Hogyan telepítsük a DoH-t Firefox, Opera, vagy Chrome alá

PCLinuxOS Magazine – 2019. december

Írta: Paul Arnote (parnote)

A DNS over HTTPS (DoH-ként szokták említeni) pár hónap óta a címlapokon szerepel. Alapvetően ez csak egy újabb „privát fogaskerék” az Internetet mozgató rendszerhez.

Tökéletes? Távolról sem, de legalább van. A DoH segít elkerülni, hogy az internetszolgáltató (ISP) naplózza, mely lapokat kerestél fel. Természetesen vannak még módszerek, amivel az ISP megtudhatja, mely oldalakat keresel fel. Azok használata nem olyan egyszerű, mint simán naplózni a géped és a szolgáltató között cserélt – titkosítatlan – DNS-címeket.

A DoH betömi ezt az átláthatósági rést úgy, hogy a DNS-kérést a szokásos HTTPS-forgalom részévé teszi. Ahelyett, hogy a kérés kódolatlan sima szövegként menne az 53-as porton, a HTTPS által használt 443-as port titkosított forgalmának részévé válik. Így az ISP-nek nem olyan egyszerű elfogni a DNS-kéréseket, mintha az 53-as porton titkosítatlanul érkezne.

A DoH lehetővé teszi a helyi ISP szűrőinek kikerülését és hozzáférni a szolgáltató, vagy a helyi kormány által egyébként blokkolt tartalmakat. A brit ISP-k egy csoportja ezért nevezte a Mozillát a 2019. év internetes gazemberének, mivel „a törekvése a DNS over HTTPS bevezetésére kikerülhetővé teszi a Nagy Britanniában kötelező szűrést és szülői felügyeletet, aláásva a brit biztonsági szabványokat.”

Természetesen, ez egy túlegyszerűsített magyarázata a DoH működésének. Aki a DoH működéséről tisztább képet szeretne kapni, annak a Mozilla Hacks „A **Cartoon Intro To DNS Over HTTPS**” című cikkét ajánlom, a PCLinuxOS Magazine e számában olvasható.

Nem a DoH az egyetlen versenyző. Egy másik a DoT nevű eljárás (DNS TLS fölött), ami egyesek szerint jobb és biztonságosabb. A DoH megjelenése nem jelenti a DoT végét. Mégha a DoT-nak láthatóan sok támogatója van, szerintem a DoH gyorsabb elfogadottságának oka, hogy könnyebb alkalmazni. Feltételezésem szerint, még sokat fogunk hallani a DoT-tábor felől azt követően, hogy a TLS 1.3 specifikációit véglegesítették.

Végül is, a **legtöbb** nagy böngésző (a Mozilla Firefox 70-től kezdődően) megkezdte a DoH alkalmazását. Akkor lássuk, hogyan kapcsoljuk be Firefox, Opera és Google Chrome alatt. Igen tudom, vannak más böngészők is, a PCLinuxOS tárolóiban 20, vagy több böngésző található, közte a Flashpeak Slimjet, a Vivaldi, a Brave stb.. És nem, nem fogom megnézni, hogyan kell engedélyezni a DoH-t mindegyiken. Például, megnéztem a Slimjet-et (a telepített böngészőim közül egy) és nem találtam semmiféle DoH beállítási lehetőséget. Öt különféle böngésző van gépemen és nem fogom a többit is telepíteni csak azért, hogy lássam, támogatják-e a DoH-t és kitaláljam, hogyan alkalmazható.

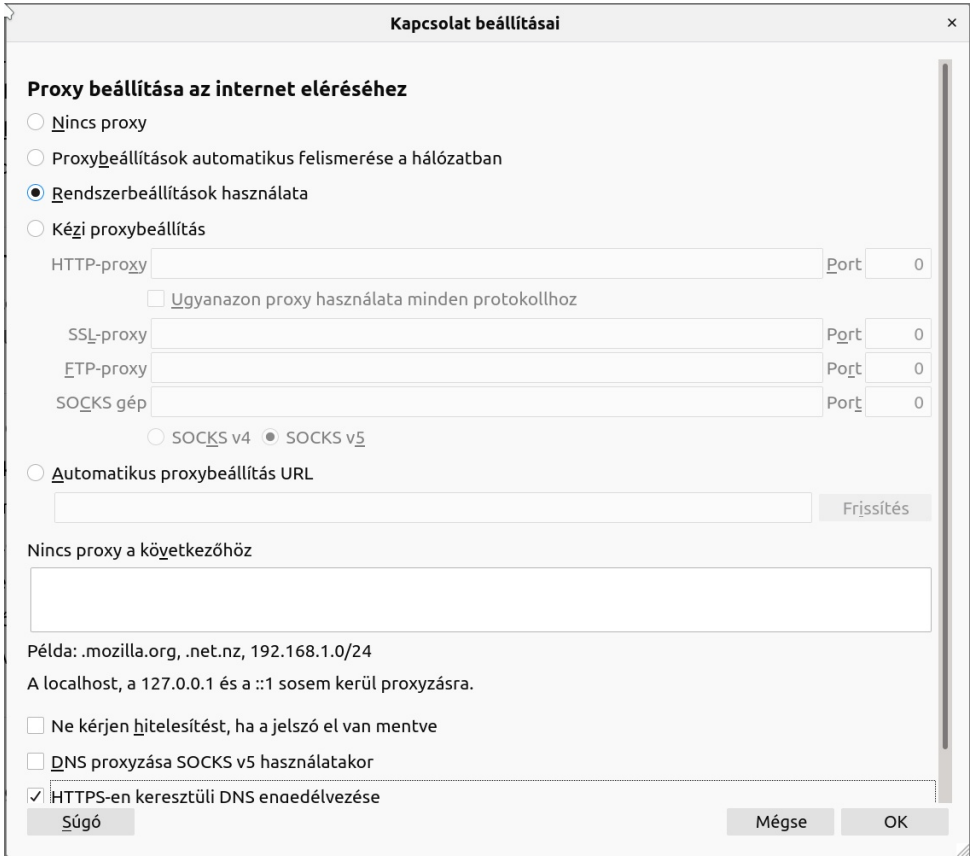
Ha te a „többi” böngésző egyikét használod, látogasd meg a fórumot, hogy kiderítsd a DoH bekapcsolásának módját, ha egyáltalán támogatott. Szívesen megjelentetnék egy olyan írást a PCLinuxOS Magazine-ban, amiben leírod a folyamatot mindenkinek.

Nos, akkor lássuk!

Firefox

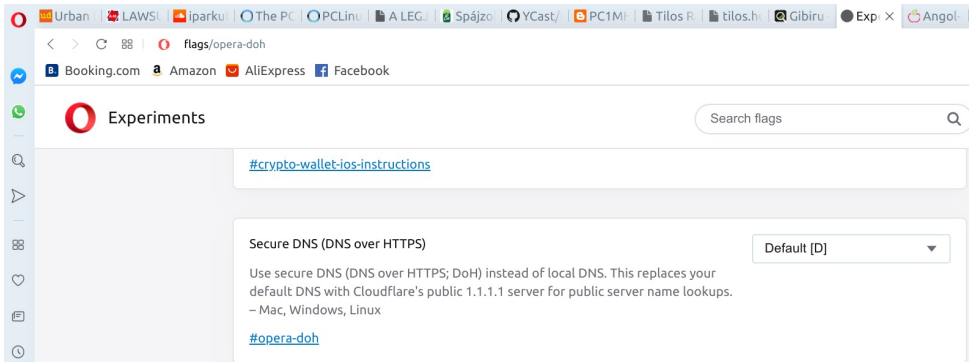
A Mozilla kezdte az egész DoH-t azzal, hogy a Firefox 70-ben lehetővé tette a DNS over HTTPS bekapcsolását. A bekapcsoláshoz a Firefox Szerkesztés menüjében válaszd ki a Beállításokat. Az Általános fülnél menj le a Hálózati beállításokig. Kattints a Beállítások gombra.

A megjelenő párbeszédablakban (ismét) görgess le a végéig. Helyezz egy jelölést a „HTTPS-en keresztüli DNS” előtti négyzetbe, ahogy azt a fenti képen láthatod. Ha bejelölted, akkor be tudod állítani, hogy az alapbeállítás szerinti



szervert (Cloudflare) használja-e vagy mást. A legtöbb felhasználónak megfelel a Cloudflare kiválasztása. A Mozilla és a Cloudflare partnerek a DNS-szolgáltatás anonimizálásában.

Opera

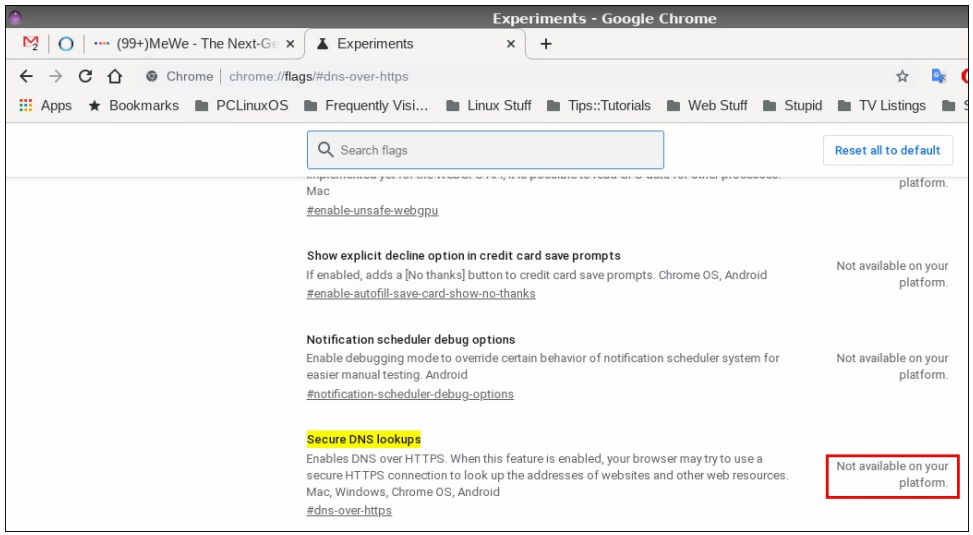


Az Opera híres a felhasználó adatainak védelme iránti törekvéseiről, így nem csoda, hogy a DoH-t is támogatja. A DoH használatára az Operát rávenni a következő pár, egyszerű lépéssel lehet.

Először, nyiss egy lapot és irányítsd az opera://flags/opera-doh címre. Ez elérhetővé tesz egy sor külső kísérleti operabeállítást.

Másodszor, görgess le a listában addig, amíg meg nem találod a „Secure DNS”-t (DNS over HTTPS) a kísérleti beállításoknál, ahogy a képen van. Látni fogod, hogy az Operában a DoH „Default [D]” alapból. A [D] azt jelenti, hogy kikapcsolt. Kattints a lenyíló menüre és váltsd át „Enabled”-re.

Google Chrome



A Google igazi csalódás, amiről feltételezhettük, hogy csatlakozott a DoH mozgalomhoz, mivel azt a felhasználók internetes magánszférájának védelmét erősítőként hirdeti. Sajnálatos módon a „Secure lookups” beállításoknál a Google Chrome közli: Not available on your platform (a platformodon nem érhető el), ahogy a fenti képen pirossal kiemelve látható. Minthogy nem használok más rendszert (Windows, Mac), így nem tudom megítélni, vajon arról van-e szó ismét, hogy a Google nem nyújt megfelelő támogatás a Linuxhoz (miközben a Linuxot használja a működéséhez minden tekintetben … ismét a jó öreg képmutatás).

Nos, a Google Chrome felhasználói ehetik a kefét, amikor a DoH használata kerül szóba. Egyszerűen elérhetetlen, legalábbis Linuxra. Huh! Mintha újabb ok

kellett volna, hogy utáljam a Chrome böngészőt. A DoH használata Google Chrome-mal Linux alatt … nos … jó öreg blöff.

Összegzés

Természetesen előnyös a DoH bekapcsolása a böngészőben, mivel a többség általában azon keresztül kapcsolódik az Internethez. De nem minden történik a böngészőben, tehát bármilyen DNS-kérés a böngészőn kívül, nem kap titkosítást.

Ám, van egy alternatív eljáárás, ami talán jobb is mint a DoH és folyamatos védelmet biztosít, mind a böngészőn belül, mind azon kívül. A PCLinuxOS Magazine 2018. májusi számában megjelentettünk a Cloudflare 1.1.1.1 DNS szolgáltatásáról egy rövid cikket. A DNS-szolgáltatód Cloudflare DNS szolgáltatására cserélésével az összes DNS-kérésed védelmet kap, minden internetes adatra.

A DoH, még 40 évvel a rendszer kialakítása után is, a személyes adatok védelme tekintetében képes jelentősen továbbfejleszteni a DNS-szolgáltatást. A vizsgálataim során úgy találtam, hogy a DoH sehol sincs alapból bekapcsolva. Tartozol magadnak annyival, hogy egy újabb védelmi réteget képezve bekapcsolod. Emellett, az ISP-dnek valóban szüksége van arra, hogy tudja, merre jártál a neten? Nem, de a sokan mások próbálnak minél többet leszívni a személyes és magán adataidról. Miért könnyítsük meg a dolgukat?

Screenshot Showcase

Posted by PendragonUK, November 9, 2019, running Mate.