Naam: _____ Datum: _____ Score: _____

Hoe kies je een VPN Werkblad

Beoordeling van VPN-aanbieders, beveiligingsstandaarden, audits en logbeleid

LEEROVERZICHT VPN

LEERLING
STUDENTENSTATUS
Network Defender-traject

VEILIG
VERBINDINGSSTATUS
Gegevenspakketten afschermen

ACTIEF
LEKBESCHERMING
Bescherming tegen DNS- en IPv6-lekken

Welkom! Dit activiteitenpakket leidt je door de basisprincipes van virtuele privénetwerken (VPN's). Je verkent hoe versleutelde tunnels je gegevens beveiligen, hoe netwerkprotocollen werken en hoe je privacylekken herkent en beperkt.

CONTROLEPUNTEN VAN HET WERKBLAD

- [ ] **Deel 1-4: Beheers VPN-begrippen en -protocollen.**
- [ ] **Deel 5-7: Los kruiswoord- en woordzoekpuzzels op.**
- [ ] **Deel 8-9: Los casestudy's en de codeopdracht op.**
- [ ] **Deel 10: Bekijk de pagina's met veelgestelde vragen (basis en gevorderd).**
- [ ] **Deel 11: Ontdek 10 interessante feiten uit de praktijk.**
- [ ] **Bonus: Snel denken-uitdaging.**

Open de VPN.com-VPN-gids

URL: https://www.vpn.com/nl/vpn/

Jouw leertraject: VPN

- Beoordeel de jurisdictie van aanbieders en zero-logs-beleid voor privacy.
- Vergelijk tunnelingprotocollen zoals WireGuard en OpenVPN op snelheid.
- Analyseer beveiligingsfuncties zoals kill switches en servernodes met alleen RAM.
- Onafhankelijke beveiligingsaudits en prijsplannen herkennen bij het kiezen.
- Kies serverlocaties op basis van je behoefte aan snelheid en geoblokkades omzeilen.

INSTRUCTIES VOOR HET SELECTIEWERKBLAD

Beantwoord de meerkeuzevragen en de vragen waar/onwaar, vul de zinnen aan met behulp van de woordenbank, koppel de definities en los de kruiswoordpuzzel en de woordzoeker op. Pas je kennis toe op het kiezen van een veilige VPN-infrastructuur. Sluit af met de bonusopdracht Snel denken.

EEN VPN KIEZEN (INLEIDING)

Het kiezen van de juiste VPN vereist dat je verder kijkt dan de marketinghype. Een betrouwbare aanbieder moet een bewezen zero-logsbeleid, veilige versleutelingsprotocollen en open-sourceclients hebben. Door beveiligingsfuncties, rechtsgebieden en snelheidsprestaties te beoordelen, kun je een VPN kiezen die past bij wat je nodig hebt om je digitaal te beschermen.

LEES ELK CONTROLEPUNT ZORGVULDIG EN KIES OF SCHRIJF HET JUISTE ANTWOORD.

Controlepunt 1: Meerkeuzeopdracht

1. 1. Wat is de belangrijkste factor bij het kiezen van een veilige VPN-aanbieder?
   - A. Het aantal serverlanden
   - B. Een onafhankelijk geauditeerd no-logsbeleid
   - C. De laagste maandelijkse prijscategorie
   - D. Opzichtige reclamesponsoring

2. 2. Welk VPN-protocol biedt de beste balans tussen snelheid en controleerbaarheid?
   - A. PPTP (verouderd)
   - B. L2TP/IPsec
   - C. Alleen OpenVPN via TCP
   - D. WireGuard

3. 3. Waarom moeten gebruikers gratis VPN's vermijden voor gevoelige activiteiten?
   - A. Ze zijn verboden in de Verenigde Staten
   - B. Ze verkopen vaak je browsegeschiedenis
   - C. Ze ondersteunen geen basale webbrowsing
   - D. Ze vereisen speciale hardware om verbinding te maken

4. 4. Wat bepaalt de wettelijke jurisdictie van het land waar een aanbieder is gevestigd?
   - A. De snelheid van de serververbinding
   - B. De soorten ondersteunde apparaten
   - C. Lokale wetten over gegevensbewaring en huiszoekingsbevelen
   - D. Het visuele thema van de clienttoepassing

5. 5. Wat is het belangrijkste doel van de 'kill switch'-functie van een VPN-client?
   - A. Om internettoegang te blokkeren als de VPN-verbinding wegvalt
   - B. Om alle geïnstalleerde toepassingen op het apparaat te verwijderen
   - C. Om de snelheid van de serververbinding te verdubbelen
   - D. Om het besturingssysteem opnieuw te starten als het inactief is

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Een VPN beschermt je apparaat tegen malwaredownloads en virusbestanden.

○ Waar ○ Onwaar

7 Vraag 7

7. Onafhankelijke audits door bureaus zoals Deloitte verifiëren beweringen over het niet bijhouden van logs.

○ Waar ○ Onwaar

8 Vraag 8

8. De wetten van het thuisland van een aanbieder hebben geen invloed op de privacy van gebruikersgegevens.

○ Waar ○ Onwaar

9 Vraag 9

9. De compacte codebase van WireGuard is gemakkelijker te controleren dan die van OpenVPN.

○ Waar ○ Onwaar

10 Vraag 10

10. Gratis VPN's verkopen vaak advertenties of volgen gebruikers om de serverkosten te dekken.

○ Waar ○ Onwaar

Controlepunt 3: Kernbegrippen invullen

Lees elke zin hieronder en vul de open plek in met de juiste term uit de woordenbank.

1. Een onafhankelijk geverifieerd beleid, bekend als _____, verplicht een VPN-aanbieder om je online geschiedenis niet vast te leggen.

2. Het moderne protocol _____ levert hoge snelheid en gebruikt een zeer kleine codebase.

3. Een veiligheidsfunctie genaamd de _____ stopt al het verkeer als de VPN-verbinding plotseling uitvalt.

4. Het beoordelen van de wettelijke _____ van een aanbieder bepaalt of die onder bewakingsverdragen valt.

5. Het beveiligen van het netwerk met _____ zorgt ervoor dat gebruikersdata na een herstart niet blijft bestaan.

6. Het verifiëren van een zero-knowledge-claim vereist een onafhankelijke _____ door gerenommeerde beveiligingsbedrijven.

WOORDENBANK

AUDIT GRATIS VPN JURISDICTIE KILL SWITCH NO-LOGS RAM-ONLY SERVERS SPLIT TUNNELING WIREGUARD

Schrijf hier je antwoorden:

1.
2.
3.
4.
5.
6.

Controlepunt 4: Netwerkbegrippen koppelen

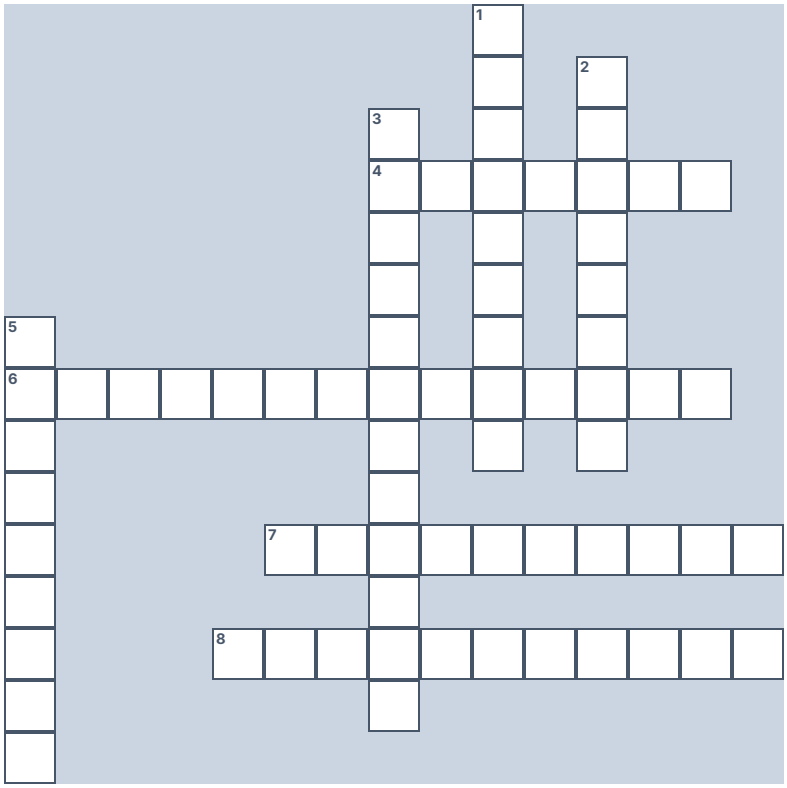
DEFINITIES KOPPELEN

Koppel elke term aan de linkerkant aan de juiste definitie aan de rechterkant door de bijbehorende letter (A-H) in het invulvak te schrijven.

☐	1. WireGuard	A	Risicovolle verbindingsdienst die vaak geld verdient door surfgegevens te registreren en te verkopen.
☐	2. Geauditeerde logs	B	Veiligheidsmechanisme dat internetroutering blokkeert als de beveiligde tunnel wegvalt.
☐	3. Rechtsgebied	C	Internationale alliantie voor het delen van inlichtingen tussen de VS, het VK, Canada, Australië en Nieuw-Zeeland.
☐	4. Kill switch	D	Hardware-infrastructuur die op vluchtig geheugen draait, zodat gegevens niet op schijf worden opgeslagen.
☐	5. Five Eyes	E	Het geografische gebied dat de wettelijke verplichtingen van de VPN-aanbieder bepaalt.
☐	6. Gratis VPN	F	Modern, snel protocol dat ongeveer 4.000 regels goed controleerbare code gebruikt.
☐	7. Servers met alleen RAM	G	Volwassen, breed geauditeerd open-sourceprotocol met een veel grotere codebase dan WireGuard.
☐	8. OpenVPN	H	Privacyclaim geverifieerd door onafhankelijke cyberbeveiligingsbedrijven van derden.

Controlepunt 5: Kruiswoordpuzzel

Los de kruiswoordpuzzel op door letters in de actieve witte vakjes te typen. De nummers komen overeen met de aanwijzingen hieronder.



HORIZONTAAL

4. Volwassen, veel geauditeerd open-sourceprotocol met een veel grotere codebase dan WireGuard (7)

6. Hardware-infrastructuur die volledig op vluchtig geheugen draait, zodat er geen data wordt opgeslagen (14)

7. Veiligheidsmechanisme dat internetverkeer blokkeert als de beveiligde tunnel wegvalt (10)

8. Het geografische gebied dat de wettelijke verplichtingen van de VPN-aanbieder bepaalt (11)

VERTICAAL

1. Modern, snel protocol met ongeveer 4.000 regels zeer goed controleerbare code (9)

2. Internationale alliantie voor het delen van inlichtingen tussen de VS, het VK, Canada, Australië en Nieuw-Zeeland (8)

3. Privacybelofte die door onafhankelijke externe cyberbeveiligingsbedrijven is geverifieerd (12)

5. Risicovolle verbindingsdienst die vaak geld verdient door browsergegevens te loggen en te verkopen (9)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

Gebruikers van schermlezers en toetsenborden kunnen de antwoorden van de kruiswoordpuzzel rechtstreeks typen in de tekstvelden hieronder.

HORIZONTAAL

4 horizontaal: Volwassen, veel geauditeerd open-sourceprotocol met een veel grotere codebase dan WireGuard (7 letters):

6 horizontaal: Hardware-infrastructuur die volledig op vluchtig geheugen draait, zodat er geen data wordt opgeslagen (14 letters):

7 horizontaal: Veiligheidsmechanisme dat internetverkeer blokkeert als de beveiligde tunnel wegvalt (10 letters):

8 horizontaal: Het geografische gebied dat de wettelijke verplichtingen van de VPN-aanbieder bepaalt (11 letters):

VERTICAAL

1 verticaal: Modern, snel protocol met ongeveer 4.000 regels zeer goed controleerbare code (9 letters):

2 verticaal: Internationale alliantie voor het delen van inlichtingen tussen de VS, het VK, Canada, Australië en Nieuw-Zeeland (8 letters):

3 verticaal: Privacybelofte die door onafhankelijke externe cyberbeveiligingsbedrijven is geverifieerd (12 letters):

5 verticaal: Risicovolle verbindingsdienst die vaak geld verdient door browsergegevens te loggen en te verkopen (9 letters):

Controlepunt 6: Verborgen woorden zoeken

Zoek de 8 belangrijkste vakwoorden die in het onderstaande rooster verborgen zijn. Woorden kunnen horizontaal, verticaal of diagonaal staan.

D K T S V R Z E H E S C A L Q
I C Z D R A U G E R I W M K F
E V R U O P E N V P N A S I W
L J M M H H N H R F K T V L R
E I T C I D S I R U J E W H B
B U F Y O Y W S H T E X A P U
S N N Z O I Q T I Y P V U O U
G U K A E P M K E A N V G G P
O Q X Y J K V S J Y W Y P J I
L Z I N P V S I T A R G J N A
O R A M O N L Y S E R V E R S
N E I A S A J F W E K Z K E K
Q N K I L L S W I T C H J A F
O K N D N C D H I B A P R L P
W T I Y F Y S G X W H F R T N

WOORDENLIJST

WIREGUARD NOLOGSBELEID JURISDICTIE KILLSWITCH FIVEEYES GRATISVPN
RAMONLYSERVERS OPENVPN

Controlepunt 6, alternatief: Toegankelijk woordenschat koppelen

Koppel elk van de 8 vaktermen uit de woordzoeker aan de juiste definitie door de letter (A-H) in de lege ruimte te schrijven.

BEGRIPPEN

- **A. WIREGUARD**
- **B. NOLOGSBELEID**
- **C. JURISDICTIE**
- **D. KILLSWITCH**
- **E. FIVEEYES**
- **F. GRATISVPN**
- **G. RAMONLYSERVERS**
- **H. OPENVPN**

DEFINITIES EN KOPPELVELDEN

1. Internationale alliantie voor het delen van inlichtingen tussen de VS, het VK, Canada, Australië en Nieuw-Zeeland.
2. Modern, snel protocol met ongeveer 4.000 regels zeer goed controleerbare code.
3. Volwassen, veel geauditeerd open-sourceprotocol met een veel grotere codebase dan WireGuard.
4. Risicovolle verbindingsdienst die vaak geld verdient door browsergegevens te loggen en te verkopen.
5. Veiligheidsmechanisme dat internetverkeer blokkeert als de beveiligde tunnel wegvalt.
6. Hardware-infrastructuur die volledig op vluchtig geheugen draait, zodat er geen data wordt opgeslagen.
7. Het geografische gebied dat de wettelijke verplichtingen van de VPN-aanbieder bepaalt.
8. Privacybelofte die door onafhankelijke externe cyberbeveiligingsbedrijven is geverifieerd.

Controlepunt 7: Opdracht met door elkaar gehaalde woorden

Ontcijfer de letters hieronder om kernbegrippen van VPN's te onthullen. Schrijf je antwoorden in de invulvelden.

1. UGEIWARDR
2. SEUJIDRTCII
3. EIFEYSEV
4. AYRROELSSE VRMN
5. OEEBDLGLSNI O
6. CSLITKIWHL
7. SGPNVTRIA
8. PNNOPVE

Bonusopdracht: Snel denken

3 ANTWOORDEN PER CATEGORIE. WIE DE LIJST ALS EERSTE INVULT, WINT.

1	Dingen die een VPN kan verbergen			
2	Dingen die belangrijker zijn dan de prijs			
3	Plekken om VPN-reviews te lezen			
4	Dingen waartegen een VPN je niet kan beschermen			
5	Vragen voor een VPN-verkoopteam			
6	Dingen die je internetprovider kan zien			
7	Punten op je checklist bij het kiezen van een VPN			
8	Plekken waar je een VPN zou gebruiken			
9	Waarschuwingssignalen bij een VPN-aanbieder			
10	Woorden die met privacy te maken hebben			
11	Dingen die je als eerste zou testen			
12	Beloften van een goede VPN-aanbieder			
13	Redenen om een VPN te gebruiken tijdens het reizen			
14	Apparaten die een VPN kunnen gebruiken			
15	Mythes over VPN's			

Controlepunt 8: Casestudy's VPN

Pas de concepten die je hebt geleerd toe om de onderstaande praktijkscenario's op te lossen.

SARAH (STUDENTE IN EEN KOFFIEZAAK)

👷 "Hoi! Ik zit bij Coffee & Bytes. Er is een onbeveiligd openbaar netwerk met de naam 'Free_Wi-Fi_No_Password'. Ik wil inloggen op mijn school-e-mail en mijn opdracht uploaden, maar ik ben bang voor hackers. Wat zijn de risico's van dit netwerk zonder VPN, en hoe beveiligt een VPN mijn gegevens?"

ALEX (REIZENDE STUDENT)

👷 "Oh nee! Ik ben voor een project in het buitenland en probeer een documentaire over biologie te kijken die op een server in mijn thuisland wordt gehost. Maar de site zegt 'Deze video is niet beschikbaar op je huidige locatie.' Waarom word ik geblokkeerd, en hoe kan een VPN me helpen om hem te kijken?"

Controlepunt 9: De code ontcijferen

Ontcijfer om je training selectiegids af te ronden dit verborgen bericht over het kiezen van een veilige infrastructuur.

LETTER-NAAR-CIJFER-VERSLEUTELINGSSLEUTEL

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

22 5 18 7 5 12 9 10 11 10 5

18 1 16 16 15 18 20 5 14 13 5 20 5 5 14

22 5 9 12 9 7 19 25 19 20 5 5 13

Ontcijferd bericht:

TIP: ELK GETAL STAAT VOOR DE POSITIE VAN DIE LETTER IN HET ALFABET (BIJV. 1 = A, 2 = B, 26 = Z).

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: Hoe verdient het geld?

Controleer het bedrijfsmodel. Abonnementen, freemium-abonnementen en gegevensverkoop beïnvloeden allemaal in hoeverre je een VPN kunt vertrouwen, en een dienst die nooit je gegevens verzamelt, kan ze niet verkopen. Lees eerst het privacybeleid. [1]

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.

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-verkeerspakketten eruitzien als gewoon HTTPS-webverkeer (poort 443). Dat helpt 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: Waarom controleren wie een VPN beheert en onderschrijft?

Reputatie is belangrijk. Zoek uit wie de eigenaren en leiders van het bedrijf zijn, zoek naar openbare audits door derden en kijk wat onafhankelijke beveiligingsexperts en de pers zeggen voordat je het vertrouwt. [1]

Deel 11: 10 interessante VPN-feiten en inzichten uit de praktijk

Bekijk deze waardevolle feiten en inzichten uit de praktijk over de geschiedenis, de markt en de technologie van VPN's.

1. EERSTE VPN-PROTOCOL

PPTP (Point-to-Point Tunneling Protocol), een vroeg VPN-protocol van een groep onder leiding van Microsoft uit de jaren 1990, wordt nu als onveilig beschouwd, dus moderne VPN's gebruiken WireGuard of OpenVPN. [1]

2. MARKTWAARDERING

De wereldwijde VPN-markt is snel gegroeid, aangedreven door de toenemende behoefte aan thuiswerken en de beveiligingseisen van bedrijven.

3. DE WIREGUARD-REVOLUTIE

WireGuard heeft een sterk gestroomlijnde codebase die is ontworpen voor efficiëntie, waardoor het gemakkelijker te controleren is op beveiligingslekken dan traditionele protocollen. [3]

4. STRIKTE AUDITSTANDAARDEN

Toonaangevende VPN-aanbieders huren bedrijven als Deloitte, KPMG of PwC in om beweringen over no-logs te controleren, en beveiligingsbedrijven als Cure53 om hun apps en servers te testen. [4]

5. OORSPRONG VAN DE 5-EYES-ALLIANTIE

Het inlichtingenpartnerschap Five Eyes van de VS, het VK, Canada, Australië en Nieuw-Zeeland is voortgekomen uit de samenwerking op het gebied van signalenspionage tussen de geallieerden in de Tweede Wereldoorlog.

6. DEEP PACKET INSPECTION

Geavanceerde firewalls zetten Deep Packet Inspection (DPI) in om metagegevens van netwerkpakketten te analyseren en standaardkenmerken van VPN-verbindingen te blokkeren.

7. ZAKELIJK GEBRUIK

Veel organisaties geven medewerkers op afstand een VPN om interne systemen zoals databases te bereiken, waardoor VPN's een veelgebruikt beveiligingsmiddel op het werk zijn.

8. GEDECENTRALISEERDE VPN'S

Gedecentraliseerde VPN's (dVPN's) verdelen verkeer over een netwerk van nodes die door peers worden beheerd, waardoor er minder afhankelijkheid is van één gecentraliseerde aanbieder.

9. TOR TEGENOVER VPN-ANONIMITEIT

Een VPN tunnelt verkeer via één aanbieder, terwijl Tor (The Onion Router) verkeer via drie vrijwilligersrelays stuurt (guard, middle, exit) om de privacy te maximaliseren. [5]

10. KOSTEN VAN DATALEKKEN

Een VPN combineren met een zero-trust-toegangsmodel, dat elke gebruiker en elk apparaat controleert, helpt organisaties gegevens te beschermen en de schade van datalekken te beperken.

Technische referenties en bronnen

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

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.

https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

Antwoordsleutel: VPN-aanbieders, beveiligingsnormen, audits en logbeleid beoordelen

1 **Beleid voor geauditeerde logs** PROTOCOLLEN — **Juist antwoord: B**

DOCENTENNOTITIE

Een onafhankelijk geauditeerd no-logsbeleid is de meest praktische manier om beweringen van een aanbieder over zero-knowledge-privacy te controleren. Opzichtige marketing of eigen beweringen zijn niet voldoende. Bron: Deloitte Advisory, Cure53 Audit.

2 **Superioriteit van WireGuard** LATENTIE — **Juist antwoord: D**

DOCENTENNOTITIE

WireGuard biedt moderne, snelle verbindingsroutering in kernelruimte met een compacte codebase (~4.000 regels), waardoor audits zeer efficiënt zijn. Bron: IETF Protocol RFC, WireGuard Project.

3 **Vraag 3** — **Juist antwoord: B**

DOCENTENNOTITIE

Gratis VPN's betalen ook voor servers, en de FTC waarschuwt dat sommige VPN-apps gebruikersgegevens delen met derden, bijvoorbeeld om advertenties te tonen.

4 **Rechtsgebieden** ROUTERINGSBEHEER — **Juist antwoord: C**

DOCENTENNOTITIE

Jurisdictie bepaalt of de VPN onder toezichtswetten, lokale verplichtingen tot gegevensbewaring en geheime gerechtelijke bevelen van de overheid valt. Bron: Privacy Rights Clearinghouse.

5 **Bescherming door kill switch** PRIVACY — **Juist antwoord: A**

DOCENTENNOTITIE

De kill switch verbreekt direct de routering van de netwerkadapter van het systeem als de tunnel wegvalt, waardoor lekken van je echte IP-adres en DNS worden voorkomen. Bron: IETF Tunnel RFC.

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Beperkingen van malware** IP-MASKERING — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Een VPN biedt een veilige, versleutelde pijplijn, maar scant geen inhoud of bestanden. Antivirussoftware is nodig om malware te blokkeren. Bron: Deloitte Advisory.

7 **Onafhankelijke audits** SNELHEDEN — **Juist antwoord: Waar**

DOCENTENNOTITIE

Auditrapporten verifiëren de configuratie van de serversoftware, de naleving van de opstelling met alleen RAM en het ontbreken van logdatabases. Bronvermelding: Deloitte Advisory, Cure53 Audit.

8 **Vraag 8** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Aanbieders moeten de wetten van hun thuisland volgen, waaronder mogelijk regels voor gegevensbewaring en bevelen om gegevens die ze bezitten uit te leveren.

9 **Grootte van de protocolcodebase** FIREWALLS — **Juist antwoord: Waar**

DOCENTENNOTITIE

Een kleinere codebase verkleint het potentiële aanvalsoppervlak en maakt het voor beveiligingsteams makkelijker de integriteit van het protocol te verifiëren. Bron: WireGuard Project.

10 **Monetisering via advertenties** NO-LOGS — **Juist antwoord: Waar**

DOCENTENNOTITIE

Zonder abonnementskosten zijn gratis VPN's afhankelijk van datamining, verkeersprofilering en het injecteren van advertenties in de browser om inkomsten te genereren. Bron: EDRi Retention Guidelines.

Woordenlijstsleutels en beoordelingsrubriek

Beoordelingsrubriek voor docenten: Geef 1 punt voor elke juiste koppeling (totaal 8 punten) en elk juist contextbegrip (totaal 6 punten).

CONTROLEPUNT 4: ANTWOORDEN BEGRIPPEN KOPPELEN

F 1. WireGuard	H 2. Geauditeerde logs	E 3. Rechtsgebied	B 4. Kill switch
C 5. Five Eyes	A 6. Gratis VPN	D 7. Servers met alleen RAM	G 8. OpenVPN

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 NO-LOGS	2 WIREGUARD	3 KILL SWITCH	4 JURISDICTIE
5 RAM-ONLY SERVERS	6 AUDIT		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 E – FIVEEYES	2 A – WIREGUARD	3 H – OPENVPN	4 F – GRATISVPN
5 D – KILLSWITCH	6 G – RAMONLYSERVERS	7 C – JURISDICTIE	8 B – NOLOGSBELEID

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen WireGuard, Geauditeerde logs en Rechtsgebied in eigen woorden kunnen uitleggen en van elk een voorbeeld kunnen geven.

Casestudy's:
Laat leerlingen hun aanbevelingen onderbouwen met feiten uit het werkblad in plaats van met aannames.

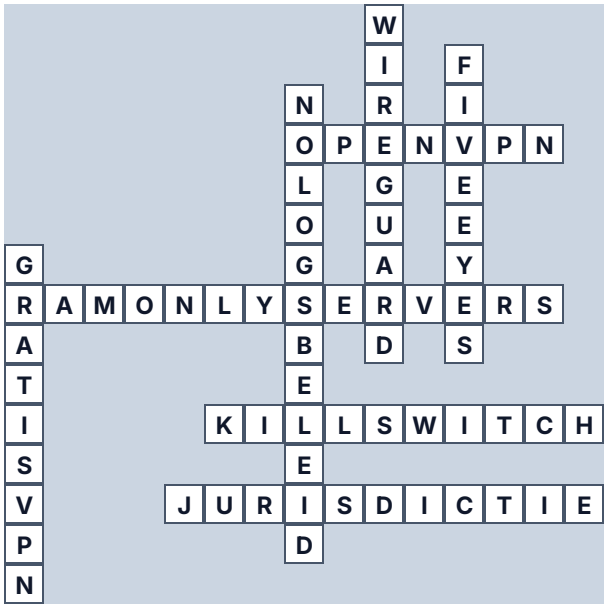
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

D	K	T	S	V	R	Z	E	H	E	S	C	A	L	Q
I	C	Z	D	R	A	U	G	E	R	I	W	M	K	F
E	V	R	U	O	P	E	N	V	P	N	A	S	I	W
L	J	M	M	H	H	N	H	R	F	K	T	V	L	R
E	I	T	C	I	D	S	I	R	U	J	E	W	H	B
B	U	F	Y	O	Y	W	S	H	T	E	X	A	P	U
S	N	N	Z	O	I	Q	T	I	Y	P	V	U	O	U
G	U	K	A	E	P	M	K	E	A	N	V	G	G	P
O	Q	X	Y	J	K	V	S	J	Y	W	Y	P	J	I
L	Z	I	N	P	V	S	I	T	A	R	G	J	N	A
O	R	A	M	O	N	L	Y	S	E	R	V	E	R	S
N	E	I	A	S	A	J	F	W	E	K	Z	K	E	K
Q	N	K	I	L	L	S	W	I	T	C	H	J	A	F
O	K	N	D	N	C	D	H	I	B	A	P	R	L	P
W	T	I	Y	F	Y	S	G	X	W	H	F	R	T	N

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

4 horizontaal: OPENVPN Volwassen, veel geauditeerd open-sourceprotocol met een veel grotere codebase dan WireGuard (7 letters)

6 horizontaal: RAMONLYSERVERS Hardware-infrastructuur die volledig op vluchtig geheugen draait, zodat er geen data wordt opgeslagen (14 letters)

7 horizontaal: KILLSWITCH Veiligheidsmechanisme dat internetverkeer blokkeert als de beveiligde tunnel wegvalt (10 letters)

8 horizontaal: JURISDICTIE Het geografische gebied dat de wettelijke verplichtingen van de VPN-aanbieder bepaalt (11 letters)

VERTICAAL

1 verticaal: WIREGUARD Modern, snel protocol met ongeveer 4.000 regels zeer goed controleerbare code (9 letters)

2 verticaal: FIVEEYES Internationale alliantie voor het delen van inlichtingen tussen de VS, het VK, Canada, Australië en Nieuw-Zeeland (8 letters)

3 verticaal: NOLOGSBELEID Privacybelofte die door onafhankelijke externe cyberbeveiligingsbedrijven is geverifieerd (12 letters)

5 verticaal: GRATISVPN Risicovolle verbindingsdienst die vaak geld verdient door browsergegevens te loggen en te verkopen (9 letters)

Sleutel voor husselwoorden en coderaadsel

Beoordelingssleutel voor de woordenschatopdracht met door elkaar gehusselde woorden en de Geheime codeopdracht.

SLEUTEL WOORDEN ORDENEN

1. UGEIWARDR — WIREGUARD
2. SEUJIDRTCII — JURISDICTIE
3. EIFEYSEV — FIVEEYES
4. AYRROELSSEVRMN — RAMONLYSERVERS
5. OEEBDLGLSNIO — NOLOGSBELEID
6. CSLITKIWHL — KILLSWITCH
7. SGPNVTRIA — GRATISVPN
8. PNNOPVE — OPENVPN

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"VERGELIJK JE RAPPORTEN MET EEN VEILIG SYSTEEM"

Antwoordsleutel casestudy's

A Scenario A: Beveiliging van openbare netwerken

SNIFFING EN VERSLEUTELING | Het dilemma van Sarah

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Risico's: Packet sniffing, onderschepping van gegevens en man-in-the-middle-aanvallen. Iemand op hetzelfde netwerk van de koffiezaak zou haar inloggegevens of huiswerkbestand kunnen onderscheppen.
- VPN-bescherming: versleutelt de payloads van netwerkpakketten, waardoor onderschept tunnelverkeer onleesbaar is voor passieve afluisteraars op het lokale netwerk wanneer de VPN correct is geconfigureerd.

B Scenario B: Toegang tot geblokkeerde bronnen

GEOBLOKKADES EN IP-ADRESSEN | Het dilemma van Alex

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Reden van blokkade: de streamingdienst gebruikt geoblokkering, waarbij het lokale IP-adres van de reiziger wordt gekoppeld aan zijn fysieke land en op basis van territoriale licenties wordt geblokkeerd.
- Hoe VPN helpt: Zijn echte locatie maskeren door verkeer te routeren via een server in zijn thuisland. De site ziet het IP-adres van het thuisland, waardoor toegang mogelijk is.