Naam: _____ Datum: _____ Score: _____

Hoe verberg je jouw IP-adres Werkblad

Je IP-adres verbergen, locatie maskeren, proxy, Tor en DNS-/WebRTC-lekken voorkomen

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

- Leg uit hoe IP-adressen werken en hoe ze locaties verraden.
- Vergelijk proxy's, Tor en VPN's voor het verbergen van netwerkadressen.
- Methoden herkennen om DNS- en WebRTC-lekken op te sporen en te voorkomen.
- Begrijp hoe websites gebruikers volgen via hun openbare IP-adres.
- Beoordeel multihop-routering en versleutelde tunnels voor IP-bescherming.

INSTRUCTIES WERKBLAD IP-BESCHERMING

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 verbergen van je IP-adres en het voorkomen van lekken. Sluit af met de bonusopdracht Snel denken.

JE IP-ADRES VERBERGEN (INLEIDING)

Je IP-adres is een digitaal postadres dat je fysieke locatie en netwerkgedrag zichtbaar maakt. Je IP-adres verbergen is de eerste verdedigingslinie tegen online tracking, doelgroepprofilering en geoblokkades. Als je begrijpt hoe je je adres veilig maskeert, help je je privacy online te beschermen.

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

Controlepunt 1: Meerkeuzeopdracht

1. Wat onthult het openbare IP-adres van een apparaat aan websites die je bezoekt?

- A. Het creditcardnummer van de gebruiker
- B. Je ongeveer locatie en de naam van je internetprovider
- C. De volledige lokale bestandsmap
- D. De taalinstellingen van het toetsenbord

2. Welke methode verbergt je IP-adres en versleutelt al het verkeer op systeemniveau?

- A. Een standaard webproxy
- B. Je browsercookies wissen
- C. Een virtueel privénetwerk (VPN)
- D. Je eigen firewall uitschakelen

3. Wat is een grote privacybeperking van het gebruik van een gratis webproxy?

- A. Het versleutelt gegevensverkeer op openbare netwerken niet
- B. Er moet een extern besturingssysteem worden geïnstalleerd
- C. Het is volledig illegaal in de Verenigde Staten
- D. Het vereist een speciale telefoonlijnverbinding

4. Hoe biedt het Tor-netwerk gebruikers een hoge mate van anonimiteit?

- A. Door verbindingssnelheden te verhogen
- B. Door verkeer te routeren via drie relays die door vrijwilligers worden beheerd
- C. Door je naam te registreren in een wereldwijde database
- D. Door toegang te beperken tot alleen overheidsinstanties

5. Wat is een DNS-lek?

- A. Een fout bij het verzenden van een e-mail naar het verkeerde adres
- B. Wanneer DNS-verzoeken de VPN-tunnel omzeilen en naar de internetprovider gaan
- C. Een hardwarestoring in de voeding van de lokale router
- D. Een update van het stuurprogramma van de lokale netwerkadapter

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Een proxyserver versleutelt achtergrondverkeer van het besturingssysteem net zoals een VPN.

○ Waar ○ Onwaar

7 Vraag 7

7. Tor-routering is zeer veilig, maar verlaagt de browsesnelheid van het netwerk.

○ Waar ○ Onwaar

8 Vraag 8

8. WebRTC-lekken kunnen tijdens een actieve VPN-sessie je echte IP-adres onthullen.

○ Waar ○ Onwaar

9 Vraag 9

9. Met een VPN aan en zonder lekken kan je internetprovider niet zien welke websites je bezoekt.

○ Waar ○ Onwaar

10 Vraag 10

10. Je IP-adres verbergen blokkeert tracking via browserfingerprinting.

○ 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 beveiligde tunnel die je domeinquery's toch blootstelt, heet een _____ .

2. Browsergebaseerde API's voor spraak- en videocommunicatie, zoals _____ , kunnen per ongeluk je eigen IP-adres lekken.

3. Een _____ leidt browserverkeer om, maar versleutelt de payload van pakketten niet.

4. De meerlaagse versleuteling van het _____ biedt een hoge mate van anonimiteit.

5. Je openbare _____ wordt toegewezen door je telecomaanbieder en verraadt je regio.

6. Het omzeilen van regionale mediablokkades lukt door _____ van je locatie.

WOORDENBANK

COOKIES DNS-LEK IP-ADRES ISP-TRACKING MASKERING TOR-NETWERK WEBPROXY WEBRTC

Schrijf hier je antwoorden:

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

Controlepunt 4: Netwerkbegrippen koppelen

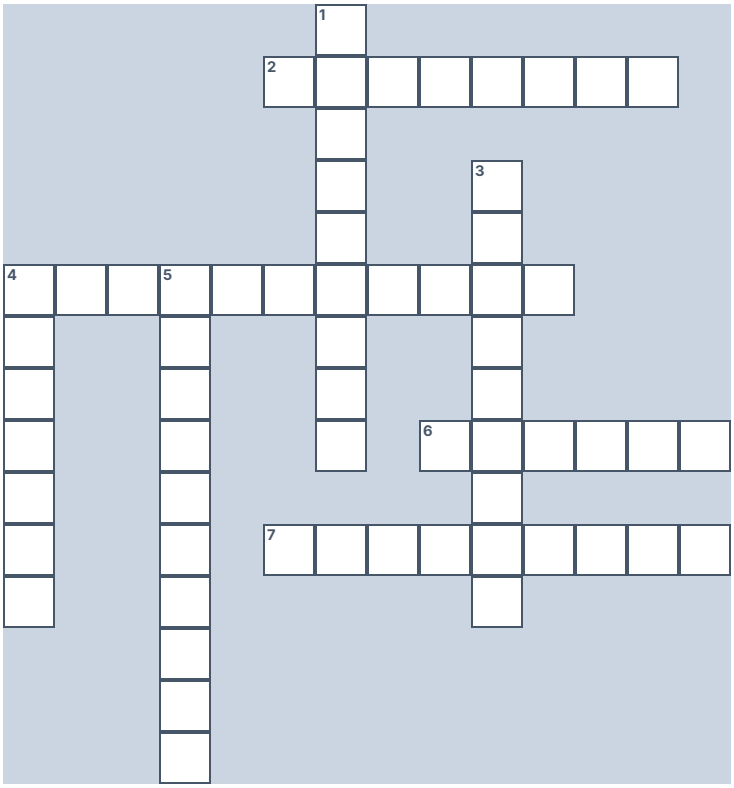
DEFINITIES KOPPELEN

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. IP-adres	A	Versleutelt al het verkeer van een apparaat en routeert het via een VPN-server.
☐	2. VPN-tunnel	B	Leidt gegevens via drie vrijwilligersservers en versleutelt bij elke stap een laag.
☐	3. Tor-netwerk	C	Verbinding routeren via een server in een ander land om geoblokkades te omzeilen.
☐	4. Webproxy	D	Uniek numeriek label dat een apparaatinterface op internet identificeert.
☐	5. DNS-lek	E	Leidt browserverkeer om op de applicatielaag zonder systeemversleuteling.
☐	6. WebRTC-API	F	Het loggen van de bestemmingen van onversleuteld internetverkeer door je telecomprovider.
☐	7. Locatie verbergen	G	Query's die buiten de VPN-tunnel worden opgelost, waardoor bezochte domeinen zichtbaar worden voor de ISP.
☐	8. Tracking door de internetprovider	H	Browserfunctie voor spraak en video die tunnels kan omzeilen en echte IP-adressen kan onthullen.

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

2. Leidt browserverkeer om op applicatieniveau zonder systeemversleuteling (8)

4. Het loggen van de bestemmingen van onversleuteld internetverkeer door je telecomaanbieder (11)

6. Query's die buiten de VPN-tunnel worden omgezet, waardoor bezochte domeinen aan de provider worden getoond (6)

7. Verbinding via een server in een ander land leiden om geoblokkades te omzeilen (9)

VERTICAAL

1. Browserfunctie voor spraak en video die tunnels kan omzeilen en echte IP-adressen kan blootleggen (9)

3. Versleutelt al het verkeer van een apparaat en leidt het via een VPN-server (9)

4. Uniek numeriek label dat een apparaatinterface op internet identificeert (7)

5. Leidt data via drie vrijwilligersservers en versleutelt bij elke stap een laag (10)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

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

HORIZONTAAL

2 horizontaal: Leidt browserverkeer om op applicatieniveau zonder systeemversleuteling (8 letters):

4 horizontaal: Het loggen van de bestemmingen van onversleuteld internetverkeer door je telecomaanbieder (11 letters):

6 horizontaal: Query's die buiten de VPN-tunnel worden omgezet, waardoor bezochte domeinen aan de provider worden getoond (6 letters):

7 horizontaal: Verbinding via een server in een ander land leiden om geoblokkades te omzeilen (9 letters):

VERTICAAL

1 verticaal: Browserfunctie voor spraak en video die tunnels kan omzeilen en echte IP-adressen kan blootleggen (9 letters):

3 verticaal: Versleutelt al het verkeer van een apparaat en leidt het via een VPN-server (9 letters):

4 verticaal: Uniek numeriek label dat een apparaatinterface op internet identificeert (7 letters):

5 verticaal: Leidt data via drie vrijwilligersservers en versleutelt bij elke stap een laag (10 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.

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

WOORDENLIJST

IPADRES VPNTUNNEL TORNETWERK WEBPROXY DNSLEK WEBRTCAPI MASKERING ISPTRACKING

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. IPADRES**
- **B. VPNTUNNEL**
- **C. TORNETWERK**
- **D. WEBPROXY**
- **E. DNSLEK**
- **F. WEBRTCAPI**
- **G. MASKERING**
- **H. ISPTRACKING**

DEFINITIES EN KOPPELVELDEN

1. Leidt browserverkeer om op applicatieniveau zonder systeemversleuteling.
2. Verbinding via een server in een ander land leiden om geoblokkades te omzeilen.
3. Browserfunctie voor spraak en video die tunnels kan omzeilen en echte IP-adressen kan blootleggen.
4. Uniek numeriek label dat een apparaatinterface op internet identificeert.
5. Leidt data via drie vrijwilligersservers en versleutelt bij elke stap een laag.
6. Het loggen van de bestemmingen van onversleuteld internetverkeer door je telecomaanbieder.
7. Query's die buiten de VPN-tunnel worden omgezet, waardoor bezochte domeinen aan de provider worden getoond.
8. Versleutelt al het verkeer van een apparaat en leidt het via een VPN-server.

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. **DEIRSAP** _____
2. **RNTOEKWETR** _____
3. **DSLKEN** _____
4. **EGNKIRMAS** _____
5. **NUPLNTVEN** _____
6. **XYPOWREB** _____
7. **CWPIARETB** _____
8. **ICGAPIRSNKT** _____

Bonusopdracht: Snel denken

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

1	Redenen om een VPN te gebruiken tijdens het reizen			
2	Browsers die je kent			
3	Dingen die een VPN kan verbergen			
4	Woorden die met privacy te maken hebben			
5	Woorden uit dit werkblad die je wilt onthouden			
6	Dingen die een website uit je IP-adres kan afleiden			
7	Cijfers of tekens in een IP-adres			
8	Mythes over VPN's			
9	VPN-diensten die je kent			
10	Dingen die je internetprovider kan zien			
11	Beloften van een goede VPN-aanbieder			
12	Dingen die je echte IP-adres kunnen lekken			
13	Redenen om je locatie te verbergen			
14	Manieren om je IP-adres te verbergen			
15	Apparaten die een VPN kunnen gebruiken			

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 IP-verhulling af te ronden dit geheime bericht over het verbergen van je digitale sporen.

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 2 5 18 7 10 5 1 4 18 5 19 13 5 20

5 5 14 22 5 18 2 15 18 7 5 14 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: Verbergt een webproxy mijn IP-adres?

Ja, maar alleen voor verkeer dat er doorheen wordt gestuurd, meestal je browser. De meeste webproxy's versleutelen je gegevens niet, dus je internetprovider of de netwerkbeheerder kan nog steeds zien wat je verstuurt en ontvangt.

Q5: Is het legaal om mijn IP-adres te verbergen?

In veel landen wel, maar sommige beperken of verbieden VPN's en andere hulpmiddelen om een IP-adres te verbergen. Je IP-adres verbergen maakt een illegale handeling nooit legaal, dus controleer de lokale wetgeving voordat je er een gebruikt.

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: Verbergt Tor mijn IP-adres?

Ja. Tor stuurt je verkeer via drie vrijwilligersrelays (guard, middle en exit), zodat websites het adres van het exitrelay zien en geen enkel relay zowel weet wie je bent als waar je naartoe gaat. [1]

Q7: Wat onthult mijn IP-adres?

Je openbare IP-adres onthult meestal je internetprovider en een benaderde locatie, zoals je land of stad. Sites kunnen het ook gebruiken om je bezoeken aan elkaar te koppelen en geoblokkades toe te passen.

Q8: Hoe controleer ik dat het verborgen is?

Maak verbinding met je VPN, ga naar een site die je IP-adres controleert en voer DNS- en WebRTC-lektests uit. Het IP-adres en de DNS-servers die worden getoond, moeten van de VPN zijn, niet van je isp. Als je echte IP-adres verschijnt, schakel dan lekbescherming in.

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: Waarom kunnen websites me nog volgen nadat ik mijn IP-adres heb verborgen?

Je IP-adres verbergen stopt browserfingerprinting niet. Trackers kunnen details zoals je schermresolutie, geïnstalleerde lettertypen en browserinstellingen combineren tot een identificator, en ook cookies of ingelogde accounts kunnen je identificeren, dus gebruik ook een browser die gericht is op privacy. [3]

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: Kan IPv6-verkeer mijn echte IP-adres lekken?

Ja, als je VPN alleen IPv4 tunnelt. Je apparaat kan dan IPv6-verkeer buiten de tunnel versturen, waarbij een door je internetprovider toegewezen adres wordt blootgegeven. Gebruik een VPN die IPv6 tunnelt of blokkeert en controleer dat met een IPv6-lektest.

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: Maakt split tunneling mijn echte IP-adres zichtbaar?

Ja, voor de apps die je uitsluit. Verkeer dat buiten de tunnel wordt verstuurd, gebruikt je echte IP-adres, en volgens RFC 8828 kan WebRTC het ISP-adres onthullen onder een VPN met split tunneling, tenzij de browser dit beperkt. [2]

Q7: Wat is een gedeeld IP-adres en hoe helpt het de privacy?

Bij een gedeeld IP-adres lijken veel VPN-gebruikers tegelijkertijd online met hetzelfde adres. Dat maakt het voor een website veel moeilijker om één bezoek aan jou te koppelen dan bij een dedicated IP-adres dat alleen jij gebruikt.

Q8: Kan mijn ISP zien dat ik een VPN gebruik om mijn IP-adres te verbergen?

Meestal wel. Je internetprovider kan zien dat je verbinding maakt met het IP-adres van een VPN-server, wanneer je verbinding maakt en hoeveel gegevens je verstuurt, maar niet welke websites je bezoekt of wat er in de versleutelde tunnel zit.

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: Is een proxy of een VPN beter om mijn IP-adres te verbergen?

Een VPN is meestal beter. Hij verbergt je IP-adres voor elke app op het apparaat en versleutelt het verkeer, terwijl een webproxy doorgaans alleen de browser dekt en vaak geen versleuteling toevoegt.

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.

2. VINGERAFDRUKKEN MAKEN

Je IP-adres verbergen stopt browserfingerprinting niet, waarmee je kunt worden geïdentificeerd aan de hand van details zoals je schermresolutie en geïnstalleerde lettertypen. [3]

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.

4. BLOOTSTELLING VAN HET ADRES VIA WEBRTC

RFC 8828 waarschuwt dat WebRTC zowel het openbare adres van een VPN als het ISP-adres waarover de VPN loopt kan achterhalen, tenzij de browser dit beperkt. [2]

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. HERGEBRUIK VAN TOR-CIRCUITS

Tor gebruikt hetzelfde circuit ongeveer tien minuten en bouwt dan een nieuw circuit, waardoor je browse-activiteit moeilijker aan elkaar te koppelen is. [1]

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. [1]

10. PROXY'S VERSUS VPN-TUNNELS

Een webproxy wijzigt het IP-adres dat een site ziet voor je browserverkeer, maar versleutelt dat verkeer in tegenstelling tot een VPN meestal niet en dekt ook geen andere apps op je apparaat. [5]

Technische referenties en bronnen

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

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[1] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] 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

Antwoordsleutel: IP-adressen verbergen, locatie maskeren, proxy, Tor en DNS-/WebRTC-lekken voorkomen

1 Vraag 1

Juist antwoord: B

DOCENTENNOTITIE

Wat onthult het openbare IP-adres van een apparaat aan websites die je bezoekt? → Je ongeveer locatie en de naam van je internetprovider

2 VPN-systeemversleuteling LATENTIE

Juist antwoord: C

DOCENTENNOTITIE

In tegenstelling tot proxy's, die alleen browserverkeer omleiden, maakt een VPN een systeembrede versleutelde tunnel die achtergrondapplicaties, games en OS-verzoeken beveiligt. Bron: Tor Project Relays, W3C WebRTC API.

3 Ontbrekende proxyversleuteling WIFI-BEVEILIGING

Juist antwoord: A

DOCENTENNOTITIE

Webproxy's sturen alleen browserverkeer door zonder de payload van pakketten te versleutelen, waardoor je netwerkbeheerder of provider je inhoudsverkeer nog steeds kan traceren. Bron: IETF Proxy Vulnerabilities.

4 Vraag 4

Juist antwoord: B

DOCENTENNOTITIE

Hoe biedt het Tor-netwerk gebruikers een hoge mate van anonimiteit? → Door verkeer te routeren via drie relays die door vrijwilligers worden beheerd

5 DNS-tunnellekken PRIVACY

Juist antwoord: B

DOCENTENNOTITIE

Een DNS-lek treedt op wanneer aanvragen voor domeinnaamresolutie de VPN-tunnel omzeilen en rechtstreeks naar de resolvers van je internetprovider gaan, waardoor bezochte domeinen zichtbaar worden. Bron: DNSSEC Tunnel Testing, EFF Tracking Evasion.

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Details over proxybeperkingen** IP-MASKERING — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Proxy's werken op de toepassingslaag en missen de systeembrede integratie met netwerkdrivers die een VPN-tunnel heeft. Bron: IETF Proxy Vulnerabilities.

7 **Vraag 7** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Verkeer doorsturen via drie relays van vrijwilligers met gelaagde versleuteling voegt latentie toe, dus Tor is meestal trager dan een directe verbinding.

8 **Vraag 8** — **Juist antwoord: Waar**

DOCENTENNOTITIE

WebRTC kan lokale adressen onthullen en, bij sommige VPN-opstellingen, het door de internetprovider toegewezen openbare IP-adres onder de tunnel (RFC 8828).

9 **Vraag 9** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Zonder DNS- of WebRTC-lekken ziet de internetprovider alleen versleuteld verkeer naar de VPN-server, niet de sites die je bezoekt.

10 **Grenzen van fingerprinting** NO-LOGS — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Fingerprinting richt zich op configuratiegegevens van het apparaat (schermresolutie, lettertypen, plug-ins) die zichtbaar blijven, zelfs wanneer het IP-adres is verborgen. Bronvermelding: EFF Tracking Evasion.

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

D 1. IP-adres	A 2. VPN-tunnel	B 3. Tor-netwerk	E 4. Webproxy
G 5. DNS-lek	H 6. WebRTC-API	C 7. Locatie verbergen	F 8. Tracking door de internetprovider

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 DNS-LEK	2 WEBRTC	3 WEBPROXY	4 TOR-NETWERK
5 IP-ADRES	6 MASKERING		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 D – WEBPROXY	2 G – MASKERING	3 F – WEBRTCAPI	4 A – IPADRES
5 C – TORNETWERK	6 H – ISPTRACKING	7 E – DNSLEK	8 B – VPNTUNNEL

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen IP-adres, VPN-tunnel en Tor-netwerk 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.

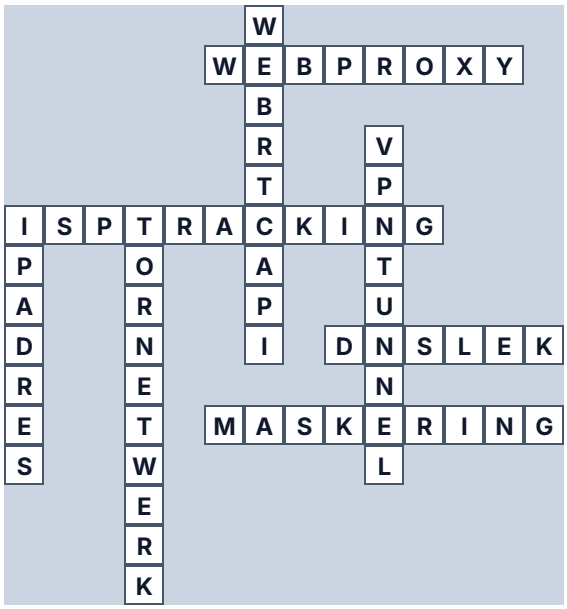
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

2 horizontaal: WEBPROXY Leidt browserverkeer om op applicatieniveau zonder systeemversleuteling (8 letters)

4 horizontaal: ISPTRACKING Het loggen van de bestemmingen van onversleuteld internetverkeer door je telecomaanbieder (11 letters)

6 horizontaal: DNSLEK Query's die buiten de VPN-tunnel worden omgezet, waardoor bezochte domeinen aan de provider worden getoond (6 letters)

7 horizontaal: MASKERING Verbinding via een server in een ander land leiden om geoblokkades te omzeilen (9 letters)

VERTICAAL

1 verticaal: WEBRTCAPI Browserfunctie voor spraak en video die tunnels kan omzeilen en echte IP-adressen kan blootleggen (9 letters)

3 verticaal: VPNTUNNEL Versleutelt al het verkeer van een apparaat en leidt het via een VPN-server (9 letters)

4 verticaal: IPADRES Uniek numeriek label dat een apparaatinterface op internet identificeert (7 letters)

5 verticaal: TORNETWERK Leidt data via drie vrijwilligersservers en versleutelt bij elke stap een laag (10 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. DEIRSAP — **IPADRES**
2. RNTOEKWETR — **TORNETWERK**
3. DSLKEN — **DNSLEK**
4. EGNKIRMAS — **MASKERING**
5. NUPLNTVEN — **VPNTUNNEL**
6. XYPOWREB — **WEBPROXY**
7. CWPIARETB — **WEBRTCAPI**
8. ICGAPIRSNKT — **ISPTRACKING**

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"VERBERG JE ADRES MET EEN VERBORGEN 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.