Saku-Petteri Alatalo

VPN-tunnelointiprotokollan valitseminen ja hyödyntäminen liikenteen salaamiseksi

Tradenomi

Tietojenkäsittely

Kevät 2021

KAMK • University of Applied Sciences

Tiivistelmä

Tekijä: Alatalo Saku-Petteri

Työn nimi: VPN-tunnelointiprotokollan valitseminen ja hyödyntäminen liikenteen salaamiseksi

Tutkintonimike: Tradenomi (AMK), tietojenkäsittely

Asiasanat: VPN, tunnelointi, virtuaaliverkko, Pritunl

Opinnäytetyön tavoitteena oli vertailla eri VPN-tunnelointiprotokollia, valita vertailun perusteella parhaiten soveltuva protokolla liikenteen salaamiseksi ja toteuttaa tulosten perusteella yksityinen virtuaaliverkko ympäristö (VPN). Vertailtavia tunnelointiprotokollia käydään läpi yhteensä viisi kappaletta. Vertailun perusteella päädyttiin toteuttamaan OpenVPN-protokollapohjainen yksityinen virtuaaliverkko. Virtuaaliverkon toteuttamiseksi käytettiin hyväksi Pritunl-sovellusta, joka on vapaaseen lähdekoodiin pohjautuva yksityisen virtuaaliverkon luomiseksi käytettävä sovellus. Opinnäytetyö koostuu kahdesta kokonaisuudesta: teoriaosuudesta, jossa vertaillaan tunnelointiprotokollia ja tutustutaan kolmannen osapuolen sovellukseen nimeltä Pritunl sekä käytännön toteutuksesta.

Opinnäytetyön aikana toteutettiin Kajaanin Ammattikorkeakoulun datacenter-opiskelijoilla käytössä olevaan konesali-infrastruktuuriin yksityinen virtuaaliverkko Pritunl-nimistä sovellusta käyttämällä. Yksityisverkon toteuttamisen päällimmäinen syy on datapakettien salaaminen ja yksityisyyden parantaminen liikuttaessa internetissä.

Työlle asetetut tavoitteet saavutettiin. Aikaan saatiin yksityinen virtuaaliverkko, jota käyttämällä lähtevä liikenne saadaan salattua siten, etteivät samassa verkkoympäristössä sijaitsevat laitteet pääse arkaluontoisiin tietoihin käsiksi.

Abstract

Author(s): Alatalo Saku-Petteri

Title of the Publication: Choosing and Utilizing VPN Tunneling Protocol to Improve Security

Degree Title: Bachelor of Business Administration, Business Information Technology

Keywords: VPN, tunneling, Pritunl

This Bachelor's thesis is focused on comparing different VPN tunneling protocols, choosing the most suitable one and building a virtual private network (VPN) environment upon it. Five tunneling protocols were considered, among which OpenVPN tunneling protocol outshined other competitors. In order to deploy OpenVPN protocol in use, third party software called Pritunl was needed. Pritunl is an open-source based software that utilizes the OpenVPN protocol for establishing connections between the client machine and deployed VPN server. The thesis is divided between a theory part and practical part.

The thesis was implemented in Kajaani University of Applied Sciences where datacenter students have access to private on-site datacenter infrastructure. The VPN infrastructure is built upon the servers residing in the datacenter using the Pritunl software. The reason for creating virtual private network is to ensure data security and integrity for users when browsing the Internet.

The goals for the thesis were met. The most suitable tunneling protocol was found after comparing the alternatives, and a working VPN infrastructure was successfully built. Pritunl was able to protect the outgoing data by directing the traffic through established tunnel between the client machine and the VPN server.

Sisällys

Lyhenteet ja määritelmät

ESP	Encapsulating Security Payload, joka parantaa yhteyden luottamuksellisuutta. Pitää yllä yhteydettömän datan eheyden ja vastaa saapuvan datan alkuperän todentamisesta.
IKE	Internet Key Exchange, joskus myös IKEv1 ja IKEv2 riippuen versiosta. IKE-protokollalla luodaan SA IPSec-pohjaisissa VPN-yhteyksissä.
IPv4	32-bittinen numerosarja, joka on uniikki jokaisella koneella. Verrattavissa kotiosoitteeseen postittaessa.
IPv6	64-bittinen numerosarja, joka on uniikki jokaisella koneella. Uusin käytössä oleva IP-protokolla. Verrattavissa kotiosoitteeseen postittaessa.
LCP	Link Control Protocol. Neuvottelee ja sopii datalähetysstandardeista PPP-protokollaa käytettäessä.
NAT	Network Address Translator muokkaa lähtevien datapakettien IP-osoitteen NAT:iin määritellyn IP-osoitteen mukaiseksi.
NAS	Network Access Serveriä käytetään etäyhteyksien muodostamiseen etenkin puhelinverkkoyhteyksissä.
NCP	Network Control Protocol vastaa ylimääräisten verkkotason protokollien neuvottelusta lähetettäessä datapaketteja käyttämällä PPP-protokollaa.
OSI-malli	Interconnection Reference Model, seitsemänkerroksinen tiedonsiirtoprotokollien yhdistelmää kuvaava malli.
Pritunl	Pritunl on sovellus, jota käyttämällä mahdollistetaan yksityisen virtuaaliverkon luominen. Koostuu kahdesta osasta, palvelinkoneelle asennettavasta sovelluksesta sekä asiakaskoneelle asennettavasta sovelluksesta.

SA	Security Association, jolla tarkoitetaan salausattribuuttien määrittämistä kahden eri verkkoympäristön välille turvallisen kommunikoinnin takaamiseksi. Esimerkiksi symmetrisen salausavaimen luonti, jota käytetään liikenteen salaamisen ja salauksen purkamiseen.
TCP	Transmission Control Protocol, varmistava tiedonsiirtoprotokolla. Protokolla varmistaa datapakettien pääsemisen perille.
UDP	User Datagram Protocol, varmistamaton tiedonsiirtoprotokolla. Datapaketit kulkevat ilman yhteyden muodostamisen varmentamista.
VPN	Virtual Private Network, yksityinen virtuaaliverkko. Salaa lähtevän dataliikenteen muodostamalla sille putken, jota pitkin datapaketit kuljetetaan suojatun palvelimen kautta määränpäähän.

1 Johdanto

”Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet.”

“Yksityisyys ei ole vaihtoehto, eikä sen kuulu olla maksu, jonka me olemme valmiita maksamaan päästäksemme internetiin.”

– Gary Kovacs. [1.]

Internetin yksityisyys on ollut viime aikoina mediassa pinnalla ympäri maailmaa. Tarkastelun alle ovat joutuneet suuret sosiaalisen median jätit, joista erityisesti Facebook ja sen omistaja Mark Zuckerberg. Asia puhkesi niin laajaksi, että tämän pohjalta toteutettiin jopa täysimittaisia dokumentteja, kuten suuren suosion kerännyt ”The Great Hack” (2019). Dokumentti perustuu brittiläiseen analytiikkafirman Cambridge Analyticaan ja Analytican käyttämään tapaan, miten ihmisistä kerättyä dataa hyödynnettiin vuonna 2016 järjestetyissä presidentinvaaleissa Amerikassa. [2.]

Yksityisiin tietoihin päästään luvatta käsiksi myös kotimaassa, eikä siihen aina pääse itse vaikuttamaan. Viimeisin esimerkki tapahtuneesta on uutinen psykoterapiakeskus Vastaamon tietomurrosta. Murtautuja julkaisi verkkoon yksityisiä asiakastietoja sekä vei yritykseltä 450 000 euron edestä rahaa. [3.]

Miten omalla toiminnalla pystyy vaikuttamaan, etteivät yksityiset tiedot ajaudu ulkopuolisten käsiin? Vastaamon tietomurron kaltaisissa tilanteissa vastuun joutuu kantamaan IT-sektorin johtoporras, mutta Facebookin kaltaista tietojen keräämistä vastaan on olemassa suojautumiskeinoja. Yksi näistä keinoista on virtuaalisen yksityisverkon (VPN) käyttö, jota hyödyntämällä voidaan suojata omalta laitteelta ulkoverkkoon lähtevä liikenne.

Yksityistä virtuaaliverkkoa voidaan käyttää muutamaan eri käyttötarkoitukseen, mutta tämän opinnäytetyön tarkoituksena on tutkia oman virtuaaliverkon pystyttämistä lähtevän liikenteen salaamisen parantamiseksi. Yksityisen virtuaaliverkon läpi kulkeva liikenne on salattu muilta samassa verkossa olevilta käyttäjiltä, jonka vuoksi VPN-sovellus on hyödyksi käytettäessä julkisia verkkoyhteyksiä, joita löytyy esimerkiksi junista tai hotelleista.

Yksityinen virtuaaliverkko tullaan luomaan hyödyntämällä Pritunl-nimistä, avoimeen lähdekoodiin pohjautuvaa sovellusta. Pritunlin tekniikka poikkeaa monista muista VPN-järjestelmistä siten,

että OpenVPN-pohjaiset ratkaisut vaativat erillisten ohjelmistojen asentamisen asiakas- ja palvelinkoneelle. OpenVPN-protokollaa käyttävät yhteydet muodostetaan OSI-mallin toisella tai kolmannella tasolla ja liikenne tunneloidaan käyttämällä joko UDP- tai TCP-protokollaa. [4.]

2 Virtuaalinen yksityisverkko (VPN)

Virtuaalinen yksityisverkko parantaa internetin käyttäjän yksityisyyttä ja anonymiteettiä tunneloimalla liikenteen yksityisen virtuaaliverkon kautta [5]. Tunneloinnin tärkeys korostuu etenkin käytettäessä julkisia verkkoyhteyksiä, kuten kahvilan tai hotellin WiFi-yhteyksiä. Tunneloimalla liikenteen yksityisen virtuaaliverkon kautta datapaketit salataan, jotta samaa julkista verkkoyhteyttä käyttävät päätelaitteet eivät pääse vahingossa tai tahallaan käsiksi käyttäjien arkaluontoisiin tietoihin, kuten käyttäjätunnuksiin ja salasanoihin.

Tunneloinnin toinen hyöty datapakettien salaamisen lisäksi on oman julkisen IP-osoitteen piilottaminen julkiverkossa. Tunneloitu liikenne siirtyy viimeiseksi julkiverkkoon VPN:n määrittelemän päätepisteen kautta ja käyttää päätepisteelle määriteltyä IP-osoitetta, jonka vuoksi käyttäjän oma IP-osoite paljastuu VPN-palveluntarjoajalle eikä kenellekään muulle. [5.] Koska käyttäjän IP-osoite pysyy piilossa, palveluntarjoajien ja hakukoneiden mahdollisuus seurata ja tallentaa käyttäjäkohtaisia hakutietoja ei ole mahdollista, sillä haku- ja käyttötiedot kohdistuvat VPN-palvelimen julkiseen IP-osoitteeseen.

Kolmas virtuaalisen yksityisverkon potentiaali piilee käyttäjän mahdollisuudessa valita kohdemaa, mitä kautta tunneloitu liikenne kulkee julkiverkkoon. Moni suuri sivusto tarjoaa käyttäjilleen näkymän, joka on räätälöity käyttäjän kohdemaan mukaiseksi. Tämän vuoksi käyttäjä ei välttämättä pääse käsiksi haluamaansa tietoon, mikäli sivusto on rajannut tiedon käyttäjän kohdemaan ulkopuolelle. Rajoitusongelmien kiertämiseksi VPN tarjoaa monesti eri maihin sijoitettuja kohdepalvelimia, joiden avulla halutulle sivustolle voidaan mennä eri maan kautta. Esimerkiksi suoratoistojätti Netflix tarjoaa käyttäjilleen eri tarjonnan käyttäjän kohdemaan mukaan. Netflixin tarjontaa voidaan kuitenkin laajentaa vaihtamalla VPN-palvelimen kohdemaata ja selaamalla tarjontalista uudelleen läpi.

2.1 VPN:n hyödyntäminen opinnäytetyössä

Tässä opinnäytetyössä tullaan käsittelemään etäyhteyden muodostavaa VPN:ää (Remote-access VPN) ja sen hyödyntämistä, eikä oteta kantaa yritysverkkoja keskenään yhdistäviin VPN:iin (Site-

to-site). Vaikka etäyhteyden muodostavat VPN-palvelimet kytketään usein kuluttajille suunniteltuihin VPN-palveluihin, voidaan samaa ideologiaa hyödyntää työelämässä. Työntekijälle voidaan mahdollistaa oikeus päästä käsiksi työpaikan verkkoympäristöön ja tämän tunnelin luominen työntekijän päätelaitteen ja työpaikan VPN-palvelimen välillä tuo mukanaan monia tietoturvaparannuksia. [6]

Etäyhteyden muodostaminen oli alun perin keino mahdollistaa työntekijän pääsy yrityksen verkkoympäristöön mistä tahansa päin maailmaa tahansa, turvallisesti. VPN-palveluille tuttuun tapaan etäyhteyden mahdollistavilla VPN-palvelimilla on tarkoitus suojata arkaluontoinen data. Etäyhteyden muodostavilla VPN:illä työntekijän päätelaite on yhdessä palvelimen kanssa vastuussa lähtevän- ja saapuvan dataliikenteen salaamisesta ja salauksen purkamisesta. [7.]

Etäyhteyden muodostava VPN vaatii toimiakseen joko NAS-palvelimen tai VPN-yhdyskäytävän käyttäjien autentikointia varten. Työntekijä yhdistyykin oikeasti NAS-palvelimeen, kun halutaan muodostaa yhteys työpaikan verkkoympäristöön ja siellä sijaitsevaan VPN-palvelimeen. Yleisin keino autentikoinnin hoitamiseksi on työntekijän päätelaitteelle asennettava VPN-asiakasohjelma, joka kommunikoi VPN-yhdyskäytävän kanssa. Onnistuneen autentikoinnin jälkeen työntekijän päätelaitteen ja työpaikan verkkoympäristön välille luodaan virtuaalinen tunneli. [7.]

Kun tunneli päätelaitteen ja kohdepalvelimen välille on luotu, kaikki data työntekijän päätelaitteelta on kapseloitu ja salattu VPN-palvelimen toimesta. Datapaketit kulkevat tunnelin läpi VPN-yhdyskäytävälle, joka sijoittuu työpaikan verkkoympäristön ulkopuolelle. Yhdyskäytävä purkaa sille saapuneet salatut datapaketit ja välittää datapakettien sisällön yrityksen verkkoympäristöön. Salaus toimii myös toiseen suuntaan – työpaikan verkkoympäristöstä lähetetyt datapaketit salataan yhdyskäytävän toimesta ja työntekijän päätelaitteelle asennettu VPN-asiakasohjelma purkaa yhdyskäytävän muodostaneen salauksen. [7.] Kappaleessa 2.2 ja sen jälkeisissä alakappaleissa perehdytään tarkemmin, miten eri protokollissa toteutetaan yhteyden muodostaminen.

2.2 Point-to-point protokolla (PPP)

PPP on jo pitkään olemassa ollut protokolla, jota voidaan hyödyntää suorien yhteyksien muodostamisessa eri verkkolaitteiden välille. PPP toimii OSI-mallin ensimmäisellä, toisella ja kolmannella kerroksella ja koostuu kolmesta pääkomponentista: monia protokollia sisältävien tietosähkeiden

kapseloinnista tiedonsiirtoa varten, yhteyden muodostamisesta ja konfiguroinnista verkkolaitteiden välillä LCP:n avulla sekä NCP:n käyttämistä verkkokerroksella erilaisten verkkokerroksen tiedonsiirtoprotokollien mahdollistamiseksi. [8.]

PPP:tä hyödynnetään useasti datapakettien kapseloinnissa TCP/IP-pohjaisissa verkkoyhteyksissä. Pisteestä pisteeseen-yhteyden muodostamiseksi tarvitaan WAN-linkki kahden eri verkkopaikan välille, modeemi ja joissain tapauksissa reititin sekä määritelty protokolla. WAN-yhteydet vaihtelevat usein, joten on tärkeä konfiguroida PPP monien eri yhteystyyppien varalle. Peruskonfigurointi on kuitenkin yksinkertaista ja yleisohjeet kattavat suurimman osan nykypäivän WAN-yhteyksistä. Tämän vuoksi PPP on vielä laajalti käytössä oleva protokolla. [9.]

LCP:n ja NCP:n käyttö PPP-pohjaisessa yhteydessä TCP/IP-verkossa muodostuu usean vaiheen kautta: Ensimmäisessä vaiheessa käyttäjä lähettää ensin LCP-viestejä konfiguroidakseen ja testatakseen yhteyden, jonka jälkeen molemmat osapuolet vaihtavat viestejä keskenään keskustellakseen millaiseen linkkiin tiedonsiirrossa päädytään. Tämän vaiheen jälkeen käyttäjän päätelaite lähettää NCP-viestejä määritelläkseen verkkotason protokollavalinnan, joista yksi eniten käytössä olevista protokollista on IP-protokolla. Viimeisessä vaiheessa määritellyn linkin kautta voidaan lähettää IP-protokollan avulla paketteja ja kehyksiä, jonka jälkeen NCP ja LCP viestien avulla muodostettu yhteys suljetaan ohjatusti. [9.]

3 Tunnelointiprotokollat

VPN-yhteyden muodostamiseksi on olemassa monia erilaisia tunnelointiprotokollia. Tunnelointiprotokollista valitaan yksi opinnäytetyön toteuttamiseksi ja valinnan helpottamiseksi protokollille voidaan antaa eri kriteereitä. Toteutettavan ympäristön kuuluu olla mahdollisimman hyvin saavutettavissa vaikeammissakin olosuhteissa. Yksi haastavista ympäristöistä on esimerkiksi hotellin avointa verkkoympäristöä käytettäessä, sillä hotellin palomuuri voi estää VPN-yhteyden muodostamisen. [10] Hotellin julkisen verkon skenaariota voidaan käyttää kuviteltuna testiympäristönä, jonka ongelmien syntymistä voidaan ehkäistä valittaessa käytettävä tunnelointiprotokolla.

Hotellin palomuurit olettavat monesti VPN-yhteyden olevan SSL-liikennettä ja pyrkivät estämään etäyhteyden muodostamisen sen mukaisesti. Tämänkaltaiset estot voidaan kiertää muutamalla eri keinolla: HTTPS-pohjaisella liikenteellä ja 443 porttia käyttämällä. HTTPS-liikenne käyttämällä 443-porttia on normaalin kaltaista verkkoliikennettä, jota ei palomuurisäännöissä erikseen estetä, sillä muuten tavallinen verkkosivujen selaaminen häiriintyy. Mahdollisten palomuurisääntöjen vuoksi on tärkeää kiinnittää huomiota tunnelointiprotokollan käyttämään porttiin ja liikenteen tyyppiin. [10.] Muita tunnelointiprotokollien tarkasteltavia ominaisuuksia ovat yhteyden nopeus, salaus sekä lähdekoodin avoimuus.

Vertailtavaksi valitaan viisi eri tunnelointiprotokollaa, jotka ovat laajalti käytössä. Näihin protokolliin tullaan perehtymään syvällisemmin kolmannessa luvussa. Vertailtavat tunnelointiprotokollat ovat PPTP, L2TP, IKEv2, SSTP ja OpenVPN, jotka valittiin vertailtaviksi niiden yleisyyden vuoksi. [11.] [12.]

3.1 PPTP

PPTP esiteltiin ensimmäistä kertaa vuonna 1999 tunnelointiprotokollana, joka on paranneltu versio jo aiemmin luvussa 2.2 käsitellystä PPP-protokollasta, sisältäen tunnelointiominaisuuden, joka PPP-protokollasta puuttuu. Alun perin PPTP suunniteltiin Windows-käyttöjärjestelmille, mutta protokolla herätti maailmalla suurta kiinnostusta ja pian protokollaa oli mahdollista hyödyntää myös muilla usein käytetyillä käyttöjärjestelmillä, kuten esimerkiksi Linuxilla ja macOS:llä. [13.]

PPTP-asiakasohjelma muodostaa PPTP-palvelimen ja asiakaskoneen välille yhteyden, jota kutsutaan tunneliksi. PPTP kapseloi verkkoon lähtevät datapaketit ja lisää datapakettiin IP-paketin otsikon (IP-header), jonka avulla kaikki datapaketin kanssa tekemisissä olevat laitteet kohtelevat datapakettia IP-pakettina. Kun lähetetty datapaketti pääsee perille PPTP-palvelimelle, ohjaa palvelin paketin kohdelaitteelle. [13.]

Yhteyden muodostamiseen tarvitaan kohdepalvelimen IP-osoite, käyttäjätunnus ja salasana. Datapaketit kapseloidaan Ciscon kehittämällä IP-tunnelointiprotokollalla GRE:llä (Generic Routing Encapsulation) ja liikenne ohjataan palvelimen TCP-porttiin 1723 ja IP-porttiin 47. PPTP tukee maksimissaan 128-bittisiä salausavaimia. [13.]

PPTP käyttää kuitenkin nykypäivän standardien mukaan vanhentunutta teknologiaa, joka on altis monia eri uhkia vastaan. Yksi esimerkki tietoturva-aukoista on dokumentoidut todisteet siitä, että NSA on onnistunut kaappaamaan ja purkamaan PPTP:tä käyttävää liikennettä. PPTP:llä on myös autentikointiin liittyviä, laajalti tunnettuja tietoturvapuutteita. [14.] Hakkerit käyttävät usein hyödykseen tietoturvapuutteita, jonka vuoksi PPTP:n soveltaminen tämän opinnäytetyön käytännön osuutta varten ei ole paras vaihtoehto ja luku PPTP-protokollan tiimoilta voidaan pitää lyhyehkönä.

Käsiteltäessä tunnelointiprotokollia on kuitenkin hyvä käydä PPTP läpi lähinnä protokollan edelläkävijän roolin vuoksi. PPTP on vielä laajalti käytössä sen nopeiden yhteyksien, käyttöjärjestelmäintegraatioiden ja vanhuuden vuoksi, mikäli aikanaan toimivaa tunnelointiprotokollaa ei ole syystä tai toisesta korvattu turvallisemmilla ja ajantasaisemmilla tunnelointiprotokollilla.

3.2 L2TP/IPsec

L2TP on lyhenne englanninkielisistä sanoista Layer 2 Tunneling Protocol. Tunnelointiprotokollan nimi viittaa OSI-mallin toiseen kerrokseen, siirtokerrokseen, jota protokolla hyödyntää toimiakseen. L2TP julkistettiin vuonna 1999, ja se on yhdessä Microsoftin ja Ciscon suunnittelema protokolla, joka on jatkoa edeltäjälleen PPTP:lle. [15.] L2TP-protokolla hyödyntää monia Microsoftin ja Ciscon ominaisuuksia L2F (Layer 2 Forwarding) protokollasta, jota hyödynnetään esimerkiksi PPP:n kaltaisen puhelinverkon analogisen liittymän kautta muodostettavissa VPN-yhteyksissä Internetin yli. L2TP-protokolla ei kuitenkaan tarjoa itse minkäänlaista salausta tunnelin läpi kulkevalle liikenteelle, vaan vastaa pelkästään tunnelin luomisesta ja ylläpidosta VPN-palvelimen ja

kohdelaitteen välillä. Tämän vuoksi puhuttaessa L2TP:stä puhutaan samalla myös usein IPSec:istä joka hoitaa tunnelin läpi kulkevan liikenteen salaamisen. [16.]

Kuinka L2TP-protokolla ja IPSec toimivat keskenään VPN-yhteyden muodostamiseksi? Ensiksi IPSec aloittaa keskustelun sopiakseen yhteyden muodostamiseksi käytettävät salausattribuutit käyttämällä hyödyksi IKE:ä ja UDP-porttia 500. Yhteyden muodostamisen jälkeen ESP-prosessi muodostetaan tiedonsiirron mahdollistamiseksi käyttämällä IP-protokollaa ja porttia 50. Kun ESP-prosessi on valmis kahden eri verkkoympäristön välillä, jotka tässä tapauksessa olisivat päätelaitteen verkkoympäristö ja päätelaitteelle asennettu VPN-asiakasohjelma sekä yrityksen verkkoympäristössä sijaitseva VPN-palvelin, voidaan juuri luotua turvattua kanavaa hyödyntää tunnelin muodostamiseksi. IPSecin osuus on tämän jälkeen hoidettu ja yhteyden muodostamisen lopusta vastaa L2TP. L2TP neuvottelee käytettävästä protokollasta ja tunnelin muodostamisesta käyttämällä TCP porttia 1701 ja IPSecin pystyttämää salattua kanavaa. [16.]

L2TP on varteenotettava vaihtoehto opinnäytetyötä varten, muttei niistä kuitenkaan paras. Vaikka L2TP on monella saralla edeltäjäänsä PPTP:tä parempi vaihtoehto, kuten IPSecin mahdollistama 256-bittinen salaus ja käyttöönoton helppous Windows- ja macOS-pohjaisilla päätelaitteilla, tuo L2TP mukanaan myös omat ongelmansa. L2TP/IPSecin tuplakapselointi on tietoturvallinen, mutta vaatii päätelaitteelta hieman tavallista enemmän suorittimelta ja verkkoyhteyden nopeudelta saumattoman toimivuuden takaamiseksi. L2TP-yhteys voidaan myös blokata NAT:ia hyödyntävissä palomuuriratkaisuissa, vaikkakin tämän ongelman kiertämiseksi on olemassa konfigurointikeinoja. L2TP- ja PPTP-tunnelointiprotokollan väliltä L2TP on lähes aina PPTP:tä parempi vaihtoehto. Luvussa 3.3 siirrytään tarkastelemaan IKEv2-teknologiaa, joka päihittää vertaillussa molemmat aikaisemmin läpi käydyt tunnelointiprotokollat.

3.3 IKEv2

IKEv2 on yhdessä Microsoftin ja Ciscon kehittämä protokolla, joka on rakennettu IPSec-protokollan pohjalta, ja se on julkaistu vuonna 2005 [17]. Lähempää tutkittuna IKEv2 ei ole tunnelointiprotokolla, vaan pikemminkin salausprotokolla. IKEv2 kuitenkin käyttäytyy toiminnaltaan tunnelointiprotokollan tavoin ja on laajalti käytetty tunneloimiseen, jonka vuoksi IKEv2 ansaitsee paikan vertailulistalta ja on vahva haastaja muihin tunnelointiprotokolliin verrattuna. Sen vahvoja ominaisuuksia haastajana on korkea yhteysnopeus, vahvan salauksen saavuttaminen AES-

lohkosalausmenetelmää käyttämällä sekä MOBIKE:n hyödyntämisen mahdollisuus. MOBIKE tekee mahdolliseksi VPN-yhteyden ylläpitämisen ilman katkoja, vaikka verkkoympäristö muuttuu päätelaitteella, esimerkiksi siirryttäessä WiFi-verkosta käyttämään puhelimen omaa dataverkkoa. MOBIKE tekee IKEv2:sta houkuttelevan vaihtoehdon etenkin mobiililaitekäytössä. [18.]

Kuten muidenkin tunnelointiprotokollien tapauksessa, IKEv2 on vastuussa salatun tunnelin muodostamisesta päätelaitteen ja kohdepalvelimen välillä. Ensiksi yhteyden muodostamisessa autentikoidaan käyttäjän ja palvelimen välinen yhteys, jonka jälkeen laitteet sopivat käytettävästä salausattribuutista. IKEv2 protokolla käyttää liikennöimiseen UDP-paketteja ja UDP-porttia 500. [18.]

Vaikka IKEv2 pääsee hyviin nopeuksiin raskaasta salauksesta huolimatta, ei tunnelointiprotokolla välttämättä ole vaihtoehdoista paras mahdollinen. Tunnelin ylläpitäminen verkkoympäristöjen vaihtuessa on mukava lisäominaisuus, mutta se ei saa protokollavertailua kallistumaan IKEv2 eduksi. Lähdekoodi ei ole täysin avoin kaikille, joten takaportin mahdollisuus on aina olemassa. Myös liikennöimiseen käytetty UDP-portti 500 voi monessa tapauksessa olla torjuttu käytössä olevan palomuurin toimesta, mikä rajoittaa VPN-yhteyden muodostamisen mahdottomaksi. [18.] Luvun 3.4 sisältämä tunnelointiprotokolla SSTP tulee tarjoamaan ratkaisun ainakin muutamaan edelliseen ongelmaan.

3.4 SSTP

SSTP on lyhenne englanninkielisistä sanoista Secure Socket Tunneling Protocol ja se on Microsoftin kehittämä tunnelointiprotokolla, joka julkaistiin vuonna 2007. Protokollan avulla voidaan lähettää OSI-mallin toisen kerroksen paketteja käyttämällä HTTPS-yhteyttä. [19] PPTP-protokollan tapaan SSTP lähettää PPP-liikennettä, mutta suojaa sen käyttämällä hyväksi SSL/TLS-kanavaa. Tämän suojausmekaniikan vuoksi SSTP on PPTP:tä parempi vaihtoehto, sillä SSL/TLS vastaa liikenteen salauksesta, salausavaimen neuvottelusta sekä datan muuttumattomuudesta lähetyksen aikana. SSTP luo monen tunnelointiprotokollan tavoin turvallisen yhteyden VPN-asiakaskoneen ja -palvelimen välille, jonka läpi kulkeva liikenne on salattu. [20.]

SSTP tarjoaa monia teknisiä etuja, jotka tekevät siitä mielenkiintoisen vaihtoehdon opinnäytetyön toteuttamiseksi. Eniten positiivista huomiota herättää SSTP:n liikennöimiseen käytettävä portti

443. Liikenne on TCP-liikennettä ja 443-portti on HTTPS-liikenteelle tyypillinen portti, jota ei monissa palomuuriratkaisuissa tulla erikseen estämään. Vakioportti 443 tekee SSTP:stä otollisen ehdokkaan varsinkin silloin, kun asiakaskoneen verkkoympäristö vaihtuu toistuvasti ja tarvitaan keino päästä käsiksi työpaikan verkkoympäristöön. TCP-liikenne vaatii kuitenkin päätelaitteen verkkoyhteydeltä hieman UDP-yhteyttä enemmän. [20.]

SSTP tulee olemaan tämän listan toiseksi paras vaihtoehto, jonka ero ykkösvalintaan ei jää paljosta kiinni. HTTPS-liikenne 443-portin yli kiertää monet palomuurille asetetut estot ja suurin ero ensimmäisen ja toisen sijan välillä tuleekin löytymään kehityspäästä. Microsoft on kehittänyt SSTP:n yksin, eikä lähdekoodi ole täysin avoin. SSTP tukee myös pelkästään TCP-pohjaisia yhteyksiä, joka hidastaa yhteysnopeutta verrattuna UDP-pohjaiseen yhteyteen. [20.] Luvussa 3.5 esitellään lopullinen vaihtoehto, joka ottaa viimeisetkin protokollapuutteet huomioon.

3.5 OpenVPN

Viimeisenä tarkasteluun nostetaan OpenVPN, joka on yksi laajalti käytetyimmistä tunnelointiprotokollista. OpenVPN julkaistiin keväällä vuonna 2001, ja sitä on jatkuvasti kehitetty ja ylläpidetty tähän päivään saakka. OpenVPN on alun perin James Yonanin luoma tunnelointiprotokolla, jonka lähdekoodi on kaikille avoin. [21.]

Lähdekoodin avoimuutta tunnelointiprotokollissa ei voida ottaa itsestäänselvyytenä ja se toimii hyvin tunnelointiprotokollan eduksi haastajiinsa nähden. Kaikilla on mahdollisuus tarkistaa lähdekoodista mitä sovellus tekee ja miten, mikä vahvistaa turvallisuuden tunnetta. Vasta-argumentiksi voidaan puolestaan nostaa avoimesta lähdekoodista mahdolliset tietoturva-aukot. Viimeisin ulkopuolisen toimittama tietoturvatarkastus suoritettiin vuosien 2016-2017 aikana kryptografi Matthew D. Greenin toimesta. Tarkistuksessa nousi esiin kaksi pientä ongelmaa, jotka eivät kuitenkaan vaarantaneet käyttäjädataa. Esiin nousseet ongelmat korjattiin nopeasti seuraavan päivityksen mukana. Kryptografi Green kuvailee yleisesti OpenVPN-tunnelointiprotokollaa salauksen puolesta vankaksi. [22] Internet tarjoaa myös kattavan listan keinoista, joilla OpenVPN-pohjaisia VPN-yhteyksiä voidaan vielä salauksen puolesta parantaa.

OpenVPN:n läpi kulkeva liikenne on SSTP:n tavoin HTTPS-liikennettä. Liikenteen tyyppi mahdollistaa vahvan SSL 3.0-salausstandardin hyödyntämisen liikenteen suojaamiseksi ja salausavaimet voivat olla pituudeltaan 256-bittisiä. HTTPS-liikenteelle tyypilliseen tapaan OpenVPN liikennöi datan kulkemaan vakiona 443-porttia pitkin, mikä tarjoaa hyvät mahdollisuudet VPN-yhteyden

muodostamiseksi tavallista vahvemminkin suojatun palomuuriverkon takaa. OpenVPN tukee myös molempia UDP- ja TCP-protokollia, jonka vuoksi on mahdollista valita nopeamman tai varmemman verkkoyhteyden väliltä käyttötarpeiden mukaan. [21.]

Protokollassa on myös pieniä haittapuolia, jotka ovat mainitsemisen arvoisia. Suurin osa edellisissä kappaleissa läpi käydyistä protokollista on integroitu siten, että ne ovat Windows-pohjaisilla käyttöjärjestelmillä helposti käyttöönotettavissa. OpenVPN-pohjaisen VPN-yhteyden luomiseksi joudutaan lataamaan kolmannen osapuolen sovellus, joka tulee tämän opinnäytetyön tapauksessa olemaan Pritunl niminen sovellus. Vahva salaus tuo myös mukanaan suuremman rasituksen verkkoyhteydelle, jonka vuoksi yhteyden nopeus voi kärsiä. Nopeusongelmien ehkäisemiseksi opinnäytetyössä valitaan verkkoyhteydelle kevyempi, UDP-protokolla. UDP-protokollaa käyttämällä pyritään välttämään hitaiden yhteyksien syntyminen. [21.]

3.6 Yhteenveto

Vertailussa voidaan todeta OpenVPN-protokollan täyttävän eniten haluttuja ominaisuuksia etsittäessä kaikkein vikasietoisinta vaihtoehtoa vertailukohteiden väliltä. OpenVPN jää jälkeen muista protokollista ainoastaan nopeudessa, mikä johtuu pitkälti OpenVPN:n käyttämästä salausmekaanikasta ja sen raskaudesta. Tätä voidaan kuitenkin tasapainottaa valitsemalla UDP-protokolla TCP-protokollan sijaan. Käytettäessä TCP-protokollaa jokaisen lähetetyn datapaketin jälkeen varmistetaan paketin saapuminen perille, joka kuormittaa internetyhteyttä. UDP-protokollaa käytettäessä tätä varmistusta ei tapahdu. Taulukossa 1 nähdään vielä visuaalisesti vertailun tulokset.

Nimi	Nopeus	HTTPS	443-Portti	Salaus	UDP	Avoin lähdekoodi
PPTP	Hyvä	Ei	Ei	Huono	Ei	Ei
L2TP/IPSec	Keskiverto	Ei	Ei	Hyvä	Kyllä	Ei
IKEv2	Hyvä	Ei	Ei	Hyvä	Kyllä	Ei
SSTP	Keskiverto	Kyllä	Kyllä	Hyvä	Ei	Ei
OpenVPN	Keskiverto	Kyllä	Kyllä	Hyvä	Kyllä	Kyllä

Taulukko 1. Vertailu eri VPN-protokollien välillä.

Ennen siirtymistä lukuun 4 on tarpeellista mainita WireGuard-niminen VPN-protokolla. WireGuard on jätetty vertailulistan ulkopuolelle ainoastaan siksi, koska se on suhteellisen uusi ja vielä kovan päivitystahdin alla. Ensimmäinen versio WireGuardista julkaistiin vuonna 2018, ja se on ominaisuuksiltaan täysin vertailukelpoinen OpenVPN:n kanssa, tarjoten vielä nopeamman yhteyden verrattuna OpenVPN:ään poikkeavan salausmekaniikan vuoksi. [23.] Tulevaisuudessa WireGuard tulee olemaan erittäin varteenotettava vaihtoehto laajalti käytettäväksi VPN-protokollaksi, mutta opinnäytetyön kirjoitushetkellä vertailukohteiksi on valittu jo laajalti käytössä olevia VPN-protokollia.

4 Pritunl

Pritunl on vapaaseen lähdekoodiin pohjautuva VPN-sovellus, joka koostuu asiakaskoneelle asennettavasta asiakasohjelmasta ja VPN-palvelimelle asennettavasta palvelinohjelmasta. VPN-palvelimen hallinnointi tapahtuu verkon yli tapahtuvan hallinnointipaneelin kautta. Hallinnointi verkon kautta mahdollistaa käyttäjälle suoraviivaisen tavan hyödyntää OpenVPN-protokollaa, joka on vapaan lähdekoodin VPN-palvelimissa laajalti käytössä oleva protokolla. Pritunl erottuu muista haastajistaan parhaiten siten, että suurin osa käyttäjien ja palvelimien konfiguroinnista tapahtuu verkon hallintapaneelin kautta, jonka vuoksi asetusten konfigurointi on sujuvaa.

VPN-yhteyden autentikointiin voidaan käyttää monia tapoja yhteyden muodostamiseksi. OpenVPN tarjoaa autentikointiin valmiiksi palvelimelle ja asiakkaalle annettuja avaimia, sertifikaattipohjaisia kirjautumismenetelmiä sekä käyttäjätunnuksesta ja salasanasta koostuvaa autentikointimenetelmää. [24] OpenVPN:n tarjoamien vaihtoehtojen väliltä voidaan valita tapauskohtaisesti itselle toimivin vaihtoehto.

Verkotuksessa OpenVPN tukee UDP- ja TCP-protokollia. Vaikka TCP-protokollapohjaisen liikenteen käyttäminen on mahdollista, on datapakettien lähettäminen UDP-protokollaa käyttämällä suotavampaa. TCP-protokollan suurin hyöty on datapakettien perille pääsyn varmentamisessa, mutta protokolla vaatii nopean verkkoyhteyden toimiakseen ilman nopeusongelmia. OpenVPN tukee IPv6-protokollaa liikenteen tunneloimiseksi ja tunneloitava liikenne on yhteistyökykyinen, vaikka palomuuriin on määritelty käyttöön NAT, jonka avulla muutetaan asiakaskoneelta lähtevien datapakettien IP-osoite valmiiksi määritellyn IP-osoitteen mukaiseksi. [24.]

4.1 Pritunlin salaus

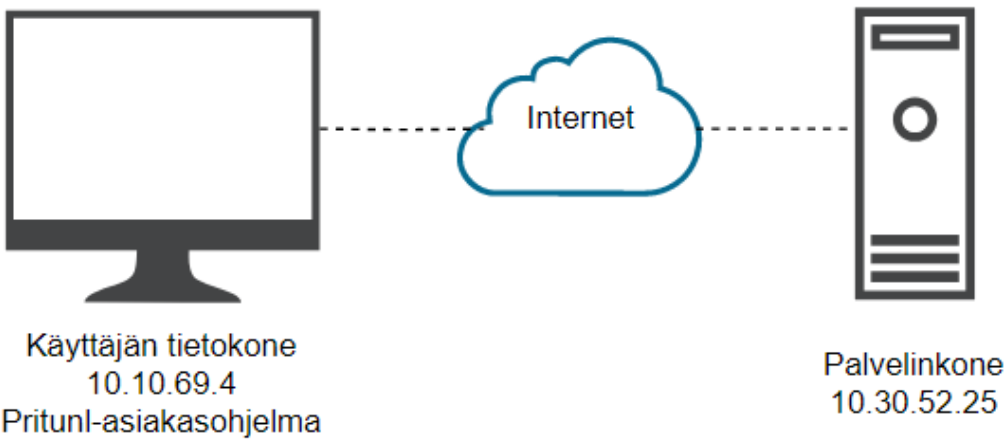
OpenVPN on kompleksi kokonaisuus, joka hyödyntää monia eri salausmenetelmiä turvallisen yhteyden muodostamiseksi. Kokonaisuuden ymmärrettävyyden parantamiseksi onkin syytä käydä tarkemmin läpi liikenteen salaamiseksi käytettävää teknistä kokonaisuutta. OpenVPN käyttää liikenteen salaamiseksi mukautettua mallia yhdistämällä SSL- ja TLS-salaukset keskenään. SSL- ja TLS- salausprotokollilla voidaan hyödyntää julkisen avaimen käyttöä ja salata HTTPS-protokollaa käyttävä liikenne.

Avainparin luomiseen käytetään avuksi OpenSSL-kirjastoa, joka tarjoaa myös työkalut sertifikaattien käyttöä varten. Sertifikaattien hyödyntäminen tapahtuu OSI-mallin kolmostasolla ja käyttää vakiona 443 porttia. HTTPS-liikenne eroaa HTTP-liikenteestä siten, että HTTP-liikenteessä teksti kuljetetaan salaamattomana ilmitekstinä. [25.]

Edellä mainittujen salausmekanismien lisäksi OpenVPN-protokollapohjainen VPN-palvelin toimii myös välityspalvelimen roolissa. Asiakaskoneelta lähtevien datapakettien kapseloinnin ja suojaamisen jälkeen OpenVPN ohjaa lähtevän liikenteen käyttäjän valitseman välityspalvelimen kautta. Välityspalvelimen NAT hoitaa lähteville datapaketeille välityspalvelimelle määritellyn IP-osoitteen, jonka vuoksi julkiverkkoon lähteneet datapaketit kulkevat eri IP-osoitteella, millä ne ovat alun perin kohdelaitteelta lähteneet. Vastaanotettu data puolestaan käy läpi tismalleen saman prosessin, mutta päinvastaisessa järjestyksessä kuin lähetettäessä. [26.]

4.2 Asennuksen esivalmistelut

Projektin asennukset voidaan jaotella kahteen osioon: virtuaalikoneen asennukseen ja käyttöönottoon sekä Pritunl-palvelimen asennukseen ja käyttöönottoon. Asennusluvuissa esitellään ja käydään läpi, mitä valintoja projektin käytännön osiossa on toteutettu ja luku koostuu pitkälti asennuksen aikana heränneistä huomioista. Kuvasta 1 ilmenee käytettävät IP-osoitteet, jotka sijaitsevat datacenter-opiskelijoille käytössä olevassa VMware-virtualisointiympäristön ensimmäisessä ja kolmannessa virtuaaliverkossa.



Kuva 1. Arkkitehtuurikuva toteutettavasta ympäristöstä

4.3 Virtuaalikoneen asennus ja konfigurointi

Projektin teknisessä osuudessa ensimmäinen asia on virtuaalikoneen luominen. Valittu virtuaalikone on Linux-pohjainen CentOS 8 käyttöjärjestelmällä varustettu kone. Koneella on käytössä yksi ydin (1 CPU), yksi gigabitti muistia ja 12 gigabittia kovalevytilaa. Koneelle ei ole tarkoitus asentaa mitään muuta kuin Pritunl-palvelimelle välttämättömät asennukset. Virtuaalikone sijaitsee Kajaanin ammattikorkeakoulun datacenter-opiskelijoille käytössä olevassa VMware-virtualisointiympäristössä.

Virtuaalikoneen luonnin yhteydessä määritetään koneelle perusasetukset kuntoon. Perusasetuksiin kuuluu käytettävän näppäimistön kielen valinta, päivämääräasetukset, verkkoasetukset, kiintolevyasema ja mihin käyttöön virtuaalikonetta ollaan luomassa. Tätä projektia varten virtuaalikone määritetään palvelimen rooliin.

Koneen asetusten asettamisen jälkeen koneelle annetaan myös root-käyttäjän salasana sekä luodaan uusi ”saku”-niminen käyttäjä tietoturvallisuuden parantamiseksi, jotta sisäänkirjautuminen ei ole mahdollista täydet oikeudet omaavalla root-käyttäjällä. [27.]

Virtuaalikoneen asennuksen jälkeen varmistetaan vielä haluttujen asetusten, kuten IP-osoitteiden konfiguroinnin ja käyttäjäasetusten olevan kunnossa Pritunl-palvelun käyttöönottoa varten, jonka jälkeen ajetaan ohjelmistopäivitykset. Tämän jälkeen siirrytään asentamaan Pritunl-palvelin juuri luodulle virtuaalikoneelle.

4.4 Pritunl-palvelimen asennus

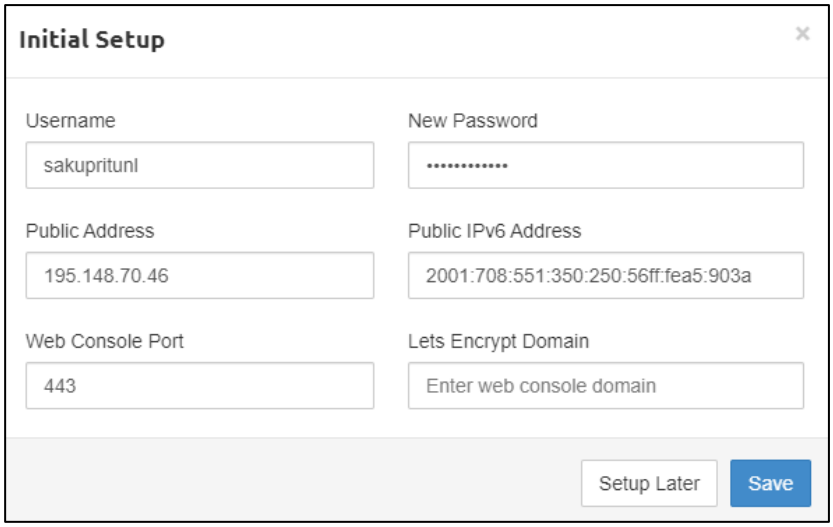
Pritunl-palvelimen asentamisvaiheesta löytyy valmistajan sivuilta suoraviivaiset ja kattavat ohjeet, joita hyödyntämällä asennus sujuu suoraviivaisesti [28]. Dokumentin CentOS 8 -kohdasta voidaan kopioida ja liittää tarvittavat komennot miltei sellaisenaan. Ainoa käsin muutettava kohta löytyy yleisen avaimen hakemisessa, jossa joudutaan osoitteen perään antamaan portti, mitä pitkin avain haetaan. Tässä projektissa portti on vakio http-portti, eli 80. Muokattu linja näyttää siis tältä:

```
gpg --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 7568D9BB55FF9E5287D586017AE645C0CF8E292A
```

Virtuaalikoneelle ladataan ja asennetaan Pritunl-palvelimen ominaisuudet, jonka jälkeen palvelin on käyttövalmiissa kunnossa. Virtuaalikoneeseen ei tarvitse enää ottaa SSH-yhteyttä, sillä Pritunl-

palvelimen konfigurointi voidaan suorittaa nettiselaimen kautta antamalla virtuaalikoneen IP-osoite.

Kuvassa 2 esitellään Pritunl asetukset ensimmäisen kirjautumiskerran jälkeen. Ensimmäisen sisäänkirjautumiseen vaadittavat tiedot saadaan syöttämällä terminaaliin komento ”sudo pritunl default-password”, jonka jälkeen seuraava kuva avautuu.



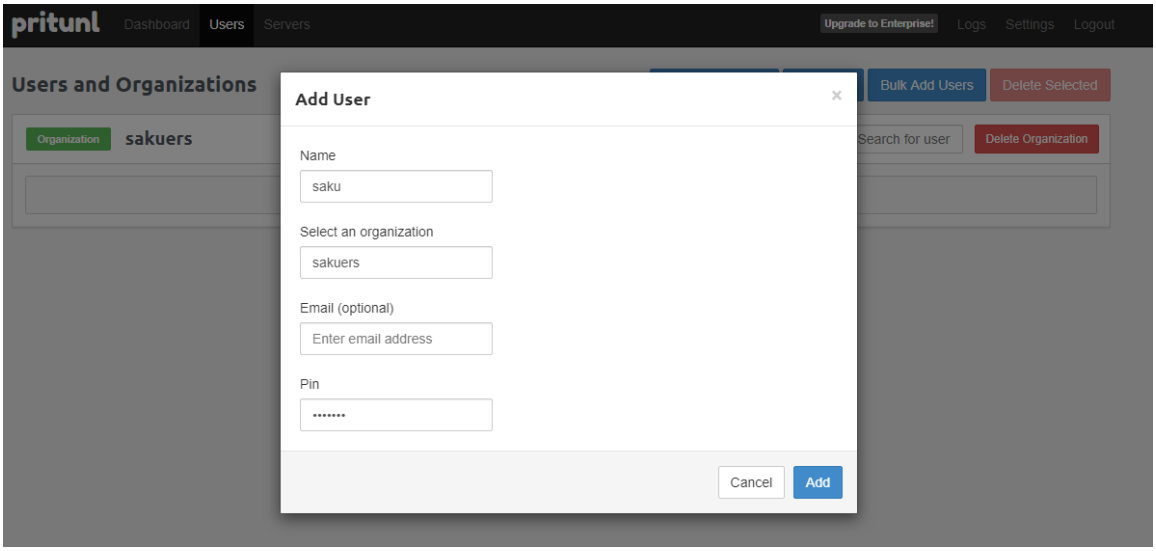
Kuva 2. Ensimmäisen sisäänkirjautumisen jälkeinen asetusten konfigurointi.

4.5 Palvelimen sisäinen konfigurointi

Palvelinta päästään hallinnoimaan verkkoliittymän yli. Seuraavaksi palvelimen asetuksia tullaan muokkaamaan siten, että mahdollistetaan yhteyden luominen asiakkaan ja palvelimen välille. Asetusten säätäminen koostuu kolmesta vaiheesta: organisaation ja käyttäjien luomisesta sekä uuden palvelimen lisäämisestä.

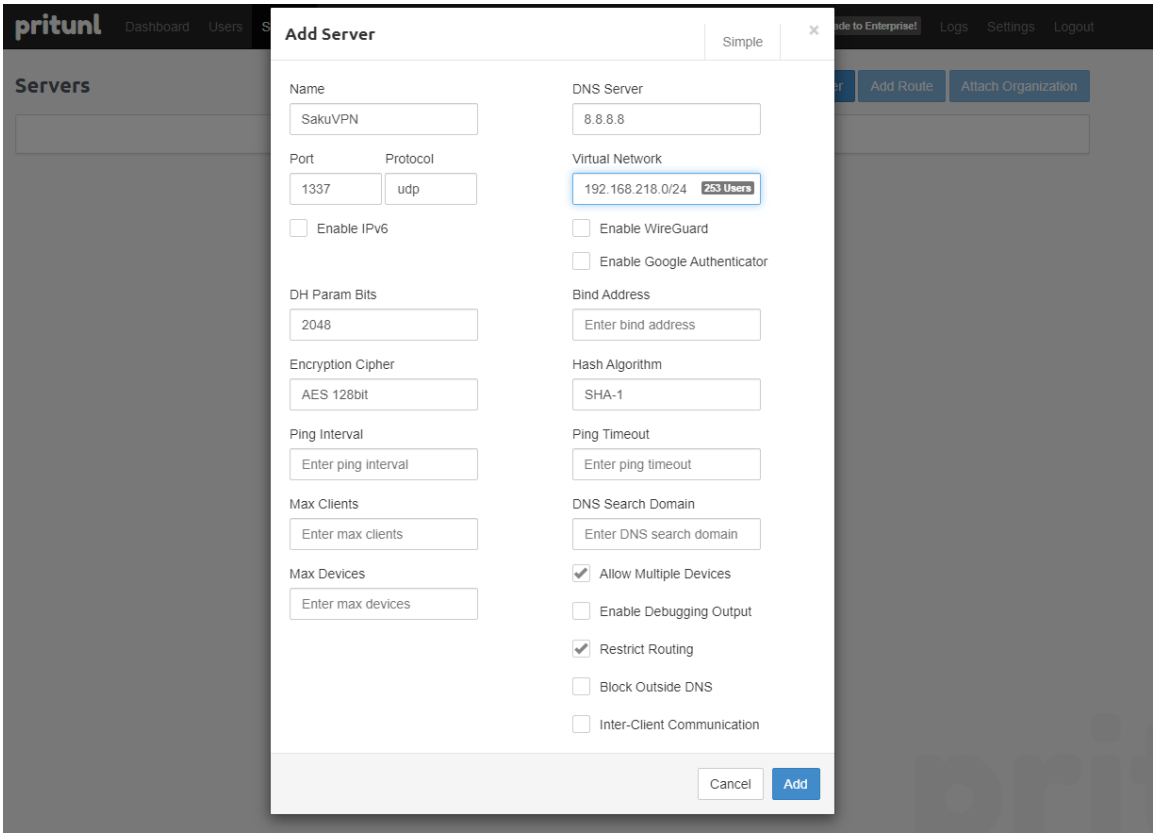
Ensimmäiseksi luodaan uusi organisaatio. Tämä onnistuu helposti navigoimalla ensiksi ”Users” välilehdelle ja valitsemalla oikealta ylhäältä ”Add Organization.” Organisaation nimeksi luomisvaiheessa annetaan nimi ”Sakuers.”

Organisaation ollessa valmis voidaan siihen määrittää käyttäjiä. Kuvassa 3 nähdään, miten luodulle käyttäjälle määritetään nimi, organisaatioalue ja PIN-koodi. PIN-koodi toimii salasanana yhteyden muodostamisessa asiakkaan tietokoneen ja kohdepalvelimen välillä.



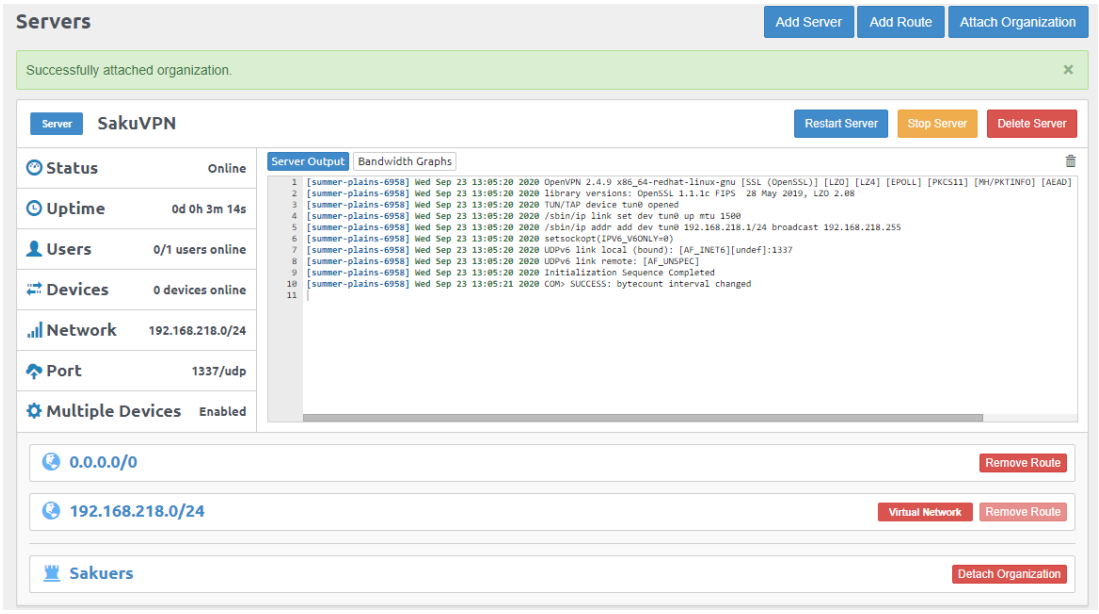
Kuva 3. Käyttäjän luonti ja liittäminen organisaatioon.

Viimeiseksi jäljellä on palvelimen luonti, johon juuri tehty käyttäjä ottaa asiakaskoneelta yhteyden. Palvelimelle annetaan nimi, määritellään portti, jonka kautta verkkoliikenne kulkee ja annetaan oikeudet käyttäjille yhdistää monella eri laitteella käyttäen yhtä tunnusta samanaikaisesti. Tämän lisäksi estetään samassa virtuaaliverkossa olevia laitteita näkemästä tai kommunikoimasta keskenään tietoturvasyistä. Kuvassa 4 nähdään palvelimelle asetetut parametrit. Palvelimen luonnin jälkeen lisätään juuri luotu ”SakuVPN”-palvelin osaksi ”Sakuers”-organisaatiota.



Kuva 4. Palvelimen luontiin käytetyt parametrit.

Viimeiseksi vielä käynnistetään palvelin painamalla ”Start Server”, jonka jälkeen palvelin on onnistuneesti käynnissä ja on aika siirtyä testaamaan. Kuvassa 5 hahmottuu ylläpitäjälle aukeava näkymä, josta voidaan kattavasti seurata palvelimen tapahtumia ja säätää tarvittaessa asetuksia.



Kuva 5. Asennuksen jälkeinen hallintanäkymä.

4.6 Testaus

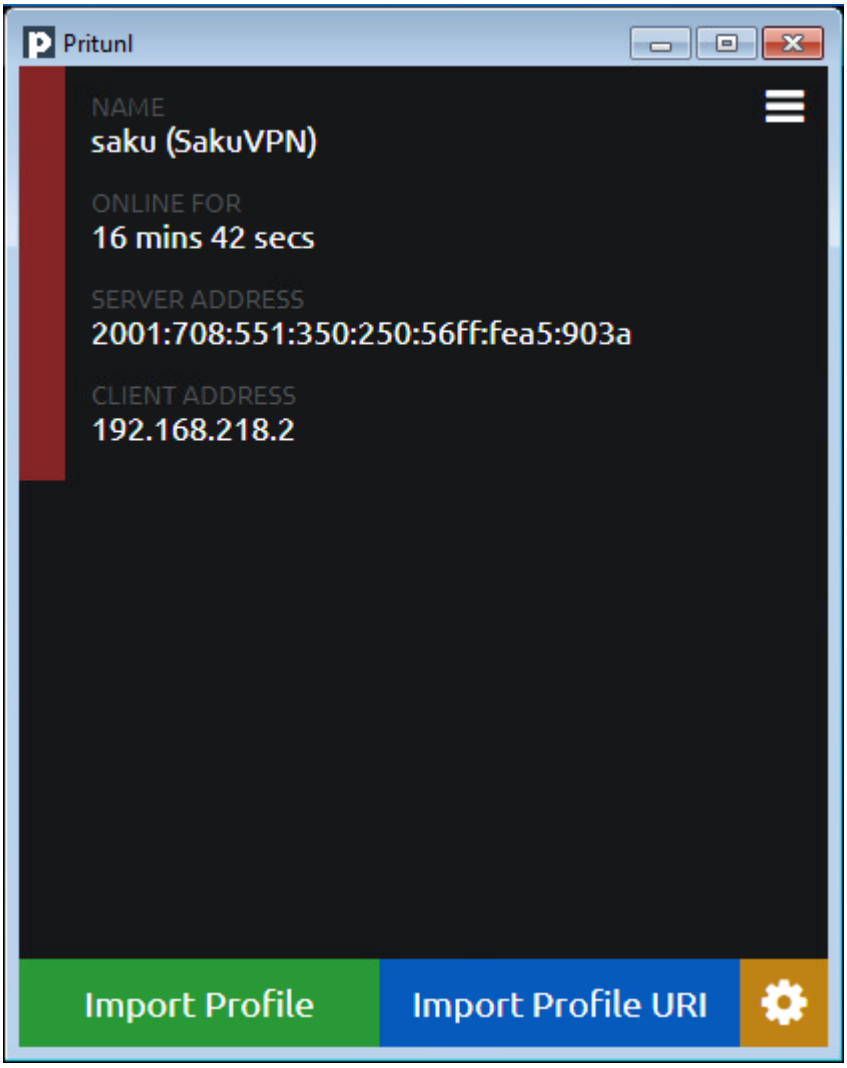
Viimeiseksi vuorossa on ympäristön testaus. Tätä varten luodaan uusi virtuaalikone, joka toimii asiakkaan roolissa testaustilanteessa. Asiakaskone ottaa yhteyden palvelinkoneeseen, jonka jälkeen yhteyden tiedot tulevat näkymään asiakkaan Pritunl-sovelluksessa, jos kaikki sujuu suunnitelman mukaan.

Aluksi luodaan uusi virtuaalikone, joka on datacenter-opiskelijoille käytössä olevaan VMware-virtualisointiympäristöön asennettu Windows 7 Enterprise -versiolla varustettu virtuaalikone. Sille on annettu käyttöön yhden gigabitin suoritinyksikkö, kaksi gigabittiä muistia ja kolmekymmentä gigabittiä tallennustilaa.

Vaikka asiakaskone ja palvelinkone sijaitsevat fyysisesti saman infrastruktuurin alaisuudessa, voidaan koneille silti määrittää IP-osoitteet kahdesta eri virtuaaliverkon IP-osoiteavaruudesta. Palvelinkoneelle annettu IP-osoite kuuluu kolmannen virtuaaliverkon osoitelistaan, kun taas puolestaan asiakaskoneelle annetaan IP-osoite ensimmäisen virtuaaliverkon osoitelistasta. Eri virtuaaliverkosta lähtevällä liikenteellä kuuluisi olla eriävät julkiset IP-osoitteet, jolloin niitä tarkastelemalla ja vertaamalla voidaan varmentaa VPN-yhteyden toimivuus. Toteutettavassa ympäristössä ei kuitenkaan edellä mainittua tarkastelua suoriteta, sillä palvelua ei olla ottamassa täysipäiväiseen käyttöön, jonka vuoksi sitä ei viedä julkiverkkoon virtuaaliympäristön tietoturvan takaamiseksi.

Asiakaskoneella haettiin ja asennettiin Pritunlin valmistajan sivuilta asiakaskoneille suunniteltu sovellus, jonka avulla muodostetaan yhteys palvelinkoneeseen. Asiakaskoneelle joudutaan myös tuomaan Pritunl-palvelimen verkkoliittymän kautta asiakaskoneelle .tar-tiedosto, joka sisältää kaikki oleelliset tiedot yhteyden luomista varten. Kun .tar-tiedosto on asiakaskoneella, aukaistaan Pritunl asiakaskoneella ja kuljetetaan .tar-tiedosto Pritunl-sovellusikkunan päälle.

Nyt kaikki tarvittavat tiedot löytyvät asiakaskoneen Pritunl-sovelluksesta ja sovellukseen tulee näkyviin halutun käyttäjän käyttäjätiedot. Valitaan ylänurkasta asetukset ja painetaan kohdasta ”Connect.” Tämän jälkeen Pritunl kysyy vielä aiemmin määriteltyä PIN-koodia, jonka jälkeen yhteys muodostuu asiakaskoneen ja palvelinkoneen välille kuvan 6 mukaisesti.



Kuva 6. Asiakkaan Pritunl-näkymä onnistuneen yhteydenluonnin jälkeen.

5 Yhteenveto

Opinnäytetyön tarkoituksena oli parantaa ymmärrystä virtuaaliverkkoihin, tutustua yksityisen virtuaaliverkon tarjoamiin etuihin, testiympäristön luomiseen sekä sovelluksen testaamiseen.

Kokonaisuus siitä, mitä kaikkea yksityinen virtuaaliverkko tarjoaa ja mitä konepellin alla käytännön tasolla tapahtuu, kasvoi projektin aikana huomattavasti. Olin kuullut paljon puhetta yksityisistä virtuaaliverkoista jo ennen projektin alkua, mutta varsinkin käytännön osuus vahvisti asiantuntevuutta.

Tekninen toteutus sujui suoraviivaisesti ja alkuperäinen tavoite saavutettiin. Aiheen laajuus poikkeaa kuitenkin siitä, mitä kaikkea ajattelin projektiin aluksi sisällyttää. Alun perin tarkoituksena oli myös vertailla oman virtuaaliverkon hintaa kaupallisiin tuotteisiin ja kirjoittaa teknistä infoa lisää Pritunlista, mutta projektin edetessä nämä ajatukset hiljalleen hautautuivat.

Opinnäytetyön edetessä myös kirjoitukselliset asiat vahvistuivat. Mitä pidemmälle työ eteni, sitä rutiinimaisemmalta myös kirjoitukselliset muodollisuudet alkoivat tuntumaan. Tästä parhaimpana esimerkkinä on lähdeviittauksien merkintä. Projektin alussa merkitsemiseen uppoutui tuhottomasti aikaa. Lopussa lähdeviittauksien merkitsemistä ei puolestaan tarvinnut sen suuremmin miettiä, vaan se tuntui luonnolliselta osalta dokumentointia.

Käytännön osuudessa olisi myös ollut mahdollista viedä VPN-palvelin julkiverkkoon ja tutkia sovelluksen käyttäytymistä siten. Palvelun julkiverkkoon vienti vaikutti kuitenkin teoriatasolla todella samalta kuin testiympäristössä toteutettu ympäristö, jonka vuoksi jätin tämän toteuttamatta. Mikäli palvelu olisi mennyt jokapäiväiseen käyttöön, voisi tilanne olla erilainen. Olen kuitenkin pääosin tyytyväinen opinnäytetyön aikana saavutettuihin tuloksiin.

Lähteet

[1] Transkripti teknologiaguru Gary Kovacsin antamasta puheesta TED2012-konfferenssissa. Viitattu 14.03.2021 http://tinyurl.com/czzwvvc4

[2] Amerikkalaisen verkkolehtijätin The Guardianin uutinen, jossa käsitellään Facebookin keräämän datan hyödyntämistä presidentinvaaleissa. Viitattu 27.10.2020 https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

[3] Psykoterapiakeskus Vastaamoon kohdistuneen tietomurron pohjalta luotu, Helsingin Sanomien julkaisema uutinen. Viitattu 27.10.2020 https://www.hs.fi/kotimaa/art-2000006699117.html

[4] OpenVPN -yhteisön viralliset foorumisivut, joilla kerrotaan yksityisen virtuaaliverkon ominaisuuksista. Viitattu 30.09.2020 https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn

[5] Norton on maailmalla laajasti tunnettu palomuuripalveluistaan ja on julkaissut artikkelin kotisivuillaan mitä ja miksi VPN kannattaa hommata. Viitattu 08.10.2020 https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

[6] Artikkeli siitä, miten pieni yritys voi hyötyä VPN-palvelimesta. Viitattu 27.02.2021 https://www.europeanbusinessreview.com/5-ways-your-small-business-can-benefit-from-a-vpn/

[7] VPN:n toiminnasta kertova artikkeli. Viitattu 27.02.2021 https://computer.howstuffworks.com/vpn.htm#:~:text=Most%20VPNs%20rely%20on%20tunneling,that%20reaches%20across%20the%20internet.&text=That%20outer%20packet%20protects%20the,of%20packets%20is%20called%20encapsulation.

[8] Ciscon kuvailu PPP protokollasta ja mistä osista protokolla koostuu. Viitattu 27.01.2021. https://www.cisco.com/c/en/us/tech/wan/point-to-point-protocol-ppp/index.html

[9] Verkkoyhteysteknologiaa käsittelevä artikkeli. Viitattu 02.03.2021 https://www.sciencedirect.com/topics/computer-science/network-control-protocol

[10] Hotellin palomuurieston kiertämiseksi olevia neuvoja. Viitattu 10.03.2021 https://windowsreport.com/vpn-doesnt-work-hotel/

[11] Artikkeli, jossa käsitellään viittä yleisesti käytettyä tunnelointiprotokollaa. Viitattu 10.03.2021 https://www.netmotionsoftware.com/blog/connectivity/vpn-protocols

[12] Artikkeli, jossa käsitellään viittä yleisesti käytettyä tunnelointiprotokollaa. Viitattu 10.03.2021 https://www.technadu.com/vpn-protocols/8436/

[13] PPTP-protokollaa käsittelevä artikkeli. Viitattu 02.03.2021 https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-pptp/

[14] Artikkeli NSA:n VPN-liikenteen vakoilemisesta ja vakoilun hyödyntämiskohteista. Viitattu 01.02.2021 https://hacker10.com/internet-anonymity/secret-documents-show-the-nsa-is-spying-on-vpn-users/

[15] Internet Engineering Task Forcen vuonna 1999 julkaisema dokumentti, jossa käsitellään L2TP protokollaa. Viitattu 02.02.2021 https://tools.ietf.org/html/rfc2661

[16] L2TP-protokollaa käsittelevä artikkeli. Viitattu 02.03.2021 https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-l2tp/

[17] Internet Engineering Task Forcen vuonna 2005 julkaisema dokumentti, jossa käsitellään IKEv2 protokollaa. Viitattu 11.02.2021 https://tools.ietf.org/html/rfc4306

[18] IKEv2-protokollaa käsittelevä artikkeli. Viitattu 03.03.2021 https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-ikev2/

[19] Microsoftin vuonna 2020 julkaisema dokumentti, jossa käsitellään SSTP-protokollaa. Viitattu 17.02.2020 https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp/c50ed240-56f3-4309-8e0c-1644898f0ea8

[20] SSTP-protokollaa käsittelevä artikkeli. Viitattu 03.03.2021 https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-sstp/

[21] OpenVPN-protokollaa käsittelevä artikkeli. Viitattu 03.03.2021 https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-openvpn/

[22] Internet Engineering Task Forcen vuonna 2005 julkaisema dokumentti, jossa käsitellään IKEv2 protokollaa. Viitattu 11.02.2021 https://tools.ietf.org/html/rfc4306

[23] WireGuard-protokollaa käsittelevä artikkeli. Viitattu 04.03.2021 https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-wireguard/

[24] OpenVPN:n sivuilta löytyvä ohjekirja, jossa perehdytään tarkemmin OpenVPN:n protokolliin. Viitattu 22.10.2020 https://openvpn.net/community-resources/openvpn-protocol/

[25] OpenVPN:n yhteisösivuilta löytyvä tarkempi katsaus kryptografiaan. Viitattu 27.10.2020 https://openvpn.net/community-resources/openvpn-cryptographic-layer/

[26] OpenVPN:n yhteisösivulta löytyvät ohjeet VPN-palvelimen konfigurointiin. Viitattu 27.03.2021 https://openvpn.net/community-resources/how-to/#:~:text=OpenVPN%20is%20a%20full%2Dfeatured,group%2Dspecific%20access%20control%20policies

[27] Root – kirjautumisen estämiseen käytetyt ohjeet ja perustelut kyseiselle menettelylle. Viitattu 18.09.2020 https://www.howtogeek.com/howto/linux/security-tip-disable-root-ssh-login-on-linux/

[28] Valmistajan dokumentaatio, joiden mukaan Pritunl-palvelimen asennus on suoritettu. Listasta suorittu kohtaa CentOS 8. Viitattu 18.09.2020 https://docs.pritunl.com/docs/installation