Tampereen ammattikorkeakoulu

Always On VPN:n käyttöönotto

Kimmo Ylimäki

OPINNÄYTETYÖ
Toukokuu 2020

Tietojenkäsittely
Tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma
Tietoverkot

YLIMÄKI, KIMMO
Always On VPN:n käyttöönotto

Opinnäytetyö 37 sivua
Toukokuu 2020

Tämän opinnäytetyön tavoitteena oli löytää helppokäyttöinen, luotettava, nopea ja taloudellisesti sopiva etäyhteyspalvelu korvaamaan toimeksiantajan nykyinen käytössä oleva palvelu. Opinnäytetyön tarkoituksena oli löytää tähän käyttötarkoitukseen soveltuva palvelu vertailemalla eri etäyhteyspalveluiden ominaisuuksia. Korvattava järjestelmä oli vanhentunut ja liian kallis toiminnallisuuteen nähden.

Opinnäytetyön käytännön tehtävänä oli asentaa uusi etäyhteyspalvelu yrityksen omalle palvelinalustalle ja saada se toimimaan mahdollisimman hyvin. Tutkimuksessa tultiin tulokseen, ettei nykyaikaisten etäyhteyspalveluiden välillä ole valtavia eroavaisuuksia toiminnallisuuden tai turvallisuuden osalta. Suurimmat eroavaisuudet löytyvät käyttöönotossa.

Ongelmia palvelun toimivaksi saamiseksi oli loppujen lopuksi vähän ja ne ratkesivat muutaman tunnin tutkimisen jälkeen. Suurin haaste toteutusvaiheessa oli koneiden oma palomuuri, joka esti liikennettä ulkoverkkoon. Eniten ongelmia tutkimusvaiheessa tuottivat erilaisten salaus- ja selvennysprotokollien ominaisuuksien vertaileminen. Toimeksiantaja on ollut tyytyväinen uuden etäyhteyspalvelun toimintaan ja aikoo jatkossa käyttää pääasiallisena palveluna.

Asiasanat: tietoverkot, vpn, always on vpn

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Network Services

YLIMÄKI, KIMMO
Deploying Always On VPN

Bachelor's thesis 37 pages
May 2020

The aim of this thesis was to find an easy-to-use, reliable, fast and economically suitable remote connection service to replace the client's current service. The purpose of this thesis was to find the service suitable by comparing the features of different remote connection services. The system to be replaced was outdated and too expensive in terms of its functionality.

The practical task of the thesis was to install a new remote connection service on the company's own server platform and to make it work as well as possible. The study concluded that there are no major differences in functionality or security between modern remote access services. The biggest differences are in the implementation.

In the end, there were very few problems in making the service work, and they were resolved after a few hours of research. The biggest challenge during the implementation phase was the client computers own firewall, which blocked traffic to the external network. Comparing the properties of different encryption and authentication protocols posed the most problems in the research phase. The client has been satisfied with the new remote access service and intends to use it mainly for its remote connections in the future.

Key words: information networks, vpn, always on vpn

SISÄLLYS

1 JOHDANTO 6
2 MIKÄ ON VPN? 8
2.1. VPN-protokollat 10
2.1.1 OpenVPN 11
2.1.2 IKEv2/IPsec 11
2.1.3 L2TP/IPsec 12
2.1.4 PPTP 12
2.1.5 SSTP 13
2.2. Autentikointiprotokollat 14
2.2.1 PAP – Password Authentication Protocol 14
2.2.2 CHAP – Challenge-handshake authentication protocol 15
2.2.3 EAP 15
2.3. Palvelimelle asennettava VPN-palvelu 16
2.3.1 Always On VPN 17
2.3.2 StrongSwan 17
2.3.3 SoftEther 18
2.3.4 WireGuard 18
3 YMPÄRISTÖ 20
3.1. Verkko 20
3.2. Palvelimet 21
4 KÄYTTÖÖNOTTO 22
4.1. Verkon muutokset 23
4.2. Palvelin 25
4.2.1 RRAS-palvelun asennus 27
4.2.2 RRAS-palvelun käyttöönotto 27
4.2.3 NPS 28
4.2.4 Active Directory ryhmän luominen 29
4.2.5 PKI:n asennus 29
4.3. DNS ohjaus 30
4.4. Palomuuri 30
4.5. Ongelmat 32
5 POHDINTA 33
LÄHTEET 35

ERITYISSANASTO

AD CS	Active Directory Certificate Services
AES	Advanced Encryption Standard
Authentication	Varmennus, todennus
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Dynamic Name Server
Encryption	Salaus
ESP	Encapsulating Security Payload
HTTPS	Hypertext Transfer Protocol Secure
ID	Identity
IP	Internet Protocol
MOBIKE	Mobility and Multihoming
MPLS	Multiprotocol Label Switching
NAT	Name Address Translation
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
RRAS	Routing and Remote Access Service
SHA	Secure Hash Algorithm
SMS	Short Message Service
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

1 JOHDANTO

Tämän opinnäytetyön tavoite on luoda toimeksiantajalle luotettava ja helppokäyttöinen etäyhteyspalvelu sekä kartuttaa opinnäytetyön luojan ammattitaitoa. Tarkoituksena on vertailla erilaisia VPN-palveluita toisiinsa käyttäen hyväksi erilaisia internetistä löytyviä lähteitä. Nykyisen etäyhteyspalvelun heikkoutena on, että jokaisesta käyttäjästä pitää maksaa kiinteä kuukausimaksu riippumatta siitä kuinka paljon palvelua käytetään. Palvelu on myös tekniikaltaan vanhentunut ja ajoittain liian hidas asiakkaan käyttötarkoitukseen. Tässä opinnäytetyössä on muutettu kaikki asiakkaan IP-osoitteet, palvelinten nimet sekä yrityksen nimi toimeksiantajan yksityisyyden suojaamiseksi. Tämä ei vaikuta teknisestä näkökulmasta katsottuna dokumentin ajankohtaisuuteen.

Asiakkaan tarve uudelle etäyhteyspalvelulle ei ole kriittinen, mutta päivitys on pitkään toivottu asia. Useat työntekijät tarvitsevat pääsyn palvelimelle työskennellessään etänä eri puolella Suomea sekä mahdollisesti ulkomailla. Työntekijät joutuvat olemaan pitkiäkin aikoja yritysverkon ulkopuolella mikä tekee etäyhteyspalvelusta välttämättömän yrityksen toiminnalle. Yhteyden avulla ajetaan muutamia ohjelmia palvelimelta, joiden käyttö vaatii tietyn kiinteän IP-osoitteen ulkoverkossa kyseisiä ohjelmia varten. Yhteyttä käytetään myös tiedostojen siirtämiseen palvelimelle sekä työntekijöiden kesken. Nykyinen palveluntarjoajan VPN-palvelu toimii käyttämällä joko erillistä client-ohjelmaa tai selainta, joihin kumpaankin kirjaudutaan käyttäjien omilla Active Directory tunnuksilla sekä varmentamalla SMS-viestinä kännykkään tulevaa kertakäyttösalasanaa hyödyntäen.

Tätä tutkimusta voidaan hyödyntää tilanteissa, kun pitää etsiä ja ottaa käyttöön palvelimella toimiva VPN-palvelu, mikäli kiinteällä palomuurilla toteutettava etäyhteyspalvelu ei ole mahdollinen tai toivottava ratkaisu. Useat tässä työssä tutkittavat VPN-palvelut ovat suhteellisen uusia ja todennäköisesti ajankohtaisia vielä vuosienkin päästä. Hetken tutkimisen jälkeen huomasin, että palveluista löytyy suhteellisen hyvin dokumentaatiota ja paljon eri ohjeita käyttöönottoon liittyen. Ikävä kyllä suurin osa dokumentaatiosta ei ole kovin syvällistä ja suurim-

maksi osaksi saman asian toistamista. Tämä voi aiheuttaa sen, että vastaan tulee ongelmia, joihin ei löydy suoraan vastausta vaan ratkaisu pitää löytää kokeilemalla ja tutkimalla itse.

Tutkimus toteutetaan vertailemalla VPN-palveluiden vahvuuksia sekä heikkouksia ja valitsemalla tutkituista vaihtoehdoista tilanteeseen parhaiten sopiva palvelu. Koska etäyhteyspalveluiden valmistajien omat sivut ovat huono lähde palvelun toimivuuden vertailuun, suurin osa vertailumateriaalista tulee todennäköisesti löytymään erilaisista blogeista sekä internetkeskusteluista. Alan kirjallisuus soveltuu hyvin varsinkin, kun selitetään erilaisten protokollien ja autentikointimenetelmien toimintaa mutta palveluiden vertailuun ne eivät sovellu läheskään yhtä hyvin.

2 MIKÄ ON VPN?

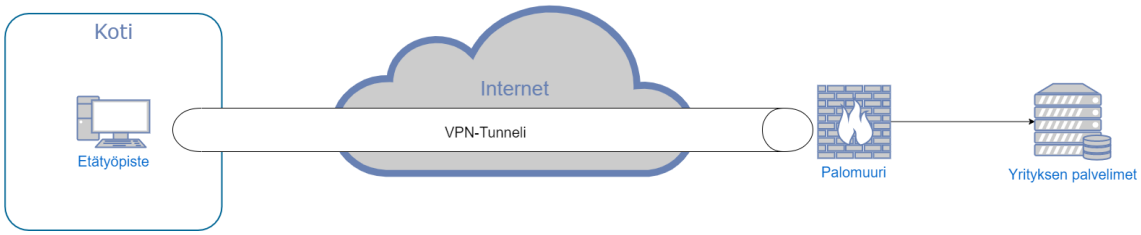
VPN eli Virtual Private Network sai nykyisessä muodossaan alkunsa vuonna 1996, jolloin ensimmäisen oikean VPN-protokollan PPTP:n kehitys alkoi (Vyprvpn 2016). PPTP julkaistiin lopulta vuonna 1999, ja se kehitettiin mahdollistamaan ihmisten töiden tekeminen kotoa käsin. Aluksi vain isot yritykset käyttivät VPN-palveluita korkeiden käyttökustannusten takia. Mahdollisuus ladata ja jakaa tiedostoja turvallisesti etänä oli kuitenkin riittävän hyvä syy jatkaa VPN-palveluiden käyttöä, ja lopulta palvelut laajenivat myös pienemmille yrityksille sekä yksityisten käyttäjien laitteisiin. (Zagradanin 2020.)

Kaikkien VPN yhteyksien tarkoitus on periaatteessa sama; luoda salattu ja turvallinen yhteys kahden laitteen välille. Laitteet voivat olla esimerkiksi kannettavia tietokoneita, palvelimia, palomuureja tai vaikka kännyköitä. Kännyköissä käytettävät VPN-yhteydet ovat kasvattaneet suosiotaan valtavasti viimeisten vuosien aikana lähinnä älypuhelimien suosion kasvun takia. Vaikka pilvipalvelut ovat yleistyneet merkittävästi viime vuosina ne eivät ole korvanneet VPN-yhteyksiä täysin. Osa turvallisen yhteyden luomiseen käytetyistä VPN-protokollista on aikojen saatossa vanhentunut joko epäluotettavuuden tai turvallisuuden vuoksi ja niitä ei enää suositella käytettäväksi. (Vpnoverview 2020.)

Teknisesti katsottuna VPN salaa liikenteen luomalla suojatun tunnelin kahden laitteen välille. Tunnelin suojataan käyttämällä erilaisia yhdistelmiä salausmenetelmiä sekä todennusmenetelmiä. Yleisimmät käytössä olevat salausmenetelmät ovat DES, 3DES, RSA, Blowfish, Twofish sekä AES, ja yleisimpiä todennusmenetelmiä ovat MD5, SHA-1, SHA-256, SHA-384 sekä SHA-512. (Juniper 2019; Stevens 2020.) Joskus SHA-256, 384 sekä 512 todennusmenetelmistä käytetään myös yhteistermiä SHA-2. Näiden ohella löytyy lukuisia enemmän ja vähemmän luotettavia vaihtoehtoja. Yleinen sääntö on, että mitä paremmin liikenne on suojattu, sitä enemmän laskentatehoa laitteistolta vaaditaan.

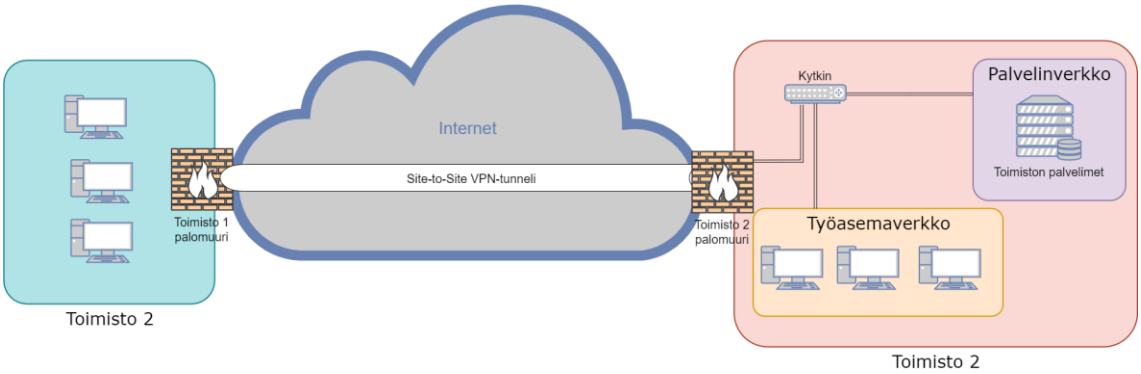
VPN-yhteyksiä voidaan käyttää monella eri tapaa yhteyden suojaamiseksi. Yrityksellä voi olla VPN etänä työskenteleviä työntekijöitä varten, jotka ottavat työpisteeltään suojatun yhteyden yrityksen tiloissa sijaitsevaan julkisesta verkosta tietyille porteille auki olevaan palvelimeen. Tällä tavalla työntekijä voi ottaa

etäyhteyden yrityksen muihin palvelimiin tämän kyseisen suojatun yhteyden kautta käyttämällä kyseisten palvelimien sisäverkon osoitetta (kuva 1). Tällöin vältytään tilanteelta, jossa palvelin pitäisi avata helposti murrettavissa olevalle liikenteelle joko jostain tietystä IP-osoitteesta tai jopa koko ulkoverkosta. On myös hyvin yleistä, että yrityksen käyttämät ulkoiset pilvipalvelut on rajattu vain tietylle julkiselle IP-osoitteelle pilvipalveluiden palveluntarjoajan johdosta, jonka saa vain käyttämällä liikenne ensin palvelinkeskuksessa, jota kautta liikenne lähtee lopullisesti ulkoverkkoon. Näissä tapauksissa liikenne kulkee kyseiseen pilvipalveluun toimiston verkon kautta, jolloin palveluun menevä liikenne saa julkisen IP-osoitteen toimiston verkosta. (VPNmentor 2020.)



KUVA 1 Tyypillinen VPN-yhteys etätyöpisteen sekä yrityksen välillä.

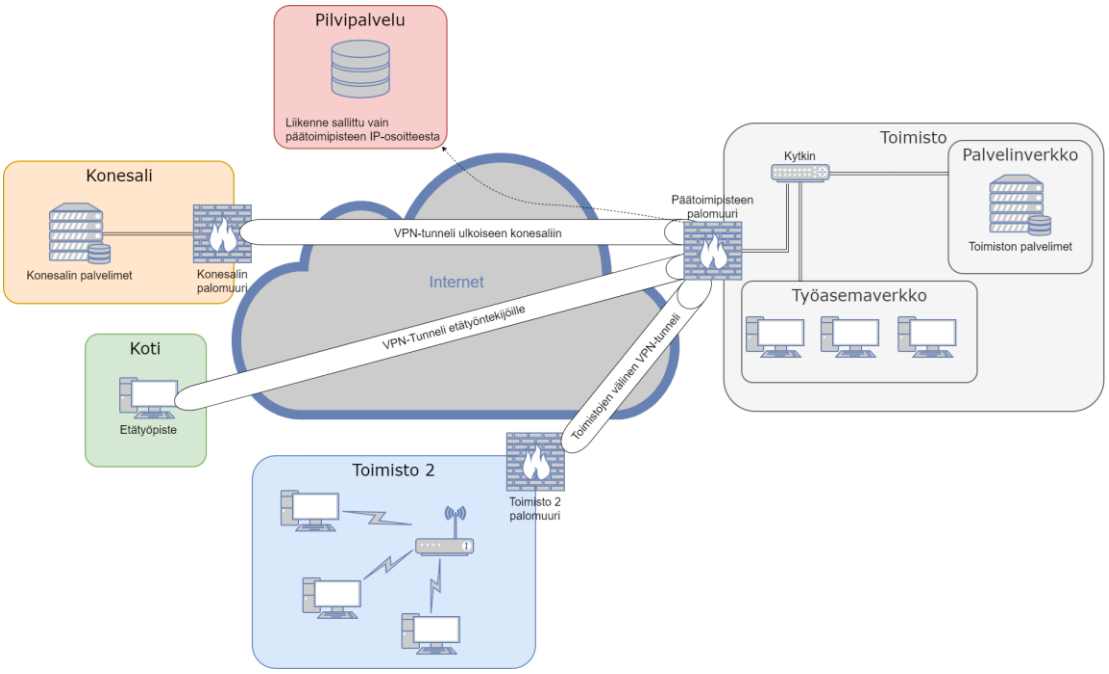
Yrityksillä on myös usein käytössään niin kutsuttuja site-to-site VPN-tunneleita (kuva 2), jossa yhdistetään kaksi eri toimipistettä keskenään. Toimipisteet voivat olla esimerkiksi saman yrityksen toimistoja tai yrityksen oma toimipiste sekä ulkoinen konesali, jossa kaikki tai osa yrityksen palvelimista sijaitsee.



KUVA 2 Tyypillinen site-to-site VPN-tunneli

Tietotekniikan ollessa nykyään yrityksien elinehto on myös erittäin tyypillistä, että yrityksellä on käytössään VPN-tunneleita sekä etätyöntekijöitä, että toimistojen tai ulkoisten palvelimien yhteyksiä varten (kuva 3). On myös yleistä, että muun muassa IT-palveluntarjoajat haluavat VPN-tunnelin omasta toimistostaan

asiakkaan toimistolle helpottaakseen etäyhteyksien ottamista asiakkaan laitteisiin.



KUVA 3 Tyypillinen yritysverkko, jossa hyödynnetään VPN-teknologiaa

2.1. VPN-protokollat

Teknologioiden edistyessä uusia VPN-protokollia on luotu helpottamaan käyttöä ja parantamaan verkon turvallisuutta tehden suojatusta liikenteestä vaikeampaa murtaa. Erilaiset suojaukset ovat koko ajan testauksen ja seurannan alla niin hyvää kuin pahaa tahtovien tahojen toimesta. Tällä hetkellä turvalliseksi koettu protokolla ei välttämättä ole turvallinen enää viiden vuoden päästä, mikä tarkoittaa, että mikäli järjestelmä halutaan pitää suojattuna, yrityksen tietoturvasta vastaavan tahon tulee seurata alan uusimpia muutoksia tarkasti ja rakentaa uutta tai päivittää aiempia järjestelmiä tietoturvariskin löytyessä. VPN-protokollat on myös luotu jokin tietty asia mielessä, esimerkiksi jotkut ovat nopeampia mutta turvattomampia tai päinvastoin turvallisempia ja hitaampia käytössä. (Phillips 2017.) Seuraavissa kappaleissa käsitellään muutamia yleisimpiä VPN-protokollia sekä niiden vahvuuksia että heikkouksia.

2.1.1 OpenVPN

OpenVPN on avoimen lähdekoodin VPN-protokolla, joka julkaistiin alun perin vuonna 2001. Se on nykyisin yksi yleisimmin käytetyistä VPN-protokollista, ja on vanhaan ikäänsä nähden hyvin turvallinen. OpenVPN:ää saa tarkastella ja parantaa kuka tahansa haluamallaan tavalla, mikä osallaan selittää sen pitkäikäisyyden. (Mocan 2019c.) Salatakseen datan OpenVPN käyttää OpenSSL-salauskirjastoa ja lisätäkseen turvallisuutta on mahdollista käyttää mm. AES, 3DES tai Camellia-salauksia näiden lisäksi. Tällä hetkellä OpenVPN on kokonaisuudessaan yksi turvallisimmista sekä parhaiten tuetuista VPN-protokollista. Tuki OpenVPN varten löytyy useista eri alustoista, kuten Windows, Mac OS, Linux, Android, iOs, Solaris, FreeBSD sekä QNX. (Temblay.)

Nopeuden osalta OpenVPN ei ole kärkikastia johtuen suurimmaksi osaksi paljon tehoa vievän salauksen takia. OpenVPN on kuitenkin suurimpaan osaan käyttötarkoituksista riittävän nopea. Yksi keino saada OpenVPN liikenteestä nopeampaa on hyödyntää UDP-liikennettä tunnelin luomiseen koska UDP-liikenteessä ei ole TCP:n tapaan rajoitettu lähtevien pakettien kokoa. (Lowendtalk 2015.)

2.1.2 IKEv2/IPsec

IKEv2 tulee sanoista Internet Key Exchange version 2, ja yhdessä IPsecin kanssa ne luovat VPN-protokollan. Ciscon ja Microsoftin yhteistyönä kehittämä VPN-protokolla on kasvattanut viime vuosina paljon suosiotaan sen turvallisuuden ja nopeuden takia. IKEv2 kykenee myös nostamaan automaattisesti katkenneen yhteyden laitteiden välillä. (Mocan 2019d.) IKE-protokolla käyttää IPsec-tunnelin luomiseen laitteiden välille UDP porttia 500, jonka jälkeen IPsec-datapaketit lähetetään ESP:n avulla. Mikäli yhteyden aloittajan ja vastaanottajan välillä havaitaan NAT, liikennöinti vaihtuu UDP portille 4500. (Pauly, Touati & Mantha.)

IKEv2 tukee 256-bittistä suojausta, ja pystyy käyttämään AES, 3DES, Camelia sekä ChaCha20 -salausmenetelmiä. Lisäksi IKEv2/IPsec tukee Perfect Forward

Secrecyä, joka tarkoittaa, että salausavaimen murtaminen ei johda aiemmin salattujen viestien aukeamiseen. Tämä perustuu istuntokohtaisiin avaimiin, jotka luodaan salausavaimen perusteella. IKEv2/IPsec käyttää myös MOBIKE:a, joka mahdollistaa verkon tai rajapinnan vaihdon yhteyden aikana ilman katkosta tehden yhteydestä luotettavamman liikkuessa tai yhteyden katketessa hetkellisesti. Turvallisuuden kannalta IKEv2 on hyvä, mutta ei täysin ongelmaton. 2018 tuli julki kummankin IKEv1 sekä IKEv2 osalta ongelma, jossa lyhyt salasana aiheuttaa suoran tietoturvariskin. Tämä on kuitenkin helppo kiertää käyttämällä vahvaa salasanaa. (Matthews 2018.)

2.1.3 L2TP/IPsec

L2TP/IPsec toimii luomalla ensiksi tunnelin kahden laitteen välille hyödyntäen IPseciä, jonka jälkeen tätä kanavaa käytetään L2TP tunnelin luomiseen. Tämän jälkeen IPseciä käytetään myös siirtämään L2TP -enkapsuloitua käyttäjän dataa. Verrattuna pelkän IPsecin toimintaan L2TP/IPsec on jonkin verran vaativampi prosessorille (varsinkin mikäli käytetään ESPtä). Hyötynä L2TP/IPsec kykenee kuljettamaan myös UDP -paketteja tunnelin yli. L2TP/IPsec hyödyntää UDP portteja 500, 1701 sekä 4500 tunnelin luomiseen. (Townsley & Valencia 1999.)

L2TP tulee sanoista Layer 2 Tunneling Protocol, eikä se itsessään suojaa liikennettä vaan luo yhteyden kahden laitteen välille. Tämän takia L2TP:tä käytetään usein jonkun toisen protokollan kanssa salaa datan. Nopeuden osalta L2TP/IPsec ei ole yhtä nopea kuin OpenVPN ja törmää joskus ongelmiin sen käyttämien porttien takia. (ExpressVPN.)

2.1.4 PPTP

Ensimmäinen VPN-protokolla PPTP eli Point-to-Point Tunneling Protocol julkistettiin vuonna 1999 kolmen vuoden kehityksen tuloksena. Se toimi alun perin vain Windows-käyttöjärjestelmillä mutta levisi nopeasti muillekin alustoille. (Mocan 2019a.) PPTP-tunneli luodaan kahden laitteen välille käyttäen GRE-enkapsulointia ja TCP-porttia 1723. Nopeuden suhteen PPTP on hyvä valinta. Pienet

laitteistovaatimukset tarkoittavat, että suojattu tunneli voidaan luoda laitteeseen, vaikka kyseinen laite olisikin vanhentunut ja sen laskentateho alhainen.

Kuitenkin turvallisuuden osalta PPTP on riittämätön nykypäivän vaatimuksiin nähden. Sen käyttämät todennusmenetelmät MS-CHAP-v1 sekä MS-CHAP-v2 on kumpikin kyetty murtamaan, ja Yhdysvaltain tiedusteluvirasto NSA on todistetusti murtanut muun muassa Afganistanin hallituksen salattua liikennettä, joka on ollut suojattu PPTP:llä. (Durret 2015.)

2.1.5 SSTP

SSTP eli Secure Socket Tunneling Protocol julkaistiin Windows Vistan julkaisun yhteydessä, ja on käytössä myös Windows 7, Windows 8 sekä Windows 10 käyttöjärjestelmissä (Mocan 2019b). SSTP on täysin Microsoftin omistama, eikä sen lähdekoodia ole koskaan julkaistu. Tunnelin luomiseen SSTP käyttää TCP porttia 443, joka on käytössä myös HTTPS-liikenteelle. SSTP on helppo käyttöönotettava ja nopea valinta mikäli netin nopeus ei ole liian hidas. (Mocan 2019c.)

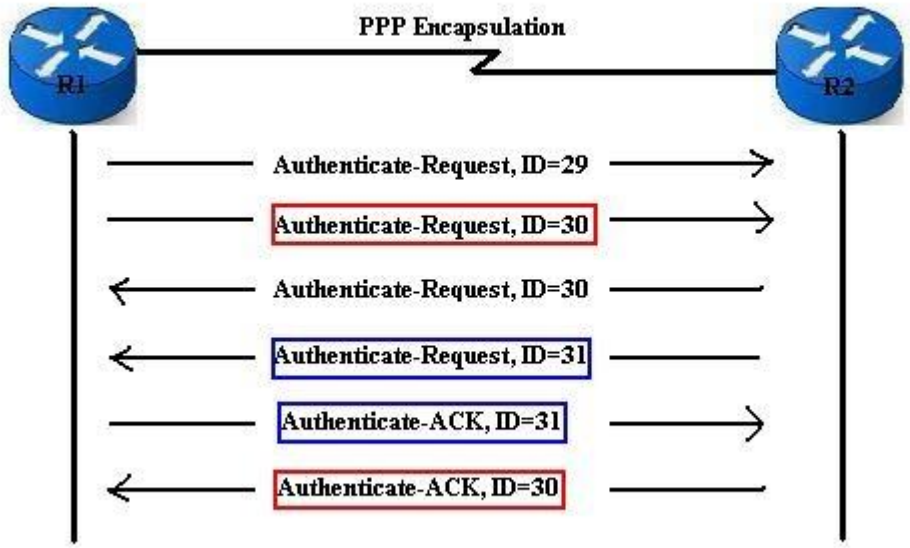
Turvallisuuden kannalta SSTP:tä pidetään kyseenalaisena. Microsoft on todistetusti työskennellyt NSA:n kanssa, joten on hyvin todennäköistä, että tarpeen vaatiessa ulkopuoliset ovat kykeneväisiä seuraamaan SSTP:llä suojattua liikennettä. (Griggs 2013.) SSTP:n turvallisuus riippuukin lähinnä siitä, kuinka paljon käyttäjä luottaa Microsoftiin. Yksi suuri hyöty SSTP protokollassa on sen käyttämä portti 443. Koska HTTPS-liikenne käyttää samaa porttia, on hyvin epätodennäköistä, että operaattori tai palomuuri tarkoituksella estäisi VPN-yhteyden luomista. Muun muassa Kiinan valtio pyrkii hallinnoimaan VPN-tunnelien luomista omalla maaperällään, joten portin 443 käyttö lisää yhteyden luotettavuutta. (VPNdada.)

2.2. Autentikointiprotokollat

Sen lisäksi että kahden laitteen välillä kulkeva liikenne suojataan, on myös tärkeää, että kirjautuminen on suojattu. Mikäli ulkopuoliset pääsevät kirjautumaan ja luomaan suojatun yhteyden oman laitteen ja kohdepalvelimen tai kohdeverkon välille niin suojatun yhteyden merkitys katoaa täysin. Seuraavissa kappaleissa käsitellään yleisimpiä käytössä olevia selvennys eli autentikointiprotokollia. (Griffin.)

2.2.1 PAP – Password Authentication Protocol

PAP eli Password Authentication Protocol on todentamismenetelmä, jossa salasana sekä käyttäjänimi lähetetään verkon yli laitteeseen, jossa sitä verrataan nimi-salasana pareihin, jotka on usein salattu. PAP lähettää salasanan sekä käyttäjänimen selkokielisenä verkon yli, joka tekee siitä vaarallisen käyttää (kuva 4). (Webopedia) Tästä syystä PAP:ia pidetään yleisesti vanhentuneena teknologiana, jota tulee käyttää ainoastaan, mikäli vaihtoehtoja ei ole. (Loyd & Simpson 1992.)



KUVA 4 PAP selvennys

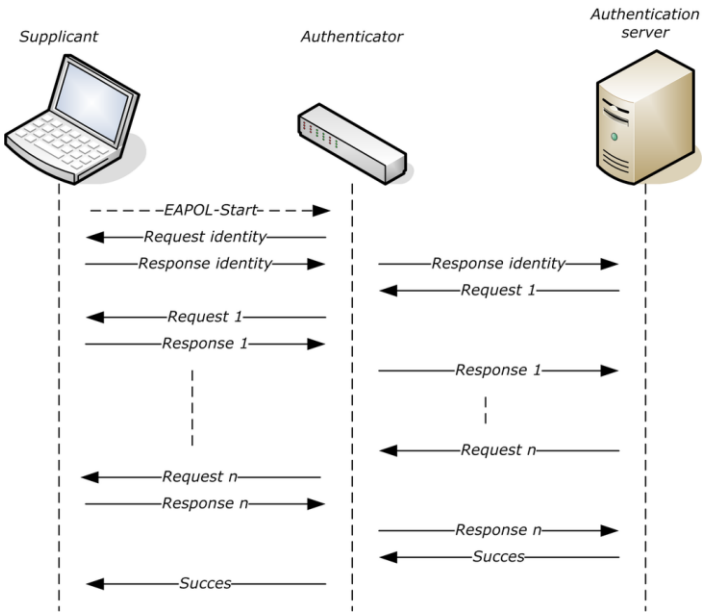
2.2.2 CHAP – Challenge-handshake authentication protocol

Huomattavasti turvallisempi PAP:iin verrattuna, CHAP eli Challenge Handshake Authentication Protocol on todentamismenetelmä, jossa todentamisagentti lähettää clientille sattumanvaraisen numerosarjan sekä ID-arvon. Sekä palvelimella että clientillä on myös ennalta sovittu salasana. Client ketjuttaa sattumanvaraisen numeron, ID:n sekä ennalta sovitun salasanan yhdeksi viestiksi ja laskee yhdensuuntaisen tarkisteen hyödyntäen MD5-salausta. Tämä arvo lähetetään selventämispalvelimelle, jossa kyseinen arvo puretaan ja verrataan clientin arvoon. Client pääsee kirjautumaan, mikäli arvot ovat samat. (Simpson 1996.)

Microsoftin oma versio CHAP-selvennyksestä on nimeltään MS-CHAP ja siitä löytyy kaksi versiota, MS-CHAPv1 sekä MS-CHAP-v2, jotka eivät ole keskenään yhteensopivia. Kumpaakin selventämismenetelmää pidetään vanhentuneena, vaikka MS-CHAPv2 on yhä yleisesti käytössä varsinkin PEAP/MSCHAPv2 muodossa langattomaan verkkoon autentikoinnissa. Tämäkin on kyetty murtamaan tekemällä oikeaa langatonta verkkoa imitoiva verkko, jolloin yhdistävä kone yrittää yhdistää automaattisesti tähän väärään imitaatioverkkoon. (Securew2.) Always On VPN käyttötarkoitukseen tämä ongelma ei kuitenkaan vaikuta koska kyseistä selvennysmenetelmää ei käytetä langattomaan verkkoon kirjautuessa.

2.2.3 EAP

EAP eli Extensible Authentication Protocol on käyttäjien tunnistusprotokolla, joka toimii käyttäen kolmea eri tekijää, joilla kullakin on oma roolinsa. Vastaanottajana toimii mikä tahansa laite, joka koittaa todentaa itsensä ja saada valtuudet liittyä verkkoon. Autentikaattorina toimiva laite keskustelee palvelimen sekä vastaanottajan välissä. Palvelin toimii EAP:ssa käyttäjän tai laitteen selventäjänä (kuva 5). EAP voi käyttää monia eri keinoja käyttäjän todentamiseen kuten EAP-MD5 jossa viesti salataan MD5:lla tai EAP-IKEv2 jossa salaus tapahtuu IKEv2 avulla. (StrongSwan 2018b.)



KUVA 5 EAP toiminta MD5:lla

2.3. Palvelimelle asennettava VPN-palvelu

Palvelimelle asennettavia VPN-palveluita on kehitetty monia erilaisia. Kaikki pyrkivät lähtökohtaisesti antamaan mahdollisimman hyvän käyttökokemuksen niin käyttöönoton kuin käytön osalta. Kaikki tässä opinnäytetyössä läpi käytävät VPN-palvelut ovat kirjoitushetkellä ajankohtaisia niin nopeuden, luotettavuuden sekä turvallisuuden osalta niiden käyttämien ajankohtaisten protokollien vuoksi. Erilaisia palvelimelle asennettavia VPN-palveluja ei ollut hirveän vaikea löytää, ja tässä työssä tutkin muutamaa yleisesti käytössä olevaa palvelua (Bischoff 2018). Seuraavaksi käsitellään läpi eri vaihtoehtoja palvelimelle asennettavista VPN-palveluista.

Käytännössä VPN-palvelun asentaminen ympäristöön vaatii muutaman asian. Ympäristössä pitää olla oma palvelunsa, joka hoitaa yhteyden palvelimen sekä clientin välillä kuten RRAS tai SoftEther. Ympäristössä pitää olla myös palvelin, josta VPN-palvelu pääsee tarkistamaan, että yhteyden avaamista pyrkivä laite tai käyttäjä saa sen avata. Tätä roolia hoitaa muun muassa Windows-ympäristössä NPS ja Linux-ympäristöissä esimerkiksi OpenLDAP. On myös tärkeää, että palvelimella, jossa VPN-palvelu on, löytyy joko kiinteä IP-osoite ulkoverkosta tai mahdollisuus ohjata liikenne kyseiselle palvelimelle NAT:in avulla.

2.3.1 Always On VPN

Always On VPN on Microsoftin oma etäyhteyspalvelu, jonka pohjana toimii Windows-palvelimella pyörivä RRAS -palvelu. Always On VPN luotiin korvaamaan monien mielestä vaikeasti käyttöönotettava Direct Access. (Tulloch 2020.) Toisin kuin Direct Accessissa, Always On VPN sallii yhteydet muistakin kuin domainiin liitetyistä koneista sallien yhteydet myös Azure Active Directoryyn liitetyistä laitteista sekä esimerkiksi koneelta, joka ei ole lainkaan domainissa. Suurimmat erot Always On VPN:n ja Direct Accessin välillä ovat, että Direct Access käyttää IPsec-protokollaa IPv6:n yli, kun taas Always On VPN käyttää eri protokollia IPv4 yli. Tästä syystä Always On VPN on huomattavasti luotettavampi tilanteissa, jossa internet-yhteys ei ole hyvin toimiva, mikä on yleistä työskennellessä kotoa käsin tai 4g-yhteyden perässä. (Hicks 2018.) Always On VPN on Microsoftin kehittämä ja toimii Windows -palvelimella, ja se voi hyödyntää IKEv2, SSTP, L2TP/IPsec sekä PPTP -protokollia.

Käyttöönoton osalta Always On VPN vaikuttaisi Windowsiin tottuneelle erittäin helpolta. Asentaminen vaatii muutamien yleisessä käytössä olevien palveluiden kuten NPS, AD sekä PKI käyttämistä sekä jotain osaamista verkkolaitteista. Dokumentaatio on todella laajaa sekä netistä löytyy useita eri sivustoja, jotka käsittelevät Always On VPN käyttöönottoa eri mahdollisuuksilla. Vaikka käyttöönotto vaikuttaa hieman SoftEtheriä monimutkaisemmalta se on silti helposti käyttöönotettavan rajoissa. Myös virallinen tuki Microsoftilta tekee Always On VPN:stä haluttavan palvelun käyttöönottaa. Turvallisuus Always On VPN:ssä riippuu hyvin pitkälti siitä mitä protokollia käytetään tunnelin luomiseen ja käyttäjien selventämiseen.

2.3.2 StrongSwan

StrongSwan on avoimeen lähdekoodiin perustuva VPN-taustaprosessi, joka luo suojatun yhteyden kahden laitteen välille. StrongSwan on jatkoa aikaisemmalle FreeS/WAN projektille. Alun perin StrongSwan kehitettiin Linux-käyttöjärjestelmälle ja sitä on jatkettu tekemällä versiot Andoidille, FreeBSD:lle, Mac OS X:lle, Windowsille sekä muille vähemmän tunnetuille alustoille. Palvelimen osalta StrongSwanin pystyy asentamaa Linux pohjaisille alustoille sekä Windows 2008

R2 tai uudemmille palvelimille (StrongSwan 2018b). Selvennys onnistuu Windows palvelimelta hyödyntäen muun muassa Radiusta tai LDAP:ia.

StrongSwan -projekti keskittyy konfiguraation yksinkertaisuuteen, vahvoihin salausprotokolliin sekä modulaariseen suunnitteluun hyvillä laajennusmahdollisuuksilla. (StrongSwan 2018a.) Tämä vaikuttaisi pitävänsä jollain tasolla paikkaansa netistä löytyvien ohjeiden perusteella. Turvallisuuden osalta StrongSwan käyttää pääasiallisesti IKEv2 -protokollaa mutta tuki IKEv1 löytyy myös käyttäjien toiveiden mukaan. Tästä syystä StrongSwania voidaan pitää hyvin turvallisena ja tähän käyttötarkoitukseen riitävänä.

2.3.3 SoftEther

SoftEther tulee valmistajansa mukaan sanoista Software Ethernet. Valmistaja ilmoittaa SoftEtherin olevan helposti käyttöönotettava VPN-palvelu, joka käyttää hyväkseen TCP-liikennettä luoden kahden pisteen välille tunnelin joko L2TP tai L2TP/IPsec käyttäen. SoftEther clientin voi asentaa Windowsille, Linuxille, FreeBSDlle, Solarikselle tai Mac OS X:lle ja palvelimen voi asentaa Windows-alustalle.

Kokonaisuutena SoftEther vaikuttaa erittäin varteenotettavalta vaihtoehdolta VPN-palveluksi. Käyttöönotossa on käytettävänä helppokäyttöisen oloinen graafinen käyttöliittymä. Käyttöönotossa luodaan sertifikaatti, joka asennetaan ensimmäisellä kerralla yhteyttä otettaessa client-koneella. Käyttäjiä voidaan hallita niin palvelimelta itseltään kuin myös Active Directoryä hyödyntäen. (SoftEther 2019.)

2.3.4 WireGuard

Alun perin WireGuard kehitettiin Linux-käyttöjärjestelmälle, mutta on sittemmin levinnyt myös Windowsiin, Mac OS X:n, BSD:hen, iOS:n ja Androidiin. WireGuard on myös mahdollista asentaa Windows palvelimelle, vaikka se ei olekaan virallisesti tuettu ominaisuus. (Chang 2020.) WireGuard on ollut mukana Linux kernelissä versiosta 5.6 lähtien, ja sen tarkoitus on korvata jo hyvään ikään päässyt OpenVPN (Prakash 2020).

WireGuard on valmistajansa mukaan yksinkertainen käyttöönotettava, luotettava ja helppokäyttöinen. Tämä vaikuttaisi ohjeiden perusteella pitävänsä paikkaansa. Vaikka käyttöönotto vaatii Linux-tyyppisesti komentorivin käyttöä eikä graafista käyttöliittymää löydy niin täytettävien rivien määrä vaikuttaisi hyvin pieneltä. WireGuardin saa käyttämään korkeita UDP-portteja, normaalisti porttia 51820. (Donenfeld 2016.)

3 YMPÄRISTÖ

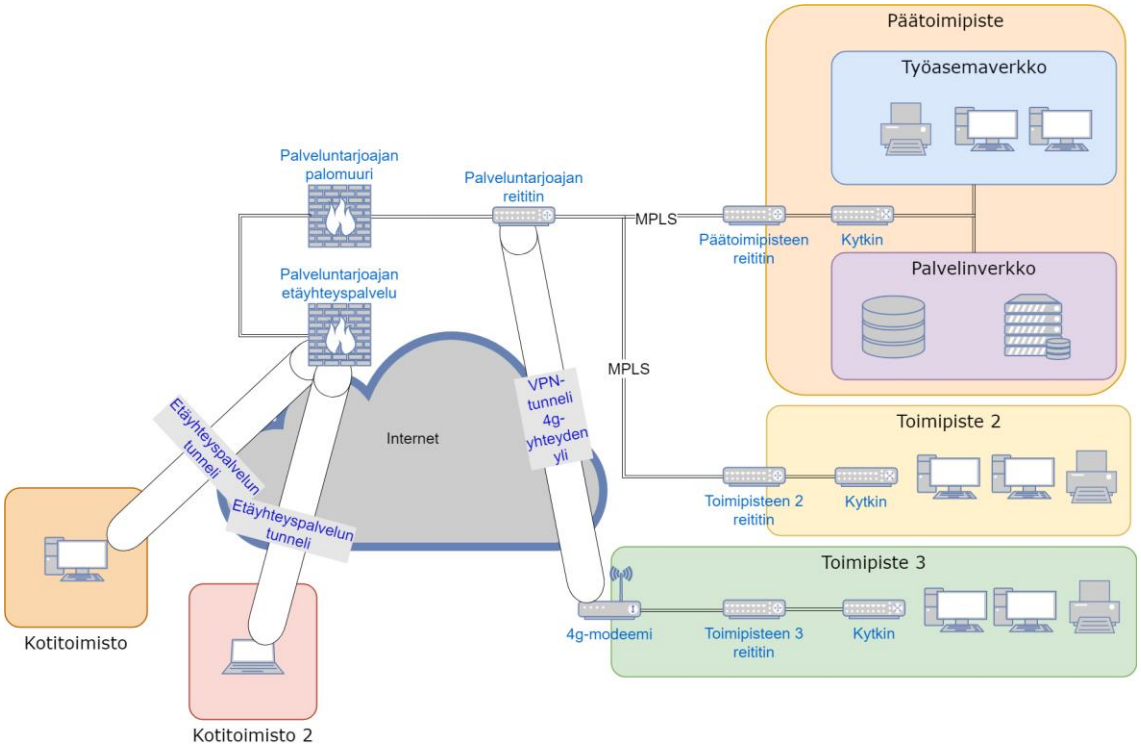
VPN-palvelun voi ottaa käyttöön monella eri tapaa, mutta alusta asti oli selvää, että palvelimelle asennettava palvelu on tähän käyttötarkoitukseen oikea vaihtoehto. Kiinteän palomuurin käyttöönotto olisi ollut mahdollinen vaihtoehto käytännössä ainoastaan siinä tapauksessa, mikäli se olisi asennettu palveluntarjoajan konesaliin, jonne kaikki MPLS-yhteydet päättyvät. Loppujen lopuksi se olisi vaatinut huomattavasti enemmän työtä sekä rahaa verrattuna palvelimelle asennettavaan palveluun.

Toivottavia ominaisuuksia tässä selvityksessä VPN-palvelulle on muutama. Koska asiakasyrityksen ympäristö on toteutettu täysin Windows-pohjalla ja asiakkaan oma IT-puoli on työskennellyt huomattavasti enemmän Windows-puolella muihin alustoihin verrattuna, olisi toivottavaa, että palvelun voi asentaa Windows palvelimelle. Olisi myös hyvä, että olisi mahdollista hyödyntää nykyistä ympäristöä muun muassa kirjautumisen yhteydessä, ettei tunnuksia tarvitse tehdä useaan eri paikkaan. Palvelun tulisi olla loppukäyttäjälle helppokäyttöinen ja riittävän nopea ohjelmien ajamiseen palvelimelta sekä tiedostojen siirtämiseen VPN yli.

Asiakkaalla on käytössään oma palvelinalusta päätoimipisteellään, jossa pyörii domain controller, tiedostopalvelin, database, tulostuspalvelin sekä etätyöpöydät virtuaalisina palvelimina. Alusta on VMWare-pohjainen ja sen versio on 6.7. Kaikki alustalla pyörivät palvelimet ovat uudehkoja Windows-pohjaisia palvelimia, joita päivitetään aktiivisesti.

3.1. Verkko

Asiakasyrityksen palvelimet pyörivät yrityksen omassa palvelinalustassa, josta on yhteys kaikkiin toimipisteisiin joko MPLS:n avulla tai VPN-tunneloidulla 4g-liittymällä. Joistakin toimipisteistä löytyy kumpikin MPLS- sekä 4g-liittymä. Jokaisella toimipisteellä on vähintään yksi oma verkkonsa 24-maskilla. Liikenne ulkoverkkoon toimii palveluntarjoajan palomuurin kautta joka toimipisteestä (kuva 6). Palvelinsalissa on palvelinalustan sekä reitittimen välissä yksi Aruba-merkkinen kytkin.



KUVA 6 Havainnekuva asiakasyrityksen verkkokokonaisuudesta

3.2. Palvelimet

Asiakkaan palvelimet sijaitsevat verkossa 192.168.0.0/24. Always On VPN palvelun käyttöönotossa tarvittavat palvelimet ovat Active Directory, Certificate Authority, Network Policy Server sekä Routing and Remote Access Service. Active Directory sekä NPS löytyvät kumpikin palvelimelta DC01, jonka osoite on 192.168.0.51, Certificate Authority löytyy palvelimelta DB02 osoitteella 192.168.0.53 ja RRAS palvelu tulee löytymään samasta verkosta osoitteella 192.168.0.61. Kaikkien palvelimien käyttöjärjestelmänä toimii Windows Server 2012 R2. Palvelimilla sekä työasemilla toimi F-Securen palomuuri, jonka hallinnasta vastaa palveluntarjoaja.

4 KÄYTTÖÖNOTTO

Vertailtuani eri vaihtoehtoja tulin siihen lopputulokseen, että paras vaihtoehto on ottaa käyttöön Always On VPN -palvelu, joka on kaikilla asiakkaan työasemilla tuettu sekä pyörii Windows -ympäristössä mikä helpottaa palvelun perustamista, vian etsimistä sekä korjausta. Käyttäjien selvennys tapahtuu koneille asennettavaa sertifikaattia hyödyntäen, jonka jälkeen VPN-yhteys luodaan automaattisesti käyttäjän ollessa toimistoverkon ulkopuolella. Tämän lisäksi Microsoftin tuki palvelulle, asiakkaan aiempi kokemus Microsoftin kanssa sekä Always On VPN yleisyys tekivät päätöksestä loppujen lopuksi helpon. Vaikka jotkin muut vaihtoehdot olivat erittäin varteenotettavia ja todennäköisesti olisivat olleet käytännössä yhtä hyviä ratkaisuita, tähän tapaukseen Always On VPN vaikutti oikealta vaihtoehdolta.

Always On VPN:llä on joitakin minimivaatimuksia toimiakseen. Ympäristössä pitää olla käytössä ainakin yksi DNS -palvelin, jossa on sisäinen sekä ulkoinen DNS -alue. Tässä tapauksessa ulkoisesta DNS:stä vastaa palveluntarjoajan oma DNS-palvelin ja sisäverkossa toimina DNS-palvelin on DC01 -palvelimella. Active Directory -pohjainen PKI sekä Active Directory Certificate Services on myös pakollisia. Palvelimen osalta Microsoft vaatii Windows 2012 r2 palvelimille vähintään 1.4GHz prosessorin, 512MB RAM-muistia, 32GB tallennustilaa sekä vähintään yhden gigabit ethernet adapterin. Suositeltavaa olisi, että resursseja palvelimelle olisi varattu enemmän. (Microsoft.)

Palvelin vaatii pyöriäkseen joko virtuaalisen tai fyysisen palvelimen, jolle saa asennettua tai on asennettuna jo NPS -palvelu. Mikäli verkossa on jo NPS -palvelu jollain palvelimella asennettuna, sitä voi muokata uuden palvelimen asentamisen sijaan. Myös RRAS -palvelu piti asentaa verkon yhdyskäytäväksi. Always On VPN -palvelun käyttöönotto vaati toimia sekä osaamista riippuen siitä, kuinka sen toteuttaa Active Directorystä, sertifikaateista, palomuureista, verkoista sekä DNS-ohjauksista. Seuraavaksi käydään läpi yksi mahdollinen keino ottaa Always On VPN -palvelu käyttöön ja sen toimivaksi saamiseen vaaditut toimet.

4.1. Verkon muutokset

Koska tätä käyttötarkoitusta varten päätin luoda oman verkkon palvelinta sekä käyttäjiä varten, piti asiakkaan reitittimellä sekä kytkimillä tehdä toimenpiteitä että oikea verkko saadaan palvelimille asti ja toimimaan oikealla tavalla. Reitittimenä asiakkaalla on toimitiloissaan Mikrotik-merkkinen reititin, jonka käyttöjärjestelmä RouterOS pohjautuu Linuxiin. Kytkimet ovat kaikki HP:n tai Aruban valmistamia ja suhteellisen uusia. Asiakkaan päätoimipisteen verkko on rakennettu VLAN:eja hyödyntäen, jolloin VPN-verkkoa varten pitää luoda oma VLAN sekä yhdyskäytävä. Reitittimelle pääsee kirjautumaan joko valmistajan omaa graafista Winbox-ohjelmistoa käyttäen tai SSH:lla, jota käytetään myös kytkimille kirjautumiseen. Käytin SSH-yhteyttä kummankin reitittimen sekä kytkimien asetuksien lisäämiseen.

VLAN:in sain lisättyä reitittimelle menemällä ensin oikean interfacen alle, johon lisätään VLAN, tässä tapauksessa 250. VLAN nimetään VLAN ID:n ja käyttötarkoituksen mukaan. VLAN ID tuli verkon osoitteesta 192.168.250.0/24 ja ether2 on portti mistä asiakkaan verkot lähtevät kytkimille ja lopuksi palvelinalustalle (taulukko 1).

TAULUKKO 1 VLAN:in lisääminen reitittimelle

```
interface vlan
add name=vlan250-vpn vlan-id=250 interface=ether2
```

Koska reititin toimii yhdyskäytävänä, sille tulee antaa osoite 192.168.250.1/24 -verkosta. On tyypillistä käyttää yhdyskäytävän osoitteena joko ensimmäistä tai viimeistä vapaata osoitetta verkossa, joten annoin reitittimelle osoitteen 192.168.250.1/24 jossa aliverkon peitteenä on 255.255.255.0 (taulukko 2).

TAULUKKO 2 IP-osoitteen lisääminen reitittimelle

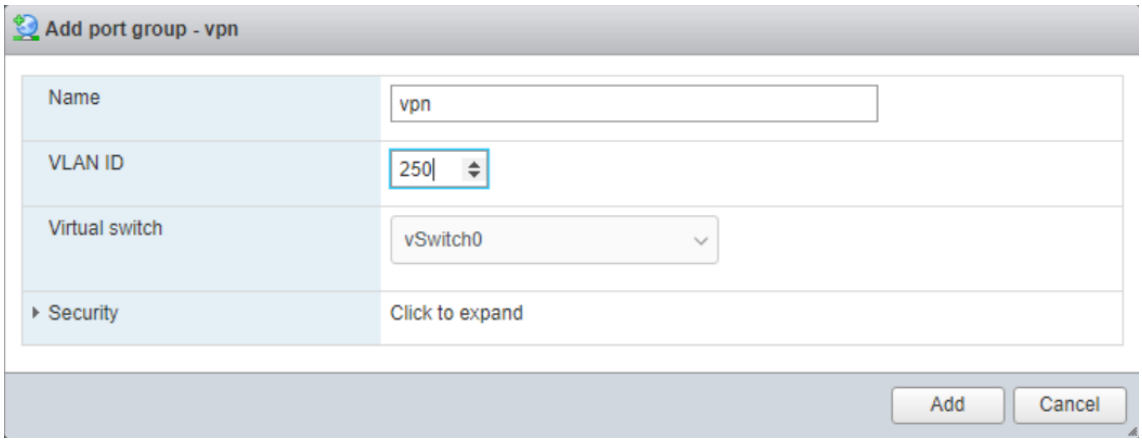
```
ip address
add address=192.168.250.1/24 interface=vlan250-vpn
```

Sain asetukset kytkimille kirjautumalla niihin sisälle ja lisäämällä VLAN 250 reitittimeltä tulevaan porttiin 48 sekä palvelimelle menevään porttiin 47. Tässä tapauksessa VLAN lisätään tagged-tilaan koska käytössä on muitakin verkkoja. Verkoille kannattaa antaa nimi myös kytkimillä, mikä voi helpottaa vian etsintää tulevaisuudessa (taulukko 3).

TAULUKKO 3 VLAN:in tekeminen tagged tilaan tiettyihin portteihin

```
configure terminal
vlan 250 name vpn tagged 47,48
```

Näiden toimenpiteiden jälkeen VLAN 250 menee palvelinalustalle asti, jonka jälkeen lisäsin sen myös palvelinalustalle. Palvelinalustana asiakkaalla toimii VMWare johon saa yhteyden asiakkaan omasta verkosta selaimella tai omalla vSphere clientilla. Kirjautumisen jälkeen avasin vasemmalta palkilta Networkin, josta valitsin Add Port Group. Tämän jälkeen annoin Port Groupille nimen vpn ja VLAN ID kohtaan laitoin 250. Virtual switch kohtaan vSwitch0 on tässä tapauksessa ainoa vaihtoehto ja Security kohtaan riitti valmiit asetukset, jolloin ne periytyivät suoraan vSwitch0:lta (kuva 7).



KUVA 7 VPN-verkon lisääminen alustalle

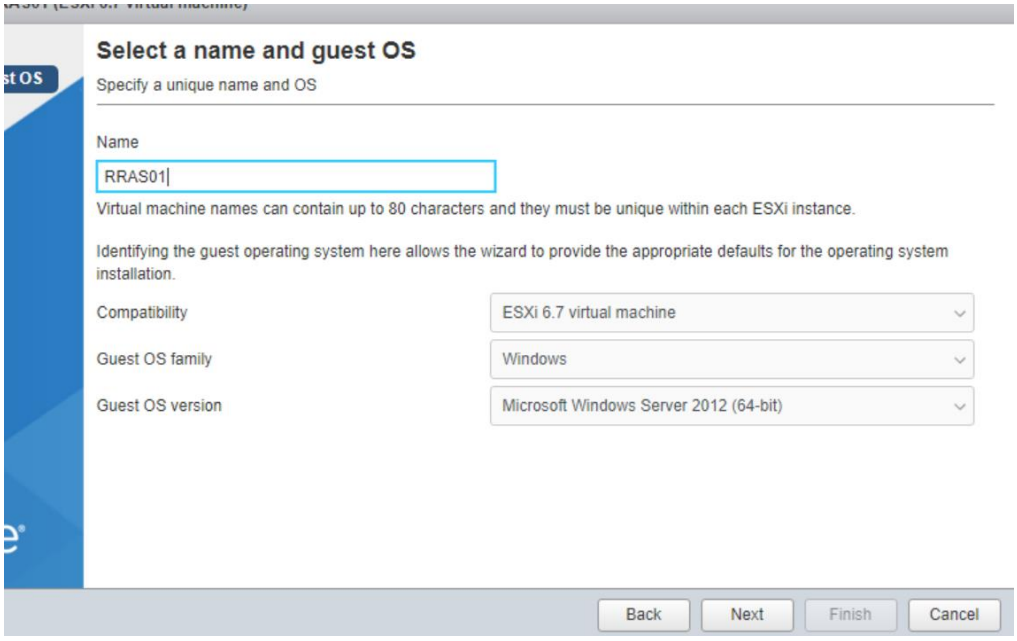
Koska asiakkaan palomuuri sijaitsee palveluntarjoajan konesalissa, pitää palveluntarjoajan reitittimelle kertoa, että verkko 192.168.250.0/24 löytyy asiakkaan reitittimen takaa. Asiakkaan reitittimen linkkiverkon osoitteena toimii 10.100.250.201/30 (taulukko 4).

TAULUKKO 4 Reitin lisääminen palveluntarjoajan reitittimelle

```
ip route add dst-address=192.168.250.0/24 gate-
way=10.100.250.201/30
```

4.2. Palvelin

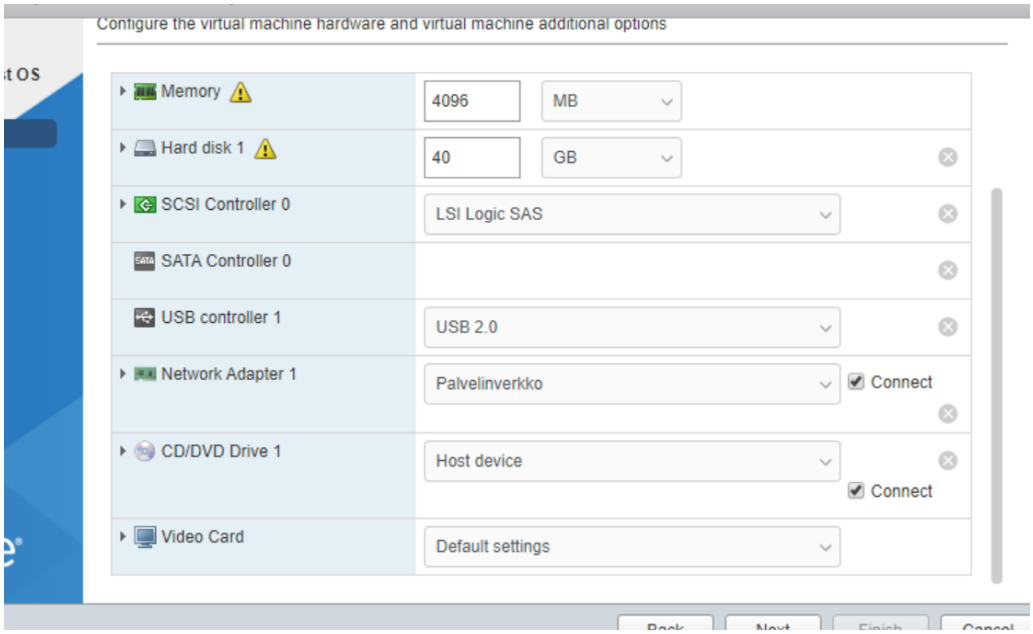
Etäyhteyksiä varten piti tehdä pelkästään etäyhteyksiä varten tarkoitettu oma palvelimensa, jolla pyörii tarvittava RRAS-palvelu. Muut tarvittavat palvelut löytyivät verkosta ennestään mikä helpotti projektin toteutusta. Asiakkaan alustana toimii VMWare ESXi versio 6.7.0. Palvelimen lisäämiseksi valitsin Virtual Machines oikealla hiiren näppäimellä, josta painoin Create/Register VM. Eteen aukeaa ikkuna, joka pyytää täyttämään palvelimen pystyttämiseen vaadittavat tiedot. Valitsin ensimmäisestä ikkunasta Create a New Virtual Machine ja Next, toisessa ikkunassa annamme palvelimelle nimen RRAS01 (kuva 8). Compatibility kohtaan valitsin ESXi:n version ESXi 6.7 virtual machine, Guest OS Family kohtaan Windows ja version kohtaan palvelimelle tulevan käyttöjärjestelmän Windows Server 2012 (64bit).



KUVA 8 Virtuaalikoneen luominen

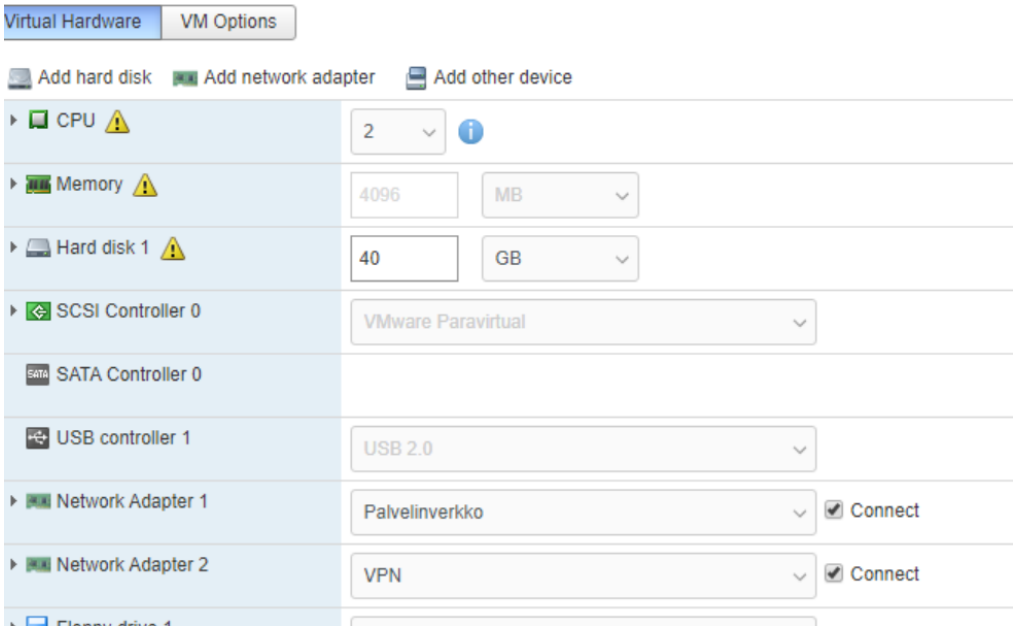
Seuraavassa ikkunassa valitsin kohteen johon virtuaalikone sekä sen virtuaaliset asemat asennetaan. Asiakkaalta löytyi tähän sopiva SSDRAID01 -asema.

Seuraavassa ikkunassa valitsin palvelimelle sopivat asetukset, että se toimii kunnolla. Prosessoriytimiä annoin kyseiselle koneelle 2, muistia 4Gb ja tallennustilaa 40Gb. Tässä vaiheessa valitsin verkkokortiksi Palvelinverkon, joka on 192.168.0.0/24 alueella (kuva 9). Lopuksi valitsemme Next ja Finish.



KUVA 9 Virtuaalikoneen luominen

VPN-verkon lisäsin palvelimelle painamalla RRAS01 -palvelinta hiiren oikealla, valitsemalla Edit settings ja painamalla aukeavasta ikkunasta Add network adapter. Uuteen verkkoadapteriin valitsin juuri luomani VPN-verkon (kuva 10).



KUVA 10 VPN verkkoadapterin lisääminen

Tämän jälkeen uudelleenkäynnistin palvelimen ja asensin sille käyttöjärjestelmän. Käyttöjärjestelmän asennuksen jälkeen kirjauduin sisään ja annoin palvelimelle osoitteeksi jo valmiiksi löytyvästä palvelinverkosta 192.168.0.0/24 osoitteen 192.168.0.61 jonka kautta palvelin keskustelee muiden palvelinverkon palvelimien kanssa. VPN-verkkoa varten palvelimen toiselle verkkokortille annetaan osoite 192.168.250.2/24. Idea on, että tämä VPN-palvelun osoitealue toimii alueena josta etäkäyttäjät saavat IP-osoitteensa sekä yhdistävät ulkoverkosta. Palvelimen käyttöjärjestelmänä toimii Windows Server 2012 R2, joka on yleisessä käytössä asiakasyrityksellä.

4.2.1 RRAS-palvelun asennus

Itse VPN-yhteyden hallintaa hoitaa Remote and Routing Access Service, johon käyttäjät ottavat ulkoverkosta yhteyden ja joka jakaa reitit sekä IP-osoitteet käyttäjille. Uudelle RRAS-palvelua varten perustetulle palvelimelle asensin Remote Access -roolin valitsemalla Server Managerista Manage – Add Roles and Features ja valitsemalla oikea palvelin. Tämän jälkeen rooliksi valitsin Remote Access ja vein asennuksen loppuun painamalla Next ja lopussa Finish. Asennuksen jälkeen RRAS on asentunut ja se voidaan avata.

4.2.2 RRAS-palvelun käyttöönotto

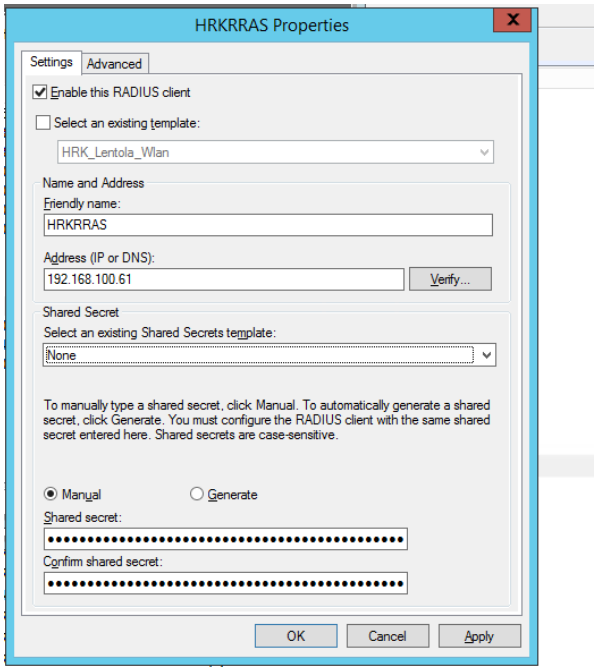
Palvelimen asennuksen jälkeen käyttöönotossa aukaisin Routing and Remote Access -palvelun, josta painoin RRAS01-palvelinta hiiren oikealla ja valitsin Properties. Täältä pääsin säätämään RRAS-palvelimen asetuksia. General kohdassa valitsin Enable this computer as a: IPv4 Router ja LAN and demand-dial routing, sekä laitoin IPv4 Remote access server kohtaan ruksin. Securityssä pääsin määräämään millä keinolla käyttäjät varmentuvat. Koska tätä käyttötarkoitusta varten valitsin Radiuksen, valitaan se. Tämän jälkeen Configure -kohdasta painamme Add ja laitamme palvelimen nimen RRAS01.toimisto.asiakasyritys.fi sekä valitsemamme pre-shared keyn joka löytyy myös NPS-palvelimelta RRAS01 -clientin alta.

IPv4 kohtaan määrittelemme mistä osoitealueesta käyttäjät saavat IP-osoitteensa. Tähän laitamme Add -kohdan kautta Start IP address 192.168.250.10 ja

End IP address kohtaan 192.168.250.250. Tässä tapauksessa osoitteita, joita käyttäjät voivat saada on yhteensä 241 mikä on enemmän kuin riittävästi tähän käyttötarkoitukseen. Muutama osoite jätettiin vapaaksi mahdollista vianetsintää varten.

4.2.3 NPS

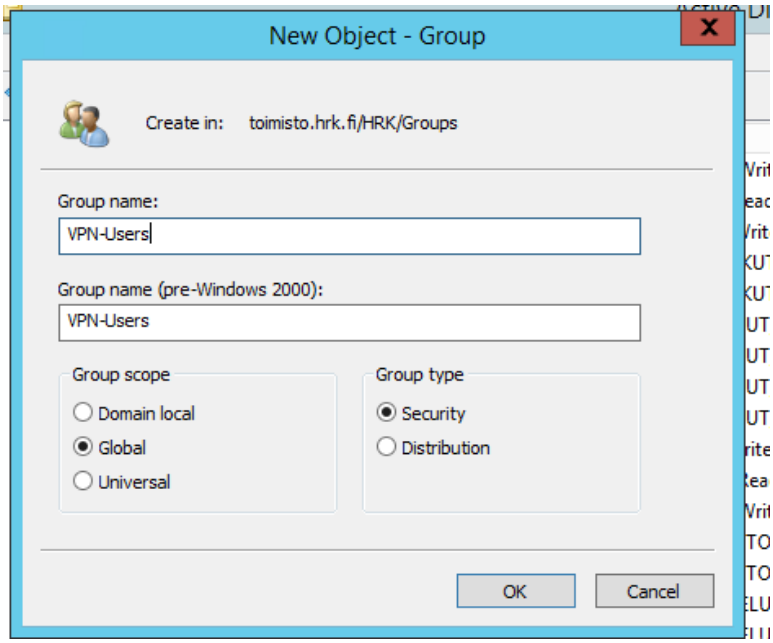
NPS eli Network Policy Server on käyttäjien selventämiseen käytetty palvelin, tunnetaan nykyään myös nimellä NAP, joka tulee sanoista Network Access Protection. Käytännössä NPS mahdollistaa Radius palvelimen, proxyn tai Policy Servicen luomisen. Jotta sain palvelimelle radiuksen, konfiguroin ensimmäiseksi NPS-palvelimelle oma radius-clientin RRAS-palvelinta varten. Tämä tapahtuu painamalla NPS-palvelimelta RADIUS Clients and Serverin alta Radius Clientsiä oikealla hiiren näppäimellä ja valitsemalla New. Tämän jälkeen täytetään tarvittavat tiedot, eli palvelimen nimi RRAS01, RRAS palvelimen sisäverkon osoite palvelinverkon puolella 192.168.0.61 sekä shared secret key (kuva 11). Seuraavaksi muutokset hyväksytään jonka jälkeen konfiguraatio NPS-palvelimen osalta on valmis. Mikäli shared secret key hukkuu jostain syystä sen saa näkyviin aukaisemalla taas properitiesin kautta RAS-palvelimen asetukset ja painamalla pohjalta löytyvää Generatea jolloin nykyinen salausavain tulee näkyviin.



KUVA 11 Radius Clientin luominen

4.2.4 Active Directory ryhmän luominen

Active Directory palvelimella hallitaan käyttäjiä, koneita sekä ryhmiä. Lisäämällä tietyt käyttäjät tai koneet ryhmiin voimme määritellä kyseisten käyttäjien sekä koneiden oikeuksia. On myös mahdollista lisätä ryhmiä toisten ryhmien sisään niin kuin tässä tein. AD-palvelimelle loin oman VPN-Users -ryhmän, jolla voidaan hallita käyttäjä- tai konekohtaisesti kuka pääsee kirjautumaan omalla koneellaan tai tunnuksillaan etäyhteyspalveluun. Tämän VPN-Users -ryhmän loin yrityksen alla olevaan Groups kansioon valitsemalla New – Group ja antamalla nimeksi VPN-Users (kuva 12), valitsemalla scopeksi Global sekä Group typeksi Security. Lopuksi lisäsin Domain Computers ryhmään VPN-Users ryhmän, joka tarkoittaa, että kaikki koneet Domain Computers ryhmässä kykenevät yhdistämään Always On VPN:ään.



KUVA 12 VPN-Users -ryhmän luominen

4.2.5 PKI:n asennus

Seuraavaksi tein sertifikaatin, joka asennetaan jokaiselle koneelle, josta on tarkoitus päästä yhdistämään VPN:ään. Tämä onnistuu kirjautumalla Certificate Authority palvelimelle, tässä tapauksessa DB02 -palvelimelle ja avaamalla Certificate Authority. Täällä valitsin Certificate Templates hiiren oikealla, jonka jäl-

keen painoin Manage. Tämän jälkeen eteen aukeaa Certificate Templates Console, jonka kautta pääsemme hallitsemaan sertifikaatteja. Tein kopion Users -sertifikaatista valitsemalla se hiiren oikealla ja painamalla Duplicate Template. Tämän jälkeen annoin oikeat asetukset sertifikaatille. Nimeksi sertifikaatille annoin VPN-Users, compatibility välilehdeltä valitaan Certification Authority kohtaan Windows Server 2012 R2 ja Certificate Recipient kohtaan Windows 8.1 / Windows Server 2012 R2. Request Handling -välilehdeltä valitsin Allow private key to be exported pois, Cryptography välilehdeltä valitsin Provided Category kohtaan Key Storage Provider ja Providers kohtaan valitsin Microsoft Platform Crypto Provider sekä toiseksi Microsoft Software Key Storage Provider. Security välilehdessä lisäsin VPN-Users ryhmän painamalla Add ja etsimällä oikea ryhmä, jonka jälkeen VPN-Users -ryhmälle annetaan Permission for VPN-Users kohdassa Allow Read, Enroll ja Autoenroll.

4.3. DNS ohjaus

DNS-ohjaus tehdään palveluntarjoajan DNS-palvelimella. Tässä tapauksessa riitti, että tein A-recordin asiakkaan domainin alle. Koska asiakkaan kaikki toimipisteistä ulos kulkeva liikenne menee saman palomuurin kautta, palvelinta varten ei tarvinnut varata omaa julkista IP-osoitettaan. DNS-ohjaus toteutetaan osoitteeseen vpn.asiakasyritys.fi, joka ohjaa liikenteen julkiseen IP-osoitteeseen 123.123.123.123. Muita tarvittavia tietoja DNS-merkinnälle on jo ennalta mainittu tyyppi, joka on A-record, TTL, joka tulee sanoista Time to Live, joka määrittelee kuinka pitkäksi aikaa rekursiivinen DNS-palvelin tallentaa tiedon. Tässä tapauksessa arvoksi annetaan 10800 joka vastaa kolmea tuntia. Toiminnallisuuden kannalta DNS-ohjaus ei ole kriittinen, mutta palvelimen nimi on huomattavasti helpompi muistaa verrattuna IP-osoitteeseen. DNS-palvelimena toimii palveluntarjoajan oma nimenselvennyspalvelin.

4.4. Palomuuri

Kun liikenne on ohjattu nimen perusteella tiettyyn julkiseen IP-osoitteeseen, se piti kääntää oikealle palvelimelle. Tässä tapauksessa saapuva liikenne tulee

UDP-portteihin 500 sekä 4500. Tämä vaatii, että palvelimella on oma sisäverkon osoitteensa, johon liikenne ohjataan, sekä palomuurilta tai vastaavalta reitittävältä laitteelta löytyy julkinen IP-osoite, josta liikenne voidaan ohjata.

NAT-sääntö toteutetaan palomuurilla siten, että liikenteen saapuessa julkiseen osoitteeseen se ohjataan eteenpäin palvelimen sisäverkon osoitteeseen. Koska tämä on toimeksiantajan ainoa sen verkossa oleva VPN-ratkaisu, oli mahdollista, että käytin palvelinverkolle varattua omaa julkista osoitetta tässä tapauksessa. Tämä kuitenkin estää muiden UDP portteja 500 ja 4500 käyttävien palveluiden käytön samalla osoitteella (taulukko 5).

TAULUKKO 5 Toimeksiantajalle tehdyn NAT-säännön logiikka

Source Original	Source Translated	Destination Original	Destination Translated	Services Original	Services Translated
Any	Original	123.123.123.123	192.168.250.2	UDP500, UDP4500	Original

NAT-säännön tekeminen palomuurille vaatii myös oman liikenteen sallivan sääntönsä. Jokaisella palomuurivalmistajalla on oma tapansa toimia liikenteen sallimisesta. Tässä tapauksessa oli tärkeää huomioida, että liikenne tulee sallia sisäverkon zoneen julkisella osoitteella. Tässä tapauksessa sääntö tehdään Sonicwall-merkkiseen palomuuriin, johon julkiverkosta sisäverkkoon tulevan liikenteen salliva sääntö vaatii toimiakseen, että kohdealue liikenteelle on customers, jonka alta löytyy toimeksiantajan sisäverkon laitteet, mutta osoite on julkinen 123.123.123.123. Normaalin logiikan mukaan liikenne sallittaisiin palvelimen sisäverkon osoitteeseen 192.168.250.2. Tämä voi aiheuttaa sekaannusta, mikäli palomuurit eivät ole tuttuja (taulukko 6).

TAULUKKO 6 Liikenteen salliva sääntö

Source Zone	Destination Zone	Source Address	Destination Address	Services	Action
WAN	Customers	Any	123.123.123.123	UDP500, UDP4500	Allow

4.5. Ongelmat

Käyttöönotossa tuli muutama ongelma vastaan. Koneiden oma palomuuri esti UDP liikennettä porteista 500 sekä 4500 ulospäin vaikka koneen omilta palomuureilta löytyi sääntö sallia kaikki UDP liikenne ulkoverkkoa kohden. Tämä korjaantui tekemällä koneiden palomuuriin oma salliva sääntönsä nimenomaan näille porteille, kun liikenne menee ulkoverkkoon.

Myös sertifikaatin asentaminen koneelle osoittautui omalla tavallaan hankalaksi. Sertifikaatin asennuksen jälkeen huomasin, että yhteys ei toiminut, joten aluksi epäilin vian olevan sertifikaatissa. Todellisuudessa tämän voi toteuttaa vain silloin kun on yhteys asiakkaan palvelinverkkoon, joka onnistuu palveluntarjoajan VPN-palvelua hyödyntäen. Tämän jälkeen kone vaatii uudelleenkäynnistyksen jotta tehdyt muutokset astuvat voimaan.

5 POHDINTA

Vuosi 2020 on ollut tähän asti etätyöskentelyn kannalta erittäin tärkeä vuosi. Yritykset ovat entistä enemmän tajunneet etäpalveluiden tärkeyden. Yrityksen toiminnan kannalta on erittäin tärkeää, että työntekijöillä on mahdollisuus tehdä töitä myös etänä, mikäli työpaikalle tuleminen jostain syystä estyy. Työn tekeminen aloitettiin alun perin loppuvuodesta 2019, jolloin asiakas kertoi toiveensa toisesta VPN-palvelusta.

Opinnäytetyön tavoitteena oli löytää luotettava ja helppokäyttöinen VPN ratkaisu asiakkaalle, jossa joillakin työntekijöillä on etäyhteys käytössä päivittäin. Projektin loppumisen jälkeen pääsin kysymään asiakkaalta mielipidettä siitä, kuinka Always On VPN käyttö on muuttanut toimintaa, hyvässä tai huonossa. Pääasiassa muutos on ollut positiivinen. Always On VPN on huomattavasti helppokäyttöisempi aiempaan VPN-palveluun verrattuna. Myös tiedostojen siirto palvelimelle on huomattavasti nopeampaa mikä tekee työn tekemisestä etänä paljon sujuvampaa.

Muutama kehityskohta tuli myös keskustelussa esille. Koska asiakkaalla on tarve myös tarjota etäyhteys joillekin yrityksen ulkopuolisille tekijöille olisi suotavaa, että kuka tahansa pystyisi kirjautumaan VPN-palveluun riippumatta siitä onko kyseisellä käyttäjällä oikeaa sertifikaattia. Tämä onnistuisi tekemällä Always On VPN SSTP-tunnelia hyödyntäen. Oletusarvo Always On VPN:llä on että SSTP on ensisijainen tapa yhdistää palvelimelle jonka jälkeen käytetään IKEv2. Koska tässä projektissa päätettiin toteuttaa täysin hyödyntäen IKEv2 koneella täytyy olla oikea sertifikaatti asennettuna. On mahdollista saada SSTP toimimaan IKEv2:n varmistukseksi. Tämä on mahdollista toteuttaa mutta sovimme sen myöhemmälle ajankohdalle. Jälkikäteen katsottuna olisi kannattanut käyttää SSTP:tä myös sen toimintavarmuuden takia. Ilmeisesti joissain tilanteissa IKEv2 liikennettä on estetty joissain paikoissa mikä tekee työskentelemisen kyseisessä paikassa haasteelliseksi. SSTP:n käyttämä TCP-portti 443 olisi hyvin todennäköisesti ollut sallittujen joukossa ja etätyöskentely olisi ollut mahdollista.

Always On VPN käyttöönottoon tarvittavat lähteet löytyivät loppujen lopuksi helposti. Vaikka lähteitä ei hirveästi ollutkaan, käyttöönotto oli riittävän helppo toteuttaa eikä suuria ongelmia tullut vastaan. Microsoftin osalta dokumentaatio vaikutti hieman keskeneräiseltä ja useassa kohdassa oli luotettavampaa käyttää jonkun ulkopuolisen tekemää ohjetta tai dokumentaatiota.

Opinnäytetyön tarkoituksena oli selvittää yritykselle helposti käyttöönotettava sekä luotettavan VPN-palvelu ja ottaa se käyttöön. Uskon päässeeni työn lopputavoitteeseen. Työn tuloksia voidaan soveltaa niin pienissä sekä isoissa yrityksissä, vaatimuksena että yrityksellä on omia palvelimia. Tulevaisuuden kannalta kannattaa kuitenkin aina tutustua uusimpiin teknologioihin ja tehdä päätös tutustumisen pohjalta. VPN-protokollista löytyy aina joskus turvallisuusaukkoja sekä ongelmia, jotka tekevät niistä teknisesti katsottuna vanhentuneita.

LÄHTEET

Bischoff, P. 2018. 6 Open Source Tools for Making your own VPN. Luettu 18.3.2020
https://opensource.com/article/18/8/open-source-tools-vpn

Chang, H. 2020. How to setup WireGuard VPN server on Windows. Luettu 8.3.2020.
https://www.henrychang.ca/how-to-setup-wireguard-vpn-server-on-windows/

Donenfeld, J. 2016. WireGuard: a new VPN tunnel. Luettu 29.3.2020
https://lwn.net/Articles/693015/

Durret, J. 2015. Secret documents show the NSA is spying on VPN users. Luettu 20.3.2020.
https://hacker10.com/internet-anonymity/secret-documents-show-the-nsa-is-spying-on-vpn-users/

ExpressVPN. What is L2TP/IPsec. Luettu 12.4.2020.
https://www.expressvpn.com/fi/what-is-vpn/protocols/l2tp

Griffin, L. Authentication Protocols: Definition & Examples. Luettu 13.5.2020.
https://study.com/academy/lesson/authentication-protocols-definition-examples.html

Griggs, B. 2013. Report: Microsoft collaborated closely with NSA. Luettu 21.3.2020.
https://edition.cnn.com/2013/07/12/tech/web/microsoft-nsa-snooping/index.html

Hicks, R. 2017. DirectAccess is now Always On VPN. Luettu 18.3.2020
https://directaccess.richardhicks.com/directaccess-is-now-always-on-vpn/

Hicks, R. 2018. What is the difference between Direct Access and Always On VPN. Luettu 2.4.2020.
https://directaccess.richardhicks.com/2018/02/05/what-is-the-difference-between-directaccess-and-always-on-vpn/

Juniper. 2019. Authentication Algorithms. Luettu 29.3.2020.
https://www.juniper.net/documentation/en_US/junos/topics/concept/ipsec-authentication-solutions.html

Lowendtalk. 2015. Why is VPN so slow. Luettu 12.4.2020.
https://www.lowendtalk.com/discussion/40099/why-openvpn-is-so-slow-cool-story

Loyd, B. Simpson, W. 1992. PPP Authentication Protocols. Luettu 12.5.2020
https://tools.ietf.org/html/rfc1334

Matthews, K. 2018. Security Gaps Found in IPsec. Luettu 2.4.2020.
https://hackernoon.com/security-gaps-found-in-ipsec-5a075b44609e?gi=a8b84ed0d0c0

Microsoft. Always On VPN deployment for Windows Server and Windows 10. Luettu 17.03.2020.
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/always-on-vpn-deploy

Mocan, T. 2019a. What is PPTP. Luettu 20.3.2020.
https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-pptp

Mocan, T. 2019b. What is SSTP. Luettu 22.3.2020.
https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-sstp/#definition

Mocan, T. 2019c. What is OpenVPN. Luettu 24.3.2020.
https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-openvpn/

Mocan, T. 2019d. What is IKEv2. Luettu 29.3.2020.
https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-ikev2/

Pauly, T. Touati, S. Mantha, R. TCP Encapsulation of IKEv2 and IPSec Packets. Luettu 2.4.2020.
https://tools.ietf.org/id/draft-pauly-ipsecme-tcp-encaps-04.xml

Phillips, G. 2017. The 5 Major VPN Protocols Explained. Luettu 11.5.2020
https://www.makeuseof.com/tag/major-vpn-protocols-explained/

Prakash, A. 2020. What is WireGuard. Luettu 29.3.2020.
https://itsfoss.com/wireguard/

Simpson, W. 1996. PPP Challenge Handshake Authentication Protocol (CHAP). Luettu 12.5.2020.
https://tools.ietf.org/html/rfc1994

SoftEther. 2019. Authentication Using NT Domain Controller or Active Directory Con-troller. Luettu 8.5.2020.
https://www.softether.org/4-docs/1-manu-al/2._SoftEther_VPN_Essential_Architecture/2.2_User_Authentication#Authentication_Using_NT_Domain_Controller_or_Active_Directory_Controller

Securew2. PEAP MSCHAPv2 Vulnerability. Luettu 20.4.2020.
https://www.securew2.com/blog/peap-mschapv2-vulnerability/

Stevens, P. 2020. Encryption Algorithms. Luettu 25.3.2020.
https://www.toptenreviews.com/encryption-algorithms

StrongSwan. 2018a. About StrongSwan. Luettu 20.3.2020.
https://www.strongswan.org/about.html

StrongSwan. 2018b. StrongSwan on Windows. Luettu 12.4.2020.
https://wiki.strongswan.org/projects/strongswan/wiki/Windows

Townsley, W. Valencia, A. 1999. Layer Two Tunneling Protocol "L2TP". Luettu 12.5.2020.
https://tools.ietf.org/html/rfc2661

Temblay, T. OpenVPN and the Platforms on which it runs. Luettu 24.3.2020.
https://www.fastestvpnguide.com/openvpn-and-the-platforms-on-which-it-runs/

Tulloch, M. 2020. Always On VPN. Luettu 18.3.2020.
http://techgenix.com/always-on-vpn/

VPNdada. Which VPN Protocol to Use. Luettu 22.3.2020.
https://www.vpndada.com/which-vpn-protocol-to-use-openvpn-vs-pptp-vs-l2tp-vs-sstp/

VPNmentor. 2020. Different Types of VPNs and When to Use Them. Luettu 12.5.2020.
https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/

VPNoverview. 2020. VPN explained: How does it work? Why would you use it? Luettu 11.5.2020
https://vpnoverview.com/vpn-information/what-is-a-vpn/

Vyprvpn. 2016. A Brief History of VPNs. Luettu 20.3.2020.
https://www.goldenfrog.com/blog/brief-history-of-vpns

Webopedia. PAP – Password Authentication. Luettu 12.4.2020.
https://www.webopedia.com/TERM/P/PAP.html

Zagradanin, I. 2020. The History of VPN. Luettu 12.4.2020.
https://www.geosurf.com/blog/history-of-vpn-the-quest-for-a-better-internet/