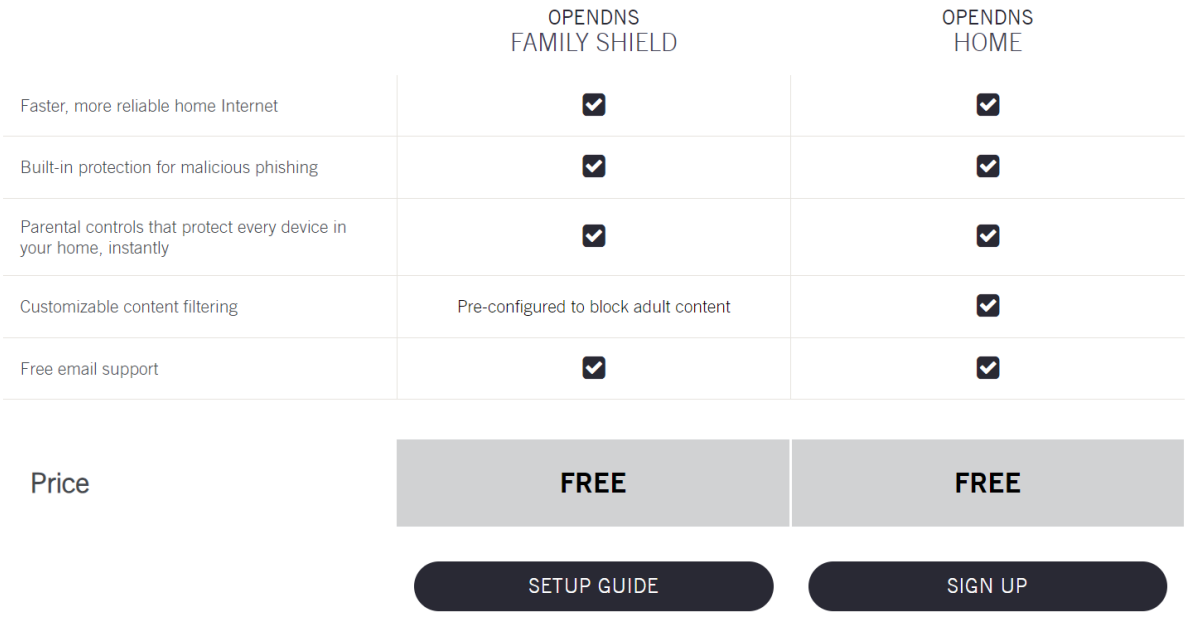
„OpenDNS“ interneto turinio filtravimo sprendimas – tėvų kontrolės priemonė

„OpenDNS“ – tai paprastas ir nemokamas interneto turinio filtravimo sprendimas namų vartotojams. Šį sprendimą galima naudoti praktiškai visuose, prie interneto prisijungti galinčiuose įrenginiuose: kompiuteriuose, mobiliuosiuose įrenginiuose, maršrutizatoriuose, DNS (angl. Domain Name System) serveriuose. Taip pat jis veikia visų pagrindinių operacinių sistemų (Windows, Linux, Mac OS) aplinkoje. Naudojant „OpenDNS“, vartotojų įrenginiuose nereikia diegti jokios papildomos programinės įrangos, tik pakeisti juose DNS nustatymus, o visas interneto turinio filtrų konfigūravimas atliekamas specialiai tam skirtame tinklalapyje www.opendns.com.

Paskyros sukūrimas ir konfigūravimas

Norint pradėti naudotis „OpenDNS“ tėvų kontrolės priemone, pirmiausia reikia susikurti paskyrą tinklalapyje www.opendns.com. Atsidarę tinklalapį, kairėje pusėje pasirenkame „Home Parental Control“ ir apačioje spaudžiame „Learn More“. Galimi du tėvų kontrolės paskyros tipai (1 pav.):

- „OpenDNSHome“ – nemokama paskyra, suteikianti galimybę koreguoti interneto turinio filtravimo nustatymus, naudotis statistikos rinkimo galimybe ir apsauga nuo „Phishing“ ir kenkėjiškos programinės įrangos atakų.
- „OpenDNSFamilyShield“ – nemokama paskyra, automatiškai sukonfigūruota blokuoti suaugusiems skirtą turinį.



1 pav. Du galimi „OpenDNS“ tėvų kontrolės paskyros tipai

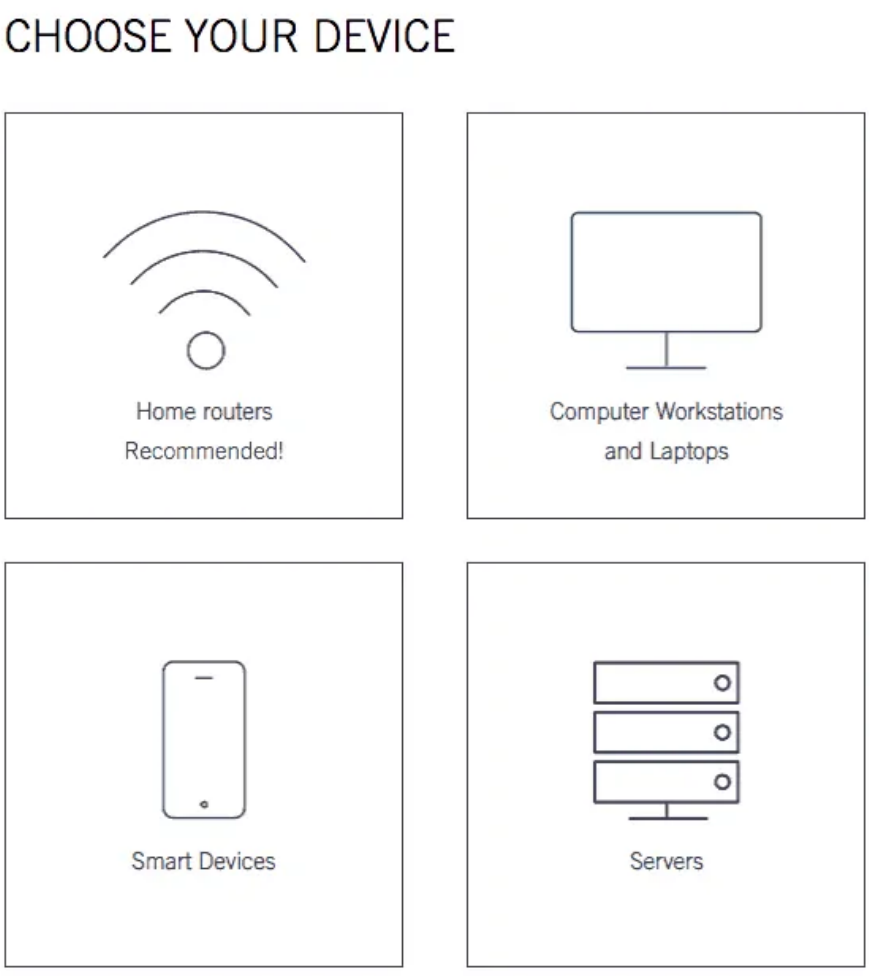
Pastaba: „OpenDNS“ mokamos versijos nebėra. „Cisco” išskyrė „OpenDNS“ kaip nemokamą produktą , o mokamus variantus paliko „Cisco” platformoje.

Kadangi „OpenDNS Home“ paskyra turi galimybę keisti filtravimo nustatymus ir yra nemokama, toliau nagrinėsime būtent šią paskyrą.

Pasirinkę paskyrą, spaudžiame „Sign up“. Pasirodžiusioje registracijos formoje reikia įvesti galiojantį el. pašto adresą, kuriuo bus atsiųsta registracijos aktyvavimo nuoroda, pasirinkti šalį, ir įvesti savo sukrutą slaptažodį.

Užpildžius registracijos formą, reikia pasirinkti įrenginį, kuriame bus naudojama „OpenDNS“ tėvų kontrolės priemonė, ir operacinę sistemą (jei tai bus kompiuteris ar DNS serveris) arba įrenginio modelį (jei tai bus maršrutizatorius) (2. pav.). Namų vartotojams rekomenduojama rinktis maršrutizatorių (jei toks yra), nes taip yra lengviau užtikrinti filtravimo priemonės saugumą.

Be to, maršrutizatoriuje įdiegtas „OpenDNS“ sprendimas leidžia užtikrinti interneto turinio kontrolę visiems lokalaus tinklo naudotojams vienu metu. Nesvarbu, koks tai įrenginys ir kokiu būdu, belaidžiu ar laidiniu, jis yra prisijungęs prie maršrutizatoriaus.



2 pav. Įrenginio, kuriame bus naudojama „OpenDNS“ tėvų kontrolės priemonė, pasirinkimas

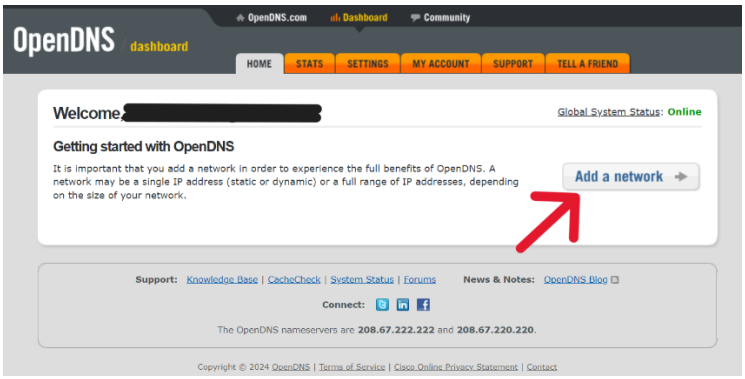
Įrenginių konfigūravimas yra labai paprastas. Reikia pakeisti maršrutizatoriaus ar kito įrenginio, kuriame norite naudoti šį interneto turinio filtravimo sprendimą, DNS adresus į „OpenDNS“ adresus. Šiuos adresus galima rasti tinklalapyje https://www.opendns.com/setupguide/

Diegimo į instrukcijas skirtingiems maršrutizatoriams nuoroda : https://support.opendns.com/hc/en-us/sections/206253667-Individual-Router-Configurations

Pasirinkus norimą įrenginį, pateikiamos detalios instrukcijos, kaip tinkamai atlikti jo nustatymus, t.y. pakeisti DNS adresus.

Jeigu nustatymai atlikti teisingai, reikia prisijungti prie el. pašto ir aktyvuoti gautą nuorodą, kuri automatiškai jus nukreips į „OpenDNS“ valdymo skydą (angl. – dashboard).

Prisijungus prie paskyros, pirmiausia reikės pridėti naudotojo tinklo ar įrenginio išorinį IP adresą, paspaudžiant „Add a network“ (3 pav.).

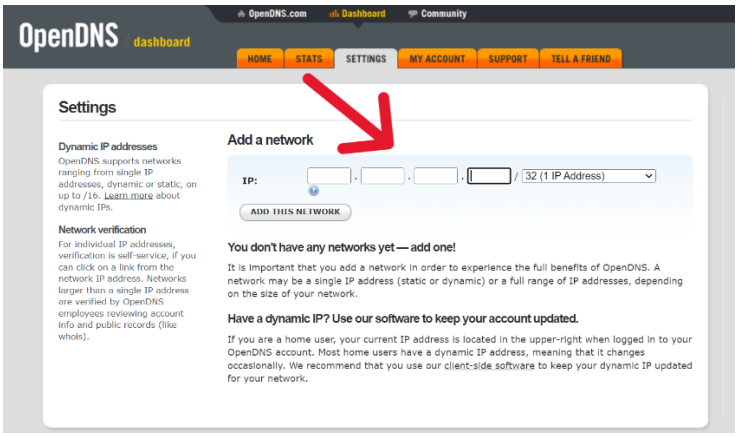


3 pav. Tinklo sukūrimas

IP adreso nustatymas

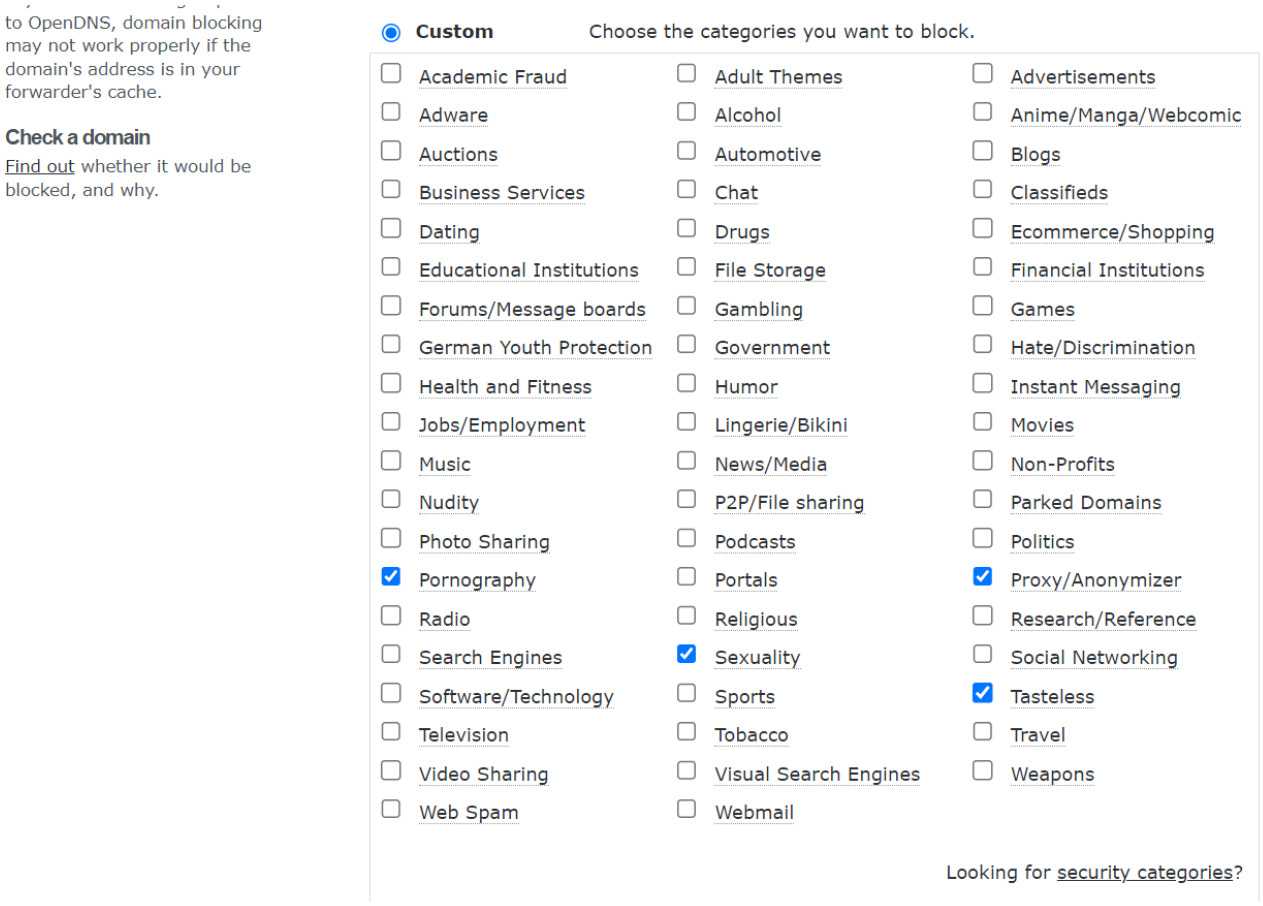
Jei naudotojas jungiasi prie „OpenDNS“ paskyros iš to tinklo, kurį norės apsaugoti, sistema IP adresą nustato pati. Naudotojui reikia tik patvirtinti paspaudžiant mygtuką „Add this network“ (4 pav.). Jei norite pakeisti siūlomą IP adresą į kitą, tiesiog ištrinkite senąjį ir vietoje jo įveskite naująjį.

4 pav. Tinklo ar įrenginio, kuriame bus naudojama „OpenDNS“ tėvų kontrolės priemonė, IP adresas



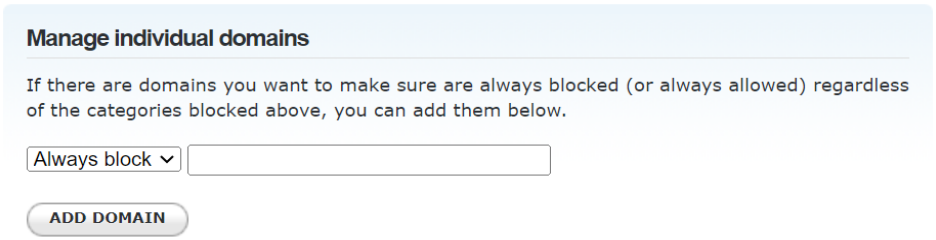
Įtraukus IP adresą, galima pereiti prie interneto turinio filtravimo nustatymų.

Yra penki galimi interneto turinio filtravimo lygiai: aukštas – blokuojamos 27 tinklalapių kategorijos, vidutinis – blokuojama 14 kategorijų, žemas – blokuojamos 5 kategorijos. Taip pat yra lygis „custom“, kurį naudotojas gali susikonfigūruoti pats iš 60 tinklalapių kategorijų, ir lygis „none“, kuriame neblokuojama nė viena tinklalapių kategorija (5 pav.).



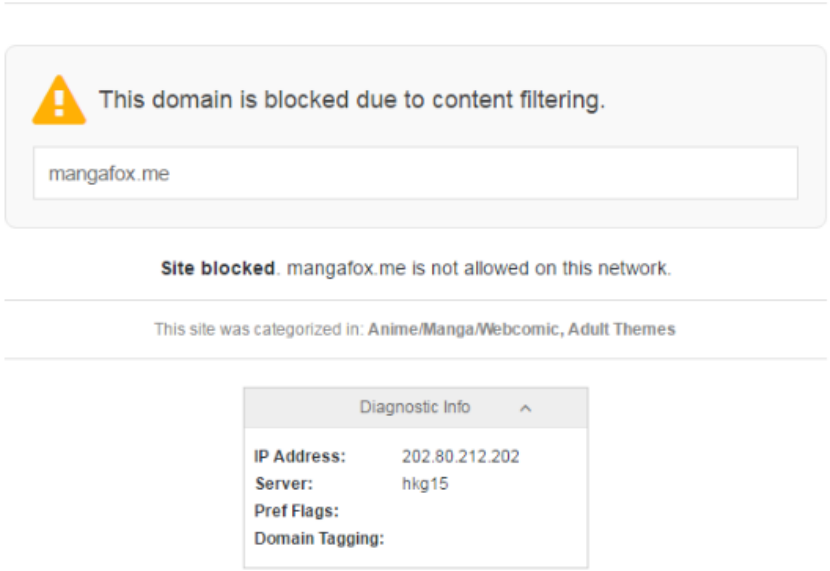
5 pav. Interneto turinio filtravimo kategorijos

Jei pasirinkus tam tikrą interneto turinio filtravimo lygį blokuojami ne visi norimi tinklalapiai ar blokuojama per daug, galite tuos tinklalapius įrašyti skiltyje „Manage individual domains“ kaip leidžiamus arba draudžiamus, t.y. sudaryti „baltuosius“ ir „juoduosius“ sąrašus (6 pav.). Įrašote tinklalapio pavadinimą į laukelį, pasirenkate „visada blokuoti“ ar „visada leisti“ ir spaudžiate „Add domain“.



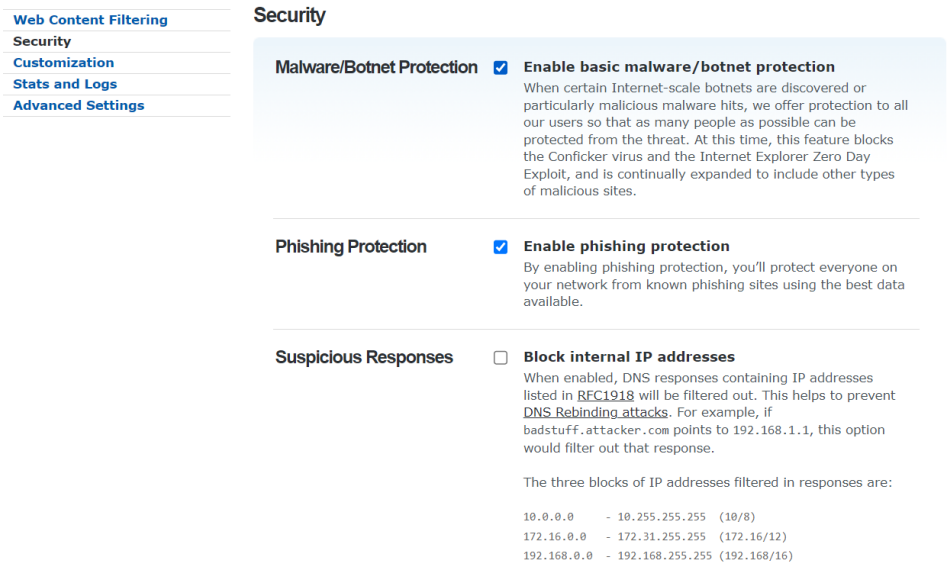
6 pav. Leidžiamų ir draudžiamų tinklalapių sąrašai

Bandant atverti draudžiamą tinklalapį, pasirodys įspėjamasis langas, kuriame bus pranešama, kad šis tinklalapis yra draudžiamas (9 pav.)



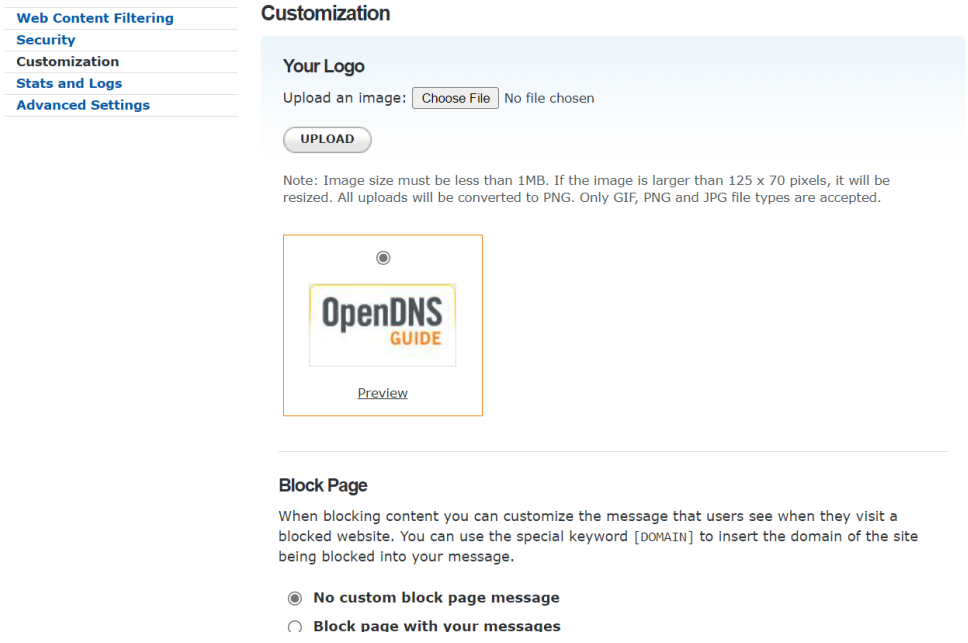
9. pav. Pranešimas, kad šis tinklalapis yra neleistinas

Be interneto turinio filtravimo, „OpenDNS“ taip pat siūlo ir saugumo nustatymus. Skyrelyje „Security“, einančiame po interneto turinio filtravimo nustatymų, galite aktyvuoti apsaugą nuo kenkėjiškos programinės įrangos , „phishing“ atakų ir dublikuotų, netikrų tinklalapių (7pav.).

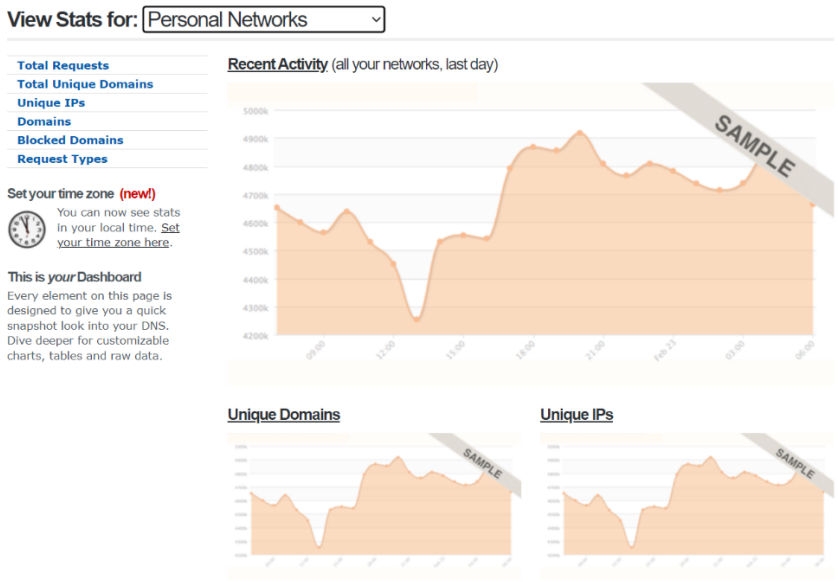


7 pav. „OpenDNS“ saugumo nustatymai

„Customization“ skiltyje galima nustatyti kokį atvaizdą ir tekstą vaizduot norint prisijungti prie draudžiamo tinklalapio (8 pav.)

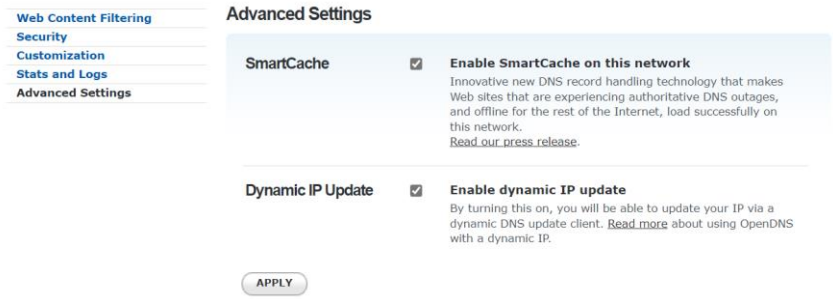


Skyrelyje „Stats and logs“ galima aktyvuoti statistikos rinkimą. Aktyvavus šį nustatymą, visa statistika pateikiama skyriuje „Stats“. Jame galėsite matyti, kiek užklausų buvo išsiųsta, kiek ir kokių tinklalapių aplankyta, kiek tinklalapių užblokuota (9 pav.). Statistikoje aptikus nepageidaujamą tinklalapį, jį iš karto galima įtraukti į draudžiamų tinklalapių sąrašą.



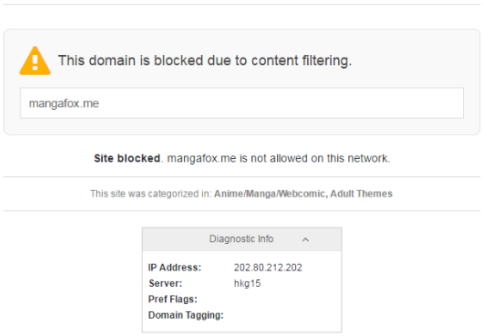
9 pav. Naudotojo interneto turinio statistika

„Advanced settings“ skiltyje (10 pav.) galima nustatyti „SmartCache“ funkciją, kuri išsaugo tinklalapį laikinojoje atmintyje, tam atvejui, jeigu tinklalapis taptų nepasiekiamas. „Dynamic IP update “ funkcija aktyvuoja kintamojo IP adreso opciją. Pvz: jeigu jūsų IP adresas yra kintamas, filtravimo įrankis automatiškai aptiks jūsų naująjį IP adresą jeigu jūsų kompiuteryje bus įdiegta „DNS update client“ programa.



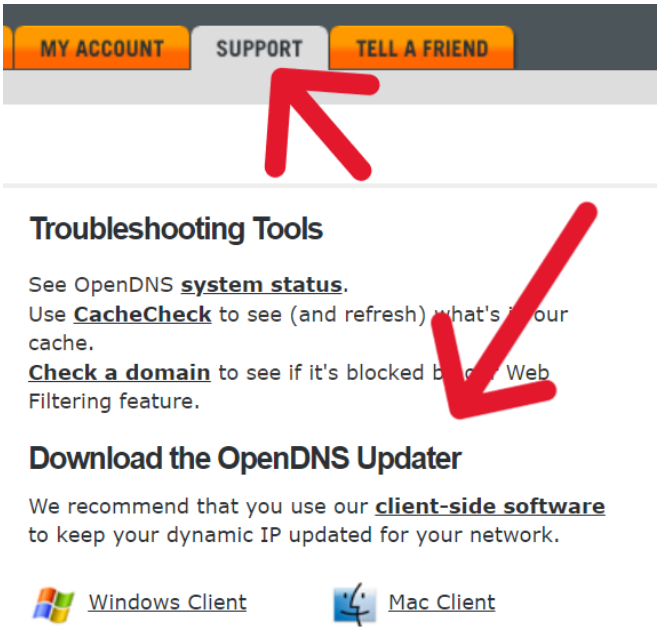
10 pav. „Advanced settings“ skiltis

Bandant atverti draudžiamą tinklalapį, pasirodys įspėjamasis langas, kuriame bus pranešama, kad šis tinklalapis yra draudžiamas (9 pav.)



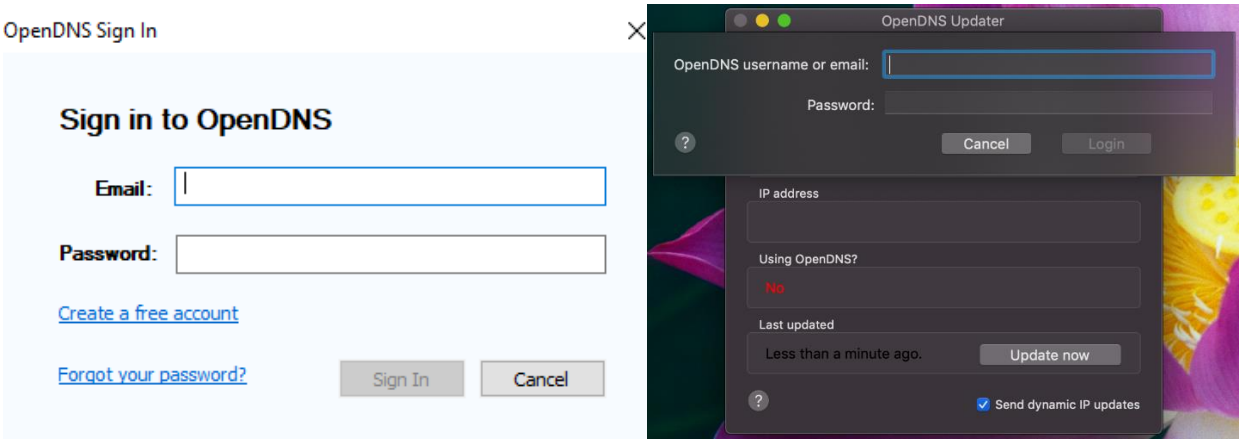
9. pav. Pranešimas, kad šis tinklalapis yra neleistinas.

Jeigu tinklo ar įrenginio išorinis IP adresas nepastovus (dinaminis), ir interneto paslaugų teikėjas jį gali bet kada pakeisti, rekomenduojama vartotojo kompiuteryje įsidiegti „ OpenDNS Updater“, kuris automatiškai tikrina IP adresą. Šiam pasikeitus, pakoreguojamas ir „OpenDNS Updater“ paskyroje nustatytas IP adresas, kad apsauga veiktų nepertraukiamai. Programą galima rasti „Support“ skyriuje (10 pav.).



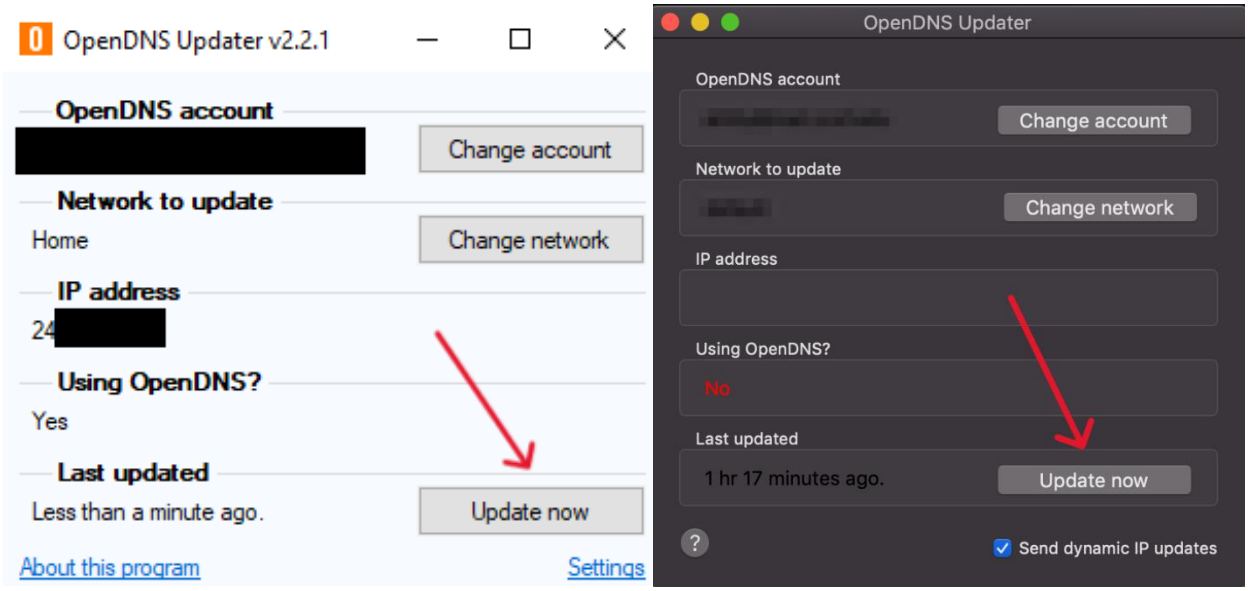
10 pav. „OpenDNS Updater“

„OpenDNS Updater“ įdiegiama suvedus vartotojo duomenis (11 pav.)



11 pav. „OpenDNS Updater“ nustatymas Windows ir MacOS operacinėse sistemose

Pasikeitus IP adresui programa pati turėtų jį aptikti ir perduoti sistemai. Tačiau, jeigu dėl kažkokių priežąsčių naujas IP adresas neperesikėlė, visada galima atlikti „Update now“ opciją (12 pav.)



12 pav. IP adreso atnaujinimas

„OpenDNS“ sprendimo naudotojai turėtų atkreipti dėmesį į tai, kad norint užtikrinti tinkamą saugumo lygį, reikia imtis papildomų priemonių. Jei sprendimas naudojamas kompiuteryje, jame reikia sukurti atskirus profilius kompiuterio naudotojams, apribojant galimybes keisti kompiuterio nustatymus – šiuo atveju DNS įrašus. Jei „OpenDNS“ naudojamas maršrutizatoriuje, patį įrenginį reikėtų apsaugoti slaptažodžiu, kad vaikai ar kiti pašaliniai asmenys negalėtų prisijungti ir keisti maršrutizatoriaus nustatymų.

Taip pat svarbu konfigūruojant „OpenDNS“ visada blokuoti tinklalapių kategoriją „Proxy/Anonimyzer“, kuri neleidžia naudotis „proxy“ serveriais ir anoniminiu naršymu. Ši tinklalapių kategorija automatiškai blokuojama jau nuo žemiausio interneto turinio blokavimo lygmens. Tačiau dalis „proxy“ serverių vis tiek būna pasiekiami.

Pastaba: Pakeitus interneto turinio filtravimo nustatymus, jų atsinaujinimo reikia gerokai palaukti, nors teigiama, kad pakeitus nustatymus, jie atsinaujina per 3 minutes.