Emri: _____ **Data:** _____ **Pikët:** _____

PIKA E KONTROLLIT 10

Pyetje të shpeshta për VPN-në

Fletë pune interaktive dhe udhëzues studimi

Bazuar në Udhëzuesin VPN.com për VPN-në: **https://www.vpn.com/sq/vpn/**

Fletë pune: Çfarë është një VPN

Pika e kontrollit 10: Pyetje të shpeshta bazë për VPN-në (Pjesa A)

Rishiko pyetjet dhe përgjigjet më të zakonshme që kanë klientët e mundshëm për përdorimin e rrjeteve private virtuale.

Q1: Çfarë është një VPN dhe si funksionon?

Një Rrjet Privat Virtual (VPN) enkripton lidhjen tënde të internetit dhe e drejton trafikun tënd përmes një serveri të sigurt të largët. Kjo maskon adresën tënde publike IP dhe kufizon atë që vëzhguesit e rrjetit lokal dhe ISP-ja jote mund të shohin për trafikun e drejtuar përmes tunelit të VPN-së.

Q2: Pse duhet të përdor një VPN?

Një VPN mbron privatësinë tënde dixhitale, siguron lidhjen tënde në rrjete Wi-Fi publike (si kafenetë ose aeroportet), mund të zvogëlojë ngadalësimin e bazuar në aktivitet kur ISP-ja nuk mund ta identifikojë llojin e trafikut të enkriptuar, anashkalon kufizimet gjeografike për të hyrë në përmbajtje globale dhe ndihmon në sigurimin e burimeve të punës në distancë.

Q3: A më bën një VPN plotësisht anonim në internet?

Jo. Ndërsa një VPN e fsheh adresën tënde IP dhe enkripton trafikun, mund të gjurmohesh ende përmes cookie-ve të shfletuesit, llogarive aktive (si Google ose Facebook), fingerprinting-ut të shfletuesit, ose nëse ofruesi yt VPN regjistron të dhënat e tua.

Q4: A do ta ngadalësojë një VPN shpejtësinë e internetit tim?

Po, pak. Procesi i enkriptimit dhe distanca fizike deri te serveri VPN shtojnë vonesë dhe ngarkesë shtesë. Ndikimi ndryshon sipas ofruesit, protokollit, distancës së serverit, pajisjes dhe kushteve të rrjetit.

Q5: A është e ligjshme përdorimi i një VPN-je?

Përdorimi i VPN-së është i ligjshëm në shumë vende, por disa juridiksione i kufizojnë, i rregullojnë ose i bllokojnë shërbimet VPN. Përdoruesit duhet të verifikojnë ligjet aktuale lokale para përdorimit. Për më shumë detaje, konsulto udhëzuesit e ligjshmërisë në VPN.com.

Pika e kontrollit 10: Pyetje të shpeshta bazë për VPN-në (Pjesa B)

Rishiko pyetjet dhe përgjigjet më të zakonshme që kanë klientët e mundshëm për përdorimin e rrjeteve private virtuale.

Q6: A mund të përdor një VPN falas?

VPN-të falas mund të mbështeten te reklamat, veçoritë e kufizuara, analitika e përdorimit, kufijtë e të dhënave ose modele të tjera monetizimi. Përdoruesit duhet të shqyrtojnë politikën e privatësisë, pronësinë, auditimet dhe modelin e biznesit të ofruesit përpara përdorimit.

Q7: Çfarë është një politikë "no-logs"?

Një politikë no-logs përshkruan cilat të dhëna aktiviteti dhe lidhjeje thotë një ofrues se nuk i ruan. Shtrirja e saktë ndryshon, ndaj lexuesit duhet të shqyrtojnë politikën dhe gjetjet e auditimeve të pavarura.

Q8: Si ta zgjedh VPN-në më të mirë?

Kërko politika no-logs të audituara, protokolle të forta (WireGuard, OpenVPN), vendndodhje të sigurta serverësh, shpejtësi të larta, serverë vetëm me RAM, funksion kill switch dhe juridiksion jashtë aleancave të ndarjes së inteligjencës (si 5/9/14 Eyes).

Q9: A mund ta përdor një VPN në telefonin dhe televizorin tim smart?

Po. Ofruesit modernë të VPN-ve ofrojnë aplikacione të dedikuara për iOS, Android, macOS, Windows, Linux dhe televizorë inteligjentë, si dhe konfigurime në ruter për të mbrojtur të gjitha pajisjet në rrjetin e shtëpisë sate.

Q10: Çfarë është një Kill Switch?

Kill Switch është një veçori sigurie që e shkëput automatikisht pajisjen tënde nga interneti nëse lidhja VPN bie. Kjo parandalon rrjedhjen e të dhënave të tua të pa enkriptuara ose të adresës reale IP.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për VPN-në (Pjesa C)

Eksploro aspektet teknike dhe strukturore të rrjeteve private virtuale dhe të protokolleve të sigurta të tunelimit.

Q1: Cili është ndryshimi midis WireGuard, OpenVPN dhe IKEv2?

WireGuard është një protokoll modern dhe i lehtë (vetëm ~4,000 rreshta kodi) që ofron shpejtësi të larta dhe kohë të shpejta lidhjeje. OpenVPN është një protokoll me kod të hapur shumë i sigurt dhe i provuar. IKEv2 është i shkëlqyer për pajisjet celulare falë aftësisë për t'u rilidhur shpejt kur ndërrohen rrjetet. [4]

Q2: Çfarë është rrugëzimi double VPN ose Multi-Hop?

Multi-Hop e rutuon trafikun tënd nëpër dy ose më shumë serverë VPN në sekuencë. Kjo shton një shtresë të dytë enkriptimi dhe ndihmon ta mbajë të fshehur adresën tënde të vërtetë IP nga hop-i i dytë nëse një server kompromentohet.

Q3: Çfarë është rrjedhja e WebRTC dhe si e parandalon një VPN?

WebRTC është një protokoll i shfletuesit që mund të zbulojë adresat e tua reale IP lokale dhe publike edhe kur një VPN është aktive. VPN-të premium bllokojnë ose falsifikojnë kërkesat WebRTC në aplikacionet e tyre për desktop/celular dhe në shtesat e shfletuesit.

Q4: Çfarë janë serverët vetëm me RAM dhe pse kanë rëndësi?

Serverët tradicionalë i shkruajnë të dhënat në disqet e ngurtë, të cilët mund të konfiskohen ose kompromentohen. Serverët vetëm me RAM (pa disk) funksionojnë tërësisht në memorie të paqëndrueshme (RAM). Kur serveri riniset ose fiket, të dhënat e mbajtura në memorie fshihen.

Q5: Si i anashkalon Obfuscation bllokimet e VPN-ve?

Maskimi (obfuscation, ose "Stealth VPN") e shndërron trafikun VPN që të duket si trafik i zakonshëm HTTPS (porti 443). Kjo mund ta ndihmojë të kalojë Inspektimin e Thellë të Paketave (DPI) që përdorin qeveritë ose rrjetet e shkollave/zyrave për të bllokuar VPN-të.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për VPN-në (Pjesa D)

Eksploro aspektet teknike dhe strukturore të rrjeteve private virtuale dhe të protokolleve të sigurta të tunelimit.

Q6: Çfarë është Split Tunneling dhe kur duhet ta përdor?

Split Tunneling të lejon të zgjedhësh cilat aplikacione rrugëzohen përmes tunelit të enkriptuar VPN dhe cilat lidhen drejtpërdrejt me internetin. Përdore për të drejtuar aplikacionet e ndjeshme bankare përmes VPN-së, ndërsa lojërat lokale lidhen drejtpërdrejt, duke shmangur vonesën e shtuar nga VPN-ja.

Q7: Si funksionon Forward Secrecy (Perfect Forward Secrecy)?

PFS siguron që për çdo seancë të krijohet një çelës enkriptimi unik e i përkohshëm. Edhe nëse një çelës privat kompromentohet në të ardhmen, ai nuk mund të përdoret për të deshifruar seancat e kaluara ose të ardhshme, sepse ato përdorën çelësa të pavarur.

Q8: Çfarë janë aleancat 5/9/14 Eyes dhe pse duhet të më interesojnë?

Juridiksioni mund të ndikojë në procesin ligjor me të cilin përballet një ofrues, por rreziku praktik i privatësisë varet edhe nga të dhënat që ruan ofruesi, arkitektura e tij teknike, pronësia, raportimi i transparencës dhe historiku i auditimeve.

Q9: Çfarë është mbrojtja nga rrjedhjet e DNS-së?

Mbrojtja nga rrjedhjet e DNS e detyron pajisjen tënde t'i dërgojë kërkesat e kërkimit të faqeve të internetit (kërkesat DNS) nëpërmjet serverëve DNS privatë dhe të enkriptuar të VPN-së, në vend të serverëve të ISP-së sate. Kjo e pengon ISP-në tënde të gjurmojë se cilat faqe vizitoni.

Q10: A mund ta kapërcejë një VPN ngadalësimin e internetit nga ISP-ja?

Ndonjëherë. Një VPN mund të ndihmojë kur një ISP ngadalëson në mënyrë selektive veprimtari të identifikueshme, por nuk do ta kapërcejë mbingarkesën, kufijtë e të dhënave, kufizimet e shpejtësisë në nivel llogarie ose cilësinë e dobët të rrjetit.

Referenca teknike dhe burime

Botime të cituara, specifikime kriptografike dhe standarde zyrtare dokumentesh të përdorura në këtë fletë pune.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[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