HAMK
Hämeen ammatti-
korkeakoulu

Azuren tarjoamat VPN-ratkaisut pk-yritykselle

Ammattikorkeakoulututkinnon opinnäytetyö

Tieto- ja viestintätekniikka, insinööri (AMK)

Syksy 2023

Panu Virta

HAMK
Hämeen ammatti-
korkeakoulu

Tieto- ja viestintätekniikka, insinööri (AMK) Tiivistelmä
Tekijä Panu Virta Vuosi 2023
Työn nimi Azuren tarjoamat VPN-ratkaisut pk-yritykselle
Ohjaaja Teemu Järvenpää

Opinnäytetyön tavoitteena oli tarjota kattava katsaus Azuren VPN-ratkaisuihin, niiden ominaisuuksiin, kustannuksiin ja soveltuvuuteen pk-yritysten tarpeisiin. Tarkoituksena oli myös selvittää keskeiset työvaiheet VPN-ratkaisun käyttöönottoa varten.

Opinnäytetyön teoriaosuudessa syvennyttiin VPN:än toimintaan ja pilvipalveluiden virtuaaliverkkojen teoriatietoon sekä keskeisten työvaiheiden selvittämiseen ja ratkaisuiden kustannuksiin. Opinnäytetyön toiminnallisessa osuudessa toteutettiin kolme erilaista VPN-ratkaisua. Kaikkien ratkaisujen kohdalla kuvattiin käyttöönoton vaatimat toimenpiteet ja selvitettiin toteutuksen arvioidut kustannukset, hallinnointi ja laajennettavuus mahdollisuudet.

Työn tuloksena saatiin selvitettyä Azuren tarjoamien VPN-ratkaisuiden käyttöönottoon vaaditut keskeiset toimenpiteet sekä arviot kunkin toteutuksen kustannuksista. Johtopäätöksenä voidaan todeta, että Azure tarjoaa monipuolisia ja skaalautuvia VPN-ratkaisuja, jotka soveltuvat myös pk-yrityksille.

Avainsanat Azure, IPSec, pilvipalvelut, TLS, VPN
Sivut 28 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Information and Communication Technology Abstract
Author Panu Virta Year 2023
Subject Azure VPN solutions for Small and Medium Sized Enterprises
Supervisor Teemu Järvenpää

The aim of this thesis was to provide a comprehensive overview of Azure's VPN solutions, their features, costs, and suitability for the needs of small and medium enterprises. The purpose was also to identify the key steps for the implementation of a VPN solution.

In the theoretical part of the thesis, the focus was on the operation of VPNs and the theoretical knowledge of virtual networks in cloud services, as well as identifying the key steps and costs of the solutions. In the practical part of the thesis, three different VPN solutions were implemented. For all solutions, the procedures required for implementation were described, and the estimated costs, management, and scalability options of each implementation were investigated.

As a result of the work, the key steps required for the implementation of Azure's VPN solutions were identified, as well as estimates of the costs of each implementation. In conclusion, it can be stated that Azure offers versatile and scalable VPN solutions that are also suitable for small and medium enterprises.

Keywords Azure, cloud services, IPSec, TLS, VPN
Pages 28 pages

Sisällys

Kuvat, taulukot ja kaavat

1 Johdanto

Virtual Private Network -tekniikka (VPN) ja pilvipalvelut eivät ole mitään uusia asioita. Pilvipalvelut ja niiden tarjoamat resurssit ovat yleistyneet vauhdilla. Microsoft Azure, yhtenä johtavista pilvipalvelualustoista, tarjoaa monipuolisen ympäristön, jossa voidaan toteuttaa erilaisia tietotekniikkaratkaisuja. VPN-yhteydet ovat keskeisiä turvallisen ja yksityisen tiedonsiirron varmistamisessa internetin välityksellä, ja niillä on erityisen tärkeä rooli yritysten tietoturvassa, erityisesti kun siirrytään yhä enemmän etätyöskentelyn ja hajautetun toiminnan malleihin. VPN-yhteyksille on edelleen tarve, uudemmat tekniikat kuten Software-Defined Wide Area Network (SD-WAN), Secure Access Service Edge (SASE) ovat kalliita verrattuna VPN-yhteyksiin. Turvalliset tietoliikenneyhteydet ovat tärkeä osa nykyaikaista verkon hallintaa, ja niiden merkitys korostuu jatkuvasti digitalisoituvassa maailmassa.

Tämän opinnäytetyön tarkoituksena on tutkia VPN-yhteyksien käyttöönottoa ja hallintaa Microsoft Azuren pilvipalveluissa, pk-yrityksen näkökulmasta. Tarkoituksena on vastata tutkimuskysymyksiin ”Minkälaisia VPN-ratkaisuja Azure tarjoaa?” ja ”Kuinka Azuren VPN-ratkaisut soveltuvat Pk-yrityksen käyttöön?” Opinnäytetyössä perehdytään VPN-tekniikoihin sekä perehdytään IKEv2/IPsec ja SSL/TLSVPN protokolliin. Opinnäytetyö käsittelee VPN-yhteyksien teknisiä perusteita, niiden konfigurointia Azure-ympäristössä. Opinnäytetyö on rajattu keskittymään vain Azuren tarjoamiin VPN-palveluihin.

2 Varmennetut verkkoyhteydet

2.1 VPN

VPN-tekniikka on verkkojen turvallisuutta ja yksityisyyttä lisäävä teknologia. Se luo salatun yhteyden käyttäjän laitteen ja VPN-palvelimen välille. Tätä salattua yhteyttä kuvataan yleensä tunneliksi, jonka sisällä käyttäjän data kulkee avoimessa verkossa. (Liu ym., 2006, s. 213) VPN tarjoaa salatun yhteyden, piilottaa käyttäjän IP-osoitteen, mahdollistaa maantieteellisten rajoitusten kiertämisen, suojaa yksityisyyden, takaa turvalliset etäyhteydet organisaatioille ja yhdistää hajautettuja paikallisia verkkoja turvallisesti internetin yli. VPN-tekniikkaa käytetään eri protokollien avulla. (Kapersky, n.d.)

VPN-tunnelointi viittaa prosessiin, jossa VPN luo suojatun yhteyden kahden erillisen verkon välille internetin yli. Tässä prosessissa käyttäjän tietoliikenne paketoidaan ja salataan ennen sen lähettämistä internetin kautta, ja vastaanottopäässä se puretaan ja salaus avataan. Tunnelointi on olennainen osa VPN-teknologiaa, sillä se varmistaa, että data pysyy salassa ja suojattuna myös julkisen internetin kautta kuljettaessa. (Cloudflare, n.d.)

2.2 VPN-ratkaisut

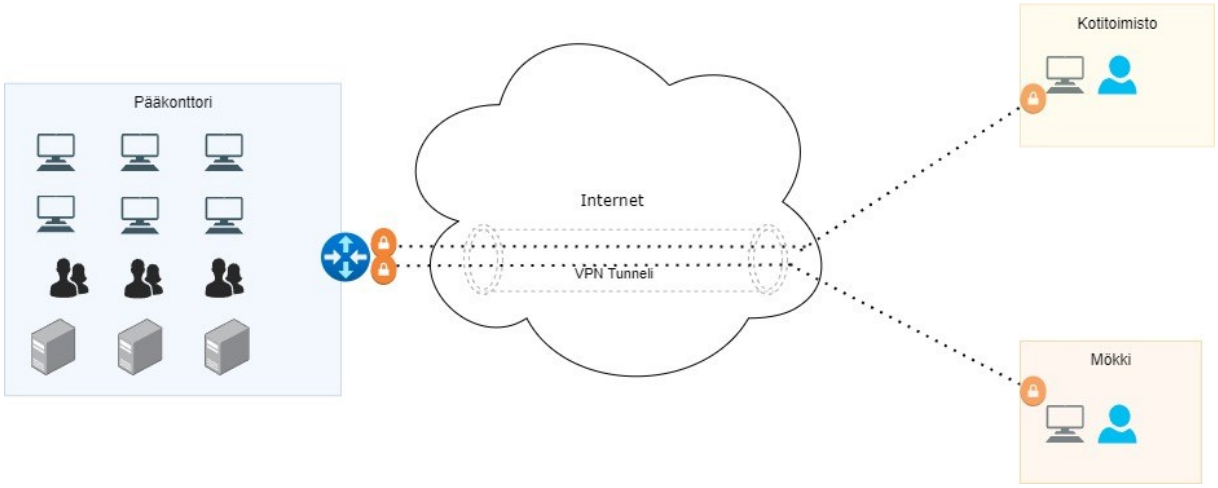
Yleensä puhutaan kahden tyyppisistä VPN-ratkaisuista, Remote-access ja Site-to-Site.

Remote Access VPN tarkoittaa etäyhteyden muodostamista tietoverkkoon turvallisesti internetin välityksellä. Se mahdollistaa etätyöntekijöiden, matkustavien työntekijöiden tai etätoimistojen pääsyn yrityksen tai organisaation sisäiseen verkkoon turvallisesti ja salatun yhteyden kautta. Tämä on erityisen tärkeää silloin, kun käyttäjät tarvitsevat pääsyn yrityksen resursseihin tai tietoihin muista kuin organisaation omista tiloista tai sisäverkoista. (PaloAlto Networks n.d.)

Remote Access VPN -ratkaisussa etäkäyttäjät käyttävät yleisesti ottaen VPN-ohjelmistoa tai VPN-sovellusta omilla laitteillaan, kuten tietokoneillaan, älypuhelimillaan tai tableteillaan. Kun he muodostavat VPN-yhteyden organisaation verkkoon, heidän tietonsa salataan ja reititetään turvallisesti organisaation sisäverkkoon. Tämä salattu yhteys estää ulkopuolisia tarkkailemasta tai sieppaamasta käyttäjän liikennettä, mikä lisää tietoturvaa.
Remote Access VPN mahdollistaa myös organisaation työntekijöiden turvallisen yhteyden yrityksen resursseihin mistä tahansa, mikä lisää työntekijöiden joustavuutta ja mahdollistaa etätyöskentelyn tehokkaasti. Tämäntyyppinen VPN-ratkaisu auttaa myös suojautumaan

avoimissa Wi-Fi-verkoissa liikkuvilta uhilta, koska kaikki tiedonsiirto on salattua. (Fortinet, n.d.-b.) Kuvassa 1 on esitetty esimerkkikuva Remote Access -ratkaisusta.

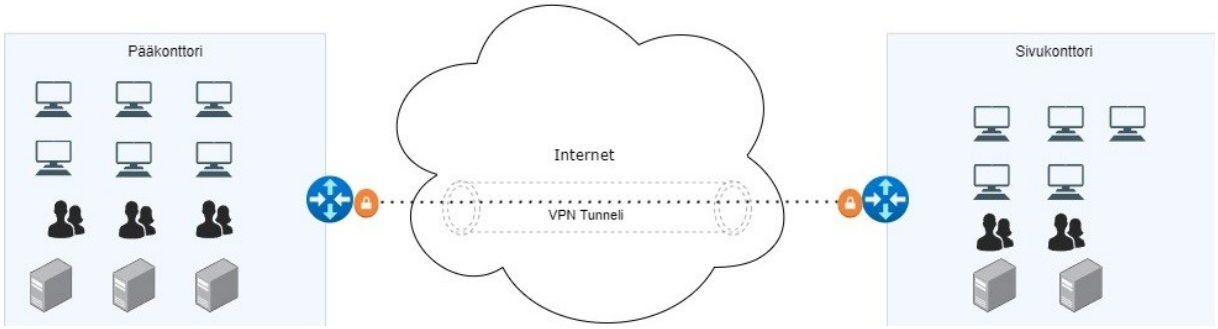
Kuva 1. Remote Access VPN-yhteys.



Site-to-Site VPN tarkoittaa yhteyden muodostamista kahden tai useamman erillisen lokaalin verkon välille internetin tai muiden julkisten verkkojen yli. Tämän tyyppinen VPN-yhteys mahdollistaa organisaatioiden eri sijaintien välisen turvallisen ja salatun tietoliikenteen. (Odom, 2021, s. 325).

Site-to-Site VPN perustuu yleensä erillisiin laitteisiin, kuten VPN-palvelimiin tai VPN-reitittimiin, jotka on asennettu kunkin verkon laitaan. Nämä laitteet luovat suojatun tunnelin organisaatioiden verkkojen välille, näin tietoja voidaan turvallisesti ja salattuna lähettää ja vastaanottaa organisaation sisäisten verkkojen välillä. Tämä on erityisen hyödyllistä yrityksille, joilla on useita toimipisteitä tai sivukonttoreita eri paikoissa. Kun Site-to-Site VPN on konfiguroitu ja muodostettu, se on jatkuvasti päällä, sitä ei tarvitse erikseen käynnistää. (Fortinet, n.d.-c.) Kuvassa 2 on esitetty esimerkkikuva Site-to-Site-ratkaisusta.

Kuva 2. Site-to-Site VPN-yhteys.



2.3 VPN-protokollat

VPN-protokollat ovat käytäntöjä tai standardeja, jotka määrittelevät tai mahdollistavat laitteiden tai ohjelmien väliset yhteydet. Näitä protokollia käytetään salatun ja turvallisen yhteyden luomiseen internetin yli. Muutamia yleisiä VPN-protokollia ovat: PPTP (Point-to-Point Tunneling Protocol), L2TP/IPsec (Layer 2 Tunneling Protocol with IP Security), OpenVPN, IKEv2/IPsec (Internet Key Exchange Version 2 with IP Security) ja SSL/TLSVPN (Secure Socket Layer Protocol / Transport Layer Security). Jokaisella näistä protokollista on omat vahvuutensa ja heikkoutensa, ja valinta riippuu käyttäjän tarpeista ja turvallisuusvaatimuksista. (Nordlayer, n.d.)

2.3.1 IKEv2/IPsec

IPsec (Internet Protocol Security) tarkoittaa ryhmää protokollia, jotka suojaavat tietoliikennettä IP-verkoissa. Se tarjoaa salauksen, datan eheyden sekä lähettäjän ja vastaanottajan todennuksen. Vuonna 1995 Internet Engineering Task Force (IETF) perusti IP Security (ipsec) -työryhmän. Työryhmä määritteli ja standardisoi IPsec-protokollan. RFC1825. (Atkinson, 1995, s. 1)

IPsec VPN perustuu kahdelle pääprotokollalle: Authentication Header (AH) ja Encapsulating Security Payload (ESP). AH-protokolla tarjoaa tietojen eheyden tarkistamisen ja lähettäjän todennuksen, mutta se ei tarjoa salauksen suojaa tietojen salaamiseksi. AH varmistaa, että data on pysynyt muuttumattomana matkan aikana ja että se on peräisin todelliselta lähettäjältä. Tämä tehdään laskemalla tarkistussumma koko IP-paketista, mukaan lukien IP-otsikko ja itse data. Tämä tarkistussumma lasketaan lähettäjän päässä ja se tarkistetaan vastaanottajan päässä. Jos tarkistussumma ei täsmää, tiedetään, että data on joko vioittunut tai sitä on muokattu matkan varrella. (Kent, 2005, s. 8–9)

ESP on keskeinen osa IPsec-protokollaa, joka tarjoaa sekä tietojen salausta että eheyden ja alkuperän varmistamista Internet-yhteyksissä. ESP:n tarkoitus on suojata IP-paketin sisältämät tiedot ja mahdollistaa turvallinen tiedonsiirto epäluotettavien verkkojen, kuten Internetin, kautta. ESP salaa IP-paketin sisällön, jotta ulkopuoliset tahot eivät voi lukea tai ymmärtää välitettyä tietoa. Salaus varmistaa tietojen yksityisyyden ja suojaa ne ulkopuolisten silmiltä. Tätä prosessia kutsutaan kapseloinniksi, jossa alkuperäinen IP-paketti kääritään uuden ESP-otsikon ja ESP-siirtotietojen sisään. (Kent, 2005, s. 8–9)

IKEv2(Internet Key Exchange Version 2) on protokolla, joka toimii yhdessä IPsecin kanssa. Se on vastuussa salausavaimen vaihdosta, joka on tarpeen IPsec-tunnelin luomiseksi. IKEv2

mahdollistaa turvallisen ja automaattisen vaiheittaisen prosessin, joka auttaa kahden laitteen turvallista tunnistamista ja avainten vaihtoa. IKEv2 on päivitetty versio avaimen vaihto protokollasta, se hyödyntää moderneja salausalgoritmeja ja varmistaa, että avaimet vaihdetaan turvallisesti. (Kaufman, 2005, s.2–3)

Avaimenvaihtoprosessi alkaa, kun laite pyytää toista laitetta muodostamaan turvallisen yhteyden. Osapuolet neuvottelevat turvallisuusparametreista, kuten salaus- ja todennusmenetelmistä. Kun sopivat parametrit on valittu, ne käyttävät Diffie-Hellman-avaimenvaihtoprotokollaa luomaan yhteisen salaisen avaimen. Tämän jälkeen molemmat osapuolet todentavat toisensa käyttäen sovittuja todentamismenetelmiä, kuten digitaalisia allekirjoituksia tai ennalta jaettuja avaimia. Kun avaimet on vaihdettu ja todennus suoritettu, turvallinen yhteys on muodostettu. IKEv2 tukee yhteyden jatkuvaa ylläpitoa ja pystyy uudistamaan avaimet ja neuvottelemaan turvallisuusparametrit uudelleen tarvittaessa. (Cisco, 2013)

2.3.2 SSL/TLSVPN

TLS on kryptografinen protokolla, jota käytetään turvaamaan tietoliikenne internetissä ja muissa tietoverkoissa. TLS-protokolla tarjoaa salauksen, joka suojaa tiedot luvattomalta pääsyltä tai tarkkailulta liikkuessaan verkossa. Se takaa myös tietojen eheyden ja varmistaa, että tietoliikenne ei ole muuttunut matkalla. TLS on käytännössä seuraaja SSL-protokollalle (Secure Sockets Layer). Alun perin TLS-protokolla kehitettiin parantamaan SSL:n tietoturvaa. Vaikka termi "SSL" on yhä laajalti käytössä, kun puhutaan verkkosivustojen salauksesta, käytännössä nykyään käytetään TLS-protokollaa. (OWASP, n.d.)

Kun Hypertext Transfer Protocol (HTTP) yhdistetään TLS-protokollaan, syntyy Hypertext Transfer Protocol Secure-yhteys (HTTPS), joka on suojattu ja salattu. Tässä prosessissa selain ja palvelin neuvottelevat yhteysasetuksista lähettämällä toisilleen tervehdysviestejä. Selain tarkistaa palvelimen varmenteen, jonka on myöntänyt luotettava sertifikaattien myöntäjä, varmistaakseen palvelimen aitouden. Tämän jälkeen selain luo satunnaisen salausavaimen ja lähettää sen palvelimelle salattuna palvelimen julkisella avaimella. Palvelin purkaa tämän avaimen käyttämällä omaa yksityistä avaintaan. Tämän vaiheen jälkeen kaikki lähetetty ja vastaanotettu tieto on salattu tällä symmetrisellä avaimella, mikä takaa tiedon luottamuksellisuuden ja eheyden. TLS-protokollaa käytetään laajasti verkkosivustojen suojauksessa mukaan lukien verkkokauppatapahtumat, sähköpostin salaaminen ja yleisesti kaikki muut tilanteet, joissa turvallisuus ja yksityisyys ovat tärkeitä. TLS:n eri versiot eroavat toisistaan käytetyissä salausalgoritmeissa ja muissa turvallisuuteen liittyvissä yksityiskohdissa. (Ilya Grigorik, n.d.)

TLS-protokollaa voidaan myös hyödyntää VPN-yhteyksissä. TLSVPN käyttää TLS-protokollaa luomaan salatun yhteyden käyttäjän laitteen ja VPN-palvelimen välille. Tämä tarkoittaa, että tietoliikenne näiden kahden pisteen välillä on salattua ja suojattua ulkopuolisilta tarkkailijoilta. TLSVPN-ratkaisut ovat yleensä helppokäyttöisempiä kuin esimerkiksi IPsec-ratkaisut. (Liu ym., 2006, s. 236–237)

2.4 Varmenteet

Varmenteet ovat digitaalisia sertifikaatteja tai todistuksia, jotka ovat keskeisiä internetin tietoturvassa. Ne toimivat digitaalisen identiteetin todentajina, ikään kuin sähköisinä henkilökortteina, varmistaen että olet yhteydessä oikeaan palveluun tai henkilöön. Varmenteita käytetään myös salatun yhteyden luomiseen, esimerkiksi verkkoselaimen ja palvelimen välillä, mikä suojaa tiedonsiirtoa ulkopuolisten pääsyltä. Nämä varmenteet myöntävät ja allekirjoittaa luotettu taho, kuten sertifiointiviranomainen (CA), joka varmistaa varmenteen haltijan identiteetin. Jokaisella digitaalisella varmenteella on määritelty alku- ja päättymispäivä. Nämä päivämäärät määrittävät, milloin varmenne on ensimmäisen kerran käytettävissä ja milloin se lakkaa olemasta kelvollinen. Voimassaoloaika voi vaihdella lyhyestä ajanjaksosta esimerkiksi yksi kuukausi, useisiin vuosiin ja ne täytyy uusia säännöllisesti pysyäkseen voimassa ja luotettavina. Varmenteen voimassaoloajan asettaa varmenteen myöntäjä, joka on yleensä luotettu sertifikaattien myöntäjä. Varmenteet ovat siis olennainen osa nykyaikaista digitaalista tietoturvaa, suojaten yksityisyyttä ja turvaten tietojen siirron verkossa. (Okta, 2023.)

2.5 Virtuaaliverkot

Virtuaaliverkko (Virtual Network) on verkko, joka on luotu ohjelmistopohjaisesti ja joka toimii fyysisten verkkojen päällä. Virtuaaliverkot mahdollistavat tietokoneiden, palvelinten ja muiden laitteiden kommunikoinnin keskenään samassa fyysisessä verkossa tai maantieteellisesti hajautetuissa ympäristöissä, kuten eri toimipisteiden välillä, käyttäen internetiä tai muita verkkoja. Virtuaaliverkoissa fyysiset verkkolaitteet, kytkimet, reitittimet ovat korvattu ohjelmistopohjaisilla ratkaisuilla, virtualisoimalla nämä laitteet. (VMware, n.d.)

2.6 Pilvipalvelut

Pilvipalvelut viittaavat erilaisiin palveluihin ja resursseihin, jotka ovat saatavilla internet-yhteyden avulla, sen sijaan että ne olisivat paikallisesti omassa tietokoneessa tai organisaation palvelimilla. Pilvipalvelut tarjoavat useita etuja, kuten joustavuus, ketteryys ja kustannustehokkuus. Pilvipalveluita voi skaalata tarpeen mukaan ylös tai alas, mikä mahdollistaa joustavuuden liiketoiminnan tarpeisiin. Pilvipalvelut tarjoavat helpon pääsyn monenlaisiin teknologioihin, kuten laskenta, tallennus ja tietokannat, esineiden Internetiin, koneoppimiseen ja analytiikkaan. Pilvipalvelut ovat kustannustehokkaampia, koska yritysten ei tarvitse investoida omaan infrastruktuuriin sekä sen ylläpitoon ja maksat vain siitä mitä käytät. (Amazon, n.d.)

3 Microsoft Azure

Microsoft Azure on Microsoftin tarjoama pilvipalvelualusta, joka tarjoaa laajan valikoiman pilvipalveluita ja -resursseja, kuten laskentaa, tallennusta, tietokantoja. Azure mahdollistaa sovellusten kehittämisen, testaamisen, käyttöönoton ja hallinnoinnin pilvessä. Yritykset voivat käyttää Azure-palveluja rakentaakseen, testatakseen ja käyttääkseen sovelluksiaan pilvessä, mikä tarjoaa joustavuutta, skaalautuvuutta ja kustannustehokkuutta liiketoiminnan tarpeisiin. Azurea voidaan hallita joko Azure portaalin kautta, osoitteesta azure.portal.com tai komentotulkin avulla, esim. Azure CLI, Powershell. (Microsoft, n.d.-b)

3.1 Azure VNET (virtuaaliverkko)

Azure-virtuaaliverkot (Azure Virtual Networks) ovat Azure-pilvipalvelussa olevia hajautettuja ja yksityisiä verkkoja. Nämä virtuaaliverkot mahdollistavat Azure-palveluiden ja resurssien turvallisen ja eristetyn käytön. Virtuaaliverkkojen avulla voit luoda omia erillisiä verkkoalueita Azure-pilvessä, jotka vastaavat organisaatiosi tarpeita.

Kun luot virtuaaliverkon Azure-palvelussa, voit määrittää sen IP-osoiteavaruuden, aliverkot, reitityssäännöt ja muut verkon asetukset. Virtuaaliverkot voivat myös olla yhteydessä toisiin Azure-verkkoihin tai muihin verkkoihin, kuten organisaatiosi olemassa olevaan sisäiseen verkkoon (Site-to-Site VPN) tai yksittäisten käyttäjien tai etätoimipisteiden laitteisiin (Point-to-Site VPN). (Microsoft, 2023d)

3.2 Azure VPN-palvelut

Azure tarjoaa useita erilaisia verkkojen yhdistämisratkaisuja. Tässä osioissa käydään läpi tämän työn osalta tärkeimmät ja relevantit palvelut.

3.2.1 VPN Gateway

Azure VPN Gateway on palvelu, joka käyttää virtuaalista verkkoyhdyskäytävää salatun liikenteen lähettämiseen Azure-virtuaaliverkon ja paikallisen ympäristön välillä julkisen internetin kautta. VPN gateway mahdollistaa myös salatun liikenteen Azuressa olevien virtuaaliverkkojen välillä. Azure tarjoaa useaa erilaista mallia, joiden ominaisuudet vaihtelevat. Muuttuvina ominaisuuksina on muun muassa VPN-tunnelien määrä, nopeus ja reititys ominaisuudet. VPN gatewayn hinta nousee mitä paremmat ominaisuudet sillä on. Tämän työn osalta relevantit tyypit ovat Basic, VpnGw1. VPN tyypin vaihtaminen pienempään tai suurempaan, jotka ovat samaa sukupolvea, onnistuu ilman isoa katkoa VPN yhteyksissä kaikilta muilta, paitsi Basic mallia ei pysty vaihtamaan ilman että pitää luoda kokonaan uusi VPN gateway. Kuvassa 3 sivulla 9 on esitetty kaikki Azuren tarjoamat Gateway mallit, kirjoitushetkellä joulukuu 2023. (Microsoft, 2023b)

Kuva 3. Eri VPN Gateway tyypit (Microsoft, 2023d)

VPN Gateway Generation	SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput Benchmark	BGP	Zone-redundant	Supported Number of VMs in the Virtual Network
Generation1	Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported	No	200
Generation1	VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	No	450
Generation1	VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	No	1300
Generation1	VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	No	4000
Generation1	VpnGw1AZ	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	Yes	1000
Generation1	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	Yes	2000
Generation1	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	Yes	5000
Generation2	VpnGw2	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported	No	685
Generation2	VpnGw3	Max. 30	Max. 128	Max. 1000	2.5 Gbps	Supported	No	2240
Generation2	VpnGw4	Max. 100*	Max. 128	Max. 5000	5 Gbps	Supported	No	5300
Generation2	VpnGw5	Max. 100*	Max. 128	Max. 10000	10 Gbps	Supported	No	6700
Generation2	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported	Yes	2000
Generation2	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	2.5 Gbps	Supported	Yes	3300
Generation2	VpnGw4AZ	Max. 100*	Max. 128	Max. 5000	5 Gbps	Supported	Yes	4400
Generation2	VpnGw5AZ	Max. 100*	Max. 128	Max. 10000	10 Gbps	Supported	Yes	9000

3.2.2 Point-to-site

Azuressa Point-to-Site VPN (P2S VPN) on VPN-ratkaisu, joka mahdollistaa yksittäisten laitteiden tai käyttäjien turvallisen yhteyden Azure-verkkoon internetin yli. Tämä tarkoittaa sitä, että etätyöntekijät, etätoimipisteet tai muut yksittäiset laitteet voivat turvallisesti muodostaa yhteyden Azure-verkkoon ja käyttää sen resursseja, kuten virtuaalikoneita, tallennustilaa tai tietokantoja, salatun yhteyden kautta. P2S VPN:ssä käyttäjän tietokoneelle tai muulle laitteelle asennetaan VPN-asiakasohjelmisto, joka mahdollistaa salatun yhteyden muodostamisen Azuren virtuaaliverkkoon. (Microsoft, 2023a)

3.2.3 Site-to-Site

Azuressa Site-to-Site VPN (S2S VPN) on VPN-ratkaisu, joka mahdollistaa kahden tai useamman erillisen verkon välillä turvallisen ja salatun yhteyden. Tämä tarkoittaa, että

organisaation sisäiset verkot voivat olla turvallisesti yhteydessä Azuren virtuaaliverkkoon internetin yli. Organisaation verkkoon asennetaan VPN-reititin tai VPN-laitteisto, joka on konfiguroitu luomaan turvallinen yhteys Azureen. Tämä mahdollistaa organisaation resurssien, kuten palvelinten, tietokantojen ja muiden laitteiden, turvallisen käytön Azuren virtuaaliverkossa olevien palveluiden kanssa. (Microsoft, 2023c)

3.3 Entra ID

Entra ID on Microsoftin tarjoama pilvipohjainen identiteetinhallintapalvelu. Se on Azure-pohjainen versio perinteisestä Active Directory -palvelusta, jota useimmat organisaatiot käyttävät paikallisessa verkossaan. Se tarjoaa useita identiteetin- ja pääsynhallintatoimintoja pilvessä sijaitsevien sovellusten, palveluiden ja resurssien turvalliseen hallintaan. Sitä käytetään organisaatioissa käyttäjien, ryhmien ja laitteiden identiteettien hallintaan sekä käyttöoikeuksien määrittämiseen eri sovelluksiin ja palveluihin. Entra ID mahdollistaa turvallisen ja hallitun tavan hallita käyttäjiä ja heidän pääsyoikeuksiaan pilviympäristöissä ja yritysverkoissa. Se tarjoaa muun muassa kertakirjautumis (SSO) mahdollisuuden, joka helpottaa käyttäjien kirjautumista eri sovelluksiin yhdellä kirjautumisella. Entra ID sisältää myös tietoturvatoimintoja, kuten monivaiheinen tunnistautuminen (MFA), joka parantaa organisaation tietoturvaa. Entra ID tunnettiin aiemmin nimellä Azure Active Directory. Microsoft aloitti nimen muutos prosessin kesäkuussa 2023, jonka on tarkoitus olla valmiina vuoden 2023 loppuun mennessä. (Microsoft, 2023g)

3.4 Kustannukset

Azuren tarjoamien VPN ratkaisuiden kustannukset koostuvat VPN gatewayn mallista sekä Azuresta ulospäin lähtevästä liikenteestä. Liikenteestä ensimmäiset 100 gigatavua / kk ovat ilmaiset, tämä on jaettuna kaikille käyttäjille, jotka käyttävät samaa VPN gatewaytä. (Microsoft, 2023b)

Kustannuksia laskiessa, pitää ottaa huomioon se, että kun VPN gateway on luotu, se on aina päällä sitä ei voi pysäyttää esim. viikonlopuiksi tai loma-ajoiksi. Pelkästään VPN-gateway tulee maksamaan joko Basic-malli 28,8 € / kk tai VPNGw1-malli 129,4 € / kk. Kuvassa 4 näkyvät Basic ja VPNGw1-mallien kustannukset.

Kuva 4. VPN gatewayn kustannukset. (Microsoft, n.d.-a)

VPN Gateway Type	Price	Bandwidth	S2S Tunnels	P2S Tunnels
Basic	€0.04/hour	100 Mbps	Max 10 1-10: Included	Max 128 1-128: Included
VpnGw1	€0.1797/hour	650 Mbps	Max 30 1-10: Included 11-30: €0.015/hour per tunnel	Max 250 1-128: Included 129-250: €0.010/hour per connection

Dataliikenteen määrää on vaikea arvioida ja tästä tulevia kustannuksia on hankala laskea. Kustannuslaskelmia laskiessa käytin dataliikenne määränä omaa työpäivän aikana liikkuvaa datan määrää. Seurasin omaa datan käyttöä työpäivän aikana, joka oli keskimäärin 1,1 Gt per päivä. Keskiarvona laskettuna 21.5 työpäivällä se on 21,5 * 1,1 = 23,65 Gt. Tällä datamäärällä tuo ilmainen 100 Gt riittää neljälle käyttäjälle. Laskelmat on laskettu 23,65 Gt datamäärällä per käyttäjä.

Taulukko 1 Kustannuslaskelma.

Käyttäjämäärä	Datan määrä / Gt	Yli 100Gt rajan kustannukset	Basic / 28,8 €	VPNGw1 / 129,4 €
1–5	23,65–118,25	1,38 €	30,18 €	130,78 €
6–10	141,9–236,5	3,17 € - 10,33 €	31,97 € - 39,13 €	132,57 € - 139,73 €
11–20	260,15–473	12,12 € - 28,24 €	40,92 € -57,04 €	141,51 € - 157,64 €

50	1182	81,15 €	109,95 €	210,55 €

Basic-mallin kustannukset ovat maltilliset. Pienemmille yrityksille tai testaukseen, joissa ei ole tarvetta suurille resursseille tai erikoisominaisuuksille, Basic-malli tarjoaa taloudellisesti järkevän ratkaisun. Tämä voi olla houkutteleva vaihtoehto, erityisesti aloitteleville yrityksille tai projekteille, joissa budjetti on rajallinen. Kuitenkin, jos Basic-mallia käytetään tilanteissa, jossa samanaikaisia käyttäjiä on yli viisi, sen tarjoama 100 Mbps:n nopeus ei ole riittävä. Nopeus voi olla riittävä pienemmille tiimeille tai vähemmän datan siirtoa vaativille sovelluksille, mutta kun käyttäjien määrä kasvaa, tämä rajoitus alkaa haitata verkon suorituskykyä. Basic-mallissa, point-to-site-yhteyksissä ainoa saatavilla oleva tunnistautumismenetelmä on varmennepohjainen. Tämä tarkoittaa, että käyttäjien täytyy käyttää digitaalisia varmenteita todistaakseen identiteettinsä ja saadakseen pääsyn verkkoon. Vaikka varmennepohjainen tunnistautuminen on turvallinen menetelmä, se voi olla rajoittava, jos organisaatiossa tarvitaan monipuolisempia tunnistautumismenetelmiä, kuten kaksivaiheista tunnistautumista tai muita käyttäjätunnistusmekanismeja.

VPNGw1-mallin kustannukset ovat huomattavasti suuremmat kuin Basic-mallin. Tämä tarkoittaa, että taloudellinen investointi VPNGw1:een on merkittävä, ja se on tärkeä tekijä, erityisesti budjettitietoisille organisaatioille. Tämän kustannuseron syy on VPNGw1-mallin tarjoamat lisäominaisuudet ja parempi suorituskyky. Toisin kuin Basic-malli, VPNGw1 tarjoaa nopeamman yhteyden. Tämä nopeampi yhteys on erityisen tärkeä suuremmille käyttäjämäärille tai sovelluksille, jotka vaativat paljon datan siirtoa ja nopeaa yhteysnopeutta. Nopeampi yhteys parantaa käyttäjäkokemusta, vähentää viivettä ja mahdollistaa suuremman datamäärän käsittelyn lyhyemmässä ajassa. VPNGw1-malli tarjoaa useampia vaihtoehtoja käyttäjien tunnistautumiseen, mikä on tärkeää organisaatioille, jotka tarvitsevat joustavuutta ja monipuolisuutta turvallisuusratkaisuissaan. Näihin vaihtoehtoihin kuuluvat esimerkiksi kaksivaiheinen tunnistautuminen, Entra ID -pohjainen tunnistautuminen. Tämä monipuolisuus parantaa verkkojen turvallisuutta ja käyttäjäystävällisyyttä, mahdollistaa paremman käyttäjien hallinnan ja auttaa vastaamaan erilaisiin turvallisuusvaatimuksiin.

4 Toteutus

Tämä on opinnäytetyön toiminnallinen osuus. Tässä osiossa toteutetaan kaikki työn 3 eri VPN-ratkaisua. Ratkaisuiden konfigurointi kuvataan ja toimivuus testataan. Osiossa käsitellään nimenomaan vain VPN:än toimintaan liittyvät asiat.

Kaikissa toteutuksissa on käytetty Azuren ilmaista tiliä, jolla saadaan 30 päivän ajaksi käytettäväksi Azuren palveluihin 200 $. Lisäksi käytössä oli Windows 10 virtuaalityöasema, joka virtualisoitiin VMware Workstationissa.

VPN-yhteyden toimivuus testattiin niin että Azuressa olevaan virtuaalikoneeseen otettiin RDP-yhteys VPN-yhteyden muodostamisen jälkeen. Virtuaalikoneella ei ollut julkista IP-osoitetta, joten siihen ei saanut RDP-yhteyttä otettua suoraan internetin ylitse.

4.1 Point-to-Site VPN – Varmennepohjainen tunnistautuminen

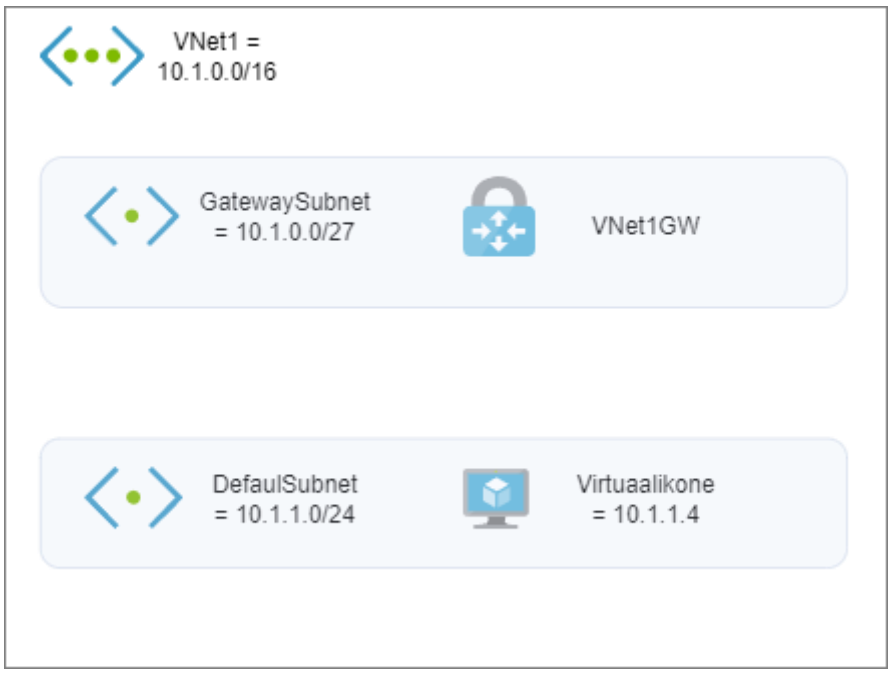
Tässä toteutetaan Remote-access yhteys, eli työasema liitetään VPN-yhteyden avulla Azuren virtuaaliverkkoon. Tässä toteutuksessa käyttäjä tunnistetaan sertifikaatin avulla.

VPN gatewayn tyypiksi valittiin Basic, joka valittavista gateway-malleista halvin ja ominaisuuksiltaan heikkotasoisin. Basic gatewayn luominen ei onnistu suoraan Azure Portalista, vaan se pitää luoda Azure CLI:n tai Powershellin kautta. Toimivaa VPN-yhteyttä varten pitää Azureen luoda virtuaaliverkko, johon VPN-gateway luodaan, näiden tulee olla samassa Azure-alueessa. Virtuaaliverkolle täytyy antaa nimi ja sille pitää määrittää oma verkkoalueensa sekä aliverkot, myös gateway tarvitsee oman aliverkkonsa, VPN gateway tarvitsee myös julkisen IP-osoitteen. Virtuaaliverkko luotiin alueelle ”northeurope” ja verkon osoitealue on 10.1.0.0/16 ja tälle määritettiin aliverkot 10.1.0.0/27 ja 10.1.1.0/24. Sivulla 14 Kuvissa 5 ja 6 näkyvät virtuaaliverkon ja gatewayn luonnin määritykset, sekä verkkotopologia.

Kuva 5. Basic VPN-gateway määritykset.

```
$location = "northeurope"
$resourceGroup = "VNet1Test"
$vnetAddressSpace = "10.1.0.0/16"
$gatewaySubnet = "10.1.0.0/27"
$defaultSubnet = "10.1.1.0/24"
New-AzResourceGroup -Name $resourceGroup -Location $location
$subnetConfig = New-AzVirtualNetworkSubnetConfig -Name GatewaySubnet -AddressPrefix $gatewaySubnet
$subnetConfig2 = New-AzVirtualNetworkSubnetConfig -Name Default -AddressPrefix $defaultSubnet
$vngwPIP = New-AzPublicIpAddress -Name VNet1GWpip -ResourceGroupName $resourceGroup -Location $location -Sku Basic -
AllocationMethod Dynamic
$vnet = New-AzVirtualNetwork -Name VNet1 -ResourceGroupName $resourceGroup -Location $location -AddressPrefix
$vnetAddressSpace -Subnet $subnetConfig $subnetConfig2
$subnet = Get-AzVirtualNetworkSubnetConfig -Name GatewaySubnet -VirtualNetwork $vnet
$vngwIpConfig = New-AzVirtualNetworkGatewayIpConfig -Name vngwipconfig -SubnetId $subnet.Id -PublicIpAddressId $vngwPIP.Id
New-AzVirtualNetworkGateway -Name VNet1GW -ResourceGroupName $resourceGroup -Location $location -IpConfigurations
$vngwIpConfig -GatewayType Vpn -VpnType RouteBased -GatewaySku Basic
```

Kuva 6. Azuren verkkotopologia.



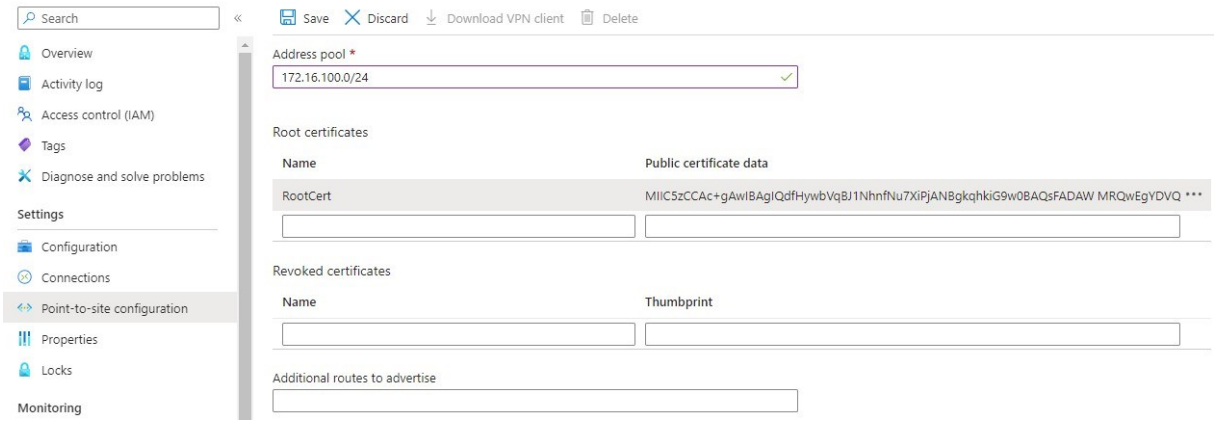
VPN-yhteyden muodostamista varten käyttäjät täytyy tunnistaa. Tunnistautumista varten Azure portaaliin pitää viedä juurivarmenne, jota vasten käyttäjät tunnistautuvat. Tässä työssä käytettiin Self signed -varmennetta, joka sopii testiympäristöihin, mutta tuotantoympäristöissä on syytä käyttää luotettua varmenteiden myöntäjää (Certificate Authtority). Varmenteen luominen onnistuu Windows-ympäristössä Powershelillä kuvassa 7 näkyvillä komennoilla. Varmenne pitää vielä avata selkokieliseksi, jotta se voidaan viedä Azureen. Tämä onnistuu Windows-ympäristössä, Certificate Export Wizard -työkalulla, seuraamalla työkalun ohjeita.

Kuva 7. Juurivarmenteen luonti.

```
PS C:\Users\PC> $params = @{
>>      Type = 'Custom'
>>      Subject = 'CN=P2SRootCert'
>>      KeySpec = 'Signature'
>>      KeyExportPolicy = 'Exportable'
>>      KeyUsage = 'CertSign'
>>      KeyUsageProperty = 'Sign'
>>      KeyLength = 2048
>>      HashAlgorithm = 'sha256'
>>      NotAfter = (Get-Date).AddMonths(24)
>>      CertStoreLocation = 'Cert:\CurrentUser\My'
>> }
PS C:\Users\PC> $cert = New-SelfSignedCertificate @params
```

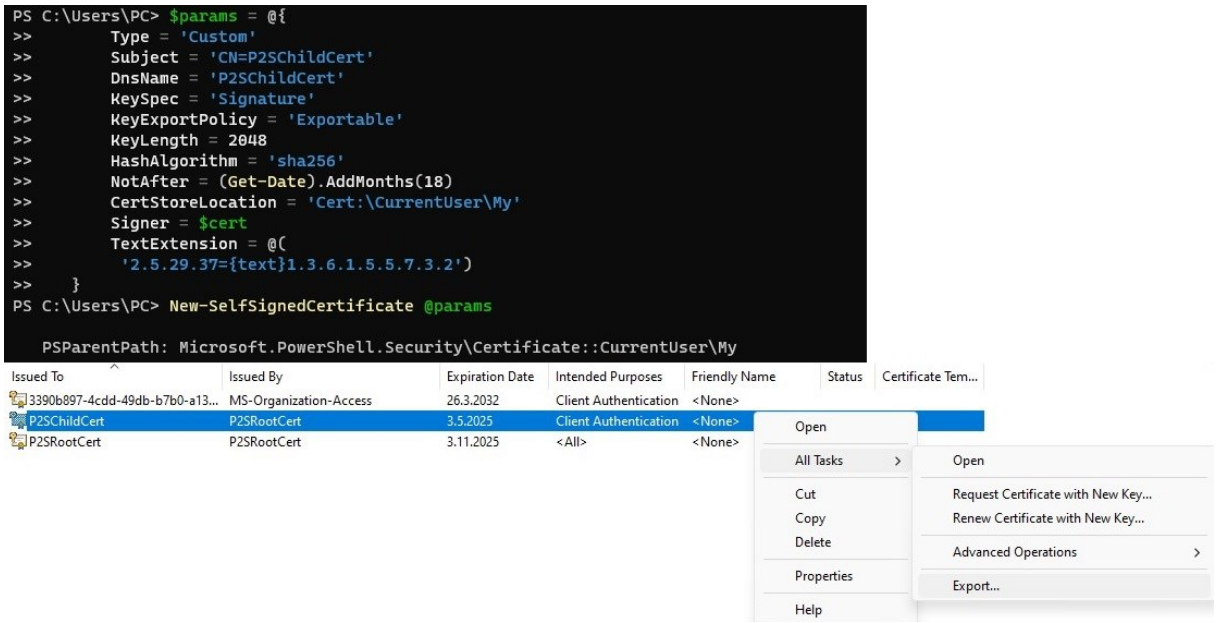
Azure portalissa konfiguroidaan point-to-site yhteys, johon pitää määrittää VPN-käyttäjien osoitealue sekä juurivarmenteen tiedot. Kuvassa 8 näkyy Point-to-site yhteyden konfiguraatio.

Kuva 8. Point-to-site konfiguraatio.



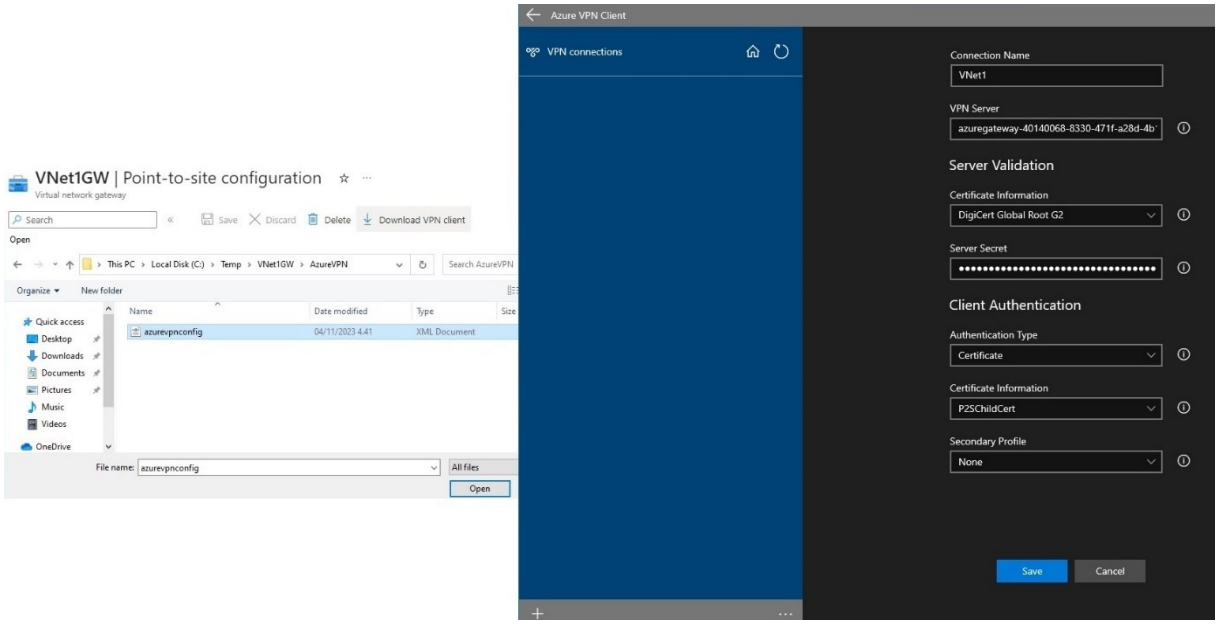
Tässä kohtaa on konfigurointi Azuren osalta valmis, seuraavaksi siirrytään työaseman konfiguraatioon ja vpn-yhteyden muodostamiseen. Jokainen käyttäjä tarvitsee varmenteen työasemalleen, jotta vpn-yhteyden muodostaminen onnistuu. Tämä on tämän toteutuksen hallinnan kannalta hankalin ja työläin osuus, varsinkin jos käyttäjiä on monta. Käyttäjävarmenne luodaan juurivarmenteen pohjalta. Varmenteen luominen onnistuu Windows-ympäristössä Powershelillä kuvassa 9 sivulla 16 näkyvillä komennoilla. Käyttäjävarmenne pitää viedä jokaiselle työasemalle ja asentaa erikseen.

Kuva 9. Käyttäjävarmenteen luonti.



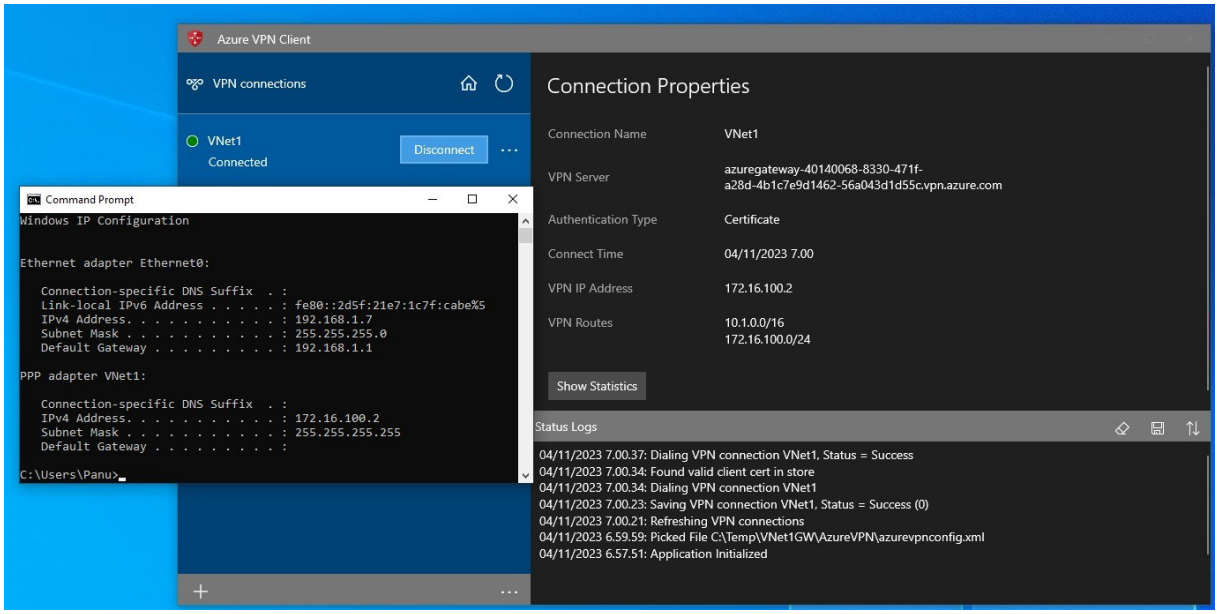
Kun käyttäjävarmenne on luotu ja tallennettu, se pitää viedä työasemalle ja asentaa. Työasemalle pitää myös asentaa Azure VPN Client sovellus, tämän saa ladattua Microsoft Storesta tai Microsoftin sivuilta. VPN sovellukseen pitää tuoda VPN-yhteyden konfiguraatiot, ne löytyvät Azure Portalista, konfiguraatiotiedot löytyvät azurevpnconfig.xml tiedostosta, jotka voidaan tuoda suoraan VPN sovellukseen. Tämä näkyy kuvassa 10.

Kuva 10. VPN asetusten vienti.



VPN-asetusten määrityksen jälkeen, kuvassa 11 näkyy että yhteys muodostui ja RDP-yhteyden ottaminen Azuren virtuaaliverkossa olevaan koneeseen onnistui.

Kuva 11. VPN-yhteyden testaaminen.

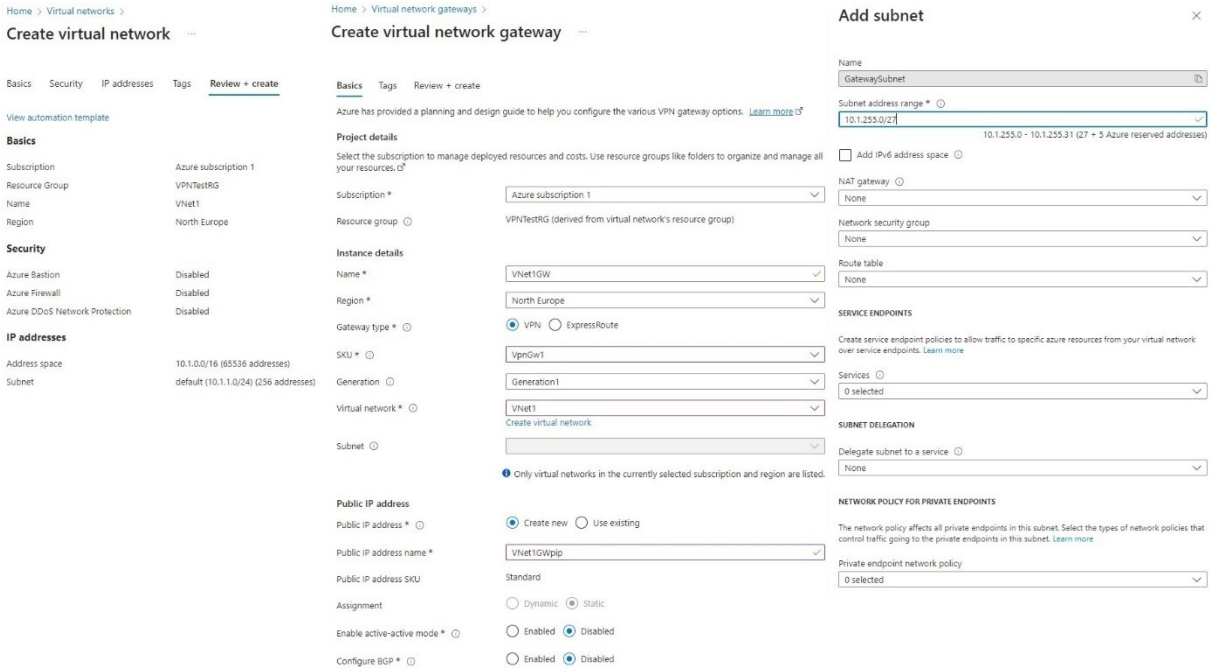


4.2 Point-to-Site VPN - EntraID tunnistautuminen

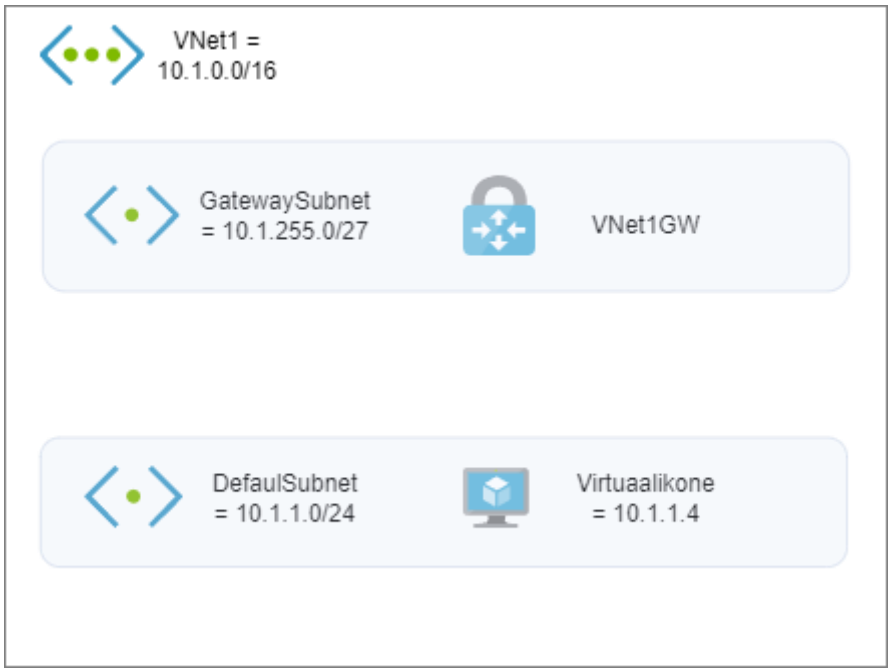
Tässä toteutetaan Remote-access yhteys, eli työasema liitetään VPN-yhteyden avulla Azuren virtuaaliverkkoon.

Tässä toteutuksessa käyttäjä tunnistetaan Entra ID:n avulla. Tähän toteutukseen valittiin VpnGw1 malli siitä syystä, että siihen on mahdollista konfiguroida Entra ID tunnistautuminen, tätä mahdollisuutta Basic-tyypissä ei ole. Jos aiemman toteutuksen malli olisi ollut VpnGw1, niin olisimme voineet vain muokata P2S-yhteyden konfiguraatiota ja lisätä mahdollisuuden Entra ID tunnistautumiselle. VpnGw1 luonti on mahdollista tehdä Azure Portalin tai Cli komentorivitulkin kautta, tässä demonstroidaan, kuinka se onnistuu Azure Portalin kautta. Tässäkin aluksi pitää luoda Azureen virtuaaliverkko johon VPN gateway luodaan. Virtuaaliverkolle täytyy antaa nimi ja sille pitää määrittää oma verkkoalueensa sekä aliverkot, myös gateway tarvitsee oman aliverkkonsa, VPN Gateway tarvitsee myös julkisen IP-osoitteen. Virtuaaliverkko luotiin alueelle ”northeurope” ja verkon osoitealue on 10.1.0.0/16 ja tälle määritettiin aliverkot 10.1.255.0/27 ja 10.1.1.0/24. Sivulla 18 kuvissa 12 ja 13 näkyy virtuaaliverkon ja gatewayn luonti sekä verkkotopologia.

Kuva 12. Virtuaaliverkon ja gatewayn luonti.



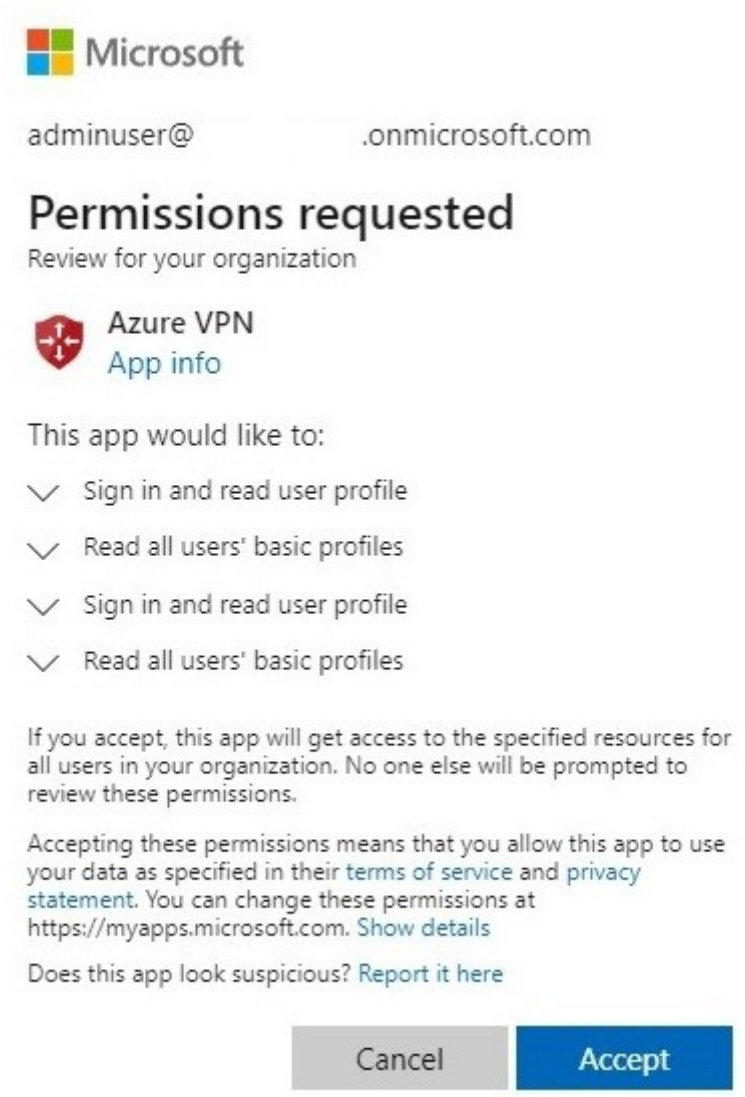
Kuva 13. Azuren verkkotopologia



Ennen P2S yhteyden konfigurointia, pitää ottaa käyttöön Microsoft Entra ID ja Azure VPN sovellukselle pitää antaa oikeudet kirjautua ja lukea käyttäjien tietoja. Azure Portalin haulla haettiin Microsoft Entra ID ja luotiin uusi tenant, lisensointi versio oli ilmainen. Ilmaisversio aiheutti jotain hankaluuksia käyttäjien hallintaa ajatellen, mutta tähän testiversioon se oli ihan riittävä. Samalla luotiin testikäyttäjä sekä admin-käyttäjä. Azure VPN sovelluksen luvitus

onnistuu helposti, Microsoftin dokumentaatiosta löytyvä suoran linkin kautta. Luvat antaakseen pitää Admin-käyttäjän kirjautua sisään Azure Portaliin. Kuvassa 14 näkyy luvituskysely. Luvituksen jälkeen VPN sovellus näkyy Microsoft Entra ID:ssä Enterprise applications kohdan alla.

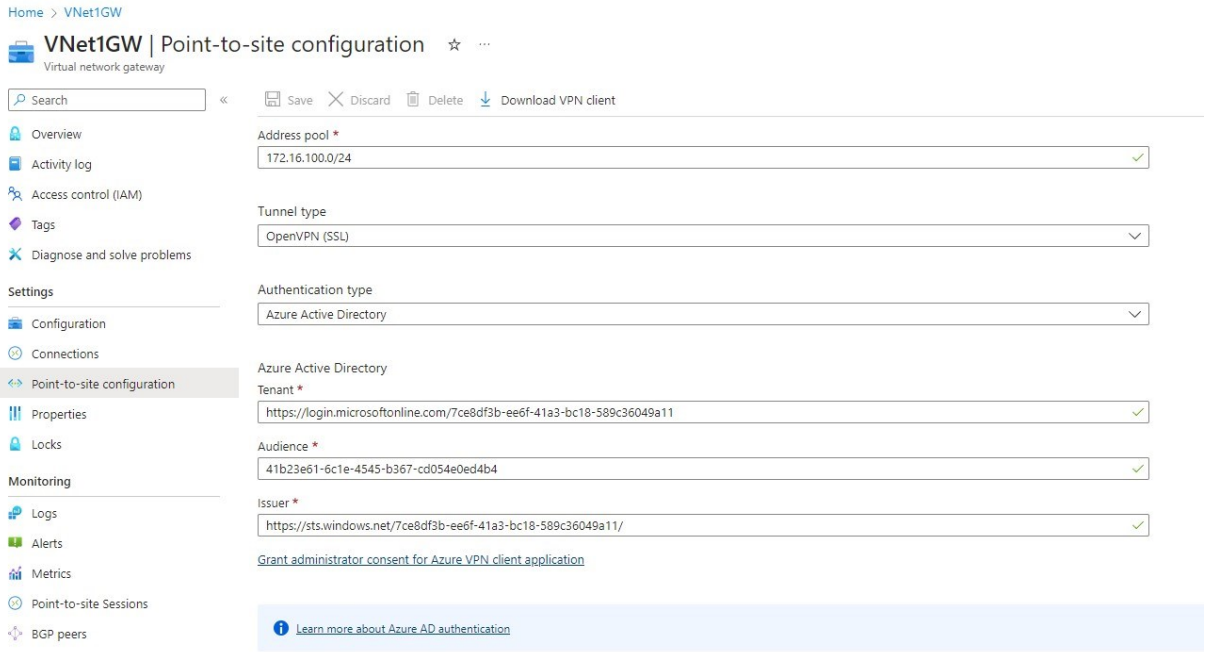
Kuva 14. VPN sovelluksen luvitus.



Luvituksen jälkeen pitää antaa myös käyttäjille pääsy VPN sovellukseen, Microsoft suosittelee, että luvat annettaisiin ryhmän kautta, eikä suoraan yksittäisille käyttäjille. (Microsoft, 2022) Tässä vastaan tuli ilmaisen version rajallisuus, ilmaisversiossa ei ole mahdollista luvittaa sovelluksen käyttöä ryhmän kautta vain suoraan yksittäisille käyttäjille.

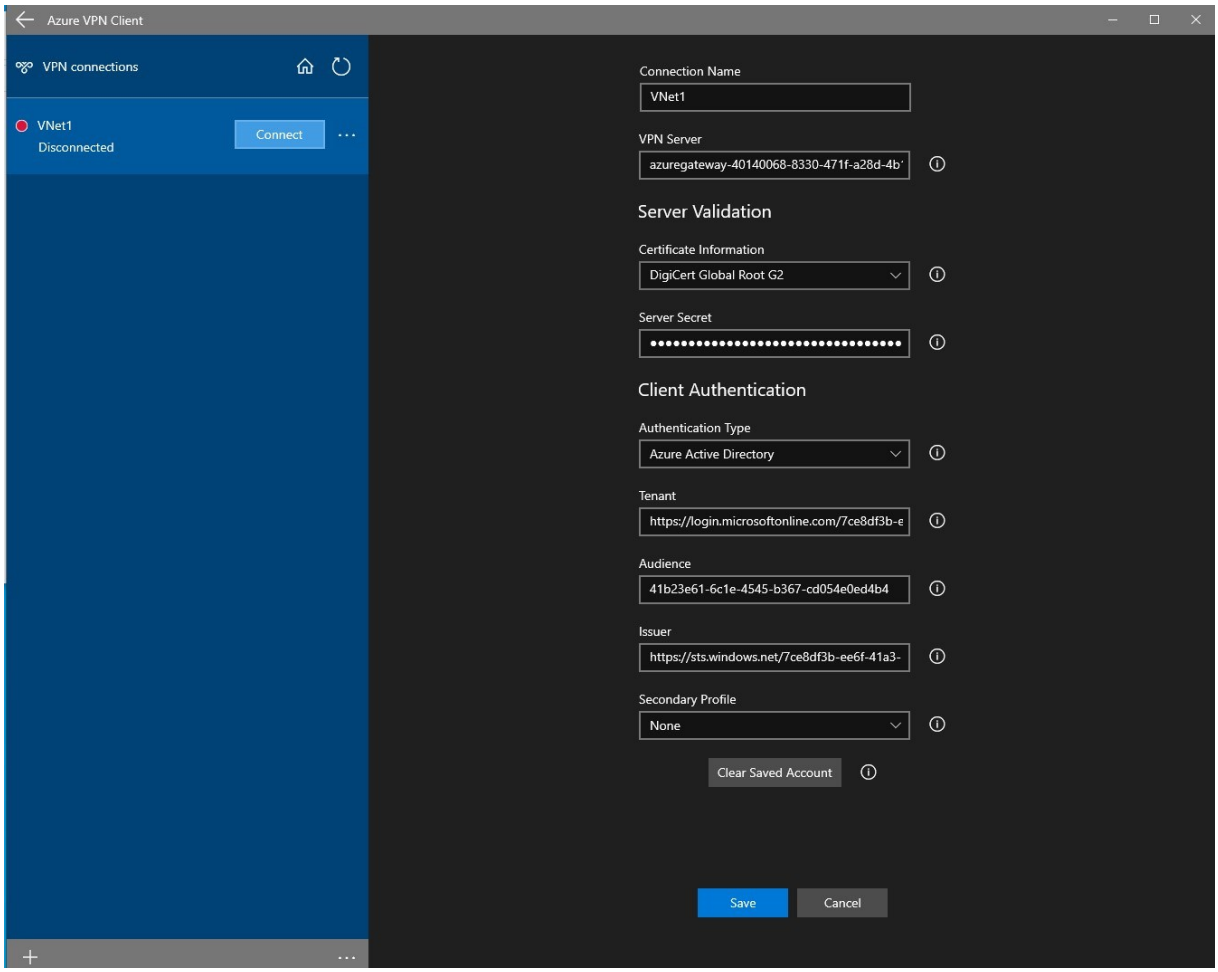
Seuraavaksi oli vuorossa point-to-site yhteyden konfigurointi. Yhteydelle pitää määrittää käyttäjien osoitealue, tunnelin tyyppi, autentikointi tapa, sekä Entra ID:n tiedot. Kuvassa 15 näkyy määritykset. Entra ID:n tiedot löytyvä helposti Microsoftin dokumentaatiosta.

Kuva 15. P2S-yhteyden konfigurointi.



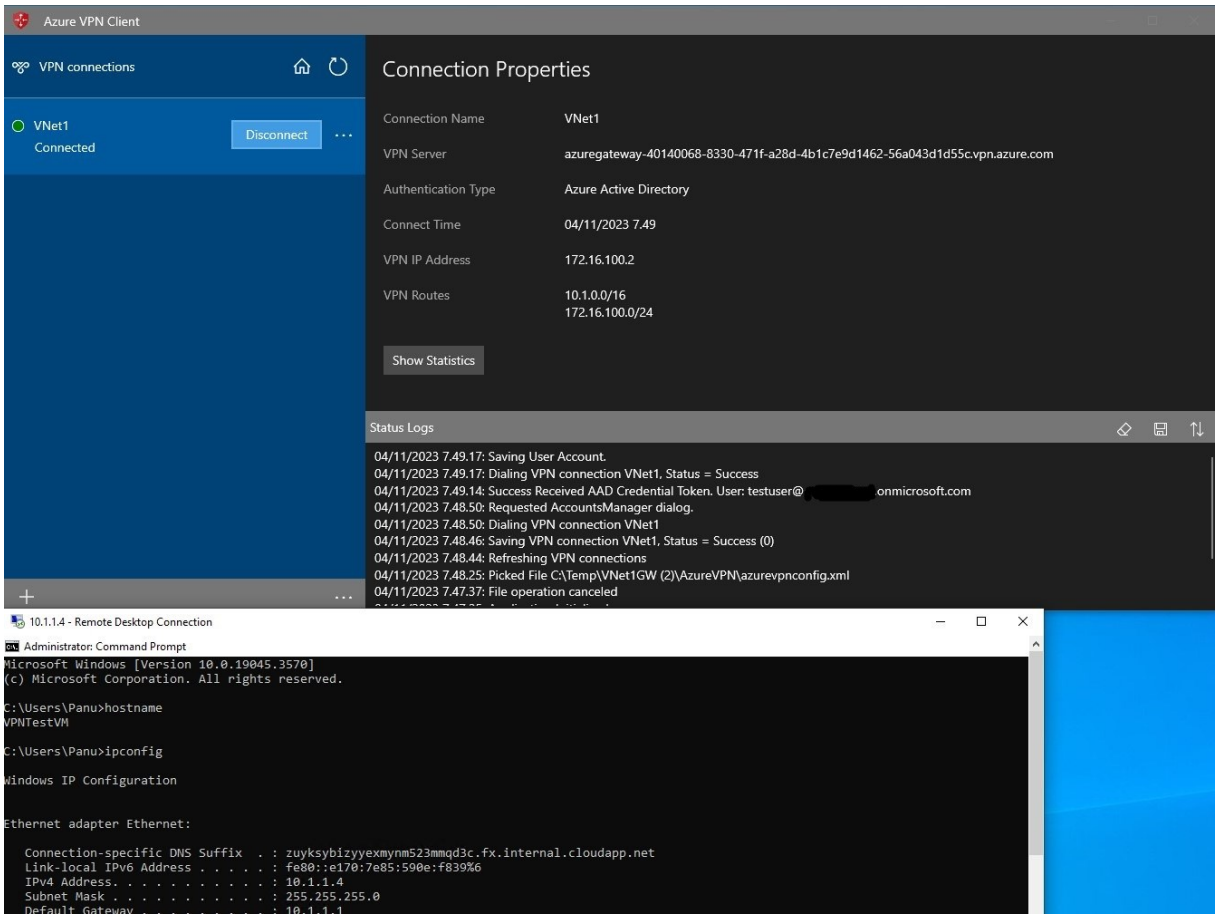
Tallennuksen jälkeen edetään samoin kuin aikaisemmassa toteutuksessa, eli ladataan VPN-yhteyden konfiguraatiot, jotka löytyvät Azure Portalista, konfiguraatiotiedot löytyvät azurevpnconfig.xml tiedostosta, joka tuodaan VPN sovellus. Kuvassa 16 sivulla 21 näkyy tuodut VPN-asetukset.

Kuva 16. VPN asetukset.



Yhteyden muodostamisessa tulee heti Microsoftin kirjautumisikkuna, jossa pyydetään syöttämään käyttäjätunnus ja salasana. Tunnusten syöttämisen jälkeen VPN-yhteys muodostuu. Kuvassa 17 sivulla 22 on esitetty muodostunut yhteys sekä RDP-yhteyden onnistuminen Azuren virtuaalikoneeseen.

Kuva 17. Onnistunut VPN-yhteys.

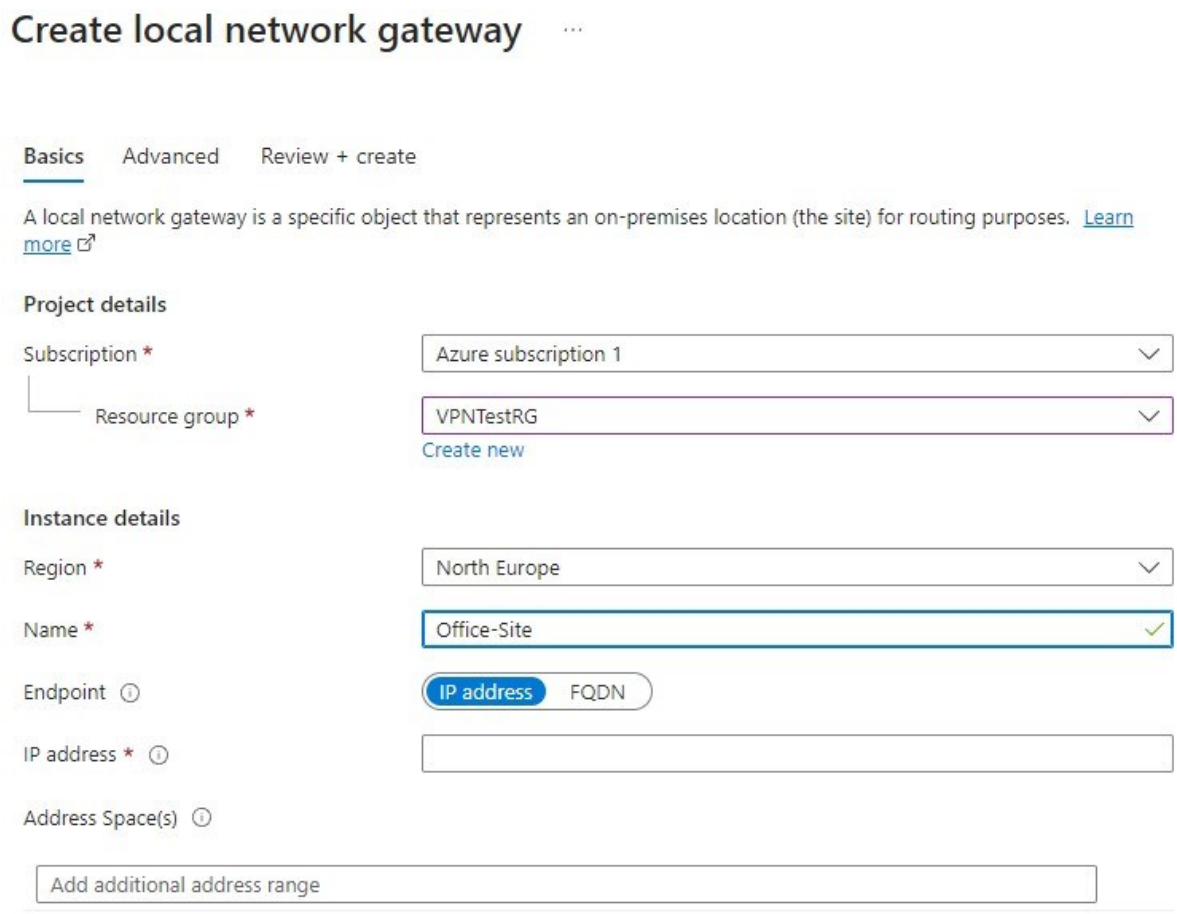


4.3 Site-to-Site VPN

Tässä toteutetaan Site-to-Site yhteys, eli koko toimistoverkko liitetään VPN-yhteyden avulla Azuren virtuaaliverkoon.

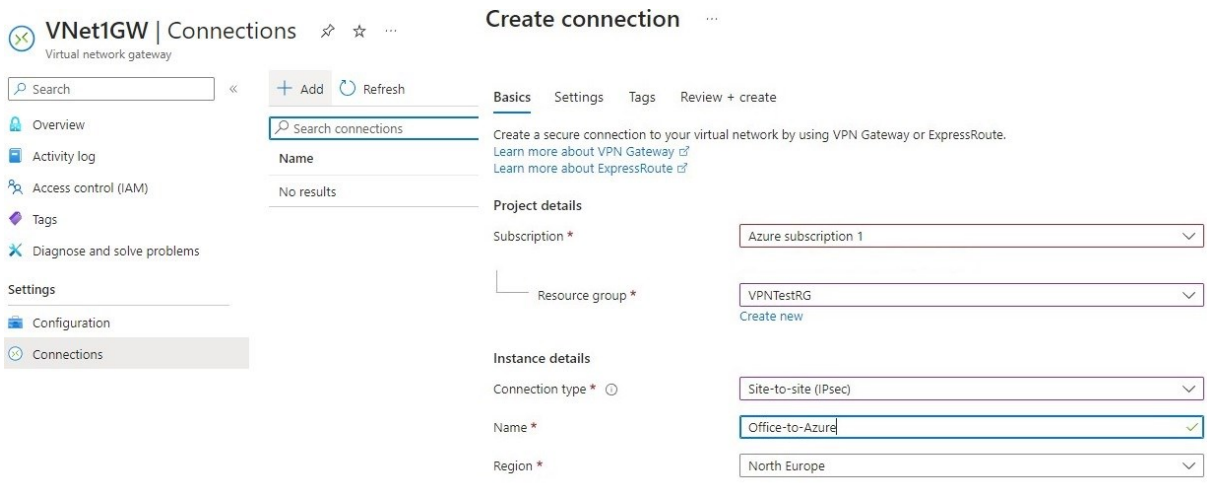
Tässä toteutuksessa voidaan käyttää myös VpnGw1 mallia, sekä voimme käyttää jo viimeksi luotua virtuaaliverkkoa sekä gatewaytä. Virtuaaliverkko on alueella ”northeurope” ja verkon osoitealue on 10.1.0.0/16 ja aliverkot 10.1.255.0/27 ja 10.1.1.0/24. Toteutuksessa on sama verkkotopologia kuin aikaisemmassa toteutuksessa. Topologia on esitelty kuvassa 13 sivulla 18. Gatewaylle tuli Azuren määrityksessä julkinen ip-osoite joka tarvitaan myöhemmässä vaiheessa toimiston vpn-laitteen konfigurointia varten. Lisäyksenä aiempiin toteutuksiin pitää Azuressa luoda Local network gateway, tämä edustaa toimistoverkon objektia, jota vasten yhteys luodaan. Local gatewayn luontia varten tarvitaan alue, johon se sijoitetaan, nimi, vpn-laitteen ip-osoite sekä toimistoverkon osoitealueet. Kuvassa 18 sivulla 23 on esitetty Local gateway asetukset.

Kuva 18. Local gateway määritykset.

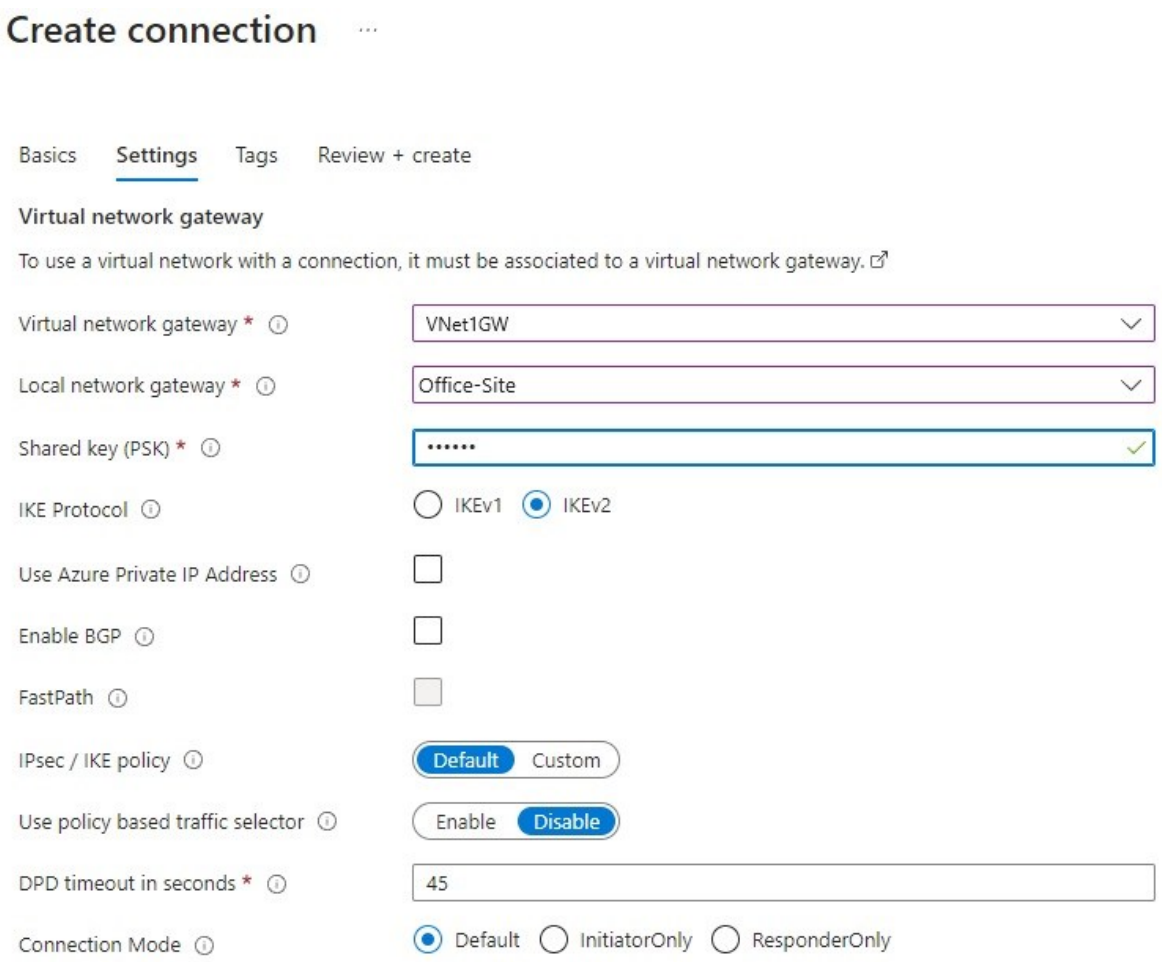


Tämän jälkeen luodaan itse site-to-site yhteys Azuressa. Se luodaan VPN gatewayn asetuksista, connection-kohdasta. Luontia varten yhteydelle pitää antaa yhteystyyppi, nimi, sijainti. Yhteyden asetuksista pitää vielä asettaa haluttu Virtual network gateway, Local network gateway sekä Shared key. Kuvissa 19 ja 20 sivulla 24 näkyvät nämä määritettyinä.

Kuva 19. Yhteyden konfigurointi.



Kuva 20. Site-to-site yhteyden asetukset.



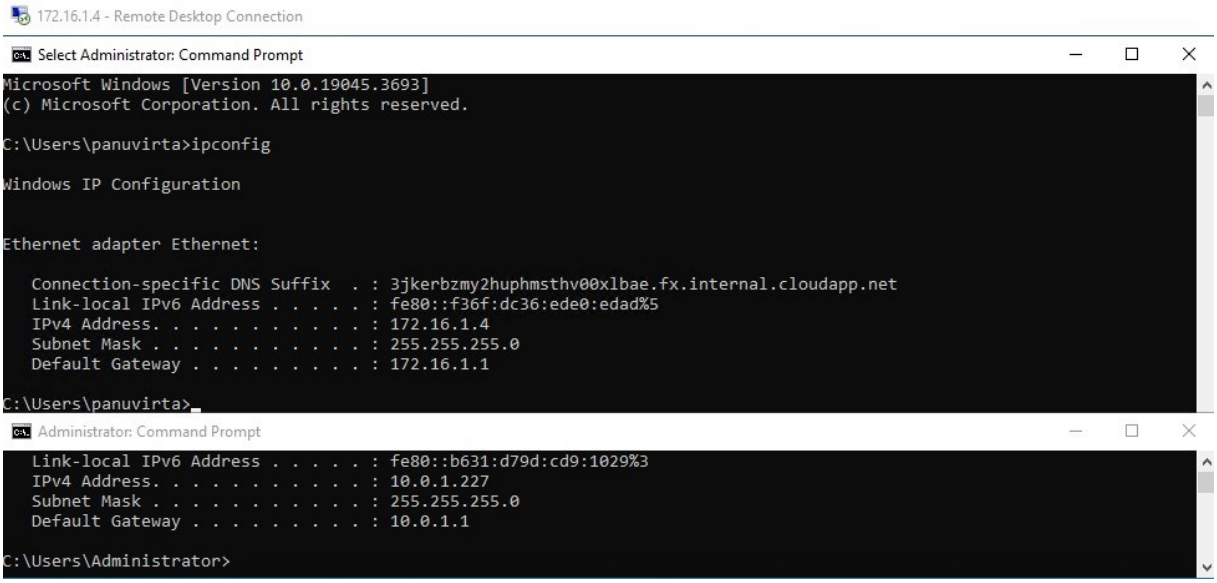
Seuraavaksi konfiguroitiin vpn-laitteelle site-to-site yhteys. Laitteena toimi PaloAlton palomuuri. Palomuurille pitää luoda tunnel-interface, security zone, IKE gateway-profiili,

IPsec tunneli. Konfiguroinnin jälkeen, pienen hetken kuluttua yhteys muodostuu. Azure Portalista näkyy, että tunneli on yhdistänyt. Kuvassa 21. näkyy että tunneli on yhdistänyt.

Kuva 21. Onnistunut S2S yhteys.

Nyt kun toimistoverkosta on luotu yhteys Azureen, niin erillistä konfigurointia työasemalle ei tarvinnut tehdä. Kuvassa 22 näkyy RDP-yhteyden onnistuminen Azuren virtuaalikoneeseen.

Kuva 22. Onnistunut RDP-yhteys.



5 Johtopäätökset ja pohdinta

Azure tarjoaa useita eri VPN-ratkaisuja, joista varmasti löytyy jokaiselle yritykselle sopiva ratkaisu. Perus VPN-yhteyden konfigurointi on melko simppeliä, mutta laajempien kokonaisuuksien rakentamiseen ja hallintaan vaaditaan syvempää osaamista Azure ympäristössä. Tarkkoja kustannuksia on vaikea laskea, koska ne riippuvat niin paljon liikkuvan datan määrästä ja yrityksen tarpeista.

Azure VPN gateway ei tarjoa full tunnel mahdollisuutta, eli kaikkea verkkoliikennettä ei voi kierrättää Azuren kautta. Siinä mielessä Azuren VPN gateway ei toimi samalla lailla kuin perinteiset VPN ratkaisut. Jos halutaan kaikki verkkoliikenne kierrättää Azuren kautta, Azure tarjoaa myös siihen kykeneviä ratkaisuja kuten Azure Expressroute ja Azure Virtual WAN.

Varmennepohjainen ratkaisu on parhaiten soveltuva pienille yrityksille, joissa on enintään 5–10 työntekijää, pienissä tiimeissä varmenteiden hallinnointi on yksinkertaisempaa. Jokaiselle käyttäjälle on luotava, jaettava ja mahdollisesti uusittava omat varmenteet, mikä suuremmissa yrityksissä voi muodostua hyvin työlääksi prosessiksi. Toisaalta Basic-mallin tarjoama nopeus ei riitä suurille käyttäjämäärille. Tämä rajoitus tulee selvästi esille, kun verkossa on paljon käyttäjiä, sillä suurempi käyttäjämäärä vaatii enemmän kaistanleveyttä tehokkaan datakuljetuksen varmistamiseksi. Basic-mallin alhainen nopeus voi johtaa hitaaseen yhteysnopeuteen ja tehottomuuteen, mikä ei tue tehokasta työskentelyä suurissa ympäristöissä. Lisäksi Basic-mallin skaalautuvuuden puute on merkittävä ongelma, erityisesti yrityksille, jotka suunnittelevat laajentavansa pilvipalveluiden käyttöä. Mallissa ei ole mahdollista nostaa yhteyden nopeutta, mikä rajoittaa yrityksen kykyä kasvaa ja sopeutua laajeneviin tarpeisiin. Tämän lisäksi Basic-malli tarjoaa vain varmennepohjaisen tunnistautumisen, jolloin muita tunnistautumismenetelmiä ei ole saatavilla. Tämä voi olla rajoittava tekijä, erityisesti organisaatioille, jotka tarvitsevat monipuolisempia ja turvallisempia tunnistautumisvaihtoehtoja. Näin ollen, vaikka varmennepohjainen ratkaisu ja Basic-mallin VPN-gateway ovat sopivia ratkaisuja pienille yrityksille, ne eivät välttämättä ole parhaita valintoja suurempia kasvutavoitteita tai joustavampia verkkoratkaisuja tarvitseville organisaatioille. Tämän toteutuksen arvioidut kustannukset 1–20 käyttäjällä ovat 28,8 € ja 57,04 € välillä. Tämä hinta vaihtelee käyttäjien siirtämän datan määrän mukaan.

Entra ID -tunnistautumispohjainen ratkaisu on hyvä valinta yritykselle, joka suunnittelee laajentavansa pilvipalveluiden käyttöä tai jonka käyttäjämäärä on jo kasvanut. Entra ID mahdollistaa käyttäjien oikeuksien hallinnan tehokkaasti ryhmien avulla. Ryhmäpohjainen hallinta tekee oikeuksien määrittämisestä ja käyttäjähallinnasta selkeämpää ja joustavampaa, erityisesti suuremmissa organisaatioissa. Lisäksi Entra ID -tunnistautumisen laajentaminen on suhteellisen helppoa. Sen gateway-mallia voidaan muuttaa ilman, että se aiheuttaa merkittäviä käyttökatkoja. Tämä joustavuus on arvokasta, kun yrityksen tarpeet muuttuvat ja kasvavat. Se mahdollistaa verkkoratkaisujen mukauttamisen ja päivittämisen ilman pitkiä käyttökatkoja, mikä on tärkeää yrityksen jatkuvan toiminnan kannalta. Kokonaisuudessaan Entra ID:n tunnistautumispohjainen ratkaisu on hyvin soveltuva vaihtoehto dynaamisille yrityksille, jotka odottavat kasvua ja jotka tarvitsevat tehokkaan, helposti hallittavan ja skaalautuvan tunnistautumisjärjestelmän. Tämän toteutuksen arvioidut kustannukset 1–20 käyttäjällä ovat 130,78 € ja 157,64 € välillä. Tämä hinta vaihtelee käyttäjien siirtämän datan määrän mukaan.

Site-to-site-ratkaisu on kaikista perinteisin VPN-yhteyksien toteutustapa. Tässä ratkaisussa on käytetty samaa gateway-mallia kuin Entra ID -toteutuksessa, mikä takaa hyvän skaalautuvuuden. Vaikka tämä toteutus ei suoraan tue etätyöskentelyä, siihen voidaan lisätä

Entra ID -tunnistautumispohjainen Remote access-VPN-yhteys, mikä mahdollistaa etätyöskentelyn. Kun arvioidaan site-to-site-ratkaisun kustannuksia, on tärkeää huomioida, että toimistolle on hankittava VPN-yhteyden mahdollistava laite. Tämä voi olla esimerkiksi palomuuri tai reititin. Nämä laitteet ovat olennainen osa yhteyden muodostamista ja niiden hankintakustannukset tulee sisällyttää kokonaiskustannusten arviointiin. Tämän toteutuksen arvioidut kustannukset ilman palomuuria tai reititintä 1–20 käyttäjällä ovat 130,78 € ja 157,64 € välillä. Tämä hinta vaihtelee käyttäjien siirtämän datan määrän mukaan.

Vertailun vuoksi tutustuttiin vielä kolmannen osapuolen ratkaisuun, jolla voitaisiin toteuttaa remote-access vpn-yhteys. Tähän valikoitu Fortinetin FortiGate 60F -palomuuri. Laitteella ei ole rajoituksia VPN-käyttäjien määrässä, mikä tekee siitä joustavan ratkaisun eri kokoisten organisaatioiden tarpeisiin. Lisäksi se kykenee muodostamaan jopa 200 site-to-site-tunnelia, mikä osoittaa sen soveltuvuuden laajoihin verkkorakenteisiin. TLS-VPN-yhteyksissä laitteen suoritusteho yltää jopa 900 Mbps nopeuteen. (Fortinet, n.d.-a)

FortiGate 60F -palomuuri kustantaa 889 € ja se sisältää perustason lisenssin. Perustason lisenssi mahdollistaa laitteen toiminnan ja tarjoaa perusominaisuuksia, mutta Fortinet ei tarjoa minkäänlaista tukea, jos laitteen käytössä ilmenee ongelmia. Tämä voi olla merkittävä haittapuoli, erityisesti teknisesti vaativissa käyttöympäristöissä. Laitteen kustannukset voivat kasvaa, jos tarvitaan lisää tukipalveluita. Esimerkiksi 1-vuoden FortiGate-lisenssi, joka sisältää 24/7 tuen ja muita turvallisuusominaisuuksia, maksaa 399 euroa. Tämä on merkittävä lisäkustannus, mutta se voi olla tarpeellinen, jos vaaditaan jatkuvaa teknistä tukea ja kehittyneempiä turvallisuusominaisuuksia. Hinnat on katsottu suoraan Dustin.fi verkkokaupasta. (Dustin, n.d.)

Laitteen konfigurointi vaatii asiantuntemusta ja ei välttämättä onnistu ilman aiempaa kokemusta. Tämä voi olla haaste pienille yrityksille tai organisaatioille, joilla ei ole käytettävissään kokenutta IT-henkilöstöä. Kokonaisuudessaan FortiGate 60F tarjoaa monipuolisia ominaisuuksia VPN-yhteyksien toteuttamiseen, mutta sen tehokas hyödyntäminen vaatii sekä taloudellisia resursseja että teknistä osaamista.

6 Yhteenveto

Opinnäytetyön tavoitteena oli tarjota kattava katsaus Azuren VPN-ratkaisuihin, niiden ominaisuuksiin, kustannuksiin ja soveltuvuuteen pk-yritysten tarpeisiin. Tarkoituksena oli myös vastata tutkimuskysymyksiin ”Minkälaisia VPN-ratkaisuja Azure tarjoaa?” ja ”Kuinka Azuren VPN-ratkaisut soveltuvat pk-yrityksen käyttöön?” Toiminnallisessa osuudessa oli tarkoitus toteuttaa kolme erilaista ratkaisua ja kuvata kunkin toteutuksen eri vaiheet.

Opinnäytetyö onnistui ilman suurempia ongelmia. Suurimmat haasteet olivat Site-to-Site yhteyden toteutuksen kanssa, koska tässä piti konfiguroida PaloAlton palomuuria, josta minulla ei ollut aikaisempaa kokemusta. Lopputuloksena opinnäytetyö tarjoaa vastaukset asetettuihin tutkimuskysymyksiin. Kolme erilaista VPN-ratkaisua saatiin toteutettua onnistuneesti. Työssä käydään läpi jokaisen toteutuksen hyvät ja huonot puolet. Opinnäytetyö osoittaa, kuinka Azuren VPN-ratkaisut tarjoavat monipuolisia ja skaalautuvia vaihtoehtoja yritysten erilaisiin verkkotarpeisiin, mukaan lukien tietoturvan, luotettavuuden ja kustannustehokkuuden näkökulmat.

Opinnäytetyön aihe valikoitui tekijän omasta kiinnostuksesta Azure verkkopalveluita ja VPN-yhteyksiä kohtaan. Opinnäytetyöprosessin aikana opin paljon VPN-yhteyksistä, Azuren tarjoamista verkkopalveluista ja niiden konfiguroinnista. Tämä työ laajensi merkittävästi minun ymmärrystäni ja osaamista, näiden aiheiden parissa.

Lähteet

Atkinson, R. (1995). *Security Architecture for the Internet Protocol* https://datatracker.ietf.org/doc/html/rfc1825

Amazon. (n.d.). *What is cloud computing?* Haettu 25.10.2023 osoitteesta https://aws.amazon.com/what-is-cloud-computing/

Cisco. (2013). *IKEv2 Packet Exchange and Protocol Level Debugging* https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/115936-understanding-ikev2-packet-exch-debug.html

Cloudflare. (n.d.). *What is tunneling?* Haettu 5.12.2023 osoitteesta https://www.cloudflare.com/learning/network-layer/what-is-tunneling/

Dustin. (n.d.). *FortiGate 60F -palomuuri* Haettu 12.12.2023 osoitteesta https://www.dustin.fi/product/5011227621/fortigate-60f--palomuuri

Fortinet. (n.d.-a). *FortiGate FortiWiFi 60F Series – Datasheet* Haettu 7.112.2023 osoitteesta https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf

Fortinet. (n.d.-b). *What is a Remote Access VPN?* Haettu 24.10.2023 osoitteesta https://www.fortinet.com/resources/cyberglossary/remote-access-vpn

Fortinet. (n.d.-c). *What Is A Site-to-Site VPN?* Haettu 24.10.2023 osoitteesta https://www.fortinet.com/resources/cyberglossary/what-is-site-to-site-vpn

IBM. (n.d.). *What is cloud computing?* Haettu 25.10.2023 osoitteesta https://www.ibm.com/topics/cloud-computing

Ilya Grigorik (n.d.). *Transport Layer Security.* Haettu 25.10.2023 osoitteesta https://hpbn.co/transport-layer-security-tls/

Kapersky. (n.d.). *What is VPN? How It Works, Types of VPN.* Haettu 24.10.2023 osoitteesta https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

Kaufman, C. (2005). *Internet Key Exchange* (IKEv2) Protocol. https://datatracker.ietf.org/doc/html/rfc4306

Kent, S. (2005). *Security Architecture for the Internet Protocol.* https://datatracker.ietf.org/doc/html/rfc4301

Liu, D., Miller, S, Lucas, M., Singh, A., Davis, J. (2006). *Firewall Policies and VPN Configurations*. Syngress.

Microsoft. (n.d.-a). *VPN Gateway pricing.* Haettu 25.10.2023 osoitteesta https://azure.microsoft.com/en-us/pricing/details/vpn-gateway/

Microsoft. (n.d.-b). *What is Azure?* Haettu 25.10.2023 osoitteesta https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/

Microsoft. (2022.). *What is Azure role-based access control (Azure RBAC)?* https://learn.microsoft.com/en-us/azure/role-based-access-control/overview

Microsoft. (2023.a). *About Point-to-site VPN.* https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about

Microsoft. (2023.b). *Bandwidth pricing* https://azure.microsoft.com/en-us/pricing/details/bandwidth/

Microsoft. (2023.c). *Tutorial: Create a site-to-site VPN connection in the Azure portal* https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal

Microsoft. (2023.d). *What is Azure Virtual Network?* https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

Microsoft. (2023.e). *What is Azure VPN Gateway?* https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

Microsoft. (2023.f). *What is Azure VPN Gateway?* https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

Microsoft. (2023.g). *What is Microsoft Entra ID?* https://learn.microsoft.com/en-us/entra/fundamentals/whatis

Nordlayer (n.d.). *Most common VPN protocols.* Haettu 24.10.2023 osoitteesta https://nordlayer.com/learn/vpn/types-and-protocols/

Odom, W. (2021). *CCNA 200-301, Volume 2, Official Cert Guide*. Cisco Press

Okta. (2023.). *What Is a Digital Certificate?* Definition and Examples https://www.okta.com/identity-101/digital-certificate/

OWASP. (n.d.). *Transport Layer Protection Cheat Sheet.* Haettu 25.10.2023 osoitteesta https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

PaloAlto Networks. (n.d.). *What Is a Remote Access VPN?* Haettu 24.10.2023 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn

VMware. (n.d.). *What is virtual Networking?* Haettu 30.10.2023 osoitteesta https://www.vmware.com/topics/glossary/content/virtual-networking.html