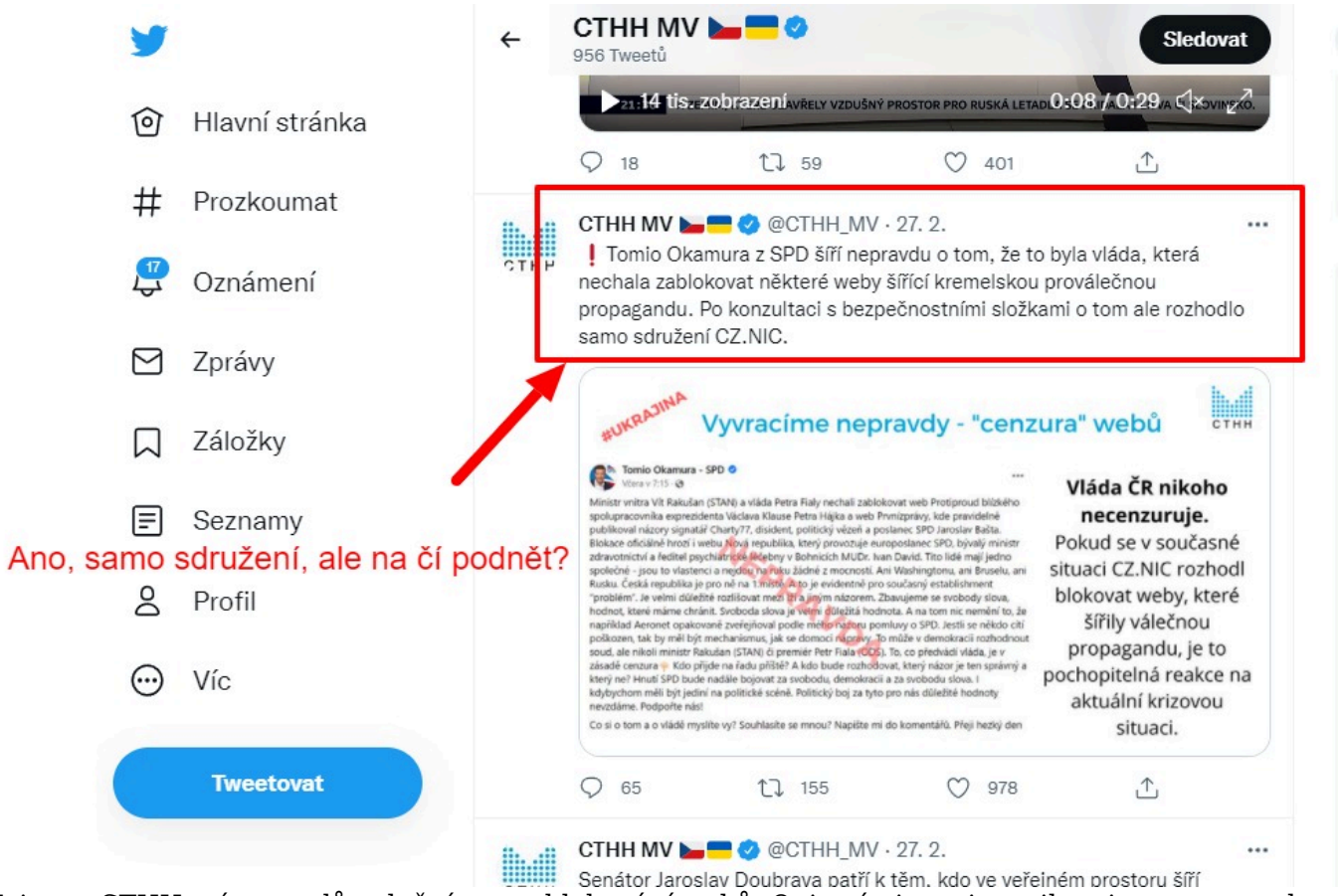
INFORMAČNÍ VÁLKA SE V ČR ROZJELA NA PLNÉ OBRÁTKY. AERONET.NEWS PŘINÁŠÍ NÁVOD, JAK NADÁLE ČÍST STÁTNÍ CENZUROU BLOKOVANÉ ZPRAVODAJSKÉ WEBY! BLOKACE LZE ALE SNADNO OBEJÍT!

- CZ24 News | 1. března 2022

ČESKO/SLOVENSKO: Po dohodě v redakci jsme se rozhodli mimořádně v nastalé situaci zařadit nikoliv zpravodajský článek, ale ve své podstatě tutorial a návod, jak v současné době v ČR a na Slovensku přistupovat na weby, které se internetoví poskytovatelé (ISP) rozhodnou z důvodu "vyššího blaha" prostě zablokovat. **Jdete na web a najednou se objeví zpráva, že doména nebyla nalezena, že neexistuje, že doména nemohla být přeložena (resolved) na číselnou IP adresu serveru atd.** Lidé bez zkušeností začnou panikařit a myslí si, že jejich oblíbený server skončil, shořel, vyletěl do povětří a nic z něj nezůstalo.



Vnitro a CTHH má toto zdůvodnění pro zablokování webů. Oni prý nic, oni muzikanti… to samo od sebe sdružení CZ.NIC

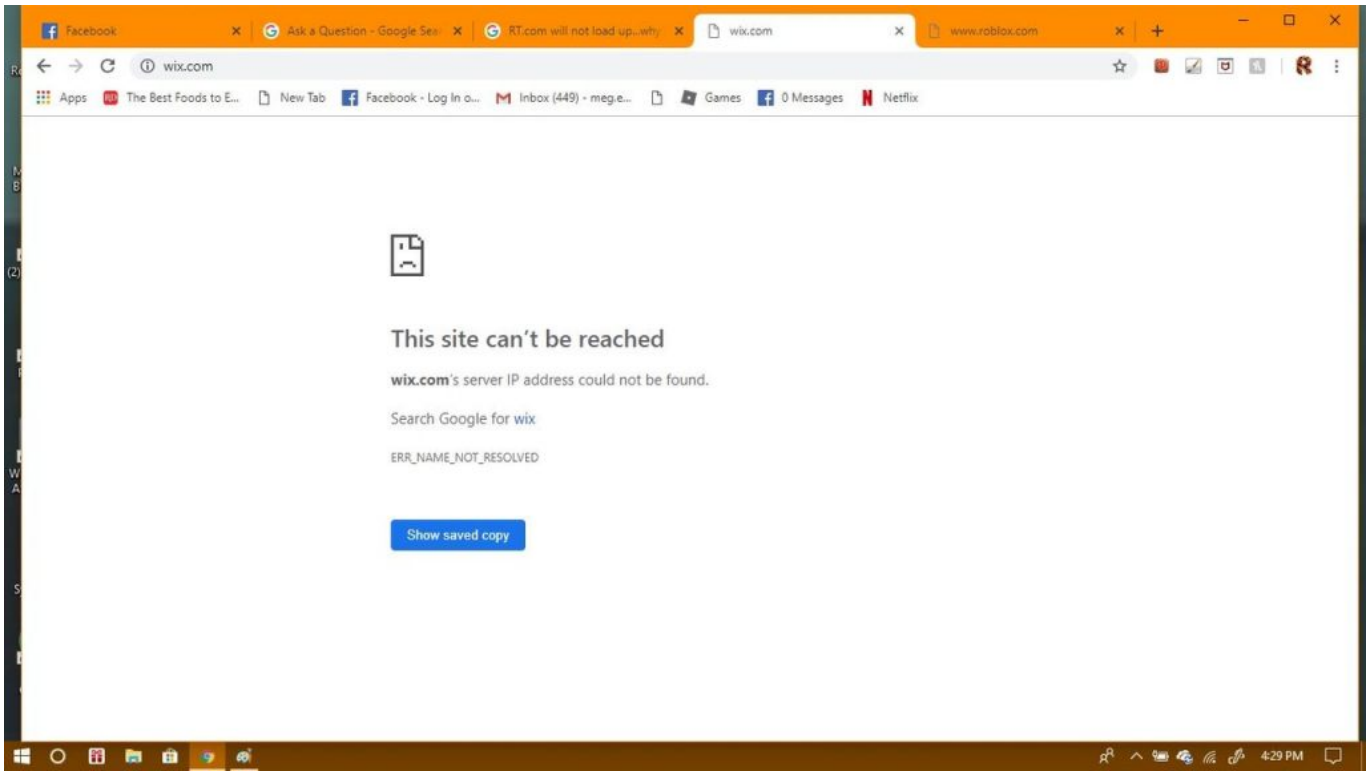
Ve skutečnosti nikam nezmizel, to jenom váš zkorumpovaný ISP operátor (anebo národní doménový správce) si uzurpuje právo vám jako zákazníkům určovat, co nesmíte číst, kam nesmíte chodit na web a odkud čerpat novinky a informace. Tohle svinstvo 28. února začal podle informací svým klientům dělat v ČR už i český T-Mobile, který provedl blokaci na svých DNS serverech a vynuloval záznamy o naší nové doméně AERONET.NEWS a tím si jako myslí, že přináší společnosti jakousi

ochranu před špatným vlivem.

Velký bratr T-Mobile chce rozhodovat, co jeho zákazníci chtějí číst. Naše rada? Bojkot a okamžité zrušení smluv s T-Mobile pro hrubé porušení lidských práv a smluvních podmínek! Pokud ale nechcete anebo musíte u T-Mobile zůstat, máme pro vás několik řešení. Všechna tato řešení pro vás nachystal náš administrátor, bez kterého bychom už dávno nefungovali. Budu tedy jen de facto citovat a de facto opisovat z jeho návodu. Nejprve tedy začneme analýzou.

Ministerstvo pravdy vás může zablokovat z dosahu alternativy celkem 3 způsoby

Blokování internetového provozu může probíhat na celkem 3 úrovních. První úrovní je blokace na úrovni Doménové národní autority. Druhou úrovní je blokace na úrovni síťových DNS serverů jednotlivých ISP operátorů. ISP operátor je dodavatel vašeho internetového připojení. A třetí úrovní blokády je blokace na úrovní datového provozu, tedy na úrovni datových paketů. Řekneme si, jak čelit všem těmto 3 typům blokací a jak je pohodlně obejít.



Domain not resolved – Doménu nešlo přeložit na DNS serveru

Je mi jasné, že mnoho našich čtenářů nemá technické IT znalosti a potřebují pomoc a právě tento adminův návod se o to má postarat. Pojďme si tedy říct, jak obcházet jednotlivé typy blokací a jak dál a nerušeně číst vaše oblíbené weby, pochopitelně nejen AE News. **Návod je univerzální a očekávám, že jej budete masově a široce šířit v ČR i na Slovensku, třeba ve formě PDF, to je jedno. Společně to dáme, společně cenzuru udoláme a svoboda nakonec zvítězí!**

Blokace na úrovni Doménové národní autority

Tento typ blokace znamená, že vydavatel vaší domény, který je určený koncovkou domény, se rozhodne vyřadit vaši doménu z tzv. aktivní zóny. V podstatě to znamená, že když se všechny DNS servery na světě začnou ptát na tuto doménu, tak doménová zóna národního operátora jim vrátí nulu. **Žádný DNS server na světě tak již není schopen doménu překládat na číselnou adresu**

serveru, bez ohledu na to, jestli se připojujete do internetu napřímo, nebo přes VPN, nebo přes TOR Browser či Opera Browser, to prostě potom nehraje roli. Žádný DNS server na světě již doménu nedokáže přeložit na číslo serverového stroje. V takovém případě přichází na řadu svépomoc, kterou poskytují jak operační systémy Windows, tak i MacOS. Jedná se způsob, jak počítači říct, jakou číselnou IP adresu serveru má zablokovaná doména v podobě nějakého názvu. A jako příklad použijeme náš AERONET.NEWS server.

Návod pro počítače Windows

Počítač Windows umí fungovat i bez DNS serverů a k tomu slouží soubor *hosts*, který na počítači najdete ve složce c:\Windows\System32\drivers\etc\

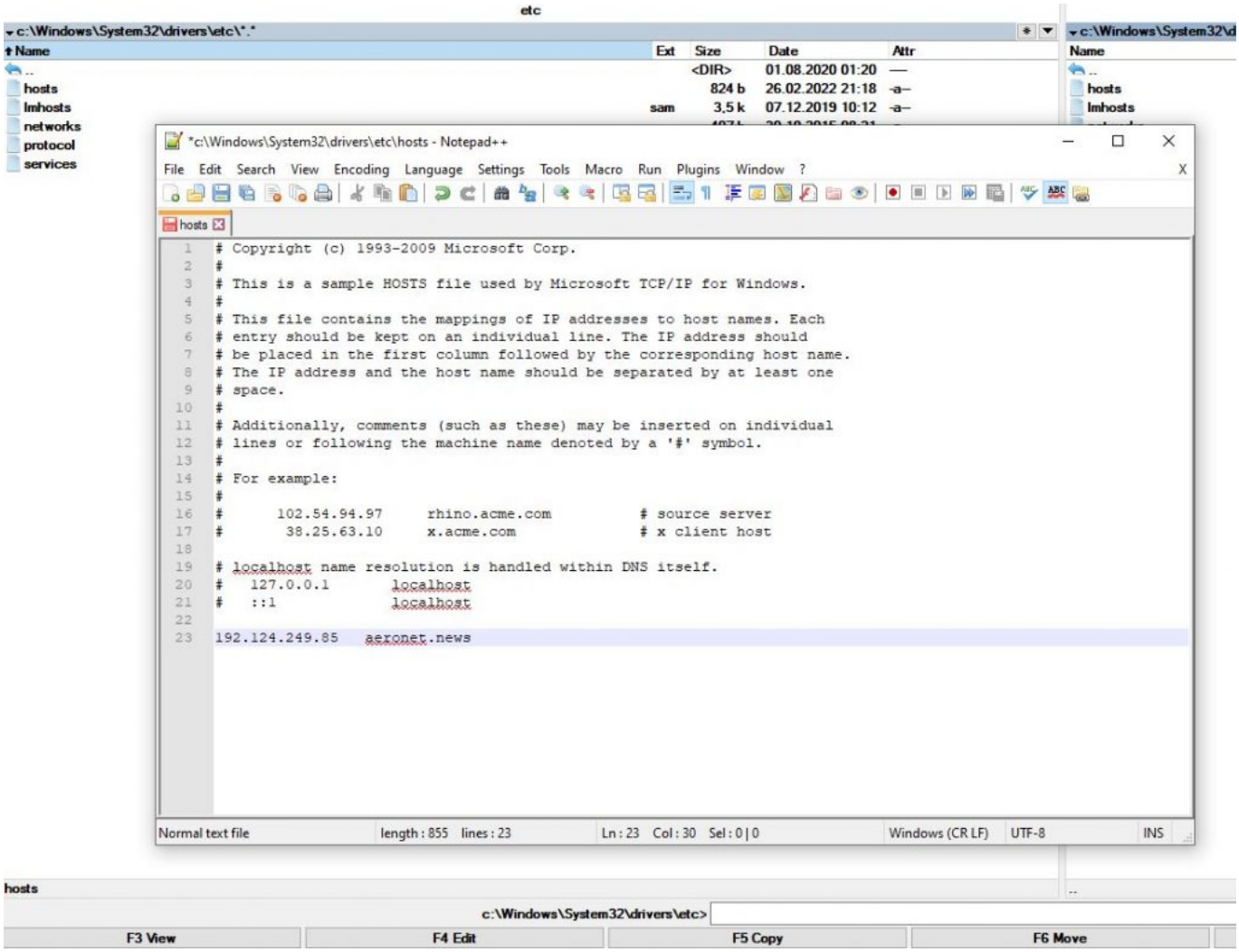
Soubor otevřete s právy administrátora jakýmkoliv textovým editorem, nejčastěji pomocí Notepad.exe a podle obrázku níže napíšete do souboru následující řádek:

192.124.249.85 aeronet.news

…a rovnou si tam na další nový řádek pod to do *hosts* přidejte i náš partnerský web SVCS:

104.21.234.228 svobodny-vysilac.cz www.svobodny-vysilac.cz

V některých případech nejde upravovat soubor *hosts* v adresáři \etc\ přímo a musíte soubor nejprve zkopírovat jinam, třeba do složky Dokumenty, tam provedete úpravu souboru a potom zpátky soubor překopírujete do složky \etc\ a potvrdíte přepis původního souboru s právy administrátora. Hotovo, šmitec. Od tohoto okamžiku můžete přistupovat na server i v případě, že by někdo z operátorů vám přestal na svých DNS překládat webovou adresu .news našeho webu. Preventivně, pro všechny případy, strýčka Příhodu a podobné exoty, náš administrátor doporučuje si tuto úpravu udělat preventivně teď a hned, abyste byli připraveni. Jak říká admin, tohle řešení je geniální v tom, že je úplně zadarmo!



Nemusíte kupovat VPN účet, nemusíte řešit TOR Browser, který je podle admina už bohužel prakticky nepoužitelný, protože jeho nody, tedy šifrovací uzly, jsou na blacklistech všech firewallů, protože jsou zneužívány hackery k páchání trestné činnosti. **Proto na TOR Browser nespoléhejte.** A v případě Doménové národní blokace by vám ani nepomohl, protože je-li doména vyřazena z aktivní zóny národního správce, tak číslo IP adresy ze serveru vám prostě nikdo nepřeloží, ani TOR Browser. Nevýhodou tohoto řešení se souborem *hosts* je situace, kdy se změní server a číslo jeho IP adresy. Potom je potřeba záznam v *hosts* opět ručně upravit odpovídajícím způsobem.

Automatizovaný skript pro lenochy, který stačí spustit jako Správce

Pokud chcete import do souboru *hosts* s IP adresami 8 zablokovaných českých serverů a dvou serverů SVCS přenechat na skriptu, můžete si ho zde stáhnout a následně postupujete takto:

Download: HostDNSimport

A: Rozbalte stažený .zip soubor do svého počítače Windows

B Spusťte soubor ***HostDNSimport.bat*** pravým tlačítkem myši a vyberte "**spustit jako správce/run as administrator**".

C: Na obrazovce se objeví výzva pro udělení souhlasu s udělením role správce. Potvrďte. Proběhne

import.

D: Následně stiskněte kombinaci tlačítek Windows+R (kulaté tlačítko Windows vlevo vedle mezerníku).

E: Napište ***cmd*** a stiskněte Enter.

F: Do černé příkazové řádky napište tento text: **ipconfig /flushdns**

G: Poté do příkazové řádky napište ***exit***, čímž ji ukončíte.

Skript si v budoucnu můžete sami upravovat, pokud se budou měnit domény a/nebo jejich IP adresy. Ovšem pozor: Na firemních počítačích s aktivní Group Policy skript selže a k zápisu do *hosts* nedojde, protože nastavená politika zakazuje na úrovni delegace vyšších práv zápis do *hosts*. Pokud ale nejde o firemní nebo podnikový počítač, tak tyto obavy mít nemusíte.

Blokace na úrovni síťových DNS serverů

Tento typ blokace je značně odlišný od předchozího typu blokace. V tomto případě je doména jako taková v pořádku, je dostupná pro každého z celého světa, jenom není dostupná pro zákazníky sítě ISP operátora, který si prostě hraje na ***Ministerstvo pravdy*** a chce rozhodovat, jaké servery jeho klienti nesmí mít možnost navštěvovat. V tomto případě máte na výběr. Buď použijete postup uvedený výše a upravíte si soubor *hosts* v počítači, anebo si prostě ve svém počítači a mobilu změníte DNS servery.

T-Mobile ČR se rozhodl změnit profesi a nově se považuje za Ministerstvo pravdy. Bude určovat, co si jeho zákazníci smí a nesmí číst na webu v jeho síti.

Abyste tomu rozuměli, pokud sami IT nerozumíte, tak vám to vysvětlíme. Když si pořídíte a koupíte internet na doma nebo do mobilu, tak vám smluvní poskytovatel internetu (ISP provider) nacpe do počítače či do mobilu jeho vlastní DNS servery. A to je problém. ISP operátor potom na svých DNS serverech si může blokovat překlad domén (resolving) všem svým klientům. Přesně tohle 28. února

2022 provedl T-Mobile v ČR všem svým klientům s našim Aeronetem. Jak z toho ven? Snadná pomoc. Změňte si DNS servery v počítači a v mobilu na zahraniční poskytovatele DNS služeb.

Změna DNS v počítači Windows

Jděte v Ovládacích panelech Windows do nabídky **Centrum síťových připojení a sdílení**, zvolte Změnit nastavení adaptéru, vyberte typ připojení, obvykle se nazývá **Připojení k místní síti**, pravým tlačítkem myši klikněte na ikonou připojení a zvolte Vlastnosti. Objeví se adaptér vašeho připojení, obvykle Realtek, pokud jde o kabelové připojení šňůrou. Zvolte volbu **Protokol IP verze 4** a dole klikněte na tlačítko Vlastnosti. A nyní zvolíte volbu Použít následující adresy serverů DNS. Ty adresy jsou vždy dvě a dáme vám teď na výběr. Můžete si vybrat:

Google DNS servery

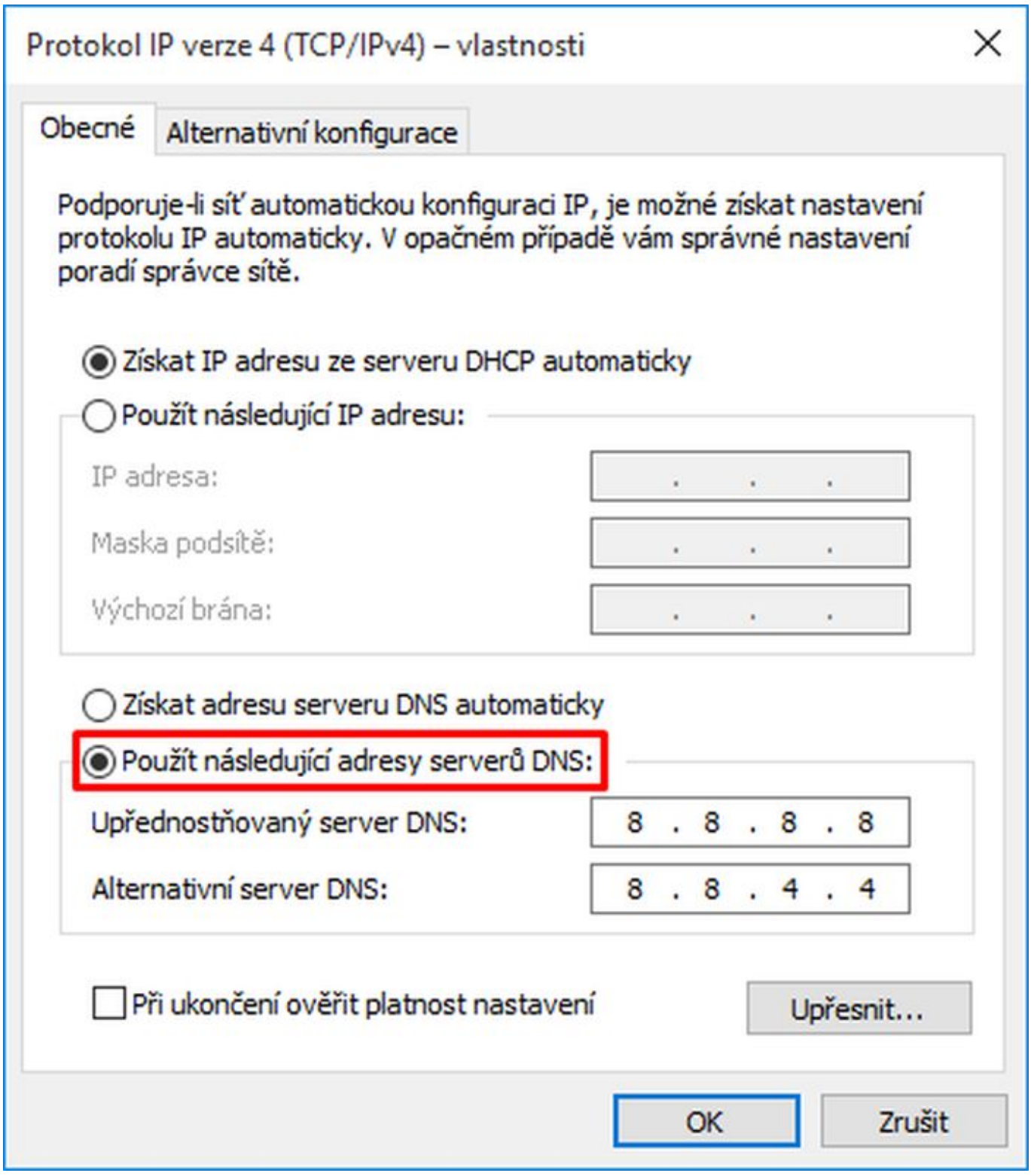
8.8.8.8 a druhý 8.8.4.4

Cloudflare DNS servery

1.1.1.1 a druhý 1.0.0.1

OpenDNS servery

208.67.222.222 a druhý 208.67.220.220

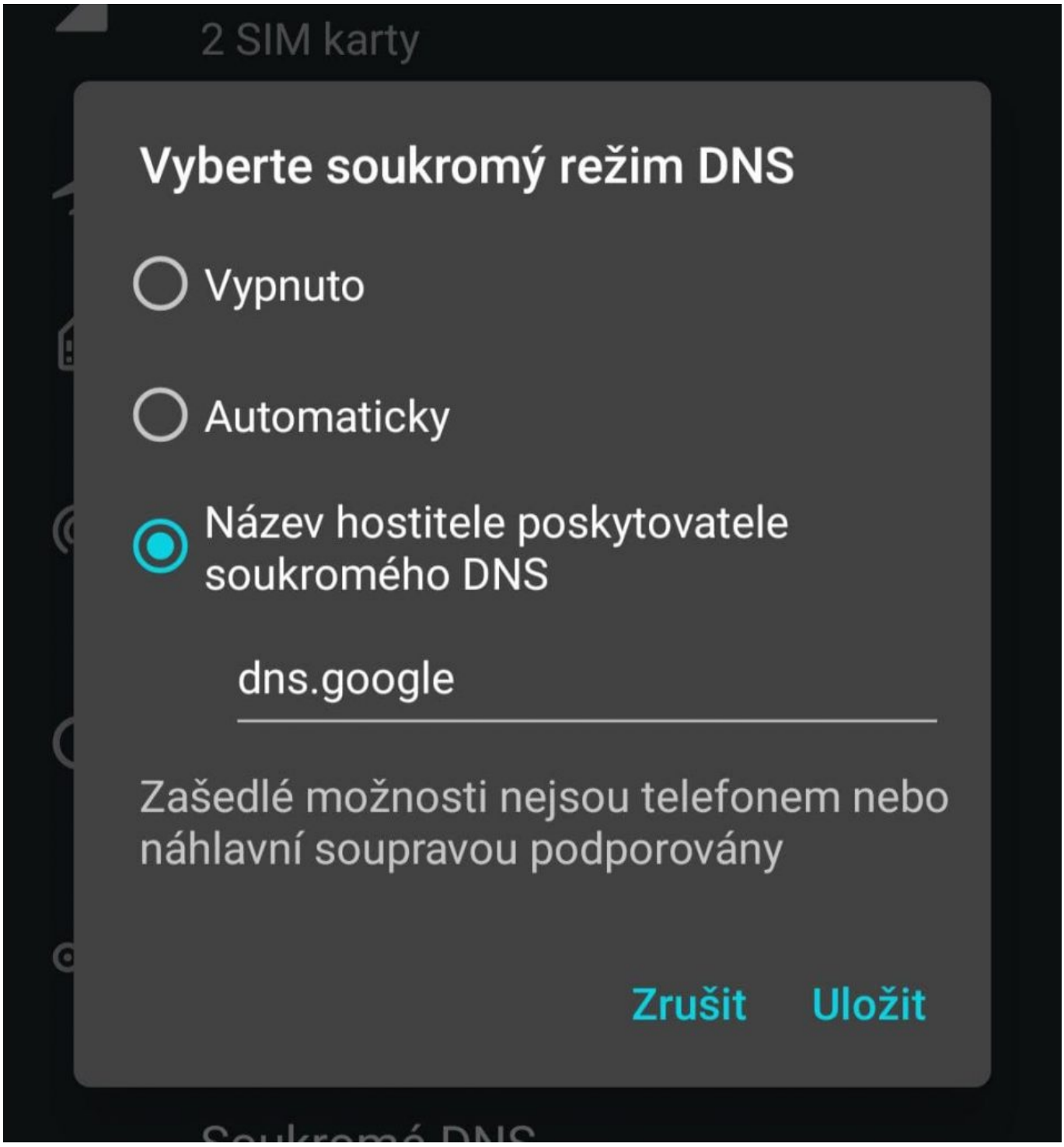


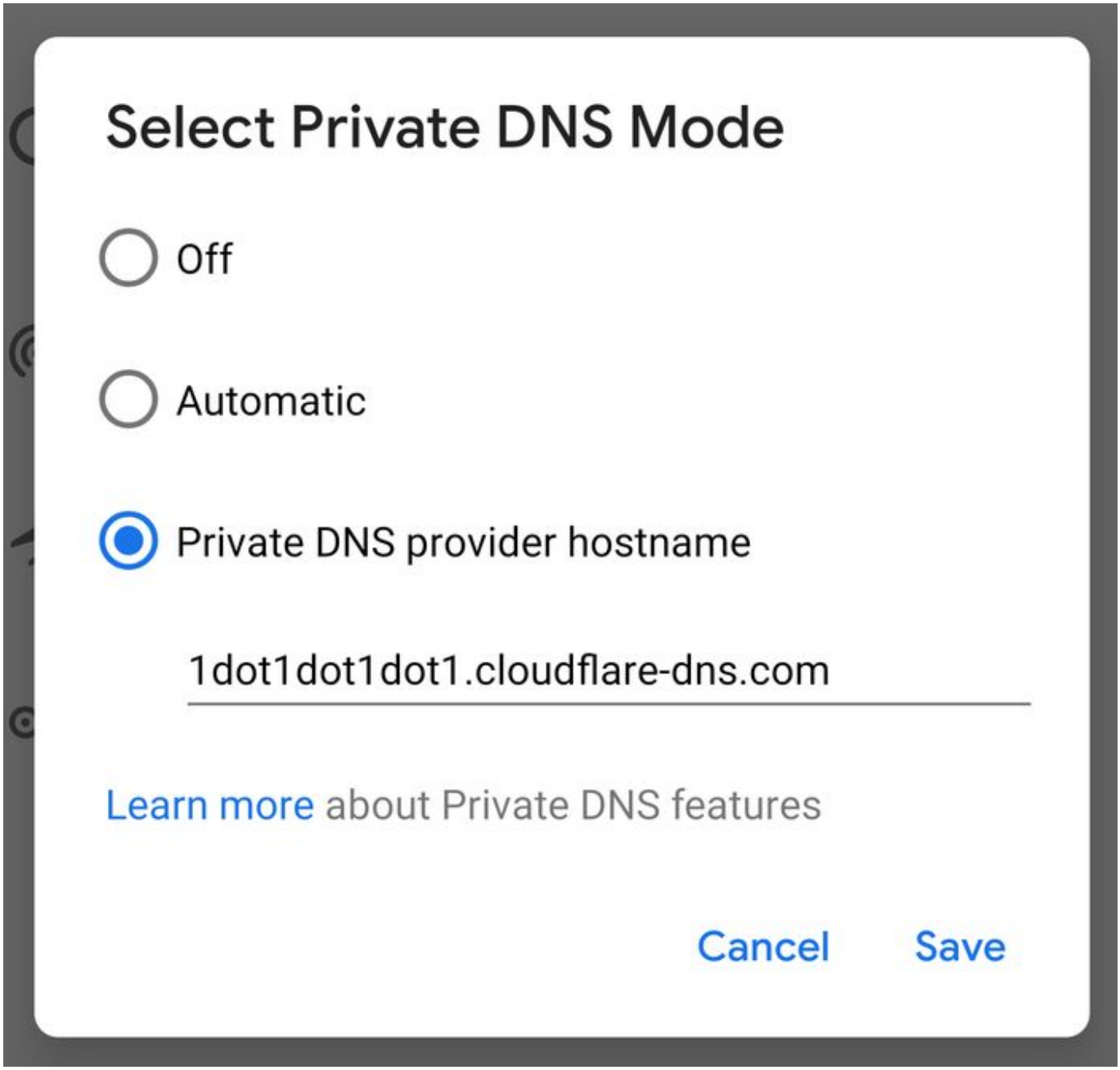
Po vložení nových DNS serverů klikněte na tlačítko OK a máte hotovo. Od této chvíle již vám T-Mobile (nejen) náš AERONET.NEWS blokovat nebude. Obrázkový postup výše uvedené úpravy najdete **zde**.

Změna DNS v mobilu

Lidé si ovšem nejen náš web prohlížejí i na mobilech, takže i tam je potřeba změnit DNS. Ale jak? V první řadě je třeba říct, že musíte mít u sebe telefon na platformě Android 9 anebo novější. Na telefonech s Android 8 a staršími to fungovat (bez rootu) nebude. Klikněte v mobilu na ikonu **Nastavení** mobilu a nahoře **do políčka vyhledávání napište *DNS***. Systém vám automaticky vyhledá nastavení, které bude znít jako "**Soukromá DNS"** nebo "**Privátní DNS nastavení"** apod.

Ve výchozím stavu je DNS nastaveno na “Automaticky” a je potřeba nastavení přepnout na “**Nakonfigurovat soukromou službu DNS**“. V tomto případě do políčka napíšete místo číselných adres pouze tento řetězec: **dns.google** pro Google DNS servery, anebo vložte tento řetězec: **1dot1dot1dot1.cloudflare-dns.com** pro Cloudflare DNS servery.



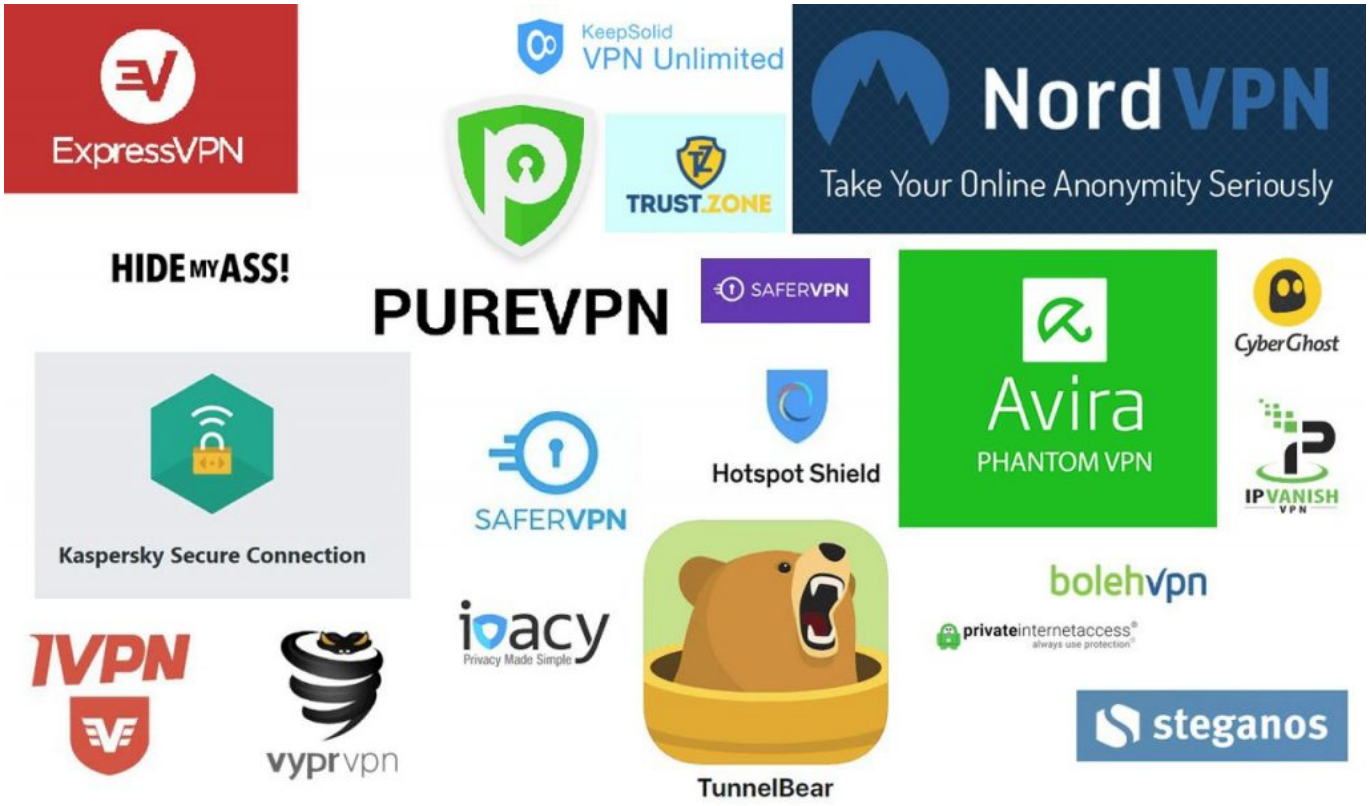


Tím nastavíte do telefonu výše zmíněné Google DNS servery. Výhoda tohoto nastavení je, že vám toto privátní DNS bude fungovat přes WIFI i přes mobilní data. Vlastní DNS jde nastavit i pro telefony iPhone, ale u nich bohužel jen pro WIFI připojení. Velmi kvalitní a podrobný návod ve slovenštině najdete **zde**. A tím se dostáváme pomalu do finále. Povíme si něco o třetí možnosti blokace webů, o té technicky nejnáročnější a pro ISP operátora nejdražší a technicky nejnákladnější.

Blokace na úrovni datového provozu

Tato forma blokace je používána v Čínské lidové republice a získala přezdívku **Velká Čínská ohnivá (firewall) zeď**. Jedná se o blokaci na úrovní hloubkové analýzy a filtrování veškerého internetového provozu obyvatelstva. Operátoři ISP provozují tzv. kontrolní brány, což jsou mohutná clusterová pole tisíců počítačů, které kontrolují jednotlivé pakety, na jaký server míří a od koho. **Každý paket musí být zachycen, ověřen, hlavička zkontrolována a porovnána se seznamem čínského Ministerstva pro informace.** Jakmile se zjistí, že někdo komunikuje s blokovaným webem, přenos je zablokován a odesílatel je ihned zadržen útvarem pořádkové policie a osobě je vystavena pokuta po sepsání protokolu.

Incident má potom dopad na jeho sociální skóre v kreditním systému ČLR. V České republice se tyto blokace na úrovní internetového provozu mohou nasazovat pouze u malých lokálních ISP operátorů s několika desítkami až stovkami klientů v síti. To je dostatečně malý počet klientů na to, aby brány provozovatele dokázaly analyzovat datový tok. **Čím větší operátor, tím větší geometrickou řadou vzrůstají finanční náklady na kontrolu obrovského množství dat.** Naštěstí, tento typ blokace lze snadno obejít pomocí VPN připojení.



Vybraní poskytovatelé VPN služeb

VPN připojení je defacto šifrovaný tunel, který začíná na vašem počítači nebo mobilu a končí daleko v cizině, odkud teprve váš datový přenos z tunelu vylézá a putuje dále na cílový server. Opačná cesta k vám probíhá stejně, ale v obráceném směru. **Váš ISP operátor neví, co přenášíte, a neví ani kam a na jaký server se chcete připojit. Operátor vidí jenom kryptovaný tunel.** Možná si řeknete, proč ISP operátor nemůže zakázat kryptované tunely?

Protože by potom nefungovaly banky, podniky, úřady atd. Ty všechny používají VPN sítě. ISP operátor totiž vidí, že ustanovujete šifrované spojení se serverem X.X.X.X a nemůže vědět, jestli je ustanovení realizováno velkou bankou, podnikem, organizací s cílem komunikace s vámi jako koncovým klientem, anebo jde o nějakou jinou komunikaci s cílem přečíst si závadový server. Proto ani Velká čínská ohňová zeď neblokuje VPN spojení, protože není možné určit a rozlišit, jestli jde o bankovní, firemní, podnikovou nebo soukromou komunikaci.

Nákup VPN je investicí do svobody

Pořídit si VPN vám vyřeší problém s blokací č. 2 a č. 3. S prvním typem blokace na úrovni Doménové národní blokace vám nepomůže. Tam pomůže jen editace souboru hosts. A jaké VPN použít? Tak v první řadě můžete použít VPN zabudované **v prohlížeči Opera [1]**, a toto VPN je zdarma. Je však velmi pomalé, ale jako nouzovka to postačuje. Aktivace VPN je snadná, v prohlížeč vlevo vedle URL řádku klikněte na obdélník VPN a zapněte VPN síť. Hotovo. Bohužel, toto VPN je velmi pomalé, v různou denní a noční dobu běží různě rychle nebo spíš pomalu, takže administrátor doporučuje

placené VPN.

Investice se vám mnohonásobně vrátí. Seznam nejlepších VPN najdete zde. Administrátor doporučuje NordVPN, ExpressVPN anebo HideMyAss. Koncový výběr je pouze na vás. Všichni poskytovatelé VPN mají aplikace jak pro Windows, tak i pro mobily Android a iOS. Aplikace si nainstalujete do počítače a mobilu a zapnete si zemi, pod jejíž IP adresou se chcete necenzurovaně připojovat do internetu. Je to jednoduché.

Fialova a Rakušanova vládní mašinerie v ČR se rozhodla budovat v ČR českou kopii Velké čínské ohňové zdi.

Ještě jedna věc k TOR Browseru, protože tato otázka se stále opakuje a vrací. Proč vám TOR Browser nefunguje na Aeronetu? Proč se vám objevuje blokační hláška našeho firewallu? Protože drtivá většina šifrovacích uzlů TORu je dnes na černých listinách bezpečnostních firem a provozovatelů firewallů, protože skrze infrastrukturu TORu probíhají denně miliony hackerských útoků.

TOR Browser je tak prakticky už nepoužitelný pro anonymizaci návštěv webů. Musíte přesedlat na placená VPN. Bohužel, s tím se nedá nic dělat. Nyní tedy víte, jak bojovat proti blokacím. Toto je stav totální informační války, kdy už nejen vlády zemí, ale i soukromé firmy si dovolují stavět se do rolí arbitrů a rozhodovat, co si smíte a nesmíte přečíst. Této situaci se musí každý přizpůsobit a přijmout opatření k obejití blokací, pokud chce nadále mít přístup na servery alternativy.

-VK-

Šéfredaktor AE News

ZDROJ