

## „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](http://www.opendns.com).

### Paskyros sukūrimas ir konfigūravimas

Norint pradėti naudotis „OpenDNS“ tėvų kontrolės priemone, pirmiausia reikia susikurti paskyrą tinklalapyje [www.opendns.com](http://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.

	OPENDNS FAMILY SHIELD	OPENDNS HOME
Faster, more reliable home Internet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Built-in protection for malicious phishing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Parental controls that protect every device in your home, instantly	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Customizable content filtering	Pre-configured to block adult content	<input checked="" type="checkbox"/>
Free email support	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Price	<b>FREE</b>	<b>FREE</b>
	<a href="#">SETUP GUIDE</a>	<a href="#">SIGN UP</a>

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.

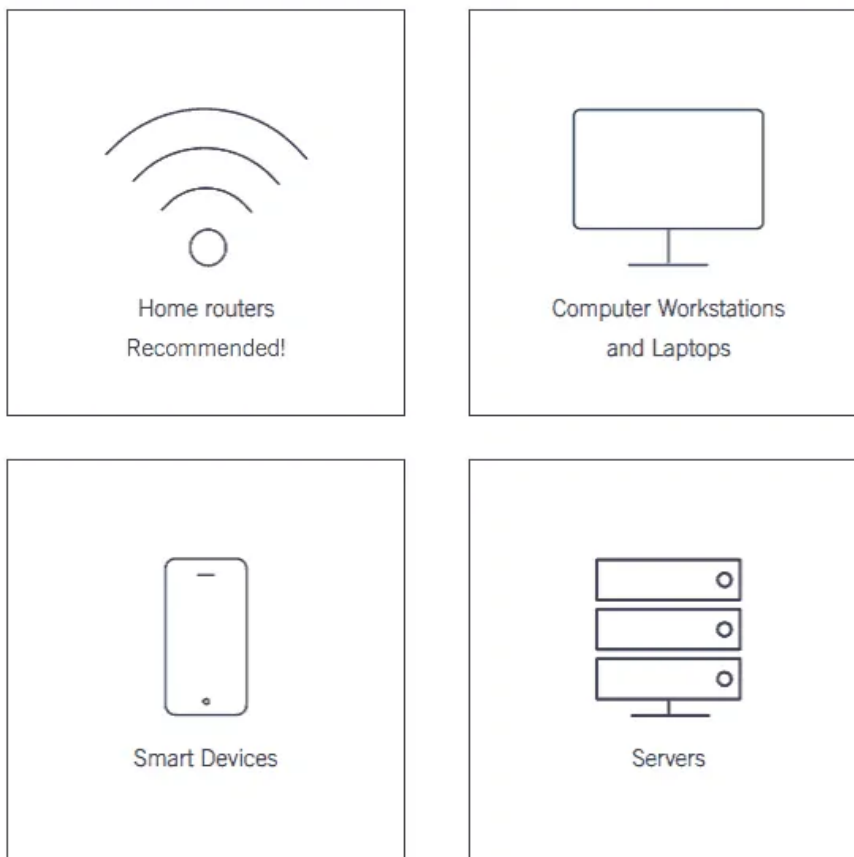
Kadangi „OpenDNS Home“ paskyra turi galimybę keisti filtravimo nustatymus ir yra nemokama, toliau nagrinėsime būtent šią paskyrą.

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 sukurtą 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 koku būdu, belaidžiu ar laidiniu, jis yra prisijungęs prie maršrutizatoriaus.

## CHOOSE YOUR DEVICE



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

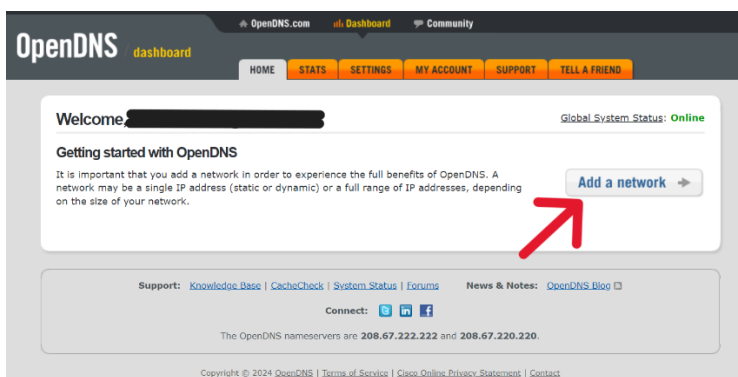
Įrenginių konfigūravimas yra labai paprastas. Reikia pakeisti maršrutizatoriaus ar kito įrenginio, kuriame norite naudoti šį interneto turinio filtravimo sprendimą, DNS adresus į „OpenDNS“ adresus. Šiuos adresus galima rasti tinklalapyje <https://www.opendns.com/setupguide/>

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.).

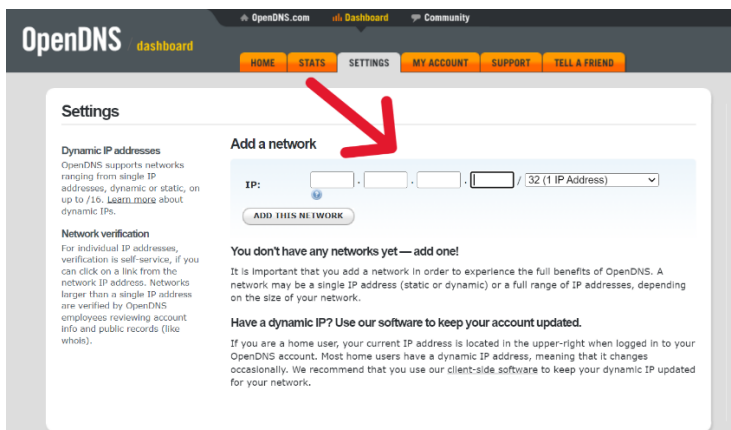


3 pav. Tinklo sukūrimas

### 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.).

to OpenDNS, domain blocking may not work properly if the domain's address is in your forwarder's cache.

#### Check a domain

[Find out](#) whether it would be blocked, and why.

**Custom** Choose the categories you want to block.

<input type="checkbox"/> <a href="#">Academic Fraud</a>	<input type="checkbox"/> <a href="#">Adult Themes</a>	<input type="checkbox"/> <a href="#">Advertisements</a>
<input type="checkbox"/> <a href="#">Adware</a>	<input type="checkbox"/> <a href="#">Alcohol</a>	<input type="checkbox"/> <a href="#">Anime/Manga/Webcomic</a>
<input type="checkbox"/> <a href="#">Auctions</a>	<input type="checkbox"/> <a href="#">Automotive</a>	<input type="checkbox"/> <a href="#">Blogs</a>
<input type="checkbox"/> <a href="#">Business Services</a>	<input type="checkbox"/> <a href="#">Chat</a>	<input type="checkbox"/> <a href="#">Classifieds</a>
<input type="checkbox"/> <a href="#">Dating</a>	<input type="checkbox"/> <a href="#">Drugs</a>	<input type="checkbox"/> <a href="#">Ecommerce/Shopping</a>
<input type="checkbox"/> <a href="#">Educational Institutions</a>	<input type="checkbox"/> <a href="#">File Storage</a>	<input type="checkbox"/> <a href="#">Financial Institutions</a>
<input type="checkbox"/> <a href="#">Forums/Message boards</a>	<input type="checkbox"/> <a href="#">Gambling</a>	<input type="checkbox"/> <a href="#">Games</a>
<input type="checkbox"/> <a href="#">German Youth Protection</a>	<input type="checkbox"/> <a href="#">Government</a>	<input type="checkbox"/> <a href="#">Hate/Discrimination</a>
<input type="checkbox"/> <a href="#">Health and Fitness</a>	<input type="checkbox"/> <a href="#">Humor</a>	<input type="checkbox"/> <a href="#">Instant Messaging</a>
<input type="checkbox"/> <a href="#">Jobs/Employment</a>	<input type="checkbox"/> <a href="#">Lingerie/Bikini</a>	<input type="checkbox"/> <a href="#">Movies</a>
<input type="checkbox"/> <a href="#">Music</a>	<input type="checkbox"/> <a href="#">News/Media</a>	<input type="checkbox"/> <a href="#">Non-Profits</a>
<input type="checkbox"/> <a href="#">Nudity</a>	<input type="checkbox"/> <a href="#">P2P/File sharing</a>	<input type="checkbox"/> <a href="#">Parked Domains</a>
<input type="checkbox"/> <a href="#">Photo Sharing</a>	<input type="checkbox"/> <a href="#">Podcasts</a>	<input type="checkbox"/> <a href="#">Politics</a>
<input checked="" type="checkbox"/> <a href="#">Pornography</a>	<input type="checkbox"/> <a href="#">Portals</a>	<input checked="" type="checkbox"/> <a href="#">Proxy/Anonymizer</a>
<input type="checkbox"/> <a href="#">Radio</a>	<input type="checkbox"/> <a href="#">Religious</a>	<input type="checkbox"/> <a href="#">Research/Reference</a>
<input type="checkbox"/> <a href="#">Search Engines</a>	<input checked="" type="checkbox"/> <a href="#">Sexuality</a>	<input type="checkbox"/> <a href="#">Social Networking</a>
<input type="checkbox"/> <a href="#">Software/Technology</a>	<input type="checkbox"/> <a href="#">Sports</a>	<input checked="" type="checkbox"/> <a href="#">Tasteless</a>
<input type="checkbox"/> <a href="#">Television</a>	<input type="checkbox"/> <a href="#">Tobacco</a>	<input type="checkbox"/> <a href="#">Travel</a>
<input type="checkbox"/> <a href="#">Video Sharing</a>	<input type="checkbox"/> <a href="#">Visual Search Engines</a>	<input type="checkbox"/> <a href="#">Weapons</a>
<input type="checkbox"/> <a href="#">Web Spam</a>	<input type="checkbox"/> <a href="#">Webmail</a>	

[Looking for security categories?](#)

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“.

### Manage individual domains

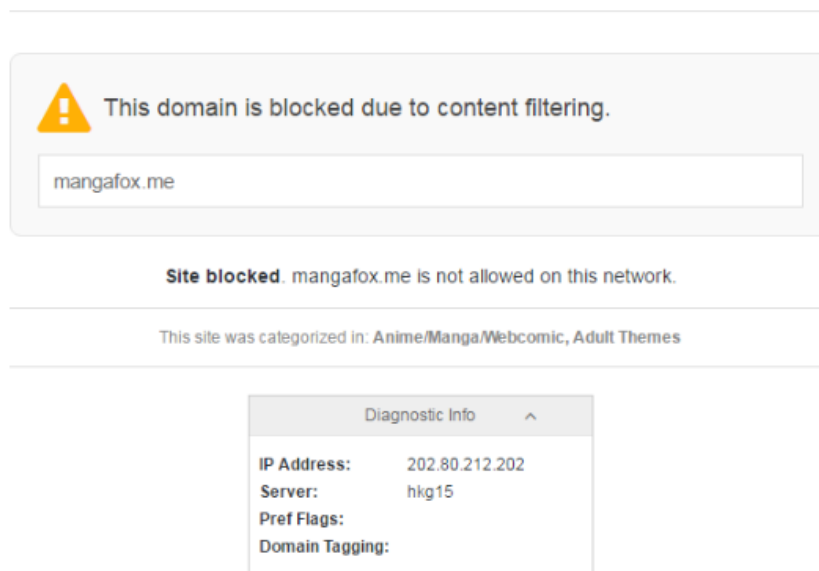
If there are domains you want to make sure are always blocked (or always allowed) regardless of the categories blocked above, you can add them below.

Always block

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.)



The screenshot shows a network error message. At the top, there is a yellow warning triangle icon followed by the text "This domain is blocked due to content filtering." Below this, the domain "mangafox.me" is displayed in a text box. Underneath, it says "Site blocked. mangafox.me is not allowed on this network." Further down, it states "This site was categorized in: Anime/Manga/Webcomic, Adult Themes". At the bottom, there is a "Diagnostic Info" section with a dropdown arrow, containing the following details:

Diagnostic Info	
IP Address:	202.80.212.202
Server:	hkg15
Pref Flags:	
Domain Tagging:	

### 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 graminės įrangos, „phishing“ atakų ir dubliuotų, netikrų tinklalapių (7pav.).

- Web Content Filtering
- Security
- Customization
- Stats and Logs
- Advanced Settings

## Security

- Malware/Botnet Protection**  **Enable basic malware/botnet protection**  
When certain Internet-scale botnets are discovered or particularly malicious malware hits, we offer protection to all our users so that as many people as possible can be protected from the threat. At this time, this feature blocks the Conficker virus and the Internet Explorer Zero Day Exploit, and is continually expanded to include other types of malicious sites.
- Phishing Protection**  **Enable phishing protection**  
By enabling phishing protection, you'll protect everyone on your network from known phishing sites using the best data available.
- Suspicious Responses**  **Block internal IP addresses**  
When enabled, DNS responses containing IP addresses listed in [RFC1918](#) will be filtered out. This helps to prevent [DNS Redirection attacks](#). For example, if badstuff.attacker.com points to 192.168.1.1, this option would filter out that response.
- The three blocks of IP addresses filtered in responses are:
- |             |   |                 |              |
|-------------|---|-----------------|--------------|
| 10.0.0.0    | - | 10.255.255.255  | (10/8)       |
| 172.16.0.0  | - | 172.31.255.255  | (172.16/12)  |
| 192.168.0.0 | - | 192.168.255.255 | (192.168/16) |

7 pav. „OpenDNS“ saugumo nustatymai

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

- Web Content Filtering
- Security
- Customization
- Stats and Logs
- Advanced Settings

## Customization

### Your Logo

Upload an image:  No file chosen

Note: Image size must be less than 1MB. If the image is larger than 125 x 70 pixels, it will be resized. All uploads will be converted to PNG. Only GIF, PNG and JPG file types are accepted.

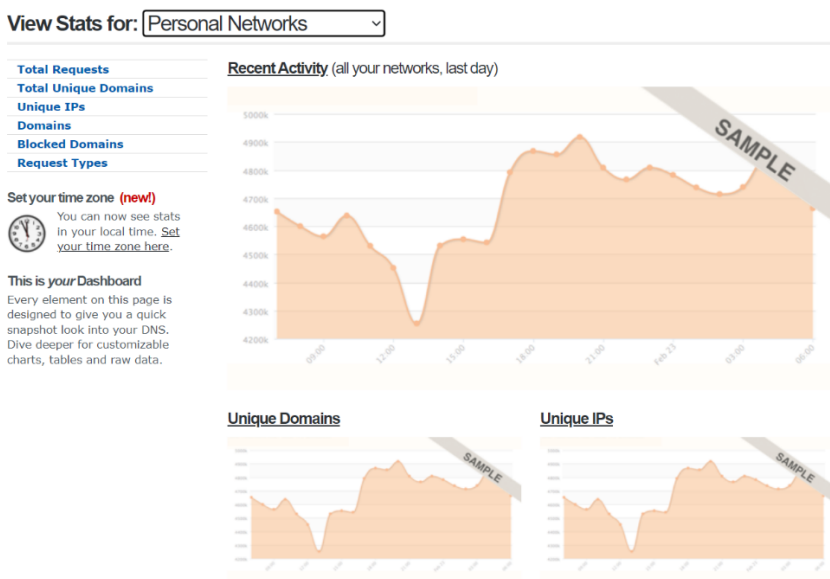


### Block Page

When blocking content you can customize the message that users see when they visit a blocked website. You can use the special keyword [DOMAIN] to insert the domain of the site being blocked into your message.

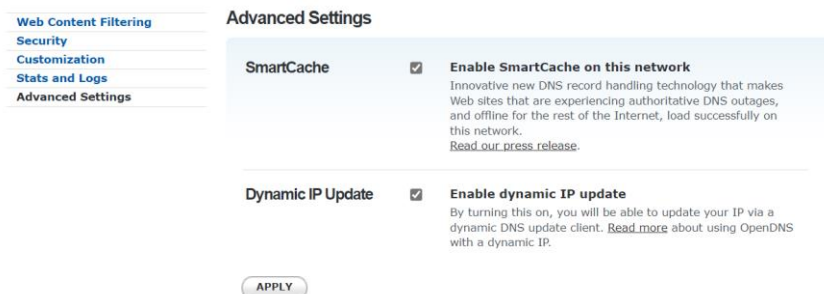
- No custom block page message
- Block page with your messages

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 naujajį IP adresą jeigu jūsų kompiuteryje bus įdiegta „DNS update client“ programa.



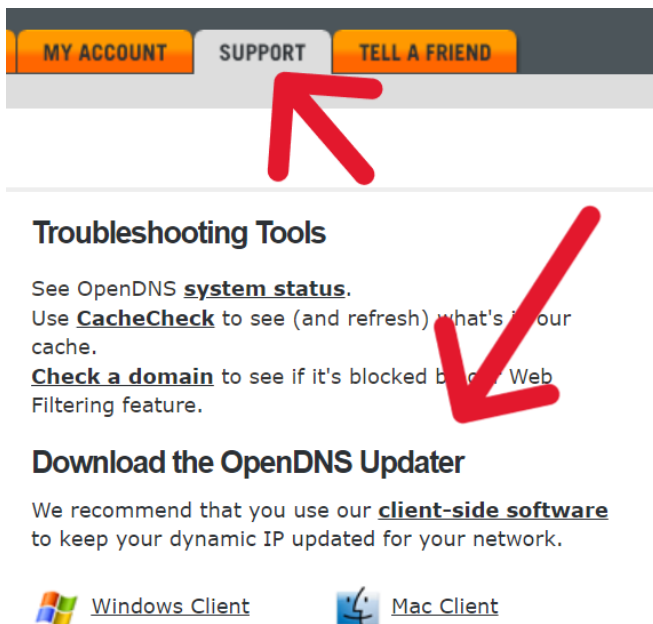
10 pav. „Advanced settings“ skiltis

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.

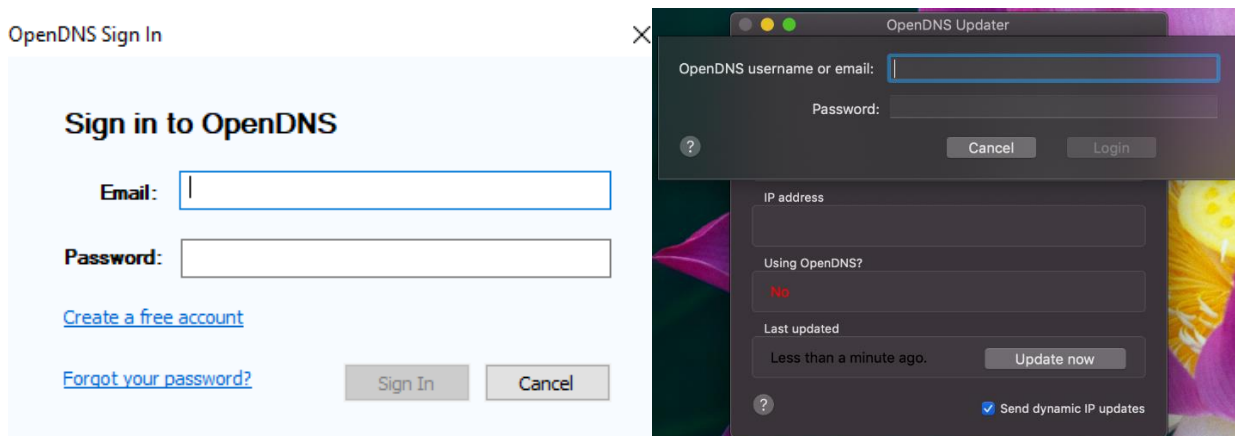
Jeigu tinklo ar įrenginio išorinis IP adresas nepastovus (dinaminis), ir interneto paslaugų teikėjas jį gali bet kada pakeisti, rekomenduojama vartotojo kompiuteryje įsidiesti „OpenDNS Updater“, kuris automatiškai tikrina IP adresą. Šiam pasikeitus, pakoreguojamas ir „OpenDNS Updater“ paskyroje nustatytas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



10 pav. „OpenDNS Updater“

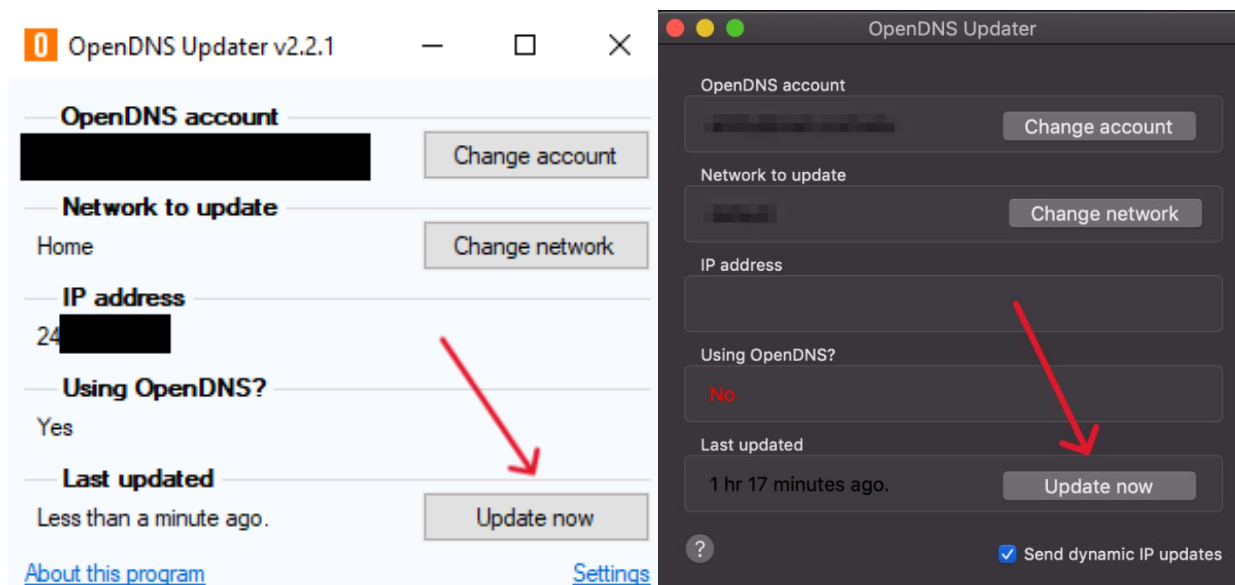


„OpenDNS Updater“ įdiegiama suvedus vartotojo duomenis (11 pav.)



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 priežasčių 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.