Navn: _____ Dato: _____ Poeng: _____

KONTROLLPUNKT 10

Vanlige spørsmål om VPN

Interaktivt arbeidsark og studieveiledning

Basert på VPN.coms VPN-veiledning: **https://www.vpn.com/no/vpn/**

Arbeidsark: Hva er et VPN

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om VPN (Del A)

Gå gjennom de vanligste spørsmålene og svarene potensielle kunder har om bruk av virtuelle private nettverk.

Q1: Hva er en VPN, og hvordan fungerer den?

Et virtuelt privat nettverk (VPN) krypterer internettforbindelsen din og ruter trafikken gjennom en sikker ekstern server. Dette maskerer den offentlige IP-adressen din og begrenser hva observatører på lokale nettverk og internettleverandøren din kan se om trafikk som rutes gjennom VPN-tunnelen.

Q2: Hvorfor bør jeg bruke en VPN?

En VPN beskytter ditt digitale personvern, sikrer tilkoblingen din på offentlige Wi-Fi-nettverk (som kafeer eller flyplasser), kan redusere aktivitetsbasert struping når internettleverandøren ikke kan identifisere typen kryptert trafikk, omgår geografiske begrensninger for å få tilgang til globalt innhold og bidrar til å sikre ressurser for fjernarbeid.

Q3: Gjør en VPN meg helt anonym på nett?

Nei. Selv om en VPN skjuler IP-adressen din og krypterer trafikk, kan du fortsatt spores via informasjonskapsler i nettleseren, aktive kontoer (som Google eller Facebook), nettleserens fingeravtrykk eller hvis VPN-leverandøren din logger dataene dine.

Q4: Vil en VPN gjøre internetthastigheten min tregere?

Ja, litt. Krypteringsprosessen og den fysiske avstanden til VPN-serveren gir ekstra ventetid og belastning. Effekten varierer med leverandør, protokoll, serveravstand, enhet og nettverksforhold.

Q5: Er det lovlig å bruke en VPN?

Bruk av VPN er lovlig i mange land, men noen jurisdiksjoner begrenser, regulerer eller blokkerer VPN-tjenester. Brukere bør kontrollere gjeldende lokale lover før bruk. For mer informasjon, se veiledningene om lovlighet på VPN.com.

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om VPN (Del B)

Gå gjennom de vanligste spørsmålene og svarene potensielle kunder har om bruk av virtuelle private nettverk.

Q6: Kan jeg bruke en gratis VPN?

Gratis VPN-er kan være basert på reklame, begrensede funksjoner, bruksanalyse, datagrenser eller andre inntektsmodeller. Brukere bør gå gjennom leverandørens personvernerklæring, eierskap, revisjoner og forretningsmodell før bruk.

Q7: Hva er en policy om ingen logging («no-logs»)?

En retningslinje om ingen logging beskriver hvilke aktivitets- og tilkoblingsdata en leverandør sier at den ikke oppbevarer. Det nøyaktige omfanget varierer, så leserne bør gjennomgå retningslinjen og funnene fra uavhengige revisjoner.

Q8: Hvordan velger jeg den beste VPN-en?

Se etter revisjonsgodkjente policyer om ingen logging, sterke protokoller (WireGuard, OpenVPN), sikre serverplasseringer, høy hastighet, servere som kun bruker RAM, en kill switch-funksjon og jurisdiksjon utenfor etterretningsallianser (som 5/9/14 Eyes).

Q9: Kan jeg bruke en VPN på telefonen og smart-TV-en min?

Ja. Moderne VPN-leverandører tilbyr egne apper for iOS, Android, macOS, Windows, Linux og smart-TV-er, i tillegg til ruteroppsett som beskytter alle enhetene i hjemmenettverket ditt.

Q10: Hva er en Kill Switch?

En kill switch er en sikkerhetsfunksjon som automatisk kobler enheten din fra internett hvis VPN-tilkoblingen faller ut. Dette hindrer at ukrypterte data eller den virkelige IP-adressen din lekker ut.

Kontrollpunkt 10: Avanserte vanlige spørsmål om VPN (Del C)

Utforsk tekniske og strukturelle sider ved virtuelle private nettverk og sikre tunnelprotokoller.

Q1: Hva er forskjellen mellom WireGuard, OpenVPN og IKEv2?

WireGuard er en moderne, lettvekts protokoll (bare ca. 4000 kodelinjer) som gir høy hastighet og raske tilkoblingstider. OpenVPN er en svært sikker, velprøvd protokoll med åpen kildekode. IKEv2 er utmerket for mobile enheter fordi den kan koble til igjen raskt når du bytter nettverk. [4]

Q2: Hva er dobbel VPN eller Multi-Hop-ruting?

Multi-hop ruter trafikken din gjennom to eller flere VPN-servere i rekkefølge. Dette gir et ekstra lag med kryptering og bidrar til å holde den virkelige IP-adressen din skjult for den andre serveren hvis én server blir kompromittert.

Q3: Hva er WebRTC-lekkasje, og hvordan forhindrer en VPN den?

WebRTC er en nettleserprotokoll som kan avsløre dine ekte lokale og offentlige IP-adresser selv når et VPN er aktivt. Premium VPN-er blokkerer eller forfalsker WebRTC-forespørsler i appene for skrivebord og mobil og i nettleserutvidelsene sine.

Q4: Hva er servere som kun bruker RAM, og hvorfor er de viktige?

Tradisjonelle servere skriver data til harddisker, som kan beslaglegges eller kompromitteres. Servere kun med RAM (diskløse) kjører helt i flyktig minne (RAM). Når serveren startes på nytt eller slås av, slettes data i minnet.

Q5: Hvordan omgår obfuskering VPN-blokkeringer?

Obfuskering (eller «Stealth VPN») skjuler VPN-trafikk slik at den ser ut som vanlig HTTPS-trafikk (port 443). Dette kan hjelpe den med å komme forbi dyp pakkeinspeksjon (DPI), som myndigheter eller skole- og kontornettverk bruker for å blokkere VPN.

Kontrollpunkt 10: Avanserte vanlige spørsmål om VPN (Del D)

Utforsk tekniske og strukturelle sider ved virtuelle private nettverk og sikre tunnelprotokoller.

Q6: Hva er split tunneling, og når bør jeg bruke det?

Split tunneling lar deg velge hvilke apper som rutes gjennom den krypterte VPN-tunnelen, og hvilke som kobler seg direkte til internett. Bruk det til å rute sensitive bankapper gjennom VPN-en mens lokale spill kobler seg direkte, slik at du unngår forsinkelsen VPN-en legger til.

Q7: Hvordan fungerer Forward Secrecy (Perfect Forward Secrecy)?

PFS sørger for at det genereres en unik, midlertidig krypteringsnøkkel for hver eneste økt. Selv om en privat nøkkel skulle bli kompromittert i fremtiden, kan den ikke brukes til å dekryptere tidligere eller fremtidige økter, fordi de brukte uavhengige nøkler.

Q8: Hva er alliansene 5/9/14 Eyes, og hvorfor bør jeg bry meg?

Jurisdiksjon kan påvirke den juridiske prosessen en leverandør kan møte, men den praktiske personvernrisikoen avhenger også av hvilke data leverandøren beholder, den tekniske arkitekturen, eierskapet, åpenhetsrapportering og revisjonshistorikken.

Q9: Hva er beskyttelse mot DNS-lekkasjer?

DNS-lekkasjebeskyttelse tvinger enheten din til å sende oppslagsforespørsler for nettsteder (DNS-forespørsler) gjennom VPN-ens private, krypterte DNS-servere i stedet for internettleverandørens servere. Dette hindrer internettleverandøren din i å spore hvilke nettsteder du besøker.

Q10: Kan en VPN omgå struping av internett fra internettleverandøren?

Noen ganger. En VPN kan hjelpe når en internettleverandør selektivt bremser identifiserbare aktiviteter, men den løser ikke overbelastning, datagrenser, hastighetsgrenser på kontonivå eller dårlig nettverkskvalitet.

Tekniske referanser og kilder

Siterte publikasjoner, kryptografiske spesifikasjoner og offisielle dokumentstandarder som er brukt i dette arbeidsarket.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[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