OpenVPN: más VPN szolgáltatások

PCLinuxOS Magazine – 2013. szeptember

Írta: Paul Arnote (parnote)

A PCLinuxOS Magazine e számában korábban (és a PCLinuxOS fórumon), Texstar az Open VPN VPNBook-kal való használatáról írt (Synaptic-ból telepítendő). Ugyanakkor Texstar a fórumos beírása óta napvilágot látott olyan információ, ami az ingyenes VPN szolgáltatásokat gyanússá teheti.

Csak óvatosan!

A VPNBook-ot Anonymus hacktivisták (hacker activist) azzal vádolják, hogy az Anonymus tagjai tevékenységével kapcsolatos naplófájlokat a hatóságoknak kiadták. Az Anonymus 2013. január 20-i Google+ stream-jének teljes anyaga (szöveg és kép) itt olvasható. A képben elmostam azokat a részeket, amik néhány olvasót bánthatnak. Ha a képet szerkesztetetlenül szeretnéd látni, látogasd meg az előbbi hivatkozáson a Google+ aktuális hozzászólását.

A vpnbook.com és a voxility.com naplói néhány, az #Anonymushoz köthető tevékenységgel kapcsolatos ítéletre váró Anon-tag esetén, a bírósági bizonyítékok és vádak között jelentek meg. Ne használjátok ezeket a szolgáltatásokat. Tudj róla és terjeszd.

Ha nem folytatsz rejtegetni való „illegális”, vagy „kétes” tevékenységet, akkor a VPNBook az igényeidet jól szolgálhatja. De, ha az Anonymus vádjai jogosak, akkor az adott online tevékenységed naplói a hatóságok számára „vizsgálati célból” szabadon hozzáférhetők. Ez a tény az Internet VPN-es elérésének fő célját rombolja le.

Íme, ahogy Pete Zaborszky, a „Best VPN” honlapon egy cikkében vázolta a helyzetet:

Miközben nem tudjuk, hogy a vád valós-e, vagy sem, gyanús, hogy a román Voxility cég ingyen kínál teljes értékű csomagot, ami dicsekvése szerint nagy sebességű, 128, vagy 256 bites AES titkosítású OpenVPN és PPTP protokollal, sávszélességi korlát nélküli, a használható szolgáltatások (pl. P2P) tekintetében korlátozás nélküli, és a naplókat hetente törli (ami csak az IP címet és a kapcsolat idejét jegyzi, de nem a felhasználó tevékenységét).

A VPNBook azt mondja, hogy a szolgáltatást hirdetésekből tartja fenn, de meglepő, hogy Open VPN titkosítású két európai, valamint egy-egy brit és amerikai szerverrel rendelkezik.

Természetesen, ha a vád nem igaz (vagy téged nem zavar), akkor az ingyenes ajánlat paraméterei érdemessé tehetik a VPNBook-ot a kipróbálásra...”

A VPNBook **azt hírdeti**, hogy nem tartja nyilván az ő VPN-jéhez kapcsolódva folytatott internet-tevékenységedet (látogasd meg a honlapjukat az Anonymus-idézetben található hivatkozáson keresztül, hogy lásd te is). Mindazonáltal Zaborszky egy nagyon komoly felvetést tesz a válaszában. Hogyan lehet ilyen nagy sebességű, OpenVPN és PPTP protokollos, 128, vagy 256 bites AES titkosítású, sávkorlát nélküli, korlátlan és a hetente törölt naplózású … teljes értékű csomagot ingyen, nem kevesebb mint négy külön szerveren ajánlani, hirdetésből fenntartott szolgáltatással?

Azt kapod, amiért fizettél

A régi mondás, hogy „azt kapod amiért fizettél” valóban igaznak látszik, amikor a Virtual Private Network szolgáltatót választasz. Szerencsére a Best VPN honlap nemcsak vizsgálja a VPN-eket, de a legjobb OpenVPN kompatibilis szolgáltatókról listát is vezet.

Majd mindegyik VPN-alternatíva fizetős szolgáltatás. Az árak havi 4 USD és úgy 20 USD között mozognak. Néhány VPN-szolgáltató ajánl egyéves előfizetési lehetőséget is, általában jelentős költség megtakarítással az hónapról-hónapra fizetéshez képest. Például, a HideMyAss.com, az egyik legmagasabban jegyzett VPN szolgáltatónál, az írás születésekor éppen elérhető volt egy különleges

ajánlat. Eszerint a „különleges” ajánlat szerint, a havi díj 9,99 $, miközben az éves 59,99 $. A szolgáltatást az egész évre előre kifizetve a havi díj 4,99 $-ra jön ki (az egész évre leosztva).

Miért használjunk Virtual Private Network-öt?

Ha még nem lennél meggyőződve a VPN használatának értékéről, tekintsük át az előnyöket.

Szinte alig van olyan ezen a földön, aki ne hallott volna az NSA megfigyeléseiről, ami nem csak külföldiekre, hanem amerikai állampolgárokra is kiterjed. Közülünk sokan használtak már nyílt, publikus Wifi csatlakozási pontot (hotspot). Többségünk egyre inkább látja és aggasztja a személyes adatok kutatása az Interneten. A VPN használata megoldás a problémákra.

Megnövelt az online biztonság. A VPN titkosítja az Internet-forgalmadat, megakadályozza a leskelődőket és hekkereket az online adataid könnyű elfogásában. Ez különösen akkor hasznos, amikor nyílt, ingyenes és publikus Wifi hotspot-ot használsz.

Minden internetalkalmazással működik. Web proxy-hoz képest, ami a csak böngészőn keresztül feltöltött tartalmat védi, a VPN az összes internet-alkalmazásod esetében működik. Ez azt jelenti, hogy a Pidgin csevegésed, az IRC chat-ed és minden egyéb online tevékenységed védve van az internetkapcsolatod becsövezése által.

Látszólagosan egy másik országban leszel. VPN-t használva megváltoztathatod az online személyiségedet, hogy úgy tűnjön, egy másik országban laksz. Ez lehetővé teszi, hogy a felhasználók megtekintsenek olyan tartalmakat, amik általában tiltottak egy adott országban, mint néhány iBBC-, YouTube-anyag, programok a Hulu-n, vagy a NetFlix-en, stb.. A VPN e tulajdonságának kihasználása gyakran elég a használatának indoklásához, különösen, ha a világ egy olyan részén élsz, ahol szigorú korlátozások vonatkoznak az Internetre.

Anonim internetszemélyiség. Amikor VPN-re csatlakozol, az online személyiséged (jellemzően az adott IP címed) rejtésre kerül a VPN-szerver, vagy -szolgáltató egyik anonim IP címe mögé.

Kormányzati-szintű biztonság. A legtöbb VPN a világ kormányai által használt szintű titkosítási szabványokat alkalmazza.

Cenzúra kikerülése. VPN-t használva kiiktathatod a cenzúrát, függetlenül attól, hogy az helyi jellegű-e (mint egy irodában), internetszolgáltató-függő-e (forgalom szűrés), vagy weblap blokkolás-e (irodában, vagy kormány által).

Összegzés

Vagyis, noha a Texstar a cikkében említett VPNBook szolgáltató gyanakvásra adhat okot, vannak más VPN-szolgáltatók, akik egy kicsit „biztonságosabbak” az adataidat és a naplózást tekintve (ha naplóznak egyáltalán … néhány szolgáltató egyáltalán nem készít). Természetesen, ezért a biztonságért fizetned kell. Minden attól függ, hogy mennyire akarod biztonságban látni az adataidat és a internetezési szokásaidat. Mennyire akarod elkerülni, hogy mások képesek legyenek az internettevékenységed vizsgálatára?