Ainm: _____ Dáta: _____ Scór: _____

SEICPHOINTE 10

Ceisteanna coitianta faoi VPN

Bileog oibre idirghníomhach agus treoir staidéir

Bunaithe ar: Treoir VPN.com ar VPNanna: **https://www.vpn.com/ga/vpn/**

Bileog oibre: Cad is VPN ann

Seicphointe 10: Ceisteanna coitianta faoi VPN – bunleibhéal (Cuid A)

Athbhreithnigh na ceisteanna agus na freagraí is coitianta a bhíonn ag ionchasaithe faoi líonraí príobháideacha fíorúla a úsáid.

Q1: Cad is VPN ann agus conas a oibríonn sé?

Criptíonn Líonra Príobháideach Fíorúil (VPN) do nasc idirlín agus ródaíonn sé do thrácht trí fhreastalaí iargúlta slán. Folaíonn sé seo do sheoladh IP poiblí agus cuireann sé teorainn leis an méid is féidir le breathnóirí líonra áitiúil agus do SIL a fheiceáil faoin trácht a ródaítear tríd an tollán VPN.

Q2: Cén fáth ar cheart dom VPN a úsáid?

Cosnaíonn VPN do phríobháideacht dhigiteach, slánaíonn sé do nasc ar líonraí Wi-Fi poiblí (ar nós caifé nó aerfoirt), is féidir leis maolú bunaithe ar ghníomhaíocht a laghdú nuair nach féidir leis an SIL cineál an tráchta chriptithe a aithint, seachnaíonn sé srianta geografacha chun rochtain a fháil ar ábhar domhanda, agus cuidíonn sé le hacmhainní oibre cianda a shlánú.

Q3: An ndéanann VPN mé go hiomlán gan ainm ar líne?

Ní hea. Cé go bhfolaíonn VPN do sheoladh IP agus go gcriptíonn sé trácht, is féidir tú a rianú fós trí fhianáin bhrabhsálaí, cuntais ghníomhacha (cosúil le Google nó Facebook), méarlorgaireacht bhrabhsálaí, nó má logálann do sholáthraí VPN do chuid sonraí.

Q4: An moillíonn VPN luas mo chuid idirlín?

Tá, beagán. Cuireann an próiseas criptithe agus an fad fisiciúil go dtí an freastalaí VPN latency agus forchostas leis. Athraíonn an tionchar de réir soláthraí, prótacail, faid freastalaí, gléis, agus dálaí líonra.

Q5: An bhfuil sé dlíthiúil VPN a úsáid?

Tá úsáid VPN dleathach i go leor tíortha, ach cuireann roinnt dlínsí srian le seirbhísí VPN, rialaíonn siad iad, nó blocálann siad iad. Ba cheart d'úsáideoirí na dlíthe áitiúla reatha a fhíorú roimh úsáid. Le haghaidh tuilleadh sonraí, féach ar na treoracha dlíthiúlachta ar VPN.com.

Seicphointe 10: Ceisteanna coitianta faoi VPN – bunleibhéal (Cuid B)

Athbhreithnigh na ceisteanna agus na freagraí is coitianta a bhíonn ag ionchasaithe faoi líonraí príobháideacha fíorúla a úsáid.

Q6: An féidir liom VPN saor in aisce a úsáid?

Féadfaidh VPNanna saor in aisce brath ar fhógraíocht, gnéithe teoranta, anailísíocht úsáide, caipíní sonraí nó samhlacha eile monaraithe airgid. Ba cheart d'úsáideoirí polasaí príobháideachta, úinéireacht, iniúchtaí agus samhail ghnó an tsoláthraí a athbhreithniú sula n-úsáideann siad é.

Q7: Cad é polasaí "gan logaí"?

Déanann polasaí gan logaí cur síos ar an ngníomhaíocht agus na sonraí nasctha a deir soláthraí nach gcoinníonn sé. Athraíonn an scóip chruinn, mar sin ba cheart do léitheoirí athbhreithniú a dhéanamh ar an bpolasaí agus ar thorthaí iniúchta neamhspleácha.

Q8: Conas a roghnaím an VPN is fearr?

Lorg polasaithe gan logaí atá iniúchta, prótacail láidre (WireGuard, OpenVPN), suíomhanna slána freastalaí, luasanna tapa, freastalaithe RAM amháin, gné kill switch, agus dlínse lasmuigh de chomhghuaillíochtaí comhroinnte faisnéise (cosúil leis na 5/9/14 Súil).

Q9: An féidir liom VPN a úsáid ar mo ghuthán agus ar mo theilifís chliste?

Tá. Cuireann soláthraithe VPN nua-aimseartha aipeanna tiomnaithe ar fáil do iOS, Android, macOS, Windows, Linux, agus teilifíseáin chliste, chomh maith le socruithe ródaire chun gach gléas i do líonra baile a chosaint.

Q10: Cad is Kill Switch ann?

Is gné slándála é Kill Switch a dhícheanglaíonn do ghléas ón idirlíon go huathoibríoch má thiteann an nasc VPN. Cuireann sé seo cosc ar do shonraí gan chriptiú nó ar do fhíor-sheoladh IP a shceitheadh.

Seicphointe 10: Ceisteanna coitianta faoi VPN – ardleibhéal (Cuid C)

Déan iniúchadh ar ghnéithe teicniúla agus struchtúracha de líonraí príobháideacha fíorúla agus prótacail tollánaithe slán.

Q1: Cad é an difríocht idir WireGuard, OpenVPN, agus IKEv2?

Is prótacal nua-aimseartha éadrom é WireGuard (~4,000 líne cód amháin) a thairgeann luasanna tapa agus amanna ceangail tapa. Is prótacal foinse oscailte an-slán, tástáilte sa chath é OpenVPN. Tá IKEv2 sármhaith do ghléasanna soghluaiste mar gheall ar a chumas athcheangal go tapa agus líonraí á n-athrú. [4]

Q2: Cad is ródú VPN dúbailte nó Multi-Hop ann?

Ródaíonn ilphreab do thrácht trí dhá fhreastalaí VPN nó níos mó i ndiaidh a chéile. Cuireann sé seo dara ciseal criptithe leis agus cuidíonn sé le do sheoladh IP fíor a choinneáil i bhfolach ón dara preab má chuirtear feidhmiú freastalaí amháin i gcontúirt.

Q3: Cad é sceitheadh WebRTC agus conas a chuireann VPN cosc air?

Is prótacal brabhsálaí é WebRTC a fhéadann do sheoltaí IP áitiúla agus poiblí fíora a nochtadh fiú nuair atá VPN gníomhach. Blocálann VPNanna préimhe iarratais WebRTC nó déanann siad iad a bhréagnú ina n-aipeanna deisce/soghluaiste agus ina n-iarmhíreanna brabhsálaí.

Q4: Cad iad freastalaithe RAM amháin agus cén fáth a bhfuil siad tábhachtach?

Scríobhann freastalaithe traidisiúnta sonraí chuig tiomántáin chrua, ar féidir iad a urghabháil nó a chur i gcomhréiteach. Ritheann freastalaithe RAM amháin (gan diosca) go hiomlán i gcuimhne luaineach (RAM). Nuair a atosaítear an freastalaí nó nuair a mhúchtar é, glantar na sonraí atá i gcuimhne.

Q5: Conas a sheachnaíonn Obfuscation bacanna VPN?

Folaíonn doiléirsiú (nó "Stealth VPN") trácht VPN ionas go mbeidh cuma thrácht HTTPS choitianta (port 443) air. Is féidir leis cabhrú leis Iniúchadh Domhain Paicéad (DPI) a sheachaint, rud a úsáideann rialtais nó líonraí scoile/oifige chun VPNanna a bhlocáil.

Seicphointe 10: Ceisteanna coitianta faoi VPN – ardleibhéal (Cuid D)

Déan iniúchadh ar ghnéithe teicniúla agus struchtúracha de líonraí príobháideacha fíorúla agus prótacail tollánaithe slán.

Q6: Cad é Tollánú Scoilte agus cathain ba cheart dom é a úsáid?

Ligeann tollánú scoilte duit a roghnú cé na haipeanna a ródaítear tríd an tollán criptithe VPN agus cé acu a cheanglaíonn go díreach leis an idirlíon. Úsáid é chun aipeanna baincéireachta íogaire a ródú tríd an VPN agus cluichí áitiúla ag ceangal go díreach, ag seachaint latency a chuireann an VPN leis.

Q7: Conas a oibríonn Rúndacht Chinnte chun Tosaigh (Perfect Forward Secrecy)?

Cinntíonn PFS go ngintear eochair chriptithe uathúil, shealadach do gach seisiún. Fiú má chuirtear eochair phríobháideach i mbaol amach anseo, ní féidir í a úsáid chun seisiúin san am a chuaigh thart ná sa todhchaí a dhíchriptiú mar gur úsáid siad eochracha neamhspleácha.

Q8: Cad iad comhghuaillíochtaí 5/9/14 Eyes agus cén fáth ar cheart dom cúram a dhéanamh díobh?

Féadfaidh dlínse tionchar a imirt ar an bpróiseas dlí a bhféadfadh soláthraí aghaidh a thabhairt air, ach braitheann an baol praiticiúil príobháideachta freisin ar na sonraí a choinníonn an soláthraí, ar a ailtireacht theicniúil, ar a úinéireacht, ar thuairisciú trédhearcachta agus ar stair iniúchta.

Q9: Cad é cosaint ar Sceitheadh DNS?

Cuireann cosaint ar sceitheadh DNS iallach ar do ghléas fiosruithe cuardaigh suíomh gréasáin (fiosruithe DNS) a sheoladh trí fhreastalaithe DNS príobháideacha criptithe an VPN seachas trí fhreastalaithe do ISP. Cuireann sé seo cosc ar do ISP rianú a dhéanamh ar na suíomhanna a thugann tú cuairt orthu.

Q10: An féidir le VPN srianadh idirlín SSI a sheachaint?

Uaireanta. D'fhéadfadh VPN cabhrú nuair a mhoillíonn ISP gníomhaíochtaí inaitheanta go roghnach, ach ní shárófar plódú, caipeanna sonraí, teorainneacha luais ar leibhéal an chuntais, nó droch-cháilíocht líonra leis.

Tagairtí teicniúla agus foinsí

Foilseacháin luaite, sonraíochtaí cripteagrafacha agus caighdeáin oifigiúla doiciméad a úsáideadh ar fud na bileoige oibre seo.

TAGAIRTÍ ACADÚLA AGUS TIONSCAIL

[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