Naam: _____ Datum: _____ Score: _____

CONTROLEPUNT 10

Veelgestelde vragen over VPN

Interactief werkblad en studiegids

Gebaseerd op de VPN.com-VPN-gids: **https://www.vpn.com/nl/vpn/**

Werkblad: wat is een VPN

Controlepunt 10: Veelgestelde vragen over VPN – basis (Deel A)

Bekijk de meestgestelde vragen en antwoorden die potentiële klanten hebben over het gebruik van virtuele privénetwerken.

Q1: Wat is een VPN en hoe werkt het?

Een Virtual Private Network (VPN) versleutelt je internetverbinding en leidt je verkeer via een beveiligde externe server. Dit verbergt je openbare IP-adres en beperkt wat lokale netwerkwaarnemers en je internetprovider kunnen zien van het verkeer dat via de VPN-tunnel loopt.

Q2: Waarom zou ik een VPN gebruiken?

Een VPN beschermt je digitale privacy, beveiligt je verbinding op openbare wifinetwerken (zoals in koffiebars of op luchthavens), kan throttling op basis van activiteit verminderen wanneer de internetprovider het type versleuteld verkeer niet kan herkennen, omzeilt geoblokkades om toegang te krijgen tot wereldwijde content en helpt bronnen voor werken op afstand te beveiligen.

Q3: Maakt een VPN me online volledig anoniem?

Nee. Een VPN verbergt je IP-adres en versleutelt verkeer, maar je kunt nog steeds worden gevolgd via browsercookies, actieve accounts (zoals Google of Facebook), browser-fingerprinting, of als je VPN-aanbieder je gegevens logt.

Q4: Zal een VPN mijn internetsnelheid vertragen?

Ja, een klein beetje. Het versleutelingsproces en de fysieke afstand tot de VPN-server zorgen voor extra latentie en overhead. De invloed verschilt per aanbieder, protocol, serverafstand, apparaat en netwerkomstandigheden.

Q5: Is het gebruik van een VPN legaal?

VPN-gebruik is in veel landen legaal, maar sommige rechtsgebieden beperken, reguleren of blokkeren VPN-diensten. Gebruikers moeten de actuele lokale wetgeving controleren voordat ze een VPN gebruiken. Raadpleeg voor meer informatie de gidsen over legaliteit op VPN.com.

Controlepunt 10: Veelgestelde vragen over VPN – basis (Deel B)

Bekijk de meestgestelde vragen en antwoorden die potentiële klanten hebben over het gebruik van virtuele privénetwerken.

Q6: Kan ik een gratis VPN gebruiken?

Gratis VPN's kunnen vertrouwen op advertenties, beperkte functies, gebruiksanalyses, datalimieten of andere verdienmodellen. Gebruikers moeten het privacybeleid, het eigendom, de audits en het bedrijfsmodel van de aanbieder bekijken voordat ze de dienst gebruiken.

Q7: Wat is een "no-logs"-beleid?

Een no-logsbeleid beschrijft welke activiteits- en verbindingsgegevens een aanbieder zegt niet te bewaren. De exacte reikwijdte verschilt, dus lezers moeten het beleid en de bevindingen van onafhankelijke audits doornemen.

Q8: Hoe kies ik de beste VPN?

Let op auditeerde no-logsbeleid, sterke protocollen (WireGuard, OpenVPN), veilige serverlocaties, hoge snelheden, servers die alleen RAM gebruiken, een kill switch en een rechtsgebied buiten inlichtingenallianties (zoals de 5/9/14 Eyes).

Q9: Kan ik een VPN op mijn telefoon en smart-tv gebruiken?

Ja. Moderne VPN-aanbieders bieden speciale apps voor iOS, Android, macOS, Windows, Linux en smart-tv's, evenals routerinstellingen om alle apparaten in je thuisnetwerk te beschermen.

Q10: Wat is een kill switch?

Een kill switch is een beveiligingsfunctie die je apparaat automatisch van het internet loskoppelt als de VPN-verbinding wegvalt. Zo voorkom je dat je onversleutelde gegevens of je echte IP-adres lekken.

Controlepunt 10: Veelgestelde vragen over VPN – gevorderd (Deel C)

Verken technische en structurele aspecten van virtuele privénetwerken en beveiligde tunnelprotocollen.

Q1: Wat is het verschil tussen WireGuard, OpenVPN en IKEv2?

WireGuard is een modern, lichtgewicht protocol (slechts ongeveer 4.000 regels code) met hoge snelheden en snelle verbindingstijden. OpenVPN is een zeer veilig, beproefd open-sourceprotocol. IKEv2 is uitstekend voor mobiele apparaten, omdat het snel opnieuw verbinding kan maken bij het wisselen van netwerk. [4]

Q2: Wat is dubbele VPN- of multihoprouting?

Multihop routeert je verkeer achtereenvolgens via twee of meer VPN-servers. Dit voegt een tweede laag versleuteling toe en helpt je echte IP-adres verborgen te houden voor de tweede hop als een server wordt gecompromitteerd.

Q3: Wat is WebRTC-lekken en hoe voorkomt een VPN dat?

WebRTC is een browserprotocol dat je echte lokale en openbare IP-adres kan onthullen, zelfs als een VPN actief is. Premium-VPN's blokkeren of vervalsen WebRTC-verzoeken in hun desktop-/mobiele apps en browserextensies.

Q4: Wat zijn servers die alleen RAM gebruiken en waarom zijn ze belangrijk?

Traditionele servers schrijven gegevens naar harde schijven, die in beslag genomen of gecompromitteerd kunnen worden. Servers met alleen RAM (schijfloos) draaien volledig in vluchtig geheugen (RAM). Wanneer de server opnieuw wordt opgestart of uitgeschakeld, worden de gegevens in het geheugen gewist.

Q5: Hoe omzeilt obfuscatie VPN-blokkades?

Obfuscatie (of "stealth-VPN") laat VPN-verkeer eruitzien als gewoon HTTPS-verkeer (poort 443). Dat kan helpen om langs Deep Packet Inspection (DPI) te komen, die overheden of school- en kantoornetwerken gebruiken om VPN's te blokkeren.

Controlepunt 10: Veelgestelde vragen over VPN – gevorderd (Deel D)

Verken technische en structurele aspecten van virtuele privénetwerken en beveiligde tunnelprotocollen.

Q6: Wat is split tunneling en wanneer moet ik het gebruiken?

Met split tunneling kies je welke apps via de versleutelde VPN-tunnel lopen en welke rechtstreeks verbinding maken met internet. Gebruik het om gevoelige bank-apps via de VPN te laten lopen terwijl lokale games rechtstreeks verbinden, zodat je latentie door de VPN vermijdt.

Q7: Hoe werkt Forward Secrecy (Perfect Forward Secrecy)?

PFS zorgt ervoor dat voor elke sessie een unieke, tijdelijke versleutelingssleutel wordt gegenereerd. Zelfs als een privésleutel in de toekomst wordt gecompromitteerd, kan die niet worden gebruikt om eerdere of toekomstige sessies te ontsleutelen, omdat die onafhankelijke sleutels gebruikten.

Q8: Wat zijn de 5/9/14 Eyes-bondgenootschappen en waarom zou ik dat belangrijk vinden?

Jurisdictie kan van invloed zijn op de juridische procedure waarmee een aanbieder te maken kan krijgen, maar het praktische privacyrisico hangt ook af van welke gegevens de aanbieder bewaart, zijn technische architectuur, eigendom, transparantierapportages en auditgeschiedenis.

Q9: Wat is bescherming tegen DNS-lekken?

DNS-lekbescherming zorgt ervoor dat je apparaat opzoekverzoeken voor websites (DNS-verzoeken) verstuurt via de privé, versleutelde DNS-servers van de VPN in plaats van via de servers van je isp. Zo kan je isp niet volgen welke sites je bezoekt.

Q10: Kan een VPN het afknijpen van het internet door de internetprovider omzeilen?

Soms. Een VPN kan helpen wanneer een ISP selectief herkenbare activiteiten vertraagt, maar het lost congestie, datalimieten, snelheidslimieten op accountniveau of een slechte netwerkkwaliteit niet op.

Technische referenties en bronnen

Geciteerde publicaties, cryptografische specificaties en officiële documentstandaarden die in dit werkblad worden gebruikt.

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[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