Elias Hippi

Selvitys Always On VPN- tai Azure VPN -ratkaisun sopivuudesta Re-ceptumin työympäristöön

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Ohjelmistotuotanto

Insinöörityö

31.10.2023

Tiivistelmä

Tekijä:	Elias Hippi
Otsikko:	Selvitys Always On VPN- tai Azure VPN -ratkaisun sopivuudesta Receptumin työympäristöön
Sivumäärä:	35 sivua
Aika:	31.10.2023
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Ohjelmistotuotanto
Ohjaajat:	Vastuuarvioija Jorma Räty

Avainsanat: Azure VPN, Always On VPN, VPN

Opinnäytetyön toimeksiantona oli löytää Receptum Oy:lle uusi VPN-ratkaisu korvaamaan Direct Access. Vertailussa oli kaksi eri vaihtoehtoa: Always On VPN ja Azure VPN. Tavoitteena oli arvioida näiden kahden VPN-ratkaisun ominaisuuksia sekä laatia lopuksi teoreettinen käyttöönotto.

Tutkimusmenetelmänä käytimme kehittäjätutkimusta, joka auttoi meitä vertailemaan näiden kahden ratkaisun vahvuuksia ja heikkouksia sekä arvioimaan niiden kustannuksia. Näiden tulosten perusteella teimme päätöksen, mikä ottaa huomioon Receptumin tulevaisuuden tarpeet sekä heidän mielipiteensä VPN-ratkaisusta. Haasteita kuitenkin aiheuttivat hinnat, jotka olivat monien eri tekijöiden vaikutuksen alaisia. Lisäksi teoreettinen käyttöönotto oli haasteellinen, koska emme pystyneet vielä toteuttamaan sitä käytännössä.

Lopputuloksena pystyimme löytämään ratkaisun yrityksen tarpeisiin ja laadimme myös nopean ohjeen helpottamaan varsinaista käyttöönottoa. On kuitenkin tärkeää huomata, että tämä teoreettinen käyttöönotto toimii perustana oikealle käyttöönotolle, mutta se ei korvaa varsinaista toteutusta.

Abstract

Author:	Elias Hippi
Title:	Suitability of Always On VPN or Azure VPN for Receptum
Number of Pages:	35 pages
Date:	31.10.2023
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communications Technology
Professional Major:	Software Engineering
Supervisors:	Jorma Räty, Project Manager

Keywords: Azure VPN, Always On VPN, VPN

The aim of this study was to find a VPN solution for replacing Direct Access at Receptum Oy. Two options were considered: Always On VPN and Azure VPN. The objective was to evaluate both VPNs and provide a plan for implementation.

To compare the two solutions, a research methodology called developer research was followed. Details about each VPN option, including their strengths, weaknesses, and associated costs were gathered. This analysis helped make a decision while considering Receptums requirements and their views on VPN technology.

However, challenges primarily related to pricing, which were influenced by factors were encountered. Additionally, the theoretical implementation presented difficulties as it was not possible to perform any actions at this stage.

In the end at a solution was found along with a guide to facilitate the implementation. It is important to note that the provided guide serves as a basis for implementation and does not directly represent the deployment process.

Sisällys

Lyhenteet

1 Johdanto 1

2 Receptum Oy 2

2.1 Konserni 2
2.2 Millainen on Direct Access? 2

3 VPN-teknologiat 4

3.1 VPN 4
3.2 Liiketoiminta ja etätyö 5
3.3 Protokollat 5
3.4 Todennusprotokollat 8
3.5 Mitä VPN-Tyyppejä on 10

4 Always On VPN 13

4.1 Tekniikkaa 13
4.2 Mitä hyötyjä ja haittoja Always on VPN? 14
4.3 Ominaisuuksia 15
4.4 Hinnoittelu 16

5 Azure VPN 17

5.1 Tekniikka 17
5.2 Mitä hyötyjä ja haittoja Azure VPN:llä on? 17
5.3 Ominaisuuksia 18
5.4 Hinnoittelu 19

6 VPN:n valinta 20

6.1 Vertailu ja päätös 20
6.2 Miten sopisi Receptumille? 22

7 Teoreettinen käyttöönotto 23

7.1 Suunnittelu 23
7.2 Toteutus 24
7.2.1 VPN Gatewayn luonti 25

7.2.2 Sertifikaattien luonti 27
7.2.3 P2S-konfigurointi 28
7.3 Jatko 29
8 Tulokset ja yhteenveto 30
Lähteet 32
Liitteet

Lyhenteet:

RRAS: Routing and Remote Access Service. Reititys- ja etäkäyttöpalvelu.

SA: Security Association. Suojausassosiaatio.

SSL: Secure Sockets Layer. Suojauskerros.

SSTP: Secure Socket Tunneling Protocol. Suojauskerros tunnelointi protokolla.

TLS: Transport Layer Security. Kuljetus suojauskerros.

WAN: Wide Area Network. Laajaverkko.

WIP: Windows Information Protection. Windowsin Tietosuoja.

VPN: Virtual Private Network. Virtuaalinen yksityinen verkko.

AD: Active Directory. Käyttäjä tietokanta.

CHAP: Challenge-Handshake Authentication Protocol. Challenge-Handshake-todennusprotokolla.

EAP: Extensible Authentication Protocol. Laajentuva todennusprotokolla.

GRE: Generic Routing Encapsulation. IP-tunnelointiprotokolla.

HTTPS: Hypertext Transfer Protocol Secure. Salattu yhteys selaimen ja palvelimen välillä.

IIS: Internet Information Services. Palvelinohjelmistokokonaisuus.

IKEv2: Internet Key Exchange version 2. Avaintenvaihtoprotokolla.

IP: Internet Protocol. Internetti protokolla.

IPsec: Internet Protocol Security. Internetti suojausprotokolla.

ISATAP: Intra Site Automatic Tunnel Addressing Protocol. Automaattinen tunneli protokolla.

L2TP: Layer 2 Tunneling Protocol. Kerroksen 2 tunnelointiprotokolla.

NLS: Network Location Server. Verkkosijainti.

PAP: Password Authentication Protocol. Salasana suojaus protokolla.

PEAP: Protected Extensible Authentication Protocol. Suojattu laajentuva tunnistusprotokolla.

PPP: Point-to-Point Protocol. Digitaalisen tiedonsiirron protokolla.

PPTP: Point-to-Point Tunneling Protocol. VPN-tunnelointiprotokolla.

RADIUS: Remote Authentication Dial in User Service. Internetin standardi-protokolla.

1 Johdanto

Nykyään suurin osa ihmisistä viettää aikaa internetissä ja siitä on tullut iso osa meidän jokapäiväistä elämäämme. Täten on tärkeää suojata yksityisyytemme käytettäessä internetiä. Tähän tarkoitukseen on onneksi kehitetty VPN, joka piilottaa todellisen sijaintimme ja toimii näin suojana meille. Liike-elämässä VPN:t mahdollistavat etätyöskentelyn, koska voimme muodostaa yhteyden työpaikkamme verkkoon mistä tahansa ja näin käsitellä yrityksen sisäisiä resursseja.

Opinnäytetyön tarkoituksena oli selvittää yhteistyössä Receptum Oy:n kanssa, kumpi kahdesta VPN-vaihtoehdosta, Always On VPN vai Azure VPN, olisi sopivampi ratkaisu. Tutkimustyö aloitettiin, koska yrityksessä käytetty VPN-ratkaisu, Direct Access, on tulevaisuudessa "end of life," eli sen tukemisen loppuu jossain vaiheessa. On kuitenkin huomioitava, että Microsoft tarjoaa toistaiseksi täyden tuen vielä Direct Accessille.

Tavoitteena opinnäytetyössä oli vertailla, kumpi VPN-vaihtoehdoista olisi ylläpidoltaan kustannustehokkaampi, soveltuisi paremmin Receptumin työympäristöön, olisi helpommin jaettavissa yrityksen sisällä sekä sopisi paremmin yrityksen laitekantaan ja tulevaisuuden tarpeisiin. Otetaan myös huomioon mahdollisuus käyttää tulevaisuudessa muita laitteita kuin Fujitsun kannettavia, joissa on Windows-käyttöjärjestelmä.

Opinnäytetyössä tulemme tarkastellaan yksityiskohtaisesti, mikä on Receptum, VPN:ää ja siihen liittyvää teoriaa, kuten protokollia ja muita VPN-tekniikoita. Käsitellään perusteellisesti molemmat VPN-vaihtoehdot ja lopuksi pohditaan teoreettisesti, miten VPN voitaisiin ottaa käyttöön Receptumin työympäristössä. Lopputuloksena pyrimme saamaan selkeä päätöksen siitä, kumpi VPN-vaihtoehto otetaan käyttöön, miksi juuri se valittiin, ja miten se käytännössä otetaan käyttöön yrityksen työympäristössä.

2 Receptum Oy

2.1 Konserni

Receptum on apteekkitoimialalla toimiva yritys, joka on kehittänyt MAXX-nimisen käyttöjärjestelmän apteekeille, mikä helpottaa siten apteekkien asiakaspalvelua. Receptum tarjoaa apua apteekeille erilaisissa teknisissä ongelmissa, kuten internet- ja käyttöjärjestelmäongelmissa sekä laitteistoon liittyvissä asioissa. Yritys tarjoaa teknisen tuen lisäksi laitteistoa asiakkailleen, jota sitten ylläpidetään ja huolletaan. Receptum palvelee myös suun terveydenhuollon alalla. Tällä hetkellä Receptum toimii Suomessa, Ruotsissa ja Norjassa. Yrityksessä työskentelee noin 100 henkilöä, joilla on päivittäisessä työssään tarve toimivalle ja helppokäyttöiselle VPN:lle. Moni työntekijä tekee etätöitä koronapandemian jälkeen, joten VPN:stä on tullut korvaamaton työväline. Tämän vuoksi tämä opinnäytetyö on Receptumille erityisen tärkeä.

Receptum käyttää tällä hetkellä vielä Direct Access -nimistä VPN-ratkaisua, joka alkaa olla vanhentunut eikä enää toimi yrityksen työympäristössä luotettavasti. Työntekijät kohtaavat ongelmia Direct Accessin kanssa, kuten yhteyksien katkeilua ja kyvyttömyyttä uudelleen liittyä VPN:ään. Lisäksi usein joudutaan käynnistämään tietokone uudelleen, jotta saadakseen Direct Access toimimaan.

2.2 Millainen on Direct Access?

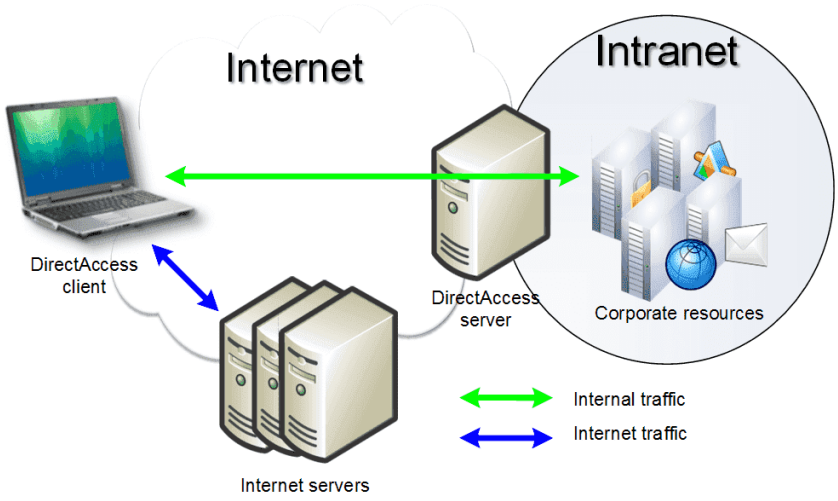
Direct Accessin tarkoituksena on muodostaa automaattisesti suojattu ja todennettu yhteys yrityksen verkkoon aina, kun käyttäjän laite on kytkettynä yritysverkon ulkopuoliselle verkolle. Näin käyttäjän ei tarvitse itse manuaalisesti muodostaa yhteyttä. [1.]

Direct Access -yhteyksien muodostaminen tapahtuu automaattisesti käyttäjän laitteen toimesta ja tarjoaa suojatun sekä luotettavan tavan päästä yritysverkkoon etäältä. Direct Access tarjoaa järjestelmänvalvojille mahdollisuuden hallita etäyhteydessä olevia käyttäjiä ja heidän laitteitaan, ja se on hyödyllinen

monissa erilaisissa tilanteissa, kuten etäylläpidossa ja tietoturvan hallinnassa. Juuri tästä syystä se tekee etätyöskentelystä ja pääsystä yritysverkkoon vaivatonta ja turvallista käyttäjille, ja tarjoaa samalla hallinnollisen kontrollin järjestelmänvalvojille. [2.]

Direct Access -ympäristössä keskeisin osa-alue on Network Location Server (NLS), joka toimii web-palvelimena ja on varustettu SSL-varmenteella. NLS määrittää, ovatko käyttäjät tällä hetkellä yrityksen sisäverkossa vai sen ulkopuolella. On tärkeää huomata, että NLS-palvelin ei saa olla saavutettavissa julkisesta Internetistä, jotta turvallisuus säilyy. Kun Direct Access on konfiguroitu käyttäjän laitteelle, laite tarkistaa ensin yhteyden NLS-palvelimeen joko käynnistyksen yhteydessä tai verkkoliitäntöjen vaihdon yhteydessä. [2.]

Turvallisen yhteyden luomiseksi käyttäjän ja yrityksen sisäverkon välille Direct Access hyödyntää IPv6-protokollaa yhdessä IPSecin kanssa. On kuitenkin tärkeää huomata, että käyttäjän laitteen ei tarvitse olla liitettynä IPv6-verkkoon, eikä yrityksen sisäverkon tarvitse tukea IPv6:ta, sillä Direct Access käyttää erilaisia IPv6-siirtotekniikoita automaattisesti IPv6-liikenteen tunneloimiseen IPv4-verkoissa. Näitä tunnelointitekniikoita ovat muun muassa 6to4, Teredo ja IP-HTTPS. IPv4-sisäverkossa tunnelointi toteutetaan NAT64- tai ISATAP-tekniikoilla. Tämä mahdollistaa turvallisen ja saumattoman yhteyden käyttäjän laitteen ja yrityksen sisäverkon välillä riippumatta käytössä olevasta verkkoprotokollasta. [2.]



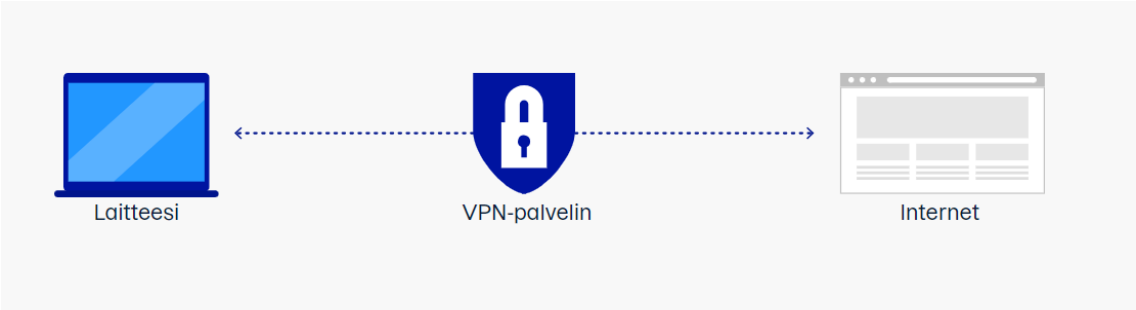
Kuva 1. Direct Accessin toiminta [3]

Kuvassa 1 käytetään päästä päähän -toteutusta, jossa kaikki käyttäjän sisäverkkoon suuntautuva liikenne käsitellään ja suojataan IPsecin avulla. Direct Access -palvelin toimii järjestelyssä portinvartijana, ja sen tehtävänä on mahdollistaa suojattu IPsec-liikenne. [3.]

3 VPN-teknologiat

3.1 VPN

VPN tulee sanoista Virtual Private Network, ja se on yhä tärkeämpi osa maailmaamme, jossa Internet on olennainen osa jokapäiväistä elämäämme. VPN toimii välittäjänä tietokoneen ja kohdepalvelimen välillä. Sen sijaan, että luottaisiin laitteen ja palvelimen väliseen viestintään, VPN lisää oman salauksensa ja ohjaa viestinnän omien palvelimiensa kautta. VPN-palvelu luo "tunnelin" tietokoneen ja kohdepalvelimen välille (katso kuva 2). Tunneli mahdollistaa tietojen lähettämisen niin, ettei kukaan muu verkossa voi salakuunnella tai siepata niitä. [4.]



Kuva 2. VPN-toiminta [5]

Teknisesti VPN muodostaa yhteyden, jossa laite kommunikoi VPN-verkon kautta paikallisen verkon sijaan, mukaan lukien julkinen Wi-Fi. VPN-palvelimella tallennetuilla tunnistetiedoilla suoritetaan todennus, jonka jälkeen saadaan yhteyden VPN-palvelimiin. Kun tunneli on määritetty, voimme käyttää virtuaalista

verkkoyhteyttä oman koneen ja VPN-palvelimen välillä, mikä salaa ja suojaa tietoja mahdollisia salakuuntelijoita vastaan. [4.]

3.2 Liiketoiminta ja etätyö

Yritykset voivat hyödyntää VPN-ratkaisuja tietoliikenteen suojaamiseen ja turvaamiseen. VPN-yhteyksiä, joita yritykset ja muut organisaatiot käyttävät, käytetään turvallisesti yhdistämään etätyöntekijät ja sivukonttorit tarvittaviin sovelluksiin, tietoihin, työkaluihin ja resursseihin työtehtäviensä hoitamiseksi.

Monet organisaatiot ovat perinteisesti käyttäneet kehämäisiä suojamalleja yritysverkkojensa turvaamiseen. Yritys-VPN:t täydentävät näitä suojamalleja tarjoamalla etätyöntekijöille ja sivukonttoreiden työntekijöille virtuaalisen verkon, jonka kautta he voivat käyttää yritysverkkoa mistä tahansa maailman kolkasta julkisen tai yksityisen internetyhteyden avulla. [6.]

Kehämäisessä suojamallissa yrityksen IT-tiimi rakentaa turvaverkkoja, jotka rajoittuvat organisaation fyysisiin rakenteisiin ja sijainteihin ja keskittävät tietoturvatoimenpiteet yrityksen omiin tiloihin. Tämä linjaus fyysisten rakenteiden ja tietoverkon välillä on mahdollistanut verkkoturvallisuuden ammattilaisille verkon käytön yksinkertaistamisen, seurannan ja hallinnan.

Vaikka pääkonttorissa työskentelevät työntekijät voivat muodostaa suoran yhteyden yrityksen verkkoon, kun he ovat organisaation tiloissa, sivukonttoreiden työntekijät, etätyöntekijät ja matkustavat työntekijät, jotka liikkuvat suojatun alueen ulkopuolella, tarvitsevat VPN:n turvallisen verkkoyhteyden luomiseksi, kun he työskentelevät missä tahansa. [7.]

3.3 Protokollat

VPN-protokollien olisi sisällettävä useita avainominaisuuksia turvallisen yhteyden luomiseksi. Ominaisuudet käsittävät tunneloinnin, tietojen vahvistuksen, tietojen koskemattomuuden, tietojen salauksen ja toistojen torjunnan. Tunnelointi

tarkoittaa käytännössä yhden datapaketin piilottamista toisen datapaketin sisään. Se mahdollistaa turvallisen siirtymisen tiedonsiirron aikana käyttäjän ja palvelimen välillä. [7.]

Tietojen vahvistus varmistaa, että kaikki osapuolet ovat aitoja ja että vastaanotetut tiedot ovat peräisin oikeilta käyttäjiltä. Tietojen koskemattomuus on olennaista, jotta voidaan taata, ettei tietoja ole muutettu tai vahingoitettu siirron aikana. Tietojen salaus on erityisen tärkeää julkisessa verkossa, ja se auttaa suojaamaan tietoja ulkopuolisilta tarkkailijoilta ja ylläpitämään yksityisyyttä. [7.]

Toistojen torjunta on toimenpide, joilla estetään haitalliset toistohyökkäykset, jotka lähettävät paketteja tuplana tai paketteja lähetetään todella myöhässä. Yhteyden aikana se auttaa ylläpitämään tietoturvaa. Juuri näiden ominaisuuksien avulla VPN-yhteydet takaavat turvallisuuden sekä suojelevat tietokoneen monenlaisilta uhilta. [7.]

Point-to-Point Tunneling Protocol (PPTP) on VPN-protokolla, joka käyttää tunnelointia ja vastaa käyttäjän tunnistamisesta, tietojen eheydestä ja tietojen salaamisesta. PPTP perustuu Point-to-Point eli PPP-protokollaan, joka on tiedonsiirtoprotokolla, joka mahdollistaa suoran yhteyden muodostamisen verkkolaitteiden välillä. Käyttäjän tunnistaminen tapahtuu ennen tiedonsiirtoa, ja PPTP mahdollistaa PPP:n tunneloimisen verkkoon. Se toteutetaan käyttämällä GRE-protokollaa PPP-paketin kuljettamiseen. [8.]

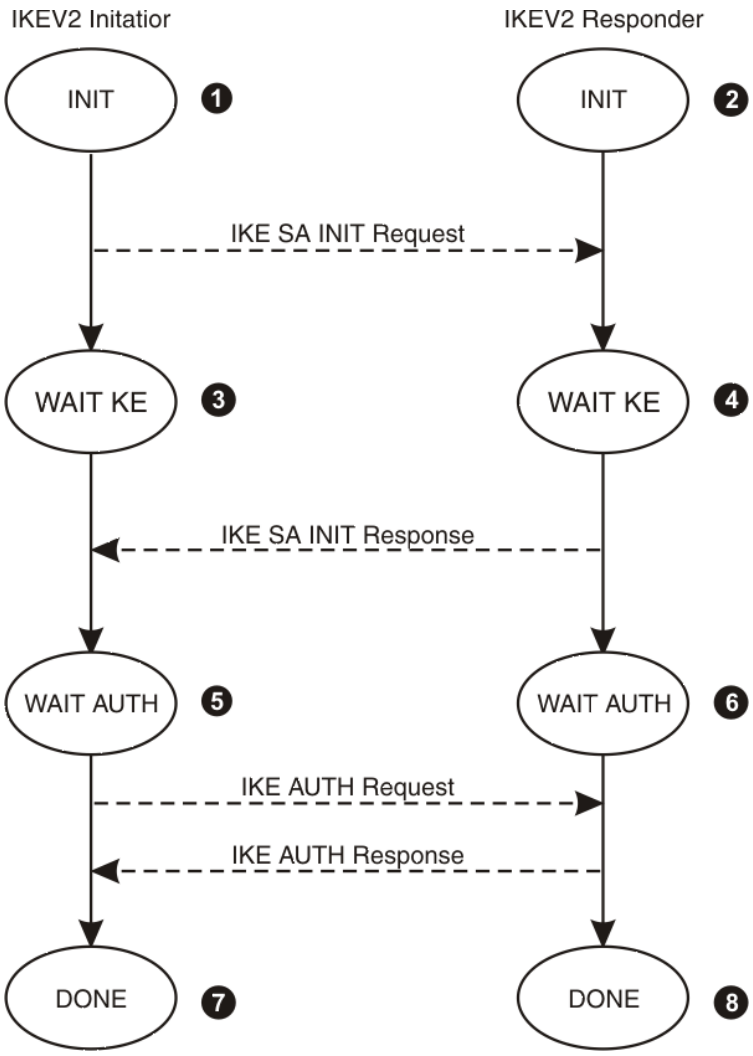
Layer 2 Tunneling Protocol (L2TP) yhdistää PPTP-protokollan ja Ciscon L2F-protokollan ominaisuudet, kun laajennetaan PPTP:n toiminnallisuutta. Sen tavoitteena on mahdollistaa yhteyden luominen kahden käyttäjän ja sovellusten välillä ilman häiriöitä. L2TP mahdollistaa Layer 2 -protokollan ja PPP-protokollan vuorovaikutuksen laajentamalla PPP-mallia. [8.]

Useimmat L2TP-toteutukset käyttävät IPSec-tietoliikenneprotokollaa täydentämään L2TP:ää, sillä L2TP ei yksinään tarjoa riittävää tietojen luottamuksellisuutta. IPSec on Layer 3 -protokolla, joka suojaa IP-paketteja kerroksessa 3 ja

sitä ylemmissä kerroksissa. Se varmistaa tietojen eheyden ja todentamisen HMAC-toimintojen avulla, ja tarjoaa salausalgoritmit tietojen luottamuksellisuuden takaamiseksi. IPSec määrittelee myös pakettien kentät ja niiden kuljetustavan, joko tunneli- tai kuljetusmuodossa. Tunnelimuotoa käytetään Site-to-Site - ja Host-to-Site-yhteyksissä, ja suojaakin alkuperäisen paketin kokonaan. Kuljetusmuotoa käytetään tiettyihin point-to-point-yhteyksiin. [9, s. 203–205.]

Internet Key Exchange version 2 (IKEv2) on standardipohjainen avaimenhallintaprotokolla, joka perustuu IPsec VPN -protokollaan. IKEv2 on paranneltu versio alkuperäisestä IKE-protokollasta ja tukee vahvaa salauslaitteistoa etäyhteyksille. IKEv2 on yhteensopiva myös useiden VPN-laitteiden kanssa. IKEv2 perustuu Diffie-Hellman-avainvaihtoprotokollaan ja käyttää useita salausalgoritmeja turvallisuusvaatimusten täyttämiseksi. Protokolla luo ja ylläpitää jaettua tilaa IP-datagrammien päiden välillä ja suorittaa keskinäisiä todennuksia, jonka jälkeen perustaa IKEv2-tietoturvayhteyden, jota kutsutaan myös SA:ksi eli on looginen yhteys, jossa on kaksi dataa siirtävää laitetta.IKE-SA suorittaa kaksi tärkeää toimintoa käyttämällä tallennettuja jaettuja salaisia tietoja. Nämä ovat perustaa CHILD-SA:n ESP-protokollalle tai AH-todennusotsikolle ja määrittävät, mitä salausalgoritmeja SA:t käyttävät. [10.]

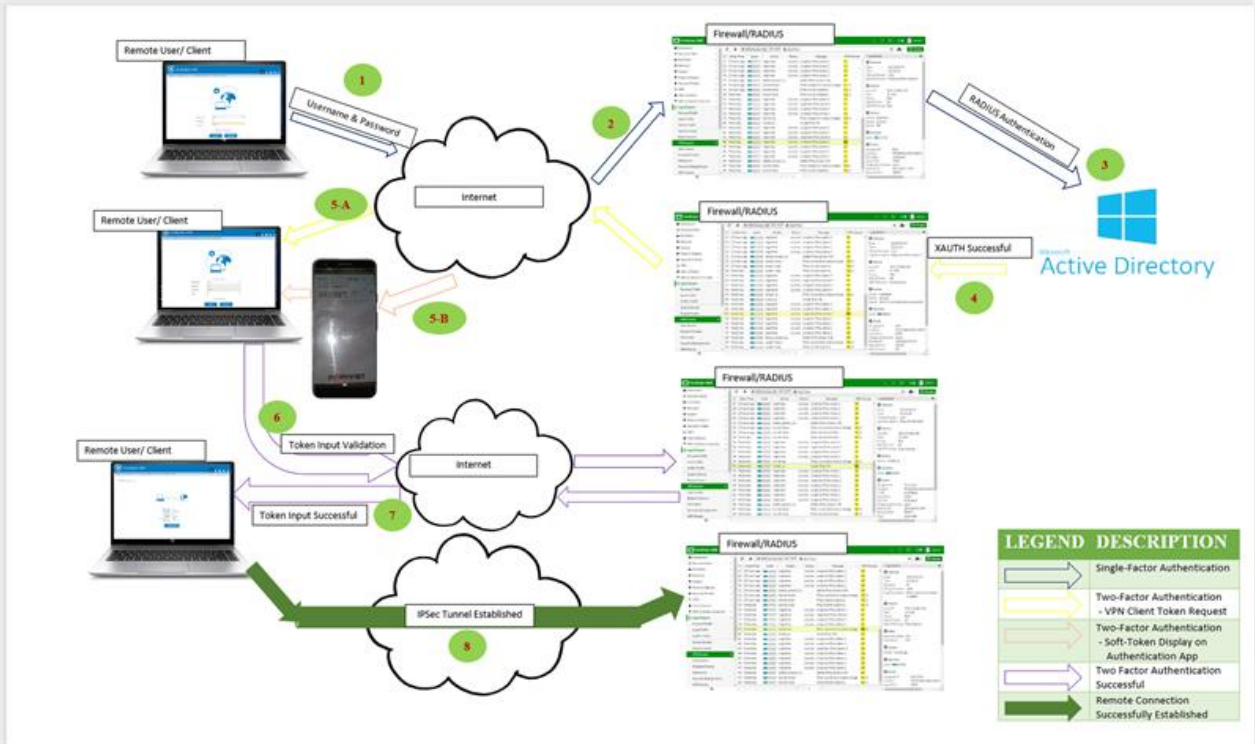
IKEv2 käyttää myös pyyntö/vastausparina varmistaakseen luotettavuuden. Nämä neljä erilaista vaihtoa ovat IKE_SA_INIT (ensimmäinen vaihto, jossa neuvotellaan IKE-SA-suojauksesta), IKE_AUTH (toinen vaihto, jossa lähetetään identiteettejä ja niihin liittyvät salaukset), CREATE_CHILD_SA (tarvittaessa lisää CHILD-SA-määrityksiä) ja INFORMATIONAL (huoltovaihto, joka ylläpitää SA:ita ja voi suorittaa erilaisia toimintoja, kuten SA:n poiston tai virheilmoitukset). Joissakin tilanteissa kaikkia vaihtoja ei tarvitse suorittaa. Esimerkki vaihdoksista on kuvassa 3. [11.]



Kuva 3. IKEv2 IKE SA:n vaihdot [11]

3.4 Todennusprotokollat

Password Authentication Protocol (PAP) käyttää yksinkertaista kaksivaiheista kättelyä linkin luomiseen. Tässä menetelmässä käyttäjä lähettää käyttäjänimensä ja salasanansa palvelimelle, joka tarkistaa ne, kuten kuvan 4 ylemmässä kuvasarjassa.



Kuva 4. Password Authentication Protocol [7]

Jos käyttäjä ja salasana ovat oikein, pääsee käyttäjä palvelimelle. Samalla tavalla toimii myös tokenilla tehty kirjautuminen, kuten kuvan 4 alemmassa kuvasarjassa. Valitettavasti PAP lähettää salasanat avoimena tekstinä, mikä tekee niistä haavoittuvia toistohyökkäyksille. [12.]

Challenge-Handshake Authentication Protocol (CHAP) toimii kolmivaiheisen kättelyn kautta. Ensimmäisessä vaiheessa palvelin lähettää haasteen käyttäjälle, joka vastaa toisessa vaiheessa siihen yksisuuntaisella hashilla. kolmannessa vaiheessa, jos vastaus on oikein, todennus onnistuu ja yhteys muodostetaan. CHAP suojaa salasanoja toistohyökkäyksiltä ja hallitsee haasteiden taajuutta ja ajoituksia. [13.]

Extensible Authentication Protocol (EAP) on laajasti käytetty todennuskehys, jota usein käytetään PPP-yhteyksissä ja langattomissa verkoissa. Se tarjoaa tuen monille erilaisille todennusmekanismeille, kuten tokeneille, varmenteille,

älykorteille ja kertakäyttöisille salasanoille. EAP laajentaa PPP:n käyttämiä todennusprotokollia. [14.]

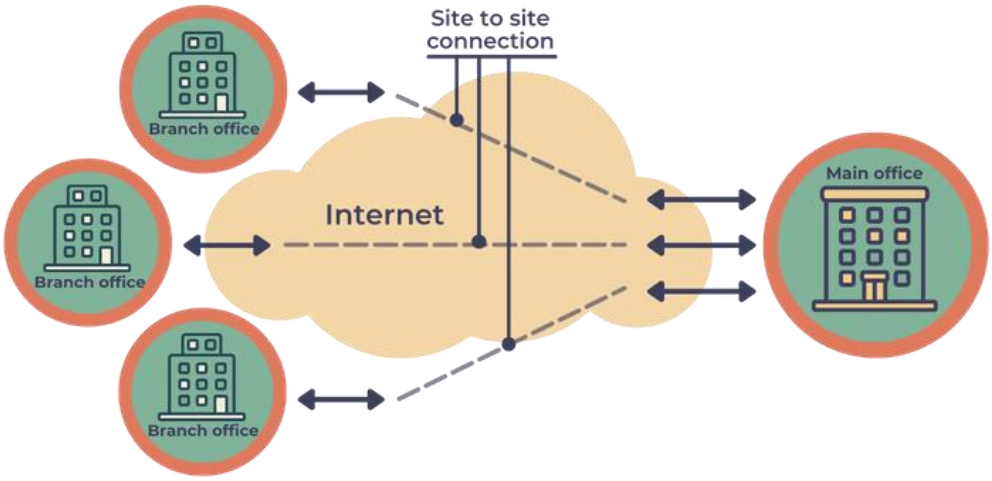
Protected Extensible Authentication Protocol (PEAP) on protokolla, joka suojaa EAP-viestintäkanavia. Se hyödyntää julkisen avaimen salausvarmennetta EAP:n sisällä ja auttaa palvelimia varmentamaan itsensä. PEAPin tarkoituksena on ratkaista tietoturvahaasteita tietyissä todennusympäristöissä ja varmistaa turvallinen todennusprosessi. Kun PEAP-keskustelu käynnistyy, EAP-palvelin ja EAP-asiakas aloittavat vuorovaikutuksen ja sopivat PEAP-keskustelun käyttämisestä. Tässä vaiheessa EAP-palvelin toimii PEAP-palvelimena, kun taas EAP-asiakas toimii PEAP-vertaisena. [15.]

Todennusprotokollat ovat tärkeitä tietoturvan kannalta, ja niitä käytetään laajasti erilaisissa verkkoyhteyksissä suojamaan käyttäjien tunnistetietoja ja varmistamaan VPN:n turvallinen yhteydenmuodostus.

3.5 Mitä VPN-Tyyppejä on

VPN:llä on viisi tunnettua toteutustapaa, jotka tarjoavat erilaisia mahdollisuuksia verkkoyhteyksien suojaamiseen ja organisaation verkkoyhteyksien laajentamiseen. Valinta VPN-tyypin välillä riippuu, mitä käyttötarpeita käyttäjällä on, organisaation turvallisuusvaatimuksista, mutta myös monet organisaatiot voivat jopa hyödyntää useita näistä tyyppisitä samaan aikaan eri tarkoituksiin.

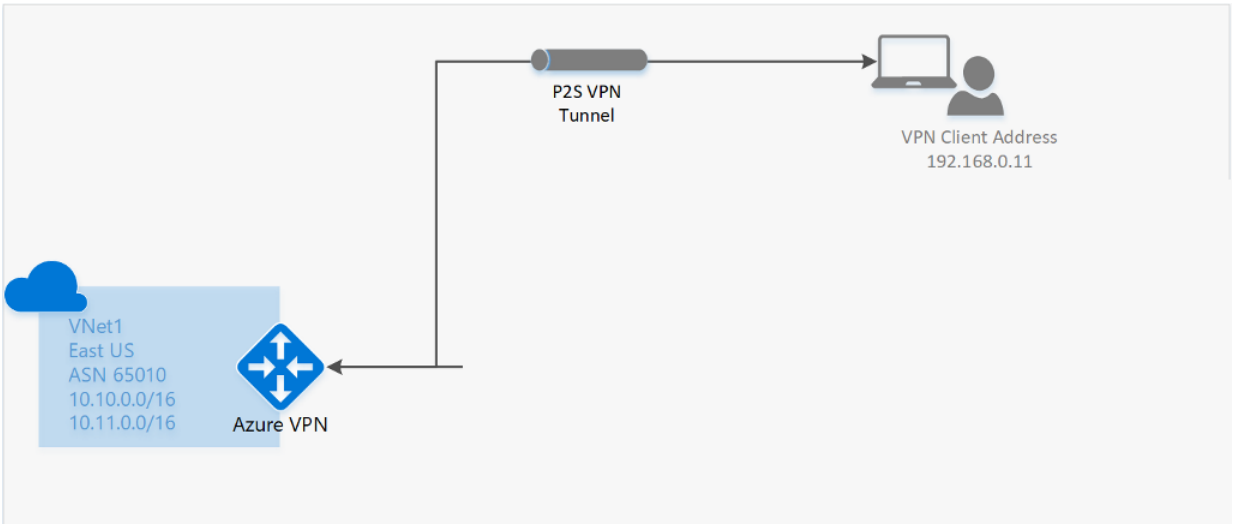
Site-to-Site VPN on suunniteltu organisaatioille, jotka tarvitsevat turvallisen tietoliikenneyhteyden kahden tai useamman toimipisteen välille.



Kuva 5. Site-to-Site VPN [16]

Site-to-Site VPN luo salatun yhteyden kahden verkon välille, mikä mahdollistaa turvallisen tiedonsiirron eri sijaintien välillä. Kuvan 5 ratkaisu tunnetaan tarkemmin lähiverkkojen välisinä VPN-verkkoina tai lähiverkkojen välisinä WAN VPN -yhteyksinä. Se mahdollistaa turvallisten yhteyksien luomisen eri lähiverkkojen välille käyttämällä julkisia välittäjäverkkoja välityksellä. [16.]

Point-to-Site VPN -yhdyskäytäväyhteyden avulla voidaan luoda turvallinen yhteys virtuaaliverkkoon yksittäisestä tietokoneesta. Ratkaisu on erityisen hyödyllinen etätyötä tekeville henkilöille, jotka haluavat muodostaa yhteyden esimerkiksi Azure VNets -verkkoihin etäpaikastaan, kuten kodistaan tai muualta, missä he ovatkaan. P2S VPN tarjoaa vaihtoehdon käytettäväksi S2S VPN:n sijaan silloin, kun on vain muutamia yksittäisiä käyttäjiä, jotka tarvitsevat yhteyden virtuaaliverkkoon on kuvassa 6. [17.]

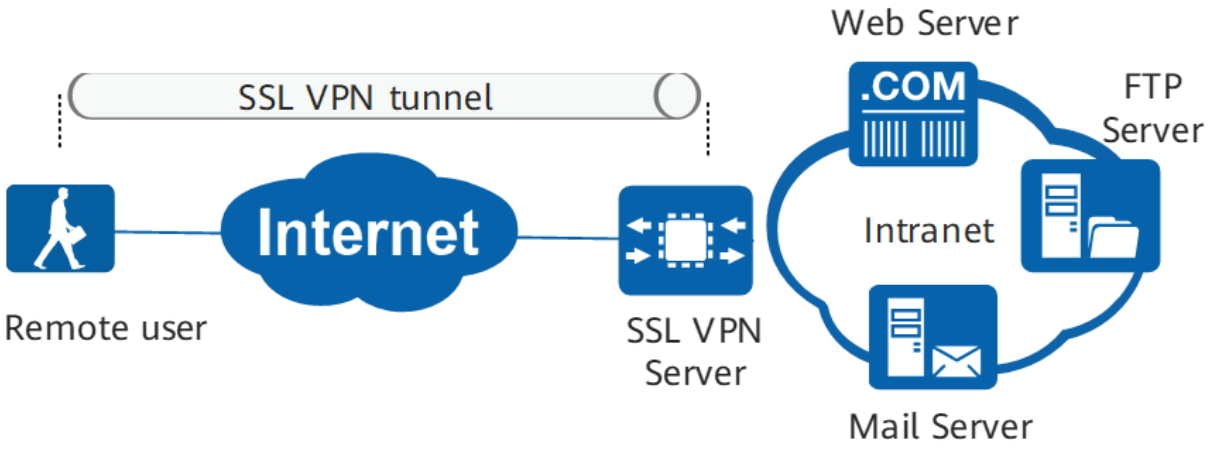


muokattu Kuva 6. Point-to-Site VPN yhteyden muodostus. [17]

Remote Access VPN mahdollistaa etätyöntekijöille ja liikkuville käyttäjille turvallisen pääsyn organisaation sisäiseen verkkoon internetin kautta, mikä mahdollistaa sen, että etäkäyttäjät voivat käyttää organisaation resursseja, kuten tiedostoja, sovelluksia ja muita verkkoressursseja, etäältä, ikään kuin he olisivat fyysisesti organisaation sisäisessä verkossa. [18.]

Mobile VPN on suunniteltu erityisesti älypuhelimille ja mobiililaitteille. Sen pääasiallinen tarkoitus on tarjota turvallinen ja salattu yhteys liikkuville käyttäjille, jotka tarvitsevat pääsyn organisaation resursseihin ollessaan matkoilla. Mobiili VPN on erityisen hyödyllinen tilanteissa, joissa käyttäjien on käytettävä julkisia verkkoyhteyksiä, kuten lentokenttien tai kahviloiden Wi-Fi-verkkoja, koska se suojaa heidän tietoliikennettään mahdollisilta uhilta. [19.]

Secure Socket Layer VPN mahdollistaa käyttäjien pääsyn organisaation verkkoon turvallisesti käyttämällä web-selainta. Tyyppi perustuu SSL/TLS-salausprotokolliin eikä vaadi erillistä VPN-ohjelmistoa.



Kuva 7. SSL VPN [20]

Käyttäjät voivat käyttää SSL VPN:ää useilta laitteilta mistä tahansa, kunhan heillä on internet yhteys. Käyttäjä voi yksinkertaisesti avata web-selaimen, syöttää oikeat kirjautumistiedot ja käyttää turvallista yhteyttä organisaation verkkoon on kuvassa 7. [20.]

4 Always On VPN

4.1 Tekniikkaa

Always On VPN hyödyntää perinteisiä VPN-protokollia, kuten (IKEv2, SSTP ja L2TP/IPSec), mikä mahdollistaa sen käytön monissa erilaisissa verkko-olosuhteissa. Lisäksi se tukee uusia ominaisuuksia, kuten ehdollista pääsyä, Windows Hello for Business -todennusta, Azure-pilviympäristön integrointia laite- ja profiilihallintaan sekä monivaiheista todennusta. Always On VPN -yhteys käyttää kahdentyyppistä tunnelia luodakseen turvallisen etäyhteyden. Nämä kaksi tunnelityyppiä ovat käyttäjätunneli sekä laitetunneli.

Käyttäjätunneli luodaan silloin, kun käyttäjä kirjautuu omalle verkkolaitteelleen, kuten tietokoneelleen, ja käyttää sitä päästäkseen yritysverkon resursseihin. Tunneli on erinomainen valinta tilanteissa, joissa käyttäjän tarvitsee jakaa tiedostoja tai saada oikeus käyttää tiettyjä sovelluksia yritysverkossa.

Laitetunnelissa käyttäjän ei tarvitse olla kirjautuneena tietokoneeseen, jotta laitetunneli voidaan muodostaa. Se luodaan automaattisesti, kun tietokone käynnistetään ja se saa yhteyden Internetiin. Soveltuu tilanteisiin, joissa tarvitaan pääsyä Active Directory -palvelimelle tai muihin hallintapalvelimiin, kuten Configuration Manageriin, ilman, että käyttäjä joutuu kirjautumaan erikseen. Laitetunneli varmistaa, että tietokone on luotettavasti sekä turvallisesti yhdistynyt yritysverkkoon heti, kun se on käynnistetty. [21.]

Lisäksi Always On VPN tarjoaa muita hyödyllisiä ominaisuuksia, kuten WIP-integraation (Windows Information Protection), liikennesuodattimet VPN-verkon käytön rajoittamiseksi ja sovelluksiin perustuvan VPN-yhteyden muodostamisen. Näiden ominaisuuksien ansiosta Always On VPN on varteenotettava ratkaisu organisaatioille, jotka tarvitsevat turvallisen ja käyttäjäystävällisen etäyhteyden. [22.]

4.2 Mitä hyötyjä ja haittoja Always on VPN?

Always on VPN tuo hyviä etuja. Se tuo samalla vanhoille käyttöjärjestelmille haittoja. Siksi Always on VPN ei välttämättä sovi ihan jokaiselle yritykselle tai yksityishenkilölle, keillä on vanha pc-käyttöjärjestelmä käytössä.

Etujen joukossa on tuen tarjoaminen kaikille Windows 10 -käyttöjärjestelmän versioille, myös Windows 10 Home- ja Professional -versioille sekä uusille Windows 11 -käyttöjärjestelmille. Se mahdollistaa etäyhteyden käytön sekä IPv4- että IPv6-protokollilla, ja se on infrastruktuuririippumaton, mikä tarkoittaa, että se voi toimia erilaisten verkkoinfrastruktuurien kanssa. Lisäksi Always On VPN ei ole sidottu pelkästään Windowsin omaan RRAS-tukeen, vaan sitä voidaan käyttää myös kolmannen osapuolen verkkolaitteiden kanssa. [22.]

Haittana on, että Always On VPN ei ole käytettävissä Windows 7 -käyttöjärjestelmällä, joten se ei sovi kaikille vanhemman Windows-version käyttäjille. Hallinnan osalta on tapahtunut muutoksia, eikä sitä voi enää hallita suoraan Active Directoryn tai ryhmäkäytänteiden avulla. Sen sijaan määritykset ja hallinta

voidaan suorittaa käyttämällä Microsoft Intunea, Microsoft System Center Configurationia tai Powershellia. [22.]

Always On VPN tarjoaisi monipuolisen ja joustavan etäyhteysratkaisun yrityksille, mutta sen käyttö edellyttää valitettavasti Windows 10 -käyttöjärjestelmää tai uudempaa Windows 11 -käyttöjärjestelmää sekä uusia hallintatyökaluja vanhojen perinteisten menetelmien sijaan. [22.]

4.3 Ominaisuuksia

Always On VPN -ratkaisu mahdollistaa läpinäkyvän ja saumattoman yhteyden. Joka toteuttaa hyödyntämällä automaattista laukaisua, se perustuu joko sovelluksen käynnistämiseen tai nimitilan tarkkuuspyyntöihin. VPN-yhteys voidaan muodostaa automaattisesti ja huomaamatta, kun käyttäjä tarvitsee sitä, esimerkiksi tietyn sovelluksen käyttämiseen.

VPN-profiilien laitetunneli on toinen tärkeä ominaisuus. Se mahdollistaa erillisen infrastruktuuritunnelin käytön yhteyksien tarjoamiseksi käyttäjille, jotka eivät ole kirjautuneet yrityksen verkkoon. Laitetunneli voidaan määrittää vain laitteille, jotka on liitetty yrityksen verkkotunnukseen (domain-joined) ja käyttävät IKEv2-laitevarmenteen todentamista. Ominaisuus mahdollistaa turvallisen yhteyden luomisen yritysverkkoon, vaikka käyttäjä ei olisikaan kirjautunut yritysverkkoon. [22.]

Automaattinen tunnelityyppi on vielä yksi tärkeä toiminto. Sitä voidaan käyttää vaihtamaan VPN-yhteyden protokollaa IKEv2:sta SSTP:hen automaattisesti. Se on hyödyllistä tilanteissa, joissa käyttäjät ovat palomuurien tai välityspalvelimien takana. Automaattinen protokollamuutos on mahdollista käyttäjätunnelissa, joka tukee sekä SSTP:tä että IKEv2:ta, mutta se ei ole saatavilla laitetunnelissa, joka tukee vain IKEv2-protokollaa.

Always On VPN on paremmin integroitu Windows-käyttöjärjestelmiin ja kolmannen osapuolen ratkaisuihin. Tarjoten laajemman tuen erilaisille yhteysmenetelmille ja mahdollistaen sujuvamman kokemuksen käyttäjille. [23.]

Always On VPN hyödyntää uusia ja kehittyneitä tietoturvaominaisuuksia, jotka mahdollistavat tietynlaisen suojauksen. Voimme siis rajoittaa tiettyjä liikennetyyppejä, määrittää, mitkä sovellukset saavat käyttää VPN-yhteyttä, sekä valita, millaisia todennusmenetelmiä käytetään yhteyksien muodostamiseen. Sillä kun yhteydet ovat käytössä lähes jatkuvasti tietoturva on ensiarvoisen tärkeää. [23.]

4.4 Hinnoittelu

Always On VPN -ratkaisujen hinnoittelu yrityksissä vaihtelee merkittävästi riippuen monista tekijöistä. Yritystason VPN-ratkaisut, kuten Always On VPN, tarjoavat jatkuvan ja automaattisen VPN-yhteyden organisaation verkkoon. Hinnoittelu riippuu usein organisaation koosta, tarpeista ja budjetista. Tärkeitä seikkoja, jotka vaikuttavat Always On VPN -hinnoitteluun yrityksissä, ovat käyttäjämäärä, laitemäärä ja tarvittava palvelinkapasiteetti.

Käyttäjämäärä on yleinen hinnoittelutekijä, ja Alway on VPN maksaa lisää käyttäjämäärän perusteella. Mitä enemmän käyttäjiä organisaatiossa on, sitä enemmän palvelu maksaa. Laitemäärä on myös vaikuttaa kustannuksiin, kun tarvitaan VPN-yhteydet useille laitteille. Palvelinkapasiteetti ja infrastruktuurin lisää kustannuksia, jos yrityksen on ylläpidettävä useita palvelimia VPN-yhteyksien hallintaa varten. [24.]

Lisäominaisuudet vaikuttavat myös hinnoitteluun. Jos yritys tarvitsee erityisiä tietoturvaominaisuuksia, kuten monikerroksista tietoturvaa tai tarkkaa käyttäjähallintaa, nämä lisäävät kustannuksia. Tuki ja ylläpito ovat toinen tekijä, joka vaikuttaa hinnoitteluun. Kun yritys haluaa saada teknistä tukea ja palvelun ylläpitoa, se tuo lisähintaa Always on VPN:lle. Receptumille Always on VPN olisi ilmainen, sillä se kuuluisi kaikkiin muihin ohjelmiin lisänä, joka olisi tietenkin hyvä juttu. [24.]

5 Azure VPN

5.1 Tekniikka

Azure VPN on Microsoft Azuren tarjoama palvelu, jonka avulla käyttäjät ja yritykset voivat liittää paikalliset verkkonsa tai yksittäiset laitteet turvallisesti virtuaaliseen verkkoon niin sanotusti Azure-pilvessä. Luomalla suojatun yhteyden Internetin kautta Azure VPN antaa käyttäjille mahdollisuuden käyttää Azure-virtuaaliverkkonsa resursseja ikään kuin he olisivat paikallisessa verkossaan. [25.]

Azure VPN Gateway tukee monipuolisia VPN-protokollia, mukaan lukien Site-to-Site VPN ja Point-to-Site VPN. Tämä mahdollistaa joustavan yhteyksien muodostamisen organisaation paikallisten verkkojen ja Azure-pilven välille. Site-to-Site VPN mahdollistaa turvalliset ja pysyvät yhteydet organisaation eri sijaintien välillä, kun taas Point-to-Site VPN tarjoaa helpon ja turvallisen pääsyn Azure-verkkoon etätyöntekijöille ja kumppaneille. Azure VPN hyödyntää perinteisiä VPN-protokollia, kuten (IKEv2, SSTP ja L2TP/IPSec), mikä mahdollistaa sen käytön monissa erilaisissa verkko-olosuhteissa sekä luo hyvän tietoliikenteen salauksen ja turvallisen avainvaihdon. Kaikki tiedot, jotka kulkevat Azure VPN Gatewayn läpi, ovat suojattuja ja yksityisiä. [26.]

Azure tarjoaa yhden tunnelin suorituskyvyn jopa 1 Gbps ja useilla tunneleilla jopa 1,25 Gbps, mikä parantaa pääsyä VNeteihin. Tämä tapahtuu uusilla yhdyskäytäviä, jotka ovat nimeltään VpnGw1, VpnGw2 ja VpnGw3. VpnGw1 tarjoaa nopeudella 650 Mbps 6,5x nopeuden ja VpnGw2 1Gbps tarjoaa 5x suorituskyvyn parannuksen. VPN-yhdyskäytävä VpnGw3 on 1.25Gbps useilla yhdyskäytävillä, mutta tarvitsee toimiakseen nopeaa ja luotettavaa verkon nopeutta. [27.]

5.2 Mitä hyötyjä ja haittoja Azure VPN:llä on?

Azure VPN:n yksi hyvistä puolista on, että palvelusta maksetaan vain sen verran, mitä sitä käytetään eli periaate ” pay-as-you-go -malli” eli on kustannustehokas. Mutta hinnat voivat nousta korkeiksi suurten liikennemäärien tai

monimutkaisten konfiguraatioiden yhteydessä, jolloin sen käyttö aiheuttaa kustannuksia ja Azure VPN voi tulla kalliiksi.

Yksi Azuren hyödyistä on sen turvallisuus. Se käyttää suojaukseen kaksivaiheista tunnistautumista. Käyttäjät joutuvat antamaan lisävahvistuksen kirjautuessaan VPN-yhteyteen, mikä lisää merkittävästi VPN-palvelun turvallisuutta. Azure VPN mahdollistaa myös eri verkkosegmenttien eristämisen toisistaan, mikä estää haitallisten toimintojen leviämisen verkon sisällä. Yritykset voivat luoda erilliset VPN-yhteydet ja ohjauspolitiikat eri osille verkkoa.

Azure Portal tarjoaa keskitetyn hallinnan VPN-yhteyksille, ja organisaatio voi tarkkailla ja seurata VPN-liikennettä reaaliajassa. Juuri tämän takia se auttaa tunnistamaan mahdolliset uhkat ja tietoturvariskit nopeasti. Azure on myös hyvää, sillä siinä on mahdollisuus luoda varmuuskopioita VPN-asetuksista ja konfiguraatioista. Täten voidaan palauttaa nopeasti toimintakyky ongelmatilanteissa tai hyökkäysten jälkeen, mikä on iso hyöty yrityksissä.

Huono puoli on Gatewayn oikeaoppinen konfigurointi. Sillä Azure vaatii syvempää asiantuntemusta verkkojen ja tietoturvan alueilta, ja virheelliset asetukset voivat aiheuttaa toimintahäiriöitä ja vaarantaa VPN -turvallisuuden. Lisäksi Azuressa ylläpitotehtävät, kuten päivitykset ja vianmääritys, voivat olla vaativia.

Azure VPN Gatewayn suorituskyky voi myös olla haaste, erityisesti suurten liikennemäärien vuoksi. Suorituskyky vaihtelee ja vaikuttaa verkon vasteaikaan. Eli se on otettava huomioon erityisesti yrityksissä, jotka käyttävät vaativia sovelluksia. [28.]

5.3 Ominaisuuksia

Azure VPN tarjoaa laajan valikoiman ominaisuuksia, jotka tekevät siitä houkuttelevan vaihtoehdon yrityksille. Yksi tärkeimmistä ominaisuuksista on monipuolisuus. Se tukee nimittäin useita erilaisia VPN-ratkaisuja ja protokollia. Juuri tämän ansiosta yritys voi valita parhaiten tarpeisiisi sopivan vaihtoehdon, olipa

kyseessä sitten käyttötarkoituksessa Site-to-Site VPN organisaation eri sijaintien välille tai Point-to-Site VPN etäkäyttöä varten.

Azure VPN mahdollistaa myös helpon skaalautuvuuden. Kapasiteettia voidaan lisätä tarpeen mukaan. Tämä soveltuu niin pienille yrityksille kuin suurille organisaatioillekin. Joustavuus tekeekin siitä ihanteellisen ratkaisun yrityksille, joiden tarpeet voivat muuttua ajan myötä. [28.]

Tietoturva on ensisijaisen tärkeää VPN-ratkaisuissa, ja Azure VPN tarjoaa useita tietoturvaominaisuuksia. Azure Active Directoryä voidaan käyttää käyttäjähallintaan ja monikerroksiseen autentikointiin. Azure hyödyntää Azure Firewallia ja muita palomuuriratkaisuja, kun suojataan verkkoyhteyksiä. [28.]

Azure VPN tukee myös verkkojen eristämistä ja erilaisia suojauksen hallintatyökaluja. VPN-yhteyksiä muokataan tarpeiden mukaan ja Azure Monitoria ja Azure Security Centeriä käytetään valvomaan ja hallitsemaan verkkoturvaa reaaliaikaisesti. Se tarjoaa lisäksi hyvän integraation muiden Azure-palveluiden kanssa, eli sitä voidaan yhdistää muihin Azure-ratkaisuihin, kuten Azure Virtual Networkiin ja Azure Active Directoryyn.

Azuressa on myös ominaisuus, jonka avulla voidaan myös helposti hallita ja seurata VPN-yhteyksiä Azure-portaalin avulla. Se tekee ylläpidosta ja vianmäärityksestä vaivatonta. Azure VPN Gateway mahdollistaa turvallisen, joustavan ja helppokäyttöisen tavan integroida Azure-pilven organisaation verkkoinfrastruktuuriin. [29.]

5.4 Hinnoittelu

Azure VPN -ratkaisujen hinnoittelu yrityksissä vaihtelee monten tekijöiden mukaan. Azure on pilvipalvelualusta, joka tarjoaa laajan valikoiman palveluita, mukaan lukien erilaisia VPN-ratkaisuja yrityksille. Hinnoitteluun vaikuttavat tekijät kuten valitut palvelut, kapasiteetti, käyttöaika ja lisäominaisuudet. [28.]

Azure VPN -ratkaisujen hinnoittelu perustuu yleensä käyttäjien tai organisaation tarvitseman kapasiteetin määrään. Mitä enemmän palveluita ja kapasiteettia tarvitaan, sitä suuremmat kustannukset voivat olla. Valitut palvelut vaikuttavat myös hintaan. [30.]

Käyttöaika on toinen merkittävä tekijä hinnoittelussa. Azure käyttää pay-as-you-go-mallia, jossa maksetaan vain käytöstä. Voidaan siis valita joustava maksutapa, joka perustuu täysin siihen aikaan, kuinka paljon palvelua käytetään. Tämän lisäksi yritys voi harkita pidempää sopimusaikaa, mikä voi tarjota alennuksia. Eli se on paras vaihtoehto isoille yrityksille. [31.]

Lisäominaisuudet, kuten varmuuskopiot, valvonta ja tuki, voivat myös vaikuttaa hinnoitteluun. Organisaation erityistarpeet ja vaatimukset vaikuttavat siihen, mitä lisäominaisuuksia tarvitaan, ja siten myös hintaan. [31.]

6 VPN:n valinta

6.1 Vertailu ja päätös

Tutkimuksen tarkoituksena oli löytää Receptumille uusi VPN nykyisen tilalle, ja lähdimme tutkimaan asiaa eri näkökohtien kautta. Merkittäviä tekijöitä olivat VPN:n tekniikka, hinta, VPN:n tarjoamat ominaisuudet sekä VPN:n hyvät ja huonot puolet. Näitä asioita selvitimme etsimällä tarkat tiedot molemmista VPN-ratkaisuista.

Kun olimme tarkastelleet tietoja ja keskustelleet pitkään työnantajan kanssa, päätimme valita Azure VPN:n. Azure valittiin pääasiassa siksi, ettei Receptum enää halunnut fyysisiä laitteita, vaan kaikki toiminnot ja ominaisuudet haluttiin siirtää pilveen. Lisäksi Receptum oli siirtymässä yhä enemmän pilvipalveluiden käyttöön.

Awlays On VPN:nnässä "Always On" -toiminto on erinomainen, sillä sitä ei tarvitse erikseen käynnistää – VPN-yhteys muodostuu automaattisesti, kun käyttäjä käynnistää tietokoneen. Tämä tarjoaa hyvän käyttäjäkokemuksen niille,

joilla ei ole laajaa kokemusta tietokoneista. Mutta voimme myös käyttää Always On -toimintoa ja konfiguroida sen Azure VPN -tunneleihin, jolloin saamme saman toiminnon myös Azure VPN:lle. Voimme siis halutessamme määritellä Azure VPN -yhdyskäytävän tunnistamaan RADIUS-palvelimen, joka tukee "Always On VPN" -yhteyksiä. On kuitenkin huomioitava, että RADIUS-palvelimen on oltava saavutettavissa VPN-yhdyskäytävän aliverkosta.

Teknisten näkökohtien osalta huomasimme, että molemmat VPN-ratkaisut tukevat suurta osaa samoista tekniikoista. Niissä ei siis ollut merkittäviä eroja, emmekä siten voineet valita parempaa ratkaisua Receptumille pelkästään näiden tekijöiden perusteella. Molemmat tukivat samankaltaisia protokollia, kuten IKEv2, SSTP ja L2TP/IPSec.

Lisäksi huomasimme tutkimuksissamme, että Azuren skaalautuvuus on erinomaista, ja voimme helposti lisätä käyttäjiä tarpeen mukaan. Tämä tuo myös lisäturvaa valintaamme. Always On VPN:ssä on kuitenkin haittapuolena se, että se ei tue vanhempia Windows-versioita, mikä voisi vaatia Receptumin käyttäjiä päivittämään koneet uusimpiin Windows-versioihin. Tämä voi aiheuttaa toiminnan haasteita, koska vanhempia Windows-versioita ei välttämättä haluta päivittää. Azure VPN:n konfigurointi voi olla vaativampaa kuin Always On VPN:n, mutta Receptumissa on osaavaa henkilöstöä, joka auttaa oikeiden konfiguraatioiden tekemisessä ilman ongelmia.

Hinta oli yksi tarkastelun kohteista, ja Always On VPN on selvästi edullisempi vaihtoehto kuin Azure VPN. Nykyisten sertifikaattien ansiosta Receptumin on saanut Microsoftilta partnerisopimuksen, jonka takia ei tarvitsisi maksaa mitään Always On VPN:n käytöstä. Toki saattaa tulla joitain pieniä lisämaksuja, jos halutaan lisäominaisuuksia. Vertailun perusteella Azure VPN voisi tulla kalliiksi, koska Microsoft laskuttaa liikenteen mukaan, eli mitä enemmän käytetään sitä enemmän maksaa, vaikka yrityksellä olisi Microsoftin partnerisuus. Ratkaisuna tähän voisi olla liikenteen rajoittaminen vain niihin tarpeellisiin kohteisiin, jotka vaativat VPN-yhteyden, kuten Kelan, Ruotsin ja Norjan yhteydet sekä muut

vastaavat yhteydet eikä käytettäisi Receptumin OneDrivea, Outlookia ja SharePointia VPN:nä. Tällä tavoin voitaisiin minimoida liikenne ja alentaa hintaa.

6.2 Miten sopisi Receptumille?

Receptumin siirtäessä yhä enemmän resursseja pilveen ja pyrkiessään lopulta siirtymään kokonaan pilvipohjaiseen ympäristöön Azure VPN on täydellinen VPN-vaihtoehto Receptumille. Azure on täysin pilvipohjainen ja tarjoaa mahdollisuuden luoda turvallisen yhteyden Azure-pilviin ja muihin Azure-verkkoihin ilman tarvetta hallita omaa VPN-infrastruktuuria. Azuren avulla voidaan myös poistaa tarve fyysiselle laitteistolle, joka aikaisemmin ylläpiti VPN-yhteyksiä Receptumin tiloissa.

Receptumin työntekijämäärä ja VPN-yhteyden tarve vaihtelevat, joten Azuren skaalautuvuus on merkittävässä roolissa. Resursseja voidaan skaalata ylös tai alas tarpeen mukaan, mikä voi säästää kustannuksia ja varmistaa tehokkaan käytön. Samalla voidaan helposti lisätä tai vähentää kapasiteettia ilman fyysisiä laitteiden muutoksia.

Azure VPN:n hallinta ja seuranta ovat helppoa Azure Portalin kautta. Receptum voi valvoa ja konfiguroida VPN-yhteyksiä keskitetysti, mikä vähentää ja yksinkertaistaa VPN-ympäristön ylläpitoa. Tietoturva on erityisen tärkeää Receptumille, ja Azure tarjoaa laajan valikoiman tietoturvapalveluita, kuten Azure Security Centerin, joka auttaa havaitsemaan ja torjumaan päivittäin kohdistuvia tietoturvariskejä.

Receptum käyttää päivittäin Azure Active Directorya tunnistautumiseen ja käyttöoikeuksien hallintaan, ja Azure VPN tarjoaa hyvän integraation sen kanssa. Tämä mahdollistaa helpon ja turvallisen pääsyn hallintaan ja käyttöoikeuksien hallintaan, mikä on tärkeä osa Receptumin tietoturvaa.

Receptumin työntekijät työskentelevät eri puolilta Suomea ja jopa ulkomailta, joten yhteisen verkon tarve on olennainen. Azure VPN:n avulla voidaan helposti

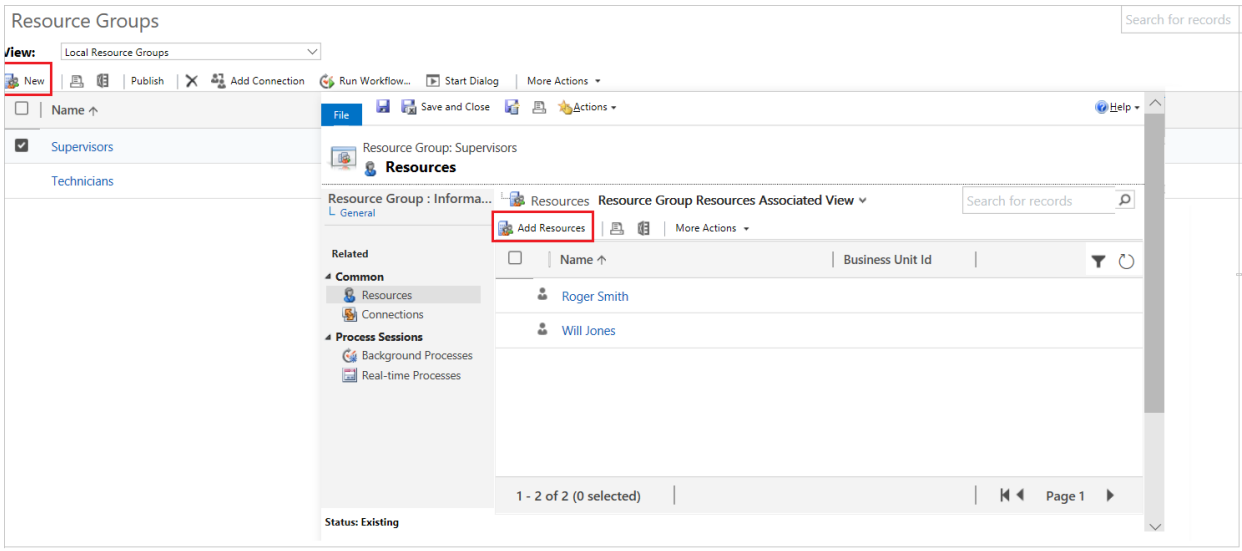
luoda ja yhdistää eri käyttäjät ja sijainnit yhteen yksityiseen verkkoon, joka on erityisen hyödyllistä Receptumille, ja joka toimii hajautettujen tiimien ja toimistojen kanssa eri paikoissa, mikä helpottaa yhteistyötä ja resurssien jakamista yrityksen sisällä.

7 Teoreettinen käyttöönotto

7.1 Suunnittelu

Lähdimme suunnittelemaan Azure VPN:n käyttöönottoa yrityksen kanssa tarpeiden kartoituksen kautta. Mietimme, miksi tarvitsimme VPN:ää, kuinka monta yhteyttä tarvitsemme, resurssiryhmän luominen ja kuinka paljon voimme laittaa resursseja tähän. Ensimmäiseksi päädyimme siihen, että tavoitteena olisi liittää etätyöntekijöitä yrityksen verkkoon. Tähän VPN-ratkaisuksi valitsimme Point to Site -ratkaisun. Toiseksi mietimme, että aluksi valitsisimme meidän testiryhmäämme 5-10 testikäyttäjää, jottei saataisi kaaosta aikaiseksi yrityksessä, jos alettaisiin vaihtamaan heti nykyistä VPN:ää pois. Lisäksi saisimme nopeasti palautteen käyttäjiltä, miten VPN toimii, mitä asetuksia pitäisi muuttaa ja pitäisikö kehittää ja muokata meidän määritelmiämme Azuressa.

Receptumin siirtyessä kokonaan Azuren pilvipalveluiden maailmaa, ei tarvitse miettiä Azure-tilin luomista, vaan voimme käyttää nykyisiä tilejä. Tähän projektiin loimme uuden resurssiryhmän (katso kuva 8), jotta on helpompi ohjata projektiamme. Loisimme ryhmän nimeltä ” AzureVPN-ReceptumTesti”. Kun olemme tämän vaiheen tehneet, odotamme ja seuraamme prosessia, jonka jälkeen saamme ilmoituksen onnistuneesta ryhmän luomisesta. Näiden ollessa valmista, voimme lisätä omat tarvittavat resurssit kuten Virtual Networkin sekä VPN Gatewayn. Sen jälkeen rupeamme rakentamaan ja toteuttamaan meidän VPN-konfigurointejamme. [33.]

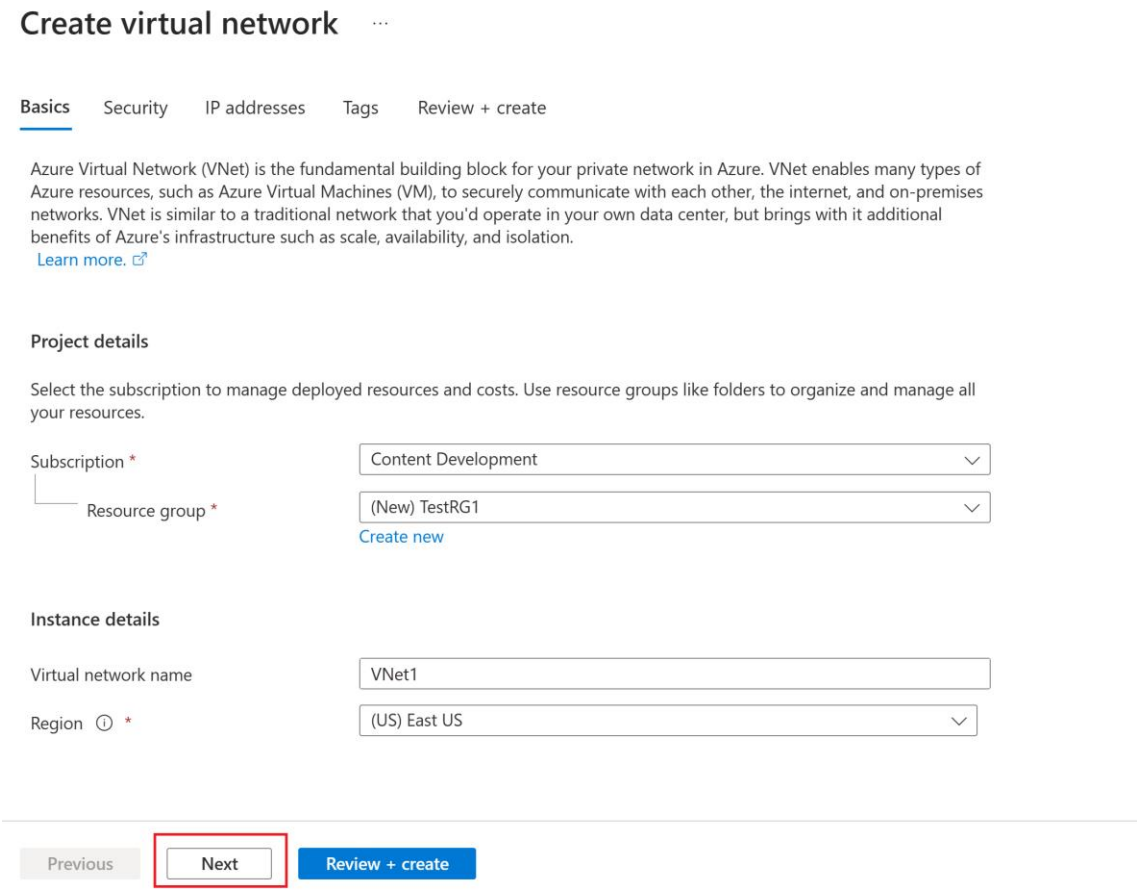


Kuva 8. Resurssiryhmän luominen [33]

7.2 Toteutus

Aloitimme toteutuksen tekemällä resurssiryhmäämme Virtual Networking Microsoftin ohjeiden mukaisesti. Tämä toimii virtuaalisen verkon perustana. Teemme erikseen virtuaalisenverkon käyttämällä Azure-portaalia, jotta se olisi mahdollisimman yksinkertaista tehdä. Ensimmäiseksi olemme tehneet jo suunnitteluvaiheessa resurssiryhmän, jonne teemme meidän uuden virtuaalisen verkkomme. Etsimällä Azure-portaalista virtuaaliset verkot, voimme luoda ja alkaa muokkaamaan sitä haluamillemme asetuksille. Ensimmäiseksi kuvassa 9 pystymme lisäämään oman tilauksemme, resurssiryhmämme, nimen virtuaaliselle verkolle sekä vielä sen, mikä on oma alueemme. Näihin tietoihin vaihdamme jo

tekemämme resurssiryhmän nimen sekä eri toimialueen eli North Europen.

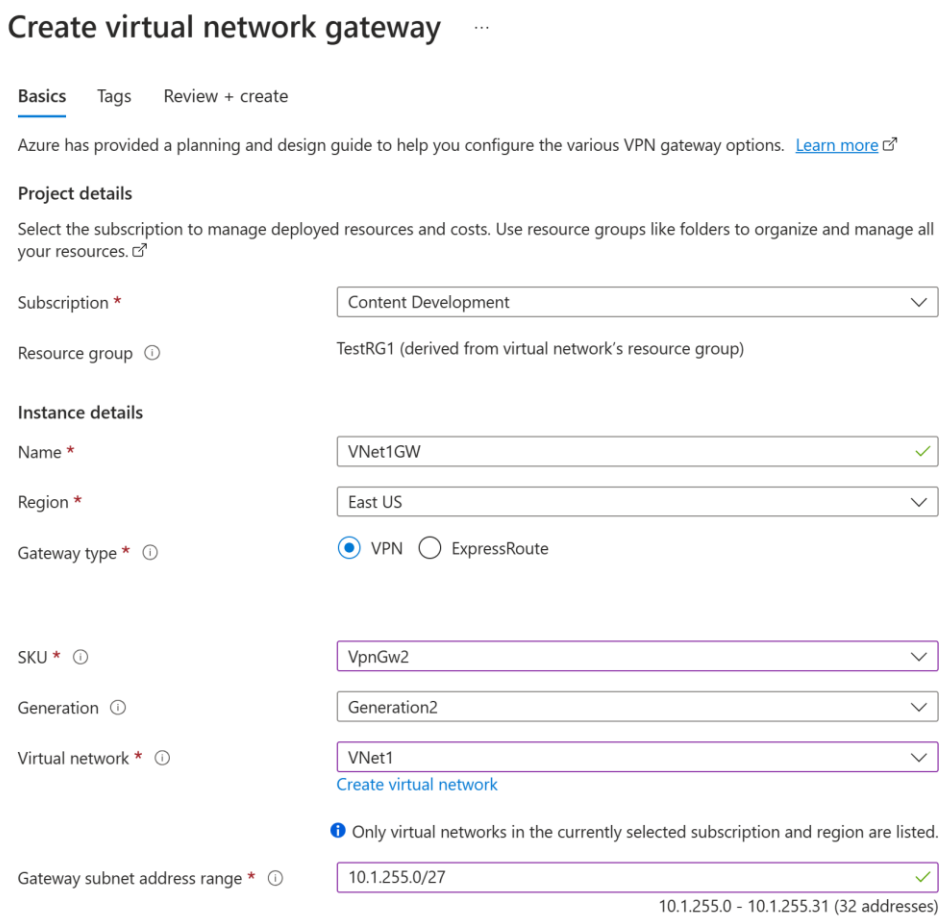


Kuva 9. Azuren virtuaaliset verkkoasetukset [34]

Seuraavissa välilehdissä jätimme kaikki asetukset oletusasetuksiin, sillä meidän ei tarvinnut muokata niitä. Täten voimme nyt katsoa ja luoda meidän tekemämme virtuaalisen verkon ja tämä osio on valmis. Seuraavaksi teemme meille VPN Gatewayn.

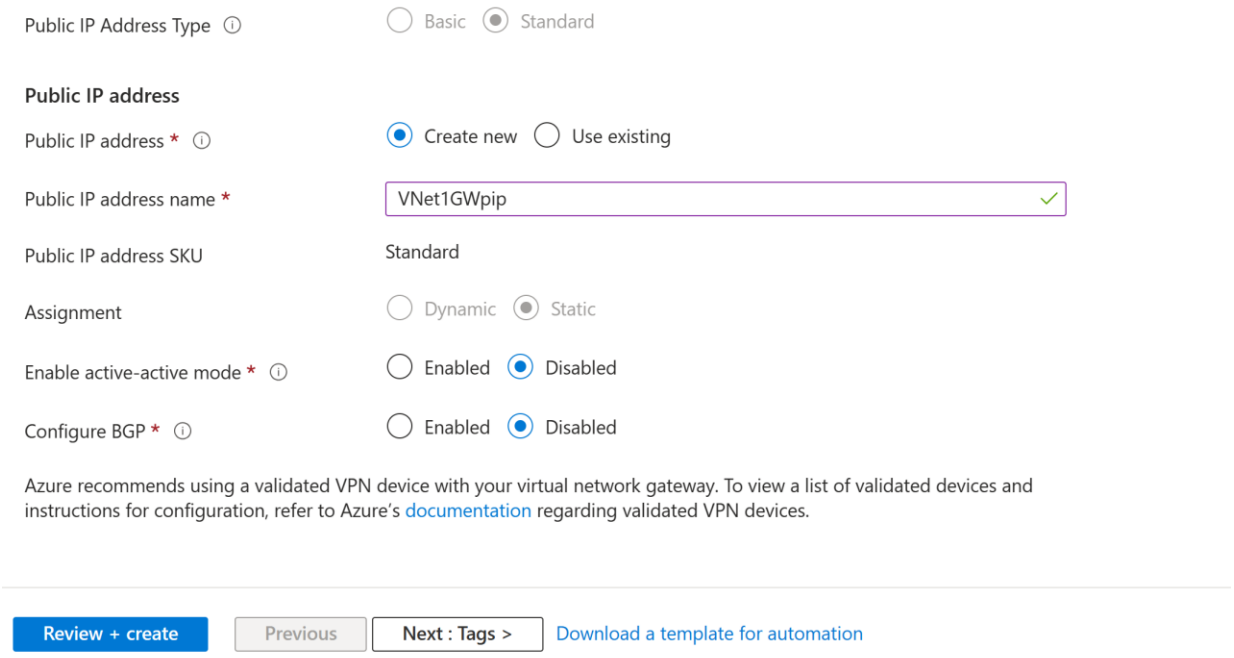
7.2.1 VPN Gatewayn luonti

Aloitamme samalla tavalla kuin virtuaalisen verkonluonnissa eli etsimme taas Azure-portaalista VPN Gatewayn, josta avautuu ”Basics” -näkymä (katso kuva 10), johon voimme alkaa taas muokkaamaan omia asetuksia.



Kuva 10. VPN Gatewayn asetukset [34]

Lisäämme taas oman nimen Gatewaylle ja juuri luomamme virtuaalisen verkkomme sekä vaihdamme alueen North Europeen, jotta saamme mahdollisimman hyvän yhteyden. Meidän ei tarvitse välittää ”Gateway subnet address rangesta”, sillä meillä on virtuaalisessa verkossa gateway subnet eli tuota kohtaa ei edes näy. Seuraavaksi määritellään julkinen IP-osoite kuvassa 11. Nämä asetukset määrittävät julkisen IP-osoiteobjektin, joka liitetään VPN-yhdyskäytävään. Julkinen IP-osoite määritetään tälle objektille, kun VPN-yhdyskäytävä luodaan. Ainoa kerta, kun ensisijainen julkinen IP-osoite muuttuu, on yhdyskäytävän poistaminen ja luominen uudelleen. [34.]



Kuva 11. Julkisen IP-osoitteen arvot [34]

Kun olemme tehneet nämä, voimme tarkistella asetuksiamme ja todetessamme, että kaikki on kunnossa, luodaan VPN gateway, jossa voi mennä peräti 45 minuuttia. Seuraavaksi luomme meille tarvittavat sertifikaatit. [34.]

7.2.2 Sertifikaattien luonti

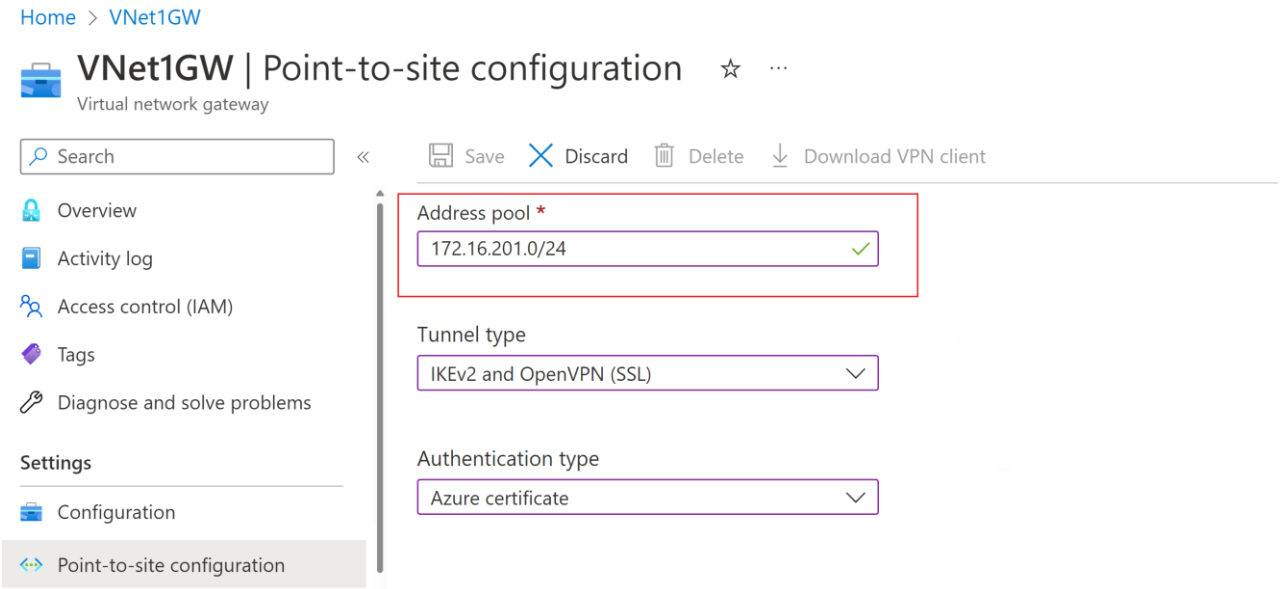
Azure käyttää varmenteita asiakkaiden todentamiseen, jotka muodostavat yhteyden virtuaaliseen verkkoon point-to-site VPN-yhteyden kautta. Tarvitsemme siis varmenteen, jotta voimme käyttää yhteyttä. Kun olemme hankkineet juurivarmenteen, meidän tulee ladata julkisen avaimen tiedot Azureen. Tämä juurivarmenne on "luottettu" Azuressa ja antaa P2S-yhteyden kautta yhteyden virtuaaliseen verkkoon. Juurivarmenteessa käytämme jo olemassa olevaa varmenneketjua, sillä tarvitsemme yritysvarmennetta. [34.]

Jokaisessa asiakastietokoneessa, jonka yhdistämme virtuaaliseen verkkoon Point-to-Site-yhteydellä, on oltava asennettuna asiakasvarmenne. Luomme tämän varmenteen juurivarmenteesta ja asennamme sen jokaiselle

asiakastietokoneelle. Jos tätä ei ole tehty oikein, todennus epäonnistuu, kun yritämme muodostaa yhteyden virtuaaliseen verkkoon. Teemme taas yritysserti-fikaatin mukaisesti eli aluksi luodaan asiakasvarmenne, jonka yleisnimen arvo on nimi@omaverkkotunnus.com. Tämän jälkeen varmistamme, että asiakasvar-menne perustuu käyttäjän varmennemalliin, jonka käyttäjäluettelon ensimmäi-senä kohteena on Client Authentication. [34.]

7.2.3 P2S-konfigurointi

Siirrymme seuraavaksi määrittelemään P2S-yhteyden konfiguroinnit. Menemme luomaamme yhdyskäytävään ja valitsemme vasemmasta ruudusta Point-to-site-määritykset. Lisäämme Address pool box -kohdassa yksityisen IP-osoitealueen, jota haluamme käyttää (katso kuva 12). VPN-asiakkaat saavat dynaamisesti IP-osoitteen määrittelemältämme alueelta. Aliverkon vähimmäispeite on 29-bittinen aktiiviselle/passiiviselle määritykselle ja 28-bittinen aktiiviselle/aktiiviselle määri-tykselle.

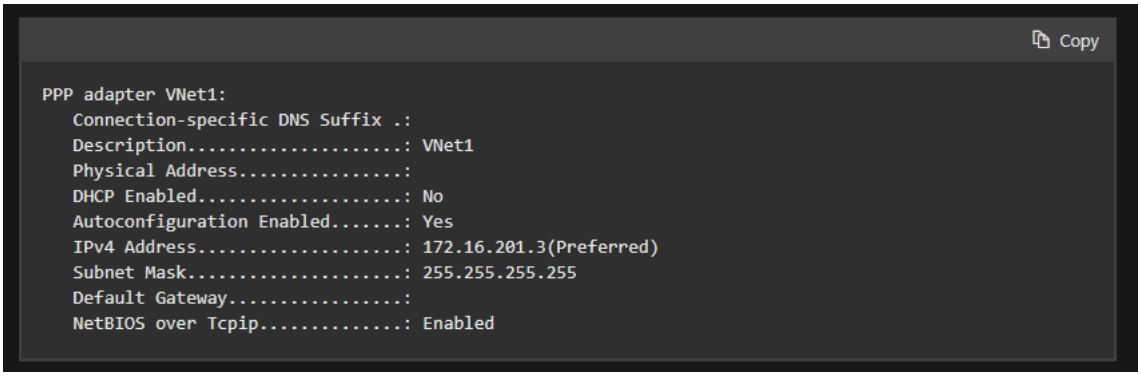


Kuva 12. P2S-konfiguraatio ikkuna [34]

Tunnelityypiksi voimme valita useita tunnelityyppejä, kuten IKEv2 ja Open-VPN(SSL) tai IKEv2 ja SSTP (SSL). Tällä kertaa valitsemme tähän IKEv2- ja

OpenVPN (SSL) -tunnelityypin, kuten kuvassa x nähdään. Lopuksi valitsemme vielä Azure-sertifikaatin Authentication typeen. [34.]

Lopuksi tarvitsee vielä lisätä meidän juuri sertifikaatin ja asiakassertifikaatin, jotta P2S-yhteys toimisi. Näin olemme saaneet tehtyä omat konfiguroinnit P2S-yhteyden luomiseen. Tarvitsemme vielä Azure VPN Clientin sekä lopuksi testata yhteyttä. Käyttämällä komentokehotetta ja suorittamalla ipconfig/all -komennon, joka antaa kuvan 13 mukaisen ikkunan. [34.]



Kuva 13. Komentokehote komennolla ipconfig/all [34]

7.3 Jatko

Jatkoa nähden on tärkeä suunnitella myös uudet reititykset ja avaukset kelaan sekä muihin vastaaviin paikkoihin kuten Ruotsiin tai Norjaan, sillä nykyinen Direct Access ei pääse tiettyihin paikkoihin vaan on käytettävä toista VPN:ää, jotta nuo yhteydet toimisivat. Eli on tärkeätä reitittää oikealla tavalla liikenne, ettei joutuisi käyttämään eri VPN-yhteyksiä eri paikkoihin, jos esimerkiksi kelan liikenne halutaan yrityksen pääkonttorin kautta, jolloin sen on pakko mennä sitä kautta toimiakseen.

Kun olemme ottaneet uuden VPN-ratkaisun käyttöön, on ensiarvoisen tärkeää tarjota käyttäjille riittävä koulutus ja ohjeistus. Voitaisiin esimerkiksi toteutetaa tekemällä selkeä ja helppolukuinen käyttöohje, joka auttaa käyttäjiä

ymmärtämään, miten ottaa yhteys Azure VPN:nään, mitä turvallisuuskäytäntöjä noudattaa ja kuinka hyödyntää VPN:nää tehokkaasti.

On myös tärkeää suunnitella, miten seuraamme sekä ylläpidämme uutta VPN:ää. Siihen voisi sisältyä VPN-yhteyksien aktiivinen seuranta, sertifikaattien hallinta ja päivitysten aikatauluttaminen. Lisäksi on äärimmäisen tärkeää laatia varmuuskopiointi- ja palautussuunnitelma Azure VPN -konfiguraatiolle. Suunnitelma auttaisi varmistamaan, että yrityksemme voisi palauttaa VPN-toiminnan normaaliksi mahdollisten häiriöiden, vikojen tai katkosten takia.

Jatkossa tarvitsemme vielä Receptumin oikeat IP-osoitteet ja myöhemmin selviävät lisäkonfiguraatiot. Lisäksi suoritamme oikean käyttöönoton yhteydessä VPN-konfiguraatiot, jotta Always On -toiminnallisuus toimii. Eli tämä tarkoittaa, että kun kone käynnistetään, se muodostaa automaattisesti yhteyden VPN:ään eikä käyttäjän tarvitse erikseen liittyä siihen. Kun olemme saaneet nämä asiat kunnolla valmiiksi ja testanneet Azure VPN:n toiminnan, voimme ottaa sen käyttöön koko Receptumissa ja poistaa Direct Accessin käytöstä kokonaan.

8 Tulokset ja yhteenveto

Opinnäytetyön tarkoituksena oli valita kahden VPN-vaihtoehdon väliltä toinen. Tutkimme molempien ominaisuuksia ja harkitsimme tulevaisuutta Receptumin näkökulmasta. Lopulta päätimme valita Azure VPN:n. Yksi keskeinen syy Azure VPN:n valintaan oli Receptumin tuleva siirtyminen kokonaan pilvipalveluiden käyttöön ja tarve luopua fyysisistä laitteista.

Tutkimustyö sujui hyvin, ja onnistuin myös tekemään teoreettisen käyttöönoton Azure VPN:lle Microsoftin ohjeiden avulla. Kuitenkin on tärkeä huomioida, että teoreettinen käyttöönotto tehtiin kiireellisen aikataulun vuoksi, jolloin käytettiin oletusarvoja eikä voitu vielä tarkasti määrittää kaikkia arvoja, koska konkreettista käyttöönottoa ei ollut tehty. Todellisessa käyttöönotossa voi olla muutoksia, eikä ohjeiden mukaan toimiminen aina ole mahdollista. Ongelmia aiheutui myös hinnoittelun osalta, sillä se voi vaihdella useiden tekijöiden, kuten

käyttäjämäärän ja olemassa olevien sertifikaattien, perusteella. Siksi esitetyt hinnat olivat vain karkeita arvioita ja tarkentuvat vasta käytännön käyttöönoton yhteydessä.

Yhteenvetona voidaan todeta, että olemme onnistuneet valitsemaan sopivan VPN-ratkaisun ja hankkineet kattavan käsityksen molemmista vaihtoehdoista. Azure VPN sopii parhaiten Receptumin tulevaisuuden tarpeisiin, koska se on täysin pilvipohjainen ratkaisu. Olemme myös luoneet teoreettisen käyttöönotto-mallin, joka toimii apuna oikean käyttöönoton suunnittelussa Receptumille.

Lähteet

1 DirectAccess. 2023. Verkkoaineisto. < https://learn.microsoft.com/en-us/windows-server/remote/remote-access/directaccess/directaccess>. 20.6.2023. Luettu 5.9.2023.

2 Hicks, Richard m. 2016. Verkkoaineisto. DirectAccess vs. VPN. < https://directaccess.richardhicks.com/2016/02/08/directaccess-vs-vpn/>. 8.2.2016. Luettu 5.9.2023.

3 Pietroforte, Michael. 2009. Verkkoaineisto. Windows 7 DirectAccess – Features. < https://4sysops.com/archives/windows-7-directaccess-features/>. 2.2.2009. Luettu 6.9.2023.

4 What Is a VPN?. Verkkoaineisto. < https://www.proofpoint.com/au/threat-reference/vpn>. Luettu 6.9.2023

5 Mikä on VPN?. Verkkoaineisto. < https://www.proofpoint.com/au/threat-reference/vpn>. Luettu 6.9.2023.

6 What Is a Business VPN? Understand Its Uses and Limitations. Verkkoaineisto. < https://www.paloaltonetworks.com/cyberpedia/what-is-a-business-vpn-understand-its-uses-and-limitations>. Luettu 7.9.2023

7 Kwabena-Adade, Grace Dzifa. Yeboah-Boateng, Ezer Osei. 2020. Verkkoaineisto. Remote Access Communications Security: Analysis of User Authentication Roles in Organizations. <https://www.scirp.org/journal/paperinformation.aspx?paperid=101548>. 3.7.2020. Luettu 8.9.2023.

8 Mikä on VPN-tunneli?. Verkkoaineisto. < https://www.expressvpn.com/fi/what-is-vpn/vpn-tunnel>. Luettu 8.9.2023.

9 Harrington, Jan L. 2007. Kirja. Ethernet Networking for the Small Office and Professional Home Office. < https://www.sciencedirect.com/topics/computer-science/point-tunneling-protocol>. Luettu 9.9.2023.

10 Zola, Andrew. Gillis, Alexander S. 2022. Verkkoaineisto. Internet Key Exchange (IKE). < https://www.techtarget.com/searchsecurity/definition/Internet-Key-Exchange>. 1.2.2022. Luettu 9.9.2023.

11 Interpreting IKEv2 IKE SA states. 2014. Verkkoaineisto. <https://www.ibm.com/docs/en/zos/2.1.0?topic=exchanges-interpreting-ikev2-ike-sa-states>. Luettu 9.9.2023.

12 User Authentication. Verkkoaineisto. < https://www.softether.org/4-docs/1-manual/2._SoftEther_VPN_Essential_Architecture/2.2_User_Authentication>. Luettu 10.9.2023.

13 Loshin, Peter. 2021. Verkkoaineisto. CHAP (Challenge-Handshake Authentication Protocol). < https://www.techtarget.com/searchsecurity/definition/CHAP-Challenge-Handshake-Authentication-Protocol>. 1.9.2021. Luettu 10.9.2023.

14 Extensible Authentication Protocol (EAP) for network access. 2023. Verkkoaineisto. < https://learn.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/network-access?tabs=eap-tls%2Cserveruserprompt-eap-tls%2Ceap-sim>. 19.6.2023. Luettu 10.9.2023.

15 Sheldon, Robert. 2023. Verkkoaineisto. Protected Extensible Authentication Protocol (PEAP). < https://www.techtarget.com/searchsecurity/definition/PEAP-Protected-Extensible-Authentication-Protocol>. Luettu 10.9.2023.

16 York, Helga. 2023. Verkkoaineisto. Main Types of VPN and Their Features. < https://www.helpwire.app/blog/vpn-types/>. 2.3.2023. Luettu 11.9.2023.

17 About Point-to-Site VPN. 2023. Verkkoaineisto. About Point-to-Site VPN. <https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about>. Luettu 11.9.2023

18 What Is a Remote Access VPN?. Verkkoaineisto. < https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn>. Luettu 12.9.2023.

19 Holetzky, Sherry. 2023. Verkkoaineisto. What is a Mobile VPN?. <https://www.easytechjunkie.com/what-is-a-mobile-vpn.htm?expand_article=1>. Luettu 12.9.2023.

20 Shutong, Liu. 2022. Arti Verkkoaineisto kkeli. What Is SSL VPN?. < https://info.support.huawei.com/info-finder/encyclopedia/en/SSL+VPN.html>. 9.8.2022. Luettu 13.9.2023.

21 WELEKWE, AMAKIRI. 2022. Verkkoaineisto. Always On VPN -The Business & IT Use Case. < https://www.comparitech.com/net-admin/always-on-vpn-business-it/>. 24.2.2022. Luettu 14.9.2023.

22 Hicks, R. M. N.d. Verkkoaineisto. DirectAccess is now Always On VPN. <https://directaccess.richardhicks.com/directaccess-is-now-always-on-vpn/>. Luettu 14.9.2023.

23 About Always On VPN. 2023. Verkkoaineisto. < https://learn.microsoft.com/en-us/windows-server/remote/remote-access/overview-always-on-vpn>. 23.5.2023. Luettu 15.9.2023.

24 KINDON, JAMES. 2020. Verkkoaineisto. Microsoft Always-On VPN. < https://www.insentragroup.com/us/insights/geek-speak/modern-workplace/microsoft-always-on-vpn/>. 9.4.2020. Luettu 15.9.2023.

25 Kumar Arjun. 2023. Verkkoaineisto. What is Azure VPN. < https://www.linkedin.com/pulse/what-azure-vpn-arjun-kumar>. 2.4.2023. Luettu 16.9.2023.

26 About VPN devices and IPsec/IKE parameters for Site-to-Site VPN Gateway connections. 2023. Verkkoaineisto. < https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices>. 6.10.2023. Luettu 19.9.2023.

27 Khalidi,Yousef. 2017. Verkkoaineisto. New Azure VPN Gateways now 6x faster. < https://azure.microsoft.com/en-us/blog/new-azure-vpn-gateways-now-6x-faster/>. 13.6.2017. Luettu 20.9.2023.

28 What is Azure VPN Gateway?. 2023. Verkkoaineisto. < https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>. Luettu 21.9.2023.

29 VPN Gateway. Verkkoaineisto. < https://azure.microsoft.com/en-us/products/vpn-gateway>. Luettu 21.9.2023.

30 Azure pricing. Verkkoaineisto <https://azure.microsoft.com/en-us/pricing/#product-pricing>. Luettu 21.9.2023.

31 Solokhine, Serguei. 2022. Verkkoaineisto. What is Azure VPN, and how does it work?. < https://www.techradar.com/features/what-is-azure-vpn-and-how-does-it-work >. 26.7.2022. Luettu 22.9.2023.

32 M. HICKS, RICHARD. 2019. Verkkoaineisto. Always On VPN with Azure Gateway. < https://directaccess.richardhicks.com/2019/08/26/always-on-vpn-with-azure-gateway/>. 26.8.2019. Luettu 23.9.2023.

33 Resurssiryhmän luominen tai muuttaminen (Customer Service -sovellus). 2023. Verkkoaineisto. < https://learn.microsoft.com/fi-fi/dynamics365/customer-service/create-edit-resource-group>. Luettu 5.10.2023.

34 Configure server settings for P2S VPN Gateway connections - certificate authentication - Azure portal. Verkkoaineisto. <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>. Luettu 9.10.2023.