Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2023

Antti Suuronen

Tor-välityspalvelinten asennus ja ylläpito

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikka

2023 | 49 sivua

Antti Suuronen

Tor-välityspalvelinten asennus ja ylläpito

Tor-ohjelmisto salaa ja reitittää tietoliikennettää Tor-verkoksi kutsutun, Tor-välityspalvelimista muodostuvan tietoverkon kautta. Tämä mahdollistaa esimerkiksi Internetin anonyymin käytön. Tor mahdollistaa pääsyn Internetiin myös tilanteissa, joissa esimerkiksi valtio pyrkii estämään sen erilaisilla teknisilla ratkaisuilla, kuten palomuureilla.

Opinnäytetyössä asennettiin ja konfiguroitiin kolme Tor-välityspalvelinta Tor Projectin laatimien ohjeiden ja suositusten mukaisesti. Palvelinten toimintaa seurattiin kuuden kuukauden ajan.Tarkoituksena oli laatia tarkka kuvaus palvelinten asennuksesta, konfiguroinnista ja ylläpidosta. Työssä arvioitiin myös palvelinten ylläpidosta aiheutuvia kustannuksia sekä mahdollista oikeudellista vastuuta.

Palvelinten toimintaa tarkkailtaessa kävi ilmi, että Tor Projectin suosituksissa ei ole huomioitu nopeiden tietoliikenneyhteyksien mahdollistamaa suurta reititettävän tietoliikenteen määrää. Tästä johtuen suosituksen mukainen RAM-muistin määrä osoittautui liian vähäiseksi. Tor Projectin ohjeet havaittiin osin ylimalkaisiksi sekä aloittelijalle sopimattomiksi.

Opinnäytetyössä ei käsitelty Tor-välityspalvelinten toiminnan optimointia tai pyritty löytämään sopivaa laitteistokokoonpanoa välityspalvelimelle. Työtä voisi jatkaa esimerkiksi selvittämällä sopivan RAM-muistin määrän erilaisille reititettävän tietoliikenteen määrille.

Asiasanat:

Tor-verkko, sipulireititys, palvelimet

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2023 | 49 pages

Antti Suuronen

The Installation and Configuration of Tor Relay Nodes

The focus of this thesis was in the process of installation and configuration of Tor Relay Nodes. Three separate Tor Relay Nodes were installed and configured, and the whole process was documented in detail. The aim was to document every step taken. Thus this thesis includes every steps taken, including the renting of the server equipment and domain names, the configuration of the Tor Server software and verifying the proper installation and monitoring of the running Tor Relay Nodes.

As this thesis is a detailed documentation of the process of installing and configuring the Tor Relay Nodes, it could serve as a practical source of information for the process described.

Keywords:

Tor Network, Onion Routing, Servers

Sisältö

Liitteet

Kuvat

Taulukot

Käytetyt lyhenteet

DNS	Domain Name System. Nimipalvelujärjestelmä.
PTR	Pointer Record. Liittää verkkotunnisteen verkko-osoitteeseen.
VPS	Virtual Private Server. Virtualisointitekniikalla tuotettu palvelin.
WHOIS	Kyselyprotokolla, jolla haetaan verkkotunnusrekisteritietoja.

1 Johdanto

Tor, (The Onion Router), on avoimen lähdekoodin ohjelmisto, joka mahdollistaa tietoliikenteen kerroksellisen salauksen ja reitittämisen siten, että käyttäjän sijainti, henkilöllisyys sekä itse tietoliikenteen sisältö on salattu. Tor-ohjelmisto mahdollistaa myös Internetin käytön tilanteissa, joissa käyttö olisi muutoin hankalaa tai mahdotonta. Tällainen tilanne syntyy esimerkiksi valtion pyrkiessä rajaamaan tai estämään Internetin käyttöä erilaisin teknisin ratkaisuin. Torin käytön mahdollistaa tuhansien Tor-välityspalvelinten muodostama maailmanlaajuinen verkko, jotka kutsutaan Tor-verkoksi. Näitä välityspalvelimia ylläpitävät erilaiset organisaatiot sekä yksityishenkilöt eri puolilla maailmaa. (Tor Project 2023a.)

Tässä opinnäytetyössä tarkastellaan Tor-välityspalvelimia niiden asennuksen ja ylläpidon kannalta. Kaikissa työvaiheissa on pyritty seuraamaan Tor Projectin tuottamaa ohjeistusta ja muuta dokumentaatiota mahdollisimman tarkasti. Eri työvaiheet kuvataan käytännönläheisesti ja yksityiskohtaisesti, jotta lukija voi tarvittaessa toistaa ne myös itse.

Opinnäytetyötä varten perustettiin kolme Tor-välityspalvelinta, joiden toimintaa ja ylläpitoa tarkasteltiin puolen vuoden ajan. Opinnäytetyössä tarkastellaan palvelinten perustamiseen liittyviä kysymyksiä, kuten laitteistolle asetettuja vaatimuksia, sopivien palveluntarjoajien löytämistä sekä tietysti myös erilaisia palvelinten ylläpidosta aiheutuvia kustannuksia. Sivuan myös kysymystä välityspalvelimen ylläpitäjän mahdollisesta rikosoikeudellisesta vastuusta tilanteissa, joissa hänen ylläpitämänsä palvelimen kautta on reitittynyt tietoliikennettä, joka liittyy esimerkiksi tietomurtoihin tai tietoliikenteen häirintään.

Työssä pyritään selvittämään myös se, miten hyvin Tor Projectin tuottama ohjeistus sekä suositukset laitteistokokoonpanojen osalta toimivat käytännössä, ja voiko niitä noudattaen saavuttaa hyvän lopputuloksen.

Rajaan käsiteltävien aiheiden ulkopuolelle niin kutsutut Tor-piilopalvelut, eli Tor-verkossa toimivat sivustot. En myöskään käsittele esimerkiksi Tor-verkkoon kuuluvia välitys- tai siltapalvelimia kuten Snowflakea.

Theseus-verkkosivustolta (2023) on tätä kirjoittaessa löydettävissä useita Tor-verkkoa käsitteleviä opinnäytetöitä, mutta niistä yksikään ei kuvaile Tor-välityspalvelinten asennusta tai ylläpitoa. Jo julkaistuissa opinnäytteissä kuvaillaan Tor-verkkoa yleensä tai Tor-verkon eri käyttötarkoituksia erikseen. Tämän opinnäytetyön aiherajaus ja lähestymistapa poikkeaa jo aiemmin julkaistuista opinnäytetöistä, ja näin ollen se osaltaan myös täydentää aihetta käsittelevien opinnäytteiden kokoelmaa.

2 Tor-verkosta

Tor-verkko koostuu noin 6 500 välityspalvelimesta (Tor Metrics 2023a). Nämä välityspalvelimet reitittävät TCP -tietoliikenneprotokollan mukaista verkkoliikennettä TLS -protokollan mukaisesti salattuna. Tor-sovellusta käytettäessä tietoliikenne reititetään vähintään kolmen välityspalvelimen kautta ennen sen reitittymistä kohdeosoitteeseensa. Tätä kolmen välityspalvelimen ryhmää kutsutaan piiriksi. Piirin sisällä välitettävä data myös salataan kolmella kerroksella, ja kukin välityspalvelin purkaa salauksesta yhden kerroksen. Tämän vuoksi tätä reititystekniikkaa kutsutaan sipulireititykseksi; sipulin rakenteen voi myös kuvata koostuvan useista kerroksista. (Platzer ym. 2021, 139-140.)

2.1 Solut

Dingledinen ym. (2019) mukaan Tor-verkon välityspalvelinten välinen liikenne reitittyy tietoliikennepakketteina, joita kutsutaan soluiksi. Soluja käytetään Tor-piirin muodostamiseen, säilyttämiseen sekä purkuun. Näiden reititykseen liittyvien toimintojen lisäksi soluja käytetään myös itse datan siirtoon.

Solun koko on aina 512 tavua. Solu voi olla tyypiltään joko kontrollisolu (engl. control cell) tai viestisolu (engl. relay cell) (Dingledine ym. 2019.)

Kontrollisolu

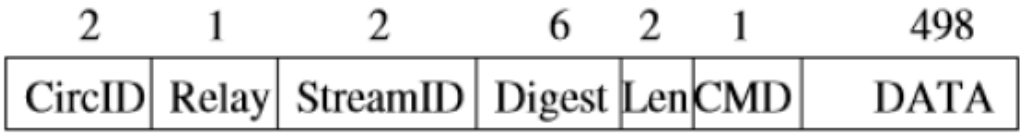
Kuvassa 1 esitetään kontrollisolun rakenne.

Kuva 1. Kontrollisolun rakenne (Dingledine ym. 2019)

Kentät 1 ja 2 kuvaavat otsaketta, DATA-kenttä on varattu hyötykuormalle. CircID-kenttä sisältää tiedon piiristä, johon solu kuuluu. CMD sisältää komennon, joka määrittelee välityspalvelimen toiminnan solun osalta. Solun sisältämän komennon mukaan piiri joko muodostetaan (CREATE), tuhotaan (DESTROY) tai säilytetään (PADDING). (Dingledine ym. 2019)

Viestisolu

Kuvassa 2 esitetään viestisolun rakenne.



Kuva 2. Viestisolun rakenne (Dingledine ym. 2019)

Tor-protokollanmäärityksen mukaisesta kontrollisolusta poiketen viestisolun otsake koostuu CircID- ja CMD-kenttien lisäksi StreamID, Digest ja Len -kentistä. Tämä johtuu siitä, että viestisoluja käytetään reitityksen lisäksi myös itse datan siirtoon. Data voi liittyä esimerkiksi verkkoselaimen muodostamaan liikenteeseen.

Relay-kentän informaation perusteella solu reititetään Tor-piirin sisällä. Digest sisältää tarkistesumman, joka on laskettu solun hyötykuorman datasta. Len sisältää tiedon datan koosta (engl length, eli pituus tavuina). StreamID nimeää datavirran, johon solu kuuluu piirissä. Datavirtoja voi olla samassa piirissä useita riippuen esimerkiksi käytettävien sovellusten määrästä (Dingledine ym. 2019.)

2.2 Sipulireitityksen salaus

Tor-solut salataan kerroksittain siten, että piirin jokainen välityspalvelin kykenee purkamaan salauksesta yhden kerroksen, jotka kutsutaan sipulinkuoreksi (engl. onion skin). Salaus perustuu Diffle-Heffman -avainpareihin. (Ollila 2016)

Jos liikenne Tor-piirissä reititetään kolmen välityspalvelimen kautta, salataan Tor-solu ensin viimeisen välityspalvelimen julkisella avaimella. Tämän jälkeen toiseksi viimeisellä ja lopulta ensimmäisellä. Viestin kulkiessa palvelinten läpi kukin palvelin kykenee purkamaan salauksesta vain omaa sipuliavaintaan vastaavan kerroksen. Lopulta piirin viimeinen palvelin kykenee lukemaan koko viestin ja reitittämään sen eteenpäin lopulliselle vastaanottajalle. (Ollila 2016).

2.3 Tor-piirin palvelimet

Tor-piirin muodostamiseen tarvitaan lista käytettävissä olevista välityspalvelimista sekä ainakin kolme välityspalvelinta.

Hakemistopalvelin (engl. Directory Authority) on erityinen välityspalvelin, joka ylläpitää ja jonka kautta jaetaan tieto käytettävissä olevista välityspalvelimista ja niiden julkisista sipuliavaimista. Hakemistopalvelimia on useita, ja niiden tiedot on sisällytetty Tor-ohjelmistoon ennalta. (Dingledine ym. 2019)

Tulopalvelin

Ensimmäinen Tor-piirin välityspalvelin on niin sanottu tulopalvelin (engl. guard relay). Tämä välityspalvelin ottaa vastaan asiakasohjelman lähettämät Tor-solut, purkaa omaa julkista avainta vastaavan salauskerroksen ja reitittää liikenteen seuraavalle välityspalvelimelle. Tämä välityspalvelin tietää solujen lähettäjän sekä piirin seuraavan palvelimen, mutta ei viimeistä palvelinta tai datan lopullista vastaanottajaa. (Dingledine ym. 2019.)

Keskipalvelin

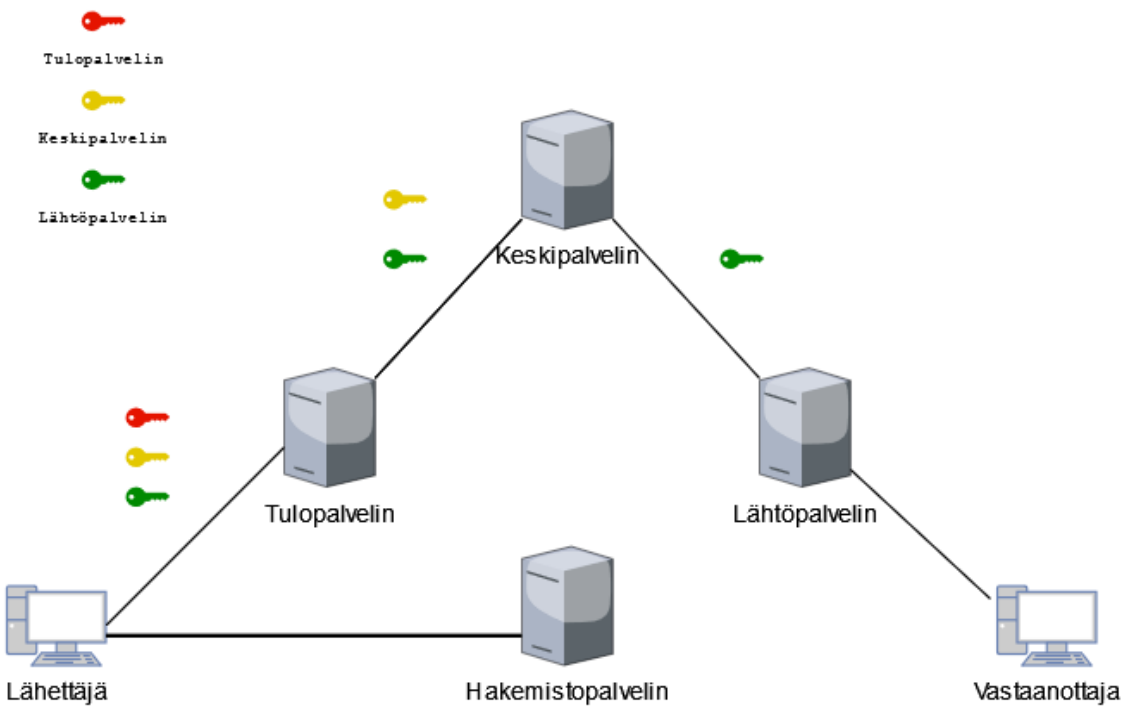
Piirissä seuraavaa palvelinta kutsutaan keskipalvelimeksi (engl. middle relay). Tämä palvelin toimii tulopalvelimen sekä piirin viimeisen palvelimen välissä. Palvelin vastaanottaa solut tulopalvelimelta, purkaa omaa salausavainta vastaavan kerroksen salauksesta ja välittää solun eteenpäin. Tämä palvelin tuntee tulopalvelimen sekä piirissä viimeisenä olevan lähtöpalvelimen, muttei datan lopullista vastaanottajaa eikä lähettäjää. (Dingledine ym. 2019.)

Lähtöpalvelin

Lähtöpalvelin (engl. Exit Node) on piirin viimeinen palvelin. Sen avatessa salauksen viimeisen kerroksen on solu salaamaton. Tämä palvelin reitittää liikenteen sen lähettäjän osoittamaan kohteeseen, esimerkiksi julkiselle HTTP-palvelimelle. Lähtöpalvelin ei tiedä, mistä liikenne on piiriin lähetetty. Se näkee vain palvelimen, jonne datavirta reititetään, sekä välipalvelimen, jolta se vastaanottaa solut.

Kun data reititetään edelläkuvatulla tavalla kolmen palvelimen kautta, datan vastaanottava palvelin näkee vain Tor-piiristä tulleen datan lähettäjän, eli lähtöpalvelimen. Näin ollen datan alkuperäinen lähettäjä jää tuntemattomaksi. (Dingledine ym. 2019.)

Kuvassa 3 esitetään Tor-piirin toiminta. Lähettäjä noutaa listauksen piirin palvelimista hakemistoauktoriteetilta. Tämän jälkeen lähettäjä muodostaa piirin kautta yhteyden vastaanottajaan. Lähettäjän ja Tulopalvelimen välinen yhteys on salattu piirin kaikkien kolmen palvelimen salausavaimilla. Tämän jälkeen salausta puretaan kerroksittain, kunnes Lähtöpalvelimen ja vastaanottajan välinen viesti on salaamaton.



Kuva 3. Viestisolun rakenne (Dingledine ym. 2019)

3 Välityspalvelinten laitteistovaatimukset ja palveluntarjoajan valinta

Tor-välityspalvelimen asennusta valmisteltaessa on syytä ottaa huomioon eräitä laitteistolle asetettuja vähimmäisvaatimuksia. Nämä vähimmäisvaatimukset ovat luonteeltaan suosituksia, joten palvelinohjelmiston voi asentaa myös vaatimuksista poikkeaviin laitteistoihin. Suosituksia noudattaen on kuitenkin todennäköisempää onnistua toimivan ja vakaan palvelimen asennuksessa.

Laitteistolle asetettavat vähimmäisvaatimukset riippuvat ensisijaisesti palvelimen kautta reititettävän verkkoliikenteen määrästä. Mitä suuremmaksi määrä kasvaa, sitä enemmän suoritustehoa palvelimelta vaaditaan. Ensisijaisesti kuormitus kohdistuu palvelinjärjestelmän suorittimeen sekä RAM-muistiin. (Tor Project 2023)

3.1 Tietoliikenneyhteydet

Keskipalvelimelle suositellaan tietoliikenneyhteyttä, jossa voidaan samanaikaisesti lähettää sekä vastaanottaa tietoliikennettä nopeudella 16 Mbit/s. Lisäksi palvelimen tulisi kyetä käsittelemään vähintään 7 000 samanaikaisesta TCP-yhteyttä. Lähtöpalvelimen osalta suositellaan tietoliikenneyhteyttä, joka kykenee nopeuteen 100 Mbit/s. Lisäksi on huomattava, että 7 000 samanaikaista yhteyttä toteutuu vain harvoin, todellisuudessa määrät ovat moninkertaisia. (Tor Project 2023)

Verkkoliikenteen määrän osalta suositellaan varautumaan vähintään. 100 Gt:uun kuukaudessa. Jos mahdollista, kannattaa hankkia palvelu, johon sisältyy rajaton määrä verkkoliikennettä.

Nämä tietoliikenneyhteydelle asetetut suositukset on vain harvoin mahdollista toteutaa kuluttaja-asiakkaille tarjottavilla Internet-liittymillä ja reitittimillä. Tämän vuoksi onkin suositeltavaa hankkia välityspalvelinta varten VPS tai dedikoitu palvelin tarkoitukseen sopivalta palveluntarjoajalta. (Tor Project 2023b). Palveluntarjoajia ja palvelimen hankintaa käsitellään seuraavassa luvussa.

3.2 Muu laitteisto

Kuten mainittu, muulle laitteistolle asetettavat vaatimukset riippuvat käsiteltävän verkkoliikenteen määrästä.

Tässä esitetään ne vähimmäisvaatimukset, joita Tor Project (2023b) suosittelee muistille, suorittimelle sekä kiintolevylle.

Muistia tulisi olla vähintään 512 MB, jos kyse on muusta kuin lähtöpalvelimesta, ja jos tietoliikenneyhteyden siirtonopeus alle 40 Mbit/s. Jos siirtonopeus on tätä suurempi, tulisi muistia olla ainakin 1 GB. Lähtöpalvelimelle suositellaan ainakin 1,5 GB muistia.

Ohjeistuksen mukaan mikä tahansa nykyaikainen suoritin käy, mikäli se tukee AES-NI -tekniikkaa. AES-NI, eli Advanced Encryption Standard New Instructions, on nykyaikaisiin suorittimiin sisältyvä ominaisuus, joka mahdollistaa AES-salauksen tehokkaan käsittelyn. (Rott 2023)

Välityspalvelinohjelmisto vie itsessään vain noin 200 MB tallennustilaa. Kiintolevyn kokoa arvioitaessa kannattaa kuitenkin muistaa, että myös käyttöjärjestelmä itsessään vaatii tilaa, samaten muu ohjelmisto.

3.3 Palveluntarjoajan valinta

Kuten edellisessä luvussa todettiin, välityspalvelinten vaatima teho erityisesti verkkolaitteiden osalta vaatii olosuhteet, jotka toteutuvat yleensä lähinnä palvelinkeskuksissa. Tämän vuoksi päädyin itsekin valitsemaan kullekin kolmesta välityspalvelimesta sopivan VPS-palveluntarjoajan.

Palveluntarjoajaa valitessani kiinnitin ensisijaisesti huomioni tarjottaviin laitteistoresursseihin, eli siihen, että edellisessä kappaleessa mainitut vaatimukset täyttyisivät.

Palveluntarjoajaa valittaessa on kiinnitettävä huomiota myös käyttöehtoihin sekä mahdollisiin muihin asiakkaalle esitettyihin käyttöön liittyviin rajoituksiin. Nämä määritellään yleensä palveluntarjoajan verkkosivustoilla asiakirjoissa, kuten *Terms of Service* ja *Acceptable Use Policy.* Näissä määritellään eriasteisella tarkkuudella mitä ohjelmistoja asiakas saa vuokraamallaan palvelimella käyttää sekä esimerkiksi minkälaisia materiaaleja palvelimella voi pitää tallennettuna tai jakaa yleisölle. Tyypillisesti hyväksyttyjen käyttötarkoitusten ulkopuolelle rajataan asiat, kuten suoratoistopalvelut, tekijänoikeudella suojatun materiaalin levittäminen (piratismi), laitteiston käyttö tietomurtoihin tai tietoliikenteen häiritään, porno sekä Tor-välityspalvelimet.

Havaintoni mukaan erityisesti lähtöpalvelimen ylläpito ja käyttö palvelimilla koetaan ongelmalliseksi, sillä tämän palvelimen julkinen IP-osoite liittyy tietoliikenteeseen, joka palvelimelta reitittyy vastaanottajille. Tämän vuoksi on mahdollista, että palvelimen IP-osoite päätyy esimerkiksi erilaisille IP-osoitteiden estolistoille, joille erilaiset toimijat keräävät IP-osoitteita, joiden epäillään liittyvän laittomiin toimiin, roskapostin lähetykseen tai muuhun epätoivottavaan käyttäytymiseen. Palveluntarjoajat eivät pidä toivottavana, että heidän osoiteavaruuteensa liittyvät osoitteet joutuvat estolistoille, koska tämä haittaa liiketoimia ja mainetta. Muut Tor-välityspalvelimet ovat vähemmän ongelmallisia, sillä niiden IP-osoitteet eivät näy Tor-piirin ulkopuolelle reitittyvään liikenteeseen.

Sopivan palveluntarjoajan etsintään voi käyttää apuna Tor Projectin Tor Relay Search -palvelua. Palvelussa voi hakea välityspalvelinten tietoja erilaisilla hakuehdoilla. Välityspalvelimen IP-osoiteen perusteella on mahdollista selvittää palvelimen käyttämä palveluntarjoaja.

Tarjotun laitteiston ja käyttöehtojen lisäksi tarkastelin myös palvelinvuokran kokonaiskustannuksia. Tyypillisesti hintaan sisältyy itse laitteiston lisäksi myös

yksi IPv4-osoite, joissain tapauksissa myös IPv6-osoite. Yleisesti ottaen voidaan sanoa, että välityspalvelimelle sopiva VPS-palvelu maksaa noin 10 euroa kuukaudessa.

3.3.1 Valitut palveluntarjoajat ja laitteistokokoonpanot

Valitsemani palveluntarjoajat välityspalvelimille ovat Privex Inc, BlueVPS OÜ sekä Oy Creanova Hosting Solutions Ltd.

Privex mainitsee markkinointitiedotteissaan, että lähtöpalvelimen käyttö on tietyin ehdoin sallittua. Tästä on kuitenkin erikseen sovittava palvelua tilattaessa. He edellyttävät myös tiettyjen asetusten käyttöä liikenteen suodatuksen osalta. Tarkennan tätä kappaleessa, jossa käsittelen palvelinten asennusta ja konfigurointia.

BlueVPS sekä Creanova ovat palveluntarjoajia, jotka esiintyvät usein palveluntarjoajina välityspalvelimille. Tämän voi todeta esimerkiksi käyttämällä Tor Relay Searchia. Kummankaan yrityksen käyttöehdot eivät myöskään kiellä asiakkaita ajamasta Tor -välityspavelimia heidän tarjoamillaan VPS-palvelimilla, joten molemmat yritykset käyvät tarkoitusta varten hyvin.

3.3.2 Välityspalvelinten kokoonpanot ja kustannukset

Opinnäytetyössäni käytettyjen palvelinten kokoonpanot kuvataan oheisissa taulukoissa.

Privex Inc

Taulukko 1. Privex Incin tarjoama VPS-palvelimen kokoonpano sekä kuukausihinta.

Käyttöjärjestelmä	Debian 11
Prosessori	Intel Broadwell 2 ydintä, 2,4Ghz
Muisti	2 GB
Kiintolevy	25 GB
Verkkoyhteys	100 Mbit/s
IP-osoitteet	1 IPv4, 1 IPv6
Kuukausihinta	$14,80

BlueVPS

Taulukko 2. BlueVPS:n tarjoama VPS-palvelimen kokoonpano sekä kuukausihinta.

Käyttöjärjestelmä	Debian 11
Prosessori	3 ydintä, 3 Ghz (QEMU)
Muisti	1 GB
Kiintolevy	20 GB
Verkkoyhteys	1 Gbit/s
IP-osoitteet	1 IPv4, 1 IPv6
Kuukausihinta	$12

Creanova Hosting Solution

Taulukko 3. CreaNovan tarjoama VPS-palvelimen kokoonpano sekä kuukausihinta.

Käyttöjärjestelmä	Debian 10
Prosessori	3 ydintä, 2,4 GHz (Common KVM)
Muisti	6 GB
Kiintolevy	100 GB
Verkkoyhteys	1 Gbit/s
IP-osoitteet	1 IPv4, 1 IPv6
Kuukausihinta	12 €

4 Välityspalvelinten konfigurointi

Opinnäytetyötä varten valituissa VPS-palvelimissa on esiasennettuna Debian GNU/Linux-käyttöjärjestelmä sekä sen mukana toimiva valikoima erilaisia ohjelmistoja, mutta ei Tor-ohjelmistoa. Jotta näitä palvelimia voidaan käyttää välityspalvelimina, on niihin asennettava tätä varten tarvittava Tor Projectin tuottama ja ylläpitämä ohjelmisto.

Palvelimen ylläpitäjän vastuulla on myös ylläpitämänsä palvelimen tietoturva. Tämä mainitaan usein myös VPS-palveluntarjoajan käyttöehdoissa. Yksinkertaisimmillaan tämä voidaan ymmärtää siten, että palvelinta tai sille asennettuja ohjelmistoja voi käyttää vain ylläpitäjä itse tai hänen valtuuttamansa muut henkilöt.

Palvelimien toimintaa ja niiden kautta kulkevan tietoliikenteen määrää voidaan seurata erilaisin ohjelmistoin. Tällaisen ohjelmiston asennus on suositeltavaa, jotta palvelimen tilaa ja resurssien riittävyyttä voidaan seurata. Mikäli palvelin vaikuttaisi toimivan virheellisesti, voidaan monitorointiohjelmiston keräämää tietoa käyttää apuna ongelmien syyn selvittämisessä.

4.1 Toimenpiteet ennen Tor-ohjelmiston asennusta

Käyttäjätunnukset ja salasanat

Tässä luvussa esitetyt valmistelevat toimenpiteet suoritettiin samankaltaisina kullekin kolmelle palvelimelle. Kussakin palvelimessa on käytössä Debian Linux, joten niiden valmistelu sekä käytetyt komennot ja konfiguroinnit tehtiin yhtenevällä tavalla.

Palvelimen käyttöönotto aloitettiin kirjautumalla palvelimelle SSH-ohjelmistoa käyttäen. Palvelimen käyttöä varten oli saatu käyttäjätunnus sekä salasana palveluntarjoajalta. Käyttäjätunnus oli `root`, joka on Linux -käyttöjärjestelmän pääkäyttäjätunnus.

Tätä tunnusta käytetään yleensä Linuxin ylläpitotoimenpiteissä, kuten tehtäessä muutoksia käyttöjärjestelmään tai asennettaessa ohjelmistoja.

Pääkäyttäjätunnuksen salasana vaihdettiin käyttäen komentoa `passwd`.

Tämän jälkeen Tor-ohjelmiston käyttöä varten luotiin käyttäjä `tor:` `useradd -m tor`.

Edellä mainittu komento luo käyttäjätunnuksen `tor` sekä tälle kotihakemiston sijaintiin `/home/tor`. Tässä hakemistossa sijaitsevat käyttäjätunnuksen henkilökohtaiset tiedostot sekä käyttäjätunnukseen liittyvät ohjelmistojen konfigurointeja määrittelevät tiedostot. Tor-ohjelmistojen käyttöä varten luotiin oma käyttäjätunnus, jotta ohjelmistoja ei käytettäisi pääkäyttäjätunnuksella. Pääkäyttäjällä on rajoittamaton luku- ja kirjoitusoikeus kaikkiin käyttöjärjestelmän osiin sekä tiedostoihin. Jos ulkopuolinen henkilö saisi esimerkiksi ohjelmistohaavoittuvuuden kautta hallintaansa ohjelmiston, jota käytetään pääkäyttäjäoikeuksin, saattaisi hyökkääjä saada myös pääkäyttäjän oikeudet muuhun järjestelmään. Tämän vuoksi välityspalvelinohjelmista käytetään sille varatulla käyttäjätunnuksella.

Tor -käyttäjälle luotiin salasana komennolla `passwd tor`.

Pääsynhallinta

Palvelimelle kirjaudutaan SSH-ohjelmistoa käyttäen, joten pääsynhallintaa koskevat asetukset tulee tehdä muokkaamalla SSH-palvelimen asetuksia. Asetuksia muokattiin siten, että palvelimelle ei voi kirjautua pääkäyttäjänä SSH:n avulla, eikä kirjautumiseen voi käyttää salasanaa. Kirjautumiseen voi käyttää vain SSH-avainparia. Tällä tavoin pyrin estämään väsytyshyökkäyksen kohdentamisen palvelimelle. Väsytyshyökkäyksellä pyritään kirjautumaan palvelimelle syöttämällä erilaisten käyttäjätunnusten sekä salasanojen yhdistelmiä niin kauan, että jokin yhdistelmä osoittautuu oikeaksi. (Wikipedia 2023). Kömpelyydestään huolimatta tämä hyökkäystapa on aktiivisessa käytössä.

Pääkäyttäjän kirjautuminen SSH-palvelimelle sekä kirjautuminen SSH-avainpareilla toteutettiin tekemällä tiedostoon `/etc/ssh/sshd_config` seuraavat muutokset.

Tiedoston rivillä 38 oleva määritys `#PubkeyAuthentication yes` muutetaan muotoon `PubkeyAuthentication yes`, jollon kirjautuminen SSH-avainparin julkisella avaimella sallitaan. Vastaavasti kirjautuminen salasanalla estetään muuttamalla tiedoston rivillä 58 oleva määritys muodosta `#PasswordAuthentication yes` muotoon `PasswordAuthentication no`.

Pääkäyttäjän kirjautuminen SSH:illä estettiin muokkaamalla rivin 33 määritys `#PermitRootLogin prohibit-password` muotoon `PermitRootLogin no`.

Muutosten jälkeen SSH-palvelin käynnistettiin uudelleen komennolla `systemctl restart sshd`.

Koska kirjautuminen palvelimelle on mahdollista vain SSH-avainpareilla, loin itselleni tätä käyttötarkoitusta varten SSH-avainparin henkilökohtaisella PC-tietokoneellani komennolla `ssh-keygen`. Tämän jälkeen siirsin julkisen avaimen kohdepalvelimelle komennolla `ssh-copy-id [palvelimen IP]`.

NetData

Palvelimen toimintaa ja tietoliikenteen määrää kuvaavan tiedon tallennusta ja esittämistä varten asennettiin ohjelmisto nimeltä NetData.

NetDatan kehittäjäyhteisö suosittelee ohjelmiston asennusta tarkoitusta varten luodulla Kickstart scriptillä seuraavasti:

```
wget -O /tmp/netdata-kickstart.sh https://my-netdata.io/kickstart.sh
&& sh /tmp/netdata-kickstart.sh
```

Netdatan hallintanäkymää ja asetuksia käytetään verkkoselaimella. Jotta päästään hallintanäkymään, tulee verkkoselain ohjata osoitteeseen http://127.0.0.1:19999. IP-osoite voi olla myös palvelimen julkinen IP-osoite, jos pääsy on sallittu myös Internetistä. Koska NetData ei tue minkäänlaista salasanasuojausta hallintanäkymänsä osalta, kannattaa pääsy julkisesta verkosta rajata pois. Tämä tapahtuu muokkaamalla tiedostoa

```
/etc/netdata/netdata.conf

[web]
    allow connections from = localhost
    allow management from = localhost
```

Tämä sallii pääsyn hallintanäkymään vain paikallisverkosta. Käytännössä tämä tarkoittaa sitä, että etäkäyttö verkkoselaimella mahdollistuu vain, jos palvelimelle on muodostettu SSH-tunneli, jonka kautta verkkoselaimen liikenne reititetään NetDatan hallintanäkymään. Tunneli luodaan käyttäen seuraavaa komentoa omalla PC-tietokoneella: `ssh -N -D 19999 tor@[palvelimen ip].` Tämän jälkeen verkkoselaimen välityspalvelinasetuksissa määritellään palvelimeksi oma tietokone ja portiksi 19999.

4.2 Tor-ohjelmiston asennus ja konfigurointi

Tor-ohjelmiston käytöstä ja jakelusta määrätään "3-clause BSD"-lisenssillä (Tor License 2019.) Lisenssin mukaan ohjelmiston käyttö ja edelleen levittäminen on maksutonta. Kyseisen lisenssin perusteella Tor on vapaan lähdekoodin ohjelmisto, joten myös sen lähdekoodi on vapaasti saatavilla sekä levitettävissä. Tästä huolimatta ohjelmistoa ei useinkaan toimiteta esiasennettuna käyttöjärjestelmän mukana, vaan se on asennettava erikseen.
The Tor Project on tuottanut ohjeet Tor-ohjelmiston asentamista ja konfigurointia varten. Tätä opinnäytetyötä tehdessä noudatettiin Tor Projectin ohjeita välityspalvelinten asennuksesta sekä konfiguroinnista, joten kuvailen ohjeita ja tekemiäni valintoja konfiguroinnin osalta seuraavissa luvuissa.

4.2.1 Asennus

Tor-ohjelmiston asennus Linux -käyttöjärjestelmään tapahtuu aina samoin. Asennuksenjälkeisellä konfiguroinnilla voidaan määritellä toimiiko palvelin lähtöpalvelimena vai ei. Esittelen ensin Tor-ohjelmiston asennuksen, jonka

jälkeen esitän välityspalvelinten konfiguroinnin omissa luvuissaan.Tor Projectin ohjeissa kerrotaan varsin seikkaperäisesti ohjelmiston asennuksesta Linux -käyttöjärjestelmälle. Tor Projectin ohjeistuksessa (Tor Relay Operations: Technical setup 2023) suositellaan käyttämään asennuspakettien latauksessa Tor Projectin jakelukanavia, sekä varmistamaan pakettien autenttisuus vertaamalla paketin tuottamaa GPG -tarkistesummaa ohjeistuksessa mainittuun.

Aluksi ohjeissa suositellaan asennettavaksi apt-transport-https -ojelmisto, joka mahdollistaa asennuspakettien noudon salatun HTTP-yhteyden avulla. Asennus suoritetaan komennolla

```
apt install apt-transport-https
```

Tämän jälkeen muokataan Debianin Apt -paketinhallintaohjelmiston konfigurointia siten, että asennettavien ohjelmistojen nouto Tor Projectin ylläpitämästä pakettivalikoimasta mahdollistuu. Tämä tapahtuu siten, että hakemistoon `/etc/apt/sources.list.d/` luodaan tiedosto `tor.list`. `Tor.list` tiedostoon kirjoitetaan Apt -ohjelmiston käyttämät tiedot Tor Projectin tarjoamien asennuspakettien sijainnista sekä GPG-avaimista. GPG-avainpareja käytetään edellämainitun GPG -varmistesumman vertaamiseen.
Koska välityspalvelimeni käyttävät Debian Linux -käyttöjärjestelmää sekä 64-bittistä prosessoriarkkitehtuuria, sijainnit määritellään seuraavasti:

```
deb     [signed-by=/usr/share/keyrings/tor-archive-keyring.gpg]
https://deb.torproject.org/torproject.org stable main
```

Signed-by= osoittaa gpg-avainten sijainnin, ja alempi rivi on URL Tor Projectin asennuspaketeille sekä määrittely käyttämäni Debian Linuxin jakeluversiolle. Ennen pakettien noutamista tulee noutaa GPG-avain, jolla varmennetaan pakettien autenttisuus. Tämä tapahtuu komennolla

```
wget -qO-
https://deb.torproject.org/torproject.org/A3C4F0F979CAA22CDBA8F512EE8C
BC9E886DDD89.asc | gpg --dearmor | tee /usr/share/keyrings/tor-
archive-keyring.gpg >/dev/null
```

Koska GPG-avain tai sen sijainti voi muuttua, on suositeltavaa tarkistaa ajantasaisin ohjeistus Tor Projectin sivustolta.

Kun edelläkuvatut Apt-ohjelmiston konfiguroinnit on suoritettu, voidaan Tor-ohjelmisto asentaa komennoilla:

```
apt update
apt install tor deb.torproject.org-keyring
```

Apt varmistaa asennuspakettien autenttisuuden ennen asennusta, jonka jälkeen ohjelmisto asennetaan käyttöjärjestelmän osaksi. Debian konfiguroi käyttöjärjestelmän SystemD-komponentin siten, että Tor käynnistetään automaattisesti käyttöjärjestelmän uudellenkäynnistyksen yhteydessä. Tor myös käynnistetään asennuksen yhteydessä.

4.2.2 Konfigurointi

Tor-ohjelmiston konfigurointi tapahtuu muokkaamalla `torrc` -nimistä tekstitiedostoa, joka sijaitsee hakemistossa `/etc/tor`. Tätä tiedostoa muokkaamaalla voidaan vaikuttaa monipuolisesti ohjelmiston toimintaan, jonka vuoksi ylläpitäjällä on paljon mahdollisuuksia mukauttaa ohjelmistoa vastaamaan omia tarpeitaan sekä päämääriään. Tiedostoa muokkaamalla vaikutetaan myös siihen, toimiiko ohjelmisto Tor-verkon välityspalvelimena vai ei. Tämän lisäksi vaikutetaan siihen, toimiiko ohjelmisto lähtöpalvelimena vai ei. On syytä huomata, että `torrc` -tiedostoa on ehdottomasti muokattava aina, kun halutaan käyttää ohjelmistoa välityspalvelimena, sillä oletusasetukset eivät sellaisenaan aktivoi ohjelmiston välityspalvelinominaisuuksia.

Tulo- ja keskipalvelin

Konfigurointi tapahtuu muokkaamalla tekstinkäsittelyohjelmistolla `torrc` -tiedostoa. Debian Linuxin mukana tulee esiasennettuna joitakin

tekstinkäsittelyohjelmia, kuten Nano ja Vim. On kuitenkin tärkeää valita ohjelmisto siten, ettei se jätä tekstiin ylimääräisiä symboleja tai muotoilumerkkejä, kuten jotkut toimisto-ohjelmistot saattavat tehdä. Tämän vuoksi Nano tai Vim ovat kumpikin hyviä valintoja.
Tiedoston `torrc` muokkaaminen tapahtuu pääasiassa siten, että halutun avainsanan edestä poistetaan # -merkki. Tämä aktivoi avainsanan kuvaaman toiminnallisuuden tai ominaisuuden itse ohjelmistossa. Muokkaamisen avuksi tiedostossa on lyhyet kuvaukset kunkin avainsanan toiminnasta ja merkityksestä. Tämän lisäksi Tor Projectin dokumentaatio tarjoaa laajempaa tietoa näiden avainsanojen ominaisuuksista sekä vaikutuksista ohjelmiston toimintaan. Avainsanan jälkeen kirjoitetaan tyypillisesti joitain määreitä tai argumentteja, joilla ohjelmiston toiminnallisuuteen vaikutetaan.

Tor-välityspalvelimella on tyypillisesti nimi, jolla se erottautuu Tor-verkossa. Tämän vuoksi `torrc` -tiedoston rivin 102 avainsana `NickName` aktivoidaan ja valitaan välityspalvelimelle nimi kirjoittamalla se avainsanan perään:

```
NickName anotherlegitrelay.
```

Edellä mainitulla esimerkillä välityspalvelimen nimeksi tulee anotherlegitrelay. Välityspalvelimelle voidaan määritellä myös ylläpitäjän yhteystiedot, jotta Tor Project voi ottaa häneen yhteyttä esimerkiksi palvelimessa havaitun häiriön vuoksi. Tämä tehdään rivillä 131:

```
ContactInfo Relayops <relayops AT tutanota DOT com>
```

Yllä olevassa esimerkissä ylläpitäjän nimeksi mainitaan Relayops ja sähköpostiosoitteeksi relayops@tutanota.com. @ ja . -merkit on korvattu sanoilla AT ja DOT, jotta automaattisesti sähköpostiosoitteita etsivät ohjelmistot eivät tunnistaisi osoitetietoa sähköpostiosoitteeksi. Nämä tiedot nimittäin löytyvät Tor Projectin julkaisemalla verkkosivulla, joka luettelee aktiiviset välityspalvelimet. (Tor Metrics 2023).

Rivillä 85 määritellään tietoliikenneportti saapuvalle tietoliikenteelle. Käytän porttia 443, mutta portti voi olla mikä tahansa. Jos palvelimella on käytössä palomuuriohjelmisto, on syytä muistaa avata valittu portti saapuvalle tietoliikenteelle.

```
ORPort 443
```

Koska palvelin ei toimi lähtöpalvelimena, asetetaan avainsanan ExitRelay arvoksi 0 rivillä 186.

```
ExitRelay 0
```

Tor-ohjelmistoa voidaan käyttää myös esimerkiksi verkkoselaimen, sähköpostin tai pikaviestimien tietoliikenteen reitittämiseen Tor-verkon kautta. Jos ohjelmistoa haluaa käyttää vain välityspalvelimena, tulee avainsanan `SocksPort` arvoksi asettaa 0 rivillä 20.

```
SocksPort 0
```

Jos ylläpitää useampaa kuin yhtä välityspalvelinta, on suositeltavaa määritellä palvelimet avainsanalla MyFamily rivillä 157. Tämä tapahtuu lisäämällä avainsanan perään kunkin välityspalvelimen key identity fingerprint. Tämä tieto löytyy tiedostosta `/var/log/tor/fingerprint`. Tällä tavoin määritellään saman ylläpitäjän hallinnoimat välityspalvelimet, ja samalla pyritään varmistamaan, että Tor-liikennettä ei reititetä useamman kuin yhden saman henkilön tai organisaation hallinnoiman välityspalvelimen kautta.
Koska ylläpidän kolmea välityspalvelinta, olen määritellyt `MyFalimy`-avainsanan seuraavasti:

```
MyFamily F852A11B7725DC294DF7063B590C582883B1310F
7B288A194C9D5B7EA8F3093EDF3CEE6A512F8B98
B92EA9BCE0ADF008C8EF373A384E1FEC064B6895
```

Muokkaamani `torrc` -tiedosto on tämän opinnäytetyön liitteenä (Liite 1.)

Lähtöpalvelin

Lähtöpalvelimen konfigurointi eroaa joiltain osin edelläkuvailluista tulo- ja keskipalvelimen konfiguroinneista. Yhteistä edellämainituille konfiguroineille on, että myös lähtöpalvelimen osalta on aktivoitava avainsanat `SocksPort`, `NickName`, `ContactInfo`, `ORPort`, `ExitRelay`, sekä `MyFamily`. Kaikki nämä

avainsanat aktivoidaan samoin kuin edelläkuvatussa konfiguraatiossa. Poikkeuksen tekee `ExitRelay`, joka saa arvoksi 1. Tästä seuraa se, että palvelin toimii lähtöpalvelimen roolissa.

Lähtöpalvelimen kautta Internetiin reitittyvä tietoliikenne saa lähettävän laitteen IP-osoitteeksi lähtöpalvelimen IP-osoitteen. Tämän vuoksi Tor Project suosittelee, että palvelimen IP-osoitteelle varattaisiin verkkotunnus (engl. domain name), josta kävisi ilmi, että kyseessä on Tor-verkkoon kuuluva lähtöpalvelin. Lisäksi on suositeltavaa, että palvelimelle ladattaisiin HTML-sivu, joka ilmaisee tämän saman asian. Tor Project on laatinut HTML-sivun, jota voi halutessaan käyttää tähän tarkoitukseen. (Tor Project. Relay Operations: Exit Relay). Sivua tulisi käyttää siten, että kun verkkoselaimen ohjaa lähtöpalvelimen IP-osoitteeseen tai verkkotunnuksen mukaiseen osoitteeseen, saa nähtäväkseen tämän sivun. Sivulla kerrotaan, että kyseessä on Tor-verkon lähtöpalvelin. Lisäksi sivulla kerrotaan lyhyestä Tor -verkosta sekä siitä, että palvelimen ylläpitäjä ei välttämättä kontrolloi liikennettä, vaan liikennettä reititetään palvelimen kautta yleiseen verkkoon.

Lähtöpalvelimen tulee toimia myös DNS-palvelimena, sillä se reitittää tietoliikennettä Internetiin, jolloin on pystyttävä yhdistämään IP-osoite sitä vastaavaan verkkotunnukseen sekä päinvastoin. Tämä saavutetaan Debian Linux-käyttöjärjestelmällä käyttämällä Unbound DNS-palvelinohjelmistoa. Ohjelmisto ei tyypillisesti vaadi konfigurointia asennuksensa jälkeen, joten käyttöönotto on suoraviivaista. Se tapahtuu antamalla seuraavat komennot:

```
apt install unbound
cp /etc/resolv.conf /etc/resolv.conf.backup
echo nameserver 127.0.0.1 > /etc/resolv.conf
```

Ensimmäinen komento aikaansaa Unboundin asennuksen. Toisella rivillä otetaan kopio muokkaamattomasta resolv.conf -tiedostosta, ja viimeisellä rivillä määritellään ensisijaisen DNS-palvelimen osoitteeksi kyseinen palvelin.

Tätä opinnäytetyötä varten vuokrasin Privex-yritykseltä virtuaalipalvelimen, jonka olen konfiguroinut lähtöpalvelimeksi. Neuvotellessani palvelimen vuokrauksesta yrityksen kanssa, he asettivat sopimuksen ehdoksi sen, että suodattaisin palvelimen kautta reitittyvää tietoliikennettä siten, että tietyt kohdeosoitteiden portit estettäisiin kaikissa tapauksissa. Tämä tarkoittaa käytännössä sitä, että tietoliikenteen ohjaaminen kohdeosoitteiden tiettyihin portteihin olisi aina estetty riippumatta kohdeosoitteesta.

Privexin käytännöt Tor-verkon lähtöpalvelinten ylläpidon osalta on esitetty heidän verkkosivuillaan. Sen mukaan he käsittelevät kaikki saamansa viralliset valitukset ylläpidettävään lähtöpalvelimeen liittyen, mikäli palvelimen ylläpitäjä sitoutuu suodattamaan tietoliikennettä Tor Projectin *Reduced Exit Policy* -sääntöillä. Lisäksi Privex pyytää estämään tietoliikenteen reitittymisen kohdeosoitteen porttiin 22, eli SSH-palvelimen oletusporttiin.

Reduced Exit Policy -säännöt on esitelty Tor Projectin dokumentaatiossa Tor Project, Reduced Exit Policy, 2023.). Ne toimivat siten, että säännöillä määritellään portit, joihin liikennettä reititetään ja kaikki muut portit ovat estettyjä. Eli jos porttia ei erikseen ole listattuna säännöissä, siihen ei reititetä tietoliikennettä. Säännöt määritellään kirjoittamalla ne torrc -tiedostoon. Esimerkiksi kirjoittamalla `ExitPolicy accept *:20-21` sallitaan reititys portteihin 20-21. Säännöt luetellaan allekain käyttäen ExitPolicy -avainsanaa. Listauksen viimeiseksi riviksi tulee `ExitPolicy reject *:*` josta seuraa, että kaikki ne portit joita ei ole listattu, on estetty.

Privex ei tarjoa verkkotunnuksia, joten hankin verkkotunnuksen Njalla -nimiseltä palveluntarjoajalta. Njalla vuokraa erihintaisia verkkotunnuksia asiakkailleen siten, että asiakkaan ei tarvitse antaa omia yhteystietojaan yritykselle. Kuka tahansa voi siis hyvin helposti ja nopeasti hankkia itselleen verkkotunnuksen. Halutessaan vuokran voi myös maksaa nimettömästi esimerkiksi erilaisilla virtuaalivaluutoilla. Maksuvälineeksi käy myös yleisimmät pankki- ja luottokortit. (Njal.la 2023.)

Hankin itselleni verkkotunnuksen torexitnode.fans. Annoin tämän jälkeen palvelimelleni verkkotunnuksen swedxitnode.torexitnode.fans. Pyysin tämän jälkeen, että Privex määrittelisi DNS-järjestelmään liittyvät PTR-tiedot siten, että palvelimeni IP-osoite 185.130.46.141 käännettäisiin palvelimeni verkkotunnukseksi.
Näin saavutetaan Tor Projectin suosittelema tilanne, jossa palvelimen verkkotunnus ja IP-osoite on helposti ymmärrettävissä Tor-lähtöpalvelimen käytössä olevaksi. Näin palvelimelta tuleva tietoliikennekin on helposti määriteltävissä Tor-verkosta julkiseen verkkoon reititetyksi tietoliikenteeksi. Lähtöpalvelimen konfigurointitiedosto muokkauksineen on opinnäytetyön liitteenä.

5 Ylläpito

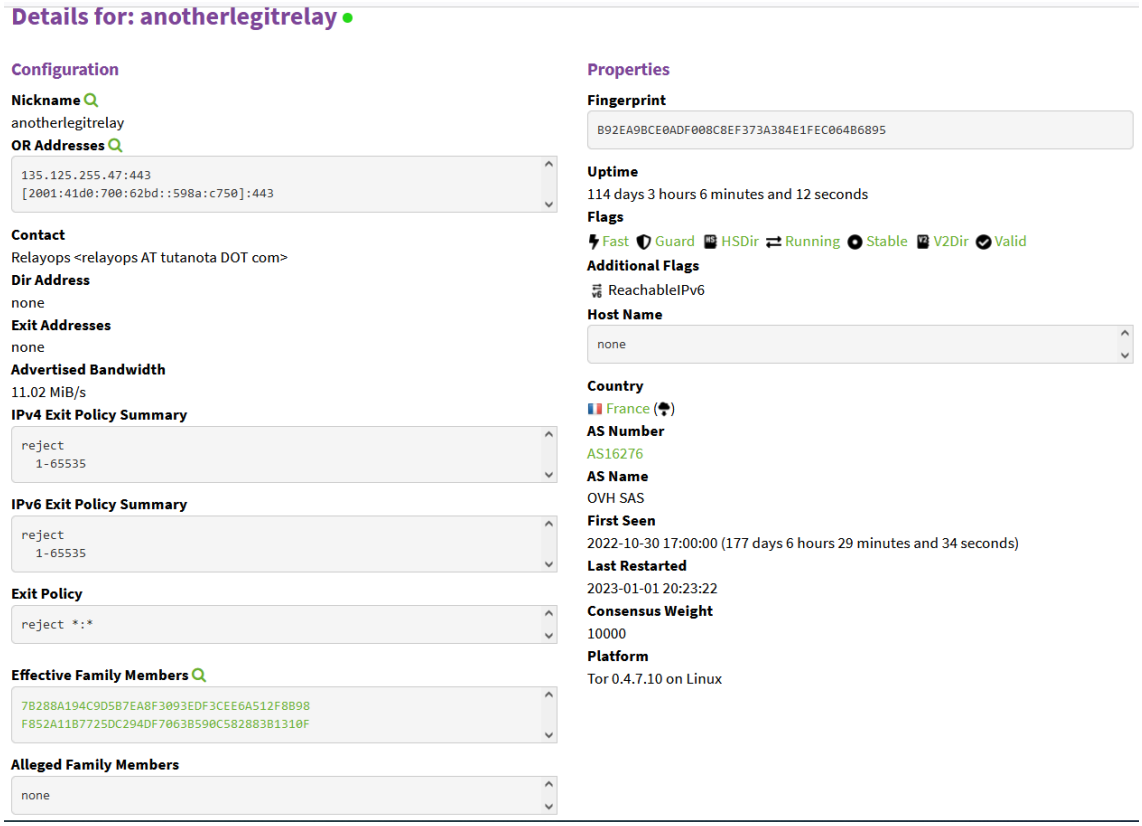
Käynnissäolevien välityspalvelinten toimintaa voi havainnoida valvontatyökalujen tuottaman tilannetiedon sekä lokitiedostojen merkintöjen avulla. Palvelinten toiminnan seuraaminen ja mahdollisiin häiriöihin reagointi kuuluvat ylläpitäjän tehtäviin. Lisäksi palvelinten toiminnan havainnointi on osa opinnäytetyötäni, joten käsittelen käyttämiäni havainnointimenetelmiä sekä niiden avulla saatuja havaintoja tässä luvussa.

5.1 Tilannetiedon lähteet

Tor Metrics

Tor Project tarjoaa Tor Metrics -sivustollaan tilastotietoa liittyen Tor-verkkoon, sen palvelimiin, palveluihin sekä käyttäjiin. Tällä sivulla on mahdollista hakea myös tietoja yksittäisistä välityspalvelimista. Hakutermeinä voi käyttää esimerkiksi välityspalvelimen maantieteellistä sijaintia, sen nimeä tai verkko-osoitetta. Välityspalvelimen ylläpitäjä voi käyttää Tor Metricsin tarjoamaa tietoa muodostaessaan käsitystä palvelimensa tilasta ja toiminnasta. (Tor Metrics 2023).

Kuvassa 4 on ote Tor Metrics -sivuston tuottamasta välityspalvelinta koskevasta tiedosta. Kyseessä on välityspalvelin nimeltä ’anotherlegitrelay’. ja se on yksi kolmesta ylläpitämästäni palvelimesta. Tiedoista käy ilmi palvelimen verkko-osoitteet, keskimääräinen tiedonsiirtonopeus, ExitPolicy-määrittelyt, MyFamily-määrittelyt, palvelimen yksilöivä Fingerpint -tiivistesumma, yhtäjaksoisen käynnissäolon aika sekunnin tarkkuudella, palvelimen ominaisuuden ja rooli Tor-verkossa, mahdollinen verkkotunnus, maantieteellinen sijainti, liittymisaika osaksi Tor-verkkoa, edellisen uudelleenkäynnistyksen ajankohta sekä tietoa Tor-ohjelmistosta.

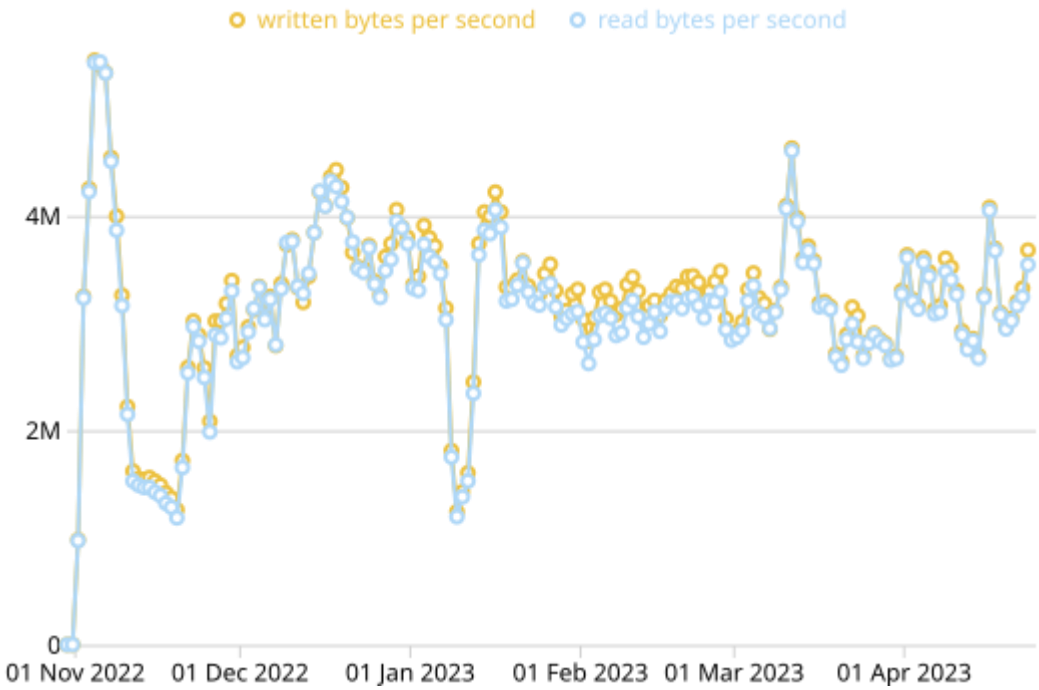


Kuva 4. Kuvakaappaus Tor Metrics -sivustolta palvelimesta anotherlegitrelay (Tor Metrics 2023b)

Näitä tietoja voidaan käyttää ennen kaikkea arvioitaessa konfiguroinnin oikeellisuutta. Jos palvelin esimerkiksi käynnistyy lyhyin väliajoin uudelleen, sille ei myönnetä ’Stable’ -merkintää. Jos palvelin ei ole saavutettavissa, sille ei myönnetä ’Running’-merkintää.

’Valid’-merkintä puuttuu palvelimilta, joiden ohjelmistoversio ei ole enää tuettu tai hyväksytty käyttöön Tor-välityspalvelimissa. Jos ylläpitäjä on konfiguroinut välityspalvelimensa siten, että se tarjoaa käyttäjälle luetteloa tunnetuista ”piilopalveluista” (engl. Tor Hidden Services), tämän konfiguroinnin oikeellisuus ilmenee ’HSDir’-merkinnästä. (Tor Project 2023b).

Tor Metrics tarjoaa myös tilastotietoa, jota voidaan käyttää palvelimen toiminnan seurantaan.

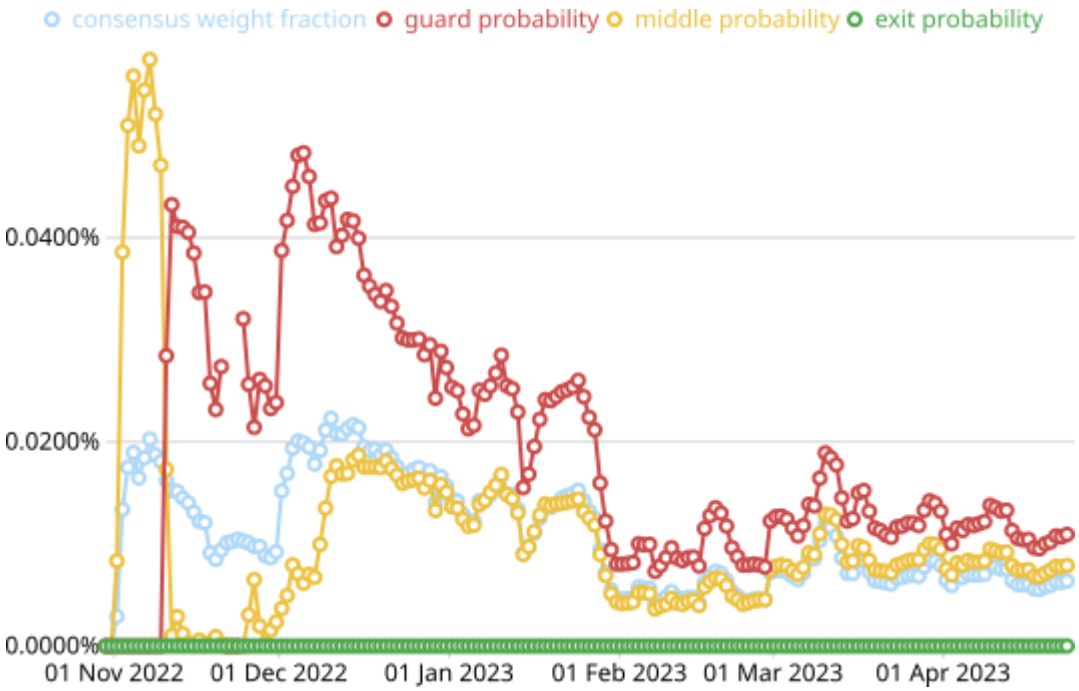


Kuva 5. Kuvakaappaus Tor Metrics -sivustolta palvelimesta anotherlegitrelay (Tor Metrics 2023b)

Kuvassa 5 esitetään välityspalvelimen Tor-verkon osana reitittämän tietoliikenteen määrää kuluneen 6 kuukauden aikana. Tämä kuvaaja kuvaa vain palvelimen tietoliikenteen määrää Tor-verkon osalta, joten tähän kuvaajaan ei sisälly kaikkea palvelimen käsittelemää tietoliikennettä.

Kuvaajan tarjoamaa tietoa voidaan käyttää arvioitaessa palvelimen toimintaa. Kuvaajasta voidaan tulkita, että palvelimen liittyessä osaksi Tor-verkkoa marraskuun alussa vuonna 2022 sen välittämän tietoliikenteen määrä oli korkeimmillaan mittausjakson aikana. Tietoliikenteen määrä myös laski jyrkästi ennen kuun vaihtumista joulukuuksi. Tammikuussa puolestaan tapahtui jyrkkä pudotus.

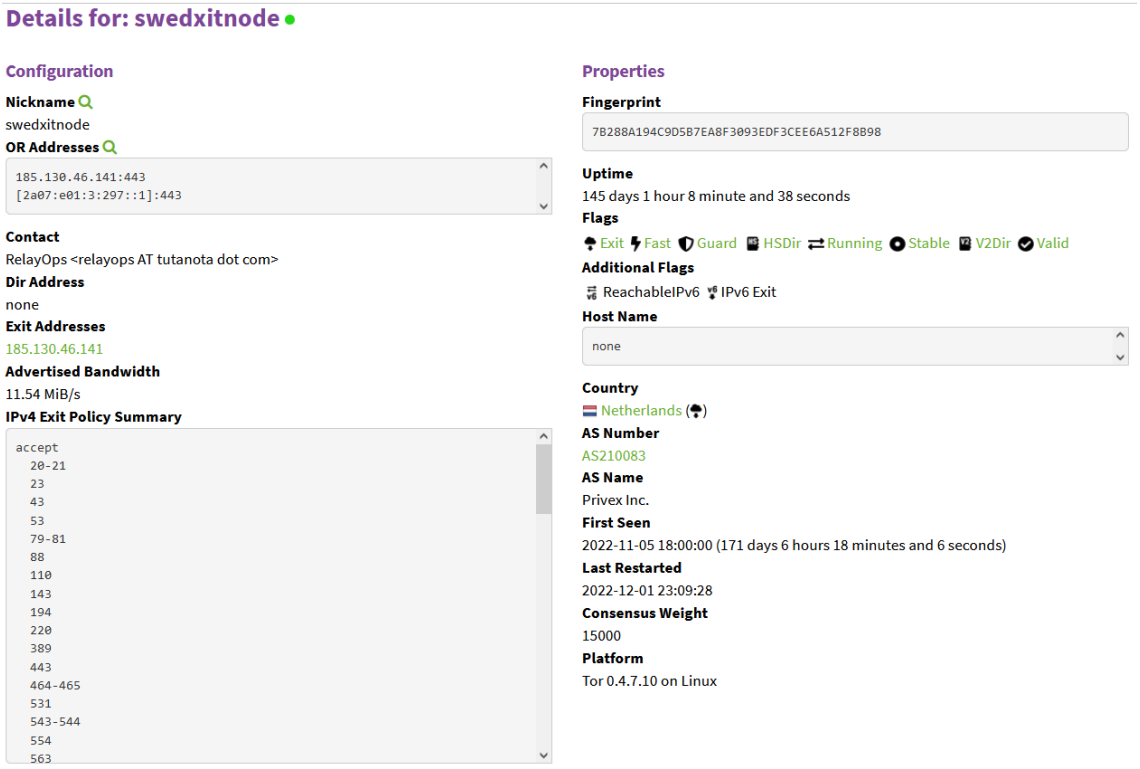
Tor Metrics tarjoaa kuvaajan liittyen myös niin kutsuttuun Consensus Weight -arvoon.



Kuva 6. Tor metrics sivuston kuvaaja välityspalvelimen Consensus Weight -arvon muutoksesta ajassa. (Tor Metrics 2023b)

Kuvassa 6 esitetään Tor-välityspalvelimen roolin muodostumista osana Tor-verkkoa. Uuden välityspalvelimen liittyessä osaksi verkkoa, sen toimintaa arvioidaan reitittämällä sen kautta jatkuvasti suurempia määriä tietoliikennettä. Tämän voi havaita aiemmasta kuviosta. Palvelimen vakautta ja luotettavuutta arvioidaan sen suorituskyvyn sekä yhtäjakoisen toiminta-ajan mukaan, ja tämän jälkeen sille annetaan ominaisuuksiensa perusteella sopiva rooli joko tulo- tai keskipalvelimena. (Tor Blog 2013). Jos palvelin on konfiguroitu avainsanalla `ExitRelay 1`, tätä prosessia ei käydä läpi, vaan palvelimesta tulee lähtöpalvelin. Koska ’anotherlegitrelay’ on konfiguroitu avainsanalla `ExitRelay 0`, siitä ei voi tulla lähtöpalvelin, jolloin myös sen ’exit probability’ -arvo kuvaajassa on jatkuvasti 0 %.

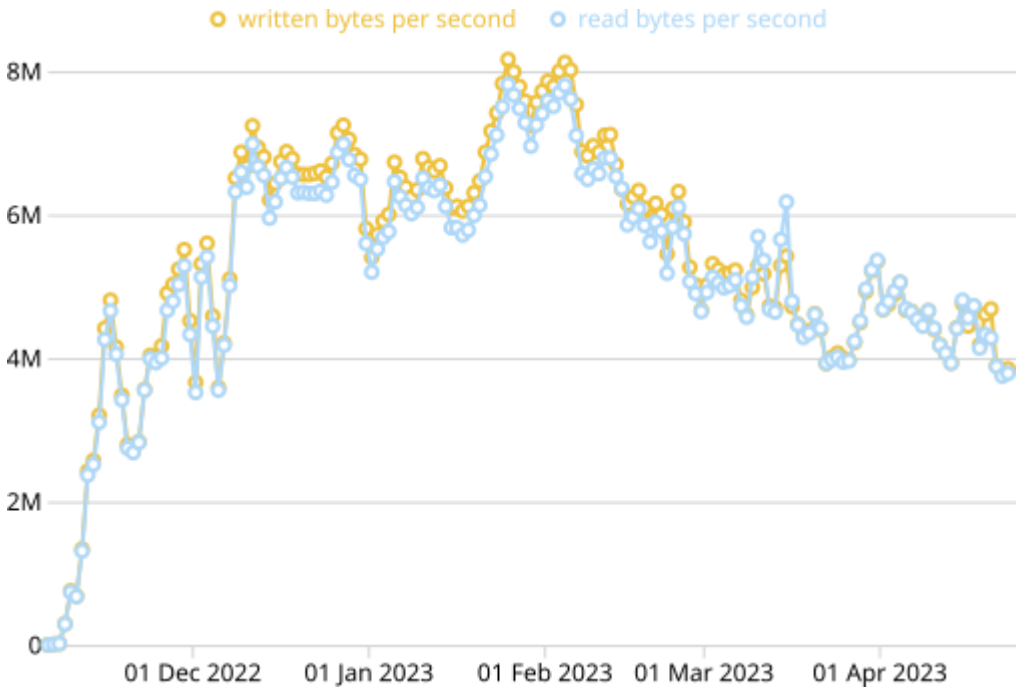
Edellämainitut sivuston tarjoamat tiedot riippuvat tietysti palvelimen roolista. Lähtöpalvelimeni osalta sivusto tarjoaa seuraavanlaisia tietoja.



Kuva 7. Kuvakaappaus lähtöpalvelimen tiedoista Tor Metrics -sivustolla. (Tor Metrics 2023c).

Kuvassa 7 voidaan nähdä lähtöpalvelimen ero muihin välityspalvelintyyppeihin. Koska kyseessä on lähtöpalvelin, sille on määritelty tietoliikenteen porttikohtaisia sääntöjä palveluntarjoajan sopimusehtojen mukaisesti. Ne on listattu myös palvelimen tiedoissa. Lisäksi palvelin on merkitty myös merkinnöillä ’Exit’, eli kyseessä on lähtöpalvelin.

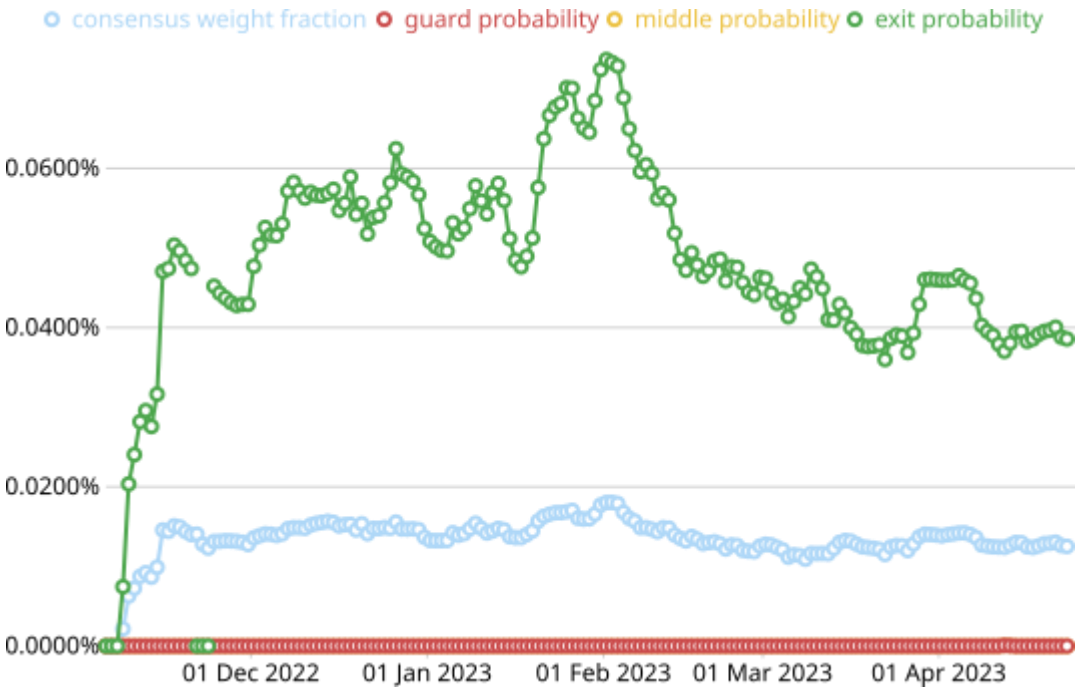
Myös tämän palvelimen välittämän tietoliikenteen määrää esitetään kuvaajan avulla.



Kuva 8. Tor Metrics -sivuston kuvaaja swedxitnode-palvelimen reitittämästä tietoliikenteen määrästä (Tor Metrics 2023c.)

Kuvan 8 mukaan palvelimen tietoliikennemäärät kuluneen kuuden kuukauden osalta poikkeavat suuresti ’anotherlegitrelayn’ määristä vastaavalla ajalla. Tämä selittynee palvelimen roolilla Tor-verkossa.

Roolin muodostumista voidaan myös havainnoida sivuston tarjoamasta kuvaajasta.



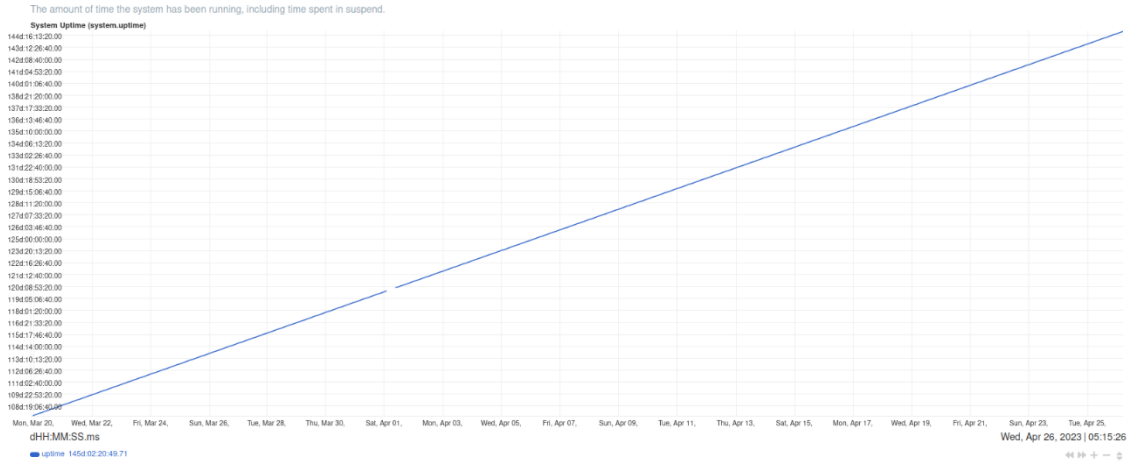
Kuva 9. Lähtöpalvelimen swedxitrelay Consensus Weightin muodostuminen (Tor Metrics 2023c).

Kuvasta 9 voidaan tulkita, että palvelin on aina toiminut lähtöpalvelimena. Se johtuu tietysti siitä, että palvelin on konfiguroitu avainsanalla `ExitRelay 1`.

Netdata

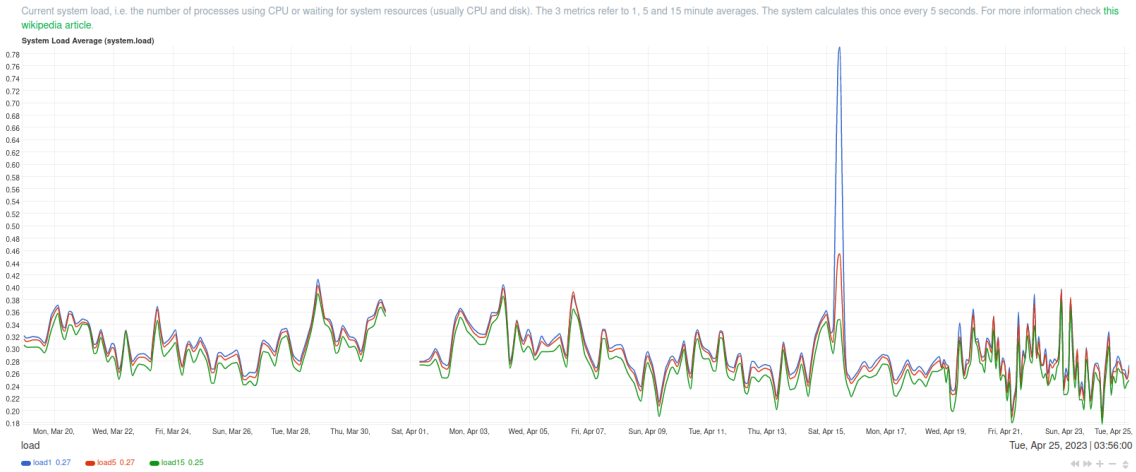
NetData -ohjelmisto kerää, tallentaa sekä visualisoi palvelimen toimintaa kuvaavaa dataa valittujen asetusten mukaisesti. Tätä dataa voidaan käyttää palvelimen tilan ja toimivuuden havainnointiin. Koska Tor Metrics tarjoaa vain rajoitetusti tietoa palvelimen tilasta, NetDatan keräämä tieto täydentää tilannekuvaa.

Esimerkiksi lähtöpalvelimen tilaa kuluneen kuukauden ajalta voidaan havainnoida Netdatan avulla käyttäen hyväksi kerättyä tietoa käynnissäoloajasta, verkkoliikenteestä, prosessorien kuormasta sekä käytetystä muistista.



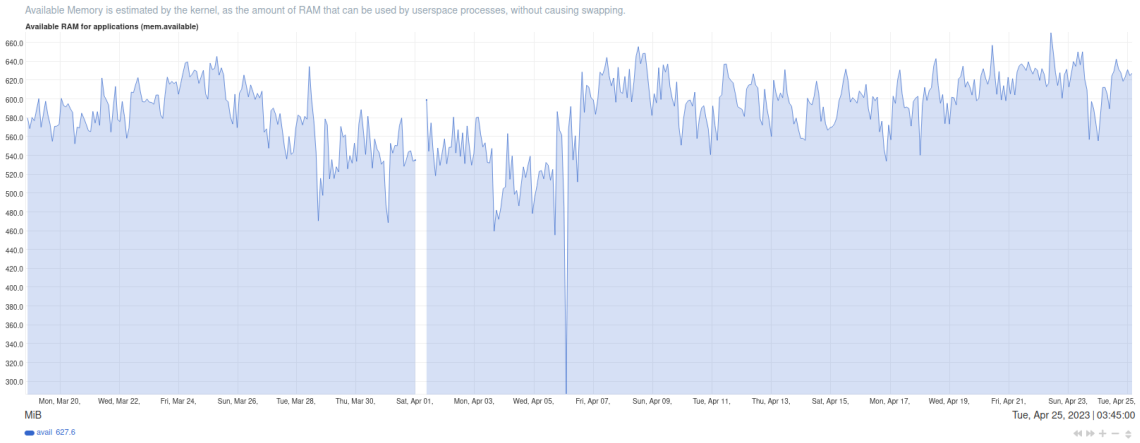
Kuva 10. NetData-ohjelmiston kuvaaja swedxitnode-palvelimen käynnissäoloajasta.

Kuva 10 kuvaa palvelimen käynnissäoloajan kumulatiivista kertymistä noin kuukauden ajalta. Maaliskuun 31. päivän osalta tiedot eivät ole täydellisia ohjelmiston toimintahäiriön vuoksi. Palvelin on on tätä kirjoittaessa ollut yhtäjaksoisesti käynnissä 141 päivää.



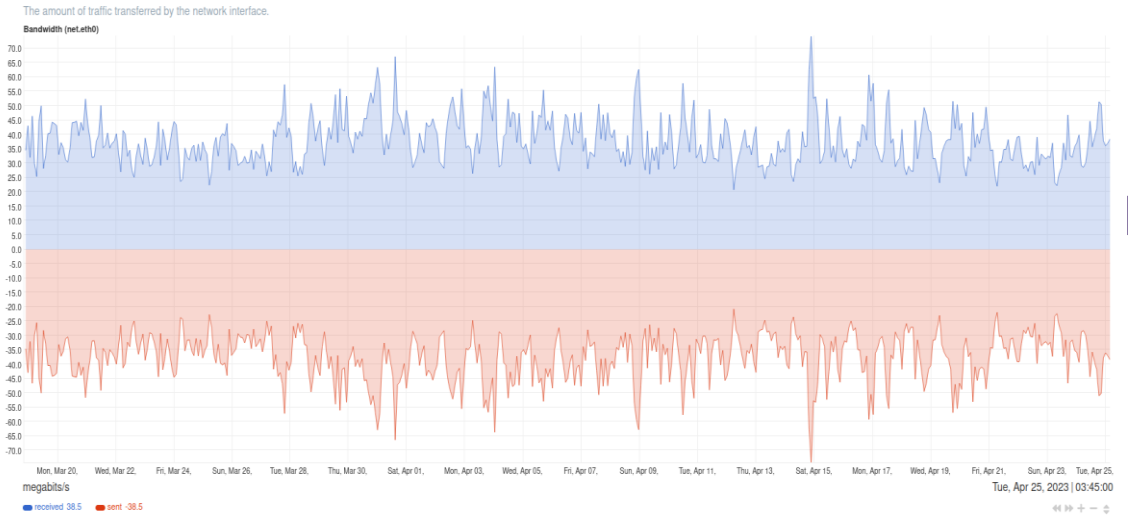
Kuva 11. NetData -ohjelmiston kuvaaja palvelinkuormasta.

Kuvassa havainnollisestaan lähtöpalvelimen kuormitusta eli sitä prosessien määrää, jotka hyödyttävät järjestelmän resursseja, kuten prosessoreja tai kiintolevyjä. Mitä suurempi y-akselin arvo on, sitä suurempaa järjestelmään kohdistuva kuormitus on.



Kuva 12. NetData-ohjelmiston tuottama kuvaaja lähtöpalvelimen keskusmuistin käyttöasteesta.

Kuvassa 12 havainnollistetaan lähtöpalvelimen käytettävissä olevan vapaan keskusmuistin määrää. Käytettävissä olevan muistin määrä kertoo osaltaan siitä, onko järjestelmän muistin määrä riittävällä tasolla käyttötarkoitukseensa nähden. Kuvasta voidaan päätellä, että muistia on tarpeeseen nähden varsin vähän. Y-akselin arvo ilmaisee vapaan muistin määrää megatavuina. Kuvaajasta voi arvioida että vapaan muistin määrä on yleensä 400 - 650 megatavun välillä. Tästä johtuen voidaan olettaa, että järjestelmässä voi ilmetä vakauteen liittyviä ongelmia. Varmuuden saamiseksi tarvittaisiin kuitenkin myös muita tietoja.



Kuva 13. Kuvaaja lähtöpalvelimen reitittämästä tietoliikenteestä.

NetData mahdollistaa myös verkkoliikenteen määrän visualisoinnin. Kuvassa 13 esitetään lähtöpalvelimen verkkoadapterin välittämää tietoliikennettä kuukauden ajalta.

Lokitiedostot

Tor-ohjelmisto tallentaa oletusarvoisesti lokitiedostonsa hakemistoon `/var/log/tor`. Nämä tiedostot tallentavat ohjelmistoon liittyvät tiedot, kuten erilaiset virhetilanteet tai uudelleenkäynnistymiset. Lisäksi ohjelmistosta on mahdollista kerätä reaaliaikaista tietoa `MetricsPort` -ominaisuuden kautta. `MetricsPort` aktivoidaan kirjoittamalla `torrc` -tiedostoon seuraavat rivit:

```
MetricsPort 127.0.0.1:9035
MetricsPortPolicy accept 127.0.0.1
```

Tämän jälkeen tiedot voidaan noutaa komennolla

```
curl http://127.0.0.1:9035/metrics
```

Hakemistossa `/var/log` sijaitsevat myös Debian Linux -käyttöjärjestelmän lokitiedostot, joihin kirjoitetaan käyttöjärjestelmän toimintaan liittyvät tapahtumat.

5.2 Havaintoja välityspalvelinten toiminnasta

Seurasin noin puolen vuoden ajan palvelinten toimintaa käyttäen apunani edellämainittuja tilannetiedon lähteitä. Pyrin kiinnittämään huomiota etenkin palvelinten vakauteen eli siihen, kuinka virheettömästi sekä yhtäjaksoisesti palvelimet toimivat. Kiinnitin huomiota myös palvelinten suorituskykyyn eli siihen, paljonko palvelimet kykenivät reitittämään tietoliikennettä osana Tor-verkkoa.

En pyrkinyt juurikaan etsimään keinoja käyttöjärjestelmän, sen komponenttien tai välityspalvelinten toiminnan optimointiin tai muokkaamiseen. Tarkoitukseni oli selvittää, minkälaiseen lopputulokseen voidaan päästä, mikäli noudatetaan Tor Projectin sivustollaan tarjoamia ohjeita ja suosituksia konfiguroinnin sekä laitteistokokoonpanon osalta. Pyrin seuraamaan näitä ohjeita ja suosituksia mahdollisimman tarkasti, jotta saavutettu lopputulos vastaisi ohjeita ja suosituksia. Näin ollen lopputulosta voi mielestäni pitää sellaisena, että siitä voidaan johtaa johtopäätökset ohjeistuksen mahdollisista puutteista, mutta myös ansioista.

5.2.1 Välityspalvelinten vakaudesta

Keväällä 2023 välityspalvelin legitrelayfi on ollut yhtäjaksoisesti toiminnassa 170 vuorokautta, anotherlegitrelay 115 vuorokautta ja swedxitnode 145 vuorokautta. Palvelinten siirtoteho Tor metricsin mukaan on melko samankaltainen. Legitrelayfin osalta se on 12,31 MB/s, anotherlegitrelayn 12,4 MB/s ja swedxitnoden 12,1 MB/s. (Tor Metrics 2023).

Arvioitaessa palvelinten tämänhetkistä suorituskykyä ja vakautta, voidaan mielestäni todeta, että palvelimet toimivat asianmukaisesti. Noin 12,6 MB/s jatkuva reititysteho koostuu sekä vastaanotetusta että lähetetystä tietoliikenteestä, joten pidän mitattua arvoa jopa yllättävän hyvänä.

Tämä siksi, että palvelinten on itse reitityksen lisäksi myös käsiteltävä tietoliikenteeseen liittyvää kerroksellista salausta. Tor Metrics -sivusto antaa kullekin välityspalvelimelle merkinnät ’Stable’ ja ’Fast’, joten myös Tor Projectin arviointikriteeristön mukaan palvelimet toimivat nopeasti ja vakaasti.

Perustettaessa välityspalvelimia tilanne oli toisenlainen. Palvelimet olivat varsin epävakaita, ja ne käynnistyivät usein uudelleen. Tor-ohjelmisto kirjoitti usein lokitiedostoonsa `/var/log/tor/notices` varoituksia, kuten:

```
Nov 12 06:29:42.000 [warn] Your computer is too slow to handle this
many circuit creation requests! Please consider using the
MaxAdvertisedBandwidth config option or choosing a more restricted
exit policy. [187126 similar message(s) suppressed in last 60 seconds]
```

```
Nov 12 07:21:37.000 [notice] General overload -> Ntor dropped
(3123044) fraction 47.1795% is above threshold of 0.5000%
```

Tämänkaltaiset viestit johtuivat havaintoni mukaan usein siitä, että käytettävissä oleva RAM-muisti sekä swap-välimuisti olivat kokonaisuudessaan käytössä. Koska tarve muistille oli suurempaa kuin käytettävissä oleva muisti, Tor-ohjelmisto käynnistettiin automaattisesti uudelleen käyttöjärjestelmän toimesta. Tätä tapahtui kaikkien kolmen palvelimen osalta usein.

CreaNovalta ostetun palvelimen osalta tätä tapahtui hyvin usein, ja tarkemmin syytä selvittäessäni kävi ilmi, että palvelimelle ei oltu osioitu swap-muistitilaa lainkaan. Tyypillisesti swap-tila osioidaan käyttöjärjestelmän asennuksen yhteydessä, mutta näin ei oltu toimittu. Loin palvelimelle 2 GB suuruisen swapfile-tiedoston, joka toimii swap-muistitilana käyttöjärjestelmälle. Tämä vakautti myös Tor-välityspalvelimen toimintaa.

Voidaan siis sanoa, että 1-2 GB RAM-muistia on liian vähän, mikäli palvelimen tietoliikennekapasiteetti palveluntarjoajan määritelmän mukaan on 1 GB/s. Tor-ohjelmisto vaatii tällaisessa olosuhteessa paljon muistia toimiakseen oikein, ja muistin täyttyessä ohjelma käynnistetään uudelleen.

Toisaalta Tor-verkko toimii siten, että uuden palvelimen liittyessä siihen tätä uutta palvelinta testataan. Kun palvelin on ollut osa verkkoa pidempään, eli joitain kuukausia, sen toiminta vakautuu. Tämä johtuu siitä, että palvelimelle reititetään tietoliikennettä nopeudella, jolla palvelin vielä kykenee toimimaan oikein ja vakaasti. Näin ollen voidaan myös päätellä, että palvelinten toimintaan riittää myös noin 1 GB RAM-muistia, mutta tätä voidaan pitää ehdottomasti miniminä.

Kiintolevytila tai kiintolevyn toiminta yleensä ei ole aiheuttanut mitään huomioitavaa koko tarkkailujakson aikana. En ole havainnut mitään, mikä viittaisi siihen, että kiintolevyn kapasiteetti olisi riittämätöntä tai että kiintolevy toimisi muulla tavoin epätoivottavasti. Tämä koskee kaikkia kolmea palvelinta.

Prosessorikapasiteetti ei ole myöskään osoittautunut riittämättömästi. Tor ohjelmistona käyttää vain yhtä prosessoriydintä, joka on itse ohjelmstoon liittyvä ominaisuus ja johon ylläpitäjä ei sinänsä voi konfiguroinnilla vaikuttaa. Tämä yllättävä ohjelmistoon liittyvä rajoite estää hyödyntämästä useampaa prosessoriydintä. Tästä johtuen prosessointiteho ei muodostanut ongelmia kokeilujakson aikana, sillä jokaisessa palvelimessa oli useampi prosessoriydin.

Jokainen palvelin sijaitsee palvelinsalissa, jossa ne on liitetty tietoverkkoon 1 Gb/s -siirtotehoisella liitännällä. Koska kukin palvelin kuluttaa jatkuvasti vain noin 12 MB/s siirtokapasiteettia, voidaan arvioida, että 1 Gb/s on riittävästi. 1 Gb/s mahdollistaisi 100 MB/s nopeudella tapahtuvan jatkuvan tiedonsiirron, mutta palvelinten muut komponentit eivät tätä mahdollista. Uskoisin, että tämänkaltaiset siirtonopeudet vaatisivat ensinnäkin merkittävästi suuremman määrän käytettävissä olevaa RAM-muistia, swapia ja mahdollisesti tehokkaamman prosessoriytimen. En ole tätä kuitenkaan kokeellisesti todennut tämän kokeilujakson aikana, mutta pidän tätä todennäköisenä.

Muita havaintoja

Minulle ei ole toimitettu lainkaan sähköpostia liittyen palvelinteni toimintaan tai niiden välittämään tietoliikenteeseen. Kukaan palveluntarjoajista ei ole viestinyt minulle, että palvelimeni toimisivat epätarkoituksenmukaisesti, tai että palvelimeni kautta olisi reititetty tietoliikennettä, joka vaatisi minulta toimenpiteitä. En ole esimerkiksi saanut lainkaan pyyntöjä suodattaa tietoliikennettä tai pyyntöä keskeyttää palvelinteni toimintaa. Olen avannut viesintää varten sähköpostitilin Tutanota -palveluntarjoajalta, ja maininnut tämän tilin, relayops@tutanota.com myös `torrc` -tiedostoissa, mutta sähköpostiviestejä ei ole saapunut.

Olen käyttänyt palvelimien vuokrasopimuksia tehdessäni ja palveluntarjojajien kanssa viestiessä oppilaitokseni minulle luovuttamaa sähköpostitiliä, mutta sinne ei ole laskujen lisäksi toimitettu muuta palvelimiin liittyvää.

Privexin kanssa tekemäni sopimuksen mukaan he käsittelevät mahdolliset väärinkäytöksistä johtuvat yhteydenotot, jos käytän `Reduced Exit Policy` -suodatusta. Tämä lienee syy sille, miksei palvelimeen liittyviä sähköposteja ole tullut.

Ylläpitäjän vastuusta

Tor Project suosittelee välityspalvelimen konfigurointiin liittyvissä ohjeissaan, että palvelimen ylläpitäjä tutustuisi paikalliseen lainsäädäntöön etenkin, jos tarkoitus on ylläpitää lähtöpalvelinta. Tämä johtuu siitä, että lähtöpalvelimen kautta reitittyvä tietoliikenne saattaa joissain tapauksissa liittyä vaikkapa tietomurron yritykseen, sensuroidun aineiston hankintaan tai muuhun paikallisen lainsäädännön mukaan laittomaan toimintaan. (Tor Project 2023).

Verkkopalvelujen sekä palvelinten ylläpitäjän vastuusta sekä verkkolaitteiden toiminnasta säädetään Laissa sähköisen viestinnän palveluista. (Laki sähköisen viestinnän palveluista 7.11.2014/917.)

Esimerkiksi Lain sähköisen viestinnän palveluista 21:172 antaa viranomaiselle oikeuden muuttaa palvelimelta reititettävää tietoliikennettä tai estää sen. Lain 29:244 taas antaa viranomaiselle oikeuden esimerkiksi poistaa palvelimen tai verkkolaitteen tietoverkosta, mikäli laite on tietoverkon kriittisessä osassa ja aiheuttaa esimerkiksi vakavaa varaa kansalliselle turvallisuudelle tai sitä voidaan käyttää esimerkiksi tiedusteluun. Lisäksi lain 33:272 velvoittaa ylläpitäjää puuttumaan tai estämään palvelimen kautta reitittyvän tietoliikenteen, jos on tiedossa, että kyseessä on rikollinen toiminta.

Tätä opinnäytetyötä varten tekemissäni tutkimuksissa ei ole ilmennyt tapauksia, joissa henkilö olisi tuomittu rikoksesta siksi, että hän olisi ylläpitänyt nimenomaan välityspalvelinta. En ole myöskään löytänyt yhtäkään tapausta, jossa poliisi tai muu viranomainen olisi vaatinut ylläpitäjää keskeyttämään välityspalvelimensa toiminnan.

Tor-verkossa liittyvän palvelun ylläpidosta on annettu Korkeimmassa oikeudessa ennakkopäätös. (KKO 2022:11.) Tässä tapauksessa oli kyse huumausainerikoksista sekä avunannosta niihin tilanteessa jossa syytettynä ollut mies oli ylläpitänyt Tor-verkon piilopalvelua. Miehen käytiin kauppaa huumausaineilla, ja syytettynä olleen miehe rikosvastuuta punnittiin myös ennakkopäätöksellä. Korkein oikeus katsoi, että mies oli rikosvastuussa ja syyllistyi myös avunantoon, sillä hän ylläpiti tätä keskustelualuetta ja myös aktiivisesti seurasi keskusteluja ja ajoittain myös poisti sääntöjen vastaisia viestejä. Tämä tapaus ei sinänsä suoraan rinnastu välityspalvelimen ylläpitoon. Välityspalvelimen ylläpitäjä ei voi aktiivisesti seurata palvelimensa kautta kulkevaa viestiliikennettä tai sen sisältöä.

Käsitykseni mukaan välityspalvelimen ylläpitäjällä on lainsäädäntömme mukaan velvollisuus varmistua siitä, että hänen palvelimensa ei aiheuta häiriötä tietoverkkojen toiminnalle tai muiden tietoverkon käyttäjien viestinnälle. Lisäksi vastuisiin kuuluu olla asentamatta palvelua tai verkkolaitetta jonka tarkoitus on vaarantaa kansallinen turvallisuus tai toimia välineenä laittomalle tiedustelutoiminnalle. Palvelin voidaan myös tietyin edellytyksin määrätä suljettavaksi.

6 Pohdintaa

Tämän opinnäytetyön tarkoitus oli tutkia Tor-välityspalvelinten toimintaa ja ylläpitoa. Opinnäytteessä yhdistyy moni minua kiinnostava aihe, kuten Linux-käyttöjärjestelmä, palvelimet, virtualisointi ja tietoverkot. Lisäksi aihevalintaa ohjasi havainto siitä, että Tor-välityspalvelimista ei ole juurikaan kirjoitettu suomeksi. Aiheesta ei ole tiettävästi kirjoitettu ainuttakaan ammattikorkeakoulun opinnäytetyötä ennen tätä.

Opinnäytetyön tarkoitus oli havainnollistaa työvaiheet, jotka liittyvät palvelinten konfigurointiin aina palveluntarjoajan etsinnästä palvelimen toiminnan tarkkailuun. Osa työstä käsitteli myös kysymystä siitä, ovatko annetut ohjeet sekä laitekokoonpanoa koskevat suositukset sillä tasolla, että niitä seuraamalla voi saavuttaa hyvän lopputuloksen. Työssä huomioidaan myös palvelinten ylläpitoon liittyvät kustannukset.

Voidaan myös todeta, että Tor Projectin tuottamat ohjeet ja suositukset ovat sellaisia, että niitä seuraamalla voidaan saada aikaan toimiva välityspalvelin. Ohjeet ovat kuitenkin luonteeltaan sellaisia, että niiden seuraaminen vaatinee hyvät lähtötiedot Linux-käyttöjärjestelmästä sekä Internetistä. Ohjeissa ei juurikaan paneuduta esimerkiksi verkkotunnuksiin, DNS-järjestelmän toimintaan tai Linux-käyttöjärjestelmään. Kaikkia näitä aiheita olisi kuitenkin hyvä tuntea jo ennen kuin ryhtyy ohjeita seuraamaan, sillä moni ohjeiden kohdan ymmärrys riippuu aiheiden hyvästä ymmärryksestä. Aloittelijalle Tor Projectin ohjeet voivat siis olla liiankin haastavia.

Lähteet

Dingledine, R., Mathewson, N & Syverson, P. 2019. Tor: The Second-Generation Onion Router. Viitattu 20.4.2023. https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.html

Rott, J. 2022. Intel® Advanced Encryption Standard Instructions (AES-NI). Viitattu 13.5.2023. https://www.intel.com/content/www/us/en/developer/articles/technical/advanced-encryption-standard-instructions-aes-ni.htm

KKO:2022:11. Huumausainerikos - Törkeä huumausainerikos Rangaistuksen määrääminen - Rangaistuksen mittaaminen. R2020/792. 24.2.2022.

Laki sähköisen viestinnän palveluista 7.11.2014/917

Njal.la 2023. About Njalla. Viitattu 13.5.2023. https://njal.la/about/

Ollila, M. 2016. Tor-verkko. Opinnäytetyö (AMK). Tietotekniikka. Riihimäki. Viitattu 20.4.2023. http://www.theseus.fi/handle/10024/120440.

Platzer, F., Schäfer, M. and Steinebach, M. 2021. Critical Traffic Analysis on the Tor Network. Journal of Cyber Security and Mobility. River Publishers. Vol. 10. 133-160.

Theseus. 2023. Theseus - ammattikorkeakoulujen opinnäytetyöt ja julkaisut verkossa. Viitattu 13.5.2023. https://www.theseus.fi/

Tor Blog. 2013. The Lifecycle of a new relay. Viitattu 20.4.2023. https://blog.torproject.org/lifecycle-of-a-new-relay/

Tor License. 2019. Viitattu 15.5.2023. https://gitweb.torproject.org/tor.git/plain/LICENSE

Tor Metrics. 2023. Viitattu 15.5.2023. https://metrics.torproject.org/

Tor metrics. 2023a. Servers. Tor Metrics-sivusto. Viitattu 26.4.2023. https://metrics.torproject.org/networksize.html

Tor Metrics. 2023b. Relay Search. Relay Search -sivuston koontisivu anotherlegitrelay-palvelimesta. Viitattu 26.4.2023. https://metrics.torproject.org/rs.html#details/B92EA9BCE0ADF008C8EF373A384E1FEC064B6895

Tor Metrics 2023c. Relay Search. Relay Search.sivuston koontisivu swedxitnodesta. Viitattu 26.4.2023. https://metrics.torproject.org/rs.html#details/7B288A194C9D5B7EA8F3093EDF3CEE6A512F8B98

Tor Project. 2023. Relay Operations. Tor Community-sivusto. Viitattu 26.4.2023. https://community.torproject.org/relay/relays-requirements/

Tor Project. 2023a. About Tor Project: History. Viitattu 20.4.2023. https://www.torproject.org/about/history/

Tor Project. 2023b. Dir-spec. Viitattu 20.4.2023. https://gitlab.torproject.org/tpo/core/torspec/-/blob/main/dir-spec.txt

Wikipedia. Väsytyshyökkäys. Viitattu 10.5.2023 https://fi.wikipedia.org/wiki/V%C3%A4sytyshy%C3%B6kk%C3%A4ys

Torrc-konfigurointitiedosto

```
## Configuration file for a typical Tor user
## Last updated 9 October 2013 for Tor 0.2.5.2-alpha.
## (may or may not work for much older or much newer versions of Tor.)
##
## Lines that begin with "## " try to explain what's going on. Lines
## that begin with just "#" are disabled commands: you can enable them
## by removing the "#" symbol.
##
## See 'man tor', or https://www.torproject.org/docs/tor-manual.html,
## for more options you can use in this file.
##
## Tor will look for this file in various places based on your
platform:
## https://www.torproject.org/docs/faq#torrc


## Tor opens a socks proxy on port 9050 by default -- even if you
don't
## configure one below. Set "SocksPort 0" if you plan to run Tor only
## as a relay, and not make any local application connections
yourself.
SocksPort 0 # Default: Bind to localhost:9050 for local connections.
#SocksPort 192.168.0.1:9100 # Bind to this address:port too.


## Entry policies to allow/deny SOCKS requests based on IP address.
## First entry that matches wins. If no SocksPolicy is set, we accept
## all (and only) requests that reach a SocksPort. Untrusted users who
## can access your SocksPort may be able to learn about the
connections
## you make.
#SocksPolicy accept 192.168.0.0/16
#SocksPolicy reject *
```

```
## Logs go to stdout at level "notice" unless redirected by something

## else, like one of the below lines. You can have as many Log lines
as

## you want.

##

## We advise using "notice" in most cases, since anything more verbose

## may provide sensitive information to an attacker who obtains the
logs.

##

## Send all messages of level 'notice' or higher to
/var/log/tor/notices.log

Log notice file /var/log/tor/notices.log

## Send every possible message to /var/log/tor/debug.log

#Log debug file /var/log/tor/debug.log

## Use the system log instead of Tor's logfiles

#Log notice syslog

## To send all messages to stderr:

#Log debug stderr


## Uncomment this to start the process in the background... or use

## --runasdaemon 1 on the command line. This is ignored on Windows;

## see the FAQ entry if you want Tor to run as an NT service.

RunAsDaemon 1


## The directory for keeping all the keys/etc. By default, we store

## things in $HOME/.tor on Unix, and in Application Data\tor on
Windows.

#DataDirectory /var/lib/tor


## The port on which Tor will listen for local connections from Tor

## controller applications, as documented in control-spec.txt.

#ControlPort 9051
```

```
## If you enable the controlport, be sure to enable one of these
## authentication methods, to prevent attackers from accessing it.
#HashedControlPassword
16:872860B76453A77D60CA2BB8C1A7042072093276A3D701AD684053EC4C
#CookieAuthentication 1

############### This section is just for location-hidden services ###

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

#HiddenServiceDir /var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22

################ This section is just for relays #####################
#
## See https://www.torproject.org/docs/tor-doc-relay for details.

## Required: what port to advertise for incoming Tor connections.
ORPort 443
## If you want to listen on a port other than the one advertised in
## ORPort (e.g. to advertise 443 but bind to 9090), you can do it as
## follows.  You'll need to do ipchains or other port forwarding
## yourself to make this work.
```

```
#ORPort 443 NoListen

#ORPort 127.0.0.1:9090 NoAdvertise


## The IP address or full DNS name for incoming connections to your

## relay. Leave commented out and Tor will guess.

#Address noname.example.com


## If you have multiple network interfaces, you can specify one for

## outgoing traffic to use.

# OutboundBindAddress 10.0.0.5


## A handle for your relay, so people don't have to refer to it by
key.

Nickname legitrelayfi


## Define these to limit how much relayed traffic you will allow. Your

## own traffic is still unthrottled. Note that RelayBandwidthRate must

## be at least 20 KB.

## Note that units for these config options are bytes per second, not
bits

## per second, and that prefixes are binary prefixes, i.e. 2^10, 2^20,
etc.

#RelayBandwidthRate 100 KB  # Throttle traffic to 100KB/s (800Kbps)

#RelayBandwidthBurst 200 KB # But allow bursts up to 200KB/s
(1600Kbps)


## Use these to restrict the maximum traffic per day, week, or month.

## Note that this threshold applies separately to sent and received
bytes,

## not to their sum: setting "4 GB" may allow up to 8 GB total before

## hibernating.

##

## Set a maximum of 4 gigabytes each way per period.

#AccountingMax 4 GB
```

```
## Each period starts daily at midnight (AccountingMax is per day)
#AccountingStart day 00:00
## Each period starts on the 3rd of the month at 15:00 (AccountingMax
## is per month)
#AccountingStart month 3 15:00

## Administrative contact information for this relay or bridge. This
line
## can be used to contact you if your relay or bridge is misconfigured
or
## something else goes wrong. Note that we archive and publish all
## descriptors containing these lines and that Google indexes them, so
## spammers might also collect them. You may want to obscure the fact
that
## it's an email address and/or generate a new address for this
purpose.
ContactInfo relayops AT tutanota DOT com
## You might also include your PGP or GPG fingerprint if you have one:
#ContactInfo 0xFFFFFFFF Random Person <nobody AT example dot com>

## Uncomment this to mirror directory information for others. Please
do
## if you have enough bandwidth.
DirPort 9030 # what port to advertise for directory connections
## If you want to listen on a port other than the one advertised in
## DirPort (e.g. to advertise 80 but bind to 9091), you can do it as
## follows.  below too. You'll need to do ipchains or other port
## forwarding yourself to make this work.
#DirPort 80 NoListen
#DirPort 127.0.0.1:9091 NoAdvertise
## Uncomment to return an arbitrary blob of html on your DirPort. Now
you
## can explain what Tor is if anybody wonders why your IP address is
## contacting them. See contrib/tor-exit-notice.html in Tor's source
```

```
## distribution for a sample.

#DirPortFrontPage /etc/tor/tor-exit-notice.html


## Uncomment this if you run more than one Tor relay, and add the
identity

## key fingerprint of each Tor relay you control, even if they're on

## different networks. You declare it here so Tor clients can avoid

## using more than one of your relays in a single circuit. See

## https://www.torproject.org/docs/faq#MultipleRelays

## However, you should never include a bridge's fingerprint here, as
it would

## break its concealability and potentionally reveal its IP/TCP
address.

MyFamily
B92EA9BCE0ADF008C8EF373A384E1FEC064B6895,F852A11B7725DC294DF7063B590C5
82883B1310F,7B288A194C9D5B7EA8F3093EDF3CEE6A512F8B98


## A comma-separated list of exit policies. They're considered first

## to last, and the first match wins. If you want to _replace_

## the default exit policy, end this with either a reject *:* or an

## accept *:*. Otherwise, you're _augmenting_ (prepending to) the

## default exit policy. Leave commented to just use the default, which
is

## described in the man page or at

## https://www.torproject.org/documentation.html

##

## Look at https://www.torproject.org/faq-abuse.html#TypicalAbuses

## for issues you might encounter if you use the default exit policy.

ExitRelay   0

## If certain IPs and ports are blocked externally, e.g. by your
firewall,

## you should update your exit policy to reflect this -- otherwise Tor

## users will be told that those destinations are down.

##

## For security, by default Tor rejects connections to private (local)
```

```
## networks, including to your public IP address. See the man page
entry

## for ExitPolicyRejectPrivate if you want to allow "exit enclaving".

##

#ExitPolicy accept *:6660-6667,reject *:* # allow irc ports but no
more

#ExitPolicy accept *:119 # accept nntp as well as default exit policy

#ExitPolicy reject *:* # no exits allowed


## Bridge relays (or "bridges") are Tor relays that aren't listed in
the

## main directory. Since there is no complete public list of them,
even an

## ISP that filters connections to all the known Tor relays probably

## won't be able to block all the bridges. Also, websites won't treat
you

## differently because they won't know you're running Tor. If you can

## be a real relay, please do; but if not, be a bridge!

#BridgeRelay 1

## By default, Tor will advertise your bridge to users through various

## mechanisms like https://bridges.torproject.org/. If you want to run

## a private bridge, for example because you'll give out your bridge

## address manually to your friends, uncomment this line:

#PublishServerDescriptor 0
```

¶.....Osan vaihto (seuraava sivu).....

Lähtöpalvelimen torrc-konfigurointitiedosto

```
## Configuration file for a typical Tor user
## Last updated 9 October 2013 for Tor 0.2.5.2-alpha.
## (may or may not work for much older or much newer versions of Tor.)
##
## Lines that begin with "## " try to explain what's going on. Lines
## that begin with just "#" are disabled commands: you can enable them
## by removing the "#" symbol.
##
## See 'man tor', or https://www.torproject.org/docs/tor-manual.html,
## for more options you can use in this file.
##
## Tor will look for this file in various places based on your
platform:
## https://www.torproject.org/docs/faq#torrc
MetricsPort 127.0.0.1:9035
MetricsPortPolicy accept 127.0.0.1



## Tor opens a socks proxy on port 9050 by default -- even if you
don't
## configure one below. Set "SocksPort 0" if you plan to run Tor only
## as a relay, and not make any local application connections
yourself.
SocksPort 0# Default: Bind to localhost:9050 for local connections.
#SocksPort 192.168.0.1:9100 # Bind to this address:port too.


## Entry policies to allow/deny SOCKS requests based on IP address.
## First entry that matches wins. If no SocksPolicy is set, we accept
## all (and only) requests that reach a SocksPort. Untrusted users who
## can access your SocksPort may be able to learn about the
connections
```

```
## you make.

#SocksPolicy accept 192.168.0.0/16

#SocksPolicy reject *


## Logs go to stdout at level "notice" unless redirected by something

## else, like one of the below lines. You can have as many Log lines
as

## you want.

##

## We advise using "notice" in most cases, since anything more verbose

## may provide sensitive information to an attacker who obtains the
logs.

##

## Send all messages of level 'notice' or higher to
/var/log/tor/notices.log

Log notice file /var/log/tor/notices.log

## Send every possible message to /var/log/tor/debug.log

#Log debug file /var/log/tor/debug.log

## Use the system log instead of Tor's logfiles

#Log notice syslog

## To send all messages to stderr:

#Log debug stderr


## Uncomment this to start the process in the background... or use

## --runasdaemon 1 on the command line. This is ignored on Windows;

## see the FAQ entry if you want Tor to run as an NT service.

RunAsDaemon 1


## The directory for keeping all the keys/etc. By default, we store

## things in $HOME/.tor on Unix, and in Application Data\tor on
Windows.

#DataDirectory /var/lib/tor
```

```
## The port on which Tor will listen for local connections from Tor
## controller applications, as documented in control-spec.txt.
#ControlPort 9051
## If you enable the controlport, be sure to enable one of these
## authentication methods, to prevent attackers from accessing it.
#HashedControlPassword
16:872860B76453A77D60CA2BB8C1A7042072093276A3D701AD684053EC4C
#CookieAuthentication 1

############### This section is just for location-hidden services ###

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

#HiddenServiceDir /var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22

################ This section is just for relays #####################
#
## See https://www.torproject.org/docs/tor-doc-relay for details.

## Required: what port to advertise for incoming Tor connections.
ORPort 443
ORPort [2a07:e01:3:297::1]:443
```

```
## If you want to listen on a port other than the one advertised in
## ORPort (e.g. to advertise 443 but bind to 9090), you can do it as
## follows.  You'll need to do ipchains or other port forwarding
## yourself to make this work.
#ORPort 443 NoListen
#ORPort 127.0.0.1:9090 NoAdvertise

## The IP address or full DNS name for incoming connections to your
## relay. Leave commented out and Tor will guess.
Address swedxitnode.torexitnode.fans
IPv6Exit 1

## If you have multiple network interfaces, you can specify one for
## outgoing traffic to use.
# OutboundBindAddress 10.0.0.5

## A handle for your relay, so people don't have to refer to it by
key.
Nickname swedxitnode

## Define these to limit how much relayed traffic you will allow. Your
## own traffic is still unthrottled. Note that RelayBandwidthRate must
## be at least 20 KB.
## Note that units for these config options are bytes per second, not
bits
## per second, and that prefixes are binary prefixes, i.e. 2^10, 2^20,
etc.
#RelayBandwidthRate 100 KB  # Throttle traffic to 100KB/s (800Kbps)
#RelayBandwidthBurst 200 KB # But allow bursts up to 200KB/s
(1600Kbps)

## Use these to restrict the maximum traffic per day, week, or month.
## Note that this threshold applies separately to sent and received
bytes,
```

```
## not to their sum: setting "4 GB" may allow up to 8 GB total before

## hibernating.

##

## Set a maximum of 4 gigabytes each way per period.

#AccountingMax 4 GB

## Each period starts daily at midnight (AccountingMax is per day)

#AccountingStart day 00:00

## Each period starts on the 3rd of the month at 15:00 (AccountingMax

## is per month)

#AccountingStart month 3 15:00


## Administrative contact information for this relay or bridge. This
line

## can be used to contact you if your relay or bridge is misconfigured
or

## something else goes wrong. Note that we archive and publish all

## descriptors containing these lines and that Google indexes them, so

## spammers might also collect them. You may want to obscure the fact
that

## it's an email address and/or generate a new address for this
purpose.

ContactInfo RelayOps <relayops AT tutanota dot com>

## You might also include your PGP or GPG fingerprint if you have one:

#ContactInfo 0xFFFFFFFF Random Person <nobody AT example dot com>


## Uncomment this to mirror directory information for others. Please
do

## if you have enough bandwidth.

DirPort 80 # what port to advertise for directory connections

## If you want to listen on a port other than the one advertised in

## DirPort (e.g. to advertise 80 but bind to 9091), you can do it as

## follows.  below too. You'll need to do ipchains or other port

## forwarding yourself to make this work.

#DirPort 80 NoListen
```

```
#DirPort 127.0.0.1:9091 NoAdvertise

## Uncomment to return an arbitrary blob of html on your DirPort. Now
you

## can explain what Tor is if anybody wonders why your IP address is

## contacting them. See contrib/tor-exit-notice.html in Tor's source

## distribution for a sample.

DirPortFrontPage /etc/tor/tor-exit-notice.html


## Uncomment this if you run more than one Tor relay, and add the
identity

## key fingerprint of each Tor relay you control, even if they're on

## different networks. You declare it here so Tor clients can avoid

## using more than one of your relays in a single circuit. See

## https://www.torproject.org/docs/faq#MultipleRelays

## However, you should never include a bridge's fingerprint here, as
it would

## break its concealability and potentionally reveal its IP/TCP
address.

MyFamily
B92EA9BCE0ADF008C8EF373A384E1FEC064B6895,F852A11B7725DC294DF7063B590C5
82883B1310F,7B288A194C9D5B7EA8F3093EDF3CEE6A512F8B98


## A comma-separated list of exit policies. They're considered first

## to last, and the first match wins. If you want to _replace_

## the default exit policy, end this with either a reject *:* or an

## accept *:*. Otherwise, you're _augmenting_ (prepending to) the

## default exit policy. Leave commented to just use the default, which
is

## described in the man page or at

## https://www.torproject.org/documentation.html

##

## Look at https://www.torproject.org/faq-abuse.html#TypicalAbuses

## for issues you might encounter if you use the default exit policy.

##
```

```
## If certain IPs and ports are blocked externally, e.g. by your
firewall,

## you should update your exit policy to reflect this -- otherwise Tor

## users will be told that those destinations are down.

##

## For security, by default Tor rejects connections to private (local)

## networks, including to your public IP address. See the man page
entry

## for ExitPolicyRejectPrivate if you want to allow "exit enclaving".

##

ExitRelay 1

ExitPolicy accept *:20-21     # FTP

#ExitPolicy accept *:22        # SSH

ExitPolicy accept *:23        # Telnet

ExitPolicy accept *:43        # WHOIS

ExitPolicy accept *:53        # DNS

ExitPolicy accept *:79        # finger

ExitPolicy accept *:80-81     # HTTP

ExitPolicy accept *:88        # kerberos

ExitPolicy accept *:110       # POP3

ExitPolicy accept *:143       # IMAP

ExitPolicy accept *:194       # IRC

ExitPolicy accept *:220       # IMAP3

ExitPolicy accept *:389       # LDAP

ExitPolicy accept *:443       # HTTPS

ExitPolicy accept *:464       # kpasswd

ExitPolicy accept *:465       # URD for SSM (more often: an
alternative SUBMISSION port, see 587)

ExitPolicy accept *:531       # IRC/AIM

ExitPolicy accept *:543-544   # Kerberos

ExitPolicy accept *:554       # RTSP

ExitPolicy accept *:563       # NNTP over SSL
```

```
ExitPolicy accept *:587       # SUBMISSION (authenticated clients
[MUA's like Thunderbird] send mail over STARTTLS SMTP here)
ExitPolicy accept *:636       # LDAP over SSL
ExitPolicy accept *:706       # SILC
ExitPolicy accept *:749       # kerberos
ExitPolicy accept *:853       # DNS over TLS
ExitPolicy accept *:873       # rsync
ExitPolicy accept *:902-904   # VMware
ExitPolicy accept *:981       # Remote HTTPS management for firewall
ExitPolicy accept *:989-990   # FTP over SSL
ExitPolicy accept *:991       # Netnews Administration System
ExitPolicy accept *:992       # TELNETS
ExitPolicy accept *:993       # IMAP over SSL
ExitPolicy accept *:994       # IRCS
ExitPolicy accept *:995       # POP3 over SSL
ExitPolicy accept *:1194      # OpenVPN
ExitPolicy accept *:1220      # QT Server Admin
ExitPolicy accept *:1293      # PKT-KRB-IPSec
ExitPolicy accept *:1500      # VLSI License Manager
ExitPolicy accept *:1533      # Sametime
ExitPolicy accept *:1677      # GroupWise
ExitPolicy accept *:1723      # PPTP
ExitPolicy accept *:1755      # RTSP
ExitPolicy accept *:1863      # MSNP
ExitPolicy accept *:2082      # Infowave Mobility Server
ExitPolicy accept *:2083      # Secure Radius Service (radsec)
ExitPolicy accept *:2086-2087 # GNUnet, ELI
ExitPolicy accept *:2095-2096 # NBX
ExitPolicy accept *:2102-2104 # Zephyr
ExitPolicy accept *:3128      # SQUID
ExitPolicy accept *:3389      # MS WBT
ExitPolicy accept *:3690      # SVN
```

```
ExitPolicy accept *:4321      # RWHOIS
ExitPolicy accept *:4643      # Virtuozzo
ExitPolicy accept *:5050      # MMCC
ExitPolicy accept *:5190      # ICQ
ExitPolicy accept *:5222-5223 # XMPP, XMPP over SSL
ExitPolicy accept *:5228      # Android Market
ExitPolicy accept *:5900      # VNC
ExitPolicy accept *:6660-6669 # IRC
ExitPolicy accept *:6679      # IRC SSL
ExitPolicy accept *:6697      # IRC SSL
ExitPolicy accept *:8000      # iRDMI
ExitPolicy accept *:8008      # HTTP alternate
ExitPolicy accept *:8074      # Gadu-Gadu
ExitPolicy accept *:8080      # HTTP Proxies
ExitPolicy accept *:8082      # HTTPS Electrum Bitcoin port
ExitPolicy accept *:8087-8088 # Simplify Media SPP Protocol, Radan
HTTP
ExitPolicy accept *:8232-8233 # Zcash
ExitPolicy accept *:8332-8333 # Bitcoin
ExitPolicy accept *:8443      # PCsync HTTPS
ExitPolicy accept *:8888      # HTTP Proxies, NewsEDGE
ExitPolicy accept *:9418      # git
ExitPolicy accept *:9999      # distinct
ExitPolicy accept *:10000     # Network Data Management Protocol
ExitPolicy accept *:11371     # OpenPGP hkp (http keyserver protocol)
ExitPolicy accept *:19294     # Google Voice TCP
ExitPolicy accept *:19638     # Ensim control panel
ExitPolicy accept *:50002     # Electrum Bitcoin SSL
ExitPolicy accept *:64738     # Mumble
ExitPolicy reject *:*
```

```
## Bridge relays (or "bridges") are Tor relays that aren't listed in
the

## main directory. Since there is no complete public list of them,
even an

## ISP that filters connections to all the known Tor relays probably

## won't be able to block all the bridges. Also, websites won't treat
you

## differently because they won't know you're running Tor. If you can

## be a real relay, please do; but if not, be a bridge!

BridgeRelay 0

## By default, Tor will advertise your bridge to users through various

## mechanisms like https://bridges.torproject.org/. If you want to run

## a private bridge, for example because you'll give out your bridge

## address manually to your friends, uncomment this line:

#PublishServerDescriptor 0
```