Enw: _____ **Dyddiad:** _____ **Sgôr:** _____

PWYNT GWIRIO 10

Cwestiynau Cyffredin am VPN

Taflen Waith Ryngweithiol a Chanllaw Astudio

Yn seiliedig ar Ganllaw VPN gan VPN.com: **https://www.vpn.com/cy/vpn/**

Taflen Waith Beth yw VPN

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am VPN (Rhan A)

Adolygwch y cwestiynau a'r atebion mwyaf cyffredin sydd gan ddarpar gwsmeriaid am ddefnyddio rhwydweithiau preifat rhithwir.

Q1: Beth yw VPN a sut mae'n gweithio?

Mae Rhwydwaith Preifat Rhithwir (VPN) yn amgryptio eich cysylltiad â'r rhyngrwyd ac yn llwybro eich traffig drwy weinydd pell diogel. Mae hyn yn cuddio eich cyfeiriad IP cyhoeddus ac yn cyfyngu ar yr hyn y gall arsylwyr y rhwydwaith lleol a'ch ISP ei weld am draffig a lwybrir drwy dwnnel y VPN.

Q2: Pam dylwn i ddefnyddio VPN?

Mae VPN yn diogelu eich preifatrwydd digidol, yn sicrhau eich cysylltiad ar rwydweithiau Wi-Fi cyhoeddus (fel siopau coffi neu feysydd awyr), gall leihau arafu bwriadol ar sail gweithgarwch pan na all yr ISP adnabod y math o draffig wedi'i amgryptio, yn osgoi cyfyngiadau daearyddol i gyrchu cynnwys byd-eang, ac yn helpu i ddiogelu adnoddau gweithio o bell.

Q3: A yw VPN yn fy ngwneud yn gwbl ddienw ar-lein?

Na. Er bod VPN yn cuddio eich cyfeiriad IP ac yn amgryptio traffig, gallwch gael eich olrhain o hyd drwy gwcis porwr, cyfrifon gweithredol (fel Google neu Facebook), olion bysedd porwr, neu os yw eich darparwr VPN yn logio eich data.

Q4: A fydd VPN yn arafu cyflymder fy rhyngrwyd?

Ie, ychydig. Mae'r broses amgryptio a'r pellter ffisegol i weinydd y VPN yn ychwanegu oedi a gorbenion. Mae'r effaith yn amrywio yn ôl y darparwr, y protocol, pellter y gweinydd, y ddyfais ac amodau'r rhwydwaith.

Q5: A yw defnyddio VPN yn gyfreithlon?

Mae defnyddio VPN yn gyfreithlon mewn llawer o wledydd, ond mae rhai awdurdodaethau'n cyfyngu ar wasanaethau VPN, yn eu rheoleiddio neu'n eu rhwystro. Dylai defnyddwyr wirio'r cyfreithiau lleol cyfredol cyn eu defnyddio. Am ragor o fanylion, edrychwch ar y canllawiau cyfreithlondeb ar VPN.com.

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am VPN (Rhan B)

Adolygwch y cwestiynau a'r atebion mwyaf cyffredin sydd gan ddarpar gwsmeriaid am ddefnyddio rhwydweithiau preifat rhithwir.

Q6: A allaf ddefnyddio VPN am ddim?

Gall VPNs am ddim ddibynnu ar hysbysebu, nodweddion cyfyngedig, dadansoddeg defnydd, capiau data, neu fodelau gwneud arian eraill. Dylai defnyddwyr adolygu polisi preifatrwydd, perchnogaeth, archwiliadau a model busnes y darparwr cyn eu defnyddio.

Q7: Beth yw polisi "dim logiau"?

Mae polisi dim logiau yn disgrifio pa ddata gweithgarwch a chysylltu y mae darparwr yn dweud nad yw'n ei gadw. Mae'r union gwmpas yn amrywio, felly dylai darllenwyr adolygu'r polisi a chanfyddiadau archwiliadau annibynnol.

Q8: Sut mae dewis y VPN gorau?

Chwiliwch am bolisïau dim logiau wedi'u harchwilio, protocolau cryf (WireGuard, OpenVPN), lleoliadau gweinyddion diogel, cyflymderau uchel, gweinyddion RAM yn unig, nodwedd kill switch, ac awdurdodaeth y tu allan i gynghreiriau rhannu cudd-wybodaeth (fel y 5/9/14 Eyes).

Q9: A allaf ddefnyddio VPN ar fy ffôn a fy nheledu clyfar?

Ie. Mae darparwyr VPN modern yn cynnig apiau pwrpasol ar gyfer iOS, Android, macOS, Windows, Linux a setiau teledu clyfar, yn ogystal â gosodiadau llwybrydd i ddiogelu pob dyfais ar eich rhwydwaith cartref.

Q10: Beth yw Kill Switch?

Nodwedd ddiogelwch yw Kill Switch sy'n datgysylltu eich dyfais o'r rhyngrwyd yn awtomatig os bydd cysylltiad y VPN yn gollwng. Mae hyn yn atal eich data heb ei amgryptio neu eich cyfeiriad IP go iawn rhag gollwng.

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am VPN (Rhan C)

Archwilio agweddau technegol a strwythurol ar rwydweithiau preifat rhithwir a phrotocolau twnelu diogel.

Q1: Beth yw'r gwahaniaeth rhwng WireGuard, OpenVPN ac IKEv2?

Protocol modern ac ysgafn yw WireGuard (dim ond ~4,000 o linellau cod) sy'n cynnig cyflymderau cyflym ac amseroedd cysylltu cyflym. Protocol ffynhonnell agored hynod ddiogel sydd wedi'i brofi'n drylwyr yw OpenVPN. Mae IKEv2 yn ardderchog ar gyfer dyfeisiau symudol oherwydd ei allu i ailgysylltu'n gyflym wrth newid rhwydweithiau. [4]

Q2: Beth yw VPN dwbl neu lwybro Aml-Hop?

Mae Aml-hop yn llwybro eich traffig drwy ddau neu fwy o weinyddion VPN yn eu trefn. Mae hyn yn ychwanegu ail haen o amgryptio ac yn helpu i gadw eich cyfeiriad IP go iawn yn gudd rhag yr ail hop os caiff un gweinydd ei gyfaddawdu.

Q3: Beth yw gollwng WebRTC a sut mae VPN yn ei atal?

Protocol porwr yw WebRTC a all ddatgelu eich cyfeiriadau IP lleol a chyhoeddus go iawn hyd yn oed pan fydd VPN yn weithredol. Mae VPNs premiwm yn blocio neu'n ffugio ceisiadau WebRTC yn eu rhaglenni bwrdd gwaith/symudol a'u hestyniadau porwr.

Q4: Beth yw gweinyddion RAM-yn-unig a pham maen nhw'n bwysig?

Mae gweinyddion traddodiadol yn ysgrifennu data i yriannau caled, y gellir eu cipio neu eu cyfaddawdu. Mae gweinyddion RAM yn unig (heb ddisg) yn rhedeg yn gyfan gwbl mewn cof anweddol (RAM). Pan gaiff y gweinydd ei ailgychwyn neu ei ddiffodd, caiff data yn y cof ei ddileu.

Q5: Sut mae cuddio (Obfuscation) yn osgoi rhwystrau VPN?

Mae cuddio (neu "VPN Llechwraidd") yn cuddio traffig VPN fel ei fod yn edrych fel traffig HTTPS cyffredin (porth 443). Gall hyn ei helpu i fynd heibio i Archwilio Pecynnau Dwfn (DPI) a ddefnyddir gan lywodraethau neu rwydweithiau ysgolion/swyddfeydd i rwystro VPNs.

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am VPN (Rhan D)

Archwilio agweddau technegol a strwythurol ar rwydweithiau preifat rhithwir a phrotocolau twnelu diogel.

Q6: Beth yw Twnelu Hollt a phryd y dylwn ei ddefnyddio?

Mae Twnelu Hollt yn gadael i chi ddewis pa apiau sy'n llwybro drwy dwnnel VPN wedi'i amgryptio a pha rai sy'n cysylltu'n uniongyrchol â'r rhyngrwyd. Defnyddiwch ef i lwybro apiau bancio sensitif drwy'r VPN tra bo gemau lleol yn cysylltu'n uniongyrchol, gan osgoi cuddni ychwanegol y VPN.

Q7: Sut mae Cyfrinachedd Ymlaen (Cyfrinachedd Ymlaen Perffaith) yn gweithio?

Mae PFS yn sicrhau bod allwedd amgryptio unigryw, dros dro yn cael ei chynhyrchu ar gyfer pob sesiwn unigol. Hyd yn oed os caiff allwedd breifat ei pheryglu yn y dyfodol, ni ellir ei defnyddio i ddadgryptio sesiynau'r gorffennol na'r dyfodol oherwydd eu bod wedi defnyddio allweddi annibynnol.

Q8: Beth yw cynghreiriau 5/9/14 Eyes a pham y dylai fod o bwys i mi?

Gall awdurdodaeth effeithio ar y broses gyfreithiol y gall darparwr ei hwynebu, ond mae'r risg ymarferol i breifatrwydd hefyd yn dibynnu ar ba ddata y mae'r darparwr yn ei gadw, ei bensaernïaeth dechnegol, ei berchnogaeth, ei adroddiadau tryloywder a'i hanes archwilio.

Q9: Beth yw diogelwch rhag Gollyngiadau DNS?

Mae diogelu rhag gollyngiadau DNS yn gorfodi eich dyfais i anfon ymholiadau chwilio gwefannau (ymholiadau DNS) drwy weinyddion DNS preifat, wedi'u hamgryptio, y VPN yn hytrach na gweinyddion eich ISP. Mae hyn yn atal eich ISP rhag olrhain pa wefannau rydych yn ymweld â nhw.

Q10: A all VPN osgoi sbarduno rhyngrwyd gan ISP?

Weithiau. Gall VPN helpu pan fydd ISP yn arafu gweithgareddau adnabyddadwy yn ddetholus, ond ni fydd yn goresgyn tagfeydd, capiau data, terfynau cyflymder ar lefel cyfrif, nac ansawdd rhwydwaith gwael.

Cyfeiriadau a Ffynonellau Technegol

Cyhoeddiadau a ddyfynnwyd, manylebau cryptograffig, a safonau dogfennau swyddogol a ddefnyddiwyd ar draws y daflen waith hon.

CYFEIRIADAU YSGOLHEIGAIDD A DIWYDIANT

[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