Nafn: _____ Dagsetning: _____ Stig: _____

ÁFANGI 10

Algengar spurningar um VPN

Gagnvirkt verkefnablað og námsleiðbeiningar

Byggt á: VPN-leiðarvísi VPN.com: **https://www.vpn.com/is/vpn/**

Verkefnablað: Hvað er VPN

Áfangi 10: Algengar spurningar um VPN – grunnstig (Hluti A)

Farðu yfir algengustu spurningar og svör sem væntanlegir viðskiptavinir hafa um sýndareinkanet.

Q1: Hvað er VPN og hvernig virkar það?

Sýndareinkanet (VPN) dulkóðar nettenginguna þína og beinir umferðinni í gegnum öruggan fjarnetþjón. Þetta felur opinberu IP-töluna þína og takmarkar það sem eftirlitsaðilar á staðarneti og netþjónustuveitan þín geta séð um umferð sem fer um VPN-göngin.

Q2: Hvers vegna ætti ég að nota VPN?

VPN verndar stafræna persónuvernd þína, tryggir tenginguna á opnum Wi-Fi netum (eins og á kaffihúsum eða flugvöllum), getur dregið úr hraðatakmörkunum sem byggjast á virkni þegar netþjónustuveitan getur ekki greint hvers konar dulkóðuð umferð er um að ræða, fer framhjá landfræðilegum takmörkunum til að nálgast efni um allan heim og hjálpar til við að tryggja auðlindir í fjarvinnu.

Q3: Gerir VPN mig algerlega nafnlausan á netinu?

Nei. Þótt VPN feli IP-töluna þína og dulkóði umferð er enn hægt að rekja þig með vafrakökum, virkum reikningum (eins og Google eða Facebook), fingrafaragreiningu vafra eða ef VPN-þjónustuveitan skráir gögnin þín.

Q4: Hægir VPN á nethraðanum mínum?

Já, örlítið. Dulkóðunarferlið og líkamleg fjarlægð að VPN-netþjóninum bæta við seinkun og álagi. Áhrifin eru breytileg eftir þjónustuveitu, samskiptareglu, fjarlægð að netþjóni, tæki og netaðstæðum.

Q5: Er löglegt að nota VPN?

Notkun VPN er lögleg í mörgum löndum, en sum lögsagnarumdæmi takmarka, stýra eða loka á VPN-þjónustu. Notendur ættu að kanna gildandi staðbundin lög áður en þeir nota VPN. Nánari upplýsingar er að finna í leiðbeiningum um lögmæti á VPN.com.

Áfangi 10: Algengar spurningar um VPN – grunnstig (Hluti B)

Farðu yfir algengustu spurningar og svör sem væntanlegir viðskiptavinir hafa um sýndareinkanet.

Q6: Get ég notað ókeypis VPN?

Ókeypis VPN geta reitt sig á auglýsingar, takmarkaða eiginleika, notkunargreiningu, gagnahámark eða önnur tekjulíkön. Notendur ættu að kynna sér persónuverndarstefnu þjónustuveitunnar, eignarhald, úttektir og viðskiptalíkan áður en þeir nota hana.

Q7: Hvað er stefna um „engar skrár“ („no-logs“)?

Stefna um engar skrár lýsir því hvaða virkni og tengigögn þjónustuveita segist ekki varðveita. Umfangið er mismunandi, svo lesendur ættu að fara yfir stefnuna og niðurstöður óháðra úttekta.

Q8: Hvernig vel ég besta VPN-ið?

Leitaðu að úttektuðum stefnum um enga skráningu, sterkum samskiptareglum (WireGuard, OpenVPN), öruggum staðsetningum netþjóna, miklum hraða, netþjónum með eingöngu vinnsluminni, kill switch-eiginleika og lögsögu utan leyniþjónustusamstarfs (eins og 5/9/14 Eyes).

Q9: Get ég notað VPN í símanum og snjallsjónvarpinu?

Já. Nútímalegar VPN-þjónustuveitur bjóða sérstök forrit fyrir iOS, Android, macOS, Windows, Linux og snjallsjónvörp, auk beinauppsetninga sem vernda öll tæki á heimilisnetinu.

Q10: Hvað er Kill Switch?

Kill switch er öryggiseiginleiki sem aftengir tækið þitt sjálfkrafa frá netinu ef VPN-tengingin rofnar. Þetta kemur í veg fyrir að ódulkóðuð gögn þín eða raunveruleg IP-tala leki út.

Áfangi 10: Algengar spurningar um VPN – framhaldsstig (Hluti C)

Kannaðu tæknilega og uppbyggingarlega þætti sýndareinkaneta og öruggra göngusamskiptareglna.

Q1: Hver er munurinn á WireGuard, OpenVPN og IKEv2?

WireGuard eru nútímalegar, léttar samskiptareglur (aðeins um 4.000 kóðalínur) sem bjóða upp á mikinn hraða og stuttan tengitíma. OpenVPN eru mjög öruggar og margreyndar opnar samskiptareglur. IKEv2 hentar vel fyrir farsíma því það getur tengst fljótt aftur þegar skipt er um net. [4]

Q2: Hvað er tvöfalt VPN eða Multi-Hop-leiðarval?

Multi-Hop beinir umferð þinni í gegnum tvo eða fleiri VPN-netþjóna í röð. Það bætir við öðru lagi dulkóðunar og hjálpar til við að halda raunverulegri IP-tölu þinni falinni fyrir öðru hoppinu ef einn netþjónn er í hættu.

Q3: Hvað er WebRTC-leki og hvernig kemur VPN í veg fyrir hann?

WebRTC er samskiptaregla í vöfrum sem getur afhjúpað raunverulegar staðar- og opinberar IP-tölur þínar jafnvel þegar VPN er virkt. Vönduð VPN loka á eða afvegaleiða WebRTC-beiðnir í forritum fyrir borðtölvur og síma og í vafraviðbótum.

Q4: Hvað eru netþjónar sem keyra eingöngu í vinnsluminni og hvers vegna skipta þeir máli?

Hefðbundnir netþjónar skrifa gögn á harða diska sem hægt er að leggja hald á eða brjótast inn í. Netþjónar eingöngu með vinnsluminni (RAM) án diska keyra alfarið í rokgjörnu minni (RAM). Þegar netþjónninn er endurræstur eða slökkt er á honum eyðast gögnin í minninu.

Q5: Hvernig kemst dulbúningur (Obfuscation) framhjá VPN-lokunum?

Dulbúningur (eða „Stealth VPN“) lætur VPN-umferð líta út eins og venjulega HTTPS-umferð (gátt 443). Það getur hjálpað henni að komast framhjá djúpri pakkaskoðun (DPI), sem stjórnvöld eða skóla- og skrifstofunet nota til að loka á VPN.

Áfangi 10: Algengar spurningar um VPN – framhaldsstig (Hluti D)

Kannaðu tæknilega og uppbyggingarlega þætti sýndareinkaneta og öruggra göngusamskiptareglna.

Q6: Hvað er skipting umferðar (Split Tunneling) og hvenær ætti ég að nota hana?

Split Tunneling leyfir þér að velja hvaða forrit fara um dulkóðuðu VPN-göngin og hver tengjast beint við internetið. Notaðu það til að beina viðkvæmum bankaforritum um VPN meðan staðbundnir leikir tengjast beint og forðast þannig svartíma sem VPN bætir við.

Q7: Hvernig virkar framvirk leynd (Perfect Forward Secrecy)?

PFS tryggir að einstakur, tímabundinn dulkóðunarlykill sé búinn til fyrir hverja einustu lotu. Jafnvel þótt einkalykill komist í hættu síðar er ekki hægt að nota hann til að afkóða fyrri eða síðari lotur, því þær notuðu óháða lykla.

Q8: Hvað eru bandalögin 5/9/14 Eyes og hvers vegna ætti mér ekki að standa á sama?

Lögsaga getur haft áhrif á lagalegt ferli sem þjónustuveita gæti staðið frammi fyrir, en raunveruleg persónuverndaráhætta fer einnig eftir því hvaða gögn þjónustuveitan varðveitir, tæknilegri uppbyggingu, eignarhaldi, gagnsæisskýrslum og úttektarsögu.

Q9: Hvað er vörn gegn DNS-leka?

DNS-lekavörn lætur tækið þitt senda vefuppflettingar (DNS-fyrirspurnir) í gegnum dulkóðaða einka-DNS-þjóna VPN-þjónustunnar í stað þjóna netþjónustuveitunnar þinnar. Þetta kemur í veg fyrir að netþjónustuveitan þín geti fylgst með því hvaða vefsvæði þú heimsækir.

Q10: Getur VPN sneitt hjá hraðatakmörkunum netþjónustuveitu?

Stundum. VPN getur hjálpað þegar netþjónustuveita hægir sértækt á þekkjanlegri virkni, en það vinnur ekki bug á þrengslum, gagnamörkum, hraðatakmörkunum á reikningi eða lélegum netgæðum.

Tæknilegar heimildir og tilvísanir

Heimildir, dulritunarforskriftir og opinberir skjalastaðlar sem vísað er til í þessu verkefnablaði.

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637