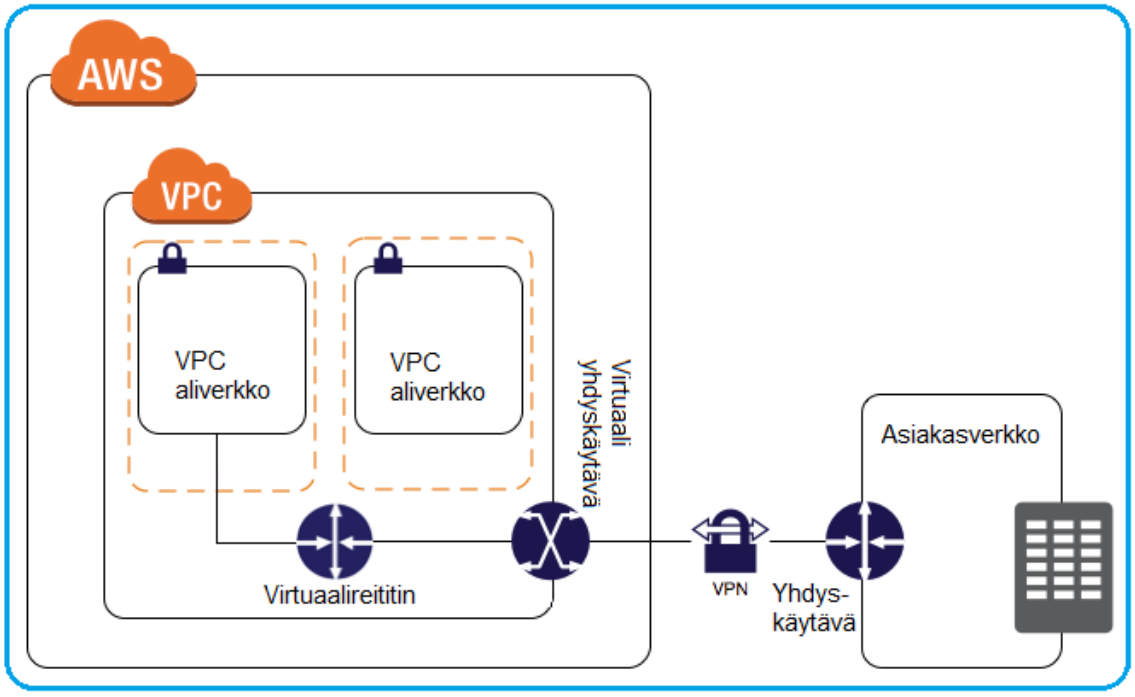
Edellä mainittujen luokkien lisäksi Amazon on jakanut sovelluskehitykseen ja järjestelmähallintaan liittyvät tuotteet omaan luokkaansa. Increase Developer Productivity and Operational Efficiency -otsikon alle on sijoitettu sovelluksia ja palveluja kuten sovelluskehitystyökaluja, valvontasovelluksia, resurssinhallintatyökaluja ja erilaisia pääsynhallintaan (Access Control) tai tietoturvaan (Key Storage, Application Firewall) liittyviä tuotteita.

4.2 Hybridiarkkitehtuuri Amazonin tuotteilla

Tässä opinnäytetyössä rajatun kaltainen hybridipalvelu tehtäisiin perustamalla palveluntarjoajalle yksityinen, ns. Private Cloud -tyyppinen palvelu eli yksityinen virtuaaliverkko (VPC). Virtuaaliverkko yhdistettäisiin asiakkaan sisäiseen tietoverkkoon ja omiin (pilvi)palveluihin [kuvio 2]. Molemmat verkot olisivat luonteeltaan sisäisiä, julkisista verkoista eristettyjä, vaikka palveluntarjoajan osuus teknisesti sijaitsee julkisessa pilvipalvelussa. Amazonin tuotteita ei tällä hetkellä ole saatavilla yrityksien omiin konesaleihin,

vaan palvelut ovat yksinomaan pilvipalveluita. Hybridi palvelu voisi täten olla esimerkiksi järjestelmä, jonka tietokanta on yrityksen omilla palvelimilla, mutta asiakkaita palveleva ja helposti kuormituksen mukaan skaalattava osuus toimisi pilvipalvelusta käsin.

Amazonin pilvipalveluympäristö voidaan yhdistää asiakkaan ympäristöön joko julkisen internetin kautta tai rakentamalla asiakkaan ja palveluntarjoajan välille kokonaan yksityinen erillisverkko. Hybridin palvelun rakentamiseen liittyvät tuotteet, kuten VPC, Direct Connect ja VPN, löytyvät Amazonin ydinpilvipalvelujen tuotevalikoimasta.



Kuvio 2. Periaatekuva, asiakasverkko, VPN ja VPC

4.2.1 Amazon VPC

Amazon Virtual Private Cloud (VPC) -tuotteen avulla voidaan rakentaa suojattu ja julkiselta verkkoliikenteeltä eristetty pilvipalvelukokonaisuus eli yksityinen virtuaaliverkko. Amazonin tuotenimi tavanomaiselle, julkiselle public cloud -tyyppiselle, pilvipalvelukokonaisuudelle on Amazon Elastic Compute Cloud (EC2 tai EC2 Classic). VPC:ssa ajetaan samoja EC2-yhteensopivia pilvipalveluresursseja kuin tavanomaisessa pilvipalveluratkaisussa. VPC:n peruspilvipalvelua laajemmat ominaisuudet antavat palvelun ylläpitäjälle enemmän työkaluja ja ominaisuuksia. Kustannustehokkainta olisi käyttää tavanomaista pilvipalvelua, mutta jossain palvelun elinkaaren vaiheessa laajemmille ominaisuuksille on tyypillisesti tarvetta.

VPC on pilvipalvelutuote, jolla asiakas voi määritellä käyttöönsä yksityisen, muusta pilvipalvelusta ja julkisesta internetistä eristetyn palvelualueen. Asiakas voi hallita ja määrittää alueensa palvelut, verkkoasetukset ja esimerkiksi tietoturva-asetukset itse. Oletusarvoillaan Amazonin virtuaaliverkkoa luotaessa syntyy yksityinen IP-verkko, julkinen IP-osoite ja vastaava yhdyskäytävä. Tässä opinnäytetyössä kuvatun kaltaisessa hybridimallissa virtuaaliverkolle tarvitsee yksinkertaisimmillaan määritellä vain sisäiset RFC 1918 -määritelmän mukaiset yksityiset IP-osoitteet eikä julkista osoitetta tai julkista yhdyskäytävää tarvita. Jos virtuaaliverkolle tai jollekin sen tarjoamalle palvelulle tarvitaan myös julkinen osoite, saadaan sellainen käyttöön Amazonille varatuista julkisista osoitteista. Asiakkaan itse rekisteröimien julkisten IP-osoitteiden käyttö vaatii virtuaaliverkon tietoliikenteen reitityksen asiakkaan oman verkon kautta internetiin.

Tavanomaiseen julkiseen pilvipalveluratkaisuun verrattuna yksityisen virtuaaliverkon käyttö mahdollistaa esimerkiksi seuraavat toiminnot tai määrittelyt:

- staattisten IP-osoitteiden käyttämisen
- useiden IP-osoitteiden ja verkkoliitäntöjen määrityksen samalle instanssille
- sekä lähtevän että tulevan verkkoliikenteen suodattamisen
- resurssikohtaisten pääsynhallintalistojen (ACL) käyttämisen
- pääsynhallintalistojen vaihtamisen tuotannon aikana.

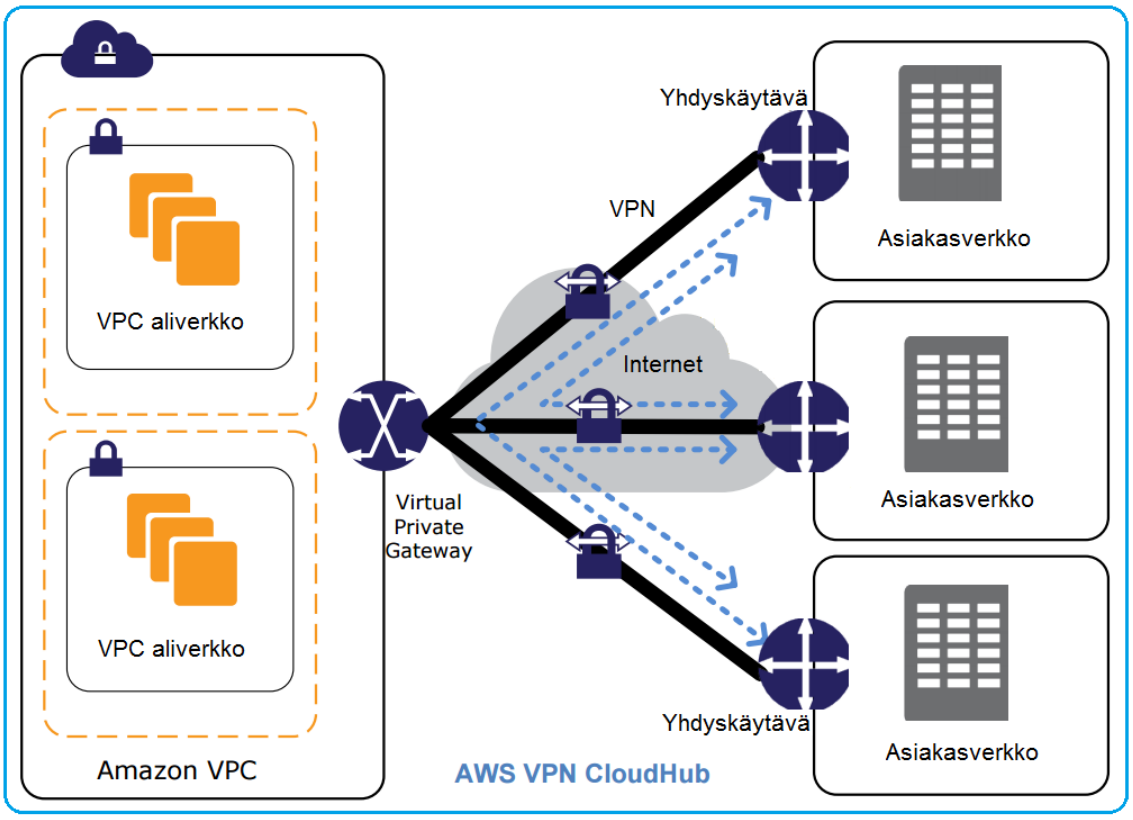
Edellä mainituista ominaisuuksista ovat verkkoteknisesti hyödyllisiä erityisesti kiinteiden IP-osoitteiden käyttömahdollisuus sekä käytönaikainen mahdollisuus vaihtaa pääsylistoja. [16.]

4.2.2 Virtual Private Network (VPN)

Tavanomainen tapa yhdistää virtuaaliverkko asiakkaan omaan verkkoympäristöön on välittää verkkojen välinen tietoliikenne turvallisesti ja yksityisesti Virtual Private Network (VPN) -yhteyden avulla. Verkkojen välinen tietoliikenne välitetään tällöin salattuna tavanomaisen internetyhteyden kautta. [10; 11.]

VPN-yhteys voidaan muodostaa laitepohjaisesti reitittimestä reitittimeen tai ohjelmistopohjaisesti, esimerkiksi yksittäisille tietokoneille, VPN-asiakasohjelman avulla. Ohjelmistopohjaisen VPN-yhteyden voi muodostaa myös VPN-yhteyttä tukevan laitteen (appliance) avulla. AWS tukeutuu VPN-yhteyden tunneloinnin osalta IPSec (Internet Protocol security) VPN-protokollien käyttöön. VPN-yhteys muodostetaan yhdyskäytävien välille,

ja Amazonin palvelussa yhteys koostuu aina kahdesta IPsec-tunnelista. Vika- tai huoltotilanteissa liikenne välitetään automaattisesti toisen tunnelin kautta. Paremman vikasietoisuuden saavuttamiseksi VPN-tunnelien päätepisteet sijaitsevat fyysisesti eri datakeskuksissa. Useiden asiakasverkkojen liittämistä helpottamaan Amazon tarjoaa ratkaisun nimeltä ”AWS VPN CloudHub”. Ratkaisussa samaan yhdyskäytävään liitetään useampia VPN- tai erillisverkkoyhteyksiä [kuvio 3].



Kuvio 3. Usean asiakasverkon yhdistäminen Cloudhub-tekniikalla [13]

Amazonilta löytyy luettelo laitteista, joiden toimivuus on VPN-yhteyden kanssa testattu. Lista on jaettu sen mukaan, tukeeko laite staattista vai dynaamista reititystä. Jos jokin laite tai ohjelmisto ei tue VPN-yhteyttä, Amazon kehottaa etsimään tietoa käyttäjäfoorumeiltaan tai käyttämään yleisohjetta, jossa VPN-yhteyden muodostamisen edellytykset ovat kuvattu. Testattujen laitteiden lista ei ole erityisen kattava verrattuna saatavilla olevien laitteiden määrään, mutta yleisesti tuetun VPN-protokollan käyttö mahdollistaa myös muiden laitteiden käyttämisen. [13; 20.]

Jos virtuaaliverkon liittämiseen käytetään kahta tai useampaa rinnakkaista VPN-yhteyttä, Amazonin ratkaisuja käytettäessä VPN-yhteydet ovat aktiivisia samanaikaisesti. Vikatilanteessa kaikki liikenne ohjataan automaattisesti toimiviin VPN-yhteyksiin. Lisäksi,

vikasietoisuuden parantamiseksi tai muihin verkkoihin suuntautuvan liikenteen reitittämiseksi omia yhteyksiään käyttäen, VPN-yhteyksien rinnalle on mahdollista perustaa myös erillisverkkoyhteys. [13; 14.]

Amazonin materiaali tukeutuu VPN-tunneloinnissa ainoastaan IPSec-arkkitehtuurin mukaisen salauksen käyttöön. Dokumentaation mukaan VPN-yhteyden voi muodostaa myös palomuurin läpi sillä edellytyksellä, että palomuuri tukee IPsec-yhteyden muodostamiseen tarvittavien protokollien käyttöä. On tunnettua, että eräissä salausprotokollissa, kuten IKE:ssä on turvallisuusongelmia, joten IPSec-kehykseen perustuva salaustekniikka ei todennäköisesti ole kaikilta osin täysin turvallinen [17]. VPN-arkkitehtuureja on saatavilla myös muita, joskus kustannustehokkaampia ratkaisuja, kuten OpenVPN. Tätä opinnäytetyötä kirjoittaessa esimerkiksi OpenVPN-arkkitehtuuriin perustuvan tunneloinnin käyttöön ohjeistavat vain kolmannen osapuolen dokumentaatiot ja esimerkit.

Liikenne virtuaaliverkon resursseilta ja aliverkoista voidaan reitittää VPN-tunneliin joko staattisesti tai dynaamisesti BGP-reititysprotokollan (Border Gateway Protocol) avulla. Dokumentaatio tukeutuu ainoastaan BGP:n käyttöön. Yhdyskäytävään voi asettaa joko yritykselle määritellyn julkisen BGP-verkkonumeron (ASN) tai käyttää yksityisiä ASN-numeroita. [18.]

4.2.3 Amazon Direct Connect

Amazon Direct Connect (AWS Direct Connect) -tuotteella on mahdollista rakentaa asiakaskohtainen ja yksityinen erillisverkko (dedicated network).

Amazonin tarjoama erillisverkkotuote on asiakkaalle kytkettävä yhteys, eikä sen avulla kuljetettavaa tietoliikennettä välitetä missään vaiheessa muun julkisen internetliikenteen joukossa. Pilvipalvelusta tehdään tällöin lähes kiinteä osa yrityksen omaa paikallisverkkoa. Ennen erillisverkkoyhteyden käyttöönottoa yhteys pitää kytkeä. Palveluntarjoajalta löytyy tätä varten esimerkiksi lista kumppaniyrityksistä, jotka tarjoavat erillisverkkopalvelua ja auttavat yhteyden kytkemisessä. Dokumentaatiossa esitetään valokuituyhteyden porttinopeuksiksi 1 Gbps tai 10 Gbps, mutta pienemmät porttinopeudet ovat mahdollisia tietoliikenneyhteyden tarjoavan kumppaniyrityksen kautta. Amazon ei dokumentaatiossaan esittele syvällisemmin erillisverkkotuotteeseen tarjottavia verkkotekniikoita, vaan dokumentaatio keskittyy opastamaan palvelujen liittämiseen.

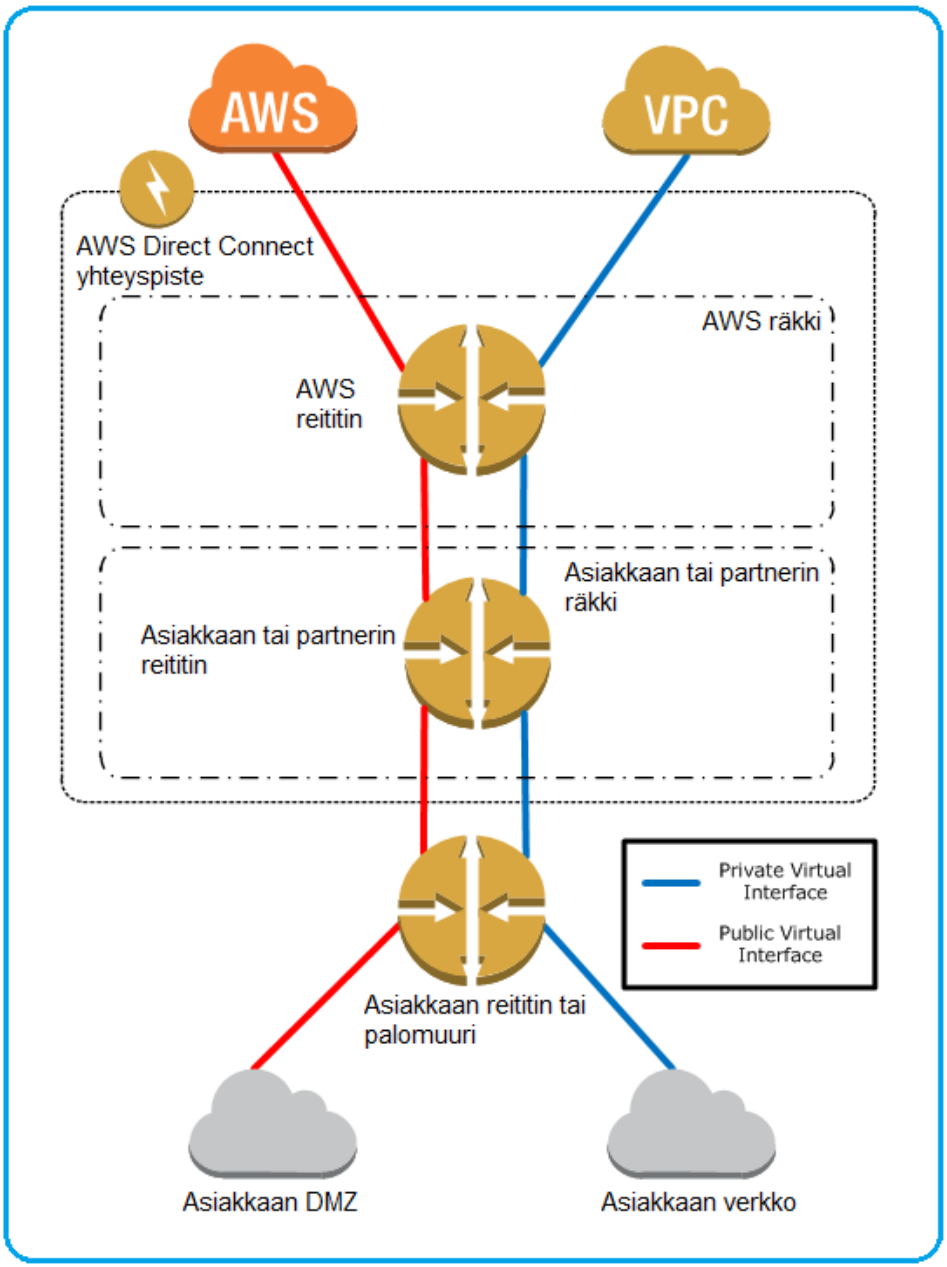
Verkkoliikenne erillisverkon kautta Amazonin palveluihin, kuten virtuaaliverkkoihin, edellyttää IEEE 802.1Q (VLAN) -standardin mukaisten virtuaalilähiverkkojen ja virtuaaliverkkoliitäntöjen (virtual interface) luomista kutakin pilvipalveluresurssia kohden. Yrityksen omia, paikallisia VLAN-verkkoja, ei voi sellaisenaan laajentaa erillisverkkoon, vaan erillisverkkoyhteydelle perustetaan omat VLAN-verkot. Erillisverkkoyhteys edellyttää BGP:n käyttöä reititysprotokollana. [12; 14.]

Erillisverkkoyhteyden käyttöönoton edellytykset

- fyysinen sijainti lähellä AWS Direct Connect -yhteyspistettä tai yhteyden rakentaminen Amazonin partneriverkostoon (APN) kuuluvan yrityksen kanssa
- teknisesti yhteensopiva valokuituportti
- BGP-reititysprotokollan käyttö ja reititettävien IP-verkkojen ASN-numerointi
- yhdyskäytävät ja vastaavat verkkoliitännät (Virtual Private Gateways, Interfaces) sekä VLAN-tunnisteet
- jos erillisverkkoyhteydellä liitytään VPC-virtuaaliverkkoon, verkkoliittymien (interfaces) osoitteet tulee valita 169.254.0.0/16 verkosta.

Yksityisen erillisverkon hyödyt perustuvat suureen ja vakaaseen tiedonvälityskapasiteettiin ja yhteyden turvallisuuteen. Erillisverkkoyhteyden käyttö voi täten olla perusteltua, jos palvelussa on tarpeen liikuttaa erityisen suuria tietomääriä tai palvelu vaatii reaaliaikaisen tiedonsiirron. Voi myös olla, että palvelulle suunnitellut tietoturvavaatimukset eivät esimerkiksi salli tiedonvälitystä julkisen internetin kautta edes VPN-yhteyden välityksellä.

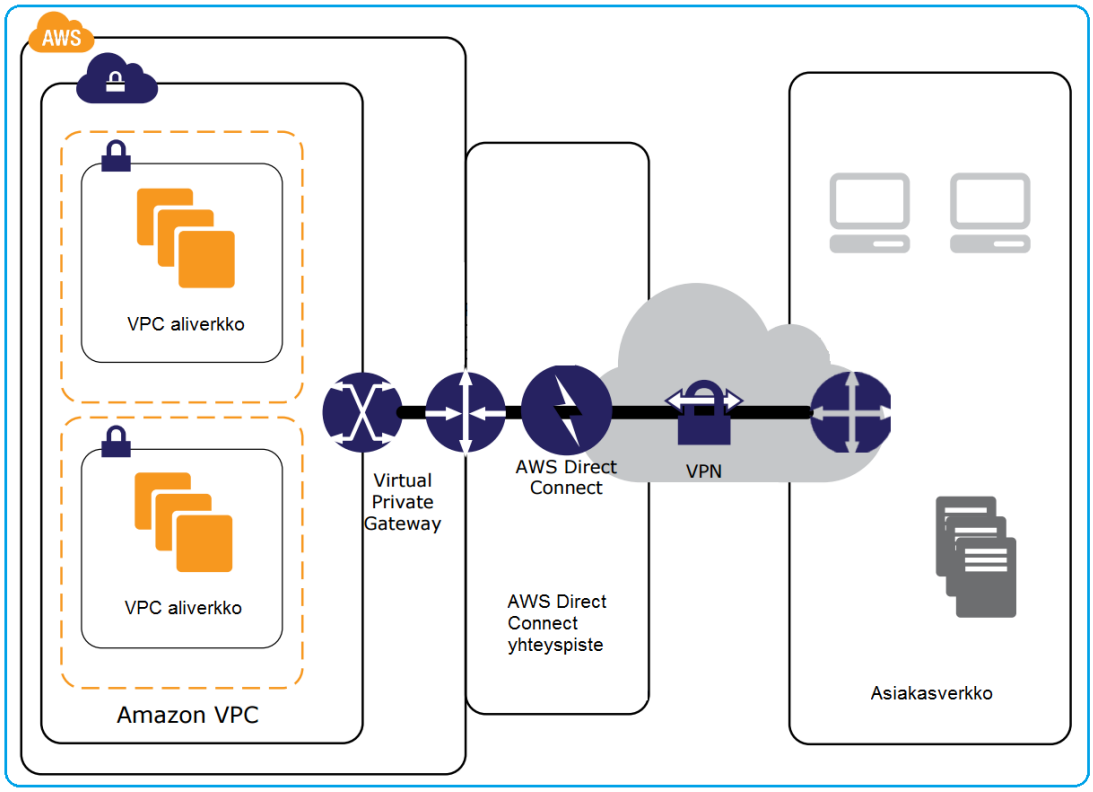
Erillisverkko ei ole sellaisenaan vikasietoinen yhteys, eikä sille tätä opinnäytetyötä kirjoittaessa tarjota Amazonin puolesta palvelun laadun takaavaa SLA-sopimusta. Vikasietoisuuden parantamiseksi erillisverkkoyhteyksiä voidaan rakentaa useampia tai varayhteydeksi voidaan rakentaa esimerkiksi internet-yhteyttä käyttävä VPN-yhteys. Erillisverkkoyhteys on verkkoliikenteen kannalta aina ensisijainen yhteys, eikä kuormantasaus ole mahdollista esimerkiksi rinnakkaisen VPN-yhteyden kanssa. Amazon tarjoaa erillisverkkoyhteyksiä tällä hetkellä neljästätoista sijainnista, joista suurin osa on Yhdysvalloissa. Euroopassa on tarjolla kaksi yhteyspistettä. [12.]



Kuvio 4. AWS Direct Connect -periaatekuva

4.2.4 AWS Direct Connect ja VPN-yhteys sarjassa

Amazonin virtuaaliverkon voi liittää yritysverkkoon myös niin, että asiakasverkosta muodostetaan VPN-yhteys Amazonin erillisverkon yhteyspisteeseen [kuvio 5]. Yhteyspisteen ja virtuaaliverkkopalveluiden välille taas on kytketty erillisverkkoyhteydet. Edellä mainitun kaltaisesta ratkaisusta hyötyvät erityisesti hybridiverkkomallit, joissa palveluntarjoajalle on perustettu useita virtuaaliverkkoja. Näin virtuaaliverkkojen resurssit saataisiin yhdistettyä toisiinsa nopealla ja vakaalla tietoliikenneyhteydellä. [14.]



Kuvio 5. AWS Direct Connect ja VPN-yhteys sarjassa

4.2.5 AWS VPC Peering

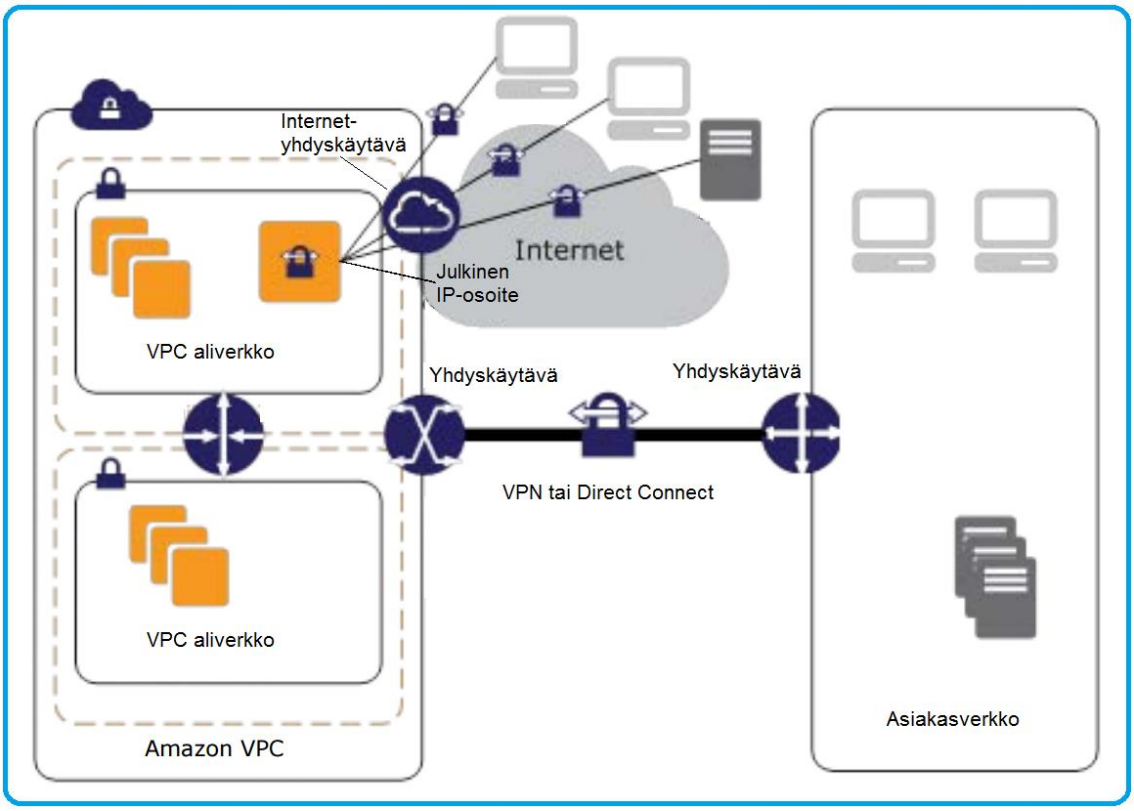
Kaksi tai useampi rinnakkaista virtuaaliverkkoa voidaan liittää toisiinsa myös VPC Peering -tekniikalla. Peering on vaihtoehtoinen tekniikka VPN-yhteydelle tai erillisverkkoyhteydelle. Peering-tekniikalla voidaan esimerkiksi liittää kaksi palveluntarjoajalla sijaitsevaa rinnakkaista virtuaaliverkkoa toisiinsa. Vaikka hybridimuotoinen palvelu on mahdollista toteuttaa myös niin, että palveluntarjoajalle perustettaisiin rinnakkaisia virtuaaliverkkoja, ei peering-tekniikkaa käsitellä tässä yhteydessä laajemmin. Opinnäytetyössä rajatun kaltaisessa hybridimallissa pilvipalvelu liitettäisiin yritysverkkoon joko VPN-yhteyksillä tai erillisverkoilla. [15]

4.3 VPC:n määrittelyyn ja ominaisuuksiin liittyvät huomiot

4.3.1 Yhdyskäytävä ja oletusarvot

Jos pilvipalveluun luodaan yksityinen virtuaaliverkko (VPC) oletusarvoillaan, siihen asetetaan esimerkiksi tarvittavat IP-verkot ja -osoitteet sekä internetyhdyskäytävä, jolla pilvipalvelun resurssit voivat liikennöidä internetiin. Oletusarvoisesti liikennöinti palvelua kohti on estetty, mutta liikennöinti palvelusta ulospäin on sallittu. Yhdyskäytävä tekee tarvittaessa osoitteenmuunnoksen (NAT). Opinnäytetyössä rajatun kaltaista hybridiä kokonaisuutta rakennettaessa internet-yhdyskäytävää ei tarvita, jos palvelua ei tarjota julkiseen internetiin tai liikenne aiotaan välittää asiakkaan oman tietoverkon kautta. Liitettäessä virtuaaliverkko VPN- tai erillisverkkoyhteydellä, pitää näitä varten luoda omat yhdyskäytävät. [18.]

Virtuaaliverkosta internetiin palvelua tarjoavalle resurssille asetetaan sisäisen osoitteen pariksi julkinen IP-osoite Amazonille varatusta yleisestä osoitevarastosta. Osoite on dynaaminen ja saattaa muuttua. Resurssille voidaan myöhemmin asettaa staattinen, asiakkaalle pysyvästi varattu, julkinen IPv4 IP -osoite. Kullekin asiakkaalle on varattavissa IPv4-osoitteiden rajallisuudesta johtuen vain muutama kiinteä osoite. Kiinteä osoite on Amazonin palvelussa tuotenimellä Elastic IP. Elastic IP on allokoitavissa dynaamisesti resurssilta toiselle, ja tällöin osoitteen vaihto esimerkiksi vikatilanteissa on helppoa. Ainoastaan sisäisille asiakkaille suunnatuissa hybridipalveluissa internetyhdyskäytävää tai julkisia osoitteita ei tarvita ja ne voidaan jättää pois jo suunnittelun alussa. Hybridiratkaisuja suunniteltaessa on lisäksi huomioitava, että Elastic IP-osoitteen käyttö ei ole mahdollista, jos VPC:n tietoliikenne on reititetty asiakkaan sisäiseen tietoliikenneverkkoon ja sen kautta internetiin. [18.]



Kuvio 6. Periaatekuva, VPC varustettuna kahdella yhdyskäytävällä

4.3.2 VPC-reititys

VPC sisältää oletusarvoisesti kaksi reititystaulua: ensisijaisen ja asiakaskohtaisen taulun. Ensisijaisella taululla huolehditaan esimerkiksi siitä, että virtuaaliverkon resurssit voivat liikennöidä oletusarvoisesti keskenään sekä palvelusta ulospäin. Hybridiä ratkaisua rakennettaessa tietoliikenteen reititys on Amazon VPC:ssä mahdollista tehdä staattisilla reiteillä, ts. reititystauluja muokkaamalla, tai dynaamisena Border Gateway Protocol (BGP) -reititysprotokollan avulla. Sekä Amazonin että Microsoftin virtuaaliverkkotuotteessa tukeudutaan dynaamisen reitityksen osalta täysin BGP:n käyttöön reititysprotokollana. [18.]

4.3.3 VPC:n tietoturva

Amazon VPC:n tietoturva verkkoliikenteen osalta perustuu asetettaviin turvallisuusryhmiin (Security Groups) ja pääsylistoihin (ACL). Liikennettä sallivia tai rajoittavia ryhmiä voidaan asettaa kullekin instanssille tai resurssille. Pääsylistoja puolestaan voidaan asettaa aliverkoille. Oletusryhmät sallivat liikenteen oletusarvoisesti sisältä ulospäin,

mutta sisään tuleva liikenne on estetty. Turvallisuusryhmillä verkkoliikennettä sallitaan (sisään tai ulos) määrittelemällä liikenteessä käytettävä portti, protokolla ja IP-osoite tai aliverkko sekä mahdolliset parametrit. [18.]

4.3.4 VPC:n tekniset rajoitukset

Palveluntarjoaja on määritellyt VPC-palvelulleen lukuisia teknisiä rajoituksia. Esimerkiksi IP-aliverkkojen määrä on oletusarvoisesti rajattu kahteensataan per VPC tai VPN-yhteyksiä voidaan muodostaa kymmenen per VPC. Amazonin palveluja käytettäessä useimpia näistä rajoituksista voidaan lieventää erillisellä toimenpiteellä. Kummankin käsiteltävän palveluntarjoajan teknisten rajojen oletusarvot ovat hieman erilaisia ja määrien kasvattaminen lisää palvelun käyttökustannuksia. [18]

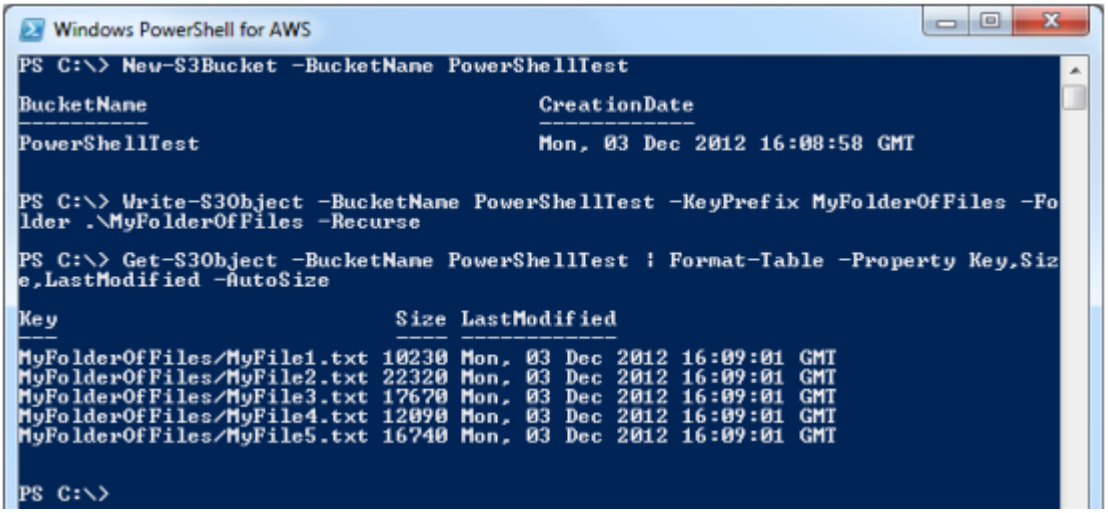
4.4 AWS-palveluiden hallinta

Amazonin tekninen dokumentaatio on selkeää ja kohtuullisen järjestelmällisesti esitettyä. Dokumentaatio sisältää esimerkkejä ja malleja yleisimmille hybridiverkkokonfiguraatioille.

Amazonin pilvipalvelutuotteita voi hallita eri työkaluilla. Nopein tapa aloittaa pilvipalvelujen käyttö on kirjautua palveluihin selainpohjaisen käyttöliittymän kautta. Lisäksi Amazon tarjoaa esimerkiksi valmiit ohjelmointirajapinnat (API) sekä komentorivipohjaiset työkalut (CLI tools) tavanomaisille käyttöjärjestelmille. Lisäksi on huomattava, että Amazon on lisännyt ohjelmistotuen ja valmiit rajapinnat lähinnä Microsoft-pohjaisten ympäristöjen hallintaan käytetyille työkaluille kuten Windows PowerShellille [kuvio 6] ja Microsoft System Center Operations Manager -järjestelmälle. [30.] Mahdollisuus käyttää yhtenäisiä työkaluja Amazonin pilvipalvelujen sekä yrityksen oman infrastruktuurin hallintaan on selkeä etu. Tästä hyötyvät järjestelmien kehittäjät, pääkäyttäjät ja näiden kautta järjestelmien hallintaa tuottava organisaatio. Tyypillisesti yrityksen oma tietotekninen ympäristö tällöin hyödyntää Microsoftin tuotteita.

Windows PowerShell on Microsoftin vuonna 2006 julkaisema komentorivipohjainen tehtävänhallintatyökalu tai -viitekehys. PowerShellin komentojen avulla järjestelmän pääkäyttäjät voivat esimerkiksi luoda monimutkaisia, mutta helposti toistettavia komentorivejä. Komentorivimuodossa annettujen käskykokonaisuuksien avulla voidaan esimerkiksi tuottaa monimutkaisia pilvipalveluresursseja tai muuttaa niiden asetuksia yhdellä

komentoketjulla. PowerShell-komentoketjuja voidaan myös kutsua muista ohjelmista tai esimerkiksi asiakasportaaleista, jolloin voidaan esimerkiksi tuottaa lisäarvopalveluja tai kehittää itsepalveluratkaisuja.



Kuvio 7. Esimerkkikuva. PowerShell-ikkuna ja AWS-komentorivejä

5 Microsoft Corporation ja Azure

Microsoft Corporation on amerikkalainen teknologiayritys. Yritys on Yhdysvaltain suurimpia, ja se tarjoaa esimerkiksi lukuisia ohjelmisto- ja kuluttajatuotteita. Microsoft tunnetaan laajalti esimerkiksi Windows-käyttöjärjestelmästä sekä Office-ohjelmistoistaan. Kuluttajatuotteista voidaan mainita esimerkiksi Xbox-pelikonsoli.

Microsoftin pilvipalvelualusta julkaistiin vuonna 2008. Palvelun kaupallinen julkaisu tapahtui vuonna 2010 nimellä Windows Azure ja vuodesta 2014 alkaen nimellä Microsoft Azure. Myös Azure tarjoaa lukuisia tuotteita eri pilvipalvelutyypeille, mutta tässä opinnäytetyössä tarkastellaan lähemmin vain Azuren verkko-ominaisuuksia ja liitettävyyttä. [24.]

5.1 Pilvipalvelualusta Microsoft Azure

Azure perustuu palvelinlaitteisiin ja ohjelmistoihin, joita on asennettu yli sataan konesaliin eri puolilla maapalloa. Microsoftin pilvipalvelu on jaettu kolmeen loogiseen kokonaisuuteen: Office 365 -palveluun, josta tarjotaan virtuaalisia Office-tuotteita, julkiseen pilvipalveluun nimeltä ”public IP addresses in Azure”, ja virtuaaliverkkopalveluihin [24]. Microsoft on esimerkiksi tuottanut pilvi- ja konesalikäyttöä varten suunnitellut räkkipalvelimet sekä Azurea palvelevan käyttöjärjestelmän itse. Palvelinlaitteille on annettu tuotenimeksi Open CloudServer (OCS). [21.]

Microsoft esittelee markkinointimateriaalissaan pilvipalvelutuotteet luokiteltuna käyttötarkoituksensa mukaan. Luokittelu on kaksitasoinen. Esimerkiksi identiteetinhallinta tai verkkopalvelut ovat omina tuoteryhminään, ja kuhunkin ryhmään liittyvät tuotteet on listattu näiden alle. Microsoftin materiaali esittelee hybridiä palveluratkaisua rakentavalle kaksi erityisen kiinnostavaa tuoteryhmää. Tuoteryhmä nimeltä Hybrid Integration sisältää esimerkiksi tuotteet BizTalk Services, Service Bus, Backup ja Site Recovery. Verkkotuotteiden (Networking) valikoimasta löytyvät esimerkiksi yksityinen virtuaaliverkko (Virtual Network VNet), VPN-yhteys (VPN Gateway) ja erillisverkkotuote (ExpressRoute). [24.]

5.2 Hybridiarkkitehtuuri Azuren tuotteilla

Microsoft on sijoittanut Hybrid Integration -tuoteryhmään esimerkiksi integraatiotuotteita, joita asiakas voi käyttää yhdistämään julkisissa verkoissa olevia laitteita tai sovelluksia yrityksen sisäverkossa toimiviin palveluihin. Esimerkiksi palvelintuotteella Biztalk Services on Hybrid Connections -ominaisuus, jonka avulla mobiilisovellus voi hakea dataa yrityksen sisäverkossa sijaitsevan Microsoft SQL -palvelimen tietokannasta. Palveluiden yhdistämiseen ei tällöin tarvita erityisten verkkoyhteyksien määrittelyä tai yritysverkon liittämistä pilvipalveluun, vaan liikennöinti voidaan tehdä esimerkiksi tavanomaisella HTTP-protokollalla palomuurin läpi.

Toinen esimerkki pilvi-integroidusta tuotteesta on Azure Backup -varmistuspalvelu, jolla dataa, esimerkiksi virtuaalikoneita tai kansiorakenteita, voi varmistaa pilvipalvelussa sijaitsevaan tallennustilaan. Tuoteryhmälle annetun nimen mukaisesti ryhmästä löytyvillä tuotteilla voidaan luoda hybridejä tai pilvi-integroituja palveluja. Näitä tuotteita ei tässä

opinnäytetyössä käsitellä tarkemmin, koska työssä esitetty hybridipalvelu on rajattu niin, että yrityksen sisäverkko yhdistettäisiin kiinteästi pilvipalveluun.

Azuren tarjoomaa käytettäessä hybridipalvelu rakennettaisiin perustamalla palveluntarjoajalle yksityinen virtuaaliverkko (VNet) ja luomalla yhteys asiakkaan verkon ja pilvipalvelun välille joko VPN-yhteyksillä tai kokonaan yksityisillä erillisverkoilla. Microsoftin tuotteilla on mahdollista luoda varayhteydet VPN-yhteyksillä, kun pääyhteys on tehty erillisverkkoyhteydellä. Lisäksi on mahdollista liittää useita asiakasverkkoja yhteiseen virtuaaliverkkoon. Järjestelmä olisi tietoliikennejärjestelyiden osalta hyvin pitkälle samanlainen kuin Amazonin tuotteilla tehtynä. Amazonin palveluista poiketen Microsoftin palvelut ja palvelimet voidaan asentaa myös yrityksen omaan konesaliin, joten Microsoftin tuotteilla voidaan rakentaa perinteisellä tavalla hybridi pilvipalvelu, jossa resurssit voivat läpinäkyvästi sijaita yrityksen omissa tai ulkoisissa palveluissa.

Azuren tuotenimi yksityiselle pilvipalvelualueelle eli yksityiselle virtuaaliverkolle on Azure Virtual Network (VNet). Amazonin palvelusta poiketen Microsoft on tuotteistanut yhdyskäytävät ja tarjoaa kahta eri tekniikkaan perustuvaa VPN-yhteyttä. Erillisverkkotuote puolestaan on tuotenimellä ExpressRoute. [24]

5.2.1 Azure-virtuaaliverkko (VNet)

Kuten Amazonin vastaava tuote, Microsoft Azuren yksityinen virtuaaliverkko (VNet) tarjoaa palvelun, jolla asiakas saa pilvipalvelusta käyttöönsä julkisesta internetistä eristetyn osuuden. Asiakas voi määritellä esimerkiksi virtuaaliverkkonsa palvelut, tietoturva-asetukset tai verkkoasetukset, kuten IP-osoitteet, IP-aliverkot ja tietoliikenteen reitityksen. Hybridimallissa yksityiseen virtuaaliverkkoon luodut palvelut voidaan avata julkiseen internetiin, pelkästään yrityksen sisäverkkoon tai kumpaankin. Palveluiden saatavuutta voi tehostaa käyttämällä esimerkiksi kuormantasausta tai valitsemalla virtuaaliverkon fyysinen sijainti lähellä asiakasta.

Kummankin palveluntarjoajan tuotteet sisältävät samoja tai samankaltaisia ominaisuuksia, ja merkittäviä teknisiä eroja on hankala löytää. Esimerkiksi Microsoft tarjoaa palvelussaan asiakkaalle varatun julkisen ja dynaamisen IP-osoitteen, ja Amazonilla vastaava ominaisuus on tuotenimellä Elastic IP. Microsoftin asiakas saa oletusarvoisesti käyttöönsä 20 varattua IP-osoitetta ja Amazonin asiakas viisi. Asiakas voi varata kummaltakin palveluntarjoajalta käyttöönsä useampia osoitteita lisämaksua vastaan.

5.2.2 Azure VPN

Kumpikin palveluntarjoaja mahdollistaa virtuaaliverkkopalvelunsa liittämisen yritysverkkoon VPN-yhteyksillä. Molempien palveluntarjoajien käyttämät VPN-palvelut ja käytettävissä olevat verkkotekniikat ovat samankaltaisia. Myös Microsoftin virtuaaliverkon voi yhdistää asiakasverkkoon laitepohjaisesti, IPSec-protokollien käyttöön perustuen tai sopivan, SSTP-protokollia tukevan, VPN-ohjelmiston avulla [25]. Microsoft kutsuu laitepohjaista VPN-yhteyttä termillä ”Site-to-Site” ja ohjelmistopohjaista yhteyttä nimellä ”Point-to-Site”. Jälkimmäinen tapa on Microsoftin dokumentaation mukaan tarkoitettu vain muutamien tietokoneiden yhdistämiseksi virtuaaliverkkoon. Henkilökohtaiseen tietokoneeseen asennettu VPN-ohjelmisto on kuitenkin yleinen tapa luoda turvallinen yhteys yritysverkon ja käyttäjän koneen välille. Hybridi palvelumalli ei pakota käyttämään palvelua vain yritysverkosta käsin, joten mahdollisuus luoda yhteys yksittäisen tietokoneen ja palvelun välille voi olla toimiva ratkaisu esimerkiksi pienille etätoimistoille.

Microsoft on tuotteistanut yhdyskäytäväratkaisut ja erottelee tuotteet erilaisen suorituskyvyn ja eräiden ominaisuuksien avulla. VPN-yhdyskäytäviä on suorituskyvyn perusteella tarjolla kolmea tyyppiä: perus-, vakio- ja suurikapasiteettinen yhdyskäytävä (Gateway SKU). Lisäksi yhdyskäytävät on jaettu reititysmallin perusteella staattisiin ja dynaamisiin [27]. Hybridin palvelun suunnittelun kannalta on tärkeä huomioida esimerkiksi, että edullisin VPN-yhdyskäytävä (Basic SKU) ei mahdollista VPN-yhteyden käyttöä erillisverkkoyhteyden rinnalla, eikä staattisesti reitittävään yhdyskäytävään voi liittyä VPN-sovelluksella.

Amazonin palvelusta poiketen Microsoft tarjoaa kaikille VPN-yhteyksille tarvittaessa laadun takaavan SLA-sopimuksen [24;26]. Kummankaan palveluntarjoajan lista laitteista, joiden toiminta VPN-yhteyden kanssa on vahvistettu, ei ole erityisen kattava tarjolla olevien laitteiden määrään verrattuna. Listat kuitenkin sisältävät merkittävimpien laitevalmistajien laitteita sekä niiden tuetut ohjelmistoversiot. [24]

5.2.3 Azure-erillisverkko ExpressRoute

Microsoftin tuotenimi erillisverkkopalvelulle on ExpressRoute. Kuten Amazoninkin vastaavalla tuotteella, ExpressRouten avulla voidaan sopivan kumppaniyrityksen kanssa rakentaa asiakaskohtainen erillisverkko, jossa tietoliikenne välitetään yrityksen verkosta

pilvipalveluun täysin omalla kytkennällään [kuvio 8.] Amazonin tuotteesta poiketen Microsoft tarjoaa erillisverkkotuotteelleen palvelun laatua takaavan SLA-sopimuksen.

Tehokkaan tietoliikenneyhteyden lisäksi erillisverkon käytöllä saavutetaan muita etuja, esimerkiksi virtuaaliverkon ja yritysverkon välissä ei tarvitse tehdä osoitteenmuunnosta (NAT). Jos erillisverkolla liitytään virtuaaliverkkopalvelujen lisäksi myös Microsoftin muihin (julkisiin) pilvipalveluihin, tulee osoitteenmuunnos kuitenkin tehdä. Kuten Amazoninkin palvelussa, asiakkaan paikallisverkon virtuaalilähiverkkoja (VLAN) ei voida Microsoftin tuotteellakaan laajentaa erillisverkon avulla virtuaaliverkkoon.

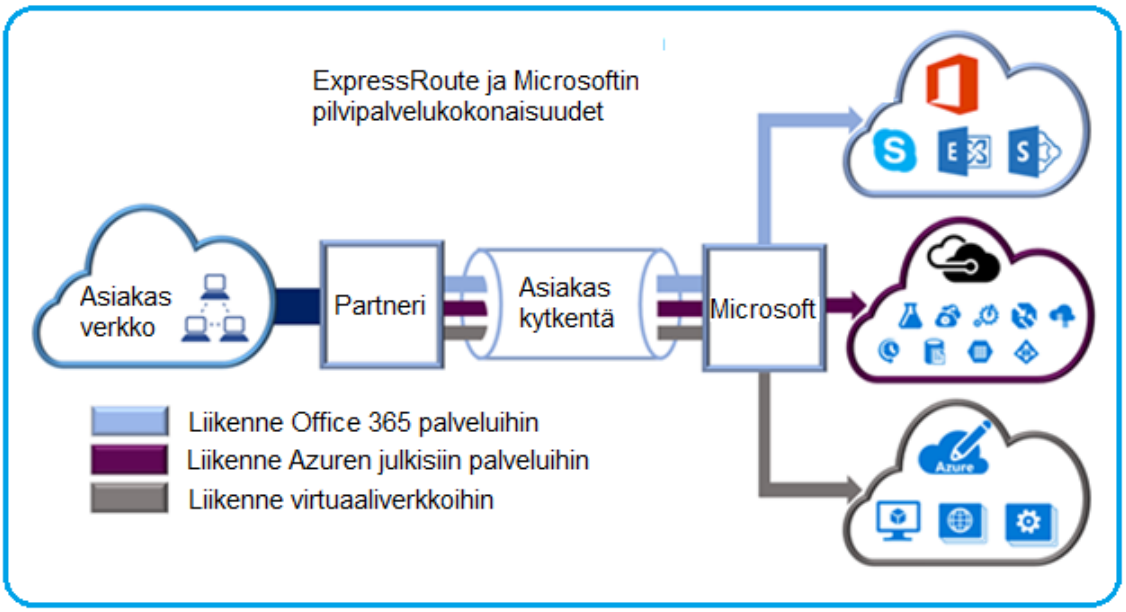
Microsoft esittelee dokumentaatiossaan erillisverkkotuotteessaan käytettyjä tietoverkkotekniikoita hieman syvällisemmin kuin Amazon. Microsoftin tarjoama erillisverkkoyhteys voi olla joko OSI-mallin siirtokerrostasolla (layer 2) kytkentäinen (Layer 2 Cross-Connect), PPPoE-tekniikkaan tai MPLS VPN -tekniikkaan perustuva, julkisista verkoista loogisesti erotettu yhteys tai yhteys voidaan rakentaa fyysisenä ns. ethernet-tason kytkentänä jos palveluntarjoaja sen mahdollistaa. Microsoftin palveluja käytettäessä erillisverkko luodaan vikasietoisuuden takia kytkemällä aina kaksi rinnakkaista yhteyttä. Yhteydet voivat olla rinnakkaisia kytkentöjä tai käytössä voivat olla rinnakkaiset aktiivilaitteet. Erillisverkkoyhteys tukee porttinopeuksia välillä 50Mbps – 10Gbps. Oletusarvoisesti erillisverkkoyhteys voidaan muodostaa samassa maanosassa (geopolitical region) sijaitsevaan pilvipalveluun. Erillisverkkoyhteys toiselle alueelle on mahdollista lisätuotteella nimeltä ExpressRoute premium. Erillisverkkopalvelua tarjoavia yhteyspisteitä on tämänhetkisen materiaalin perusteella maailmanlaajuisesti 22 kappaletta, joista kolme palvelee yksinomaan Yhdysvaltojen hallitusta. Euroopassa on kolme yhteyspistettä.

Erillisverkkotuotteen dokumentaatio tukeutuu ainoastaan BGP-reititysprotokollan käyttöön dynaamisessa reitityksessä. Jos virtuaaliverkosta lähtevä liikenne on esimerkiksi tarkoitus reitittää yritysverkon kautta internetiin, tulee reititysprotokollana käyttää BGP:tä.

5.2.4 Azure BGP -verkot

Reititys pitää erillisverkkoyhteyttä käytettäessä hoitaa BGP:n avulla. Microsoft on jakanut pilvipalvelunsa kolmeen loogiseen kokonaisuuteen. Kokonaisuudet ovat Office 365, julkiset pilvipalvelut sekä virtuaaliverkot [kuvio 8]. Kokonaisuuksia vastaavat BGP-virtuaaliverkot (BGP peering) on nimetty seuraavasti: Azure public, Azure private ja Microsoft.

Varsinaisen tietoliikenneyhteyden perustamisen lisäksi Microsoftin pilvipalveluihin liittyminen edellyttää ainakin yhden ExpressRoute circuit -ominaisuuden aktivoimista. Ominaisuudet on Microsoftin palvelussa tuotteistettu ja niillä on määritellyt kustannukset. Hybridissä palvelumallissa ExpressRoute circuit -tuotteen palveluavaimeen (service key) pitää yhdistää vähintään Azure private BGP-verkon tunniste, jotta liikennöinti virtuaaliverkkoon onnistuu. BGP reititysprotokollan käyttämät ASN-verkkonumerot voivat olla julkisia tai yksityisiä.



Kuvio 8. Periaatekuva. Azuren palvelukokonaisuudet ja ExpressRoute-yhteys.

5.2.5 Azure Vnet-to-Vnet

Microsoftin palvelussa rinnakkaisten virtuaaliverkkojen yhdistämiseen voidaan käyttää VPN-yhdyskäytäviä ja VPN-tunneleita. Virtuaaliverkkojen välille luodaan ns. ”VNet-to-VNet gateway connection”. Hybridi toimintamalli ei rajoita verkkojen määrää vaan palveluntarjoajalle voidaan tarpeen vaatiessa perustaa useampia virtuaaliverkkoja. Amazonin palvelussa taas rinnakkaisten virtuaaliverkkojen yhdistämiseen käytettävää tekniikkaa kutsutaan nimellä Peering.

5.3 Azure-huomiot

5.3.1 VNet-tietoturva

Azuren tietoturvamäärittelyt verkkoliikenteen osalta hoidetaan pääpiirteittäin kuten Amazoninkin tuotteissa. Resurssin ”päätepisteisiin” (endpoints) voidaan määritellä pääsylistoja (ACL). Azuressa termillä ”päätepiste” tarkoitetaan resurssilla olevaa tietoliikenneporttia ja protokollaa, joiden kautta resurssi liikennöi. Pilvipalveluinstansseille sekä aliverkoille voidaan asettaa verkkoliikennettä kontrolloivia turvaryhmiä (NSG). NSG-ryhmien säännöt määritellään samankaltaisesti kuin Amazonin tuotteessa. Säännölle asetetaan nimi, järjestysnumero (priority), lähde- ja kohdeportit, IP-osoitteet tai -alueet, käytettävä protokolla sekä salliva tai kieltävä sääntö.

5.3.2 Azuren resurssimallit

Eräs merkittävimmistä pilvipalveluresurssien luontiin ja hallintaan vaikuttavista asioista on Microsoftin tuotteita käytettäessä se, että resurssi voi olla luotu kahden eri ikäpolven mallin (template) perusteella. Käytetystä resurssimallista riippuen resurssilla on erilaiset ominaisuudet ja resurssia hallitaan eri tavalla. Eri mallin perusteella luodut resurssit eivät ole keskenään täysin yhteensopivia. Uudempaa resurssien hallintamallia kutsutaan lyhenteellä ARM (Azure Resource Model) ja vanhempaa mallia termeillä ”classic model” tai ”service management model”. Resurssi on edelleen mahdollista tuottaa kumman tahansa mallin perusteella, vaikka uudempaa mallia suositellaan.

Esimerkiksi virtuaaliverkkoon perustetulla virtuaalikoneella on aina verkkokortti (NIC), mutta ainoastaan uudemman mallin (ARM) perusteella luodun virtuaalikoneen verkkokortille voidaan asettaa turvaryhmä (NSG). Vanhemman resurssimallin mukaisia resursseja käytettäessä NSG-ryhmä on asetettavissa vain kullekin IP-aliverkolle. Tämän lisäksi NSG-ryhmien lokitiedot ovat käytettävissä vain resursseilla, jotka on luotu uudemman resurssimallin pohjalta.

NSG-ryhmiä voi olla vain yksi per resurssi, mutta sama NSG-ryhmä voi kuitenkin olla samanaikaisesti usean eri resurssin käytössä. Kuhunkin virtuaaliverkkoon voi määritellä useita IP-aliverkkoja ja näiden välistä liikennettä voi hallita esimerkiksi muokkaamalla

kunkin aliverkon turvaryhmää. Hybridimallissa, jos VPN-yhdyskäytävä tai erillisverkkoyhteys ovat omissa aliverkoissaan, ei aliverkkoon dokumentaation mukaan tule asettaa NSG-ryhmää. Koska hybridi toimintamalli edellyttää jatkuvaa tietoliikenneyhteyttä yritysverkon ja palveluntarjoajan verkon ja sen palvelujen välillä on käytännössä järkevä käyttää enemmän ominaisuuksia tarjoavia, uudempaan malliin perustuvia resursseja. [24.]

5.3.3 Azure VNet -reititys

Microsoftin virtuaaliverkkotuotteen sisäänrakennettua reititysmallia kutsutaan dokumentaatiossa termillä System Routes. Tämän ominaisuuden avulla virtuaaliverkon resurssit liikennöivät oletusarvoisesti, ilman erikseen määriteltäviä reittejä tai yhdyskäytäviä, keskenään ja muihin resursseihin esimerkiksi internetissä. Resurssit voivat sijaita samassa tai eri IP-aliverkossa. Oletuksena syntyvät reitit perustuvat kolmeen sääntöön (Local VNet rule, On-premises rule ja Internet rule). Oletussääntöjä ei voi muokata. Jälkimmäinen sääntö käyttää sisäistä yhdyskäytävää nimeltä ”infrastructure internet gateway” reittinä internetiin. On-premises-sääntö puolestaan hybridimallissa reitittäisi liikenteen yritysverkon ja pilvipalvelun yhdistävään VPN-yhdyskäytävään. Sisäisen reitityksen malli on hyvin samankaltainen kuin Amazonin vastaavalla palvelulla. Amazonin ratkaisussa virtuaaliverkon sisäisen reitityksen määrittäviä reititystauluja voi muokata tai niitä voi tuottaa lisää, kuitenkin niin, että oletusreittiä joka mahdollistaa resurssien välisen liikennöinnin virtuaaliverkon sisällä, ei voi poistaa, tai muuttaa. [24.]

Microsoftin materiaali korostaa, että tavallisesti järjestelmän oletusreitit ovat riittäviä. Käyttäjän määrittelemää reititystä (UDR) tarvitaan esimerkiksi, jos halutaan reitittää kaikki liikenne resurssista toiseen jonkin muun resurssin, kuten virtuaalisen palomuurin kautta. Erillistä palomuuriohjelmistoa voidaan käyttää verkkoliikenteen kontrolloimiseen virtuaaliverkossa ja tällöin palomuurin tulisi toimia virtuaalilaitteena virtuaaliverkon sisällä. Koska oletusreittejä ei ole tarkoitus muokata, reitin valinta perustuu reitityssääntöjen priorisointiin. Käyttäjän määrittelemällä reitillä pitää olla korkeampi prioriteetti kuin oletusreiteillä. Hybridimallissa käyttäjän määrittelemää reititystä tarvitaan, jos halutaan esimerkiksi vaikuttaa tietoliikenteeseen sisäisen palomuurin avulla tai jos muutoin halutaan reitittää liikenne oletusmallista poikkeavalla tavalla. [24.]

5.3.4 Azure-yhdyskäytävät

Hybridin palvelun toimintamalli, jossa virtuaaliverkon ja yritysverkon välille luodaan liikennöintiä varten VPN-tunneli, edellyttää VPN-yhdyskäytävän (VPN gateway) luomista kumpaankin verkkoon. Koska oletusreitit luodaan automaattisesti, tällaisessa mallissa ei oletusreitityssääntöjen takia tarvita käyttäjän määrittelemää reititystä ollenkaan ellei liikennettä jostain syystä haluta reitittää poikkeavalla tavalla.

Azuren tuotteilla hybridiä palvelukokonaisuutta rakennettaessa kullekin liitäntätekniikalle tulee valita oikean tyyppinen yhdyskäytävä. Yhdyskäytävät on Microsoftin palvelussa tuotteistettu, ja niillä on tyypistä riippuen erilaiset kustannukset. Yhdyskäytävä valitaan joko staattisen (policy-based VPN) tai dynaamisen (route-based VPN) reititystarpeen perusteella, ja millaiseen kytkentään yhdyskäytävä tarvitaan. Tämän opinnäytetyön mukaisessa hybridissä palvelumallissa yhdyskäytävä olisi vähintään asiakasverkon virtuaaliverkkoon yhdistävä (Site-to-Site VPN) tai erillisverkkotuotteelle (ExpressRoute) sopiva. [27.]

5.3.5 Huomioita Azuren verkko-ominaisuuksista

Azuressa ICMP-protokolla ei ole käytettävissä esimerkiksi kuormantasaajan (Azure Load Balancer) takana oleville resursseille. Lähtökohtaisesti tämä estää esimerkiksi Ping-työkalun käyttöön perustuvat ratkaisut, kuten yksinkertaisen saavutettavuuskyselyn, joka tehtäisiin virtuaaliverkon ulkopuolelta, kuormantasaajan läpi, suoraan palvelun IP-osoitteeseen. Virtuaaliverkon sisällä, esimerkiksi aliverkkojen välillä, ICMP on käytettävissä. [24] Nykyään monet palvelut eivät enää vastaa ping-paketteihin, joten tällöin palvelun saavutettavuus on selvitettävä muulla tavalla, kuten porttikyselyillä.

Amazonin palvelussa ICMP taas voidaan sallia tietoturvasäännöissä. Amazonin tuki perinteisille internet-tekniikoille tuntuu tästä syystä olevan parempi. Hybridissä palvelumallissa ei sinänsä tarvitse ottaa kantaa tällaisin yksityiskohtiin, mutta asialla saattaa olla merkitystä palvelualustaa valittaessa.

5.4 Azuren hallinta

Kuten Amazoninkin palveluja, Microsoft Azuren pilvipalveluja voidaan hallita usealla työkalulla. Tyypillinen tapa aloittaa palvelujen hallinta on kirjautua selainkäyttöiseen portaaliin, mutta pääkäyttäjille on tarjolla muita työkaluja kuten sovellusrajapinnat (API), asiakasohjelmistot ja esimerkiksi monipuoliset PowerShell-komentokirjastot. Eräs tärkeimmistä yrityksille suunnatuista verkkoresurssien hallintajärjestelmistä on Microsoft System Center Configuration Manager 2012, jolla voidaan esimerkiksi hallita sekä sisäisiä että ulkoisia pilvipalveluja samalla tuotteella. Myös Amazon tarjoaa rajapintoja System Centeriä varten.

Selainportaalia käytettäessä tulee muistaa, että tarjolla on yhä kaksi teknisesti erilaista portaalia. Uusin hallintaportaali on lähtökohtaisesti tarkoitettu uudemman hallintamallin (ARM) mukaisten resurssien hallintaan ja perinteinen vanhemman mallin (classic model) mukaisille. Kummallakaan portaalilla ei voi hallita kaikkia palveluja [28] eli joidenkin resurssien tai niiden tiettyjen ominaisuuksien hallinta on pakko tehdä jollakin muulla työkalulla, kuten PowerShell-komennoilla [29].

5.5 Azuren rajoitukset

Microsoft on määritellyt Azuren tekniset rajoitukset kahteen luokkaan, palvelukohtaisiin rajoituksiin ja asiakkaan tilauskohtaisiin rajoituksiin (Subscription limits). Esimerkiksi julkisten IP-osoitteiden määrä (Dynamic Public IP addresses) per tilaus on rajoitettu viiteen. Palvelun dokumentaatiosta löytyy kattava listaus rajoista. Kuten Amazoninkin palvelussa, asiakas voi pyytää raja-arvojen kasvattamista tiettyyn maksimimäärään asti. [24.]

5.6 Azure Stack ja Nano Server

Nykyiset Microsoftin tuotteilla rakennetut hybridiratkaisut perustuvat tyypillisesti Windows Server -palvelinohjelmiston eri versioihin sekä System Center -tuotteeseen. Myös Azure on jo saatavilla yrityksien omiin konesaleihin. Microsoft on esitellyt toukokuussa 2015 Azure Stack -nimisen tuotteen, jonka tarkoitus on mahdollistaa esimerkiksi pilvipalveluiden tai itse toteutettujen (pilvi)sovellusten toiminta joko yrityksen omasta konesa-

lista tai rinnakkain palveluntarjoajan pilvipalvelun kanssa. Tässä konseptissa julkisen pilvipalvelun resursseja sekä omassa konesalissa toimivaa pilvipalvelua hallittaisiin samoilla työkaluilla. [23.]

Lisäksi Microsoft on julkistanut huhtikuussa 2015 uuden pilvipalvelujen tuottamiseen suunnitellun palvelinkäyttöjärjestelmän nimeltä Nano Server [22]. Nano Server on vielä kehitysvaiheessa, mutta ilman graafista käyttöliittymää toimivan palvelimen hallinta tullaan todennäköisesti tekemään pitkälti komentotulkin ja PowerShell-komentojen avulla.

6 Yhteenveto

Tässä opinnäytetyössä vertaillut pilvipalveluntarjoajat ja niiden tarjoamat hybridin palvelun rakentamiseen soveltuvat liitäntätuotteet ovat verkkoteknisesti pitkälle toistensa kaltaisia. Molemmat palveluntarjoajat esimerkiksi käyttävät samoja tai samankaltaisia salaustekniikoita ja reititysratkaisuja. Joitakin eroja kuitenkin löytyy. Esimerkiksi Amazonin VPN-yhteys vaikuttaa teknisesti vikasietoisemmalta ratkaisulta, koska se rakentuu kahdesta VPN-tunnelista, jotka ovat fyysisesti eri sijainnissa. Toisaalta Microsoft tarjoaa Amazonin palveluista poiketen liityntätuotteilleen palvelun laatua takaavat SLA-sopimukset. Amazonin palvelun parempi tuki esimerkiksi ping-protokollalle viittaa siihen, että Amazonin palvelut olisivat kypsempiä, ja esimerkiksi tuki perinteisille internettekniikoille olisi hieman parempi.

Eräs mainittava ero Amazonin palvelun eduksi on se, että Microsoftin tuotteita käytettäessä huomataan nopeasti, että joidenkin ominaisuuksien käyttö vaatii jonkin määrätyn työkalun eikä kaikkia palveluiden hallintaan liittyviä asioita voi hoitaa samalla hallintavälineellä. Amazonin hallintatyökalut vaikuttavat kypsemmiltä, mutta internetjulkaisuista löytyy kuitenkin viitteitä, että Amazoninkaan tarjoamat välineet eivät ole aivan loppuun asti kehitettyjä, vaan joidenkin asetusten tekeminen onnistuu vain määrätyillä työkaluilla [31].

Toinen mainittava ero Amazonin palvelun eduksi liittyy Microsoftin palvelumalleihin. Tekniset erot Microsoftin tarjoamilla, eri ikäpolven toiminta- ja resurssimalleilla (ARM ja Classic model), ovat suuret ja käytännössä niiden rinnakkaiselo aiheuttaa hankaluuksia palveluiden hallinnalle. Uudet palvelut kannattaa käytännössä rakentaa ainoastaan uudempiin palvelumalleihin perustuen.

Palvelujen oletusrajoituksista tai kustannuksista, kuten esimerkiksi peruspalveluun sisältyvistä ominaisuuksista tai niiden määristä, on vaikea löytää oleellisia eroja. Microsoftin palvelussa esimerkiksi eri ominaisuuksien tuotteistaminen vaikuttaa pidemmälle viedyltä. Amazonin palveluiden kustannukset taas näyttävät perustuvan pitkälti siirrettävän datan määrään. Molempien palvelujen suuren tuotemäärän ja kohtuullisen monimutkaisen hinnoittelumallin takia merkittävien erojen löytäminen vaatisi tarkemman analyysin jonkin tarkkaan rajatun esimerkkipalvelun perusteella.

Suurin periaatteellinen ero tässä opinnäytetyössä esiteltyjen palveluntarjoajien välillä on kuitenkin se, että Amazon tarjoaa ainoastaan internetistä toimivia palveluja ja mahdollisuuden liittyä niihin, kun taas Microsoftin tuotevalikoimasta löytyy palveluja ja tuotteita, jotka voidaan asentaa yrityksen omaan IT-infrastruktuuriin. Näin ollen ainoastaan Microsoftin tuotteilla voi rakentaa todellisen hybridin palvelun, jossa asiakkaita palveleva (pilvipalvelu)resurssi voi toimia läpinäkyvästi kummankin infrastruktuurin alueelta. Palveluiden keskitetyn hallinnan tuottamisen kannalta erityisen suuressa roolissa on Microsoftin System Center Configuration Manager -järjestelmä.

Lähteet

1 Gartner 2014. Critical Success Factors for Hybrid Cloud Computing, <http://www.gartner.com/newsroom/id/2745417> (Luettu: 27.1.2016).

2 NIST 2011. Special Publication 800-145 The NIST Definition of Cloud Computing, Peter Mell, Timothy Grance.

3 Wikipedia 2016. Cloud computing. <https://en.wikipedia.org/wiki/Cloud_computing> (Luettu: 27.1.2016).

4 Network Exchange Blog 2015. Top 5 Reasons Hybrid Cloud Makes Sense, Scott Koegler. <http://networkingexchangeblog.att.com/enterprise-business/top-5-reasons-hybrid-cloud-makes-sense/#fbid=RBFcX1IVnM0> (Luettu: 30.1.2016)

5 The Cloud Zone 2015. 5 Reasons Why Hybrid Cloud Is Becoming the "New Normal", Sheza Gary. <https://dzone.com/articles/5-causes-why-hybrid-cloud-is-becoming-the-new-norm> (Luettu: 30.1.2016)

6 RightScale 2015 State of the Cloud Report. Markkinatutkimus RightScale, Inc.

7 Network World 2015. Gartner shows two-horse race in IaaS cloud: AWS and Microsoft Azure, Brandon Butler. < http://www.networkworld.com/article/2924814/cloud-computing/gartner-shows-two-horse-race-in-iaas-cloud-aws-and-microsoft-azure.html> (Luettu: 30.1.2016)

8 Journal of Information Sciences and Computing Technologies(JISCT) 2015. A New Computing Environment Using Hybrid Cloud, Rao, Naveena, David, Narayana.

9 Network World 2015. Gartner: Amazon’s cloud is 10x bigger than its next 14 competitors, combined, Brandon Butler. <http://www.networkworld.com/article/2925186/cloud-computing/gartner-amazon-s-cloud-is-10x-bigger-than-its-next-14-competitors-combined.html> (Luettu: 31.1.2016)

10 Amazon Cloud Products 2016. Verkkojulkaisu. <https://aws.amazon.com/products/?nc2=h_ql_ny_livestream_blu> (Luettu: 31.1.2016).

11 Amazon Web Services, Hybrid Architechtures 2016. Verkkojulkaisu. <https://aws.amazon.com/enterprise/hybrid/> (Luettu: 31.1.2016).

12 Amazon Web Services, Direct Connect frequently asked questions 2016. Verkkojulkaisu. <https://aws.amazon.com/directconnect/faqs/> (Luettu: 7.2.2016).

13 Amazon Virtual Private Cloud Connectivity Options 2014, Steve Morad <AWS_Amazon_VPC_Connectivity_Options.pdf>.

14 What is AWS Direct Connect? Versio 22.10.2013. Verkkojulkaisu. <http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html> (Luettu: 7.2.2016).

15 VPC Peering Overview. Verkkojulkaisu 2016. < http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-peering-overview.html> (Luettu: 8.2.2016).

16 Benefits of Using a VPC. Verkkojulkaisu 2016. <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-vpc.html#concepts-vpc> (Luettu: 8.2.2016).

17 Don't stop using IPsec just yet, No Hats IP & DNS Security Specialists. Verkkojulkaisu 2014. <https://nohats.ca/wordpress/blog/2014/12/29/dont-stop-using-ipsec-just-yet/> (Luettu 8.2.2016).

18 Your Default VPC and Subnets, Amazon Virtual Private Cloud user guide 2016. Verkkojulkaisu. <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/default-vpc.html> (Luettu 10.2.2016).

19 Amazon Feature Guide: Amazon EC2 Elastic IP Addresses 2012. Verkkojulkaisu. <http://aws.amazon.com/articles/1346> (Luettu 10.2.2016).

20 Amazon VPC FAQs, What customer gateway devices are known to work with Amazon VPC? Verkkojulkaisu 2016. <http://aws.amazon.com/vpc/faqs/#C9> (Luettu 14.2.2016).

21 Microsoft's Open CloudServer, Drake, Shaw, Vaid. Verkkojulkaisu 2015. Microsofts_Open_CloudServer_Strategy_Brief.pdf. (Luettu 15.2.2016).

22 Windows Server Blog, Microsoft Announces Nano Server for Modern Apps and Cloud. Verkkojulkaisu 2015. <https://blogs.technet.microsoft.com/windowsserver/2015/04/08/microsoft-announces-nano-server-for-modern-apps-and-cloud/> (Luettu 15.2.2016).

23 Ars technica, Your own personal Azure: Microsoft's new Azure Stack for private clouds. Verkkojulkaisu 2015. <http://arstechnica.com/information-technology/2015/05/your-own-personal-azure-microsofts-new-azure-stack-for-private-clouds/> (Luettu 15.2.2016).

24 Microsoft Azure, The cloud for modern business. Verkkojulkaisu 2016, tuotedokumentaatio ja sähköiset resurssit.<https://azure.microsoft.com> (Luettu 15.2.2016).

25 Wikipedia, Secure Socket Tunneling Protocol. Verkkojulkaisu 2016.<https://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol> (Luettu 27.2.2016).

26 Amazon Web Services, Amazon VPC FAQs. Verkkojulkaisu 2016. <https://aws.amazon.com/vpc/faqs/> (Luettu 27.2.2016).

27 Microsoft Azure, About VPN gateways. Verkkojulkaisu 2016. <https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-about-vpngateways/#gateway-skus> (Luettu 28.2.2016).

28 Microsoft Azure, Azure portal availability chart. Verkkojulkaisu 2016. <https://azure.microsoft.com/en-us/features/azure-portal/availability/> (Luettu 1.3.2016).

29 Wintellect, Is Microsoft Changing Azure Too Much? Ballard 2015. Verkkojulkaisu. <http://www.wintellect.com/devcenter/paulballard/is-microsoft-changing-azure-too-much> Luettu 1.3.2016,

30 Amazon Webservices documentation. Verkkojulkaisu 2016. <http://docs.aws.amazon.com/> (Luettu 2.3.2016).

31 Solinor, Kohti palvelimettomia palveluja. Heinonen 2016. Verkkojulkaisu. <https://solinor.fi/blog/posts/kohti-palvelimettomia-palveluja> (Luettu 4.3.2016).