Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

ALEKSI SUUTALA

Kotiverkon suojaaminen Raspberry Pi:n DNS-palvelun avulla

TIETOJENKÄSITTELYN TUTKINTO-OHJELMA
2023

TIIVISTELMÄ

Suutala, Aleksi: Kotiverkon suojaaminen Raspberry Pi:n DNS-palvelun avulla
Opinnäytetyö, AMK
Tietojenkäsittelyn tutkinto-ohjelma
Huhtikuu 2023
Sivumäärä: 46

Opinnäytetyön tavoitteena oli rakentaa mahdollisimman turvallinen, kevyt ja kustannustehokas DNS-palvelin ratkaisu, jolla pyrittiin estämään tehokkaasti haitalliset verkkosivustot, seuraimet ja mainonta sisäverkkoon kytketyillä päätelaitteilla. Työssä päädyttiin käyttämään tämän tavoitteen saavuttamiseksi Adguard Home nimistä ohjelmistoa ja Raspberry Pi:tä.

Tässä opinnäytetyössä käytiin ensiksi yleisesti läpi, mikä on Raspberry Pi, sen historia ja julkaistut mallit. Tämän jälkeen siirryttiin käsittelemään DNS:n historiaa, toimintaperiaatetta ja DNS-palvelintyyppejä. Perehdyttiin myös DNS:n suojaaviin protokolliin ja tietoturvalaajennuksiin. Näiden jälkeen käsiteltiin DNS-sinkhole-palvelin, sen toiminta ja DNS-palvelinohjelmistot, jotka olivat mahdollista asentaa Raspberry Pi:lle. Lopuksi syvennyttiin miten ja miksi palvelin otetaan käyttöön ja millaisia tuloksia tällä palvelimella saavutettiin.

Avainsanat: Raspberry Pi, Linux, DNS, DNS-suodatus, tietoturva, tietoverkot

Abstract

Suutala, Aleksi: Securing your home network using the Raspberry Pi's DNS service
Bachelor's thesis
Degree programme in Business Information Systems
April 2023
Number of pages: 46

The aim of the thesis was to build secure, lightweight, and cost-effective DNS server solution as possible to effectively block malicious websites, followers and advertising on endpoints connected to the internal network. To achieve this goal, a software called Adguard Home and Raspberry Pi was used.

In this thesis, first was discussed in general terms what a Raspberry Pi is, its history and the models that have been released. Then moved on to the history of DNS, how it works and the types of DNS servers. Also looked at the protocols and security extensions that protect DNS. This was followed by a discussion of the DNS sinkhole server, how it works and the DNS server software that could be installed on the Raspberry Pi. Finally, we had dived into how and why to deploy the server and what results were achieved with this server.

Keywords: Raspberry Pi, Linux, DNS, DNS-filtering, information security, information networks

SISÄLLYS

1 JOHDANTO 5
2 KÄYTETTÄVÄ ALUSTA 6
2.1 Raspberry Pi:n historia 7
2.2 Raspberry Pi:n mallit 7
2.2.1 Ensimmäiset 1A/B mallit 8
2.2.2 Toinen sukupolvi 8
2.2.3 Kolmas sukupolvi 8
2.2.4 Neljäs ja tämän hetken uusin sukupolvi 9
2.2.5 Pääsarjasta poikkeavat sivumallit 9
3 DNS:N MÄÄRITELMÄ 11
3.1 DNS:n toimintaperiaate 12
3.1.1 Auktoritatiivinen ja rekursiivinen DNS 12
3.1.2 DNS-hakuprosessi 13
3.2 Julkiset ja yksityiset DNS-palvelimet 14
3.2.1 Julkiset DNS-palveluntarjoajat 14
3.2.2 Yksityisen DNS-palvelimen hyödyt ja haitat 15
3.3 DNS:n suojaavat protokollat ja laajennukset 16
3.3.1 DNSSEC 16
3.3.2 DNS over HTTPS/TLS 17
3.3.3 DNSCrypt 17
3.3.4 DNS over QUIC 17
4 DNS SINKHOLE -PALVELIN 18
4.1 DNS sinkhole-palvelimen toiminta 19
5 PALVELIMEN KÄYTTÖÖNOTTO 20
5.1 Alustan valinta ja testiympäristö 21
5.2 Raspberry Pi OS Lite 22
5.3 SSH ja sen käyttäminen palvelimen määrittelyyn 24
5.4 AdGuard Home:n asentaminen, määrittely ja ominaisuudet 27
6 PALVELIMEN TOIMINNALLISUUS 36
7 YHTEENVETO 44
LÄHTEET 45

1 JOHDANTO

Nimipalvelin eli DNS on olennainen osa jokapäiväistä kommunikointia verkossa ja on yksi suuri haavoittuvuus verkkoturvallisuudessa. DNS kehitettiin aikakaudella, jolloin turvallisuus ei ollut etusijalla. Lähiaikoina on tullut esille entistä enemmän DNS-huijauksia, joissa muutetaan DNS-palvelimien tietoja ohjaamalla DNS-palvelin antamaan pyydetylle verkkotunnukselle haitallisen sivuston IP-osoite vastineeksi. Käyttäjän siirtyessä sivustolle pyritään kaappaamaan syötettyjä henkilökohtaisia tietoja. Tätä vastaan DNS:ään on julkaistu eri tietoturvalaajennuksia ja käytetään eri verkkoprotokollia tietosuojan ja tietoturvan parantamiseksi. Useat kolmannen osapuolen DNS-palveluntarjoajat pyrkivät tarjoamaan monipuolisia ja tietoturvakeskeisiä ratkaisuja. Oman tai yrityksen tietosuojaa ja tietoturvaa pystyy parantamaan verkossa käyttämällä luotettavia DNS-palvelimia ja pitämään laitteiden päivityksen ajan tasalla. Lisäturvaa voidaan saada myös asentamalla lähiverkkoon esimerkiksi sinkhole-tyylinen DNS-palvelin, joka suodattaa pois kolmannen osapuolen sivustoilta tulevia haitallisia mainoksia, seuraimia ja muita haitallisia sivustoja.

Kukaan ei pidä häiritsevistä ja mahdollisesti haitallisista mainoksista ja muista huijauksista, seurannasta ja haitoista verkossa. Näistä syistä opinnäytetyössä tulemme sinkhole-tyylisen DNS-palvelimen lopuksi asentamaan käyttäen Adguard Home nimistä ohjelmistoa ja tietoturva keskeistä ja luotettavaa julkista DNS-palveluntarjoajaa Quad9:siä. Pelkästään Quad9 käyttäminenkin parantaa verkossa selailun turvallisuutta laajojen uhkatiedustelulähteiden ansiosta.

2 KÄYTETTÄVÄ ALUSTA

Raspberry Pi on noin luottokortin kokoinen minitietokone, joka on yhteensopiva minkä tahansa syöttö- ja lähdelaitteen kanssa, kuten hiiren, näppäimistön, näytön tai television. Tämä tekee laitteesta käytännössä edullisen ja täysimittaisen tietokoneen. (Basumallick, 2022.)

Raspberry Pi on ohjelmoitava laite. Laitteessa on kaikki tavallisen tietokoneen emolevyn olennaiset ominaisuudet, mutta siinä ei ole oheislaitteita eikä sisäistä tallennustilaa. Käyttöönottoa varten tarvitset esimerkiksi SD-kortin, joka sijoitetaan sille varattuun tilaan. SD-kortille on asennettava käyttöjärjestelmä, jotta tietokone käynnistyy. Alusta on yhteensopiva esimerkiksi eri Linux-käyttöjärjestelmien kanssa. (Basumallick, 2022.)

Raspberry Pi pohjautuu yleisesti avoimen lähdekoodin ohjelmistoihin. Aikaisemmin mainitut Linux-käyttöjärjestelmät ovat tällaisia. Avoimuus tekee Raspberry Pi:stä luotettavan ja räätälöitävän. Kun ohjelmistojen lähdekoodi on luettavissa, tiedetään tarkalleen, mitä ohjelmistot todellisuudessa tekevät. Raspberry Pi ei ole pelkästään tavallinen tietokone. Raspberry Pi on kokonaisuudessaan erittäin monipuolinen ja käytännöllinen alusta erilaisiin käyttötarkoituksiin ja projekteihin. Esimerkiksi voit rakentaa Raspberry Pi:stä fyysisen elektronisen FM-radion, IoT-laitteita, kuten verkkoon kytketyn sääaseman tai ääniohjattavan kodin automaatiojärjestelmän. Hyvin yleinen käyttötarkoitus Raspberry Pi:lle on toimia jonkinlaisena palvelimena kuten DNS-palvelin, Web-palvelin, mediapalvelin, tiedostopalvelin tai tulostuspalvelin. Luvussa 3 perehdytään näistä DNS:ään tarkemmin.

2.1 Raspberry Pi:n historia

Eben Upton, Raspberry Pi:n perustajajäsen ja Cambridgen yliopiston alumni, pohti millainen erittäin edullisen tietokoneen tulisi olla. Hänelle tuolloin yksi tärkeimmistä vaatimuksista oli kestävyys. Lapsuudessa Upton kasvoi BBC Micro -tietokoneen parissa ja tämä herätti hänessä innostuksen ohjelmointia kohtaan. Tämä tietokone oli toinen Cambridgen suunnittelemastaan 1980-luvun suuresta tietokoneesta. Toinen näistä oli Sinclair Spectrum, joka opetti kokonaisen sukupolven brittiläisiä tietokoneharrastajia koodaamaan. (Collins, 2022.)

Edullisen ja tehokkaasti toimivan tietokoneen suunnittelu vaati asiantuntemusta teknologian ja teollisuuden aloilta. Tätä varten syntyi ryhmä, johon kuuluivat Cambridgen tietotekniikan ja teknologian laitoksen professorit Robert Mullins ja Alan Mycroft, Cambridgen yrittäjä Jack Lang sekä muita Cambridgen tietotekniikan tutkijoita, insinöörejä ja teollisuusyrittäjiä. Ryhmä päätyi 25 dollarin hintaan osittain siksi, että se vastasi suunnilleen oppikirjan hintaa tuolloin. (Collins, 2022.)

2.2 Raspberry Pi:n mallit

Vuonna 2006 Eben Upton alkoi työstää ensimmäisiä konseptejaan. Alunperin hän suunnitteli luovansa kaksi eri mallia: A, jonka tarkoituksena oli olla halpa ja B, joka olisi tehokkaampi, mutta kalliimpi malli A:han verrattuna. Vuonna 2011 alfa- ja beetalaitteet saatiin valmistettua, ennen yleiselle markkinoille julkaistua ensimmäistä virallista mallia. (Fromaget, n.d.)

2.2.1 Ensimmäiset 1A/B mallit

Raspberry Pi 1B on ensimmäinen malli, joka julkaistiin 29 helmikuuta 2012. Tässä mallissa on yksiytiminen 700Mhz ARM:n prosessori ja sisältää 256MT keskusmuistia. Helmikuussa 2013 julkaistiin edullisempi ja kevennetty A-malli, jossa B-mallin sijaan oli vain 256MT keskusmuistia. Heinäkuussa 2014 julkaistiin pienillä päivityksillä B+ malli, joka korvasi edeltävän B-mallin. Tässä mallissa on 4 USB 2.0 porttia kahden sijaan, alhaisempi virrankulutus ja SD-kortti päivitetty Micro-SD korttiin. Samoin A-malli korvattiin mallilla A+ marraskuussa samanlaisilla päivityksillä, kuten mallille B+ tehtiin. (Fromaget, n.d.)

2.2.2 Toinen sukupolvi

Yllättäen Raspberry Pi 1A -malli ei saanut toisen sukupolven mallia. Helmikuussa 2015 julkaistiin vain Raspberry Pi 2B, jossa on tehokkaampi 900MHz neliytiminen ARM-prosessori ja 1 gigatavun verran keskusmuistia. Lokakuussa 2016 tästä julkaistiin 2B-versio 1.2, jossa hieman nopeampi prosessori 1.2Ghz ja piiri on päivitetty 64-bitin arkkitehtuuriin. (Fromaget, n.d.)

2.2.3 Kolmas sukupolvi

Raspberry Pi B:n versio 3 julkaistiin helmikuussa 2016. Tämä malli on sama edellisen 2B-versio 1.2:n kanssa, mutta tähän malliin on integroitu emolevyyn Wi-Fi ja Bluetooth. Kaksi vuotta myöhemmin maaliskuussa 2018 Pi 3 B+ -malli julkaistiin, jossa oli nopeampi Gigabitin Ethernet-portti ja tehokkaampi 1.4Ghz prosessori. Hieman myöhemmin marraskuussa 2018 julkaistiin tällä kertaa A-mallista päivitetty Pi 3 A+ -malli 1.4Ghz, jossa oli neliydinprosessori, 512MT keskusmuisti, Gigabitin Ethernet-portti, Wi-Fi ja Bluetooth, kuten 3 B+ -mallissa. (Fromaget, n.d.)

2.2.4 Neljäs ja tämän hetken uusin sukupolvi

Raspberry Pi 4B on vuonna 2019 julkaistu malli, joka on suuri parannus suoritusteholtaan edellisiin malleihin verrattuna. Sen keskusmuisti vaihtelee 1 Gt:stä kahdeksaan gigatavuun asti. (Basumallick, 2022.)

2.2.5 Pääsarjasta poikkeavat sivumallit

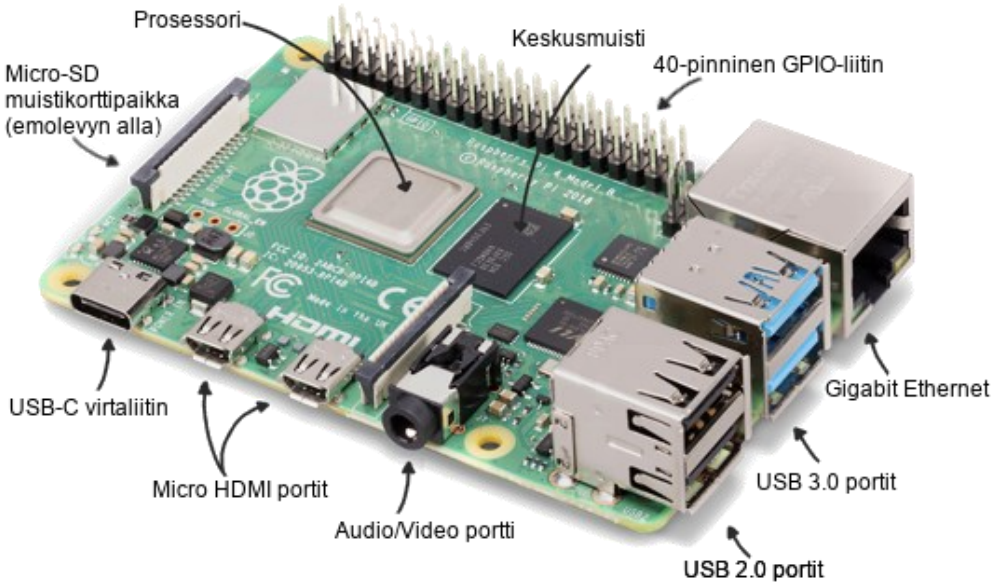
Pääsarjan A- ja B-mallien rinnalle on myös julkaistu vuosien varrella eri sivumalleja. Näitä ovat Raspberry Pi Zero, Raspberry Pi Pico ja Raspberry Pi 400.

Zero on kooltaan puolta pienempi kuin ensimmäisen sukupolven A+ -malli, mutta on suorituskyvyltään ja teknisiltä ominaisuuksiltaan vastaava. Pi 400 pohjautuu Raspberry Pi 4B -malliin, mutta se on rakennettu näppäimistön sisälle, jossa on enemmän liitäntöjä ja hieman tehokkaampi prosessori 4B-malliin verrattuna. Pico-mallit ovat poikkeus kaikista muista malleista. Pico ei ole suunniteltu normaaliin työpöytäkäyttöön. Picoa käytetään vain fyysisessä tietotekniikassa, kuten Arduinoa.

Alla olevassa taulukossa on listaus kaikista aikaisemmin mainituista malleista ja niiden tarkemmat tekniset spesifikaatiot.

Taulukko 1. Raspberry Pi:n mallit ja niiden tekniset spesifikaatiot.

Malli	Versio	Prosessori	Keskusmuisti	Ethernet	WiFi/Bluetooth	Julkaisu
Raspberry Pi	B	32-bit ARM 11 700MHz 1-ydin	256 Mt / 512 Mt	Kyllä	Ei	helmikuu 2012
Raspberry Pi	A	32-bit ARM 11 700MHz 1-ydin	256 Mt	Ei	Ei	helmikuu 2013
Raspberry Pi	B+	32-bit ARM 11 700MHz 1-ydin	512 Mt	Kyllä	Ei	heinäkuu 2014
Raspberry Pi	A+	32-bit ARM 11 700MHz 1-ydin	512 Mt	Ei	Ei	marraskuu 2014
Raspberry Pi Zero	Zero	32-bit ARM 11 1Ghz 1-ydin	512 Mt	Ei	El	marraskuu 2015
Raspberry Pi Zero	W / WH	32-bit ARM 11 1Ghz 1-ydin	512 Mt	El	Kyllä	helmikuu 2017
Raspberry Pi Zero	2 W	64-bit ARM Cortex A53 1Ghz 4-ydin	512 Mt	El	Kyllä	lokakuu 2021
Raspberry Pi 2	B	32-bit ARM Cortex A7 900MHz 4-ydin	1 Gt	Kyllä	Ei	helmikuu 2015
Raspberry Pi 2	B v1.2	64-bit ARM Cortex A53 900MHz 4-ydin	1 Gt	Kyllä	Ei	lokakuu 2016
Raspberry Pi 3	B	64-bit ARM Cortex A53 1.2Ghz 4-ydin	1 Gt	Kyllä	Kyllä	helmikuu 2016
Raspberry Pi 3	A+	64-bit ARM Cortex A53 1.4Ghz 4-ydin	512 Mt	Ei	Kyllä (dual band)	marraskuu 2018
Raspberry Pi 3	B+	64-bit ARM Cortex A53 1.4Ghz 4-ydin	1 Gt	Kyllä (Gigabit)	Kyllä (dual band)	maaliskuu 2018
Raspberry Pi 4	B	64-bit ARM Cortex A72 1.5Ghz 4-ydin	1 Gt / 2 Gt / 4 Gt	Kyllä (Gigabit)	Kyllä (dual band)	kesäkuu 2019
Raspberry Pi 4	B	64-bit ARM Cortex A72 1.5Ghz 4-ydin	8 Gt	Kyllä (Gigabit)	Kyllä (dual band)	toukokuu 2020
Raspberry Pi 4	400	64-bit ARM Cortex A72 1.8Ghz 4-ydin	4 Gt	Kyllä (Gigabit)	Kyllä (dual band)	marraskuu 2020
Raspberry Pi Pico	Pico	32-bit Arm Cortex-M0+ 133MHz 2-ydin	264 kt	Ei	Ei	tammikuu 2021
Raspberry Pi Pico	W	32-bit Arm Cortex-M0+ 133MHz 2-ydin	264 kt	El	Kyllä/ei	kesäkuu 2022



Kuva 1. Raspberry Pi 4B malli ja tämän portit ja liitännät. (Raspberry Pi, n.d.)

Nyt yli yksitoista vuotta myöhemmin tietokone, joka suunniteltiin osittain kestämään lapsuuden rajua ja rankkaa menoa, on myös löytänyt kodin kymmenistä tuhansista teollisuussovelluksista eri puolilla maailmaa. Sen mukautuvuus, vakaus ja edullinen hinta tekevät Raspberry Pi:stä ihanteellisen eri sovelluksiin ja käyttötarkoituksiin. (Collins, 2022.)

3 DNS:N MÄÄRITELMÄ

Domain Name System eli DNS esiteltiin ensimmäisen kerran Internet Engineering Task Force -ryhmässä (IETF) vuonna 1983. DNS otettiin käyttöön vuonna 1985 ja on ollut käytössä siitä lähtien. Erillisistä DNS-palvelimista koostuva verkon nimipalvelujärjestelmä on joukko tietokoneita ja palvelimia, jotka kääntävät vaikeasti muistettavat IP-osoitteet ihmisystävällisiksi verkkotunnuksiksi. (Crane, 2021.)

DNS on tehokas työkalu, jota käytetään lähes kaikkialla. DNS:n avulla sovellukset ja järjestelmät voivat hakea resursseja ja palveluja, joiden kanssa ne voivat olla vuorovaikutuksessa. DNS käyttää porttia 53, joka on lähes aina auki järjestelmissä, palomuureissa ja päätelaitteissa. DNS-kyselyjen lähettämiseen käytetään UDP-protokollaa (User Datagram Protocol). Jos UDP-kysely epäonnistuu useita kertoja, siirrytään käyttämään TCP-protokollaa (Transmission Control Protocol). (Hinchliffe, 2019.)

DNS voidaan yleisesti jättää huomiotta tietoturvan kannalta. Näistä syistä DNS on täydellinen valinta hyökkääjille, jotka etsivät aina avointa, usein huomiotta jätettyä protokollaa. (Hinchliffe, 2019.)

Uutta verkkosivua suunniteltaessa täytyy valita verkkotunnus ja vahvistaa, että se on käytettävissä. Tämän jälkeen verkkotunnus rekisteröidään ja se muunnetaan verkko-osoitteeksi eli URL-osoitteeksi DNS:n avulla. Rekisteröinti varmistaa käyttäjän kirjoittaessa URL-osoitteen, että se vie hänet verkkosivustolle eikä muualle. (Dhillon, 2015.) IP-osoitteet voivat olla päällekkäisiä useissa verkoissa verkko-osoitekäännöksen NAT:in (Network Address Translation) avulla. Järjestelmillä on kuitenkin Universal Unique Identifiers (UUID), jotka voivat luoda yksilöllisen tunnisteen. (Hinchliffe, 2019.)

3.1 DNS:n toimintaperiaate

Nimipalvelin hallinnoi laajaa tietokantaa, joka yhdistää verkkotunnukset niiden IP-osoitteisiin. DNS on protokolla, joka kuuluu UDP tai TCP ja IP-protokolla-joukkoon kuuluviin standardeihin. Näillä standardeilla tietokoneet vaihtavat tietoja internetissä ja monissa lähiverkoissa. Käyttäjät hakevat tietoja DNS:stä viittaamalla resolver-kirjastoon(ratkaisija), joka lähettää kyselyjä useille nimipalvelimille ja toimii tällöin myös vastaajana. (Mazerik, 2021.)

Tietokoneiden keskinäiseen kommunikointiin internetissä tarvitaan kaikilla verkon käyttäjillä yksilöllinen osoite. IP-osoitteiden avulla käyttäjät tietävät, mihin palvelimiin niiden pitäisi ottaa yhteyttä. Tätä varten on olemassa internetin nimipalvelujärjestelmä DNS. (Ionos, 2022.)

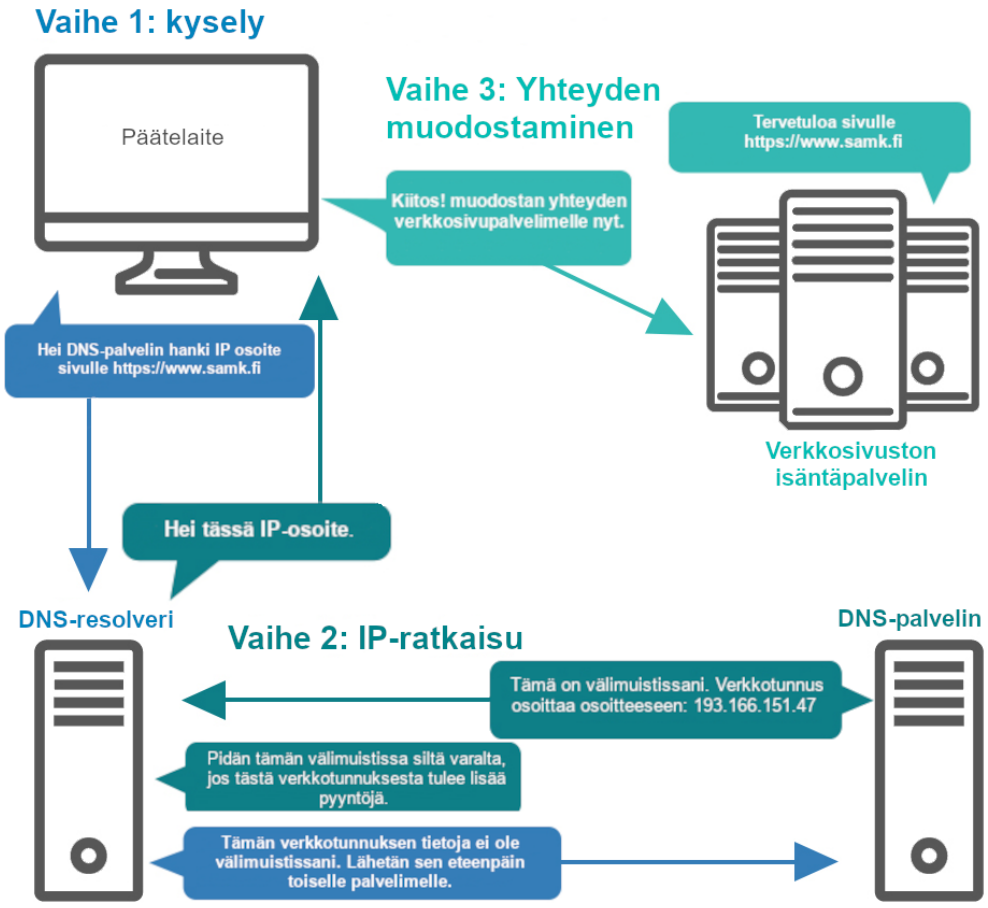
Yleisin IP-osoitetyyppi (IPv4) koostuu neljästä numerosarjasta, jotka erotetaan toisistaan pisteillä. Esimerkiksi lähiverkon osoite on 192.168.1.25. Kukin IPv4-osoite on 32-bittinen. IPv6 IP-osoitteet koostuvat kahdeksasta neljän heksadesimaaliluvun ryhmästä, jotka erotetaan kaksoispisteillä. IPv6-osoitteet ovat 128-bittisiä. Nämä luotiin, koska pelättiin IPv4 IP-osoitteiden loppuvan kesken. (Crane, 2021.)

3.1.1 Auktoritatiivinen ja rekursiivinen DNS

Auktoritatiiviset DNS-palvelimet ovat verkkotunnusten tietojen ylläpitäjiä ja tallettavat verkkosivustojen IP-osoitteen tiedot. Rekursiiviset DNS-palvelimet puolestaan ovat suoraan vuorovaikutuksessa loppukäyttäjän kanssa ja lukevat käyttäjän DNS-kyselyt. (Raymond, 2021.) Rekursiivinen palvelin käy läpi ensimmäisenä välimuistissa olevat verkkotunnisteet. Kysytyn verkkotunnuksen tiedon puututtua rekursiivinen palvelin hakee tietoja erillisistä auktoritatiivisista palvelimista, kunnes pystyy kommunikoimaan auktoritatiiviselle palvelimelle, joka sisältää halutun verkkotunnuksen IP-osoitteen. (Quad9, 2022.)

3.1.2 DNS-hakuprosessi

Kuvassa (kuva 2) käyttäjä haluaa ottaa internetiin kytketyllä päätelaitteella yhteyden selaimen välityksellä osoitteeseen www.samk.fi. Tämän kyselyn verkkotunnus välittyy lähimpänä olevalle rekursiiviselle DNS-palvelimelle. Tätä palvelinta kutsutaan resolveriksi eli ratkaisijaksi.



Kuva 2. DNS:n toiminta käytännössä. (Dhillon, 2015.)

Kuvassa resolverilla ei ole pyydetyn verkkotunnuksen IP-osoitetta välimuistissa, joten tämä välittää sen internetin välityksellä rekursiivinen nimipalvelimen tapaan juurinimipalvelimelle (Root name server). Juurinimipalvelin on ylimmän tason DNS-palvelin, joka arkistoi esimerkiksi .com, .net ja .fi-verkkotunnuspäätteitä. Kysely kohdistuu .fi-aluetunnukseen, jonka juuripalvelin ilmoittaa revolverille. Resolveri lähettää kyselyn seuraavaksi ylätason .fi-verkkotunnuspäätteen DNS-palvelimille ja lopuksi kysely lähetetään annetun verkkotunnuksen DNS-palvelimelle. Tämän kyselyketjun jälkeen resolverilla on tiedossa pyydetyn verkkotunnuksen IP-osoite, joka tallennetaan välimuistiin

resolverille tai päätelaitteen selaimeen. Lopuksi IP-osoite lähetetään käyttäjän päätelaitteelle, jonka avulla käyttäjä pystyy muodostamaan yhteyden verkkosivuston web-palvelimelle.

3.2 Julkiset ja yksityiset DNS-palvelimet

Jokaiselle internetiin kytketylle laitteelle määräytyy tai määritellään DNS-palvelimen IP-osoite. Yleisesti käytetään internet-palveluntarjoajan, esimerkiksi DNA:n, omaa julkista DNS-palvelinta. Suurimmaksi osaksi käytättäjistä internet-palveluntarjoajan oma nimipalvelin riittää. (NordLayer, 2022.) Operaattoreiden nimipalvelimet suodattavat tuloksia Keskusrikospoliisin mukaan laittomasta sisällöstä internetissä ja heillä on mahdollista valvoa kulkevaa internet liikennettä. Operaattorien nimipalvelimet eivät tarjoa vaihtoehtoisia suodatuslistoja haitallisia tai aikuisille tarkoitettua sisältöä vastaan, ja tarjoavat suppeammat tietoturva protokollat muihin kolmannen osapuolen tarjoamiin julkisiin nimipalvelimiin verrattuna.

3.2.1 Julkiset DNS-palveluntarjoajat

Julkisen kolmannen osapuolen nimipalvelinta valittaessa täytyy ymmärtää ja luottaa siihen, mitä ominaisuuksia palveluntarjoaja antaa, ja mitä nämä tekevät palvelun käyttäjän datalla. Yleisesti käytettyjä luotettavia palveluntarjoajia ovat Cloudflare, Quad9, Google ja OpenDNS. Perehdytään näistä tietosuojakeskeisiin Cloudflareen ja Quad9:n hieman tarkemmin.

1.1.1.1 on Cloudflaren ylläpitämä julkinen DNS-resolveri, joka tarjoaa nopeutta ja yksityisyyttä. 1.1.1.1 ei kerää yksilöiviä käyttäjätietoja. Cloudflare kerää lokia vain virheenkorjauksia varten ja näitä säilytetään ainoastaan 24 tuntia. Cloudflare on yhdysvaltalainen yhtiö ja lähin palvelin sijaitsee Helsingissä. Suomessa 1.1.1.1 toimii yleisesti muihin palveluntarjoajiin verrattuna kaikkein nopeinten.

Quad9 on voittoa tavoittelematon organisaatio. Quad9:n ovat perustaneet International Business Machines (IBM), Packet Clearing House (PCH) ja Global Cyber Alliance (GCA). Quad9:n pääkonttori sijaitsee Sveitsissä. Quad9 käyttää yli 20:tä uhkatiedustelulähdettä estääkseen suurimman osan haavoittuvuuksista, haittaohjelmista, lunnasohjelmista, vakoiluohjelmista ja muista mahdollisesti haitallisista sivustoista. (Ionescu, 2022.) Quad9 kerää tietoa anonyymisti käyttäjien maantieteellisestä sijainnista. Tätä tietoa käytetään haitallisten hyökkäyksien analysoinnin kehittämiseen. Lähin palvelin sijaitsee Tampereella.

Alla olevassa taulukossa (taulukko 2) on listattuna aikaisemmin mainittujen yleisesti käytettyjen DNS-palvelimien lisäksi muita ilmaisia toimivaksi ja luotettavaksi luokiteltuja julkisia palveluntarjoajia.

Taulukko 2. Julkisia DNS-palvelimia ja niiden IP-osoitteet.

Palveluntarjoaja	Ensisijainen DNS IPv4	Toissijainen DNS IPv4	Ensisijainen DNS IPv6	Toissijainen DNS IPv6
DNA	62.241.198.245	62.241.198.246	2001:14b8:1000::1	2001:14b8:1000::2
Cloudflare	1.1.1.1	1.0.0.1	2606:4700:4700::1111	2606:4700:4700::1001
Quad9	9.9.9.9	149.112.112.112	2620:fe::fe	2620:fe::9
Google	8.8.8.8	8.8.4.4	2001:4860:4860::8888	2001:4860:4860::8844
OpenDNS	208.67.222.222	208.67.220.220	2620:119:35::35	2620:119:53::53
AdGuard DNS	94.140.14.14	94.140.15.15	2a10:50c0::ad1:ff	2a10:50c0::ad2:ff
DNS.WATCH	84.200.69.80	84.200.70.40	2001:1608:10:25::1c04:b12f	2001:1608:10:25::9249:d69b
SafeDNS	195.46.39.39	195.46.39.40	2001:67c:2778::3939	2001:67c:2778::3940
CleanBrowsing	185.228.168.9	185.228.169.9	X	X

3.2.2 Yksityisen DNS-palvelimen hyödyt ja haitat

Eri yritykset yhdistävät usein julkisia ja yksityisiä DNS-palvelimia. Yleinen konfiguraatio on ylläpitää ulkoista auktoritatiivista DNS-palvelinta, joka käsittelee julkisia kyselyjä ja erillistä palvelinta, joka sisältää julkisen DNS:n tarjoamia auktoritatiivisia tietoja. Tämän yleisen konfiguraation avulla julkinen palvelin ei tunne yksityistä vastinettaan. (NordLayer, 2022.)

Oman yksityisen DNS-palvelimen perustaminen yritykselle tai itselle tarjoaa useita etuja, kuten lisää joustavuutta, hallintaa ja oikein määriteltynä turvallisuutta. Muutokset voi tehdä nopeasti, jos jokin menee pieleen. Myöskään ei tarvitse odottaa, että kolmas osapuoli ratkaisee ongelman. Omaa DNS-palvelinta täytyy kuitenkin ylläpitää säännöllisin päivityksin ja korjauksin, ettei haavoittuvuuksia ei pystytä käyttämään hyväksi vahingoittamalla ja saastuttamalla DNS-palvelinta ja siihen kytkettyjä laitteita. (Crane, 2021.)

3.3 DNS:n suojaavat protokollat ja laajennukset

Kuten jo johdannossa todettiin DNS kehitettiin aikakaudella, jolloin turvallisuus ei ollut etusijalla. Itsestään DNS protokollana ei ole turvallinen. DNS vaatii erillisiä palveluita ja protokollia vahvistaakseen ja laajentaakseen suojausta. DNS:ään standardisoidaan edelleen uusia suojausta parantavia laajennuksia ja protokollia.

3.3.1 DNSSEC

Domain Name System Security Extensions lisää DNS-resolverille DNS-tietojen alkuperän todennuksen. DNSSEC todentaa DNS:n käyttämällä digitaalisia allekirjoituksia, jotka perustuvat julkisen avaimen salaukseen. Tämä estää resolvereita tallentamasta väärennettyjä DNS-tietoja välimuistiin ja estää välimuistin myrkyttämisen (cache poisoning). DNSSEC:n tarkoituksena on estää DNS-huijaukset verkossa, jossa pyritään ohjaamaan käyttäjät haitallisille valesivustoille pyydetyn sivun sijasta. (Tunggal, 2021.)

3.3.2 DNS over HTTPS/TLS

DNS over HTTPS (DoH) on internetin protokolla, joka siirtää nimipalvelimen tiedot salattuna HTTPS-yhteyksien kautta. Normaali DNS-viestintä on haavoittuvainen, koska viestintä lähetetään tavallisena luettavana tekstinä, eikä salattuna. DoH:n avulla DNS-kyselyt ovat salattuja ja kolmannen osapuolen tarkkailija ei voi lukea näitä. DNS over TLS-protokollalla (DoT) saavutetaan sama DoH:n verrattuna, mutta DNS over TLS-palvelulla on oma porttinsa, portti 853. DNS HTTPS:n kautta käyttää eri porttia, porttia 443. Tämä internetportti on nykyinen standardi kaikelle HTTPS-viestinnälle. (Cihodariu, 2021.)

3.3.3 DNSCrypt

DNSCrypt on verkkoprotokolla, joka yhdessä DNSSEC:n kanssa auttaa todentamaan DNS-liikenteen. DNSCrypt varmistaa kyselyiden yhtenäisyyden asiakas- ja palvelinpuolella salaamalla DNS-liikenteen. DNSCrypt-protokollaa käytetään myös vähentämään tai estämään UDP-pohjaisia palvelunestohyökkäyksiä (DoS). (Catania, 2021.)

3.3.4 DNS over QUIC

DNS over QUIC (DoQ) lisää DNS:n tietosuojaa mahdollisimman pienellä viiveellä. Liikenne salataan yhdistämällä siirto- ja salauksen kättelyt yhteen, joka vähentää tällöin viivettä. DoQ käyttää QUIC-verkkoprotokollaa (quick) DNS-kyselyjen siirtoprotokollana. Salatut DNS-protokollat, kuten DoT ja DoH ovat jo yleisessä käytössä. Näillä protokollilla on kuitenkin useita puutteita, koska ne perustuvat TCP:hen. DoQ pyrkii korjaamaan nämä QUICi:n ominaisuuksilla. DoQ:n käyttöönottoa aloitettiin julkisessa internetissä 5. heinäkuuta 2021. (Kosek, 2022.) DoQ on suhteellisen uusi protokolla DNS-kyselyjen lähettämiseen. DoQ:sta tuli standardi vasta toukokuussa 2022. AdGuard DNS on ensimmäinen julkinen DNS-resolveri, joka tukee uutta DoQ-protokollaa. (AdGuard, 2022.)

4 DNS SINKHOLE -PALVELIN

DNS sinkholen avulla voidaan estää pääsy haitallisiin URL-osoitteisiin omassa kotiverkossa tai yrityksen verkoissa. DNS sinkholea kutsutaan myös mustaksi aukoksi. DNS sinkholea käytetään väärän DNS-resoluution antamiseen ja käyttäjien polun vaihtamiseen erilaisiin resursseihin haitallisen tai saavuttamattoman sisällön sijaan. DNS sinkhole ohittaa DNS-pyynnön ja antaa DNS-sinkholeen määritetyn vastauksen. DNS sinkhole ei anna verkkotunnuksen auktoritatiivisen omistajan ratkaista verkkotunnusta. DNS sinkhole sieppaa DNS-pyynnön ja vastaa määritetyllä auktoritatiivisella vastauksella. (Mazerik, 2021.)

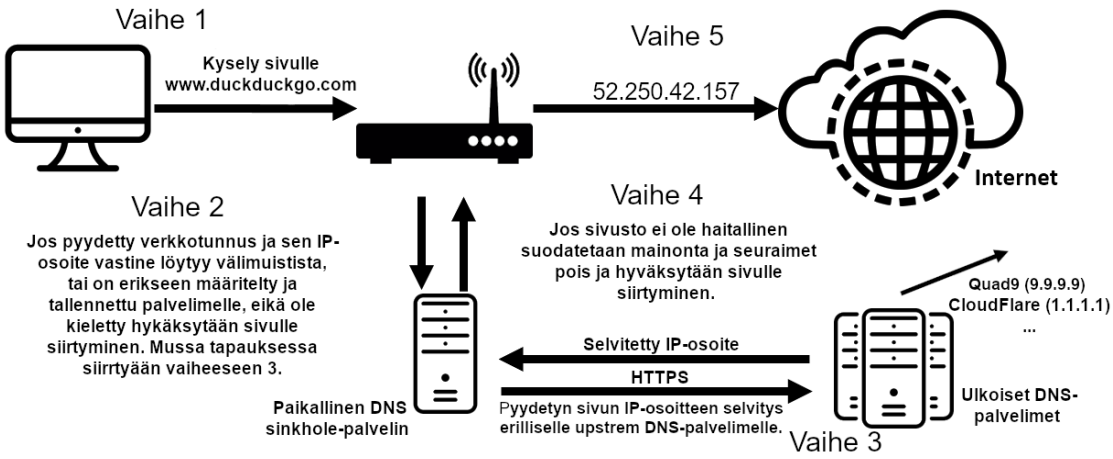
DNS-suodatus on tekniikka, jolla estetään pääsy tietynlaiselle sisällölle Internetissä. DNS-suodatusta käytetään erityisesti estämään pääsy mainospalvelimille tai haitallisille verkkosivustoille. Suodattava DNS-palvelin ei lähetä takaisin tällaisten sivustojen IP-osoitteita. Suodatussäännöt kertovat DNS-palvelimille, mitkä verkkotunnukset on estettävä tai sallittava. Nämä säännöt ovat merkkijonoja, jotka ovat kirjoitettu tiettyä syntaksia käyttäen. Erillisten sääntöjen ryhmää kutsutaan suodattimeksi. (Fedotova, 2022.)

AdGuard Home ja Pi-hole ovat molemmat yksityisiä DNS-palvelinohjelmistoja sisäverkossa. Nämä perustuvat sinkhole-palvelimen toimintaan. Molemmat ovat avoimen lähdekoodin ohjelmistoja. Näiden avulla voidaan toteuttaa koko verkon kattava haitallisten sivujen ja mainosten estopalvelin, joka suojaa kaikkia samaan verkkoon kytkettyjä laitteita ilman, että laitteille tarvitsee asentaa erillisiä ohjelmistoja. Molemmat voidaan asentaa tavalliselle Windows- tai Linux-työasemalle, verkkoon liitetylle tallennusjärjestelmälle (NAS), tai yleisesti käytettävälle Raspberry Pi:lle esimerkiksi Raspberry Pi 4B-mallille (kuva 1).

Pi-hole on yleisemmin käytetty ja tunnetumpi ohjelmisto AdGuard Homeen verrattaessa. Molempia päivitetään säännöllisesti eri tietoturvakorjauksilla ja uusilla ominaisuuksilla, mutta tällä hetkellä AdGuard Home sisältää ja tukee enemmän ominaisuuksia ja muokattavuutta Pi-holeen verrattuna.

4.1 DNS sinkhole-palvelimen toiminta

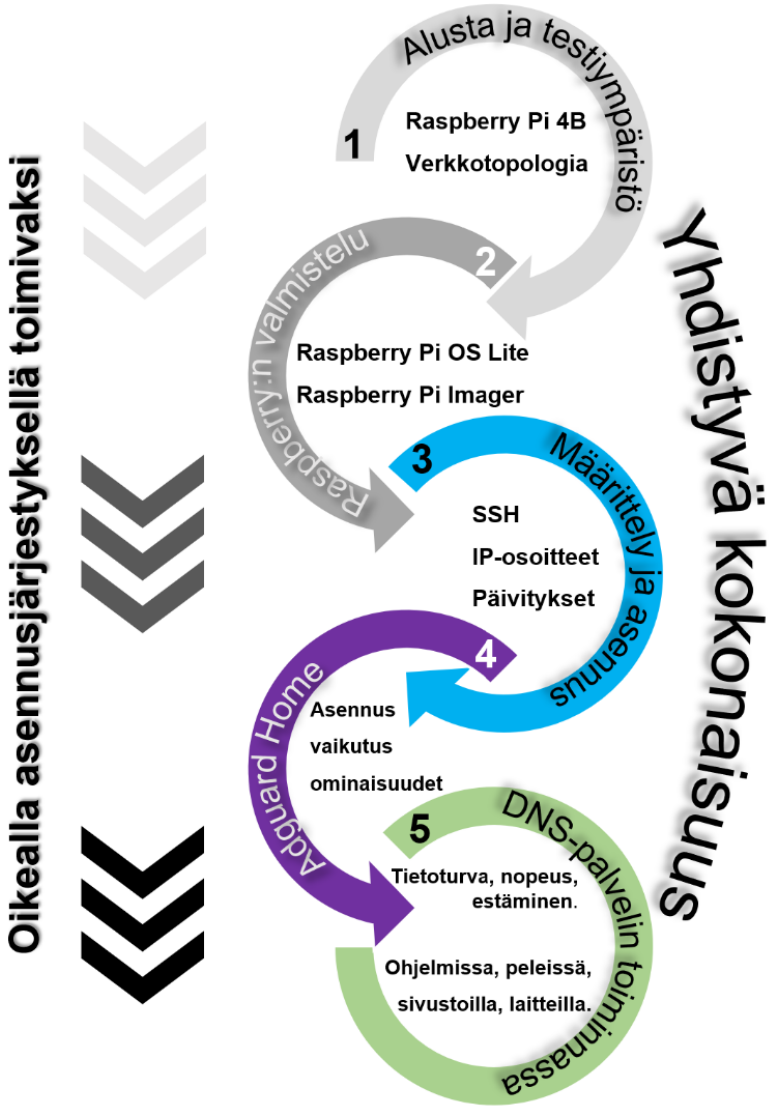
Alla olevassa kuvassa (kuva 3) käyttäjän päätelaite on yhteydessä verkkoon langattoman reitittimen kautta. Käyttäjä tekee konsolin tai selaimen kautta DNS-kyselyn ositteeseen www.duckduckgo.com. Kysely siirtyy sisäverkossa olevalle yksityiselle sinkhole-palvelimelle. Sinkhole-palvelin palauttaa kysytyn sivuston IP-osoitteen, jos tämä on muistissa eikä kielletty. Muuten palvelin lähettää kyselyn salatusti HTTPS:n välityksellä internetissä oleville rekursiivisille DNS-resolvereille. Resolveri kommunikoi auktoritatiivisten DNS-palvelimille selvittääkseen verkkotunnuksen IP-osoitteen. Quad9 tukee DNSSEC- ja DNSCrypt-todennusta, joten näitä käytetään oikeudellisuuden varmistaessa. Lopuksi sinkhole-palvelin suodattaa sivustolta kolmannen osapuolen mainonnan pois ja päätelaite siirtyy kysytylle verkkosivustolle.



Kuva 3. DNS sinkhole-palvelimen toimintakaavio. (Induste, 2020.)

5 PALVELIMEN KÄYTTÖÖNOTTO

Tulevilla sivuilla käsitellään, asennetaan, määritellään ja esitetään DNS-palvelimen käyttöönotto alla olevan prosessikaavion määrittelyn mukaisessa kokonaisuudessa ja toimintajärjestyksessä. Ensimmäisenä keskitytään alustan valintaan ja testiympäristöön. Tämän jälkeen siirrytään yleisiin alustan valmisteluihin ja asennukseen. Edellisen jälkeen tehdään tarvittavia komentoja ja määrittelyjä Adguard Home:n asennusta varten. Lopuksi esitellään Adguard Home:n asennus, sen tuomat vaikutukset ympäristöön ja ominaisuudet. Lopulta esitetään valmiin DNS-palvelimen toiminta eri näkökulmista.



Kuva 4. Prosessikaavio määritettävästä kokonaisuudesta ja toimintajärjestyksestä.

5.1 Alustan valinta ja testiympäristö

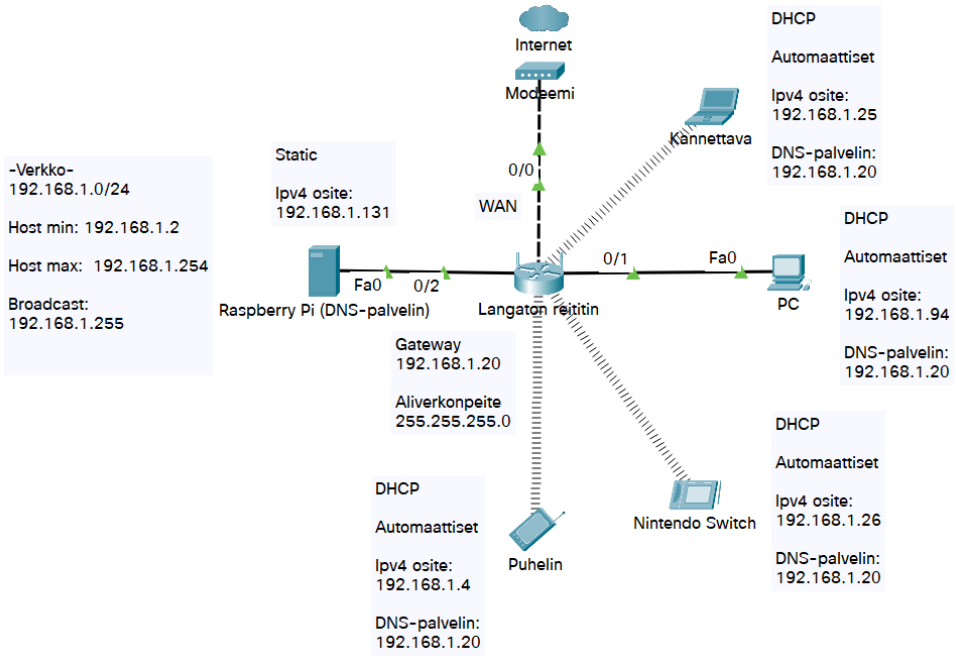
DNS sinkhole-palvelimen alustana toimii uusi 2 Gt keskusmuistia sisältävä Raspberry Pi 4B (kuva 1) ja massamuistina 32 Gt Micro-SD kortti. Vallitsevan komponentti pulan syystä saatavuus Raspberry Pi:n eri malleista on erittäin huono ja saatavilla olevien mallien hinta on normaalista huomattavasti korkeampi. Tästä huolimatta aikaisemmin mainittu malli, jonka pakettitarjouksen mukana tulivat lisäksi kaikki tarvittava, kotelo, virtalähde, microHDMI -kaapeli, passiiviset lämpösiilit ja Micro-SD kortti. Tämä paketti maksoi silti vain 149,90 euroa. Vanhoja käytettyjä pöytäkoneita saa huomattavasti edullisempaan hintaan, mutta Raspberry:n kompakti koko, alhainen virrankulutus, hiljaisuus riittävän passiivisen jäähdytyksen ansiosta ja luotettavuus tekevät siitä parhaan valinnan tähän kyseiseen käyttötarkoitukseen. Näiden seikkojen lisäksi Raspberry:lle on vuosien varrella muodostunut yhteisö eri harrastajia ja asiantuntijoita, joiden avulla eri ohjelmistot ja käyttöjärjestelmät ovat yleisesti hyvin optimoituja ja vakaita.

Kuten johdannossa jo mainittiin, lähiaikoina on tullut esille entistä enemmän DNS-huijauksia ja lisäturvaa saadaan asentamalla lähiverkkoon sinkhole-tyylinen DNS-palvelin. Tulevaisuudessa kolmannen osapuolen selainlaajennuksia mainosten ja sivustojen estoon tullaan mahdollisesti rajoittamaan. Lähiaikoina verkkosivustoilla ja eri alustoilla on esiintynyt mainoksia mainostenestolaajennusten käytöstä huolimatta. Eri sivustot ja palvelut myös keräävät paljon tietoja käyttäjästä ja käytettävästä laitteesta, jota käyttäjät eivät edes huomaa tai tiedä. Kuten myös luvussa 3 mainittiin, operaattorien nimipalvelimet tarjoavat suppeamman tietoturvan ja heidän on mahdollista valvoa kulkevaa internet liikennettä.

Ratkaisu tähän ongelmaan on asentaa oman lähiverkon kattava mainosten, seuraimien ja haitallisten sivustojen estävä ohjelmisto AdGuard Home Raspberry Pi:lle. Tämä tulee suojaamaan kaikki samaan verkkoon kytketyt laitteet. Päätelaitteille ei tarvitse asentaa muita ohjelmistoja ja mahdolliset selaimessa olevat mainostenesto-ohjelmistot esimerkiksi uBlock Origin voi halutessaan jättää. Esimerkiksi YouTubessa DNS-tasoinen mainostenesto ei ole

täydellinen nopeasti vaihtuvien kolmannen osapuolen mainospalvelimien takia. Selainlaajennus mahdollisesti poistaa mainokset, joita DNS-tason esto ei ehdi tai pysty poistamaan.

Alla olevassa kuvassa (kuva 5) on käytössä oleva ympäristö, johon palvelin tullaan asentamaan. Kyseessä on normaali 24-aliverkonmaskin C-luokan verkko. Verkko 192.168.1.0/24 on langattoman reitittimen DHCP-palvelimen (Dynamic Host Configuration Protocol) osoiteavaruuden määrittämä verkko käytettäville päätelaitteille. Palvelin tullaan asentamaan määrittämällä tälle staattinen pysyvä IP-osoite 192.168.1.131. Päätelaitteet saavat nimipalvelimen IP-osoitteen automaattisesti reitittimen kautta.



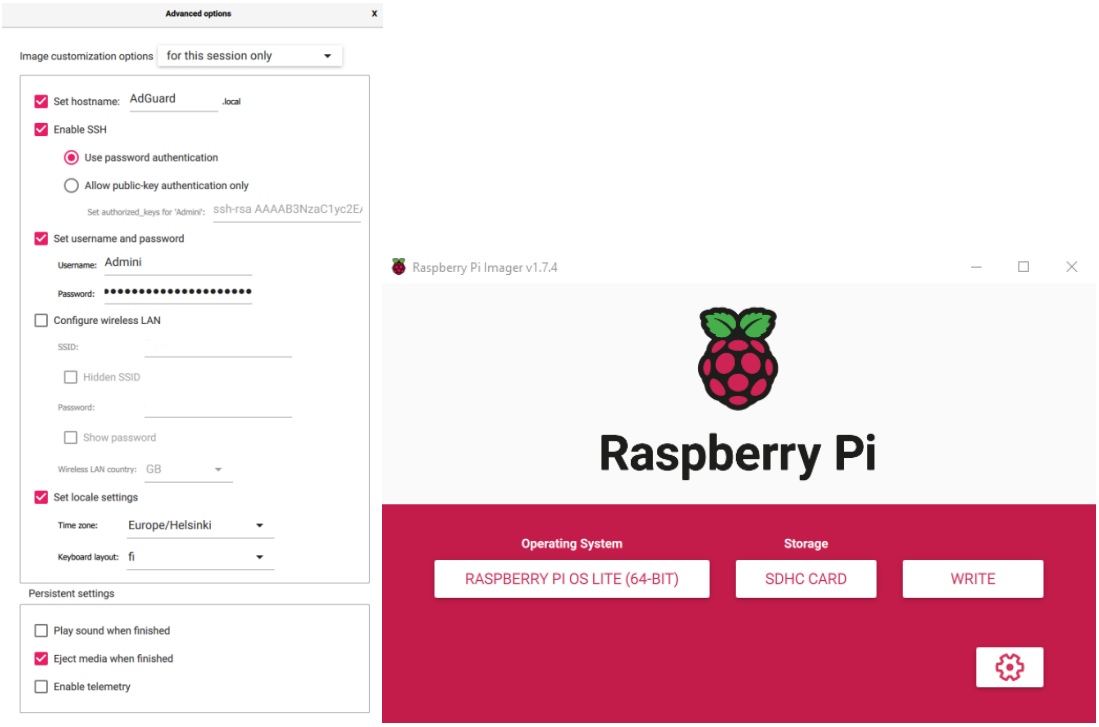
Kuva 5. Kuvankaappaus Cisco Packet Tracer:illa luodusta käytössä olevasta verkkotopologiasta.

5.2 Raspberry Pi OS Lite

Raspberry Pi:lle kehitetty käyttöjärjestelmä Raspberry Pi OS, joka on aiemmin tunnettu nimellä Raspbian. Raspberry Pi OS:n Lite-versio on Debian:in uusimpaan versioon 11 perustuva minimaalinen levykuva (image). Tämä sisältää vain ydinkäyttöjärjestelmän ja käynnistyy komentoriville graafisen työpöydän sijasta. (Mullins, 2020.)

2 helmikuuta 2022-alkaen on ollut mahdollista asentaa Raspberry Pi OS Lite vakaana 64-bittisenä versiona. 64-bittinen käyttöjärjestelmä on julkaistu ja tuettu tällä hetkellä Raspberry Pi 3:lle, 4:lle ja Zero 2:lle, ja saavuttaa hieman nopeamman prosessoinnin yleisesti ottaen 32-bittiseen versioon verrattaessa. (Adrian, 2022.) Palvelimella käyttöjärjestelmä ei yleensä tarvitse erillistä graafista työpöytää, koska kaikki tarvittavat määrittelyt ja hallinta onnistuu komentorivin avulla. Graafisen työpöydän uupuminen myös vähentää palvelimen näytönohjaimen kuormitusta ja yleistä laitteiston resurssien käyttöä.

Levykuvan kirjottaminen ja yleisien asetusten määrittäminen kuten isäntänimen (hostname), SSH:n, käyttäjätilin luonti, näppäimistön ja lokaation asetus, onnistuvat yksinkertaisesti Micro-SD kortille käyttäen Raspberry Pi Imager -ohjelmistoa (kuva 6). Ohjelmiston kirjottaessa levykuvan Micro-SD kortille, kortti siirretään tämän jälkeen Raspberry Pi:hin ja käynnistetään määritystä varten kytkemällä näppäimistö, hiiri ja näyttö. Asetusten määrittely ja hallinta onnistuu myös päättömästi (headless) SSH:n avulla. Palvelin tullaan määrittelemään ja ylläpitämään tässä tapauksessa SSH:lla nopean ja yksinkertaisen hallinnan takia.



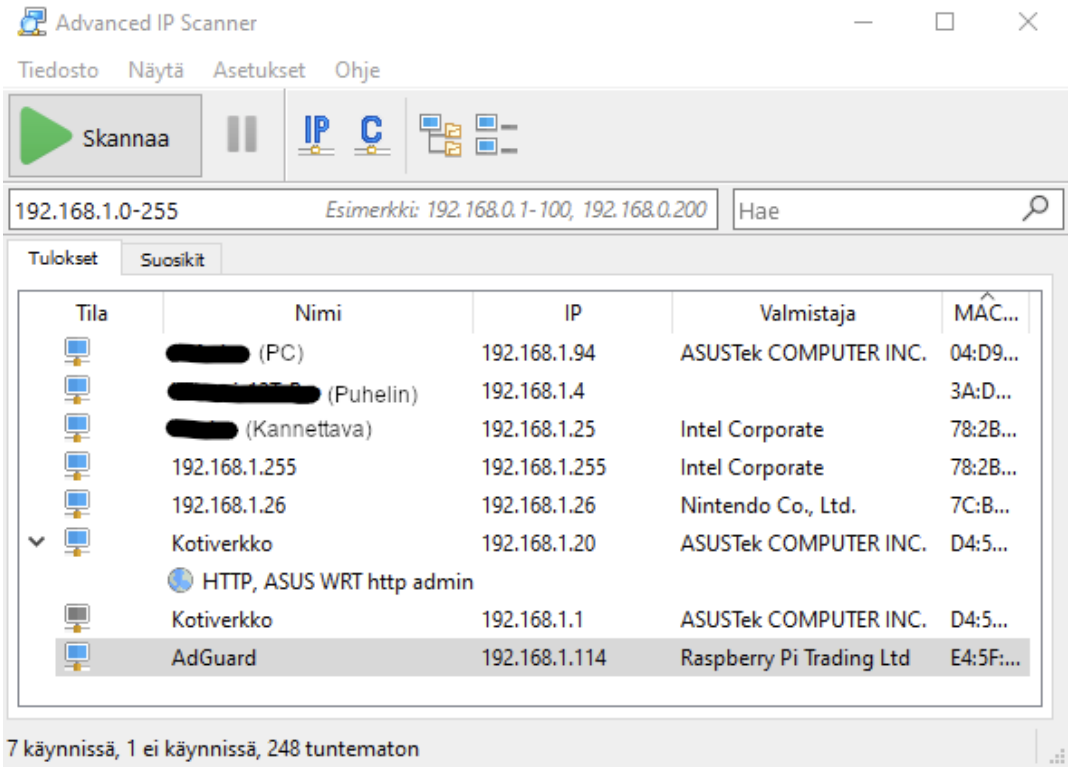
Kuva 6. Kuvankaappaukset Raspberry Pi Imager-ohjelmiston advanced välilehdelle määritellyistä asetuksista ja alkunäkymästä.

5.3 SSH ja sen käyttäminen palvelimen määrittelyyn

SSH eli Secure Shell Protocol on etähallintaprotokolla, jonka avulla voi käyttää, hallita ja muokata etäpalvelimia internetin kautta. SSH-palvelu luotiin turvalliseksi korvaajaksi vanhemmalle salaamattomalle Telnet:ille. SSH varmistaa, että kaikki viestintä etäpalvelimelle ja etäpalvelimelta tapahtuu salattuna oletuksena TCP-portista 22. SSH käyttää kahta erillistä avainta salaukseen ja salauksen purkamiseen. Näitä kahta avainta kutsutaan julkiseksi ja yksityiseksi avaimeksi. Yhdessä nämä muodostavat julkisen ja yksityisen avaimen parin. Kuka tahansa voi käyttää julkista avainta viestin salaamiseen ja tämän voi purkaa vain vastaanottaja, jolla on hallussaan yksityinen avain. Ennen kuin SSH-yhteys palvelimelle myönnetään, toteutetaan tunnistetietojen todentaminen. Yleisesti SSH-käyttäjät käyttävät tunnistautumiseen käyttäjänimeä ja salasanaa. (Domantas, 2023.)

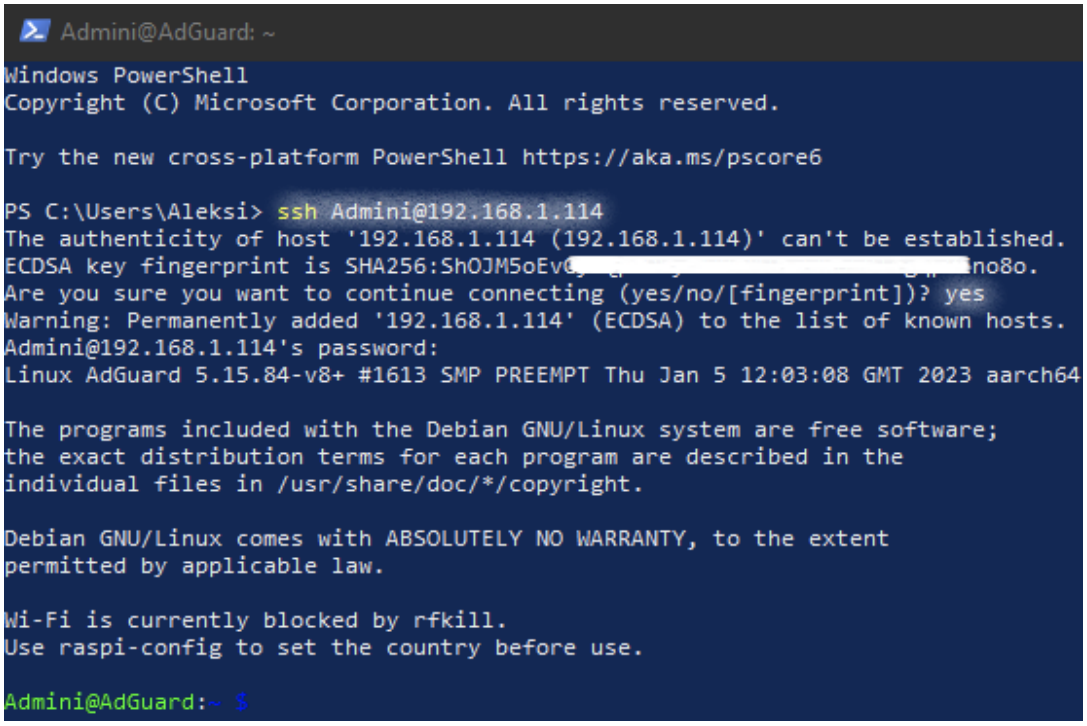
Avainparin luominen tehdään yleensä antamalla komento `ssh-keygen`. Yksityinen avain pysyy vain käyttäjällä ja julkinen avain lähetetään palvelimelle normaalisti `ssh-copy-id` komennolla. Palvelin tallentaa julkisen avaimen ja sallii pääsyn vain niille käyttäjille, joilla on vastaava yksityinen avain siihen. SSH yhdistämiseen käytetään yleisesti ohjelmia kuten PuTTY, Windows PowerShell, Windows:in tai Linux:in oma komentokehote (command prompt).

Ennen SSH:lla yhdistämistä täytyy tietää kohteen IP-osoite. Tässä tapauksessa Raspberry saa vapaan osoitteen reitittimen DHCP-palvelimen osoiteavaruudesta. Reitittimen antaman IP-osoitteen saa helpoiten selville katsomalla reitittimen hallintapaneelista, käyttämällä Advanced IP Scanner ohjelmistotyökalua (kuva 7) tai antamalla komento `arp -a` komentokehotteeseen. ARP (Address Resolution Protocol) yhdistää laitteiden IP-osoitteet kiinteään fyysiseen osoitteeseen eli MAC-osoitteeseen (Media Access Control). Komento `arp -a` näyttää tällä hetkellä tiedossa olevien osoitteiden reititystaulun.



Kuva 7. Kuvankaappaus suoritetusta verkonskannauksesta käyttäen tunnettua ja luotettavaa Advanced IP Scanner ohjelmistoa.

Yhdistäminen onnistuu tässä tapauksessa antamalla komento päätelaiteella PowerShelliin `ssh Admini@192.168.1.114`, jossa ensimmäinen on määritelty käyttäjänimi ja perässä kohteen IP-osoite. Kuten kuvassa 8 näkyy, ensimmäisellä yhdistyskerralla uudesta päätelaitteesta varoitetaan autenttisuuden todentamisen puutteesta ja esitetään tiedossa oleva julkisen SSH-avaimen sormenjälki. Tarkoituksena on varmistaa ja tunnistaa yhteyttä muodostava päätelaite. Ennen palvelimelle yhdistämisen hyväksymistä `yes` -komennolla täytyy varmistaa, että yhdistettävä kohde on oikea. Julkinen esitetty sormenjälki täytyy vastata palvelimen julkisen avaimen sormenjälkeä. Varoitus autenttisuudesta voi ilmetä uudelleen, jos SSH-palvelin on asennettu uudestaan palvelimella. Siirtyessä palvelimelle, päätelaiteelle tallentuu palvelimen osoite ja avain known hosts -tiedostoon.



Kuva 8. Kuvankaappaus ensimmäisestä SSH yhdistämisestä uudesta päätelaitteesta PowerShell:illä.

Aina uuden käyttöjärjestelmän asennuksen yhteydessä ensimmäisenä täytyy hakea ja asentaa uusimmat päivitykset. Linuxi:ssa tämä tehdään yleisesti päätteessä komennoilla, eikä graafisen sovelluksen kautta. Debian 11, johon Raspberry Pi Lite pohjautuu, uusimmat päivityspaketit saadaan haettua komennolla `sudo apt update`. Uusien päivityspakettien asentaminen ja käyttöönotto toteutuu komennolla `sudo apt upgrade` tai `sudo apt full-upgrade`, joka poistaa myös vanhat käyttämättömät paketit. `Sudo apt autoremove` komentoa voidaan myös käyttää poistamaan paketteja, jotka asennettiin automaattisesti muiden pakettien riippuvuuksien täyttämiseksi. Tämän komennon käyttöjärjestelmä mainitsee, jos huomaa käyttämättömiä paketteja ohjelmiston poiston yhteydessä, joita ei enää tarvita.

5.4 AdGuard Home:n asentaminen, määrittely ja ominaisuudet

Ennen AdGuard Home:n asentamista täytyy Raspberry:lle määritellä staattinen IP-osite. Tämä varmistaa, että SSH-yhdistäminen onnistuu jatkossakin samaan osoitteeseen ja reititin päätelaitteineen tietävät aina missä osoitteessa nimipalvelin sijaitsee. IP-osoitetiedot saadaan määriteltyä muokkaamalla dccpcd.conf tiedostoa komennolla `sudo nano /etc/dhcpcd.conf`. Tähän tiedostoon tehdään kuvan 9 mukaiset määrittelyt. Interface määrittelee käytetäänkö Wi-Fi:ä vai ethernet:tiä. Static ip adress asettaa Raspberry:lle staattisen pysyvän IP-osoitteen ja static routers määrittää gateway -osoitteen reitittimelle, jota kautta yhdistetään verkkoon. Static domain name servers on nimipalvelimen osoite. Osoite 127.0.0.1 on localhost -osoite, joka viittaa itse laitteeseen.

```
# Example static IP configuration:
#interface eth0
#static ip_address=192.168.0.10/24
#static ip6_address=fd51:42f8:caae:d92e::ff/64
#static routers=192.168.0.1
#static domain_name_servers=192.168.0.1 8.8.8.8 fd51:42f8:caae:d92e::1

# It is possible to fall back to a static IP if DHCP fails:
# define static profile
#profile static_eth0
#static ip_address=192.168.1.23/24
#static routers=192.168.1.1
#static domain_name_servers=192.168.1.1

# fallback to static profile on eth0
#interface eth0
#fallback static_eth0

interface eth0
static ip_address=192.168.1.131/24
static routers=192.168.1.20
static domain_name_servers=127.0.0.1
```

Kuva 9. Kuvankaappaus dccpcd.conf tiedostoon määritellyistä IP-asetuksista.

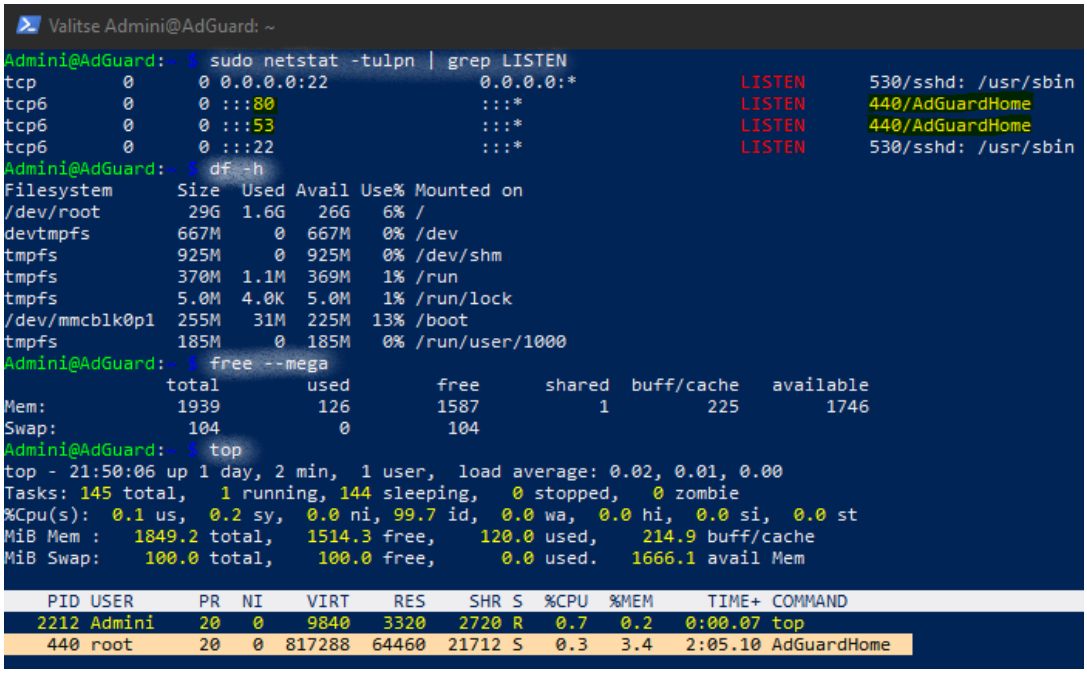
AdGuard Home avaa portin 53, joka on yleinen portti DNS-kyselyjä varten. Debian:iin on määritelty oletuksena oma system resolved määrittely DNS-kyselyjä varten portissa 53. Tämä on suositeltavaa ottaa pois käytöstä, koska käytetään omaa AdGuard:in DNS-palvelinta.

System resolved saadaan otettua pois käytössä komennoilla `sudo systemctl stop systemd-resolved` ja tämän jälkeen `sudo systemctl disable systemd-resolved`. Nämä ja edelliset määrittelyt astuvat voimaan käynnistämällä Raspberry uudelleen komennolla `sudo reboot`.

AdGuard Home asentuu yksinkertaisesti Raspberry:lle alla olevan kuvan (kuva 10) komennolla. Komennon suorittamisessa tapahtuu virhe, koska verkkotunnuksen IP-osoitetta ei pystytä selvittämään. Tämän syynä on määritelty localhost-osoite. Raspberry:lle täytyy määrittää nimipalvelimen osoitteeksi gateway:n osoite, jossa nimipalvelin vielä sijaitsee. Väliaikaisen nimipalvelin osoitteen muutoksen jälkeen komento suoriutuu ja Adguard Home asentuu. Raspberry pystyy nyt käsittelemään verkkotunnusten IP-osoite vastineet AdGuard:in kautta, joten kuvan 8 määritykset voidaan palauttaa.

Kuva 10. Kuvankaappaus AdGuard Home:n asentavasta komennosta.

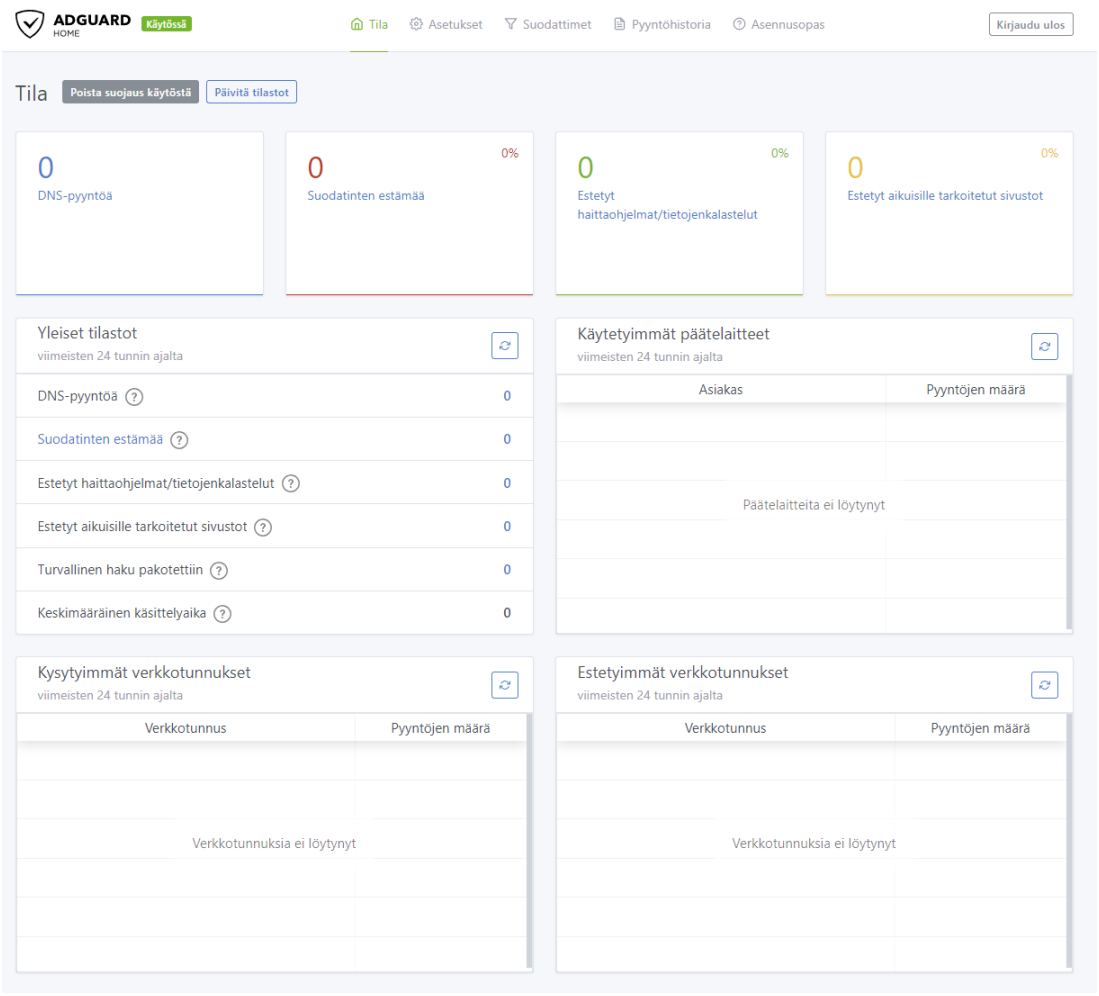
Adguard Home:n tekemät muutokset järjestelmään ja laitteiston kuormituksen voidaan tarkastella eri komennoin (kuva 11). `Sudo netstat -tulpn | grep LISTEN` komento, jossa listataan kaikki TCP ja UDP portit suodattaen listaukseen vain avoinna olevat portit. Adguard Home on määritellyt ja avannut portit 80 ja 53. Portti 80 on yleinen HTML portti, jossa pyörii paikallisesti Adguard Home:n web server hallintapaneeli. Komennoin `df -h`, `free --mega` ja `top`, nähdään tallennustilan käyttö, keskusmustin käyttö megatavuina ja yleinen listaus eri suoritteillaan olevista prosesseista ja niiden laitteisto kuormituksen. Kuten tilastoista huomataan AdGuard Home on hyvin kevyt ja pieni ohjelmisto suorittaa.



Kuva 11. Kuvankaappaus suoritetuista komennoista.

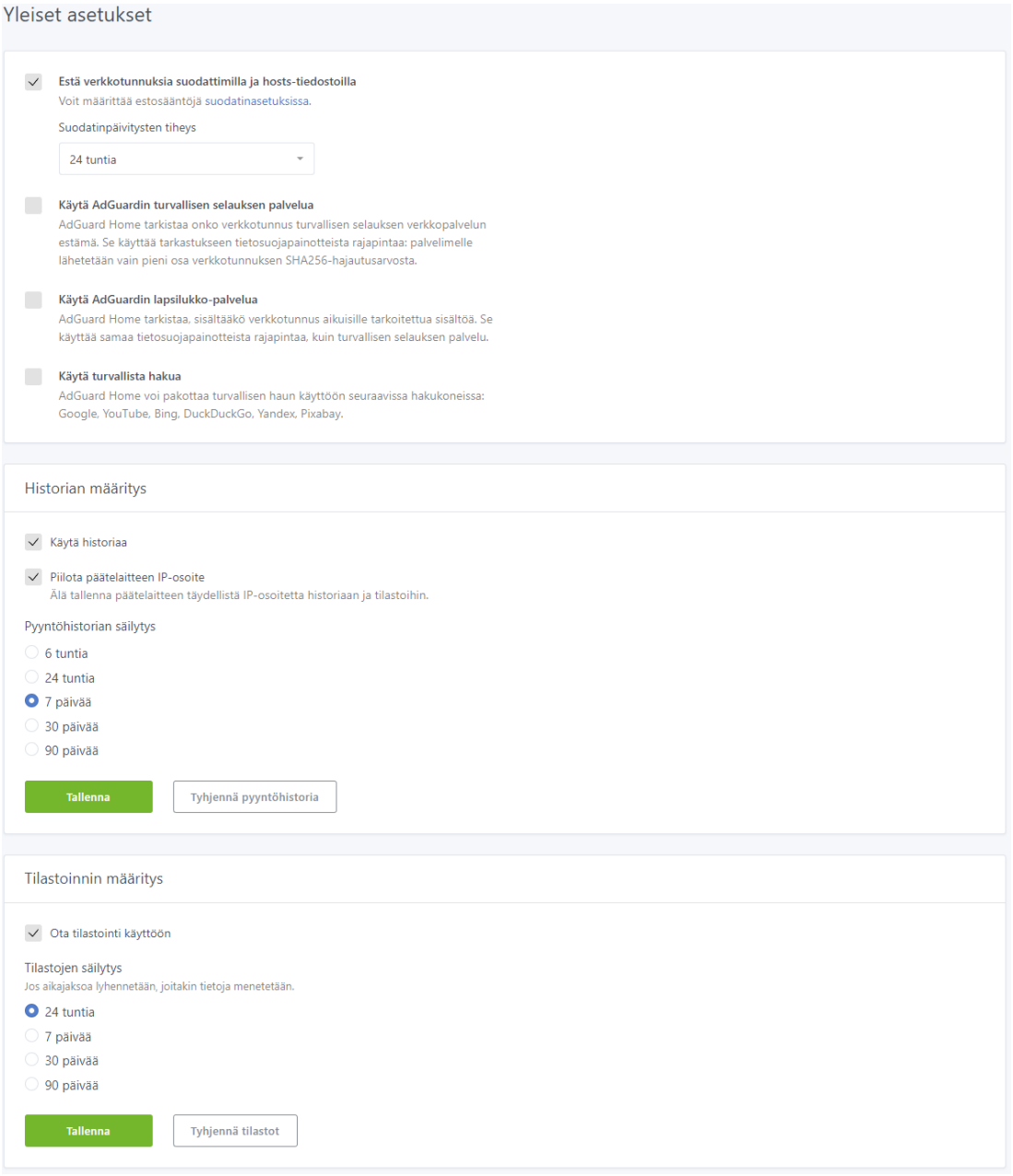
Adguard Home:n hallintasivun avulla määritetään kaikki DNS-asetukset, suodatinlistat ja muut yleiset asetukset ja päivitykset. Hallintapaneeliin pääsee kirjoittamalla selaimeen Raspberry:n IP-osoitteen. Alkuesittelyn, käyttäjänimen ja salasanan asettamisen vaiheiden jälkeen avautuu monitorointi ja tilasto näkymä (kuva 12). Adguard Home sisältää kattavan kokonaisuuden muokattavuutta ja määrittelyä. Adguard Home:n voi myös esimerkiksi määritellä DHCP-palvelimeksi ja hallintapaneelin voi salata HTTPS:sään. Tämän tekeminen vaatii varmenteen ja domainin hankkimista. Sisäverkossa tämä ei ole tarpeellista ja reititin toimii DHCP-palvelimena.

Seuraavilla tulevilla sivulla käydään läpi ainoastaan kohtia ja asetuksia, joihin on tehty määrittelyjä ja muutoksia.



Kuva 12. Kuvankaappaus hallintapaneelin aloitusnäkymästä asennuksen jälkeen.

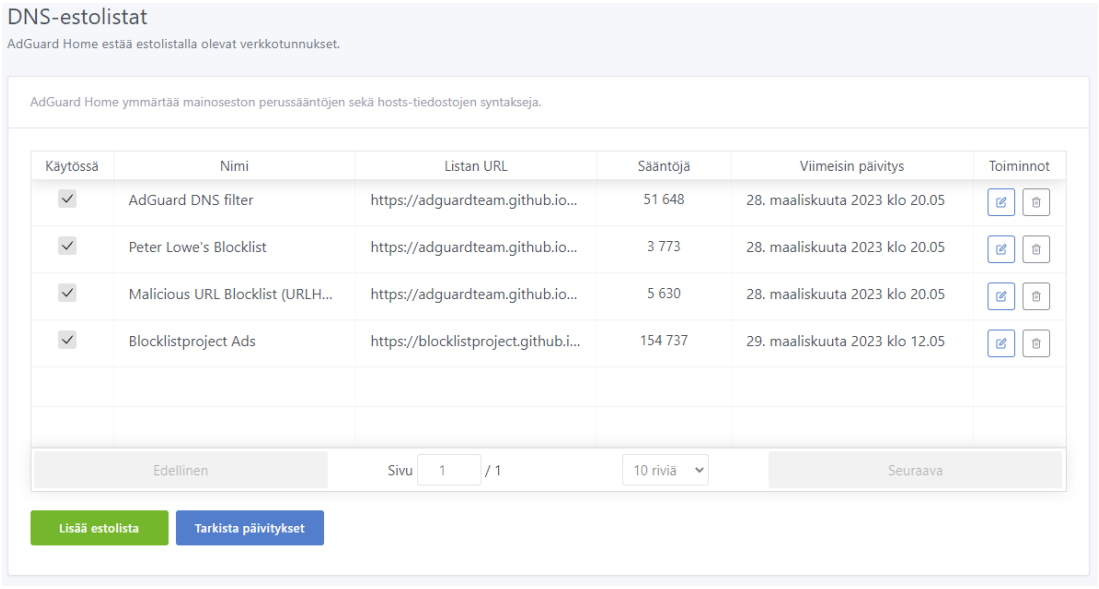
Yleisissä asetuksissa (kuva 13) voidaan määritellä erillisten DNS-estolistojen päivitys tiheys. Eri haitalliset osoitteet, mainospalvelimet ja seuraimet vaihtelevat ja lisääntyvät jatkuvasti, joten näitä tulee jatkuvasti päivittää. Pyyntöhistoria, joka sisältää kaikki hyväksytyt ja estetyt DNS-kyselyt kaikilla laitteilla, säilytetään vain seitsemän päivän ajalta ilman tarkkoja laitteiden IP-osoitteita. Tämän jälkeen historia tyhjennetään Raspberry:n tilan säästämiseksi ja yksityisyyden suojaamiseksi. Tilastoinnit näkyvät hallintapaneelin etusivulla, jotka sisältävät päivän ajalta kysytyimmät ja estetyimmät verkkotunnukset.



Kuva 13. Kuvankaappaus Adguard Home:n yleisten asetuksien välilehdeltä.

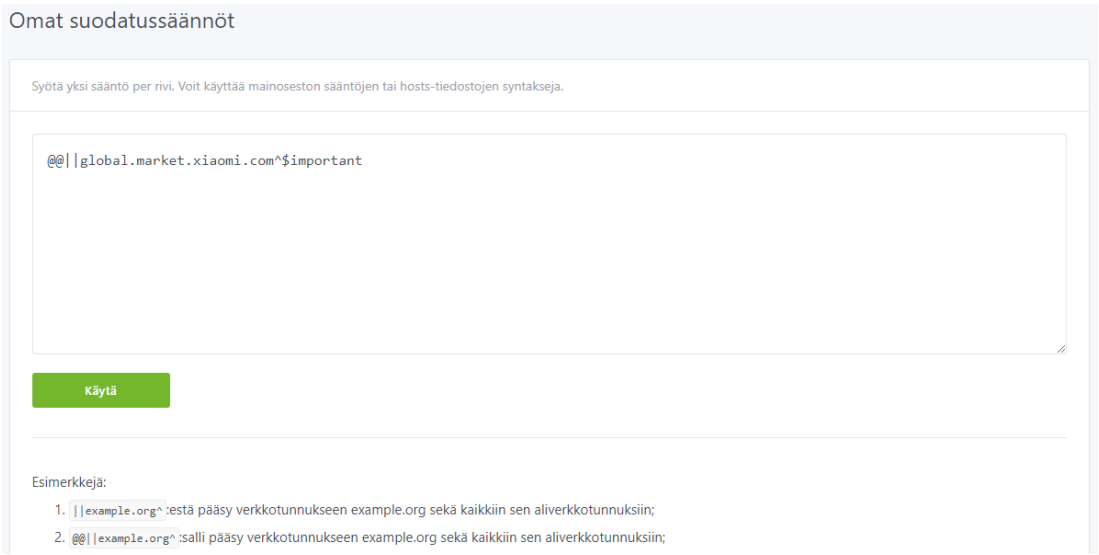
Oletuksena Adguard Home käyttää ainoastaan yhtä suurta ylimpänä olevaa estolistaa (kuva 14). Painikkeella lisää estolista voidaan lisätä muita AdGuard Home:n valmiiksi listattuja ja tuettuja estolistoja. Peter Lowe's blocklist ja Malicious URL Blocklist ovat molemmat luotettavia ja toimivia estolistoja, jotka sisältyvät myös uBlock Origin: iin oletuksena. Nämä estolistat suodattavat pois yleisiä seuraimia verkossa ja estävät haitallisille sivuille pääsyn palomuurin tapaisesti. Erillisiä estolistoja AdGuard Home:n valmiiksi listattujen lisäksi voi lisätä, jos nämä on kirjoitettu AdGuard:in omalla tuetulla syntaksilla. Blocklistproject Ads on suuri ja tehokkaasti toimiva erillinen yli 150-tuhatta riviä sisältävä listaus mainos- ja seurainpalvelimien estämiseksi.

Estolistoissa enempi ei välttämättä ole parempi. Liian aggressiivinen estolistojen käyttö voi rikkoa eri sivuja ja tehdä eri palveluja käyttökelvottomaksi. Usean suuren estolistan lisääminen myös kuormittaa ja hidastaa palvelinta enemmän.



Kuva 14. Kuvankaappaus määritetyistä Adguard Home:n DNS-estolistoista.

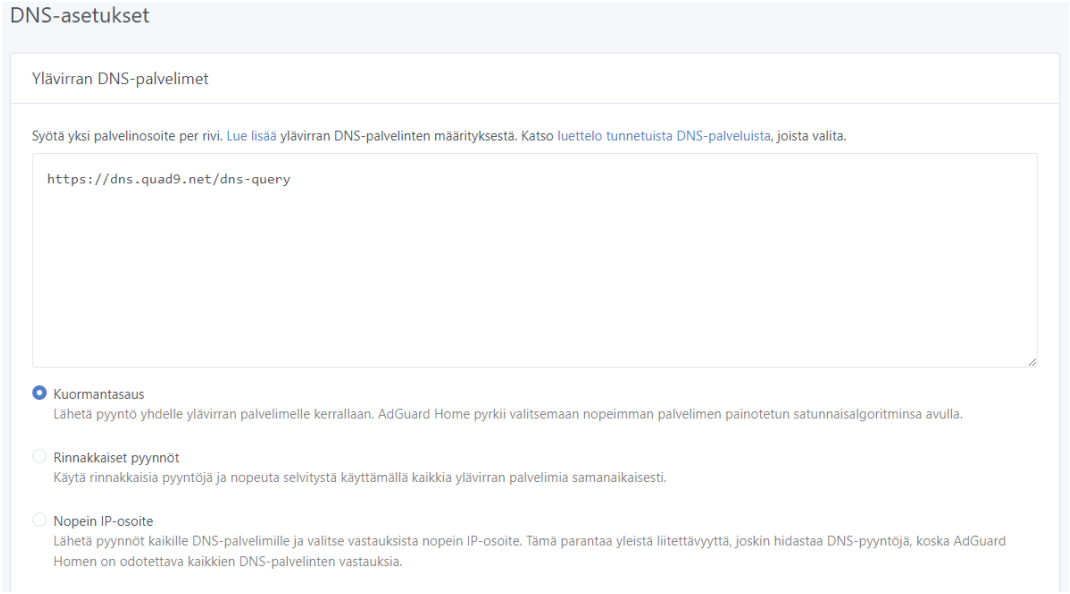
Omia DNS-suodatussääntöjä voi estolistojen lisäksi manuaalisesti määrittää. Esimerkkinä kuvassa 15 sallitaan verkkotunnus, jonka kautta Xiaomi:n puhelin hakee päivityksiä järjestelmäsovellusten päivittäjä sovelluksessa. Ilman tätä määritystä Blocklistproject Ads estolista estää tämän verkkotunnuksen ratkaisemisen. Sallimisen lisäksi eri verkkotunnuksia voidaan myös kieltää ja Ad Guard Home sisältää myös välilehden Estetyt palvelut, jonka avulla voi kokonaan estää käyttämästä esimerkiksi eri sosiaalisen median palveluita.



Kuva 15. Kuvankaappaus Adguard Home:n omat suodatussäännöt välilehdeltä.

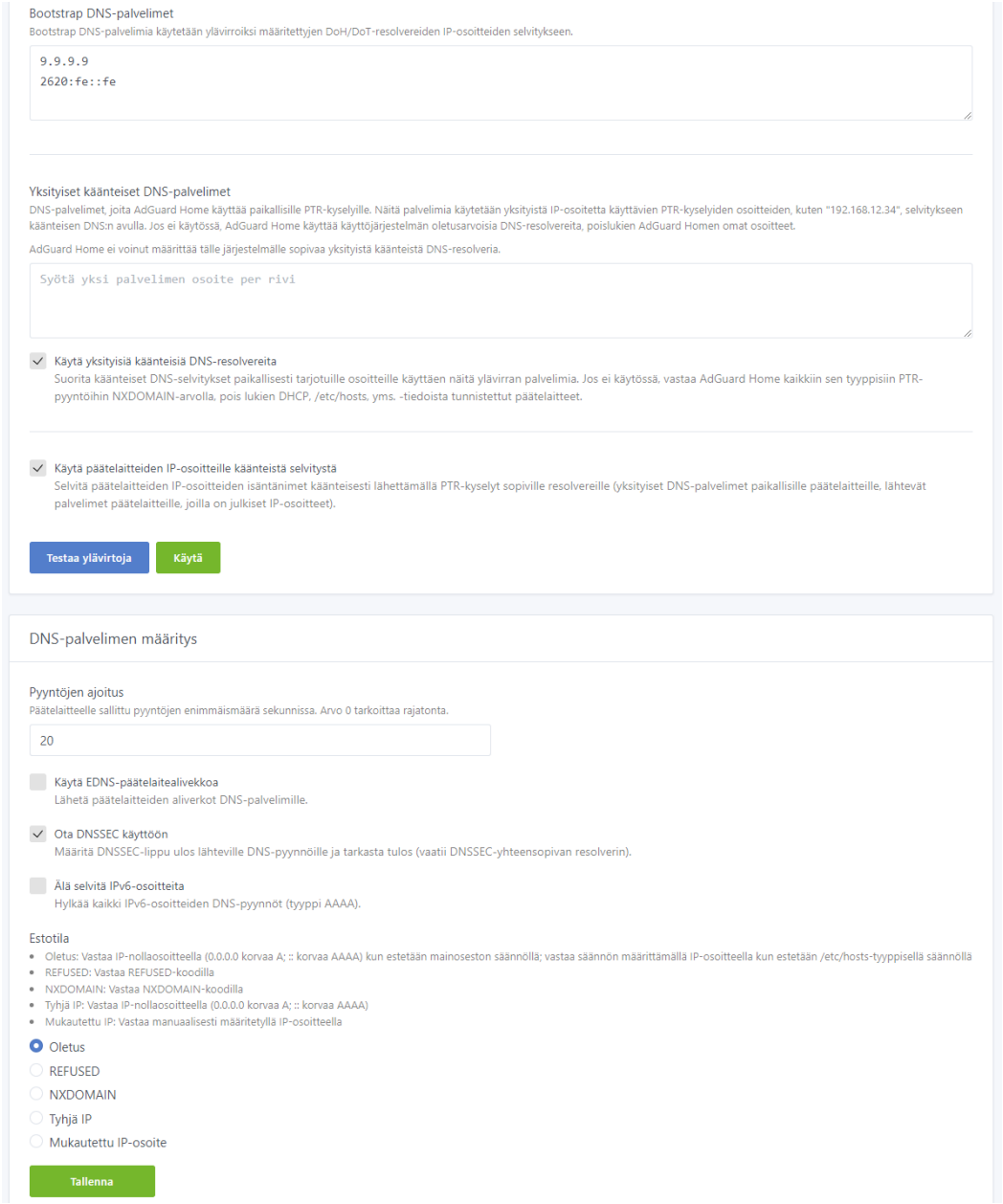
Adguard Home ei toimi resolverina. Adguard Home välittää DNS-kyselyn salattuna DoH:n avulla erillisille julkisille ylävirran eli upstream DNS-resolvereille. Oletuksena Adguard Home käyttää yllättävästi Quad 9:stä osoitetta, joka ei sisällä DNSSEC-todennusta ja haittaohjelmien estolistaa. Kuvassa 16 on määritelty käyttämään resolverina Quad 9:sin oletusosoitetta, joka sisältää DNSSEC-todennuksen ja suodatinlistan haittaohjelmista ja haitallisista sivustoista. Määritelty revolveri selvittää kysytyn verkkotunnuksen IP-osoitevastineen ja Adguard Home:n kautta selvitetty IP-soite siirtyy sitä kysyttävälle päätelaitteelle.

Adguard Home:en on myös mahdollista halutessaan määrittää useita eri julkisia resolvereita. Tämä voi nopeuttaa DNS-kyselyjen käsittelyaikaa, koska Adguard Home pyrkii tällöin lähettämään kyselyt aina nopeammalle resolverille tai usealle samanaikaisesti.



Kuva 16. Kuvankaappaus Adguard Home:en määritetyistä ylävirran DNS-palvelin asetuksista.

DNS-palvelimen asettamisen jälkeen tulee Bootstarp -osoitekenttään antaa resolverin salatun HTTPS verkkotunnuksen IP-osoite vastine (kuva 17). Bootstarp DNS-palvelimia käytetään ylävirroiksi määritettyjen DoH-resolver:ien IP-osoitteiden selvitykseen. Quad 9:siilä nämä osoitteet ovat 9.9.9.9 ja IPv6 osoite 2620:fe::fe. Quad9 tukee DNSSEC-todennusta, joten tämän voidaan ottaa käyttöön AdGuard Home:ssa. DNSSEC-todentamisen onnistuminen verkkotunnukselle ilmaistaan AdGuard Home:n pyyntöhistoriassa vihreällä lukko symbolilla.



Kuva 17. Kuvankaappaus Adguard Home:n DNS-asetukset välilehdelle tehdystä määrittelyistä.

6 PALVELIMEN TOIMINNALLISUUS

Adguard Home:n asetusten määrittelyn jälkeen reititin ja siihen yhdistetyt päätelaitteet täytyvät tietää missä nimipalvelin sijaitsee. Asus-reitittimessä tämä onnistuu yksinkertaisesti määrittelemällä manuaalisesti WAN DNS-asetuskohtaan DNS-palvelin1 kenttään Raspberry:n IP-osoite 192.168.1.131. Oletuksena nimipalvelimen IP-osoite on palveluntarjoajan määrittelemä.

Nimipalvelimen toiminnallisuuden voi varmistaa usealla eri tavalla. Adguard Home:en määritelty Quad 9 resolveri:n käyttö voidaan varmistaa tarkistamalla sivulla on.quad9.net. Jos sivuston vastaus on yes, Adguard Home välittää kyselyt quad9:n kautta. Antamalla komennon `nslookup -type=txt proto.on.quad9.net` Windows:in komentokehotteeseen kertoo käytettävän protokollan, joka tässä tapauksessa on DoH.

F-Secure Router Checker DNS-kaappaustestin avulla kuvassa nähdään oikealla vähemmän tarkkoja tietoja internetin käyttäjästä, koska quad9 käyttää useita eri palvelimia ja DNSSEC todentamista. Tämä parantaa ja lisää tietosuojaa ja tietoturvaa.

Router Checkerin tulokset:

DNS:n IP	62.197[redacted]
AS-numero	160[redacted]
AS-organisaatio	DNA Oy
Palveluntarjoaja	DNA Oy
Organisaatio	DNA Oy
Maanosan koodi	EU
Maanosan nimi	Europe
Maan koodi	FI
Maan nimi	Finland
Rekisteröity maan koodi	FI
Rekisteröity maan nimi	Finland
Tunnettu julkinen DNS-palvelin	

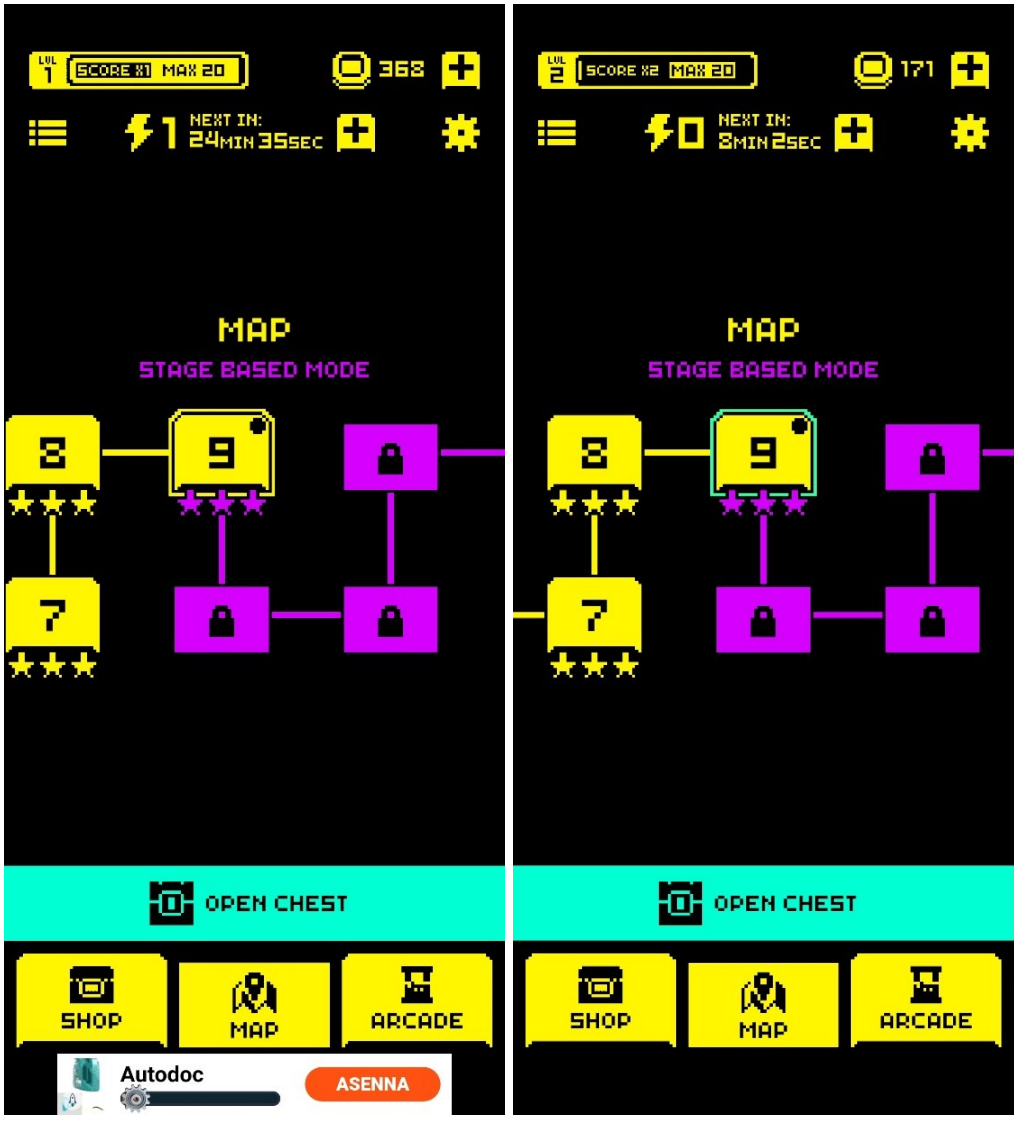
Router Checkerin tulokset:

DNS:n IP	109.200[redacted]
AS-numero	495[redacted]
AS-organisaatio	i3d B.V.
Palveluntarjoaja	i3d B.V.
Organisaatio	i3d B.V.
Maanosan koodi	EU
Maanosan nimi	Europe
Maan koodi	NL
Maan nimi	Netherlands
Rekisteröity maan koodi	NL
Rekisteröity maan nimi	Netherlands
Tunnettu julkinen DNS-palvelin	

Kuva 18. Kuvankaappaus F-Secure Router Checker tuloksista Adguard Home:n kautta (oikealla) ja ilman (vasemmalla).

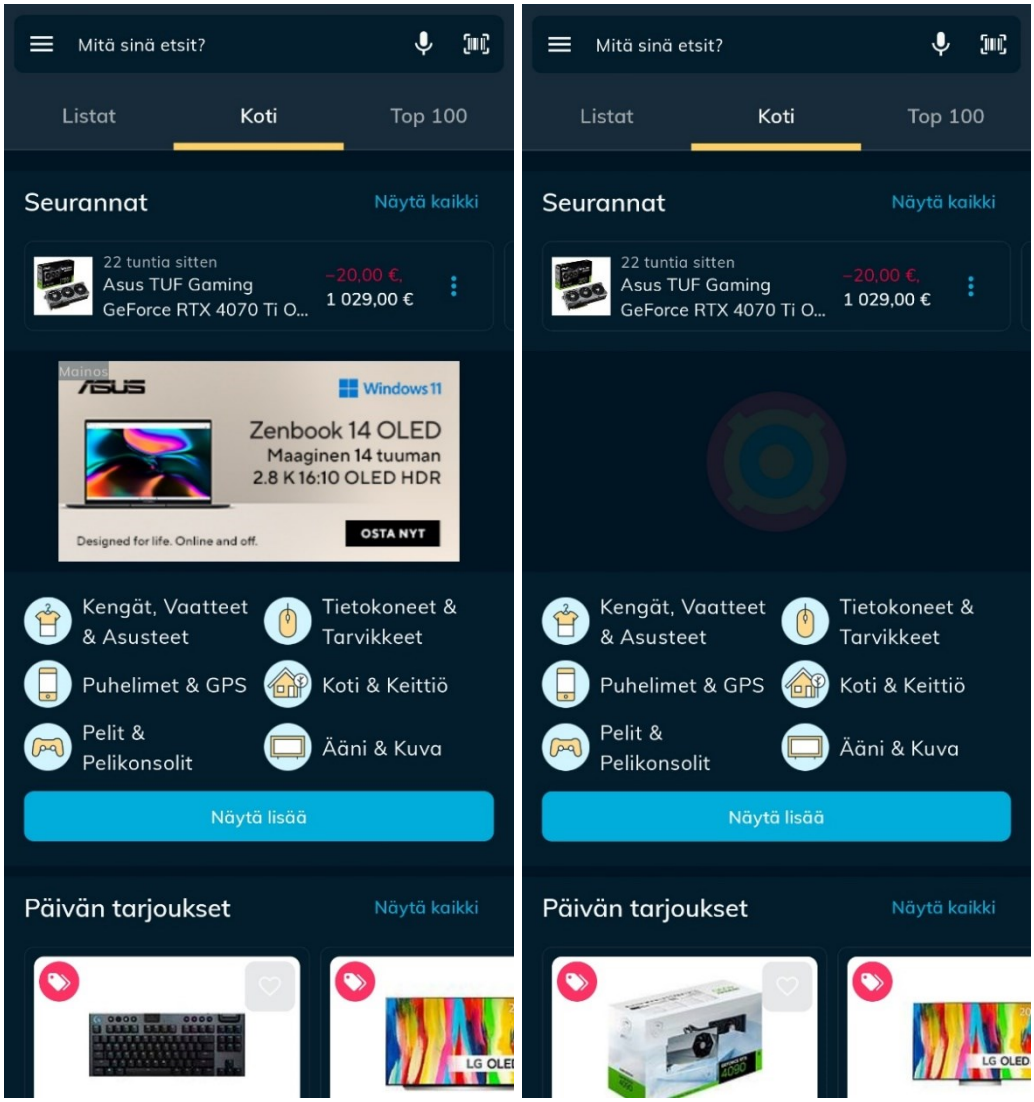
Loppukäyttäjille päällimmäisenä näkyy eri sivustojen, sovellusten ja pelien mainosten poistuminen lähes kokonaan näkyvistä ja verkkosivujen hieman nopeampi latausnopeus, kun mainoksia ja muita ärsykkeitä ja seuraimia ei tulla lataamaan kolmansilta osapuolilta. Kuten seuraavissa tulevissa kuvankaappaus esimerkeissä nähdään vasemmalla puolella ilman AdGuard Home:n käyttöä ja oikealla puolella AdGuard Home:n kanssa.

Alla olevassa kuvassa vasemmalla nähdään mobiilipeleissä hyvin yleinen häiritsevä bannerimainos. Mainokset eivät välttämättä ole haitallisia, mutta voivat kerätä tietoja käyttäjästä niitä painaville. Myös Ilman Adguard Home:a jokaisen kentän läpäisyn jälkeen peliin ilmestyi lyhyt kokonäytön videomainos.



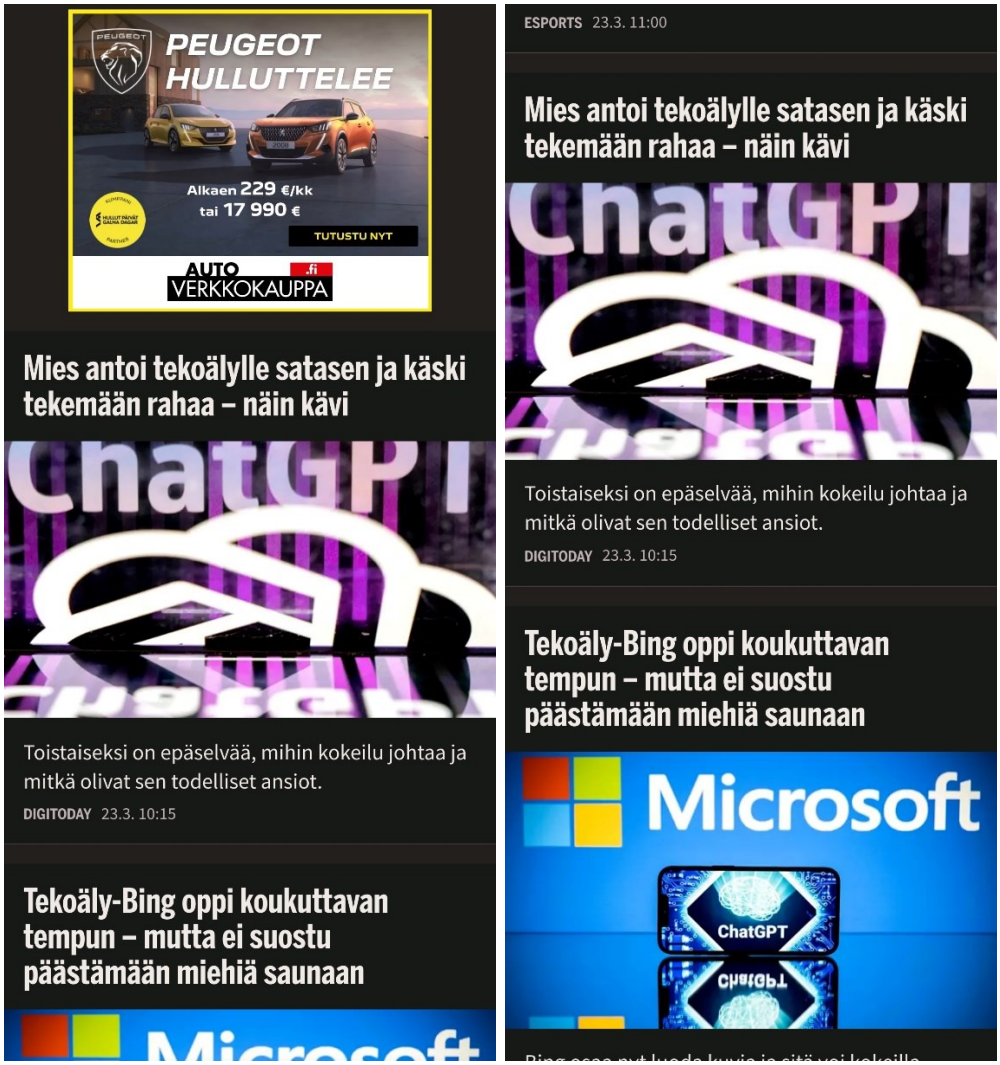
Kuva 19. Kuvankaappaukset tunnetusta mobiilipelistä Tomb of the Mask, joka käyttää yleistä bannerimainosta.

Alla olevassa kuvassa nähdään hintaopas-sovellus, jossa mainoksille on varattu kiinteä pysyvä paikka. Tämän tyyppisten mainosten poisto jättää sovellukseen tai samantyylistä mainostustapaa käyttäville sivustoille tyhjän paikan. Tämä on silti parempi ja vähemmän häiritsevä käyttäjälle.



Kuva 20. Kuvankaappaukset hintaopas-sovelluksesta, joka käyttää natiivimainontaa.

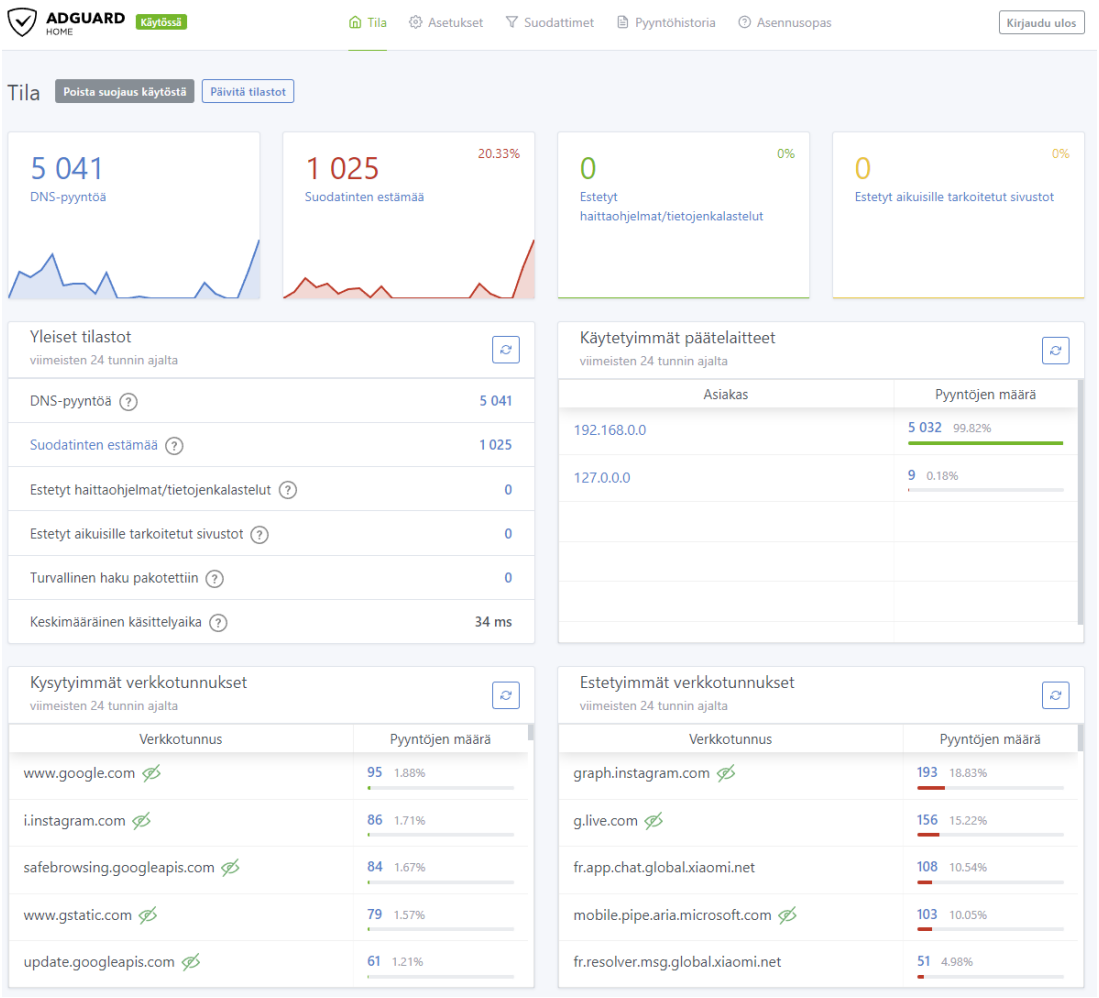
Alla on verkkosivustolta Ilta-Sanomat kuvankaappaukset ilman Adguard Home:a ja sen kanssa. Verkkosivustoilla on yleisesti riippuvia normaalia mainoksia, joille ei ole varattu erillistä paikkaa manuaalisesti. Mainosten poistaminen ei jätä jälkiä sivustolle, ja sivusto mukautuu dynaamisesti ilman mainosta.



Kuva 21. Kuvankaappaukset Ilta-Sanomista, joka käyttää normaalia mainosta ilman staattista paikkaa.

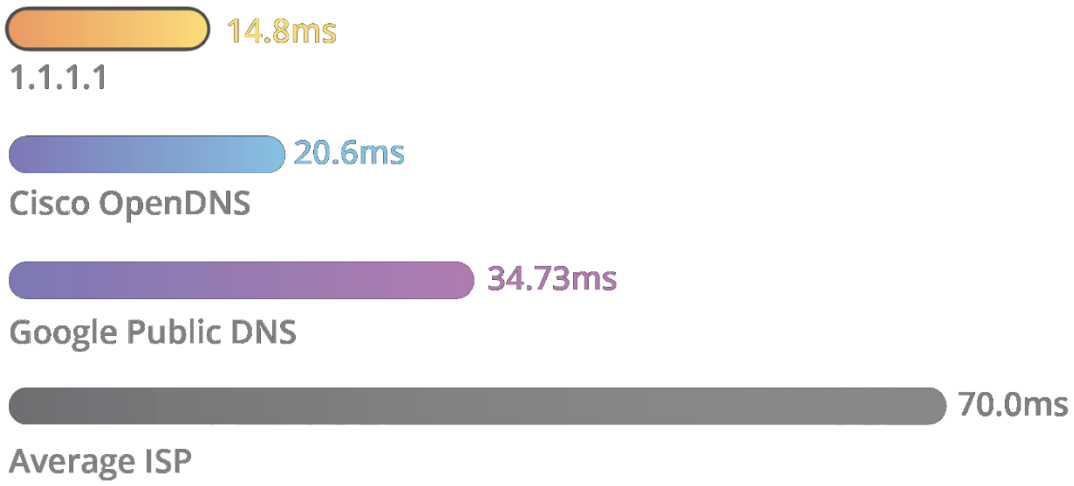
Kuten alla olevasta tilastoista nähdään liikenteestä, on suodatettu pois huomattava määrä eri mainospalvelimia ja käyttäjästä dataa keräämiä tahoja. Tilastot ovat määritelty säilyvän 24-tuntia, joka on myös Adguard Home:n oletus asetus. Jo noin 24-tunnin aikana on tehty yli viisituhatta DNS-pyyntöä ja näistä noin viidesosa on suodatettu pois eri suodattimien toimesta.

Sosiaaliset mediat kuten tässä tapauksessa Instagram on estetyimpien verkkotunnusten ensimmäisenä. Varsinkin Sosiaaliset mediat keräävät ja seuraavat paljon palvelun käyttäjää eri verkkotunnusten kautta. Toisena on suuryritysten verkkotunnukset Microsoft ja Xiaomi, jotka tiedetäänkin keräävän käyttäjästä dataa taustalla ja Xiaomi käyttää myös eri mainospalvelimia. Ilman Adguard Home:a näitä ei huomioitaisi ollenkaan.



Kuva 22. Kuvankaappaus hallintapaneelin aloitusnäkymästä olevista tilastoista.

Kuten edellisestä kuvasta huomataan keskimääräinen käsittelyaika 24 tunnin aikana on ollut 34 millisekuntia. Yleisesti käsittelyaika on vaihdellut yli 20 millisekunnin ja alle 40 millisekunnin välillä. Alla olevassa kuvassa nähdään Cloudflare:n väittämät keskiarvoiset käsittelyajat yleisille DNS-palveluntarjoajille. Suomalalaisten operaattoreiden nimipalvelimien käsittelyajat ovat Cloudflare:n väittämää käsittelyaikaa huomattavasti alhaisempi.



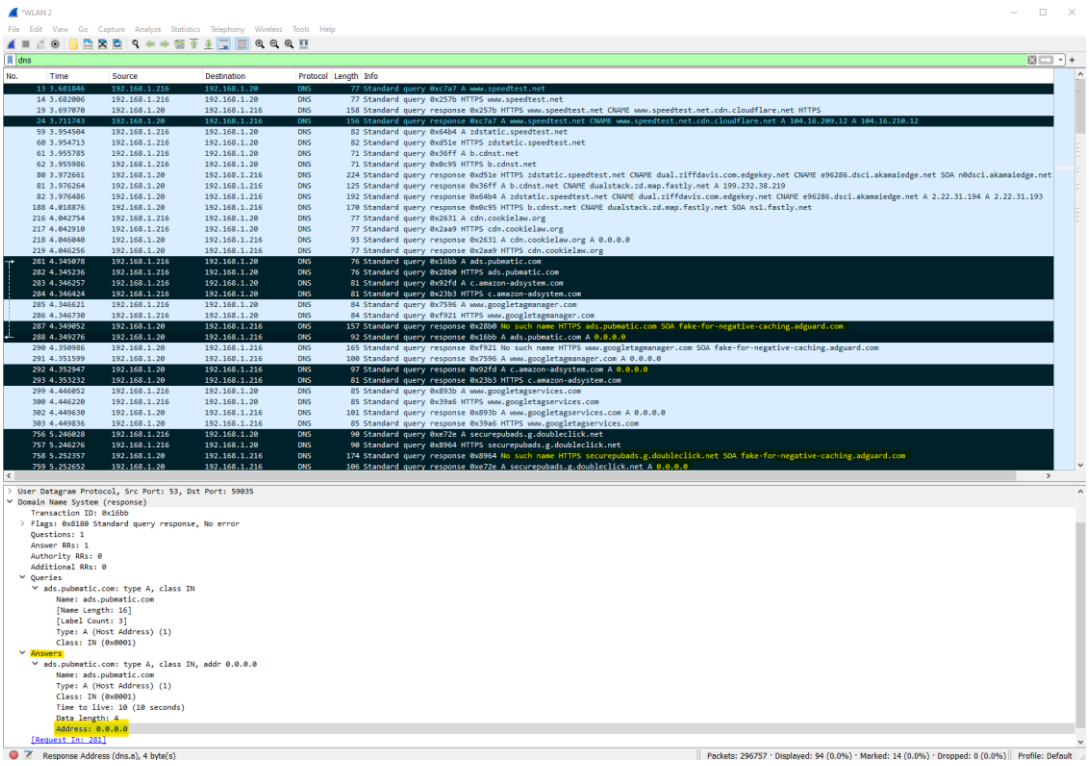
Kuva 23. Keskiarvoiset kyselynopeudet eri DNS-palveluntarjoajilla Cloudflaren mukaan. (Cloudflare, n.d.)

Yleinen verkonnopeus ja viive Adguard Home:a käyttäessä ei hidastunut. Ilman Adguard Home:a ja Adguard Home:n kanssa, Ookla:n Speedtest -sivuston mukaan nopeustulokset ja ping-viive olivat samat.

Testatessa Ilta-Sanomat verkkosivulle siirtyessä saatiin tulokset 1.07,1.10 ja 1.12-sekunttia. Ajat otettiin Firefox-selaimessa Ilta-Sanomat sivuston linkkiä hakutuloksissa klikkaamalla ja lopettamalla, kun sivuston sisältö latautui. Tuloksien välissä tyhjättiin selaustiedot. Puolestaan ilman AdGuard Home:a tulokset olivat 1.65, 1.56 ja 1.52-sekunttia. Nämä luvut eivät ole kaukana toisistaan, koska Ilta-Sanomat-sivustolla ei ole kovin paljon erillisiä mainoksia, ja käytössä olevan verkon latausnopeus on hieman yli 200 megabittiä sekunnissa. Loppukäyttäjä huomaa silti eron nopeudessa ja mainosten häviämisessä. Lisäksi Ilta-Sanomat sivuston eväste kysely estyy Adguard Home:n avulla, jota edes uBlock Origin selaintasoinen mainostenesto-ohjelmisto ei pysty estämään.

Huomattavamman eron nopeudessa saavutetaan siirtyessä sellaisille sivustoille verkossa, joissa käytetään suuri määrä mainontaa ja eri seuraamia.

Esimerkiksi aikaisemmin mainittu Ookla:n Speedtest -sivusto sisältää useita mainoksia. Verkkosivustolle siirtyessä sivusto lataa myös samalla useita eri mainos sivustoja. Näiden mainos sivustojen hakua voidaan tarkemmin analysoida Wireshark -nimisellä pakettianalysaattori ohjelmalla. Wireshark:in avulla pystytään kaappaamaan, tallentamaan ja analysoimaan tietoliikennettä. Kuten alla olevasta kuvasta nähdään suoritettu pakettikaappaus Wiresharki:lla, josta on suodatettu näkyviin vain DNS-protokollaa käyttävät paketit. Paketit numeroin 13 ja 24, ovat kysely ja vastaus paketteja kysytylle speedtest.net -sivustolle. Loput mustalla taustalla merkityt paketit ovat puolestaan eri mainossivustoille ja palvelimelle tehdyistä DNS-kyselyistä ja vastauksista. Nämä erottuvat tässä tapauksessa verkkotunnuksesta, jotka sisältävät merkkijonon ads, eli mainokset. Kaikkia mainos- ja seuranta palvelimia on hankalempi tunnistaa pelkästään verkkotunnusta tarkkailemalla. Kuten huomataan Adguard Home ei anna sivustojen selvittää niiden IP-osoitteitaan. Adguard Home vastaa IP-osoitteella 0.0.0.0, joka ei johda mihinkään.



Kuva 24. Kuvankaappaus tehdystä pakettikaappauksesta Wireshark:illa.

Quad 9:sin tai AdGuard Home:n suodatinlistojen avulla haitallisille, erikseen estetyille sivustoille tai palveluille siirtyminen estetään kokonaan palomuurin kaltaisesti. Alla olevassa esimerkissä AdGuard Home:n estetyt palvelut välilehdellä on määritelty estämään YouTuben käyttö kokonaan. Tämä on hyödyllistä esimerkiksi yrityksissä, jossa halutaan estää henkilökuntaa käyttämästä tämänkaltaista palvelua.

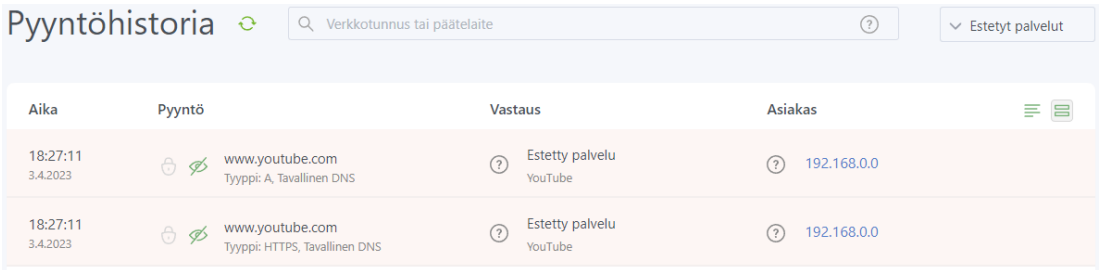
Sivustoon ei saada yhteyttä

Osoitteessa https://www.youtube.com/?gl=FI&hl=fi oleva sivu saattaa olla väliaikaisesti pois käytöstä tai se on voitu siirtää pysyvästi uuteen osoitteeseen.

ERR_ADDRESS_INVALID

Kuva 25. Sivustolle siirtyminen estetty.

AdGuard Home:n pyyntöhistoriassa nähdään kaikki sallitut ja estetyt DNS-kyselyt. Alla olevassa kuvassa pyyntöhistoria on suodatettu näyttämään ainoastaan estetyt palvelut. Estetylle sivustolle siirtymis- yrityksen jälkeen AdGuard Home:n historiaan tallentuu tästä loki merkintä.



Kuva 26. AdGuard Home:een tallentunut lokitieto palvelun estosta.

7 YHTEENVETO

Opinnäytetyön aihe oli minulle mielenkiintoinen tutkimusprojekti nimipalvelimia ja Raspberry Pi -alustaa kohtaan. Opinnäytetyön avulla opin lisää, miten nimipalvelin käytännössä toimii ja ennen hieman vieras Raspberry Pi tuli minulle tutuksi kuten myös Debian Linux. Tietoverkot ja tietoturva ovat minulle henkilökohtaisesti mielenkiintoisia aiheita ja tärkeitä omaa alaa ja uraa kohtaan. Tämän opinnäytetyön avulla näkemys tietoturvasta ja tietoverkoista avartui huomattavasti, ja toivottavasti myös tämän opinnäytetyön lukijalla.

Palvelinratkaisu toteutti sille tarkoitetut tavoitteet, eli estämään tehokkaasti haitalliset verkkosivustot, seuraimet ja mainonta samaan verkkoon kytketyillä laitteilla. Puutteet DNS-tasoisesta estosta oli tiedossa, kuten mainittu YouTube. Tähän on mahdollisesti AdGuard Home:n kehitystiimin mukaan tulossa tulevaisuudessa ratkaisu.

Tämän työn toteutuksen avulla oli tarkoitus myös antaa tarvittava taustatieto ja asennusohjeistus, jolla on mahdollista muiden halukkaiden ja kiinnostuneiden rakentaa oma DNS-palvelin. Mielestäni saavutin tämän tavoitteeni työlläni. Asennettava palvelu perustuu avoimeen lähdekoodiin ja on tällöin myös muokattavissa omiin tarkoituksiin ja jatkokehitysmahdollisuuksiin.

Omia jatkokehitysideoita olisi käyttää jotain VPN palveluntarjoajaa tai ratkaisua tämän DNS-palvelimen lisäksi kehittäen yksityisyyttä ja tietosuojaa entisestään. Hallintapaneeli olisi myös samalla tarkoitus salata HTTPS:sään. Tämän tekeminen vaatii varmenteen ja domainin hankkimista ja jatkoselvittelyjä.

Loppujen lopuksi olen erittäin tyytyväinen opinnäytetyön kokonaisuuteen. Opinnäytetyölläni olin pyrkinyt tuomaan esille ohjelmistoja, joita opintojeni aikana tuli myös käytettyä. Omasta mielestäni oli tärkeää myös ylläpitää opinnäytetyössäni yhtenäistä visuaalista ilmettä kuvissa ja taulukoissa, joiden avulla sain mielestäni hyvin selvennettyä käsiteltäviä asioita.

LÄHTEET

AdGuard. (20.6.2022). DNS-over-QUIC is now officially a proposed standard. https://adguard.com/en/blog/dns-over-quic-official-standard.html

Adrian, C. (3.3.2022). Let's install Raspberry Pi OS Lite 64-Bit on SD Card to use headless. https://che-adrian.medium.com/lets-install-raspberry-pi-os-lite-64-bit-on-sd-card-to-use-headless-587a32a72527

Basumallick, C. (26.8.2022). What is Raspberry Pi? models, features, and uses. https://www.spiceworks.com/tech/networking/articles/what-is-raspberry-pi/#_001

Catania, S. (12.11.2021). DNSCrypt. What it is. How it works. What it's used for. https://www.internetx.com/en/news-detailview/dnscrypt-what-it-is-how-it-works-what-its-used-for/

Cihodariu, M. (13.7.2021). DNS over HTTPS (DoH): Definition, Implementation, Benefits, and More. https://heimdalsecurity.com/blog/dns-over-https-doh/

Cloudflare. (N.d.). What is 1.1.1.1? Haettu 30.1.2023 osoitteesta https://www.cloudflare.com/learning/dns/what-is-1.1.1.1/

Collins, S. (28.2.2022). The life of Pi: Ten years of Raspberry Pi. https://www.cam.ac.uk/stories/raspberrypi

Crane, C. (11.3.2021). What Is a DNS server and why the Internet wouldn't work without the DNS System. https://resources.experfy.com/software-ux-ui/what-is-a-dns-server-and-why-the-internet-wouldnt-work-without-the-dns-system/

Dhillon, N. (16.7.2015). How does DNS work? https://www.stantonstreet.com/blog/how-does-dns-work/

Domantas, G. (3.3.2023). What Is SSH: Understanding Encryption, Ports and Connection. https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work

Fedotova, A. (24.11.2022). What is DNS filtering. https://adguard.com/en/blog/what-is-dns-filtering.html

Fromaget, P. (N.d.). The Epic Story of the Raspberry Pi. Haettu 15.12.2022 osoitteesta https://raspberrytips.com/raspberry-pi-history/

Hinchliffe, A. (15.3.2019). DNS Tunneling: how DNS can be (ab)used by malicious actors. https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors/

Induste. (12.4.2020). Install a PiHole: A universal ad blocker! https://induste.com/threads/installer-un-pihole-un-bloqueur-de-pub-universel.634409/

Ionescu, S. (22.8.2022). Quad9 DNS review. https://www.techradar.com/reviews/quad9-dns

Ionos. (21.11.22). How to set up your own DNS server with Raspberry Pi. https://www.ionos.com/digitalguide/server/configuration/how-to-make-your-raspberry-pi-into-a-dns-server/

Kosek, M. (29.3.2022). A first look at DNS over QUIC. https://blog.apnic.net/2022/03/29/a-first-look-at-dns-over-quic/

Mazerik, R. (17.5.2021). Understanding DNS sinkholes – A weapon against malware. https://resources.infosecinstitute.com/topic/dns-sinkhole/

Mullins, P. (24.6.2020). Customize your Raspberry Pi operating system for everyday use. https://opensource.com/article/20/6/custom-raspberry-pi

NordLayer. (6.12.2022). Public vs. private DNS servers. https://nordlayer.com/blog/public-vs-private-dns-servers/

Quad9. (5.10.2022). What's the Difference Between Recursive DNS and Authoritative DNS – 2022. https://www.quad9.net/news/blog/what-s-the-difference-between-recursive-dns-and-authoritative-dns-2022/

Raspberry Pi. (N.d.). Raspberry Pi 4. Haettu 17.12.2022 osoitteesta https://www.raspberrypi.com/products/raspberry-pi-4-model-b/

Raymond, S. (16.6.2021). Authoritative vs recursive DNS: what you need to know. https://www.dnsfilter.com/blog/authoritative-vs-recursive-dns

Tunggal, A. (11.10.2021). DNSSEC: What Is It and Why Is It Important? https://www.upguard.com/blog/dnssec